UNIVERSITÀ DEGLI STUDI DI TRENTO
Facoltà di Scienze Matematiche, Fisiche e Naturali

PhD Thesis

Classifying semisimple orbits of θ-groups

Advisor:
Dr. Willem A. de Graaf

PhD Student:
Dott. Francesco Oriente

April, 23 - 2012

Contents

Introduction

The topic of this thesis is the problem of classifying semisimple orbits of a particular class of reductive algebraic groups, called θ-groups. They were introduced by Vinberg in 1976, and are defined in the following way. Let G be a reductive connected algebraic group, and $\mathfrak{g}$ its Lie algebra. For any automorphism θ of $\mathfrak{g}$ of finite order m, one can consider the $\mathbb{Z}/m\mathbb{Z}$-grading of $\mathfrak{g}$,

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \mathfrak{g}_1 \oplus \ldots \oplus \mathfrak{g}_{m-1}$$

where $\mathfrak{g}_i$ is the eigenspace of θ with eigenvalue ω^i, being ω a primitive m-th root of unity. Let G_0 be the connected subgroup of G with Lie algebra $\mathfrak{g}_0$. The group G_0 together with its action on $\mathfrak{g}_1$, is called a θ-group. An important fact is that in this situation an orbit is closed if and only if it consists of elements of $\mathfrak{g}_1$ that are semisimple (as elements of $\mathfrak{g}$).

Vinberg showed that all Cartan subspaces of $\mathfrak{g}_1$ (i.e., maximal subspaces consisting of commuting semisimple elements) are conjugate under G_0. This implies that every closed, or what is the same, semisimple orbit has a point in a fixed Cartan subspace $\mathfrak{c} \subset \mathfrak{g}_1$. Furthermore, two elements of $\mathfrak{c}$ lie in the same G_0-orbit if and only if they are conjugate under the *little Weyl group* $W_0 = N_{G_0}(\mathfrak{c})/Z_{G_0}(\mathfrak{c})$. We can remark that all the Cartan subspaces have the same dimension: it is called the *rank* of $(G_0, \mathfrak{g}_1)$.

Vinberg also discovered that W_0 is a complex refection group and moreover, by the Chevalley-Shephard-Todd theorem, the ring of invariants $\mathbb{C}[\mathfrak{c}]^{W_0}$ is freely generated by l fundamental invariants. Furthermore different semisimple orbits are separated by the polynomial invariants of W_0 on $\mathfrak{c}$. This means that two elements of $\mathfrak{c}$ lie in different W_0-orbits (and hence in different G_0-orbits) if and only if there is at least one fundamental invariant taking different values on these elements. For this reason we consider the classification of the semisimple orbits to be complete if we have a Cartan subspace, generators of the corresponding little Weyl group, and its fundamantal invariants.

For θ-groups arising from the classical Lie algebras A_n, B_n, C_n, D_n Vinberg got the little Weyl groups using theoretical considerations. For other ones arising from simple Lie algebras of exceptional type also it is possible trying to solve the problem by means of 'ad-hoc' arguments, and this has been done in several cases (leading sometimes to wrong results as I discovered); I refer to [24], [6], [18] for examples of this. In my approach, instead, I have adopted a more systematic method using computational techniques. This consists of the following steps:

- find a Cartan subspace $\mathfrak{c}$ of $\mathfrak{g}_1$,
- find generators for the little Weyl group $W_0 = N_{G_0}(\mathfrak{c})/Z_{G_0}(\mathfrak{c})$.

Being already available algorithms to compute the fundamental invariants of a complex reflection groups given its generators (see [5], [21]), my work was reduced, essentially, to the above points.

In order to represent Lie algebras I have considered a multiplication table relative to a Chevalley basis, with respect to which all structure constants are integers. Algorithms for getting such a representation for a given Lie algebra are available too (see [7]). The conjugacy classes (in $\mathrm{Aut}(\mathfrak{g})$) of the finite order automorphisms of $\mathfrak{g}$ have been classified by Kac in terms of so-called *Kac diagrams*. From the Kac diagram of an automorphism θ of order m working over the field $\mathbb{Q}(\omega)$, being ω a primitive m-th root of unity, one can easily compute the matrix of θ relative to the given basis of $\mathfrak{g}$. Then by linear algebra we can construct bases of $\mathfrak{g}_0$ and $\mathfrak{g}_1$.

