MASTER'S THESIS

Jordan Blocks of Unipotent Elements in Spin Groups

Robin Ammon

Supervisor:
Prof. Dr. Gunter Malle

TU KAISERSLAUTERN
DEPARTMENT OF MATHEMATICS

July 2020

Contents

Introduction

The main objective of this thesis is to determine the Jordan blocks of the images of the unipotent elements of the spin groups under the spin and half-spin representations over an algebraically closed field of good characteristic, that is, of characteristic different from 2. It is motivated by the work of Lawther who in his paper [Law95] has calculated the Jordan block sizes of unipotent elements in exceptional algebraic groups. Similar studies have been made by Korhonen [Kor19] for certain representations of special linear, symplectic and special orthogonal groups.

The first part of this thesis is about introducing the objects of interest and investigating some of their properties. In the context of algebraic groups, the spin groups may be defined to be the simply connected simple algebraic groups of types B_m and D_m. In this work, using the theory of Clifford algebras, we construct the spin groups first as abstract groups associated with a quadratic form over an arbitrary field. Our aim is then to show that over algebraically closed fields, these groups are indeed algebraic groups and fit into the right place in the classification. Afterwards, we define the representations of the spin groups that we are interested in, the spin and half-spin representations.

Having introduced the key objects, in the rest of the thesis we are working towards the computation of the Jordan blocks of unipotent elements. Combining methods from representation theory with statements on the structure of Clifford algebras, we obtain results on the behaviour of restrictions of spin representations that lay the foundations for our later computations. To deal with special kinds of unipotent conjugacy classes and in particular regular unipotent elements, these results are complemented with a geometric approach that involves calculations with root subgroups and which is inspired by [Law95].

We present an algorithm that – mostly recursively – for any given dimension computes the Jordan blocks of the unipotent elements of the spin group under the spin and half-spin representations in a given characteristic different from 2 and which has been implemented in the computer algebra system `GAP`. Based on our algorithmic approach, we prove that for every dimension there exists a bound such that in all characteristics greater than this bound, the blocks of the unipotent elements in the given dimension are the same as those in characteristic 0. Moreover, we give some constraints that the Jordan blocks of the unipotent elements have to fulfill in certain dimensions.

In detail, this thesis is structured as follows: In the first two chapters, we collect results from the theories of algebras, bilinear forms and quadratic forms to provide the theoretical background on which the rest of the thesis is being built up. Chapter 1 is mostly concerned with finite-dimensional algebras over an arbitrary field and besides some constructions of special kinds of algebras associated to a vector space contains the results on representations of algebras and graded algebras that will be needed afterwards. In Chapter 2 we then introduce the necessary notions and constructions from the theory of bilinear forms and quadratic forms.

We proceed in Chapter 3 with defining and investigating Clifford algebras. Since this material will be used in many places, we go into more detail and in particular analyze the algebra structure of Clifford algebras. Moreover, we construct the spin groups for quadratic forms whose associated bilinear form is nondegenerate as subgroups of the units of Clifford algebras.

In Chapter 4 we show that the spin groups are algebraic groups and investigate their properties in more detail; in particular, we determine their root system and root subgroups. For this, we first give an introduction to the theory of algebraic groups and state those results that will be needed for our purposes. Furthermore, we take a closer look at special orthogonal groups and their properties because they are closely related to the spin groups.

The spin and half-spin representations are introduced in Chapter 5. They are constructed and analyzed with the aid of the results from Chapters 3 and 4. We pay particular attention to the question in which way (products of) lower-dimensional spin groups are contained in higher-dimensional ones and to how the spin representations behave when restricted to such lower-dimensional spin groups.

Chapter 6 is about conjugacy classes in algebraic groups. Most importantly, we describe the conjugacy classes of unipotent elements of spin groups by using information on the conjugacy classes of unipotent elements of special orthogonal groups. Complementing this approach with our knowledge on the root subgroups, we give representatives for each unipotent class of the spin group.

In Chapter 7 we finally combine the results from chapters three to six in an algorithm that for any given dimension computes the Jordan blocks of the images of the unipotent elements of the spin group under the spin and half-spin representations in a given characteristic different from 2. We investigate and explain some of the obtained computational results and from our algorithmic approach derive statements on the dependence of the Jordan blocks of the unipotent elements on the characteristic of the underlying field.

The Appendix contains the implementation of our algorithm in `GAP` that has been used to obtain the computational results stated in Chapter 7.

In this thesis, we aim at providing a detailed account on how the spin groups and spin representations can be constructed and what their properties are. To this end, we collect and supplement results that are scattered around many textbooks. Whenever possible, we try to give examples and try to illustrate how our specific constructions relate to the general theory of algebraic groups. The leading focus remains the determination of the Jordan blocks of unipotent elements of spin groups under the spin and half-spin representations which requires our detailed analysis of the involved objects. Besides the descriptions of the restrictions of spin representations, the main result of this thesis is the algorithm in Section 7.1 that solves the problem of determining the Jordan blocks in question.

We assume basic knowledge of linear algebra, group theory, topology and commutative algebra. At the beginning of each section, we state the assumptions under which we work and give the references on which the section is based. If there is some reference that particularly refers to a single result, we indicate this before the respective statement.

Conventions. Throughout this thesis, k denotes a field. We will specify further properties of k at the beginning of each chapter, if applicable. We say that k is *quadratically closed* if every univariate quadratic polynomial over k has a root in k and we say that k is *algebraically closed* if every non-constant univariate polynomial over k has a root in k. The symbol $\mathbb{N}$ denotes the natural numbers including 0. We use the notation $\mathbb{Z}_2 := \mathbb{Z}/2\mathbb{Z}$. By $\mathrm{Mat}_n(k)$ we denote the k-algebra of $(n \times n)$-matrices with entries in k and by $\mathrm{GL}_n(k)$ or just GL_n the group of invertible $(n \times n)$-matrices over k. We frequently omit zeros in matrices; empty spaces will symbolize an appropriate number of zeros. For brevity, we write 0 for the trivial vector space and 1 for the trivial group.

1 Algebras

In this chapter, we collect all results concerning algebras that will be needed for our later investigations. After an introductory section, we proceed by introducing the necessary tools from the representation theory of finite-dimensional algebras. The third section is concerned with graded algebras while in the remaining two sections we construct and study two important examples of such algebras, namely the tensor algebra and the exterior algebra.

All results from this chapter are well-known and we refer the reader to the books mentioned at the beginning of each section for more background and details.

1.1 Basic Definitions and Notation

We quickly recapitulate the basic notions from the theory of algebras over k and introduce some notation. See for example [Bou74], Sections III.1.1, III.1.2 and III.1.4 for the material that is discussed in this section.

Definition 1.1. An *algebra over* k or k-*algebra* is a k-vector space A together with a k-bilinear map $A \times A \to A$, $(x, y) \mapsto xy$, called the *multiplication* of A. A k-algebra is called *associative* if the multiplication is associative and is called *unital* if multiplication admits an identity element (usually written 1 or 1_A).

In the following, if not explicitly stated otherwise, by a k-algebra we will always mean an associative k-algebra with unit element 1. Thus, a k-algebra has the structure of a ring. A *homomorphism* of k-algebras (or simply algebra homomorphism) is a k-linear map that is compatible with multiplication and maps identity element to identity element (i.e., it is a ring homomorphism which is linear). We have the usual notions of *subalgebra*, *ideal* and *quotient algebra*, where by an ideal we shall always mean a two-sided ideal. If $S \subseteq A$ is a subset of the k-algebra A, then we write $\langle S \rangle_{k\text{-alg.}}$ to denote the subalgebra of A that is generated by S.

If A is a k-algebra, then we will identify k with the subalgebra $\{\, c \cdot 1 \mid c \in k \,\}$ of A. We therefore simply write c for the element $c \cdot 1$ of A. We denote by

$$A^\times := \{\, x \in A \mid \text{there exists } y \in A \text{ with } xy = yx = 1 \,\}$$

the group of units of A and by

$$Z(A) := \{\, x \in A \mid xy = yx \text{ for all } y \in A \,\}$$

the centre of A. Note that we always have $k \subseteq Z(A)$ and that $Z(A)$ is a subalgebra of A.

The *opposite algebra* A^{op} of A is the k-vector space A with multiplication given by $x \cdot y := yx$ (reversing the multiplication of A). One easily sees that this is again a k-algebra. If B is another k-algebra, then an *antihomomorphism* between A and B is an algebra homomorphism $t\colon A \to B^{\mathrm{op}}$. In other words, it is a k-linear map $t\colon A \to B$ satisfying $t(1_A) = 1_B$ and $t(xy) = t(y)t(x)$ for all $x, y \in A$.

Example 1.2. Two very important examples of k-algebras are the endomorphism algebra $\mathrm{End}(V)$ of a k-vector space V and the matrix algebra $\mathrm{Mat}_n(k)$ over k. If V is of finite dimension n and $\mathcal{B} = (v_1, \dots, v_n)$ is a basis of V, then we denote by

$$[\cdot]_{\mathcal{B}}\colon \mathrm{End}(V) \xrightarrow{\sim} \mathrm{Mat}_n(k),\ f \mapsto [f]_{\mathcal{B}},$$

the algebra isomorphism that sends an endomorphism to its matrix with respect to $\mathcal{B}$. We write $c_{\mathcal{B}}\colon V \to k^n$ for the coordinate map associated with $\mathcal{B}$, which sends $\sum_{i=1}^n a_i v_i$ to $(a_1, \dots, a_n)$ and satisfies

$$[f]_{\mathcal{B}} x = (c_{\mathcal{B}} \circ f \circ c_{\mathcal{B}}^{-1})(x) \qquad \text{for } f \in \mathrm{End}(V) \text{ and } x \in k^n. \tag{1.1}$$

Of further interest in this context are the matrices $E_{ij} := (\delta_{ri}\delta_{sj})_{r,s} \in \mathrm{Mat}_n(k)$ for $i, j \in \{1, \dots, n\}$ which form a basis of $\mathrm{Mat}_n(k)$. If $M = (m_{rs})_{r,s} \in \mathrm{Mat}_n(k)$, then it holds that

$$E_{ij} M = \sum_{t=1}^n m_{jt} E_{it}, \qquad M E_{ij} = \sum_{t=1}^n m_{ti} E_{tj}. \tag{1.2}$$

In particular, we have $E_{ij} E_{lm} = \delta_{jl} E_{im}$.

We continue with introducing basic terminology.

Definition 1.3. Let A be a k-algebra.

(a) A is called *simple* if the only ideals of A are $\{0\}$ and A.

(b) A is said to be a *central simple k-algebra* if A is simple and satisfies $Z(A) = k$.

An important example of a central simple k-algebra is the endomorphism algebra:

Lemma 1.4. *Let V be a finite-dimensional k-vector space. Then the endomorphism algebra* $\mathrm{End}(V)$ *is a central simple k-algebra.*

Proof. We may equivalently show that $\mathrm{Mat}_n(k)$ is a central simple k-algebra for $n \in \mathbb{N}$. Let $0 \neq I \trianglelefteq \mathrm{Mat}_n(k)$ be a nonzero ideal and let $0 \neq M = (m_{rs})_{r,s} \in I$. Then M has a nonzero entry, say $m_{pq} \neq 0$. For arbitrary $i, j \in \{1, \dots, n\}$ we have $E_{ip} M E_{qj} = m_{pq} E_{ij} \in I$ by (1.2). But the E_{ij} form a basis of $\mathrm{Mat}_n(k)$, so $I = \mathrm{Mat}_n(k)$, showing that $\mathrm{Mat}_n(k)$ is simple. The statement for the centre follows easily from (1.2) as well. □

We next take a look at some constructions. First, consider two k-vector spaces V and W. We may then form the direct sum $V \oplus W$ and the tensor product $V \otimes W$. For linear maps and matrices we make the following related definitions:

Definition 1.5.

(a) If $f\colon V \to V'$ and $g\colon W \to W'$ are linear maps of k-vector spaces, then we define

$$\begin{aligned} f \oplus g &\colon V \oplus W \to V' \oplus W',\ (v, w) \mapsto (f(v), g(w)),\\ f \otimes g &\colon V \otimes W \to V' \otimes W',\ v \otimes w \mapsto f(v) \otimes g(w), \end{aligned}$$

which are again linear.

(b) For matrices $M \in \mathrm{Mat}_n(k)$ and $N \in \mathrm{Mat}_l(k)$ we put

$$M \oplus N := \begin{pmatrix} M & 0 \\ 0 & N \end{pmatrix} \in \mathrm{Mat}_{n+l}(k)$$

and

$$M \otimes N := \begin{pmatrix} m_{11}N & \cdots & m_{1n}N \\ \vdots & \ddots & \vdots \\ m_{n1}N & \cdots & m_{nn}N \end{pmatrix} \in \mathrm{Mat}_{nl}(k)$$

where $M = (m_{rs})_{r,s}$. The matrix $M \otimes N$ is called the *Kronecker product* of M and N.

Thus, if V and W are finite-dimensional with bases $\mathcal{B}$ and $\mathcal{C}$, respectively, and if $f \in \mathrm{End}(V)$ and $g \in \mathrm{End}(W)$, then $[f]_{\mathcal{B}} \oplus [g]_{\mathcal{C}}$ is the matrix of $f \oplus g$ w.r.t. the natural basis of $V \oplus W$ that is induced by $\mathcal{B}$ and $\mathcal{C}$, and $[f]_{\mathcal{B}} \otimes [g]_{\mathcal{C}}$ is the matrix of $f \otimes g$ w.r.t. the natural basis (in lexicographic order) of $V \otimes W$ coming from $\mathcal{B}$ and $\mathcal{C}$ (see also [NT89], Exercise 3.1.13).

The above constructions generalize to k-algebras, as follows: If A and B are k-algebras, then putting $(x, y) \cdot (x', y') := (xx', yy')$ and $(x \otimes y) \cdot (x' \otimes y') := xx' \otimes yy'$ for $x, x' \in A$ and $y, y' \in B$ make $A \oplus B$ and $A \otimes B$ into k-algebras. It follows that if $\varphi\colon A \to A'$ and $\psi\colon B \to B'$ are homomorphisms of k-algebras, then so are $\varphi \oplus \psi$ and $\varphi \otimes \psi$.

We have the following result regarding the endomorphism algebra:

Proposition 1.6. *Let V and W be finite-dimensional k-vector spaces.*

(i) The map

$$\mathrm{End}(V) \oplus \mathrm{End}(W) \to \mathrm{End}(V \oplus W),\ (f, g) \mapsto f \oplus g$$

is an injective algebra homomorphism.

(ii) The map

$$\mathrm{End}(V) \otimes \mathrm{End}(W) \to \mathrm{End}(V \otimes W),\ f \otimes g \mapsto f \otimes g,$$

where the right hand map is the one from Definition 1.5 (a), is an isomorphism of k-algebras.

Proof.

(i) It can easily be seen that the map is an algebra homomorphism. For injectivity, let $(f, g) \in \mathrm{End}(V) \oplus \mathrm{End}(W)$ such that $f \oplus g = 0$. Then for all $v \in V$ we have $0 = (f \oplus g)(v, 0) = (f(v), 0)$, giving $f = 0$. Analogously, one shows that $g = 0$.

(ii) Since $\mathrm{End}(V) \times \mathrm{End}(W) \to \mathrm{End}(V \otimes W)$, $(f, g) \mapsto f \otimes g$ is bilinear, the given map is well-defined and k-linear. Using the definition of multiplication in the tensor product, it is readily checked to be an algebra homomorphism. As discussed above, by choosing suitable bases, this map can be thought of as sending the matrices of f and g to their Kronecker product. But the matrices $E_{ij} \otimes E_{lm}$ form a basis of the target space and are contained in the image of the algebra homomorphism, so it must be surjective. Comparing dimensions shows that it is an isomorphism. □

1.2 Representations of Algebras

In this section, we introduce some fundamental terminology from representation theory. Furthermore, we state all results from this area that will later be needed in the construction and investigation of spin representations in Chapter 5.

All definitions and results are covered in the books [NT89] and [Jac89]. We further refer to the shorter expositions in [Nav98] and [Isa76] that also contain most of the material.

Definition 1.7. Let A be a finite-dimensional k-algebra.

(a) A *representation* of A is an algebra homomorphism $\rho\colon A \to \mathrm{End}(V)$ into the endomorphism algebra of some finite-dimensional k-vector space V. A *matrix representation* of A is an algebra homomorphism $A \to \mathrm{Mat}_n(k)$ for some $n \in \mathbb{N}$. The number $\dim V$ respectively n is called the *dimension* of the representation.

(b) An *A-module* is a finite-dimensional k-vector space V together with a k-bilinear map $A \times V \to V$, $(x, v) \mapsto x.v$ that satisfies $1_A.v = v$ for all $v \in V$.

The notions representation of A and A-module are equivalent in the sense that to every representation one may associate an A-module and vice versa, such that these maps are inverse to each other. Indeed, if $\rho\colon A \to \mathrm{End}(V)$ is a representation of A, then putting $x.v := \rho(x)(v)$ makes V into an A-module. Conversely, if V is an A-module, then we may define a representation $\rho\colon A \to \mathrm{End}(V)$ by $\rho(x)\colon V \to V$, $v \mapsto x.v$ for $x \in A$. One checks that these assignments are inverse to each other.

Hence, in order to study representations one may as well study modules. Note also that by choosing a basis one may go from a representation to a matrix representation and vice versa. For our purposes, it is more suitable to work with representations. For a more theoretic approach however, it is often more convenient to work with modules, as is done in the given sources. So we will respect both approaches, but state most results for representations.

We now collect some basic notions from the representation theory of algebras. So let A be a finite-dimensional k-algebra. Two representations $\rho\colon A \to \operatorname{End}(V)$ and $\sigma\colon A \to \operatorname{End}(W)$ of A are called *equivalent* if there is a linear isomorphism $f\colon V \to W$ such that $f \circ \rho(x) = \sigma(x) \circ f$ for all $x \in A$. We then write $\rho \cong \sigma$. In the realm of modules this translates into the statement that V and W are isomorphic as A-modules, via f.

$$\begin{tikzcd} V \arrow[r, "\rho(x)"] \arrow[d, "f"'] & V \arrow[d, "f"] \\ W \arrow[r, "\sigma(x)"'] & W \end{tikzcd}$$

A representation $\rho\colon A \to \operatorname{End}(V)$ is said to be *irreducible* if V has no A-invariant subspaces other than 0 and V, where $W \leq V$ is *A-invariant* if $\rho(x)(W) \subseteq W$ for all $x \in A$. Equivalently, the A-module V does not have a nontrivial submodule, i.e., it is a simple A-module. Finally, ρ is called *faithful* if it is injective. For the A-module V this corresponds to saying that the annihilator $\operatorname{ann}(V) := \{\, x \in A \mid x.v = 0 \text{ for all } v \in V \,\}$ is zero. Note that every nontrivial representation of a simple algebra is necessarily faithful.

Example 1.8. Let V and W be finite-dimensional k-vector spaces.

(a) Consider the k-algebra $A := \operatorname{End}(V)$. Then the representation $\operatorname{id}_A\colon \operatorname{End}(V) \to \operatorname{End}(V)$ is irreducible: Suppose that $0 \neq U \leq V$ is an A-invariant subspace and let $0 \neq u \in U$. Pick any basis $(v_1, \dots, v_n)$ of V. Since u is non-zero, there exist $f_i \in \operatorname{End}(V)$ such that $f_i(u) = v_i$ for $i = 1, \dots, n$. But then as U is A-invariant, we have $v_i = f_i(u) \in U$ for all i, giving $U = V$. Note further that id_A is clearly faithful.

(b) Suppose that $V, W \neq 0$ and let $A := \operatorname{End}(V) \oplus \operatorname{End}(W)$. Consider the representations $\pi_V\colon A \to \operatorname{End}(V)$ and $\pi_W\colon A \to \operatorname{End}(W)$ that are given by the projections. We claim that π_V and π_W are irreducible and inequivalent representations of A. Arguing as in (a), they are clearly irreducible. Now assume that there is a vector space isomorphism $f\colon V \to W$ with

$$f \circ g = f \circ \pi_V(g,h) = \pi_W(g,h) \circ f = h \circ f$$

for all $(g,h) \in \operatorname{End}(V) \oplus \operatorname{End}(W)$. Picking $g = \operatorname{id}_V$, we get $f = h \circ f$ for all $h \in \operatorname{End}(W)$ and therefore $\operatorname{End}(W) = \{\operatorname{id}_W\}$, which is a contradiction. So π_V and π_W are inequivalent. Note that both representations are not faithful.

Part (a) of the above example in particular shows that surjective representations are irreducible. The converse holds if k is algebraically closed:

Theorem 1.9 (Burnside's Theorem)**.** *Suppose that k is algebraically closed. Let A be a finite-dimensional k-algebra and let $\rho\colon A \to \operatorname{End}(V)$ be an irreducible representation of A. Then ρ is surjective.*

Proof. See [Jac89], page 213 or [Nav98], Theorem 1.19. □

We take a look at two methods to obtain new representations from given ones.

Definition 1.10. Let A and B be finite-dimensional k-algebras.

(a) Let $\rho\colon A \to \mathrm{End}(V)$ and $\sigma\colon B \to \mathrm{End}(W)$ be representations. Using the maps from Proposition 1.6, we define the *direct sum* of ρ and σ to be

$$\rho \oplus \sigma\colon A \oplus B \to \mathrm{End}(V \oplus W),\ (x, y) \mapsto \rho(x) \oplus \sigma(y),$$

and the *tensor product* of ρ and σ to be

$$\rho \otimes \sigma\colon A \otimes B \to \mathrm{End}(V \otimes W),\ x \otimes y \mapsto \rho(x) \otimes \sigma(y)$$

(which is a slight abuse of notation but which is justified by the fact that the maps in Proposition 1.6 are injective).

(b) Using concatenation of the above constructed maps with the algebra homomorphisms $A \to A \oplus A$, $x \mapsto (x, x)$ respectively $A \to A \otimes A$, $x \mapsto x \otimes x$, one defines the direct sum and the tensor product of two representations of A, which are then again representations of A.

Of course, these constructions correspond to the module theoretic constructions of direct sum and tensor product.

We now turn to the question how many irreducible representations an algebra can have, up to equivalence. For this, we need to introduce some more notions.

Definition 1.11. Let A be a finite-dimensional k-algebra.

(a) The *Jacobson radical* of A is

$$J(A) := \bigcap_{\substack{V \text{simple} \\ A\text{-module}}} \mathrm{ann}(V) = \bigcap_{\substack{\rho \text{ irreducible} \\ \text{repres. of } A}} \ker \rho.$$

(b) The algebra A is called *semisimple* if $J(A) = 0$.

Thus, by Example 1.8 (a), $\mathrm{End}(V)$ is clearly semisimple. More generally, since $J(A) \trianglelefteq A$ is a (two-sided) ideal, simple algebras are semisimple. Furthermore, Example 1.8 (b) shows that also $\mathrm{End}(V) \oplus \mathrm{End}(W)$ is semisimple, as are direct sums of simple algebras in general (see [NT89], Exercise 1.4.8).

Proposition 1.12. *Let A be a finite-dimensional k-algebra.*

(i) A is semisimple if and only if every representation of A is a direct sum of irreducible representations.

(ii) If V is a simple A-module, then putting $\overline{x}.v := x.v$ for $\overline{x} \in A/J(A)$ and $v \in V$ makes V into a simple $A/J(A)$-module. Conversely, if V is a simple $A/J(A)$-module, then putting $x.v := \overline{x}.v$ for $x \in A$ and $v \in V$ makes V into a simple A-module. In particular, A and $A/J(A)$ have the same simple modules and $A/J(A)$ is semisimple.

Proof. Statement (i) is part of Theorem 1.8.1 of [NT89]. For the second part cf. [Nav98], p. 5; it is an easy computation. ☐

Theorem 1.13. *Let A be a finite-dimensional k-algebra. Then A has only finitely many irreducible representations up to equivalence. If k is algebraically closed, then the number of irreducible representations of A is $\dim Z(A/J(A))$.*

Proof. By Proposition 1.12 (ii) we can assume that A is semisimple. Then the results can be found for example in [Isa76], Theorem 1.15 (d) and Corollary 1.17 (e) or [NT89], Theorems 1.8.6 and 2.3.14. ☐

In particular, a central simple algebra over an algebraically closed field has a unique irreducible representation (up to equivalence). We further obtain the following result which will be needed later.

Corollary 1.14. *Suppose k is algebraically closed. Let A and B be finite-dimensional central simple k-algebras, with unique irreducible representations $\rho\colon A \to \operatorname{End}(V)$ and $\sigma\colon B \to \operatorname{End}(W)$, respectively. Then $A \otimes B$ is also a central simple k-algebra, with unique irreducible representation $\rho \otimes \sigma$.*

Proof. By Theorem 1.9, ρ and σ are surjective, so Proposition 1.6 (ii) implies that the representation $\rho \otimes \sigma\colon A \otimes B \to \operatorname{End}(V \otimes W)$ is surjective as well. Then it is irreducible by Example 1.8 (a). Since A and B are simple, their representations in fact have to be isomorphisms. Counting dimensions, we infer that also $\rho \otimes \sigma$ is an isomorphism. It follows from Lemma 1.4 that $A \otimes B$ is central simple and from Theorem 1.13 that it has a unique irreducible representation which then must be $\rho \otimes \sigma$. ☐

For a more general version, see [NT89], Theorem 2.3.15. It can further be shown that the tensor product of central simple algebras is again central simple for any field k, see for example [NT89], Theorem 2.4.2 or [Lam05], Theorem IV.1.2.

1.3 Graded Algebras

Graded algebras will play a key role for studying Clifford algebras, spin groups and their representations. In this section, we develop some of their basic theory before specializing to certain kinds of graded algebras. We mainly follow [Che97], Sections I.2 and I.4 and [Bou74], Section III.3.

Throughout the section, M denotes a commutative monoid, written additively, with identity element 0.

Definition 1.15. A k-algebra A is called *M-graded* if there are k-subspaces $A_r \leq A$ for $r \in M$ such that

$$A = \bigoplus_{r \in M} A_r \text{ (as k-vector spaces)} \quad \text{and} \quad A_r \cdot A_s \subseteq A_{r+s} \quad \text{for all } r, s \in M.$$

In this case, A_r is called the *homogeneous part of degree* r of A and the elements of A_r are said to be *homogeneous of degree* r. By definition, any element $x \in A$ can uniquely be written as $x = \sum_{r \in M} x_r$ with $x_r \in A_r$, where only finitely many x_r are non-zero. The elements x_r are called the *homogeneous components* of x (*of degree* r).

A basic observation is the following:

Lemma 1.16. *Let A be an M-graded k-algebra. Then the multiplicative identity element* 1 *of A is homogeneous of degree* 0*. In particular, A_0 is a subalgebra of A which contains k.*

Proof. See [Che97], Lemma I.1.2. □

Example 1.17. The polynomial ring $A := k[X_1, \ldots, X_n]$ is an $\mathbb{N}$-graded k-algebra with homogeneous part of degree $r \in \mathbb{N}$ being the set of polynomials of total degree r. Here, the subalgebra A_0 comprises the constant polynomials, that is, we have $A_0 = k$.

We will see more examples for graded algebras in later sections, e.g. the tensor algebra (see Section 1.4), the exterior algebra (see Section 1.5) or the Clifford algebra (see Chapter 3).

The following remark shows that a grading on a k-algebra is by no means unique and that one grading may give rise to various related gradings:

Remark 1.18.

(a) Any k-algebra A is M-graded for any commutative monoid M: Putting $A_0 := A$ and $A_r := 0$ for $r \in M \setminus \{0\}$ clearly defines an M-grading on A, the *trivial grading*. This also shows that an M-grading on an algebra is not unique.

(b) Suppose that $A = \bigoplus_{r\in M} A_r$ is an M-graded k-algebra and that $\tau\colon M \to N$ is a homomorphism of commutative monoids. Then A is naturally N-graded by setting

$$A_s := \bigoplus_{r\in\tau^{-1}(s)} A_r \qquad \text{for } s \in N.$$

There are two important special cases of this:

An $\mathbb{N}$-graded k-algebra $A = \bigoplus_{r\in\mathbb{N}} A_r$ is naturally $\mathbb{Z}$-graded: Applying the above to the inclusion $\mathbb{N} \hookrightarrow \mathbb{Z}$ means that putting $A_r := 0$ for $r < 0$ extends the $\mathbb{N}$-grading of A to a $\mathbb{Z}$-grading. We sometimes implicitly consider $\mathbb{N}$-graded algebras as being $\mathbb{Z}$-graded this way.

A $\mathbb{Z}$-graded k-algebra $A = \bigoplus_{r\in\mathbb{Z}} A_r$ is naturally $\mathbb{Z}_2$-graded: Here, we consider the quotient map $\mathbb{Z} \to \mathbb{Z}_2$ and obtain that setting

$$A_{\bar{0}} := \bigoplus_{r \text{ even}} A_r, \qquad A_{\bar{1}} := \bigoplus_{r \text{ odd}} A_r$$

defines a $\mathbb{Z}_2$-grading on A. In particular, any $\mathbb{N}$-graded k-algebra may naturally be considered as a $\mathbb{Z}_2$-graded k-algebra.

We now develop some general theory before specializing to certain monoids. As usual when introducing a new structure, we first take a look at homomorphisms.

Definition 1.19. Let $A = \bigoplus_{r\in M} A_r$ and $B = \bigoplus_{r\in M} B_r$ be M-graded k-algebras. A k-algebra homomorphism $\varphi\colon A \to B$ is called *M-graded* if $\varphi(A_r) \subseteq B_r$ for all $r \in M$.

Note that such an M-graded algebra homomorphism $\varphi\colon A \to B$ by definition restricts to an algebra homomorphism $\varphi_0\colon A_0 \to B_0$ and linear maps $\varphi_r\colon A_r \to B_r$ for $r \in M$. If φ is an algebra isomorphism, then so is φ_0, and the φ_r are vector space isomorphisms (by considering the inverse of φ and its restrictions). Compositions of M-graded homomorphisms are again M-graded.

A related concept is that of homogeneous linear maps:

Definition 1.20. Let $A = \bigoplus_{r\in M} A_r$ and $B = \bigoplus_{r\in M} B_r$ be M-graded k-algebras and let $d \in M$. A linear map $f\colon A \to B$ is called *homogeneous of degree d* if $f(A_r) \subseteq B_{r+d}$ for all $r \in M$.

Thus, an M-graded algebra homomorphism $\varphi\colon A \to B$ is in particular homogeneous of degree 0. Note that if A, B and C are M-graded k-algebras and if $f\colon A \to B$ and $g\colon B \to C$ are homogeneous linear maps of degrees d and e, respectively, then $g \circ f\colon A \to C$ is homogeneous of degree $d + e$.

We next investigate ideals in the context of graded algebras.

Definition 1.21. An ideal I of an M-graded k-algebra is called *homogeneous* if the homogeneous components of any element of I again lie in I.

This notion can be characterized as follows:

Proposition 1.22. *Let $A = \bigoplus_{r \in M} A_r$ be an M-graded k-algebra and let I be an ideal of A. Then the following are equivalent:*

(i) I is homogeneous,

(ii) $I = \bigoplus_{r \in M} (I \cap A_r)$,

(iii) I can be generated by homogeneous elements.

Proof. It is clear that the first statement implies the second. For the implication from (iii) to (i) see [Che97], Theorem I.1.3. We conclude the proof by showing that statement (ii) implies statement (iii). To this end, let $\{\, x_i \mid i \in J \,\}$ be any generating system for I, so that $I = \langle\, x_i \mid i \in J \,\rangle$. Assuming (ii), for each $i \in J$ we can write

$$x_i = \sum_{r \in M} x_{i,r} \qquad \text{with } x_{i,r} \in I \cap A_r, \text{ only finitely many } x_{i,r} \text{ non-zero.}$$

But then $I = \langle\, x_{i,r} \mid i \in J, r \in M \,\rangle$ can be generated by homogeneous elements. ☐

What makes homogeneous ideals interesting is that the quotient of a graded algebra by such an ideal naturally again is a graded algebra:

Proposition 1.23. *Let $A = \bigoplus_{r \in M} A_r$ be an M-graded k-algebra and let I be a homogeneous ideal of A. Denote by $\pi\colon A \to A/I$ the canonical projection. Then the quotient algebra A/I is again M-graded, with homogeneous parts $\pi(A_r)$ for $r \in M$.*

Proof. Since π is an algebra homomorphism, we clearly have

$$A/I = \sum_{r \in M} \pi(A_r) \quad \text{and} \quad \pi(A_r) \cdot \pi(A_s) = \pi(A_r \cdot A_s) \subseteq \pi(A_{r+s}) \quad \text{for all } r, s \in M.$$

So it only remains to show that the sum in the decomposition of A/I is direct. For this, let $J \subseteq M$ be finite and for $r \in J$ let $x_r \in A_r$ with $\sum_{r \in J} \pi(x_r) = 0$. It follows that $\pi(\sum_{r \in J} x_r) = 0$, whence $\sum_{r \in J} x_r \in I$. But the x_r are precisely the homogeneous components of $\sum_{r \in J} x_r$ and I is a homogeneous ideal, giving $x_r \in I$ for all $r \in J$. Thus, we already have $\pi(x_r) = 0$ for all $r \in J$, from which we conclude that $A/I = \bigoplus_{r \in M} \pi(A_r)$, as wanted. ☐

Since we will mainly be concerned with $\mathbb{N}$-graded and $\mathbb{Z}_2$-graded k-algebras, we now specialize to this case. A useful criterion when a homomorphism between such algebras is graded is the following:

Lemma 1.24. *Let $M \in \{\mathbb{N}, \mathbb{Z}_2\}$. Let $A = \bigoplus_{r \in M} A_r$ and $B = \bigoplus_{r \in M} B_r$ be M-graded k-algebras and let $\varphi\colon A \to B$ be an algebra homomorphism. Suppose that A is generated (as an algebra) by a set $S \subseteq A_1$ and that we have $\varphi(S) \subseteq B_1$. Then φ is M-graded.*

Proof. Let $x \in A_r$ be homogeneous. Since S generates A as an algebra, there are $n \in \mathbb{N}$, a polynomial $f \in k[X_1, \ldots, X_n]$ and elements $s_1, \ldots, s_n \in S$ such that $x = f(s_1, \ldots, s_n)$. If $M = \mathbb{N}$, then by the assumption $S \subseteq A_1$, the polynomial f can be chosen to be homogeneous of degree r. If on the other hand $M = \mathbb{Z}_2$, then we may assume that every monomial of f has degree of the same parity as r. In any case, we obtain $\varphi(x) = f(\varphi(s_1), \ldots, \varphi(s_n)) \in B_r$ since $\varphi(S) \subseteq B_1$. Hence, φ is M-graded. ☐

Proposition 1.25. *Let $M \in \{\mathbb{N}, \mathbb{Z}_2\}$ and let $A = \bigoplus_{r \in M} A_r$ and $B = \bigoplus_{r \in M} B_r$ be M-graded k-algebras. For a homogeneous element $x \neq 0$ let $\delta(x) \in \mathbb{Z}$ denote the degree of x (where we interpret the elements of $\mathbb{Z}_2$ as the integers 0 and 1).*

(i) The tensor product $A \otimes B$ of k-vector spaces is again an M-graded k-algebra, with homogeneous parts given by $(A \otimes B)_t := \bigoplus_{r+s=t} A_r \otimes B_s$, and multiplication defined in the following way: For homogeneous elements $x, x' \in A$ and $y, y' \in B$ we put

$$(x \otimes y) \cdot (x' \otimes y') := (-1)^{\delta(y)\delta(x')}(xx' \otimes yy')$$

and then extend this bilinearly to a map $A \otimes B \times A \otimes B \to A \otimes B$. The M-graded k-algebra obtained this way will be denoted $A \,{}^{M}\!\!\otimes B$.

(ii) If S is a generating system for A and T is a generating system for B, then

$$\{\, x \otimes 1 \mid x \in S \,\} \cup \{\, 1 \otimes y \mid y \in T \,\}$$

is a generating system for $A \,{}^{M}\!\!\otimes B$.

Proof. It is well-known that $A \otimes B = \bigoplus_{t \in M} (A \otimes B)_t$ as vector spaces (see for example [Bou74], Proposition II.3.7). Now let $t, t' \in M$. We need to show that

$$(A \otimes B)_t \cdot (A \otimes B)_{t'} \subseteq (A \otimes B)_{t+t'}.$$

To this end, let $x_r \in A_r$ and $y_s \in B_s$, where $r + s = t$, and let $x_{r'} \in A_{r'}$ and $y_{s'} \in B_{s'}$, where $r' + s' = t'$. Then

$$(x_r \otimes y_s) \cdot (x_{r'} \otimes y_{s'}) = (-1)^{sr'} \underbrace{x_r x_{r'}}_{\in A_{r+r'}} \otimes \underbrace{y_s y_{s'}}_{\in B_{s+s'}} \in (A \otimes B)_{r+r'+s+s'} = (A \otimes B)_{t+t'},$$

which together with bilinearity shows that indeed $(A \otimes B)_t \cdot (A \otimes B)_{t'} \subseteq (A \otimes B)_{t+t'}$. Hence, with given multiplication and homogeneous parts, $A \otimes B$ is an M-graded k-algebra. Claim (ii) is obvious. ☐

Definition 1.26. Let $M \in \{\mathbb{N}, \mathbb{Z}_2\}$ and let A and B be M-graded k-algebras. The M-graded k-algebra $A \,{}^{M}\!\!\otimes B$ constructed in the above proposition is called the *M-graded tensor product* of A and B.

Proposition 1.27. *Let $M \in \{\mathbb{N}, \mathbb{Z}_2\}$ and let A, B, C and D be M-graded k-algebras.*

(i) *Suppose that we have M-graded algebra homomorphisms $\varphi\colon A \to C$ and $\psi\colon B \to C$ with the property that $\varphi(x)\psi(y) = (-1)^{\delta(x)\delta(y)}\psi(y)\varphi(x)$ for homogeneous elements $x \in A$ and $y \in B$. Then the map*

$$A \,{}^{M}\!\!\otimes B \to C,\ x \otimes y \mapsto \varphi(x)\psi(y)$$

is an M-graded algebra homomorphism.

(ii) *Suppose that $\varphi\colon A \to C$ and $\psi\colon B \to D$ are M-graded algebra homomorphisms. Then also*

$$\varphi \otimes \psi\colon A \,{}^{M}\!\!\otimes B \to C \,{}^{M}\!\!\otimes D,\ x \otimes y \mapsto \varphi(x) \otimes \psi(y)$$

is an M-graded algebra homomorphism.

Proof.

(i) Note that the map $A \times B \to C,\ (x,y) \mapsto \varphi(x)\psi(y)$ is k-bilinear, which means that the given map $\chi\colon A \,{}^{M}\!\!\otimes B \to C,\ x \otimes y \mapsto \varphi(x)\psi(y)$, is well-defined and k-linear. Now let $r, r', s, s' \in M$ and choose elements $x_r \in A_r$, $x_{r'} \in A_{r'}$, $y_s \in B_s$, $y_{s'} \in B_{s'}$. We have

$$\begin{aligned}
\chi\big((x_r \otimes y_s)\cdot(x_{r'} \otimes y_{s'})\big) &= \chi\big((-1)^{sr'}x_r x_{r'} \otimes y_s y_{s'}\big)\\
&= (-1)^{sr'}\varphi(x_r x_{r'})\psi(y_s y_{s'})\\
&= \varphi(x_r)(-1)^{sr'}\varphi(x_{r'})\psi(y_s)\psi(y_{s'})\\
&= \varphi(x_r)\psi(y_s)\varphi(x_{r'})\psi(y_{s'})\\
&= \chi(x_r \otimes y_s)\cdot\chi(x_{r'} \otimes y_{s'})
\end{aligned}$$

where we used the assumption on φ and ψ. Linearity then gives that χ is an algebra homomorphism. Finally, let $t \in M$ and let $x_r \in A_r$ and $y_s \in B_s$ where $r + s = t$. It holds that

$$\chi(x_r \otimes y_s) = \underbrace{\varphi(x_r)}_{\in C_r}\underbrace{\psi(y_s)}_{\in C_s} \in C_{r+s} = C_t,$$

implying $\chi\big((A \,{}^{M}\!\!\otimes B)_t\big) \subseteq C_t$. We conclude that χ is M-graded.

(ii) Clearly, the maps $C \to C \,{}^{M}\!\!\otimes D,\ x \mapsto x \otimes 1$, and $D \to C \,{}^{M}\!\!\otimes D,\ y \mapsto 1 \otimes y$, are M-graded algebra homomorphisms. We thus have M-graded algebra homomorphisms

$$\tilde\varphi\colon A \to C \,{}^{M}\!\!\otimes D,\ x \mapsto \varphi(x) \otimes 1, \qquad \tilde\psi\colon B \to C \,{}^{M}\!\!\otimes D,\ y \mapsto 1 \otimes \psi(y).$$

For homogeneous elements $x \in A$ and $y \in B$ these satisfy

$$\begin{aligned}
\tilde\varphi(x)\tilde{\psi(y)} &= \varphi(x) \otimes \psi(y)\\
&= (-1)^{\delta(x)\delta(y)}\big(1 \otimes \psi(y)\big)\big(\varphi(x) \otimes 1\big)\\
&= (-1)^{\delta(x)\delta(y)}\tilde{\psi(y)}\tilde\varphi(x)
\end{aligned}$$

where we used that φ and ψ are graded. The claim now follows from (i). ☐

Concluding this section, we focus entirely on finite-dimensional $\mathbb{Z}_2$-graded k-algebras. The following result shows that the endomorphism algebra of such algebras carries a natural $\mathbb{Z}_2$-grading. It may be found in Example IV.2.6 of [Lam05] or on p. 275 of [Mei13].

Lemma 1.28. *Let $A = A_0 \oplus A_1$ be a finite-dimensional $\mathbb{Z}_2$-graded k-algebra. We define*

$$\begin{aligned} \operatorname{End}(A)_0 &:= \{\, f \in \operatorname{End}(A) \mid f(A_i) \subseteq A_i \text{ for } i = 0, 1 \,\}, \\ \operatorname{End}(A)_1 &:= \{\, f \in \operatorname{End}(A) \mid f(A_i) \subseteq A_{i+1} \text{ for } i = 0, 1 \,\}, \end{aligned}$$

i.e., we let $\operatorname{End}(A)_d$ consist of the linear endomorphisms of A that are homogeneous of degree $d \in \mathbb{Z}_2$. Then the following hold:

(i) The above definitions make $\operatorname{End}(A)$ into a $\mathbb{Z}_2$-graded k-algebra.

(ii) There is an isomorphism

$$\operatorname{End}(A)_0 \xrightarrow{\sim} \operatorname{End}(A_0) \oplus \operatorname{End}(A_1), \ f \mapsto (f\big|_{A_0}, f\big|_{A_1})$$

of (ungraded) k-algebras, with inverse given by $(g, h) \mapsto (a_0 + a_1 \mapsto g(a_0) + h(a_1))$.

Proof.

(i) It clearly holds that $\operatorname{End}(A)_0 \cap \operatorname{End}(A)_1 = 0$ and $\operatorname{End}(A)_i \operatorname{End}(A)_j \subseteq \operatorname{End}(A)_{i+j}$ for all $i, j \in \mathbb{Z}_2$. Now choosing a basis of A according to the decomposition $A = A_0 \oplus A_1$, an endomorphism $f \in \operatorname{End}(A)$ is contained in $\operatorname{End}(A)_0$ if and only if its matrix w.r.t. to the chosen basis is of the form $\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right)$, and it is contained in $\operatorname{End}(A)_1$ if and only if its matrix w.r.t. to the chosen basis is of the form $\left(\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right)$. This shows that $\operatorname{End}(A) = \operatorname{End}(A)_0 \oplus \operatorname{End}(A)_1$.

(ii) This is readily verified. ☐

For these endomorphism algebras, there is a graded version of Proposition 1.6 (ii), stated, but not proved, on p. 152 of [Knu91]. This is why we now give a detailed proof.

Proposition 1.29. *Let $A = A_0 \oplus A_1$ and $B = B_0 \oplus B_1$ be finite-dimensional $\mathbb{Z}_2$-graded k-algebras. Then the map*

$$\Theta \colon \operatorname{End}(A) \,{}^{\mathbb{Z}_2}\!\!\otimes \operatorname{End}(B) \to \operatorname{End}(A \,{}^{\mathbb{Z}_2}\!\!\otimes B),$$

which for homogeneous elements $f \in \operatorname{End}(A)$, $g \in \operatorname{End}(B)$, $x \in A$ and $y \in B$ is defined by

$$\Theta(f \otimes g)(x \otimes y) := (-1)^{\delta(g)\delta(x)} f(x) \otimes g(y),$$

is an isomorphism of $\mathbb{Z}_2$-graded k-algebras.

Proof. In order to show that it is well-defined, we first construct Θ as indicated above. To this end, let $f \in \operatorname{End}(A)_d$ and $g \in \operatorname{End}(B)_e$ be homogeneous. The map

$$A_r \times B_s \to A \,{}^{\mathbb{Z}_2}\!\otimes B,\ (x,y) \mapsto (-1)^{\delta(g)\delta(x)} f(x) \otimes g(y),$$

is bilinear, thus giving rise to a linear map $A_r \otimes B_s \to A \,{}^{\mathbb{Z}_2}\!\otimes B$. These maps on the homogeneous components of $A \,{}^{\mathbb{Z}_2}\!\otimes B$ constitute a linear map $\theta(f,g) \in \operatorname{End}(A \,{}^{\mathbb{Z}_2}\!\otimes B)$. Note that $\theta(f,g)$ is homogeneous of degree $d+e$. One now easily sees that also the map

$$\operatorname{End}(A)_d \times \operatorname{End}(B)_e \to \operatorname{End}(A \,{}^{\mathbb{Z}_2}\!\otimes B),\ (f,g) \mapsto \theta(f,g),$$

is bilinear. As before, this eventually gives rise to a linear map

$$\Theta\colon \operatorname{End}(A) \,{}^{\mathbb{Z}_2}\!\otimes \operatorname{End}(B) \to \operatorname{End}(A \,{}^{\mathbb{Z}_2}\!\otimes B),$$

that is defined as desired. We have to show that it is an isomorphism of $\mathbb{Z}_2$-graded k-algebras. Since for $f \in \operatorname{End}(A)_d$ and $g \in \operatorname{End}(B)_e$ the map $\theta(f,g)$ is homogeneous of degree $d+e$, it follows that Θ is homogeneous of degree 0. Now in order to prove that Θ is an algebra homomorphism, we only need to consider homogeneous elements due to the fact that Θ is linear. So let $f \in \operatorname{End}(A)_d$, $f' \in \operatorname{End}(A)_{d'}$, $g \in \operatorname{End}(B)_e$ and $g' \in \operatorname{End}(B)_{e'}$. Further let $x_r \in A_r$ and $y_s \in B_s$. Then

$$\begin{aligned}\Theta\big((f\otimes g)(f'\otimes g')\big)(x_r \otimes y_s) &= \Theta\big((-1)^{ed'} ff' \otimes gg'\big)(x_r \otimes y_s)\\ &= (-1)^{ed'}\theta(ff', gg')(x_r \otimes y_s)\\ &= (-1)^{ed'}(-1)^{(e+e')r} ff'(x_r) \otimes gg'(y_s).\end{aligned}$$

On the other hand,

$$\begin{aligned}\Theta(f\otimes g)\Theta(f'\otimes g')(x_r \otimes y_s) &= \Theta(f\otimes g)\big(\theta(f',g')(x_r\otimes y_s)\big)\\ &= (-1)^{e'r}\theta(f,g)(f'(x_r)\otimes g'(y_s))\\ &= (-1)^{e'r}(-1)^{e(r+d')} ff'(x_r) \otimes gg'(y_s).\end{aligned}$$

Since these two expressions agree and Θ is homogeneous of degree 0, we conclude that Θ indeed is a $\mathbb{Z}_2$-graded algebra homomorphism. Bijectivity follows as in Proposition 1.6 (ii). ☐

Note that by applying the proposition with the trivial $\mathbb{Z}_2$-grading, we recover Proposition 1.6 (ii).

1.4 The Tensor Algebra

In this section, let V be a finite-dimensional vector space over k.

We introduce the tensor algebra of V and establish some of its basic properties. It will later be used to construct the exterior algebra as well as the Clifford algebra. The material from this section can for example be found in [Bou74], Section III.5.1 or [GW09], Section C.1.2.

We denote by $V^{\otimes r} := V \otimes \cdots \otimes V$ (r times) the r-fold tensor product of V with itself (where $V^{\otimes 0} := k$).

Definition 1.30. The *tensor algebra* of V is the k-vector space

$$T(V) := \bigoplus_{r\in\mathbb{N}} V^{\otimes r}$$

with multiplication given by

$$V^{\otimes r} \times V^{\otimes s} \to V^{\otimes (r+s)},\ (v_1 \otimes \cdots \otimes v_r, w_1 \otimes \cdots \otimes w_s) \mapsto v_1 \otimes \cdots \otimes v_r \otimes w_1 \otimes \cdots \otimes w_s,$$

and then extending this map linearly to a map $T(V) \times T(V) \to T(V)$.

Proposition 1.31.

(i) The tensor algebra $T(V)$ is an associative unital algebra over k.

(ii) The space V can naturally be considered as a subspace $V \leq T(V)$ of the tensor algebra that generates $T(V)$ as an algebra.

(iii) The tensor algebra is an $\mathbb{N}$-graded algebra, with homogeneous parts $T(V)_r := V^{\otimes r}$.

(iv) The tensor algebra is a $\mathbb{Z}_2$-graded algebra, with homogeneous parts $T(V)_0 := \bigoplus_{r \text{ even}} V^{\otimes r}$ and $T(V)_1 := \bigoplus_{r \text{ odd}} V^{\otimes r}$.

Proof. It is clear that $T(V)$ is an associative k-algebra, with multiplicative identity element $1 \in k = V^{\otimes 0}$. Turning to the second claim, we have a canonical injection $V = V^{\otimes 1} \hookrightarrow T(V)$ and will identify V with its image under this map, so that $V \leq T(V)$. By definition of multiplication in the tensor algebra, this subspace generates $T(V)$ as an algebra, proving (ii). Claim (iii) is clear by definition of $T(V)$, while (iv) follows from (iii) and Remark 1.18 (b). ☐

The tensor algebra can also be characterized by a universal property:

Proposition 1.32 (Universal property of the tensor algebra)**.** *If A is a k-algebra and $\varphi\colon V \to A$ is a linear map, then φ can uniquely be extended to an algebra homomorphism $\Phi\colon T(V) \to A$.*

$$\begin{tikzcd}
V \arrow[r, hook] \arrow[dr, "\varphi"'] & T(V) \arrow[d, dashed, "\exists!\ \Phi"] \\
 & A
\end{tikzcd}$$

Proof. Uniqueness is clear by Proposition 1.31 (ii). By the universal property of the tensor product, there is a linear map $V^{\otimes r} \to A,\ v_1 \otimes \cdots \otimes v_r \mapsto \varphi(v_1)\cdots\varphi(v_r)$ for each $r \in \mathbb{N}$, giving rise to a linear map $\Phi\colon T(V) \to A$. For homogeneous $x, y \in T(V)$ we have $\Phi(xy) = \Phi(x)\Phi(y)$ which implies that Φ is an algebra homomorphism. ☐

As usual, this property determines $T(V)$ uniquely up to (a unique) isomorphism of k-algebras.

Example 1.33. Suppose $\dim V = 1$. We claim that in this case $T(V) \cong k[X]$ is the polynomial ring in one variable over k. Let $0 \neq v \in V$ be a nonzero vector in V which then constitutes a basis of V. We may thus define a linear map $\varphi\colon V \to k[X],\ v \mapsto X$. By Proposition 1.32, this map extends to an algebra homomorphism

$$\Phi\colon T(V) \to k[X],\ v \mapsto X.$$

It is bijective with inverse $k[X] \to T(V), f \mapsto f(v)$, proving that $T(V) \cong k[X]$.

Example 1.34. Using the universal property from Proposition 1.32, we construct three involutions associated to the tensor algebra.

(a) The map $V \to T(V),\ v \mapsto -v$ extends to an algebra homomorphism $\eta\colon T(V) \to T(V)$. We have $\eta^2 = \mathrm{id}_{T(V)}$ by Proposition 1.32 (ii) and for $x \in T(V)_r$ it holds that $\eta(x) = (-1)^r x$.

(b) The map $V \to T(V)^{\mathrm{op}},\ v \mapsto v$ extends to an algebra homomorphism $T(V) \to T(V)^{\mathrm{op}}$, that is, to an antihomomorphism $T(V) \to T(V)$. The image of $x \in T(V)$ under this antihomomorphism will be denoted by $x^\top$. If $v_1, \dots, v_r \in V$, then we have $(v_1 \otimes \cdots \otimes v_r)^\top = v_r \otimes \cdots \otimes v_1$. Hence, $(x^\top)^\top = x$ for all $x \in T(V)$.

(c) The two maps from (i) and (ii) commute which can be seen by linearity and their respective actions on $T(V)_r$. Denoting their composition by $\bar{\cdot}$, we have $\overline{\overline{x}} = x$ for $x \in T(V)$ and $\overline{v_1 \otimes \cdots \otimes v_r} = (-1)^r v_r \otimes \cdots \otimes v_1$ for $v_1, \dots, v_r \in V$.

1.5 The Exterior Algebra

Let again V be a finite-dimensional vector space over k.

Having defined the tensor algebra in the previous section, we now construct the exterior algebra as a quotient of $T(V)$. We study its structure and define two specific endomorphisms. The topics of this section will become important in Section 3.2 where we analyze the structure of the Clifford algebra and in Chapter 5 on spin representations.

Most of the content of this section is covered in [Bou74], Section III.7 and [Lan02], Section XIX.1.

Definition 1.35. The *exterior algebra* of V is the quotient algebra

$$\textstyle\bigwedge V := T(V)/\langle\, v \otimes v \mid v \in V \,\rangle.$$

We write $v \wedge w$ for the image of $v \otimes w$ under the canonical projection $T(V) \to \bigwedge V$ and $\bigwedge^r V$ for the image of $V^{\otimes r}$ under this map.

Proposition 1.36.

(i) *The exterior algebra $\bigwedge V$ is an $\mathbb{N}$-graded k-algebra, with homogeneous parts $\bigwedge^r V$. We can naturally identify V with $\bigwedge^1 V$ and thus consider it as a subspace of $\bigwedge V$ that generates $\bigwedge V$ as an algebra.*

(ii) *The exterior algebra is a $\mathbb{Z}_2$-graded algebra, with homogeneous parts $(\bigwedge V)_0 := \bigoplus_{r \text{ even}} \bigwedge^r V$ and $(\bigwedge V)_1 := \bigoplus_{r \text{ odd}} \bigwedge^r V$.*

(iii) *For $v_1, \dots, v_r \in V$ and $\sigma \in S_r$ we have $v_1 \wedge \cdots \wedge v_r = \operatorname{sgn}(\sigma) v_{\sigma(1)} \wedge \cdots \wedge v_{\sigma(r)}$.*

(iv) *If $(v_1, \dots, v_n)$ is a basis of V, then*

$$(\, v_{i_1} \wedge \cdots \wedge v_{i_r} \mid 1 \leq i_1 < \cdots < i_r \leq n \,)$$

is a basis of $\bigwedge^r V$. In particular, $\dim \bigwedge^r V = \binom{\dim V}{r}$ and $\dim \bigwedge V = 2^{\dim V}$.

Proof. Since $\langle\, v \otimes v \mid v \in V \,\rangle$ is a homogeneous ideal of $T(V)$, the statements on the gradings are immediate from Propositions 1.31 and 1.23. The natural surjective map $V = V^{\otimes 1} \to \bigwedge^1 V$ is a bijection as $V^{\otimes 1} \cap \langle\, v \otimes v \mid v \in V \,\rangle = 0$. Hence, we may identify V with $\bigwedge^1 V$ which generates $\bigwedge V$ as an algebra by Proposition 1.31 (ii). Thus, we have proved (i) and (ii). Turning to the third claim, for $v, w \in V$ we have

$$0 = (v + w) \wedge (v + w) = v \wedge v + v \wedge w + w \wedge v + w \wedge w = v \wedge w + w \wedge v,$$

which gives $v \wedge w = -w \wedge v$. Statement (iii) then follows from this by writing σ as a product of transpositions. Finally, for (iv), we refer to [Lan02], Proposition XIX.1.1. ☐

Just as the tensor algebra, the exterior algebra can also be characterized by a universal property:

Proposition 1.37 (Universal property of the exterior algebra)**.** *If A is a k-algebra and $\varphi\colon V \to A$ is a linear map that satisfies $\varphi(v)^2 = 0$ for all $v \in V$, then φ can uniquely be extended to an algebra homomorphism $\Phi\colon \bigwedge V \to A$.*

$$\begin{tikzcd}
V \arrow[r, hook] \arrow[dr, "\varphi"'] & \bigwedge V \arrow[d, dotted, "\exists!\, \Phi"] \\
& A
\end{tikzcd}$$

Proof. Uniqueness is immediate from Proposition 1.36 (i). Application of Proposition 1.32 shows that φ extends to an algebra homomorphism $T(V) \to A$ whose kernel by assumption clearly contains the ideal $\langle\, v \otimes v \mid v \in V \,\rangle$. Thus, we obtain an algebra homomorphism $\Phi\colon \bigwedge V \to A$ with the desired property. ☐

An important application of this universal property is to establish the following isomorphism of graded algebras:

Proposition 1.38. *Let W be a further finite-dimensional k-vector space and let $M \in \{\mathbb{N}, \mathbb{Z}_2\}$. Then there is an M-graded isomorphism of k-algebras*

$$\bigwedge(V \oplus W) \to \bigwedge V \ {}^{M}\!\!\otimes \bigwedge W,\ (v, w) \mapsto v \otimes 1 + 1 \otimes w,$$

where $v \in V$ and $w \in W$.

Proof. The map

$$\varphi\colon V \oplus W \to \bigwedge V \ {}^{M}\!\!\otimes \bigwedge W,\ (v, w) \mapsto v \otimes 1 + 1 \otimes w$$

is k-linear and by the rules for mulitplication in the graded tensor product satisfies

$$\begin{aligned}\varphi(v, w)^2 &= (v \otimes 1 + 1 \otimes w)^2 \\ &= (v \wedge v) \otimes 1 + (v \otimes 1)(1 \otimes w) + (1 \otimes w)(v \otimes 1) + 1 \otimes (w \wedge w) \\ &= v \otimes w - v \otimes w \\ &= 0\end{aligned}$$

for $v \in V$ and $w \in W$. Thus, by Proposition 1.37 there exists a (unique) algebra homomorphism $\Phi\colon \bigwedge(V \oplus W) \to \bigwedge V \ {}^{M}\!\!\otimes \bigwedge W$ extending φ. This map is M-graded by Lemma 1.24 applied to the generating system $V \oplus W$ of $\bigwedge(V \oplus W)$.

Due to Propositions 1.36 (i) and 1.25 (ii), the image of Φ contains an algebra generating system of $\bigwedge V \ {}^{M}\!\!\otimes \bigwedge W$ which implies that Φ is surjective. By comparing dimensions using Proposition 1.36 (iv), it follows that it is an isomorphism. ☐

Remark 1.39. Note that the three involutions from Example 1.34 leave the ideal $\langle\, v \otimes v \mid v \in V \,\rangle$ of $T(V)$ invariant. Hence, they descend to involutions of $\bigwedge V$. These maps will be denoted by the same symbols as for $T(V)$. Taking Proposition 1.36 (iii) into account, one easily sees that their actions on $x \in \bigwedge^r V$ are given by

$$\eta(x) = (-1)^r x, \qquad x^\top = (-1)^{\frac{r(r-1)}{2}} x, \qquad \overline{x} = (-1)^{\frac{r(r+1)}{2}} x. \tag{1.3}$$

We conclude this section by introducing two linear maps on $\bigwedge V$ that will become important later.

Definition 1.40. For $v \in V$ define

$$\lambda_v\colon \bigwedge V \to \bigwedge V,\ x \mapsto v \wedge x,$$

and call this map the *left exterior multiplication by v*.

Clearly, $\lambda_v \in \operatorname{End}(\bigwedge V)$ is linear and homogeneous of degree 1. Notice also that $\lambda_v^2 = 0$. The following proposition shows that we may further associate a linear endomorphism of $\bigwedge V$ to every element of the dual space V^*. It is adapted from Proposition IV.1.7.1 of [Knu91].

Proposition 1.41. *Let* $\psi \in V^*$*. Then there exists a* k*-linear map* $\iota_\psi \in \operatorname{End}(\bigwedge V)$ *defined by*

$$\iota_\psi \colon \textstyle\bigwedge^r V \to \bigwedge^{r-1} V,\ v_1 \wedge \cdots \wedge v_r \mapsto \displaystyle\sum_{i=1}^{r} (-1)^{i-1} \psi(v_i) v_1 \wedge \cdots \wedge \widehat{v_i} \wedge \cdots \wedge v_r,$$

where the notation $\widehat{v_i}$ *means to omit* v_i*. It has the following properties:*

- *(i)* ι_ψ *is homogeneous of degree* -1*,*
- *(ii)* $\iota_\psi(v) = \psi(v)$ *for all* $v \in V$*,*
- *(iii)* $\iota_\psi \lambda_v = \psi(v)\mathrm{id}_{\bigwedge V} - \lambda_v \iota_\psi$ *for all* $v \in V$*,*
- *(iv)* $\iota_\psi(x \wedge y) = \iota_\psi(x) \wedge y + (-1)^r x \wedge \iota_\psi(y)$ *for* $x \in \bigwedge^r V$ *and* $y \in \bigwedge V$*,*
- *(v)* $\iota_\psi^2 = 0$*,*
- *(vi)* $\iota_\psi(x^\top) = (-1)^{r+1} \iota_\psi(x)^\top$ *for* $x \in \bigwedge^r V$*.*

Proof. The map $(v_1, \ldots, v_r) \mapsto \sum_{i=1}^{r} (-1)^{i-1} \psi(v_i) v_1 \wedge \cdots \wedge \widehat{v_i} \wedge \cdots \wedge v_r$ being k-multilinear, it induces a k-linear map

$$V^{\otimes r} \to \textstyle\bigwedge^{r-1} V,\ v_1 \otimes \cdots \otimes v_r \mapsto \displaystyle\sum_{i=1}^{r} (-1)^{i-1} \psi(v_i) v_1 \wedge \cdots \wedge \widehat{v_i} \wedge \cdots \wedge v_r.$$

By its definition with the alternating sign, this map factors through the ideal $V^{\otimes r} \cap \langle\, v \otimes v \mid v \in V \,\rangle$, giving rise to a linear map $\iota_\psi \colon \bigwedge^r V \to \bigwedge^{r-1} V$, as claimed.

- (i) This is clear.
- (ii) By definition, $\iota_\psi(v) = (-1)^{1-1}\psi(v) = \psi(v)$ for $v \in V$.
- (iii) Let $v \in V$ and $x \in \bigwedge V$. By linearity, we may assume that $x = v_1 \wedge \cdots \wedge v_r$ with $v_i \in V$. Applying the definition, it holds that

$$\begin{aligned}\iota_\psi(v \wedge x) &= \psi(v) v_1 \wedge \cdots \wedge v_r + \sum_{i=1}^{r} (-1)^{i} \psi(v_i) v \wedge v_1 \wedge \cdots \wedge \widehat{v_i} \wedge \cdots \wedge v_r \\ &= \psi(v) v_1 \wedge \cdots \wedge v_r - v \wedge \left(\sum_{i=1}^{r} (-1)^{i-1} \psi(v_i) v_1 \wedge \cdots \wedge \widehat{v_i} \wedge \cdots \wedge v_r \right) \\ &= \psi(v) x - v \wedge \iota_\psi(x),\end{aligned}$$

  as claimed.

(iv) We do induction on r. The cases $r = 0$ and $r = 1$ are covered by the previous parts. Now suppose that $r > 1$ and let $x \in \bigwedge^r V$. By linearity, we may assume that $x = v_1 \wedge \cdots \wedge v_r$ for $v_i \in V$. Writing $z = v_2 \wedge \cdots \wedge v_r$, we have $x = v_1 \wedge z$. Let now $y \in \bigwedge V$. The case $r = 1$ and induction give

$$\begin{aligned}\iota_\psi(x \wedge y) &= \psi(v_1)z \wedge y - v_1 \wedge \iota_\psi(z \wedge y)\\ &= \psi(v_1)z \wedge y - v_1 \wedge \iota_\psi(z) \wedge y + (-1)^r x \wedge \iota_\psi(y).\end{aligned}$$

But $\psi(v_1)z \wedge y - v_1 \wedge \iota_\psi(z) \wedge y = \iota_\psi(x) \wedge y$, proving the claim.

(v) We prove by induction on r that $\iota_\psi^2(\bigwedge^r V) = 0$. This is clear for $r \leq 1$ by part (i). Now suppose that $r \geq 2$. Note that by (iii) we have

$$\iota_\psi^2 \lambda_v = \psi(v)\iota_\psi - \iota_\psi \lambda_v \iota_\psi = \psi(v)\iota_\psi - \psi(v)\iota_\psi + \lambda_v \iota_\psi^2 = \lambda_v \iota_\psi^2$$

for $v \in V$. Thus, if $x = v_1 \wedge \cdots \wedge v_r \in \bigwedge^r V$ where $v_1, \ldots, v_r \in V$, then

$$\iota_\psi^2(x) = \iota_\psi^2 \lambda_{v_1}(v_2 \wedge \cdots \wedge v_r) = \lambda_{v_1} \iota_\psi^2(v_2 \wedge \cdots \wedge v_r) = 0$$

by induction.

(vi) We again do induction on r. For $r = 0$ both sides equal 0 and for $r = 1$ both sides equal $\psi(x)$ by part (ii). Suppse $r > 1$ and let $x \in \bigwedge^r V$. We may by linearity of both sides assume that $x = v_1 \wedge \cdots \wedge v_r$ for $v_i \in V$. Writing $z = v_2 \wedge \cdots \wedge v_r$, we have $x = v_1 \wedge z$, and part (iv) gives

$$\iota_\psi(x^\top) = \iota_\psi(z^\top \wedge v_1) = \iota_\psi(z^\top) \wedge v_1 + (-1)^{r-1}\psi(v_1)z^\top.$$

Now by induction it holds that $\iota_\psi(z^\top) = (-1)^r \iota_\psi(z)^\top$, giving $\iota_\psi(z^\top) \wedge v_1 = (-1)^r (v_1 \wedge \iota_\psi(z))^\top$ and therefore

$$\iota_\psi(x^\top) = (-1)^{r+1}(\psi(v_1)z^\top - (v_1 \wedge \iota_\psi(z))^\top) = (-1)^{r+1}(\psi(v_1)z - v_1 \wedge \iota_\psi(z))^\top.$$

But $\psi(v_1)z - v_1 \wedge \iota_\psi(z) = \iota_\psi(x)$, finishing the proof. □

Definition 1.42. Let $\psi \in V^*$. The linear map ι_ψ from above is called the *interior product with* ψ.

2 Bilinear Forms and Quadratic Forms

Throughout Chapter 2, let V be a k-vector space with $n := \dim V < \infty$.

Similarly as in the first chapter, we collect some well-known results, this time in the realm of bilinear forms and quadratic forms, that serve as the foundation for our later studies.

2.1 Bilinear Forms

In this section, we assemble some basic notions and results from the theory of symmetric and alternating bilinear forms. Our discussion is based on [Gro02], Chapters 2 and 4, [EKM08], Section 1.1 and [Lam05], Sections I.1 and I.2.

Definition 2.1. A bilinear map $B\colon V \times V \to k$ is called a *bilinear form on V*. Such a bilinear form B is said to be *symmetric* if $B(v,w) = B(w,v)$ for all $v, w \in V$ and is called *alternating* if $B(v,v) = 0$ for all $v \in V$.

Note that if B is alternating, then for all $v, w \in V$ it holds that

$$0 = B(v+w, v+w) = B(v,v) + B(v,w) + B(w,v) + B(w,w) = B(v,w) + B(w,v),$$

showing $B(v,w) = -B(w,v)$. This is referred to as *skew-symmetry.* In particular, if $\operatorname{char} k = 2$, then every alternating bilinear form is symmetric.

If $B\colon V \times V \to k$ is a bilinear form and $\mathcal{B} = (v_1, \dots, v_n)$ be a basis of V, then we write

$$M_{\mathcal{B}}(B) := (B(v_i, v_j))_{i,j} \in \operatorname{Mat}_n(k)$$

for the matrix of B with respect to $\mathcal{B}$. It is clear that $M_{\mathcal{B}}(B)$ is symmetric if and only if B is symmetric. Furthermore, recall the following properties of the matrix of a bilinear form: If $\mathcal{B} = (v_1, \dots, v_n)$ is a basis of V and $c_{\mathcal{B}}\colon V \to k^n$ denotes the corresponding coordinate map, then

$$B(v,w) = c_{\mathcal{B}}(v)^\top M_{\mathcal{B}}(B) c_{\mathcal{B}}(w) \tag{2.1}$$

for all $v, w \in V$. Moreover, if $\mathcal{C}$ is another basis of V, we have $M_{\mathcal{C}}(B) = T^\top M_{\mathcal{B}}(B) T$ where T is the matrix of the linear isomorphism $c_{\mathcal{B}} \circ c_{\mathcal{C}}^{-1}$ (w.r.t. the standard basis).

We introduce some more terminology.

Definition 2.2. Let $B\colon V \times V \to k$ be a symmetric or alternating bilinear form.

(a) Two vectors $v, w \in V$ are called *orthogonal* if $B(v,w) = 0$. In this case we write $v \perp w$. A subset $\{v_1, \ldots, v_r\}$ of V is called *orthogonal* if $v_i \perp v_j$ for $i \neq j$, i.e., if its elements are pairwise orthogonal.

(b) If $V', V'' \leq V$ are subspaces of V with $V = V' \oplus V''$ and $v' \perp v''$ for all $v' \in V'$ and $v'' \in V''$, then we write $V = V' \perp V''$ and say that V is the *orthogonal direct sum* of V' and V''.

