On Structural Aspects of Finite Simple Groups of Lie Type

by

Johanna Maria Rämö

A thesis submitted for the degree of Doctor of Philosophy

January 2011

School of Mathematical Sciences

Queen Mary, University of London

Abstract

In this PhD thesis, we consider two problems that are related to finite simple groups of Lie type. First of them is a problem mentioned in the Kourovka notebook: describe the finite simple groups in which every element is a product of two involutions. We consider the simple orthogonal groups in even characteristic, and solve the problem for them. Since other groups have been dealt with elsewhere, the problem is then solved completely.

The second part of the thesis is related to Lie algebras. Every complex simple Lie algebra has a compact real form that is associated with a compact Lie group. In this thesis, we consider the Lie algebra of type E_8, and give a new construction of its compact real form. The Lie product is defined using the irreducible subgroup of shape $2^{5+10} \cdot \mathrm{GL}_5(2)$ of the automorphism group.

Acknowledgements

I would like to thank my supervisor Robert Wilson without whom this thesis would not have been possible. I also wish to thank John Bray for filling in for Rob when he was away, Jokke Häsä for reading my work with his eagle eyes, and family and friends for helping me keep in mind that there is more to life than one's doctoral thesis.

Haluan kiittää ohjaajaani Robert Wilsonia, jota ilman tästä väitöskirjasta ei olisi tullut mitään. Kiitokset myös John Braylle, joka oli ohjaajani Robin poissa ollessa, Jokke Häsälle ja hänen haukansilmilleen sekä perheelle ja ystäville, jotka muistuttivat minua siitä, että elämässä on muutakin kuin väitöskirja.

Contents

List of Figures

List of Tables

Part I

Introduction

This thesis has two parts, both of which are related to finite simple groups of Lie type. The first part concerns Problem 14.82 in the Kourovka notebook [21]: describe the finite simple groups in which every element is a product of two involutions. A group is called strongly real if for every element there is an involution that conjugates the element to its inverse. Now the problem can be reformulated as follows: which finite simple groups are strongly real?

Here we consider the orthogonal groups in even characteristic, finding the sufficient and necessary conditions for these groups to be strongly real.

Theorem A. *Suppose that n and q are even. The finite simple group $\Omega_n^\varepsilon(q)$ is strongly real if and only if $4 \mid n$.*

The above theorem together with results proved elsewhere gives the following two corollaries:

Corollary 1. *A finite simple group is strongly real if and only if it is one following:*

i) $\mathrm{PSp}_{2n}(q)$ *where* $q \not\equiv 3 \pmod 4$ *and* $n \geq 1$*;*

ii) $\mathrm{P}\Omega_{2n+1}(q)$ *where* $q \equiv 1 \pmod 4$ *and* $n \geq 3$*;*

iii) $\mathrm{P}\Omega_9(q)$ *where* $q \equiv 3 \pmod 4$*;*

iv) $\mathrm{P}\Omega_{4n}^+(q)$ *where* $q \not\equiv 3 \pmod 4$ *and* $n \geq 3$*;*

v) $\mathrm{P}\Omega_{4n}^-(q)$ *where* $n \geq 2$*;*

vi) $\mathrm{P}\Omega_8^+(q)$ *or* ${}^3D_4(q)$*;*

vi) A_{10}*,* A_{14}*,* J_1*, or* J_2*.*

Corollary 2. *A finite simple group is strongly real if and only if it is real.*

We also study the unipotent elements of simple orthogonal groups, and show that in even characteristic and dimension they are always strongly real.

Theorem B. *When n and q are even, the unipotent elements of the finite simple group $\Omega_n^\varepsilon(q)$ are strongly real.*

The second part of the thesis concerns the Lie algebra of type E_8 and a group G of shape $2^{5+10} \cdot \mathrm{GL}_5(2)$, which is an irreducible subgroup of the automorphism group of E_8. A real semisimple Lie algebra is compact if its Killing form is negative definite, and every simple complex Lie algebra has a compact real form. Compact Lie algebras are associated with compact Lie groups. The main result of the second part of this thesis is a new construction of the compact real form of the complex Lie algebra E_8.

Recently, Wilson has given new, elementary constructions of the compact real forms of the exceptional Lie algebras G_2 [30], F_4 and E_6 [28]. He used a group of automorphisms of the Lie algebra in determining the Lie product, and we will adopt a similar approach in the case of E_8.

In the new construction the Lie algebra is written as a direct sum of 31 mutually orthogonal Cartan subalgebras. These 8-dimensional subalgebras are all copies of the real octonion algebra. The Lie product is then defined to be the unique bilinear product that is preserved in the action of the group G of shape $2^{5+10} \cdot \mathrm{GL}_5(2)$.

The first part of this thesis has been published in the Journal of Group Theory [22], and the second part submitted to a refereed journal [23].

Notation In this thesis, linear transformations and permutations are written on the right. The conjugate $b^{-1}ab$ is denoted as a^b, and the commutator $a^{-1}b^{-1}ab$ as $[a, b]$.

Part II

Strongly real elements of orthogonal groups

Chapter 1

Strongly real elements of finite simple groups

1.1 Finite simple groups

A group G is *simple* if has exactly two normal subgroups, $\{1\}$ and G. The trivial group $\{1\}$ is not simple. The finite simple groups are often called the building blocks of finite groups, as every finite group has a composition series with simple composition factors. The Jordan–Hölder Theorem states that the choice of composition series does not affect the set of composition factors.

One of the greatest achievements of finite group theory is the Classification theorem for finite simple groups.

Theorem 1.1. *Every finite simple group is isomorphic to one of the following groups:*

1. *a cyclic group C_p of prime order p;*
2. *an alternating group A_n, where $n \geq 5$;*
3. *a group of Lie type:*
    - *a) a classical group:*
        - *linear groups:* $\mathrm{PSL}_n(q)$, $n \geq 2$, *except for* $\mathrm{PSL}_2(2)$ *and* $\mathrm{PSL}_2(3)$;

unitary groups: $\mathrm{PSU}_n(q)$, $n \geq 3$, *except for* $\mathrm{PSU}_3(2)$;

symplectic groups: $\mathrm{PSp}_{2n}(q)$, $n \geq 2$, *except for* $\mathrm{PSp}_4(2)$;

orthogonal groups:

$\mathrm{P}\Omega_{2n+1}(q)$, $n \geq 3$, q *odd;*

$\mathrm{P}\Omega^+_{2n}(q)$, $n \geq 4$;

$\mathrm{P}\Omega^-_{2n}(q)$, $n \geq 4$;

b) an exceptional group of Lie type:

$$G_2(q),\ q \geq 3, \quad F_4(q), \quad E_6(q), \quad {}^2E_6(q), \quad {}^3D_4(q), \quad E_7(q), \quad E_8(q),$$
$${}^2B_2(2^{2n+1}),\ n \geq 1, \quad {}^2G_2(3^{2n+1}),\ n \geq 1, \quad {}^2F_4(2^{2n+1}),\ n \geq 1, \quad {}^2F_4(2)';$$

4. one of the 26 sporadic groups:

$$\mathrm{M}_{11},\ \mathrm{M}_{12},\ \mathrm{M}_{22},\ \mathrm{M}_{23},\ \mathrm{M}_{24},\ \mathrm{J}_1,\ \mathrm{J}_2,\ \mathrm{J}_3,\ \mathrm{J}_4,\ \mathrm{HS},\ \mathrm{McL},\ \mathrm{Suz},\ \mathrm{Ly},\ \mathrm{He},$$
$$\mathrm{Ru},\ \mathrm{O'N},\ \mathrm{Co}_1,\ \mathrm{Co}_2,\ \mathrm{Co}_3,\ \mathrm{Fi}_{22},\ \mathrm{Fi}_{23},\ \mathrm{Fi}'_{24},\ \mathrm{Th},\ \mathrm{HN},\ \mathbb{B},\ \mathbb{M}$$

More information on the classification theorem and the definitions of the groups can be found for example in the book series of Gorenstein et al. (see [11]), in the Atlas of finite groups [5] or in the book of Wilson [29].

1.2 Strongly real elements

An element of a group is called an *involution* if its order is 2.

Definition 1.2. An element g of the group G is called *real* if there exists $x \in G$ such that $x^{-1}gx = g^{-1}$. The element g is called *strongly real* if there exists an involution $i \in G$ such that $i^{-1}gi = g^{-1}$.

A group whose elements are real is called real, and a group whose elements are strongly real is called strongly real. An element of a group is real if and only if all of its complex character values are real.

All involutions are strongly real. Namely, if G is a group and $g \in G$ is an involution, we have $g^{-1}gg = g = g^{-1}$. Also, elements that are products of two involutions are strongly real. If $g = ab$ for some involutions a and b, then

$$a^{-1}ga = a^{-1}aba = ba = b^{-1}a^{-1} = g^{-1},$$

Also the involution b conjugates g to its inverse.

The converse is not necessarily true: strongly real elements are not always products of two involutions. For example, in the symmetric group S_3 the permutation (12) is strongly real since it is an involution. However, (12) is not a product of two involutions of S_3. In fact, involutions are the only elements that may be strongly real without being products of two involutions.

If $g \in G$ is strongly real, and $i \in G$ is an involution that takes g to its inverse, then

$$g = (gi)i \quad \text{and} \quad (gi)^2 = 1.$$

Now the order of the product gi is either one or two, and if g is not an involution, we know for certain that the order is two. Hence, if a strongly real element is not an involution, it is a product of two involutions. Except for the cyclic group of order two, any involution of a finite simple group is a product of two involutions, and hence all strongly real elements in finite simple groups are products of two involutions.

Lemma 1.3. *In a non-commutative finite simple group an element is strongly real if and only if it is a product of two involutions.*

Proof. Suppose that G is a non-commutative finite simple group. By the above discussion, it is enough to prove that every involution of G is a product of two involutions. Assume that $t \in G$ is an involution that is not a product of two involutions. If there is an element z of $C_G(t) \setminus \{t\}$ that is a conjugate of t, then $t = z(zt)$ is a product of two involutions. This is a contradiction, so such element does not exist and

$$\{t^g \mid g \in G\} \cap C_G(t) = \{t\}.$$

By the Glauberman Z^*-theorem ([1], Section 48, p. 261), we have

$$tO_{2'}(G) \in Z(G/O_{2'}(G)).$$

Here $O_{2'}(G)$ is the largest normal subgroup of G whose order is not divisible by 2.

By the Odd order theorem of Feit and Thompson ([1], Section 48, p. 260), groups of odd order are soluble, so the order of G must be even. It follows that $O_{2'}(G) = \{1\}$, and

$$t \in Z(G) = \{1\}.$$

This is a contradiction, and hence every element of G is a product of two involutions. □

1.2.1 Previous results

A group cannot be strongly real if it is not real. Tiep and Zalesski [27] have classified all finite quasisimple groups that are real, and this classification can be used in eliminating groups that are not strongly real.

The group G is *quasisimple* if $G/Z(G)$ is a simple group and $G = G'$, where G' is the commutator subgroup of G. In particular, simple groups are quasisimple.

Theorem 1.4. *Let G be a finite quasisimple group. All elements in G are real if and only if one of the following holds:*

i) G *is a quotient of* $\mathrm{Sp}_{2n}(q)'$ *with* $q \not\equiv 3 \pmod 4$ *and* $n \geq 1$*;*

ii) $G = \Omega_{2n+1}(q)$ *with* $q \equiv 1 \pmod 4$ *and* $n \geq 3$*;*

iii) $G = \Omega_9(q)$ *and* $q \equiv 3 \pmod 4$*;*

iv) $G = \mathrm{P}\Omega^+_{4n}(q)$ *or* $G = \Omega^+_{4n}(q)$*, where* $q \not\equiv 3 \pmod 4$ *and* $n \geq 3$*;*

v) G *is a quotient of* $\mathrm{Spin}^-_{4n}(q)$ *with* $n \geq 2$*;*

vi) $G = {}^3D_4(q)$ *or* $G/Z(G) = \mathrm{P}\Omega^+_8(q)$*;*

vii) $G = A_{10}$*,* $G = A_{14}$*,* $G = \mathrm{J}_1$ *or* $G = \mathrm{J}_2$*.*

Proof. See [27], Theorem 1.2. □

Not all real groups are strongly real. For example, the quaternion group

$$\mathbb{H} = \{\pm 1,\ \pm i,\ \pm j,\ \pm k\}$$

is real. However, this group is not strongly real since the only involutions are 1 and -1, and they are in the centre of the group.

For most finite simple groups it is already known whether they are strongly real, or equivalently, whether their elements are products of two involutions.

Theorem 1.5. *The alternating group A_n is strongly real if and only if $n \in \{5, 6, 10, 14\}$.*

Proof. The theorem was proved by Bagiński [2]. □

Theorem 1.6. *The symplectic group $\mathrm{PSp}_{2n}(q)$ is strongly real if and only if $q \not\equiv 3 \pmod 4$.*

Proof. Ellers and Nolte [7] as well as Gow [12] have proved that in $\mathrm{PSp}_{2n}(q)$ every element is a product of two involutions when q is even. Gow [13] has proved that the elements of $\mathrm{PSp}_{2n}(q)$ are products of two involutions if $q \equiv 1 \pmod 4$.

From Theorem 1.4 it follows that $\mathrm{PSp}_{2n}(q)$ is not strongly real if $q \equiv 3 \pmod 4$. □

Theorem 1.7. *Suppose that q is odd. Then the orthogonal group $\mathrm{P}\Omega_n^\varepsilon(q)$ is strongly real if and only if one of the following holds:*

i) n is odd, $n \geq 7$ and $q \equiv 1 \pmod 4$;

ii) $n = 9$ and $q \equiv 3 \pmod 4$;

iii) $4|n$, $n \geq 12$, $q \not\equiv 3 \pmod 4$ and $\varepsilon = +$;

iv) $4|n$, $n \geq 8$ and $\varepsilon = -$;

v) $n = 8$ and $\varepsilon = +$.

Proof. The theorem was proved by Knüppel and Thomsen [18]. Galt [9] has independently obtained the same results for some of the orthogonal groups. □

Theorem 1.8. *Of the sporadic groups, only* J_1 *and* J_2 *are strongly real.*

Proof. Kolesnikov and Nuzhin [19] have proved that J_1 and J_2 are strongly real. By Theorem 1.4, other sporadic groups are not strongly real. □

Recently, Galt and Vdovin [10] have considered the exceptional group ${}^3D_4(q)$ proving the following theorem.

Theorem 1.9. *The group* ${}^3D_4(q)$ *is strongly real.*

From Theorem 1.4 of Tiep and Zalesski it follows that all the finite simple groups considered thus far are strongly real if and only if they are real.

By the Classification theorem for finite simple groups and Theorem 1.4 of Tiep and Zalesski, there is only one type of finite simple groups that is real and not mentioned among the above results. It is the orthogonal group of type $\mathrm{P}\Omega^{\varepsilon}_{4n}(q)$, where q is even. In this thesis, we will prove that these groups are strongly real, and hence a finite simple group is strongly real if and only if it is real.

Chapter 2

Orthogonal groups

In this chapter we define the orthogonal groups and their subgroups that give rise to the finite simple orthogonal groups. All classical groups consist of linear transformations of a vector space that preserve a certain geometry, or *form* on the space. In the case of orthogonal groups, one has to look at symmetric bilinear forms and quadratic forms. The material introduced in this section can be found in the books of Grove [15] and Taylor [25].

2.1 Forms and orthogonal transformations

Assume that V is a finite-dimensional vector space over a field F. A *bilinear form* is a mapping $B: V \times V \to F$ such that

$$\begin{aligned} B(v+w,u) &= B(v,u) + B(w,u) \\ B(v,w+u) &= B(v,w) + B(v,u) \\ B(\alpha v,w) &= \alpha B(v,w) \\ B(v,\alpha w) &= \alpha B(v,w) \end{aligned}$$

for all $v, w, u \in V$ and $\alpha \in F$. A bilinear form B of V is called *symmetric* if

$$B(v,w) = B(w,v) \quad \text{for all } v, w \in V.$$

A *quadratic form* of V is a mapping $Q: V \to F$ satisfying

$$Q(\alpha v + \beta w) = \alpha^2 Q(v) + \alpha\beta B(v, w) + \beta^2 Q(w)$$

for all $v, w \in V$ and $\alpha, \beta \in F$, where B is a symmetric bilinear form. The form B is called the *associated bilinear form* of Q.

Example 2.1. The mapping $\mathbb{R}^n \to \mathbb{R}^n$, $(x_1, x_2, \ldots, x_n) \mapsto x_1^2 + x_2^2 + \cdots + x_n^2$ is a quadratic form of $\mathbb{R}^n$. The associated bilinear form is twice the ordinary inner product of $\mathbb{R}^n$.

Let W be a 2-dimensional vector space over the field $\mathbb{F}_3$ with basis $\{v_1, v_2\}$. If $x \in V$, we write $x = x_1 v_1 + x_2 v_2$, where $x_1, x_2 \in \mathbb{F}_3$. The mapping

$$Q_W: W \to \mathbb{F}_3, \quad Q_W(x) = x_1^2 + x_1 x_2 + \frac{1}{2} x_2^2$$

is a quadratic form of W. The associated bilinear form is

$$B_W: W \times W \to \mathbb{F}_3, \quad B(x, y) = 2x_1 y_1 + x_1 y_2 + x_2 y_1 + x_2 y_2.$$

If B is a symmetric bilinear form of V, the vectors $v_1, v_2 \in V$ are said to be *mutually orthogonal* if $B(v_1, v_2) = 0$. Similarly, subspaces V_1 and V_2 of V are mutually orthogonal if $B(v_1, v_2) = 0$ for all $v_1 \in V_1$ and $v_2 \in V_2$.

Note that quadratic forms determine the associated bilinear forms. If Q is a quadratic form and B the associated bilinear form, then

$$B(v, w) = Q(v + w) - Q(v) - Q(w)$$

for all $v, w \in F$. If the characteristic of F is odd, then the converse is also true. Since

$$Q(2v) = Q(v + v) = Q(v) + B(v, v) + Q(v)$$

and on the other hand $Q(2v) = 4Q(v)$, it follows that

$$Q(v) = \frac{1}{2} B(v, v).$$

If the characteristic of F is even, this does not hold. In fact, in that case $B(v, v) = 0$ for all $v \in V$.

If we choose some basis $\{v_1, v_2, \ldots, v_n\}$ for the vector space V, then the bilinear form B can be written as a matrix $\hat{B} = [b_{ij}]$, where $b_{ij} = B(v_i, v_j)$ for all i, j. Now it holds for all row vectors v and w that

$$B(v, w) = v\hat{B}w^\top,$$

where $w^\top$ is the transpose of w. The bilinear form B and matrix $\hat{B}$ are usually identified.

Example 2.2. If we choose the natural basis for the vector space $\mathbb{R}^n$, then matrix corresponding to the inner product of $\mathbb{R}^n$ is the identity matrix. The matrix corresponding to the bilinear form B_W of Example 2.1 is

$$\hat{B}_W = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}.$$

If B is a symmetric bilinear form of V, then the subspace

$$\mathrm{rad}(B) = \{v \in V \mid B(v, w) = 0 \text{ for all } w \in V\}.$$

is called the *radical* of B. The form B is *non-degenerate* if $\mathrm{rad}(B) = \{0\}$. Let Q be a quadratic form of V with the associated bilinear form B. The subspace

$$\mathrm{rad}(Q) = \{v \in \mathrm{rad}(B) \mid Q(v) = 0\}.$$

is the radical of Q. The form Q is called *non-singular* if $\mathrm{rad}(Q) = \{0\}$. In odd characteristic, the radicals of Q and B coincide.

Vector spaces endowed with non-singular quadratic forms give rise to the orthogonal groups. If V is a such a vector space, then a linear transformation T of V is called *orthogonal* if

$$Q(vT) = Q(v) \quad \text{for all } v \in V.$$

The orthogonal transformations of V form the *orthogonal group* $\mathrm{O}(V)$. Notice that the structure of the orthogonal group depends on the orthogonal form of V, and different forms may give different groups.

If the characteristic of F is odd, then the bilinear form determines the quadratic form, and a transformation is orthogonal precisely when it preserves the bilinear form.

In other words, if Q is a quadratic form with the associated bilinear form B, then T is orthogonal if and only if

$$B(vT, wT) = B(v, w)$$

for all $v, w \in V$. By bilinearity, it suffices to check this for all basis vectors.

If the characteristic of F is even, the situation is more complicated. In order for the transformation T to preserve the quadratic form Q, we must have both $B(vT, wT) = B(v, w)$ and $Q(vT) = Q(v)$ for all basis vectors $v, w \in V$.

The above definitions can also be expressed in matrix notation. Let $\hat{T}$ be the row matrix corresponding to the linear transformation T, and $\hat{B}$ the matrix of the bilinear form B. Now T preserves B if and only if

$$\hat{T}\hat{B}\hat{T}^{\top} = \hat{B}.$$

The orthogonal transformations can be thought of as linear mappings that preserve distances and angles. In the case of $\mathbb{R}^2$ and inner product, all reflections and rotations are orthogonal transformations. If the vector space W of Example 2.1 is equipped with the quadratic form Q_W, then the elements of the orthogonal group $O(W)$ are

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix},$$
$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

This group is in fact isomorphic to the dihedral group D_8.

Sometimes two different orthogonal forms give rise to the same orthogonal group. Two forms are said to be *equivalent* if they become equal after a change of basis. More formally, the orthogonal forms Q_1 and Q_2 of V are equivalent if there exists a linear isomorphism $T: V \to V$ such that

$$Q_1(vT) = Q_2(v)$$

for all $v \in V$. Similarly, bilinear forms B_1 and B_2 of V are said to be equivalent if $B_1(vT, wT) = B_2(v, w)$ for all $v, w \in V$ and some transformation T. In matrix notation,

this happens precisely when

$$\hat{T}\hat{B}_1\hat{T}^\top = \hat{B}_2.$$

If two orthogonal forms are equivalent, then the groups that they define are conjugate to each other. If T is the linear transformation that determines the change of basis, the orthogonal groups are conjugate to each other by T. Since equivalent forms give isomorphic groups, we will identify such forms.

If Q is a quadratic form of V and $\alpha \in F$, then $Q_\alpha : v \mapsto \alpha Q(v)$ is also a quadratic form of V. We say that the form Q_α is obtained from Q by *scaling*. The forms Q and Q_α determine the same orthogonal group, and therefore we do not need to distinguish between the two.

If the order of the field F is finite, then, up to equivalence and scaling, there are at most two non-singular quadratic forms on V.

Proposition 2.3. *Suppose that the field F is finite, and Q is a non-singular quadratic form of V.*

a) If $\dim(V) = 2m+1$, then, after scaling, there is a basis $\{v_1, v_2, \ldots, v_{2m+1}\}$ such that

$$Q\left(\sum_{i=1}^{2m+1} a_i v_i\right) = \sum_{i=1}^{m} a_i a_{i+m} + a_{2m+1}^2$$

for all $a_i \in F$.

b) If $\dim(V) = 2m$, there exists a basis $\{v_1, v_2, \ldots, v_{2m}\}$ such that either

$$Q\left(\sum_{i=1}^{2m} a_i v_i\right) = \sum_{i=1}^{m} a_i a_{i+m}$$

or

$$Q\left(\sum_{i=1}^{2m} a_i v_i\right) = \sum_{i=1}^{m} a_i a_{i+m} + a_{2m-1}^2 + a_{2m-1}a_{2m} + b a_{2m+1}^2$$

for all $a_i \in F$, where $X^2 + X + b$ is an irreducible polynomial of $F[X]$. The first quadratic form is said to be of plus type, and the second of minus type.

Proof. The proof can be found for example in [25] (Ch. 11, p. 138). The vector space V is written as a sum of as many hyperbolic spaces as possible. A hyperbolic space is a 2-dimensional space $\langle v, w\rangle$ with a quadratic form Q such that $Q(v) = 0 = Q(w)$ and $B(v, w) = 1$, where B is the associated bilinear form. We have

$$V = L_1 \oplus L_2 \oplus \cdots \oplus L_k \oplus W,$$

where each L_i is a hyperbolic space and for the subspace W it holds that $Q(w) \neq 0$ for all $w \in W$. The dimension of W is at most two. If the dimension is 1, we have case a), and if the dimension is 0 or 2, we have case b). □

If the dimension of V is odd, the orthogonal group is denoted $\mathrm{O}^0(V)$ or simply $\mathrm{O}(V)$. In even dimension, the orthogonal group of plus type is denoted $\mathrm{O}^+(V)$, and the orthogonal group of minus type is denoted $\mathrm{O}^-(V)$. We can also write $\mathrm{O}^\varepsilon_n(q)$, where n is the dimension of V, q the order of F, and ε the type of the quadratic form. For example, the quadratic form Q_W of the vector space W is of minus type. Hence the group $O(W)$ can be written as $O_2^-(3)$.

If the characteristic of F is even and the dimension of V is odd, the orthogonal group $O(V)$ is isomorphic to another type of classical group, a *symplectic group*. Symplectic groups are determined by *alternating* bilinear forms. A bilinear form B of a vector space V is alternating if

$$B(v, v) = 0 \quad \text{for all } v \in V.$$

A vector space admits a non-degenerate alternating form if and only if its dimension is even, and if the form exists, it is unique up to equivalence. Suppose that V is a vector space equipped with an alternating form B. Linear transformations that preserve B are called symplectic transformations, and they form the symplectic group $\mathrm{Sp}(V)$. In even characteristic, symmetric forms are always alternating, and the orthogonal group $O(V)$ is a subgroup of $\mathrm{Sp}(V)$.

Proposition 2.4. *If q is even, then the groups $\mathrm{O}_{2k+1}(q)$ and $\mathrm{Sp}_{2k}(q)$ are isomorphic.*

Proof. We give the outline of the proof. The details can be found in [25] (Thm 11.9, p. 143). Assume that V is a vector space over a field F. Suppose that the dimension of V is $2k+1$, and the order of F is even. Let Q be a non-singular quadratic form of V and B the associated bilinear form. Now B is alternating. It can be shown that the radical of B is 1-dimensional, and hence the vector space $V/\operatorname{rad}(B)$ is of dimension $2k$. The form B induces an alternating bilinear form on $V/\operatorname{rad}(B)$, and every element of $O(V)$ induces a symplectic transformation of $V/\operatorname{rad}(B)$. Also, every symplectic transformation of $V/\operatorname{rad}(B)$ can be lifted to a unique orthogonal transformation of V. □

2.2 Finite simple orthogonal groups

The determinant of an orthogonal transformation is always 1 or -1. The *special orthogonal group* $\mathrm{SO}(V)$ consists of the elements of $\mathrm{O}(V)$ whose determinant is 1.

From now on, we assume that Q is a non-singular quadratic form of V with the associated bilinear form B, and the scalar field F is finite. Next, we will define the subgroup $\Omega(V)$ of $\mathrm{SO}(V)$, which, apart from a few exceptions, has a simple quotient group. In literature, one can find several different ways to define $\Omega(V)$, and not all of them agree. The definitions used here are taken from the Atlas of finite groups [5].

If the characteristic of F is odd, then $\Omega(V)$ is defined using *reflections*. If $u \in V$ and $Q(u) \neq 0$, the reflection r_u is defined by the formula

$$r_u : \ V \to V, \quad r_u(v) = v - \frac{B(v,u)}{Q(u)}u.$$

In odd characteristic, every element of $O(V)$ can be written as a product of reflections. (See [15], Thm 6.6, p. 48.)

Definition 2.5. Suppose that the characteristic of F is odd. Every $g \in SO(V)$ can be written as a product $g = r_{v_1} \cdots r_{v_r}$, where each r_{v_i} is a reflection. The element g is in the subgroup $\Omega(V)$ if the product $\prod_i Q(v_i)$ is a square in F.

In even characteristic the above definition does not make sense since all elements of

F are squares. Therefore, we need to define $\Omega(V)$ in a different way. In addition, even and odd dimensions need to be considered separately.

Definition 2.6. Suppose that the characteristic of F and dimension of V are even. The element $g \in O(V)$ is in the subgroup $\Omega(V)$ if $\mathrm{rank}(\mathrm{id}_V + g)$ is even.

In even characteristic and odd dimension the orthogonal group is isomorphic to a symplectic group. From the theory of symplectic groups it follows that, apart from a few exceptions, this symplectic group is simple. We will write $\Omega(V) = O(V)$ when the characteristic of F is even and the dimension of V is odd.

Sometimes the group $\Omega(V)$ is defined to be the commutator subgroup $\mathrm{O}(V)'$ of $\mathrm{O}(V)$. This definition agrees with ours if the dimension of V is at least 3, except for the groups $\Omega_4^+(2)$ and $\Omega_5(2)$. (See Taylor [25], Thm 11.5, p. 164, and definition of $\mathrm{SO}(V)$ on p. 160. The case of even characteristic and odd dimension is dealt with in Thm 8.7, p. 72.)

The group $\mathrm{P}\Omega(V)$ is obtained from $\Omega(V)$ by factoring out the scalars. The only scalars that may be in $\Omega(V)$ are 1 and -1, and hence

$$\mathrm{P}\Omega(V) = \frac{\Omega(V)}{\Omega(V) \cap \{1, -1\}}.$$

This group is in most cases simple. Notice that if the characteristic of F is even, then $\mathrm{P}\Omega(V) = \Omega(V)$.

Proposition 2.7. *The following orthogonal groups are simple:*

a) $\mathrm{P}\Omega_{2n+1}(q)$*, when* $n \geq 2$*, except for* $\mathrm{P}\Omega_5(2)$*;*

b) $\mathrm{P}\Omega_{2n}^+(q)$*, when* $n \geq 4$*;*

c) $\mathrm{P}\Omega_{2n}^-(q)$*, when* $n \geq 4$*.*

Proof. The proof can be found for example in the book of Taylor ([25], Thm 11.48, p. 162). Taylor defines the group $\Omega(V)$ to be $\mathrm{O}(V)'$, but this does not affect the proof, except in the case of the group $\mathrm{P}\Omega_5(2)$. This group is isomorphic to the symmetric group S_6 and hence not simple ([15], Prop. 3.13, p. 28). □

Note that the above theorem does not give a complete list of finite simple orthogonal groups. When the dimension of the vector space is small, the simple orthogonal groups are in some cases isomorphic to some other finite simple groups, for example linear groups. For simplicity, those groups have been omitted from the list.

Chapter 3

Strongly real elements of orthogonal groups in even characteristic

In this section, we consider the simple group $\Omega_n^\varepsilon(q)$, where q is even, and determine when the group is strongly real. When the characteristic is even and dimension odd, the orthogonal groups are isomorphic to symplectic groups, which we already know to be strongly real. Hence, we do not need to take them into account. Tiep and Zalesski [27] have proved that $\Omega_n^\varepsilon(q)$ is real if and only if 4 divides n. The following theorem shows that the group is strongly real if and only if it is real.

Theorem A. *Suppose that n and q are even. The finite simple group $\Omega_n^\varepsilon(q)$ is strongly real if and only if $4 \mid n$.*

The theorem will be proved by using the fact that every orthogonal transformation is a product of two orthogonal involutions.

Let V be a vector space over a finite field F whose characteristic is even. We assume that V is endowed with a non-singular quadratic form Q with the associated bilinear form B. Let S be an orthogonal transformation of V.