I have considered the problem for the inner automorphisms of simple Lie algebra of exeptional type; i.e., E_6, E_7, E_8, F_4, G_2, and for the outer automorphisms of E_6.

The thesis is organised in this fashion.

In Chapter 1 I illustrate the class of complex reflection groups, to which the little Weyl groups belong. After a general presentation of the subject I report the standard list, due to Shephard and Todd, determining the complete classification of the objects.

In Chapter 2 I introduce general elements of complex Lie algebras, focussing the case of semisimple Lie algebras. Subsequently I present the classification of the simple Lie algebras arising from the one of the irreducible root systems. Finally I give some notions about automorphisms and their representation by Kac diagrams.

In Chapter 3, after a preliminary introduction of the relative algebraic-geometrical context, I give the basic definitions of algebraic groups over $\mathbb{C}$, and then of the Lie algebra of an algebraic group. The main results of the subject are presented with particular reference to connected and reductive groups. Finally I introduce the θ-groups and the other notions setting up the base for my research .

In Chapter 4 I present the computational methods, for computing generators of a little Weyl group. The final tables conclude the thesis reporting the found results.

Acknowledgements

I would like to express my gratitude to my advisor Dr. Willem A. de Graaf for his great understanding and support, all along these research years. I would also like to thank Dr. Serena Cicalò for her graceful and important help in using LaTeX.

Chapter 1

Complex reflection groups

The objects allowing to get the results of my research, belongs to a particular class of groups, introduced by a work of Shephard and Todd started in 1951. I'm referring to the *complex reflection groups* that arise from a generalisation of the classical concept of *real reflection* in a euclidean space, by intoducing the new notion of *complex reflection*. In this chapter I first introduce the preliminaries for getting the definition of complex reflection group and its connected notions. Then I present in some detail a particular class of three parameters groups, $G(m, p, n)$. Subsequently I introduce the notion of polynomial invariant of a complex reflection group, for getting to the theorem of Chevalley, Shephard and Todd that plays an important role in the computational methods. Finally I show the standard list of the irreducible complex reflection groups that determines, in fact, the complete classification of the complex reflection groups. Most of the subject is taken from [14]. Also see [2].

1.1 Preliminars

Definition 1.1.1. Given a complex vector space V of dimension n, a *hermitian form* on V is a mapping

$$(-,-) : V \times V \to \mathbb{C}$$

such that

1. $(v_1 + v_2, w) = (v_1, w) + (v_2, w)$
2. $(av, w) = a(v, w)$
3. $\overline{(v, w)} = (w, v)$

for all $v, w, v_1, v_2 \in V$ and $a \in \mathbb{C}$. The hermitian form is said to be *positive definite* if

1. $(v, v) \geq 0$ for all $v \in V$, and
2. $(v, v) = 0$ if and only if $v = 0$.

A positive definite hermitian form is also called an *inner product* on V.

Fixed a basis $e_1, \dots, e_n$ we may define an inner product on V in canonical form by

$$(u, v) = \sum_{i=1}^{n} a_i \bar{b}_i$$

where $a = \sum_{i=1}^{n} a_i e_i$ and $b = \sum_{j=1}^{n} b_j e_j$. Conversely, given an inner product on V there exists a suitable basis with respect to which the form is described in the previous fashion. So, we can say that two inner products $(-, -)$ and $[-, -]$ are *equivalent*, in the sense that there is an invertible linear transformation $\phi : V \to V$ such that $(u, v) = [\phi(u), \phi(v)]$ for all $u, v \in V$.

Let $\mathrm{GL}(V)$ be the group of all invertible linear transformations of V. A subgroup G of $\mathrm{GL}(V)$ is said to leave the form $(-, -)$ *invariant* if

$$(gv, gw) = (v, w)$$

for all $g \in G$ and all $v, w \in V$.

In this case we also say that $(-, -)$ is a *G-invariant* form.