Definition 2.3. Let B be a symmetric or alternating bilinear form on V and let $W \leq V$ be a subspace of V.

(a) The subspace

$$W^{\perp} := \{\, v \in V \mid B(v,w) = 0 \text{ for all } w \in W \,\} \leq V$$

is called the *orthogonal complement* of W. We put $\operatorname{rad} B := V^{\perp}$ and call it the *radical* of B.

(b) Define a linear map

$$l_W\colon V \to W^*,\ v \mapsto (w \mapsto B(v,w)),$$

where $W^* = \operatorname{Hom}(W,k)$ is the dual space of W.

(c) We write $B\big|_W := B\big|_{W \times W}$ for the restriction of B to $W \times W$.

Note that the restrcition of a symmetric resp. alternating biliear form clearly remains symmetric resp. alternating. The following lemma relates the objects just introduced.

Lemma 2.4. *Let B be a symmetric or alternating bilinear form on V and let $W \leq V$ be a subspace of V. The following are equivalent:*

(i) $W \cap \operatorname{rad} B = 0$,

(ii) l_W *is surjective,*

(iii) $\dim V = \dim W + \dim W^{\perp}$.

In this case, if $X \leq V$ is such that $V = W \perp X$, then $X = W^{\perp}$.

Proof. The equivalences are not hard to show, see [EKM08], Proposition 1.5. For the additional statement note that if $X \leq V$ is such that $V = W \perp X$, then $X \subseteq W^{\perp}$. Thus, the claim follows from the dimension formula (iii). ☐

In the special case $W = V$ the statements of the above lemma may be related to the matrix of B:

Lemma 2.5. *Let B be a symmetric or alternating bilinear form on V and let $\mathcal{B}$ be a basis of V. The following are equivalent:*

(i) $\operatorname{rad} B = 0$,

(ii) l_V *is an isomorphism of k-vector spaces,*

and, if $V \neq 0$,

(iii) $\det M_{\mathcal{B}}(B) \neq 0$.

Note that (iii) does not depend on the choice of basis as the matrix of B with respect to a different basis will differ from $M_{\mathcal{B}}(B)$ only by invertible matrices.

Proof. Statements (i) and (ii) are equivalent by Lemma 2.4. Now suppose that $V \neq 0$. Write $\mathcal{B} = (v_1, \ldots, v_n)$ and let $(v_1^*, \ldots, v_n^*)$ be the dual basis. Since $l_V(v_i)(v_j) = B(v_i, v_j)$, we have $l_V(v_i) = \sum_{j=1}^{n} B(v_i, v_j) v_j^*$, so that $M_{\mathcal{B}}(B)$ is the matrix of l_V with respect to the bases $\mathcal{B}$ of V and $(v_1^*, \ldots, v_n^*)$ of V^*. This shows the equivalence of (ii) and (iii). ☐

We may now define the following fundamental notion:

Definition 2.6. A symmetric or alternating bilinear form $B\colon V \times V \to k$ satisfying one (and hence all) of the conditions of Lemma 2.5 is called *nondegenerate.*

Thus, the equivalent conditions of Lemma 2.4 are for example satisfied if B is nondegenerate or if $B\big|_W$ is nondegenerate. The latter may be characterized as follows:

Lemma 2.7. *Let B be a symmetric or alternating bilinear form on V and let $W \leq V$ be a subspace of V. Then* $\operatorname{rad} B\big|_W = W \cap W^{\perp}$. *In particular, there are equivalent:*

(i) $B\big|_W$ *is nondegenerate,*

(ii) $W \cap W^{\perp} = 0$,

(iii) $V = W \perp W^{\perp}$,

and, if the equivalent conditions of Lemma 2.4 are fulfilled,

(iv) there is a subspace $X \leq V$ such that $V = W \perp X$.

Proof. By definition, we have

$$\operatorname{rad} B\big|_W = \{\, v \in W \mid B(v, w) = 0 \text{ for all } w \in W \,\} = W \cap W^{\perp},$$

proving the first claim. This immediately implies the equivalence of (i) and (ii). Clearly, (iii) implies (ii). Suppose conversely that $W \cap W^{\perp} = 0$. Then since $W \cap \operatorname{rad} B \leq W \cap W^{\perp} = 0$, we have $\dim V = \dim W + \dim W^{\perp}$ by Lemma 2.4, giving $V = W \perp W^{\perp}$. Hence, statements (ii) and (iii) are equivalent as well.

Now suppose that the conditions of Lemma 2.4 are complied with. The implication from (iii) to (iv) is trivial. Conversely, let $X \leq V$ such that $V = W \perp X$. Then by Lemma 2.4 we have $X = W^{\perp}$ which shows that (iv) implies (iii) and concludes the proof. □

We take a brief look at alternating forms. A crucial result is the following:

Proposition 2.8. *If B is a nondegenerate alternating bilinear form on V, then $\dim V$ is even.*

Proof. This is [Gro02], Corollary 2.11. □

Given a nondegenerate alternating bilinear form, the group of invertible linear transformations preserving it is an important geometric object that we now define.

Definition 2.9. Suppose that $\dim V$ is even and that $B\colon V \times V \to k$ is a nondegenerate alternating bilinear form. An invertible linear transformation $\tau \in \mathrm{GL}(V)$ is called *symplectic* if $B(\tau(v), \tau(w)) = B(v, w)$ for all $v, w \in V$. We denote by

$$\mathrm{Sp}(V) := \mathrm{Sp}(V, B) := \{\, \tau \in \mathrm{GL}(V) \mid B(\tau(v), \tau(w)) = B(v, w) \text{ for all } v, w \in V \,\}$$

the set of all symplectic invertible linear transformations with respect to B and call it the *symplectic group* of V (w.r.t. B).

It is clear that the symplectic group is a subgroup of $\mathrm{GL}(V)$ and therefore indeed is a group. One may further show:

Proposition 2.10. *Suppose that $\dim V$ is even and that $B\colon V \times V \to k$ is a nondegenerate alternating bilinear form. It holds that $\mathrm{Sp}(V) \leq \mathrm{SL}(V)$ with equality if $\dim V = 2$.*

Proof. See [Gro02], Proposition 3.1 and Corollary 3.5. □

We turn to symmetric bilinear forms for which we have the following important theorem that ensures the existence of an orthogonal basis if the characterisic of the ground field is different from 2.

Theorem 2.11 (Existence of an orthogonal basis)**.** *Let B be a symmetric bilinear form on V, and assume that $\operatorname{char} k \neq 2$. Then V has an orthogonal basis.*

Proof. We do induction on $n = \dim V$. For $n = 0$ there is nothing to show. Now suppose that $n > 0$. If $B = 0$, then any basis of V is an orthogonal basis. Thus, we may assume that $B \neq 0$. There must now exist a vector $e_1 \in V$ with $B(e_1, e_1) \neq 0$ as otherwise $0 = \frac{1}{2}B(v + w, v + w) = B(v, w)$ for all $v, w \in V$, a contradiction.

Putting $W := \mathrm{span}(e_1)$, this means that $B\big|_W$ is nondegenerate, so that Lemma 2.7 yields $V = W \perp W^{\perp}$. Hence, we may apply induction to obtain an orthogonal basis $(e_2, \ldots, e_n)$ of $W^{\perp}$. But then $(e_1, e_2, \ldots, e_n)$ is an orthogonal basis of V. □

Note that the theorem does in genereal not hold in characteristic 2 (cf. Lemma 2.31 (ii)).

2.2 Quadratic Forms

We now introduce quadratic forms and develop some of their theory. This will be fundamental for the remainder of the thesis as the ambient setting will mainly be that of a finite-dimensional vector space which is equipped with a quadratic form.

We do not make any assumptions on k, so in particular allow it to have characteristic 2. Books not including this case might have different conventions regarding some of the notions. We further attempt to keep every statement as general as possible. For most of the time we follow [EKM08], Section II.7 together with Chapter 1 of [Che97] and Chapters 5 and 12 of [Gro02]. Other references are [Tay92], Chapter 7 and for $\operatorname{char} k \neq 2$ also [Lam05], Chapter I.

Definition 2.12. A *quadratic form* on V is a map $Q\colon V \to k$ having the following two properties:

(Q1) $Q(av) = a^2Q(v)$ for all $a \in k$ and $v \in V$,

(Q2) the map $B_Q\colon V \times V \to k,\ (v,w) \mapsto Q(v+w) - Q(v) - Q(w)$ is bilinear.

We call B_Q the *bilinear form associated to* Q and frequently simply denote it by B if there is no ambiguity.

Note that the bilinear form B_Q associated to a quadratic form Q on V is automatically symmetric. Thus, the notions and results in the context of symmetric bilinear forms from the previous section apply. Observe further that

$$B_Q(v,v) = Q(2v) - Q(v) - Q(v) = 4Q(v) - 2Q(v) = 2Q(v) \tag{2.2}$$

for $v \in V$. This basic fact will be used very often in the sequel.

The following lemma shows that quadratic forms may be thought of as homogeneous polynomials of degree 2:

Lemma 2.13. *Let $Q\colon V \to k$ be a nonzero map and let $(v_1, \dots, v_n)$ be a basis of V. Then Q is a quadratic form on V if and only if there is a homogeneous polynomial $f \in k[X_1, \dots, X_n]$ of degree 2 such that*

$$Q\left(\sum_{i=1}^{n} a_i v_i\right) = f(a_1, \dots, a_n)$$

for all $(a_1, \dots, a_n) \in k^n$.

Proof. Suppose that Q is a quadratic form. Put

$$f := \sum_{i=1}^{n} Q(v_i)X_i^2 + \sum_{i<j} B_Q(v_i, v_j)X_iX_j \in k[X_1, \dots, X_n]$$

which is either zero or homogeneous of degree 2. Now let $(a_1, \dots, a_n) \in k^n$. By property (Q2) of quadratic forms we have

$$Q\Big(\sum_{i=1}^{n} a_iv_i\Big) = Q(a_1v_1) + Q\Big(\sum_{i=2}^{n} a_iv_i\Big) + B_Q\Big(a_1v_1, \sum_{i=2}^{n} a_iv_i\Big)$$

from which it follows inductively that

$$\begin{aligned} Q\Big(\sum_{i=1}^{n} a_iv_i\Big) &= \sum_{i=1}^{n} Q(a_iv_i) + \sum_{i=1}^{n} B_Q\Big(a_iv_i, \sum_{j=i+1}^{n} a_jv_j\Big) \\ &= \sum_{i=1}^{n} a_i^2 Q(v_i) + \sum_{i<j} a_ia_jB_Q(v_i, v_j) \\ &= f(a_1, \dots, a_n). \end{aligned}$$

Then since $Q \neq 0$, we must also have $f \neq 0$, so f is homogeneous of degree 2.

We turn to the converse. Since f is homogeneous of degree 2, Q clearly satisfies (Q1). In order to prove bilinearity of B_Q, it suffices to consider the monomials of f, which are of the form X_iX_j for $i, j \in \{1, \dots, n\}$. But if $a = (a_1, \dots, a_n), b = (b_1, \dots, b_n) \in k^n$, then

$$X_iX_j(a + b) - X_iX_j(a) - X_iX_j(b) = a_ib_j + b_ia_j$$

which is bilinear in a and b. It follows that B_Q is bilinear, finishing the proof. □

By definition, quadratic forms and symmetric bilinear forms are strongly connected. In fact, (2.2) implies that if $\operatorname{char} k \neq 2$, then the two theories agree:

Remark 2.14.

(a) Suppose that $\operatorname{char} k \neq 2$. If $Q\colon V \to k$ is a quadratic form, then we have $B_Q(v, v) = 2Q(v)$ for all $v \in V$ by (2.2), so that we can recover Q from B_Q as $Q(v) = \frac{1}{2}B_Q(v, v)$. Conversely, if B is a symmetric bilinear form on V, then it is easily seen that putting $Q(v) := \frac{1}{2}B(v, v)$ for $v \in V$ defines a quadratic form on V, with associated bilinear form $B_Q = B$. This may be summarized in saying that

$$\{\text{quadratic forms on } V\} \xrightarrow{\sim} \{\text{symmetric bilinear forms on } V\}, \ Q \mapsto B_Q,$$

is an isomorphism of k-vector spaces, where addition and scalar multiplication are defined pointwise for both sets. Hence, the theory of quadratic forms and the theory of symmetric bilinear forms are essentially the same in characteristic different from 2.

(b) Now assume that $\operatorname{char} k = 2$. Here, the situation is substantially different. If $Q\colon V \to k$ is a quadratic form, then equation (2.2) implies that B_Q must satisfy $B_Q(v, v) = 2Q(v) = 0$ for all $v \in V$. Hence, there are symmetric bilinear forms that are not of the form B_Q for a quadratic form Q. Even more, the symmetric bilinear form B_Q does not uniquely determine the quadratic form Q (cf. [Tay92], page 55). So the map $Q \mapsto B_Q$ considered in (a) is neither injective nor surjective in characteristic 2.

Thus, whenever we are in the case $\operatorname{char} k \neq 2$, the situation simplifies drastically. In contrast, if k is of characteristic 2, there often occur subtleties that might be difficult to deal with. We will see one more example for this now.

In Section 2.1 we have introduced the notion of a nondegenerate symmetric bilinear form and have seen that such forms have nice properties. It is therefore desirable to work with nondegenerate bilinear forms. However, it turns out that imposing this condition on the bilinear form associated to a quadratic form gives strong restrictions in characteristic 2:

Proposition 2.15. *Suppose that* $\operatorname{char} k = 2$. *Let Q be a quadratic form on V such that its associated bilinear form B_Q is nondegenerate. Then* $\dim V$ *is even.*

Proof. Since $\operatorname{char} k = 2$, equation (2.2) implies that $B_Q(v, v) = 0$ for all $v \in V$, that is, B_Q is alternating. But it is also assumed to be nondegenerate, so that Proposition 2.8 forces $\dim V$ to be even. ☐

A weaker condition is the following:

Definition 2.16. Let $Q\colon V \to k$ be a quadratic form. We say that Q is *regular*, if the subspace

$$\operatorname{rad} Q := \{\, v \in \operatorname{rad} B_Q \mid Q(v) = 0\} \leq \operatorname{rad} B_Q$$

satisfies $\operatorname{rad} Q = 0$.

In particular, Q is regular whenever B_Q is nondegenerate. In fact, if $\operatorname{char} k \neq 2$, then $\operatorname{rad} Q = \operatorname{rad} B_Q$ by Remark 2.14 (a), so that in this case the two conditions agree.

We take a brief look at restrictions.

Remark 2.17 (Restrictions of quadratic forms)**.** Let Q be a quadratic form on V and let $W \leq V$ be a subspace. Then clearly the restriction $Q\big|_W$ defines a quadratic form on W, with associated bilinear form $B_{Q|_W} = B_Q\big|_W$. In the following, if we talk about properties of a subspace $W \leq V$ that refer to a quadratic form, then we will always be considering it being equipped with the restriction of Q.

The extreme case is that the restriction to a subspace is the zero form. This situation has a special name:

Definition 2.18. Let $Q\colon V \to k$ be a quadratic form.

(a) A nonzero vector $0 \neq v \in V$ is called *singular* if $Q(v) = 0$, and *nonsingular* otherwise.

(b) A subspace $W \leq V$ is said to be *totally singular* if $Q\big|_W = 0$ and *maximal totally singular* if it is maximal w.r.t. inclusion among the totally singular subspaces.

Note that maximal totally singular subspaces clearly exist as V is finite-dimensional.

2.2.1 Maximal Totally Singular Subspaces and Lagrangian Decomposition

We take a closer look at totally singular subspaces for regular quadratic forms and investigate how large such a subspace can be.

Let $Q\colon V \to k$ be a regular quadratic form and suppose that $V \neq 0$. Then note that V itself cannot be totally singular: If so, then $B_Q = 0$, and $\operatorname{rad} B_Q = \operatorname{rad} Q = V$. But this is a contradiction. In particular, if $\dim V = 1$, then the zero subspace is a maximal totally singular subspace and there is no singular vector in V.

In presence of a totally singular subspace, the following instructive theorem yields a decomposition of V that will eventually be of great importance and which also gives an upper bound on the dimension of a totally singular subspace. It can be found in I.3.2 of [Che97]. Since the theorem will play a central role and we are going to use it very frequently, we give a detailed proof.

Theorem 2.19. *Let Q be a regular quadratic form on V and let $W \leq V$ be a totally singular subspace of dimension l, with basis $(w_1, \dots, w_l)$. Then there exist a totally singular subspace $U \leq V$ of dimension l and a basis $(u_1, \dots, u_l)$ of U such that*

(i) $B_Q(u_i, w_j) = \delta_{ij}$ *for all* $1 \leq i, j \leq l$,

(ii) $U \cap W = \{0\}$,

(iii) $B_Q\big|_{U \oplus W}$ *is nondegenerate. In particular,* $V = (U \oplus W) \perp (U \oplus W)^{\perp}$.

We furthermore have:

(iv) If W is a maximal totally singular subspace of V, then $Q(v) \neq 0$ for all elements $0 \neq v \in (U \oplus W)^{\perp}$.

Proof. The case $l = 0$ is trivial. So we may assume that $l \geq 1$. In order to define U, we inductively construct vectors $u_1, \dots, u_l \in V$ with $B(u_i, w_j) = \delta_{ij}$ for all $1 \leq i, j \leq l$ and the property that $\operatorname{span}(u_1, \dots, u_l)$ is totally singular.

Let $0 \leq p < l$ and suppose that we have already constructed $u_1, \dots, u_p \in V$ such that $B_Q(u_i, w_j) = \delta_{ij}$ for all $1 \leq i \leq p$ and $1 \leq j \leq l$ and such that $\operatorname{span}(u_1, \dots, u_p)$ is totally singular. Put $\tilde{W} := \operatorname{span}(\, w_j \mid j \neq p+1 \,) < W$. As W is totally singular and

Q is regular, we have $W \cap \operatorname{rad} B_Q \leq \operatorname{rad} Q = 0$, and analogously for $\tilde{W}$. Then Lemma 2.4 (iii) gives

$$\dim W^{\perp} = \dim V - \dim W < \dim V - \dim \tilde{W} = \dim \tilde{W}^{\perp}.$$

Hence, there exists $y \in V$ with $B_Q(y, w_j) = 0$ for all $j \neq p+1$ and $B_Q(y, w_{p+1}) \neq 0$. By scaling, we may assume that $B_Q(y, w_{p+1}) = 1$. Now set

$$y' := y - \sum_{t=1}^{p} B_Q(u_t, y) w_t.$$

Since W is totally singular, we have $B_Q\big|_W = 0$. With this, we compute

$$B_Q(y', w_j) = B_Q(y, w_j) - \sum_{t=1}^{p} B_Q(u_t, y) \underbrace{B_Q(w_t, w_j)}_{=0} = 0 - 0 = 0 \quad \text{for all } j \neq p+1,$$

$$B_Q(y', w_{p+1}) = B_Q(y, w_{p+1}) - \sum_{t=1}^{p} B_Q(u_t, y) \underbrace{B_Q(w_t, w_{p+1})}_{=0} = 1 - 0 = 1,$$

$$B_Q(u_i, y') = B_Q(u_i, y) - \sum_{t=1}^{p} B_Q(u_t, y) \underbrace{B_Q(u_i, w_t)}_{=\delta_{it}} = 0 \quad \text{for } i \leq p.$$

We put $u_{p+1} := y' - Q(y')w_{p+1}$. Then first of all,

$$B_Q(u_{p+1}, w_j) = B_Q(y', w_j) - Q(y') \underbrace{B_Q(w_{p+1}, w_j)}_{=0} = B_Q(y', w_j) = \delta_{p+1,j}$$

for all $1 \leq j \leq l$. Moreover, using the above calculations, we infer that

$$B_Q(u_i, u_{p+1}) = B_Q(u_i, y') - Q(y')B_Q(u_i, w_{p+1}) = 0 - 0 = 0 \qquad \text{for } i \leq p$$

and

$$\begin{aligned} Q(u_{p+1}) &= B_Q(y', -Q(y')w_{p+1}) + Q(y') + Q(-Q(y')w_{p+1}) \\ &= -Q(y') \underbrace{B(y', w_{p+1})}_{=1} + Q(y') + Q(y')^2 \underbrace{Q(w_{p+1})}_{=0} \\ &= 0. \end{aligned}$$

Since $\operatorname{span}(u_1, \ldots, u_p)$ is totally singular, these relations imply that also the space $\operatorname{span}(u_1, \ldots, u_p, u_{p+1})$ is totally singular. We thus indeed obtain $u_1, \ldots, u_l \in V$ with $B_Q(u_i, w_j) = \delta_{ij}$ for all $1 \leq i, j \leq l$ and the property that $\operatorname{span}(u_1, \ldots, u_l)$ is totally singular.

Define $U := \operatorname{span}(u_1, \ldots, u_l)$ which is a totally singuar subspace of V. For $j \in \{1, \ldots, l\}$ and $a_i \in k$, $i = 1, \ldots, l$ we have

$$B_Q\left(\sum_{i=1}^{l} a_i u_i, w_j\right) = \sum_{i=1}^{l} a_i B_Q(u_i, w_j) = a_j. \tag{$*$}$$

This shows that the u_i are linearly independent, so $(u_1, \dots, u_l)$ is a basis of U and $\dim U = l$. We check that the properties (i) to (iv) are met:

(i) This holds by construction.

(ii) If $v \in U \cap W$, then we may write $v = \sum_{i=1}^{l} a_i u_i$ for $a_i \in k$. From total singularity of W and $(*)$ we get that $0 = B_Q(v, w_j) = a_j$ for all j, that is, $v = 0$.

(iii) In the same way as above, $(*)$ shows that $U \cap W^\perp = 0$, and analogously one proves $U^\perp \cap W = 0$. Taking into account that $B_Q\big|_U = 0$ and $B_Q\big|_W = 0$ by total singularity, we infer that $(U \oplus W) \cap (U \oplus W)^\perp = 0$. Thus, the claim follows from Lemma 2.7.

(iv) Let W be a maximal totally singular subspace. For the sake of a contradiction, assume that there exists $0 \neq v \in (U \oplus W)^\perp$ with $Q(v) = 0$. Then

$$Q(w + av) = aB_Q(w, v) + Q(w) + a^2 Q(v) = 0 \qquad \text{for all } w \in W, a \in k,$$

which shows that $W + \operatorname{span}(v)$ is totally singular. By maximality of W, we must have $v \in W$, a contradiction to property (iii). ☐

Hence, if $W \leq V$ is totally singular, then we must have $\dim W \leq \lfloor \frac{\dim V}{2} \rfloor$. Over algebraically closed fields, totally singular subspaces of this maximum possible dimension exist:

Corollary 2.20. *Let Q be a regular quadratic form on V and suppose that k is algebraically closed. Let $W \leq V$ be a maximal totally singular subspace of V. Then $\dim W = \lfloor \frac{\dim V}{2} \rfloor$.*

Proof. Let U be as in Theorem 2.19 and let $v_1, v_2 \in (U \oplus W)^\perp$. For $a_1, a_2 \in k$ we have

$$Q(a_1 v_1 + a_2 v_2) = a_1^2 Q(v_1) + a_2^2 Q(v_2) + a_1 a_2 B_Q(v_1, v_2)$$

by (Q2). Thus, as k is algebraically closed, we find $(0, 0) \neq (a_1, a_2) \in k^2$ with the property $Q(a_1 v_1 + a_2 v_2) = 0$. By part (iv) of Theorem 2.19, we must then have $a_1 v_1 + a_2 v_2 = 0$ which shows $\dim(U \oplus W)^\perp \leq 1$. But by the same theorem,

$$\dim V = \dim(U \oplus W) + \dim(U \oplus W)^\perp = 2 \dim W + \dim(U \oplus W)^\perp.$$

The claim follows by distinguishing the cases $\dim V$ even and $\dim V$ odd. ☐

The above corollary in particular shows that under the given assumptions, all maximal totally singular subspaces of V have the same dimension. This statement is in fact true without any assumptions on k, as we will now see.

First, we need to introduce an important notion in the theory of quadratic forms.

Definition 2.21. Let V_1 and V_2 be finite-dimensional k-vector spaces and let $Q_1\colon V_1 \to k$ and $Q_2\colon V_2 \to k$ be quadratic forms. An *isometry* between Q_1 and Q_2 is a linear map $\sigma\colon V_1 \to V_2$ that satisfies $Q_2(\sigma(v)) = Q_1(v)$ for all $v \in V_1$. If there is an isometry between Q_1 to Q_2, then the quadratic forms are called *isometric.*

Lemma 2.22. *Let V_1 and V_2 be finite-dimensional k-vector spaces and let $Q_1\colon V_1 \to k$ and $Q_2\colon V_2 \to k$ be quadratic forms. Suppose that $\sigma\colon V_1 \to V_2$ is an isometry between Q_1 and Q_2. Then*

$$B_{Q_2}(\sigma(v), \sigma(w)) = B_{Q_1}(v, w) \quad \text{for all } v, w \in V_1.$$

In particular, if Q_1 is regular, then σ is injective.

Proof. The first claim is immediate from the definitions of B_{Q_i} and of an isometry. Now suppose that Q_1 is regular and let $v \in \ker \sigma$. If $w \in V_1$ is arbitrary, then

$$B_{Q_1}(v, w) = B_{Q_2}(\sigma(v), \sigma(w)) = B_{Q_2}(0, \sigma(w)) = 0,$$

showing $v \in \operatorname{rad} B_{Q_1}$. But also $Q_1(v) = Q_2(\sigma(v)) = Q_2(0) = 0$, so $v \in \operatorname{rad} Q_1$. Since Q_1 is regular, it follows that $v = 0$, that is, σ is injective. ☐

The lemma in particular shows that any isometry from a space with regular quadratic form to itself is invertible. The key tool for proving that all maximal totally singular subspaces of a vector space with regular quadratic form have the same dimension, is the following well-known theorem:

Theorem 2.23 (Witt's Extension Theorem)**.** *Let $Q\colon V \to k$ be a quadratic form and let $W_1, W_2 \leq V$ be subspaces such that $W_i \cap \operatorname{rad} B_Q = 0$ for $i = 1, 2$. Suppose that there is an isometry $\sigma\colon W_1 \to W_2$. Then there exists an isometry $\hat{\sigma}\colon V \to V$ with $\hat{\sigma}\big|_{W_1} = \sigma$.*

Proof. See [EKM08], Theorem 8.3. ☐

Corollary 2.24. *Let $Q\colon V \to k$ be a regular quadratic form. Then all maximal totally singular subspaces of V have the same dimension.*

Proof. Let W_1 and W_2 be maximal totally singular subspaces of V. Without loss of generality, we can assume that $\dim W_1 \leq \dim W_2$. The spaces being totally singular, we may construct an isometry

$$\sigma\colon W_1 \to W \leq W_2$$

from W_1 to a subspace W of W_2 with $\dim W_1 = \dim W$ simply by mapping a basis of W_1 to a basis of W. Now $W_i \cap \operatorname{rad} B_Q \leq \operatorname{rad} Q = 0$, so that we may apply Witt's Extension Theorem 2.23 in order to obtain an isometry $\hat{\sigma}\colon V \to V$ with $\hat{\sigma}\big|_{W_1} = \sigma$.

Then $\hat{\sigma}^{-1}(W_2)$ is totally singular with $W_1 \leq \hat{\sigma}^{-1}(W_2)$, so by maximality of W_1 we must have $W_1 = \hat{\sigma}^{-1}(W_2)$. But $\hat{\sigma}$ is a linear isomorphism by Lemma 2.22, giving $\dim W_1 = \dim W_2$, as claimed. ☐

This now allows us to make the following definition:

Definition 2.25. Let Q be a regular quadratic form on V. The common dimension of the maximal totally singular subspaces of V is called the *Witt index* of Q and denoted $m(Q)$.

Note that by Theorem 2.19 we always have $m(Q) \leq \lfloor \frac{\dim V}{2} \rfloor$. Furthermore, if k is algebraically closed, then $m(Q) = \lfloor \frac{\dim V}{2} \rfloor$ by Corollary 2.20. In the latter case of maximal Witt index the decomposition from Theorem 2.19 arising from a maximal totally singular subspace is particularly nice.

Definition 2.26. Let Q be a regular quadratic form on V of (maximal) Witt index $m(Q) = \lfloor \frac{\dim V}{2} \rfloor$. Then a decomposition

$$V = \begin{cases} U \oplus W, & \dim V \text{ even}, \\ (U \oplus W) \perp \operatorname{span}(z), & \dim V \text{ odd}, \end{cases}$$

where U and W are maximal totally singular subspaces of V that have appropriate bases such that the conditions of Theorem 2.19 are satisfied and where $\operatorname{span}(z) = (U \oplus W)^{\perp}$ and $Q(z) \neq 0$, is called a *Lagrangian decomposition* of V. If k is quadratically closed, we make the convention that z is chosen such that $Q(z) = 1$.

Note that by choosing a maximal totally singular subspace $W \leq V$ and a basis of that subspace, Theorem 2.19 shows that a Lagrangian decomposition always exists. The terminology is taken from [Bum13], p. 329.

Lagrangian decompositions will be crucial for explicit computations with elements of spin groups, see e.g. the examples in Section 5.1; in particular, they will also be used in Section 4.4 to determine a maximal torus and the root subgroups of the spin group.

2.2.2 Nondegenerate Quadratic Forms

We conclude the section on quadratic forms by introducing one more fundamental notion.

Definition 2.27. A quadratic form $Q\colon V \to k$ is called *nondegenerate* if it is regular and $\dim \operatorname{rad} B_Q \leq 1$.

This term is related to the previously introduced notions as follows:

Proposition 2.28. *Let $Q\colon V \to k$ be a quadratic form. The following hold:*

(i) If B_Q is nondegenerate, then Q is nondegenerate, which in turn implies that Q is regular.

(ii) Suppose that $\operatorname{char} k \neq 2$. Then Q is nondegenerate if and only if it is regular which in turn is equivalent to B_Q being nondegenerate.

(iii) *Suppose that* $\operatorname{char} k = 2$ *and that* $\dim V$ *is even. Then* Q *is nondegenerate if and only if* B_Q *is nondegenerate.*

(iv) *Suppose that* $\operatorname{char} k = 2$ *and that* $\dim V$ *is odd. Then* Q *is nondegenerate if and only if* $\dim \operatorname{rad} B_Q = 1$ *and* $Q\big|_{\operatorname{rad} B_Q} \neq 0$*. In this case, if* $0 \neq z \in \operatorname{rad} B_Q$*, then* z *is nonsingular and there is a subspace* $W \leq V$ *such that* $V = \operatorname{span}(z) \perp W$*.*

(v) *Suppose that* k *is quadratically closed. Then* Q *is nondegenerate if and only if it is regular.*

Proof. The first claim is clear. Then in order to prove (ii), it only remains to show that regularity of Q implies nondegeneracy of B_Q. But if $v \in \operatorname{rad} B_Q$, then $0 = B_Q(v, v) = 2Q(v)$ by (2.2). Since $\operatorname{char} k \neq 2$, this shows $\operatorname{rad} B_Q = \operatorname{rad} Q$ and thus proves the claim.

For (iii) and (iv) see [EKM08], Remark 7.21. For the additional statement in (iv) take W such that $V = \operatorname{span}(v) \oplus W$. Then the definition of the radical implies $V = \operatorname{span}(v) \perp W$. The last statement is the exercise on p. 114 of [Gro02]. ☐

Remark 2.29. It turns out that the notion of nondegeneracy is the correct condition to impose on a quadratic form Q in order for the geometric objects associated with Q to have the right properties, see [EKM08], p. 43. Thus, we will in the following mainly work under this assumption.

As we have seen above, if $\operatorname{char} k \neq 2$ or $\dim V$ is even, then this is the same as requiring the associated bilinear form to be nondegenerate, which is more convenient to work with. Since our final discussion focuses on the case $\operatorname{char} k \neq 2$, this explains why we in many places work under the assumption that B_Q is nondegenerate.

However, if one wants to include also the case $\operatorname{char} k = 2$ and $\dim V$ odd, one needs the more general setting of a nondegenerate quadraitc form, as was already indicated in Proposition 2.15. For a characterization of the notion of nondegeneracy of a quadratic form see also Lemma 7.16 in [EKM08].

When working in the context of nondegenerate quadratic forms and dealing with subspaces, it is important to know when the restriction of the quadratic form to the subspace is again nondegenerate, to fit into the assumptions. By Proposition 2.28, if $\operatorname{char} k \neq 2$ or the subspace in consideration is even-dimensional, this question is answered by Lemma 2.7. More generally, an important special case is the following:

Lemma 2.30. *Let* Q *be a nondegenerate quadratic form on* V *and suppose that* $V', V'' \leq V$ *are subspaces such that* $V = V' \perp V''$*. Then the restrictions* $Q\big|_{V'}$ *and* $Q\big|_{V''}$ *are nondegenerate.*

Proof. From orthogonality one easily deduces that

$$\operatorname{rad} B_Q = \operatorname{rad} B_Q\big|_{V'} \perp \operatorname{rad} B_Q\big|_{V''} \qquad \text{and} \qquad \operatorname{rad} Q \supseteq \operatorname{rad} Q\big|_{V'} \perp \operatorname{rad} Q\big|_{V''}.$$

As a consequence, both $Q\big|_{V'}$ and $Q\big|_{V''}$ are regular and the dimensions of $\operatorname{rad} B_Q\big|_{V'}$ and $\operatorname{rad} B_Q\big|_{V''}$ are bounded by 1, that is, $Q\big|_{V'}$ and $Q\big|_{V''}$ are nondegenerate. □

We finally have a look at special kinds of bases in relation to a nondegenerate quadratic form.

Lemma 2.31. *Let Q be a nondegenerate quadratic form on V.*

(i) Suppose that $\operatorname{char} k \neq 2$. *Then V has an orthogonal basis and all of these basis vectors are nonsingular.*

(ii) Suppose that $\operatorname{char} k = 2$ *and* $\dim V \geq 2$. *Then V does not have an orthogonal basis.*

Proof.

(i) By Theorem 2.11, there is an orthogonal basis $(e_1, \ldots, e_n)$ of V. Assume that $Q(e_i) = 0$ for some i. Then (2.2) yields $B_Q(e_i, e_i) = 0$, so that $e_i \in \operatorname{rad} B_Q$ due to orthogonality, a contradiction to Proposition 2.28 (ii).

(ii) Assume that there was an orthogonal basis $(e_1, \ldots, e_n)$. Then since $\operatorname{char} k = 2$, equation (2.2) gives $B_Q(e_i, e_i) = 0$ for all $i = 1, \ldots, n$. As in part (i), we infer that $e_1, \ldots, e_n \in \operatorname{rad} B_Q$, which is a contradiction to the assumption that Q is nondegenerate. □

Despite the absence of an orthogonal basis in characteristic 2, a weaker type of basis (nearly) always exists:

Proposition 2.32. *Let Q be a nondegenerate quadratic form on V. If* $\dim V \in \{2, 3\}$ *and* $\operatorname{char} k = 2$, *assume that* $|k| > 2$. *Then V has a basis consisting of nonsingular vectors.*

Proof. If $\operatorname{char} k \neq 2$, then we may for example take an orthogonal basis, see Lemma 2.31 (i). If $\operatorname{char} k = 2$ and $\dim V$ is even, then B_Q is nondegenerate by Proposition 2.28 (iii) and the claim is proven in Proposition 12.8 of [Gro02].

Now suppose that $\operatorname{char} k = 2$ and $\dim V$ is odd. Then by Proposition 2.28 (iv) there is a decomposition $V = \operatorname{span}(z) \perp W$ with z nonsingular. Since W is even-dimensional and $Q\big|_W$ is nondegenerate by Lemma 2.30, we find a basis of nonsingular vectors of W. Adding z to this basis gives a basis of V that consists of nonsingular vectors. □

2.3 The Orthogonal Group

Throughout this section, let Q be a nondegenerate quadratic form on V (cf. Remark 2.29). We denote its associated symmetric bilinear form by B.

We introduce the orthogonal and special orthogonal group associated with Q and collect some of their main properties, which will be needed later on. The interplay between the special orthogonal group and the spin group will play an important role for the study of the latter.

The material covered is taken from [Gro02], Chapters 5, 6 and 14, [Che97], Sections 1.4 and 1.5 and [Tay92], Chapter 7.

Definition 2.33. We define

$$\mathrm{O}(V) := \mathrm{O}(V,Q) := \{\,\sigma\colon V \to V \mid \sigma \text{ isometry}\,\}$$

and call it the *orthogonal group* of V (with respect to Q).

Since Q is nondegenerate, Lemma 2.22 gives

$$\mathrm{O}(V) = \{\,\sigma \in \mathrm{GL}(V) \mid Q(\sigma(v)) = Q(v) \text{ for all } v \in V\,\} \leq \mathrm{GL}(V), \tag{2.3}$$

which shows that $\mathrm{O}(V)$ is indeed a group. As to be expected, the orthogonal groups of isometric quadratic forms are essentially the same:

Proposition 2.34. *Let V_1 and V_2 be finite-dimensional k-vector spaces and let $Q_1\colon V_1 \to k$ and $Q_2\colon V_2 \to k$ be nondegenerate quadratic forms. Suppose that there is an isometry $\sigma\colon V_1 \to V_2$ between Q_1 and Q_2. Then $\mathrm{O}(V_1,Q_1) = \sigma^{-1}\,\mathrm{O}(V_2,Q_2)\sigma$. In particular, $\mathrm{O}(V_1,Q_1) \cong \mathrm{O}(V_2,Q_2)$.*

Proof. Both inclusions can be shown in a straight forward fashion. Let $\tau \in \mathrm{O}(V_2,Q_2)$ and let $v \in V_1$. Then using the isometry properties, we have

$$Q_1\big(\sigma^{-1}\tau\sigma(v)\big) = Q_2\big(\sigma\sigma^{-1}\tau\sigma(v)\big) = Q_2\big(\tau(\sigma(v))\big) = Q_2\big(\sigma(v)\big) = Q_1(v),$$

showing $\sigma^{-1}\tau\sigma \in \mathrm{O}(V_1,Q_1)$. Hence, $\mathrm{O}(V_1,Q_1) \supseteq \sigma^{-1}\,\mathrm{O}(V_2,Q_2)\sigma$. The proof of the inclusion $\sigma\,\mathrm{O}(V_1,Q_1)\sigma^{-1} \subseteq \mathrm{O}(V_2,Q_2)$ is analogous. □

We now establish some basic facts about $\mathrm{O}(V)$. Clearly, $\mathrm{O}(0) = 1$ is the trivial group. From now on, we assume that $V \neq 0$. The connection between quadratic forms and symmetric bilinear forms (cf. Remark 2.14) is expressed in the following lemma:

Lemma 2.35. *It holds that*

$$\mathrm{O}(V) \subseteq \{\,\sigma \in \mathrm{GL}(V) \mid B(\sigma(v),\sigma(w)) = B(v,w) \textit{ for all } v,w \in V\,\},$$

with equality if $\operatorname{char} k \neq 2$.

Proof. The first claim is immediate from Lemma 2.22. If $\operatorname{char} k \neq 2$, then (2.2) gives the reverse inclusion. $\square$

Corollary 2.36. *If* $\sigma \in \mathrm{O}(V)$*, then* $\det \sigma = \pm 1$.

Proof. Suppose first that $\operatorname{char} k \neq 2$ or that $\dim V$ is even, so that B is nondegenerate by Proposition 2.28. Let $\mathcal{B}$ be a basis of V and let $c_{\mathcal{B}} \colon V \to k$ denote the associated coordinate map. Then by Lemma 2.35 and (2.1) it holds that $\mathrm{O}(V)$ is contained in the set

$$\{\, \sigma \in \mathrm{GL}(V) \mid c_{\mathcal{B}}(\sigma(v))^{\top} M_{\mathcal{B}}(B) c_{\mathcal{B}}(\sigma(w)) = c_{\mathcal{B}}(v)^{\top} M_{\mathcal{B}}(B) c_{\mathcal{B}}(w) \text{ for all } v, w \in V \,\}.$$

From (1.1) we get $c_{\mathcal{B}}(\sigma(v)) = [\sigma]_{\mathcal{B}} c_{\mathcal{B}}(v)$. Bijectivity of the coordinate map then yields

$$\mathrm{O}(V) \subseteq \{\, \sigma \in \mathrm{GL}(V) \mid [\sigma]_{\mathcal{B}}^{\top} M_{\mathcal{B}}(B) [\sigma]_{\mathcal{B}} = M_{\mathcal{B}}(B) \,\}.$$

Since $\det M_{\mathcal{B}}(B) \neq 0$ by Lemma 2.5, we infer that any $\sigma \in \mathrm{O}(V)$ satisfies $(\det \sigma)^2 = (\det [\sigma]_{\mathcal{B}})^2 = 1$, that is, $\det \sigma = \pm 1$. For the case $\operatorname{char} k = 2$ (and $\dim V$ odd) see [Gro02], p. 127. $\square$

We will now see that orthogonal transformations of determinant -1 exist, by introducing an important family of such elements.

Definition 2.37. Let $u \in V$ with $Q(u) \neq 0$. Then the map

$$s_u \colon V \to V,\ v \mapsto v - \frac{B(v,u)}{Q(u)} u,$$

is called the *reflection along* u or *reflection through the hyperplane* $\operatorname{span}(u)^{\perp}$.

We derive some properties of these reflections.

Proposition 2.38. *Let* $u \in V$ *with* $Q(u) \neq 0$*. The reflection along* u *has the following properties:*

- *(i)* $s_u \in \mathrm{O}(V)$.
- *(ii)* $s_{cu} = s_u$ *for all* $c \in k^{\times}$.
- *(iii)* $s_u(u) = -u$ *and if* $v \perp u$ *then* $s_u(v) = v$*. In particular,* $s_u^2 = \mathrm{id}_V$.
- *(iv)* $\det s_u = -1$.

Proof.

- (i) Clearly, s_u is linear. For $v \in V$, the defining properties of a quadratic form give

$$\begin{aligned} Q(s_u(v)) &= Q\left(v - \frac{B(v,u)}{Q(u)}u\right) \\ &= Q(v) + Q\left(-\frac{B(v,u)}{Q(u)}u\right) + B\left(v, -\frac{B(v,u)}{Q(u)}u\right) \\ &= Q(v) + \frac{B(v,u)^2}{Q(u)^2}Q(u) - \frac{B(v,u)}{Q(u)}B(v,u) \\ &= Q(v), \end{aligned}$$

so indeed $s_u \in \mathrm{O}(V)$.

(ii) This holds by bilinearity of B and (Q1).

(iii) The first claim follows directly from (2.2), while the second claim is trivial. For the additional statement first suppose that $\operatorname{char} k \neq 2$ and put $U := \operatorname{span}(u)$. Since here $B(u,u) = 2Q(u) \neq 0$, the restriction $B\big|_U$ is nondegenerate. Lemma 2.7 implies that $V = U \perp U^\perp$, so that the statement $s_u^2 = \mathrm{id}_V$ follows from the two claims just shown. Now if $\operatorname{char} k = 2$, then for $v \in V$ we simply compute

$$\begin{aligned} s_u^2(v) &= s_u\left(v - \frac{B(v,u)}{Q(u)}u\right) \\ &= v - \frac{B(v,u)}{Q(u)}u - \frac{B\left(v - \frac{B(v,u)}{Q(u)}u, u\right)}{Q(u)}u \\ &= v - 2\frac{B(v,u)}{Q(u)}u + \frac{B(v,u)B(u,u)}{Q(u)^2}u \\ &= v, \end{aligned}$$

where we used $B(u,u) = 2Q(u) = 0$.

(iv) If $\operatorname{char} k = 2$, then as $(\det s_u)^2 = 1$ by (iii), we have $\det s_u = 1 = -1$. Otherwise, $V = U \perp U^\perp$ with $U = \operatorname{span}(u)$ as shown in the proof of part (iii). With respect to a basis according to this decomposition, the matrix of s_u has the form $\operatorname{diag}(-1, 1, \ldots, 1)$, giving the result. □

The following subgroup of $\mathrm{O}(V)$ is of great importance.

Definition 2.39. The *special orthogonal group* $\mathrm{SO}(V)$ of V (with respect to Q) is defined to be the kernel of the determinant homomorphism $\det\colon \mathrm{O}(V) \to \{\pm 1\}$ if $\operatorname{char} k \neq 2$ or $\dim V$ is odd, and is defined to be the kernel of the so-called pseudodeterminant $d\colon \mathrm{O}(V) \to \mathbb{Z}_2$ if $\operatorname{char} k = 2$ and $\dim V$ is even. For the latter, see [Gro02], pages 129–131 or [Tay92], page 160.

Corollary 2.40. *We have* $|\mathrm{O}(V) : \mathrm{SO}(V)| = 2$ *unless* $\operatorname{char} k = 2$ *and* $\dim V$ *is odd, in which case* $\mathrm{O}(V) = \mathrm{SO}(V)$.

Proof. From Proposition 2.38 (iv) it follows that $\det\colon \mathrm{O}(V) \to \{\pm 1\}$ is surjective, proving the claim in case $\operatorname{char} k \neq 2$ or $\dim V$ is odd. For the remaining case we refer to [Gro02], pages 130–131. ☐

A further fundamental property of the reflections along nonsingular vectors is that in case that B is nondegenerate they form a generating system of $\mathrm{O}(V)$, as the following famous theorem shows:

Theorem 2.41 (E. Cartan-Dieudonné)**.** *If* $\operatorname{char} k \neq 2$*, then every element of* $\mathrm{O}(V)$ *is a product of at most* $\dim V$ *reflections* s_u *where* $u \in V$ *with* $Q(u) \neq 0$*. In particular, these reflections generate the orthogonal group* $\mathrm{O}(V)$*.*

If $\operatorname{char} k = 2$ *and* $\dim V$ *is even, then the orthogonal group is still generated by the reflections along nonsingular vectors, except in the case where* $|k| = 2$*,* $\dim V = 4$ *and* Q *has Witt index* 2*.*

Proof. A proof for $\operatorname{char} k \neq 2$ can for example be found in the books [Lam05] (Theorem I.7.1) and [Gro02] (Theorem 6.6). A proof under the assumption that B is nondegenerate (which then covers also the remaining case by Proposition 2.28) is given in [Che97], I.5.1. ☐

In terms of this generating system, the special orthogonal group may be described as follows:

Proposition 2.42. *Suppose that* B *is nondegenerate and that we are not in the case where* $|k| = 2$*,* $\dim V = 4$ *and* Q *has Witt index* 2*. Then it holds that*

$$\mathrm{SO}(V) = \langle\, s_u s_v \mid u, v \in V \text{ with } Q(u), Q(v) \neq 0 \,\rangle \leq \mathrm{O}(V)$$

is the subgroup of $\mathrm{O}(V)$ *consisting of the products of an even number of reflections.*

Proof. Suppose first that $\operatorname{char} k \neq 2$. Then $\mathrm{SO}(V) = \{\, \sigma \in \mathrm{O}(V) \mid \det \sigma = 1 \,\}$. Since $\mathrm{O}(V)$ is generated by reflections by Theorem 2.41 and reflections have determinant -1 by Proposition 2.38 (iv), the claim follows. For the case $\dim V$ even and $\operatorname{char} k = 2$ see [Tay92], Theorem 11.44. ☐

This also provides an alternative way to define the special orthogonal group. Theorem 2.41 and Proposition 2.42 will be fundamental tools for establishing the connection between the (s)pin group and the (special) orthogonal group in Section 3.3.

3 Clifford Algebras

Throughout this chapter, V is a vector space over k with $n := \dim V < \infty$ and Q is a quadratic form on V with associated (symmetric) bilinear form B.

Building on Chapters 1 and 2, we introduce the notion of a Clifford algebra which will be fundamental for our study of spin groups as well as spin representations. After thoroughly examining the structure of these algebras, we eventually construct the spin groups as subgroups of the units of Clifford algebras.

3.1 Basic Properties

In this section, we introduce Clifford algebras and deduce some fundamental properties of these. Here, we do not make any assumptions on Q. The material is fairly standard and can be found in many textbooks. For most of the section, we follow the approach from [Gro02], Chapters 8 and 13 and [Lam05], Section V.1. See also the expositions in [BtD85], [Che97], [Jac89], [Knu91] and [Mei13].

We define Clifford algebras via a universal property and afterwards prove uniqueness and existence (see Propositions 3.2 and 3.3). There are several other options, including first constructing the Clifford algebra explicitly and then deducing its universal property (see Chapter 14 of [Lou01] for a review on possible definitions). We opted for the given approach because most of the time we will use the Clifford algebra as an abstract object satisfying a universal property rather than employing its concrete construction.

Definition 3.1. A *Clifford algebra* for (V, Q) is a k-algebra C together with a linear map $\varepsilon\colon V \to C$ such that the following two axioms hold:

(C1) $\varepsilon(v)^2 = Q(v) \cdot 1$ for all $v \in V$.

(C2) If A is a k-algebra and $\varphi\colon V \to A$ is a linear map satisfying $\varphi(v)^2 = Q(v) \cdot 1$ for all $v \in V$, then there exists a unique algebra homomorphism $\hat{\varphi}\colon C \to A$ such that $\varphi = \hat{\varphi} \circ \varepsilon$.

$$\begin{tikzcd} V \arrow[r, "\varepsilon"] \arrow[dr, "\varphi"'] & C \arrow[d, dotted, "\exists!\ \hat{\varphi}"] \\ & A \end{tikzcd}$$

We will also write $C = C(V) = C(Q) = C(V, Q)$ if necessary.

Recall that if A is a k-algebra, then we view k as a subalgebra of A via $c \mapsto c \cdot 1$ and commonly write c for the element $c \cdot 1$ of A where $c \in k$. For example, axiom (C1) will frequently be written as $\varepsilon(v)^2 = Q(v)$.

Note that for the bilinear form B, axiom (C1) means that

$$\begin{aligned} B(v,w) &= Q(v+w) - Q(v) - Q(w) \\ &= \varepsilon(v+w)^2 - \varepsilon(v)^2 - \varepsilon(w)^2 \\ &= \varepsilon(v)\varepsilon(w) + \varepsilon(w)\varepsilon(v) \end{aligned}$$

for $v, w \in V$.

Proposition 3.2 (Uniqueness of Clifford algebras)**.** *A Clifford algebra for* (V,Q) *is unique up to isomorphism of* k*-algebras.*

Proof. Suppose that C_1 and C_2 are two Clifford algebras for (V,Q), with linear maps $\varepsilon_1\colon V \to C_1$, resp. $\varepsilon_2\colon V \to C_2$ attached to them. Applying (C2) to these linear maps, we obtain algebra homomorphisms $\widehat{\varepsilon_1}\colon C_2 \to C_1$ and $\widehat{\varepsilon_2}\colon C_1 \to C_2$ such that $\varepsilon_1 = \widehat{\varepsilon_1} \circ \varepsilon_2$ resp. $\varepsilon_2 = \widehat{\varepsilon_2} \circ \varepsilon_1$. This results in $\varepsilon_1 = \widehat{\varepsilon_1} \circ \widehat{\varepsilon_2} \circ \varepsilon_1$. But by (C2), id_{C_1} is the unique algebra endomorphism of C_1 with this property, so we must have $\widehat{\varepsilon_1} \circ \widehat{\varepsilon_2} = \mathrm{id}_{C_1}$. Analogously, $\widehat{\varepsilon_2} \circ \widehat{\varepsilon_1} = \mathrm{id}_{C_2}$, proving that $\widehat{\varepsilon_2}\colon C_1 \to C_2$ is an isomorphism of k-algebras. ☐

Proposition 3.3 (Existence of Clifford algebras)**.** *Let* $T := T(V)$ *be the tensor algebra of* V *and consider its ideal*

$$I := \langle\, v \otimes v - Q(v) \mid v \in V \,\rangle \trianglelefteq T.$$

Then $C := T/I$ *is a Clifford algebra for* (V,Q)*, the linear map* $\varepsilon\colon V \to C$ *being the restriction to* V *of the canonical projection* $\pi\colon T \to C = T/I$*.*

Proof. By definition of I we have

$$\varepsilon(v)^2 = \pi(v)^2 = \pi(v \otimes v) = v \otimes v + I = Q(v) + I = Q(v) \cdot 1_{T/I}$$

for all $v \in V$, that is, (C1) holds.

In order to prove (C2) let A be a k-algebra and let $\varphi\colon V \to A$ be a linear map with $\varphi(v)^2 = Q(v) \cdot 1$ for all $v \in V$. By the universal property of T (Proposition 1.32), φ extends to an algebra homomorphism $\Phi\colon T \to A$. For $v \in V$ we have

$$\Phi(v \otimes v - Q(v)) = \Phi(v)^2 - \Phi(Q(v)) = \varphi(v)^2 - Q(v) \cdot 1 = 0,$$

showing that $I \subseteq \ker \Phi$. Thus, Φ gives rise to an algebra homomorphism

$$\hat{\varphi}\colon C = T/I \to A,\ x + I \mapsto \Phi(x).$$

For $v \in V$ this means that $(\hat{\varphi} \circ \varepsilon)(v) = \hat{\varphi}(v + I) = \Phi(v) = \varphi(v)$, i.e., $\hat{\varphi} \circ \varepsilon = \varphi$. It remains to show that $\hat{\varphi}$ is unique with this property. By Proposition 1.31 (ii), V generates T as an algebra, so $\varepsilon(V) = \pi(V)$ generates $C = T/I$ as an algebra. It follows that the algebra homomorphism $\hat{\varphi}\colon C \to A$ is already uniquely determined by the condition $\hat{\varphi} \circ \varepsilon = \varphi$, establishing (C2). ☐

This means that we can talk about *the* Clifford algebra associated to the tuple (V, Q). For the remainder of this section, we will denote it by C and will write $\varepsilon\colon V \to C$ for the linear map attached to it. We now start to investigate its properties.

The realization of the Clifford algebra as a quotient of the tensor algebra will be useful to establish some basic facts about C. We first look at an example.

Example 3.4.

(a) If $Q = 0$, then the ideal in the above proposition becomes $\langle\, v \otimes v \mid v \in V \,\rangle$ which means that $C(V, 0) = \bigwedge V$ is exactly the exterior algebra of V. Thus, the Clifford algebra may be viewed as a generalization of the exterior algebra.

(b) If $V = 0$, then $T(V) = k$ and the ideal from above is the zero ideal. So in this case the Clifford algebra is just the ground field k.

(c) We consider the case $\dim V = 1$. Pick $0 \neq v \in V$ and let $c := Q(v) \in k^\times$. By Example 1.33, there is an isomorphism $T(V) \cong k[X]$, $v \mapsto X$, under which the ideal I from Proposition 3.3 corresponds to $\langle X^2 - c\rangle$. Thus in this case we have $C \cong k[X]/\langle X^2 - c\rangle$, a field if c is not a square in k and a commutative ring with zero divisors otherwise.

(d) Suppose that $k = \mathbb{R}$ and $V = \mathbb{R}^n$ for $n \geq 1$. We consider the quadratic form $R_n\colon V \to k$, $(x_1, \ldots, x_n) \mapsto -\sum_{i=1}^n x_i^2$ and write $C_n := C(\mathbb{R}^n, -\sum x_i^2)$ for the corresponding Clifford algebra. These Clifford algebras are sometimes referred to as the *classical Clifford algebras* and are studied extensively for example in [ABS64].

By part (c), as $R_1(1) = -1$, it holds that $C_1 \cong \mathbb{R}[X]/\langle X^2 + 1\rangle \cong \mathbb{C}$ is the $\mathbb{R}$-algebra of complex numbers. In fact, it is possible to determine all the algebras C_n for $n \geq 1$, see [ABS64], §4.

Corollary 3.5. *The Clifford algebra C is generated by $\varepsilon(V)$ as an algebra.*

Proof. This has been shown in the proof of Proposition 3.3. ☐

We can also easily find a vector space generating system for C.

Lemma 3.6. *Let $(v_1, \ldots, v_n)$ be a basis of V. Then the set*

$$\{\, \varepsilon(v_{i_1}) \cdots \varepsilon(v_{i_r}) \mid 1 \leq i_1 < \cdots < i_r \leq n,\ r \in \mathbb{N} \,\}$$

generates C as a vector space (note that we allow $r = 0$ in which case the product is the empty product, equal to 1). In particular, $\dim C \leq 2^{\dim V}$.

Proof. This follows from Corollary 3.5, using property (C1) and the equation $B(v, w) = \varepsilon(v)\varepsilon(w) + \varepsilon(w)\varepsilon(v)$ for $v, w \in V$, cf. [Knu91], IV.1.5. See also [Che97], II.1.2. ☐

Our aim is to show that in fact $\dim C = 2^{\dim V}$, so that if $(v_1, \dots, v_n)$ is a basis of V, then the set above forms a basis of C. To this end, we will establish a $\mathbb{Z}_2$-grading on C which will prove very useful in the following.

Definition 3.7. We put

$$C_0 := \operatorname{span}(\,\varepsilon(v_1)\cdots\varepsilon(v_r) \mid v_i \in V,\, r \in \mathbb{N} \text{ even}\,),$$
$$C_1 := \operatorname{span}(\,\varepsilon(v_1)\cdots\varepsilon(v_r) \mid v_i \in V,\, r \in \mathbb{N} \text{ odd}\,).$$

By Lemma 3.6, clearly $C = C_0 + C_1$. To show that this in fact defines a $\mathbb{Z}_2$-grading on C, we will again use that C can be thought of as a quotient of the tensor algebra. Recall that $T := T(V)$ is a $\mathbb{Z}_2$-graded algebra with homogeneous parts

$$T_0 = \bigoplus_{i \text{ even}} V^{\otimes i}, \qquad T_1 = \bigoplus_{i \text{ odd}} V^{\otimes i},$$

see Proposition 1.31 (iv). We now show the spaces C_0 and C_1 defined above are exactly the homogeneous parts of the grading of C that is inherited from the grading of T:

Proposition 3.8 ($\mathbb{Z}_2$-grading of C)**.** *Using the notation from Proposition 3.3 and from above, we have $C_0 = \pi(T_0)$ and $C_1 = \pi(T_1)$. In particular, $C = C_0 \oplus C_1$ and this decomposition defines a $\mathbb{Z}_2$-grading on C.*

Proof. The identities $C_0 = \pi(T_0)$ and $C_1 = \pi(T_1)$ immediately follow from the equation

$$\pi(v_1 \otimes \cdots \otimes v_r) = \pi(v_1)\cdots\pi(v_r) = \varepsilon(v_1)\cdots\varepsilon(v_r)$$

for $v_i \in V$. Now $T = T_0 \oplus T_1$ is $\mathbb{Z}_2$-graded and with respect to this grading, the ideal $I = \langle\, v \otimes v - Q(v) \mid v \in V \,\rangle$ is homogeneous by Proposition 1.22, since it is generated by homogeneous elements (of degree 0). But then Proposition 1.23 implies that the quotient $C = T/I$ also carries the structure of a $\mathbb{Z}_2$-graded algebra, with homogeneous parts $\pi(T_0) = C_0$ and $\pi(T_1) = C_1$. ☐

Recall that by Lemma 1.16, this means that C_0 is a subalgebra of C with $k \subseteq C_0$ and note also that $\varepsilon(V) \subseteq C_1$. The next proposition describes the Clifford algebra of an orthogonal direct sum and is a key ingredient in determining the dimension of C.

Proposition 3.9. *If $V', V'' \leq V$ are subspaces such that $V = V' \perp V''$, then there is a $\mathbb{Z}_2$-graded k-algebra isomorphism $C(V) \cong C(V') \,{}^{\mathbb{Z}_2}\!\!\otimes C(V'')$.*

Proof. Denote by $\varepsilon_1\colon V' \to C(V')$ and $\varepsilon_2\colon V'' \to C(V'')$ the linear maps attached to $C(V')$ and $C(V'')$, respectively. We define a linear map

$$\varphi\colon V = V' \perp V'' \to C(V') \,{}^{\mathbb{Z}_2}\!\!\otimes C(V''),\; v' + v'' \mapsto \varepsilon_1(v') \otimes 1 + 1 \otimes \varepsilon_2(v'').$$

Now let $v = v' + v'' \in V$, where $v' \in V'$ and $v'' \in V''$. Using the definition of multiplication in the $\mathbb{Z}_2$-graded tensor product and the fact that $\varepsilon_1(v')$ and $\varepsilon_2(v'')$ are homogeneous of degree 1, we obtain

$$\begin{aligned}\varphi(v)^2 &= \varepsilon_1(v')^2 \otimes 1 + \varepsilon_1(v') \otimes \varepsilon_2(v'') - \varepsilon_1(v') \otimes \varepsilon_2(v'') + 1 \otimes \varepsilon_2(v'')^2\\ &= Q(v') \otimes 1 + 1 \otimes Q(v'')\\ &= (Q(v') + Q(v'')) \cdot (1 \otimes 1)\\ &= Q(v) \cdot 1_{C(V')^{\mathbb{Z}_2}\otimes C(V'')},\end{aligned}$$

where the last equality holds by orthogonality of v' and v''. Thus, by axiom (C2), there exists an algebra homomorphism $\hat{\varphi}\colon C(V) \to C(V')\ {}^{\mathbb{Z}_2}\!\otimes C(V'')$ with $\hat{\varphi} \circ \varepsilon = \varphi$. It is $\mathbb{Z}_2$-graded by Lemma 1.24 and Corollary 3.5.

Conversely, and again using (C2), the linear maps $\psi_1 := \varepsilon\big|_{V'}$ and $\psi_2 := \varepsilon\big|_{V''}$ give rise to algebra homomorphisms $\hat{\psi_1}\colon C(V') \to C(V)$ and $\hat{\psi_2}\colon C(V'') \to C(V)$ with $\hat{\psi_i} \circ \varepsilon_i = \psi_i$, which are again $\mathbb{Z}_2$-graded by Lemma 1.24. For $v' \in V'$ and $v'' \in V''$ by orthogonality we have

$$\begin{aligned}\hat{\psi_1}(\varepsilon_1(v'))\hat{\psi_2}(\varepsilon_2(v'')) + \hat{\psi_2}(\varepsilon_2(v''))\hat{\psi_1}(\varepsilon_1(v')) &= \varepsilon(v')\varepsilon(v'') + \varepsilon(v'')\varepsilon(v')\\ &= B(v', v'')\\ &= 0,\end{aligned}$$

which implies that $\hat{\psi_1}(x')\hat{\psi_2}(x'') = (-1)^{\delta(x')\delta(x'')}\hat{\psi_2}(x'')\hat{\psi_1}(x')$ for homogeneous elements $x' \in C(V')$ and $x'' \in C(V'')$, where $\delta(\cdot) \in \{0, 1\}$ denotes their degree. Hence, we may apply Proposition 1.27 (i) to obtain a $\mathbb{Z}_2$-graded algebra homomorphism

$$\Psi\colon C(V')\ {}^{\mathbb{Z}_2}\!\otimes C(V'') \to C(V),\ x' \otimes x'' \mapsto \hat{\psi_1}(x')\hat{\psi_2}(x'').$$

We check that $\hat{\varphi}$ and Ψ are inverse to each other. For $v' \in V'$ and $v'' \in V''$ we have

$$\begin{aligned}(\Psi \circ \hat{\varphi})\big(\varepsilon(v' + v'')\big) &= \Psi\big(\varepsilon_1(v') \otimes 1 + 1 \otimes \varepsilon_2(v'')\big)\\ &= \hat{\psi_1}\big(\varepsilon_1(v')\big) + \hat{\psi_2}\big(\varepsilon_2(v'')\big)\\ &= \varepsilon(v' + v'').\end{aligned}$$

Since $\varepsilon(V)$ generates $C(V)$ as an algebra by Corollary 3.5, this implies that $\Psi \circ \hat{\varphi} = \mathrm{id}_{C(V)}$. In order to show that also $\hat{\varphi} \circ \Psi = \mathrm{id}_{C(V')^{\mathbb{Z}_2}\otimes C(V'')}$, we employ the algebra generating system from Proposition 1.25 (ii). For $v' \in V'$ we have

$$(\hat{\varphi} \circ \Psi)(\varepsilon_1(v') \otimes 1) = \hat{\varphi}(\psi_1(v')) = \hat{\varphi}(\varepsilon(v')) = \varphi(v') = \varepsilon_1(v') \otimes 1,$$

and similarly one proceeds for the elements $1 \otimes \varepsilon_2(v'')$. This finishes the proof. □

Note that by Example 3.4 (a), when applying this proposition to the quadratic form $Q = 0$, we partly recover Proposition 1.38. With the aid of the above proposition, we can finally show the follwing:

Theorem 3.10. *Let C be the Clifford algebra for (V, Q) with linear map $\varepsilon\colon V \to C$ attached to it. Then the following hold:*

- *(i)* $\dim C = 2^{\dim V}$*,*
- *(ii) if $(v_1, \ldots, v_n)$ is a basis of V, then*

$$(\, \varepsilon(v_{i_1}) \cdots \varepsilon(v_{i_r}) \mid 1 \le i_1 < \cdots < i_r \le n,\, r \in \mathbb{N}\,)$$

  is a basis of C,
- *(iii) the linear map ε is injective.*

Proof. For the first claim we do induction on $\dim V$. If $\dim V = 0$, then $C = k$ by Example 3.4 (b) and the claim holds. In case $\dim V = 1$, we have $C \cong k[X]/\langle X^2 - c\rangle$ by part (c) of Example 3.4, where $v \in V \setminus \{0\}$ and $c = Q(v)$. Here, the residue classes of 1 and X form a k-basis of C, so indeed $\dim C = 2 = 2^{\dim V}$.

Now suppose that $\dim V \ge 2$. Assume first $\operatorname{char} k \ne 2$. Then V has an orthogonal basis by Theorem 2.11 which allows us to find subspaces $V', V'' \le V$ with $1 \le \dim V', \dim V'' < \dim V$ and such that $V = V' \perp V''$. Induction and Proposition 3.9 give

$$\dim C = \dim C(V') \,{}^{\mathbb{Z}_2}\!\!\otimes C(V'') = \dim C(V') \cdot \dim C(V'') = 2^{\dim V'} \cdot 2^{\dim V''} = 2^{\dim V}.$$

If $\operatorname{char} k = 2$ and $\operatorname{rad} B \ne 0$, we have $V = \operatorname{span}(v) \perp V''$ for $0 \ne v \in \operatorname{rad} B$ and V'' a complement of $\operatorname{span}(v)$, and the above argument applies. If B is nondegenerate, then one may show that there is a decomposition $V = V' \perp V''$ with $\dim V' = 2$ and that $\dim C(V') = 4$, so that one may again apply Proposition 3.9, see [Gro02], Proposition 13.8. This proves (i).

Part (ii) now follows from Lemma 3.6 and (i) as the given set has cardinality $2^{\dim V}$. In order to prove the third claim let $0 \ne v \in V$. By (ii), the element $\varepsilon(v) \in C$ is linearly independent (extend v to a basis of V), which implies $\varepsilon(v) \ne 0$. ☐

Corollary 3.11. *For $V \ne 0$ the homogeneous parts of C have dimensions* $\dim C_0 = \dim C_1 = 2^{\dim V - 1}$.

Proof. Let $(v_1, \ldots, v_n)$ be a basis of V. Then for $j \in \{0, 1\}$, the set

$$B_j := \{\, \varepsilon(v_{i_1}) \cdots \varepsilon(v_{i_r}) \mid 1 \le i_1 < \cdots < i_r \le n,\, r \equiv j \pmod 2 \,\}$$

is clearly contained in C_j. But by Theorem 3.10 (ii), $B_0 \cup B_1$ is a basis of C and we know that $C = C_0 \oplus C_1$, so B_j must in fact be a basis of C_j. ☐

We have seen in Theorem 3.10 (iii) that the linear map $\varepsilon\colon V \to C$ is injective. This gives us a canonical way to consider V as a subspace of C. Henceforth, if $v \in V$, we will simply write v for the element $\varepsilon(v)$ of C. For example, the Clifford axioms become:

$$\begin{tikzcd} V \arrow[r, hook] \arrow[dr, "\varphi"'] & C \arrow[d, dotted, "\exists!\ \hat{\varphi}"] \\ & A \end{tikzcd}$$

(C1) $v^2 = Q(v)$ for all $v \in V$.

(C2) If A is a k-algebra and $\varphi\colon V \to A$ is a linear map satisfying $\varphi(v)^2 = Q(v)$ for all $v \in V$, then there is a unique algebra homomorphism $\hat{\varphi}\colon C \to A$ extending φ.

Recall that (C1) implies that

$$vw + wv = B(v, w) \qquad \text{for all } v, w \in V \tag{3.1}$$

and that V generates C as an algebra by Corollary 3.5.

The next proposition addresses the question in which way Clifford algebras are compatible with isometries of quadratic forms. It can be found on p. 29 of [Mei13].

Proposition 3.12. *Let V_1 and V_2 be two finite-dimensional k-vector spaces and let $Q_1\colon V_1 \to k$ and $Q_2\colon V_2 \to k$ be quadratic forms. Suppose that $\sigma\colon V_1 \to V_2$ is an isometry between Q_1 and Q_2.*

Then σ extends to a $\mathbb{Z}_2$-graded algebra homomorphism $C(\sigma)\colon C(V_1, Q_1) \to C(V_2, Q_2)$. We have $C(\mathrm{id}_V) = \mathrm{id}_{C(V)}$ and $C(\tau \circ \sigma) = C(\tau) \circ C(\sigma)$, if $\tau\colon V_2 \to V_3$ is an isometry between Q_2 and a third quadratic form.
In particular, if σ is bijective, then so is $C(\sigma)$, so that there is an isomorphism $C(V_1, Q_1) \cong C(V_2, Q_2)$ of $\mathbb{Z}_2$-graded algebras.

$$\begin{tikzcd} V_1 \arrow[r, hook] \arrow[d, "\sigma"] & C(V_1, Q_1) \arrow[d, "C(\sigma)"] \\ V_2 \arrow[r, hook] & C(V_2, Q_2) \end{tikzcd}$$

Proof. Being an isometry, $\sigma\colon V_1 \to V_2 \subseteq C(V_2, Q_2)$ satisfies $\sigma(v)^2 = Q_2(\sigma(v)) = Q_1(v)$ for all $v \in V_1$, so that it extends as claimed by axiom (C2). Here, $C(\sigma)$ is $\mathbb{Z}_2$-graded by Lemma 1.24. The maps from the further claims clearly agree on the respective algebra generating systems from Corollary 3.5, so they must be equal. ☐

We conclude this section by introducing three involutions associated with the Clifford algebra C that will play an important role for the definition of the spin group.