Theorem 3.1. *The transformation S is a product of two orthogonal involutions of V.*

Proof. The theorem has been proved by Wonenburger [31] in odd characteristic, Gow [12] and Ellers and Nolte [7] in even characteristic. Djoković [6] has independently proved the same result in all characteristics. □

It follows from the theorem that there is an orthogonal involution of V that conjugates S to its inverse. Indeed, if a transformation is a product of involutions H_1 and H_2, then either of the involutions conjugates the transformation to its inverse. We will show that in some cases these involutions are in $\Omega(V)$.

3.1 Decomposition of the vector space

In order to use Theorem 3.1, we need to understand how it is proved. All the proofs use some kind of decomposition of the vector space, and we choose a similar approach. We will use the decomposition introduced by Wonenburger, where the vector space is written as a sum of so called cyclic and bicyclic subspaces. The decomposition is related to the minimal polynomial of the transformation S. Before describing what the decomposition looks like, we introduce some definitions.

3.1.1 Cyclic and bicyclic spaces

A vector space V is called *cyclic* relative to the linear transformation S if it has a basis

$$\{v, vS, \ldots, vS^{n-1}\},$$

where v is some element of V. The element v is called a *generator* of V, and the *order* p of v is defined to be the polynomial of least degree having the property $v.p(S) = 0$. If V is a cyclic vector space relative to S, then the order p is the minimal polynomial of S, and $\deg(p) = \dim(V)$.

A vector space V is called *bicyclic* relative to S if $V = U \oplus W$, where U and W are cyclic relative to S, and have generators of the same order.

3.1.2 The reciprocal of a polynomial

Let p be a polynomial such that $p(0) \neq 0$. The *reciprocal* of p is the monic polynomial

$$\tilde{p} = p(0)^{-1} X^n p(X^{-1}),$$

where $n = \deg(p)$. The polynomial p is called *self-reciprocal* if $p = \tilde{p}$.

For example, the reciprocal of the polynomial $p = X^3 + 2X^2 - X + 5$ is

$$\tilde{p} = \frac{1}{5} X^3 \left(\frac{1}{X^3} + \frac{2}{X^2} - \frac{1}{X} + 5 \right) = \frac{1}{5} + \frac{2}{5} X - \frac{1}{5} X^2 + X^3.$$

Assume that the polynomial p is self-reciprocal. Now $p(0)^2 = 1$. Also, if p has a root α, then α^{-1} is a root of p and has the same multiplicity as α. This shows that the following lemma holds.

Lemma 3.2. *The only irreducible self-reciprocal monic polynomials of odd degree are* $X + 1$ *and* $X - 1$.

3.1.3 Decomposition

We will now describe the decomposition of Wonenburger [31]. Wonenburger considered only odd characteristic, and we cannot use the involutions defined in her paper. However, the decomposition itself does not require the characteristic to be even. The results quoted below hold in both even and odd characteristic.

Let S be an orthogonal transformation of a vector space V. We will see that the space V can be decomposed into cyclic and bicyclic subspaces that are S-invariant, non-singular, and orthogonal to each other.

Suppose that $p \in F[X]$ is the minimal polynomial of S. The transformation S is conjugate to its inverse by a linear transformation of V, and hence the minimal polynomial p is self-reciprocal ([31], p. 332). We can write

$$p = \prod_i r_i^{h_i},$$

where each $r_i \in F[X]$, and either r_i is self-reciprocal and irreducible, or $r_i = g_i \tilde{g}_i$, where g_i is irreducible but not self-reciprocal.

Denote

$$K_i = \ker(r_i(S)^{h_i}).$$

Now we have $V = \bigoplus K_i$. The subspaces K_i are non-singular and orthogonal to each other ([31], Corollary, p. 333). If $r_i = g_i\tilde{g}_i$ for some irreducible polynomial g_i, the subspace K_i can be written as a sum of cyclic subspaces that are mutually orthogonal ([31], Lemma 1, p. 334). If the polynomial r_i is self-reciprocal, the subspace K_i can be written as a sum of cyclic and bicyclic subspaces that are mutually orthogonal (see [31], Lemma 4, p. 336, and also p. 337).

Hence, each K_i is a direct sum of non-singular cyclic and bicyclic subspaces that are mutually orthogonal. Write $K_i = \bigoplus V_j$, where V_j is either cyclic or bicyclic. We have seen above that if V_j is a cyclic subspace, the minimal polynomial of $S|_{V_j}$ has one of the following forms:

a) r^h, where r is self-reciprocal and irreducible

b) $(g\tilde{g})^h$, where g is irreducible but not self-reciprocal.

If $V_j = U \oplus W$ is a bicyclic subspace, the minimal polynomial of both $S|_U$ and $S|_W$ is r^h, where r is irreducible and self-reciprocal.

Decompose the space V into cyclic and bicyclic subspaces, say $V = \bigoplus V_j$. For each subspace V_j it will be relatively easy to find an orthogonal involution H_j that conjugates $S|_{V_j}$ to its inverse. Then $H = \bigoplus H_j$ is an involution that conjugates S to its inverse. Since the subspaces are orthogonal to each other, H is an orthogonal transformation of V.

3.2 Finding the involutions

We wish to show that if the dimension of V is divisible by 4 and the transformation S is in $\Omega(V)$, the inverting involution H can be chosen in such a way that it is also an element of $\Omega(V)$. In fact, we will show that for all orthogonal transformations of V, the inverting involution can be chosen to be in $\Omega(V)$.

When the dimension of the space and characteristic of the field are both even, an element A of $O(V)$ is in $\Omega(V)$ if and only if $\text{rank}(I + A)$ is even. Hence, we just need to find an inverting involution H_j for each cyclic and bicyclic subspace V_j in the decomposition of V, and calculate $\text{rank}(I+H_j)$. Then we consider the sum of the ranks to determine whether $H = \bigoplus H_j$ is an element of $\Omega(V)$.

3.2.1 Cyclic subspaces

Suppose that we have a cyclic space $V = \langle v, vS, \dots vS^{n-1} \rangle$.

Proposition 3.3. *There is an orthogonal involution J such that $JSJ = S^{-1}$, and*

$$\text{rank}(I + J) = \begin{cases} \textit{even} & \textit{if } n \equiv 0 \textit{ or } n \equiv 1 \pmod 4 \\ \textit{odd} & \textit{if } n \equiv 2 \textit{ or } n \equiv 3 \pmod 4. \end{cases}$$

Proof. Let $vS^iJ = vS^{n-i-1}$ for all $i \in \{0, \dots, n-1\}$. With respect to the basis $\{v, vS, \dots, vS^{n-1}\}$, we can write

$$J = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

Gow ([12], Lemma 2.8, p. 587) has shown that J is an orthogonal involution that conjugates S to its inverse.

We give here another proof for the orthogonality of J, as the involution will be needed also in the bicyclic case, and we want to have a closer look at its properties. It is enough to prove that J preserves B and Q on the basis vectors. The transformation S preserves B, so it follows that

$$B(vS^iJ, vS^jJ) = B(vS^{n-i-1}, vS^{n-j-1}) = B(vS^j, vS^i)$$

for all $i, j \in \{0, \ldots, n-1\}$. This means that $JBJ^\top = B^\top$. Since B is symmetric, the involution J preserves B. Similarly,

$$Q(vS^iJ) = Q(vS^{n-i-1}) = Q(vS^i)$$

for all $i \in \{0, \ldots, n-1\}$, and we can conclude that J is orthogonal.

Since we have

$$I + J = \begin{bmatrix} 1 & 0 & \cdots & 0 & 1 \\ 0 & 1 & \cdots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & \cdots & 1 & 0 \\ 1 & 0 & \cdots & 0 & 1 \end{bmatrix},$$

the rank of $I + J$ is even if $n \equiv 0$ or $n \equiv 1 \pmod 4$, and odd if $n \equiv 2$ or $n \equiv 3 \pmod 4$. □

3.2.2 Bicyclic subspaces

Suppose now that we have a bicyclic space $V = U \oplus W$, where

$$U = \langle u, uS, \ldots uS^{n-1} \rangle \text{ and } W = \langle w, wS, \ldots wS^{n-1} \rangle.$$

We assume first that the dimension n is even.

Proposition 3.4. *There is an orthogonal involution L such that $LSL = S^{-1}$ and* $\operatorname{rank}(I + L)$ *is even.*

Proof. Let L be the linear transformation defined by $uS^iL = uS^{n-i}$ and $wS^iL = wS^{n-i}$ for all $i \in \{0, \ldots, n-1\}$. Now we can write

$$L = \begin{bmatrix} K & 0 \\ 0 & K \end{bmatrix},$$

where K some $n \times n$-matrix.

The proof of Lemma 4 in [7] shows that the involution L is orthogonal and inverts S. We notice that $\operatorname{rank}(I + L) = 2 \operatorname{rank}(I + K)$, which proves the claim. □

Unfortunately, the involution L cannot be used when n is odd because then it might not be orthogonal. Also, the involutions constructed by Ellers and Nolte in [7] are not necessarily elements of $\Omega(V)$, and cannot therefore be used here.

The case of bicyclic subspaces where n is odd is the most difficult one, and we need to know precisely what the forms B and Q look like before showing that the chosen involutions are orthogonal.

Assume that n is odd. By Lemma 3.2, the minimal polynomial of both $S|_U$ and $S|_W$ is $p = (X+1)^n$. Let $\{v_1, v_2, \ldots, v_n\}$ be a basis of U with respect to which $S|_U$ is in the Jordan normal form, and $\{v_{n+1}, v_{n+2}, \ldots, v_{2n}\}$ a basis of W with respect to which $S|_W$ is in the Jordan normal form. Now

$$\begin{aligned}
v_1 S &= v_1 \\
v_2 S &= v_1 + v_2 \\
&\vdots \\
v_n S &= v_{n-1} + v_n \\
v_{n+1} S &= v_{n+1} \\
v_{n+2} S &= v_{n+1} + v_{n+2} \\
&\vdots \\
v_{2n} S &= v_{2n-1} + v_{2n}.
\end{aligned}$$

The matrix of B can be written in block form as

$$B = \begin{bmatrix} B_1 & B_2 \\ B_3 & B_4 \end{bmatrix},$$

where the blocks correspond to the subspaces U and W with respect to $\{v_1, \ldots, v_n\}$

and $\{v_{n+1}, \ldots, v_{2n}\}$. We will show that the block B_1 is of the form

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \alpha_1 \\ 0 & 0 & \cdots & 0 & 0 & 0 & \alpha_1 & \alpha_2 \\ 0 & 0 & \cdots & 0 & 0 & \alpha_1 & \alpha_1+\alpha_2 & \alpha_3 \\ 0 & 0 & \cdots & 0 & \alpha_1 & \alpha_2 & \alpha_1+\alpha_2+\alpha_3 & \alpha_4 \\ 0 & 0 & \cdots & \alpha_1 & \alpha_1+\alpha_2 & \alpha_1+\alpha_3 & \alpha_1+\alpha_2+\alpha_3+\alpha_4 & \alpha_5 \\ \vdots & \vdots & \iddots & & & & & \vdots \\ 0 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 & \cdots & \alpha_{n-1}, \end{bmatrix}$$

for some $\alpha_i \in F$. The block B_4 also has the same form, but the entries may take different values than the entries of B_1. The block B_2 is of the form

$$\begin{bmatrix} 0 & \cdots & 0 & 0 & 0 & 0 & 0 & \beta_1 \\ 0 & \cdots & 0 & 0 & 0 & 0 & \beta_1 & \beta_2 \\ 0 & \cdots & 0 & 0 & 0 & \beta_1 & \beta_1+\beta_2 & \beta_3 \\ 0 & \cdots & 0 & 0 & \beta_1 & \beta_2 & \beta_1+\beta_2+\beta_3 & \beta_4 \\ 0 & \cdots & 0 & \beta_1 & \beta_1+\beta_2 & \beta_1+\beta_3 & \beta_1+\beta_2+\beta_3+\beta_4 & \beta_5 \\ 0 & \cdots & \beta_1 & \beta_2 & \beta_2+\beta_3 & \beta_2+\beta_4 & \beta_1+\beta_2+\beta_3+\beta_4+\beta_5 & \beta_6 \\ \vdots & \iddots & & & & & & \vdots \\ \beta_1 & \beta_{n+1} & \beta_{n+2} & \beta_{n+3} & \beta_{n+4} & \beta_{n+5} & \cdots & \beta_n \end{bmatrix}$$

for some $\beta_i \in F$. Finally, $B_3 = B_2^\top$ as B is symmetric.

The following lemma shows that the entries of each block are determined recursively.

Lemma 3.5. *Let*

$$i \in \{1, 2, \ldots, 2n\} \setminus \{1, n+1\} \quad \textit{and} \quad j \in \{1, 2, \ldots, 2n\} \setminus \{n, 2n\}.$$

Then

$$B(v_i, v_j) = B(v_{i-1}, v_j) + B(v_{i-1}, v_{j+1}).$$

Proof. We have

$$\begin{aligned} B(v_i, v_{j+1}) &= B(v_iS, v_{j+1}S) = B(v_{i-1} + v_i, v_j + v_{j+1}) \\ &= B(v_{i-1}, v_j) + B(v_{i-1}, v_{j+1}) + B(v_i, v_j) + B(v_i, v_{j+1}). \end{aligned}$$

Hence, $B(v_i, v_j) = B(v_{i-1}, v_j) + B(v_{i-1}, v_{j+1})$. □

The first $n-1$ entries in the top row of each block B_i are equal to zero.

Lemma 3.6. *Suppose that $j \in \{1, \ldots, n-1\}$. Then*

$$\begin{aligned} &a) \quad B(v_1, v_j) = 0 \\ &b) \quad B(v_{n+1}, v_{n+j}) = 0 \\ &c) \quad B(v_1, v_{n+j}) = 0 \\ &d) \quad B(v_{n+1}, v_j) = 0. \end{aligned}$$

Proof. a) Let $j \in \{1, \ldots, n-1\}$. Since $B(v_1, v_{j+1}) = B(v_1S, v_{j+1}S) = B(v_1, v_j) + B(v_1, v_{j+1})$, we have $B(v_1, v_j) = 0$.

Parts b), c) and d) are proved similarly. □

Except for the first row and last column of each block B_i, there is an explicit formula for the entries of B.

Lemma 3.7. *Suppose that $i \in \{2, \ldots, n\}$ and $j \in \{1, \ldots, n-1\}$. Then*

$$\begin{aligned} &a) \quad B(v_i, v_j) = \sum_{k=1}^{i+j-n} \binom{i-k-1}{n-j-1} B(v_k, v_n) \\ &b) \quad B(v_{n+i}, v_{n+j}) = \sum_{k=1}^{i+j-n} \binom{i-k-1}{n-j-1} B(v_{n+k}, v_{2n}) \\ &c) \quad B(v_i, v_{n+j}) = \sum_{k=1}^{i+j-n} \binom{i-k-1}{n-j-1} B(v_k, v_{2n}) \\ &d) \quad B(v_{n+i}, v_j) = \sum_{k=1}^{i+j-n} \binom{i-k-1}{n-j-1} B(v_{n+k}, v_n). \end{aligned}$$

Proof. a) We argue by induction on i. Suppose first that $i = 2$. We can assume that $j = n - 1$ because otherwise the sum is trivially zero. Now we have

$$\sum_{k=1}^{i+j-n} \binom{i-k-1}{n-j-1} B(v_k, v_n) = \sum_{k=1}^{1} \binom{-k+1}{0} B(v_k, v_n) = \binom{0}{0} B(v_1, v_n) = B(v_1, v_n).$$

On the other hand, we have

$$\begin{aligned} B(v_i, v_j) &= B(v_2, v_j) = B(v_1, v_j) + B(v_1, v_{j+1}) = B(v_1, v_{j+1}) \\ &= \begin{cases} B(v_1, v_n) & \text{if } j = n-1 \\ 0 & \text{if } j \neq n-1 \end{cases} \end{aligned}$$

by Lemmas 3.5 and 3.6 a), so the claim holds when $i = 2$.

Suppose then that the claim holds for some $i \in \{2, \ldots, n-1\}$. From Lemma 3.5 it follows that $B(v_{i+1}, v_j) = B(v_i, v_j) + B(v_i, v_{j+1})$. If $j \neq n-1$, we can use the induction hypothesis and Pascal's rule to obtain

$$\begin{aligned} &B(v_i, v_j) + B(v_i, v_{j+1}) \\ &= \sum_{k=1}^{i+j-n} \binom{i-k-1}{n-j-1} B(v_k, v_n) + \sum_{k=1}^{i+j-n+1} \binom{i-k-1}{n-j-2} B(v_k, v_n) \\ &= \sum_{k=1}^{i+j-n+1} \binom{i-k-1}{n-j-1} B(v_k, v_n) + \sum_{k=1}^{i+j-n+1} \binom{i-k-1}{n-j-2} B(v_k, v_n) \\ &= \sum_{k=1}^{i+j-n+1} \binom{i-k}{n-j-1} B(v_k, v_n). \end{aligned}$$

If $j = n - 1$, we have by the induction hypothesis

$$\begin{aligned} B(v_i, v_j) + B(v_i, v_{j+1}) &= B(v_i, v_{n-1}) + B(v_i, v_n) \\ &= \sum_{k=1}^{i-1} \binom{i-k-1}{0} B(v_k, v_n) + B(v_i, v_n) = \sum_{k=1}^{i} \binom{i-k}{0} B(v_k, v_n) \\ &= \sum_{k=1}^{i+j-n+1} \binom{i-k}{n-j-1} B(v_k, v_n). \end{aligned}$$

This means that the claim holds for $i + 1$.

Parts b), c) and d) are proved similarly. □

Each block B_i is anti-triangular.

Lemma 3.8. *Suppose that* $i \in \{1, \ldots, n\}$.

$$\begin{aligned} &a) \quad B(v_i, v_j) = 0 \text{ when } j \in \{1, \ldots, n-i\} \\ &b) \quad B(v_{n+i}, v_j) = 0 \text{ when } j \in \{n+1, \ldots, 2n-i\} \\ &c) \quad B(v_i, v_j) = 0 \text{ when } j \in \{n+1, \ldots, 2n-i\}. \end{aligned}$$

Proof. a) If $i = 1$, then the claim holds by Lemma 3.6 a). Therefore, we can assume that $i > 1$, and use Lemma 3.7 a) to obtain

$$B(v_i, v_j) = \sum_{k=1}^{i+j-n} \binom{i-k-1}{n-j-1} B(v_k, v_n).$$

Because $j \leq n - i$, we have $i + j - n \leq 0$, and hence $B(v_i, v_j) = 0$.

Parts b) and c) are proved similarly. □

The entries on the anti-diagonal of a block B_i are all equal.

Lemma 3.9. *Suppose that* $i \in \{1, \ldots, n\}$. *Then*

$$\begin{aligned} &a) \quad B(v_i, v_{n-i+1}) = B(v_1, v_n) \\ &b) \quad B(v_{n+i}, v_{2n-i+1}) = B(v_{n+1}, v_{2n}) \\ &c) \quad B(v_i, v_{2n-i+1}) = B(v_1, v_{2n}). \end{aligned}$$

Proof. a) The claim clearly holds if $i = 1$, so we can assume that $i > 1$ and use Lemma 3.7 a). Now

$$B(v_i, v_{n-i+1}) = \sum_{k=1}^{1} \binom{i-k-1}{i-2} B(v_k, v_n) = B(v_1, v_n).$$

Parts b) and c) are proved similarly. □

The formula that gives the entries of B_i takes a particularly simple form on the entries right below the anti-diagonal of B_i.

Lemma 3.10. *Suppose that $i \in \{2, \dots, n\}$. Then*

$$a) \quad B(v_i, v_{n-i+2}) = \begin{cases} B(v_2, v_n) & \text{if } i \text{ is even} \\ B(v_2, v_n) + B(v_1, v_n) & \text{if } i \text{ is odd} \end{cases}$$

$$b) \quad B(v_{n+i}, v_{2n-i+2}) = \begin{cases} B(v_{n+2}, v_{2n}) & \text{if } i \text{ is even} \\ B(v_{n+2}, v_{2n}) + B(v_{n+1}, v_{2n}) & \text{if } i \text{ is odd} \end{cases}$$

$$c) \quad B(v_i, v_{2n-i+2}) = \begin{cases} B(v_2, v_{2n}) & \text{if } i \text{ is even} \\ B(v_2, v_{2n}) + B(v_1, v_{2n}) & \text{if } i \text{ is odd.} \end{cases}$$

Proof. a) By Lemma 3.7 a) we have

$$\begin{aligned} B(v_i, v_{n-i+2}) &= \sum_{k=1}^{2} \binom{i-k-1}{i-3} B(v_k, v_n) \\ &= \binom{i-2}{i-3} B(v_1, v_n) + \binom{i-3}{i-3} B(v_2, v_n) \\ &= (i-2)B(v_1, v_n) + B(v_2, v_n). \end{aligned}$$

The claim now follows.

Parts b) and c) are proved similarly. □

Lemma 3.11. *Suppose that $n > 1$.*

a) We have $B(v_1, v_n) = 0$, $Q(v_1) = 0$ and $B(v_1, v_{2n}) \neq 0$.

b) We have $B(v_{n+1}, v_{2n}) = 0$, $Q(v_{n+1}) = 0$ and $B(v_{n+1}, v_n) \neq 0$.

Proof. a) Since n is odd, we have $B(v_n, v_2) = B(v_2, v_n) + B(v_1, v_n)$ by Lemma 3.10 a). It follows that $B(v_1, v_n) = 0$.

Because

$$Q(v_2) = Q(v_2 S) = Q(v_1 + v_2) = Q(v_1) + Q(v_2) + B(v_1, v_2)$$

and $B(v_1, v_2) = 0$ by Lemma 3.6 a), we know that $Q(v_1) = 0$. From parts a) and c) of Lemma 3.8 it follows that $B(v_1, v_j) = 0$ for all $j \in \{1, \dots, n-1, n+1, \dots 2n-1\}$,

and we have just seen that $B(v_1, v_n) = 0$. If $B(v_1, v_{2n}) = 0$, then $v_1 \in \mathrm{rad}(V)$. Since V is non-singular, the vector v_1 must be zero which is impossible. Thus, we know that $B(v_1, v_{2n}) \neq 0$.

b) The proof is similar. □

In the block B_1, every other entry in the last column is determined by the entries above it. The same holds for $B_2 + B_3$.

Lemma 3.12. *Suppose that $i \in \{1, \ldots, n\}$ is odd. Then*

$$B(v_i, v_n) = \sum_{k=1}^{i-1} a_k B(v_k, v_n)$$

and

$$B(v_i, v_{2n}) + B(v_{n+i}, v_n) = \sum_{k=1}^{i-1} a_k \left(B(v_k, v_{2n}) + B(v_{n+k}, v_n)\right)$$

for some $a_1, \ldots, a_{i-1} \in F$.

Proof. We start by showing that there exist such $a_1, \ldots, a_{i-1} \in F$ that the first equation holds. Let $s = (n + i)/2$. By Lemma 3.7 a), we have

$$B(v_s, v_s) = \sum_{k=1}^{i} \binom{s-k-1}{n-s-1} B(v_k, v_n).$$

The last term of this sum is $B(v_i, v_n)$, and hence we have

$$B(v_s, v_s) = \sum_{k=1}^{i-1} \binom{s-k-1}{n-s-1} B(v_k, v_n) + B(v_i, v_n).$$

Since the characteristic of F is even, B is alternating and $B(v_s, v_s) = 0$. It follows that

$$B(v_i, v_n) = \sum_{k=1}^{i-1} \binom{s-k-1}{n-s-1} B(v_k, v_n).$$

This means that we can choose

$$a_k = \binom{s-k-1}{n-s-1}.$$

Next, we need to prove that the second equation of the claim holds for the $a_1, \dots a_{i-1}$ that we have chosen. By parts c) and d) of Lemma 3.7, we have

$$B(v_s, v_{n+s}) + B(v_{n+s}, v_s) = \sum_{k=1}^{i} \binom{s-k-1}{n-s-1} (B(v_k, v_{2n}) + B(v_{n+k}, v_n)).$$

As above, we now notice that

$$\begin{aligned} &B(v_s, v_{n+s}) + B(v_{n+s}, v_s) \\ &= \sum_{k=1}^{i-1} \binom{s-k-1}{n-s-1} (B(v_k, v_{2n}) + B(v_{n+k}, v_n)) + B(v_i, v_{2n}) + B(v_{n+i}, v_n). \end{aligned}$$

Because $B(v_s, v_{n+s}) + B(v_{n+s}, v_s) = 0$, it follows that

$$\begin{aligned} B(v_i, v_{2n}) + B(v_{n+i}, v_n) &= \sum_{k=1}^{i-1} \binom{s-k-1}{n-s-1} (B(v_k, v_{2n}) + B(v_{n+k}, v_n)) \\ &= \sum_{k=1}^{i-1} a_k (B(v_k, v_{2n}) + B(v_{n+k}, v_n)). \end{aligned}$$

□

Next we show that the basis can be chosen in such a way that $B_1 = B_2 + B_3$. It can also be assumed that $B(v_n, v_{2n}) = Q(v_n)$.

Lemma 3.13. *We can choose the basis $\{v_1, \dots, v_{2n}\}$ in such a way that the following hold:*

a) $B(v_i, v_j) = B(v_i, v_{n+j}) + B(v_{n+i}, v_j)$ *for all* $i, j \in \{1, \dots, n\}$

b) $B(v_n, v_{2n}) = Q(v_n)$.

Proof. a) Consider first the case $n = 1$. We have $B(v_1, v_1) = 0 = B(v_1, v_2) + B(v_2, v_1)$, and hence the claim holds.

Suppose now that $n > 2$. By Lemma 3.5, the values $B(v_i, v_j)$ are determined recursively. Hence, it is enough to prove the claim when $i = 1$ and $j \in \{1, \dots, n\}$, and when $i \in \{2, \dots, n\}$ and $j = n$.

Case 1: We start by showing that the claim holds when $i = 1$ and $j \in \{1, \dots, n\}$. If $j \neq n$, then we have $B(v_1, v_{n+j}) + B(v_{n+1}, v_j) = 0$ by parts c) and d) of Lemma 3.6.

If $j = n$, we substitute $i = n$ in Lemma 3.9 c), to obtain $B(v_1, v_{2n}) + B(v_{n+1}, v_n) = 2B(v_1, v_{2n}) = 0$.

On the other hand, we have $B(v_1, v_j) = 0$ for all $y \in \{1, \ldots, n\}$ by Lemmas 3.6 a) and 3.11 a). Hence, the claim holds when $i = 1$.

Case 2: Next we prove that the claim holds when $i = 2$ and $j = n$. Suppose first that $B(v_2, v_n) \neq 0$. From Lemma 3.10 c), substituting $i = n$, we obtain

$$B(v_2, v_{2n}) + B(v_{n+2}, v_n) = B(v_2, v_{2n}) + B(v_2, v_{2n}) + B(v_1, v_{2n}) = B(v_1, v_{2n}).$$

We will show that the basis can be chosen in such a way that $B(v_2, v_n) = B(v_1, v_{2n})$.

By Lemma 3.11 a), we have $B(v_1, v_{2n}) \neq 0$. Write

$$a = \frac{B(v_2, v_n)}{B(v_1, v_{2n})},$$

and let

$$v_i' = \begin{cases} v_i & \text{if } i \in \{1, \ldots, n\} \\ av_i & \text{if } i \in \{n+1, \ldots, 2n\}. \end{cases}$$

Since S is still in the Jordan normal form with respect to the basis $\{v_1', \ldots, v_{2n}'\}$, all the earlier results hold, and the basis can be changed. We have

$$B(v_1', v_{2n}') = aB(v_1, v_{2n}) = B(v_2, v_n) = B(v_2', v_n'),$$

so the claim holds if $B(v_2, v_n) \neq 0$.

We can now suppose that $B(v_2, v_n) = 0$. We may also assume that $B(v_{n+2}, v_{2n}) = 0$ because otherwise the spaces $U = \langle v_1, v_2, \ldots, v_n \rangle$ and $W = \langle v_{n+1}, v_{n+2}, \ldots, v_{2n} \rangle$ could be interchanged.

Let

$$v_i' = \begin{cases} v_i + v_{n+i} & \text{if } i \in \{1, \ldots n\} \\ v_i & \text{if } i \in \{n+1, \ldots 2n\}. \end{cases}$$

As before, we can change to the basis $\{v_1', \ldots, v_{2n}'\}$. Since by assumption

$$B(v_2, v_n) = 0 = B(v_{n+2}, v_{2n}),$$

it follows that

$$\begin{aligned} B(v_2', v_n') &= B(v_2, v_n) + B(v_2, v_{2n}) + B(v_{n+2}, v_n) + B(v_{n+2}, v_{2n}) \\ &= B(v_{n+2}, v_{2n}) + B(v_2, v_{2n}) + B(v_{n+2}, v_n) + B(v_{n+2}, v_{2n}) \\ &= B(v_2', v_{2n}') + B(v_{n+2}', v_n'). \end{aligned}$$

Thus, the claim holds when $i = 2$ and $j = n$.

Case 3: Finally, we show that we can choose $B(v_i, v_n) = B(v_i, v_{2n}) + B(v_{n+i}, v_n)$ for all $i \in \{3, \dots n\}$. Suppose that i is the smallest index for which

$$B(v_i, v_n) \neq B(v_i, v_{2n}) + B(v_{n+i}, v_n).$$

Assume first that i is odd. By Lemma 3.12, the values $B(v_i, v_n)$ and $B(v_i, v_{2n}) + B(v_{n+i}, v_n)$ depend only on the values of the form for indices smaller than i, and they do that in exactly the same way. Since the equality holds for all the smaller indices, we must have $B(v_i, v_n) = B(v_i, v_{2n}) + B(v_{n+i}, v_n)$.

Now we know that i is even. Write

$$b = \frac{\sum_{k=1}^{i-2} \binom{n-1-k}{n-1-i} B(v_k, v_{2n}) + B(v_{i-1}, v_{2n}) + B(v_i, v_n)}{B(v_1, v_{2n})}$$

and let

$$v_l' = \begin{cases} v_l & \text{if } l \in \{1, \dots i-2\} \\ v_l + b v_{l-i+2} & \text{if } l \in \{i-1, \dots n\} \\ v_l & \text{if } l \in \{n+1, \dots 2n\}. \end{cases}$$

The transformation S is still in the Jordan normal form with respect to the basis $\{v_1', \dots, v_{2n}'\}$. If $l \in \{1, \dots, i-2\}\}$, then

$$B(v_l', v_n') = B(v_l, v_n) + bB(v_l, v_{n-i+2}) = B(v_l, v_n)$$

by Lemma 3.8 a). Also, we have

$$\begin{aligned} B(v_{i-1}', v_n') &= B(v_{i-1}, v_n) + bB(v_{i-1}, v_{n-i+2}) + bB(v_1, v_n) + b^2 B(v_1, v_{n-i+2}) \\ &= B(v_{i-1}, v_n) \end{aligned}$$

by Lemmas 3.9 a) and 3.8 a). This means that the change of basis does not affect the values of the form for indices smaller than i.