Lemma 1.1.2. *If G is a finite subgroup of $\mathrm{GL}(V)$, there exists a G-invariant inner product on V.*

If $(-, -)$ is any inner product on V, we say that $x \in \mathrm{GL}(V)$ is *unitary* (or an *isometry*) if $(xv, xw) = (v, w)$ for all $v, w \in V$; that is, $(-, -)$ is $\langle x \rangle$-invariant.

A basis $e_1, \dots, e_n$ for V is *orthogonal* if $(e_i, e_j) = 0$ for all $i \neq j$; it is *orthonormal* if in addition $(e_i, e_i) = 1$ for all i. Let M be the matrix of $x \in \mathrm{GL}(V)$ with respect to an orthonormal basis of V. Then x is unitary if and only if M is a *unitary matrix*; i.e., $M\overline{M}^t = I$, where $\overline{M}^t$ denotes the transpose of the complex conjugate of M and I is the identity matrix.

The group of all isometries of V is denoted by $U(V)$ and called the *unitary group* of the form. Its subgroup of transformations of determinant 1 is called the *special unitary group*. The corresponding group of unitary matrices will be denoted by $U_n(\mathbb{C})$ and $SU_n(\mathbb{C})$, where $n := \dim V$. The group $U(V)$ depends on the form but, as any two inner product are equivalent, $U(V)$ is unique up to conjugacy in $\mathrm{GL}(V)$. With this notation the previous lemma says that any finite subgroup of $\mathrm{GL}(V)$ is a subgroup of $U(V)$ for an appropriate inner product.

Let V be a complex vector space of dimension n, equipped by an inner product $(-, -)$.

Definition 1.1.3. If U is a subset of V we call *orthogonal complement* of U the subspace $U^{\perp} := \{v \in V \mid (u, v) = 0 \text{ for all } u \in U\}$.

If U and W are subspaces of V, we write $V = U \perp W$ to indicate that $V = U \oplus W$ and $(u, w) = 0$ for all $u \in U$ and $w \in W$. It is easy to check that $V = U \perp W$ if and only if $W = U^{\perp}$. Further, $U^{\perp\perp} = U$ and $\dim U + \dim U^{\perp} = \dim V$ for any subspace $U \subset V$.

Definition 1.1.4. Let 1 be the identity element of $\mathrm{GL}(V)$. For $g \in \mathrm{GL}(V)$ and $H \subset \mathrm{GL}(V)$, put

1. $\mathrm{Fix}\ g := \mathrm{Ker}(1 - g) = \{v \in V \mid gv = v\}$,
2. $V^H := \mathrm{Fix}_V(H) := \{v \in V \mid hv = v \text{ for all } h \in H\}$,
3. $[V, g] := \mathrm{Im}(1 - g)$.

Remark 1.1.5. If $g \in U(V)$, then $[V, g] = (\mathrm{Fix}\ g)^{\perp}$.

Definition 1.1.6. A linear transformation g is said to be a *reflection* if the order of g is finite and $\dim[V, g] = 1$.

If g is a reflection, the subspace Fix g is a hyperplane, called the *reflecting hyperplane* of g. We call g a *unitary* reflection if it preserves the inner form $(-.-)$. In this case Fix g is orthogonal to $[V, g]$ and $V = [V, g] \perp \mathrm{Fix}\ g$.

Let $g \in \mathrm{GL}((V)$ be a reflection of order m. Then the cyclic group $\langle g \rangle$ has order m and so leaves invariant a suitable inner product. Thus every reflection g is a unitary reflection with respect to some form. If $H = \mathrm{Fix}\ g$, then g leaves invariant the line (one-dimensional subspace) $H^{\perp}$. Hence, with respect to a basis adapted to the decomposition $V = H^{\perp} \perp H$, g has matrix $\mathrm{diag}[\zeta, 1, \ldots, 1]$, where ζ is a primitive m-th root of unity.

Definition 1.1.7. A *root* of a line l of V is any nonzero vector of l. If g is a unitary reflection, a root of g is a root of the line $[V, g]$. A root a is *short*, *long* or *tall* if (a, a) is 1, 2 or 3, respectively.