Proposition 3.13. *The map $V \to V \subseteq C$, $v \mapsto -v$ extends to an algebra homomorphism $\alpha\colon C \to C$ that has the following properties:*

(i) $\alpha^2 = \mathrm{id}_C$. *In particular, α is an automorphism.*

(ii) *We have $\alpha(x_0) = x_0$ for $x_0 \in C_0$ and $\alpha(x_1) = -x_1$ for $x_1 \in C_1$. In particular, if $\operatorname{char} k \neq 2$, then*

$$C_0 = \{\, x \in C \mid \alpha(x) = x \,\}, \qquad C_1 = \{\, x \in C \mid \alpha(x) = -x \,\}.$$

Proof. Clearly, $v \mapsto -v$ is linear and satisfies $(-v)^2 = v^2 = Q(v)$, so by (C2) it extends to an algebra homomorphism $\alpha\colon C \to C$. Since $\alpha^2(v) = v$ for all $v \in V$ and V generates C as an algebra, we have $\alpha^2 = \mathrm{id}_C$. The first two claims of (ii) follow from the definitions of C_0 and C_1 and the fact that

$$\alpha(v_1 \cdots v_r) = \alpha(v_1) \cdots \alpha(v_r) = (-1)^r v_1 \cdots v_r$$

for $v_i \in V$. Turning to the last claim, clearly $C_0 \subseteq \{\, x \in C \mid \alpha(x) = x \,\}$ by what we have just shown. Conversely, let $x \in C$ with $\alpha(x) = x$. Writing $x = x_0 + x_1$ with $x_i \in C_i$, this means

$$x_0 + x_1 = x = \alpha(x) = \alpha(x_0) + \alpha(x_1) = x_0 - x_1,$$

so $2x_1 = 0$. Since here $\operatorname{char} k \neq 2$, we infer that $x_1 = 0$, that is, $x = x_0 \in C_0$. The claim for C_1 is proved analogously. ☐

This gives an alternative way to define C_0 and C_1, if $\operatorname{char} k \neq 2$. Note that in characteristic 2, however, α is the identity on C, and this method does not carry over.

Proposition 3.14. *There exists a unique antihomomorphism $\tau\colon C \to C$ with $\tau\big|_V = \mathrm{id}_V$. It has the following properties:*

- *(i)* $\tau^2 = \mathrm{id}_C$. *In particular, τ is an antiautomorphism.*
- *(ii)* $\tau(C_0) = C_0$, $\tau(C_1) = C_1$.
- *(iii)* $\alpha \circ \tau = \tau \circ \alpha$.

Proof. By axiom (C2), the map $V \to V \subseteq C^{\mathrm{op}}$, $v \mapsto v$, extends uniquely to an algebra homomorphism $C \to C^{\mathrm{op}}$, that is, to an antihomomorphism $\tau\colon C \to C$ with $\tau\big|_V = \mathrm{id}_V$. For $v_i \in V$ we thus have $\tau(v_1 \cdots v_r) = v_r \cdots v_1$. From this and linearity of τ and α the remaining claims follow easily. ☐

Definition 3.15. The algebra automorphism $\alpha\colon C \to C$ from above is called the *main involution* of C, while the antiautomorphism $\tau\colon C \to C$ is called the *main antiautomorphism* of C. Their composition is denoted by $\bar{\cdot}$ and is called *conjugation* on C.

We immediately have:

Corollary 3.16.

- *(i) Conjugation is an antiautomorphism of C satisfying* $\bar{\cdot}^2 = \mathrm{id}_C$,
- *(ii)* $\overline{v} = -v$ *for all* $v \in V$,
- *(iii)* $\overline{C_0} = C_0$, $\overline{C_1} = C_1$.

Example 3.17. In the Clifford algebra $\mathbb{R}[X]/\langle X^2+1\rangle \cong \mathbb{C}$ from Example 3.4 (d), conjugation is just the ordinary complex conjugation (which can be seen by looking at the effect of conjugation on the basis elements).

We have constructed the three maps α, τ and $\bar{\cdot}$ as usual by using the universal property of the Clifford algebra. Alternatively, viewing the Clifford algebra as a quotient of the tensor algebra (see Proposition 3.3), they may be obtained from the related maps from Example 1.34 that are associated to the tensor algebra and leave the ideal $\langle\, v \otimes v - Q(v) \mid v \in V\,\rangle$ invariant (cf. [ABS64], p. 6).

Finally, we take a look at a special element of C whose relevance will become apparent in the next section. The following result may be found on page 35 of [Mei13] and in parts in Proposition I.3.3 of [LM89].

Lemma 3.18. *Suppose that V has an orthogonal basis $(e_1,\dots,e_n)$. We consider the element $\zeta := e_1\cdots e_n \in C$. It has the following properties:*

(i) $\zeta v = (-1)^{n-1} v\zeta$ *for all* $v \in V$,

(ii) $\overline{\zeta} = (-1)^{\frac{n(n+1)}{2}}\zeta$,

(iii) $\zeta^2 = (-1)^{\frac{n(n-1)}{2}} Q(e_1)\cdots Q(e_n)$.

Proof. The proof is based on the equations $e_i^2 = Q(e_i)$ for all i and $e_ie_j = -e_je_i$ for $i \neq j$ that follow from axiom (C1).

(i) Since the e_i form a basis of V, it suffices to prove this equation for $v = e_i$ where $i = 1,\dots,n$. Choosing one such i and swapping e_i with the other basis vectors an appropriate number of times, we calculate

$$\zeta e_i = (-1)^{n-i} e_1\cdots e_ie_ie_{i+1}\cdots e_n = (-1)^{n-i}(-1)^{i-1}e_i\cdot e_1\cdots e_n = (-1)^{n-1}e_i\zeta,$$

as claimed.

(ii) By Corollary 3.16 (i) and (ii) we have

$$\overline{\zeta} = (-1)^n e_n\cdots e_1 = (-1)^n(-1)^{n-1}\cdots(-1)e_1\cdots e_n = (-1)^{\frac{n(n+1)}{2}}\zeta,$$

again using the rules for swapping the basis vectors.

(iii) As before, we get

$$\begin{aligned}\zeta^2 &= e_1\cdots e_n\cdot e_1\cdots e_n\\ &= (-1)^{n-1}(-1)^{n-2}\cdots(-1)e_1^2\cdots e_n^2\\ &= (-1)^{\frac{n(n-1)}{2}}Q(e_1)\cdots Q(e_n),\end{aligned}$$

first executing $n-1$ swaps of e_1, then $n-2$ swaps of e_2, and so on. ☐

3.2 The Algebra Structure of C

Let again C denote the Clifford algebra for (V, Q).

In Theorem 3.10 we have determined the vector space structure of the Clifford algebra. In this section we now investigate the algebra structure of the $\mathbb{Z}_2$-graded algebra C and its even subalgebra C_0. This will be of particular interest for our study of spin representations later in Chapter 5.

The exposition is mainly based on [Knu91], Sections IV.2 and IV.3, [Che97], Section 2.2 and [GW09], Sections 6.1.2 and 6.1.3. See also [EKM08], Section II.11 and, for $\operatorname{char} k \neq 2$, Section 3.2 of [Mei13] and Section V.2 of [Lam05].

We start off with a computational lemma that will be used for constructing some explicit algebra homomorphisms and will also later become important for computations.

Lemma 3.19. *Suppose that Q is a regular quadratic form and has Witt index $m = \lfloor\frac{\dim V}{2}\rfloor$. Let $U, W \leq V$ be maximal totally singular subspaces with bases $(u_1, \ldots, u_m)$ and $(w_1, \ldots, w_m)$, respectively, that constitute a Lagrangian decomposition $V = U \oplus W$ resp. $V = (U \oplus W) \perp \operatorname{span}(z)$ of V. Then there are linear maps*

$$U \to \operatorname{End}(\textstyle\bigwedge W),\ u \mapsto \iota_u, \qquad W \to \operatorname{End}(\textstyle\bigwedge W),\ w \mapsto \lambda_w,$$

where λ_w is the map from Definition 1.40 and ι_u is defined by

$$\iota_u \colon \textstyle\bigwedge W \to \bigwedge W,\ z_1 \wedge \cdots \wedge z_r \mapsto \displaystyle\sum_{i=1}^{r} (-1)^{i-1} B(u, z_i) z_1 \wedge \cdots \wedge \widehat{z_i} \wedge \cdots \wedge z_r,$$

where $z_1, \ldots, z_r \in W$. If $\dim V$ is odd, there is an additional linear map $\operatorname{span}(z) \to \operatorname{End}(\bigwedge W)$, $az \mapsto \eta_a$, where

$$\eta_a \colon \textstyle\bigwedge W \to \bigwedge W,\ z_1 \wedge \cdots \wedge z_r \mapsto (-1)^r a\ z_1 \wedge \cdots \wedge z_r,$$

again for $z_1, \ldots, z_r \in W$. These maps have the following properties:

(i) We have $\iota_u^2 = \lambda_w^2 = 0$ and $\eta_a^2 = a^2 \mathrm{id}_{\wedge W}$ for all $u \in U$, $w \in W$ and $a \in k$.

(ii) It holds that

$$\iota_u \lambda_w + \lambda_w \iota_u = Q(u + w)\mathrm{id}_{\wedge W}, \qquad \iota_u \eta_a + \eta_a \iota_u = \lambda_w \eta_a + \eta_a \lambda_w = 0$$

for all $u \in U$, $w \in W$ and $a \in k$.

(iii) Let $1 \leq i_1 < \cdots < i_r \leq m$ and put $I := \{i_1, \ldots, i_r\}$. Further let $j \in \{1, \ldots, m\}$ and define $e := |\{\, i \in I \mid i < j \,\}|$. Then

$$\lambda_{w_j}(w_{i_1} \wedge \cdots \wedge w_{i_r}) = \begin{cases} 0, & j \in I, \\ (-1)^e w_{i_1} \wedge \cdots \wedge w_j \wedge \cdots \wedge w_{i_r}, & j \notin I, \end{cases}$$

where w_j *is inserted at the appropriate position such that the indices are ascending, and*

$$\iota_{u_j}(w_{i_1} \wedge \cdots \wedge w_{i_r}) = \begin{cases} (-1)^e w_{i_1} \wedge \cdots \wedge \widehat{w_j} \wedge \cdots \wedge w_{i_r}, & j \in I, \\ 0, & j \notin I. \end{cases}$$

In particular, the matrices of λ_{w_j}*,* ι_{u_j} *and* η_a *w.r.t. the basis of* $\bigwedge W$ *that is induced by the basis* $(w_1, \ldots, w_m)$ *of* W *have entries in* $\{0, 1, -1\}$ *and at most one non-zero entry in each row and column.*

Proof. For $u \in U$, the mapping $W \to k$, $w \mapsto B(u, w)$ clearly defines an element of the dual space W^*. We see that ι_u is the interior product with this map, hence is well-defined by Proposition 1.41. Linearity of the three maps into $\mathrm{End}(\bigwedge W)$ is obvious.

(i) The claims for λ_w and η_a are clear. The statement for ι_u is part (v) of Proposition 1.41.

(ii) Let $u \in U$ and $w \in W$. The first claim is Proposition 1.41 (iii), taking into account that $B(u, w) = Q(u + w)$ as u and w are totally singular. Now if $a \in k$ and $z_1, \ldots, z_r \in W$, then

$$\begin{aligned} \iota_u \eta_a(z_1 \wedge \cdots \wedge z_r) &= \iota_u((-1)^r a z_1 \wedge \cdots \wedge z_r) = (-1)^r a \iota_u(z_1 \wedge \cdots \wedge z_r), \\ \eta_a \underbrace{\iota_u(z_1 \wedge \cdots \wedge z_r)}_{\in \bigwedge^{r-1} W} &= (-1)^{r-1} a \iota_u(z_1 \wedge \cdots \wedge z_r), \end{aligned}$$

which means that $\iota_u \eta_a + \eta_a \iota_u = 0$. Similarly, one has $\lambda_w \eta_a + \eta_a \lambda_w = 0$.

(iii) The claim for λ_w is clear by definition of $\bigwedge W$ and Proposition 1.36 (iii). The claim for ι_u is immediate from Theorem 2.19 (i). $\square$

3.2.1 Even Dimension

It turns out that the structure of C depends on the parity of $\dim V$. We first study the case of even dimension.

Recall that for a vector space W, the exterior algebra $\bigwedge W$ is naturally $\mathbb{Z}_2$-graded which then induces a $\mathbb{Z}_2$-grading also on the endomorphism algebra $\mathrm{End}(\bigwedge W)$ (cf. Lemma 1.28). The following theorem now determines the structure of the $\mathbb{Z}_2$-graded algebra C. It is taken from [Knu91], Proposition IV.2.1.1 and its proof.

Theorem 3.20. *Suppose that* $\dim V$ *is even,* k *is algebraically closed and* Q *is nondegenerate. Let* $m := m(Q) = \frac{\dim V}{2}$ *be the Witt index of* Q.

(i) Let $U, W \leq V$ be maximal totally singular subspaces with bases $(u_1, \ldots, u_m)$ and $(w_1, \ldots, w_m)$, respectively, that constitute a Lagrangian decomposition $V = U \oplus W$ of V.

Then the map $V \to \mathrm{End}(\bigwedge W),\ u + w \mapsto \iota_u + \lambda_w$, extends to an isomorphism $\Phi_{U,W} \colon C \to \mathrm{End}(\bigwedge W)$ of $\mathbb{Z}_2$-graded k-algebras. In particular, C is a central simple k-algebra.

(ii) Suppose that $V', V'' \leq V$ are even-dimensional subspaces of V such that $V = V' \perp V''$. Let $U', W' \leq V'$ and $U'', W'' \leq V''$ be maximal totally singular subspaces with associated bases such that they constitute respective Lagrangian decompositions $V' = U' \oplus W'$ and $V'' = U'' \oplus W''$.

Then putting $U := U' \perp U''$ and $W := W' \perp W''$ and choosing the natural bases coming from those of the summands defines a Lagrangian decomposition $V = U \oplus W$ of V. Furthermore, there is a commutative diagram

$$\begin{tikzcd}
C(V') \, {}^{\mathbb{Z}_2}\!\otimes C(V'') \arrow[r, "\Theta\circ(\Phi_{U',W'}\otimes\Phi_{U'',W''})"] \arrow[d, "\Psi"'] & \mathrm{End}(\bigwedge W' \, {}^{\mathbb{Z}_2}\!\otimes \bigwedge W'') \arrow[d, "\Omega"] \\
C(V) \arrow[r, "\Phi_{U,W}"'] & \mathrm{End}(\bigwedge W)
\end{tikzcd}$$

of $\mathbb{Z}_2$-graded algebra isomorphisms, where Ψ is the isomorphism from Proposition 3.9, Θ is the isomorphism from Proposition 1.29, and

$$\Omega \colon \mathrm{End}(\textstyle\bigwedge W' \, {}^{\mathbb{Z}_2}\!\otimes \bigwedge W'') \to \mathrm{End}(\bigwedge W),\ f \mapsto F \circ f \circ F^{-1},$$

with $F \colon \bigwedge W' \, {}^{\mathbb{Z}_2}\!\otimes \bigwedge W'' \to \bigwedge W$ the $\mathbb{Z}_2$-graded isomorphism from Proposition 1.38.

Proof. By Lemma 3.19, the map $\varphi_{U,W} \colon V \to \mathrm{End}(\bigwedge W),\ u + w \mapsto \iota_u + \lambda_w$ is linear and satisfies $\varphi_{U,W}(v)^2 = Q(v)\mathrm{id}_{\bigwedge W} = Q(v) \cdot 1_{\mathrm{End}(\bigwedge W)}$ for all $v = u + w \in V$. Hence, by Clifford axiom (C2) it extends to an algebra homomorphism $\Phi_{U,W} \colon C \to \mathrm{End}(\bigwedge W)$, which is $\mathbb{Z}_2$-graded by Lemma 1.24 applied to the generating system $V \subseteq C_1$. In order to prove that this is an isomorphism, we will employ the commutative diagram from the second part of the theorem.

Thus, turning to (ii), it follows easily from orthogonality that U and W constitute a Lagrangian decomposition of V. Dealing with algebra homomorphisms, it suffices to check commutativity of the diagram on a generating system of $C(V') \, {}^{\mathbb{Z}_2}\!\otimes C(V'')$. By Proposition 1.25 (ii) and Corollary 3.5 we may for this take the set comprising the elements $v' \otimes 1$ and $1 \otimes v''$ for $v' \in V'$ and $v'' \in V''$.

So let now $v' \in V'$ and $v'' \in V''$ and write $v' = u' + w'$ and $v'' = u'' + w''$ according to the Lagrangian decompositions of V' and V''. Since in the diagram we end up with maps in $\mathrm{End}(\bigwedge W)$, we need to check that they agree on arbitrary homogeneous elements of $\bigwedge W$. In view of the isomorphism F, such an element is given by $x = x' \wedge x''$, where $x' \in \bigwedge^r W'$ and $x'' \in \bigwedge^s W''$. Now as seen in the proof of Proposition 3.9, Ψ maps $v' \otimes 1$ to v' and $1 \otimes v''$ to v''. Hence, chasing the element $v' \otimes 1$ first down and then right, we end up with $\Phi_{U,W}(v')$. Going the other way, one obtains

$$\begin{aligned}\big(\Omega \circ \Theta \circ (\Phi_{U',W'} \otimes \Phi_{U'',W''})\big)(v' \otimes 1) &= (\Omega \circ \Theta)(\Phi_{U',W'}(v') \otimes 1)\\ &= F \circ \Theta(\Phi_{U',W'}(v') \otimes 1) \circ F^{-1}.\end{aligned}$$

Plugging in x, we have

$$\begin{aligned}(F \circ \Theta(\Phi_{U',W'}(v') \otimes 1) \circ F^{-1})(x' \wedge x'') &= F(\Phi_{U',W'}(v')(x') \otimes x'')\\ &= \Phi_{U',W'}(v')(x') \wedge x''.\end{aligned}$$

Commutativity in this case then follows from the observation

$$\begin{aligned}\Phi_{U,W}(v')(x' \wedge x'') &= (\iota_{u'} + \lambda_{w'})(x' \wedge x'')\\ &= \big((\iota_{u'} + \lambda_{w'})(x')\big) \wedge x''\\ &= \Phi_{U',W'}(v')(x') \wedge x''.\end{aligned}$$

For the element $1 \otimes v''$ the argument is very similar. Here, Proposition 1.36 (iii) and Proposition 1.41 (iv) yield that $\Phi_{U,W}(v'')(x' \wedge x'') = (-1)^r x' \wedge \Phi_{U'',W''}(v'')(x'')$. This, together with the sign in the definition of Θ, shows that both paths of the diagram give the same map also for $1 \otimes v''$. Hence, we have shown that the diagram commutes.

It only remains to prove that $\Phi_{U,W}$ is an isomorphism. For this, we do induction on $n = \dim V$. If $n = 0$, then $V = W = 0$, so $C = k$ by Example 3.4 (b), and also $\bigwedge W = k$. Here, the claim is trivial. Suppose that $n = 2$. Then $m = 1$ and $(1, w_1)$ is a basis of $\bigwedge W$ by Proposition 1.36 (iv). Since $\iota_{u_1}(1) = 0$ and $\iota_{u_1}(w_1) = 1$, the endomorphism $\iota_{u_1} = \Phi_{U,W}(u_1)$ has the matrix $\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)$ with respect to this basis. Similarly, $\lambda_{w_1} = \Phi_{U,W}(w_1)$ has the matrix $\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right)$. But these matrices generate $\mathrm{Mat}_2(k)$ as an algebra, which shows that $\Phi_{U,W}$ is surjective. Since $\dim C = 2^2 = 4$ by Theorem 3.10 (i) and $\dim \mathrm{End}(\bigwedge W) = 2^2 = 4$, it must be an isomorphism.

Now suppose that $n > 2$ is even. In view of the commutative diagram from (ii) and the fact that Ψ, Θ and Ω are isomorphisms, we only need to show that there are subspaces $V', V'' \leq V$ with $\dim V', \dim V'' \geq 2$ and $V = V' \perp V''$; then induction will yield the claim. If $\operatorname{char} k \neq 2$, we may simply use an orthogonal basis for this. It remains the case $\operatorname{char} k = 2$. By definition of nondegeneracy, we find a vector $y \in V \setminus \operatorname{rad} B_Q$ and then also some $v \in V$ with $B_Q(y, v) \neq 0$. As we are in characteristic 2, equation (2.2) shows that $B_Q(y, y) = B_Q(v, v) = 0$ and that y and v are linearly independent. Thus, $Y := \operatorname{span}(y, v)$ is 2-dimensional, and $B_Q\big|_Y$ is nondegenerate by Lemma 2.5 (iii). Lemma 2.7 (iii) then gives $V = Y \perp Y^{\perp}$, as desired. $\square$

The assumption that k be algebraically closed is there to ensure that also the restricted quadratic forms have maximal Witt index. There is a slightly more general version of the theorem for so-called hyperbolic quadratic forms, over any field, see [Knu91], Proposition IV.2.1.1. Regarding the proof of part (i), it can alternatively be shown that for a regular quadratic form of maximal Witt index the map $\Phi_{U,W}$ defines an irreducible representation of C (see [GW09], Theorem 6.1.3); then over an algebraically closed field it must be surjective by Theorem 1.9 and therefore an isomorphism by dimension count.

More generally, without assumptions on the Witt index, one has:

Theorem 3.21. *Suppose that* $\dim V$ *is even. Then* Q *is nondegenerate if and only if* C *is a central simple* k*-algebra.*

Proof. This is Proposition 11.6 of [EKM08]. For the forward implication see also [Che97], II.2.1, [Lam05], Theorem V.2.5 (for $\operatorname{char} k \neq 2$) or [Gro02], Proposition 13.11 (for $\operatorname{char} k = 2$). Note that here nondegeneracy of Q is equivalent to nondegeneracy of B_Q by Proposition 2.28. One may use a compatibility property of the Clifford algebra with field extensions (cf. [Che97], II.1.5) and then apply Theorem 3.20. ☐

Involving graded homomorphisms, Theorem 3.20 also reveals the structure of the even subalgebra C_0.

Theorem 3.22. *Suppose that* $\dim V > 0$ *is even,* k *is algebraically closed and* Q *is nondegenerate. Let* $U, W \leq V$ *be maximal totally singular subspaces with associated bases that constitute a Lagrangian decomposition* $V = U \oplus W$ *of* V*.*

Then the $\mathbb{Z}_2$*-graded algebra isomorphism* $\Phi_{U,W} \colon C \to \operatorname{End}(\bigwedge W)$ *from Theorem 3.20 restricts to a* k*-algebra isomorphism*

$$C_0 \xrightarrow{\sim} \operatorname{End}(\textstyle\bigwedge W)_0 \cong \operatorname{End}\big((\bigwedge W)_0\big) \oplus \operatorname{End}\big((\bigwedge W)_1\big).$$

In particular, C_0 *is the direct sum of two isomorphic ideals that are themselves central simple* k*-algebras, and* $Z(C_0) \cong k \oplus k$*. If* $\operatorname{char} k \neq 2$ *and* $(e_1, \dots, e_n)$ *is an orthogonal basis of* V*, then* $(1, e_1 \cdots e_n)$ *is a basis for* $Z(C_0)$*.*

Proof. It is clear from the definition of graded algebra homomorphisms that we obtain an algebra isomorphism $C_0 \xrightarrow{\sim} \operatorname{End}(\bigwedge W)_0$ by restricting. The second isomorphism is from Lemma 1.28 (ii).

Now let $\operatorname{char} k \neq 2$ and let $(e_1, \dots, e_n)$ be an orthogonal basis of V. We show that $\zeta := e_1 \cdots e_n \in Z(C_0)$. Since n is even, clearly $\zeta \in C_0$. In order to see that it commutes with every element of C_0, it suffices to check that it commutes with every element of an algebra generating system of C_0. By its definition, it is clear that C_0 is generated by the set $\{\, uv \mid u, v \in V\}$ as an algebra. But if $u, v \in V$, then Lemma 3.18 (i) implies that $\zeta uv = uv\zeta$, giving $\zeta \in Z(C_0)$. By Theorem 3.10 (ii), the elements 1 and $\zeta = e_1 \cdots e_n$ are linearly independent, so they must form a basis of $Z(C)$ since $\dim Z(C) = 2$. ☐

Dropping the assumptions on k, one may show the following result for the even subalgebra:

Theorem 3.23. *Suppose that* $\dim V > 0$ *is even and* Q *is nondegenerate. Then exactly one of the following cases occurs:*

(1) C_0 *is a simple algebra and* $Z(C_0)$ *is a quadratic separable extension of* k*,*

(2) C_0 *is the direct sum of two isomorphic ideals that are themselves central simple* k*-algebras, and* $Z(C_0) \cong k \oplus k$*.*

In any case, $\dim Z(C_0) = 2$*. If* $\operatorname{char} k \neq 2$ *and* $(e_1, \ldots, e_n)$ *is an orthogonal basis of* V*, then* $(1, e_1 \cdots e_n)$ *is a basis for* $Z(C_0)$*.*

Proof. This is [Che97], II.2.3. See also [Lam05], Theorem V.2.5 ($\operatorname{char} k \neq 2$) and [Gro02], Theorem 13.12 ($\operatorname{char} k = 2$). ☐

For a basis of $Z(C_0)$ in the case $\operatorname{char} k = 2$ see p. 123 of [Gro02].

3.2.2 Odd Dimension

We now turn to the odd-dimensional case. Here, the situation will turn out to be complementary to the even-dimensional case.

Theorem 3.24. *Suppose that* $\dim V$ *is odd. Then* Q *is nondegenerate if and only if* C_0 *is a central simple* k*-algebra.*

Proof. For the reverse implication see [EKM08], Proposition 11.6. Suppose conversely that Q is nondegenerate. Then due to Lemma 2.31 (i) respectively Proposition 2.28 (iv) there is a decomposition $V = \operatorname{span}(v) \perp Y$ with $c := Q(v) \neq 0$. By Lemma 2.30, the quadratic form $Q\big|_Y$ is nondegenerate, and then so is the form $-cQ\big|_Y$. We have a linear map $Y \to C_0(V, Q),\ y \mapsto vy$ which by (3.1) satisfies

$$(vy)^2 = vyvy = -v^2y^2 = -Q(v)Q(y) = -cQ(y).$$

Using (C2), it extends to an algebra homomorphism $\Phi\colon C(Y, -cQ\big|_Y) \to C_0(V, Q)$. Now $C(Y, -cQ\big|_Y)$ is simple by Theorem 3.21 and $\ker \Phi \trianglelefteq C(Y, -cQ\big|_Y)$ is a proper ideal (as $\Phi(1) = 1$), which forces Φ to be injective. Moreover, by Theorem 3.10 (i) and Corollary 3.11, we have $\dim C(Y, -cQ\big|_Y) = \dim C_0(V, Q)$, so that Φ is an isomorphism, and $C_0(V, Q)$ is central simple. ☐

This time, building on the structure of the even subalgebra, we establish the following structure theorem for the Clifford algebra, taken from [Che97], II.2.6.

Theorem 3.25. *Suppose that* $\dim V$ *is odd and that* Q *is nondegenerate. Then the centre* $Z(C)$ *is* 2*-dimensional, and a basis is given as follows: If* $\operatorname{char} k \neq 2$ *and* $(e_1, \dots, e_n)$ *is an orthogonal basis of* V*, then* $(1, e_1 \cdots e_n)$ *is a basis of* $Z(C)$ *and if* $\operatorname{char} k = 2$ *and* $0 \neq z \in \operatorname{rad} B_Q$*, then* $(1, z)$ *is a basis of* $Z(C)$*. Furthermore, there is an isomorphism of* k*-algebras*

$$\mu \colon C_0 \otimes Z(C) \to C, \ x \otimes y \mapsto xy.$$

In particular, if $\operatorname{char} k \neq 2$*, then either* C *is simple or it is the direct sum of two isomorphic ideals that are themselves central simple* k*-algebras.*

Proof. If $\operatorname{char} k \neq 2$ and $(e_1, \dots, e_n)$ is an orthogonal basis of V, put $\zeta := e_1 \cdots e_n$. Lemma 3.18 (i) gives $\zeta v = v \zeta$ for all $v \in V$, so that $\zeta \in Z(C)$ by Corollary 3.5. In characteristic 2, if $0 \neq z \in \operatorname{rad} B_Q$, then by Proposition 2.28 (iv) there is a subspace $Y \leq V$ such that $V = \operatorname{span}(z) \perp Y$. Hence, (3.1) implies that $zv = vz$ for all $v \in V$, that is, $z \in Z(C)$. Let now $\xi \in C_1$ denote ζ resp. z, depending on the characteristic. Then 1 and ξ are contained in the centre of C, and they are linearly independent by Theorem 3.10 (ii).

Let $x \in Z(C)$ and write $x = x_0 + x_1$ with $x_0 \in C_0$ and $x_1 \in C_1$. For $y \in C_i$ we have

$$x_0 y + x_1 y = xy = yx = yx_0 + yx_1$$

which by comparing homogeneous components gives $x_0 y = y x_0$ and $x_1 y = y x_1$. Thus, $x_0, x_1 \in Z(C)$ and in particular, $x_0 \in Z(C_0)$. Then Theorem 3.24 gives $x_0 \in k$. Since also $x\xi \in Z(C)$, we have $(x\xi)_0 = x_1 \xi \in k$, so $x_1 \in k\xi$ as $\xi^2 \in k$. We conclude $x \in \operatorname{span}(1, \xi)$. Therefore, $Z(C) = \operatorname{span}(1, \xi)$ is 2-dimensional.

Clearly, μ defines a k-linear map, and by definition of the centre even an algebra homomorphism. We have $C_0 \subseteq \operatorname{im} \mu$ and as $\xi C_0 = C_1$ also $C_1 \subseteq \operatorname{im} \mu$, which proves that μ is surjective. Since $\dim Z(C) = 2$, Theorem 3.10 (i) and Corollary 3.11 show that μ is an isomorphism. We set $c := \xi^2 \in k^\times$. Then there is an isomorphism $k[X]/\langle X^2 - c \rangle \cong Z(C)$ by sending X to ξ. If c is not a square in k, then $Z(C)$ is a field and hence a simple algebra and [NT89], Theorem 2.4.2 shows that C is simple. If c is a square, then in characteristic different from 2 the Chinese Remainder Theorem shows $Z(C) \cong k \oplus k$, so that C is the direct sum of two isomorphic ideals that are themselves central simple k-algebras. □

Again, if k is algebraically closed, there is even more insight, as is shown by the subsequent theorem which is based on [GW09], Proposition 6.1.6.

Theorem 3.26. *Suppose that* $\dim V$ *is odd,* k *is algebraically closed and* Q *is nondegenerate. Let* $m := m(Q) = \frac{\dim V - 1}{2}$ *be the Witt index of* Q*. Let* $U, W \leq V$ *be maximal totally singular subspaces with bases* $(u_1, \dots, u_m)$ *and* $(w_1, \dots, w_m)$*, respectively, that constitute a Lagrangian decomposition* $V = (U \oplus W) \perp \operatorname{span}(z)$ *of* V*.*

Then the map $V \to \operatorname{End}(\bigwedge W) \oplus \operatorname{End}(\bigwedge W)$*,* $u + w + az \mapsto (\iota_u + \lambda_w + \eta_a, \iota_u + \lambda_w - \eta_a)$ *extends to an (ungraded) algebra homomorphism* $\Phi_{U,W} \colon C \to \operatorname{End}(\bigwedge W) \oplus \operatorname{End}(\bigwedge W)$

which is an isomorphism if $\operatorname{char} k \neq 2$. *In particular, in the latter case* C *is the direct sum of two isomorphic ideals that are themselves central simple* k*-algebras.*

Proof. As in the proof of Theorem 3.20, it follows immediately from Lemma 3.19 that we may apply (C2) in order to obtain the algebra homomorphism $\Phi_{U,W}$ by extending the given map.

Now assume for the rest of the proof that $\operatorname{char} k \neq 2$. We prove that $\Phi_{U,W}$ is surjective. Note that Theorem 3.20 shows that both component functions of $\Phi_{U,W}$ are surjective. Thus, if we can prove that $(\mathrm{id}_{\bigwedge W}, 0), (0, \mathrm{id}_{\bigwedge W}) \in \operatorname{im} \Phi_{U,W}$, then this will give surjectivity of $\Phi_{U,W}$. Let $j \in \{1, \dots, m\}$ and let $1 \leq i_1 < \cdots < i_r \leq m$. Put $I := \{i_1, \dots, i_r\}$. Then Lemma 3.19 (iii) implies that

$$\begin{aligned}[][\iota_{u_j}, \lambda_{w_j}](w_{i_1} \wedge \cdots \wedge w_{i_r}) &= \begin{cases} -\lambda_{w_j} \iota_{u_j}(w_{i_1} \wedge \cdots \wedge w_{i_r}), & j \in I, \\ \iota_{u_j} \lambda_{w_j}(w_{i_1} \wedge \cdots \wedge w_{i_r}), & j \notin I, \end{cases} \\ &= \begin{cases} -w_{i_1} \wedge \cdots \wedge w_{i_r}, & j \in I, \\ w_{i_1} \wedge \cdots \wedge w_{i_r}, & j \notin I. \end{cases}\end{aligned}$$

Thus, we have

$$[\iota_{u_1}, \lambda_{w_1}] \cdots [\iota_{u_m}, \lambda_{w_m}](w_{i_1} \wedge \cdots \wedge w_{i_r}) = (-1)^r w_{i_1} \wedge \cdots \wedge w_{i_r} = \eta_1(w_{i_1} \wedge \cdots \wedge w_{i_r})$$

and therefore $(\eta_1, \eta_1) = \Phi_{U,W}([u_1, w_1] \cdots [u_m, w_m]) \in \operatorname{im} \Phi_{U,W}$. But clearly also $(\eta_1, -\eta_1) = \Phi_{U,W}(z)$ is contained in the image, so that

$$(\eta_1, \eta_1)(\eta_1, -\eta_1) = (\eta_1^2, -\eta_1^2) = (\mathrm{id}_{\bigwedge W}, -\mathrm{id}_{\bigwedge W}) \in \operatorname{im} \Phi_{U,W}.$$

Being an algebra homomorphism, we have $\Phi_{U,W}(1) = (\mathrm{id}_{\bigwedge W}, \mathrm{id}_{\bigwedge W})$ from which we infer that $(2\mathrm{id}_{\bigwedge W}, 0), (0, -2\mathrm{id}_{\bigwedge W}) \in \operatorname{im} \Phi_{U,W}$. Since $\operatorname{char} k \neq 2$, we finally obtain that $(\mathrm{id}_{\bigwedge W}, 0)$ and $(0, \mathrm{id}_{\bigwedge W})$ are in the image of $\Phi_{U,W}$, proving its surjectivity. As the target space has dimension $2 \cdot (2^m)^2$ by Propostion 1.36 (iii), and this equals $2^{2m+1} = 2^{\dim V} = \dim C$ by Theorem 3.10 (i), we conclude that $\Phi_{U,W}$ is an isomorphism. □

3.3 Construction of the Spin Groups

This section is dedicated to finally constructing the central object of this thesis, the spin group $\mathrm{Spin}(V)$, as a subgroup of the units of the Clifford algebra. We first define the so-called Clifford group that will then contain the spin group as a subgroup. We eventually use some of the theory of Clifford algebras to derive first properties of $\mathrm{Spin}(V)$.

Working in the realm of geometry, we consider nondegenerate quadratic forms. In addition, to avoid problems with the case $\operatorname{char} k = 2$ and $\dim V$ odd and to be able to exploit the Cartan-Dieudonné Theorem 2.41, we assume in this section that B is nondegenerate. If $\operatorname{char} k = 2$, then by Proposition 2.15 this assumption forces $\dim V$ to be even; however, for our eventual discussion and computations in the setting where $\operatorname{char} k \neq 2$, this is no limitation and the correct assumption (cf. Proposition 2.28)

We mainly follow the exhibitions given in [ABS64] and [BtD85], together with Section 3.1 of [Mei13]. The former only treat the case $k = \mathbb{R}$, while the latter only deals with fields of characteristic different from 2, but the constructions generalize to arbitrary fields, with minor modifications of proofs in characteristic 2. For the general case, but using slightly different conventions, see also [Knu91], Section IV.6, [Che97] and [Jac89]. Some of the material is also covered in Section 6.3 of [GW09] and in Section I.2 of [LM89].

We denote by C the Clifford algebra for (V, Q). Recall from Section 3.1 that associated with C we have the main involution α, the main antiautomorphism τ and the conjugation map $\bar{\cdot}$ which also is an antiautomorphism.

3.3.1 The Clifford Group

As mentioned, we start by introducing the Clifford group. Recall that we view V as a subspace of C.

Definition 3.27. The *Clifford group* of (V, Q) is

$$\Gamma := \{\, x \in C^\times \mid \alpha(x) v x^{-1} \in V \text{ for all } v \in V \,\}.$$

If we want to specify Q and V, we also write $\Gamma = \Gamma(V, Q) = \Gamma(Q)$. We further put $\Gamma_0 := \Gamma \cap C_0$.

Lemma 3.28. *For $x \in \Gamma$, the map*

$$\rho_x \colon V \to V,\ v \mapsto \alpha(x) v x^{-1}$$

is a linear isomorphism. In particular, $\Gamma = \{\, x \in C^\times \mid \alpha(x) V x^{-1} = V \,\}$ is a group, $\Gamma_0 \leq \Gamma$ is a subgroup, and $\rho \colon \Gamma \to \mathrm{GL}(V),\ x \mapsto \rho_x$ is a representation of Γ.

Proof. Linearity of ρ_x is clear. If $v \in \ker \rho_x$, then $\alpha(x) v x^{-1} = 0$, which by invertibility of x gives $v = 0$, establishing injectivity of ρ_x. But V is finite-dimensional, so ρ_x must in fact be an isomorphism.

The statement about the shape of Γ is clear by what we have just shown. To prove that Γ is a group, let $x, y \in \Gamma$ and $v \in V$. Then $xy \in C^\times$ and

$$\alpha(xy) v (xy)^{-1} = \alpha(x) \underbrace{\alpha(y) v y^{-1}}_{\in V} x^{-1} \in V,$$

so $xy \in \Gamma$. Now by the first part, there exists $w \in V$ with $v = \alpha(x) w x^{-1}$. Hence,

$$\alpha(x^{-1}) v x = \alpha(x)^{-1} \alpha(x) w x^{-1} x = w \in V,$$

showing that $x^{-1} \in \Gamma$ and thereby that Γ is a group. Finally,

$$\rho_x \rho_y(v) = \rho_x(\alpha(y)vy^{-1}) = \alpha(x)\alpha(y)vy^{-1}x^{-1} = \alpha(xy)v(xy)^{-1} = \rho_{xy}(v),$$

which gives $\rho_x\rho_y = \rho_{xy}$. We conclude that ρ is a representation. $\square$

Definition 3.29. The representation $\rho\colon \Gamma \to \mathrm{GL}(V)$ is called the *twisted adjoint representation* of Γ.

We immediately obtain that the Clifford group is fixed by the main involution and the main antiautomorphism:

Lemma 3.30. *We have* $\alpha(\Gamma) = \Gamma$ *and* $\tau(\Gamma) = \Gamma$. *In particular, also* $\overline{\Gamma} = \Gamma$.

Proof. Let $x \in \Gamma$ and let $v \in V$. Using Propositions 3.13 and 3.14, we have

$$\begin{aligned}\alpha(\alpha(x))v\alpha(x)^{-1} &= \alpha^2(x)\alpha(-v)\alpha(x^{-1}) = \alpha(\underbrace{-\alpha(x)vx^{-1}}_{\in V}) \in V,\\ \alpha(\tau(x))v\tau(x)^{-1} &= \tau(\alpha(x))\tau(v)\tau(x^{-1}) = \tau(x^{-1}v\alpha(x)) = \tau(\alpha(\underbrace{-\alpha(x^{-1})vx}_{\in V})) \in V,\end{aligned}$$

showing $\alpha(\Gamma) \subseteq \Gamma$ and $\tau(\Gamma) \subseteq \Gamma$. Since α and τ are involutions, it follows that $\alpha(\Gamma) = \Gamma$ and $\tau(\Gamma) = \Gamma$. $\square$

We now investigate the twisted adjoint representation in more detail. Its kernel is given as follows:

Proposition 3.31. *It holds that* $\ker\rho = k^\times$.

Proof. Suppose first that $\operatorname{char} k = 2$. Then $\alpha = \mathrm{id}_C$ and we get $\ker\rho = Z(C)^\times$ as V generates C as an algebra by Corollary 3.5. So here, the claim follows from Theorem 3.21.

Now assume that $\operatorname{char} k \neq 2$. The inclusion $k^\times \subseteq \ker\rho$ is clear. For the converse, let $x \in \ker\rho$ and write $x = x_0 + x_1$ with $x_0 \in C_0$ and $x_1 \in C_1$. Then $\alpha(x) = x_0 - x_1$ by Proposition 3.13 (ii), whence

$$x_0v - x_1v = \alpha(x)v = vx = vx_0 + vx_1$$

for all $v \in V$. Comparing homogeneous components, we have $x_0v = vx_0$ and $x_1v = -vx_1$ for all $v \in V$. The first equation gives $x_0 \in Z(C)$ and also $x_0 \in Z(C_0)$, noting that C_0 is generated by the products of two elements of V. Thus, Theorems 3.21 and 3.24 imply that $x_0 \in k$.

In only remains to show that $x_1 = 0$. By Lemma 2.31 (i), there is an orthogonal basis $(e_1, \dots, e_n)$ of V, and all basis vectors are nonsingular. From (3.1) we deduce that $e_ie_j = -e_je_i$ for $i \neq j$. Now fix $i \in \{1, \dots, n\}$. Expressing x_1 in terms of the basis of C that comes from $(e_1, \dots, e_n)$ (cf. the proof of Corollary 3.11) and swapping the basis vectors appropriately, we may write $x_1 = e_i y_0 + y_1$ with $y_0 \in C_0$ and $y_1 \in C_1$ such that no term of y_0 and y_1 involves e_i. Using again the relation $e_i e_j = -e_j e_i$ for $i \neq j$, the equation $x_1 v = -v x_1$ for $v = e_i$ reads

$$Q(e_i)y_0 - e_i y_1 = x_1 e_i = -e_i x_1 = -Q(e_i)y_0 - e_i y_1.$$

This implies $2Q(e_i)y_0 = 0$ and therefore $y_0 = 0$ as e_i is nonsingular. Thus, $x_1 = y_1$, that is, no term of the basis expression of x_1 involves e_i. Since i was arbitrary, we must have $x_1 = 0$. ☐

In order to determine also the image of ρ, we need some auxiliary results. In particular, we need to know more concrete elements of the Clifford group. Besides the units in k, an important class of elements of Γ are the nonsingular vectors of V:

Lemma 3.32. *Let $u \in V$ with $Q(u) \neq 0$. Then $u \in \Gamma$ and $\rho_u = s_u$ is the reflection along u.*

Proof. By (C1) we have $u^2 = Q(u)$, so $u\big(\frac{u}{Q(u)}\big) = \big(\frac{u}{Q(u)}\big)u = 1$ and therefore $u \in C^\times$. Now let $v \in V$. Using (3.1) and Proposition 3.13 (ii), we get

$$\alpha(u)vu^{-1} = -uvu^{-1} = (vu - B(v,u))u^{-1} = v - \frac{B(v,u)}{Q(u)}u = s_u(v) \in V,$$

proving the lemma. ☐

In view of Theorem 2.41 this already shows that the orthogonal group $\mathrm{O}(V)$ is contained in the image of ρ. In order to establish the reverse inclusion, we need an auxiliary map that will also be central for the definition of the spin group.

Definition 3.33. The map $N\colon C \to C,\ x \mapsto x\overline{x}$ is called the *norm* of C.

Lemma 3.34. *The norm of C has the following properties:*

- *(i)* $N(a) = a^2$ *for all* $a \in k$ *and* $N(v) = -Q(v)$ *for all* $v \in V$.
- *(ii)* $N(\alpha(x)) = \alpha(N(x))$ *for all* $x \in C$.
- *(iii)* $N(\Gamma) \subseteq k^\times$. *In particular, the restricted norm* $N\big|_\Gamma\colon \Gamma \to k^\times$ *is a group homomorphism.*
- *(iv)* *If* $x \in \Gamma$, *then* $N(x) = \overline{x}x$.

Proof. Part (i) is immediate from Corollary 3.16 and (C1). If $x \in C$, then the definition of conjugation and Proposition 3.14 (iii) give

$$N(\alpha(x)) = \alpha(x)\overline{\alpha(x)} = \alpha(x)\alpha^2(\tau(x)) = \alpha(x\overline{x}) = \alpha(N(x)),$$

thus proving the second claim.

We now turn to part (iii). Let $x \in \Gamma$. Then $\overline{x} \in \Gamma$ by Lemma 3.30, so that $N(x) = x\overline{x} \in \Gamma$. Now let $v \in V$. Since $\alpha(\overline{x})v\overline{x}^{-1} \in V$ and $\tau\big|_V = \mathrm{id}_V$, it follows that

$$\alpha(\overline{x})v\overline{x}^{-1} = \tau\big(\alpha(\overline{x})v\overline{x}^{-1}\big) = \alpha(x^{-1})vx,$$

whence $\alpha(x\overline{x})v = vx\overline{x}$. But this means $x\overline{x} = N(x) \in \ker \rho$. Proposition 3.31 shows that $N(x) \in k^\times$. Thus, if $x, y \in \Gamma$, then

$$N(xy) = (xy)(\overline{xy}) = xy\overline{y}\,\overline{x} = xN(y)\overline{x} = x\overline{x}N(y) = N(x)N(y),$$

that is, $N\big|_\Gamma$ is a group homomorphism.

For the final claim, let $x \in \Gamma$. By definition, we have $N(x) = x\overline{x}$ which gives $\overline{x} = x^{-1}N(x)$. But $N(x) \in k^\times$ by part (iii), so $\overline{x} = N(x)x^{-1}$ and therefore $N(x) = \overline{x}x$. ☐

With these results available, we can now deal with the image of ρ.

Proposition 3.35. *It holds that $\rho(\Gamma) \subseteq \mathrm{O}(V)$. Suppose now that we are not in the case that $|k| = 2$, $\dim V = 4$ and Q has Witt index 2. If $x \in \Gamma$, then there exist $c \in k^\times$ and vectors $v_1, \ldots, v_r \in V$ with $Q(v_i) \neq 0$ such that $x = cv_1 \cdots v_r$. In particular, every element of Γ is homogeneous.*

Proof. Let $x \in \Gamma$. We have $\rho_x \in \mathrm{GL}(V)$ and need to check that it is an isometry, so let $v \in V$. Since $\rho_x(v) \in V$, we may apply Lemma 3.34 (i) to obtain

$$Q(\rho_x(v)) = -N(\rho_x(v)) = -\rho_x(v)\overline{\rho_x(v)} = -\alpha(x)vx^{-1}\overline{x^{-1}}\,\overline{v}\,\overline{\alpha(x)}.$$

Now $x^{-1}\overline{x^{-1}} = N(x^{-1}) \in k^\times$ by Lemma 3.34 (iii), so $x^{-1}\overline{x^{-1}}$ commutes with the other factors. We further have $v\overline{v} = N(v) = -Q(v)$, giving

$$Q(\rho_x(v)) = Q(v)N(x^{-1})N(\alpha(x)).$$

Since $N(x) \in k^\times$ by Lemma 3.34 (iii), the second part of that lemma implies that $N(\alpha(x)) = \alpha(N(x)) = N(x)$. We conclude again with Lemma 3.34 (iii) that

$$Q(\rho_x(v)) = Q(v)N(x^{-1})N(x) = Q(v)N(1) = Q(v),$$

showing $\rho_x \in \mathrm{O}(V)$ and therefore $\rho(\Gamma) \subseteq \mathrm{O}(V)$.

Suppose now that we are not in the case that $|k| = 2$, $\dim V = 4$ and Q has Witt index 2. Then together with the above, Thereom 2.41 shows that if $x \in \Gamma$, then there exist $v_1, \ldots, v_r \in V$ with $Q(v_i) \neq 0$ such that $\rho(x) = s_{v_1} \cdots s_{v_r}$. Lemma 3.32 and Proposition 3.31 imply that there is $c \in k^\times$ such that $x = cv_1 \cdots v_r$. ☐

For $x \in C \setminus \{0\}$ homogeneous denote by $\delta(x) \in \mathbb{Z}_2$ the degree of x. By the above proposition, we have a group homomorphism $\delta\colon \Gamma \to \mathbb{Z}_2$ whose kernel clearly equals Γ_0.

Theorem 3.36. *Suppose that* $V \neq 0$ *and we are not in the case that* $|k| = 2$*,* $\dim V = 4$ *and* Q *has Witt index* 2*. Then* $\rho(\Gamma) = \mathrm{O}(V)$ *and* $\rho(\Gamma_0) = \mathrm{SO}(V)$*. In particular, there is a commutative diagram of groups*

$$\begin{tikzcd}
 & & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & k^\times \arrow[r] \arrow[d, equal] & \Gamma_0 \arrow[r, "\rho"] \arrow[d] & \mathrm{SO}(V) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & k^\times \arrow[r] & \Gamma \arrow[r, "\rho"] \arrow[d, "\delta"] & \mathrm{O}(V) \arrow[r] \arrow[d, "D"] & 1 \\
 & & \mathbb{Z}_2 \arrow[r, "\sim"] \arrow[d] & C_2 \arrow[d] & \\
 & & 1 & 1 &
\end{tikzcd}$$

with exact rows and columns, where C_2 *is the cyclic group of order 2 and* $D\colon \mathrm{O}(V) \to C_2$ *denotes the determinant if* $\operatorname{char} k \neq 2$ *and the pseudodeterminant otherwise.*

Proof. Since the generating system of $\mathrm{O}(V)$ from Theorem 2.41 is contained in $\rho(\Gamma)$ by Lemma 3.32, it holds that $\mathrm{O}(V) \subseteq \rho(\Gamma)$. Analogously, using Proposition 2.42, we have $\mathrm{SO}(V) \subseteq \rho(\Gamma_0)$. Proposition 3.35 implies that $\rho(\Gamma) = \mathrm{O}(V)$. Furthermore, if $x \in \Gamma_0$, then this proposition shows that there are $c \in k^\times$ and vectors $v_1, \ldots, v_r \in V$ with $Q(v_i)$ such that $x = cv_1 \cdots v_r$, where r needs to be even as $x \in C_0$. Thus, we have $\rho(x) = s_{v_1} \cdots s_{v_r} \in \mathrm{SO}(V)$ and we conclude that $\rho(\Gamma_0) = \mathrm{SO}(V)$. Taking Proposition 3.31 into account, we have shown exactness of the rows of the diagram.

The right long column is exact by Definition 2.39 and Corollary 2.40. Taking any nonsingular vector $v \in V$, we have $v \in \Gamma$ by Lemma 3.32, and it holds that $\delta(v) = 1$. This shows surjectivity of δ and thereby exactness of the left long column.

It only remains to prove commutativity of the lower square. Let $x \in \Gamma$. Then by what was shown above and Proposition 3.31 we have $\rho(x) \in \mathrm{SO}(V)$ if and only if $x \in \Gamma_0$. This proves commutativity. □

3.3.2 Pin and Spin

Having established the above two exact sequences for the twisted adjoint representation we now proceed by constructing two subgroups of the Clifford group, the spin group and the pin group. We use the norm homomorphism from Lemma 3.34 (iii).

Definition 3.37. We define the *pin group* of (V, Q) to be

$$\operatorname{Pin}(V) := \{\, x \in \Gamma \mid N(x) = 1 \,\} = \ker N\big|_{\Gamma}$$

and the *spin group* of (V, Q) to be

$$\operatorname{Spin}(V) := \{\, x \in \Gamma_0 \mid N(x) = 1 \,\} = \ker N\big|_{\Gamma_0} = \operatorname{Pin}(V) \cap C_0.$$

Being kernels of group homomorphisms, $\operatorname{Pin}(V)$ and $\operatorname{Spin}(V)$ are clearly groups. We are generally more interested in the spin group than the pin group which comes from the fact that the former is simple as an algebraic groups (see Theorem 4.53). It will turn out that the pin group plays the same role for the spin group as the orthogonal group plays for the special orthogonal group, as we shall soon see. The group $\operatorname{Pin}(V)$ is a useful tool for studying $\operatorname{Spin}(V)$ which will now be our main objective.

Example 3.38 (Lowest dimensional spin groups)**.** We take a look at the spin groups in dimensions 0, 1 and 2.

(a) Let $\dim V = 0$. Then $C = C_0 = k$ by Example 3.4 (b), and the norm map $N\colon C \to C$ is squaring. Thus, $\Gamma_0 = k^\times$ and $\operatorname{Spin}(V) = \{\pm 1\}$.

(b) Let $\dim V = 1$. Here, C_0 is 1-dimensional by Corollary 3.11, and $k \subseteq C_0$, so that $C_0 = k$. We again get $\Gamma_0 = k^\times$ and $\operatorname{Spin}(V) = \{\pm 1\}$.

(c) Let $\dim V = 2$ and let (v_1, v_2) be a basis of V. By Corollary 3.11, C_0 is 2-dimensional, with basis $(1, v_1v_2)$. But then the element v_1v_2 generates C_0 as an algebra, so C_0 is commutative. Hence, also the spin group $\operatorname{Spin}(V)$ is commutative. For a more precise description of $\operatorname{Spin}(V)$ under some assumptions on k and Q see Corollary 3.41.

By Theorem 3.36 and Lemma 3.34 (i) there is an exact sequence $1 \to \{\pm 1\} \to \operatorname{Spin}(V) \xrightarrow{\rho} \operatorname{SO}(V)$, and similarly for $\operatorname{Pin}(V)$. The question now arises whether the final map is surjective, as it is for the even Clifford group Γ_0. This can be answered in the affirmative if we are able to normalize a preimage of $\sigma \in \operatorname{SO}(V)$ in Γ_0 in such a way that it is contained in $\operatorname{Spin}(V)$. Since the norm restricts to squaring on k, we thus get surjectivity at least over quadratically closed fields:

Theorem 3.39. *Suppose that k is quadratically closed, $V \neq 0$, and that we are not in the case that $|k| = 2$, $\dim V = 4$ and Q has Witt index 2. Then, with notation as* *in Theorem 3.36, there is a commutative diagram of groups*

$$\begin{tikzcd}
 & & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & \{\pm 1\} \arrow[r] \arrow[d, equal] & \mathrm{Spin}(V) \arrow[r, "\rho"] \arrow[d] & \mathrm{SO}(V) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \{\pm 1\} \arrow[r] & \mathrm{Pin}(V) \arrow[r, "\rho"] \arrow[d, "\delta"] & \mathrm{O}(V) \arrow[r] \arrow[d, "D"] & 1 \\
 & & \mathbb{Z}_2 \arrow[r, "\sim"] \arrow[d] & C_2 \arrow[d] & \\
 & & 1 & 1 &
\end{tikzcd}$$

with exact rows and columns. In particular, we have $|\mathrm{Pin}(V) : \mathrm{Spin}(V)| = 2$ *and it holds that* $\mathrm{Spin}(V) \trianglelefteq \mathrm{Pin}(V)$ *is normal.*

Proof. In view of Theorem 3.36 and Proposition 3.31, it only remains to show surjectivity of the restrictions of ρ and δ. Since k is quadratically closed, we find $v \in V$ with $Q(v) = -1$. By Lemmas 3.32 and 3.34 (i), this element is contained in $\mathrm{Pin}(V)$. Moreover, $\delta(v) = 1$, proving that δ is surjective.

Now let $\sigma \in \mathrm{O}(V)$. By Theorem 3.36, there is $x \in \Gamma$ such that $\rho(x) = \sigma$. We have $N(x) \in k^\times$ by Lemma 3.34 (iii), so as k is quadratically closed there is $c \in k^\times$ such that $c^2 = N(x)^{-1}$. Then $N(cx) = c^2 N(x) = 1$, i.e., $cx \in \mathrm{Pin}(V)$, and $\rho(cx) = \rho(x) = \sigma$. This shows that ρ: $\mathrm{Pin}(V) \to \mathrm{O}(V)$ is surjective. The same proof works for the restriction to $\mathrm{Spin}(V)$. ☐

The above diagram will be of fundamental importance for the further study of the spin group in Section 4.4. More generally, Proposition 2.42 and Lemmas 3.32 and 3.34 (i) imply that we have a diagram as above if for each nonsingular $u \in V$ there is $c \in k^\times$ with $c^2 = -Q(u)^{-1}$ (in which case $N(cu) = 1$). This for example applies to the quadratic forms from Example 3.4 (d).

It turns out, however, that ρ is in general not surjective, cf. [Knu91], Theorems IV.6.2.6 and IV.6.3.1. But since we are eventually working over algebraically closed fields, the above result is sufficient for our discussion. We proceed by proving some more results for spin groups over quadratically closed fields.

Corollary 3.40 (A generating system for $\mathrm{Spin}(V)$)**.** *Suppose that k is quadratically closed and that we are not in the case that* $|k| = 2$, $\dim V = 4$ *and Q has Witt index*

2. *If* $x \in \operatorname{Spin}(V)$*, then there exist* $u_1, \ldots, u_r \in V$ *with* r *even and* $Q(u_i) = -1$ *such that* $x = \pm u_1 \cdots u_r$*. In particular, we have*

$$\operatorname{Spin}(V) = \langle\, uv \mid u, v \in V \text{ with } Q(u) = Q(v) = -1 \,\rangle$$

if furthermore $V \neq 0$*.*

Proof. Let $x \in \operatorname{Spin}(V)$. Proposition 3.35 implies that there are $c \in k^\times$ and vectors $u_1, \ldots, u_r \in V$ with r even and $Q(u_i) \neq 0$ such that $x = cu_1 \cdots u_r$. Since k is quadratically closed, we may assume that $Q(u_i) = -1$ by normalizing. Then Lemma 3.34 gives $1 = N(x) = c^2$, so that indeed $x = \pm u_1 \cdots u_r$.

For the generating system use again Lemmas 3.32 and 3.34 to ensure the inclusion from right to left. Note that if $V \neq 0$, then there is $u \in V$ with $Q(u) = -1$, so that $-1 = Q(u) = u^2$. This together with the above gives the other inclusion. □

One application of this is the determination of the spin group in dimension 2.

Corollary 3.41. *Let* $\dim V = 2$*. Suppose that* k *is quadratically closed and that* V *contains a singular vector. Then* $\operatorname{Spin}(V) \cong k^\times$*.*

Proof. By assumption and Theorem 2.19, Q has maximal Witt index. Thus, there is a Lagrangian decomposition $V = U \oplus W$. Letting (u) and (w) be the corresponding bases of U and W, respectively, we have $Q(u) = Q(w) = 0$ and $B(u, w) = 1$. Hence, for $a, b \in k$ we have $Q(au + bw) = ab$, which means that the elements $v \in V$ with $Q(v) = -1$ are precisely the ones of the form $cu - c^{-1}w$ for $c \in k^\times$. We see from Corollary 3.40 that $\operatorname{Spin}(V)$ is generated by the elements

$$(cu - c^{-1}w)(-du + d^{-1}w) = cd^{-1}uw + dc^{-1}wu$$

for $c, d \in k^\times$. Thus, we may define a map

$$\gamma\colon k^\times \to \operatorname{Spin}(V),\ t \mapsto tuw + t^{-1}wu.$$

In order to show that γ is a group homomorphism, we let $s, t \in k^\times$. Bearing in mind $u^2 = 0$ and $w^2 = 0$, it holds that

$$\gamma(s)\gamma(t) = (suw + s^{-1}wu)(tuw + t^{-1}wu) = st(uw)^2 + s^{-1}t^{-1}(wu)^2.$$

But $1 = B(u, w) = uw + wu$, giving $(uw)^2 = uw(1 - wu) = uw$ and similarly $(wu)^2 = wu$. Therefore, $\gamma(s)\gamma(t) = stuw + (st)^{-1}wu = \gamma(st)$, showing that γ indeed is a group homomorphism. It is surjective since its image contains all generators of $\operatorname{Spin}(V)$. Finally, let $t \in \ker\gamma$, so that

$$1 = tuw + t^{-1}wu = t(1 - wu) + t^{-1}wu = t + wu(t^{-1} - t).$$

By Theorem 3.10 (ii), the elements 1 and wu are k-linearly independent in $C \supseteq \operatorname{Spin}(V)$, so it follows that $t = 1$. We conclude that γ is an isomorphism of groups. □

Lemma 3.42. *Suppose that k is quadratically closed and if* $\dim V = 2$ *and* $\operatorname{char} k = 2$ *assume that $|k| > 2$. Then $C_0 = \langle \mathrm{Spin}(V)\rangle_{k\text{-alg.}} = \mathrm{span}(\mathrm{Spin}(V))$.*

Proof. First note that $\langle \mathrm{Spin}(V)\rangle_{k\text{-alg.}} = \mathrm{span}(\mathrm{Spin}(V))$ since $\mathrm{Spin}(V)$ is a group with respect to multiplication in C. Furthermore, the inclusion $C_0 \supseteq \langle \mathrm{Spin}(V)\rangle_{k\text{-alg.}}$ is clear. For the remaining inclusion note that $C_0 = \langle uv \mid u, v \in V\rangle_{k\text{-alg.}}$ by definition. Since V has a basis consisting of nonsingular vectors by Proposition 2.32 and as k is algebraically closed, it follows that

$$\begin{aligned} C_0 &= \langle\, uv \mid u, v \in V \text{ with } Q(u), Q(v) \neq 0 \,\rangle_{k\text{-alg.}} \\ &= \langle\, uv \mid u, v \in V \text{ with } Q(u) = Q(v) = -1 \,\rangle_{k\text{-alg.}} \end{aligned}$$

which is contained in $\langle \mathrm{Spin}(V)\rangle_{k\text{-alg.}}$ by Lemmas 3.32 and 3.34. □

With a different approach, the statement can also be shown to hold for arbitrary fields, unless $\dim V = 2$, Q has Witt index 1 and $|k| \in \{2, 3\}$, see [Che97] Lemma 1 of Section 2.4 and the proofs of II.4.3 and II.5.1.

The above result will later become important in the context of spin representations. As a first consequence, it allows us to determine the centre of $\mathrm{Spin}(V)$. For $k = \mathbb{C}$, the subsequent result can be found in [Var04], page 208, and [Mei13], page 70. We use the approach described in the latter reference and give a detailed proof.

Proposition 3.43 (The centre of $\mathrm{Spin}(V)$)**.** *Suppose that k is quadratically closed.*

- *(i) If* $\dim V$ *is odd, then* $Z(\mathrm{Spin}(V)) = \{\pm 1\}$.
- *(ii) In even dimension, there are the following cases:*
  - *(1) If* $\dim V \in \{0, 2\}$, *then* $Z(\mathrm{Spin}(V)) = \mathrm{Spin}(V)$
  - *(2) Suppose that* $\dim V \geq 4$ *is even. If* $\operatorname{char} k = 2$, *then* $Z(\mathrm{Spin}(V)) = 1$. *If* $\operatorname{char} k \neq 2$, *let $(e_1, \dots, e_n)$ be an orthogonal basis of V with $Q(e_i) = -1$ and put $\zeta := e_1 \cdots e_n$. Then*

$$Z(\mathrm{Spin}(V)) = \{\pm 1, \pm\zeta\} \cong \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}_2, & n \equiv 0 \pmod 4, \\ \mathbb{Z}_4, & n \equiv 2 \pmod 4. \end{cases}$$

Proof. The general theme of this proof is to make use of Lemma 3.42 in order to translate the question from $\mathrm{Spin}(V)$ to C_0, where we know how the centre looks like. More concretely, if $x \in Z(\mathrm{Spin}(V))$ and the assumptions of the above lemma are met, then it implies that $x \in Z(C_0)$ since x commutes with every element of a set of generators of C_0.

Thus, since for odd-dimensional V, the k-algebra C_0 is central simple by Theorem 3.24 and the norm restricts to squaring on k, we have $Z(\mathrm{Spin}(V)) \subseteq \{\pm 1\}$ in case (i), the other inclusion being trivial. The claim for dimensions 0 and 2 follows from Example 3.38.

From now on assume that $\dim V \geq 4$ is even. First suppose that $\operatorname{char} k \neq 2$. Note that the given orthogonal basis exists by Lemma 2.31 and that the conditions $Q(e_i) = -1$ ensure that $\pm\zeta \in \operatorname{Spin}(V)$ and therefore $\pm\zeta \in Z(\operatorname{Spin}(V))$ by Theorem 3.23.

Now let $x \in Z(\operatorname{Spin}(V))$. Then x being central in C_0 and $Z(C_0)$ having basis $(1, \zeta)$ by Theorem 3.23, there exist $a, b \in k$ such that $x = a + b\zeta$. By the definition of the spin group we have

$$1 = N(x) = x\overline{x} = (a + b\zeta)(a + b\overline{\zeta}) = a^2 + ab\overline{\zeta} + ab\zeta + b^2\zeta\overline{\zeta}. \qquad (*)$$

We distinguish two cases. If $n \equiv 0 \pmod 4$, then by Lemma 3.18 (ii) we have that $\overline{\zeta} = \zeta$. Since $\zeta\overline{\zeta} = N(\zeta) \in k$, Theorem 3.10 (ii) and $(*)$ imply that $2ab = 0$. As $\operatorname{char} k \neq 2$, this means that $a = 0$ or $b = 0$. If on the other hand $n \equiv 2 \pmod 4$, then Lemma 3.18 (ii) says that $\overline{\zeta} = -\zeta$. By the defining properties of Γ and $\operatorname{Spin}(V)$, we have

$$\alpha(x)e_1x^{-1} = xe_1\overline{x} = (a + b\zeta)e_1(a + b\overline{\zeta}) \in V.$$

Taking again Lemma 3.18 into account, this results in

$$e_1(a - b\zeta)(a - b\zeta) = e_1(a^2 + b^2\zeta^2) - 2abe_1\zeta \in V,$$

where $a^2 + b^2\zeta^2 \in k$ and $e_1\zeta = Q(e_1)e_2 \cdots e_n$. Expressing the above element of V in the basis $(e_1, \ldots, e_n)$, the assumption $n \geq 4$ and Theorem 3.10 (ii) imply that $2abQ(e_1) = 0$, that is, $a = 0$ or $b = 0$. Thus, we have seen that in any case, either $x = a \in k$ or $x = b\zeta$ with $b \in k$. Application of the norm yields $x = \pm 1$ or $x = \pm\zeta$. The structure of the unit group follows from Lemma 3.18 (iii).

Finally, assume that $\operatorname{char} k = 2$. The proof proceeds by a similar approach as before. We first need to describe the centre of C_0. Following the discussion on p. 123 of [Gro02], there is a basis $(u_1, v_1, \ldots, u_m, v_m)$ of V (where $m = \frac{n}{2}$) with $Q(u_1) \neq 0$ and the subsequent properties: Putting $z := \sum_{i=1}^m u_iv_i$ and $\nu := \sum_{i=1}^m Q(u_i)Q(v_i)$, it holds that $Z(C_0) = \operatorname{span}(1, z)$, $zu_1 = u_1z + u_1$, $z^2 = \nu + z$ and $\overline{z} = m + z$. Thus, if $x \in Z(\operatorname{Spin}(V))$, there are $a, b \in k$ with $x = a + bz$. The equation $(*)$ holds with ζ replaced by z and by the above properties amounts to

$$1 = a^2 + abm + b^2\nu + (b^2m + b^2)z.$$

If $n \equiv 0 \pmod 4$, then m is even and the above equation yields $b^2 = 0$, so $b = 0$ and $x = a \in k$. Since $N(x) = 1$ we get $x = 1$. Now suppose $n \equiv 2 \pmod 4$, that is, $m = 1 \in k$. Similarly as above, the condition $\rho_x(u_1) \in V$ here means that

$$xu_1\overline{x} = (a + bz)u_1(a + b + bz) = u_1(a^2 + b^2 + b^2\nu) + b^2u_1z \in V$$

from which we get $b^2u_1z = b^2Q(u_1)v_1 + b^2\sum_{i=2}^m u_1u_iv_i \in V$. Since $m = \frac{n}{2} \geq 2$, Theorem 3.10 (ii) forces $b^2 = 0$ and we obtain $x = 1$ as before. This finishes the proof. ☐

The above proof uses the structure theory of Clifford algebras. Alternatively, one may compute the centre of $\operatorname{SO}(V)$ and use the upper exact row from Theorem 3.39 to obtain a description of $Z(\operatorname{Spin}(V))$.

Remark 3.44. Using the lower long row from Theorem 3.39, one may show that under the appropriate assumptions, the group $\mathrm{Pin}(V)$ is generated by the elements -1 and $v \in V$ with $Q(v) = -1$ and that $C = \langle \mathrm{Pin}(V) \rangle_{k\text{-alg.}}$. Together with the results from Section 3.2, the latter may be used to compute the centre of $\mathrm{Pin}(V)$.

4 Algebraic Groups

We assume that k is algebraically closed.

In this chapter, we introduce all relevant concepts and results from the theory of algebraic groups that are needed in order to show that the spin groups are algebraic groups and to examine their properties as such. Our aim is to show that the spin groups fit into the right place in the classification of semisimple algebraic groups which is achieved at the end of Section 4.4.

4.1 Geometric Background and Basic Definitions

In this section, we define algebraic groups and a few basic notions associated with them. To provide the necessary background, we begin with a short recapitulation of (affine) varieties and basic algebraic geometry and collect some facts from this area that will be used in the sequel. The material can be found in [Hum95b], Sections 1-3, [MT11], Chapter 1 and [Spr98], Chapter 1.