By Lemma 3.7 c), we have

$$B(v'_n, v'_{n+i}) = \sum_{k=1}^{i} \binom{n-k-1}{n-i-1} B(v'_k, v'_{2n}).$$

It follows that

$$B(v'_i, v'_{2n}) + B(v'_{n+i}, v'_n) = \sum_{k=1}^{i-1} \binom{n-k-1}{n-i-1} B(v'_k, v'_{2n}). \tag{3.14}$$

Since i is even and n is odd, we know that $\binom{n-i}{n-i-1} = n-i$ is odd. Therefore, the coefficient of $B(v'_{i-1}, v'_{2n})$ in the sum (3.14) is equal to 1. Now we have

$$\begin{aligned}
\sum_{k=1}^{i-1} \binom{n-k-1}{n-i-1} B(v'_k, v'_{2n}) &= \sum_{k=1}^{i-2} \binom{n-k-1}{n-i-1} B(v'_k, v'_{2n}) + B(v'_{i-1}, v'_{2n}) \\
&= \sum_{k=1}^{i-2} \binom{n-k-1}{n-i-1} B(v_k, v_{2n}) + B(v_{i-1}, v_{2n}) + bB(v_1, v_{2n}) \\
&= B(v_i, v_n)
\end{aligned}$$

by the definition of b.

On the other hand, we notice that

$$B(v'_i, v'_n) = B(v_i, v_n) + bB(v_i, v_{n-i+2}) + bB(v_2, v_n) + b^2 B(v_2, v_{n-i+2}).$$

Since i is even, we have $B(v_i, v_{n-i+2}) = B(v_2, v_n)$ by Lemma 3.10 a). Also, since $i \geq 3$, we must in fact have $i \geq 4$. Now it follows from Lemma 3.8 a) that $B(v_2, v_{n-i+2}) = 0$. Hence, we have $B(v'_i, v'_n) = B(v_i, v_n)$, and can conclude that $B(v'_i, v'_{2n}) + B(v'_{n+i}, v'_n) = B(v'_i, v'_n)$.

b) Let

$$c = \frac{B(v_n, v_{2n}) + Q(v_n)}{B(v_1, v_{2n})},$$

and write

$$v'_i = \begin{cases} v_i & \text{if } i \in \{1, \dots n-1\} \\ v_i + cv_1 & \text{if } i = n \\ v_i & \text{if } i \in \{n+1, \dots 2n\}. \end{cases}$$

The transformation S is still in the Jordan normal form with respect to the basis $\{v'_1, \dots v'_{2n}\}$. We need to make sure that the change of basis does not affect the results of part a).

Firstly, we notice that if $i, j \neq n$, then $B(v'_i, v'_j) = B(v_i, v_j)$. Also, the statement of part a) clearly holds if $i, j = n$.

This means we can assume that $i \neq n$ and $j = n$. From Lemma 3.6 a), we obtain

$$B(v'_i, v'_n) = B(v_i, v_n) + cB(v_i, v_1) = B(v_i, v_n).$$

Also, we have

$$\begin{aligned} B(v'_i, v'_{2n}) + B(v'_{n+i}, v'_n) &= B(v_i, v_{2n}) + B(v_{n+i}, v_n) + cB(v_{n+i}, v_1) \\ &= B(v_i, v_{2n}) + B(v_{n+i}, v_n) \end{aligned}$$

by Lemma 3.6 c). Hence, the results of part a) hold for the basis $\{v'_1, \dots, v'_{2n}\}$.

Now we have

$$B(v'_n, v'_{2n}) = B(v_n, v_{2n}) + cB(v_1, v_{2n}) = Q(v_n)$$

by the definition of c.

On the other hand, from Lemma 3.11 a) it follows that

$$Q(v'_n) = Q(v_n + cv_1) = Q(v_n) + c^2 Q(v_1) + cB(v_1, v_n) = Q(v_n).$$

Thus, the basis can be chosen in such a way that $B(v_n, v_{2n}) = Q(v_n)$. □

Now we know enough about the forms B and Q, and can finally introduce the involutions that are used in this section.

Proposition 3.15. *There is an orthogonal involution M such that $MSM = S^{-1}$ and* $\operatorname{rank}(I + M)$ *is odd.*

Proof. Write $u = v_n$ and $w = v_{2n}$. We notice that $U = \langle u, uS, \dots, uS^{n-1} \rangle$ and $W = \langle w, wS, \dots, wS^{n-1} \rangle$.

Let M be the linear transformation defined by $uS^iM = uS^{n-i-1}$ and $wS^iM = uS^{n-i-1} + wS^{n-i-1}$ for all $i \in \{0, \ldots, n-1\}$. We can write

$$M = \begin{bmatrix} J & 0 \\ J & J \end{bmatrix},$$

where J is the involution defined in Proposition 3.3.

Now M is an involution, the rank of $I + M$ is n, and by assumption n is odd. The next task is to show that M conjugates S to its inverse. Let S_1 be the matrix of $S|_U$ and $S|_W$. Since we know by Proposition 3.3 that $JS_1J = (S_1)^{-1}$, it follows that

$$MSM = \begin{bmatrix} J & 0 \\ J & J \end{bmatrix} \begin{bmatrix} S_1 & 0 \\ 0 & S_1 \end{bmatrix} \begin{bmatrix} J & 0 \\ J & J \end{bmatrix} = \begin{bmatrix} JS_1J & 0 \\ 2JS_1J & JS_1J \end{bmatrix} = S^{-1}.$$

Finally, it needs to be shown that M preserves the quadratic form Q. It is enough to show that M preserves B and Q for the basis vectors. Recall that B was originally written in block form

$$B = \begin{bmatrix} B_1 & B_2 \\ B_3 & B_4 \end{bmatrix},$$

and by Lemma 3.13 a), it can be assumed that $B_1 = B_2 + B_3$. This was done with respect to the basis $\{v_1, \ldots, v_{2n}\}$. Since we have changed the basis, the blocks are now written with respect to the basis

$$\{u, uS, \ldots, uS^{n-1}, w, wS, \ldots, wS^{n-1}\}.$$

However, after the change of basis Lemma 3.13 a) still holds. Suppose that T is the change of basis matrix. The matrix of T can be written in block form

$$T = \begin{bmatrix} T_1 & 0 \\ 0 & T_1 \end{bmatrix}.$$

After the change of basis, the matrix of B is

$$TBT^\top = \begin{bmatrix} T_1B_1T_1^\top & T_1B_2T_1^\top \\ T_1B_3T_1^\top & T_1B_4T_1^\top \end{bmatrix},$$

where $T_1 B_1 T_1^\top = T_1(B_2 + B_3)T_1^\top = T_1 B_2 T_1^\top + T_1 B_3 T_1^\top$.

We will now prove that M preserves B, and begin by observing that

$$\begin{aligned} MBM^\top &= \begin{bmatrix} J & 0 \\ J & J \end{bmatrix} \begin{bmatrix} B_1 & B_2 \\ B_3 & B_4 \end{bmatrix} \begin{bmatrix} J & J \\ 0 & J \end{bmatrix} \\ &= \begin{bmatrix} JB_1J & JB_1J + JB_2J \\ JB_1J + JB_3J & JB_1J + JB_3J + JB_2J + JB_4J \end{bmatrix}. \end{aligned}$$

Since S preserves B, we have $S_1 B_i S_1^\top = B_i$ for every $i \in \{1, 2, 3, 4\}$. This means that each B_i can in fact be regarded as a bilinear form that is preserved by S_1. From the proof of Proposition 3.3, it follows that $JB_iJ = B_i^\top$ for every i.

Using this, and observing that $B_1^\top = B_1$, $B_4^\top = B_4$ and $B_2 = B_3^\top$, we obtain

$$MBM^\top = \begin{bmatrix} B_1 & B_1 + B_3 \\ B_1 + B_2 & B_1 + B_2 + B_3 + B_4 \end{bmatrix} = \begin{bmatrix} B_1 & B_2 \\ B_3 & B_4 \end{bmatrix} = B.$$

This means that M preserves B.

Because S preserves Q, we have

$$Q(uS^iM) = Q(uS^{n-1-i}) = Q(uS^i)$$

for all $i \in \{0, \dots, n-1\}$. Also,

$$\begin{aligned} Q(wS^iM) &= Q(uS^{n-1-i} + wS^{n-1-i}) \\ &= Q(uS^{n-1-i}) + Q(wS^{n-1-i}) + B(uS^{n-1-i}, wS^{n-1-i}) \\ &= Q(u) + Q(w) + B(u, w) \end{aligned}$$

for all $i \in \{0, \dots, n-1\}$. By Lemma 3.13 b), we can choose

$$B(u, w) = B(v_n, v_{2n}) = Q(v_n) = Q(u),$$

and hence $Q(wS^iM) = Q(w) = Q(wS^i)$. Thus, M preserves the quadratic form Q and is therefore orthogonal. □

3.3 The proof of the main theorem

Proof of Theorem A. Suppose that V is a vector space of even dimension over a field whose characteristic is even. Tiep and Zalesski [27] have shown that $\Omega(V)$ is not real if the dimension of V is not divisible by 4. Hence, we can assume that 4 divides $\dim(V)$.

We decompose V into cyclic and bicyclic subspaces V_i as explained in Section 3.1. If the dimension of a subspace V_i is divisible by four, then it is either a cyclic space or a bicyclic space consisting of two cyclic spaces of even dimension. By Propositions 3.3 and 3.4, the involution H_i can be chosen in such a way that $\operatorname{rank}(I + H_i)$ is even.

If we have a subspace of dimension 2 modulo 4, then it is either a cyclic space or a bicyclic space consisting of two cyclic spaces of odd dimension. By Propositions 3.3 and 3.15, the involution H_i can be chosen in such a way that $\operatorname{rank}(I + H_i)$ is odd.

Suppose that we have a subspace V_i of odd dimension. Now V_i cannot be bicyclic. Since the dimension is odd, the minimal polynomial of $S|_{V_i}$ cannot be of the form $(g_i\tilde{g}_i)^{h_i}$. Hence, it must have form $r_i^{h_i}$, where r_i is self-reciprocal and irreducible. Since the degree of r_i has to be odd, it follows from Lemma 3.2 that $r = X + 1$. However, in this case the subspace is singular. (This follows for example from the proof of Lemma 3.11. The matrix of the bilinear form on V_i is of the same form as the block B_1 in Section 3.2.2.) Hence, there cannot be any cyclic spaces of odd dimension.

Since $4 \mid \dim(V)$, and none of the spaces V_i has odd dimension, there must be an even number of subspaces of dimension 2 modulo 4. Now we know that

$$\sum \operatorname{rank}(I + H_i) = \operatorname{rank}(I + H)$$

is even. Thus, we can conclude that $\Omega(V)$ is strongly real. □

Chapter 4

Strongly real unipotent elements of orthogonal groups

A linear transformation is called *unipotent* if its minimal polynomial is of the form $(X-1)^k$ for some $k \in \{1, 2, \dots\}$. In a group of Lie type, every element can be written uniquely as a product of a unipotent and a semisimple element. (A transformation is semisimple if it is diagonalisable.)

Theorem B. *When n and q are even, the unipotent elements of the finite simple group $\Omega_n^\varepsilon(q)$ are strongly real.*

The proof of the theorem is similar to the one of Theorem A. As before, suppose that V is a vector space over a finite field F with characteristic 2. Assume that V is endowed with a non-singular quadratic form Q with the associated bilinear form B. We will restrict our study to the case where $\dim(V) = n$ is even.

Let S be an orthogonal transformation of V. As in Section 3.1, the vector space V can be written as a direct sum of subspaces that are cyclic or bicyclic with respect to S.

Proposition 4.1. *Suppose that $V = \langle v, vS, \dots, vS^{n-1} \rangle$ is a cyclic vector space. If $n \equiv 2 \pmod 4$ and S is unipotent, there is an orthogonal involution K such that $KSK = S^{-1}$ and $\operatorname{rank}(I+K)$ is even.*

Proof. Suppose that the minimal polynomial of S is $p = \sum_{k=0}^{n} a_k X^k$. Since p is self-reciprocal, we have $a_0 = 1 = a_n$ and $a_k = a_{n-k}$ for all $k \in \{1, \ldots, n-1\}$.

Define the linear transformation K by $vS^iK = vS^{n-i}$ for all $i \in \{0, \ldots, n-1\}$. We can write

$$K = \begin{bmatrix} 1 & a_1 & a_2 & \cdots & a_2 & a_1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

Ellers and Nolte [7] have shown that K is an orthogonal involution that conjugates S to its inverse.

Now we have

$$I + K = \begin{bmatrix} 0 & a_1 & a_2 & \cdots & a_2 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 1 & \cdots & 1 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 1 & \cdots & 1 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

We notice that if n is odd, then the first row is linearly dependent on the other rows. On the other hand, if n is even, then all elements in row $(n/2) + 1$ are equal to zero. Hence, we have

$$\operatorname{rank}(I + K) = \begin{cases} (n-1)/2 & \text{if } n \text{ is odd} \\ (n-2)/2 & \text{if } n \text{ is even and } a_{n/2} = 0 \\ n/2 & \text{if } n \text{ is even and } a_{n/2} \neq 0. \end{cases}$$

Suppose then that S is unipotent and $n \equiv 2 \pmod 4$. Let $m \in \mathbb{N}$ be such that $n = 4m + 2$. Since S is unipotent, we have $p = (X+1)^n$, and hence

$$a_k = \binom{n}{k} \quad \text{for all } k \in \{0, \ldots, n\}.$$

We notice that

$$\begin{aligned} a_{n/2} = a_{2m+1} &= \binom{n}{2m+1} \\ &= \sum_{k=0}^{2m+1} \binom{2m+1}{k}\binom{2m+1}{2m+1-k} \\ &= 2\sum_{k=0}^{m} \binom{2m+1}{k}\binom{2m+1}{2m+1-k} = 0 \end{aligned}$$

because the characteristic of F is even. Thus, we know that

$$\operatorname{rank}(I+K) = \frac{n-2}{2} = 2m.$$

□

Proposition 4.2. *Suppose that n is odd and*

$$V = \langle u, uS, \dots uS^{n-1}\rangle \oplus \langle w, wS, \dots wS^{n-1}\rangle$$

is a bicyclic vector space. There is an orthogonal involution N such that $NSN = S^{-1}$ and $\operatorname{rank}(I+N)$ *is even.*

Proof. Let N be the linear transformation of V defined by

$$uS^iN = uS^{n-i} \quad \text{and} \quad wS^iN = wS^{n+1-i}$$

for all $i \in \{0, \dots, n-1\}$. Let P be the linear transformation of W defined by

$$wS^iP = wS^{n+1-i}$$

for all $i \in \{0, \dots, n-1\}$. Now we can write

$$N = \begin{bmatrix} K & 0 \\ 0 & P \end{bmatrix},$$

where K is the linear transformation defined in Proposition 4.1.

The proof of Lemma 4 in [7] shows that N is an orthogonal involution that conjugates S to its inverse. We will show that $\operatorname{rank}(I+N)$ is even.

By Lemma 3.2, the minimal polynomial of $S|_W$ is $p = (X+1)^n$. Suppose that $p = \sum_{k=0}^{n} a_i X^i$, where $a_i \in F$. We notice that $a_1 = \binom{n}{1} = n$ is odd, and therefore $a_1 = a_{n-1} = 1$.

Since $S^n = \sum_{k=0}^{n-1} a_i S^i$, we have

$$\begin{aligned} S^{n+1} &= \sum_{k=0}^{n-1} a_i S^{i+1} = \sum_{k=1}^{n-1} a_{i-1} S^i + S^n = \sum_{k=1}^{n-1} a_{i-1} S^i + \sum_{k=0}^{n-1} a_i S^i \\ &= a_0 + \sum_{k=1}^{n-1} (a_{i-1} + a_i) S^i. \end{aligned}$$

Now we can write

$$\begin{aligned} P &= \begin{bmatrix} a_0 & a_0+a_1 & a_1+a_2 & a_2+a_3 & \cdots & a_{n-3}+a_{n-2} & a_{n-2}+a_{n-1} \\ a_0 & a_1 & a_2 & a_3 & \cdots & a_{n-2} & a_{n-1} \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & 1+a_2 & a_2+a_3 & \cdots & a_3+a_2 & a_2+1 \\ 1 & 1 & a_2 & a_3 & \cdots & a_2 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 \end{bmatrix}. \end{aligned}$$

It follows that

$$I+P=\begin{bmatrix} 0 & 0 & 1+a_2 & a_2+a_3 & \cdots & a_3+a_2 & a_2+1 \\ 1 & 0 & a_2 & a_3 & \cdots & a_2 & 1 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & 1 & \cdots & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 1 & \cdots & 1 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

Because n is odd, all the entries in row $(n+3)/2$ are equal to zero. Also, the top row is linearly dependent of the rows 3 to n. On the other hand, the second row is clearly linearly independent of the other rows. Now we have

$$\operatorname{rank}(I+P)=1+\frac{n-3}{2}=\frac{n-1}{2}.$$

In the proof of Proposition 4.1 we noticed that $\operatorname{rank}(I+K)=\frac{n-1}{2}$. Now

$$\operatorname{rank}(I+N)=\operatorname{rank}(I+K)+\operatorname{rank}(I+P)=n-1,$$

and therefore $\operatorname{rank}(I+N)$ is even. □

Proof of Theorem B. Let V be a vector space of even dimension over a field whose characteristic is even. Suppose that $S\in\Omega(V)$ is unipotent. Decompose V into cyclic and bicyclic subspaces V_i as in the proof of Theorem A. (See Section 3.3.)

Suppose first that we have a cyclic subspace V_i. As in the proof of Theorem A, there cannot be cyclic spaces of odd dimension, and hence the dimension of V_i must be even. By Propositions 3.3 and 4.1, the involution H_i can be chosen in such a way that $\operatorname{rank}(I+H_i)$ is even.

Assume then that we have a bicyclic subspace V_i. By Propositions 3.4 and 4.2, the involution H_i can be chosen in such a way that $\operatorname{rank}(I+H_i)$ is even.

Now $\sum\operatorname{rank}(I+H_i)=\operatorname{rank}(I+H)$ is even, and therefore $H\in\Omega(V)$. Thus, S is strongly real. □

Part III

A symmetric construction of the compact real form of the Lie Algebra E_8

Chapter 5

Lie Algebras

5.1 Simple Lie algebras

In this section we introduce Lie algebras and their basic properties. All the material of the section is not needed in proving the main results, but will give the reader an idea of the nature of Lie algebras. The definitions and results are taken from the books of Carter [4] and Jacobson [16]. The reader may also find the book by Erdmann and Wildon useful [8].

A *Lie algebra* is a vector space $\mathfrak{L}$ over a field K, endowed with a so-called Lie product $[\cdot,\cdot]$. The Lie product satisfies the following properties:

1. It is bilinear.
2. $[x,x]=0$ for every $x\in\mathfrak{L}$.
3. $[[x,y],z]+[[z,x],y]+[[y,z],x]=0$ for all $x,y,z\in\mathfrak{L}$.

Axiom 3 is called the *Jacobi identity*.

Notice that the Lie product is anti-symmetric. Namely, if $\mathfrak{L}$ is a Lie algebra and $x,y\in L$, then from Axioms 1 and 2 it follows that

$$0=[x+y,x+y]=[x,x]+[x,y]+[y,x]+[y,y]=[x,y]+[y,x].$$

If the characteristic of the field K is odd, Axiom 2 is equivalent with anti-symmetry.

For example, the vector space of $n \times n$-matrices over a field K is a Lie algebra if the Lie multiplication is defined as

$$[A, B] = AB - BA,$$

where the product on the right hand side is the ordinary matrix multiplication.

For each element x of a Lie algebra $\mathfrak{L}$, we define the *adjoint mapping*

$$\operatorname{ad} x : \ \mathfrak{L} \to \mathfrak{L}, \quad y \mapsto [x, y].$$

The mapping $\operatorname{ad} x$ is a linear transformation, and can therefore be written as a matrix with respect to some basis of $\mathfrak{L}$. Using the adjoint mapping, it is possible to define a symmetric bilinear form on $\mathfrak{L}$. The *Killing form* $(\cdot, \cdot)$ is defined by

$$(x, y) = \operatorname{tr}(\operatorname{ad} x . \operatorname{ad} y),$$

where $\operatorname{tr}(\operatorname{ad} x . \operatorname{ad} y)$ is the trace of the matrix $\operatorname{ad} x . \operatorname{ad} y$.

An *automorphism* of a Lie algebra $\mathfrak{L}$ is a linear isomorphism g of $\mathfrak{L}$ for which it holds that

$$[vg, wg] = [v, w]g$$

for all $v, w \in \mathfrak{L}$. The automorphism group of a Lie algebra $\mathfrak{L}$ is denoted $\operatorname{Aut}(\mathfrak{L})$. Automorphisms of a Lie algebra preserve the Killing form.

A *Cartan subalgebra* $\mathfrak{H}$ of a Lie algebra $\mathfrak{L}$ is a subalgebra for which the following hold

1. $\underbrace{[[[\mathfrak{H}, \mathfrak{H}], \mathfrak{H}], \ldots, \mathfrak{H}]}_{r} = 0$ for some r. ($\mathfrak{H}$ is nilpotent)
2. If $[x, h] \in \mathfrak{H}$ for all $h \in \mathfrak{H}$, then $x \in \mathfrak{H}$. ($\mathfrak{H}$ is self-normalising)

Every Lie Algebra $\mathfrak{L}$ over $\mathbb{C}$ has a Cartan subalgebra ([16], III.1, Thm 1, p. 59), and all the Cartan subalgebras of $\mathfrak{L}$ are isomorphic ([16], IX.2, Thm 3, p. 273).

An *ideal* of a Lie algebra $\mathfrak{L}$ is a subspace $\mathfrak{I}$ such that $[x, a] \in \mathfrak{I}$ for all $x \in \mathfrak{L}$ and $a \in \mathfrak{I}$. Since the Lie product is anti-symmetric, all ideals are two-sided. The Lie

algebra $\mathfrak{L}$ is called *simple* if it does not have any non-trivial ideals, and $[\mathfrak{L}, \mathfrak{L}] \neq \{0\}$. A Lie algebra is *semisimple* if it is a direct sum of simple Lie algebras. A complex Lie algebra is semisimple if and only if its Killing form is non-degenerate ([16], III.4, Cartan's criterion, p. 69).

Suppose that $\mathfrak{L}$ is a simple Lie algebra over $\mathbb{C}$ with a Cartan subalgebra $\mathfrak{H}$. Now $\mathfrak{L}$ can be decomposed into a direct sum of $\mathfrak{H}$ and some 1-dimensional subspaces that are invariant under multiplication by $\mathfrak{H}$:

$$\mathfrak{L} = \mathfrak{H} \oplus \mathfrak{L}_{r_1} \oplus \mathfrak{L}_{r_2} \oplus \cdots \oplus \mathfrak{L}_{r_k}. \tag{5.1}$$

This is called the *Cartan decomposition* of $\mathfrak{L}$ with respect to $\mathfrak{H}$.

Suppose that $\mathfrak{L}_r$ is one of the $\mathfrak{H}$-invariant subalgebras in the Cartan decomposition of $\mathfrak{L}$, and e_r is a generator of $\mathfrak{L}_r$. If $h \in \mathfrak{H}$, there is an element λ_h of $\mathbb{C}$ such that $[h, e_r] = \lambda_h e_r$. Now we can define the mapping

$$r : \ \mathfrak{H} \to \mathbb{C}, \quad r(h) = \lambda_h.$$

The mappings $r_1, r_2, \ldots, r_k$ corresponding to the subalgebras $\mathfrak{L}_{r_1}, \mathfrak{L}_{r_2}, \ldots, \mathfrak{L}_{r_k}$ are called *roots* of $\mathfrak{L}$. They are elements of the dual space of $\mathfrak{H}$. It can be shown that the Killing form of $\mathfrak{L}$, when restricted to $\mathfrak{H}$, is non-degenerate, and hence every element of the dual space is in one-to-one correspondence with an element of $\mathfrak{H}$ via this form ([16], IV.1, Result II, p. 109). It follows that the roots can be considered as elements of the Cartan subalgebra $\mathfrak{H}$: the root r corresponds to the element $\tilde{r} \in \mathfrak{H}$ for which it holds that $r(h) = (\tilde{r}, h)$ for all $h \in \mathfrak{H}$.

If the roots of a Lie algebra are considered as elements of the Cartan subalgebra $\mathfrak{H}$, the Killing form can be applied to the roots. The form restricted to $\mathfrak{H}$ has rational values and is positive definite ([16], IV.2, Result XIV, p. 118). The set $\mathfrak{H}_{\mathbb{R}}$ of real linear combinations of roots can therefore be considered as a Euclidean space. The set of roots is called the *root system* of $\mathfrak{L}$ and denoted Φ. Every root system contains a subset Π of *fundamental roots*. The set Π is a linearly independent subset of $\mathfrak{H}_{\mathbb{R}}$, and every root is a real linear combination of roots in Π with coefficients which are either all non-negative or all non-positive.

When considered as elements of the Cartan subalgebra $\mathfrak{H}$, the fundamental roots form a basis of $\mathfrak{H}$ ([16], Section IV.1, Result III, p. 109). The number of fundamental roots (or the dimension of $\mathfrak{H}$) is called the *rank* of $\mathfrak{L}$.

Usually it is convenient to use the scalar multiple $h_r = 2r/(r,r)$ of the root r. We can now write

$$\mathfrak{H} = \langle h_r \mid r \in \Pi \rangle.$$

Each 1-dimensional root space $\mathfrak{L}_r$ has a generator e_r. For a complex simple Lie algebra $\mathfrak{L}$, it is possible to choose a basis

$$\{h_r, e_s \mid \ r \in \Pi, \ s \in \Phi\}$$

in such a way that the Lie products of the basis vectors are the following:

$$\begin{aligned}
[h_r, h_s] &= 0 && r, s \in \Phi \\
[h_r, e_s] &= A_{rs} e_s && r \in \Pi, s \in \Phi \\
[e_r, e_{-r}] &= h_r && r \in \Phi \\
[e_r, e_s] &= 0 && \text{if } r + s \notin \Phi \\
[e_r, e_s] &= N_{rs} e_{r+s} && \text{if } r + s \in \Phi,
\end{aligned} \tag{5.2}$$

where A_{rs} and N_{rs} are integers depending on r and s. A basis obtained this way is called a *Chevalley basis* of $\mathfrak{L}$. (See [4], Thm 4.2.1, p. 56.)

Example 5.3. Consider the Lie algebra $\mathfrak{sl}_{n+1}(\mathbb{C})$ consisting of complex $(n+1)\times(n+1)$-matrices whose trace is zero. The Lie product is defined as

$$[A, B] = AB - BA.$$

The diagonal matrices in $\mathfrak{sl}_{n+1}(\mathbb{C})$ form a Cartan subalgebra $\mathfrak{H}$, and we can write

$$\mathfrak{sl}_{n+1}(\mathbb{C}) = \mathfrak{H} \oplus \sum_{i \neq j} \mathbb{C} e_{ij},$$

where e_{ij} is a matrix with 1 in the (i,j)-position and 0 elsewhere. For the diagonal matrix $h = \operatorname{diag}(\alpha_0, \ldots, \alpha_n)$ we have

$$[h, e_{ij}] = h e_{ij} - e_{ij} h = (\alpha_i - \alpha_j) e_{ij}.$$

Now the fundamental roots of $\mathfrak{sl}_{n+1}$ are the mappings

$$\begin{aligned}
&p_1 : \mathfrak{H} \to \mathbb{C}, && \operatorname{diag}(\alpha_0, \ldots, \alpha_n) \mapsto \alpha_0 - \alpha_1, \\
&p_2 : \mathfrak{H} \to \mathbb{C}, && \operatorname{diag}(\alpha_0, \ldots, \alpha_n) \mapsto \alpha_1 - \alpha_2, \\
&\vdots \\
&p_n : \mathfrak{H} \to \mathbb{C}, && \operatorname{diag}(\alpha_0, \ldots, \alpha_n) \mapsto \alpha_{n-1} - \alpha_n.
\end{aligned}$$

The element h_{p_i} of $\mathfrak{H}$ corresponding to the root p_i is

$$h_{p_i} = \operatorname{diag}(0, \ldots, 0, 1, -1, 0, \ldots, 0),$$

where 1 is in the ith entry. The elements h_{p_i}, e_{ij} form a Chevalley basis of the Lie algebra. It can be shown that $\mathfrak{sl}_{n+1}(\mathbb{C})$ is simple.

The properties of a root system can be described in a *Dynkin diagram*. The diagram lists the fundamental roots and the angles between them in the Euclidean space $\mathfrak{H}_{\mathbb{R}}$. For example, the Dynkin diagram of the Lie algebra $\mathfrak{sl}_{n+1}(\mathbb{C})$ is described in Figure 5.1.

Figure 5.1: The Dynkin diagram of the root system of the Lie algebra $\mathfrak{sl}_{n+1}(\mathbb{C})$

In a Dynkin diagram, each node corresponds to a fundamental root. If p and q are fundamental roots, it can be shown that

$$\frac{4(p,q)^2}{(p,p)(q,q)} = 4\cos^2\theta \in \{0, 1, 2, 3\},$$

where θ is the angle between p and q ([4], Section 3.4, p. 39). If the above quantity is equal to n, the roots p and q are joined by n edges in the Dynkin diagram. For example, roots that are orthogonal to each other are not connected. If the angle between the roots p and q is $2\pi/3$, then $4\cos^2\theta = 1$ and the roots are joined by one edge.

The complex simple Lie algebras can be classified up to isomorphism by their root systems. There are four infinite families of simple Lie algebras corresponding to root

systems of type A_n, B_n, C_n and D_n. The index indicates the rank of the Lie algebra. The Lie algebra $\mathfrak{sl}_{n+1}$ of Example 5.3 is of type A_n. There are also five exceptional Lie algebras whose root systems are denoted G_2, F_4 E_6, E_7 and E_8. The simple Lie algebras and some of their properties are listed in Table 5.1. The proofs can be found in Jacobson ([16], Sections IV.5 and IV.6, p. 128–146).

Lie algebra	dimension	rank	number of roots
A_l $(l \geq 1)$	$l(l+2)$	l	$2(l+1)$
B_l $(l \geq 2)$	$l(2l+1)$	l	$2l^2$
C_l $(l \geq 3)$	$l(2l+1)$	l	$2l^2$
D_l $(l \geq 4)$	$l(2l-1)$	l	$2l(l-1)$
G_2	14	2	12
F_4	52	4	48
E_6	78	6	72
E_7	133	7	126
E_8	248	8	240

Table 5.1: The simple Lie algebras

5.1.1 The Lie algebra E_8

We will now construct a root system of type E_8. The details are taken from Carter ([4], Section 3.6, p. 48). Using the root system, one can then construct a Lie algebra of type E_8.