Any line in $\mathbb{C}^n$ contains long, short and tall roots, each of which is unique up to multiplication by an element of $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$

Definition 1.1.8. We call *complex reflection group* a finite subgroup of $U(V)$ that is generated by reflections.

Proposition 1.1.9. *Every finite subgroup of* $\mathrm{GL}(V)$ *that is generated by reflections is a complex reflection group with respect to some inner product on* V.

It is important to note that the concept 'complex reflection group' includes the representation as well as the group. A given group may act as a reflection group or otherwise. For example, for $\zeta := \exp(2\pi i/m)$, the element $\mathrm{diag}[\zeta, 1, \dots, 1]$ generates a cyclic reflection group of order m, but the (isomorphic) group generated by $\mathrm{diag}[\zeta, \zeta, 1, \dots, 1]$ is not a reflection group.

Definition 1.1.10. Given a nonzero vector $a \in V$ and a m-th root of unity $\alpha \neq 1$, define the map $r_{a,\alpha} : V \to V$ by

$$r_{a,\alpha}(v) := v - (1-\alpha)\frac{(v,a)}{(a,a)}a$$

Proposition 1.1.11. *$r_{a,\alpha}$ is a unitary reflection of order m.*

Proposition 1.1.12. *If r is a unitary reflection of order m in $U(V)$ and a is a root of r of length 1, there exists a primitive m-th root of unity α such that for all $v \in V$ it is*

$$r_{a,\alpha}(v) = r$$

Proposition 1.1.13. *Consider a root a of a unitary reflection r of order m, and let α, β be primitive m-th root of unity. Then*

1. $r_{a,\alpha} r_{\alpha,\beta} = r_{a,\alpha\beta}$
2. *For $g \in U(V)$, $g r_{a,\alpha} g^{-1} = r_{ga,\alpha}$*
3. *For $\lambda \in \mathbb{C}$ such that $\lambda \neq 0$, $r_{\lambda a,\alpha} = r_{a,\alpha}$.*

Proposition 1.1.14. *If $g \in U(V)$ and $g r_{a,\alpha} g^{-1} = r^k_{a,\alpha}$ for some k, then $k = 1$. In other words, a reflection is not conjugate to any proper power.*

Proposition 1.1.15. *The unitary reflections $r_{a,\alpha}$ and $r_{b,\beta}$ commute if and only if $\mathbb{C}a = \mathbb{C}b$ or $(a,b) = 0$.*

Proposition 1.1.16. *A subspace W of V is invariant with respect to the reflection r if and only if $W \subset \mathrm{Fix}\ r$ or $[V,r] \subset W$.*

Corollary 1.1.17. *If r is a unitary reflection with root a, then the subspace W is invariant with respect to r if and only if $a \in W$ or $a \in W^{\perp}$.*

I recall that if V is a complex vector space of dimension n, a *linear representation* of a group G on V is a homomorphism $\rho : G \to \mathrm{GL}(V)$. In this case we say that G *acts* on V, and call V a *G-module*. Usually we put $g.v := \rho(g)(v)$ for all $g \in G$ and for all $v \in V$. The representation is said to be *faithful* if it is injective. A *G-submodule* of V is a vector subspace U such that $g.u \in U$ for all $g \in G$ and all $u \in U$. The G-module V is called *irreducible* if 0 and V are its only G-submodules.

Let G be a complex reflection group. Then the G-module V is called the *natural* (or *reflection*) *representation* of G. If V is an irreducible G-module, we say that G is an *irreducible* complex reflection group.

Theorem 1.1.18. *Suppose that G is a finite group generated by reflections on V, which leaves the inner product $(-,-)$ invariant. Then V is the direct sum of pairwise orthogonal subspaces $V_1, \ldots, V_m$ such that the restriction G_i of G to V_i acts irreducibly on V_i and $G = G_1 \times \cdots \times G_m$. If W is an irreducible subspace of V that is not fixed pointwise by every element of G, then $W = V_i$ for some i.*

Proposition 1.1.19. *We have*

$$V = V^G \perp V_1 \perp \ldots \perp V_k,$$

where the V_i are nontrivial irreducible G-modules.

Definition 1.1.20. We call *support* of a complex reflection group $G \subset U(V)$ the subspace M of V spanned by the roots of the reflections in G.