Subsets of k^n of the form

$$V(I) := \{a = (a_1, \dots, a_n) \in k^n \mid f(a) = 0 \text{ for all } f \in I\}$$

for an ideal $I \trianglelefteq k[T_1, \dots, T_n]$ are called *algebraic sets.* Declaring the algebraic sets to be the closed subsets, defines a topology on k^n, the *Zariski topology.* Then also the algebraic sets themselves become topological spaces, equipped with the subspace topology. An algebraic set together with this topology is (provisionally) called an *affine variety.* Associated with an affine variety X we have its *ideal*

$$I(X) := \{f \in k[T_1, \dots, T_n] \mid f(x) = 0 \text{ for all } x \in X\}$$

and the *coordinate algebra* $k[X] := k[T_1, \dots, T_n]/I(X)$. The latter can be thought of as the k-algebra of polynomial functions on X.

A *morphism* between affine varieties $X \subseteq k^n$ and $Y \subseteq k^m$ is a map $\varphi\colon X \to Y$ that can be given by polynomial functions in the coordinates of X, which means that there are $\psi_1, \dots, \psi_m \in k[X]$ such that $\varphi(x) = (\psi_1(x), \dots, \psi_m(x))$ for all $x \in X$. A morphism $\varphi\colon X \to Y$ is called an *isomorphism* if there is a morphism $\psi\colon Y \to X$ with $\psi \circ \varphi = \mathrm{id}_X$ and $\varphi \circ \psi = \mathrm{id}_Y$; hence, φ is an isomorphism if and only if it is bijective and the inverse map is again a morphism. Associated with a morphism $\varphi\colon X \to Y$ is a k-algebra homomorphism

$$\varphi^*\colon k[Y] \to k[X],\ f \mapsto f \circ \varphi.$$

This assignment behaves functorially; in particular, φ is an isomorphism if and only if φ^* is a k-algebra isomorphism. It holds that concatenations of morphisms are again morphisms and that the inclusion $X \hookrightarrow Y$ of a closed subset $X \subseteq Y$ is a morphism. Hence, restrictions of morphisms to closed subsets remain morphisms. Furthermore, morphisms are continuous with respect to the Zariski topology.

If $X \subseteq k^n$ and $Y \subseteq k^m$ are affine varieties, then so is their product $X \times Y \subseteq k^{n+m}$. In particular, it carries the Zariski topology and we will always consider it being equipped with this topology which is in general different from the product topology. It holds that the projections $X \times Y \to X$ and $X \times Y \to Y$ are morphisms, and that $k[X \times Y] \cong k[X] \otimes k[Y]$.

Note that any finite-dimensional k-vector space is an affine variety. Indeed, picking a linear isomorphism to an affine space k^n allows one to define a variety structure on the vector space. It does not depend on the chosen linear isomorphism since linear isomorphisms $k^n \to k^n$ are isomorphisms of varieties. With this structure, linear maps between vector spaces are morphisms of varieties, being given by multiplication with a constant matrix. Moreover, vector subspaces are closed subsets as they are kernels of linear maps.

These concepts are generalized by the notion of a *variety* (cf. [Hum95b], Section 2); then an *affine variety* is a variety that is isomorphic to an affine variety $X \subseteq k^n$ as defined before. An important example for this is the following: If $X \subseteq k^n$ is an affine variety and $f \in k[X]$ is a polynomial function on X, then $D(f) := \{\, x \in X \mid f(x) \neq 0 \,\}$ is an open subset of X and is an affine variety in the new sense. It is called a *principal open subset*. Indeed, $D(f)$ is isomorphic to

$$\{\, (x, a) \in X \times k \mid f(x) \cdot a = 1 \,\} \subseteq k^{n+1}$$

and so has coordinate algebra $k[D(f)] \cong k[X]_f$, the localization of $k[X]$ at f. It holds that if $\varphi\colon X \to Y$ is a morphism of varieties and $U \subseteq X$ and $V \subseteq Y$ are open subsets with $\varphi(U) \subseteq V$, then U and V are varieties, and the restriction $\varphi\big|_U\colon U \to V$ is again a morphism.

Recall that a topological space is called *irreducible* if it cannot be written as the union of two proper closed subsets, and is called *connected* if it cannot be written as the disjoint union of two proper closed subsets. In particular, any irreducible space is connected. Furthermore, the image of an irreducible respectively connected space under a continuous map is again irreducible respectively connected. An affine variety X is irreducible if and only if $k[X]$ is an integral domain. If X and Y are irreducible affine varieties, then so is $X \times Y$.

An (affine) variety X is a *Noetherian* topological space, that is, every descending chain of closed subsets must become stationary. As such, it has finitely many maximal irreducible subsets. These are closed and cover X and are called the *irreducible components* of X. Similarly, X is the disjoint union of finitely many closed connected subsets. These are uniquely determined and called the *connected components* of X.

Let X be an affine variety. If X is irreducible, then $k[X]$ is an integral domain and the *dimension* of X is defined to be $\dim X := \operatorname{trdeg}_k k(X)$, the transcendence degree of $k(X)$ over k, where $k(X)$ is the field of fractions of $k[X]$. For an arbitrary affine variety X with irreducible components $X_1, \dots, X_r$ the dimension is defined to be $\dim X := \max_i \dim X_i$. This notion of dimension agrees with that for the topological space X (cf. [Bor91], AG §9). We have the following important fact:

Proposition 4.1. *Let X be an irreducible (affine) variety. Suppose that $Y \subsetneq X$ is a proper closed subset. Then $\dim Y < \dim X$.*

Proof. This is [MT11], Proposition 1.22. □

Furthermore, it holds that an affine variety is 0-dimensional if and only if it is finite, and for two affine varieties X and Y we have $\dim X \times Y = \dim X + \dim Y$.

With these geometric notions and concepts available, one may now define algebraic groups.

Definition 4.2. A group G is called a *linear algebraic group* if it is an affine variety and the group operations

$$G \times G \to G,\ (x, y) \mapsto xy, \qquad G \to G,\ x \mapsto x^{-1},$$

are morphisms of varieties.

The term "linear" refers to the circumstance that G is an *affine* variety and stems from the fact that any linear algebraic group may be embedded into a general linear group (see Theorem 4.11). From now on, we will drop the term "linear" and simply speak of algebraic groups since we will exclusively be dealing with affine varieties in this context.

Example 4.3.

(a) The additive group $\mathbf{G}_\mathrm{a} := (k, +)$ is an affine variety since it is given by $V(0) \subseteq k$. Its coordinate algebra is $k[\mathbf{G}_\mathrm{a}] = k[T]$. Hence, $\mathbf{G}_\mathrm{a}$ is irreducible, and $\dim \mathbf{G}_\mathrm{a} = 1$. The group operations $k \times k \to k,\ (x, y) \mapsto x + y$ and $k \to k,\ x \mapsto -x$ are clearly given by polynomials, so $\mathbf{G}_\mathrm{a}$ is an algebraic group.

(b) The multiplicative group $\mathbf{G}_\mathrm{m} := (k^\times, \cdot)$ is a principal open subset of k, given by non-vanishing of $T \in k[T]$. Hence, it is an affine variety, with coordinate algebra $k[\mathbf{G}_\mathrm{m}] \cong k[T]_T \cong k[T, T^{-1}]$. Again, the group operations are morphisms, so that $\mathbf{G}_\mathrm{m}$ is an algebraic group. Looking at $k[\mathbf{G}_\mathrm{m}]$ we infer that $\mathbf{G}_\mathrm{m}$ is irreducible, and that $\dim \mathbf{G}_\mathrm{m} = 1$.

(c) More generally, the general linear group $\mathrm{GL}_n \subseteq k^{n^2}$ is an algebraic group. It is the principal open subset given by non-vanishing of the determinant and has coordinate algebra $k[\mathrm{GL}_n] \cong k[T_{ij} \mid i \leq i,j \leq n]_{\det(T_{ij})}$. It follows that GL_n is irreducible with $\dim \mathrm{GL}_n = n^2$. Mulitplication clearly is a morphisms of varieties. By Cramer's rule, the same holds for inversion. Note that $\mathrm{GL}_1 = \mathbf{G}_{\mathrm{m}}$.

If V is a k-vector space of finite dimension n, then by choosing a basis of V we obtain a group isomorphism $\mathrm{GL}(V) \cong \mathrm{GL}_n$. For two different bases, these isomorphisms only differ by an inner automorphism of GL_n which is an isomorphism of varieties. Thus, we may use the variety structure on GL_n to make $\mathrm{GL}(V)$ into an algebraic group, and this does not depend on the choice of basis.

Example 4.4. We look at two possibilities to obtain new algebraic groups from known ones.

(a) By the properties of affine varieties and morphisms, closed subgroups of algebraic groups are again algebraic groups. An important example for this is the group

$$\mathrm{D}_n := \{ \operatorname{diag}(c_1, \ldots, c_n) \mid c_i \in k^\times \} \leq \mathrm{GL}_n$$

of invertible diagonal matrices.

(b) If G and H are algebraic groups, then so is $G \times H$, with the usual group operations.

A basic, yet fundamental result in the theory of algebraic groups is the following:

Proposition 4.5. *Let G be an algebraic group. Then the following hold:*

(i) The irreducible components of G are pairwise disjoint, so they are the connected components of G.

(ii) The irreducible component G° containing $1 \in G$ is a closed normal subgroup of G of finite index and whose cosets are the irreducible components of G.

(iii) Any closed subgroup of G of finite index contains G°.

Proof. See [MT11], Proposition 1.13, or [Hum95b], Proposition 7.3. □

Thus, for an algebraic group G the notions irreducible and connected agree. We will from now on use the term connected for this property.

Corollary 4.6. *Let G and H be algebraic groups. Then the following hold:*

(i) $(G \times H)^\circ = G^\circ \times H^\circ$.

(ii) If $H \leq G$ is closed, then $H^\circ \leq G^\circ$.

Proof.

(i) Since G° and H° are irreducible affine varieties, so is $G^\circ \times H^\circ$. Therefore, it must be contained in a maximal irreducible subset of $G \times H$, that is, in an irreducible component. But we have $(1,1) \in G^\circ \times H^\circ$ which implies that $G^\circ \times H^\circ \subseteq (G\times H)^\circ$. Conversely, by Proposition 4.5 (ii), $G^\circ \times H^\circ \trianglelefteq (G \times H)^\circ$ is a closed subgroup of finite index $|G : G^\circ||H : H^\circ|$. Hence, part (iii) of the above proposition shows that $(G \times H)^\circ \subseteq G^\circ \times H^\circ$.

(ii) As above, $G^\circ \times H^\circ \subseteq G \times G$ is an irreducible subset. Application of the multiplication map yields that $G^\circ H^\circ \subseteq G$ is irreducible. With the same reasoning as in part (i) it follows that $G^\circ H^\circ \subseteq G^\circ$, giving $H^\circ \leq G^\circ$ by the fact that $1 \in G^\circ$. □

We next study morphisms between algebraic groups.

Definition 4.7. Let G and G' be algebraic groups. A map $\varphi\colon G \to G'$ is called a *morphism of algebraic groups* if it is a group homomorphism as well as a morphism of varieties and is called an *isomorphism (of algebraic groups)* if it is a group isomorphism and simultaneously an isomorphism of varieties.

It is clear that the restriction of a morphism of algebraic groups to a closed subgroup is again a morphism of algebraic groups. In addition, we have the following properties:

Proposition 4.8. *Let $\varphi\colon G \to G'$ be a morphism of algebraic groups. Then the following hold:*

(i) $\ker\varphi$ *is a closed subgroup of* G *and* $\operatorname{im}\varphi$ *is a closed subgroup of* G',

(ii) $\varphi(G^\circ) = \varphi(G)^\circ$,

(iii) $\dim\ker\varphi + \dim\operatorname{im}\varphi = \dim G$.

Proof. See [Hum95b], Proposition 7.4 B, or [Bor91], Corollary 1.4. □

Definition 4.9. Let $\varphi\colon G \to G'$ be a morphism of algebraic groups.

(a) If φ is an isormorphism onto its image, then it is called an *embedding of algebraic groups.*

(b) If $G' = \mathrm{GL}(V)$ for some finite-dimensional k-vector space V, then φ is called a *rational representation* of G.

(c) If φ is surjective and has finite kernel, then it is called an *isogeny.*

Example 4.10.

(a) The determinant map $\det\colon \mathrm{GL}_n \to \mathbf{G}_\mathrm{m}$ is a morphism of algebraic groups since it is clearly given by a polynomial function in the coordinates. The kernel of det is the special linear group SL_n which is then an algebraic group by Proposition 4.8 (i), being a closed subgroup of GL_n. By Example 4.3 and Proposition 4.8 (iii) we have $\dim\mathrm{SL}_n = n^2 - 1$.

Analogously as for the general linear group, if V is a k-vector space of finite dimension n, then $\mathrm{SL}(V)$ can be naturally considered as an algebraic group via the basis representation isomorphism $\mathrm{SL}(V) \cong \mathrm{SL}_n$.

(b) The map $\mathbf{G}_{\mathrm{a}} \to \mathrm{GL}_2,\ a \mapsto \left(\begin{smallmatrix} 1 & a \\ & 1 \end{smallmatrix}\right)$ is an embedding of algebraic groups.

More generally, every algebraic group can be embedded into a general linear group:

Theorem 4.11. *Let G be an algebraic group. Then there is an embedding of algebraic groups $G \hookrightarrow \mathrm{GL}_n$ for some $n \in \mathbb{N}$.*

Proof. See [Hum95b], Theorem 8.6, [Spr98], Theorem 2.3.7, or [Bor91], Proposition 1.10. ☐

4.2 Some Results on Algebraic Groups

In this section, we collect some results from the theory of algebraic groups that will be needed for our investigation of the spin groups and spin representations. We quickly introduce the necessary notions and for the results refer to the literature as the proofs require a deeper study of the theory involved. For a thorough treatment of this theory and references for the stated results, see the books [Hum95b], [Spr98], [MT11], [Bor91] and [Gec03].

4.2.1 Jordan Decomposition

Let V be a finite-dimensional k-vector space. An element $s \in \mathrm{End}(V)$ is called *semisimple* if it is diagonalizable. It follows from the existence of Jordan normal forms that if $x \in \mathrm{End}(V)$ is an endomorphism of V, then there exist unique $s \in \mathrm{End}(V)$ semisimple and $n \in \mathrm{End}(V)$ nilpotent such that $x = s + n$ and $sn = ns$ (additive Jordan decomposition). We now want to derive a multiplicative version of this. For this, we need to introduce the following notion:

Definition 4.12. Let V be a finite-dimensional k-vector space. An endomorphism $u \in \mathrm{End}(V)$ is called *unipotent* if $u - 1$ is nilpotent.

Lemma 4.13. *Let V be a finite-dimensional k-vector space and let $u \in \mathrm{End}(V)$.*

(i) u is unipotent if and only if all eigenvalues of u are 1.

(ii) If u is unipotent and $x \in \mathrm{End}(V)$ is conjugate to u, then also x is unipotent.

(iii) Suppose that $p := \operatorname{char} k > 0$. Then u is unipotent if and only if it has p-power order.

(iv) Suppose that $\operatorname{char} k = 0$. If $u \neq 1$ and u is unipotent, then u has infinite order.

Proof. The first claim follows from the fact that an endomorphism is nilpotent if and only if all its eigenvalues are 0. For part (ii) note that if $x \in \mathrm{End}(V)$ is conjugate to u, then they have the same eigenvalues. Thus, the second statement follows from part (i).

Now suppose that $p := \operatorname{char} k > 0$. The element $u - 1$ is nilpotent if and only if there is some $r \in \mathbb{N}$ such that $0 = (u-1)^{p^r} = u^{p^r} - 1$. This shows that u is unipotent if and only if it has p-power order. Finally, suppose that $\operatorname{char} k = 0$ and that $1 \neq u$ is unipotent. Then the Jordan normal form of u must contain a non-trivial Jordan block J_i, $i \geq 2$. But this Jordan block has infinite order in characteristic 0, so also u has infinite order. ☐

From the additive Jordan decomposition one may now derive:

Proposition 4.14 (Multiplicative Jordan decomposition)**.** *Let V be a k-vector space of finite dimension and let $x \in \mathrm{GL}(V)$.*

(i) There are unique $x_s, x_u \in \mathrm{GL}(V)$ such that $x = x_s x_u$, where x_s is semisimple, x_u is unipotent and $x_s x_u = x_u x_s$.

(ii) If $y \in \mathrm{GL}(V)$ commutes with x, then $(xy)_s = x_s y_s$ and $(xy)_u = x_u y_u$.

Proof. See [Hum95b], Lemma 15.1 B. ☐

This can be generalized to algebraic groups as follows:

Theorem 4.15 (Jordan decomposition in algebraic groups)**.** *Let G be an algebraic group and let $g \in G$.*

(i) For any embedding e of G into some $\mathrm{GL}(V)$ for V a finite-dimensional k-vector space there exist unique $g_s, g_u \in G$ such that $g = g_s g_u$ where $e(g_s)$ is semisimple, $e(g_u)$ is unipotent, and $g_s g_u = g_u g_s$.

(ii) The decomposition $g = g_s g_u = g_u g_s$ is independent of the chosen embedding.

(iii) If $\varphi\colon G \to G'$ is a morphism of algebraic groups, then we have $\varphi(g_s) = \varphi(g)_s$ and $\varphi(g_u) = \varphi(g)_u$.

(iv) If $h \in G$ commutes with g, then $(hg)_s = h_s g_s$ and $(hg)_u = h_u g_u$.

Proof. The first three parts are [MT11], Theorem 2.5. For statement (iv) take any embedding $e\colon G \hookrightarrow \mathrm{GL}(V)$ for V a finite-dimensional k-vector space, cf. Theorem 4.11. Then the claim follows from Proposition 4.14 and parts (i) and (ii). ☐

Definition 4.16. Let G be an algebraic group and let $g \in G$. The decomposition $g = g_s g_u = g_u g_s$ from Theorem 4.15 is called the *Jordan decomposition* of g, and g_s and g_u are called the *semisimple* respectively *nilpotent part* of g. The element g is called *semisimple* if $g = g_s$ and is called *unipotent* if $g = g_u$. We write G_s for the set of semisimple elements of G and G_u for the set of unipotent elements of G. The group G is called *unipotent* if $G = G_u$.

Note that $g \in G$ is semisimple if and only if $g_u = 1$ and is it unipotent if and only if $g_s = 1$. Hence, $G_s \cap G_u = 1$. Morphisms of algebraic groups map semisimple elements to semisimple elements and unipotent elements to unipotent elements.

4.2.2 Tori

Two types of subgroups play a major role in the structure theory of algebraic groups.

Definition 4.17.

(a) An algebraic group is called a *torus* if it is isomorphic to D_n for some $n \in \mathbb{N}_{>0}$.

(b) Let G be an algebraic group. A *Borel subgroup* of G is a closed, connected, solvable subgroup of G that is maximal with respect to these properties.

With the aid of Borel subgroups, many questions regarding algebraic groups can be translated to questions on connected solvable algebraic groups, whose structure is known (cf. [Hum95b], Chapter VII, or [MT11], Chapter 4).

Definition 4.18. Let G be an algebraic group. A *character* of G is a morphism of algebraic groups $\chi\colon G \to \mathbf{G}_{\mathrm{m}}$ and a *cocharacter* of G is a morphism of algebraic groups $\gamma\colon \mathbf{G}_{\mathrm{m}} \to G$. The set of all characters of G is denoted by $X(G)$ and the set of all cocharacters is denoted by $Y(G)$.

Note that setting $(\chi_1 + \chi_2)(g) := \chi_1(g)\chi_2(g)$ for $\chi_1, \chi_2 \in X(G)$ and $g \in G$ defines a character $\chi_1 + \chi_2 \in X(G)$. This operation makes $X(G)$ into an abelian group. With the analogous construction, also $Y(G)$ is an (additively written) abelian group, provided that G is commutative.

We will mostly be considering characters and cocharacters of tori. If T is a torus, then as mentioned above, $X(T)$ and $Y(T)$ are abelian groups, referred to as the character resp. cocharacter group of T. Furthermore, the groups $X(T)$ and $Y(T)$ are closely related via a so-called perfect pairing, see [MT11], Proposition 3.6.

We study tori in more detail. Using the theory of Borel subgroups, one can show:

Proposition 4.19.

(i) An algebraic group is a torus if and only if it is connected and consists of semisimple elements.

(ii) Images of tori under morphisms of algebraic groups are tori.

Proof. For statement (i) see for example [MT11], Exercise 10.23 or [Spr98], Exercise 6.3.7. The second claim follows from the first and Theorem 4.15 (iii). ☐

A torus $T \leq G$ of an algebraic group G is called *maximal* if it is maximal among the subtori of G with respect to inclusion. These have the following properties:

Proposition 4.20. *Let G be an algebraic group.*

(i) All maximal tori of G are conjugate.

(ii) If $\varphi\colon G \to G'$ is a surjective morphism of algebraic groups, then φ sends maximal tori to maximal tori, and all maximal tori of G' are obtained this way.

Proof. The first claim is [MT11], Corollary 6.5. For part (ii) see [Hum95b], Corollary 21.3 C or [Bor91], Proposition 11.14. ☐

Definition 4.21. Let G be an algebraic group. The dimension of a maximal torus of G is called the *rank* of G and is denoted $\operatorname{rk} G$.

Note that the rank is well-defined by Proposition 4.20 (i).

4.2.3 The Radical

If $N, N' \trianglelefteq G$ are closed, connected, normal and solvable subgroups of an algebraic group G, then one may show that also NN' has these properties (cf. [Spr98], 6.4.14). This motivates the next definition.

Definition 4.22. Let G be an algebraic group.

(a) The unique maximal closed, connected, normal, solvable subgroup of G is called the *radical* of G and denoted $R(G)$. The *unipotent radical* of G is $R_u(G) := R(G)_u$.

(b) The group G is called *reductive* if $R_u(G) = 1$ and is called *semisimple* if it is connected and satisfies $R(G) = 1$.

One can show that the unipotent radical is the unique maximal closed, connected, unipotent subgroup of G (see [MT11], p. 41). Note that semisimple algebraic groups are reductive.

Example 4.23. The general linear group GL_n is connected reductive. However, it is not semisimple since $Z(\mathrm{GL}_n) \cong \mathbf{G}_\mathrm{m}$ is a non-trivial closed, connected, normal and solvable subgroup. An example of a semisimple algebraic group is the special linear group SL_n. See [MT11], Example 6.17 for detailed explanations of the above facts.

Let us introduce one more related notion.

Definition 4.24. An algebraic group is called *simple* if it is semisimple, non-trivial and has no non-trivial proper closed connected normal subgroups.

Note that a simple algebraic group need not be simple as an abstract group (cf. Example 4.31).

The subsequent proposition about isogenies will be helpful for establishing the simplicity of the spin group (see Theorem 4.53).

Proposition 4.25. *Let G and G' be algebraic groups with G connected and suppose that $\varphi\colon G \to G'$ is an isogeny. Then the following hold:*

(i) $\ker\varphi \subseteq Z(G)$,

(ii) if G' is semisimple, then so is G,

(iii) if G' is simple, then so is G.

Proof.

(i) By definition of an isogeny, $\ker\varphi \trianglelefteq G$ is a finite normal subgroup. Then it follows from [MT11], Exercise 10.4 that it is contained in the centre of G.

(ii) Taking continuity and surjectivity of φ as well as Proposition 4.8 (i) into account, the group $\varphi(R(G))$ is closed, connected, normal and solvable. Hence, $\varphi(R(G)) \subseteq R(G')$. But $R(G') = 1$ by assumption, giving $R(G) \subseteq \ker\varphi$. Since $R(G)$ is connected and $\ker\varphi$ is finite, we get $R(G) \subseteq (\ker\varphi)^\circ = 1$, that is, G is semisimple.

(iii) By part (ii), G is semisimple. It cannot be trivial by surjectivity of φ. Let $N \trianglelefteq G$ be a normal subgroup that is closed and connected. It follows as above that $\varphi(N) \trianglelefteq G'$ is closed, connected and normal. But G' is simple, so either $\varphi(N) = 1$ or $\varphi(N) = G'$. In the former case, we infer that $N = 1$, using the same arguments as in part (ii). We turn to the latter case and want to show that $N = G$. Assume that $N < G$. Then $\dim N < \dim G$ by Proposition 4.1. Thus, Proposition 4.8 (iii) gives

$$\dim\varphi(N) = \dim N - \dim\ker\varphi\big|_N = \dim N < \dim G = \dim G',$$

a contradiction. So we must have $N = G$, which shows that G is simple. □

4.2.4 Roots and the Classification of Semisimple Algebraic Groups

The importance of the definitions from the previous section is that there exist strong results on the structure of connected reductive groups and that such groups may be classified. A main ingredient in this classification are the so-called roots. They are usually defined via the adjoint action of a maximal torus of G on the Lie algebra of G (see for example [MT11], Section 8.1), where the Lie algebra may be constructed as the tangent space of G at the identity element (cf. [Hum95b], Section 9; it can be shown that this space carries the structure of a Lie algebra). To avoid all these constructions, we use the following equivalent definition from [GM16], 1.3.1:

Definition 4.26. Let G be a connected reductive algebraic group, let $T \leq G$ be a maximal torus, and let $\alpha \in X(T)$. Then α is a *root of G relative to T* if there exists a morphism of algebraic groups $u_\alpha \colon \mathbf{G}_\mathrm{a} \to G$ which is an isomorphism onto its image and which satisfies $tu_\alpha(a)t^{-1} = u_\alpha(\alpha(t)a)$ for all $t \in T$ and $a \in \mathbf{G}_\mathrm{a}$. The group $U_\alpha := \operatorname{im} u_\alpha \leq G$ is called the *root subgroup* corresponding to α. The set of roots of G relative to T is denoted by $R(G)$ or $R(G,T)$ and called the *root system* of G (with respect to T).

By [GLS97], Remark 1.9.6, the properties of the root system of a connected reductive algebraic group G do not depend on the choice of maximal torus. This justifies that we speak of *the* root system of G and omit the torus in the notation. When working with the root system without reference to a maximal torus, we always implicitly assume that a maximal torus has been chosen.

It turns out that the root system of a connected reductive algebraic group carries some structure as well. To describe it, we need the notion of an abstract root system:

Remark 4.27 (Abstract root systems)**.** We follow [Hum95b], Appendix and [MT11], Section 9.1. Let E be a finite-dimensional real vector space. An element $s \in \mathrm{GL}(E)$ is called a *reflection along* $0 \neq \alpha \in E$ if $s(\alpha) = -\alpha$ and s fixes pointwise a subspace of E of codimension 1. A subset $R \subseteq E$ is called an *abstract root system* in E if it satisfies the following properties:

(R1) R is finite, $0 \notin R$, and $\operatorname{span}(R) = E$;

(R2) if $\alpha \in R$ and $c\alpha \in R$ for some $c \in \mathbb{R}$, then $c = \pm 1$;

(R3) for each $\alpha \in R$ there exists a reflection $s_\alpha \in \mathrm{GL}(E)$ along α that stabilizes R;

(R4) if $\alpha, \beta \in R$, then $s_\alpha(\beta) - \beta$ is an integral multiple of α.

Let now R be an abstract root system in E. The elements of R are then called *roots* and the integer $\dim E$ is called the *rank* of R. One can show that there exists a positive definite bilinear form on E which is invariant under the group generated by the s_α for $\alpha \in R$. In the following, we always assume that such a bilinear form has been chosen.

A subset Δ of R is called a *base* of R if it is a vector space basis of E and has the property that every root $\beta \in R$ is an integral linear combination $\beta = \sum_{\alpha\in\Delta} c_\alpha \alpha$ where either all c_α are non-negative or all c_α are non-positive. The elements of Δ are then called *simple roots.* The root system R is said to be *decomposable*, if it can be written as the disjoint union of two non-empty and mutually orthogonal subsets. Otherwise, it is called *indecomposable.*

One can show that every root system has a base. Associated with an abstract root system R is its *Dynkin diagram* which is a graph that comes about as follows: Choose a base Δ of R. Then the simple roots are the nodes of the Dynkin diagram. Depending on the order of $s_\alpha s_\beta$ and the length of α and β, two nodes α and β are joined by up to three edges which may carry an arrow pointing from one node to the other (see [MT11], p. 66). One can show that a root system is indecomposable if and only if its Dynkin diagram is connected.

It holds that two abstract root systems are isomorphic if and only if their Dynkin diagrams agree where an isomorphism between root systems R and R' is a vector space isomorphism between the underlying real vector spaces that sends R to R' and preserves the integers occuring in (R4). This allows to classify all indecomposable root systems by determining all connected Dynkin diagrams. See [MT11], Theorem 9.6 for this classification and a table of all possible connected Dynkin diagrams.

Let G be a semisimple algebraic group. One may consider $R(G)$ as a subset of the real vector space $X(T)\otimes_{\mathbb{Z}}\mathbb{R}$ and show that it is an abstract root system in $X(T)\otimes_{\mathbb{Z}}\mathbb{R}$ (see [Hum95b], Theorem 27.1 or [MT11], Proposition 9.2). Hence, the notions and results from Remark 4.27 apply to $R(G)$. An important property of the root system is that it allows to study G by investigating this combinatorial structure. One example for this is the following:

Proposition 4.28. *Let G be a semisimple algebraic group. Then G is simple if and only if $R(G)$ is indecomposable.*

Proof. See [MT11], Theorem 9.13, or [Bor91], Proposition 14.10. ☐

It turns out that the root system of a semisimple algebraic group G already almost determines its isomorphism type. To obtain a classification, there is one more additional piece of information necessary. It comes about as follows:

To each root $\alpha \in R(G)$, one may associate a so-called *coroot* $\alpha^\vee \in Y(T)$, see [MT11], p. 60. The set of coroots $R^\vee(G)$ then is an abstract root system in $Y(T)\otimes_{\mathbb{Z}}\mathbb{R}$, and the quadruple $(X(T), R(G), Y(T), R^\vee(G))$ has the properties of what is called a *root datum* (see [MT11], Definition 9.10 and Proposition 9.11). Therefore, it is called the *root datum* of G. This combinatorial structure now comprises enough information to determine the isomorphism type of G:

Theorem 4.29 (Classification of Semisimple Algebraic Groups)**.** *Two semisimple algebraic groups are isomorphic if and only if they have isomorphic root data. For each semisimple root datum there exists a semisimple algebraic group which realizes it.*

Proof. This is [MT11], Theorem 9.13. See also [Spr98], Theorems 9.6.2 and 10.1.1 or [GM16], Section 1.3. ☐

For the notion of isomorphism of root data, see [GM16], 1.2.2. The theorem may be extended to connected reductive groups, see [GM16] or [Spr98].

The possible root data for a fixed root system and therefore the different semisimple algebraic groups with a given root system can be classified with the aid of a finite group associated to the root system. Let G be a semisimple algebraic group with root datum $(X(T), R, Y(T), R^\vee)$. By [MT11], p. 70, there is an injective group homomorphism $X(T) \hookrightarrow \mathrm{Hom}(\mathbb{Z}R^\vee, \mathbb{Z}) =: \Omega$, and the quotient group $\Lambda(R) := \Omega/\mathbb{Z}R$ is finite. It only depends on R and is called the *fundamental group* of R. The root data for the root system R correspond exactly to the subgroups of $\Lambda(R)$. See [MT11], Table 9.2 or [Hum95b], p. 231 for a table of the fundamental groups of the indecomposable root systems.

Since $\mathbb{Z}R \leq X(T) \leq \Omega$, the quotient $X(T)/\mathbb{Z}R$ is a subgroup of $\Lambda(R)$ and together with R determines the isomorphism type of G. For the different semisimple groups with the same root system there is the following terminology:

Definition 4.30. Let G be a semisimple algebraic group with maximal torus T and root system $R := R(G, T)$. Let Ω be as above. If $X(T) = \mathbb{Z}R$, i.e. $X(T)/\mathbb{Z}R = 1$, then G is said to be of *adjoint type*. If $X(T) = \Omega$, i.e. $X(T)/\mathbb{Z}R = \Lambda(R)$, then G is called *simply connected*.

Example 4.31. Recall from Example 4.23 that SL_n is a semisimple algebraic group. One can show that its root system $R(\mathrm{SL}_n)$ is of type A_{n-1} (see for example [MT11], Example 9.8). Thus, Proposition 4.28 implies that SL_n is a simple algebraic group. It turns out that it is of simply connected type (cf. Table 9.2 of [MT11]).

4.3 The Special Orthogonal Group

Let V be a finite-dimensional vector space over k and let Q be a quadratic form on V. We assume that Q is nondegenerate.

We are going to prove that the orthogonal group and the special orthogonal group, that were introduced in Section 2.3, are algebraic groups. In addition, we state some of their geometric properties and describe a maximal torus, the root system and the root subgroups of $\mathrm{SO}(V)$. This study is motivated by the fact that the groups $\mathrm{Spin}(V)$ and $\mathrm{SO}(V)$ are closely connected, cf. Theorem 3.39. Indeed, in the Section 4.4, we will frequently use properties of the special orthogonal group to derive properties of the spin groups.

All results from this section are standard, see the references given in Section 4.2. We start off by showing that $\mathrm{O}(V)$ and $\mathrm{SO}(V)$ are algebraic groups:

Lemma 4.32. *The orthogonal group* $\mathrm{O}(V)$ *and the special orthogonal group* $\mathrm{SO}(V)$ *are closed subgroups of* $\mathrm{GL}(V)$*. In particular, they are algebraic groups.*

Proof. It follows from Lemma 2.13 that the condition $Q(\sigma(v)) = Q(v)$ for $v \in V$ is a polynomial condition in the coordinates of σ. Hence, $\mathrm{O}(V) \leq \mathrm{GL}(V)$ is closed. If $\operatorname{char} k \neq 2$ or $\dim V$ is odd, then $\mathrm{SO}(V) = \mathrm{O}(V) \cap \mathrm{SL}(V)$ which is clearly closed as well. In even dimension in characteristic 2, the claim for $\mathrm{SO}(V)$ follows from the exercise on page 130 of [Gro02] which shows that the pseudodeterminant is a morphism. ☐

Now in order to investigate the properties of the algebraic groups $\mathrm{O}(V)$ and $\mathrm{SO}(V)$ and to have easier computations, we would like to specialize to a specific quadratic form. This is justified by the following theorem:

Theorem 4.33. *All nondegenerate quadratic forms on* V *are isometric.*

Proof. This follows from [Gro02], Theorem 4.4 (for $\operatorname{char} k \neq 2$) and Theorem 12.9 (for $\operatorname{char} k = 2$) and relies on the assumption that k is algebraically closed. ☐

Definition 4.34. Let $n \in \mathbb{N}_{>0}$. If $n = 2m$ is even, define

$$Q_n \colon k^n \to k,\ (x_1, \dots, x_n) \mapsto x_1 x_{2m} + x_2 x_{2m-1} + \cdots + x_m x_{m+1},$$

and if $n = 2m+1$ is odd, define

$$Q_n \colon k^n \to k,\ (x_1, \dots, x_n) \mapsto x_1 x_{2m+1} + x_2 x_{2m} + \cdots + x_m x_{m+2} + x_{m+1}^2.$$

We further put

$$\mathrm{O}_n := \{ A \in \mathrm{GL}_n \mid Q_n(Ax) = Q_n(x) \text{ for all } x \in k^n \}$$

in the respective cases.

Lemma 4.35. *For* $n \in \mathbb{N}_{>0}$*, the map* Q_n *is a nondegenerate quadratic form on* k^n*, and* O_n *is an algebraic group.*

Proof. Clearly, Q_n satisfies (Q1). One calculates that $B_{Q_n} \colon k^n \times k^n \to k$ maps an element $\big((x_1, \dots, x_n), (y_1, \dots, y_n)\big) \in k^n \times k^n$ to $x_1 y_n + x_2 y_{n-1} + \cdots + x_n y_1$ if $n = 2m$ is even, and to

$$x_1 y_{2m+1} + \cdots + x_m y_{m+1} + 2 x_{m+1} y_{m+1} + x_{m+2} y_m + \cdots + x_{2m+1} y_1$$

if $n = 2m+1$ is odd, so that the matrix of B_{Q_n} with respect to the standard basis of k^n is

$$K_n := \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix} \qquad \text{respectively} \qquad \begin{pmatrix} & & K_m \\ & 2 & \\ K_m & & \end{pmatrix}.$$

If n is even or $\operatorname{char} k \neq 2$, it is thus clear that the matrix of B_{Q_n} is invertible, so B_{Q_n} is nondegenerate by definition, see Lemma 2.5. Then also Q_n is nondegenerate by Proposition 2.28. If $\operatorname{char} k = 2$ and n is odd, then one has $\operatorname{rad} B_{Q_n} = \operatorname{span}(e_{m+1})$ (the $(m+1)$-st standard basis vector), and $Q_n(e_{m+1}) = 1 \neq 0$. Hence, also in this case Q_n is nondegenerate by Proposition 2.28 (iv).

Finally, note that O_n is the group coming from $\mathrm{O}(k^n, Q_n)$ by choosing the standard basis, hence is an algebraic group by Lemma 4.32. ☐

The above proof and Lemma 2.35 also show that if $\operatorname{char} k \neq 2$, then O_n is (isomorphic to) the group

$$\{ A \in \mathrm{GL}_n \mid A^\top K_n A = K_n \}$$

with K_n defined as above. Now by Theorem 4.33 and Proposition 2.34, every orthogonal group of a nondegenerate quadratic form on an n-dimensional k-vector space is isomorphic as an algebraic group to O_n. The specific choice of Q_n will simplify computations; for example, there is a maximal torus of a particularly nice shape, see Proposition 4.39.

From now on, let $n \in \mathbb{N}_{>0}$ and let $m := \lfloor \frac{n}{2} \rfloor$ be the Witt index of Q_n (see Corollary 2.20).

The special orthogonal group SO_n is defined as before. It turns out that it is the connected component of the identity of O_n:

Proposition 4.36. *The special orthogonal group* SO_n *is connected and it holds that* $\mathrm{SO}_n = \mathrm{O}_n^\circ$.

Proof. For the connectedness of SO_n see [Gec03], Theorem 1.7.4 (c) and Theorem 1.7.8 (take the remark on page 36 into account). Then Corollary 4.6 (ii) implies that $\mathrm{SO}_n = \mathrm{SO}_n^\circ \leq \mathrm{O}_n^\circ$. Conversely, by Corollary 2.40 and Lemma 4.32, the special orthogonal group is a closed subgroup of O_n of finite index. It follows from Proposition 4.5 (iii) that $\mathrm{O}_n^\circ \leq \mathrm{SO}_n$. ☐

This gives an alternative way of defining SO_n over algebraically closed fields (cf. [MT11], Definition 1.15).

The next proposition will become important later. It is the same construction as on page 314 of [Bum13].

Proposition 4.37. *Suppose that* $V', V'' \leq V$ *are subspaces such that* $V = V' \perp V''$. *Then the map*

$$\mathrm{O}(V') \times \mathrm{O}(V'') \to \mathrm{O}(V),\ (\sigma, \tau) \mapsto \sigma \oplus \tau,$$

is an embedding of algebraic groups. In particular, there are embeddings of algebraic groups

$$\mathrm{SO}(V') \hookrightarrow \mathrm{SO}(V') \times \mathrm{SO}(V'') \hookrightarrow \mathrm{SO}(V),$$

the first being given by $\sigma \mapsto (\sigma, 1)$ *and the second being the restriction of the above map.*

Proof. To check that the map is well-defined, let $v = v' + v'' \in V$ with $v' \in V'$ and $v'' \in V''$, and let $\sigma \in \mathrm{O}(V')$ and $\tau \in \mathrm{O}(V'')$. By orthogonality, we have

$$Q\big((\sigma \oplus \tau)(v)\big) = Q\big(\sigma(v') + \tau(v'')\big) = Q\big(\sigma(v')\big) + Q\big(\tau(v'')\big) = Q(v') + Q(v'') = Q(v),$$

so $\sigma \oplus \tau \in \mathrm{O}(V)$. By Proposition 1.6 (i), the map is an injective group homomorphism.

Picking a basis according to the orthogonal decomposition $V = V' \perp V''$, the matrix of $\sigma \oplus \tau$ with respect to this basis is a block diagonal matrix, the two diagonal blocks being the matrix of σ with respect to part of the basis that is contained in V' and the matrix of τ with respect to the rest of the basis vectors. Thus, the given map is a morphism of varietes. Furthermore, in this setting, the inverse map from the image to $\mathrm{O}(V') \times \mathrm{O}(V'')$ is given by $\left(\begin{smallmatrix} A & \\ & B \end{smallmatrix}\right) \mapsto (A, B)$, so it is a morphism.

The statement for the special orthogonal groups follows from Proposition 4.36 in combination with Corollary 4.6 (i). ☐

We continue by collecting important properties of the algebraic group SO_n.

Proposition 4.38. *It holds that* $\dim \mathrm{SO}_n = \frac{n(n-1)}{2}$.

Proof. This follows from Corollary 1.5.14 of [Gec03] (note the remark on page 36 regarding characteristic 2). ☐

Proposition 4.39. *Suppose that* $n = 2m$ *is even. Then*

$$T := \{\, \mathrm{diag}(t_1, \ldots, t_m, t_m^{-1}, \ldots, t_1^{-1}) \mid t_i \in k^\times \,\} = D_n \cap \mathrm{SO}_n \leq \mathrm{SO}_n$$

is a maximal torus of SO_n. *If* $n = 2m + 1$ *is odd, then*

$$T := \{\, \mathrm{diag}(t_1, \ldots, t_m, 1, t_m^{-1}, \ldots, t_1^{-1}) \mid t_i \in k^\times \,\} = D_n \cap \mathrm{SO}_n \leq \mathrm{SO}_n$$

is a maximal torus of SO_n. *In particular, for any* n *we have* $\mathrm{rk}\,\mathrm{SO}_n = m = \lfloor \frac{n}{2} \rfloor$.

Proof. See [MT11], Example 6.7 and Exercise 10.19. ☐

Using [MT11], Example 6.7 (4), one shows as in [MT11], Example 6.17 (4) that SO_n is reductive. See also [Spr98], Exercise 7.4.7. We now describe the root system of SO_n. Let T be the maximal torus from Proposition 4.39. For $i = 1, \ldots, m$ we denote by $\varepsilon_i \colon T \to \mathbf{G}_\mathrm{m}$ the map that sends an element $t \in T$ to its i-th diagonal entry. It is clear that $\varepsilon_i \in X(T)$. These characters now play an important role for determining the root system of SO_n which turns out to depend on the parity of n:

Theorem 4.40. *Suppose that $n = 2m$ is even. For $1 \le i < j \le m$ define maps*

$$\begin{aligned} u_{\varepsilon_i-\varepsilon_j} \colon \mathbf{G}_{\mathrm{a}} &\to \mathrm{SO}_{2m},\ a \mapsto I_{2m} + a(E_{i,j} - E_{2m+1-j,2m+1-i}), \\ u_{-\varepsilon_i+\varepsilon_j} \colon \mathbf{G}_{\mathrm{a}} &\to \mathrm{SO}_{2m},\ a \mapsto I_{2m} + a(-E_{j,i} + E_{2m+1-i,2m+1-j}), \\ u_{\varepsilon_i+\varepsilon_j} \colon \mathbf{G}_{\mathrm{a}} &\to \mathrm{SO}_{2m},\ a \mapsto I_{2m} + a(E_{i,2m+1-j} - E_{j,2m+1-i}), \\ u_{-\varepsilon_i-\varepsilon_j} \colon \mathbf{G}_{\mathrm{a}} &\to \mathrm{SO}_{2m},\ a \mapsto I_{2m} + a(E_{2m+1-i,j} - E_{2m+1-j,i}). \end{aligned}$$

These are morphisms of algebraic groups that are isomorphisms onto their respective image. Put

$$R := \{\, \pm(\varepsilon_i - \varepsilon_j), \pm(\varepsilon_i + \varepsilon_j) \mid 1 \le i < j \le m \,\}.$$

Then for each $\alpha \in R$ it holds that $tu_\alpha(a)t^{-1} = u_\alpha(\alpha(t)a)$ for all $t \in T$ and $a \in \mathbf{G}_{\mathrm{a}}$. In particular, $R = R(\mathrm{SO}_{2m})$ is the root system of SO_{2m} and the $U_\alpha := \operatorname{im} u_\alpha$, $\alpha \in R$ are the root subgroups of SO_{2m}. A basis of R is given by

$$\Delta := \{\, \varepsilon_i - \varepsilon_{i+1} \mid 1 \le i \le m-1 \,\} \cup \{\varepsilon_{m-1} + \varepsilon_m\},$$

and R is of type D_m.

Proof. The first part is a straight forward computation. See [GW09], page 94 for the corresponding results for the Lie algebra. For the root system, see [MT11], Example 11.7, [Bor91] 23.4 and 23.5, or [Spr98], Exercise 7.4.7 and Exercise 8.2.11. ☐

Theorem 4.41. *Suppose that $n = 2m+1$ is odd. For $1 \le i < j \le m$ define maps*

$$\begin{aligned} u_{\varepsilon_i-\varepsilon_j} \colon \mathbf{G}_{\mathrm{a}} &\to \mathrm{SO}_{2m+1},\ a \mapsto I_{2m+1} + a(E_{i,j} - E_{2m+2-j,2m+2-i}), \\ u_{-\varepsilon_i+\varepsilon_j} \colon \mathbf{G}_{\mathrm{a}} &\to \mathrm{SO}_{2m+1},\ a \mapsto I_{2m+1} + a(-E_{j,i} + E_{2m+2-i,2m+2-j}), \\ u_{\varepsilon_i+\varepsilon_j} \colon \mathbf{G}_{\mathrm{a}} &\to \mathrm{SO}_{2m+1},\ a \mapsto I_{2m+1} + a(E_{i,2m+2-j} - E_{j,2m+2-i}), \\ u_{-\varepsilon_i-\varepsilon_j} \colon \mathbf{G}_{\mathrm{a}} &\to \mathrm{SO}_{2m+1},\ a \mapsto I_{2m+1} + a(E_{2m+2-i,j} - E_{2m+2-j,i}), \end{aligned}$$

and for $1 \le i \le m$ define

$$\begin{aligned} u_{\varepsilon_i} \colon \mathbf{G}_{\mathrm{a}} &\to \mathrm{SO}_{2m+1},\ a \mapsto I_{2m+1} + 2aE_{i,m+1} - aE_{m+1,2m+2-i} - a^2E_{i,2m+2-i}, \\ u_{-\varepsilon_i} \colon \mathbf{G}_{\mathrm{a}} &\to \mathrm{SO}_{2m+1},\ a \mapsto I_{2m+1} + 2aE_{2m+2-i,m+1} - aE_{m+1,i} - a^2E_{2m+2-i,i}. \end{aligned}$$

These are morphisms of algebraic groups that are isomorphisms onto their respective image. Put

$$R := \{\, \pm(\varepsilon_i - \varepsilon_j), \pm(\varepsilon_i + \varepsilon_j) \mid 1 \le i < j \le m \,\} \cup \{\, \pm\varepsilon_i \mid 1 \le i \le m \,\}.$$

Then for each $\alpha \in R$ it holds that $tu_\alpha(a)t^{-1} = u_\alpha(\alpha(t)a)$ for all $t \in T$ and $a \in \mathbf{G}_{\mathrm{a}}$. In particular, $R = R(\mathrm{SO}_{2m+1})$ is the root system of SO_{2m+1} and the $U_\alpha := \operatorname{im} u_\alpha$, $\alpha \in R$ are the root subgroups of SO_{2m+1}. A basis of R is given by

$$\Delta := \{\, \varepsilon_i - \varepsilon_{i+1} \mid 1 \le i \le m-1 \,\} \cup \{\varepsilon_m\},$$

and R is of type B_m.

Proof. This is analogous to Theorem 4.40. See again [GW09], page 94, or [Spr98], Exercise 7.4.7 and Exercise 8.2.11, for example. ☐

Theorem 4.42. *The special orthogonal group* SO_n *is a semisimple algebraic group for* $n \geq 3$*. It is simple for* $n = 3$ *and* $n \geq 5$*.*

Proof. By Proposition 4.36, the special orthogonal group is connected. As mentioned above, it further is reductive. Now for $n \geq 3$, Example 2.4.11 of [Gec03] shows that $Z(\mathrm{SO}_n) = \{\pm 1\}$. Alternatively, this follows from [MT11], Theorem 8.17 (h) and Theorems 4.40 and 4.41. In particular, $Z(\mathrm{SO}_n)^\circ = 1$, so that Corollary 8.22 and Proposition 6.20 of [MT11] imply that SO_n is semisimple. If $n = 3$ or $n \geq 5$, the root system of SO_n, which has been described in Theorems 4.40 and 4.41, is indecomposable by [MT11], Theorem 9.6. Hence, SO_n is simple by Proposition 4.28. ☐

Note that $\mathrm{SO}_1 = 1$ is the trivial group and that SO_2 is abelian, isomorphic to $\mathbf{G}_\mathrm{m}$, see [Gec03], pages 33 and 35. Moreover, SO_4 fails to be simple because its root system $D_2 \cong A_1 \times A_1$ is decomposable. One can show that SO_{2m+1} is of adjoint type whereas SO_{2m} is neither adjoint nor simply connected, see Table 9.2 of [MT11].

Remark 4.43 (Symplectic Groups)**.** Suppose that $n = 2m$ is even and that B is a nondegenerate alternating bilinear form on V. With the aid of (2.1), one sees that the symplectic group $\mathrm{Sp}(V)$ is an algebraic group. Analogous to Theorem 4.33, one has that all nondegenerate alternating bilinear forms on V are equivalent (see [Gro02], Corollary 2.12), where two bilinear forms are called equivalent if there is a linear automorphism of V that preserves the bilinear forms (see [Gro02], p. 17). It follows that all symplectic groups of nondegenerate alternating bilinear forms on an n-dimensional vector space are isomorphic as algebraic groups.

As for the orthogonal groups, one therefore chooses a certain bilinear form in order to study the symplectic groups. Let $J_n := \left(\begin{smallmatrix} & K_m \\ -K_m & \end{smallmatrix}\right)$ where K_m is defined as in the proof of Lemma 4.35. The matrix J_n is skew-symmetric and invertible and therefore gives rise to a nondegenerate alternating bilinear form on k^n. Similarly as for the orthogonal groups, we put

$$\mathrm{Sp}_n := \{\, A \in \mathrm{GL}_n \mid A^\top J_n A = J_n \}.$$

This is clearly an algebraic group. One may prove that $\dim \mathrm{Sp}_n = 2m^2 + m$ (see [Gec03], Corollary 1.5.14). Furthermore, one can show that Sp_n is a simply connected simple algebraic group of type C_m, see Table 9.2 of [MT11].

4.4 Spin Groups as Algebraic Groups

In this section, let V be a finite-dimensional vector space over k and let Q be a quadratic form on V with associated symmetric bilinear form B. By C we denote the

Clifford algebra for (V, Q) and by Γ we denote its Clifford group. Recall from Section 3.3 that Γ comes with the twisted adjoint representation $\rho\colon \Gamma \to \mathrm{GL}(V)$.

We assume that B is nondegenerate (cf. Remark 2.29). Let $n := \dim V$. Since k is algebraically closed, Q has maximal Witt index $m := m(Q) = \lfloor \frac{n}{2} \rfloor$ by Corollary 2.20. We fix a Lagrangian decomposition $V = U \oplus W$ respectively $V = (U \oplus W) \perp \mathrm{span}(z)$ of V, with respect to bases $(u_1, \ldots, u_m)$ of U and $(w_1, \ldots, w_m)$ of W.

After having constructed the groups $\mathrm{Pin}(V)$ and $\mathrm{Spin}(V)$ as certain subgroups of the unit group $C^\times$ of the Clifford algebra in Section 3.3, we now show that they are in fact algebraic groups and derive some of their geometric properties. Our aim is to show that $\mathrm{Spin}(V)$ is a simply connected simple algebraic groups of type D_m if n is even, respectively of type B_m if n is odd. Furthermore, we explicitly determine the root subgroups of the spin group which will play a major role in our discussion of representatives for the unipotent conjugacy classes of $\mathrm{Spin}(V)$ in Section 6.3, and in our main algorithm in Section 7.1.

While the theoretical facts from this section are essentially well-known (cf. [KMRT98], Theorems 25.10 and 25.12), there scarcely is literature on the explicit constructions and proofs. The only reference that discusses some of the aspects in more detail is the book [GW09]. We are therefore going to provide explicit proofs for all statements in this section and indicate whenever they are adapted from [GW09].

As announced, we first verify that $\mathrm{Pin}(V)$ and $\mathrm{Spin}(V)$ are in fact algebraic groups. This is well-known (cf. [GW09], pages 317–318), and we now give a detailed proof.

Proposition 4.44.

(i) The unit group $C^\times$ is an algebraic group,

(ii) the groups $C_0^\times$, Γ, Γ_0, $\mathrm{Pin}(V)$ and $\mathrm{Spin}(V)$ are closed subgroups of $C^\times$,

(iii) the map $\rho\colon \Gamma \to \mathrm{GL}(V)$ is a rational representation.

In particular, we have an isogeny $\rho\colon \mathrm{Spin}(V) \to \mathrm{SO}(V)$.

Proof. Depending on the parity of $\dim V$, there are k-algebra isomorphisms $C \cong \mathrm{End}(\bigwedge W)$ respectively $C \cong \mathrm{End}(\bigwedge W) \oplus \mathrm{End}(\bigwedge W)$, as was shown in Theorems 3.20 and 3.25. In both cases, we may regard C as an affine variety in which addition and multiplication are morphisms of varieties (corresponding to matrix addition and multiplication). Note that this structure does not depend on the chosen Lagrangian decomposition since all maximal totally singular subspaces of V have the same dimension and linear isomorphisms are morphisms of varieties.

For the unit group we obtain $C^\times \cong \mathrm{GL}(\bigwedge W)$ respectively $C^\times \cong \mathrm{GL}(\bigwedge W) \times \mathrm{GL}(\bigwedge W)$. Example 4.3 (c) shows that $C^\times$ is an algebraic group. Furthermore, we may view $C^\times$ as a principal open subset of C. Observe that V and C_0, being vector subspaces, are closed subsets of C. By the properties of the $\mathbb{Z}_2$-grading, we have $C_0^\times = C_0 \cap C^\times$. Hence, $C_0^\times \leq C^\times$ is a closed subgroup.

Since the main involution $\alpha\colon C \to C$ and the main antiautomorphism $\tau\colon C \to C$ are linear maps, they are morphisms of varieties. Thus, also the norm $N\colon C \to C$ is a morphism of varieties, noting that multiplication in C is a morphism. Restricting to the princial open subset $C^\times$, we obtain a morphism $\alpha\big|_{C^\times}\colon C^\times \to C$. In addition, Cramer's rule implies that inversion $C^\times \to C,\ x \mapsto x^{-1}$ is a morphism of varieties. Then for $v \in V$ the map

$$f_v\colon C^\times \to C,\ x \mapsto \alpha(x)vx^{-1},$$

is a morphism as well. It follows that the Clifford group

$$\Gamma = \{\, x \in C^\times \mid \alpha(x)vx^{-1} \in V \text{ for all } v \in V \,\} = \bigcap_{v\in V} f_v^{-1}(V)$$

is an intersection of closed subsets of $C^\times$ and therefore a closed subgroup of $C^\times$. Moreover, also $\mathrm{Pin}(V) = \Gamma \cap N^{-1}(1)$ is closed in $C^\times$. Closedness of Γ_0 and $\mathrm{Spin}(V)$ follow from that of C_0.

The representation $\rho\colon \Gamma \to \mathrm{GL}(V)$ is given by $\rho_x\colon V \to V,\ v \mapsto \alpha(x)vx^{-1}$, for $x \in \Gamma$. Using the identifications from above and choosing a basis for V, the image of a basis element under ρ_x is given by multiplication of this element with matrices whose entries are polynomials in the coordinates of $x \in \Gamma$. Thus, the coordinates of ρ_x are polynomial in the coordinates of x, that is, $\rho\colon \Gamma \to \mathrm{GL}(V)$ is a rational representation. ☐

Having established a variety structure on $\mathrm{Spin}(V)$, we next present two geometric lemmas that are needed in the sequel.

Lemma 4.45. *Suppose that* $\varphi\colon C_0 \to \mathrm{End}(X)$ *is a representation of* C_0 *on a finite-dimensional* k*-vector space* X*. Then the restriction* $\varphi\big|_{\mathrm{Spin}(V)}\colon \mathrm{Spin}(V) \to \mathrm{GL}(X)$ *is a morphism of varieties, hence a rational representation of* $\mathrm{Spin}(V)$*.*

Proof. As in the proof of Proposition 4.44 we consider C as an affine variety with princial open subset $C^\times$, which is an algebraic group. Now $C_0 \leq C$ is closed as it is a vector subspace, and we may regard $\varphi\colon C_0 \to \mathrm{End}(X)$ as a morphism of varieties. As in the above proof we have $C_0^\times = C_0 \cap C^\times$ which shows that $C_0^\times \subseteq C_0$ is open since $C^\times \subseteq C$ is open. Hence, the restriction $\varphi\big|_{C_0^\times}\colon C_0^\times \to \mathrm{GL}(X)$ is a morphism of varieties. This remains true when restricting further to the closed subgroup $\mathrm{Spin}(V) \leq C_0^\times$. ☐

Lemma 4.46. *Let* V_1 *and* V_2 *be finite-dimensional* k*-vector spaces and let* $Q_1\colon V_1 \to k$ *and* $Q_2\colon V_2 \to k$ *be quadratic forms with the property that the associated bilinear forms are nondegenerate. Let* $H \leq \mathrm{Spin}(V_2)$ *be a closed subgroup. Suppose that* $A \leq C(V_2)$ *is a subalgebra with* $H \subseteq A$ *and that* $\varphi\colon A \to C(V_1)$ *is an algebra homomorphism with* $\varphi(H) \subseteq \mathrm{Spin}(V_1)$*. Then the restriction* $\varphi\big|_H\colon H \to \mathrm{Spin}(V_1)$ *is a morphism of varieties.*

Proof. We again use the geometric model from Proposition 4.44. As a vector subspace, $A \leq C(V_2)$ is closed, and so $\varphi\colon A \to C(V_1)$ is a morphism of varieties. Now $\mathrm{Spin}(V_2) \subseteq C(V_2)$ is the intersection of an open and a closed subset by Proposition 4.44. Hence, so is $H \subseteq C(V_2)$. Intersecting with A, also $H \subseteq A$ is the intersection of an open and a closed subset. Thus, restricting the morphism φ successively to these subsets results in a morphism $\varphi\big|_H\colon H \to \mathrm{Spin}(V_1)$. □

We now show that the graded algebra homomorphisms of Clifford algebras that are induced by isometries (see Proposition 3.12) preserve the corresponding spin groups:

Theorem 4.47. *Let V_1 and V_2 be finite-dimensional k-vector spaces and let $Q_1\colon V_1 \to k$ and $Q_2\colon V_2 \to k$ be quadratic forms with the property that the associated bilinear forms are nondegenerate. Suppose that $\sigma\colon V_1 \to V_2$ is an isometry between Q_1 and Q_2.*

Then σ extends to a homomorphism $C(\sigma)\colon C(V_1, Q_1) \to C(V_2, Q_2)$ of $\mathbb{Z}_2$-graded algebras that satsifies $C(\sigma)(\mathrm{Spin}(V_1)) \subseteq \mathrm{Spin}(V_2)$ and whose restriction to $C_0(V_1, Q_1)$ is injective. In particular, the map

$$e := C(\sigma)\big|_{\mathrm{Spin}(V_1)}\colon \mathrm{Spin}(V_1) \to \mathrm{Spin}(V_2)$$

is an embedding of algebraic groups, and we have a commutative diagram

$$\begin{tikzcd}
\mathrm{Spin}(V_1) \arrow[r, hook] \arrow[d, hook, "e"'] & C_0(V_1) \arrow[r, hook] \arrow[d, hook] & C(V_1) \arrow[d, "C(\sigma)"] \\
\mathrm{Spin}(V_2) \arrow[r, hook] & C_0(V_2) \arrow[r, hook] & C(V_2)
\end{tikzcd}$$

with middle map the restriction of $C(\sigma)$ to $C_0(V_1)$. If σ is bijective, then the three vertical maps are isomorphisms.

Proof. The claim on extension of σ has been proved in Proposition 3.12. To see that $C(\sigma)$ maps $\mathrm{Spin}(V_1)$ into $\mathrm{Spin}(V_2)$, it suffices to prove that it maps a generating system of $\mathrm{Spin}(V_1)$ into the group $\mathrm{Spin}(V_2)$. Since σ is an isometry, this is clearly satisfied for the generating system from Corollary 3.40.

Injectivity of the restriction to $C_0(V_1, Q_1)$ follows from the structure of the Clifford algebra. Depending on the parity of $\dim V_1$, either $C(V_1, Q_1)$ or $C_0(V_1, Q_1)$ is a simple algebra, as was shown in Section 3.2. Hence, by considering the kernel of the non-zero map $C(\sigma)$ respectively its restriction, it follows that either $C(\sigma)$ is injective already, or at least the restriction to $C_0(V_1, Q_1)$.

By what was shown above, it holds that e is an injective group homomorphism. In order to prove that it is a morphism of varieties, one proceeds exactly as in Lemma 4.45, with $\mathrm{End}(X)$ replaced by $C_0(V_2, Q_2)$. Now define $H := e(\mathrm{Spin}(V_1)) \leq \mathrm{Spin}(V_2)$, a closed subgroup by Proposition 4.8 (i). Put $A := C(\sigma)(C_0(V_1)) \leq C(V_2)$. Then this is a subalgebra with $H \subseteq A$. By injectivity, the map

$$\psi := C(\sigma)\big|_{C_0(V_1)} \colon C_0(V_1) \to A$$

is an isomorphism of k-algebras. Hence, so is its inverse $\varphi := \psi^{-1} \colon A \to C_0(V_1)$. Lemma 4.46 shows that the restriction $\varphi\big|_H \colon H \to \mathrm{Spin}(V_1)$ is a morphism of varieties. This proves that e is an embedding of algebraic groups.

Finally, if σ is bijective, then the respective restrictions of $C(\sigma^{-1})$ give the desired inverses of the vertical maps. ☐

Taking Theorem 4.33 into account, the above theorem in particular shows that the isomorphism type of the spin group does not depend on the chosen quadratic form, but only on $\dim V$. In accordance with Definition 4.34 we put $\mathrm{Spin}_n := \mathrm{Spin}(k^n, Q_n)$.

We next want to investigate the properties of the algebraic group $\mathrm{Spin}(V)$. Recall that the spin groups in dimensions 0 and 1 have been determined in Example 3.38. In both cases, $\mathrm{Spin}(V)$ is equal to the finite group $\{\pm 1\}$. Therefore, we assume that

$$n = \dim V \geq 2, \qquad \text{or equivalently,} \qquad m = m(Q) \geq 1$$

for the remainder of the chapter.

4.4.1 A Maximal Torus, Connectedness and Simplicity

From Proposition 4.44 and Theorem 3.39 we know that the twisted adjoint representation restricts to an isogeny $\rho \colon \mathrm{Spin}(V) \to \mathrm{SO}(V)$ with kernel $\ker\rho = \{\pm 1\}$. This closely relates the algebraic groups $\mathrm{Spin}(V)$ and $\mathrm{SO}(V)$. One may use this isogeny to derive properties of the spin group from those of $\mathrm{SO}(V)$. A different approach is to use the construction of $\mathrm{Spin}(V)$ and properties of Clifford algebras, see for instance Proposition 3.43. The next proposition is an example for the former method:

Proposition 4.48. *The spin group has dimension* $\dim \mathrm{Spin}(V) = \frac{n(n-1)}{2}$ *and rank* $\mathrm{rk}\,\mathrm{Spin}(V) = m$.

Proof. Since $\ker\rho$ is finite, we have $\dim \mathrm{Spin}(V) = \dim \mathrm{SO}(V)$ by Proposition 4.8 (iii). The fact $\dim \mathrm{SO}(V) = \frac{n(n-1)}{2}$ has been stated in Proposition 4.38.

Let $T \leq \mathrm{Spin}(V)$ be a maximal torus. Then by Proposition 4.20 (ii), its image $\rho(T) \leq \mathrm{SO}(V)$ is also a maximal torus. Since $\mathrm{rk}\,\mathrm{SO}(V) = m$ by Proposition 4.39, it follows that

$$m = \dim \rho(T) = \dim \rho(T) - \dim \ker \rho\big|_T = \dim T,$$

that is, $\mathrm{rk}\,\mathrm{Spin}(V) = m$. ☐

Thus, a maximal torus of $\mathrm{Spin}(V)$ has dimension m. We will now explicitly construct such a torus, closely following [GW09], Lemma 6.3.4 and Theorem 6.3.5. First, we need a lemma.

Lemma 4.49. *For $i \in \{1, \dots, m\}$, the map*

$$\gamma_i \colon \mathbf{G}_\mathrm{m} \to \mathrm{Spin}(V), \;\; c \mapsto cu_iw_i + c^{-1}w_iu_i,$$

is an injective morphism of algebraic groups. For all $i, j \in \{1, \dots, m\}$ and $c \in \mathbf{G}_\mathrm{m}$ the following relations hold inside the Clifford algebra:

$$\gamma_i(c)u_j\gamma_i(c^{-1}) = \begin{cases} c^2u_i, & i = j, \\ u_j, & i \neq j, \end{cases} \qquad \gamma_i(c)w_j\gamma_i(c^{-1}) = \begin{cases} c^{-2}w_i, & i = j, \\ w_j, & i \neq j, \end{cases}$$

and, if V is odd-dimensional, furthermore $\gamma_i(c)z\gamma_i(c^{-1}) = z$. In particular, if $i \neq j$, then $\gamma_i(c)\gamma_j(d) = \gamma_j(d)\gamma_i(c)$ for all $c, d \in \mathbf{G}_\mathrm{m}$.

Proof. For computations we will use the equations (C1) and (3.1), together with Theorem 2.19 (i). For example, one has $u_i^2 = 0$ by singularity, and $u_iw_iu_i = u_i(1-u_iw_i) = u_i$. Orthogonal elements may be swapped at the cost of a minus sign.

We show that γ_i is well-defined. For this, let $c \in \mathbf{G}_\mathrm{m}$. By Corollary 3.16 (ii) we have $\overline{\gamma_i(c)} = cw_iu_i + c^{-1}u_iw_i$. Hence, the relations mentioned above give

$$\gamma_i(c)\overline{\gamma_i(c)} = u_iw_iu_iw_i + w_iu_iw_iu_i = u_iw_i + w_iu_i = 1$$

and analogously $\overline{\gamma_i(c)}\gamma_i(c) = 1$ which shows that $\gamma_i(c)$ is invertible in C, with inverse $\overline{\gamma_i(c)} = \gamma_i(c^{-1})$. Furthermore, $N(\gamma_i(c)) = 1$. Next, we establish the three claimed relations. This amounts to a simple computation. For example, one has

$$\begin{aligned} \gamma_i(c)u_j\gamma_i(c^{-1}) &= (cu_iw_i + c^{-1}w_iu_i)u_j(c^{-1}u_iw_i + cw_iu_i) \\ &= \begin{cases} cu_iw_iu_icw_iu_i = c^2u_i, & i = j, \\ u_j\gamma_i(c)\gamma_i(c^{-1}) = u_j, & i \neq j. \end{cases} \end{aligned}$$

The other computations are analogous. Since the u_j and w_j and, if applicable, z form a basis of V, we infer from these relations that $\gamma_i(c) \in \Gamma$. The element further having norm 1 and being contained in C_0, it follows that $\gamma_i(c) \in \mathrm{Spin}(V)$, that is, γ_i is well-defined.

That γ_i is an injective group homomorphism is shown exactly as in the proof of Corollary 3.41. Finally, using the identifications $C^\times \cong \mathrm{GL}(\bigwedge W)$ respectively $C^\times \cong \mathrm{GL}(\bigwedge W) \times \mathrm{GL}(\bigwedge W)$ from Theorems 3.20 and 3.25, Lemma 3.19 (iii) shows that the coordinates of $cu_iw_i + c^{-1}w_iu_i$ are polynomial in c and c^{-1}. Thus, γ_i is a morphism of varieties. ☐

Theorem 4.50. *With notations as in Lemma 4.49, define*

$$\gamma\colon \mathbf{G}_{\mathrm{m}}^m \to \mathrm{Spin}(V),\ (c_1,\dots,c_m) \mapsto \gamma_1(c_1)\cdots\gamma_m(c_m).$$

Then the following hold:

(i) The map γ is a morphism of algebraic groups with finite kernel

$$\ker\gamma = \{\, (c_1,\dots,c_m) \in \mathbf{G}_{\mathrm{m}}^m \mid c_i = \pm 1 \text{ and } c_1\cdots c_m = 1 \,\}.$$

(ii) The image $T := \gamma(\mathbf{G}_{\mathrm{m}}^m)$ is a maximal torus of Spin(V).

(iii) Consider V to be equipped with basis the $(u_1,\dots,u_m,w_m,\dots,w_1)$ respectively $(u_1,\dots,u_m,z,w_m,\dots,w_1)$. Then with respect to this basis, we have

$$\rho(\gamma(c_1,\dots,c_m)) = \begin{cases} \mathrm{diag}(c_1^2,\dots,c_m^2,c_m^{-2},\dots,c_1^{-2}), & \dim V \text{ even},\\ \mathrm{diag}(c_1^2,\dots,c_m^2,1,c_m^{-2},\dots,c_1^{-2}), & \dim V \text{ odd}. \end{cases}$$

for all $c_1,\dots,c_m \in \mathbf{G}_{\mathrm{m}}$.

Proof.

(i) The first statement is immediate from Lemma 4.49. Turning to the kernel, let $(c_1,\dots,c_m) \in \ker\gamma$ and let $i \in \{1,\dots,m\}$. Using again Lemma 4.49 we have

$$u_i = \gamma_1(c_1)\cdots\gamma_m(c_m)u_i = c_i^2 u_i \gamma_1(c_1)\cdots\gamma_m(c_m) = c_i^2 u_i$$

in the Clifford algebra. The element u_i being linearly independent by Theorem 3.10 (ii), it follows that $c_i^2 = 1$, that is, $c_i = \pm 1$. Since $\gamma_i(-1) = -1$, we need to have $c_1\cdots c_m = 1$, as claimed. The other inclusion is clear.