Let $\{v_1, v_2, \ldots, v_8\}$ be an orthonormal basis of a Euclidean space V. Define

$$\Pi = \{p_1,\ p_2,\ p_3,\ p_4,\ p_5,\ p_6,\ p_7,\ p_8\},$$

where

$$\begin{aligned} p_1 &= v_1 - v_2, & p_5 &= v_5 - v_6, \\ p_2 &= v_2 - v_3, & p_6 &= v_6 - v_7, \\ p_3 &= v_3 - v_4, & p_7 &= v_6 + v_7, \\ p_4 &= v_4 - v_5, & p_8 &= -\frac{1}{2}\sum_{i=1}^{8} v_i. \end{aligned}$$

Let

$$\Phi = \left\{ \pm v_i \pm v_j \mid i \neq j \right\} \cup \left\{ \frac{1}{2}\sum_{i=1}^{8} \varepsilon_i v_i \mid \varepsilon_i = \pm 1, \prod_{i=1}^{8} \varepsilon_i = 1 \right\}.$$

The set Φ is a root system of type E_8, and Π is a set of fundamental roots of Φ. The Dynkin diagram of Φ is described in Figure 5.2.

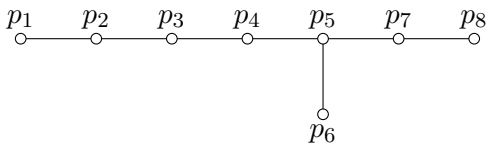

Figure 5.2: The Dynkin diagram of the root system of type E_8

Now we can take a 248-dimensional free vector space $\mathfrak{L}$ generated by the symbols h_r, $r \in \Pi$ and e_s, $s \in \Phi$, and define the Lie multiplication as in Equation (5.2). The coefficients A_{pq} and N_{rs} are determined as follows. For $r, s \in \Phi$, write

$$A_{rs} = \frac{2(r,s)}{(r,r)},$$

where $(\cdot,\cdot)$ is the usual scalar product of V. In the case of our root system, it holds for all fundamental roots p and q that

$$A_{pq} = \begin{cases} 2 & \text{if } p = q \\ -1 & \text{if } p \text{ and } q \text{ are joined in the Dynkin diagram} \\ 0 & \text{otherwise.} \end{cases}$$

If $r + s \in \Phi$, define $N_{rs} = \pm(p+1)$, where p is the greatest integer for which $s - pr$ is an element of Φ. Now N_{rs} is either 1 or -1. The signs of the coefficients N_{rs} must be

chosen so that the Jacobi identity holds. Further details can be found in Carter ([4], Prop. 4.22, p. 58).

5.2 Compact real forms

Suppose that $\mathfrak{L}$ is a Lie algebra over the field F, and F is a subfield of K. Now $\mathfrak{L}_K = K \otimes_F \mathfrak{L}$ is a Lie algebra over the field K. We say that the Lie algebra $\mathfrak{L}_K$ is obtained from $\mathfrak{L}$ by extending the base field. If $\mathfrak{L}$ is a complex Lie algebra, and $\mathfrak{L}_0$ is such a real Lie algebra that $(\mathfrak{L}_0)_{\mathbb{C}} = \mathfrak{L}$, then $\mathfrak{L}_0$ is called a *real form* of $\mathfrak{L}$.

When a complex simple Lie algebra is constructed from a root system with a Chevalley basis, the structure constants are all integers. Hence, the construction works also over the real numbers. The algebras obtained this way are called the *split real forms* of the complex simple Lie algebras.

A semisimple Lie algebra over the field $\mathbb{R}$ is called *compact* if its Killing form is negative definite. In Lie theory, compact Lie algebras are associated with the compact Lie groups. The split real forms given by the standard construction are not compact.

The following theorem states that every complex semisimple Lie algebra has a *compact real form*.

Theorem 5.4. *Suppose that $\mathfrak{L}$ is a semisimple Lie algebra over the complex numbers. Then there exists a compact Lie algebra $\mathfrak{L}_0$ over the real numbers such that $(\mathfrak{L}_0)_{\mathbb{C}} = \mathfrak{L}$.*

Proof. A detailed proof can be found in Jacobson ([16], IV.7, Thm 10, p. 147). One first chooses a Chevalley basis $\{h_r, e_s, e_{-s}\}$ and scales it so that $(e_s, e_{-s}) = -1$ for all roots $s \in \Phi$. The compact real form of $\mathfrak{L}$ is then generated by the vectors

$$\sqrt{-1}h_r, \quad e_s + e_{-s}, \quad \sqrt{-1}(e_s - e_{-s})$$

over $\mathbb{R}$ □

Any two compact real forms of a complex Lie algebra are isomorphic ([24], II.10, Corollary C, p. 59).

Example 5.5. Let $\mathfrak{N}$ be the vector space $\mathbb{R}^3$ endowed with the normal vector cross product $[v, w] = v \times w$. Now $\mathfrak{N}$ is a simple Lie algebra, and it has a basis

$$i = (1, 0, 0), \quad j = (0, 1, 0), \quad k = (0, 0, 1).$$

The Lie products of the basis elements are

$$[i, j] = k, \ [j, k] = i, \ [k, i] = j.$$

With respect to the basis $\{i, j, k\}$, the matrix of the Killing form is

$$\begin{bmatrix} -2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{bmatrix},$$

so the Killing form is negative-definite, and $\mathfrak{N}$ is a compact Lie algebra. The Lie algebra $\mathfrak{N}$ is of type A_1.

Also the Lie algebra $\mathfrak{sl}_2(\mathbb{R})$ of real 2×2 matrices with zero trace is 3-dimensional and of type A_1. It has a Chevalley basis

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \ \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \ \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix},$$

and the Lie products of the basis elements are

$$[h, e] = 2e, \ [h, f] = -2f, \ [e, f] = h.$$

The Lie algebras $\mathfrak{N}$ and $\mathfrak{sl}_2(\mathbb{R})$ are not isomorphic, but if we extend the base field to $\mathbb{C}$, then there is an isomorphism between them:

$$\begin{aligned} i &\mapsto \frac{1}{2}\sqrt{-1}h \\ j &\mapsto \frac{1}{2}\sqrt{-1}(e + f) \\ k &\mapsto \frac{1}{2}(e - f). \end{aligned}$$

The Lie algebra $\mathfrak{N}$ is the compact real form, and $\mathfrak{sl}_2(\mathbb{R})$ is the split real form of the complex Lie algebra A_1.

5.3 Multiplicative orthogonal decompositions

If $\mathfrak{L}$ is a complex simple Lie algebra, it has a decomposition

$$\mathfrak{L} = \mathfrak{H}_1 \oplus \mathfrak{H}_2 \oplus \cdots \oplus \mathfrak{H}_m,$$

where each $\mathfrak{H}_i$ is a Cartan subalgebra. (See [20], Part I, p. 12.) If all the subalgebras $\mathfrak{H}_i$ are orthogonal to each other with respect to the Killing form, the decomposition is called an *orthogonal decomposition*. If for all i and j it also holds that

$$[\mathfrak{H}_i, \mathfrak{H}_j] \subseteq \mathfrak{H}_k \quad \text{for some } k,$$

then the decomposition is called a *multiplicative orthogonal decomposition*.

For example, the Lie algebra $\mathfrak{N}$ that was defined in Example 5.5 has a multiplicative orthogonal decomposition

$$\mathfrak{N} = \langle i \rangle \oplus \langle j \rangle \oplus \langle k \rangle.$$

Not all simple Lie algebras have such decompositions. A complex simple Lie algebra admits a multiplicative orthogonal decomposition if and only if it is of type A_1, B_{2^m-1} ($m \geq 2$), D_{2^m} ($m \geq 2$), G_2 or E_8. (See [20], Thm 3.3.5, page 96.)

The automorphism group of the decomposition

$$\mathfrak{L} = \mathfrak{H}_1 \oplus \mathfrak{H}_2 \oplus \cdots \oplus \mathfrak{H}_m$$

consists of the automorphisms of $\mathfrak{L}$ that stabilise the decomposition. In other words, the automorphism $\phi \in \mathrm{Aut}(\mathfrak{L})$ is an automorphism of the decomposition if for all i it holds that

$$\mathfrak{H}_i \phi = \mathfrak{H}_j$$

for some j.

Theorem 5.6. *The complex Lie algebra E_8 has a unique multiplicative Cartan decomposition up to $\mathrm{Aut}(E_8)$-conjugacy. The automorphism group of the decomposition has shape*

$$2^{5+10} \cdot GL_5(2).$$

Proof. Thompson [26] has given a construction of the multiplicative decomposition of E_8, and also proved that all such decompositions are conjugate under the automorphisms of E_8. Another construction can be found in the book of Kostrikin and Tiep ([20], Thm 3.3.5, p. 96). □

Chapter 6

A new construction of the compact real form of the Lie algebra E_8

Recently, Wilson has given elementary constructions of the compact real forms of the exceptional Lie algebras G_2 [30], F_4 and E_6 [28]. Wilson used an irreducible subgroup of the automorphism group of the Lie algebra in defining the Lie product, and we will choose a similar strategy for E_8. The group used in our construction has shape $2^{5+10} \cdot \mathrm{GL}_5(2)$.

We start by constructing a group G of shape $2^{5+10} \cdot \mathrm{GL}_5(2)$ as mappings of a 248-dimensional vector space $\mathfrak{L}$. The space is built from 31 copies of the real octonion algebra. The Lie product is then defined to be the unique bilinear product on $\mathfrak{L}$ that is preserved in the action of G. The action of the group G is irreducible, and it follows that the Lie algebra $\mathfrak{L}$ must be compact.

The 31 copies of the octonion algebra will all be Cartan subalgebras of $\mathfrak{L}$. They are orthogonal to each other, and the product of two subalgebras always lies in a third one. Hence, the construction given here is also a multiplicative orthogonal decomposition of E_8.

There are other related constructions of E_8 in the literature. For example, Thompson [26], Kostrikin and Tiep [20] and Grishkov [14] have given constructions of the multiplicative orthogonal decomposition of E_8. Since we define the Lie product using the group G, our construction exhibits more symmetry than the previous ones. Also, we express the action of G on the Lie algebra in an elementary form.

6.1 Preliminaries

6.1.1 The real octonion algebra

The real octonion algebra $\mathbb{O}$ is an 8-dimensional vector space with basis vectors

$$1,\ i_0,\ i_1,\ i_2,\ i_3,\ i_4,\ i_5,\ i_6.$$

We will often write $1 = i_\infty$. Now

$$\mathbb{O} = \{a_\infty 1 + a_0 i_0 + a_1 i_1 + \cdots + a_6 i_6 \mid a_\infty, a_i \in \mathbb{R}\}.$$

The vector 1 is a multiplicative identity, and the squares of the other basis vectors are all equal to -1:

$$i_0^2 = i_1^2 = \cdots = i_6^2 = -1.$$

Otherwise the multiplication is defined as follows: the octonions i_t, i_{t+1} and i_{t+3} behave as the quaternions i, j and k. The subscripts are understood modulo 7.

There is another way of expressing the rules of multiplication. We have $i_r i_s = \pm i_t$, when i_r, i_s and i_t are on the same line in Figure 6.1. The arrow indicates the sign of the product. For example, $i_1 i_2 = i_4$ and $i_2 i_1 = -i_4$.

Notice that the octonion multiplication is not associative. For instance, we have

$$(i_0 i_1) i_2 = i_3 i_2 = -i_5$$

and

$$i_0 (i_1 i_2) = i_0 i_4 = i_5.$$

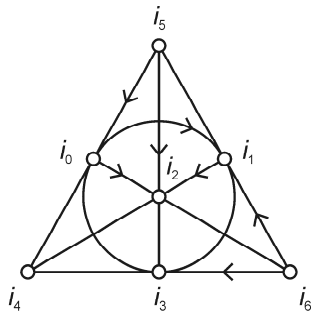

Figure 6.1: Multiplication diagram of octonions

Lemma 6.1. *For octonions i_r, i_s and i_t it holds that*

$$(i_r i_s)i_t = \pm i_r(i_s i_t).$$

If i_r, i_s, i_t are on the same line in Figure 6.1, then $(i_r i_s)i_t = i_r(i_s i_t)$. Otherwise $(i_r i_s)i_t = -i_r(i_s i_t)$.

Proof. If i_r, i_s and i_t are on the same line in Figure 6.1, the subalgebra they generate is isomorphic to a subalgebra of the quaternions. The quaternion algebra is associative, and hence $(i_r i_s)i_t = i_r(i_s i_t)$.

If i_r, i_s and i_t are not on the same line, we may assume that they are equal to i_0, i_1 and i_2. Namely, the octonion algebra has automorphisms

$$i_t \mapsto i_{t+1}$$

$$i_t \mapsto i_{2t}$$

$$(i_0, i_1, \ldots, i_6) \mapsto (i_0, i_2, i_1, i_6, -i_4, -i_5, i_3),$$

where subscripts are understood modulo 7 ([29], Section 4.3.2, p. 120). Any triple (i_r, i_s, i_t) satisfying our assumptions can be taken to $(\pm i_0, \pm i_1, \pm i_2)$ under these mappings. We have already seen that the claim holds for i_0, i_1 and i_2, which concludes the proof. □

Right and left multiplication by an element a of $\mathbb{O}$ define the mappings

$$R_a : \mathbb{O} \to \mathbb{O}, \quad x \mapsto xa \quad \text{and}$$
$$L_a : \mathbb{O} \to \mathbb{O}, \quad x \mapsto ax.$$

These mappings are needed in our construction of E_8, and the following lemma will then prove to be useful.

Lemma 6.2. *For octonions i_r and i_s it holds that*

$$R_{i_r} R_{i_s} = \begin{cases} -1 & \text{if} \quad r = s \\ -R_{i_s} R_{i_r} & \text{if} \quad r \neq s \end{cases}$$

and

$$L_{i_r} L_{i_s} = \begin{cases} -1 & \text{if} \quad r = s \\ -L_{i_s} L_{i_r} & \text{if} \quad r \neq s. \end{cases}$$

Proof. We start by proving that $R_{i_r} R_{i_r} = -1$. For this, it is enough to show that $(i_t i_r) i_r = -i_t$ for all octonions i_t. By Lemma 6.1, we have

$$(i_t i_r) i_r = i_t (i_r i_r) = i_t (-1) = -i_t,$$

and the claim holds.

Suppose then that $r \neq s$. Now we need to show that $(i_t i_r) i_s = -(i_t i_s) i_r$ for all octonions i_t. If t is equal to r or s, or the octonions i_t, i_s and i_r are on the same line in Figure 6.1, it follows from Lemma 6.1 that

$$(i_t i_r) i_s = i_t (i_r i_s) = -i_t (i_s i_r) = -(i_t i_s) i_r.$$

Otherwise we have

$$(i_t i_r) i_s = -i_t (i_r i_s) = i_t (i_s i_r) = -(i_t i_s) i_r.$$

Thus, it holds that $R_{i_r} R_{i_s} = -R_{i_s} R_{i_r}$.

The proof is similar for the left multiplication. □

6.1.2 On the structure of $2^{5+10} \cdot \mathrm{GL}_5(2)$

A group of shape $2^{5+10} \cdot \mathrm{GL}_5(2)$ is a non-split extension of a so called special group 2^{5+10} by the linear group $\mathrm{GL}_5(2)$. In this section, we define the concepts needed in understanding the structure of the group.

We start with the group $\mathrm{GL}_5(2)$. The linear group $\mathrm{GL}_n(q)$ consists of all invertible $n \times n$-matrices over the finite field of q elements. The order of $\mathrm{GL}_n(q)$ is

$$(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}),$$

and hence $|\mathrm{GL}_5(2)| = 9999360$. The group $\mathrm{GL}_5(2)$ is a simple group.

Next, we define special groups. If G is a group, then the *Frattini subgroup* $\Phi(G)$ of G is the intersection of all the maximal subgroups of G. Let G be a finite p-group, that is, a group whose order is a power of the prime p. The group G is called *special* if

$$Z(G) = G' = \Phi(G),$$

where G' is the commutator subgroup of G.

Lemma 6.3. *Let G be a p-group. Now $G/\Phi(G)$ is an elementary abelian group, and if H is a normal subgroup of G such that G/H is elementary abelian, then $\Phi(G) \leq H$.*

Proof. The proof can be found in Aschbacher ([1], Ch. 8, Thm 23.2, p. 105). □

It follows from the lemma that the commutator subgroup of a p-group is always a subset of the Frattini subgroup.

Lemma 6.4. *The centre of a special p-group is elementary abelian.*

Proof. See Aschbacher ([1], Ch. 8, Thm 23.7, p. 108). □

We denote the elementary abelian group of order p^k simply as p^k. For example, the group 2^5 is the elementary abelian group whose order is 32.

If G is a special group of order p^n and the order of $Z(G)$ is p^k, then we say that G is of shape p^{k+m}, where $m = n - k$. For example, if the group E has shape 2^{5+10},

then it is a special group of order 2^{15}. The centre, commutator subgroup and Frattini subgroup of E all coincide, have order 2^5 and are elementary abelian. The quotient group $E/Z(E)$ is the elementary abelian group 2^{10}.

Finally, we discuss group extensions. Suppose that A and B are groups. The group G is an extension of A by B if A is a normal subgroup of G and G/A is isomorphic to B. If G has a subgroup $\bar{B}$ isomorphic to B, and every element of G can be written uniquely as a product of an element of A and an element of $\bar{B}$, then G is a split extension, or semidirect product. In this case, the group $\bar{B}$ is called the *complement* of A. The split extension is denoted $G = A : B$. If the extension is non-split, we write $G = A \cdot B$.

A group G of shape $2^{5+10} \cdot \mathrm{GL}_5(2)$ is a non-split extension of a special group 2^{5+10} by the group $\mathrm{GL}_5(2)$. In other words, G has as normal subgroup a group E of shape 2^{5+10}, and $G/E \cong \mathrm{GL}_5(2)$. The group E does not have a complement isomorphic to $\mathrm{GL}_5(2)$ in G.

6.2 Construction of a group of automorphisms

We will now start constructing a group $G = \langle x, y, z, d, e \rangle$ that acts on a 248-dimensional vector space and is of the form $2^{5+10} \cdot \mathrm{GL}_5(2)$.

Let $\mathfrak{L}$ be the real vectorspace

$$\mathfrak{L} = \mathfrak{H}_0 \oplus \mathfrak{H}_1 \oplus \cdots \oplus \mathfrak{H}_{30}, \tag{6.5}$$

where each subspace $\mathfrak{H}_r$ is a copy of the octonion algebra $\mathbb{O}$. The octonion basis $1, i_0, i_1, \ldots, i_6$ of the subspace $\mathfrak{H}_r$ will be denoted as

$$\boldsymbol{\infty}_r,\ \mathbf{0}_r,\ \mathbf{1}_r, \ldots, \mathbf{6}_r.$$

Also, we write

$$\mathcal{B} = \{\boldsymbol{\infty}, \mathbf{0}, \mathbf{1}, \ldots, \mathbf{6}\}.$$

We index the subspaces $\mathfrak{H}_r$ by non-zero elements of the 5-dimensional vector space

$$\mathbb{F}_{32} = \mathbb{F}_2[X]/\langle X^5 + X^2 + 1 \rangle.$$

The space $\mathbb{F}_{32}$ consists of the cosets of the polynomials $0, 1, X, \ldots, X^{30}$, and the cosets of 1, X, X^2, X^3 and X^4 form a basis. Addition in $\mathbb{F}_{32}$ is denoted as $\boxplus$.

Let S be the set of non-zero vectors of $\mathbb{F}_{32}$. To simplify the notation, we will identify the coset of the element X^k with the natural number k. Now

$$S = \{0, 1, \ldots 30\}.$$

The subset $\{r, s, t\}$ of S is a called a block if $X^r + X^s + X^t = 0$ in $\mathbb{F}_2[X]/(X^5+X^2+1)$, or in other words, if $r \boxplus s = t$. The group $\mathrm{GL}_5(2)$ acts on S preserving the blocks.

6.2.1 The group $\mathrm{GL}_5(2)$

The group $\mathrm{GL}_5(2)$ acts on the index set $S = \mathbb{F}_{32} \setminus \{0\}$, and is generated by three elements, $\bar{x}$, $\bar{y}$ and $\bar{z}$, that are defined as follows:

$\bar{x}$: $\quad k \mapsto k + 1$

$\bar{y}$: $\quad k \mapsto 2k$

$\bar{z} = (2, 16)(3, 6)(4, 8)(5, 9)(7, 28)(10, 20)(11, 21)(12, 17)(19, 25)(22, 26)(23, 30)(27, 29).$

Here the sum and product are taken modulo 31. Note that the subgroup generated by $\bar{x}$ and $\bar{y}$ is the semidirect product of the form $31 : 5$.

The matrices of the mappings with respect to the basis $\{0, 1, 2, 3, 4\}$ are

$$\bar{x} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{bmatrix}, \quad \bar{y} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}, \quad \bar{z} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

It can be seen that all $\bar{x}$, $\bar{y}$ and $\bar{z}$ are elements of $GL_5(2)$. Since $\bar{x}$ and $\bar{y}$ generate a maximal subgroup of $GL_5(2)$, the group $GL_5(2)$ is generated by $\bar{x}$, $\bar{y}$ and $\bar{z}$.

The mappings $\bar{x}$, $\bar{y}$ and $\bar{z}$ are permutations of the index set S of the subspaces. We will lift them to linear transformations x, y and z of $\mathfrak{L}$ that permute the subspaces the same way as $\bar{x}$, $\bar{y}$ and $\bar{z}$ do.

The mapping $x : \mathfrak{L} \to \mathfrak{L}$ maps $\mathfrak{H}_r$ to $\mathfrak{H}_{r+1}$, and is defined by

$$x : \ b_r \mapsto b_{r+1},$$

where $b \in \mathcal{B}$ is an element of the octonion basis and $r \in S$. The order of x is 31.

We define the mapping $y : \mathfrak{L} \to \mathfrak{L}$ by using a mapping of the octonion algebra $\mathbb{O}$. Let $\pi \colon \mathbb{O} \to \mathbb{O}$ be the mapping that first permutes the basis vectors of $\mathbb{O}$ as (02346) and then negates $\mathbf{0}$ and $\mathbf{3}$. We can write $\pi = (02346) \cdot N_{0,3}$. The mapping $y : \mathfrak{L} \to \mathfrak{L}$ maps $\mathfrak{H}_r$ to $\mathfrak{H}_{2r}$ and is defined by

$$y : \ b_r \mapsto (b\pi R_p)_{2r},$$

where R_p is the right multiplication by $p = \frac{1}{2}(\mathbf{0} - \mathbf{3} + \mathbf{5} - \mathbf{6})$, $b \in \mathcal{B}$ and $r \in S$.

For example, we have

$$\mathbf{0}_1 y = (\mathbf{0}_1 \pi R_p)_{2r} = \mathbf{2}_2 \cdot \frac{1}{2}(\mathbf{0}_2 - \mathbf{3}_2 + \mathbf{5}_2 - \mathbf{6}_2) = \frac{1}{2}(-\mathbf{0}_2 - \mathbf{3}_2 - \mathbf{5}_2 - \mathbf{6}_2).$$

The action of y is described in detail in Table 6.1. The order of y is 5, and we have $x^y = x^2$.

y	$\mathfrak{H}_r$	$\to$	$\mathfrak{H}_{2r}$
	$\boldsymbol{\infty}_r$	$\mapsto$	$\frac{1}{2}(\mathbf{0}_{2r} - \mathbf{3}_{2r} + \mathbf{5}_{2r} - \mathbf{6}_{2r})$
	$\mathbf{0}_r$	$\mapsto$	$\frac{1}{2}(-\mathbf{0}_{2r} - \mathbf{3}_{2r} - \mathbf{5}_{2r} - \mathbf{6}_{2r})$
	$\mathbf{1}_r$	$\mapsto$	$\frac{1}{2}(-\mathbf{0}_{2r} - \mathbf{3}_{2r} + \mathbf{5}_{2r} + \mathbf{6}_{2r})$
	$\mathbf{2}_r$	$\mapsto$	$\frac{1}{2}(-\boldsymbol{\infty}_{2r} - \mathbf{1}_{2r} - \mathbf{2}_{2r} - \mathbf{4}_{2r})$
	$\mathbf{3}_r$	$\mapsto$	$\frac{1}{2}(\mathbf{0}_{2r} - \mathbf{3}_{2r} - \mathbf{5}_{2r} + \mathbf{6}_{2r})$
	$\mathbf{4}_r$	$\mapsto$	$\frac{1}{2}(\boldsymbol{\infty}_{2r} - \mathbf{1}_{2r} + \mathbf{2}_{2r} - \mathbf{4}_{2r})$
	$\mathbf{5}_r$	$\mapsto$	$\frac{1}{2}(-\boldsymbol{\infty}_{2r} - \mathbf{1}_{2r} + \mathbf{2}_{2r} + \mathbf{4}_{2r})$
	$\mathbf{6}_r$	$\mapsto$	$\frac{1}{2}(\boldsymbol{\infty}_{2r} - \mathbf{1}_{2r} - \mathbf{2}_{2r} + \mathbf{4}_{2r})$

Table 6.1: The values of the mapping y on the subspace $\mathfrak{H}_r$

The mapping $z : \mathfrak{L} \to \mathfrak{L}$ is of order 2, and is such that $y^z = y^{-1}$. This means that $z = yzy$. Hence, we need to define the values of z on only one subspace $\mathfrak{H}_r$ in each

orbit under the element $\bar{y}$. In every orbit, there is a subspace that z fixes as a set. These subspaces are $\mathfrak{H}_0$, $\mathfrak{H}_1$, $\mathfrak{H}_{13}$, $\mathfrak{H}_{14}$, $\mathfrak{H}_{15}$, $\mathfrak{H}_{18}$ and $\mathfrak{H}_{24}$, and the action of z on them is defined in Table 6.2.

z	
$\mathfrak{H}_0$	$(02)(36) \cdot N_{\infty,1} \cdot R_{\frac{1}{2}(-\infty+3-4+6)}$
$\mathfrak{H}_1$	$(04)(16) \cdot N_{\infty,1,2,3,5,6}$
$\mathfrak{H}_{13}$	$(26)(45) \cdot N_{0,1,2,6}$
$\mathfrak{H}_{14}$	$(013)(245) \cdot N_{0,1,3,6} \cdot R_{\frac{1}{2}(-\infty+0+1+3)}$
$\mathfrak{H}_{15}$	$(023)(156) \cdot N_{0,6} \cdot R_{\frac{1}{2}(-\infty+1-5-6)}$
$\mathfrak{H}_{18}$	$(05)(13) \cdot N_{1,2,3,6} \cdot R_{\frac{1}{2}(-1+2-3-6)}$
$\mathfrak{H}_{24}$	$(\infty062)(1435) \cdot N_{0,3,4,5} \cdot R_{\frac{1}{2}(\infty+0+2+6)}$

Table 6.2: Action of z. Here the permutations permute the octonion basis vectors, the mapping $N_{a_1,\ldots,a_m}$ negates the basis vectors $a_1, \ldots a_m$ and R_a is left multiplication by $a \in \mathbb{O}$.

For example, we have

$$\mathbf{0}_0 z = \mathbf{2}_0 \cdot \frac{1}{2}(-\boldsymbol{\infty}_0 + \mathbf{3}_0 - \mathbf{4}_0 + \mathbf{6}_0) = \frac{1}{2}(\mathbf{0}_0 - \mathbf{1}_0 - \mathbf{2}_0 + \mathbf{5}_0)$$

and

$$\begin{aligned}\boldsymbol{\infty}_7 z =& \boldsymbol{\infty}_7 yzy = \frac{1}{2}(\mathbf{0}_{14} - \mathbf{3}_{14} + \mathbf{5}_{14} - \mathbf{6}_{14})zy \\ =& \frac{1}{2}(-\mathbf{0}_{14} + \mathbf{3}_{14} + \mathbf{5}_{14} - \mathbf{6}_{14})y = \frac{1}{2}(-\boldsymbol{\infty}_{28} + \mathbf{0}_{28} + \mathbf{2}_{28} + \mathbf{6}_{28}).\end{aligned}$$

The group D

Next, we construct an elementary abelian group D whose order is 2^5. It will be a normal subgroup of the group G.

Let $\tilde{D}$ be the dual space of the 5-dimensional vector space $\mathbb{F}_{32}$. It has a basis $\tilde{d}_0, \tilde{d}_1, \tilde{d}_2, \tilde{d}_3, \tilde{d}_4$, where for each $r \in \{0, \ldots, 4\}$, $\tilde{d}_r$ maps the basis vector s of $\mathbb{F}_{32}$ as

follows:

$$s\tilde{d_r} = \begin{cases} 1 & \text{if } s = r \\ 0 & \text{otherwise.} \end{cases}$$

Each $\tilde{d_r}$ induces a mapping $d_r : \mathfrak{L} \to \mathfrak{L}$. These mappings act on $\mathfrak{L}$ by changing the signs of some of the subspaces $\mathfrak{H}_r$. If r is a basis vector of $\mathbb{F}_{32}$, $s \in S$ and $v_s \in \mathfrak{H}_s$, then

$$v_s d_r = \begin{cases} -v_s & \text{if } s\tilde{d_r} = 1 \\ v_s & \text{otherwise.} \end{cases}$$

For any $v \in \mathfrak{L}$ we define vd_r by extending linearly.

For example, the mapping d_0 negates the subspace $\mathfrak{H}_0$, and fixes the subspaces $\mathfrak{H}_1$, $\mathfrak{H}_2$, $\mathfrak{H}_3$ and $\mathfrak{H}_4$. Since $5 = 0 \boxplus 2$, the mapping d_0 negates the subspace $\mathfrak{H}_5$.

Let D be the group generated $d_0, d_1, \ldots, d_4$. It is isomorphic to the elementary abelian group $\tilde{D}$. The action of the generators is described in Table 6.3.

Lemma 6.6. *The group D is normalised by the mappings x, y and z.*

Proof. Suppose that $g \in D$. We wish to show that g^x is an element of D. The mapping $g^x = x^{-1}gx$ acts on $\mathfrak{L}$ by changing the sign of some of the subspaces $\mathfrak{H}_r$. Therefore, it can be viewed as a mapping from the index set S to $\mathbb{F}_2$. In fact, this mapping is $\bar{x}^{-1}\tilde{g}$, where $\tilde{g}$ is the element of $\tilde{D}$ corresponding to g. Since $\bar{x}$ and $\tilde{g}$ are linear mappings, also $\bar{x}^{-1}\tilde{g}$ is a linear mapping, and hence an element of $\tilde{D}$. Thus, we know that $g^x \in D$.