Definition 1.1.21. We call *rank* of a complex reflection group G the dimension of its support, and *reflection subgroup* of G a subgroup H that is generated by reflections.

If G is generated by the reflections $r_1, \ldots, r_k$ with roots $a_1, \ldots, a_k$, we can define a graph Γ with vertex set $R := \{a_1, \ldots, a_k\}$ by joining a_i to a_j whenever a_i and a_j are neither equal nor orthogonal. We can observe that in this definition it is possible to have $|R| < k$.

Proposition 1.1.22. *If G is a complex reflection group with support V and graph Γ then V is an irreducible G-module if and only if Γ is connected.*

Corollary 1.1.23. *Suppose that G is a complex reflection group and that H is a reflection subgroup of G acting irreducibly on its support W. If $r \in G$ is a reflection with root a such that $a \notin W \cup W^\perp$, then $\langle H, r\rangle$ acts irreducibly on $W \oplus \mathbb{C}a$.*

Corollary 1.1.24. *Any irreducible reflection group of rank n has an irreducible reflection subgroup of rank n with n generators.*

Theorem 1.1.25. *If G_1 and G_2 are irreducible complex reflection groups, then G_1 and G_2 are conjugate in* $\mathrm{GL}(V)$ *if and only if they are conjugate in $U(V)$.*

Suppose that G is a complex reflection group and that $\dim V = n$. Let $r_1, \ldots, r_l$ be reflections in G with roots $a_1, \ldots, a_l$. Then, for $1 \leq i \leq l$ there exist linear maps $\phi_i \in V^*$ such that

$$r_i(v) = v - \phi_i(v)a_i$$

for all $v \in V$. The Cartan coefficient of the pair a_i, a_j of roots is defined as $\langle a_i \mid a_j \rangle := \phi_j(a_i)$. Hence $r_i(a_i) = (1 - \langle a_i \mid a_i \rangle)a_i$ and therefore $1 - \langle a_i \mid a_i \rangle$ is a primitive m_i-th root of unity, where m_i is the order of r_i.

Definition 1.1.26. The *Cartan matrix* of the reflections $r_1, \ldots, r_l$ with respect to the roots a_i is the $l \times l$ matrix $C := (\langle a_i \mid a_j \rangle)$.

If G is a euclidean reflection group and if the a_i are the simple roots (see §2.5), then C is the usual Cartan matrix of G.

Definition 1.1.27. By analogy with the euclidean case, the group $W(C)$ generated by the reflections $r_1, \ldots, r_l$ is called the *Weyl group* of C.

Proposition 1.1.28. *The following results hold:*

1. *$W(C)$ is completely determined by the Cartan matrix C.*
2. *In general, $W(C)$ is not finite.*

Definition 1.1.29. Let G be a complex reflection group generated by reflections $r_1, \ldots, r_l$, with Cartan matrix C corresponding to a certain set of corresponding roots. If the entries of C belong to a field F, then G is said to be *definable* over F.

Definition 1.1.30. Let G be a subgroup of $\mathrm{GL}(V)$ and $g \in G$. Let then $\chi(g)$ denote the trace of the linear transformation g. The function $\chi : G \to \mathbb{C}$ is called the *character* of the representation of G in V, and $\mathbb{Q}(\chi)$ is the field generated by the values $\chi(g)$, for all $g \in G$.

Definition 1.1.31. We call the *field of definition* $\mathbb{Q}(G)$ of a complex reflection group G the field $\mathbb{Q}(\chi)$, where χ is the character of the natural representation.

Theorem 1.1.32 (Benard, 1976)**.** *Every representation of a complex reflection group is definable over its field of definition.*

Corollary 1.1.33. *If G is a complex reflection group generated by reflections $r_1, \ldots, r_l$, then there is a Cartan matrix of these reflections with entries in $\mathbb{Q}(G)$.*

For real reflection groups as Weyl groups (see §2.4, §2.5) it is always possible to choose roots for the reflections so that the entries of the Cartan matrix are rational integers. In complex reflection groups the best we can have is that the entries of a Cartan matrix belong to the algebraic integers of the field $\mathbb{Q}(G)$.