(ii) By definition, $\mathbf{G}_{\mathrm{m}}^m \cong \mathrm{D}_m$ is a torus. Then also $T = \gamma(\mathbf{G}_{\mathrm{m}}^m)$ is a torus by Proposition 4.19 (ii). Since γ has finite kernel, Proposition 4.8 (iii) implies that $\dim T = m$. But Spin(V) has rank m by Proposition 4.48, so T needs to be maximal by Proposition 4.1.

(iii) The shape of $\rho(\gamma(c_1,\dots,c_m))$ is immediate from Lemma 4.49 and the definition of ρ. ☐

For a different model to view this maximal torus inside Spin(V), see [GW09], pages 307–309 and 319.

Example 4.51 (The spin group in dimension 2)**.** We consider the case $\dim V = 2$. Here, $m = 1$, and we write $u := u_1$ and $w := w_1$. Then by the above proposition, there is an injective morphism of algebraic groups

$$\gamma\colon \mathbf{G}_{\mathrm{m}} \to \mathrm{Spin}(V),\ c \mapsto cuw + c^{-1}wu.$$

We have $\dim \mathrm{Spin}(V) = 1$ by Proposition 4.48, so that γ is in this case in fact bijective by Propositions 4.1 and 4.8 (iii). Note that we had already established this fact in the proof of Corollary 3.41.

Furthermore, the map γ is even an isomorphism of algebraic groups in this case: Using the identifications of the proof of Proposition 4.44, the coordinates of the element $cuw + c^{-1}wu \in \mathrm{Spin}(V) \subseteq C^\times \cong \mathrm{GL}(\bigwedge W)$ with respect to the basis $(1, w)$ of $\bigwedge W$ are given by $\left(\begin{smallmatrix} c & \\ & c^{-1} \end{smallmatrix}\right)$, as one sees by a short calculation using Lemma 3.19 (iii). Thus, the inverse mapping $\left(\begin{smallmatrix} c & \\ & c^{-1} \end{smallmatrix}\right) \mapsto c$ is a morphism of varieties.

We are now ready to show that $\mathrm{Spin}(V)$ is connected, more precisely, that it is the connected component of the identity of the algebraic group $\mathrm{Pin}(V)$. We again follow [GW09], Theorem 6.3.5.

Corollary 4.52. *The spin group is connected and we have* $\mathrm{Spin}(V) = \mathrm{Pin}(V)^\circ$*.*

Proof. By Propositions 4.8 (ii) and 4.36 we have

$$\rho(\mathrm{Spin}(V)^\circ) = \rho(\mathrm{Spin}(V))^\circ = \mathrm{SO}(V)^\circ = \mathrm{SO}(V) = \rho(\mathrm{Spin}(V)).$$

Thus, if $x \in \mathrm{Spin}(V)$ is arbitrary, there exists some $y \in \mathrm{Spin}(V)^\circ$ with $\rho(x) = \rho(y)$. Then Theorem 3.39 implies that $x = \pm y$. Hence, in order to prove that $\mathrm{Spin}(V) = \mathrm{Spin}(V)^\circ$, it only remains to show that $-1 \in \mathrm{Spin}(V)^\circ$. Now with notation as in Theorem 4.50, we have $-1 = \gamma(-1, 1, \dots, 1) \in T$. But T is connected, so Corollary 4.6 (ii) gives $-1 \in \mathrm{Spin}(V)^\circ$.

Having established that the spin group is connected, Corollary 4.6 (ii) implies that $\mathrm{Spin}(V) = \mathrm{Spin}(V)^\circ \leq \mathrm{Pin}(V)^\circ$. On the other hand, $\mathrm{Spin}(V) \leq \mathrm{Pin}(V)$ is closed of finite index by Theorem 3.39, so we must have $\mathrm{Pin}(V)^\circ \leq \mathrm{Spin}(V)$ by Proposition 4.5 (iii). ☐

Now again we use properties of $\mathrm{SO}(V)$ to obtain a result for $\mathrm{Spin}(V)$, this time, that it is a (semi-)simple algebraic group:

Theorem 4.53 ((Semi-)Simplicity of $\mathrm{Spin}(V)$)**.** *For* $\dim V \geq 3$*, the spin group is semisimple. If* $\dim V = 3$ *or* $\dim V \geq 5$*, then* $\mathrm{Spin}(V)$ *is a simple algebraic group.*

Proof. By Corollary 4.52, the spin group is connected. Then the claim follows from Theorem 4.42 and Proposition 4.25, applied to the isogeny $\rho\colon \mathrm{Spin}(V) \to \mathrm{SO}(V)$. ☐

Recall that $\mathrm{Spin}_1 = \{\pm 1\}$ by Example 3.38 (b) and that $\mathrm{Spin}_2 \cong \mathbf{G}_\mathrm{m}$ by Example 4.51.

The case $\dim V = 4$ is similar as for the special orthogonal group: We will see later in Theorem 4.57 that the root system of Spin_4 is decomposable. Thus, by Proposition 4.28, the group Spin_4 is in fact not a simple algebraic group. This makes dimension 4 a somewhat special case, see for example also Proposition 5.9.

Corollary 4.54 (Commutator subgroup of $\mathrm{Spin}(V)$)**.** *For* $\dim V \geq 3$*, it holds that* $[\mathrm{Spin}(V), \mathrm{Spin}(V)] = \mathrm{Spin}(V)$*.*

Proof. This follows from Theorem 4.53 and [MT11], Theorem 8.21. $\square$

4.4.2 Root System and Root Subgroups

In the following, let $\dim V \geq 3$ and let $T = \gamma(\mathbf{G}_{\mathrm{m}}^m)$ be the maximal torus of $\mathrm{Spin}(V)$ from Theorem 4.50. We have seen that $\mathrm{Spin}(V)$ is a (semi-)simple algebraic group and will next determine the root system and the root subgroups of $\mathrm{Spin}(V)$ with respect to T.

Let $\mathcal{B}$ denote the basis $(u_1, \dots, u_m, w_m, \dots, w_1)$ resp. $(u_1, \dots, u_m, z, w_m, \dots, w_1)$ of V. By (1.1), this choice of basis gives an isomorphism from $\mathrm{O}(V)$ to the orthogonal group $\{\, A \in \mathrm{GL}_n \mid \tilde{Q}(Ax) = \tilde{Q}(x) \text{ for all } x \in k^n \,\}$ where

$$\tilde{Q} \colon k^n \to k,\ x \mapsto Q(c_{\mathcal{B}}^{-1}(x)).$$

Suppose that $n = 2m$ is even and let $x = (x_1, \dots, x_{2m}) \in k^n$. Then by Theorem 2.19 we have

$$\begin{aligned}
\tilde{Q}(x) &= Q(x_1 u_1 + \dots + x_m u_m + x_{m+1} w_m + \dots + x_{2m} w_1) \\
&= B\Big(\sum_{i=1}^m x_i u_i, \sum_{j=1}^m x_{m+j} w_{m+1-j}\Big) \\
&= \sum_{i=1}^m \sum_{j=1}^m x_i x_{m+j} B(u_i, w_{m+1-j}) \\
&= \sum_{i=1}^m x_i x_{2m+1-i}
\end{aligned}$$

which shows that $\tilde{Q} = Q_n$ is the quadratic form from Definition 4.34. With the same arguments, one shows that this also holds for odd n. Hence, the map $\sigma \mapsto [\sigma]_{\mathcal{B}}$ induces an isomorphism $\mathrm{O}(V) \to \mathrm{O}_n$, and then also an isomorphism $\mathrm{SO}(V) \to \mathrm{SO}_n$. In the sequel, we write T' for the maximal torus of $\mathrm{SO}(V)$ that corresponds to the respective torus from Proposition 4.39 under the above isomorphism. We denote the roots of $\mathrm{SO}(V)$ with respect to T' with the same symbols as those of SO_n.

Theorem 4.50 shows that we have $\rho(T) = T'$. For a character $\chi \in X(T')$ we define $\hat{\chi} := \chi \circ \rho \in X(T)$.

We need two computational lemmas.

Lemma 4.55. *Let* $u, v \in V$ *be two vectors with* $u \perp v$ *and where* u *is singular. For* $a \in k$ *put* $x_a := 1 + auv \in C$*. Then* $x_a \overline{x_a} = \overline{x_a} x_a = 1$ *and* $x_{a+b} = x_a x_b$ *for all* $a, b \in k$*.*

Proof. This is an easy computation. By orthogonality and (3.1) we have $uv+vu=0$. In addition, singularity gives $u^2=0$ and Corollary 3.16 yields $\overline{x_a}=1+avu$. It follows that

$$x_a\overline{x_a}=1+avu+auv+a^2uv^2u=1+a^2Q(v)u^2=1.$$

Similarly for $\overline{x_a}x_a$. Finally, for $a,b\in k$ we have

$$x_ax_b=1+auv+buv+ab(uv)^2=1+(a+b)uv-abvu^2v=x_{a+b},$$

as claimed. □

Lemma 4.56. *Let $a\in k$ and let $i,j\in\{1,\dots,m\}$ with $i\neq j$. Then the following hold:*

(i) Put $x:=1+au_iw_j\in C$. Then for $l\in\{1,\dots,m\}$ we have

$$xu_lx^{-1}=\begin{cases}u_l, & l\neq j,\\ u_j+au_i, & l=j,\end{cases}\qquad xw_lx^{-1}=\begin{cases}w_l, & l\neq i,\\ w_i-aw_j, & l=i,\end{cases}$$

and, if V is odd-dimensional, $xzx^{-1}=z$. Moreover, $x\in\operatorname{Spin}(V)$.

(ii) Put $x:=1+aw_iu_j\in C$. Then for $l\in\{1,\dots,m\}$ we have

$$xu_lx^{-1}=\begin{cases}u_l, & l\neq i,\\ u_i-au_j, & l=i,\end{cases}\qquad xw_lx^{-1}=\begin{cases}w_l, & l\neq j,\\ w_j+aw_i, & l=j,\end{cases}$$

and, if V is odd-dimensional, $xzx^{-1}=z$. Moreover, $x\in\operatorname{Spin}(V)$.

(iii) Put $x:=1+au_iu_j\in C$. Then for $l\in\{1,\dots,m\}$ we have

$$xu_lx^{-1}=u_l,\qquad xw_lx^{-1}=\begin{cases}w_l, & l\neq i,j,\\ w_i-au_j, & l=i,\\ w_j+au_i, & l=j,\end{cases}$$

and, if V is odd-dimensional, $xzx^{-1}=z$. Moreover, $x\in\operatorname{Spin}(V)$.

(iv) Put $x:=1+aw_iw_j\in C$. Then for $l\in\{1,\dots,m\}$ we have

$$xu_lx^{-1}=\begin{cases}u_l, & l\neq i,j,\\ u_i-aw_j, & l=i,\\ u_j+aw_i, & l=j,\end{cases}\qquad xw_lx^{-1}=w_l,$$

and, if V is odd-dimensional, $xzx^{-1}=z$. Moreover, $x\in\operatorname{Spin}(V)$.

(v) Suppose that $\dim V$ is odd and put $x:=1+au_iz\in C$. Then for $l\in\{1,\dots,m\}$ we have

$$xu_lx^{-1}=u_l,\qquad xw_lx^{-1}=\begin{cases}w_l, & l\neq i,\\ w_i-az-a^2u_i, & l=i,\end{cases}$$

and $xzx^{-1}=z+2au_i$. Moreover, $x\in\operatorname{Spin}(V)$.

(vi) *Suppose that* $\dim V$ *is odd and put* $x := 1 + aw_i z \in C$. *Then for* $l \in \{1, \dots, m\}$ *we have*

$$xu_l x^{-1} = \begin{cases} u_l, & l \neq i, \\ u_i - az - a^2 w_i, & l = i, \end{cases} \qquad xw_l x^{-1} = w_l,$$

and $xzx^{-1} = z + 2aw_i$. *Moreover,* $x \in \mathrm{Spin}(V)$.

Proof. We exemplarily give a proof for (i). The other parts are very similar. As in the proof of Lemma 4.49, we use the relations (C1), (3.1) and those of Theorem 2.19. By Lemma 4.55 we have $x^{-1} = \overline{x} = 1 + aw_j u_i$. By swapping orthogonal vectors, it clearly holds that $xu_l x^{-1} = u_l$ for $l \neq i, j$. With the equations mentioned above, we compute

$$xu_i x^{-1} = (1 + au_i w_j)u_i(1 + aw_j u_i) = u_i(1 + aw_j u_i) = u_i$$

and

$$\begin{aligned} xu_j x^{-1} &= (u_j + au_i(1 - u_j w_j))(1 + aw_j u_i) \\ &= u_j + au_j w_j u_i + au_i - au_i u_j w_j \\ &= u_j + au_i. \end{aligned}$$

The computations for w_l and z are analogous. Now the relations just established show that $x \in \Gamma_0$. Furthermore, we have $N(x) = 1$ by Lemma 4.55, giving $x \in \mathrm{Spin}(V)$. ☐

With these technical statements available, we can now determine root subgroups and root system of Spin(V). While the root systems are well-known (cf. [KMRT98], Theorems 25.10 and 25.12), there has not been an explicit description of the corresponding root subgroups. The description below and also parts of the proofs of Lemmas 4.55 and 4.56 have been inspired by the proof of Theorem 6.3.6 of [GW09].

Theorem 4.57. *Suppose that* $\dim V = 2m$ *is even. For* $i, j \in \{1, \dots, m\}$ *with* $i < j$ *define maps*

$$\begin{aligned} u_{\hat{\varepsilon_i} - \hat{\varepsilon_j}} &: \mathbf{G}_\mathrm{a} \to \mathrm{Spin}(V),\ a \mapsto 1 + au_i w_j, \\ u_{-\hat{\varepsilon_i} + \hat{\varepsilon_j}} &: \mathbf{G}_\mathrm{a} \to \mathrm{Spin}(V),\ a \mapsto 1 + aw_i u_j, \\ u_{\hat{\varepsilon_i} + \hat{\varepsilon_j}} &: \mathbf{G}_\mathrm{a} \to \mathrm{Spin}(V),\ a \mapsto 1 + au_i u_j, \\ u_{-\hat{\varepsilon_i} - \hat{\varepsilon_j}} &: \mathbf{G}_\mathrm{a} \to \mathrm{Spin}(V),\ a \mapsto 1 + aw_i w_j. \end{aligned}$$

These are morphisms of algebraic groups which are isomorphisms onto their respective image. Put

$$\hat{R} := \{\, \pm(\hat{\varepsilon_i} - \hat{\varepsilon_j}), \pm(\hat{\varepsilon_i} + \hat{\varepsilon_j}) \mid 1 \leq i < j \leq m \,\}.$$

Then for each $\hat{\alpha} \in \hat{R}$ *it holds that* $tu_{\hat{\alpha}}(a)t^{-1} = u_{\hat{\alpha}}(\hat{\alpha}(t)a)$ *for all* $t \in T$ *and* $a \in \mathbf{G}_\mathrm{a}$. *In particular,* $\hat{R} = R(\mathrm{Spin}(V))$ *is the root system of the spin group with respect to* T *and the groups* $U_{\hat{\alpha}} := \operatorname{im} u_{\hat{\alpha}}$, $\hat{\alpha} \in \hat{R}$, *are the root subgroups. Furthermore,* $\hat{R}$ *is of type* D_m.

Proof. We do the proof exemplarily for $\hat{\varepsilon_i} - \hat{\varepsilon_j} \in X(T)$. By Lemma 4.56, the image of $u_{\hat{\varepsilon_i}-\hat{\varepsilon_j}}$ is contained in $\mathrm{Spin}(V)$, and by Lemma 4.55, the map $u_{\hat{\varepsilon_i}-\hat{\varepsilon_j}}$ is a group homomorphism. Since 1 and u_iw_j are linearly independent in C by Theorem 3.10 (ii), it is injective. Using the coordinates as in the proof of Proposition 4.44, Lemma 3.19 (iii) shows that $u_{\hat{\varepsilon_i}-\hat{\varepsilon_j}}$ is a morphism of algebraic groups. From this we also see that the map $1 + au_iw_j \mapsto a$ is given by a polynomial in the coordinates, showing that $u_{\hat{\varepsilon_i}-\hat{\varepsilon_j}}$ is an isomorphism of algebraic groups onto its image.

Now let $t = \gamma(c_1, \ldots, c_m) \in T$, where $c_i \in \mathbf{G}_\mathrm{m}$, and let $a \in \mathbf{G}_\mathrm{a}$. Then, using Lemma 4.49, we have

$$\begin{aligned} tu_{\hat{\varepsilon_i}-\hat{\varepsilon_j}}(a)t^{-1} &= \gamma_1(c_1)\cdots\gamma_m(c_m)(1 + au_iw_j)\gamma_m(c_m^{-1})\cdots\gamma_1(c_1^{-1}) \\ &= 1 + ac_i^2u_i\gamma_1(c_1)\cdots\gamma_m(c_m)w_j\gamma_m(c_m^{-1})\cdots\gamma_1(c_1^{-1}) \\ &= 1 + ac_i^2c_j^{-2}u_iw_j \\ &= u_{\hat{\varepsilon_i}-\hat{\varepsilon_j}}(ac_i^2c_j^{-2}). \end{aligned}$$

But $(\hat{\varepsilon_i} - \hat{\varepsilon_j})(t) = c_i^2c_j^{-2}$ by Theorem 4.50 (iii), giving $tu_{\hat{\varepsilon_i}-\hat{\varepsilon_j}}(a)t^{-1} = u_{\hat{\varepsilon_i}-\hat{\varepsilon_j}}\big((\hat{\varepsilon_i} - \hat{\varepsilon_j})(t)a\big)$. Hence, we have $\hat{\varepsilon_i} - \hat{\varepsilon_j} \in R(\mathrm{Spin}(V))$. The computations for the other maps are analogous.

We have shown that $\hat{R} \subseteq R(\mathrm{Spin}(V))$. Proposition 4.48 and [MT11], Theorem 8.17 (b) imply that $|\hat{R}| = |R(\mathrm{Spin}(V))|$ which forces $\hat{R} = R(\mathrm{Spin}(V))$. Since the roots of $\mathrm{Spin}(V)$ are given by the same expressions as the ones of SO_{2m} (just with other symbols), it follows that $R(\mathrm{Spin}(V))$ is of type D_m. ☐

Theorem 4.58. *Suppose that* $\dim V = 2m + 1$ *is odd. For* $i, j \in \{1, \ldots, m\}$ *with* $i < j$ *define maps* $u_{\hat{\varepsilon_i}-\hat{\varepsilon_j}}$, $u_{-\hat{\varepsilon_i}+\hat{\varepsilon_j}}$, $u_{\hat{\varepsilon_i}+\hat{\varepsilon_j}}$ *and* $u_{-\hat{\varepsilon_i}-\hat{\varepsilon_j}}$ *as in Theorem 4.57 and for* $i \in \{1, \ldots, m\}$ *further define*

$$\begin{aligned} u_{\hat{\varepsilon_i}} &\colon \mathbf{G}_\mathrm{a} \to \mathrm{Spin}(V),\ a \mapsto 1 + au_iz, \\ u_{-\hat{\varepsilon_i}} &\colon \mathbf{G}_\mathrm{a} \to \mathrm{Spin}(V),\ a \mapsto 1 + aw_iz. \end{aligned}$$

These are morphisms of algebraic groups which are isomorphisms onto their respective image. Put

$$\hat{R} := \{\, \pm(\hat{\varepsilon_i} - \hat{\varepsilon_j}), \pm(\hat{\varepsilon_i} + \hat{\varepsilon_j}) \mid 1 \le i < j \le m \,\} \cup \{\, \pm\hat{\varepsilon_i} \mid 1 \le i \le m \,\}.$$

Then for each $\hat{\alpha} \in \hat{R}$ *it holds that* $tu_{\hat{\alpha}}(a)t^{-1} = u_{\hat{\alpha}}(\hat{\alpha}(t)a)$ *for all* $t \in T$ *and* $a \in \mathbf{G}_\mathrm{a}$. *In particular,* $\hat{R} = R(\mathrm{Spin}(V))$ *is the root system of the spin group with respect to* T *and the groups* $U_{\hat{\alpha}} := \operatorname{im} u_{\hat{\alpha}}$, $\hat{\alpha} \in \hat{R}$, *are the root subgroups. Furthermore,* $\hat{R}$ *is of type* B_m.

Proof. Proceed exactly as in Theorem 4.57. ☐

We make the following observation:

Proposition 4.59. *It holds that* $\rho(u_{\hat{\alpha}}(a)) = u_\alpha(a)$ *for all* $a \in \mathbf{G}_\mathrm{a}$ *and* $\alpha \in R(\mathrm{SO}(V))$.

Proof. This follows from Lemma 4.56 and the definition of ρ. For example, consider the root $\alpha := \varepsilon_i - \varepsilon_j$ of $\mathrm{SO}(V)$ where $\dim V$ is even. Lemma 4.56 (i) implies that $\rho(u_{\hat{\alpha}}(a))$ is given by the matrix $I_{2m} + a(E_{i,j} - E_{2m+1-j,2m+1-i})$ with respect to the basis $(u_1, \dots, u_m, w_m, \dots, w_1)$ of V. But this is precisely the matrix of $u_\alpha(a)$ with respect to the same basis by Theorem 4.40 (recall our convention on the roots of $\mathrm{SO}(V)$ in this subsection). Analogous for the other roots. □

Remark 4.60. Proposition 4.59 is a special case of a more general phenomenon described in 1.3.11 of [GM16]: Suppose that G and G' are connected reductive algebraic groups and that $\varphi\colon G \to G'$ is an isogeny. Let T be a maximal torus of G and let $T' := \varphi(T)$ be the corresponding maximal torus of G' (cf. Proposition 4.20). Let $(X(T), R, Y(T), R^\vee)$ and $(X(T'), R', Y(T'), R'^\vee)$ be the associated root data of G and G', respectively. Furthermore, let p be the characteristic exponent of $\operatorname{char} k$, i.e., $p = 1$ if $\operatorname{char} k = 0$ and $p = \operatorname{char} k$ otherwise.

Then for every root $\alpha \in R$, the group $\varphi(U_\alpha)$ is a root subgroup of G'. More precisely, there is a unique $\alpha' \in R'$ with $\varphi(U_\alpha) = U_{\alpha'}$ and if $u_\alpha\colon \mathbf{G}_{\mathrm{a}} \to U_\alpha$ and $u_{\alpha'}\colon \mathbf{G}_{\mathrm{a}} \to U_{\alpha'}$ are the corresponding isomorphisms, then there are $c_\alpha \in k^\times$ and positive integers q_α, which are integral powers of p, such that

$$\varphi(u_\alpha(a)) = u_{\alpha'}(c_\alpha a^{q_\alpha}) \qquad \text{for all } a \in \mathbf{G}_{\mathrm{a}}.$$

Even more, the group homomorphism $f\colon X(T') \to X(T), \chi' \mapsto \chi' \circ \varphi\big|_T$ induced by φ is a so-called p-isogeny of the root data of G and G' (see [GM16], 1.3.11 and 1.2.9).

For the isogeny $\rho\colon \mathrm{Spin}(V) \to \mathrm{SO}(V)$ and the maximal torus of $\mathrm{Spin}(V)$ from Theorem 4.50, we have seen that for all $\alpha \in R(\mathrm{SO}(V))$ we have $(\hat{\alpha})' = \alpha$, $c_{\hat{\alpha}} = 1$ and $q_{\hat{\alpha}} = 1$.

Proposition 4.61. *The spin group* $\mathrm{Spin}(V)$ *is simply connected.*

Proof. We only give a proof for the case $\operatorname{char} k \neq 2$. Let $R := R(\mathrm{Spin}(V), T)$. By Theorems 4.57 and 4.58 and Table 9.2 in [MT11], we have $\operatorname{char} k \nmid |\Lambda(R)|$. Hence, the proof of [MT11], Proposition 9.15 shows that $X(T)/\mathbb{Z}R \cong Z(\mathrm{Spin}(V))$. In view of Proposition 3.43, this means that

$$|X(T)/\mathbb{Z}R| = \begin{cases} 4, & \dim V \text{ even}, \\ 2, & \dim V \text{ odd}. \end{cases}$$

But this is also the cardinality of the fundamental group of R in the respective cases by Table 9.2 of [MT11] which forces $X(T)/\mathbb{Z}R = \Lambda(R)$. Thus, $\mathrm{Spin}(V)$ is simply connected. For the general statement, we refer to [KMRT98], Theorems 25.10 and 25.12. □

In low dimensions, there are some exceptional cases in which different types of root systems coincide. This phenomenon is reflected in the following isomorphisms of algebraic groups:

Corollary 4.62 (Exceptional isomorphisms)**.** *There are isomorphisms of algebraic groups*

$$\mathrm{Spin}_2 \cong \mathbf{G}_{\mathrm{m}}, \quad \mathrm{Spin}_3 \cong \mathrm{SL}_2, \quad \mathrm{Spin}_4 \cong \mathrm{SL}_2 \times \mathrm{SL}_2, \quad \mathrm{Spin}_5 \cong \mathrm{Sp}_4, \quad \mathrm{Spin}_6 \cong \mathrm{SL}_4\,.$$

Proof. For the first isomorphism, see Example 4.51. The remaining ones follow from the Classification Theorem 4.29 and the discussion subsequent to it as we now explain. By Example 4.31, SL_2 is a simply connected simple algebraic group of type A_1. Since the root systems A_1 and B_1 are isomorphic, Theorem 4.29 together with Theorem 4.58 and Proposition 4.61 implies that we must have $\mathrm{Spin}_3 \cong \mathrm{SL}_2$.

The analogous arguments apply to the remaining isomorphisms, each time using the respective isomorphisms of root systems. For the isomorphism of Spin_5 use Remark 4.43 and for the isomorphism of Spin_4 note that by [GLS97], Proposition 1.10.6, the group $\mathrm{SL}_2 \times \mathrm{SL}_2$ is simply connected with root system $A_1 \times A_1 \cong D_2$. ☐

In higher dimensions, no comparable isomorphisms exist by the structure of the root systems and the classification theorem.

5 Spin Representations

Throughout this chapter, k is algebraically closed. Let V be a finite-dimensional vector space over k of dimension $n := \dim V > 0$ and let Q be a quadratic form on V with associated symmetric bilinear form B. We again assume that B is nondegenerate.

In this chapter, we deal with the spin and half-spin representations. Their construction and a first investigation of their properties are carried out in Section 5.1. We proceed with an interludial section on nested spin groups whose results will become significant in the remainder of the chapter as well as later in Section 6.3. Returning to the study of spin representations, Section 5.3 is devoted to describing certain restrictions of these represtentations in terms of lower-dimensional spin and half-spin representations and contains results that will play a key role in our main algorithm in Section 7.1.

5.1 The Spin and Half-Spin Representations

In this section, we introduce the spin and half-spin representations which are some of the main objects of our study. We examine a couple of basic properties of these representations and explicitly compute them in low dimensions.

We make use of the results from Section 3.2 on the structure of the Clifford algebra and follow the approach of [Che97], Sections 2.4 and 2.5, and [Mei13], Section 3.7.5. These references cover the basic material, but do not contain Propositions 5.7 and 5.13 and neither of the explicit computations made in the examples from this section.

Denote by C the Clifford algebra for (V, Q). Let $m := m(Q) = \lfloor \frac{n}{2} \rfloor$ be the Witt index of Q. We fix a Lagrangian decomposition $V = U \oplus W$ respectively $V = (U \oplus W) \perp \operatorname{span}(z)$ with respect to bases $(u_1, \ldots, u_m)$ of U and $(w_1, \ldots, w_m)$ of W.

5.1.1 Construction and First Properties

We start by constructing the spin and half-spin representations which are certain (irreducible) rational representations of the spin groups. For this, we use the method from [Che97], Sections 2.4 and 2.5, and [Mei13], Section 3.7.5.

We remark that the terms irreducible and faithful and the notions of dimension and equivalence are defined for representations of groups in the analogous way as for representations of algebras (cf. Section 1.2). If $\theta_1 \colon G \to \mathrm{GL}(X_1)$ and $\theta_2 \colon G \to \mathrm{GL}(X_2)$

are representations of a group G on finite-dimensional k-vector spaces, then also the map

$$\theta_1 \oplus \theta_2 \colon G \to \mathrm{GL}(X_1 \oplus X_2),\ g \mapsto \theta_1(g) \oplus \theta_2(g)$$

is a representation of G.

We already know some (rational) representations of the spin groups: If $\theta\colon\ \mathrm{SO}(V) \to \mathrm{GL}(X)$ is any representaion of the special orthogonal group on a (finite-dimensional) k-vector space X, then it inflates to a representation

$$\theta \circ \rho\colon\ \mathrm{Spin}(V) \to \mathrm{GL}(X)$$

of $\mathrm{Spin}(V)$ on the same space, where as usual $\rho\colon\ \mathrm{Spin}(V) \to \mathrm{SO}(V)$ denotes the twisted adjoint representation. Note that for representations of the spin group obtained this way, we always have $-1 \in \ker(\theta \circ \rho)$, i.e., these representations are never faithful if $\operatorname{char} k \neq 2$. For example, the twisted adjoint representation itself is a representation $\rho\colon\ \mathrm{Spin}(V) \to \mathrm{SO}(V) \subseteq \mathrm{GL}(V)$ of dimension $\dim V$, with kernel $\{\pm 1\}$.

A different way to obtain representations of $\mathrm{Spin}(V)$ is to restrict representations of the Clifford algebra C respectively its even subalgebra C_0, which contain the spin group as a subgroup of the units. The following proposition describes the behaviour of such restrictions:

Proposition 5.1. *The restriction of a faithful resp. irreducible representation of* C_0 *to* $\mathrm{Spin}(V)$ *is a rational faithful resp. irreducible representation of* $\mathrm{Spin}(V)$*. Two such restrictions are equivalent if and only if the corresponding representations of* C_0 *are.*

Proof. Restrictions of representations of C_0 are rational representations of $\mathrm{Spin}(V)$ by Lemma 4.45. That such restrictions remain faithful is clear. The claims on being irreducible and being equivalent follow directly from the fact that $\mathrm{Spin}(V)$ generates C_0 as an algebra, as was shown in Lemma 3.42. ☐

For example, consider the regular representation $C_0 \to \mathrm{End}(C_0)$ by left multiplication, which is faithful. By the above proposition, we obtain a faithful representation $\mathrm{Spin}(V) \to \mathrm{GL}(C_0)$ of the spin group, of dimension $\dim C_0 = 2^{n-1}$. However, there are faithful (and irreducible) representations of $\mathrm{Spin}(V)$ of smaller dimension that we will now construct. For this, we first recall what we know about the representations of the Clifford algebra and its even subalgebra.

Remark 5.2 (Irreducible representations of C and C_0)**.** We recapitulate the results from Section 3.2 and put them in the context of representations.

(a) Suppose that $\dim V$ is even. By Theorem 3.20, the Clifford algebra C is a central simple k-algebra. More precisely, there is an isomorphism

$$\Phi_{U,W} \colon C \to \mathrm{End}(\textstyle\bigwedge W),\ U \oplus W \ni u + w \mapsto \iota_u + \lambda_w,$$

of $\mathbb{Z}_2$-graded k-algebras where ι_u and λ_w are as in Lemma 3.19. By Example 1.8 (a) and Theorem 1.13, $\Phi_{U,W}$ is the unique irreducible representation of C up to equivalence, and it is clearly faithful. Restricting it gives rise to (ungraded) isomorphisms

$$C_0 \xrightarrow{\sim} \mathrm{End}(\textstyle\bigwedge W)_0 \cong \mathrm{End}\big((\textstyle\bigwedge W)_0\big) \oplus \mathrm{End}\big((\textstyle\bigwedge W)_1\big)$$

of k-algebras where the second isomorphism is given by restriction to $(\bigwedge W)_0$ respectively $(\bigwedge W)_1$, see Theorem 3.22 and Lemma 1.28 (ii). Thus, C_0 is the direct sum of two isomorphic ideals that are themselves central simple k-algebras, and $Z(C_0) \cong k \oplus k$. By Example 1.8 (b) and Theorem 1.13, the algebra C_0 is a semisimple k-algebra that has two irreducible representations (up to equivalence), which are given by concatenation of the above isomorphism with the projections $\mathrm{End}\big((\bigwedge W)_0\big) \oplus \mathrm{End}\big((\bigwedge W)_1\big) \to \mathrm{End}\big((\bigwedge W)_i\big)$ for $i = 0, 1$. In other words, the simple C-module $\bigwedge W$ splits into a direct sum of the two inequivalent simple C_0-modules: $\bigwedge W = (\bigwedge W)_0 \oplus (\bigwedge W)_1$.

(b) Suppose that $\dim V$ is odd. Here, the situation is complementary. There is an (ungraded) algebra isomorphism $\Phi_{U,W} \colon C \to \mathrm{End}(\bigwedge W) \oplus \mathrm{End}(\bigwedge W)$ by Theorem 3.26, so that the Clifford algebra is semisimple and has two irreducible representations. Taking $v = z$ and $Y = U \oplus W$ in the proof of Theorem 3.24, we see that the even subalgebra C_0 is a central simple k-algebra, isomorphic to $C(U \oplus W, -Q\big|_{U \oplus W})$. Concatenation of $\Phi_{U,W}$ with a projection gives a representation

$$\Phi_{U,W,z} \colon C \to \mathrm{End}(\textstyle\bigwedge W), \; (U \oplus W) \perp \mathrm{span}(z) \ni u + w + az \mapsto \iota_u + \lambda_w + \eta_a,$$

of dimension $\dim \bigwedge W$. By part (a), this is also the dimension of the unique irreducible representation of C_0 (up to equivalence). Hence, by Proposition 1.12 (i), the restriction $\Phi_{U,W,z}\big|_{C_0}$ must be an irreducible representation of C_0, its only one up to equivalence. It is faithful as C_0 is simple.

Knowing all irreducible representations of C and C_0, we now give them a name. They give rise to the representations of $\mathrm{Spin}(V)$ that we are interested in.

Definition 5.3. Suppose that $n = \dim V$ is even.

(a) The irreducible representation $\Phi_{U,W}$ of C is called the *spin representation* of C. Its restriction to C_0 respectively $\mathrm{Spin}(V)$ is likewise called the *spin representation* of C_0 respectively $\mathrm{Spin}(V)$. The spin representation of $\mathrm{Spin}(V)$ will be denoted by Δ_n.

(b) The two irreducible representations of C_0 on $(\bigwedge W)_0$ and $(\bigwedge W)_1$ from Remark 5.2 (a) are called the *half-spin representations* of C_0. Their restrictions to $\mathrm{Spin}(V)$ are likewise called the *half-spin representations* of $\mathrm{Spin}(V)$. We denote by Δ_n^+ the representation of $\mathrm{Spin}(V)$ on $(\bigwedge W)_0$ and by Δ_n^- the representation of $\mathrm{Spin}(V)$ on $(\bigwedge W)_1$.

Definition 5.4. Suppose that $n = \dim V$ is odd. The irreducible representation $\Phi_{U,W,z}\big|_{C_0}$ of C_0 is called the *spin representation* of C_0. Its restriction to $\mathrm{Spin}(V)$ is likewise called the *spin representation* of $\mathrm{Spin}(V)$ and will be denoted by Δ_n.

Remark 5.5. We have chosen specific maps to define the spin and half-spin representations. This approach is convenient for us because we will use these maps for our computations and frequently also in proofs. Since by Remark 5.2, there is only one equivalence class of irreducible representations of C if $\dim V$ is even, respectively of C_0 if $\dim V$ is odd, the properties of the spin representation that are invariant under equivalence do not depend on the choice of map we made (and in particular not on the choice of Lagrangian decomposition either). This carries over to the corresponding representations of the spin groups by Proposition 5.1. The same holds for the half-spin representations since in even dimension, the algebra C_0 only has two equivalence classes of irreducible representations.

Thus, our approach is justified by the fact that we are only interested in properties of these representations that solely depend on their equivalence class, like dimension, irreducibility, kernel, surjectivity and most importantly conjugacy classes of elements under the representation. This also explains the notation for the spin and half-spin representations of the spin group that does not refer to any choices. It is taken from [Mei13] and [LM89].

We now study the properties of the spin and half-spin representations. We start with even dimension.

Proposition 5.6. *Suppose that* $n = \dim V$ *is even.*

(i) The spin representation Δ_n *is a faithful rational representation of* $\operatorname{Spin}(V)$ *of dimension* $2^m = 2^{\frac{n}{2}}$.

(ii) The half-spin representations Δ_n^+ *and* Δ_n^- *are inequivalent irreducible rational representations of* $\operatorname{Spin}(V)$ *of dimension* $2^{m-1} = 2^{\frac{n}{2}-1}$.

Moreover, we have $\Delta_n = \Delta_n^+ \oplus \Delta_n^-$.

Proof. This is immediate from Remark 5.2 and Proposition 5.1. For the dimension use Proposition 1.36 (iv). ☐

As the half-spin representations are irreducible and build up the spin representation, we are mostly interested in the half-spin representations rather than the spin representation in even dimension. We next relate the two representations Δ_n^+ and Δ_n^-.

Recall from Theorem 3.39 that the spin group is a normal subgroup of the pin group. Hence, conjugation by an element of $\operatorname{Pin}(V)$ defines an automorphism of $\operatorname{Spin}(V)$. This automorphism transforms the half-spin representations into each other, as follows:

Proposition 5.7. *Suppose that* $n = \dim V$ *is even. Let* $p \in \operatorname{Pin}(V) \setminus \operatorname{Spin}(V)$ *and define* $\varphi_p : \operatorname{Spin}(V) \to \operatorname{Spin}(V)$, $x \mapsto p^{-1}xp$. *Then we have* $\Delta_n^+ \circ \varphi_p \cong \Delta_n^-$ *and* $\Delta_n^- \circ \varphi_{p^{-1}} \cong \Delta_n^+$.

Proof. By Proposition 3.35 we have $p \in C_1$. Now the map $\Phi_{U,W} \colon C \to \mathrm{End}(\bigwedge W)$ is a $\mathbb{Z}_2$-graded algebra isomorphism, so it holds that $\Phi_{U,W}(p) \in \mathrm{End}(\bigwedge W)_1$. Then, as p is invertible, the restriction $\Phi_{U,W}(p)\big|_{(\bigwedge W)_0} \colon (\bigwedge W)_0 \to (\bigwedge W)_1$ is an isomorphism of k-vector spaces (see also Lemma 1.28). Let $x \in \mathrm{Spin}(V)$. By definition of the half-spin representations and since $\Phi_{U,W}$ is an algebra homomorphism, there is a commutative diagram

$$\begin{tikzcd}
(\bigwedge W)_0 \arrow[r, "\Delta_n^+(p^{-1}xp)"] \arrow[d, "\Phi_{U,W}(p)\big|_{(\bigwedge W)_0}"'] & (\bigwedge W)_0 \arrow[d, "\Phi_{U,W}(p)\big|_{(\bigwedge W)_0}"] \\
(\bigwedge W)_1 \arrow[r, "\Delta_n^-(x)"'] & (\bigwedge W)_1
\end{tikzcd}$$

which shows that the representations $\Delta_n^+ \circ \varphi_p$ and Δ_n^- of $\mathrm{Spin}(V)$ are equivalent. The proof for $\Delta_n^- \circ \varphi_{p^{-1}}$ and Δ_n^+ is analogous. ☐

Recall from Corollary 3.40 that the spin group is generated by the products uv where $u, v \in V$ with $Q(u) = Q(v) = -1$. We will frequently use this generating system to describe the spin representations concretely.

Example 5.8 (Spin and half-spin representations in dimension 2)**.** We consider the case $\dim V = 2$ and give explicit descriptions of the spin and half-spin representations. Write $u := u_1$ and $w := w_1$. We have $V = U \oplus W$ with $U = \mathrm{span}(u)$ and $W = \mathrm{span}(w)$.

As seen in the proof of Corollary 3.41, the spin group is generated by the elements $tuw + t^{-1}wu$ for $t \in k^\times$. In order to describe the spin and half-spin representations, we compute how u and w act on $\bigwedge W$. By definition, they act by the endomorphisms ι_u and λ_w whose matrices with respect to the basis $(1, w)$ of $\bigwedge W$ from Proposition 1.36 (iv) may be computed with Lemma 3.19 (iii). We obtain that the endomorphism ι_u acts by $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ and the endomorphism λ_w acts by $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$. By suitably multiplying these matrices, we see that the spin representation is given by

$$\Delta_2 \colon \mathrm{Spin}(V) \to \mathrm{GL}(\textstyle\bigwedge W),\ tuw + t^{-1}wu \mapsto \begin{pmatrix} t & \\ & t^{-1} \end{pmatrix}$$

with respect to the basis from above. It follows that the half-spin representations are given by

$$\begin{aligned}
\Delta_2^+ &\colon \mathrm{Spin}(V) \to \mathrm{GL}((\textstyle\bigwedge W)_0) = \mathbf{G}_{\mathrm{m}},\ tuw + t^{-1}wu \mapsto t, \\
\Delta_2^- &\colon \mathrm{Spin}(V) \to \mathrm{GL}((\textstyle\bigwedge W)_1) = \mathbf{G}_{\mathrm{m}},\ tuw + t^{-1}wu \mapsto t^{-1}.
\end{aligned}$$

Note that Δ_2^+ is precisely the inverse of the morphism $\gamma \colon \mathbf{G}_{\mathrm{m}} \to \mathrm{Spin}(V)$ from Example 4.51 (which again shows that γ is an isomorphism of algebraic groups as Δ_2^+ is a morphism of varieties by Proposition 5.6). Thus, Δ_2^+ and Δ_2^- are isomorphisms of algebraic groups, taking into account that $\mathrm{Spin}(V)$ is abelian by Example 3.38 (c).

Suppose again that $\dim V$ is even. By definition, the spin representation of C_0 is clearly faithful, whereas the two half-spin representations are not; in fact, they have large kernels, see Remark 5.2. As shown in Proposition 5.6 (i), also the spin representation of $\mathrm{Spin}(V)$ is faithful. Regarding the half-spin representations, the situation is much better than for C_0. In the above example, we have in particular already seen that the half-spin representations are faithful in dimension 2.

In the following proposition, we determine the kernels of the half-spin representations for all dimensions except 4. It is comparable to [Che97], III.6.1 and to Lemma 6.8.6 of [Var04]. For the proof, we use similar methods as in the latter reference, but adapted to the context of algebraic groups. It turns out that in general, the half-spin representations are either faithful or at least nearly faithful, depending on the residue of n modulo 4.

Proposition 5.9. *Suppose that $n = \dim V \neq 4$ is even.*

(i) Assume that $\operatorname{char} k = 2$. Then the half-spin representations are faithful.

(ii) Assume that $\operatorname{char} k \neq 2$ and let $(e_1, \ldots, e_n)$ be an orthogonal basis of V with $Q(e_i) = -1$. Put $\zeta := e_1 \cdots e_n$. There are two cases:

- *(1) If $n \equiv 2 \pmod 4$, then the half-spin representations are faithful.*
- *(2) If $n \equiv 0 \pmod 4$, then both half-spin representations have kernels of order 2. More precisely, the kernel of Δ_n^+ is either $\{1, \zeta\}$ or $\{1, -\zeta\}$ and the one of Δ_n^- accordingly is given by $\{1, -\zeta\}$ or $\{1, \zeta\}$.*

Proof. For $n = 2$, the claims hold by Example 5.8. We may thus assume that $n \geq 6$ from now on. Assume that $\ker \Delta_n^+ = \mathrm{Spin}(V)$. Then it follows from Proposition 5.7 that also $\ker \Delta_n^- = \mathrm{Spin}(V)$, that is, the representations Δ_n^+ and Δ_n^- are trivial. But then by Proposition 5.6, also the spin representation $\Delta_n = \Delta_n^+ \oplus \Delta_n^-$ is trivial which contradicts the fact that it is faithful. Hence, we must have $\ker \Delta_n^+ < \mathrm{Spin}(V)$ and $\ker \Delta_n^- < \mathrm{Spin}(V)$.

By the above, the subgroups $(\ker \Delta_n^\pm)^\circ \trianglelefteq \mathrm{Spin}(V)$ are proper, closed, connected and normal. Since for $n = \dim V \geq 6$, the spin group is a simple algebraic group by Theorem 4.53, we infer that $(\ker \Delta_n^\pm)^\circ = 1$, that is, $\ker \Delta_n^\pm$ is finite. Then Corollary 4.52 and [MT11], Exercise 10.4 imply that $\ker \Delta_n^\pm \subseteq Z(\mathrm{Spin}(V))$. Thus, we can now make use of Proposition 3.43 (ii).

If $\operatorname{char} k = 2$, then $Z(\mathrm{Spin}(V)) = 1$, and the claim follows immediately. Suppose now that $\operatorname{char} k \neq 2$. Then we have $Z(\mathrm{Spin}(V)) = \{\pm 1, \pm \zeta\}$. Since Δ_n^+ and Δ_n^- stem from algebra homomorphisms, we have $\Delta_n^\pm(-1) = -1$ and therefore $-1 \notin \ker \Delta_n^\pm$. Let

$$\Phi \colon C_0 \xrightarrow{\sim} \mathrm{End}\big((\textstyle\bigwedge W)_0\big) \oplus \mathrm{End}\big((\textstyle\bigwedge W)_1\big)$$

be the k-algebra isomorphism from Theorem 3.22 that via the projections gives rise to the half-spin representations. Being an isomorphism, Φ satisfies

$$\Phi(Z(C_0)) = Z\big(\mathrm{End}\big((\textstyle\bigwedge W)_0\big) \oplus \mathrm{End}\big((\textstyle\bigwedge W)_1\big)\big) = k \oplus k,$$

so that $\Phi(\pm\zeta) \in k \oplus k$. We distinguish the two cases. If $n \equiv 2 \pmod 4$, then it holds that $(\pm\zeta)^2 = -1$ by Lemma 3.18 (iii). Thus, we have $\Phi(\pm\zeta) \in k \oplus k$ with $\Phi(\pm\zeta)^2 = \Phi(-1) = (-1,-1)$. This means that neither component of $\Phi(\pm\zeta)$ can be 1, that is to say, $\pm\zeta \notin \ker \Delta_n^{\pm}$. It follows that Δ_n^+ and Δ_n^- are faithful.

If on the other hand we have $n \equiv 0 \pmod 4$, then Lemma 3.18 (iii) gives $(\pm\zeta)^2 = 1$. Hence, $\Phi(\pm\zeta)$ is one of the four elements of $k \oplus k$ whose square is $(1,1)$. However, it can neither be $(1,1)$ nor $(-1,-1)$ since Φ is bijective. As a consequence, it holds that $\{\Phi(\zeta), \Phi(-\zeta)\} = \{(1,-1),(-1,1)\}$, from which the claim follows. ☐

In order to be able to exploit the simplicity of the spin group, we had to exclude the case $\dim V = 4$. In fact, in that case, the half-spin representations are far from being faithful: If $\dim V = 4$, then $\dim \mathrm{Spin}(V) = 6$ by Proposition 4.48, whereas $\dim \mathrm{GL}\big((\bigwedge W)_0\big) = \dim \mathrm{GL}\big((\bigwedge W)_1\big) = 4$ by Example 4.3 (c) and Proposition 1.36 (iv). Hence, the kernels of the half-spin representations have dimension at least 2 by Proposition 4.8 (iii). To see even more, we explicitly describe Δ_4^+ and Δ_4^-:

Example 5.10 (Spin and half-spin representations in dimension 4)**.** Let us suppose that $\dim V = 4$. As in Example 5.8, we would like to give the spin and half-spin representations on a generating system of $\mathrm{Spin}(V)$. For a tuple of scalars $\underline{a} = (a_1, \ldots, a_4) \in k^4$ let $v_{\underline{a}} := a_1u_1 + a_2u_2 + a_3w_2 + a_4w_1 \in V$. We have $Q(v_{\underline{a}}) = a_1a_4 + a_2a_3$, as remarked after Corollary 4.54. Thus, by Corollary 3.40, the spin group is generated by the elements $x_{\underline{a},\underline{b}} := v_{\underline{a}}v_{\underline{b}}$ for $\underline{a}, \underline{b} \in k^4$ with $-1 = a_1a_4 + a_2a_3 = b_1b_4 + b_2b_3$, where an explicit calculation with (Q1) and (3.1) shows that

$$\begin{aligned} x_{\underline{a},\underline{b}} = {} & (a_1b_2 - a_2b_1)u_1u_2 + (a_1b_4 - b_4b_1)u_1w_1 + (a_1b_3 - a_3b_1)u_1w_2 \\ & + (a_2b_4 - a_4b_2)u_2w_1 + (a_2b_3 - a_3b_2)u_2w_2 \\ & + (a_4b_3 - a_3b_4)w_1w_2 + (a_4b_1 + a_3b_2). \end{aligned}$$

Now by Proposition 1.36 (iv), the vector space $\bigwedge W$ is 4-dimensional, and has basis $(1, w_1 \wedge w_2, w_1, w_2)$. We have ordered the basis in this way because $(1, w_1 \wedge w_2)$ is a basis of the $\mathrm{Spin}(V)$-invariant subspace $(\bigwedge W)_0$, and (w_1, w_2) is a basis of the $\mathrm{Spin}(V)$-invariant subspace $(\bigwedge W)_1$. This makes it easier to read off the half-spin representations later.

To desribe the spin representation, we compute the matrices of $\iota_{u_1}, \iota_{u_2}, \lambda_{w_1}$ and λ_{w_2} w.r.t. the above basis. One calculates with the aid of Lemma 3.19 (iii) that

$$\iota_{u_1} \text{ acts by } \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \qquad \iota_{u_2} \text{ acts by } \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\lambda_{w_1} \text{ acts by } \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \qquad \lambda_{w_2} \text{ acts by } \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Using the description of $x_{\underline{a},\underline{b}}$ from above, another computation shows that the spin representation is given by $\Delta_4\colon \operatorname{Spin}(V) \to \operatorname{GL}(\bigwedge W)$ where

$$x_{\underline{a},\underline{b}} \mapsto \begin{pmatrix} a_1b_4+a_2b_3 & a_2b_1-a_1b_2 & & \\ a_4b_3-a_3b_4 & a_4b_1+a_3b_2 & & \\ & & a_2b_3+a_4b_1 & a_4b_2-a_2b_4 \\ & & a_3b_1-a_1b_3 & a_1b_4+a_3b_2 \end{pmatrix}.$$

We make the observation that

$$\Delta_4(x_{\underline{a},\underline{b}}) = \begin{pmatrix} a_1 & a_2 & & \\ -a_3 & a_4 & & \\ & & a_2 & a_4 \\ & & -a_1 & a_3 \end{pmatrix} \begin{pmatrix} b_4 & -b_2 & & \\ b_3 & b_1 & & \\ & & b_3 & -b_4 \\ & & b_1 & b_2 \end{pmatrix}.$$

Hence, the relations $-1 = a_1a_4+a_2a_3$ and $-1 = b_1b_4+b_2b_3$ show that the image of the spin representation Δ_4 is contained in $\operatorname{SL}(\bigwedge W)$. The analogous statement holds for the half-spin representations which are given by $\Delta_4^+\colon \operatorname{Spin}(V) \to \operatorname{SL}\big((\bigwedge W)_0\big)$ where

$$x_{\underline{a},\underline{b}} \mapsto \begin{pmatrix} a_1b_4+a_2b_3 & a_2b_1-a_1b_2 \\ a_4b_3-a_3b_4 & a_4b_1+a_3b_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ -a_3 & a_4 \end{pmatrix} \begin{pmatrix} b_4 & -b_2 \\ b_3 & b_1 \end{pmatrix},$$

and $\Delta_4^-\colon \operatorname{Spin}(V) \to \operatorname{SL}\big((\bigwedge W)_1\big)$ where

$$x_{\underline{a},\underline{b}} \mapsto \begin{pmatrix} a_2b_3+a_4b_1 & a_4b_2-a_2b_4 \\ a_3b_1-a_1b_3 & a_1b_4+a_3b_2 \end{pmatrix} = \begin{pmatrix} a_2 & a_4 \\ -a_1 & a_3 \end{pmatrix} \begin{pmatrix} b_3 & -b_4 \\ b_1 & b_2 \end{pmatrix}.$$

We now strengthen the statement made before this example. The morphism of algebraic groups

$$(\Delta_4^+, \Delta_4^-)\colon \operatorname{Spin}(V) \to \operatorname{SL}\big((\textstyle\bigwedge W)_0\big) \times \operatorname{SL}\big((\textstyle\bigwedge W)_1\big),\ x \mapsto (\Delta_4^+(x), \Delta_4^-(x))$$

is injective since by Proposition 5.6, the spin representation $\Delta_4 = \Delta_4^+ \oplus \Delta_4^-$ is faithful. But $\dim \operatorname{Spin}(V) = 6$ by Proposition 4.48 and $\dim \operatorname{SL}\big((\bigwedge W)_0\big) = \dim \operatorname{SL}\big((\bigwedge W)_1\big) = 3$ by Example 4.10 (a), so Propositions 4.8 (iii) and 4.1 imply that (Δ_4^+, Δ_4^-) is bijective. It follows that the half-spin representations are surjective. By dimension count and Proposition 4.8 (iii), their kernels have dimension 3.

Surjectivity of Δ_4^+ and Δ_4^- can also be seen more explicitly by using the fact that the group SL_2 is generated by the matrices $\left(\begin{smallmatrix} 1 & s \\ & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & \\ t & 1 \end{smallmatrix}\right)$ for $s, t \in k$ and noticing that

$$\begin{aligned} \Delta_4^+(x_{(-1,0,0,1),(1,s,0,-1)}) = \Delta_4^-(x_{(-1,0,0,1),(1,s,0,-1)}) &= \begin{pmatrix} 1 & s \\ & 1 \end{pmatrix}, \\ \Delta_4^+(x_{(-1,0,0,1),(1,0,t,-1)}) = \Delta_4^-(x_{(-1,0,0,1),(1,0,t,-1)}) &= \begin{pmatrix} 1 & \\ t & 1 \end{pmatrix}, \end{aligned}$$

where the scalar tuples satisfy the required relations.

We turn to odd dimension, where the situation is a little easier.

Proposition 5.11. *Suppose that* $n = \dim V$ *is odd. Then the spin representation* Δ_n *is an irreducible faithful rational representation of* $\mathrm{Spin}(V)$ *of dimension* $2^m = 2^{\frac{n-1}{2}}$.

Proof. This is a direct consequence of Proposition 5.1 and Remark 5.2 (b). $\square$

Example 5.12 (The spin representation in dimension 3)**.** We consider in more detail the case $\dim V = 3$. Writing $u := u_1$ and $w := w_1$, we have $V = (U \oplus W) \perp \mathrm{span}(z)$ where $U = \mathrm{span}(u)$ and $W = \mathrm{span}(w)$. Similarly as in Example 5.10, we put $v_{\underline{a}} := a_1u + a_2z + a_3w$ for $\underline{a} = (a_1, a_2, a_3) \in k^3$. Then by Corollary 3.40, the group $\mathrm{Spin}(V)$ is generated by the elements $x_{\underline{a},\underline{b}} := v_{\underline{a}}v_{\underline{b}}$ where $\underline{a}, \underline{b} \in k^3$ are such that $Q(v_{\underline{a}}) = Q(v_{\underline{b}}) = -1$. As remarked after Corollary 4.54, the latter condition precisely means that $a_1a_3 + a_2^2 = b_1b_3 + b_2^2 = -1$. Furthermore, a calculation using (Q1), Theorem 2.19 (i) and (3.1) shows that

$$x_{\underline{a},\underline{b}} = (a_1b_3 - a_3b_1)uw + (a_1b_2 - a_2b_1)uz + (a_3b_2 - a_2b_3)wz + (a_3b_1 + a_2b_2).$$

In view of the map $\Phi_{U,W,z}$ from Remark 5.2 (b) that restricts to the spin representation, we need to compute how ι_u, λ_w and η_a act on $\bigwedge W$. As in Example 5.8, the space $\bigwedge W$ is 2-dimensional with basis $(1, w)$, and ι_u and λ_w are represented by $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$, respectively. For η_1 we calculate its matrix to be $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. This means that uw acts by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, uz acts by $\left(\begin{smallmatrix} 0 & -1 \\ 0 & 0 \end{smallmatrix}\right)$ and wz acts by $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$. Hence, the spin representation is given by $\Delta_3\colon \mathrm{Spin}(V) \to \mathrm{GL}(\bigwedge W)$ where

$$x_{\underline{a},\underline{b}} \mapsto \begin{pmatrix} a_1b_3 + a_2b_2 & a_2b_1 - a_1b_2 \\ a_3b_2 - a_2b_3 & a_3b_1 + a_2b_2 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ -a_2 & a_3 \end{pmatrix} \begin{pmatrix} b_3 & -b_2 \\ b_2 & b_1 \end{pmatrix}.$$

Now the relations $a_1a_3 + a_2^2 = -1$ and $b_1b_3 + b_2^2 = -1$ imply that both matrices on the right hand side have determinant -1, so that the image of the spin representation in fact lies in the special linear group $\mathrm{SL}(\bigwedge W)$. Since Δ_3 moreover is faithful by Proposition 5.11 and $\dim \mathrm{Spin}(V) = 3 = \dim \mathrm{SL}(\bigwedge W)$ by Proposition 4.48 and Example 4.10 (a), we deduce from Propositions 4.8 (iii) and 4.1 that the spin representation even defines a bijective morphism of algebraic groups $\Delta_3\colon \mathrm{Spin}(V) \to \mathrm{SL}(\bigwedge W)$.

The observations about the image of the spin and half-spin representations made in Examples 5.10 and 5.12 may be generalized:

Proposition 5.13. *For* $\dim V \geq 3$*, the images of the spin and half-spin representations are contained in the special linear group of linear transformations of determinant* 1.

Proof. By Corollary 4.54, it holds that $[\mathrm{Spin}(V), \mathrm{Spin}(V)] = \mathrm{Spin}(V)$. Therefore, the images of the spin and half-spin representations are contained in the commutator subgroup of the general linear group which is a subset of the special linear group by the product rule for determinants. $\square$

If $\operatorname{char} k \neq 2$, then we can say even more about the image of the spin and half-spin representations which is the topic of the next subsection.

5.1.2 Invariant Bilinear Forms

Assume that $\operatorname{char} k \neq 2$. Apart from that, keep the notation from before.

In this subsection, we construct two bilinear forms on the space $\bigwedge W$ which are under some circumstances invariant under the spin and half-spin representations. This will give even more precise information on the images of Δ_n and $\Delta_n^{\pm}$. The material is taken from [Che97], Section 3.2 and [Mei13], Section 3.4.

For clarity, we will use the notation $S := \bigwedge W$ in the following. Recall from Proposition 1.36 that S is an $\mathbb{N}$-graded k-algebra with homogeneous parts $S_r = \bigwedge^r W$ which are $\binom{n}{r}$-dimensional and have basis

$$(w_{i_1} \wedge \cdots \wedge w_{i_r} \mid 1 \leq i_1 < \cdots < i_r \leq n).$$

This grading induces a $\mathbb{Z}_2$-grading $S = S_{\overline{0}} \oplus S_{\overline{1}}$ where $S_{\overline{0}} = \bigoplus_{r \text{ even}} S_r$ and $S_{\overline{1}} = \bigoplus_{r \text{ odd}} S_r$. We keep using the notation $\overline{0}, \overline{1}$ rather than $0, 1$ for the elements of $\mathbb{Z}_2$ in this section because it is unambiguous. Recall further that we have involutory antiautomorphisms $S \to S,\ s \mapsto s^{\top}$ and $S \to S,\ s \mapsto \overline{s}$ whose properties include those listed under (1.3).

As mentioned above, the space $S_m \leq S$ is 1-dimensional, with basis $(w_1 \wedge \cdots \wedge w_m)$. In the following, let $f_m \colon S \to k$ be the linear map that sends a vector $s \in S$ to the coefficient of $w_1 \wedge \cdots \wedge w_m$ in the basis representation of s with respect to the basis of S that is induced by the basis $(w_1, \ldots, w_m)$ of W. This map is an important ingredient in the construction of two bilinear forms on S:

Lemma 5.14. *Define maps*

$$\begin{aligned} b &\colon S \times S \to k,\ (s,t) \mapsto f_m(s^{\top} \wedge t), \\ \overline{b} &\colon S \times S \to k,\ (s,t) \mapsto f_m(\overline{s} \wedge t). \end{aligned}$$

Then b and $\overline{b}$ are bilinear forms on S with the following properties:

(i) If $m \equiv 0, 1 \bmod 4$, then b is symmetric and if $m \equiv 2, 3 \bmod 4$, then b is alternating.

(ii) If $m \equiv 0, 3 \bmod 4$, then $\overline{b}$ is symmetric and if $m \equiv 1, 2 \bmod 4$, then $\overline{b}$ is alternating.

(iii) b and $\overline{b}$ are nondegenerate.

(iv) If m is even, then $b\big|_{S_{\overline{0}}}$ and $b\big|_{S_{\overline{1}}}$ are nondegenerate.

Proof. Bilinearity of b and $\overline{b}$ is clear. Let $s \in S_r$ and $t \in S_{r'}$ be homogeneous elements of S. Note that by definition of f_m, we have $b(s,t) = 0 = b(t,s)$ unless $r + r' = m$. In the latter case, (1.3) yields

$$s^\top \wedge t = (s^\top \wedge t)^{\top\top} = (t^\top \wedge s)^\top = (-1)^{\frac{m(m-1)}{2}} t^\top \wedge s,$$

showing $b(s,t) = (-1)^{\frac{m(m-1)}{2}} b(t,s)$. By bilinearity, this equation holds for all elements $s, t \in S$. Taking into account that $\operatorname{char} k \neq 2$, the first claim follows. Similarly, one shows that $\overline{b}(s,t) = (-1)^{\frac{m(m+1)}{2}} \overline{b}(t,s)$ for all $s, t \in S$ which proves the second claim.

To prove nondegeneracy of b, let $0 \neq s \in S$. Then also $s^\top \neq 0$. Let $cw_{i_1} \wedge \cdots \wedge w_{i_r}$ with $c \in k^\times$ be a term of lowest degree in the basis representation of $s^\top$ w.r.t. the basis of S that is induced by $(w_1, \dots, w_m)$. Suppose that $\{1, \dots, m\} \setminus \{i_1, \dots, i_r\} = \{j_1, \dots, j_{r'}\}$ and put $t := w_{j_1} \wedge \cdots \wedge w_{j_{r'}} \in S$. Then $r + r' = m$ and Proposition 1.36 (iii) gives

$$s^\top \wedge t = cw_{i_1} \wedge \cdots \wedge w_{i_r} \wedge w_{j_1} \wedge \cdots \wedge w_{j_{r'}} = \pm cw_1 \wedge \cdots \wedge w_m,$$

so that $b(s,t) \neq 0$. This shows $s \notin \operatorname{rad} b$ and therefore that b is nondegenerate. Analogously, one proves that $\overline{b}$ is nondegenerate.

Turning to (iv), let m be even. We show that $S = S_{\overline{0}} \perp S_{\overline{1}}$ with respect to b. It suffices to prove orthogonality for homogeneous elements. So let $s \in S_r$ with r even and let $t \in S_{r'}$ with r' odd. Since m is even, we have $r + r' \neq m$ which implies that $b(s,t) = f_m(s^\top \wedge t) = 0$. This proves $S = S_{\overline{0}} \perp S_{\overline{1}}$. Claim (iv) now follows from part (iii) and Lemma 2.7 (iv). □

The algebra homomorphisms from Remark 5.2 have the following compatibility properties with b and $\overline{b}$:

Proposition 5.15. *With notation as in Remark 5.2, we have:*

(i) If n is even, then $b(\Phi_{U,W}(x)s, t) = b(s, \Phi_{U,W}(\tau(x))t)$ for all $x \in C$ and $s, t \in S$.

(ii) If $n \equiv 1 \bmod 4$, then $b(\Phi_{U,W,z}(x)s, t) = b(s, \Phi_{U,W,z}(\tau(x))t)$ for all $x \in C$ and $s, t \in S$.

(iii) If $n \equiv 3 \bmod 4$, then $\overline{b}(\Phi_{U,W,z}(x)s, t) = \overline{b}(s, \Phi_{U,W,z}(\overline{x})t)$ for all $x \in C$ and $s, t \in S$.

Proof. By bilinearity, it suffices to prove all claims for homogeneous elements of S. Throughout, let $s \in S_r$ and $t \in S_{r'}$. Moreover, as $\Phi_{U,W}$ and $\Phi_{U,W,z}$ are algebra homomorphisms and τ and $\bar{\cdot}$ are antihomomorphisms, one sees that it suffices to prove the claims for elements of an algebra generating system of C. By Corollary 3.5, such a generating system is given by $V \subseteq C$. Note that for elements of V, τ is the identity and conjugation simplifies to negation (cf. Proposition 3.14 and Corollary 3.16).

(i) Since n is even, we have $V = U \oplus W$. By the above remarks and by bilinearity, it suffices to prove the claim for elements $x \in U$ and $x \in W$. We first consider an element $w \in W$. Then

$$(\Phi_{U,W}(w)s)^\top \wedge t = (w \wedge s)^\top \wedge t = s^\top \wedge w \wedge t = s^\top \wedge \Phi_{U,W}(\tau(w))t$$

which yields the claim for $x = w$. Now let $u \in U$. For $x = u$, both sides of the claim are zero unless $r + r' = m + 1$. So let us now assume that $r + r' = m + 1$. Then $s^\top \wedge t = 0$ which together with parts (iv) and (vi) of Proposition 1.41 gives

$$\begin{aligned} 0 &= \iota_u(s^\top \wedge t) \\ &= \iota_u(s^\top) \wedge t + (-1)^r s^\top \wedge \iota_u(t) \\ &= (-1)^{r+1} \iota_u(s)^\top \wedge t + (-1)^r s^\top \wedge \iota_u(t) \\ &= (-1)^{r+1}(\iota_u(s)^\top \wedge t - s^\top \wedge \iota_u(t)). \end{aligned}$$

It follows that

$$(\Phi_{U,W}(u)s)^\top \wedge t = \iota_u(s)^\top \wedge t = s^\top \wedge \iota_u(t) = s^\top \wedge \Phi_{U,W}(\tau(u))t,$$

proving the claim also for $x = u$.

(ii) Here, we have $V = (U \oplus W) \perp \operatorname{span}(z)$. For elements $x \in U$ and $x \in W$, the claim holds by part (i). Thus, it only remains to consider the case $x = z$. If $r + r' \neq m$, then the claim holds as $0 = 0$. Assume now that $r + r' = m$. Since $n = 2m + 1$ and $n \equiv 1 \bmod 4$, the integer m must be even. Hence, we have $(-1)^r = (-1)^{r'}$. This gives

$$(\Phi_{U,W,z}(z)s)^\top \wedge t = (-1)^r s^\top \wedge t = s^\top \wedge (-1)^{r'} t = s^\top \wedge \Phi_{U,W,z}(z)t$$

which establishes the claim also for $x = z$.

(iii) By bilinearity, it again suffices to prove the claim for the three cases $x \in W$, $x \in U$ and $x = z$. First, let $w \in W$. Then

$$\overline{\Phi_{U,W,z}(w)s} \wedge t = \overline{w \wedge s} \wedge t = \overline{s} \wedge \overline{w} \wedge t = \overline{s} \wedge \Phi_{U,W,z}(\overline{w})t$$

which shows that the claim holds for $x = w$. Not let $u \in U$. As in part (i), we may assume that $r + r' = m + 1$. Then the above reasoning and the definition of $\bar{\cdot}$ show that

$$\begin{aligned} \overline{\iota_u(s)} \wedge t &= (-1)^{r-1} \iota_u(s)^\top \wedge t \\ &= (-1)^{r-1} s^\top \wedge \iota_u(t) \\ &= (-1)^{r-1}(-1)^r \overline{s} \wedge \iota_u(t) \\ &= -\overline{s} \wedge \iota_u(t) \end{aligned}$$

which gives $\overline{\Phi_{U,W,z}(u)s} \wedge t = \overline{s} \wedge \Phi_{U,W,z}(\overline{u})t$ and therefore the claim for $x = u$. Finally, we consider z. The proof is very similar to part (ii). Again, we may assume that $r + r' = m$. Since here m is odd, we get

$$\begin{aligned}\overline{\Phi_{U,W,z}(z)s} \wedge t &= (-1)^r \overline{s} \wedge t \\ &= -\overline{s} \wedge (-1)^{r'} t \\ &= -\overline{s} \wedge \Phi_{U,W,z}(z)t \\ &= \overline{s} \wedge \Phi_{U,W,z}(\overline{z})t\end{aligned}$$

which establishes the claim for $x = z$. □

Combined with Lemmas 5.14 and 3.34 (iv), we obtain the following results on the images of $\Delta_n^\pm$ and Δ_n which depend on the residue of n modulo 8:

Corollary 5.16.

(i) Suppose that $n \equiv 3 \bmod 8$. *Then* $\overline{b}$ *is a nondegenerate alternating bilinear form on* S *with*

$$\overline{b}(\Delta_n(x)s, \Delta_n(x)t) = \overline{b}(s,t) \qquad \text{for all } x \in \mathrm{Spin}(V) \text{ and } s,t \in S.$$

In particular, the image of Δ_n *is contained in* $\mathrm{Sp}(S, \overline{b})$.

(ii) Suppose that $n \equiv 4 \bmod 8$. *Then* b, $b\big|_{S_{\overline{0}}}$ *and* $b\big|_{S_{\overline{1}}}$ *are nondegenerate alternating bilinear forms on* S, $S_{\overline{0}}$ *and* $S_{\overline{1}}$, *respectively. Moreover, we have*

$$b(\Phi_{U,W}(x)s, \Phi_{U,W}(x)t) = b(s,t) \qquad \text{for all } x \in \mathrm{Spin}(V) \text{ and } s,t \in S.$$

In particular, the image of Δ_n *is contained in* $\mathrm{Sp}(S, b)$ *and the images of* Δ_n^+ *and* Δ_n^- *are contained in* $\mathrm{Sp}(S_{\overline{0}}, b\big|_{S_{\overline{0}}})$ *and* $\mathrm{Sp}(S_{\overline{1}}, b\big|_{S_{\overline{1}}})$, *respectively.*

(iii) Suppose that $n \equiv 5 \bmod 8$. *Then* b *is a nondegenerate alternating bilinear form on* S *with*

$$b(\Delta_n(x)s, \Delta_n(x)t) = b(s,t) \qquad \text{for all } x \in \mathrm{Spin}(V) \text{ and } s,t \in S.$$

In particular, the image of Δ_n *is contained in* $\mathrm{Sp}(S, b)$.