The proofs for y and z are similar. □

Denote $d = d_0$. From the above lemma it follows that the group D contains the conjugates d^{x^m} for all $m \in \mathbb{Z}$. It is in fact true that these conjugates generate the group D. This can be seen by observing the action of the conjugates d, $d^{x^{-1}}$, $d^{x^{-2}}$, $d^{x^{-3}}$ and $d^{x^{-4}}$ on the subspaces $\mathfrak{H}_0, \ldots, \mathfrak{H}_4$. Each of them negates a subspace that the others do not negate, and therefore the group that they generate is a 5-dimensional vector space. Hence, we have

$$D = \langle d,\ d^{x^{-1}},\ d^{x^{-2}},\ d^{x^{-3}},\ d^{x^{-4}} \rangle.$$

	d_0	d_1	d_2	d_3	d_4		d_0	d_1	d_2	d_3	d_4
$\mathfrak{H}_0$	$-$	$+$	$+$	$+$	$+$	$\mathfrak{H}_{16}$	$-$	$-$	$+$	$-$	$-$
$\mathfrak{H}_1$	$+$	$-$	$+$	$+$	$+$	$\mathfrak{H}_{17}$	$-$	$-$	$+$	$+$	$-$
$\mathfrak{H}_2$	$+$	$+$	$-$	$+$	$+$	$\mathfrak{H}_{18}$	$-$	$-$	$+$	$+$	$+$
$\mathfrak{H}_3$	$+$	$+$	$+$	$-$	$+$	$\mathfrak{H}_{19}$	$+$	$-$	$-$	$+$	$+$
$\mathfrak{H}_4$	$+$	$+$	$+$	$+$	$-$	$\mathfrak{H}_{20}$	$+$	$+$	$-$	$-$	$+$
$\mathfrak{H}_5$	$-$	$+$	$-$	$+$	$+$	$\mathfrak{H}_{21}$	$+$	$+$	$+$	$-$	$-$
$\mathfrak{H}_6$	$+$	$-$	$+$	$-$	$+$	$\mathfrak{H}_{22}$	$-$	$+$	$-$	$+$	$-$
$\mathfrak{H}_7$	$+$	$+$	$-$	$+$	$-$	$\mathfrak{H}_{23}$	$-$	$-$	$-$	$-$	$+$
$\mathfrak{H}_8$	$-$	$+$	$-$	$-$	$+$	$\mathfrak{H}_{24}$	$+$	$-$	$-$	$-$	$-$
$\mathfrak{H}_9$	$+$	$-$	$+$	$-$	$-$	$\mathfrak{H}_{25}$	$-$	$+$	$+$	$-$	$-$
$\mathfrak{H}_{10}$	$-$	$+$	$+$	$+$	$-$	$\mathfrak{H}_{26}$	$-$	$-$	$-$	$+$	$-$
$\mathfrak{H}_{11}$	$-$	$-$	$-$	$+$	$+$	$\mathfrak{H}_{27}$	$-$	$-$	$+$	$-$	$+$
$\mathfrak{H}_{12}$	$+$	$-$	$-$	$-$	$+$	$\mathfrak{H}_{28}$	$+$	$-$	$-$	$+$	$-$
$\mathfrak{H}_{13}$	$+$	$+$	$-$	$-$	$-$	$\mathfrak{H}_{29}$	$-$	$+$	$+$	$-$	$+$
$\mathfrak{H}_{14}$	$-$	$+$	$-$	$-$	$-$	$\mathfrak{H}_{30}$	$+$	$-$	$+$	$+$	$-$
$\mathfrak{H}_{15}$	$-$	$-$	$-$	$-$	$-$						

Table 6.3: Action of d_0, d_1, d_2, d_3 and d_4 on the subspaces

The group E

Next, we construct a group E that is of order 2^{15}. It contains D, and is a normal subgroup of G.

We will define e to be a mapping that fixes the subspaces $\mathfrak{H}_r$ as sets, and commutes with y. As in the case of z, we only need to define the values of e for one subspace in each orbit under the element $\bar{y}$. The values are given in Table 6.4.

There is an easy way to determine the action of e on the rest of the subspaces.

Lemma 6.7. *Suppose that e acts on the subspace $\mathfrak{H}_r$ as $L_{a_1} \cdots L_{a_n}$. Now e acts on $\mathfrak{H}_{r\bar{y}}$ as $L_{a_1\pi} \cdots L_{a_n\pi}$, where $\pi = (02346) \cdot N_{0,3}$ is the mapping defined in Section 6.2.1.*

e	
$\mathfrak{H}_0$	L_5
$\mathfrak{H}_1$	$L_2L_4L_6$
$\mathfrak{H}_{13}$	$-L_2L_4$
$\mathfrak{H}_{14}$	$L_0L_1L_3$
$\mathfrak{H}_{15}$	$L_0L_3L_5$
$\mathfrak{H}_{18}$	L_6
$\mathfrak{H}_{24}$	$-L_4L_5$

Table 6.4: Action of e. Here L_b is left multiplication by the octonion $b \in \mathcal{B}$.

Proof. The mapping e acts on $\mathfrak{H}_{r\bar{y}}$ as $y^{-1}L_{a_1}\cdots L_{a_n}y$. Hence, it is enough to show that for octonions $b \in \mathcal{B}$, the mappings $L_{b\pi}$ and $y^{-1}L_by$ act the same way on a subspace $\mathfrak{H}_r$.

If $b = \boldsymbol{\infty}$, the claim clearly holds, so we can assume that $b \neq \boldsymbol{\infty}$. The mapping y consists of a permutation of the subspaces, permutation π of the octonion basis and right multiplication R_p by $p = \frac{1}{2}(\mathbf{0} - \mathbf{3} + \mathbf{5} - \mathbf{6})$. When conjugating the mapping L_b by y, we can ignore the permutations of subspaces. Now the mapping $y^{-1}L_by$ acts on a subspace $\mathfrak{H}_r$ as $R_p^{-1}\pi^{-1}L_b\pi R_p$.

The mapping $\pi^{-1}L_b\pi$ acts on the basis vectors of a subspace as follows:

$$\begin{aligned}
\pi^{-1}L_0\pi &= (\infty 2)(03)(14)(56)\cdot N_{\infty,1,3,6} = R_pL_2R_p^{-1}\\
\pi^{-1}L_1\pi &= (\infty 1)(05)(24)(36)\cdot N_{\infty,0,4,6} = R_pL_1R_p^{-1}\\
\pi^{-1}L_2\pi &= (\infty 3)(02)(16)(45)\cdot N_{2,3,4,6} = -R_pL_3R_p^{-1}\\
\pi^{-1}L_3\pi &= (\infty 4)(06)(12)(35)\cdot N_{\infty,0,2,3} = R_pL_3R_p^{-1}\\
\pi^{-1}L_4\pi &= (\infty 6)(04)(13)(25)\cdot N_{\infty,3,4,5} = R_pL_6R_p^{-1}\\
\pi^{-1}L_5\pi &= (\infty 5)(01)(26)(34)\cdot N_{\infty,1,2,4} = R_pL_5R_p^{-1}\\
\pi^{-1}L_6\pi &= (\infty 0)(15)(23)(46)\cdot N_{0,1,3,4} = -R_pL_0R_p^{-1}.
\end{aligned}$$

Now we have $\pi^{-1}L_b\pi = R_pL_{b\pi}R_p^{-1}$ for all $b \in \mathcal{B}$, and it follows that

$$R_p^{-1}\pi^{-1}L_b\pi R_p = L_{b\pi}.$$

This proves the claim. □

For example, e acts on $\mathfrak{H}_2$ as

$$L_{2\pi}L_{4\pi}L_{6\pi} = L_{-3}L_6L_{-0} = -L_3L_6(-L_0) = L_3L_6L_0.$$

The action of e on all the subspaces is described in Table 6.5.

Let E be a group that is generated by e and its conjugates by x^{-1}:

$$E = \langle e,\ e^{x^{-1}},\ e^{x^{-2}}, \ldots, e^{x^{-9}} \rangle.$$

Next, we will show that E is a special group of shape 2^{5+10}. In order to prove this, we need to determine certain commutators of elements of E. The following lemma will be useful in the calculations.

Lemma 6.8. *If*

$$A = L_{a_1} \cdots L_{a_n} \quad \textit{and} \quad B = L_{b_1} \cdots L_{b_m},$$

where $a_j, b_j, \in \mathcal{B}$ and the sets $\{a_1, \ldots, a_n\}$ and $\{b_1, \ldots, b_m\}$ have k elements in common, then

$$[A, B] = \begin{cases} 1 & \textit{if } nm + k \textit{ is even} \\ -1 & \textit{otherwise.} \end{cases}$$

Proof. In Lemma 6.2 we showed that

$$L_aL_b = \begin{cases} -1 & \text{if} \quad a = b \\ -L_bL_a & \text{if} \quad a \neq b \end{cases} \tag{6.9}$$

for all $a, b \in \mathcal{B}$.

Suppose that $A = L_{a_1} \cdots L_{a_n}$, $B = L_{b_1} \cdots L_{b_m}$ and

$$|\{a_1, \ldots, a_n\} \cap \{b_1, \ldots, b_m\}| = k.$$

Since a sign change in A or B does not affect the value of the commutator, we can assume that

$$A = L_{a_1} \cdots L_{a_k}L_{a_{k+1}} \cdots L_{a_n} \quad \text{and} \quad B = L_{a_1} \cdots L_{a_k}L_{b_{k+1}} \cdots L_{b_m}.$$

We have

$$\begin{aligned} A^{-1}B^{-1}AB &= (L_{a_n}^{-1}\cdots L_{a_{k+1}}^{-1}L_{a_k}^{-1}\cdots L_{a_1}^{-1})(L_{b_m}^{-1}\cdots L_{b_{k+1}}^{-1}L_{a_k}^{-1}\cdots L_{a_1}^{-1}) \\ &\quad \cdot (L_{a_1}\cdots L_{a_k}L_{a_{k+1}}\cdots L_{a_n})(L_{a_1}\cdots L_{a_k}L_{b_{k+1}}\cdots L_{b_m}) \\ &= (L_{a_n}^{-1}\cdots L_{a_{k+1}}^{-1}L_{a_k}^{-1}\cdots L_{a_1}^{-1})(L_{b_m}^{-1}\cdots L_{b_{k+1}}^{-1}) \\ &\quad \cdot (L_{a_{k+1}}\cdots L_{a_n})(L_{a_1}\cdots L_{a_k}L_{b_{k+1}}\cdots L_{b_m}). \end{aligned}$$

The commutator is determined in two steps. First the factors $L_{a_{k+1}}, \ldots, L_{a_n}$ are moved one by one past the product

$$L_{a_k}^{-1}\cdots L_{a_1}^{-1}L_{b_m}^{-1}\cdots L_{b_{k+1}}^{-1}.$$

This is done by using Equation 6.9. For every L_{a_j} the sign changes m times. In total, the sign is changed $(n-k)m$ times. Then the factors $L_{b_{k+1}}, \ldots, L_{b_m}$ are moved past the product

$$L_{a_1}\cdots L_{a_k}.$$

For every L_{b_j} the sign changes k times. In total, the sign is changed $(m-k)k$ times.

After this all the factors cancel out except for the sign. The commutator is equal to 1 if

$$(n-k)m + (m-k)k = nm - k^2$$

is even, and -1 otherwise. The claim now follows. □

Lemma 6.10. *The group D is the commutator subgroup of E.*

Proof. To prove that E' is a subgroup of D, it is enough to check that every commutator of the generators is in D. Since

$$[e^{x^m}, e^{x^l}] = [e, e^{x^{l-m}}]^{x^m}$$

for all integers m and l, we only need to show that $[e, e^{x^{-m}}] \in D$ for all $m \in \{1, \ldots, 9\}$.

As before, it is enough to prove this for just one generator $e^{x^{-m}}$ in each orbit under the element $\bar{y}$. We have

$$y^{-1}e^{x^{-m}}y = x^{-2m}y^{-1}eyx^{2m} = x^{-2m}ex^{2m} = e^{x^{-2m}},$$

and hence these generators are e, $e^{x^{-1}}$, $e^{x^{-3}}$, $e^{x^{-5}}$ and $e^{x^{-7}}$. Using Lemma 6.8 and Tables 6.3 and 6.5, we see that

$$\begin{aligned}
[e, e^{x^{-1}}] &= d_0 d_2 d_3 \\
[e, e^{x^{-3}}] &= d_0 d_1 d_3 \\
[e, e^{x^{-5}}] &= d_0 d_1 \\
[e, e^{x^{-7}}] &= d_0 d_1 d_2 d_4.
\end{aligned}$$

Since each of these commutators is in D, we have proved that the E' is a subset of D.

We notice that $d_0 = [e, e^{x^{-1}}][e, e^{x^{-3}}][e, e^{x^{-6}}]$, and since D is generated by the conjugates of d_0, the group D is a subset of E'. Thus, we have $D = E'$. □

Lemma 6.11. *The group E is normalised by the mappings x, y and z.*

Proof. We notice that

$$e^{x^{-10}} = d_2 d_4 e e^{x^{-3}} e^{x^{-4}} e^{x^{-9}}. \tag{6.12}$$

Hence $e^{x^{-10}} \in E$, and E is normalised by x. Since e and y commute, E is normalised by y.

It remains to verify that z normalises E. We notice that

$$z^{-1} y^{-1} e^{x^{-m}} y z = y z^{-1} e^{x^{-m}} z y^{-1},$$

and since y normalises E, it is again enough consider just one generator $e^{x^{-m}}$ in each orbit under the element $\bar{y}$. We have

$$\begin{aligned}
z^{-1} e z &= d_0 d_3 e \\
z^{-1} e^{x^{-1}} z &= d_0 d_1 d_2 d_4 e^{x^{-1}} e^{x^{-2}} e^{x^{-4}} e^{x^{-5}} e^{x^{-9}} \\
z^{-1} e^{x^{-3}} z &= e^{x^{-6}} \\
z^{-1} e^{x^{-5}} z &= d_0 d_3 e^{x^{-1}} e^{x^{-5}} e^{x^{-6}} e^{x^{-7}} e^{x^{-8}} \\
z^{-1} e^{x^{-7}} z &= d_1 d_2 d_3 e e^{x^{-1}} e^{x^{-3}} e^{x^{-4}} e^{x^{-6}} e^{x^{-9}},
\end{aligned}$$

and hence the group E is normalised by z. □

e		e	
$\mathfrak{H}_0$	L_5	$\mathfrak{H}_{16}$	$L_0L_3L_4$
$\mathfrak{H}_1$	$L_2L_4L_6$	$\mathfrak{H}_{17}$	L_6L_5
$\mathfrak{H}_2$	$L_3L_6L_0$	$\mathfrak{H}_{18}$	L_6
$\mathfrak{H}_3$	L_0L_5	$\mathfrak{H}_{19}$	$-L_0L_1L_4$
$\mathfrak{H}_4$	$-L_4L_0L_2$	$\mathfrak{H}_{20}$	L_3
$\mathfrak{H}_5$	$-L_0$	$\mathfrak{H}_{21}$	$-L_4L_0$
$\mathfrak{H}_6$	L_2L_5	$\mathfrak{H}_{22}$	$-L_0L_3$
$\mathfrak{H}_7$	$L_1L_2L_6$	$\mathfrak{H}_{23}$	$L_6L_2L_5$
$\mathfrak{H}_8$	$L_6L_2L_3$	$\mathfrak{H}_{24}$	$-L_4L_5$
$\mathfrak{H}_9$	L_4	$\mathfrak{H}_{25}$	$-L_1L_3L_6$
$\mathfrak{H}_{10}$	$-L_2$	$\mathfrak{H}_{26}$	L_3L_6
$\mathfrak{H}_{11}$	$-L_6L_2$	$\mathfrak{H}_{27}$	$L_4L_0L_5$
$\mathfrak{H}_{12}$	$-L_3L_5$	$\mathfrak{H}_{28}$	$-L_1L_2L_4$
$\mathfrak{H}_{13}$	$-L_2L_4$	$\mathfrak{H}_{29}$	$-L_3L_6L_5$
$\mathfrak{H}_{14}$	$L_0L_1L_3$	$\mathfrak{H}_{30}$	$L_2L_4L_5$
$\mathfrak{H}_{15}$	$L_0L_3L_5$		

Table 6.5: Action of e on all subspaces

Lemma 6.13. *The group E/D is an elementary abelian group of order 2^{10}.*

Proof. From Lemma 6.10 it follows that the group E/D is abelian. Also, we have $e^2 = d_0d_3 \in D$, and hence the order of an element of E/D is at most 2. Thus, E/D is an elementary abelian group. The dimension of E/D as a vector space over $\mathbb{F}_2$ can be determined using the mapping x^{-1}. It acts on E/D by conjugation, and can be considered as a linear transformation of the vector space. Since E/D is generated by the cosets $e^{x^{-m}}D$, it follows from Equation (6.12) that the transformation x^{-1} is a root of the polynomial $h = X^{10} + X^9 + X^4 + X^3 + 1 \in \mathbb{F}_2[X]$.

The polynomial h is the product of the irreducible polynomials

$$X^5 + X^3 + X^2 + X + 1 \quad \text{and} \quad X^5 + X^4 + X^3 + X + 1,$$

and since x^{-1} is not a root of either of them, h is the minimal polynomial of x^{-1}. The dimension of E/D must be greater than the degree of the minimal polynomial, which is 10. However, the vector space E/D is generated by ten elements, and hence the dimension is ten. Thus, the order of the group E/D is 2^{10}. □

Proposition 6.14. *The group E is a special group of shape 2^{5+10}.*

Proof. We need to show that $Z(E) = \Phi(E) = E'$, where $\Phi(E)$ is the Frattini subgroup of E. By Lemma 6.10, it holds that $D = E'$. Also, we know that E is a 2-group. By Lemma 6.3, the quotient group $E/\Phi(E)$ is elementary abelian, and $\Phi(E)$ is the smallest subgroup with this property. Since the quotient group E/D is elementary abelian, it follows that $\Phi(E) \leq D$. Also, we must have $E' \leq \Phi(E)$. Thus, we can conclude that $D = E' = \Phi(E)$.

It remains to show that $Z(E) = D$. The element x^{-1} can be considered as a linear transformation of the vector space E/D as in the proof of Lemma 6.13. The group D is a subgroup of $Z(E)$, and $Z(E)/D$ is an x^{-1}-invariant subspace of E/D. In the proof of Lemma 6.13 we noticed that the minimal polynomial $X^{10} + X^9 + X^4 + X^3 + 1$ of x^{-1} is a product two distinct irreducible factors of degree 5. Hence, the vector space E/D has only two non-trivial x^{-1}-invariant subspaces, and both of them are 5-dimensional. One of the subspaces is generated by the cosets of the elements

$$\begin{aligned}
&ee^{x^{-5}}e^{x^{-7}},\\
&e^{x^{-1}}e^{x^{-6}}e^{x^{-8}},\\
&e^{x^{-2}}e^{x^{-7}}e^{x^{-9}},\\
&ee^{x^{-4}}e^{x^{-8}}e^{x^{-9}},\\
&ee^{x^{-1}}e^{x^{-3}}e^{x^{-4}}e^{x^{-5}}
\end{aligned}$$

and the other is generated by the cosets of the elements

$$
\begin{aligned}
&ee^{x^{-7}}e^{x^{-9}},\\
&ee^{x^{-1}}e^{x^{-3}}e^{x^{-4}}e^{x^{-8}}e^{x^{-9}},\\
&ee^{x^{-1}}e^{x^{-2}}e^{x^{-3}}e^{x^{-5}},\\
&e^{x^{-1}}e^{x^{-2}}e^{x^{-3}}e^{x^{-4}}e^{x^{-6}},\\
&e^{x^{-2}}e^{x^{-3}}e^{x^{-4}}e^{x^{-5}}e^{x^{-7}}.
\end{aligned}
$$

Now the centre of the group E must be either E, D or a subgroup generated by one of the above sets. Since E is not commutative, and neither of the non-trivial subgroups centralises E, it follows that $D = Z(E)$. □

We will now prove that the group G is isomorphic to a non-split extension of shape $2^{5+10} \cdot \mathrm{GL}_5(2)$.

Lemma 6.15. *If the group H has the presentation*

$$
\begin{aligned}
H = \langle a, b, c \mid\ & a^{31} = 1,\ b^5 = 1,\ a^b a^{-2} = 1,\ c^2 = 1,\ b^c b = 1,\\
& (a^3 c)^5 = 1,\\
& (ca^7 ca^{-7})^3 = 1,\\
& ca^5 ca^7 ca^{13} ca^{-5} ca^{-7} ca^{-13} = 1\rangle
\end{aligned}
$$

then $H \cong \mathrm{GL}_5(2)$.

Proof. I am grateful to John Bray for this presentation of $\mathrm{GL}_5(2)$. The group $\langle \bar{x}, \bar{y}, \bar{z}\rangle$ defined in Section 6.2.1 satisfies the above relations and is isomorphic to $\mathrm{GL}_5(2)$. Hence, there is a homomorphism from H onto $\mathrm{GL}_5(2)$.

The subgroup $\langle a, b\rangle$ of H is the semidirect product $31 : 5$, and hence of order 155. Coset enumeration in MAGMA [3] gives index 64512 to this subgroup, and therefore the order of H is $9999360 = |\mathrm{GL}_5(2)|$. It follows that the homomorphism between H and $\mathrm{GL}_5(2)$ is in fact an isomorphism. □

Theorem 6.16. *The group $G = \langle x, y, z, d, e\rangle$ has shape $2^{5+10} \cdot \mathrm{GL}_5(2)$.*

Proof. By Proposition 6.14, the group E is of shape 2^{5+10}, and by Lemma 6.11, it is a normal subgroup of G. The cosets xE, yE and zE satisfy the relations given in Lemma 6.15, and hence the group G/E is isomorphic to $\mathrm{GL}_5(2)$.

Finally, we need to show that the extension does not split. Suppose that H is a complement of E in G. We know that the quotient group $G/E \cong H$ is generated by xE, yE and zE. Therefore, the group H is generated by elements x', y' and z' that are in the cosets xE, yE and zE respectively, and satisfy the relations of Lemma 6.15.

The normaliser of $\langle x' \rangle$ in H is $\langle x', y' \rangle$. Suppose that $c \in E$ normalises $\langle x' \rangle$. Now $c^{-1}x'c = (x')^m$ for some $m \in \{0, 1, \ldots, 30\}$. The subgroup E is normalised by x', and hence $(x')^{m-1} \in E$. Since $(x')^{m-1} \in H$, we have $(x')^{m-1} = 1$, and hence $m = 1$. It follows that x' centralises c. Since x' is in the coset xE and $D = E'$, the element x centralises c modulo D. However, in the proof of Proposition 6.14 we saw that the only element of E/D that is centralised by x is the identity. Hence, we have $c \in D$. Since $Z(E) = D$, the centralisers of x and x' in D coincide. The only element of D that centralises x is the identity, and we can conclude that $c = 1$. It follows that $N_G(\langle x' \rangle) = N_H(\langle x' \rangle) = \langle x', y' \rangle$.

We notice that the groups $\langle x \rangle$ and $\langle x' \rangle$ are both Sylow 31-subgroups of G. They are therefore conjugate, and also their normalisers $\langle x, y \rangle$ and $\langle x', y' \rangle$ are conjugate. It follows that there is an element g of G such that $x, y \in \langle x', y' \rangle^g \subseteq H^g$.

The element z normalises $\langle y \rangle$. Since $y \in H^g$ and H^g is a complement of E, we know that z is a product of elements h and n, where $h \in N_{H^g}(\langle y \rangle)$ and $n \in E$. Now h is in the coset zE. Hence, we have elements x, y and h of H^g that satisfy the relations in Lemma 6.15.

Now the order of $h = n^{-1}z$ is 2, so we have $n^{-1}z = zn$. Also, it holds that $hyh = (n^{-1}z)y(n^{-1}z) = y^{-1}$. We notice that

$$(n^{-1}z)y(n^{-1}z) = n^{-1}zyzn = n^{-1}y^{-1}n,$$

and hence n centralises y.

The mapping y acts on the vector space E/D by conjugation, and its fixed space

is generated by eD and cosets of the form

$$e^{x^{-k}}e^{x^{-2k}}e^{x^{-4k}}e^{x^{-8k}}e^{x^{-16k}}D.$$

However, all the latter cosets are equal to $e^{x^{-3}}e^{x^{-4}}e^{x^{-5}}e^{x^{-6}}e^{x^{-8}}D$. Of the elements of D, y centralises only 1 and d_0d_3. One can show that the element $e^{x^{-3}}e^{x^{-4}}e^{x^{-5}}e^{x^{-6}}e^{x^{-8}}d_2$ is centralised by y, and hence it follows that

$$C_E(y) = \langle d_0d_3,\ e,\ e^{x^{-3}}e^{x^{-4}}e^{x^{-5}}e^{x^{-6}}e^{x^{-8}}d_2\rangle.$$

The group $C_E(y)$ is of the shape 2^3.

We know that n^{-1} is an element of $C_E(y)$, and $n^{-1}z = h$ should satisfy the relations of Lemma 6.15. One can verify that none of the elements of $C_E(y)$ satisfy these requirements, which is a contradiction.

Thus, E does not have complement in G, and the group G is a non-split extension. □

In calculations that will follow, it is often useful to have an element of E that fixes some of the subspaces $\mathfrak{H}_r$ pointwise. For this purpose, we choose the element

$$f = d_0ee^{x^2}e^{x^5}.$$

The action of f on the subspaces $\mathfrak{H}_r$ is described in Table 6.6. When the action is written as permutations of the basis vectors, the calculations become easier.

6.3 The Lie product

6.3.1 Uniqueness

Assume that $[\cdot,\cdot] : \mathfrak{L}\times\mathfrak{L} \to \mathfrak{L}$ is a bilinear product that is invariant under the action of the group $G = \langle x, y, z, d, e\rangle$. We will show that $[\cdot,\cdot]$ is unique up to scalar multiplication.

Lemma 6.17. *If $r, s \in S$, then $[\mathfrak{H}_r, \mathfrak{H}_r] = \{0\}$ and $[\mathfrak{H}_r, \mathfrak{H}_s] \subseteq \mathfrak{H}_t$, where $\{r, s, t\}$ is a block.*

f		
$\mathfrak{H}_0$	id	id
$\mathfrak{H}_1$	$-L_0L_4L_6$	$(\infty 1)(03)(24)(56)\cdot(-1)$
$\mathfrak{H}_2$	id	id
$\mathfrak{H}_3$	$-L_1L_5L_6$	$N_{\infty,1,5,6}$
$\mathfrak{H}_4$	$L_3L_5L_6$	$(\infty 0)(13)(26)(45)$
$\mathfrak{H}_5$	id	id
$\mathfrak{H}_6$	$-L_1L_3L_4$	$(\infty 5)(04)(16)(23)\cdot(-1)$
$\mathfrak{H}_7$	$L_1L_2L_3$	$(\infty 6)(02)(15)(34)\cdot N_{\infty,0,2,6}$
$\mathfrak{H}_8$	$L_0L_3L_6$	$(\infty 5)(04)(16)(23)\cdot N_{0,1,4,6}$
$\mathfrak{H}_9$	$L_0L_1L_6$	$(\infty 4)(05)(12)(36)\cdot N_{\infty,0,4,5}$
$\mathfrak{H}_{10}$	$L_0L_3L_6$	$(\infty 5)(04)(16)(23)\cdot N_{0,1,4,6}$
$\mathfrak{H}_{11}$	$L_4L_5L_6$	$(\infty 2)(06)(14)(35)\cdot N_{\infty,2,3,5}$
$\mathfrak{H}_{12}$	$-L_0L_2L_4$	$(\infty 3)(01)(25)(46)\cdot N_{0,1,4,6}$
$\mathfrak{H}_{13}$	$L_2L_3L_4$	$(\infty 0)(13)(26)(45)\cdot N_{\infty,0,1,3}$
$\mathfrak{H}_{14}$	$L_2L_3L_6$	$(\infty 1)(03)(24)(56)\cdot N_{0,2,3,4}$
$\mathfrak{H}_{15}$	$L_1L_2L_6$	$(\infty 3)(01)(25)(46)$
$\mathfrak{H}_{16}$	$L_0L_3L_5$	$(\infty 6)(02)(15)(34)\cdot N_{\infty,1,5,6}$
$\mathfrak{H}_{17}$	$-L_0L_5L_6$	$(\infty 3)(01)(25)(46)\cdot N_{0,1,2,5}$
$\mathfrak{H}_{18}$	$-L_1L_4L_5$	$(\infty 3)(01)(25)(46)\cdot N_{\infty,0,1,3}$
$\mathfrak{H}_{19}$	$-L_0L_1L_2$	$(\infty 5)(04)(16)(23)\cdot N_{0,2,3,4}$
$\mathfrak{H}_{20}$	$-L_0L_5L_6$	$(\infty 3)(01)(25)(46)\cdot N_{0,1,2,5}$
$\mathfrak{H}_{21}$	$L_2L_5L_6$	$(\infty 4)(05)(12)(36)\cdot N_{0,3,5,6}$
$\mathfrak{H}_{22}$	$-L_0L_5L_6$	$(\infty 3)(01)(25)(46)\cdot N_{0,1,2,5}$
$\mathfrak{H}_{23}$	$L_1L_3L_6$	$(\infty 2)(06)(14)(35)\cdot N_{\infty,1,2,4}$
$\mathfrak{H}_{24}$	$L_1L_3L_5$	$(\infty 4)(05)(12)(36)\cdot N_{\infty,3,4,6}$
$\mathfrak{H}_{25}$	$-L_1L_2L_5$	$(\infty 0)(13)(26)(45)\cdot N_{\infty,0,4,5}$
$\mathfrak{H}_{26}$	$-L_1L_2L_4$	$N_{\infty,1,2,4}$
$\mathfrak{H}_{27}$	$-L_0L_2L_3$	$(\infty 4)(05)(12)(36)\cdot(-1)$
$\mathfrak{H}_{28}$	$-L_0L_2L_6$	$N_{\infty,0,2,6}$
$\mathfrak{H}_{29}$	$-L_1L_2L_4$	$N_{\infty,1,2,4}$
$\mathfrak{H}_{30}$	$L_3L_5L_6$	$(\infty 0)(13)(26)(45)$

Table 6.6: Action of f written in two different ways. Here the permutations permute the octonion basis, and the mapping $N_{a_1,\ldots,a_m}$ negates the basis vectors $a_1,\ldots a_m$.

Proof. The subspaces $\mathfrak{H}_r$ are simultaneous eigenspaces of elements of D. Since for any distinct $r_1, r_2 \in S$, there exists an element g of D such that $u_{r_1}g = -u_{r_1}$ and $u_{r_2}g = u_{r_2}$, any simultaneous eigenspace lies in one of the subspaces $\mathfrak{H}_r$.

Let $r, s \in S$, and let W be the subspace generated by the products $[v_r, v_s]$, where $v_r \in \mathfrak{H}_r$ and $v_s \in \mathfrak{H}_s$. Since D preserves the product, the subspace W is a simultaneous

eigenspace of the elements of D, and hence $W \subseteq \mathfrak{H}_t$ for some $t \in S$. Since the action of an element of D on W is a product of its actions on $\mathfrak{H}_r$ and $\mathfrak{H}_s$, we must have $t = r \boxplus s$, unless $r = s$. If $r = s$, then all the elements of D act on W as identity maps, and hence $W = \{0\}$. □

The group G acts 2-transitively on the set $\{\mathfrak{H}_r \mid r \in S\}$ and preserves the product $[\cdot, \cdot]$, so defining the product on $\mathfrak{H}_0 \times \mathfrak{H}_0$ and $\mathfrak{H}_0 \times \mathfrak{H}_2$ defines it on the whole vector space $\mathfrak{L}$. By Lemma 6.17, we know that $[\mathfrak{H}_0, \mathfrak{H}_0] = \{0\}$, and hence it is enough to determine the product on $\mathfrak{H}_0 \times \mathfrak{H}_2$.

Lemma 6.18. *The group E acts irreducibly on $\mathfrak{H}_0$.*

Proof. Suppose that K is an E-invariant subspace of $\mathfrak{H}_0$ and $K \neq \{0\}$. Let v be a non-zero element of K. Now $v = \sum_{b \in \mathcal{B}} \alpha_b b_0$ for some $\alpha_b \in \mathbb{R}$. Suppose that $a \in \mathcal{B}$ is such that $\alpha_a \neq 0$.