Definition 1.1.34. We call the *ring of definition* $\mathbb{Z}(G)$ of G the ring of algebraic integers in $\mathbb{Q}(G)$.

Theorem 1.1.35. *Let G be an irreducible complex reflection group. Then there exists a representation of G by matrices over $\mathbb{Z}(G)$.*

Theorem 1.1.36. *Every representation of a finite group G over the complex numbers (in particular, for G being a complex reflection group) is definable over the field $\mathbb{Q}(\zeta_m)$, where ζ_m is a primitive m-th root of unity such that $g^m = 1$ for all $g \in G$.*

Suppose that F is a finite abelian extension of $\mathbb{Q}$, let A be the ring of integers of F and let $\mu(A)$ be the (finite cyclic) group of roots of unity in A. The field F is fixed by complex conjugation under any embedding of F in $\mathbb{C}$ and since F is abelian there is a well-defined operation of complex conjugation on F which inverts every element of $\mu(A)$. So, if V is a vector space over F we may consider hermitian forms on V. In particular, if $e_1, \ldots, e_n$ is a basis for V, there is a well-defined hermitian forms on V expressed in canonical form with respect to it. However, given a hermitian form $(-,-)$, not necessarily we may choose an orthonormal basis for V with respect to $(-,-)$.

Suppose that G is a complex reflection group preserving a free A-submodule L of V. If $v \in L$, $g \in G$ and $g(v) = \theta v$, then $\theta^k = 1$, where k is the order of g; that is, $\theta \in \mu(A)$. It follows that we may choose roots for the reflections of G that satisfy the following definition.

Definition 1.1.37. We call a *A-root system* in a vector space V over F with inner product $(-,-)$, a pair (Σ, f) where Σ is a finite subset of V and $f : \Sigma \to \mu(A)$ is a function such that:

1. Σ spans V and $0 \notin \Sigma$,

2. for all $a \in \Sigma$ and $\lambda \in F$, we have $\lambda a \in \Sigma$ if and only if $\lambda \in \mu(A)$,

3. for all $a \in \Sigma$ and $\lambda \in \mu(A)$, we have $f(\lambda a) = f(a) \neq 1$,

4. for all $a, b \in \Sigma$, the Cartan coefficient

$$\langle a|b\rangle = (1 - f(b))\frac{(a,b)}{(b,b)}$$

belongs to A,

5. for all $a, b \in \Sigma$, we have $r_{a,f(a)}(b) \in \Sigma$ and $f(r_{a,f(a)}(b)) = f(b)$.

We say that (Σ, f) is a root system defined over A. If $W := W(\Sigma, f)$ is the group generated by the reflections $r_{a,f(a)}$, then W is a complex reflection group, called the *Weyl group* of the root system. It follows from 2. and 5. that $\mu(A)w\Sigma = \Sigma$ and W is a group of permutations of the finite set Σ. From 1. only the identity element fixes every element of Σ and therefore W is finite. The order of $r_{a,f(a)}$ is two if and only if $f(a) = -1$ and therefore every reflection of order two is uniquely determined by the line spanned by its root a. In this case we denote $r_{a,f(a)}$ by r_a.

1.2 The groups $G(m, p, n)$

In order to illustrate this special class, we need some preliminary definitions.

Definition 1.2.1. The G-module V is called *imprimitive* if for some $m > 1$ it is a direct sum $V = V_1 \oplus \cdots \oplus V_m$ of nonzero subspaces V_i $(1 \leq i \leq m)$ such that the action of G on V permutes the subspaces $V_1, \ldots, V_m$ among themselves; otherwise V is called *primitive*. The set $\{V_1, \ldots, V_m\}$ is called a *system of imprimitivity* for V.

Remark 1.2.2. According to this definition, if G is a primitive group, then V is necessarily an irreducible G-module.

Definition 1.2.3. Given an irreducible G-module I, we call the *isotypic component* V_I of V corresponding to I the sum of all G-submodules of V isomorphic to I.