Proof. We only give a proof for part (i); the other parts are analogous. Suppose that $n \equiv 3 \bmod 8$. Then n is odd and $n = 2m + 1$. By the congruence condition, we must have $m \equiv 1 \bmod 4$. Hence, by Lemma 5.14, $\overline{b}$ is a nondegenerate alternating bilinear form on S. By definition of the spin representation, Proposition 5.15 (iii) and Lemma 3.34 (iv), we have

$$\overline{b}(\Delta_n(x)s, \Delta_n(x)t) = \overline{b}(s, \Phi_{U,W,z}(\overline{x}x)t) = \overline{b}(s,t)$$

for all $x \in \mathrm{Spin}(V)$ and $s, t \in S$. □

Corollary 5.17.

(i) *Suppose that* $n \equiv 0 \bmod 8$. *Define* $q\colon S \to k,\ s \mapsto \frac{1}{2}b(s,s)$. *Then* q, $q\big|_{S_{\overline{0}}}$ *and* $q\big|_{S_{\overline{1}}}$ *are nondegenerate quadratic forms on* S, $S_{\overline{0}}$ *and* $S_{\overline{1}}$, *respectively. Moreover, we have*

$$q(\Phi_{U,W}(x)s) = q(s) \qquad \textit{for all } x \in \mathrm{Spin}(V) \textit{ and } s \in S.$$

In particular, the image of Δ_n *is contained in* $\mathrm{SO}(S,q)$ *and the images of* Δ_n^+ *and* Δ_n^- *are contained in* $\mathrm{SO}(S_{\overline{0}}, q\big|_{S_{\overline{0}}})$ *and* $\mathrm{SO}(S_{\overline{1}}, q\big|_{S_{\overline{1}}})$, *respectively.*

(ii) *Suppose that* $n \equiv 1 \bmod 8$. *Define* $q\colon S \to k,\ s \mapsto \frac{1}{2}b(s,s)$. *Then* q *is a nondegenerate quadratic form on* S *with*

$$q(\Delta_n(x)s) = q(s) \qquad \textit{for all } x \in \mathrm{Spin}(V) \textit{ and } s \in S.$$

In particular, the image of Δ_n *is contained in* $\mathrm{SO}(S,q)$.

(iii) *Suppose that* $n \equiv 7 \bmod 8$. *Define* $\overline{q}\colon S \to k,\ s \mapsto \frac{1}{2}\overline{b}(s,s)$. *Then* $\overline{q}$ *is a nondegenerate quadratic form on* S *with*

$$\overline{q}(\Delta_n(x)s) = \overline{q}(s) \qquad \textit{for all } x \in \mathrm{Spin}(V) \textit{ and } s \in S.$$

In particular, the image of Δ_n *is contained in* $\mathrm{SO}(S,\overline{q})$.

Proof. Again we only prove (i) as the other parts work analogously. So suppose that $n \equiv 0 \bmod 8$. Then n is even with $n = 2m$ where we must have $m \equiv 0 \bmod 4$. Hence, by Lemma 5.14, the bilinear forms b, $b\big|_{S_{\overline{0}}}$ and $b\big|_{S_{\overline{1}}}$ are symmetric and nondegenerate. Remark 2.14 (a) and Proposition 2.28 (i) imply that q, $q\big|_{S_{\overline{0}}}$ and $q\big|_{S_{\overline{1}}}$ are nondegenerate quadratic forms.

Let now $x \in \mathrm{Spin}(V)$ and $s,t \in S$. Then by Proposition 5.15 (i) and Lemma 3.34 (iv), it holds that

$$q(\Phi_{U,W}(x)s) = \frac{1}{2}b(\Phi_{U,W}(x)s, \Phi_{U,W}(x)s) = \frac{1}{2}b(s, \Phi_{U,W}(\tau(x)x)s) = \frac{1}{2}b(s,s) = q(s),$$

as claimed. From the definition of the spin and half-spin representation it follows that the images of Δ_n, Δ_n^+ and Δ_n^- are contained in the respective orthogonal groups. Using Proposition 5.13 and the fact that $\operatorname{char} k \neq 2$, we conclude that the images are even contained in the respective special orthogonal groups. □

To sum up the results, the images of the spin and half-spin representations are contained in the special orthogonal group if $n \equiv 0, 1, 7 \bmod 8$ and are contained in the symplectic group if $n \equiv 3, 4, 5 \bmod 8$.

Example 5.18 (The spin representation in dimension 5)**.** Suppose that $\dim V = 5$. Proceeding exactly as in the previous examples, we compute explicit matrices that describe the spin representation. Here, U and W are 2-dimensional, with bases (u_1, u_2) and (w_1, w_2), respectively, and we put $v_{\underline{a}} := a_1u_1 + a_2u_2 + a_3z + a_4w_2 + a_5w_1$ for $\underline{a} = (a_1, \ldots, a_5) \in k^5$. We have $Q(v_{\underline{a}}) = a_1a_5 + a_2a_4 + a_3^2$ and it holds that the spin group is generated by the elements $x_{\underline{a},\underline{b}} := v_{\underline{a}}v_{\underline{b}}$ for $\underline{a}, \underline{b} \in k^5$ with $Q(v_{\underline{a}}) = Q(v_{\underline{b}}) = -1$, where one computes that

$$\begin{aligned} x_{\underline{a},\underline{b}} = {} & (a_1b_2 - a_2b_1)u_1u_2 + (a_1b_5 - a_5b_1)u_1w_1 + (a_1b_4 - a_4b_1)u_1w_2 \\ & + (a_3b_1 - a_1b_3)zu_1 + (a_2b_5 - a_5b_2)u_2w_1 + (a_2b_4 - a_4b_2)u_2w_2 \\ & + (a_3b_2 - a_2b_3)zu_2 + (a_5b_4 - a_4b_5)w_1w_2 + (a_3b_5 - a_5b_3)zw_1 \\ & + (a_3b_4 - a_4b_3)zw_2 + (a_3b_3 + a_5b_1 + a_4b_2). \end{aligned}$$

The matrices for the actions of $\iota_{u_1}, \iota_{u_2}, \lambda_{w_1}$ and λ_{w_2} on $\bigwedge W$ with respect to the basis $(1, w_1 \wedge w_2, w_1, w_2)$ are as in Example 5.10. Furthermore, η_1 acts by $\operatorname{diag}(1, 1, -1, -1)$. It follows that the spin representation $\Delta_5\colon \operatorname{Spin}(V) \to \operatorname{GL}(\bigwedge W)$ is given by mapping $x_{\underline{a},\underline{b}}$ to

$$\begin{pmatrix} a_1b_5 + a_2b_4 + a_3b_3 & a_2b_1 - a_1b_2 & a_3b_1 - a_1b_3 & a_3b_2 - a_2b_3 \\ a_5b_4 - a_4b_5 & a_5b_1 + a_4b_2 + a_3b_3 & a_4b_3 - a_3b_4 & a_3b_5 - a_5b_3 \\ a_5b_3 - a_3b_5 & a_3b_2 - a_2b_3 & a_5b_1 + a_2b_4 + a_3b_3 & a_5b_2 - a_2b_5 \\ a_4b_3 - a_3b_4 & a_1b_3 - a_3b_1 & a_4b_1 - a_1b_4 & a_1b_5 + a_4b_2 + a_3b_3 \end{pmatrix}.$$

By Corollary 5.16, the image of Δ_5 is even contained in $\operatorname{Sp}(\bigwedge W)$. Moreover, Δ_5 is faithful by Proposition 5.11. Since $\dim \operatorname{Spin}(V) = 10 = \dim \operatorname{Sp}(\bigwedge W)$ by Proposition 4.48 and Remark 4.43, it follows from Propositions 4.8 (iii) and 4.1 that the spin representation defines a bijective morphism of algebraic groups $\Delta_5\colon \operatorname{Spin}(V) \to \operatorname{Sp}(\bigwedge W)$.

Remark 5.19. By Examples 5.8, 5.10, 5.12 and 5.18, the spin and half-spin representations give rise to bijective morphisms of algebraic groups

$$\begin{aligned} \Delta_2^{\pm}\colon \operatorname{Spin}_2 &\to \mathbf{G}_{\mathrm{m}}, & \Delta_3\colon \operatorname{Spin}_3 &\to \operatorname{SL}_2, \\ (\Delta_4^+, \Delta_4^-)\colon \operatorname{Spin}_4 &\to \operatorname{SL}_2 \times \operatorname{SL}_2, & \Delta_5\colon \operatorname{Spin}_5 &\to \operatorname{Sp}_4\,. \end{aligned}$$

Furthermore, by Propositions 5.9 and 5.13 and a dimension count, the half-spin representations $\Delta_6^{\pm}\colon \operatorname{Spin}_6 \to \operatorname{SL}_4$ are bijective morphisms of algebraic groups. If $\operatorname{char} k = 0$, then by [Spr98], Exercise 5.3.5 (1), bijective morphisms of algebraic groups are isomorphisms. Thus, at least in this case, the above maps realize the isomorphisms from Corollary 4.62 that have abstractly come out of the theory. It would be interesting to know whether this also holds in positive characteristic. For the maps $\Delta_2^{\pm}$ we could already establish this fact in Example 5.8.

5.2 Nested Spin Groups

In this section, we discuss possibilities to view (products of) spin groups of lower dimension as subgroups of higher-dimensional spin groups. This works similarly as for special orthogonal groups (cf. Proposition 4.37), and both constructions are related by the twisted adjoint representation $\rho\colon \mathrm{Spin}(V) \to \mathrm{SO}(V)$. While Proposition 5.20 is implicit in Section 3.7.5 of [Mei13], the other constructions do not appear in any of our references.

We start with the case of embedding a lower-dimensional spin group in a higher-dimensional one which was already dealt with in Theorem 4.47.

Proposition 5.20. *Let $V' \leq V$ be a subspace such that the restriction $B\big|_{V'}$ is nondegenerate. Let $i\colon V' \hookrightarrow V$ denote the inclusion. Then there is an embedding of algebraic groups*

$$e\colon \mathrm{Spin}(V') \hookrightarrow \mathrm{Spin}(V),\ u'v' \mapsto i(u')i(v'),$$

where $u', v' \in V'$ with $Q(u') = Q(v') = -1$. It fits into a commutative diagram

$$\begin{tikzcd}
\mathrm{Spin}(V') \arrow[r, hook] \arrow[d, hook, "e"'] & C_0(V') \arrow[r, hook] \arrow[d, hook] & C(V') \arrow[d] \\
\mathrm{Spin}(V) \arrow[r, hook] & C_0(V) \arrow[r, hook] & C(V)
\end{tikzcd}$$

where the other vertical maps are the algebra homomorphisms obtained by extending i.

Proof. This is Theorem 4.47, applied to $i\colon V' \hookrightarrow V$. ☐

Remark 5.21. Let $V' \leq V$ be a subspace such that the restriction $B\big|_{V'}$ is nondegenerate.

(a) By Proposition 5.20, there is an embedding of algebraic groups $e\colon \mathrm{Spin}(V') \hookrightarrow \mathrm{Spin}(V)$. We will use this embedding to view $\mathrm{Spin}(V') \leq \mathrm{Spin}(V)$ as a closed subgroup and will denote the elements of $\mathrm{Spin}(V')$ by the same symbol when viewed as elements of $\mathrm{Spin}(V)$, to simplify notation.

(b) Similarly, we have an injective algebra homomorphism $C_0(V') \hookrightarrow C_0(V)$ and will denote the image of an element $x \in C_0(V')$ under this map again by x. Recall from Proposition 3.9 that if $V'' \leq V$ is such that $V = V' \perp V''$, then we have $C(V) \cong C(V') \,{}^{\mathbb{Z}_2}\!\otimes C(V'')$ as $\mathbb{Z}_2$-graded k-algebras. With the notation just introduced, the isomorphism $\Psi\colon C(V') \,{}^{\mathbb{Z}_2}\!\otimes C(V'') \to C(V)$ from the proof of Proposition 3.9 restricts to an injective homomorphism

$$\psi\colon C_0(V') \otimes C_0(V'') \to C_0(V),\ x' \otimes x'' \mapsto x'x''$$

of k-algebras.

The assumption that the restriction $B\big|_{V'}$ be nondegenerate is there to comply with our general setting. A characterization of when this assumption is met for a subspace $V' \leq V$ is given in Lemma 2.7. That lemma also shows that if $V' \leq V$ is such that $B\big|_{V'}$ is nondegenerate, then one has an orthogonal decomposition $V = V' \perp (V')^{\perp}$. Hence, by Proposition 4.37, there is an embedding of algebraic groups $\mathrm{SO}(V') \hookrightarrow \mathrm{SO}(V)$. It is related to the above embedding of spin groups, as follows:

Proposition 5.22. *Let $V' \leq V$ be a subspace such that the restriction $B\big|_{V'}$ is nondegenerate. Then there is a commutative diagram*

$$\begin{tikzcd}
\mathrm{Spin}(V') \arrow[r, hook] \arrow[d, "\rho'"'] & \mathrm{Spin}(V) \arrow[d, "\rho"] \\
\mathrm{SO}(V') \arrow[r, hook] & \mathrm{SO}(V)
\end{tikzcd}$$

of algebraic groups, where the lower map is the embedding from Proposition 4.37.

Proof. We set $V'' := (V')^{\perp}$. Then, as remarked above, we have $V = V' \perp V''$. In order to check commutativity of the diagram, let $x \in \mathrm{Spin}(V')$ be arbitrary. Going right and then down in the diagram, we end up with the map $\rho(x) \in \mathrm{SO}(V)$, whereas the other path leads to $\rho'(x) \oplus \mathrm{id}_{V''} \in \mathrm{SO}(V)$. We need to check that these two maps agree, so let $v = v' + v'' \in V$ where $v' \in V'$ and $v'' \in V''$. Expressing x as a product of an even number of vectors from V' according to Corollary 3.40 yields $xv'' = v''x$ by orthogonality and (3.1). It follows that

$$(\rho'(x) \oplus \mathrm{id}_{V''})(v) = xv'x^{-1} + v'' = xv'x^{-1} + xv''x^{-1} = xvx^{-1} = \rho(x)(v),$$

proving commutativity of the diagram. □

Given an orthogonal decomposition $V = V' \perp V''$, for example originating from a nondegenerate subspace as described above, we may also consider the group $\mathrm{Spin}(V') \times \mathrm{Spin}(V'')$. There is a natural map from this product to $\mathrm{Spin}(V)$ which is almost injective and which as above is compatible with the twisted adjoint representation:

Theorem 5.23. *Suppose that $V', V'' \leq V$ are subspaces such that $V = V' \perp V''$. Then the map*

$$\beta\colon\ \mathrm{Spin}(V') \times \mathrm{Spin}(V'') \to \mathrm{Spin}(V),\ (x, y) \mapsto xy,$$

is a morphism of algebraic groups with kernel $\{(1,1), (-1,-1)\}$. It fits into a commutative diagram

$$\begin{tikzcd}
\mathrm{Spin}(V') \times \mathrm{Spin}(V'') \arrow[r, "\beta"] \arrow[d, "\rho' \times \rho''"'] & \mathrm{Spin}(V) \arrow[d, "\rho"] \\
\mathrm{SO}(V') \times \mathrm{SO}(V'') \arrow[r, hook] & \mathrm{SO}(V)
\end{tikzcd}$$

of algebraic groups, where the lower map is the embedding from Proposition 4.37.

Proof. We first show that β is in fact a group homomorphism. To this end, let $x, \tilde{x} \in \mathrm{Spin}(V')$ and $y, \tilde{y} \in \mathrm{Spin}(V'')$. By Corollary 3.40, there are vectors $v'_1, \ldots, v'_r \in V'$ and $v''_1, \ldots, v''_s \in V''$ with r and s even and which all have Q-value -1, such that

$\tilde{x} = \pm v'_1 \cdots v'_r$ and $y = \pm v''_1 \cdots v''_s$. Applying the relations $v'_i v''_j = -v''_j v'_i$ obtained from orthogonality, it follows that $\tilde{x}y = y\tilde{x}$ as r and s are even. This implies

$$\beta\big((x,y)(\tilde{x},\tilde{y})\big) = \beta(x\tilde{x}, y\tilde{y}) = x\tilde{x}y\tilde{y} = xy\tilde{x}\tilde{y} = \beta(x,y)\beta(\tilde{x},\tilde{y}),$$

that is, β is a group homomorphism. Multiplication being a morphism of varietes, it is a morphism of algebraic groups.

We turn to commutativity of the diagram. Dealing with group homomorphisms, it suffices to check this for elements of the form $(x,1)$ with $x \in \mathrm{Spin}(V')$ and $(1,y)$ with $y \in \mathrm{Spin}(V'')$. Let $x \in \mathrm{Spin}(V')$. Tracing the element $(x,1) \in \mathrm{Spin}(V') \times \mathrm{Spin}(V'')$ first right and then down, we see that it gets mapped to $\rho(x) \in \mathrm{SO}(V)$. Going down and then right, we end up with $\rho'(x) \oplus \mathrm{id}_{V''} \in \mathrm{SO}(V)$. That these two maps agree, has been shown in Proposition 5.22. Analogously, one sees that the diagram commutes for $(1,y)$ where $y \in \mathrm{Spin}(V'')$.

Finally, we need to determine the kernel of β, for which we will make use of commutativity of the diagram. Let $(x,y) \in \ker\beta$. Commutativity and injectivity of the lower map imply that $(x,y) \in \ker(\rho' \times \rho'')$, that is, $(\rho'(x), \rho''(y)) = (1,1)$. Theorem 3.39 gives $x, y \in \{\pm 1\}$ which by definition of β forces $(x,y) \in \{(1,1),(-1,-1)\}$. The other inclusion is clear. ☐

We have seen in Remark 5.21 (b) that in a similar way, there is an injective map from $C_0(V') \otimes C_0(V'')$ into $C_0(V)$. These constructions are related as follows:

Proposition 5.24. *Suppose that* $V', V'' \leq V$ *are subspaces such that* $V = V' \perp V''$. *Then the map*

$$\mathrm{Spin}(V') \times \mathrm{Spin}(V'') \to C_0(V') \otimes C_0(V''),\ (x,y) \mapsto x \otimes y,$$

is a group homomorphism into the subgroup of units, with kernel $\{(1,1),(-1,-1)\}$. *It fits into a commutative diagram*

$$\begin{tikzcd}
\mathrm{Spin}(V') \times \mathrm{Spin}(V'') \arrow[r] \arrow[d, "\beta"'] & C_0(V') \otimes C_0(V'') \arrow[d, hook, "\psi"] \\
\mathrm{Spin}(V) \arrow[r, hook] & C_0(V)
\end{tikzcd}$$

where β *is the map from Theorem 5.23 and* ψ *is the algebra monomorphism from Remark 5.21 (b).*

Proof. By the rules for multiplication in the tensor product of algebras, it is clear that the given map is a group homomorphism into the subgroup of units. Commutativity of the diagram is immediate from the definition of β and Remark 5.21 (b).

If $(x,y) \in \mathrm{Spin}(V') \times \mathrm{Spin}(V'')$ is such that $x \otimes y = 1 \otimes 1$, then commutativity of the diagram implies that $(x,y) \in \ker\beta$. But this kernel has been determined in Theorem 5.23 which yields $(x,y) \in \{(1,1),(-1,-1)\}$. The other inclusion is trivial. ☐

5.3 Restrictions of Spin Representations

Having seen in which way spin groups and their products are contained in one another, we now address the question how the spin and half-spin representations behave when restricted to a spin group of lower dimension, and how the representations of the product of two lower-dimensional spin groups that are induced by Δ_n and $\Delta_n^{\pm}$ look like. It turns out that in most cases, one can avoid computations by utilizing the results from representation theory from Section 1.2. Except for the first proposition, the results from this section are new.

We start with the case of restriction of a spin or half-spin representation to a spin group of a subspace of V of codimension 1. This result can be found in Proposition 3.21 of [Mei13].

Proposition 5.25. *Let $n \geq 2$ and let $V' \leq V$ be an $(n-1)$-dimensional subspace such that the restriction $B\big|_{V'}$ is nondegenerate.*

(i) Suppose that n is even. The restriction of any half-spin representation of $\mathrm{Spin}(V)$ to $\mathrm{Spin}(V')$ is equivalent to the spin representation of $\mathrm{Spin}(V')$:

$$\Delta_n^+\big|_{\mathrm{Spin}(V')} \cong \Delta_{n-1} \quad \text{and} \quad \Delta_n^-\big|_{\mathrm{Spin}(V')} \cong \Delta_{n-1}.$$

(ii) Suppose that n is odd. The restriction of the spin representation of $\mathrm{Spin}(V)$ to $\mathrm{Spin}(V')$ is equivalent to the spin representation of $\mathrm{Spin}(V')$:

$$\Delta_n\big|_{\mathrm{Spin}(V')} \cong \Delta_{n-1} = \Delta_{n-1}^+ \oplus \Delta_{n-1}^-.$$

Proof. By Proposition 5.20, there is a commutative diagram

$$\begin{tikzcd}
\mathrm{Spin}(V') \arrow[r, hook] \arrow[d, hook] & C_0(V') \arrow[r, hook] \arrow[d, hook] & C(V') \arrow[d] \\
\mathrm{Spin}(V) \arrow[r, hook] & C_0(V) \arrow[r, hook] & C(V)
\end{tikzcd}$$

with left hand map the standard embedding of $\mathrm{Spin}(V')$ into $\mathrm{Spin}(V)$ and the other two vertical maps algebra homomorphisms (obtained by extending the inclusion $V' \hookrightarrow V$).

(i) The half-spin representations of $\mathrm{Spin}(V)$ by definition are obtained by restricting the half-spin representations of $C_0(V)$. The left hand square of the above diagram shows that restricting a half-spin representation of $C_0(V)$ first to $\mathrm{Spin}(V)$ and then to $\mathrm{Spin}(V')$ is the same as first restricting it to $C_0(V')$ and then to $\mathrm{Spin}(V')$. We may thus take a look at the latter route.

The restriction of a half-spin representation of $C_0(V)$ to $C_0(V')$ is a $2^{\frac{n}{2}-1}$-dimensional representation of $C_0(V')$. But V' being of odd dimension $(n-1)$, the algebra $C_0(V')$ is central simple with unique irreducible representation of degree

$2^{\frac{(n-1)-1}{2}} = 2^{\frac{n}{2}-1}$ (cf. Remark 5.2 (b)). By Proposition 1.12 (i), the restriction of a half-spin representation of $C_0(V)$ to $C_0(V')$ must therefore be equivalent to the spin representation of $C_0(V')$. By Proposition 5.1, further restricting it to $\mathrm{Spin}(V')$, we end up with a representation which is equivalent to the spin representation of $\mathrm{Spin}(V')$.

(ii) Consider the (irreducible) representation $\Phi_{U,W,z} \colon C \to \mathrm{End}(\bigwedge W)$ from Remark 5.2 (b). Restricting it to $C_0(V)$ gives the spin representation of $C_0(V)$. Thus, the representation $\Delta_n\big|_{\mathrm{Spin}(V')}$ of $\mathrm{Spin}(V')$ may be obtained from the representation $\Phi_{U,W,z}$ of $C(V)$ by first going all the way left and then up in the commutative diagram.

The diagram then shows that we may equivalently first go up and then left, starting at $C(V)$. This way, the representation of $C(V')$ obtained from $\Phi_{U,W,z}$ has dimension $2^{\frac{n-1}{2}}$ which is the same as the dimension of the spin representation of $C(V')$. So they must be equivalent by Proposition 1.12 (i) and the fact that $C(V')$ is central simple. Restricting further to $C_0(V')$ and then to $\mathrm{Spin}(V')$, we end up with a representation that is equivalent to the spin representation of $\mathrm{Spin}(V')$. By commutativity of the diagram, the claim follows. ☐

Note that a subspace with the properties as in the theorem always exists if $\operatorname{char} k \neq 2$: By Lemma 2.7, one may for example take the orthogonal complement of the subspace spanned by a nonsingular vector. In particular, if $\dim V$ is odd and $V = (U \oplus W) \perp \mathrm{span}(z)$ is a Lagrangian decomposition, then the subspace $U \oplus W$ has this property. In contrast, if $\operatorname{char} k \neq 2$, such a subspace can never exist by Proposition 2.15 and nondegeneracy of B.

Example 5.26. If $\dim V$ is odd and $V = (U \oplus W) \perp \mathrm{span}(z)$ is a Lagrangian decomposition, then we obtain an embedding $\mathrm{Spin}(U \oplus W) \hookrightarrow \mathrm{Spin}(V)$, as remarked above. We illustrate Proposition 5.25 for the cases $\dim V = 3$ and $\dim V = 5$ and the restriction to the subgroup $\mathrm{Spin}(U \oplus W)$ with the examples from Section 5.1.

Suppose that $\dim V = 3$. With notation as in Examples 5.8 and 5.12, $\mathrm{Spin}(U \oplus W)$ is the subgroup of $\mathrm{Spin}(V)$ that is generated by the elements $tuw + t^{-1}wu$ for $t \in k^\times$. In terms of the generators $x_{\underline{a},\underline{b}}$ of $\mathrm{Spin}(V)$, we see that $\mathrm{Spin}(U \oplus W)$ is generated by the elements $x_{\underline{a},\underline{b}}$ with $a_2 = b_2 = 0$ since such an element equals

$$(a_1b_3 - a_3b_1)uw + a_3b_1 = a_1b_3uw + a_3b_1wu = a_1b_3uw + (a_1b_3)^{-1}wu$$

by the fact that $a_1a_3 + a_2^2 = b_1b_3 + b_2^2 = -1$. Under Δ_3, such a generator gets mapped to $\left(\begin{smallmatrix} a_1b_3 & \\ & a_3b_1 \end{smallmatrix}\right)$. Looking at Example 5.8, this is exactly how the spin representation of $\mathrm{Spin}(U \oplus W)$ w.r.t. the Lagrangian decomposition $U \oplus W$ is given.

A similar observation holds in dimension 5. Here, with notation as in Examples 5.10 and 5.18, $\mathrm{Spin}(U \oplus W)$ is the subgroup of $\mathrm{Spin}(V)$ that is generated by the elements $x_{\underline{a},\underline{b}} \in \mathrm{Spin}(V)$ with $a_3 = b_3 = 0$ (after relabelling the indices). Moreover, setting

$a_3 = b_3 = 0$ in the matrix $\Delta_5(x_{\underline{a},\underline{b}})$, we see that $\Delta_5\big|_{\mathrm{Spin}(U \oplus W)}$ is precisely the spin representation of $\mathrm{Spin}(U \oplus W)$.

We next consider the case where we are given an orthogonal decomposition $V = V' \perp V''$ which by Theorem 5.23 gives rise to a morphism of algebraic groups $\beta\colon \mathrm{Spin}(V') \times \mathrm{Spin}(V'') \to \mathrm{Spin}(V)$. By concatenation with β, a representation of $\mathrm{Spin}(V)$ then induces a representation of $\mathrm{Spin}(V') \times \mathrm{Spin}(V'')$. For the next theorem, we recall the following construction: If $\theta\colon G \to \mathrm{GL}(X)$ and $\sigma\colon H \to \mathrm{GL}(Y)$ are representations of two groups G and H, then the map

$$\theta \otimes \sigma\colon G \times H \to \mathrm{GL}(X \otimes Y),\ (g, h) \mapsto \theta(g) \otimes \sigma(h)$$

is a representation of $G \times H$, the *tensor product* of θ and σ. This is the analogon of the tensor product of representations of algebras, cf. Definition 1.10. We will see a relation between these constructions also in the proof of the following theorem which describes the representations of $\mathrm{Spin}(V') \times \mathrm{Spin}(V'')$ that are induced by the spin representation respectively the two half-spin representations of $\mathrm{Spin}(V)$. The proof uses the same technique as the one of Proposition 5.25.

Theorem 5.27. *Suppose that $V', V'' \leq V$ are subspaces such that $V = V' \perp V''$ and with $l := \dim V' \geq 1$ and $\dim V'' \geq 1$. Let $\beta\colon \mathrm{Spin}(V') \times \mathrm{Spin}(V'') \to \mathrm{Spin}(V)$ be the map from Theorem 5.23.*

(i) Suppose that n is even and that l is odd. Then the representation of $\mathrm{Spin}(V') \times \mathrm{Spin}(V'')$ obtained from any half-spin representation of $\mathrm{Spin}(V)$ via β is equivalent to the tensor product of the spin representations of $\mathrm{Spin}(V')$ and $\mathrm{Spin}(V'')$: $\Delta_n^{\pm} \circ \beta \cong \Delta_l \otimes \Delta_{n-l}$.

(ii) Suppose that n is odd. Then the representation of $\mathrm{Spin}(V') \times \mathrm{Spin}(V'')$ obtained from the spin representation of $\mathrm{Spin}(V)$ via β is equivalent to the tensor product of the spin representations of $\mathrm{Spin}(V')$ and $\mathrm{Spin}(V'')$: $\Delta_n \circ \beta \cong \Delta_l \otimes \Delta_{n-l}$.

Proof. As in Proposition 5.25, the trick is to argue with the corresponding representations of the Clifford algebras and their algebra structure, eventually making use of a dimension argument. Here, by Proposition 5.24, we have a commutative diagram

$$\begin{tikzcd}
\mathrm{Spin}(V') \times \mathrm{Spin}(V'') \arrow[r] \arrow[d, "\beta"'] & C_0(V') \otimes C_0(V'') \arrow[d, hook, "\psi"] \\
\mathrm{Spin}(V) \arrow[r, hook] & C_0(V)
\end{tikzcd}$$

with right hand map the algebra monomorphism from Remark 5.21 (b). The claims will now follow by using this diagram and, if necessary, suitably extending it to the right.

(i) The half-spin representations of $\mathrm{Spin}(V)$ are obtained by restricting the two respective half-spin representations of $C_0(V)$ which both have dimension $2^{\frac{n}{2}-1}$. The diagram shows that the representation $\Delta_n^{\pm} \circ \beta$ of $\mathrm{Spin}(V') \times \mathrm{Spin}(V'')$ may also be obtained as the representation induced by the restriction of the respective half-spin representation of $C_0(V)$ to $C_0(V') \otimes C_0(V'')$.

Now l and $n-l$ being odd, the algebras $C_0(V')$ and $C_0(V'')$ are central simple, with unique irreducible representation the respective spin representation, cf. Remark 5.2 (b). By Corollary 1.14, the only irreducible representation of the algebra $C_0(V') \otimes C_0(V'')$ (up to equivalence) is the tensor product of those two spin representations and has dimension

$$2^{\frac{l-1}{2}} 2^{\frac{n-l-1}{2}} = 2^{\frac{n-2}{2}} = 2^{\frac{n}{2}-1}.$$

But this is precisely the dimension of the representation of $C_0(V') \otimes C_0(V'')$ that results when restricting a half-spin representation of $C_0(V)$. Hence, by Proposition 1.12 (i), the restriction of a half-spin representation of $C_0(V)$ to $C_0(V') \otimes C_0(V'')$ must be equivalent to the tensor product of the spin representations of $C_0(V')$ and $C_0(V'')$. The claim now follows as the representation of $\mathrm{Spin}(V') \times \mathrm{Spin}(V'')$ that is induced by this tensor product is the tensor product of the spin representations of $\mathrm{Spin}(V')$ and $\mathrm{Spin}(V'')$, respectively, see the map in Proposition 5.24.

(ii) Without loss of generality, we assume that l is even. Note that $C(V') \otimes C_0(V'')$ is a subalgebra of $C(V')\, {}^{\mathbb{Z}_2}\!\otimes C(V'')$ that contains $C_0(V') \otimes C_0(V'')$. This leads to the extended diagram

$$\begin{tikzcd}
\mathrm{Spin}(V') \times \mathrm{Spin}(V'') \arrow[r] \arrow[d, "\beta"'] & C_0(V') \otimes C_0(V'') \arrow[r, hook] \arrow[d, hook, "\psi"] & C(V') \otimes C_0(V'') \arrow[d, hook] \\
\mathrm{Spin}(V) \arrow[r, hook] & C_0(V) \arrow[r, hook] & C(V)
\end{tikzcd}$$

where the right hand vertical map is the restriction of the isomorphism from the proof of Proposition 3.9. The proof now works as before, this time starting with an irreducible representation of $C(V)$.

The representation $\Delta_n \circ \beta$ is obtained from the representation $\Phi_{U,W,z} \colon C(V) \to \mathrm{End}(\bigwedge W)$ from Remark 5.2 (b) by going all the way left and then up in the diagram. In view of commutativity of the diagram, it only remains to show that the restriction of $\Phi_{U,W,z}$ to $C(V') \otimes C_0(V'')$ is equivalent to the tensor product of the spin representations of $C(V')$ and $C_0(V'')$.

This follows as before: Since $l = \dim V'$ is even and therefore $\dim V''$ is odd, the algebra $C(V') \otimes C_0(V'')$ is the tensor product of two central simple k-algebras. Hence, by Corollary 1.14, its only irreducible representation is the tensor product of the respective spin representations, of dimension $2^{\frac{l}{2}} 2^{\frac{n-l-1}{2}} = 2^{\frac{n-1}{2}}$. But this is also the dimension of the restriction of $\Phi_{U,W,z}$ to $C(V') \otimes C_0(V'')$, so these representations must be equivalent by Proposition 1.12 (i). $\square$

It remains the case where the dimensions of V, V' and V'' are all even. Here, we cannot argue in the same way as before because the algebra $C_0(V') \otimes C_0(V'')$ has more than one irreducible representation (namely 4 by Theorem 1.13 and [NT89], Lemma 2.4.1). Instead, we will give explicit maps to show the equivalence of representations, using Theorem 3.20.

Theorem 5.28. *Suppose that $V', V'' \leq V$ are subspaces such that $V = V' \perp V''$ and with $l := \dim V' \geq 1$ and $\dim V'' \geq 1$. Further assume that n and l are even. Then we have*

$$\Delta_n^+ \circ \beta \cong (\Delta_l^+ \otimes \Delta_{n-l}^+) \oplus (\Delta_l^- \otimes \Delta_{n-l}^-)$$

and

$$\Delta_n^- \circ \beta \cong (\Delta_l^+ \otimes \Delta_{n-l}^-) \oplus (\Delta_l^- \otimes \Delta_{n-l}^+)$$

as representations of $\mathrm{Spin}(V') \times \mathrm{Spin}(V'')$ where $\beta \colon \mathrm{Spin}(V') \times \mathrm{Spin}(V'') \to \mathrm{Spin}(V)$ is the morphism of algebraic groups from Theorem 5.23.

Proof. Let $U', W' \leq V'$ and $U'', W'' \leq V''$ be maximal totally singular subspaces with associated bases such that they constitute respective Lagrangian decompositions $V' = U' \oplus W'$ and $V'' = U'' \oplus W''$. Define $U := U' \perp U''$ and $W := W' \perp W''$. By Theorem 3.20, we then have a Lagrangian decomposition $V = U \oplus W$ (w.r.t. the natural bases of U and W). The respective spin representations of the Clifford algebras of V, V' and V'' are thus given by $\Phi_{U,W}, \Phi_{U',W'}$ and $\Phi_{U'',W''}$.

Let $F \colon \bigwedge W' \,{}^{\mathbb{Z}_2}\!\!\otimes \bigwedge W'' \to \bigwedge W$ be the $\mathbb{Z}_2$-graded algebra isomorphism from Proposition 1.38. Let $(x, y) \in \mathrm{Spin}(V') \times \mathrm{Spin}(V'')$. We claim that the diagram

$$\begin{tikzcd}
\bigwedge W' \,{}^{\mathbb{Z}_2}\!\!\otimes \bigwedge W'' \arrow[r, "\Delta_l(x) \otimes \Delta_{n-l}(y)"] \arrow[d, "F"'] & \bigwedge W' \,{}^{\mathbb{Z}_2}\!\!\otimes \bigwedge W'' \arrow[d, "F"] \\
\bigwedge W = \bigwedge(W' \perp W'') \arrow[r, "\Delta_n(xy)"'] & \bigwedge W = \bigwedge(W' \perp W'')
\end{tikzcd}$$

commutes. For this, we use the diagram from Theorem 3.20, applied to $x \otimes y$. Since x and y are homogeneous of degree 0, also the maps $\Phi_{U',W'}(x) \in \mathrm{End}(\bigwedge W')_0$ and $\Phi_{U'',W''}(y) \in \mathrm{End}(\bigwedge W'')_0$ are homogeneous of degree 0. Hence, we have

$$\begin{aligned}
\Theta \circ (\Phi_{U',W'} \otimes \Phi_{U'',W''})(x \otimes y) &= \Theta(\Phi_{U',W'}(x) \otimes \Phi_{U'',W''}(y)) \\
&= \Delta_l(x) \otimes \Delta_{n-l}(y) \in \mathrm{End}(\bigwedge W' \,{}^{\mathbb{Z}_2}\!\!\otimes \bigwedge W'')_0
\end{aligned}$$

by Proposition 1.29 (the minus-sign in the definition of Θ disappears). This means that tracing the element $x \otimes y$ in the diagram from Theorem 3.20 gives

$$\Delta_n(xy) = (\Phi_{U,W} \circ \Psi)(x \otimes y) = \Omega(\Delta_l(x) \otimes \Delta_{n-l}(y)) = F \circ (\Delta_l(x) \otimes \Delta_{n-l}(y)) \circ F^{-1},$$

noting Remark 5.21 (b) for the map Ψ. This establishes commutativity of the above diagram.

Now all maps in the diagram are homogeneous of degree 0. Hence, we still have a commutative diagram when restricting all maps to the homogeneous components of degree 0. Doing so, the lower map by definition becomes $\Delta_n^+(xy) = (\Delta_n^+ \circ \beta)(x, y)$. On the other hand, we have $(\bigwedge W'^{\mathbb{Z}_2}\otimes \bigwedge W'')_0 = ((\bigwedge W')_0 \otimes (\bigwedge W'')_0) \oplus ((\bigwedge W')_1 \otimes (\bigwedge W'')_1)$ and therefore

$$(\Delta_l(x) \otimes \Delta_{n-l}(y))\big|_{(\bigwedge W'^{\mathbb{Z}_2}\otimes \bigwedge W'')_0} = (\Delta_l^+(x) \otimes \Delta_{n-l}^+(y)) \oplus (\Delta_l^-(x) \otimes \Delta_{n-l}^-(y)).$$

This proves the equivalence of $\Delta_n^+ \circ \beta$ and $(\Delta_l^+ \otimes \Delta_{n-l}^+) \oplus (\Delta_l^- \otimes \Delta_{n-l}^-)$. The second claim follows by restricting the maps in the diagram to the homogeneous components of degree 1. ☐

The theorem in particular implies the weaker statement $\Delta_n \circ \beta \cong \Delta_l \otimes \Delta_{n-l}$ which could have also been proved using the method from Theorem 5.27. We further note:

Remark 5.29. Suppose that we have a decomposition $V = V' \perp V''$ with $l := \dim V' \geq 1$ and $\dim V'' \geq 1$. Then there is an obvious embedding of algebraic groups

$$e\colon \operatorname{Spin}(V') \to \operatorname{Spin}(V') \times \operatorname{Spin}(V''),\ x \mapsto (x, 1).$$

By definition of equivalence, concatenation of equivalent representations of $\operatorname{Spin}(V') \times \operatorname{Spin}(V'')$ with e results in equivalent representations of $\operatorname{Spin}(V')$. We apply this observation to Theorems 5.27 and 5.28.

The concatenation $\beta \circ e$ precisely defines the embedding $\operatorname{Spin}(V') \hookrightarrow \operatorname{Spin}(V)$. On the other hand, if we have representations $\theta\colon \operatorname{Spin}(V') \to \operatorname{GL}(X)$ and $\sigma\colon \operatorname{Spin}(V'') \to \operatorname{GL}(Y)$, then

$$(\theta \otimes \sigma) \circ e \cong \underbrace{\theta \oplus \cdots \oplus \theta}_{\dim Y \text{ times}} =: (\dim Y) \cdot \theta$$

by the definition of the Kronecker product of matrices. Applied to Theorems 5.27 and 5.28, we obtain the results

$$\begin{aligned}
\Delta_n^\pm\big|_{\operatorname{Spin}(V')} &\cong 2^{\frac{n-l-1}{2}} \Delta_l, \quad \text{if } n \text{ is even and } l \text{ is odd},\\
\Delta_n\big|_{\operatorname{Spin}(V')} &\cong 2^{\lfloor \frac{n-l}{2} \rfloor} \Delta_l, \quad \text{if } n \text{ is odd},\\
\Delta_n^+\big|_{\operatorname{Spin}(V')} &\cong 2^{\frac{n-l}{2}-1} \Delta_l^+ \oplus 2^{\frac{n-l}{2}-1} \Delta_l^-, \quad \text{if } n \text{ and } l \text{ are even},\\
\Delta_n^-\big|_{\operatorname{Spin}(V')} &\cong 2^{\frac{n-l}{2}-1} \Delta_l^+ \oplus 2^{\frac{n-l}{2}-1} \Delta_l^-, \quad \text{if } n \text{ and } l \text{ are even},
\end{aligned}$$

using Proposition 1.36 (iv) for the dimensions. In particular, for $n - l = 1$, we retrieve the results from Proposition 5.25.

Example 5.30. We take a look at the case $\dim V = 4$. Let $V = U \oplus W$ be a Lagrangian decomposition with respect to bases (u_1, u_2) of U and (w_1, w_2) of W. Then by Theorem 2.19, the subspaces $V' := \operatorname{span}(u_1, w_1)$ and $V'' := \operatorname{span}(u_2, w_2)$ satisfy $V = V' \perp V''$. By Example 4.51, the elements of $\operatorname{Spin}(V')$ are of the form

$tu_1w_1 + t^{-1}w_1u_1$ for $t \in k^\times$ and the elements of $\mathrm{Spin}(V'')$ are of the form $su_2w_2 + s^{-1}w_2u_2$ for $s \in k^\times$. With the matrices from Example 5.10, we compute that

$$\begin{aligned}(\Delta_4 \circ \beta)(tu_1w_1 + t^{-1}w_1u_1, su_2w_2 + s^{-1}w_2u_2) &= \mathrm{diag}(t, t^{-1}, t^{-1}, t) \cdot \mathrm{diag}(s, s^{-1}, s, s^{-1}) \\ &= \mathrm{diag}(ts, t^{-1}s^{-1}, t^{-1}s, ts^{-1}).\end{aligned}$$

which shows that

$$\begin{aligned}(\Delta_4^+ \circ \beta)(tu_1w_1 + t^{-1}w_1u_1, su_2w_2 + s^{-1}w_2u_2) &= \begin{pmatrix} ts & \\ & t^{-1}s^{-1} \end{pmatrix}, \\ (\Delta_4^- \circ \beta)(tu_1w_1 + t^{-1}w_1u_1, su_2w_2 + s^{-1}w_2u_2) &= \begin{pmatrix} t^{-1}s & \\ & ts^{-1} \end{pmatrix}.\end{aligned}$$

Moreover, by Example 5.8 we have $\Delta_2^+(tu_1w_1 + t^{-1}w_1u_1) = t$ and $\Delta_2^-(tu_1w_1 + t^{-1}w_1u_1) = t^{-1}$. Hence,

$$\begin{aligned}(\Delta_2^+ \otimes \Delta_2^+) \oplus (\Delta_2^- \otimes \Delta_2^-)(tu_1w_1 + t^{-1}w_1u_1, su_2w_2 + s^{-1}w_2u_2) &= \begin{pmatrix} ts & \\ & t^{-1}s^{-1} \end{pmatrix}, \\ (\Delta_2^+ \otimes \Delta_2^-) \oplus (\Delta_2^- \otimes \Delta_2^+)(tu_1w_1 + t^{-1}w_1u_1, su_2w_2 + s^{-1}w_2u_2) &= \begin{pmatrix} ts^{-1} & \\ & t^{-1}s \end{pmatrix}.\end{aligned}$$

This shows that $\Delta_4^+ \circ \beta \cong (\Delta_2^+ \otimes \Delta_2^+) \oplus (\Delta_2^- \otimes \Delta_2^-)$ and $\Delta_4^- \circ \beta \cong (\Delta_2^+ \otimes \Delta_2^-) \oplus (\Delta_2^- \otimes \Delta_2^+)$, in accordance with Theorem 5.28.

6 Conjugacy Classes

We assume in this chapter that k is algebraically closed.

The last piece of information that we need for our algorithm is knowledge about the conjugacy classes of unipotent elements of spin groups. Since conjugate matrices have the same Jordan normal form, it suffices to consider those conjugacy classes in order to investigate the Jordan blocks of the unipotent elements of spin groups under the spin and half-spin representations.

The first section of this chapter is concerned with generalities on conjugacy classes in semisimple algebraic groups. Afterwards, we describe the unipotent conjugacy classes of the special orthogonal group which will serve as models for the unipotent conjugacy classes of the spin group. In the final section, we discuss how we can find representatives for the conjugacy classes of unipotent elements of $\mathrm{Spin}(V)$ that will later play a key role in our main algorithm in Section 7.1.

6.1 General Results for Semisimple Algebraic Groups

In this section, we collect some general results on conjugacy classes in semisimple algebraic groups. These can be found in [Hum95a], Chapters 1 and 4 and [Ste65] and will be utilized in Sections 6.2 and 6.3.

For any group G, conjugation is an action of G on itself given by $g.x := x^g := gxg^{-1}$ for $g, x \in G$. The stabilizer of $x \in G$ under this action is the centralizer $C_G(x)$, and the orbit of x is its conjugacy class, which will be denoted x^G. By the orbit stabilizer theorem, there is a bijection

$$G/C_G(x) \xrightarrow{1:1} x^G, \; gC_G(x) \mapsto x^g.$$

If G is an algebraic group, then conjugation defines a morphism of varieties $G \times G \to G$, so that G becomes a *G-space* with respect to conjugation ([MT11], Definition 5.1). It follows that the centralizer $C_G(x) \leq G$ is a closed subgroup. Moreover, every orbit x^G is open in its closure, and conjugacy classes of minimal dimension are closed (cf. [MT11], Proposition 5.4). One characterization of closedness of conjugacy classes is the following:

Proposition 6.1. *Let G be a semisimple algebraic group and let $x \in G$. Then x^G is closed if and only if x is semisimple. In particular, $Z(G) \subseteq G_s$.*

Proof. This is [Hum95a], Corollary 1.7. ☐

We now take a look at elements whose conjugacy classes are of maximal dimension, or equivalently, whose centralizer is of minimal dimension.

Proposition 6.2. *Let G be a semisimple algebraic group and let $x \in G$. Then* $\dim C_G(x) \geq \operatorname{rk} G$.

Proof. See [Hum95a], Proposition 1.6. ☐

This motivates the following definition:

Definition 6.3. Let G be a semisimple algebraic group. An element $x \in G$ is called *regular* if $\dim C_G(x) = \operatorname{rk} G$.

This is equivalent to requiring the centralizer to have minimal possible dimension, see [Hum95a], p. 53. In particular, regular elements exist.

From now on, we focus on unipotent elements. Note that by Lemma 4.13 (ii) (and choosing an embedding into a general linear group), all elements of the conjugacy class of a unipotent element are again unipotent. Thus, the conjugacy classes of unipotent elements partition G_u. We will call a conjugacy class that is contained in G_u a *unipotent (conjugacy) class.*

We continue the discussion of regular elements. The following theorem shows that regular unipotent elements exist:

Theorem 6.4. *Let G be a semisimple algebraic group with maximal torus $T \leq G$ and root system R. Let $U_\alpha \leq G$ denote the root subgroup associated with $\alpha \in R$ and let $\Delta = \{\alpha_1, \ldots, \alpha_r\} \subseteq R$ be a set of simple roots. For each $i = 1, \ldots, r$, let $1 \neq u_i \in U_{\alpha_i}$. Then $x := u_1 \cdots u_r \in G$ is regular unipotent.*

Proof. See [Ste65], Theorem 4.6. ☐

In particular, this gives a way to compute a regular unipotent element, if the root subgroups are known. As mentioned above, all elements of the conjugacy class of a regular unipotent element are again unipotent. Even more, they are again regular as conjugate elements have isomorphic centralizers. The next theorem shows that there is exactly one such conjugacy class of regular unipotent elements:

Theorem 6.5. *Let G be a semisimple algebraic group. Then all regular unipotent elements of G are conjugate.*

Proof. This is [Hum95a], Theorem 4.6. ☐

Thus, the set of regular unipotent elements forms a single unipotent conjugacy class.

The following proposition is the key tool to determine the unipotent conjugacy classes of the spin group. It relates the unipotent classes of isogenous semisimple algebraic groups and is stated in Proposition 1.8 of [Hum95a]. We give a detailed proof.

Proposition 6.6. *Let G and G' be semisimple algebraic groups and let $\varphi\colon G \to G'$ be an isogeny. Then φ induces bijections $G_u \to G'_u$ and*

$$\{\textit{unipotent conj. classes of } G\} \xrightarrow{1:1} \{\textit{unipotent conj. classes of } G'\},\ u^G \mapsto \varphi(u)^{G'},$$

mapping regular unipotent elements to regular unipotent elements.

Proof. We clearly have $\varphi(G_u) \subseteq G'_u$ by Theorem 4.15 (iii). Now let $x, y \in G_u$ with $\varphi(x) = \varphi(y)$. Then there is $z \in \ker\varphi$ with $x = zy$. Since $\ker\varphi \subseteq Z(G)$ by Proposition 4.25 (i), part (iv) of Theorem 4.15 implies that $1 = x_s = z_s y_s = z_s$, that is, z is unipotent. But it is also semisimple by Proposition 6.1, forcing $z = 1$ and therefore $x = y$. This shows that $\varphi\colon G_u \to G'_u$ is injective.

For surjectivity of the restriction let $y \in G'_u$. Since φ is surjective, there is $x \in G$ with $\varphi(x) = y$. By Theorem 4.15 (iii) and the fact that y is unipotent, it holds that $1 = y_s = \varphi(x_s)$, giving $x_s \in \ker\varphi$. Thus, putting $u := x_u = x x_s^{-1}$, we have $u \in G_u$ and $\varphi(u) = y$.

In order to see that φ maps regular unipotent elements to regular unipotent elements, we show that $\varphi(C_G(u)) = C_{G'}(\varphi(u))$ for unipotent elements $u \in G_u$. The inclusion $\varphi(C_G(u)) \subseteq C_{G'}(\varphi(u))$ is clear. For the reverse, let $y \in C_{G'}(\varphi(u))$ and let $x \in G$ such that $\varphi(x) = y$. We thus have $\varphi(x)\varphi(u)\varphi(x^{-1}) = \varphi(u)$. Hence, there is $z \in \ker\varphi \subseteq Z(G)$ with $xux^{-1} = zu$. But u and therefore also xux^{-1} are unipotent (see Lemma 4.13 (ii)), so it follows as above that $xux^{-1} = u$, that is, $x \in C_G(u)$. This shows $\varphi(C_G(u)) = C_{G'}(\varphi(u))$. Since $\dim\ker\varphi = 0$, we infer from Propositions 4.8 (iii) and 4.20 (ii) that φ maps regular unipotent elements to regular unipotent elements.

Surjectivity of the map between the sets of classes is now clear. If $u, v \in G_u$ with $\varphi(u)^{G'} = \varphi(v)^{G'}$, then there is $x \in G$ with $\varphi(u) = \varphi(x)\varphi(v)\varphi(x^{-1})$. With the same reasoning as above, we get $u = xvx^{-1}$, that is, $u^G = v^G$. □

Applied to the isogeny $\rho\colon \mathrm{Spin}_n \to \mathrm{SO}_n$ from Proposition 4.44, this means that the unipotent classes of Spin_n are in bijection with the unipotent classes of SO_n. Thus, in order to determine the unipotent conjugacy classes of Spin_n, we may as well determine those of SO_n. This is the topic of the next section.

Note that the proof of Proposition 7.6 relies substantially on the fact that $(\ker\varphi)_u = 1$. In the special case $\rho\colon \mathrm{Spin}_n \to \mathrm{SO}_n$, this can also be proved directly, without using Proposition 7.1. To this end, let $x \in (\ker\rho)_u$ and let $e\colon \mathrm{Spin}_n \hookrightarrow \mathrm{GL}_l$ be an embedding. Then $y := e(x) \in \mathrm{GL}_l$ is unipotent with $y^2 = 1$ as $\ker\rho = \{\pm 1\}$. If $\operatorname{char} k = 2$, then the claim is clear. If $\operatorname{char} k = 0$, then by Lemma 4.13 (iv) we must have $y = 1$ as

y is unipotent and has finite order. By injectivity of e, it follows that $x = 1$. If $\operatorname{char} k =: p \geq 3$, then y has p-power order by Lemma 4.13 (iii), which again leads to $y = 1$ and $x = 1$.

6.2 Unipotent Classes of SO_n

Throughout this section, we assume that $\operatorname{char} k \neq 2$. Let $n \in \mathbb{N}_{>0}$. We denote by

$$J_i := \begin{pmatrix} 1 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 1 \end{pmatrix} \in \mathrm{Mat}_i(k)$$

the Jordan block of size $i \geq 1$ for the eigenvalue 1. By a *partition* of n we mean a tuple $(i_1^{r_{i_1}}, \ldots, i_t^{r_{i_t}})$ of strictly ascending positive integer numbers i_j with positive integer indices r_{i_j} and the property that $\sum_j r_{i_j} \cdot i_j = n$.

With the aid of the results from Chapter 3 of [LS12], we describe the unipotent conjugacy classes of the orthogonal and the special orthogonal group. For this, we work with the matrix versions O_n and SO_n as this is more convenient. Furthermore, we determine the class of regular unipotent elements of SO_n. We conclude the section by transferring the results to the unipotent classes of the spin gorup.

We first consider the easier case of the general linear group GL_n. Here, two matrices are conjugate if and only if they have the same Jordan normal form (that is, the same Jordan blocks with according multiplicities, disregarding the ordering of the blocks). Hence, the conjugacy classes of GL_n are characterized by the Jordan normal form. Now by Lemma 4.13 (i), an element $u \in \mathrm{GL}_n$ is unipotent if and only if all its eigenvalues are 1, so the unipotent conjugacy classes of GL_n are parametrized by the Jordan normal forms $\bigoplus_i J_i^{r_i}$ where $\sum_i i r_i = n$. In particular, GL_n has only finitely many unipotent conjugacy classes and these classes correspond to the partitions of n, which gives an algorithm to determine all classes.

Turning to the orthogonal group $\mathrm{O}_n \leq \mathrm{GL}_n$, it still holds that an element $u \in \mathrm{O}_n$ is unipotent if and only if all its eigenvalues are 1. This shows that the unipotent elements of O_n are contained in SO_n and that their Jordan normal form only consists of blocks with eigenvalue 1. The question arises whether the Jordan normal form again completely determines the conjugacy class. It turns out that at least for the orthogonal group, this question can be answered in the affirmative:

Theorem 6.7. *Two unipotent elements of O_n are conjugate in O_n if and only if they are conjugate in GL_n. In particular, O_n has only finitely many unipotent conjugacy classes.*

Proof. This is [LS12], Corollary 3.6 (i). □

Thus, the unipotent conjugacy classes of O_n can be described by the Jordan normal forms of unipotent elements. To determine all these classes, it only remains to identify which Jordan normal forms are actually attained by unipotent elements of O_n. For this, there is a simple criterion:

Proposition 6.8. *There is a unipotent element in* SO_n *with Jordan normal form* $\bigoplus_i J_i^{r_i}$ *if and only if* r_i *is even for each even* i.

Proof. This follows from [LS12], Corollary 3.6 (ii). $\square$

This allows one to give a complete description of the unipotent conjugacy classes of O_n. Algorithmically, one may compute (labels for) the unipotent classes from the set of partitions of n.

We now would like to determine also the unipotent classes of the special orthogonal group $\mathrm{SO}_n \trianglelefteq \mathrm{O}_n$. We will see that in this case, the analogon of Theorem 6.7 does not hold. However, we can use the knowledge about the unipotent classes of O_n to determine those of SO_n: Since O_n operates by conjugation on $(\mathrm{SO}_n)_u$ by Lemma 4.13 (ii), we have

$$(\mathrm{SO}_n)_u = \dot{\bigcup_{u \in (\mathrm{SO}_n)_u}} u^{\mathrm{O}_n}.$$

Consequently, it suffices to study the behaviour of u^{O_n} for unipotent elements u of SO_n. Note that as SO_n operates by conjugation on u^{O_n}, the class is a union of SO_n-conjugacy classes. More precisely, there is the following general statement:

Proposition 6.9. *Let* G *be a group with normal subgroup* $H \trianglelefteq G$ *and let* $x \in H$. *Then the* G*-conjugacy class* x^G *is the union of* $|G : HC_G(x)|$ *many* H*-conjugacy classes. In particular,* x^G *is a single* H*-conjugacy class if and only if* $HC_G(x) = G$.

Proof. Since H is normal in G, we have $x^G \subseteq H$. Clearly, H operates on x^G by conjugation, so x^G is the union of H-conjugacy classes. Let S denote the set of H-conjugacy classes that are contained in x^G. We need to show that $|S| = |G : HC_G(x)|$. Define an action of G on S by $g.h^H := (ghg^{-1})^H$. Since H is normal in G, the set $(ghg^{-1})^H$ is again an H-conjugacy class, so the action is well-defined.

It holds that G operates transitively on S. For, if $h_1^H, h_2^H \in S$, then h_1 and h_2 are G-conjugate to x, so there is $g \in G$ with $h_1 = gh_2g^{-1}$ which means that $g.h_2^H = (gh_2g^{-1})^H = h_1^H$. Hence, considering the orbit of $x^H \in S$, we have $|S| = |G : \mathrm{Stab}(x^H)|$ by the orbit-stabilizer theorem, where $\mathrm{Stab}(x^H)$ denotes the stabilizer of x^H in G.

Let $g \in G$. By definition, we have $g \in \mathrm{Stab}(x^H)$ if and only if $(gxg^{-1})^H = x^H$. The latter holds if and only if there is an element $h \in H$ such that $gxg^{-1} = hxh^{-1}$, that is to say, $h^{-1}g \in C_G(x)$. We infer that $\mathrm{Stab}(x^H) = HC_G(x)$. Thus, we have $|S| = |G : HC_G(x)|$, as claimed. $\square$

In our case, it holds that $|\mathrm{O}_n : \mathrm{SO}_n| = 2$ by Corollary 2.40, so if a class u^{O_n} splits in SO_n, then it must split into two conjugacy classes, and it does so if and only if $C_{\mathrm{O}_n}(u) \subseteq \mathrm{SO}_n$. This splitting can also be read off from the Jordan normal form, as the following proposition shows:

Proposition 6.10. *Let $u \in \mathrm{SO}_n$ be unipotent, with Jordan normal form $\bigoplus_i J_i^{r_i}$. Then u^{O_n} splits into two SO_n-classes if and only if $r_i = 0$ for all odd i.*

Proof. See [LS12], Lemma 3.11. □

Note that this together with Proposition 6.8 implies that splitting of O_n-classes occurs precisely if $n \equiv 0 \bmod 4$.

We are now able to describe all unipotent conjugacy classes of SO_n. The possible Jordan normal forms of unipotent elements of SO_n are those in which all eigenvalues are 1 and where even-sized blocks occur with even multiplicity. The Jordan normal form completely determines the conjugacy class of a unipotent element of SO_n, unless it does not contain an odd-sized block in which case the corresponding O_n-conjugacy class splits into two SO_n-conjugacy classes. We use this to assign labels to the unipotent conjugacy classes, as follows:

Definition 6.11.

(a) The conjugacy class of unipotent elements of O_n that have Jordan normal form $J_{i_1}^{r_{i_1}} \oplus \cdots \oplus J_{i_t}^{r_{i_t}}$ where $i_1 < \cdots < i_t$ will be denoted by $(i_1^{r_{i_1}}, \ldots, i_t^{r_{i_t}})$.

(b) The conjugacy class of unipotent elements of SO_n that have Jordan normal form $J_{i_1}^{r_{i_1}} \oplus \cdots \oplus J_{i_t}^{r_{i_t}}$ where $i_1 < \cdots < i_t$ and there is an odd i_j with $r_{i_j} \geq 1$ will be denoted by $(i_1^{r_{i_1}}, \ldots, i_t^{r_{i_t}})$.

The two conjugacy classes of unipotent elements of SO_n whose elements have Jordan normal form $J_{i_1}^{r_{i_1}} \oplus \cdots \oplus J_{i_t}^{r_{i_t}}$ where $i_1 < \cdots < i_t$ and there is no odd i_j with $r_{i_j} \geq 1$ will be denoted by $(i_1^{r_{i_1}}, \ldots, i_t^{r_{i_t}})_0$ and $(i_1^{r_{i_1}}, \ldots, i_t^{r_{i_t}})_1$.

Note that there is no ambiguity in the notation for the classes of unipotent elements of SO_n and of O_n that have Jordan normal form $J_{i_1}^{r_{i_1}} \oplus \cdots \oplus J_{i_t}^{r_{i_t}}$ where $i_1 < \cdots < i_t$ and there is an odd i_j with $r_{i_j} \geq 1$, since the two underlying sets agree. We furthermore remark that there is no canonical way to distinguish the two SO_n-classes that stem from a splitting unipotent class of O_n.

Example 6.12. We determine (labels for) the unipotent classes of SO_n for small n. One way to do this is to take the set of partitions of n and first delete those partitions in which an even number occurs with an odd multiplicity (cf. Proposition 6.8). In a second step, one identifies the partitions that do not contain an odd number, makes a copy of them and indexes them by 0 and 1, respectively. This gives labels for all unipotent classes of SO_n in the form of Definition 6.11.

We have used the computer algebra system `GAP` for these computations. The set of partitions of n may for example be computed with the `GAP`-functions `Partitions` or `IteratorOfPartitions` (or with an easy recursive algorithm). The algorithm described above is carried out by the function `classes_SO` from the Appendix. We illustrate the procedure and the results for small values of n:

If $n = 1$, then there is only one partition (1). Hence, we have one conjugacy class (1). If $n = 2$, then there are two partitions (1^2) and (2). Since the second one does not correspond to the Jordan normal form of a unipotent element of the special orthogonal group, there is one conjugacy class (1^2) of unipotent elements of SO_2.

For $n = 3$, we obtain the partitions (1^3), $(1, 2)$ and (3) and therefore the unipotent classes (1^3) and (3). The case $n = 4$ is the first in which splitting of a unipotent class of O_n into two SO_n-classes occurs. The partitions of 4 are (1^4), $(1^2, 2)$, (2^2), $(1, 3)$ and (4). Since (2^2) does not contain an odd number, it gives rise to two SO_4-classes labelled by $(2^2)_0$ and $(2^2)_1$. The remaining classes are (1^4) and $(1, 3)$.

The unipotent classes of SO_n up to $n = 8$ are displayed in Table 6.1. Observe that adding an odd number j to a class of SO_n gives a class of SO_{n+j}. Analogously, one may add an even number with an even multiplicity. We will study this phenomenon in more detail in Section 6.3.

n	Unipotent classes of SO_n
1	(1)
2	(1^2)
3	(1^3), (3)
4	(1^4), $(1,3)$, $(2^2)_0$, $(2^2)_1$
5	(1^5), $(1^2,3)$, $(1,2^2)$, (5)
6	(1^6), $(1^3,3)$, $(1^2,2^2)$, $(1,5)$, (3^2)
7	(1^7), $(1^4,3)$, $(1^3,2^2)$, $(1^2,5)$, $(1,3^2)$, $(2^2,3)$, (7)
8	(1^8), $(1^5,3)$, $(1^4,2^2)$, $(1^3,5)$, $(1^2,3^2)$, $(1,2^2,3)$, $(1,7)$, $(3,5)$, $(2^4)_0$, $(2^4)_1$, $(4^2)_0$, $(4^2)_1$

Table 6.1: Labels for the unipotent classes of SO_n for $n \leq 8$

Recall from Section 6.1 that the set of regular unipotent elements of a semisimple algebraic group forms one of the unipotent conjugacy classes. Knowing all unipotent conjugacy classes of SO_n, we would now like to identify this class of regular unipotent elements. To this end, we need to compute centralizer dimensions of unipotent elements. Proposition 3.7 (iii) of [LS12] gives a formula for the dimension of the centralizer in O_n of a unipotent element $u \in \mathrm{SO}_n$ in terms of its Jordan normal form. The following lemma shows that this dimension is in fact the same as that of the dimension of the centralizer in SO_n which is what we are interested in.

Lemma 6.13. *For every* $x \in \mathrm{SO}_n$ *we have* $\dim C_{\mathrm{SO}_n}(x) = \dim C_{\mathrm{O}_n}(x)$.

Proof. Let $x \in \mathrm{SO}_n$. By [Bor91], Theorem 6.8, the quotient $\mathrm{SO}_n C_{\mathrm{O}_n}(x)/\mathrm{SO}_n$ is an algebraic group, and the map

$$C_{\mathrm{O}_n}(x) \to \mathrm{SO}_n C_{\mathrm{O}_n}(x)/\mathrm{SO}_n,\ g \mapsto g\,\mathrm{SO}_n$$

is a morphism of algebraic groups. Its kernel is $C_{\mathrm{O}_n}(x) \cap \mathrm{SO}_n = C_{\mathrm{SO}_n}(x)$. Now by Corollary 2.40, the group $\mathrm{O}_n/\mathrm{SO}_n$ is finite, so also its subgroup $\mathrm{SO}_n C_{\mathrm{O}_n}(x)/\mathrm{SO}_n$ must be finite. Hence, Proposition 4.8 (iii) yields $\dim C_{\mathrm{O}_n}(x) = \dim C_{\mathrm{SO}_n}(x)$. □

In terms of the description of the unipotent classes of SO_n from above, we obtain:

Proposition 6.14. *The conjugacy class of* SO_n *of regular unipotent elements is given by* $(1, n-1)$ *if* n *is even and by* (n) *if* n *is odd.*

Proof. We need to determine the centralizer dimension of an element of the respective classes. With the formula from Proposition 3.7 (iii) of [LS12], we compute in the even case for $u \in (1, n-1)$ and in the odd case for $v \in (n)$ that

$$\begin{aligned} \dim C_{\mathrm{O}_n}(u) &= \frac{1}{2}(1+n-1)+1-\frac{1}{2}(1+1) = \frac{n}{2}, \\ \dim C_{\mathrm{O}_n}(v) &= \frac{1}{2}n - \frac{1}{2} = \frac{n-1}{2}. \end{aligned}$$

The claim now follows from Lemma 6.13 and Proposition 4.39. □

We study in a little more detail the phenomenon of splitting of a unipotent O_n-conjugacy class u^{O_n} into two SO_n-classes. By Propositions 6.8 and 6.10, it occurs precisely if $n \equiv 0 \bmod 4$ and can be detected from the Jordan normal form of u. Moreover, by Proposition 6.9, it may be characterized in terms of the centralizer $C_{\mathrm{O}_n}(u)$. The latter allows one to relate the two SO_n-classes emerging from u^{O_n}:

Lemma 6.15. *Suppose that* $\mathcal{C}$ *is a unipotent conjugacy class of* O_n *that splits into two* SO_n*-classes* $\mathcal{C}_0$ *and* $\mathcal{C}_1$*. Then for all* $x \in \mathrm{O}_n \setminus \mathrm{SO}_n$*, we have* $x\mathcal{C}_0x^{-1} = \mathcal{C}_1$*. Conversely, if* $u_0 \in \mathcal{C}_0$ *and* $u_1 \in \mathcal{C}_1$*, then there is some* $x \in \mathrm{O}_n \setminus \mathrm{SO}_n$ *such that* $u_1 = xu_0x^{-1}$*.*

Proof. Let $x \in \mathrm{O}_n \setminus \mathrm{SO}_n$ and $u_0 \in \mathcal{C}_0$. We have $xu_0x^{-1} \in \mathcal{C}$. Assume that $xu_0x^{-1} \in \mathcal{C}_0 = u_0^{\mathrm{SO}_n}$. Then there is an element $y \in \mathrm{SO}_n$ such that $xu_0x^{-1} = yu_0y^{-1}$, that is, $y^{-1}x \in C_{\mathrm{O}_n}(u_0)$. Now by assumption, the conjugacy class $\mathcal{C} = u_0^{\mathrm{O}_n}$ splits into two SO_n-classes, so we have $C_{\mathrm{O}_n}(u_0) \subseteq \mathrm{SO}_n$ by Proposition 6.9 and Corollary 2.40. This implies $x \in \mathrm{SO}_n$ which is a contradiction. Hence, we must have $xu_0x^{-1} \in \mathcal{C}_1$, showing $x\mathcal{C}_0x^{-1} \subseteq \mathcal{C}_1$. Analogously, one proves $x^{-1}\mathcal{C}_1x \subseteq \mathcal{C}_0$.

Now let $u_0 \in \mathcal{C}_0$ and $u_1 \in \mathcal{C}_1$. Since they both belong to the O_n-conjugacy class $\mathcal{C}$, there is some $x \in \mathrm{O}_n$ such that $u_1 = xu_0x^{-1}$. We must have $x \notin \mathrm{SO}_n$ as otherwise $u_1 \in \mathcal{C}_0$ and therefore $\mathcal{C}_0 = \mathcal{C}_1$ which is impossible. □

We finally turn to the pin and the spin groups. For the remainder of the section, let V be a vector space over k of finite dimension n and suppose that Q is a nondegenerate quadratic form on V. Recall from Section 4.3 that $\mathrm{O}(V) \cong \mathrm{O}_n$ and $\mathrm{SO}(V) \cong \mathrm{SO}_n$ as algebraic groups, so the previous results and notations apply also to $\mathrm{O}(V)$ and $\mathrm{SO}(V)$.