The mappings $f^{x^{-3}}$, f^{x^2}, and f^{x^3} act on $\mathfrak{H}_0$ by changing the signs of the basis vectors

$$\{\boldsymbol{\infty}, \mathbf{1}, \mathbf{5}, \mathbf{6}\},\ \{\boldsymbol{\infty}, \mathbf{1}, \mathbf{2}, \mathbf{4}\} \text{ and } \{\boldsymbol{\infty}, \mathbf{0}, \mathbf{2}, \mathbf{6}\},$$

respectively. The mapping d_0 changes the sign of all basis vectors.

Using the above mappings, one can eliminate from the sum $\sum_{b \in \mathcal{B}} \alpha_b b_0$ all the terms with index different from a, leaving only $\alpha_a a_0$. Hence we know that $a_0 \in K$. Every basis vector of $\mathfrak{H}_0$ can be mapped to any other basis vector by an element of E, and it follows that all the basis vectors of $\mathfrak{H}_0$ are in K. Thus $K = \mathfrak{H}_0$. □

Lemma 6.19. *The products $[\boldsymbol{\infty}_0, \boldsymbol{\infty}_2]$ and $[\boldsymbol{\infty}_0, \mathbf{1}_2]$ determine the multiplication on $\mathfrak{L}$.*

Proof. We have already seen that defining the product on $\mathfrak{H}_0 \times \mathfrak{H}_0$ and $\mathfrak{H}_0 \times \mathfrak{H}_2$ defines it on the whole vector space $\mathfrak{L}$. From Lemma 6.18 it follows that the products $[\boldsymbol{\infty}_0, v_2]$, where $v_2 \in \mathfrak{H}_2$, determine the product on $\mathfrak{H}_0 \times \mathfrak{H}_2$.

The element $f^{x^{-5}}$ fixes $\boldsymbol{\infty}_0$, and acts on $\mathfrak{H}_2$ by permuting the basis vectors as $(\infty 6)(02)(15)(34)$ and negating some of them. Hence, it is enough to determine the products $[\boldsymbol{\infty}_0, \boldsymbol{\infty}_2]$, $[\boldsymbol{\infty}_0, \mathbf{0}_2]$, $[\boldsymbol{\infty}_0, \mathbf{1}_2]$ and $[\boldsymbol{\infty}_0, \mathbf{3}_2]$.

On the other hand, the element $f^{x^{-2}}$ fixes $\boldsymbol{\infty}_0$ and permutes the basis vectors of $\mathfrak{H}_2$ as $(\infty 0)(13)(26)(45)$. Hence, it suffices to determine only the products $[\boldsymbol{\infty}_0, \boldsymbol{\infty}_2]$, and $[\boldsymbol{\infty}_0, \mathbf{1}_2]$. □

Lemma 6.20. *We have* $[\boldsymbol{\infty}_0, \mathbf{1}_2] = 0$ *and* $[\boldsymbol{\infty}_0, \boldsymbol{\infty}_2] = \alpha(\boldsymbol{\infty}_5 + \mathbf{1}_5 - \mathbf{5}_5 + \mathbf{6}_5)$*, where* $\alpha \in \mathbb{R}$*.*

Proof. Consider first the product $[\boldsymbol{\infty}_0, \mathbf{1}_2]$. By Lemma 6.17, the product $[\boldsymbol{\infty}_0, \mathbf{1}_2]$ is an element of $\mathfrak{H}_5$, and hence

$$[\boldsymbol{\infty}_0, \mathbf{1}_2] f^{x^5} = [\boldsymbol{\infty}_0, \mathbf{1}_2].$$

On the other hand, $\boldsymbol{\infty}_0 f^{x^5} = -\boldsymbol{\infty}_0$ and $\mathbf{1}_2 f^{x^5} = \mathbf{1}_2$, from which it follows that

$$[\boldsymbol{\infty}_0, \mathbf{1}_2] f^{x^5} = -[\boldsymbol{\infty}_0, \mathbf{1}_2].$$

We can conclude that $[\boldsymbol{\infty}_0, \mathbf{1}_2] = -[\boldsymbol{\infty}_0, \mathbf{1}_2] = 0$.

Consider then the product $[\boldsymbol{\infty}_0, \boldsymbol{\infty}_2]$. Suppose that

$$[\boldsymbol{\infty}_0, \boldsymbol{\infty}_2] = \alpha_\infty \boldsymbol{\infty}_5 + \alpha_0 \mathbf{0}_5 + \cdots + \alpha_6 \mathbf{6}_5,$$

where $\alpha_b \in \mathbb{R}$. Since $\boldsymbol{\infty}_0 f^{x^2} = -\boldsymbol{\infty}_0$ and $\boldsymbol{\infty}_2 f^{x^2} = \boldsymbol{\infty}_2$, we must have

$$[\boldsymbol{\infty}_0, \boldsymbol{\infty}_2] f^{x^2} = -[\boldsymbol{\infty}_0, \boldsymbol{\infty}_2] = -\alpha_\infty \boldsymbol{\infty}_5 - \alpha_0 \mathbf{0}_5 - \cdots - \alpha_6 \mathbf{6}_5.$$

On the other hand, we know that $[\boldsymbol{\infty}_0, \boldsymbol{\infty}_2] \in \mathfrak{H}_5$, so that

$$\begin{aligned}
&[\boldsymbol{\infty}_0, \boldsymbol{\infty}_2] f^{x^2} \\
&= (\alpha_\infty \boldsymbol{\infty}_5 + \alpha_0 \mathbf{0}_5 + \cdots + \alpha_6 \mathbf{6}_5) f^{x^2} \\
&= -\alpha_\infty \boldsymbol{\infty}_5 + \alpha_0 \mathbf{0}_5 - \alpha_1 \mathbf{1}_5 + \alpha_2 \mathbf{2}_5 + \alpha_3 \mathbf{3}_5 + \alpha_4 \mathbf{4}_5 - \alpha_5 \mathbf{5}_5 - \alpha_6 \mathbf{6}_5,
\end{aligned}$$

and hence we have $\alpha_0 = \alpha_2 = \alpha_3 = \alpha_4 = 0$.

Next, we notice that $\boldsymbol{\infty}_0 f^{x^{-3}} = -\boldsymbol{\infty}_0$ and $\boldsymbol{\infty}_2 f^{x^{-3}} = \boldsymbol{\infty}_2$, so that

$$[\boldsymbol{\infty}_0, \boldsymbol{\infty}_2] f^{x^{-3}} = -[\boldsymbol{\infty}_0, \boldsymbol{\infty}_2].$$

On the other hand, we have

$$\begin{aligned}[\boldsymbol{\infty}_0, \boldsymbol{\infty}_2] f^{x^{-3}} &= (\alpha_\infty \boldsymbol{\infty}_5 + \alpha_1 \mathbf{1}_5 + \alpha_5 \mathbf{5}_5 + \alpha_6 \mathbf{6}_5) f^{x^{-3}} \\ &= \alpha_5 \boldsymbol{\infty}_5 - \alpha_6 \mathbf{1}_5 + \alpha_\infty \mathbf{5}_5 - \alpha_1 \mathbf{6}_5,\end{aligned}$$

and hence $\alpha_\infty = -\alpha_5$ and $\alpha_1 = \alpha_6$.

Finally, we have $\boldsymbol{\infty}_0 f^{x^{-8}} f^{x^{-6}} = -\boldsymbol{\infty}_0$ and $\boldsymbol{\infty}_2 f^{x^{-8}} f^{x^{-6}} = \boldsymbol{\infty}_2$ from which it follows that $[\boldsymbol{\infty}_0, \boldsymbol{\infty}_2] f^{x^{-8}} f^{x^{-6}} = -[\boldsymbol{\infty}_0, \boldsymbol{\infty}_2]$. We know that

$$\begin{aligned}[\boldsymbol{\infty}_0, \boldsymbol{\infty}_2] f^{x^{-8}} f^{x^{-6}} &= (\alpha_\infty \boldsymbol{\infty}_5 + \alpha_1 \mathbf{1}_5 - \alpha_\infty \mathbf{5}_5 + \alpha_1 \mathbf{6}_5) f^{x^{-8}} f^{x^{-6}} \\ &= -\alpha_1 \boldsymbol{\infty}_5 - \alpha_\infty \mathbf{1}_5 + \alpha_1 \mathbf{5}_5 - \alpha_\infty \mathbf{6}_5,\end{aligned}$$

and hence $\alpha_\infty = \alpha_1$. Thus, we have

$$[\boldsymbol{\infty}_0, \boldsymbol{\infty}_2] = \alpha_\infty(\boldsymbol{\infty}_5 + \mathbf{1}_5 - \mathbf{5}_5 + \mathbf{6}_5).$$

□

We have now shown that the product is determined by the group G up to scalar multiplication.

6.3.2 Multiplication table

We have shown that $[\boldsymbol{\infty}_0, \mathbf{1}_2] = 0$, and can assume that $[\boldsymbol{\infty}_0, \boldsymbol{\infty}_2] = q$, where

$$q = \frac{1}{2}(\boldsymbol{\infty}_5 + \mathbf{1}_5 - \mathbf{5}_5 + \mathbf{6}_5).$$

The multiplication table for $\mathfrak{H}_0 \times \mathfrak{H}_2$ can be determined from these two values using the group E. All the other products are then obtained using the elements x, y and z.

Here we compute the multiplication table of $\mathfrak{H}_0 \times \mathfrak{H}_2$. The mappings $f^{x^{-2}}$ and $f^{x^{-5}}$ fix $\mathfrak{H}_0$ pointwise and are used in determining the first row of the multiplication table. We have $\boldsymbol{\infty}_2 f^{x^{-2}} = \mathbf{0}_2$ and hence

$$[\boldsymbol{\infty}_0, \mathbf{0}_2] = [\boldsymbol{\infty}_0 f^{x^{-2}}, \boldsymbol{\infty}_2 f^{x^{-2}}] = [\boldsymbol{\infty}_0, \boldsymbol{\infty}_2] f^{x^{-2}} = q f^{x^{-2}} = -q.$$

Similarly, we notice that $\mathbf{1}_2 f^{x^{-2}} = \mathbf{3}_2$, which means that

$$[\boldsymbol{\infty}_0, \mathbf{3}_2] = [\boldsymbol{\infty}_0 f^{x^{-2}}, \mathbf{1}_2 f^{x^{-2}}] = [\boldsymbol{\infty}_0, \mathbf{1}_2] f^{x^{-2}} = 0 f^{x^{-2}} = 0.$$

All the entries in the first row can be determined in a similar manner.

The elements in the second row are obtained using the mapping f^x. After this one can find the rest of the entries using mappings f^{x^4} and $f^{x^{-1}}$.

The multiplication table is displayed as Table 6.7. All the entries of the multiplication table can be expressed as octonion multiples of the element $q = \frac{1}{2}(\boldsymbol{\infty}_5 + \mathbf{1}_5 - \mathbf{5}_5 + \mathbf{6}_5)$. Notice that

$$\begin{aligned}
\mathbf{0}_5 q &= \frac{1}{2}(\mathbf{0}_5 - \mathbf{2}_5 + \mathbf{3}_5 + \mathbf{4}_5), & \mathbf{4}_5 q &= \frac{1}{2}(-\mathbf{0}_5 + \mathbf{2}_5 + \mathbf{3}_5 + \mathbf{4}_5),\\
\mathbf{1}_5 q &= \frac{1}{2}(-\boldsymbol{\infty}_5 + \mathbf{1}_5 - \mathbf{5}_5 - \mathbf{6}_5), & \mathbf{5}_5 q &= \frac{1}{2}(\boldsymbol{\infty}_5 + \mathbf{1}_5 + \mathbf{5}_5 - \mathbf{6}_5),\\
\mathbf{2}_5 q &= \frac{1}{2}(\mathbf{0}_5 + \mathbf{2}_5 + \mathbf{3}_5 - \mathbf{4}_5), & \mathbf{6}_5 q &= \frac{1}{2}(-\boldsymbol{\infty}_5 + \mathbf{1}_5 + \mathbf{5}_5 + \mathbf{6}_5).\\
\mathbf{3}_5 q &= \frac{1}{2}(-\mathbf{0}_5 - \mathbf{2}_5 + \mathbf{3}_5 - \mathbf{4}_5),
\end{aligned}$$

	$\boldsymbol{\infty}_2$	$\mathbf{0}_2$	$\mathbf{1}_2$	$\mathbf{2}_2$	$\mathbf{3}_2$	$\mathbf{4}_2$	$\mathbf{5}_2$	$\mathbf{6}_2$
$\boldsymbol{\infty}_0$	q	$-q$	0	$-q$	0	0	0	q
$\mathbf{0}_0$	0	0	$-\mathbf{2}_5 q$	0	$\mathbf{2}_5 q$	$\mathbf{2}_5 q$	$-\mathbf{2}_5 q$	0
$\mathbf{1}_0$	$-\mathbf{6}_5 q$	$-\mathbf{6}_5 q$	0	$-\mathbf{6}_5 q$	0	0	0	$-\mathbf{6}_5 q$
$\mathbf{2}_0$	$-\mathbf{1}_5 q$	$\mathbf{1}_5 q$	0	$-\mathbf{1}_5 q$	0	0	0	$\mathbf{1}_5 q$
$\mathbf{3}_0$	0	0	$\mathbf{4}_5 q$	0	$\mathbf{4}_5 q$	$\mathbf{4}_5 q$	$\mathbf{4}_5 q$	0
$\mathbf{4}_0$	$-\mathbf{5}_5 q$	$-\mathbf{5}_5 q$	0	$\mathbf{5}_5 q$	0	0	0	$\mathbf{5}_5 q$
$\mathbf{5}_0$	0	0	$\mathbf{0}_5 q$	0	$\mathbf{0}_5 q$	$-\mathbf{0}_5 q$	$-\mathbf{0}_5 q$	0
$\mathbf{6}_0$	0	0	$\mathbf{3}_5 q$	0	$-\mathbf{3}_5 q$	$\mathbf{3}_5 q$	$-\mathbf{3}_5 q$	0

Table 6.7: The multiplication table of $\mathfrak{H}_0 \times \mathfrak{H}_2$. Here $q = \frac{1}{2}(\boldsymbol{\infty}_5 + \mathbf{1}_5 - \mathbf{5}_5 + \mathbf{6}_5)$.

6.3.3 Existence

In this section we verify that the product can be defined consistently, as there may be many ways of deriving the rules of multiplication from the action of the group

$G = \langle x, y, z, d, e \rangle$. This amounts to checking that after the product has been determined using some elements of G, then all elements of G preserve it.

The group D was used in showing that

$$[\mathfrak{H}_r, \mathfrak{H}_s] \subseteq \mathfrak{H}_t, \quad \text{where } \{r, s, t\} \text{ is a block.} \tag{6.21}$$

Hence D preserves the product.

Once the product is determined on all pairs of subspaces in the block $\{\mathfrak{H}_0, \mathfrak{H}_2, \mathfrak{H}_5\}$, the 154 non-trivial elements of $\langle x, y \rangle$ are used in determining the product on the other 154 blocks. One needs to make sure that the action of x and y does not contradict Equation (6.21), but this follows from the fact that $\bar{x}$ and $\bar{y}$ preserve the blocks of S. Suppose that $r, s \in S$ and $t = r \boxplus s$. Now there exists $g \in \langle x, y \rangle$ such that $\mathfrak{H}_r g, \mathfrak{H}_s g \in \{\mathfrak{H}_0, \mathfrak{H}_2, \mathfrak{H}_5\}$. If $\bar{g}$ is the permutation of $\langle \bar{x}, \bar{y} \rangle$ corresponding to g, then

$$[\mathfrak{H}_r, \mathfrak{H}_s] = [\mathfrak{H}_r g, \mathfrak{H}_s g] g^{-1} \subseteq \mathfrak{H}_k g^{-1} = \mathfrak{H}_{k\bar{g}^{-1}},$$

where $k = r\bar{g} \boxplus s\bar{g} = t\bar{g}$. Hence, we obtain $[\mathfrak{H}_r, \mathfrak{H}_s] \subseteq \mathfrak{H}_t$ as desired. It follows that the product is invariant under $\langle x, y \rangle$.

Consider then the group E. It is generated by the conjugates of e by x, so it suffices to consider the mapping e. Since y preserves the product, it is enough to consider just one pair of subspaces in each orbit under $\bar{y}$. The product is zero on $\mathfrak{H}_r \times \mathfrak{H}_r$ for all $r \in S$, and hence these pairs need not be taken into account. Therefore, the products that have to be checked are

$$[\mathfrak{H}_0, \mathfrak{H}_r], \quad [\mathfrak{H}_r, \mathfrak{H}_0], \quad [\mathfrak{H}_r, \mathfrak{H}_{r+s}] \quad \text{and} \quad [\mathfrak{H}_{r+s}, \mathfrak{H}_r],$$

where $r \in \{1, 13, 14, 15, 18, 24\}$, $s \in \{1, 2, \ldots, 30\}$ and $r + s \neq 0$. There are 23040 products of basis vectors to verify. However, the number of cases can be reduced by noticing that e^2 preserves the product because $e^2 = d_0 d_3 \in D$. Now, if $[ve, we] = [v, w]e$ for some $v, w \in \mathfrak{L}$, then

$$[(ve)e, (we)e] = [ve^2, we^2] = [v, w]e^2 = [ve, we]e.$$

It follows that it is enough to consider just one pair of vectors in each orbit under the element e.

For example,

$$\begin{aligned}[\boldsymbol{\infty}_0, \boldsymbol{\infty}_1]e &= [\boldsymbol{\infty}_0 y, \boldsymbol{\infty}_1 y]y^{-1}e \\ &= \left[\frac{1}{2}(\mathbf{0}_0 - \mathbf{3}_0 + \mathbf{5}_0 - \mathbf{6}_0), \frac{1}{2}(\mathbf{0}_2 - \mathbf{3}_2 + \mathbf{5}_2 - \mathbf{6}_2)\right] y^{-1}e \\ &= \frac{1}{2}(-\mathbf{0}_5 - \mathbf{3}_5)y^{-1}e = \frac{1}{2}(\mathbf{0}_{18} + \mathbf{1}_{18})e = \frac{1}{2}(\mathbf{2}_{18} + \mathbf{5}_{18})\end{aligned}$$

and

$$\begin{aligned}[\boldsymbol{\infty}_0 e, \boldsymbol{\infty}_1 e] &= [\mathbf{5}_0, -\mathbf{5}_1] = [\mathbf{5}_0 y, -\mathbf{5}_1 y]y^{-1} \\ &= \left[\frac{1}{2}(-\boldsymbol{\infty}_0 - \mathbf{1}_0 + \mathbf{2}_0 + \mathbf{4}_0), \frac{1}{2}(\boldsymbol{\infty}_2 + \mathbf{1}_2 - \mathbf{2}_2 - \mathbf{4}_2)\right] y^{-1} \\ &= \frac{1}{2}(-\boldsymbol{\infty}_5 - \mathbf{1}_5)y^{-1} = \frac{1}{2}(\mathbf{2}_{18} + \mathbf{5}_{18}).\end{aligned}$$

The rest of the cases are similar, and they have been checked using a computer program. The code can be found in Appendix A.

Finally, we show that the mapping z preserves the product. Here we can use the fact that z normalises the group $\langle E, y\rangle$. We already know that the group $\langle E, y\rangle$ preserves the product, and hence it is enough to consider just one vector in each orbit under this group. Namely, if

$$[vz, wz] = [v, w]z$$

for some vectors $v, w \in \mathfrak{L}$, and g is an element of $\langle E, y\rangle$, then

$$\begin{aligned}[(vg)z, (wg)z] &= [(vz)g^z, (wz)g^z] = [vz, wz]g^z = [v, w]zg^z \\ &= [v, w]gz = [vg, wg]z.\end{aligned}$$

The orbits are represented by

$$[\boldsymbol{\infty}_0, \boldsymbol{\infty}_r], \quad [\boldsymbol{\infty}_r, \boldsymbol{\infty}_0], \quad [\boldsymbol{\infty}_r, \boldsymbol{\infty}_{r+s}] \quad \text{and} \quad [\boldsymbol{\infty}_{r+s}, \boldsymbol{\infty}_r],$$

where $r \in \{1, 13, 14, 15, 18, 24\}$ and $s \in \{1, \ldots, 30\}$. Again, it is enough to consider one pair in each orbit under the mapping z, so we have the products

$$[\boldsymbol{\infty}_0, \boldsymbol{\infty}_r], \quad [\boldsymbol{\infty}_r, \boldsymbol{\infty}_0], \quad [\boldsymbol{\infty}_r, \boldsymbol{\infty}_t], \quad [\boldsymbol{\infty}_t, \boldsymbol{\infty}_r],$$

where r is as above and and $t \in \{2,3,4,5,7,10,11,12,19,22,23,27\}$. In total, this makes $2 \cdot 6 + 2 \cdot 6 \cdot 12 = 156$ cases.

For example,

$$[\infty_0, \infty_1]z = \frac{1}{2}(\mathbf{0}_{18} + \mathbf{1}_{18})z = \frac{1}{4}(-\infty_{18} - \mathbf{0}_{18} - \mathbf{1}_{18} + \mathbf{2}_{18} + \mathbf{3}_{18} - \mathbf{4}_{18} + \mathbf{5}_{18} + \mathbf{6}_{18})$$

and

$$\begin{aligned}
[\infty_0 z, \infty_1 z] &= \left[\frac{1}{2}(\infty_0 - \mathbf{3}_0 + \mathbf{4}_0 - \mathbf{6}_0), -\infty_1\right] \\
&= \left[\frac{1}{2}(\infty_0 - \mathbf{3}_0 + \mathbf{4}_0 - \mathbf{6}_0)y, -\infty_1 y\right] y^{-1} \\
&= \left[\frac{1}{2}(\mathbf{2}_0 - \mathbf{4}_0 + \mathbf{5}_0 - \mathbf{6}_0), \frac{1}{2}(-\mathbf{0}_2 + \mathbf{3}_2 - \mathbf{5}_2 + \mathbf{6}_2)\right] y^{-1} \\
&= \frac{1}{4}(-\infty_5 + \mathbf{0}_5 - \mathbf{1}_5 - \mathbf{2}_5 + \mathbf{3}_5 + \mathbf{4}_5 - \mathbf{5}_5 + \mathbf{6}_5)y^{-1} \\
&= \frac{1}{4}(-\infty_{18} - \mathbf{0}_{18} - \mathbf{1}_{18} + \mathbf{2}_{18} + \mathbf{3}_{18} - \mathbf{4}_{18} + \mathbf{5}_{18} + \mathbf{6}_{18}).
\end{aligned}$$

The rest of the cases are similar, and have been checked using a computer program. (For the code, see Appendix A.)

Hence, the element z preserves the product, and we can conclude that the product is well defined.

6.3.4 Anti-symmetry

Next we prove that the product defined by the group G is anti-symmetric. Since the images of $[\infty_0, \infty_2]$ and $[\infty_0, \mathbf{1}_2]$ under G determine the whole product, it is enough to prove the claim for these two products.

In determining the products $[\infty_2, \infty_0]$ and $[\mathbf{1}_2, \infty_0]$, we will use the involution $z^{x^{-27}}$ that interchanges the subspaces $\mathfrak{H}_0$ and $\mathfrak{H}_2$.

Recall that $z = yzy$. We have

$$\begin{aligned}
\boldsymbol{\infty}_2 z^{x^{-27}} &= \boldsymbol{\infty}_{29} z x^{-27} = \boldsymbol{\infty}_{29} y^{-2} z y^{-2} x^{-27} \\
&= \frac{1}{2}(-\mathbf{2}_{30} + \mathbf{4}_{30} - \mathbf{5}_{30} + \mathbf{6}_{30}) y^{-1} z y^{-2} x^{-27} \\
&= \frac{1}{2}(-\boldsymbol{\infty}_{15} + \mathbf{3}_{15} - \mathbf{4}_{15} + \mathbf{6}_{15}) z y^{-2} x^{-27} \\
&= \frac{1}{2}(\mathbf{0}_{15} - \mathbf{1}_{15} - \mathbf{2}_{15} + \mathbf{5}_{15}) y^{-2} x^{-27} \\
&= \frac{1}{2}(\boldsymbol{\infty}_{23} - \mathbf{0}_{23} + \mathbf{2}_{23} + \mathbf{6}_{23}) y^{-1} x^{-27} \\
&= \frac{1}{2}(-\boldsymbol{\infty}_{27} + \mathbf{1}_{27} - \mathbf{2}_{27} + \mathbf{4}_{27}) x^{-27} \\
&= \frac{1}{2}(-\boldsymbol{\infty}_0 + \mathbf{1}_0 - \mathbf{2}_0 + \mathbf{4}_0)
\end{aligned}$$

and

$$\begin{aligned}
\boldsymbol{\infty}_0 z^{x^{-27}} &= \boldsymbol{\infty}_{27} z x^{-27} = \boldsymbol{\infty}_{27} y^2 z y^2 x^{-27} \\
&= \frac{1}{2}(\mathbf{0}_{23} - \mathbf{3}_{23} + \mathbf{5}_{23} - \mathbf{6}_{23}) y z y^2 x^{-27} \\
&= \frac{1}{2}(-\boldsymbol{\infty}_{15} - \mathbf{0}_{15} + \mathbf{2}_{15} - \mathbf{6}_{15}) z y^2 x^{-27} \\
&= \frac{1}{2}(\boldsymbol{\infty}_{15} - \mathbf{3}_{15} + \mathbf{4}_{15} + \mathbf{6}_{15}) y^2 x^{-27} \\
&= \frac{1}{2}(\boldsymbol{\infty}_{30} - \mathbf{1}_{30} + \mathbf{5}_{30} - \mathbf{6}_{30}) y x^{-27} \\
&= \frac{1}{2}(-\boldsymbol{\infty}_{29} + \mathbf{0}_{29} + \mathbf{2}_{29} - \mathbf{6}_{29}) x^{-27} \\
&= \frac{1}{2}(-\boldsymbol{\infty}_2 + \mathbf{0}_2 + \mathbf{2}_2 - \mathbf{6}_2).
\end{aligned}$$

From multiplication table 6.7 we can see that $[\boldsymbol{\infty}_2 z^{x^{-27}}, \boldsymbol{\infty}_0 z^{x^{-27}}] = q$. It now follows that

$$\begin{aligned}
[\boldsymbol{\infty}_2, \boldsymbol{\infty}_0] &= [\boldsymbol{\infty}_2 z^{x^{-27}}, \boldsymbol{\infty}_0 z^{x^{-27}}] z^{x^{-27}} = q z^{x^{-27}} \\
&= \frac{1}{2}(\boldsymbol{\infty}_1 + \mathbf{1}_1 - \mathbf{5}_1 + \mathbf{6}_1) z x^{-27} = \frac{1}{2}(-\boldsymbol{\infty}_1 - \mathbf{1}_1 + \mathbf{5}_1 - \mathbf{6}_1) x^{-27} \\
&= \frac{1}{2}(-\boldsymbol{\infty}_5 - \mathbf{1}_5 + \mathbf{5}_5 - \mathbf{6}_5) = -q,
\end{aligned}$$

and hence $[\boldsymbol{\infty}_2, \boldsymbol{\infty}_0] = -q = -[\boldsymbol{\infty}_0, \boldsymbol{\infty}_2]$.

Next, we determine the product $[\mathbf{1}_2, \boldsymbol{\infty}_0]$ using the mapping $z^{x^{-27}}$. We have

$$\begin{aligned}
\mathbf{1}_2 z^{x^{-27}} &= \mathbf{1}_{29} z x^{-27} = \mathbf{1}_{29} y^{-22} z y^{-2} x^{-27} \\
&= \frac{1}{2}(-\mathbf{2}_{30} - \mathbf{4}_{30} - \mathbf{5}_{30} - \mathbf{6}_{30}) y^{-1} z y^{-2} x^{-27} \\
&= \frac{1}{2}(\mathbf{0}_{15} - \mathbf{1}_{15} + \mathbf{2}_{15} - \mathbf{5}_{15}) z y^{-2} x^{-27} \\
&= \frac{1}{2}(-\mathbf{0}_{15} + \mathbf{1}_{15} - \mathbf{2}_{15} + \mathbf{5}_{15}) y^{-2} x^{-27} \\
&= \frac{1}{2}(\mathbf{1}_{23} - \mathbf{3}_{23} - \mathbf{4}_{23} + \mathbf{5}_{23}) y^{-1} x^{-27} \\
&= \frac{1}{2}(\mathbf{0}_{27} + \mathbf{3}_{27} - \mathbf{5}_{27} - \mathbf{6}_{27}) x^{-27} \\
&= \frac{1}{2}(\mathbf{0}_0 + \mathbf{3}_0 - \mathbf{5}_0 - \mathbf{6}_0).
\end{aligned}$$

Since

$$[\mathbf{1}_2 z^{x^{-27}}, \boldsymbol{\infty}_0 z^{x^{-27}}] = \left[\frac{1}{2}(\mathbf{0}_0 + \mathbf{3}_0 - \mathbf{5}_0 - \mathbf{6}_0), \frac{1}{2}(-\boldsymbol{\infty}_2 + \mathbf{0}_2 + \mathbf{2}_2 - \mathbf{6}_2)\right] = 0,$$

it follows that

$$[\mathbf{1}_2, \boldsymbol{\infty}_0] = [\mathbf{1}_2 z^{x^{-27}}, \boldsymbol{\infty}_0 z^{x^{-27}}] z^{x^{-27}} = 0 z^{x^{-27}} = 0.$$

The product $[\boldsymbol{\infty}_0, \mathbf{1}_2]$ is also zero, and hence $[\boldsymbol{\infty}_0, \mathbf{1}_2] = -[\mathbf{1}_2, \boldsymbol{\infty}_0]$.

6.3.5 The Jacobi identity

In this section we prove that the product $[\cdot, \cdot]$ satisfies the Jacobi identity

$$[[v, w], u] + [[u, v], w] + [[w, u], v] = 0$$

for all $v, w, u \in \mathfrak{L}$.

By bilinearity, it is enough to prove that

$$[[v_r, w_s], u_t] + [[u_t, v_r], w_s] + [[w_s, u_t], v_r] = 0, \tag{6.22}$$

where v_r, w_s and u_t are basis vectors of $\mathfrak{H}_r$, $\mathfrak{H}_s$ and $\mathfrak{H}_t$, respectively. There are only three cases that need to be considered.

Case 1

Suppose first that r, s and t are linearly dependent and $r = s \boxplus t$. We have $[v_r, w_s] \in \mathfrak{H}_t$, and hence $[[v_r, w_s], u_t] = 0$. Similarly one notices that $[[u_t, v_r], w_s] = 0$ and $[[w_s, u_t], v_r] = 0$, and hence

$$[[v_r, w_s], u_t] + [[u_t, v_r], w_s] + [[w_s, u_t], v_r] = 0.$$

Case 2

Suppose that r, s and t are linearly dependent and $r = s \neq t$. We will show that there is an element of G that maps the triple (v_r, w_s, u_t) to $(v_0, \boldsymbol{\infty}_0, \boldsymbol{\infty}_1)$, where $v_0 \in \mathfrak{H}_0$.