Via the isogeny $\rho\colon \mathrm{Pin}(V) \to \mathrm{O}(V)$, we infer that all unipotent elements of $\mathrm{Pin}(V)$ are contained in $\mathrm{Spin}(V)$ since the same holds for the pair $\mathrm{SO}(V) \leq \mathrm{O}(V)$ and we have $\ker \rho = \{\pm 1\} \subseteq \mathrm{Spin}(V)$. We now transfer the above results and notation from the groups $\mathrm{SO}_n \leq \mathrm{O}_n$ to the groups $\mathrm{Spin}(V) \leq \mathrm{Pin}(V)$.

Remark 6.16.

(a) Since the unipotent classes of $\mathrm{Spin}(V)$ and SO_n are in bijection by Proposition 6.6 applied to the isogeny $\rho\colon \mathrm{Spin}(V) \to \mathrm{SO}(V) \cong \mathrm{SO}_n$, we will use the same labels as for SO_n to denote the corresponding unipotent classes of $\mathrm{Spin}(V)$.

(b) Analogously as above, the isogeny $\rho\colon \mathrm{Pin}(V) \to \mathrm{O}(V) \cong \mathrm{O}_n$ induces a bijection between the sets of unipotent conjugacy classes of O_n and $\mathrm{Pin}(V)$, and we again use the same labels.

Note that knowing the unipotent classes of $\mathrm{Pin}(V)$, there is another possibility to determine the unipotent classes of $\mathrm{Spin}(V)$, by studying how the class $u^{\mathrm{Pin}(V)}$ of a unipotent element $u \in \mathrm{Spin}(V)$ behaves. This approach and the one from part (a) are compatible in the sense that the class $u^{\mathrm{Pin}(V)}$ splits into two $\mathrm{Spin}(V)$-classes if and only if the class $\rho(u)^{\mathrm{O}(V)}$ splits into two $\mathrm{SO}(V)$-classes as $\rho(C_{\mathrm{Pin}(V)}(u)) = C_{\mathrm{O}(V)}(\rho(u))$ by the proof of Proposition 6.6.

Furthermore, if the class $(i_1^{r_{i_1}}, \ldots, i_t^{r_{i_t}})$ of $\mathrm{Pin}(V)$ splits into two $\mathrm{Spin}(V)$-classes, then the commutative diagram from Theorem 3.39 shows that those are consistently labelled by $(i_1^{r_{i_1}}, \ldots, i_t^{r_{i_t}})_0$ and $(i_1^{r_{i_1}}, \ldots, i_t^{r_{i_t}})_1$.

Clearly, the statement of Lemma 6.15 also holds with O_n replaced by $\mathrm{Pin}(V)$ and SO_n replaced by $\mathrm{Spin}(V)$.

Continuing the discussion of splitting conjugacy classes, we have the following proposition which describes the two half-spin representations on split and non-split classes. We speak of matrices of two endomorphisms of the same vector space being conjugate since this property is independent of the choice of basis.

Proposition 6.17. *Suppose that n is even. Let $\mathcal{C}$ be a unipotent conjugacy class of* $\mathrm{Pin}(V)$.

(i) If $\mathcal{C}$ does not split in $\mathrm{Spin}(V)$ *and $u \in \mathcal{C}$, then the matrices of $\Delta_n^+(u)$ and $\Delta_n^-(u)$ are conjugate.*

(ii) Suppose that $\mathcal{C}$ splits into two $\mathrm{Spin}(V)$*-classes $\mathcal{C}_0$ and $\mathcal{C}_1$ and let $u_0 \in \mathcal{C}_0$ and $u_1 \in \mathcal{C}_1$. Then the matrices of $\Delta_n^+(u_0)$ and $\Delta_n^-(u_1)$ are conjugate and the matrices $\Delta_n^+(u_1)$ and $\Delta_n^-(u_0)$ are conjugate.*

Proof. In the first case, we have $C_{\mathrm{Pin}(V)}(u) \nsubseteq \mathrm{Spin}(V)$ by Proposition 6.9. Hence, we find an element $p \in C_{\mathrm{Pin}(V)}(u) \setminus \mathrm{Spin}(V)$. By Proposition 5.7, the matrices of $\Delta_n^+(p^{-1}up) = \Delta_n^+(u)$ and $\Delta_n^-(u)$ are conjugate.

Now suppose that $\mathcal{C}$ splits into two $\mathrm{Spin}(V)$-classes $\mathcal{C}_0$ and $\mathcal{C}_1$. By Lemma 6.15, there is an element $p \in \mathrm{Pin}(V) \setminus \mathrm{Spin}(V)$ such that $u_0 = p^{-1}u_1p$. Again, Proposition 5.7 shows that the matrices of $\Delta_n^+(u_0)$ and $\Delta_n^-(u_1)$ are conjugate and that the matrices of $\Delta_n^+(u_1)$ and $\Delta_n^-(u_0)$ are conjugate. ☐

This directly translates into a statement on the Jordan blocks of the respective elements under the half-spin representations as two matrices are conjugate if and only if they have the same Jordan blocks (with according multiplicities).

6.3 Representatives for Unipotent Classes of Spin Groups

Throughout this section, we assume that $\operatorname{char} k \neq 2$. Let $n \in \mathbb{N}_{>0}$ and let $m := \lfloor \frac{n}{2} \rfloor$. Let V be a vector space over k of finite dimension n and suppose that Q is a nondegenerate quadratic form on V. In the sequel, a tuple $(i_1^0, i_2^{r_{i_2}}, \dots, i_t^{r_{i_t}})$ will be interpreted as $(i_2^{r_{i_2}}, \dots, i_t^{r_{i_t}})$.

In the last section, we have determined the unipotent conjugacy classes of the special orthogonal and spin groups. For our eventual computations, we would like to find a representative for each unipotent conjugacy class. Having in mind also the results from Section 5.3 that suggest an inductive approach for calculations with the spin representations, the idea is to construct these representatives inductively, using the map β from Theorem 5.23. We are looking for a way to obtain representatives for the unipotent classes of $\mathrm{Spin}(V)$ as images of elements of $\mathrm{Spin}(V') \times \mathrm{Spin}(V'')$ under β where $V', V'' \leq V$ are such that $V = V' \perp V''$. How this works precisely and to what extent this is possible is the topic of this section. These questions have not been studied in our references.

For unipotent elements and conjugacy classes of a product of algebraic groups, note the following:

Remark 6.18. Let G and H be algebraic groups and let $g \in G$ and $h \in H$. It clearly holds that $(g,h)^{G \times H} = g^G \times h^H$. Hence, the conjugacy classes of $G \times H$ are the products of conjugacy classes of G and H.

Moreover, the element $(g,h) \in G \times H$ is unipotent if and only if both the elements $g \in G$ and $h \in H$ are unipotent: If (g,h) is unipotent, then via the projections $G \times H \to G$ and $G \times H \to H$ it follows from Theorem 4.15 (iii) that g and h are unipotent. Conversely, if g and h are unipotent, then the morphisms of algebraic groups $G \to G \times H, g \mapsto (g,1)$ and $H \to G \times H, h \mapsto (1,h)$ and Theorem 4.15 show that also $(g,h) = (g,1)(1,h) = (1,h)(g,1)$ is unipotent.

We conclude that the unipotent conjugacy classes of $G \times H$ are precisely the products of unipotent conjugacy classes of G and H.

Now given a unipotent conjugacy class $\mathcal{C}$ of $\operatorname{Spin}(V)$, we would like to find an orthogonal decomposition $V = V' \perp V''$ and unipotent classes $\mathcal{U}$ of $\operatorname{Spin}(V')$ and $\mathcal{V}$ of $\operatorname{Spin}(V'')$ such that $\beta(\mathcal{U} \times \mathcal{V}) \subseteq \mathcal{C}$. Note that finding orthogonal decompositions is not hard: Since $\operatorname{char} k \neq 2$, the space V has an orthogonal basis by Theorem 2.11, so for each $1 \leq l < n$ there is an orthogonal decomposition $V = V' \perp V''$ with $\dim V' = l$. Hence, the problem reduces to "decomposing" the class $\mathcal{C}$ into two parts that correspond to unipotent classes of lower-dimensional spin groups.

Similarly as in the previous section, we first look at the special orthogonal group and then translate the results to the spin group. Here, we again work with the matrix group SO_n. In view of Theorem 5.23 and the above discussion on orthogonal decompositions, given a unipotent class $\mathcal{C}$ of SO_n, the corresponding problem is to find $1 \leq l < n$ and unipotent classes $\mathcal{U}$ of SO_l and $\mathcal{V}$ of SO_{n-l} such that $e(\mathcal{U} \times \mathcal{V}) \subseteq \mathcal{C}$ where e is the embedding of algebraic groups from Proposition 4.37.

Recall from the previous section that the unipotent classes of SO_n are in almost all cases determined by the Jordan normal forms of their elements. Now if $u \in \mathrm{SO}_l$ has Jordan normal form $\bigoplus_i J_i^{r_i}$ and $v \in \mathrm{SO}_{n-l}$ has Jordan normal form $\bigoplus_i J_i^{s_i}$, then the image of (u, v) under the embedding e has Jordan normal form $\bigoplus J_i^{r_i+s_i}$ by the definition of e. Given a unipotent class $\mathcal{C}$ of SO_n, this observation leads to the idea of decomposing the Jordan normal form of the elements of $\mathcal{C}$ into two pieces in a suitable way such that the pieces give rise to the desired classes $\mathcal{U}$ and $\mathcal{V}$. This approach in fact works for almost all unip classes of SO_n as the following propositions show:

Proposition 6.19. *Let $\mathcal{C} = (i_1^{r_{i_1}}, \dots, i_t^{r_{i_t}})$ be a unipotent conjugacy class of O_n with $\mathcal{C} \neq (n)$ if n is odd that does not split into two SO_n-classes. Depending on the parity of i_1, we define the following:*

- *if i_1 is odd, define $l := i_1$ and $\mathcal{U} := (i_1)$. Furthermore, if the unipotent O_{n-l}-class $(i_1^{r_{i_1}-1}, i_2^{r_{i_2}}, \dots, i_t^{r_{i_t}})$ splits into two SO_{n-l}-classes, define $\mathcal{V} := (i_1^{r_{i_1}-1}, i_2^{r_{i_2}}, \dots, i_t^{r_{i_t}})_0$. Otherwise, let $\mathcal{V} := (i_1^{r_{i_1}-1}, i_2^{r_{i_2}}, \dots, i_t^{r_{i_t}})$;*
- *if i_1 is even, put $l := 2i_1$, $\mathcal{U} := (i_1^2)_0$ and $\mathcal{V} := (i_1^{r_{i_1}-2}, i_2^{r_{i_2}}, \dots, i_t^{r_{i_t}})$.*

Then l is an integer with $1 \leq l < n$, $\mathcal{U}$ is a unipotent class of SO_l and $\mathcal{V}$ is a unipotent class of SO_{n-l} and we have $e(\mathcal{U} \times \mathcal{V}) \subseteq \mathcal{C}$, where $e\colon \mathrm{SO}_l \times \mathrm{SO}_{n-l} \hookrightarrow \mathrm{SO}_n$ is the embedding of algebraic groups from Proposition 4.37.

Proof. If i_1 is odd, then we have $i_1 < n$ as otherwise $\mathcal{C} = (n)$ with n odd which is not possible by assumption. If i_1 is even, then also r_{i_1} has to be even by Proposition 6.8. Furthermore, we must have $2i_1 < n$ as otherwise $\mathcal{C} = (i_1^2)$ would be a class that splits into two SO_n-classes by Proposition 6.10 which again would contradict the assumption. Hence, l satisfies $1 \leq l < n$.

Classes with labels of $\mathcal{U}$ and $\mathcal{V}$ exist in the respective special orthogonal groups by Proposition 6.8. Note that in case i_1 is even, the class $(i_1^{r_{i_1}-2}, i_2^{r_{i_2}}, \dots, i_t^{r_{i_t}})$ cannot split into two SO-classes as otherwise also $\mathcal{C}$ would. As discussed above, the elements of $e(\mathcal{U}\times\mathcal{V})$ have Jordan normal form $J_{i_1}^{r_{i_1}} \oplus \cdots \oplus J_{i_t}^{r_{i_t}}$ which shows that $e(\mathcal{U}\times\mathcal{V}) \subseteq \mathcal{C}$. □

We turn to the case of a class that splits into two SO_n-classes. Recall that this phenomenon occurs precisely for the n with $n \equiv 0 \bmod 4$ and that the two classes of SO_n emerging this way can not be canonically distinguished. We have the following similar statement:

Proposition 6.20. *Suppose that $n = 2m$ is even and that $n \equiv 0$ mod 4. Let $\mathcal{C} = (i_1^{r_{i_1}}, \dots, i_t^{r_{i_t}})$ be a unipotent conjugacy class of O_n with $\mathcal{C} \neq (m^2)$ that splits into two SO_n-classes $\mathcal{C}_0 = (i_1^{r_{i_1}}, \dots, i_t^{r_{i_t}})_0$ and $\mathcal{C}_1 = (i_1^{r_{i_1}}, \dots, i_t^{r_{i_t}})_1$. Define $l := 2i_1$, $\mathcal{U} := (i_1^2)$ and $\mathcal{V} := (i_1^{r_{i_1}-2}, i_2^{r_{i_2}}, \dots, i_t^{r_{i_t}})$.*

Then l is an integer with $1 \leq l < n$ and $\mathcal{U}$ and $\mathcal{V}$ are splitting unipotent classes of O_l and O_{n-l}, respectively, with the property that for each $d \in \mathbb{Z}_2$ we have $e(\mathcal{U}_d \times \mathcal{V}_d) \subseteq \mathcal{C}_0$ and $e(\mathcal{U}_{d+1} \times \mathcal{V}_d) \subseteq \mathcal{C}_1$ or vice versa, where $e\colon \mathrm{SO}_l \times \mathrm{SO}_{n-l} \hookrightarrow \mathrm{SO}_n$ is the embedding of algebraic groups from Proposition 4.37.

Proof. Since $\mathcal{C}$ splits into two SO_n-classes, all integers $i_1, \dots, i_t$ and $r_{i_1}, \dots, r_{i_t}$ must be even by Propositions 6.10 and 6.8. We have $2i_1 < n$ as otherwise $\mathcal{C} = (i_1^2) = (m^2)$ which is excluded by the assumption. The classes $\mathcal{U}$ and $\mathcal{V}$ exist and split in the special orthogonal group again by Propositions 6.10 and 6.8.

Let $d \in \mathbb{Z}_2$. Since the elements of $e(\mathcal{U}_d \times \mathcal{V}_d)$ are all conjugate and have Jordan normal form $J_{i_1}^{r_{i_1}} \oplus \cdots \oplus J_{i_t}^{r_{i_t}}$, we either have $e(\mathcal{U}_d \times \mathcal{V}_d) \subseteq \mathcal{C}_0$ or $e(\mathcal{U}_d \times \mathcal{V}_d) \subseteq \mathcal{C}_1$. Assume without loss of generality that $e(\mathcal{U}_d \times \mathcal{V}_d) \subseteq \mathcal{C}_0$. We show that then $e(\mathcal{U}_{d+1} \times \mathcal{V}_d) \subseteq \mathcal{C}_1$.

For the sake of a contradition, assume that $e(\mathcal{U}_{d+1} \times \mathcal{V}_d) \subseteq \mathcal{C}_0$. Let $u_d \in \mathcal{U}_d$, $u_{d+1} \in \mathcal{U}_{d+1}$ and $v_d \in \mathcal{V}_d$. By Lemma 6.15, there is some $x \in \mathrm{O}_l \setminus \mathrm{SO}_l$ with $u_{d+1} = x u_d x^{-1}$. Now by Proposition 4.37, the embedding e is the restriction of an embedding of algebraic groups $\mathrm{O}_l \times \mathrm{O}_{n-l} \hookrightarrow \mathrm{O}_n$ which we will also denote by e. By injectivity, we have $e(x, 1) \in \mathrm{O}_n \setminus \mathrm{SO}_n$. Furthermore,

$$e(u_{d+1}, v_d) = e(x,1) e(u_d, v_d) e(x,1)^{-1} \in \mathcal{C}_0 = e(u_d, v_d)^{\mathrm{SO}_n},$$

so that there is $y \in \mathrm{SO}_n$ with $y^{-1} e(x,1) \in C_{\mathrm{O}_n}(e(u_d, v_d))$. But the O_n-conjugacy class $e(u_d, v_d)^{\mathrm{O}_n} = \mathcal{C}$ splits into two SO_n-classes which means that $C_{\mathrm{O}_n}(e(u_d, v_d)) \subseteq \mathrm{SO}_n$ by Proposition 6.9. It follows that $e(x,1) \in \mathrm{SO}_n$ which is a contradiction. Hence, we must have $e(\mathcal{U}_{d+1} \times \mathcal{V}_d) \subseteq \mathcal{C}_1$. □

In Propositions 6.19 and 6.20 we have excluded two types of conjugacy classes in the assumptions which was necessary for the proofs to work. In fact, these two types of classes can not be obtained via e from a product of two conjugacy classes, as can be seen by looking at the Jordan block structure:

If $1 \leq l < n$ and the elements of $\mathcal{U} \subseteq \mathrm{SO}_l$ have Jordan normal form $\bigoplus_i J_i^{r_i}$ and the elements of $\mathcal{V} \subseteq \mathrm{SO}_{n-l}$ have Jordan normal form $\bigoplus_i J_i^{s_i}$ then the elements of $e(\mathcal{U} \times \mathcal{V})$ have Jordan normal form $\bigoplus_i J_i^{r_i+s_i}$ which consists of multiple blocks. The elements of the class (n) for odd n have Jordan normal form J_n, so no element of (n) is in the image of $e\colon \mathrm{SO}_l \times \mathrm{SO}_{n-l} \hookrightarrow \mathrm{SO}_n$ when $1 \leq l < n$. If $n = 2m \equiv 0 \bmod 4$, the only possibility to decompose the matrix J_m^2 as a direct sum of smaller block diagonal matrices is given by $J_m \oplus J_m$. But here m is even, so by Proposition 6.8 there are no elements in SO_m with Jordan normal form J_m.

However, in these two exceptional cases, we can explicitly compute a representative for the respective unipotent class. Suppose that n is odd. Then by Proposition 6.14, the class (n) is the class of regular unipotent elements of SO_n. Hence, a representative for it is given by a regular unipotent element. Such an element may be computed with Theorem 6.4 and the descriptions of the root subgroups from Theorem 4.41.

A similar approach works for the other exceptional case:

Proposition 6.21. *Suppose that $n = 2m$ is even. Then, with notation as in Theorem 4.40, the element*

$$x := \prod_{i=1}^{m-1} u_{\varepsilon_i - \varepsilon_{i+1}}(1) = \prod_{i=1}^{m-1} (I_{2m} + E_{i,i+1} - E_{2m-i,2m+1-i}) \in \mathrm{SO}_n$$

is unipotent, with Jordan normal form J_m^2.

Proof. We prove by induction on $l \leq m-1$ that

$$P_l := \prod_{i=1}^{l} (I_{2m} + E_{i,i+1} - E_{2m-i,2m+1-i}) = I_{2m} + \sum_{i=1}^{l} \sum_{j=i+1}^{l+1} E_{i,j} - \sum_{i=1}^{l} E_{2m-i,2m+1-i}.$$

For $l = 1$, the left hand side and right hand side both equal $I_{2m} + E_{1,2} - E_{2m-1,2m}$, so the claim holds. Now suppose that $l > 1$. Recall from Example 1.2 that $E_{i,j}E_{r,s} = \delta_{jr}E_{i,s}$. This and induction give

$$\begin{aligned} P_l &= P_{l-1}(I_{2m} + E_{l,l+1} - E_{2m-l,2m+1-l}) \\ &= I_{2m} + \sum_{i=1}^{l-1} \sum_{j=i+1}^{l} E_{i,j} - \sum_{i=1}^{l-1} E_{2m-i,2m+1-i} + E_{l,l+1} \\ &\quad + \left(\sum_{i=1}^{l-1} \sum_{j=i+1}^{l} E_{i,j} \right) E_{l,l+1} - E_{2m-l,2m+1-l}. \end{aligned}$$

We compute that

$$\left(\sum_{i=1}^{l-1} \sum_{j=i+1}^{l} E_{i,j} \right) E_{l,l+1} = \sum_{i=1}^{l-1} E_{i,l}E_{l,l+1} = \sum_{i=1}^{l-1} E_{i,l+1}$$

and conclude

$$\begin{aligned} P_l &= I_{2m} + \sum_{i=1}^{l-1} \sum_{j=i+1}^{l} E_{i,j} - \sum_{i=1}^{l-1} E_{2m-i,2m+1-i} + \sum_{i=1}^{l} E_{i,l+1} - E_{2m-l,2m+1-l} \\ &= I_{2m} + \sum_{i=1}^{l} \sum_{j=i+1}^{l+1} E_{i,j} - \sum_{i=1}^{l} E_{2m-i,2m+1-i}, \end{aligned}$$

as claimed. We thus have

$$\begin{aligned} x &= P_{m-1} \\ &= I_{2m} + \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} E_{i,j} - \sum_{i=1}^{m-1} E_{2m-i,2m+1-i} \\ &= \begin{pmatrix} 1 & \cdots & 1 & & & & \\ & \ddots & \vdots & & & & \\ & & 1 & & & & \\ & & & 1 & -1 & & \\ & & & & \ddots & \ddots & \\ & & & & & 1 & -1 \\ & & & & & & 1 \end{pmatrix}, \end{aligned}$$

a block diagonal matrix with blocks

$$A := \begin{pmatrix} 1 & \cdots & 1 \\ & \ddots & \vdots \\ & & 1 \end{pmatrix} \qquad \text{and} \qquad B := \begin{pmatrix} 1 & -1 & & \\ & \ddots & \ddots & \\ & & 1 & -1 \\ & & & 1 \end{pmatrix},$$

both of size $m \times m$. Now it is easily seen that the order of $A - I_m$ and $B - I_m$ is m which means that the minimal polynomial of both A and B is $(X-1)^m$. But then a block of size m must occur in the Jordan normal form of both A and B, that is, A and B have Jordan normal form J_m. We conclude that $x = A \oplus B$ has Jordan normal form J_m^2. □

Thus, we obtain representatives for all unipotent classes of SO_n. We now translate these results to the spin group.

Remark 6.22. Let $\mathcal{C}$ be a unipotent conjugacy class of SO_n and suppose that there are $1 \leq l < n$ and unipotent conjugacy classes $\mathcal{U}$ of SO_l and $\mathcal{V}$ of SO_{n-l} such that $e(\mathcal{U} \times \mathcal{V}) \subseteq \mathcal{C}$ where $e\colon \mathrm{SO}_l \times \mathrm{SO}_{n-l} \hookrightarrow \mathrm{SO}_n$ is the embedding of algebraic groups from Proposition 4.37.

Let $\hat{\mathcal{C}}$ be the unipotent conjugacy class of $\mathrm{Spin}(V)$ that corresponds to $\mathcal{C}$ under the bijection that is induced by the isogeny $\rho\colon \mathrm{Spin}(V) \to \mathrm{SO}(V) \cong \mathrm{SO}_n$ (cf. Proposition

6.6). Since $\operatorname{char} k \neq 2$, Theorem 2.11 shows that there are subspaces $V', V'' \leq V$ with $\dim V' = l$ and $V = V' \perp V''$. Let $\hat{\mathcal{U}}$ and $\hat{\mathcal{V}}$ be the unipotent conjugacy classes of $\operatorname{Spin}(V')$ respectively $\operatorname{Spin}(V'')$ that correspond to $\mathcal{U}$ and $\mathcal{V}$ under the respective bijections between sets of unipotent conjugacy classes.

We claim that $\beta(\hat{\mathcal{U}} \times \hat{\mathcal{V}}) \subseteq \hat{\mathcal{C}}$ where β is the map from Theorem 5.23. To see this, recall from the theorem just quoted that there is a commutative diagram

$$\begin{tikzcd}
\operatorname{Spin}(V') \times \operatorname{Spin}(V'') \arrow[r, "\beta"] \arrow[d, "\rho' \times \rho''"'] & \operatorname{Spin}(V) \arrow[d, "\rho"] \\
\operatorname{SO}(V') \times \operatorname{SO}(V'') \arrow[r, hook, "e"'] & \operatorname{SO}(V)
\end{tikzcd}$$

of morphisms of algebraic groups (we use the same notation for the respective objects related to $\operatorname{SO}(V)$ and SO_n).

Let $\hat{u} \in \hat{\mathcal{U}}$ and $\hat{v} \in \hat{\mathcal{V}}$. By the definition of the bijections between the sets of conjugacy classes, we have $\rho'(\hat{u}) \in \mathcal{U}$ and $\rho''(\hat{v}) \in \mathcal{V}$. Since $e(\mathcal{U} \times \mathcal{V}) \subseteq \mathcal{C}$, the diagram shows that $\rho(\hat{u}\hat{v}) = (\rho \circ \beta)(\hat{u}, \hat{v}) \in \mathcal{C}$. Hence, under the bijection induced by ρ, the classes $(\hat{u}\hat{v})^{\operatorname{Spin}(V)}$ and $\hat{\mathcal{C}}$ get both mapped to $\mathcal{C}$, whence $(\hat{u}\hat{v})^{\operatorname{Spin}(V)} = \hat{\mathcal{C}}$. In particular, we have $\beta(\hat{u}, \hat{v}) = \hat{u}\hat{v} \in \hat{\mathcal{C}}$ which shows that $\beta(\hat{\mathcal{U}} \times \hat{\mathcal{V}}) \subseteq \hat{\mathcal{C}}$.

Together with Remark 6.16, this shows that Propositions 6.19 and 6.20 remain valid in the context of spin groups. One has to add an orthogonal decomposition $V = V' \perp V''$ as above and appropriately replace orthogonal groups by pin groups, special orthogonal groups by spin groups and e by β.

The exceptional cases can be treated analogously. For this, let in the following $V = U \oplus W$ respectively $V = (U \oplus W) \perp \operatorname{span}(z)$ be a Lagrangian decomposition of V with respect to bases $(u_1, \ldots, u_m)$ of U and $(w_1, \ldots, w_m)$ of W. Then the respective representatives are as follows:

Corollary 6.23. *Suppose that* $\dim V = 2m + 1$ *is odd. Then the element*

$$x := (1 + zu_m) \prod_{i=1}^{m-1} (1 + u_i w_{i+1}) \in \operatorname{Spin}(V)$$

is regular unipotent. In particular, $x \in (n)$.

Proof. With notation as in Theorem 4.58, one has that

$$\hat{\Delta} := \{ \widehat{\varepsilon_i} - \widehat{\varepsilon_{i+1}} \mid 1 \leq i \leq m-1 \} \cup \{ \widehat{\varepsilon_m} \},$$

is a basis for the root system $\hat{R}$ of $\operatorname{Spin}(V)$ (this works analogously as for SO_n, cf. Theorem 4.41). Hence, by Theorem 6.4, the element

$$u_{\widehat{\varepsilon_m}}(1)\prod_{i=1}^{m-1} u_{\widehat{\varepsilon_i}-\widehat{\varepsilon_{i+1}}}(1) = x \in \operatorname{Spin}(V)$$

is regular unipotent. By Proposition 6.14 and Remark 6.16 we have $x \in (n)$. ☐

Corollary 6.24. *Suppose that* $\dim V = 2m$ *is even. Then the element*

$$x := \prod_{i=1}^{m-1}(1 + u_i w_{i+1}) \in \operatorname{Spin}(V)$$

is unipotent and contained in the class (m^2) *of* $\operatorname{Pin}(V)$*.*

Proof. We use notation as in Theorems 4.57 and 4.40 and the same notation for the root subgroups of SO_n and $\mathrm{SO}(V)$. By Proposition 4.59 we have

$$\rho(x) = \rho\left(\prod_{i=1}^{m-1} u_{\widehat{\varepsilon_i}-\widehat{\varepsilon_{i+1}}}(1)\right) = \prod_{i=1}^{m-1} u_{\varepsilon_i-\varepsilon_{i+1}}(1) \in \mathrm{SO}(V).$$

The claim follows from Proposition 6.21 and Remark 6.16. ☐

7 Jordan Blocks of Images of Unipotent Elements under the Spin and Half-Spin Representations

Throughout this chapter, we assume that k is an algebraically closed field of characteristic different from 2. We write $p := \operatorname{char} k$. Let $n \in \mathbb{N}_{>0}$ and let $m := \lfloor \frac{n}{2} \rfloor$. Let V be a vector space over k of finite dimension n and suppose that Q is a nondegenerate quadratic form on V.

Recall that our main objective is to compute the Jordan blocks of the images of the unipotent elements of the spin group under the spin and half-spin representations. In this chapter, we now present an algorithm that solves this problem. It is based on our results from Chapters 4, 5 and 6 and is described in Section 7.1. In Section 7.2 we state the computational results that we have obtained in low dimensions and further prove some theoretical statements related to these results.

7.1 The Algorithm

In this section, we describe our approach to computing the Jordan blocks of unipotent elements of spin groups under the spin and half-spin representations and explain why the resulting algorithm is correct. We illustrate our procedure by explicitly computing the blocks in low dimensions.

Before starting with the description of our algorithm, we make a few observations and introduce and explain our notation.

- By Theorems 4.33 and 4.47, the results that we obtain do not depend on the chosen quadratic form but only on the dimension of the underlying vector space. For this reason, we have chosen any quadratic form on V and omit it in the notation. We speak of $\mathrm{Spin}(V)$ as the spin group in dimension $n = \dim V$.
- Since conjugate matrices have the same Jordan blocks, the Jordan block structure under the respective representations is constant on conjugacy classes. Thus, it suffices to consider the unipotent conjugacy classes of the spin group. For these classes, we use the labels from Remark 6.16. We will speak of the (Jordan) blocks of a unipotent conjugacy class under a representation.

- If u is a unipotent element of $\mathrm{Spin}(V)$, then its image under the spin representation resp. a half-spin representation is a unipotent element of the corresponding general linear group by Theorem 4.15 since Δ_n and $\Delta_n^{\pm}$ are rational representations (cf. Propositions 5.6 and 5.11). Hence, by Lemma 4.13 (i), all eigenvalues of the image of u are 1 which means that its Jordan normal form only consits of blocks for the eigenvalue 1.
- If the elements of a unipotent conjugacy class under the spin representation resp. a half-spin representation have Jordan normal form $J_{i_1}^{r_{i_1}} \oplus \cdots \oplus J_{i_t}^{r_{i_t}}$, then we use the notation $i_1^{r_{i_1}}, \ldots, i_t^{r_{i_t}}$ to denote the Jordan blocks of this class. This is also the notation used in [Law95].
- In even dimension, it suffices to give the blocks of a unipotent conjugacy class under one of the half-spin representations as the blocks under the other half-spin representation can be derived from the former ones using Proposition 6.17. Furthermore, given the blocks of a class under one half-spin representation, it is possible to compute the blocks of this class under the spin representation via the relation $\Delta_n = \Delta_n^+ \oplus \Delta_n^-$ (cf. Proposition 5.6).
- If $\mathcal{C}$ is a unipotent class of $\mathrm{Pin}(V)$ that splits into two $\mathrm{Spin}(V)$-classes $\mathcal{C}_0$ and $\mathcal{C}_1$, then these two classes can not be distinguished canonically. Therefore, we write down the results for the classes $\mathcal{C}_0$ and $\mathcal{C}_1$ under the label of the class $\mathcal{C}$, in any order.

  Then by Proposition 6.17, one of the results gives the blocks of $\mathcal{C}_0$ under Δ_n^+ and simultaneously of $\mathcal{C}_1$ under Δ_n^- and the other result gives the blocks of $\mathcal{C}_1$ under Δ_n^+ and simultaneously of $\mathcal{C}_0$ under Δ_n^-. Note that with this notation, it does not matter for which of the two half-spin representations we give the Jordan blocks.
- By definition of the spin and half-spin representations (cf. Remark 5.2 and the subsequent definitions) and Corollary 3.40 and Lemma 3.19 (iii), the coordinates of the image of an element $x \in \mathrm{Spin}(V)$ under the spin representation resp. a half-spin representation can be chosen in the prime field of k. This shows that its Jordan blocks only depend on the characteristic p of k and not on the precise field itself. Moreover, this observation lays the foundation for computer calculations.

The problem of computing all unipotent classes of the spin group has been solved in Section 6.2. Thus, we only need to worry about the Jordan blocks of a given class.

Suppose that $\mathcal{C}$ is a unipotent conjugacy class of $\mathrm{Spin}(V)$. Clearly, the blocks of $\mathcal{C}$ under equivalent representations are the same. In view of the results from Section 5.3, this leads to the idea of trying to find classes of lower-dimensional spin groups whose product maps into $\mathcal{C}$ under the map β from Theorem 5.23, in order to eventually employ a recursive algorithm. To what extent it is possible to find such classes and how to deal with the exceptional cases, has been studied in Section 6.3.

We now explicitly describe and explain the procedure for computing the Jordan blocks of a unipotent class that is based on the above ideas. We do this in a text form rather than in pseudocode in order to have easier notation and to be able to justify all steps right away since the occurring cases are quite different.

The procedure has been implemented in the computer algebra system `GAP` and has been used to compute the results displayed in Tables 7.1 and 7.2. In the descripition of the algorithm, we give references at the appropriate places to the corresponding functions from our `GAP`-code in the Appendix.

Algorithm 7.1. If $n = 1$, then we have only one unipotent conjugacy class (1) of $\mathrm{Spin}(V)$. It clearly has just one Jordan block of size 1 under Δ_1. Now suppose that $n > 1$. Working with an inductive approach, we assume that the blocks for all unipotent conjugacy classes of the spin groups in dimensions lower than n have been computed and stored.

Since we save the results under the labels of the classes of the pin group, it is more convenient to start with a class of $\mathrm{Pin}(V)$. So let $\mathcal{C}$ be a unipotent conjugacy class of $\mathrm{Pin}(V)$. There are four cases:

Case 1: n is odd and $\mathcal{C} = (n)$. Let $V = (U \oplus W) \perp \mathrm{span}(z)$ be a Lagrangian decomposition of V with respect to bases $(u_1, \ldots, u_m)$ of U and $(w_1, \ldots, w_m)$ of W. Then by Corollary 6.23, the element

$$x := (1 + zu_m) \prod_{i=1}^{m-1} (1 + u_i w_{i+1}) \in \mathrm{Spin}(V)$$

is a representative for the class $\mathcal{C}$. We may concretely compute how $\Delta_n(x)$ acts on $\bigwedge W$ and from this derive the Jordan blocks of x under the spin representation (which are also the Jordan blocks of $\mathcal{C}$), as follows: By definition of the spin representation and with notation as in Lemma 3.19, we have

$$\Delta_n(x) = (\mathrm{id}_{\bigwedge W} + \eta_1 \iota_{u_m}) \prod_{i=1}^{m-1} (\mathrm{id}_{\bigwedge W} + \iota_{u_i} \lambda_{w_{i+1}}) \in \mathrm{GL}(\textstyle\bigwedge W).$$

The matrix of $\Delta_n(x)$ with respect to the basis of $\bigwedge W$ that is induced by the basis $(w_1, \ldots, w_m)$ of W (cf. Proposition 1.36 (iv)) can easily be computed with Lemma 3.19 (iii).

Note that this is a computation that takes places solely in the prime field of k, so can easily be done by a computer. Moreover, it is not necessary to compute a Lagrangian decomposition of V; it suffices to create labels for each basis vector of $\bigwedge W$ and with these and the formulae from Lemma 3.19 (iii) compute the matrices of the endomorphisms of $\bigwedge W$ that appear in the expression for $\Delta_n(x)$ from above. This is done in the functions `matrix_of_z`, `matrix_of_w_j` and `matrix_of_u_j` for the endomorphisms η_1, λ_{w_j} and ι_{u_j}, respectively, see the Appendix.

Having computed the matrix of $\Delta_n(x)$, it only remains to determine its Jordan normal form and read off the Jordan blocks which are then the Jordan blocks of the unipotent class $\mathcal{C}$. The Jordan blocks of a unipotent matrix are computed with the function `jordan_unip`. The whole procedure described above that computes the Jordan blocks of the class (n) is carried out in the function `bigblock`.

Case 2: $n \equiv 0 \bmod 4$ *and* $\mathcal{C} = (m^2)$ *where* $m = \frac{n}{2}$. Let $V = U \oplus W$ be a Lagrangian decomposition with respect to bases $(u_1, \ldots, u_m)$ of U and $(w_1, \ldots, w_m)$ of W. Then by Corollary 6.24, the element

$$x := \prod_{i=1}^{m-1} (1 + u_i w_{i+1}) \in \mathrm{Spin}(V)$$

is a representative for the class $\mathcal{C}$ of $\mathrm{Pin}(V)$. As in case 1, we can easily compute the matrix of $\Delta_n(x)$ with respect to the basis of $\bigwedge W$ that is induced by the basis $(w_1, \ldots, w_m)$ of W.

Ordering the basis vectors of $\bigwedge W$ in such a way that the first 2^{m-1} vectors form a basis of $(\bigwedge W)_0$ and the other basis vectors form a basis of $(\bigwedge W)_1$, this matrix will be a block diagonal matrix whose two blocks are the matrices of $\Delta_n^+(x)$ and $\Delta_n^-(x)$, which makes it easy to read off the latter matrices. Matrices of u_i and w_{i+1} for $i = 1, \ldots, m-1$ with respect to such an ordering are computed with the functions `block_matrix_of_u_j` and `block_matrix_of_w_j`.

Thus, we can compute the Jordan blocks of x under Δ_n^+ and under Δ_n^-. This is the data that is stored under the label $\mathcal{C}$ (cf. the remarks at the beginning of the section).

Case 3: $\mathcal{C}$ *is not as in cases 1 and 2 and does not split into two* $\mathrm{Spin}(V)$*-classes.* By Remark 6.22, we can use Proposition 6.19 to compute unipotent classes $\mathcal{U}$ of $\mathrm{Spin}(V')$ and $\mathcal{V}$ of $\mathrm{Spin}(V'')$ such that $\beta(\mathcal{U} \times \mathcal{V}) \subseteq \mathcal{C}$ where $V = V' \perp V''$ with $1 \leq l := \dim V' < n$ and where β is the map from Theorem 5.23.

Note that since all spin groups in a given dimension are isomorphic (cf. Theorems 4.33 and 4.47), we do not explicitly need the orthogonal decomposition in the following, but only l and the class labels of $\mathcal{U}$ and $\mathcal{V}$ which are easy to compute. In our code, this is done by the function `tensor_decomp`.

Let $u \in \mathcal{U}$ and $v \in \mathcal{V}$, so that $x := \beta(u, v) \in \mathcal{C}$. We have two subcases:

(1) In either of the two cases from Theorem 5.27, the matrix of $\Delta_l(u) \otimes \Delta_{n-l}(v)$ is conjugate to the matrix of $\Delta_n(x)$ resp. $\Delta_n^+(x)$ (w.r.t. any bases), so we may use it to compute the Jordan blocks of x.

    By assumption, we know the Jordan blocks of u under Δ_l and of v under Δ_{n-l} (in even dimension, use Propositions 5.6 and 6.17 to compute those). Let J_u and J_v be the Jordan normal forms of $\Delta_l(u)$ and $\Delta_{n-l}(v)$, respectively. Then the Kronecker product $J_u \otimes J_v$ is conjugate to the matrix of $\Delta_n(x)$ resp. $\Delta_n^+(x)$. Thus, it only remains to compute the Jordan blocks of $J_u \otimes J_v$ which are then the Jordan blocks of $\mathcal{C}$. For this, we again use the function `jordan_unip`.

Note that in this step, it is desirable to have $\mathcal{U} = (1)$ whenever the class label of $\mathcal{C}$ contains a 1 since then $J_u \otimes J_v = J_v$ and the blocks of $\mathcal{C}$ can directly be read off from the results in dimension $n-1$, without any computations (this corresponds to Proposition 5.25). If possible, this will always be achieved by Proposition 6.19 and the corresponding function `tensor_decomp` by the way the classes are constructed.

(2) Suppose that we are in the case of Theorem 5.28. Then the matrix of

$$\left(\Delta_l^+(u) \otimes \Delta_{n-l}^+(v)\right) \oplus \left(\Delta_l^-(u) \otimes \Delta_{n-l}^-(v)\right)$$

is conjugate to the matrix of $\Delta_n^+(x)$. By the procedure from Proposition 6.19, the class $\mathcal{U}$ must stem from a splitting class $\mathcal{U}'$ of $\mathrm{Pin}(V')$ whereas $\mathcal{V}$ does not stem from such a class. This means that the blocks of $\Delta_{n-l}^+(v)$ and $\Delta_{n-l}^-(v)$ agree by Proposition 6.17, and are known by our assumption. Let $J_v^\pm$ be the matrix in Jordan normal form that has precisely these blocks.

Having computed the results in lower dimensions, we know the Jordan blocks of $\Delta_l^+(u)$ and $\Delta_l^-(u)$ in the sense that under the label $\mathcal{U}'$ we have stored two sets of Jordan blocks one of which are the blocks of $\Delta_l^+(u)$ and the other ones are the blocks of $\Delta_l^-(u)$. Let J_u^0 and J_u^1 be the two corresponding matrices in Jordan normal form. Now Regardless of which one is the Jordan normal form of $\Delta_l^+(u)$ and which is the Jordan normal form of $\Delta_l^-(u)$, the matrix

$$(J_u^0 \otimes J_v^\pm) \oplus (J_u^1 \otimes J_v^\pm) = (J_u^0 \oplus J_u^1) \otimes J_v^\pm$$

is conjugate to the matrix of $\Delta_n^+(x)$. Its Jordan blocks are the Jordan blocks of $\mathcal{C}$ (recall that we only compute the blocks for one half-spin representation).

Case 4: $\mathcal{C}$ is not as in cases 1 and 2 and splits into two $\mathrm{Spin}(V)$*-classes.* By Remark 6.22, proceeding as in Proposition 6.20, we obtain an integer $1 \leq l < n$ and labels for splitting unipotent classes $\mathcal{U}$ of $\mathrm{Pin}(V')$ and $\mathcal{V}$ of $\mathrm{Pin}(V'')$ such that for each $d \in \mathbb{Z}_2$ it holds that $\beta(\mathcal{U}_d \times \mathcal{V}_d) \subseteq \mathcal{C}_0$ and $\beta(\mathcal{U}_{d+1} \times \mathcal{V}_d) \subseteq \mathcal{C}_1$ or vice versa, where $V = V' \perp V''$ with $\dim V' = l$ and where β is the map from Theorem 5.23. For the computation of l and the labels for $\mathcal{U}$ and $\mathcal{V}$, see again the function `tensor_decomp` from the Appendix.

Let J_u^0 and J_u^1 be the Jordan block matrices with blocks saved under the label $\mathcal{U}$ and let J_v^0 and J_v^1 be the Jordan block matrices with blocks saved under the label $\mathcal{V}$. In addition, let $u_i \in \mathcal{U}_i$, $v_i \in \mathcal{V}_i$ and $x_i \in \mathcal{C}_i$ for all $i \in \{0,1\} = \mathbb{Z}_2$.

There is $d \in \mathbb{Z}_2$ such that J_u^0 is conjugate to the matrix of $\Delta_l^+(u_d)$ and J_u^1 is conjugate to the matrix of $\Delta_l^+(u_{d+1})$ and there is $e \in \mathbb{Z}_2$ sucht that J_v^0 is conjugate to the matrix of $\Delta_{n-l}^+(v_e)$ and J_v^1 is conjugate to the matrix of $\Delta_{n-l}^+(v_{e+1})$. Thus, by Theorem 5.28, Proposition 6.17 and the properties of $\mathcal{U}$ and $\mathcal{V}$, one of the two matrices

$$(J_u^0 \otimes J_v^0) \oplus (J_u^1 \otimes J_v^1) \qquad \text{and} \qquad (J_u^0 \otimes J_v^1) \oplus (J_u^1 \otimes J_v^0)$$

is conjugate to the matrix of $\Delta_n^+(x_0)$ and the other one is conjugate to the matrix of $\Delta_n^+(x_1)$. It remains to compute the Jordan blocks of those two matrices. This is the data that is stored under the label $\mathcal{C}$ (in any order).

The inductive approach used in the above procedure leads to the following recursive algorithm that solves the problem of determining the Jordan blocks of the unipotent classes of the spin group for any dimension:

Algorithm 7.2.

Input: A bound $B \in \mathbb{N}_{>0}$ and an integer p which is either zero or a prime number greater than 2

Output: For each dimension n up to B, a list containing all unipotent conjugacy classes of the spin group in dimension n and their Jordan blocks under the spin representation resp. a half-spin representation in characteristic p

Procedure:

```
Store the initial result that the class (1) of the spin group in dimension 1 has Jordan blocks 1.
for each dimension $n = 2, \dots, B$ do
    Compute the set $S$ of unipotent conjugacy classes of the spin group in dimension $n$ as in Example 6.12.
    for each unipotent class $\mathcal{C} \in S$ do
        Use Algorithm 7.1 to compute the Jordan blocks of $\mathcal{C}$ in characteristic $p$ and store these; if $\mathcal{C}$ stems from a splitting class $\mathcal{C}'$ of Pin($V$), use the class $\mathcal{C}'$ in Algorithm 7.1 and store the results under its label
```

This procedure is carried out in the function `all_results` which is the last one in the Appendix. The function only prints the results for the dimension that is given as the bound, but it can easily be modified to print the result for all smaller dimensions, if desired. Note that in the code and its output, we have assigned the two results for a splitting class of $\mathrm{Pin}(V)$ to the two classes of $\mathrm{Spin}(V)$ in some arbitrary order. This has only been done to execute the computations; since there is no canonical way to distinguish the two classes, there is further no way to assign one of the two results to one specific class.

In the remainder of this section, we explicitly compute the Jordan blocks of the unipotent classes of the spin groups in low dimensions, using the above algorithms. In some cases, we describe alternative possibilites to compute the Jordan blocks. The labels for the conjugacy classes in the respective examples have been read off from Table 6.1. The computational results we will obtain are displayed also in Table 7.1.

Example 7.3 (Dimension 2)**.** Suppose that $\dim V = 2$. The spin group then has only one unipotent class, with label (1^2). Proposition 6.19 applied to (1^2) gives $l = 1$ and $\mathcal{U} = \mathcal{V} = (1)$. Hence, in case 3.1 of Algorithm 7.1 we have $J_u = J_v = (1)$, so $J_u \otimes J_v = (1)$ and it follows that (1^2) has just one Jordan block of size 1 under Δ_2^+, in any characteristic. For this, we could have also used the fact that the neutral element $1 \in \mathrm{Spin}(V)$ is a representative of (1^2).

Example 7.4 (Dimension 3)**.** Suppose that $\dim V = 3$. Here, we have two unipotent classes (1^3) and (3). Since $1 \in \mathrm{Spin}(V)$ is a representative for (1^3) and the spin representation is 2-dimensional by Proposition 5.11, we see that the Jordan blocks of (1^3) are 1^2 without having to use the algorithms.

With notation as in Example 5.12 and by case 1 of Algorithm 7.1, the element $1+zu \in \mathrm{Spin}(V)$ is a representative for the class (3). By Example 5.12, since $zu = -uz$, it has matrix $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ with respect to the basis $(1, w)$ of $\bigwedge W$. We infer that the class (3) has one Jordan block under Δ_3, of size 2. Note that this is independent of $p = \operatorname{char} k$.

The blocks of (3) could have also been derived differently in this special case. Recall from Example 5.12 that the spin representation in dimension 3 is a bijective morphism of algebraic groups $\Delta_3\colon \mathrm{Spin}(V) \to \mathrm{SL}(\bigwedge W)$. Hence, by Proposition 6.6, it induces a bijection between the sets of unipotent conjugacy classes of $\mathrm{Spin}(V)$ and of $\mathrm{SL}(\bigwedge W)$.

Since by Lemma 4.13 (i) the unipotent elements of GL_n are contained in SL_n, Lemma 3.11 (ii) of [LS12] shows that the set of all possible Jordan normal forms of unipotent $(n \times n)$-matrices is a set of representatives for the unipotent classes of SL_n.

In our case, $\bigwedge W$ being 2-dimensional, the group $\mathrm{SL}(\bigwedge W)$ has two unipotent classes, consisting of the matrices with Jordan normal forms J_1^2 and J_2, respectively. Since (1^3) maps to the former class, the class (3) of $\mathrm{Spin}(V)$ has to map to the latter under the bijection induced by Δ_3. This means that the elements of (3) have Jordan normal form J_2 under the spin representation.

Example 7.5 (Dimension 4)**.** Suppose that $\dim V = 4$. This is the first time where splitting of a class of $\mathrm{Pin}(V)$ into two $\mathrm{Spin}(V)$-classes occurs. The algebraic group $\mathrm{Spin}(V)$ has the four unipotent conjugacy classes (1^4), $(2^2)_0$, $(2^2)_1$ and $(1,3)$. As before, we immediately get that the class (1^4) containing the neutral element has Jordan blocks 1^2 under Δ_4^+.

For $(1,3)$, Proposition 6.19 yields the classes $\mathcal{U} = (1)$ and $\mathcal{V} = (3)$ with $\beta(\mathcal{U} \times \mathcal{V}) \subseteq (1,3)$. By case 3.1 of Algorithm 7.1 and the results from Example 7.4, it follows that $(1,3)$ has just one Jordan block under Δ_4^+, of size 2.

To deal with the classes $(2^2)_0$ and $(2^2)_1$, we consider the corresponding class (2^2) of $\mathrm{Pin}(V)$. Then we are in case 2 of Algorithm 7.1 which states that $x := 1 + u_1 w_2 \in \mathrm{Spin}(V)$ is a representative for (2^2), where we use the notation from Example 5.10. Following that example, we compute that $\Delta_4(x)$ has the matrix

$$I_4 + \begin{pmatrix} 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0\\ 0 & 0 & -1 & 0\\ 0 & 0 & 0 & 0\\ 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & -1 & 1 \end{pmatrix}$$

with respect to the basis $(1, w_1 \wedge w_2, w_1, w_2)$ of $\bigwedge W$ (recall that Δ_4 is the restriction of an algebra homomorphism). Since the Jordan normal form of $\left(\begin{smallmatrix}1 & 0\\ -1 & 1\end{smallmatrix}\right)$ is J_2 in any characteristic, the set comprising the blocks of $(2^2)_0$ and $(2^2)_1$ under one of the two half-spin representations is given by 1^2 and 2.

Similarly as in dimension 3, knowing the blocks of (1^4) and $(1,3)$, the blocks of $(2^2)_0$ and $(2^2)_1$ can also be derived from the fact that there is a bijective morphism of algebraic groups $(\Delta_4^+, \Delta_4^-)\colon \operatorname{Spin}(V) \to \mathrm{SL}_2 \times \mathrm{SL}_2$ (see Example 5.10), as follows: By Proposition 6.6, (Δ_4^+, Δ_4^-) induces a bijection between the sets of unipotent conjugacy classes of $\operatorname{Spin}(V)$ and of $\mathrm{SL}_2 \times \mathrm{SL}_2$. Let $\mathcal{U}_1$ be the unipotent class of SL_2 of elements with Jordan normal form J_1^2 and $\mathcal{U}_2$ be the class of elements with Jordan normal form J_2 (cf. Example 7.5). Then by Remark 6.18, the group $\mathrm{SL}_2 \times \mathrm{SL}_2$ has four unipotent classes, namely $\mathcal{U}_1 \times \mathcal{U}_1$, $\mathcal{U}_1 \times \mathcal{U}_2$, $\mathcal{U}_2 \times \mathcal{U}_1$ and $\mathcal{U}_2 \times \mathcal{U}_2$.

Taking Proposition 6.17 into account, we have seen that (1^4) maps to $\mathcal{U}_1 \times \mathcal{U}_1$ under the bijection induced by (Δ_4^+, Δ_4^-), and that $(1,3)$ maps to $\mathcal{U}_2 \times \mathcal{U}_2$. Looking at the remaining classes of $\mathrm{SL}_2 \times \mathrm{SL}_2$, we recover the results for the blocks of $(2^2)_0$ and $(2^2)_1$.

Example 7.6 (Dimension 5)**.** Suppose that $\dim V = 5$. Here, the spin group has the unipotent classes (1^5), $(1^2, 3)$, $(1, 2^2)$ and (5). For the first three classes, following case 3.1 of Algorithm 7.1, we obtain $\mathcal{U} = (1)$ in Proposition 6.19 for each class. Therefore, the results from dimension 4 yield that under Δ_5, the class (1^5) has blocks 1^4, the class $(1^2, 3)$ has blocks 2^2 and the class $(1, 2^2)$ has blocks $1^2, 2$. These results hold for all p as the ones for dimension 4 do.

Turning to the class (5), step 1 of Algorithm 7.1 states that a representative for it is given by the element $x := (1 + zu_2)(1 + u_1 w_2) \in \operatorname{Spin}(V)$, where we use the notation from Example 5.18. With the results from that example, we compute that the matrix of $\Delta_5(x)$ with respect to the basis $(1, w_1 \wedge w_2, w_1, w_2)$ of $\bigwedge W$ is given by

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & -1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{pmatrix}.$$

It has Jordan normal form J_4 in any characteristic, as one may see by computing a matrix that transforms it into Jordan normal form in characteristic 0.

As in the two previous examples, the results in dimension 5 are in accordance with the fact that by Example 5.18, the spin representation defines a bijective morphism of algebraic groups $\Delta_5\colon \operatorname{Spin}(V) \to \operatorname{Sp}(\bigwedge W) \cong \mathrm{Sp}_4$ (which is specific to dimension 5) and therefore induces a bijection between the corresponding sets of unipotent conjugacy classes. We refer to [LS12], Theorem 3.1 for a description of the unipotent classes of Sp_n.

7.2 Computational Results and Observations

In this section, we list the computational results that have been obtained from our algorithms from Section 7.1 for all dimensions up to 9. In view of these results there arise theoretical questions on the Jordan blocks of unipotent elements of spin groups some of which we answer in the following. Concretely, we explain the results in dimension 8 theoretically, give a few constraints for the Jordan blocks of unipotent elements and prove that for every dimension there exists a bound such that in all characteristics greater than this bound, the blocks of the unipotent elements in the given dimension are the same as in characteristic 0.

7.2.1 Dependence on Characteristic

In general, the Jordan blocks of a unipotent matrix depend on the characteristic of the underlying field. Consequently, so do our results. We investigate to which extent this is the case in a given dimension.

In cases 3 and 4 of Algorithm 7.1, the Jordan blocks of a unipotent class of $\mathcal{C}$ are determined by calculating the Jordan blocks of a Kronecker product of two Jordan block matrices J_i and J_j. Hence, we are highly interested in how the Jordan block structure of the product $J_i \otimes J_j$ looks like. It turns out that there is a recursive formula for this which depends on the characteristic of k (see [Sri64], Theorem 5) and therefore reflects the general observation made above. However, for large enough p, this formula always yields the same blocks as in characteristic 0:

Proposition 7.7. *Let $i, j \in \mathbb{N}_{>0}$ with $i \leq j$. Suppose that $p = 0$ or $p > i + j - 2$. Then the matrix $J_i \otimes J_j$ has Jordan normal form $\bigoplus_{l=1}^{i} J_{i+j-2l+1}$.*

Proof. See [Sri64], p. 678 and Corollary 6.1. □

This gives us the hope that – even though the results of Algorithm 7.1 will in general depend on the characteristic – also the Jordan blocks of the unipotent classes of $\mathrm{Spin}(V)$ remain the same for all p greater than a certain bound. In low dimensions, we make the following observations:

Proposition 7.8. *The Jordan blocks of the unipotent classes of* $\mathrm{Spin}(V)$ *are independent of the characteristic of k for* $\dim V \leq 8$. *If* $\dim V \geq 9$*, then there always exist a unipotent class $\mathcal{C}$ of* $\mathrm{Spin}(V)$ *and $p_1, p_2 \in \mathbb{P} \cup \{0\}$ such that the Jordan blocks of $\mathcal{C}$ are different in characteristics p_1 and p_2.*

Proof. In Examples 7.3, 7.4, 7.5 and 7.6 we have seen that the Jordan blocks of the unipotent classes of $\mathrm{Spin}(V)$ are independent of the characteristic of k for $\dim V \leq 5$. Thus, for the first claim, it only remains to treat dimensions six to eight.

As remarked in case 3.1 of Algorithm 7.1, if a unipotent class $\mathcal{C}$ of $\mathrm{Spin}(V)$ is of the form $(1^{r_1}, i_2^{r_{i_2}}, \ldots, i_t^{r_{i_t}})$, then its blocks in the output of the algorithm are the same as the blocks under the spin representation of the class $(1^{r_1-1}, i_2^{r_{i_2}}, \ldots, i_t^{r_{i_t}})$. Thus, for such classes, independence of the blocks of the characteristic will carry over from the lower dimension. This means that, starting with dimension 6, we only have to check that the results are the same in all characteristics for conjugacy classes of the form

$(i_1^{r_{i_1}}, \dots, i_t^{r_{i_t}})$ with $2 \leq i_1 < \cdots < i_t$. For this, we go through Algorithm 7.1 to find out the matrix of which eventually the Jordan normal form is computed, and check it has the same blocks for all p.

We illustrate this procedure in dimension 6. Here, the only class whose label does not contain a 1 is (3^2) (see Table 6.1). We are in case 3 of Algorithm 7.1 and Proposition 6.19 yields the classes $\mathcal{U} = \mathcal{V} = (3)$ with $\beta(\mathcal{U} \times \mathcal{V}) \subseteq (3^2)$. Let $x \in (3^2)$. As described in the algorithm and by the results from dimension 3, the matrix $J_2 \otimes J_2$ is conjugate to the matrix of $\Delta_6^+(x)$.

Proposition 7.7 shows that $J_2 \otimes J_2$ has Jordan normal form $J_1 \oplus J_3$ for $p = 0$ and $p > 2$, so in all possible characteristics (recall that we assume $\operatorname{char} k \neq 2$). As a consequence, (3^2) always has Jordan blocks $1, 3$ and the results in dimension 6 are independent of the characteristic. Analogously, one proceeds for dimensions 7 and 8.

Suppose now that $\dim V = 9$. With Algorithm 7.1 one computes that the class (9) of $\operatorname{Spin}(V)$ has Jordan blocks 5 and 11 in characteristic 0 and Jordan blocks 7 and 9 in characteristic 3. Hence, the claim holds for dimension 9. If $\dim V \geq 9$, consider $\mathcal{C} := (1^{\dim V - 9}, 9)$ which is a unipotent class of $\operatorname{Spin}(V)$ by Proposition 6.8 and Remark 6.16. Put $p_1 := 0$ and $p_2 := 3$. Define $l := 9$ and let $V', V'' \leq V$ with $V = V' \perp V''$ and $\dim V' = 9$. Then with notation as in Remark 5.29, $\mathcal{U} := (9)$ is a unipotent class of $\operatorname{Spin}(V')$ with $(\beta \circ e)(\mathcal{U}) \subseteq \mathcal{C}$ (which can be seen as usual by considering the corresponding classes of the special orthogonal group).

Set $j := 2^{\frac{n-10}{2}}$ if $n = \dim V$ is even and $j := 2^{\frac{n-9}{2}}$ if n is odd. Then Remark 5.29 shows that the Jordan blocks of $\mathcal{C}$ are 5^j and 11^j in characteristic $p_1 = 0$ and 7^j and 9^j in characteristic $p_2 = 3$. This finishes the proof. □

The fact that the blocks are independent of the characteristic for dimensions two up to six is also reflected in the respective bijective morphisms of algebraic groups from Remark 5.19 that are induced by the spin representations. Due to Proposition 6.6, these morphisms induce bijections between the respective sets of unipotent conjugacy classes, in any characteristic. See also the remarks at the end of Examples 7.4, 7.5 and 7.6.

For more insight in the results in dimension 8 and their independence of the characteristic, see Section 7.2.3.

We have seen that starting from dimension 9, the results will never be the same for all characteristics. We now investigate whether there is a limit to the dependence on $\operatorname{char} k$. We start by taking a detailed look at the situation in dimension 9.

Remark 7.9 (Dimension 9)**.** Suppose that $\dim V = 9$. By Proposition 7.8 and its proof, all classes of $\operatorname{Spin}(V)$ except possibly $(2^2, 5)$, (3^3) and (9) will have the same Jordan blocks in all characteristics. We now take a closer look at these three classes.

n	Class	Jordan blocks
1	(1)	1
2	(1^2)	1
3	(1^3)	1^2
	(3)	2
4	(1^4)	1^2
	$(1, 3)$	2
	(2^2)	1^2 2
5	(1^5)	1^4
	$(1^2, 3)$	2^2
	$(1, 2^2)$	$1^2, 2$
	(5)	4
6	(1^6)	1^4
	$(1^3, 3)$	2^2
	$(1^2, 2^2)$	$1^2, 2$
	$(1, 5)$	4
	(3^2)	$1, 3$
7	(1^7)	1^8
	$(1^4, 3)$	2^4
	$(1^3, 2^2)$	$1^4, 2^2$
	$(1^2, 5)$	4^2
	$(1, 3^2)$	$1^2, 3^2$
	$(2^2, 3)$	$1, 2^2, 3$
	(7)	$1, 7$

n	Class	Jordan blocks
8	(1^8)	1^8
	$(1^5, 3)$	2^4
	$(1^4, 2^2)$	$1^4, 2^2$
	$(1^3, 5)$	4^2
	$(1^2, 3^2)$	$1^2, 3^2$
	$(1, 2^2, 3)$	$1, 2^2, 3$
	$(1, 7)$	$1, 7$
	$(3, 5)$	$3, 5$
	(2^4)	$1^5, 3$ 2^4
	(4^2)	$1^3, 5$ 4^2

Table 7.1: Jordan blocks of the unipotent classes of the spin group in dimension n for $n \leq 8$. In these cases, the results hold for all characteristics, see Proposition 7.8

By case 3.1 of Algorithm 7.1, the Jordan blocks of $(2^2, 5)$ are the Jordan blocks of the matrix

$$(J_1^2 \oplus J_2) \otimes J_4 = (J_1 \otimes J_4) \oplus (J_1 \otimes J_4) \oplus (J_2 \otimes J_4) = J_4^2 \oplus (J_2 \otimes J_4).$$

From Proposition 7.7, it follows that the Jordan blocks of $(2^2, 5)$ are the same for $p = 0$ and all $p \geq 5$. With the analogous arguments, one obtains the same result for the class (3^3).

It remains to consider the class (9). Here, we cannot argue with Proposition 7.7 since the class cannot be decomposed into two smaller pieces (cf. the discussion after Proposition 6.20). Suppose that $\operatorname{char} k = 0$. By a calculation, one sees that there is a rational matrix $T \in \mathrm{GL}_{16}(\mathbb{Q})$ that transforms the matrix of the element $\Delta_9(x)$ from case 1 of Algorithm 7.1 into Jordan normal form such that the only prime factors appearing in denominators of entries of T and the determinant of T are 2 and 3. This shows that the class (9) has the same blocks as in characteristic 0 for all $p \geq 5$ since we may in the latter case use the same transformation matrix as in characteristic 0, but defined over the respective field.

We conclude that in dimension 9, the results for $p \geq 5$ are the same as for $p = 0$. See Table 7.2 for the precise blocks.

	Jordan blocks	
Class	$p \neq 3$	$p = 3$
(1^9)	1^{16}	1^{16}
$(1^6, 3)$	2^8	2^8
$(1^5, 2^2)$	1^8, 2^4	1^8, 2^4
$(1^4, 5)$	4^4	4^4
$(1^3, 3^2)$	1^4, 3^4	1^4, 3^4
$(1^2, 2^2, 3)$	1^2, 2^4, 3^2	1^2, 2^4, 3^2
$(1^2, 7)$	1^2, 7^2	1^2, 7^2
$(1, 3, 5)$	3^2, 5^2	3^2, 5^2
$(1, 2^4)$	1^5, 2^4, 3	1^5, 2^4, 3
$(1, 4^2)$	1^3, 4^2, 5	1^3, 4^2, 5
$(2^2, 5)$	3, 4^2, 5	3, 4^2, 5
(3^3)	2^4, 4^2	2^2, 3^4
(9)	5, 11	7, 9

Table 7.2: Jordan blocks of the unipotent classes of the spin group in dimension 9 for the different values of $2 \neq p = \operatorname{char} k$ (see Remark 7.9)

In the following theorem, we generalize the observation from the above remark. The proof uses the same reasoning that we employed in dimension 9.

Theorem 7.10. *Let $n = \dim V$. There exists a bound $B_n \in \mathbb{N}$ such that for each unipotent class of* $\operatorname{Spin}(V)$*, the blocks under the spin representation resp. a half-spin representation are the same for $p = 0$ and all $p \geq B_n$.*

Proof. We argue inductively. For $n \leq 8$ we can take $B_n = 0$ by Table 7.1. Suppose now that $n \geq 9$ and let $B_1, \dots, B_{n-1}$ be the bounds for the lower dimensions. Put $B' := \max(B_1, \dots, B_{n-1})$.

Note that in Algorithm 7.1, at most one of cases 1 and 2 may occur. Depending on the parity of n, let $\mathcal{C}$ be the class of $\operatorname{Pin}(V)$ appearing in case 1 or 2 of Algorithm 7.1 (if there is no such class, skip this step) and let $x \in \operatorname{Spin}(V)$ be a representative for $\mathcal{C}$. By Lemma 3.19 (iii), the matrix of $\Delta_n(x)$ can be chosen to have entries in the prime field of k. This means that in characteristic 0, there is a rational matrix T that transforms the matrix of $\Delta_n(x)$ into its Jordan normal form.

Let $B'' \in \mathbb{N}$ be such that all prime factors appearing in the denominators of entries of T and in the determinant of T are smaller than B''. Then for all $p \geq B''$, the Jordan normal form of $\Delta_n(x)$ in characteristic p is the same as that in characteristic 0 as we can use the same transformation matrix. Hence, the claim holds for the class $\mathcal{C}$, if the bound is defined to be at least B''.

We turn to the remaining conjugacy classes. Define

$$B_n := \max(B', B'', 2^{\frac{m}{2}+1} - 1)$$

where $m = \lfloor \frac{n}{2} \rfloor$. Let $p \geq B_n$ and let $\mathcal{C}'$ be a unipotent class of $\mathrm{Spin}(V)$. We show that the blocks of $\mathcal{C}'$ in characteristic p are the same as those in characteristic 0. As explained above, this is true if $\mathcal{C}' = \mathcal{C}$.

Suppose now that $\mathcal{C}' \neq \mathcal{C}$. By construction, for all classes of lower-dimensional spin groups the blocks in characteristic p are the same as those in characteristic 0. Cases 3 and 4 of Algorithm 7.1 show that the Jordan blocks of $\mathcal{C}'$ in characteristic p may be computed from a Kronecker product of block matrices that are made up of the Jordan blocks of classes of lower-dimensional spin groups. By the above, the matrices appearing in this Kronecker product are the same in characteristic p as in characteristic 0. We additionally note that these matrices have sizes i and j with $ij \leq 2^m$ due to the dimension of the spin representation (see Propositions 5.6 and 5.11). This implies $i + j \leq 2^{\frac{m}{2}+1}$.

We therefore have $p > i + j - 2$. In this situation, Proposition 7.7 shows that the Kronecker product involved in the computation of the Jordan blocks of $\mathcal{C}'$ has the same Jordan blocks in characteristic p as in characteristic 0. We conclude that the Jordan blocks of $\mathcal{C}'$ in characteristics p and 0 agree. ☐

7.2.2 Block Structure

In this section, we point out and explain two observations on the Jordan block structure of unipotent elements of spin groups.

For the first observation, recall from Section 5.1.2 that the images of the spin and half-spin representations are contained in the special orthogonal group if $n \equiv 0, 1, 7 \bmod 8$ and are contained in the symplectic group if $n \equiv 3, 4, 5 \bmod 8$. This imposes certain constraints on the possible block structure in the respective dimensions that we now explain.

Proposition 6.8 shows that in the Jordan normal form of a unipotent element of a special orthogonal group, even sized blocks have to occur with an even multiplicity. Consequently, in dimensions that have residue 0, 1 or 7 modulo 8, the unipotent classes of $\mathrm{Spin}(V)$ must have a block structure in which even sized blocks occur with an even multiplicity. Analogously one deduces from Corollary 3.6 (ii) of [LS12] on the Jordan block structure of unipotent elements of symplectic groups that in dimensions n with $n \equiv 3, 4, 5 \bmod 8$, the unipotent classes of $\mathrm{Spin}(V)$ must have a block structure in which odd sized blocks occur with an even multiplicity. This behaviour can also be observed in the block structures displayed in Table 7.1.

In the results in Tables 7.1 and 7.2 we notice that starting with dimension 7, no class of the spin group has Jordan normal form under the spin representation that consists of just one Jordan block. With the aid of the paper [TZ13], we now show that this observation remains true also for all larger dimensions.

Theorem 7.11. *Suppose that* $\dim V \geq 7$. *Then every unipotent conjugacy class of* $\mathrm{Spin}(V)$ *has at least two (not necessarily distinct) Jordan blocks under the spin representation resp. a half-spin representation.*

Proof. We do the proof for the case $\dim V$ even; the proof for odd dimension is analogous. By Tables 7.1 and 7.2, we may assume that $n = \dim V \geq 10$.

We start with an observation on the special linear group. Let $l \in \mathbb{N}_{>0}$ and let $u \in \mathrm{SL}_l$ have Jordan normal form J_l. Then by Proposition 3.7 (i) of [LS12] it holds that $\dim C_{\mathrm{GL}_l}(u) = l$. Since k is algebraically closed, we have $\mathrm{GL}_l = Z(\mathrm{GL}_l)\,\mathrm{SL}_l$ and therefore also $\mathrm{GL}_l = C_{\mathrm{GL}_l}(u)\,\mathrm{SL}_l$. Using the same arguments as in the proof of Lemma 6.13, one shows that $\dim C_{\mathrm{GL}_l}(u) = \dim \mathrm{GL}_l \,/\, \mathrm{SL}_l + \dim C_{\mathrm{SL}_l}(u)$ which gives $\dim C_{\mathrm{SL}_l}(u) = l - 1$.

It follows from Theorem 6.5 together with [LS12], Lemma 3.11 (ii) that the regular unipotent elements of SL_l are the ones that have Jordan normal form J_l.