The group $\langle x, y, z \rangle$ acts on S as $\mathrm{GL}_5(2)$, and hence there is an element that maps $(\mathfrak{H}_r, \mathfrak{H}_s, \mathfrak{H}_t)$ to $(\mathfrak{H}_0, \mathfrak{H}_0, \mathfrak{H}_1)$. Suppose that the triple (v_r, w_s, u_t) is mapped to the triple (v_0, w_0, u_1).

The elements of E permute the basis vectors of each subspace $\mathfrak{H}_r$ and change their signs. However, the sign changes do not affect Equation (6.22), and we need not take them into account. The group E acts on the octonion basis of $\mathfrak{H}_0$ transitively, and hence (v_0, w_0, u_1) can be mapped to $(v_0, \boldsymbol{\infty}_0, u_1)$. The group $\langle f,\ f^{x^2},\ f^{x^5} \rangle$ fixes the basis elements of $\mathfrak{H}_0$ modulo signs, and acts on the octonion basis of $\mathfrak{H}_1$ transitively. Therefore, the triple $(v_0, \boldsymbol{\infty}_0, u_1)$ can be mapped to $(v_0, \boldsymbol{\infty}_0, \boldsymbol{\infty}_1)$.

Now it suffices to verify that

$$[[v_0, \boldsymbol{\infty}_0], \boldsymbol{\infty}_1] + [[\boldsymbol{\infty}_1, v_0], \boldsymbol{\infty}_0] + [[\boldsymbol{\infty}_0, \boldsymbol{\infty}_1], v_0] = 0$$

for all basis vectors v_0 of $\mathfrak{H}_0$.

First of all, we notice that $[[v_0, \boldsymbol{\infty}_0], \boldsymbol{\infty}_1] = [0, \boldsymbol{\infty}_1] = 0$ for all $v_0 \in \mathfrak{H}_0$. Our next task is to determine the products $[[\boldsymbol{\infty}_1, v_0], \boldsymbol{\infty}_0]$, where $v_0 \in \mathfrak{H}_0$. In Section 6.3.3, we saw that $[\boldsymbol{\infty}_1, \boldsymbol{\infty}_0] = \frac{1}{2}(-\mathbf{0}_{18} - \mathbf{1}_{18})$. The other products of the form $[\boldsymbol{\infty}_1, v_0]$ can now be determined using the group $\langle f^{x^{-1}},\ f^x,\ f^{x^4} \rangle$ that fixes the basis elements of $\mathfrak{H}_1$ modulo signs, and permutes the basis vectors of $\mathfrak{H}_0$. The products are displayed in

Table 6.8. Next, we notice that

$$\begin{aligned}
&[[\boldsymbol{\infty}_1, \boldsymbol{\infty}_0], \boldsymbol{\infty}_0] = \left[\frac{1}{2}(-\mathbf{0}_{18} - \mathbf{1}_{18}), \boldsymbol{\infty}_0\right] \\
&= \left[\frac{1}{2}(-\mathbf{0}_{18} - \mathbf{1}_{18})yz^{x^{-1}}, \boldsymbol{\infty}_0 yz^{x^{-1}}\right] z^{x^{-1}}y^{-1} \\
&= \left[\frac{1}{4}(-\boldsymbol{\infty}_2 - \mathbf{0}_2 - \mathbf{1}_2 + \mathbf{2}_2 - \mathbf{3}_2 + \mathbf{4}_2 + \mathbf{5}_2 + \mathbf{6}_2), \frac{1}{2}(\mathbf{1}_0 + \mathbf{3}_0 + \mathbf{4}_0 - \mathbf{5}_0)\right] z^{x^{-1}}y^{-1} \\
&= \frac{1}{4}(-\boldsymbol{\infty}_5 - \mathbf{0}_5 - \mathbf{1}_5 + \mathbf{2}_5 - \mathbf{3}_5 - \mathbf{4}_5 - \mathbf{5}_5 + \mathbf{6}_5)z^{x^{-1}}y^{-1} \\
&= \frac{1}{2}(-\boldsymbol{\infty}_1 - \mathbf{1}_1)
\end{aligned}$$

and

$$\begin{aligned}
&[[\boldsymbol{\infty}_1, \mathbf{2}_0], \boldsymbol{\infty}_0] = \left[\frac{1}{2}(\mathbf{2}_{18} + \mathbf{5}_{18}), \boldsymbol{\infty}_0\right] \\
&= \left[\frac{1}{2}(\mathbf{2}_{18} + \mathbf{5}_{18})yz^{x^{-1}}, \boldsymbol{\infty}_0 yz^{x^{-1}}\right] z^{x^{-1}}y^{-1} \\
&= \left[\frac{1}{4}(\boldsymbol{\infty}_2 - \mathbf{0}_2 - \mathbf{1}_2 - \mathbf{2}_2 + \mathbf{3}_2 + \mathbf{4}_2 - \mathbf{5}_2 + \mathbf{6}_2), \frac{1}{2}(\mathbf{1}_0 + \mathbf{3}_0 + \mathbf{4}_0 - \mathbf{5}_0)\right] z^{x^{-1}}y^{-1} \\
&= 0z^{x^{-1}}y^{-1} = 0.
\end{aligned}$$

The rest of the products $[[\boldsymbol{\infty}_1, v_0], \boldsymbol{\infty}_0]$ can be determined using the group $\langle f,\ f^{x^{-5}}\rangle$ that fixes the basis elements of $\mathfrak{H}_0$ modulo signs, and permutes the products $[\boldsymbol{\infty}_1, v_0]$. The results can be found in Table 6.8.

Finally, we need to calculate the products of the form $[[\boldsymbol{\infty}_0, \boldsymbol{\infty}_1], v_0]$, where $v_0 \in \mathfrak{H}_0$. We have already seen that $[\boldsymbol{\infty}_0, \boldsymbol{\infty}_1] = \frac{1}{2}(\mathbf{0}_{18} + \mathbf{1}_{18})$ and

$$\left[\frac{1}{2}(\mathbf{0}_{18} + \mathbf{1}_{18}), \boldsymbol{\infty}_0\right] = \frac{1}{2}(\boldsymbol{\infty}_1 + \mathbf{1}_1).$$

Also, we notice that

$$\begin{aligned}
&\left[\frac{1}{2}(\mathbf{0}_{18} + \mathbf{1}_{18}), \mathbf{2}_0\right] = \left[\frac{1}{2}(\mathbf{0}_{18} + \mathbf{1}_{18})yz^{x^{-1}}, \boldsymbol{\infty}_2 yz^{x^{-1}}\right] z^{x^{-1}}y^{-1} \\
&= \left[\frac{1}{4}(\boldsymbol{\infty}_2 + \mathbf{0}_2 + \mathbf{1}_2 - \mathbf{2}_2 + \mathbf{3}_2 - \mathbf{4}_2 - \mathbf{5}_2 - \mathbf{6}_2), \frac{1}{2}(\boldsymbol{\infty}_0 - \mathbf{0}_0 + \mathbf{2}_0 + \mathbf{6}_0)\right] z^{x^{-1}}y^{-1} \\
&= 0z^{x^{-1}}y^{-1} = 0.
\end{aligned}$$

Again, the rest of the products can be determined using the group $\langle f^{x^{-13}}, f^{x^{-15}} \rangle$ that fixes the vector $\frac{1}{2}(\mathbf{0}_{18} + \mathbf{1}_{18})$. The products are displayed in Table 6.8. From the same table one observes that $[[\boldsymbol{\infty}_1, v_0], \boldsymbol{\infty}_0] + [[\boldsymbol{\infty}_0, \boldsymbol{\infty}_1], v_0]$ for all basis vectors $v_0 \in \mathfrak{H}_0$, and hence the Jacobi identity holds.

v_0	$[\boldsymbol{\infty}_1, v_0]$	$[[\boldsymbol{\infty}_1, v_0], \boldsymbol{\infty}_0]$	$[\frac{1}{2}(\mathbf{0}_{18} + \mathbf{1}_{18}), v_0]$
$\boldsymbol{\infty}_0$	$\frac{1}{2}(-\mathbf{0}_{18} - \mathbf{1}_{18})$	$\frac{1}{2}(-\boldsymbol{\infty}_1 - \mathbf{1}_1)$	$\frac{1}{2}(\boldsymbol{\infty}_1 + \mathbf{1}_1)$
$\mathbf{0}_0$	$\frac{1}{2}(\mathbf{0}_{18} + \mathbf{1}_{18})$	$\frac{1}{2}(\boldsymbol{\infty}_1 + \mathbf{1}_1)$	$\frac{1}{2}(-\boldsymbol{\infty}_1 - \mathbf{1}_1)$
$\mathbf{1}_0$	$\frac{1}{2}(-\mathbf{4}_{18} + \mathbf{6}_{18})$	$\frac{1}{2}(-\mathbf{5}_1 - \mathbf{6}_1)$	$\frac{1}{2}(\mathbf{5}_1 + \mathbf{6}_1)$
$\mathbf{2}_0$	$\frac{1}{2}(\mathbf{2}_{18} + \mathbf{5}_{18})$	0	0
$\mathbf{3}_0$	$\frac{1}{2}(\mathbf{4}_{18} - \mathbf{6}_{18})$	$\frac{1}{2}(\mathbf{5}_1 + \mathbf{6}_1)$	$\frac{1}{2}(-\mathbf{5}_1 - \mathbf{6}_1)$
$\mathbf{4}_0$	$\frac{1}{2}(-\boldsymbol{\infty}_{18} + \mathbf{3}_{18})$	0	0
$\mathbf{5}_0$	$\frac{1}{2}(\boldsymbol{\infty}_{18} - \mathbf{3}_{18})$	0	0
$\mathbf{6}_0$	$\frac{1}{2}(-\mathbf{2}_{18} - \mathbf{5}_{18})$	0	0

Table 6.8: The values of products $[[\boldsymbol{\infty}_1, v_0], \boldsymbol{\infty}_0]$ and $[\frac{1}{2}(\mathbf{0}_{18} + \mathbf{1}_{18}), v_0]$, where v_0 is a basis vector of $\mathfrak{H}_0$

Case 3

Suppose then that r, s and t are linearly independent. As before, there is an element of G that maps the triple (v_r, w_s, u_t) to $(\boldsymbol{\infty}_0, \boldsymbol{\infty}_1, \boldsymbol{\infty}_2)$ or $(\boldsymbol{\infty}_0, \boldsymbol{\infty}_1, \mathbf{1}_2)$. This can be seen as follows.

There is an element of the group $\langle x, y, z \rangle$ that maps $(\mathfrak{H}_r, \mathfrak{H}_s, \mathfrak{H}_t)$ to $(\mathfrak{H}_0, \mathfrak{H}_1, \mathfrak{H}_2)$. Suppose that the triple (v_r, w_s, u_t) is mapped to the triple (v_0, w_1, u_2). The group E acts on the octonion basis of $\mathfrak{H}_0$ transitively, and hence (v_0, w_1, u_2) can be mapped to $(\boldsymbol{\infty}_0, v_1, w_2)$. As before, we do not need to take sign changes into consideration. The group $\langle f,\ f^{x^2},\ f^{x^5} \rangle$ fixes the octonion basis of $\mathfrak{H}_0$ modulo signs, and acts on the octonion basis of $\mathfrak{H}_1$ transitively, which means that we can assume that $(\boldsymbol{\infty}_0, v_1, w_2)$ is mapped to the triple $(\boldsymbol{\infty}_0, \boldsymbol{\infty}_1, w_2)$. Finally, the group $\langle f^{x^{-2}}, f^x f^{x^6} \rangle$ fixes the octonion bases of $\mathfrak{H}_0$ and $\mathfrak{H}_1$ modulo signs and has two orbits, represented by $\boldsymbol{\infty}_2$ and $\mathbf{1}_2$, on

the basis $\mathfrak{H}_2$.

This means that it is enough to check that

$$[[\boldsymbol{\infty}_0, \boldsymbol{\infty}_1], \boldsymbol{\infty}_2] + [[\boldsymbol{\infty}_2, \boldsymbol{\infty}_0], \boldsymbol{\infty}_1] + [[\boldsymbol{\infty}_1, \boldsymbol{\infty}_2], \boldsymbol{\infty}_0] = 0$$

and

$$[[\boldsymbol{\infty}_0, \boldsymbol{\infty}_1], \mathbf{1}_2] + [[\mathbf{1}_2, \boldsymbol{\infty}_0], \boldsymbol{\infty}_1] + [[\boldsymbol{\infty}_1, \mathbf{1}_2], \boldsymbol{\infty}_0] = 0.$$

We start by proving the first identity. In Section 6.3.3 we noticed that $[\boldsymbol{\infty}_0, \boldsymbol{\infty}_1] = \frac{1}{2}(\mathbf{0} + \mathbf{1})_{18}$. Furthermore, we have

$$\begin{aligned}
\left[\frac{1}{2}(\mathbf{0}_{18} + \mathbf{1}_{18}), \boldsymbol{\infty}_2\right] &= \left[\frac{1}{2}(\mathbf{0}_{18} + \mathbf{1}_{18})x^{-2}y^2, \boldsymbol{\infty}_2 x^{-2}y^2\right] y^{-2}x^2 \\
&= \left[\frac{1}{2}(\mathbf{3}_2 + \mathbf{5}_2), \frac{1}{2}(-\boldsymbol{\infty}_0 - \mathbf{0}_0 + \mathbf{2}_0 - \mathbf{6}_0)\right] y^{-2}x^2 \\
&= \frac{1}{4}(\mathbf{0}_5 + \mathbf{2}_5 - \mathbf{3}_5 + \mathbf{4}_5)y^{-2}x^2 \\
&= \frac{1}{4}(-\mathbf{0}_{11} - \mathbf{3}_{11} - \mathbf{5}_{11} + \mathbf{6}_{11}),
\end{aligned}$$

which means that $[[\boldsymbol{\infty}_0, \boldsymbol{\infty}_1], \boldsymbol{\infty}_2] = \frac{1}{4}(-\mathbf{0}_{11} - \mathbf{3}_{11} - \mathbf{5}_{11} + \mathbf{6}_{11})$.

On the other hand, we have

$$\begin{aligned}
[[\boldsymbol{\infty}_2, \boldsymbol{\infty}_0], \boldsymbol{\infty}_1] &= \left[\frac{1}{2}(-\boldsymbol{\infty}_5 - \mathbf{1}_5 + \mathbf{5}_5 - \mathbf{6}_5), \boldsymbol{\infty}_1\right] \\
&= \left[\frac{1}{2}(-\boldsymbol{\infty}_5 - \mathbf{1}_5 + \mathbf{5}_5 - \mathbf{6}_5)x^{-1}y^{-1}, \boldsymbol{\infty}_1 x^{-1}y^{-1}\right] yx \\
&= \left[\frac{1}{2}(\boldsymbol{\infty}_2 + \mathbf{2}_2 - \mathbf{3}_2 + \mathbf{5}_2), \frac{1}{2}(-\mathbf{2}_0 + \mathbf{4}_0 - \mathbf{5}_0 + \mathbf{6}_0)\right] yx \\
&= \frac{1}{4}(\boldsymbol{\infty}_5 - \mathbf{0}_5 - \mathbf{1}_5 + \mathbf{2}_5 - \mathbf{3}_5 - \mathbf{4}_5 + \mathbf{5}_5 + \mathbf{6}_5)yx \\
&= \frac{1}{4}(-\boldsymbol{\infty}_{11} + \mathbf{0}_{11} - \mathbf{1}_{11} - \mathbf{2}_{11} + \mathbf{3}_{11} + \mathbf{4}_{11} + \mathbf{5}_{11} - \mathbf{6}_{11}).
\end{aligned}$$

Finally, we notice that

$$\begin{aligned}
[\boldsymbol{\infty}_1, \boldsymbol{\infty}_2] &= [\boldsymbol{\infty}_1 x^{-1}y, \boldsymbol{\infty}_2 x^{-1}y]y^{-1}x \\
&= \left[\frac{1}{2}(\mathbf{0}_0 - \mathbf{3}_0 + \mathbf{5}_0 - \mathbf{6}_0), \frac{1}{2}(\mathbf{0}_2 - \mathbf{3}_2 + \mathbf{5}_2 - \mathbf{6}_2)\right] y^{-1}x \\
&= \frac{1}{2}(-\mathbf{0}_5 - \mathbf{3}_5)y^{-1}x = \frac{1}{2}(\mathbf{0}_{19} + \mathbf{1}_{19})
\end{aligned}$$

and

$$\begin{aligned}\left[\frac{1}{2}(\mathbf{0}_{19}+\mathbf{1}_{19}),\boldsymbol{\infty}_0\right] &= \left[\frac{1}{2}(\mathbf{0}_{19}+\mathbf{1}_{19})z^{x^{-14}},\boldsymbol{\infty}_0 z^{x^{-14}}\right]z^{x^{-14}}\\ &= \left[\frac{1}{2}(\mathbf{1}_2-\mathbf{6}_2),\frac{1}{2}(-\boldsymbol{\infty}_0+\mathbf{0}_0+\mathbf{1}_0+\mathbf{3}_0)\right]z^{x^{-14}}\\ &= \frac{1}{4}(\mathbf{0}_5-\mathbf{1}_5-\mathbf{4}_5-\mathbf{6}_5)z^{x^{-14}}\\ &= \frac{1}{4}(\boldsymbol{\infty}_{11}+\mathbf{1}_{11}+\mathbf{2}_{11}-\mathbf{4}_{11}).\end{aligned}$$

Hence $[[\boldsymbol{\infty}_1,\boldsymbol{\infty}_2],\boldsymbol{\infty}_0]=\frac{1}{2}(\boldsymbol{\infty}_{11}+\mathbf{1}_{11}+\mathbf{2}_{11}-\mathbf{4}_{11})$, and furthermore

$$[[\boldsymbol{\infty}_0,\boldsymbol{\infty}_1],\boldsymbol{\infty}_2]+[[\boldsymbol{\infty}_2,\boldsymbol{\infty}_0],\boldsymbol{\infty}_1]+[[\boldsymbol{\infty}_1,\boldsymbol{\infty}_2],\boldsymbol{\infty}_0]=0.$$

Similar calculations show that

$$\begin{aligned}[[\boldsymbol{\infty}_0,\boldsymbol{\infty}_1],\mathbf{1}_2] &= \frac{1}{4}(-\boldsymbol{\infty}_{11}-\mathbf{1}_{11}-\mathbf{2}_{11}+\mathbf{4}_{11}),\\ [[\mathbf{1}_2,\boldsymbol{\infty}_0],\boldsymbol{\infty}_1] &= 0,\\ [[\boldsymbol{\infty}_1,\mathbf{1}_2],\boldsymbol{\infty}_0] &= \frac{1}{4}(\boldsymbol{\infty}_{11}+\mathbf{1}_{11}+\mathbf{2}_{11}-\mathbf{4}_{11}),\end{aligned}$$

and hence $[[\boldsymbol{\infty}_0,\boldsymbol{\infty}_1],\mathbf{1}_2]+[[\mathbf{1}_2,\boldsymbol{\infty}_0],\boldsymbol{\infty}_1]+[[\boldsymbol{\infty}_1,\mathbf{1}_2],\boldsymbol{\infty}_0]=0$.

6.4 Identification of the Lie algebra

We are now ready to prove that the Lie algebra $\mathfrak{L}$ is of type E_8.

Lemma 6.23. *Suppose that $s,r\in S$ are distinct. For any $v_s\in\mathfrak{H}_s\setminus\{0\}$ there exists an element $v_r\in\mathfrak{H}_r$ such that $[v_r,v_s]\neq 0$.*

Proof. Suppose to that for some $v_s\in\mathfrak{H}_s\setminus\{0\}$ it holds that $[v_r,v_s]=0$ for all $v_r\in\mathfrak{H}_r$. We can map the subspaces $\mathfrak{H}_r$ and $\mathfrak{H}_s$ to $\mathfrak{H}_0$ and $\mathfrak{H}_2$ by an element of G, and hence assume that $r=0$ and $s=2$. Write $v_2=\sum_{a\in\mathcal{B}}\alpha_a a_2$, where $\alpha_a\in\mathbb{R}$. By assumption it holds that for all $b\in\mathcal{B}$

$$[b_0,v_2]=\Big[b_0,\sum_{a\in\mathcal{B}}\alpha_a a\Big]=0.$$

Now multiplication table 6.7 gives equations

$$\begin{aligned}
\alpha_\infty - \alpha_0 - \alpha_2 + \alpha_6 &= 0 & \alpha_1 + \alpha_3 + \alpha_4 + \alpha_5 &= 0 \\
-\alpha_1 + \alpha_3 + \alpha_4 - \alpha_5 &= 0 & -\alpha_\infty - \alpha_0 + \alpha_2 + \alpha_6 &= 0 \\
-\alpha_\infty - \alpha_0 - \alpha_2 - \alpha_6 &= 0 & \alpha_1 + \alpha_3 - \alpha_4 - \alpha_5 &= 0 \\
-\alpha_\infty + \alpha_0 - \alpha_2 + \alpha_6 &= 0 & \alpha_1 - \alpha_3 + \alpha_4 - \alpha_5 &= 0.
\end{aligned}$$

The only solution is $\alpha_a = 0$ for all $a \in \mathcal{B}$, which is a contradiction. Hence the product cannot be zero for all $v_r \in \mathfrak{H}_r$. □

Proposition 6.24. *The Lie algebra $\mathfrak{L}$ is simple.*

Proof. Suppose that I is an ideal of $\mathfrak{L}$ and $I \neq \{0\}$. We wish to show that $I = \mathfrak{L}$.

We start by showing that for any $k \in S$, the intersection $\mathfrak{H}_k \cap I$ is non-trivial. Suppose that $k \in S$ and $v \in I \setminus \{0\}$. If $r \in S$ and $v_r \in \mathfrak{H}_r$, then the product $[v, v_r]$, when expressed as a linear combination of basis vectors, does not have terms from the subalgebra $\mathfrak{H}_r$. By multiplying v subsequently by vectors from different subalgebras, it is therefore possible to obtain a vector that is in some subalgebra $\mathfrak{H}_s$. By Lemma 6.23, we may assume that the resulting product is not zero. Call this product v_s. Now we know that $v_s \in I$. Let $t = k \boxplus s$. For any $v_t \in \mathfrak{H}_t$, it holds that $[v_t, v_s] \in \mathfrak{H}_k$. Again by Lemma 6.23, there must be an element of $\mathfrak{H}_t$ for which the product is non-zero. Hence, I contains a non-zero element of $\mathfrak{H}_k$.

Now we know that I contains some non-zero vector v_2 of $\mathfrak{H}_2$. We will show that $\mathfrak{H}_{11} \subseteq I$. By Lemma 6.23, there is $b \in \mathcal{B}$ such that $[b_0, v_2] \neq 0$. From multiplication table 6.7 it can be seen that

$$[b_0, v_2] = \alpha a_5 q,$$

where $q = \frac{1}{2}(\boldsymbol{\infty}_5 + \mathbf{1}_5 - \mathbf{5}_5 + \mathbf{6}_5)$, $a \in \mathcal{B}$ and $\alpha \in \mathbb{R}$. The group E acts transitively on the set $\{a_5 q \mid a \in \mathcal{B}\}$, and hence it can be assumed that $[b_0, v_2] = q$. Now we know that $q \in I$.

Next, we notice that $[\boldsymbol{\infty}_3, q] = q_8$ and $[\mathbf{1}_3, q] = -\mathbf{6}_8 q_8$, where

$$q_8 = \frac{1}{2}(\boldsymbol{\infty}_8 + \mathbf{1}_8 - \mathbf{5}_8 + \mathbf{6}_8).$$

The products of the form $[b_6, q_8]$ and $[b_6, \mathbf{6}_8 q_8]$, where $b \in \mathcal{B}$, generate $\mathfrak{H}_{11}$, and hence $\mathfrak{H}_{11}$ is a subset of I.

Since for any $r \in S$, there is a non-zero vector of the subspace $\mathfrak{H}_{r-9}$ in I, it follows that $\mathfrak{H}_r \subseteq I$ for all $r \in S$. Thus $I = \mathfrak{L}$ and $\mathfrak{L}$ is simple. □

Theorem 6.25. *The Lie algebra $\mathfrak{L}$ is of type E_8.*

Proof. We show that the subspace $\mathfrak{H}_0$ is a Cartan subalgebra of $\mathfrak{L}$. We have $[\mathfrak{H}_0, \mathfrak{H}_0] = 0$, so $\mathfrak{H}_0$ is a nilpotent subalgebra. Suppose then that v is a non-zero element of the normaliser of $\mathfrak{H}_0$. Now $[v, w_0] \in \mathfrak{H}_0$ for all $w_0 \in \mathfrak{H}_0$. Write $v = \sum_{r \in S} v_r$, where $v_r \in \mathfrak{H}_r$. We notice that $[v_r, w_0] \in \mathfrak{H}_0$ for all v_r in the sum.

Suppose that $r \in S \setminus \{0\}$. If $v_r \neq 0$, it follows from Lemma 6.23 that there is an element $u_0 \in \mathfrak{H}_0$ such that $[v_r, u_0] \neq 0$. On the other hand, we know that $[v_r, u_0] \in \mathfrak{H}_s$, where $s = r \boxplus 0 \neq 0$. This means that $[v_r, w_0]$ is not an element of $\mathfrak{H}_0$, which is a contradiction. Therefore, we know that $v_r = 0$ for all $r \in S \setminus \{0\}$. It follows that $v = v_0 \in \mathfrak{H}_0$ and $\mathfrak{H}_0$ is its own normaliser.

Hence $\mathfrak{L}$ is a simple Lie algebra that has a Cartan subalgebra of dimension 8. Since the dimension of $\mathfrak{L}$ is 248, it must be of type E_8. □

Proposition 6.26. *The group $G = \langle x, y, z, d, e \rangle$ acts irreducibly on the Lie algebra $\mathfrak{L}$.*

Proof. Suppose that W is a G-invariant subspace of $\mathfrak{L}$ and $W \neq \{0\}$. Let v be a non-zero element of W. If v is not an element of some subalgebra $\mathfrak{H}_r$, then one can use the elements of the group D to find an element of W that is in one of the subalgebras $\mathfrak{H}_r$.

From Lemma 6.18 it follows that the subgroup E of G acts irreducibly on $\mathfrak{H}_r$. Hence, we know that $\mathfrak{H}_r \subseteq W$. Using the mapping x, one observes that $\mathfrak{H}_s \subseteq W$ for every $s \in S$, and therefore $W = \mathfrak{L}$. □

Theorem 6.27. *The Lie algebra $\mathfrak{L}$ is the compact real form of the complex Lie algebra E_8.*

Proof. We need to prove that the Killing form $(\cdot, \cdot)$ of $\mathfrak{L}$ is negative definite. Since the action of the group $G = \langle x, y, z, d, e \rangle$ is irreducible, and preserves the Killing form,

the form must be either or negative definite. (See [17], Prop. 23.10, p. 270.) positive definite We notice that

$$(\boldsymbol{\infty}_0, \boldsymbol{\infty}_0) = \operatorname{tr}(\operatorname{ad} \boldsymbol{\infty}_0 . \operatorname{ad} \boldsymbol{\infty}_0) = -120,$$

and hence the Killing form is negative definite. □

Theorem 6.28. *The decomposition* $\mathfrak{L} = \mathfrak{H}_0 \oplus \mathfrak{H}_1 \oplus \cdots \oplus \mathfrak{H}_{30}$ *is the multiplicative orthogonal decomposition of* E_8*.*

Proof. We already know that for all $r, s \in S$ it holds that $[\mathfrak{H}_r, \mathfrak{H}_s] \subseteq \mathfrak{H}_t$ for some $t \in S$. Hence, it is enough to prove that the Cartan subalgebras $\mathfrak{H}_r$ are orthogonal to each other.

Suppose that v and w are elements from two distinct Cartan subalgebras $\mathfrak{H}_r$ and $\mathfrak{H}_s$. Now the image of a Cartan subalgebra $\mathfrak{H}_t$ in $\operatorname{ad} v . \operatorname{ad} w$ is in the subalgebra $\mathfrak{H}_k$, where $k = t \boxplus r \boxplus s$. Since $r \neq s$, the subalgebra $\mathfrak{H}_k$ is distinct from $\mathfrak{H}_t$. Hence the image of $\mathfrak{H}_t$ is either in a subalgebra distinct from $\mathfrak{H}_t$, or equal to zero. Now the mapping $\operatorname{ad} v . \operatorname{ad} w$ has trace 0, and the subalgebras are mutually orthogonal. □

Bibliography

[1] M. Aschbacher, *Finite group theory*, second ed., Cambridge Studies in Advanced Mathematics, vol. 10, Cambridge University Press, Cambridge, 2000.

[2] Czesław Bagiński, *On sets of elements of the same order in the alternating group A_n*, Publ. Math. Debrecen **34** (1987), no. 3-4, 313–315.

[3] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).

[4] Roger W. Carter, *Simple groups of Lie type*, John Wiley & Sons, London-New York-Sydney, 1972, Pure and Applied Mathematics, Vol. 28.

[5] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Oxford University Press, Eynsham, 1985.

[6] D. Ž. Djoković, *The product of two involutions in the unitary group of a hermitian form*, Indiana Univ. Math. J. **21** (1971/1972), 449–456.

[7] Erich W. Ellers and Wolfgang Nolte, *Bireflectionality of orthogonal and symplectic groups*, Arch. Math. (Basel) **39** (1982), no. 2, 113–118.

[8] Karin Erdmann and Mark J. Wildon, *Introduction to Lie algebras*, Springer Undergraduate Mathematics Series, Springer-Verlag London Ltd., London, 2006.

[9] A. A. Gal′t, *Strongly real elements in finite simple orthogonal groups*, Sibirsk. Mat. Zh. **51** (2010), no. 2, 241–248.

[10] A. A. Gal′t and E. P. Vdovin, *Strong reality of finite simple groups*, Sibirsk. Mat. Zh. **51** (2010), no. 4, 610–615.

[11] Daniel Gorenstein, *Finite simple groups*, University Series in Mathematics, Plenum Publishing Corp., New York, 1982, An introduction to their classification.

[12] R. Gow, *Products of two involutions in classical groups of characteristic* 2, J. Algebra **71** (1981), no. 2, 583–591.

[13] ———, *Commutators in the symplectic group*, Arch. Math. (Basel) **50** (1988), no. 3, 204–209.

[14] Alexander N. Grishkov, *The automorphisms group of the multiplicative Cartan decomposition of Lie algebra* E_8, Internat. J. Algebra Comput. **11** (2001), no. 6, 737–752.

[15] Larry C. Grove, *Classical groups and geometric algebra*, Graduate Studies in Mathematics, vol. 39, American Mathematical Society, Providence, RI, 2002.

[16] Nathan Jacobson, *Lie algebras*, Interscience Tracts in Pure and Applied Mathematics, No. 10, Interscience Publishers (a division of John Wiley & Sons), New York-London, 1962.

[17] Gordon James and Martin Liebeck, *Representations and characters of groups*, second ed., Cambridge University Press, New York, 2001.