Let now $V = U \oplus W$ be a Lagrangian decomposition. By its definition and Propositions 5.6 and 5.13, the half-spin representation Δ_n^+ is a morphism of algebraic groups

$$\Delta_n^+ \colon \mathrm{Spin}(V) \to \mathrm{SL}\big((\textstyle\bigwedge W)_0\big)$$

where $\dim(\bigwedge W)_0 = 2^{\frac{n}{2}-1}$. We are going to show that $\Delta_n^+(\mathrm{Spin}(V))$ does not contain a regular unipotent element of $\mathrm{SL}\big((\bigwedge W)_0\big)$. Then by the above, no Jordan normal form of the image of a unipotent element of $\mathrm{Spin}(V)$ under Δ_n^+ can consist of a single Jordan block, and the claim follows.

Put $G := \Delta_n^+(\mathrm{Spin}(V))$ and $H := \mathrm{SL}\big((\bigwedge W)_0\big)$. By Proposition 5.9, the half-spin representation $\Delta_n^+ \colon \mathrm{Spin}(V) \to G$ is an isogeny of connected algebraic groups. Hence, G is a semisimple algebraic group by Theorem 4.53 and [GLS97], Proposition 1.10.3. Furthermore, by [GM16], 1.3.11 and Remark 1.2.11, there is a bijection between the root systems of $\mathrm{Spin}(V)$ and G that sends bases to bases. In particular, the root system of G has rank $\frac{n}{2}$ due to Theorem 4.57.

We are in the situation that G is a proper closed semisimple subgroup of the simple algebraic group H which is exactly the setting of Theorem 1.4 of [TZ13]. Assume that G contains a regular unipotent element of H. Then as H is of type $A_{2^{\frac{n}{2}-1}-1}$ by Example 4.31, Theorem 1.4 of [TZ13] implies that G must be of type $C_{2^{\frac{n}{2}-2}}$. Since $\frac{n}{2} < 2^{\frac{n}{2}-2}$, this is a contradiction to the fact that the root system of G has rank $\frac{n}{2}$. □

7.2.3 Triality

Looking at the results displayed in Table 7.1, there seems to be a remarkable connection between the unipotent classes in dimension 8 and their Jordan blocks. In this section, we will provide a theoretical explanation for this behaviour. It is linked to a phenomenon called *triality*. We closely follow the exposition given in [Mei13], Section 3.6 for the constructions and only give the outlines of the proofs. See also [Che97], Chapter IV.

Throughout this section, let $\dim V = 8$. Let $V = U \oplus W$ be a Lagrangian decomposition of V with respect to bases $(u_1, \dots, u_4)$ of U and $(w_1, \dots, w_4)$ of W. Let C denote the Clifford algebra for (V, Q) and let Γ be the Clifford group. Recall from Remark 5.2 (a) that there is an isomorphism

$$\Phi_{U,W} \colon C \to \operatorname{End}(\textstyle\bigwedge W),\ U \oplus W \ni u + w \mapsto \iota_u + \lambda_w$$

of $\mathbb{Z}_2$-graded k-algebras where ι_u and λ_w are as in Lemma 3.19. As in Section 5.1.2 we use the notation $S := \bigwedge W$. By Proposition 1.36, $S = S_0 \oplus S_1$ is a $\mathbb{Z}_2$-graded k-algebra and we have $\dim S_i = 2^{4-1} = 8$ for $i = 0, 1$.

By Lemma 5.14 and Corollary 5.17, there is a nondegenerate symmetric bilinear form b on S that induces a nondegenerate quadratic form $q \colon S \to k,\ s \mapsto \frac{1}{2} b(s, s)$. Furthermore, the restrictions $q_0 := q\big|_{S_0}$ and $q_1 := q\big|_{S_1}$ are nondegenerate and have the property that the image of Δ_8^+ is contained in $\mathrm{SO}(S_0, q_0)$ and the image of Δ_8^- is contained in $\mathrm{SO}(S_1, q_1)$. We thus have three rational representations

$$\begin{aligned} \rho \colon\ & \mathrm{Spin}(V) \to \mathrm{SO}(V, Q),\ x \mapsto (v \mapsto x v x^{-1}), \\ \Delta_8^+ \colon\ & \mathrm{Spin}(V) \to \mathrm{SO}(S_0, q_0),\ x \mapsto \Phi_{U,W}(x)\big|_{S_0}, \\ \Delta_8^- \colon\ & \mathrm{Spin}(V) \to \mathrm{SO}(S_1, q_1),\ x \mapsto \Phi_{U,W}(x)\big|_{S_1} \end{aligned}$$

of $\mathrm{Spin}(V)$ which are all of dimension 8. By Theorem 3.39 and Proposition 5.9, they have pairwise distinct kernels, so they are pairwise non-equivalent. Looking to find a connection between these representations, we define $\Omega := V \oplus S_0 \oplus S_1 = V \oplus S$ and

$$\mathcal{Q} \colon \Omega \to k,\ (v, s_0, s_1) \mapsto Q(v) + q_0(s_0) + q_1(s_1).$$

It is easy to see that $\mathcal{Q}$ is a quadratic form on Ω and one may show that it is again nondegenerate, see p. 44 of [EKM08]. We clearly have a morphism of algebraic groups

$$\theta \colon \mathrm{Spin}(V) \to \mathrm{SO}(\Omega, \mathcal{Q}),\ x \mapsto \rho(x) \oplus \Delta_8^+(x) \oplus \Delta_8^-(x)$$

which is injective by Proposition 5.6. We define a map

$$C_\Omega \colon \Omega \to k,\ (v, s_0, s_1) \mapsto b(\Phi_{U,W}(v) s_0, s_1).$$

Let $x \in \mathrm{Spin}(V)$ and $\omega = (v, s_0, s_1) \in \Omega$. Then by definition of the half-spin representations and Corollary 5.17 (i) it holds that

$$\begin{aligned} C_\Omega(\theta(x)\omega) &= C_\Omega(\rho_x(v), \Delta_8^+(x)s_0, \Delta_8^-(x)s_1) \\ &= b(\Phi_{U,W}(xvx^{-1})\Phi_{U,W}(x)s_0, \Phi_{U,W}(x)s_1) \\ &= b(\Phi_{U,W}(x)\Phi_{U,W}(v)s_0, \Phi_{U,W}(x)s_1) \\ &= b(\Phi_{U,W}(v)s_0, s_1) \\ &= C_\Omega(\omega). \end{aligned}$$

Conversely, every element of $\mathrm{SO}(\Omega, \mathcal{Q})$ that preserves C_Ω and the subspaces V, S_0 and S_1 is of the form $\theta(x)$ for a unique $x \in \mathrm{Spin}(V)$:

Lemma 7.12. *Suppose that* $f \in \mathrm{SO}(\Omega, \mathcal{Q})$ *is an isometry that satisfies* $f(V) \subseteq V$, $f(S_0) \subseteq S_0$ *and* $f(S_1) \subseteq S_1$ *and has the property that* $C_\Omega(f(\omega)) = C_\Omega(\omega)$ *for all* $\omega \in \Omega$. *Then there is a unique* $x \in \mathrm{Spin}(V)$ *such that* $f = \theta(x)$.

Proof. Uniqueness is clear by injectivity of θ. By assumption, we have $f\big|_S \in \mathrm{End}(S)_0$. Furthermore, by Lemma 2.22, this endomorphism is invertible. Hence, as $\Phi_{U,W}$ is a $\mathbb{Z}_2$-graded isomorphism, there is an element $x \in C_0^\times$ with $f\big|_S = \Phi_{U,W}(x)$. We are going to show that x is an element of $\mathrm{Spin}(V)$ that has the desired property.

To prove that $x \in \Gamma$, we need to ensure that $xvx^{-1} \in V$ for all $v \in V$. By Proposition 2.32, it suffices to check this for nonsingular vectors. So let $v \in V$ with $Q(v) \neq 0$. From the assumptions on f, one obtains by a lengthy calculation that

$$\Phi_{U,W}\big(f(v)\big) = f\big|_S \circ \Phi_{U,W}(v) \circ (f\big|_S)^{-1} \in \mathrm{End}(S),$$

see [Mei13], Lemma 3.3. Since x satisfies $f\big|_S = \Phi_{U,W}(x)$, this equation implies that $\Phi_{U,W}\big(f(v)\big) = \Phi_{U,W}(xvx^{-1})$. By injectivity of $\Phi_{U,W}$, we must have $xvx^{-1} = f(v) \in V$. Consequently, $x \in \Gamma$. Note that $xvx^{-1} = f(v)$ holds for all $v \in V$ by linearity.

Let $\omega = (v, s_0, s_1) \in \Omega$. Taking Proposition 5.15 (i), Lemma 3.34 (iv) and the above results into account, the equation $C_\Omega(f(\omega)) = C_\Omega(\omega)$ yields

$$\begin{aligned} b(s_0, \Phi_{U,W}(v)s_1) &= b(\Phi_{U,W}(v)s_0, s_1) \\ &= b\big(\Phi_{U,W}(f(v))f(s_0), f(s_1)\big) \\ &= b(\Phi_{U,W}(xv)s_0, \Phi_{U,W}(x)s_1) \\ &= b(s_0, \Phi_{U,W}(v\tau(x)x)s_1) \\ &= N(x)b(s_0, \Phi_{U,W}(v)s_1). \end{aligned}$$

Thus, we must have $N(x) = 1$, that is, $x \in \mathrm{Spin}(V)$. The claim $f = \theta(x)$ is now immediate from the choice of x and the equation $xvx^{-1} = f(v)$ for $v \in V$. □

This lemma is a key ingredient in the proof of the following remarkable theorem:

Theorem 7.13 (Triality)**.** *Suppose that* $\dim V = 8$*. Then there is an isometry* $J \in \mathrm{O}(\Omega, \mathcal{Q})$ *of order 3 such that*

$$J(V) = S_1, \qquad J(S_1) = S_0, \qquad J(S_0) = V.$$

Moreover, there is an automorphism of algebraic groups $j\colon \mathrm{Spin}(V) \to \mathrm{Spin}(V)$ *of order 3 with* $J \circ \theta(x) = \theta(j(x)) \circ J$ *for all* $x \in \mathrm{Spin}(V)$*. In particular, we have a commutative diagram*

$$\begin{tikzcd}
V \arrow[r, "J"] \arrow[d, "\rho(x)"] & S_1 \arrow[r, "J"] \arrow[d, "\Delta_8^-(j(x))"] & S_0 \arrow[d, "\Delta_8^+(j^2(x))"] \\
V \arrow[r, "J"'] & S_1 \arrow[r, "J"'] & S_0
\end{tikzcd}$$

for $x \in \mathrm{Spin}(V)$*.*

Proof. Since k is algebraically closed, we can choose an element $z \in V$ with $Q(z) = 1$. Analogously, there is $t_0 \in S_0$ with $q_0(t_0) = 1$. For clarity, denote the reflections associated to the nonsingular elements z and t_0 by $r_z \in \mathrm{O}(V, Q)$ and $r_{t_0} \in \mathrm{O}(S_0, q_0)$ (see Definition 2.37). Define a linear map

$$\sigma\colon V \to S_1,\ v \mapsto \Phi_{U,W}(v)t_0.$$

By the definitions from the beginning of this section and Proposition 5.15 (i) it holds that

$$\begin{aligned} q_1(\Phi_{U,W}(v)t_0) &= \frac{1}{2} b(\Phi_{U,W}(v)t_0, \Phi_{U,W}(v)t_0) \\ &= \frac{1}{2} Q(v) b(t_0, t_0) \\ &= Q(v) \end{aligned}$$

for all $v \in V$, that is to say, σ is an isometry. Since Q is nondegenerate and $\dim V = \dim S_1$, Lemma 2.22 shows that σ is bijective. We may therefore define linear maps

$$\begin{aligned} \mu&\colon \Omega \to \Omega,\ (v, s_0, s_1) \mapsto (r_z(v), \Phi_{U,W}(z)s_0, \Phi_{U,W}(z)s_1), \\ \tau&\colon \Omega \to \Omega,\ (v, s_0, s_1) \mapsto (\sigma^{-1}(s_1), r_{t_0}(s_0), \sigma(v)). \end{aligned}$$

One easily sees that $\mu, \tau \in \mathrm{O}(\Omega, \mathcal{Q})$. We define

$$J := \tau \circ \mu \in \mathrm{O}(\Omega, \mathcal{Q}).$$

This map has the desired properties and it holds that for $x \in \mathrm{Spin}(V)$, the map $J \circ \theta(x) \circ J^{-1} \in \mathrm{SO}(\Omega, \mathcal{Q})$ satisfies the assumptions of Lemma 7.12, see the proof of Theorem 3.8 of [Mei13]. One then defines $j(x)$ to be the unique element of $\mathrm{Spin}(V)$ such that $J \circ \theta(x) \circ J^{-1} = \theta(j(x))$ and checks that the map $j\colon \mathrm{Spin}(V) \to \mathrm{Spin}(V)$

obtained this way is an automorphism of abstract groups of order three, see again [Mei13].

It is also an automorphism of algebraic groups: Since θ is a morphism of algebraic groups, the coordinates of $J \circ \theta(x) \circ J^{-1}$ are polynomials in the coordinates of x. The proof of Lemma 7.12 shows that

$$j(x) = \Phi_{U,W}^{-1}\big((J \circ \theta(x) \circ J^{-1})\big|_S\big).$$

Now $\Phi_{U,W}^{-1}\colon \operatorname{End}(S) \to C$ is in particular a linear map and therefore a morphism of varieties, so that also the coordinates of $j(x)$ are polynomials in the coordinates of x. Consequently, $j\colon \operatorname{Spin}(V) \to \operatorname{Spin}(V)$ is a morphism of algebraic groups. This implies that also its inverse $j^{-1} = j^2$ is a morphism of algebraic groups, that is to say, j is an automorphism of algebraic groups. ☐

This theorem now allows us to explain the results in dimension 8. Since j is an automorphism, it maps unipotent classes to unipotent classes and preserves centralizer dimensions. Note that conjugate elements have conjugate centralizers, so the dimension of centralizers is constant on conjugacy classes. For a unipotent element $x \in \operatorname{Spin}(V)$, Lemma 6.13 and the proof of Proposition 6.6 show that

$$\dim C_{\operatorname{Spin}(V)}(x) = \dim C_{\operatorname{SO}(V)}(\rho(x)) = \dim C_{\operatorname{O}(V)}(\rho(x)).$$

Hence, we can compute the centralizer dimensions of the unipotent classes of $\operatorname{Spin}(V)$ by using Proposition 3.7 (iii) of [LS12] which states that for a unipotent element $u \in \operatorname{O}_n$ with Jordan normal form $\bigoplus_i J_i^{r_i}$, the dimension of its centralizer is given by

$$\dim C_{\operatorname{O}_n}(u) = \frac{1}{2}\sum_i i r_i^2 + \sum_{i<l} i r_i r_l - \frac{1}{2}\sum_{i \text{ odd}} r_i.$$

Due to our labelling of the unipotent classes of $\operatorname{Spin}(V)$ (cf. Remark 6.16), this gives the following centralizer dimensions:

class	(1^8)	$(1^5, 3)$	$(1^4, 2^2)$	$(1^3, 5)$	$(1^2, 3^2)$	$(1, 2^2, 3)$
centralizer dimension	28	16	18	8	10	12

class	$(1, 7)$	$(3, 5)$	$(2^4)_0$	$(2^4)_1$	$(4^2)_0$	$(4^2)_1$
centralizer dimension	4	6	16	16	8	8

Let $\mathcal{C}$ be a unipotent class of $\operatorname{Spin}(V)$ such that no other class has the same centralizer dimensions, and let $x \in \mathcal{C}$. Then $j(\mathcal{C}) = j(x)^{\operatorname{Spin}(V)} = \mathcal{C}$. Furthermore, the commutative diagram from Theorem 7.13 implies that

$$\Delta_8^-(j(x)) = J\big|_V \circ \rho(x) \circ (J\big|_V)^{-1}.$$

We infer that the blocks of $\mathcal{C}$ under the representation Δ_8^- are the same as those of the linear map $\rho(x) \in \operatorname{SO}(V)$. Analogously, also the blocks under Δ_8^+ are the same as those of $\rho(x) \in \mathrm{SO}(V)$. By our labelling, this means that if $\mathcal{C} = (i_1^{r_{i_1}}, \dots, i_t^{r_{i_t}})$, then its Jordan blocks are $i_1^{r_{i_1}}, \dots, i_t^{r_{i_t}}$.

This explains the results for all such classes $\mathcal{C}$. By the above tables, there remain six other unipotent classes of which three have centralizer dimensions 8 and three have centralizer dimensions 16. We explain the behaviour of the blocks for the three classes $(1^5, 3)$, $(2^4)_0$ and $(2^4)_1$ that share the same centralizer dimensions; the behaviour for the classes $(1^3, 5)$, $(4^2)_0$ and $(4^2)_1$ is analogous.

By our results, the class $(2^4)_0$ has different blocks under the two half-spin representations. In view of the commutative diagram from Theorem 7.13 we therefore cannot have $j((2^4)_0) = (2^4)_0$. Since j preserves centralizer dimensions, it either holds that $j((2^4)_0) = (2^4)_1$ or $j((2^4)_0) = (1^5, 3)$. Without loss of generality, we assume the former; in the latter case, the same argumentation will apply. As for the class $(2^4)_0$, we cannot have $j((2^4)_1) = (2^4)_1$. Moreover, if $j((2^4)_1) = (2^4)_0$, then

$$j((2^4)_0) = j^2((2^4)_1) = j^3((2^4)_0) = (2^4)_0$$

which is a contradiction. Hence, we must have $j((2^4)_1) = (1^5, 3)$. Since j is of order 3, this shows that j cyclically permutes the three classes $(1^5, 3)$, $(2^4)_0$ and $(2^4)_1$. Again using the diagram from Theorem 7.13, we infer that the blocks of $(1^5, 3)$ are 2^4 and the blocks saved under the label (2^4) are $1^5, 3$ and 2^4.

Note that the existence of the triality automorphism j again is evidence for the fact that the results in dimension 8 are independent of the characteristic, cf. Proposition 7.8.

Remark 7.14. The above discussion on the images of the classes $(1^5, 3)$, $(2^4)_0$ and $(2^4)_1$ under j in particular shows that j is not an inner automorphism of $\mathrm{Spin}(V)$. Hence, $\mathrm{Spin}(V)$ possesses an automorphism of algebraic groups of order 3 which is not inner. In fact, the existence of such an automorphism is very special to the spin group in dimension 8: One can show that the only semisimple algebraic groups of simply connected or adjoint type that admit an automorphism of algebraic groups of order 3 which is not inner, are those of type D_4, see [MT11], Theorem 11.12 and Table 11.1.

Conclusion

In this thesis, we have used the theories of quadratic forms and Clifford algebras to construct the spin groups for quadratic forms whose associated bilinear form is nondegenerate. We determined their root system as well as their root subgroups and have shown that these groups are the simply connected simple algebraic groups of type B_m and D_m which are known to exist by the classification of semisimple algebraic groups. Afterwards, we introduced and thoroughly studied the spin and half-spin representations. Our main goal was to compute the Jordan blocks of the images of unipotent elements of spin groups under these representations in good characteristic which we were able to achieve by combining our knowledge about the root subgroups of $\mathrm{Spin}(V)$ with the results on the behaviour of the restrictions of spin representations to (products of) lower-dimensional spin groups.

The resulting algorithm has been implemented in `GAP` and can be found in the Appendix. It computes the unipotent classes of $\mathrm{Spin}(V)$ and their Jordan blocks for any given dimension in a given characteristic different from 2. The dimensions of the spin representations growing exponentially, it highly depends on the available computing power, up to which dimension the algorithm runs in an acceptable time span. With the given implementation, we were able to compute the Jordan blocks of the unipotent classes up to dimension 20. With more computing power, also the blocks in much higher dimensions should be computable. Furthermore, we remark that it is very likely that some improvements can be made, regarding both the algorithm itself and its implementation. For example, one could use Proposition 7.7 to save a lot of computations in the respective characteristics, or more generally employ the formula from Theorem 5 of [Sri64] for the calculation of the Jordan blocks of the Kronecker product of Jordan block matrices.

Having computed the Jordan blocks of all unipotent classes (in low dimensions), there naturally arises the question what can be said about these results from a theoretical point of view and whether there exists some pattern in the results that in the best case may lead to a general formula for the Jordan blocks. Regarding these issues, we were able to prove some statements on the dependence of the results on the characteristic of the underlying field. Moreover, we gave a few constraints that the Jordan blocks have to fulfill in certain dimensions. However, this is just a first step in the analysis of our computational results which may eventually lead to some deeper statements on the Jordan blocks of unipotent elements of spin groups. Besides the general problem of finding an overall pattern, one example of an open question that arises from the low-dimensional results is whether a class that is coming from a splitting class of the pin group always has different Jordan blocks under the two half-spin representations. It would further be interesting to know whether the bound from Proposition 7.10 can be made more explicit.

Finally, one may ask about the situation in characteristic 2. Here, first of all, our construction of the spin groups only includes the case of even dimension whereas in odd dimension one has to work with nondegenerate quadratic forms (see Proposition 2.28 and Remark 2.29). One can however carry out the same construction for an arbitrary nondegenerate quadratic form; regarding the norm, one then still has a group homomorphism $N\big|_{\Gamma_0}\colon \Gamma_0 \to k^\times$ due to Theorem 3.24 and the proof of Lemma 3.34 and may define the spin group to be the kernel of this homomorphism. Since it only uses results that do not need the assumption $\operatorname{char} k \neq 2$, Proposition 3.43 also holds in odd dimension in characteristic 2, whereas results relying on Theorem 2.41 and Proposition 2.42 do not immediately carry over. However, one still obtains an algebraic group this way and may show that the twisted adjoint representation in characteristic 2 defines a bijective isogeny $\rho\colon \operatorname{Spin}(V) \to \operatorname{SO}(V)$, see [KMRT98], §23. Thus, the results from Section 4.4 remain valid since they only use this isogeny and the structure of the special orthogonal group.

One may again construct the spin and half-spin representations in the way we did as this only required results from the theory of Clifford algebras which we treated in full generality. The results from Sections 5.2 and 5.3 carry over as they do not particularly rely on the assumption $\operatorname{char} k \neq 2$. Thus, one can work with spin groups and spin representations in a very similar way as before.

A much bigger difference to the case $\operatorname{char} k \neq 2$ appears when considering the unipotent conjugacy classes of the spin group. By Proposition 6.6, we may again equivalently study the unipotent classes of the special orthogonal group. Here, the situation is substantially different in characteristic 2, see the book [LS12]. This is the main reason why we excluded the case $\operatorname{char} k = 2$ in our exposition. It would be interesting to know whether a similar approach also works to determine the Jordan blocks of unipotent elements of spin groups in this case.

Appendix: GAP code

```
#### JORDAN BLOCKS ####


# input:
#   unip_matrix: a unipotent matrix with entries either in QQ or GF(p) for a prime p
#   characteristic: the characteristic of the field, over which unip_matrix is defined
# output:
#   jordanblocks: a list that contains the sizes of the Jordan blocks of unip_matrix. the block sizes are counted without multiplicity, so one size may occur several times in the output list

# we compute the (row lengths of the) Jordan diagram of unip_matrix. the lenghts of the columns of the Jordan diagram precisely give the Jordan block sizes in the Jordan normal form of unip_matrix
# since the matrices that occur in our algebraic groups context only have entries 0, 1 and -1, it suffices for the Jordan blocks to work in the prime field of the algebraically closed field, that is, in QQ respectively GF(p)

jordan_unip := function(unip_matrix, characteristic)

    local field, size, help0, help1, i, r, rowlengths, jordanblocks, current, b;

    if characteristic = 0 then
        field := Rationals;
    else
        field := GF(characteristic);
    fi;

    size := DimensionsMat(unip_matrix)[1];

    help0 := [size];
    help1 := [];
    for i in [1 .. size] do  # go up to size to avoid computing the minimal polynomial which is slow
        r := RankMat( (unip_matrix - IdentityMat(size, field))^i ); # for unipotent matrices, all eigenvalues are 1
        Add(help0, r);
        Add(help1, r);
    od;
    Add(help1, RankMat( (unip_matrix - IdentityMat(size, field))^(size + 1) ) );
    rowlengths := help0 - help1;
```

```
    # contains the row lengths of the Jordan diagram, where row i has length dim H_i - dim H_(i-1); entry rowlenghts[i] stores the length of row i

    jordanblocks := [];
    current := Filtered(rowlengths, x -> x > 0); # delete zero entries
    b := Length(current);
    while b <> 0 do
        Add(jordanblocks, b); # length of a column in the jordan diagram gives a jordan block of that size
        current := current - ListWithIdenticalEntries(b, 1); # column is finished, so subtract one box of each row to get to next column
        current := Filtered(current, x -> x > 0);
        b := Length(current);
    od;

    return jordanblocks;

end;


# input:
#   size: an integer greater than 0
# output:
#   jblock: a matrix that is a single Jordan block of the given size

jordan_block := function(size)

    local jblock, i;

    jblock := IdentityMat(size);
    for i in [1 .. size - 1] do
        jblock[i][i + 1] := 1;
    od;

    return jblock;

end;


# input:
#   blocks_of_matrix_1: a list that contains the Jordan block sizes of a unipotent matrix with entries either in QQ or GF(p) for a prime p, counted without multiplicity
#   blocks_of_matrix_2: the same as above. the matrix must have entries in the same field
#   characteristic: the characteristic of the field, over which the matrices are defined
# output:
#   blocks: a list that that contains the sizes of the Jordan blocks of the Kronecker product of the two given matrices, counted without multiplicity

blocks_of_tensor_product := function(blocks_of_matrix_1, blocks_of_matrix_2, characteristic)

```

```
    local field, nr_blocks_1, nr_blocks_2, blocks, i, jordan_block_i, j, jordan_block_j, prod_ij, blocks_ij;

    if characteristic = 0 then
        field := Rationals;
    else
        field := GF(characteristic);
    fi;

    nr_blocks_1 := Length(blocks_of_matrix_1);
    nr_blocks_2 := Length(blocks_of_matrix_2);
    blocks := [];

    # Kronecker product is distributive over direct sum
    for i in [1 .. nr_blocks_1] do
        jordan_block_i := jordan_block(blocks_of_matrix_1[i]);

        for j in [1 .. nr_blocks_2] do
            jordan_block_j := jordan_block(blocks_of_matrix_2[j]);
            prod_ij := KroneckerProduct(jordan_block_i, jordan_block_j) * One(field);
            blocks_ij := jordan_unip(prod_ij, characteristic);
            Append(blocks, blocks_ij);
        od;

    od;

    return blocks;

end;




#### UNIPOTENT CONJUGACY CLASSES ####
# we label the unipotent classes of SO(n) by their Jordan blocks. thus they correspond to certain partitions of n. a conjugate of a unipotent matrix of GL(n) is contained in SO(n) if and only if the even sized blocks have an even multiplicity. two such matrices are conjugate in SO(n) if and only if they are conjugate in GL(n), except for the special case that the matrix only has even sized blocks. then its conjugacy class in GL(n) splits into two SO(n)-classes
# a unipotent class of SO(n) will be represented by a list of lists. each entry (but possibly the last, see below) of the class is a list with two elements, where the first element gives the size of the Jordan block and the second the multiplicity of the block.
# for example, [ [1, 2], [2, 4] ] is the representation of the class of SO(10) that comprises the elements with Jordan normal form consisting of two blocks of size 1 and four blocks of size 2.
# if n = 0 (mod 4) then splitting may occur: a unipotent class of O(n) labelled by only even sized blocks will split into two classes in SO(n), to which we refer as split classes. in the list representation, they are distinguished by adding an entry "a" resp. "b" at the end of the list
# for example, we have the unipotent classes [ [2, 2], "a"] and [ [2, 2], "b"] in SO(4)
```

```
# we use the same labelling for the corresponding unipotent classes of Spin(n)


# input:
#   n: a natural number
# output:
#   classes: a list that contains the unipotent conjugacy classes of SO(n) resp. labels for the unipotent conjugacy classes of Spin(n)

classes_SO := function(n)

    local iter, classes, part, multiplicities_list, addpart, only_even, i, p1, p2;

    iter := IteratorOfPartitions(n);
    classes := [];

    for part in iter do # Jordan normal form may be represented by a partition

        multiplicities_list := Collected(part); # collects the multiplicities of the Jordan blocks

        addpart := 1; # if this remains 1, then we will add the partition to the list of classes
        only_even := 1; # if this remains 1, then the Jordan normal form consists only of even blocks, so that we have a split class
        i := 1;

        while i <= Length(multiplicities_list) do

            if multiplicities_list[i][1] mod 2 = 0 then
            # have an even block

                if multiplicities_list[i][2] mod 2 = 0 then # with even multiplicity
                    i := i + 1;
                else # with odd multiplicity, so not a class of SO
                    addpart := 0;
                    i := Length(multiplicities_list) + 1; # jump out of while-loop
                fi;

            else
            # have an odd block

                only_even := 0;
                i := i + 1;
            fi;

        od;

        # add the partition to the list of unipotent conjugacy classes
        if addpart = 1 then
            if only_even = 1 then # class splits
```

```
                p1 := ShallowCopy(multiplicities_list);
                p2 := ShallowCopy(multiplicities_list);
                Add(p1, "a");
                Add(p2, "b");
                Add(classes, p1);
                Add(classes, p2);
            else
                Add(classes, multiplicities_list);
            fi;
        fi;

    od;

    return classes;

end;


# input:
#   class_with_one_block: a unipotent class (in the above described representation) of SO(n) (for some underlying n) that has a Jordan block of size 1
# output:
#   restricted_class: the unipotent class of SO(n-1) that is obtained from the given class by deleting one Jordan block of size 1. if this leads to a splitting class, then a list is returned, containing "splitting" as first entry and then the two split classes

# in the standard embedding SO(n-1) -> SO(n) the restricted class (in the splitting case, any of the two split classes) will map into the given class

class_restriction := function(class_with_one_block)

    local multiplicity_of_one_block, restricted_class, block_sizes_list, class_a, class_b;

    multiplicity_of_one_block := class_with_one_block[1][2]; # in our representation of unipotent classes, the blocks of size 1 come first
    restricted_class := ShallowCopy(class_with_one_block);

    if multiplicity_of_one_block = 1 then
        Remove(restricted_class, 1); # no more 1-blocks are contained

        block_sizes_list := restricted_class{[1 .. Length(restricted_class)]}[1];
        if ForAll(block_sizes_list, n -> n mod 2 = 0) then # only even blocks, so splitting occurs in the restricted class

            class_a := ShallowCopy(restricted_class);
            class_b := ShallowCopy(restricted_class);
            Add(class_a, "a");
            Add(class_b, "b");
            return ["splitting", class_a, class_b];

        else
```

```
            return restricted_class;
        fi;

    else
        restricted_class[1][2] := restricted_class[1][2] - 1; # decrease multiplicity by one

        return restricted_class;
    fi;

end;


# input:
#   decomposable_class: a unipotent class of SO(n) (for some underlying n) that neither consists of a single Jordan block, nor consists of two equally sized even blocks
# output:
#   a list of various length that contains data on how the given class may be obtained as an image of a class in an embedding SO(l) x SO(n-l) -> SO(n). more precisely, the function will return a class C_1 of SO(l) for some l < n (resp. both split classes, if there happens to be a splitting of this class) and a class C_2 of SO(n-l) (if applicable both split classes) such that (C_1, C_2) embeds into the given class. if splitting occurs, then for any choice of the spilt classes, the tuple will embed in this way
#   dimension_l: this is always the first entry of the output. it is a natural number l such that the first class is contained in SO(l)
#   if there is any splitting of the two classes that shall be returned, then the next entry of the output list is "splitting first class" or "splitting second class" or "splitting first and second class"
#   the subsequent entries of the output list are the suitable class of SO(l) (resp. both split classes) and the suitable class of SO(n-l) (resp. both split classes)

# the function always removes a block resp. blocks of lowest size in the given class in order to obtain the two classes
# the classes that are excluded in the input are precisely the ones that cannot be obtained as an image of a class in an embedding SO(l) x SO(n-l) -> SO(n)

tensor_decomp := function(decomposable_class)

    local copy, dimension_l, class_1, class_2, class_1_a, class_1_b, class_2_a, class_2_b, block_sizes_list;

    copy := ShallowCopy(decomposable_class);

    # always modify the first block of decomposable_class
    if decomposable_class[1][2] = 1 then
        # first block only has multiplicity one, and we can remove it without affecting membership of SO (it must be odd-sized)

        class_1 := [copy[1]];
        dimension_l := copy[1][1];
        Remove(copy, 1);
```

```

    # if we are in odd dimension, then the remaining part may split
    block_sizes_list := copy{[1 .. Length(copy)]}[1];
    if ForAll(block_sizes_list, n -> n mod 2 = 0) then # only even blocks, so splitting occurs

        class_2_a := Concatenation(copy, ["a"]);
        class_2_b := Concatenation(copy, ["b"]);

        return [dimension_l, "splitting second class", class_1, class_2_a, class_2_b];

    else # no splitting
        class_2 := copy;

    fi;

# now first block has multiplicity at least 2
elif decomposable_class[1][1] mod 2 = 1 then
    # first block is odd, of multiplicity >2. odd blocks can always be split off

    class_1 := [ [copy[1][1], 1] ];
    dimension_l := copy[1][1];
    copy[1][2] := copy[1][2] - 1;
    class_2 := copy;

# now first block is even, of multiplicity at least 2
elif decomposable_class[1][2] = 2 then
    # multiplicity is exactly 2

    # the first class we are creating is split
    class_1_a := [ copy[1], "a" ];
    class_1_b := [ copy[1], "b" ];
    dimension_l := 2*copy[1][1];
    Remove(copy, 1);
    class_2 := copy;

        # determine whether second class will split as well
        if class_2[Length(class_2)] = "a" then
            # original class was split, so also the second class must split
            class_2_a := ShallowCopy(class_2);
            class_2[Length(class_2)] := "b";
            class_2_b := class_2;

        elif class_2[Length(class_2)] = "b" then
            class_2_b := ShallowCopy(class_2);
            class_2[Length(class_2)] := "a";
            class_2_a := class_2;

        else
            # original class was not split, so second class does not split
            return [dimension_l, "splitting first class", class_1_a, class_1_b, class_2];
```

```
            fi;

        return [dimension_l, "splitting first and second class", class_1_a, class_1_b, class_2_a, class_2_b];

    else
        # first block is even, of multiplicity greater than 2

        class_1_a := [ [copy[1][1], 2], "a" ];
        class_1_b := [ [copy[1][1], 2], "b" ];
        dimension_l := 2*copy[1][1];
        copy[1][2] := copy[1][2] - 2;
        class_2 := copy;

            # determine whether second class will split as well
            if class_2[Length(class_2)] = "a" then
                # original class was split, so the second class must split
                class_2_a := ShallowCopy(class_2);
                class_2[Length(class_2)] := "b";
                class_2_b := class_2;

            elif class_2[Length(class_2)] = "b" then
                class_2_b := ShallowCopy(class_2);
                class_2[Length(class_2)] := "a";
                class_2_a := class_2;

            else
                # original class was not split, so second class does not split
                return [dimension_l, "splitting first class", class_1_a, class_1_b, class_2];
            fi;

        return [dimension_l, "splitting first and second class", class_1_a, class_1_b, class_2_a, class_2_b];

    fi;

    return [dimension_l, class_1, class_2];

end;




#### BIG BLOCK ####
# if W is a vector space with basis (w_1, ..., w_m) then we will represent a basis vector of the vector space exterior(W) by a list containing the indices of the basis vectors of W that are involved
# for example, the basis vector w_1 /\ w_3 of exterior(W) will simply be represented by [1, 3]
# in this way, we work with the vector space exterior(W) by working with these index tuples, which in turn are just ascending sequences of natural numbers between 1 and m, that is, combinations of [1 .. m]

```

```

# input:
#   m: the dimension of W, where V = (U + W) + span(z) is a Lagrangian decomposition of the odd-dimensional vector space V
# output:
#   mat: the matrix of the operator eta_1 on exterior(W), which is the matrix of the element z in the spin representation. it is computed with respect to the ordering of the basis of exterior(W) that comes from EnumeratorOfCombinations

matrix_of_z := function(m)

    local basis_of_exterior_W, dimension_of_exterior_W, mat, i, current_basis_vector, sign, baserep_of_image_of_current_basis_vector;

    basis_of_exterior_W := EnumeratorOfCombinations([1 .. m]); # get representatives for the basis vectors of exterior(W)
    dimension_of_exterior_W := 2^m;
    mat := [];

    for i in [1 .. dimension_of_exterior_W] do

        current_basis_vector := basis_of_exterior_W[i];
        sign := (-1)^Length(current_basis_vector);

        baserep_of_image_of_current_basis_vector := ListWithIdenticalEntries(dimension_of_exterior_W, 0);
        baserep_of_image_of_current_basis_vector[i] := sign;

        Add(mat, baserep_of_image_of_current_basis_vector);
        # write image in i-th row. since we get a diagonal matrix, we do not need to transpose later

    od;

    return mat;

end;


# input:
#   m: the dimension of W, where V = U + W respectively V = (U + W) + span(z) is a Lagrangian decomposition of V
#   j: a natural number in {1, ..., m}
# output:
#   mat: the matrix of the operator lambda_w_j on exterior(W), which is the matrix of the element w_j in the spin representation. it is computed with respect to the ordering of the basis of exterior(W) that comes from EnumeratorOfCombinations

matrix_of_w_j := function(m, j)

    local basis_of_exterior_W, dimension_of_exterior_W, mat, i, current_basis_vector, number_of_swaps, sign, image_of_current_basis_vector, pos;

```

```
    basis_of_exterior_W := EnumeratorOfCombinations([1 .. m]);
    dimension_of_exterior_W := 2^m;
    mat := NullMat(dimension_of_exterior_W, dimension_of_exterior_W); # this will be the output. initialize as zero matrix since we will only add single non-zero entries of which there are very few


    for i in [1 .. dimension_of_exterior_W] do

        current_basis_vector := basis_of_exterior_W[i];

        if j in current_basis_vector then
            # lambda_w_j maps current_basis_vector to zero, so do nothing
        else
            number_of_swaps := Length( Filtered(current_basis_vector, x -> x < j) );
            # gives how many indices are smaller than j. this is number of required swaps to move w_j (when added to the left of the current basis vector by lambda_w_j) to its place, such that the index tuple is again in ascending order
            sign := (-1)^number_of_swaps;

            # lambda_w_j will add w_j to the current basis vector. we compute the basis vector that is obtained after swapping
            image_of_current_basis_vector := ShallowCopy(current_basis_vector);
            Add(image_of_current_basis_vector, j);
            Sort(image_of_current_basis_vector);

            # compute the position of the image vector (without sign) in the basis of extetior(W)
            pos := Position(basis_of_exterior_W, image_of_current_basis_vector);

            # column i of the representing matrix has been computed
            mat[pos][i] := sign;
            # by doing it this way, we do not need to transpose at any point which we would have to do if we added the basis representation of the image vector as a row vector into an empty matrix

        fi;

    od;

    return mat;

end;


#   input:
#   m: the dimension of W, where V = U + W respectively V = (U + W) + span(z) is a Lagrangian decomposition of V
#   j: a natural number in {1, ..., m}
#   output:
#   mat: the matrix of the operator iota_u_j on exterior(W), which is the matrix of the element u_j in the spin representation. it is computed
```

```
 with respect to the ordering of the basis of exterior(W) that comes from EnumeratorOfCombinations

matrix_of_u_j := function(m, j)

    local basis_of_exterior_W, dimension_of_exterior_W, mat, i, current_basis_vector, pos_of_w_j, sign, image_of_current_basis_vector, pos;

    basis_of_exterior_W := EnumeratorOfCombinations([1 .. m]);
    dimension_of_exterior_W := 2^m;
    mat := NullMat(dimension_of_exterior_W, dimension_of_exterior_W); # this will be the output. initialize as zero matrix since we will only add single non-zero entries of which there are very few


    for i in [1 .. dimension_of_exterior_W] do

        current_basis_vector := basis_of_exterior_W[i];

        if j in current_basis_vector then
            pos_of_w_j := Position(current_basis_vector, j); # j sits at this position in current_basis_vector
            sign := (-1)^(pos_of_w_j - 1);

            image_of_current_basis_vector := ShallowCopy(current_basis_vector);
            Remove(image_of_current_basis_vector, pos_of_w_j); # remove j, the result is the image of the current basis vector under iota_j, without sign

            # compute the position of the image vector (without sign) in the basis of extetior(W)
            pos := Position(basis_of_exterior_W, image_of_current_basis_vector);

            # column i of the representing matrix has been computed
            mat[pos][i] := sign;
            # by doing it this way, we do not need to transpose at any point which we would have to do if we added the basis representation of the image vector as a row vector into an empty matrix

        else
            # iota_u_j maps current_basis_vector to zero, so do nothing
        fi;

    od;

    return mat;

end;


# input:
#   n: an odd natural number
#   characteristic: either 0 or a prime number p with p > 2
```

```
# output:
#   blocks: the Jordan blocks in given characteristic of the image under
    the spin representation of the unipotent class of Spin(n)
    corresponding to the single Jordan block class of SO(n)

bigblock := function(n, characteristic)

    local m, Prod, i, field, blocks;

    m := (n - 1)/2;

    if m = 0 then
        return [1];
    elif m = 1 then
        return [2];
    fi;


    # now m >= 2

    Prod := IdentityMat(2^m) + matrix_of_z(m) * matrix_of_u_j(m, m);
    for i in [1 .. (m - 1)] do
        Prod := Prod * (IdentityMat(2^m) + matrix_of_u_j(m, i) *
    matrix_of_w_j(m, i + 1));
    od;

    if characteristic = 0 then
        field := Rationals;
    else
        field := GF(characteristic);
    fi;

    Prod := Prod * One(field); # move to respective field

    blocks := jordan_unip(Prod, characteristic);
    return blocks;

end;




#### SQUARE BLOCK ####


# input:
#   list: a list, here typically a range [1 .. n]
# output:
#   sorted_combinations: a list with all combinations of the given list,
    that first lists all combinations of even length and then all
    combinations of odd length

CombinationsSorted := function(list)

    local all_combinations, even_combinations, odd_combinations,
    sorted_combinations;
```

```

    all_combinations := Combinations(list);
    even_combinations := Filtered(all_combinations, x -> Length(x) mod 2 = 0);
    odd_combinations := Filtered(all_combinations, x -> Length(x) mod 2 = 1);

    sorted_combinations := Concatenation(even_combinations, odd_combinations);
    return sorted_combinations;

end;


# input:
#   m: the dimension of W, where V = U + W respectively V = (U + W) + span(z) is a Lagrangian decomposition of V
#   j: a natural number in {1, ..., m}
# output:
#   mat: the matrix of the operator lambda_w_j on exterior(W), which is the matrix of the element w_j in the spin representation. it is computed with respect to the ordering of the basis of exterior(W) that comes from CombinationsSorted

# this function works exactly like matrix_of_w_j
# the only difference is the ordering of the basis of exterior(W). here, since we sort the combinations, the resulting matrix will be a block diagonal matrix with two blocks, where the first is the matrix of w_j in the half-spin^+ representation and the second is the matrix of w_j in the half-spin^- representation
block_matrix_of_w_j := function(m, j)

    local basis_of_exterior_W, dimension_of_exterior_W, mat, i, current_basis_vector, number_of_swaps, sign, image_of_current_basis_vector, pos;

    basis_of_exterior_W := CombinationsSorted([1 .. m]);
    dimension_of_exterior_W := 2^m;
    mat := NullMat(dimension_of_exterior_W, dimension_of_exterior_W);


    for i in [1 .. dimension_of_exterior_W] do

        current_basis_vector := basis_of_exterior_W[i];

        if j in current_basis_vector then

        else
            number_of_swaps := Length( Filtered(current_basis_vector, x -> x < j) );
            sign := (-1)^number_of_swaps;

            image_of_current_basis_vector := ShallowCopy(current_basis_vector);
            Add(image_of_current_basis_vector, j);
            Sort(image_of_current_basis_vector);
```

```

            pos := Position(basis_of_exterior_W,
    image_of_current_basis_vector);

            mat[pos][i] := sign;

        fi;

    od;

    return mat;

end;


# input:
#   m: the dimension of W, where V = U + W respectively V = (U + W) +
    span(z) is a Lagrangian decomposition of V
#   j: a natural number in {1, ..., m}
# output:
#   mat: the matrix of the operator iota_u_j on exterior(W), which is the
     matrix of the element u_j in the spin representation. it is computed
     with respect to the ordering of the basis of exterior(W) that comes
    from CombinationsSorted

# this function works exactly like matrix_of_u_j
# the only difference is the ordering of the basis of exterior(W). here,
    since we sort the combinations, the resulting matrix will be a block
    diagonal matrix with two blocks, where the first is the matrix of u_j
     in the half-spin^+ representation and the second is the matrix of
    u_j in the half-spin^- representation

block_matrix_of_u_j := function(m, j)

    local basis_of_exterior_W, dimension_of_exterior_W, mat, i,
    current_basis_vector, pos_of_w_j, sign, image_of_current_basis_vector
    , pos;

    basis_of_exterior_W := CombinationsSorted([1 .. m]);
    dimension_of_exterior_W := 2^m;
    mat := NullMat(dimension_of_exterior_W, dimension_of_exterior_W);


    for i in [1 .. dimension_of_exterior_W] do

        current_basis_vector := basis_of_exterior_W[i];

        if j in current_basis_vector then
            pos_of_w_j := Position(current_basis_vector, j);
            sign := (-1)^(pos_of_w_j - 1);

            image_of_current_basis_vector := ShallowCopy(
    current_basis_vector);
            Remove(image_of_current_basis_vector, pos_of_w_j);

            pos := Position(basis_of_exterior_W,
```

```
    image_of_current_basis_vector);

            mat[pos][i] := sign;

        else

        fi;

    od;

    return mat;

end;


# input:
#   n: an even natural number
#   characteristic: either 0 or a prime number p with p > 2
# output:
#   blocks: a list with two entries that describe the Jordan blocks in
    given characteristic of the image under the spin representation of
    the unipotent class of Spin(n) corresponding to the (possibly split)
    class of SO(n) whose elements have Jordan normal form composed of two
     blocks of size n/2
#       blocks[1] = blocks_plus: a list that contains the Jordan blocks
    of the      class in the half-spin^+ representation, counted without
    multiplicity
#       blocks[2] = blocks_minus: a list that contains the Jordan blocks
    of the      class in the half-spin^- representation, counted without
    multiplicity

# if n = 2 (mod 4) then the described class of Spin(n) does not split and
     the blocks in the half-spin^+ representation and in the half-spin^-
    representation agree
# if n = 0 (mod 4) then the described class of Spin(n) splits. the
    results are the blocks of one of the two classes. but we then also
    have the blocks for the second class, since for the two classes, half
    -spin^+ and half-spin^- representation are simply swapped

squareblock := function(n, characteristic)

    local field, m, Prod, i, halfspin_size, halfspin_plus_matrix,
    halfspin_minus_matrix, blocks_plus, blocks_minus, blocks;

    if characteristic = 0 then
        field := Rationals;
    else
        field := GF(characteristic);
    fi;

    m := n/2;
    if m = 1 then
        return [[1], [1]];
    fi;

    # now m >= 2
```

```
    # compute matrix of the square block class in the full spin representation
    Prod := IdentityMat(2^m);
    for i in [1 .. (m - 1)] do
        Prod := Prod * (IdentityMat(2^m) + block_matrix_of_u_j(m, i) * block_matrix_of_w_j(m, i + 1));
    od;

    Prod := Prod * One(field); # move to respective field
    # this now is due to the sorting of the basis of exterior(W) a matrix with two diagonal blocks, the first one corresponding to the half-spin^+ representation, the second to half-spin^-

    # extract the two block matrices on the diagonal
    halfspin_size := 2^(m-1);
    halfspin_plus_matrix := Prod{[1 .. halfspin_size]}{[1 .. halfspin_size]};
    halfspin_minus_matrix := Prod{[halfspin_size + 1 .. 2*halfspin_size]}{[halfspin_size + 1 .. 2*halfspin_size]};

    blocks_plus := jordan_unip(halfspin_plus_matrix, characteristic);
    blocks_minus := jordan_unip(halfspin_minus_matrix, characteristic);
    blocks := Concatenation([blocks_plus], [blocks_minus]);

    return blocks;

end;




#### ALL RESULTS ####


# input:
#   dimension: a natural number
#   characteristic: either 0 or a prime number p with p > 2
# output:
#   the function prints class labels for the unipotent conjugacy classes of Spin and their Jordan blocks in given characteristic in the spin (if dimension is odd) respectively half-spin^+ representation (if dimension is even), counted with multiplicity

# in even dimension, the blocks in the half-spin^- and spin representation can easily be determined from the ones in the half-spin^+ representation: if a class does not split, then it has the same blocks in the two half-spin representation. if it does split, then the blocks in the half-spin^- representation are the blocks in the half-spin^+ representation of the other part of the splitting class. the blocks in the full spin representation are obtained by adding the blocks of the two half-spin representations
all_results := function(dimension, characteristic)

    local list_with_all_results, results_in_dimension_1, results_in_dimension_2, current_dimension, results_in_current_dimension, conjugacy_classes_in_current_dimension,
```

```
 nr_conjugacy_classes, i, current_class_real, current_class,
current_blocks, results_in_lower_dimension,
classes_in_lower_dimension, restricted_class, class_a, class_b, pos_a
, pos_b, blocks_a, blocks_b, pos_restricted, tensor_data, dimension_l
, results_in_dimension_l, classes_in_dimension_l,
results_in_rest_dimension, classes_in_rest_dimension, class_rest,
pos_rest, blocks_ab, blocks_rest, class_l, pos_l, blocks_l, class_l_a
, class_l_b, class_rest_a, class_rest_b, pos_l_a, pos_l_b, pos_rest_a
, pos_rest_b, blocks_l_a, blocks_l_b, blocks_rest_a, blocks_rest_b,
first_blocks, second_blocks, results_in_given_dimension, nr_classes,
j, class, blocks, k;


list_with_all_results := [];
# we make a list which will contain all results for all classes for
every dimension which is smaller than or equal to the given dimension
# the list will be constructed in the following way: for each
dimension n, it shall contain a list as entry in the n-th position
# for each dimension, this list will be a list of pairs [class,
blocks] that are composed of a class of Spin in that dimension and of
 its Jordan blocks in the spin resp. half-spin^+ representation (as
usual, given by a list and counted without multiplicity)

# dimension 1
results_in_dimension_1 := [[ ["pt"], [1] ]];
Add(list_with_all_results, results_in_dimension_1);

# dimension 2
results_in_dimension_2 := [[ [[1, 2]], [1] ]];
Add(list_with_all_results, results_in_dimension_2);

# now higher dimensions
current_dimension := 3;

while current_dimension <= dimension do

    results_in_current_dimension := []; # this list will in the end
be added to list_with_all_results
    conjugacy_classes_in_current_dimension := classes_SO(
current_dimension);
    nr_conjugacy_classes := Length(
conjugacy_classes_in_current_dimension);


    # we now distinguish between odd and even dimension and apply a
suitable method for every type of conjugacy class

    #### odd-dimensional case ####
    if current_dimension mod 2 = 1 then

        for i in [1 .. nr_conjugacy_classes] do

            current_class_real :=
conjugacy_classes_in_current_dimension[i];
            current_class := StructuralCopy(current_class_real);

```

```
            ### big block case ###
            # we have separate function for this case
            if Length(current_class) = 1 and current_class[1][2] = 1 then
                current_blocks := bigblock(current_dimension, characteristic);


            ### class contains block of size 1 ###
            # work with restriction
            elif current_class[1][1] = 1 then # 1-blocks always come first

                # get the results and the conjugacy classes of one dimension lower
                results_in_lower_dimension := list_with_all_results[current_dimension - 1];
                classes_in_lower_dimension := results_in_lower_dimension{[ 1.. Length(results_in_lower_dimension) ]}[1];
                restricted_class := class_restriction(current_class);

                # we might have a splitting in the restricted class
                if restricted_class[1] = "splitting" then
                    class_a := restricted_class[2];
                    class_b := restricted_class[3];
                    pos_a := Position(classes_in_lower_dimension, class_a);
                    pos_b := Position(classes_in_lower_dimension, class_b);

                    # restricted spin representation is sum of the two half-spin representations
                    blocks_a := results_in_lower_dimension[pos_a][2];
                    blocks_b := results_in_lower_dimension[pos_b][2];
                    current_blocks := Concatenation(blocks_a, blocks_b);

                else # no splitting, restricted class has same blocks in both half-spin representations
                    pos_restricted := Position(classes_in_lower_dimension, restricted_class);
                    current_blocks := Concatenation(results_in_lower_dimension[pos_restricted][2], results_in_lower_dimension[pos_restricted][2]);
                fi;


            ### other composite classes cases ###
            # work with tensor product
            else

                # decompose the given class using the auxiliary function
                tensor_data := tensor_decomp(current_class);

```

```
                # this is the l appearing in the morphism of algebraic groups Spin(l) x Spin(n-l) -> Spin(n) from which we obtain our current class
                dimension_l := tensor_data[1];

                # get the results and classes from the lower dimensions
                results_in_dimension_l := list_with_all_results[dimension_l];
                classes_in_dimension_l := results_in_dimension_l{[ 1.. Length(results_in_dimension_l) ]}[1];
                results_in_rest_dimension := list_with_all_results[current_dimension - dimension_l];
                classes_in_rest_dimension := results_in_rest_dimension{[ 1.. Length(results_in_rest_dimension) ]}[1];

                # splitting might occur in the two classes that make up the composite class
                if tensor_data[2] = "splitting first class" then
                    class_a := tensor_data[3];
                    class_b := tensor_data[4];
                    class_rest := tensor_data[5];

                    pos_a := Position(classes_in_dimension_l, class_a);
                    pos_b := Position(classes_in_dimension_l, class_b);
                    pos_rest := Position(classes_in_rest_dimension, class_rest);

                    blocks_a := results_in_dimension_l[pos_a][2];
                    blocks_b := results_in_dimension_l[pos_b][2];
                    blocks_ab := Concatenation(blocks_a, blocks_b); # these are the blocks of the full spin representation of the first class (that lives in an even dimension)
                    blocks_rest := results_in_rest_dimension[pos_rest][2];

                    # spin representation is tensor product of the two lower dimensional (full) spin representations
                    current_blocks := blocks_of_tensor_product(blocks_ab, blocks_rest, characteristic);

                elif tensor_data[2] = "splitting second class" then
                    class_l := tensor_data[3];
                    class_a := tensor_data[4];
                    class_b := tensor_data[5];

                    pos_l := Position(classes_in_dimension_l, class_l);
                    pos_a := Position(classes_in_rest_dimension, class_a);
                    pos_b := Position(classes_in_rest_dimension, class_b);

```

```
                    blocks_l := results_in_dimension_l[pos_l][2];
                    blocks_a := results_in_rest_dimension[pos_a][2];
                    blocks_b := results_in_rest_dimension[pos_b][2];
                    blocks_ab := Concatenation(blocks_a, blocks_b); # these are the blocks of the full spin representation of the second class (that lives in an even dimension)

                    current_blocks := blocks_of_tensor_product(blocks_l, blocks_ab, characteristic);

                else # no splitting
                    class_l := tensor_data[2];
                    class_rest := tensor_data[3];

                    pos_l := Position(classes_in_dimension_l, class_l);
                    pos_rest := Position(classes_in_rest_dimension, class_rest);

                    # first class is in odd dimension, but second class might be in even dimension
                    blocks_l := results_in_dimension_l[pos_l][2];

                    if (current_dimension - dimension_l) mod 2 = 1 then
                        blocks_rest := results_in_rest_dimension[pos_rest][2];
                    else
                        blocks_rest := Concatenation(results_in_rest_dimension[pos_rest][2], results_in_rest_dimension[pos_rest][2]);
                    fi;


                    current_blocks := blocks_of_tensor_product(blocks_l, blocks_rest, characteristic);

                fi;

            fi;

            ## now current blocks have been computed

            Add(results_in_current_dimension, [current_class_real, current_blocks]);
        od;

        ## now all results in the current dimension have been computed
        Add(list_with_all_results, results_in_current_dimension);
        current_dimension := current_dimension + 1;

    #### even-dimensional case ####
    else

        for i in [1 .. nr_conjugacy_classes] do
```

```

            current_class_real := conjugacy_classes_in_current_dimension[i];
            current_class := StructuralCopy(current_class_real);


            ### square block cases ###
            # we have separate function for this case
            if Length(current_class) = 1  and current_class[1][2] = 2 then
                # then class is square of odd block as no splitting occurs as length is 1

                current_blocks := squareblock(current_dimension, characteristic)[1];

            elif Length(current_class) = 2 and current_class[1][2] = 2 and current_class[2] = "a" then
                # square of even block, a-class

                current_blocks := squareblock(current_dimension, characteristic)[1];

            elif Length(current_class) = 2 and current_class[1][2] = 2 and current_class[2] = "b" then
                # square of even block, b-class

                # take half-spin^- representation of the a-class, which is the half-spin^+ representation of the b-class
                current_blocks := squareblock(current_dimension, characteristic)[2];


            ### class contains block of size 1 ###
            # work with restriction
            elif current_class[1][1] = 1 then # 1-blocks always come first

                results_in_lower_dimension := list_with_all_results[current_dimension - 1];
                classes_in_lower_dimension := results_in_lower_dimension{[ 1.. Length(results_in_lower_dimension)]}[1];
                restricted_class := class_restriction(current_class);
                # the restricted class is in odd dimension and will not split

                # restriction of half-spin^+ representation is the spin representaion in lower dimension
                pos_restricted := Position(classes_in_lower_dimension, restricted_class);
                current_blocks := results_in_lower_dimension[pos_restricted][2];


            ### other composite classes ###
```

```
            # work with tensor product
            else

                # decompose the given class using the auxiliary function
                tensor_data := tensor_decomp(current_class);

                # this is the l appearing in the morphism of algebraic groups Spin(l) x Spin(n-l) -> Spin(n) from which we obtain our current class
                dimension_l := tensor_data[1];

                # get the results and classes from the lower dimensions
                results_in_dimension_l := list_with_all_results[dimension_l];
                classes_in_dimension_l := results_in_dimension_l{[ 1 .. Length(results_in_dimension_l) ]}[1];
                results_in_rest_dimension := list_with_all_results[current_dimension - dimension_l];
                classes_in_rest_dimension := results_in_rest_dimension{[ 1 .. Length(results_in_rest_dimension) ]}[1];

                ## case that l and n-l are both odd ##
                # just get tensor product of the lower dimensional results; there is no splitting
                if dimension_l mod 2 = 1 then

                    class_l := tensor_data[2];
                    class_rest := tensor_data[3];

                    pos_l := Position(classes_in_dimension_l, class_l);
                    pos_rest := Position(classes_in_rest_dimension, class_rest);

                    blocks_l := results_in_dimension_l[pos_l][2];
                    blocks_rest := results_in_rest_dimension[pos_rest][2];

                    current_blocks := blocks_of_tensor_product(blocks_l, blocks_rest, characteristic);

                ## case that l and n-l are both even ##
                # half-spin^+ representation is direct sum of tensor product of both half-spin^+ representations of lower dimensions and the tensor product of both half-spin^- representations of lower dimensions
                else

                    # case that current class is split, a-part
                    if current_class[Length(current_class)] = "a" then
                        # here, first and second class of tensor decomp have to split
```

```

                       class_l_a := tensor_data[3];
                       class_l_b := tensor_data[4];
                       class_rest_a := tensor_data[5];
                       class_rest_b := tensor_data[6];

                       pos_l_a := Position(classes_in_dimension_l, class_l_a);
                       pos_l_b := Position(classes_in_dimension_l, class_l_b);
                       pos_rest_a := Position(classes_in_rest_dimension, class_rest_a);
                       pos_rest_b := Position(classes_in_rest_dimension, class_rest_b);

                       blocks_l_a := results_in_dimension_l[pos_l_a][2];
                       blocks_l_b := results_in_dimension_l[pos_l_b][2];
                       blocks_rest_a := results_in_rest_dimension[pos_rest_a][2];
                       blocks_rest_b := results_in_rest_dimension[pos_rest_b][2];

                       # tensor prod of both half-spin^+ representations of lower dimensions
                       first_blocks := blocks_of_tensor_product(blocks_l_a, blocks_rest_a, characteristic);

                       # tensor prod of both half-spin^- representations of lower dimensions
                       second_blocks := blocks_of_tensor_product(blocks_l_b, blocks_rest_b, characteristic);

                       # direct sum of these
                       current_blocks := Concatenation(first_blocks, second_blocks);



                    # case that original class is split, b-part
                    elif current_class[Length(current_class)] = "b" then
                        # this class gets the half-spin^- representation of the a-part

                        class_l_a := tensor_data[3];
                        class_l_b := tensor_data[4];
                        class_rest_a := tensor_data[5];
                        class_rest_b := tensor_data[6];

                        pos_l_a := Position(classes_in_dimension_l, class_l_a);
                        pos_l_b := Position(classes_in_dimension_l, class_l_b);
                        pos_rest_a := Position(classes_in_rest_dimension, class_rest_a);
```

```
                        pos_rest_b := Position(classes_in_rest_dimension, class_rest_b);

                        blocks_l_a := results_in_dimension_l[pos_l_a][2];
                        blocks_l_b := results_in_dimension_l[pos_l_b][2];
                        blocks_rest_a := results_in_rest_dimension[pos_rest_a][2];
                        blocks_rest_b := results_in_rest_dimension[pos_rest_b][2];

                        # tensor product of half-spin^+ in dimension l and half-spin^- in dimension n-l
                        first_blocks := blocks_of_tensor_product(blocks_l_a, blocks_rest_b, characteristic);

                        # tensor product of half-spin^- in dimension l and half-spin^+ in dimension n-l
                        second_blocks := blocks_of_tensor_product(blocks_l_b, blocks_rest_a, characteristic);

                        # direct sum of these
                        current_blocks := Concatenation(first_blocks, second_blocks);

                    # original class is not split
                    else

                    # the first class has to split since l is even heres; second class then cannot split

                        class_l_a := tensor_data[3];
                        class_l_b := tensor_data[4];
                        class_rest := tensor_data[5];

                        pos_l_a := Position(classes_in_dimension_l, class_l_a);
                        pos_l_b := Position(classes_in_dimension_l, class_l_b);
                        pos_rest := Position(classes_in_rest_dimension, class_rest);

                        blocks_l_a := results_in_dimension_l[pos_l_a][2];
                        blocks_l_b := results_in_dimension_l[pos_l_b][2];
                        blocks_rest := results_in_rest_dimension[pos_rest][2];

                        # tensor prod of both half-spin^+ representations of lower dimensions
                        first_blocks := blocks_of_tensor_product(blocks_l_a, blocks_rest, characteristic);

                        # tensor prod of both half-spin^-
```

```
representations of lower dimensions
                        second_blocks := blocks_of_tensor_product(
blocks_l_b, blocks_rest, characteristic);

                        # direct sum of these
                        current_blocks := Concatenation(first_blocks,
 second_blocks);


                    fi;

                fi;

            fi;


        ## now current blocks have been computed

        Add(results_in_current_dimension, [current_class_real,
current_blocks]);


        od;

    ## now all results in the current dimension have been computed
    Add(list_with_all_results, results_in_current_dimension);
    current_dimension := current_dimension + 1;

    fi;

od;



## now for the printing

results_in_given_dimension := list_with_all_results[dimension];
Print("Printing the results in dimension ", dimension, " in
characteristic ", characteristic, "\n");
Print("\n");

nr_classes := Length(results_in_given_dimension);
for j in [1 .. nr_classes] do

    class := results_in_given_dimension[j][1];
    blocks := results_in_given_dimension[j][2];
    Sort(blocks);
    blocks := Collected(blocks);

    Print("Class label: ");
    for k in [1 .. Length(class) - 1] do # get rid of outer brackets
        Print(class[k], ", ");
    od;
    Print(class[Length(class)], "\n");

    Print("Jordan blocks: ");
```

```
        for k in [1 .. Length(blocks) - 1] do # get rid of outer brackets
            Print(blocks[k], ", ");
        od;
        Print(blocks[Length(blocks)], "\n");
        Print("\n");

    od;

end;
```

Bibliography

[ABS64] M. F. Atiyah, R. Bott, and A. Shapiro, *Clifford Modules*, Topology **3, Supplement 1** (1964), 3-38.

[Bor91] A. Borel, *Linear Algebraic Groups*, 2nd ed., Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991.

[Bou74] N. Bourbaki, *Algebra I*: *Chapters 1-3*, Hermann, Paris, 1974.

[BtD85] T. Bröcker and T. tom Dieck, *Representations of Compact Lie Groups*, Graduate Texts in Mathematics, vol. 98, Springer-Verlag, New York, 1985.

[Bum13] D. Bump, *Lie Groups*, 2nd ed., Graduate Texts in Mathematics, vol. 225, Springer-Verlag, New York, 2013.

[Che97] C. Chevalley, *The Algebraic Theory of Spinors and Clifford Algebras*, Collected Works, vol. 2, Springer-Verlag, Berlin, 1997.

[EKM08] R. Elman, N. Karpenko, and A. Merkurjev, *The Algebraic and Geometric Theory of Quadratic Forms*, Colloquium Publications, vol. 56, American Mathematical Society, Providence, Rhode Island, 2008.

[Gec03] M. Geck, *An Introduction to Algebraic Geometry and Algebraic Groups*, Oxford Graduate Texts in Mathematics, vol. 10, Oxford University Press, Oxford, 2003.

[GM16] M. Geck and G. Malle, *Reductive Groups and Steinberg Maps* (2016), available at `https://arXiv.org/abs/1608.01156`.

[GW09] R. Goodman and N. R. Wallach, *Symmetry, Representations and Invariants*, Graduate Texts in Mathematics, vol. 255, Springer-Verlag, New York, 2009.

[GLS97] D. Gorenstein, R. Lyons, and R. Solomon, *The Classification of the Finite Simple Groups, Number 3*, Mathematical Surveys and Monographs, vol. 40.3, American Mathematical Society, Providence, Rhode Island, 1997.

[Gro02] L. C. Grove, *Classical Groups and Geometric Algebra*, Graduate Studies in Mathematics, vol. 39, American Mathematical Society, Providence, Rhode Island, 2002.

[Hum95a] J. E. Humphreys, *Conjugacy Classes in Semisimple Algebraic Groups*, Mathematical Surveys and Monographs, vol. 43, American Mathematical Society, Providence, Rhode Island, 1995.

[Hum95b] ———, *Linear Algebraic Groups*, Corrected fourth printing, Graduate Texts in Mathematics, vol. 21, Springer-Verlag, New York, 1995.

[Isa76] I. M. Isaacs, *Character Theory of Finite Groups*, Academic Press, New York, 1976.

[Jac89] N. Jacobson, *Basic Algebra II*, 2nd ed., W. H. Freeman and Company, New York, 1989.

[Knu91] M.-A. Knus, *Quadratic and Hermitian Forms over Rings*, Grundlehren der mathematischen Wissenschaften, vol. 294, Springer-Verlag, Berlin Heidelberg, 1991.

[KMRT98] M.-A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol, *The Book of Involutions*, Colloquium Publications, vol. 44, American Mathematical Society, Providence, Rhode Island, 1998.

[Kor19] M. Korhonen, *Jordan blocks of unipotent elements in some irreducible representations of classical groups in good characteristic*, Proc. Amer. Math. Soc. **147** (2019), 4205-4219.

[Lam05] T. Y. Lam, *Introduction to Quadratic Forms over Fields*, Graduate Studies in Mathematics, vol. 67, American Mathematical Society, Providence, Rhode Island, 2005.

[Lan02] S. Lang, *Algebra*, Revised third edition, Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[LM89] H. B. Lawson and M.-L. Michelsohn, *Spin Geometry*, Princeton University Press, Princeton, New Jersey, 1989.

[Law95] R. Lawther, *Jordan block sizes of unipotent elements in exceptional algebraic groups*, Communications in Algebra **23** (1995), no. 11, 4125-4145.

[LS12] M. W. Liebeck and G. M. Seitz, *Unipotent and Nilpotent Classes in Simple Algebraic Groups and Lie Algebras*, Mathematical Surveys and Monographs, vol. 180, American Mathematical Society, Providence, Rhode Island, 2012.

[Lou01] P. Lounesto, *Clifford Algebras and Spinors*, 2nd ed., London Mathematical Society Lecture Note Series, vol. 286, Cambridge University Press, Cambridge, 2001.

[MT11] G. Malle and D. Testerman, *Linear Algebraic Groups and Finite Groups of Lie Type*, Cambridge Studies in Advanced Mathematics, vol. 133, Cambridge University Press, Cambridge, 2011.

[Mei13] E. Meinrenken, *Clifford Algebras and Lie Theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics, vol. 58, Springer-Verlag, Berlin Heidelberg, 2013.

[NT89] H. Nagao and Y. Tsushima, *Representations of Finite Groups*, Academic Press, Boston, 1989.

[Nav98] G. Navarro, *Characters and Blocks of Finite Groups*, London Mathematical Society Lecture Note Series, vol. 250, Cambridge University Press, Cambridge, 1998.

[Spr98] T. A. Springer, *Linear Algebraic Groups*, 2nd ed., Modern Birkhäuser Classics, Birkhäuser, Boston, 1998.

[Sri64] B. Srinivasan, *The Modular Representation Ring of a Cyclic p-Group*, Proc. London Math. Soc. **14** (1964), 677-688.

[Ste65] R. Steinberg, *Regular elements of semi-simple algebraic groups*, Publications mathématiques de l'I.H.É.S. **25** (1965), 49-80.

[Tay92] D. E. Taylor, *The Geometry of the Classical Groups*, Sigma Series in Pure Mathematics, vol. 9, Heldermann Verlag, Berlin, 1992.

[TZ13] D. Testerman and A. Zalesski, *Irreducibility in algebraic groups and regular unipotent elements*, Proc. Amer. Math. Soc. **141** (2013), 13-28.

[Var04] V. S. Varadarajan, *Supersymmetry for Mathematicians: An Introduction*, Courant Lecture Notes, vol. 11, American Mathematical Society, Providence, Rhode Island, 2004.