[18] Frieder Knüppel and Gerd Thomsen, *Involutions and commutators in orthogonal groups*, J. Austral. Math. Soc. Ser. A **65** (1998), no. 1, 1–36.

[19] S. G. Kolesnikov and Ja. N. Nuzhin, *On strong reality of finite simple groups*, Acta Appl. Math. **85** (2005), no. 1-3, 195–203.

[20] Alexei I. Kostrikin and Phạm Hũ'u Tiệp, *Orthogonal decompositions and integral lattices*, de Gruyter Expositions in Mathematics, vol. 15, Walter de Gruyter & Co., Berlin, 1994.

[21] V. D. Mazurov and E. I. Khukhro (eds.), *The Kourovka notebook*, augmented ed., Russian Academy of Sciences Siberian Division Institute of Mathematics, Novosibirsk, 1999, Unsolved problems in group theory.

[22] Johanna Rämö, *Strongly real elements of orthogonal groups in even characteristic*, J. Group Theory, DOI: 10.1515/JGT.2010.036.

[23] ———, *A symmetric construction of the compact real form of the Lie algebra E_8*, submitted.

[24] Hans Samelson, *Notes on Lie algebras*, Van Nostrand Reinhold Mathematical Studies, No. 23, Van Nostrand Reinhold Co., New York, 1969.

[25] Donald E. Taylor, *The geometry of the classical groups*, Sigma Series in Pure Mathematics, vol. 9, Heldermann Verlag, Berlin, 1992.

[26] J. G. Thompson, *A conjugacy theorem for E_8*, J. Algebra **38** (1976), no. 2, 525–530.

[27] Pham Huu Tiep and A. E. Zalesski, *Real conjugacy classes in algebraic groups and finite groups of Lie type*, J. Group Theory **8** (2005), no. 3.

[28] Robert A. Wilson, *On the compact real form of the Lie algebras of type E_6 and F_4*, preprint.

[29] ———, *The finite simple groups*, Graduate Texts in Mathematics, vol. 251, Springer-Verlag London Ltd., London, 2009.

[30] ———, *On the compact real form of the Lie algebra G_2*, Math. Proc. Cambridge Philos. Soc. **148** (2010).

[31] Maria J. Wonenburger, *Transformations which are products of two involutions*, J. Math. Mech. **16** (1966), 327–338.

Appendices

Appendix A

The computer code

The following code was used in Section 6.3.3 to verify that the mappings e and z preserve the product $[\cdot,\cdot]$. The code is written in MAGMA language [3]. It is also available from `http://www.maths.qmul.ac.uk/~jmr/`.

```
/**********Vector*space**********/

/* First we construct a basis of a 248-dimensional vector space L. The
vector space is a direct sum of 31 subspaces that all have dimension
eight. The basis elements of L are written as pairs, where the first
component of the pair indicates the index of the 8-dimensional
subspace, and the second component is a basis vector of that subspace.
*/

/* Q is the field of rational numbers. */
Q:=RationalField();

/* Construction of a basis of L. The subspaces of L are indexed by
numbers 1,...,30,31 and they correspond to the subspaces H_k. Notice
that the index 31 correspond to the subspace H_0. */
/* V is an 8-dimensional vector space. */
V:=VectorSpace(Q,8);
L:=[];
v:=Zero(V);
for k in [1..31] do
  subspace:=[];
  for j in [1..8] do
    v[j]:=1;
```

```
    subspace[j]:=<k,v>;
    v:=Zero(V);
  end for;
  L[k]:=subspace;
end for;
/* The zero vector has index -1. */
ZeroVector:=<-1,Zero(V)>;

/* Function IsEqual returns the boolean value true if the given vectors
are equal. */
IsEqual:=function(v,w)
  equal:=true;
  if (v[1] eq -1 and w[1] eq -1) then
    return true;
  else
    if not v[1] eq w[1] then
      equal:=false;
    end if;
    for i in [1..8] do
      if not v[2][i] eq w[2][i] then
        equal:=false;
break;
      end if;
    end for;
  end if;
  return equal;
end function;

/**********Group*elements**********/

/* The mappings x, y, z and e are written as pairs that consist of a
sequence of 8-dimensional row matrices and a permutation. The
8x8-matrices are defined by the action of the mapping on the subspaces
H_k, and the permutation describes how the mapping permutes the
subspaces. The index 31 corresponds to the subspace H_0.*/

/* xBlock is the 8x8-matrix associated with x. */
xBlock:=ScalarMatrix(Q,8,1);

/* xBlocks is the list of 8x8-matrices associated with x. */
xBlocks:=[GL(8,Q)|];
for i in [1..31] do
  xBlocks[i]:=xBlock;
```

```
end for;

/* xPerm is the 31-cycle associated with x. */
S31:=Sym(31);
xPerm:=S31!(1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,
23,24,25,26,27,28,29,30,31);

x:=<xBlocks, xPerm>;

/* yBlock is the 8x8-matrix associated with y. */
yBlock:=1/2*Matrix(Q,8,8,
[0, 1, 0, 0, -1, 0, 1, -1,
0, -1, 0, 0, -1, 0, -1, -1,
0, -1, 0, 0, -1, 0, 1, 1,
-1, 0, -1, -1, 0, -1, 0, 0,
0, 1, 0, 0, -1, 0, -1, 1,
1, 0, -1, 1, 0, -1, 0, 0,
-1, 0, -1, 1, 0, 1, 0, 0,
1, 0, -1, -1, 0, 1, 0, 0]);

/* yBlocks is the list of 8x8-matrices associated with y. */
yBlocks:=[GL(8,Q)|];
for i in [1..31] do
  yBlocks[i]:=yBlock;
end for;

/* yPerm is the permutation associated with y. */
yPerm:=S31!(1,2,4,8,16)(5,10,20,9,18)(13,26,21,11,22)(14,28,25,19,7)
(15,30,29,27,23)(24,17,3,6,12);

y:=<yBlocks, yPerm>;

/* For the mapping z, we need six different matrices corresponding to
the action of z on the subspaces H_0, H_1, H_13, H_15, H_18 and H_24.
*/

//H_0
zBlock0:=1/2*Matrix(Q,8,8,
[1, 0, 0, 0, -1, 1, 0, -1,
0, 1, -1, -1, 0, 0, 1, 0,
0, -1, 1, -1, 0, 0, 1, 0,
0, -1, -1, -1, 0, 0, -1, 0,
-1, 0, 0, 0, 1, 1, 0, -1,
```

```
1, 0, 0, 0, 1, -1, 0, -1,
0, 1, 1, -1, 0, 0, -1, 0,
-1, 0, 0, 0, -1, -1, 0, -1]);

//H_1
zBlock1:=Matrix(Q,8,8,
[-1, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 1, 0, 0,
0, 0, 0, 0, 0, 0, 0, -1,
0, 0, 0, -1, 0, 0, 0, 0,
0, 0, 0, 0, -1, 0, 0, 0,
0, 1, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, -1, 0,
0, 0, -1, 0, 0, 0, 0, 0]);

/*H_5
zBlock5:=1/2*Matrix(Q,8,8,
[
0, 0, 0, 1, 0, -1, 1, 1,
1, 1, -1, 0, 1, 0, 0, 0,
-1, 1, -1, 0, -1, 0, 0, 0,
-1, 1, 1, 0, 1, 0, 0, 0,
0, 0, 0, -1, 0, -1, -1, 1,
0, 0, 0, -1, 0, -1, 1, -1,
1, 1, 1, 0, -1, 0, 0, 0,
0, 0, 0, 1, 0, -1, -1, -1]);
*/

//H_13
zBlock13:=Matrix(Q,8,8,
[1, 0, 0, 0, 0, 0, 0, 0,
0, -1, 0, 0, 0, 0, 0, 0,
0, 0, -1, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, -1,
0, 0, 0, 0, 1, 0, 0, 0,
0, 0, 0, 0, 0, 0, 1, 0,
0, 0, 0, 0, 0, 1, 0, 0,
0, 0, 0, -1, 0, 0, 0, 0]);

//H_14
zBlock14:=1/2*Matrix(Q,8,8,
[-1, 1, 1, 0, 1, 0, 0, 0,
1, -1, 1, 0, 1, 0, 0, 0,
```

```
1, 1, -1, 0, 1, 0, 0, 0,
0, 0, 0, 1, 0, -1, -1, -1,
1, 1, 1, 0, -1, 0, 0, 0,
0, 0, 0, -1, 0, 1, -1, -1,
0, 0, 0, -1, 0, -1, 1, -1,
0, 0, 0, -1, 0, -1, -1, 1]);

//H_15
zBlock15:=1/2*Matrix(Q,8,8,
[-1, 0, 1, 0, 0, 0, -1, -1,
0, -1, 0, -1, 1, -1, 0, 0,
1, 0, -1, 0, 0, 0, -1, -1,
0, -1, 0, -1, -1, 1, 0, 0,
0, 1, 0, -1, -1, -1, 0, 0,
0, -1, 0, 1, -1, -1, 0, 0,
-1, 0, -1, 0, 0, 0, -1, 1,
-1, 0, -1, 0, 0, 0, 1, -1]);

//H_18
zBlock18:=1/2*Matrix(Q,8,8,
[0, 0, -1, 1, -1, 0, 0, -1,
0, 0, -1, 1, 1, 0, 0, 1,
-1, -1, 0, 0, 0, -1, 1, 0,
1, 1, 0, 0, 0, -1, 1, 0,
-1, 1, 0, 0, 0, -1, -1, 0,
0, 0, -1, -1, -1, 0, 0, 1,
0, 0, 1, 1, -1, 0, 0, 1,
-1, 1, 0, 0, 0, 1, 1, 0]);

//H_24
zBlock24:=1/2*Matrix(Q,8,8,
[1, -1, 0, 1, 0, 0, 0, -1,
-1, -1, 0, 1, 0, 0, 0, 1,
0, 0, 1, 0, -1, -1, 1, 0,
1, 1, 0, 1, 0, 0, 0, 1,
0, 0, -1, 0, -1, -1, -1, 0,
0, 0, -1, 0, -1, 1, 1, 0,
0, 0, 1, 0, -1, 1, -1, 0,
-1, 1, 0, 1, 0, 0, 0, -1]);

/* zBlocks is the list of 8x8-matrices associated with z. */
zBlocks:=[GL(8,Q)|];
```

```
zBlocks[1]:=zBlock1;
zBlocks[2]:=yBlock^-1*zBlock1*yBlock^-1;
zBlocks[3]:=yBlock^-2*zBlock24*yBlock^-2;
zBlocks[4]:=yBlock^-2*zBlock1*yBlock^-2;
zBlocks[5]:=yBlock^-1*zBlock18*yBlock^-1;
zBlocks[6]:=yBlock^2*zBlock24*yBlock^2;
zBlocks[7]:=yBlock*zBlock14*yBlock;
zBlocks[8]:=yBlock^2*zBlock1*yBlock^2;
zBlocks[9]:=yBlock*zBlock18*yBlock;
zBlocks[10]:=yBlock^-2*zBlock18*yBlock^-2;
zBlocks[11]:=yBlock^2*zBlock13*yBlock^2;
zBlocks[12]:=yBlock*zBlock24*yBlock;
zBlocks[13]:=zBlock13;
zBlocks[14]:=zBlock14;
zBlocks[15]:=zBlock15;
zBlocks[16]:=yBlock*zBlock1*yBlock;
zBlocks[17]:=yBlock^-1*zBlock24*yBlock^-1;
zBlocks[18]:=zBlock18;
zBlocks[19]:=yBlock^2*zBlock14*yBlock^2;
zBlocks[20]:=yBlock^2*zBlock18*yBlock^2;
zBlocks[21]:=yBlock^-2*zBlock13*yBlock^-2;
zBlocks[22]:=yBlock*zBlock13*yBlock;
zBlocks[23]:=yBlock*zBlock15*yBlock;
zBlocks[24]:=zBlock24;
zBlocks[25]:=yBlock^-2*zBlock14*yBlock^-2;
zBlocks[26]:=yBlock^-1*zBlock13*yBlock^-1;
zBlocks[27]:=yBlock^2*zBlock15*yBlock^2;
zBlocks[28]:=yBlock^-1*zBlock14*yBlock^-1;
zBlocks[29]:=yBlock^-2*zBlock15*yBlock^-2;
zBlocks[30]:=yBlock^-1*zBlock15*yBlock^-1;
zBlocks[31]:=zBlock0;

/* zPerm is the permutation associated with z. */
zPerm:=S31!(2,16)(3,6)(4,8)(5,9)(7,28)(10,20)(11,21)(12,17)(19,25)
(22,26)(23,30)(27,29);

z:=<zBlocks, zPerm>;

/* For the mapping e we need six different matrices corresponding to
the action of e on the subspaces H_0, H_1, H_13, H_15, H_18 and H_24.
*/

//H_0
```

```
eBlock0:=Matrix(Q,8,8,
[0, 0, 0, 0, 0, 0, 1, 0,
0, 0, 0, 0, 0, 1, 0, 0,
0, 0, 0, 0, 0, 0, 0, -1,
0, 0, 0, 0, 1, 0, 0, 0,
0, 0, 0, -1, 0, 0, 0, 0,
0, -1, 0, 0, 0, 0, 0, 0,
-1, 0, 0, 0, 0, 0, 0, 0,
0, 0, 1, 0, 0, 0, 0, 0]);

//H_1
eBlock1:=Matrix(Q,8,8,
[0, 0, 0, 0, 0, 0, -1, 0,
0, 0, 0, 0, 0, -1, 0, 0,
0, 0, 0, 0, 0, 0, 0, 1,
0, 0, 0, 0, 1, 0, 0, 0,
0, 0, 0, 1, 0, 0, 0, 0,
0, -1, 0, 0, 0, 0, 0, 0,
-1, 0, 0, 0, 0, 0, 0, 0,
0, 0, 1, 0, 0, 0, 0, 0]);

//H_13
eBlock13:=Matrix(Q,8,8,
[0, 0, 1, 0, 0, 0, 0, 0,
0, 0, 0, 0, 1, 0, 0, 0,
-1, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 1, 0, 0,
0, -1, 0, 0, 0, 0, 0, 0,
0, 0, 0, -1, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, -1,
0, 0, 0, 0, 0, 0, 1, 0]);

//H_14
eBlock14:=Matrix(Q,8,8,
[1, 0, 0, 0, 0, 0, 0, 0,
0, 1, 0, 0, 0, 0, 0, 0,
0, 0, 1, 0, 0, 0, 0, 0,
0, 0, 0, -1, 0, 0, 0, 0,
0, 0, 0, 0, 1, 0, 0, 0,
0, 0, 0, 0, 0, -1, 0, 0,
0, 0, 0, 0, 0, 0, -1, 0,
0, 0, 0, 0, 0, 0, 0, -1]);
```

```
//H_15
eBlock15:=Matrix(Q,8,8,
[0, 0, 0, 0, 0, 0, 0, -1,
0, 0, 0, 1, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, -1, 0,
0, 1, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 1, 0, 0,
0, 0, 0, 0, 1, 0, 0, 0,
0, 0, -1, 0, 0, 0, 0, 0,
-1, 0, 0, 0, 0, 0, 0, 0]);

//H_18
eBlock18:=Matrix(Q,8,8,
[0, 0, 0, 0, 0, 0, 0, 1,
0, 0, 0, 1, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 1, 0,
0, -1, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 1, 0, 0,
0, 0, 0, 0, -1, 0, 0, 0,
0, 0, -1, 0, 0, 0, 0, 0,
-1, 0, 0, 0, 0, 0, 0, 0]);

//H_24
eBlock24:=Matrix(Q,8,8,
[0, 1, 0, 0, 0, 0, 0, 0,
-1, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, -1, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, -1,
0, 0, 1, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 1, 0,
0, 0, 0, 0, 0, -1, 0, 0,
0, 0, 0, 1, 0, 0, 0, 0]);

/* eBlocks is the list of 8x8-matrices associated with e. */
eBlocks:=[GL(8,Q)|];

eBlocks[1]:=eBlock1;
eBlocks[2]:=yBlock^-1*eBlock1*yBlock;
eBlocks[3]:=yBlock^-2*eBlock24*yBlock^2;
eBlocks[4]:=yBlock^-2*eBlock1*yBlock^2;
eBlocks[5]:=yBlock^-1*eBlock18*yBlock;
eBlocks[6]:=yBlock^2*eBlock24*yBlock^-2;
eBlocks[7]:=yBlock*eBlock14*yBlock^-1;
```

```
eBlocks[8]:=yBlock^2*eBlock1*yBlock^-2;
eBlocks[9]:=yBlock*eBlock18*yBlock^-1;
eBlocks[10]:=yBlock^-2*eBlock18*yBlock^2;
eBlocks[11]:=yBlock^2*eBlock13*yBlock^-2;
eBlocks[12]:=yBlock*eBlock24*yBlock^-1;
eBlocks[13]:=eBlock13;
eBlocks[14]:=eBlock14;
eBlocks[15]:=eBlock15;
eBlocks[16]:=yBlock*eBlock1*yBlock^-1;
eBlocks[17]:=yBlock^-1*eBlock24*yBlock;
eBlocks[18]:=eBlock18;
eBlocks[19]:=yBlock^2*eBlock14*yBlock^-2;
eBlocks[20]:=yBlock^2*eBlock18*yBlock^-2;
eBlocks[21]:=yBlock^-2*eBlock13*yBlock^2;
eBlocks[22]:=yBlock*eBlock13*yBlock^-1;
eBlocks[23]:=yBlock*eBlock15*yBlock^-1;
eBlocks[24]:=eBlock24;
eBlocks[25]:=yBlock^-2*eBlock14*yBlock^2;
eBlocks[26]:=yBlock^-1*eBlock13*yBlock;
eBlocks[27]:=yBlock^2*eBlock15*yBlock^-2;
eBlocks[28]:=yBlock^-1*eBlock14*yBlock;
eBlocks[29]:=yBlock^-2*eBlock15*yBlock^2;
eBlocks[30]:=yBlock^-1*eBlock15*yBlock;
eBlocks[31]:=eBlock0;

/* ePerm is the permutation associated with e. */
ePerm:=Id(S31);

e:=<eBlocks, ePerm>;

/**********Matrix*operations**********/

/* The function Mult returns the product of block matrices a and b. */
Mult:=function(a,b)
  aBlocks:=a[1];
  aPerm:=a[2];
  bBlocks:=b[1];
  bPerm:=b[2];
  abPerm:=aPerm*bPerm;
    abBlocks:=[GL(8,Q)|];
  for i in [1..31] do
    abBlocks[i]:=aBlocks[i]*bBlocks[Image(aPerm,i)];
  end for;
```

```
  ab:=<abBlocks,abPerm>;
  return ab;
end function;

/* Construction of the identity matrix. */
IdBlocks:=[];
IdPerm:=Identity(S31);
for i in [1..31] do
  IdBlocks[i]:=ScalarMatrix(Q,8,1);
end for;
IdMatrix:=<IdBlocks, IdPerm>;

/* The function Inverse returns the inverse of a block matrix. */
Inverse:=function(a)
  aBlocks:=a[1];
  aPerm:=a[2];
  aIPerm:=aPerm^-1;
  aIBlocks:=[GL(8,Q)|];
  for i in [1..31] do
    aIBlocks[i]:=aBlocks[Image(aIPerm,i)]^-1;
  end for;
  aI:=<aIBlocks, aIPerm>;
  return aI;
end function;

/* Power(a,n) returns the nth power of a block matrix a. */
Power:=function(a,n)
  power:=IdMatrix;
  if n ge 0 then
    for i in [1..n] do
      power:=Mult(a,power);
    end for;
  else
    b:=Inverse(a);
    m:=-n;
    for i in [1..m] do
      power:=Mult(b,power);
    end for;
  end if;
  return power;
end function;

/* The function IsIdMatrix returns the boolean value true if the given
```

```
matrix is the identity matrix. */
IsIdMatrix:=function(a)
  aBlocks:=a[1];
  aPerm:=a[2];
  IsIdPerm:=true;
  if IsId(aPerm) then
    IsIdPerm:=true;
  else
    IsIdPerm:=false;
  end if;
  IsIdBlock:=true;
  for i in [1..31] do
    if not IsOne(aBlocks[i]) then
      IsIdBlock:=false;
      break;
    end if;
  end for;
  if IsIdBlock and IsIdPerm then
    return true;
  else
    return false;
  end if;
end function;

/* The function IsEqualMatrix returns the boolean value true if the
given matrices equal. */
IsEqualMatrix:=function(a,b)
  aBlocks:=a[1];
  aPerm:=a[2];
  bBlocks:=b[1];
  bPerm:=b[2];
  if not aPerm eq bPerm then
    return false;
  end if;

  EqualBlocks:=true;
  for i in [1..31] do
    if not aBlocks[i] eq bBlocks[i] then
      EqualBlocks:=false;
      break;
    end if;
  end for;
  return EqualBlocks;
```

```
end function;

/* The function Value returns the value of the given element of L in
the given matrix. */
Value:=function(v,a)
  if v[1] eq -1 then // v is the zero vector
    return ZeroVector;
  else
    imageVector:=v[2]*a[1][v[1]];
    imageIndex:=Image(a[2],v[1]);
    return <imageIndex, imageVector>;
  end if;
end function;

/* Conjugate(a,b) returns the matrix b^-1*a*b. */
Conjugate:=function(a,b)
  return Mult(Inverse(b),Mult(a,b));
end function;

/* Commutator(a,b) returns the matrix a^-1*b^-1*a*b. */
Commutator:=function(a,b)
  return Mult(Conjugate(Inverse(b),a),b);
end function;

/**********Lie*product**********/

/* The following mappings are used in determining the values of the
Lie product on the block {H_0,H_2,H_5}. */

/* s02 interchanges subspaces H_0 and H_2, fixing H_5 */
s02:=Conjugate(z,Power(x,-27));
/* s25 interchanges subspaces H_2 and H_5, fixing H_0 */
s25:=Conjugate(z,Inverse(x));

/* t20 maps (H_2,H_0) to (H_0,H_2) */
t20:=s02;
/* t05 maps (H_0,H_5) to (H_0,H_2) */
t05:=s25;
/* t50 maps (H_5,H_0) to (H_0,H_2) */
t50:=Mult(s25,s02);
/* t25 maps (H_2,H_5) to (H_0,H_2)*/
t25:=Mult(s02,s25);
/* t52 maps (H_5,H_2) to (H_0,H_2) */
```

```
t52:=Mult(s02,t50);

/* The sequence g consists of mappings that map the subspaces H_k to
the subspace H_2 fixing H_0. */

g:=[];

g[1]:=y;
g[2]:=IdMatrix;
g[4]:=Power(y,4);
g[8]:=Power(y,3);
g[16]:=Power(y,2);

g[5]:=t05;
g[10]:=Mult(Power(y,4),g[5]);
g[20]:=Mult(Power(y,3),g[5]);
g[9]:=Mult(Power(y,2),g[5]);
g[18]:=Mult(y,g[5]);

g[3]:=Mult(Power(x,2),t25);
g[6]:=Mult(Power(y,4),g[3]);
g[12]:=Mult(Power(y,3),g[3]);
g[24]:=Mult(Power(y,2),g[3]);
g[17]:=Mult(y,g[3]);

g[26]:=Mult(Power(x,5),t50);
g[21]:=Mult(Power(y,4),g[26]);
g[11]:=Mult(Power(y,3),g[26]);
g[22]:=Mult(Power(y,2),g[26]);
g[13]:=Mult(y,g[26]);

g[28]:=Mult(Power(x,5),t52);
g[25]:=Mult(Power(y,4),g[28]);
g[19]:=Mult(Power(y,3),g[28]);
g[7]:=Mult(Power(y,2),g[28]);
g[14]:=Mult(y,g[28]);

g[29]:=Mult(Power(x,2),t20);
g[27]:=Mult(Power(y,4),g[29]);
g[23]:=Mult(Power(y,3),g[29]);
g[15]:=Mult(Power(y,2),g[29]);
g[30]:=Mult(y,g[29]);
```

```
/* ProductTable02 contains the muliplication table of the basis vectors
of subspaces H_0 and H_2. (See multiplication table 7) The products,
which are in H_5, are expressed as elements of the 8-dimensional vector
space V. */

ProductTable02:=[];

ProductTable02[1]:=[];
ProductTable02[1][1]:=V![1/2, 0, 1/2, 0, 0, 0, -1/2, 1/2];
ProductTable02[1][2]:=-1*ProductTable02[1][1];
ProductTable02[1][3]:=Zero(V);
ProductTable02[1][4]:=-1*ProductTable02[1][1];
ProductTable02[1][5]:=Zero(V);
ProductTable02[1][6]:=Zero(V);
ProductTable02[1][7]:=Zero(V);
ProductTable02[1][8]:=ProductTable02[1][1];

ProductTable02[2]:=[];
ProductTable02[2][1]:=Zero(V);
ProductTable02[2][2]:=Zero(V);
ProductTable02[2][3]:=V![0, -1/2, 0, -1/2, -1/2, 1/2, 0, 0];
ProductTable02[2][4]:=Zero(V);
ProductTable02[2][5]:=-1*ProductTable02[2][3];
ProductTable02[2][6]:=-1*ProductTable02[2][3];
ProductTable02[2][7]:=ProductTable02[2][3];
ProductTable02[2][8]:=Zero(V);

ProductTable02[3]:=[];
ProductTable02[3][1]:=V![1/2, 0, -1/2, 0, 0, 0, -1/2, -1/2];
ProductTable02[3][2]:=ProductTable02[3][1];
ProductTable02[3][3]:=Zero(V);
ProductTable02[3][4]:=ProductTable02[3][1];
ProductTable02[3][5]:=Zero(V);
ProductTable02[3][6]:=Zero(V);
ProductTable02[3][7]:=Zero(V);
ProductTable02[3][8]:=ProductTable02[3][1];

ProductTable02[4]:=[];
ProductTable02[4][1]:=[1/2, 0, -1/2, 0, 0, 0, 1/2, 1/2];
ProductTable02[4][2]:=-1*ProductTable02[4][1];
ProductTable02[4][3]:=Zero(V);
ProductTable02[4][4]:=ProductTable02[4][1];
ProductTable02[4][5]:=Zero(V);
```

```
ProductTable02[4][6]:=Zero(V);
ProductTable02[4][7]:=Zero(V);
ProductTable02[4][8]:=-1*ProductTable02[4][1];

ProductTable02[5]:=[];
ProductTable02[5][1]:=Zero(V);
ProductTable02[5][2]:=Zero(V);
ProductTable02[5][3]:=V![0, -1/2, 0, 1/2, 1/2, 1/2, 0, 0];
ProductTable02[5][4]:=Zero(V);
ProductTable02[5][5]:=ProductTable02[5][3];
ProductTable02[5][6]:=ProductTable02[5][3];
ProductTable02[5][7]:=ProductTable02[5][3];
ProductTable02[5][8]:=Zero(V);

ProductTable02[6]:=[];
ProductTable02[6][1]:=V![-1/2, 0, -1/2, 0, 0, 0, -1/2, 1/2];
ProductTable02[6][2]:=ProductTable02[6][1];
ProductTable02[6][3]:=Zero(V);
ProductTable02[6][4]:=-1*ProductTable02[6][1];
ProductTable02[6][5]:=Zero(V);
ProductTable02[6][6]:=Zero(V);
ProductTable02[6][7]:=Zero(V);
ProductTable02[6][8]:=-1*ProductTable02[6][1];

ProductTable02[7]:=[];
ProductTable02[7][1]:=Zero(V);
ProductTable02[7][2]:=Zero(V);
ProductTable02[7][3]:=V![0, 1/2, 0, -1/2, 1/2, 1/2, 0, 0];
ProductTable02[7][4]:=Zero(V);
ProductTable02[7][5]:=ProductTable02[7][3];
ProductTable02[7][6]:=-1*ProductTable02[7][3];
ProductTable02[7][7]:=-1*ProductTable02[7][3];
ProductTable02[7][8]:=Zero(V);

ProductTable02[8]:=[];
ProductTable02[8][1]:=Zero(V);
ProductTable02[8][2]:=Zero(V);
ProductTable02[8][3]:=V![0, -1/2, 0, -1/2, 1/2, -1/2, 0, 0];
ProductTable02[8][4]:=Zero(V);
ProductTable02[8][5]:=-1*ProductTable02[8][3];
ProductTable02[8][6]:=ProductTable02[8][3];
ProductTable02[8][7]:=-1*ProductTable02[8][3];
ProductTable02[8][8]:=Zero(V);
```

```
/* The function Pruduct0 returns the Lie product of v and w, where v is
an element of H_0. The sequence g consists of mappings that map the
subspaces H_k to H_2. The entry g[k] maps the subspace H_k to H_2 and
fixes H_0. */

Product0:=function(v,w)
  wIndex:=w[1];
  if wIndex eq 31 then
    return ZeroVector;
  else
    prodVector:=Zero(V);
    vg:=Value(v,g[wIndex]);
    wg:=Value(w,g[wIndex]);
    for i in [1..8] do
      for j in [1..8] do
        prodVector:=prodVector+vg[2][i]*wg[2][j]*ProductTable02[i][j];
      end for;
    end for;
    product:=<5,prodVector>;
    product:=Value(product,Inverse(g[wIndex]));
    return product;
  end if;
end function;

/* Function Product gives the Lie product of two vectors. */
Product:=function(v,w)
  if v[1] eq w[1] then
    return ZeroVector;
  else
    h:=Power(x,31-v[1]);
    vh:=Value(v,h);
    wh:=Value(w,h);
    product:=Product0(vh,wh);
    product:=Value(product,Inverse(h));
    return product;
  end if;
end function;

/**********Proof**********/

/* The following procedures are used in Section 3.3 to prove that the
mappings e and z preserve the product. */
```

```
/* The procedure eInvariant prints the boolean value true if the
mapping e preserves the product. */
eInvariant:=procedure()
  for i in {1,13,14,15,18,24} do
    for j in [1..31] do
      if not j eq i then
        for k in {1..8} do
          for m in {1..8} do
            vector1:=Value(Product(L[j][k],L[i][m]), e);
            vector2:=Product(Value(L[j][k],e), Value(L[i][m],e));
            if not IsEqual(vector1, vector2) then
              print "Proof does not work!;
              return;
            end if;
            vector1:=Value(Product(L[i][m],L[j][k]), e);
            vector2:=Product(Value(L[i][m],e), Value(L[j][k],e));
            if not IsEqual(vector1, vector2) then
              print "Proof does not work!";
              return;
            end if;
          end for;
        end for;
      end if;
    end for;
  end for;
  print true;
end procedure;

/* The procedure zInvariant prints the boolean value true if the
mapping z preserves the product. */
zInvariant:=procedure()
  for i in {1,13,14,15,18,24} do
    for j in {2,3,4,5,7,10,11,12,19,22,23,27,31} do
      product1:=Value(Product(L[i][1], L[j][1]),z);
      product2:=Product(Value(L[i][1], z), Value(L[j][1],z));
      if not IsEqual(product1, product2) then
        print "Proof does not work!";
        return;
      end if;
      product1:=Value(Product(L[j][1], L[i][1]),z);
      product2:=Product(Value(L[j][1], z), Value(L[i][1],z));
      if not IsEqual(product1, product2) then
```

```
        print "Proof does not work!";
        return;
      end if;
    end for;
  end for;
  print true;
end procedure;
```