Proposition 1.2.4. *Every irreducible G-submodule of the isotypic component V_I is isomorphic to I and V is the direct sum of its distinct isotypic components.*

Theorem 1.2.5. *If G is a finite primitive subgroup of $\mathrm{GL}(V)$ and if A is an abelian normal subgroup of G, then A is cyclic and contained in the centre $Z(G)$ of G.*

Theorem 1.2.6. *If $G \subset U(V)$ is a primitive complex reflection group and if N is a normal subgroup of G, then either V is an irreducible N-module or $N \subset Z(G)$*

Let G be a group acting on the set $\Omega := \{1, \ldots, n\}$ and take any group H. Let then $B := H \times \cdots \times H$ be the direct product of n copies of H. We can define an action of G on B by

$$g.h := (h_{g(1)}, \ldots, h_{g(n)})$$

for $g \in G$ and $h := (h_1, \ldots, h_n) \in B$.

Definition 1.2.7. We call *wreath product* $H \wr G$ of H by G the semidirect product of B by G. Its elements will be written $(h; g)$ and its multiplication is given by

$$(h; g)(h'; g') := (hg.h'; gg')$$

So, if H and G are finite, the order of $H \wr G$ is $|H|^n|G|$.

Throughout we suppose H to be a finite subgroup of the multiplicative group $\mathbb{C}^\times$ of $\mathbb{C}$. This means that, for some m, H is the (cyclic) group $\boldsymbol{\mu}_m$ of m-th roots of unity.

Let V be a vector space of dimension n over $\mathbb{C}$ with an inner product (-,-) and $e_1, \ldots, e_n$ an orthonormal basis. Then the elements of B can be represented by diagonal transformations of V. In other words, with h as above, we put

$$he_i = h_i e_i \qquad \text{for } 1 \le i \le n$$

Since $h_i \overline{h}_i = 1$ for all $h_i \in H$, B is a subgroup of $U(V)$. The group G acts on V by permuting the basis vectors:

$$ge_i := e_{g(i)} \qquad \text{for } 1 \le i \le n$$

and so it may also be regarded as a subgroup of $U(V)$. The actions of $B = \boldsymbol{\mu}_m^n$ and G on V are compatible and determine an action of $\boldsymbol{\mu}_m \wr G$ on V given by

$$(h; g)e_i := h_{g(i)} e_{g(i)} \qquad \text{for } 1 \le i \le n.$$

The matrices of these linear transformations (with respect to $e_1, \ldots, e_n$) have exactly one nonzero entry in each row and column and are called *monomial matrices*. So, this representation of $\boldsymbol{\mu}_m \wr G$ is said to be the *standard monomial representation*. Thus $\boldsymbol{\mu}_m \wr G$ is represented as a subgroup of $U(V)$ and the subspaces $\mathbb{C}e_1, \ldots, \mathbb{C}e_n$ form a system of imprimitivity for $\boldsymbol{\mu}_m \wr G$.

Definition 1.2.8. Let $B := \boldsymbol{\mu}_m^n$. For each divisor p of m put

$$A(m,p,n) := \{(\theta_1, \ldots, \theta_n) \in B \mid (\theta_1, \ldots, \theta_n)^{m/p} = 1\}$$

Clearly $A(m,p,n)$ is a subgroup of index p in B and is invariant under the action of the symmetric group $\mathrm{Sym}(n)$.

We write $G(m,p,n)$ to indicate the semidirect product of $A(m,p,n)$ by $\mathrm{Sym}(n)$ (notation introduced by Shephard and Todd).

$G(m,p,n)$ is a normal subgroup of index p in $\boldsymbol{\mu}_m \wr \mathrm{Sym}(n)$ and consequently we may represent it as a group of linear transformations in the standard monomial representation, having order $m^n n!/p$.

Let regard $G(m,p,n)$ as being defined with respect to the orthonormal basis $e_1,\ldots,e_n$ for V. Then we have

Lemma 1.2.9. *The element $r \in G(m,p,n)$ is a reflection if and only if r has one of the following forms:*

1. *For some i and for some (m/p)-th root of unity $\theta \neq 1$, $r = r_{e_i,\theta}$,*
2. *For some $i \neq j$ and for some m-th root of unity $\theta, r = r_{e_i-\theta e_j,-1}$. In this case the order of r is two, $re_i = \theta e_j$, $re_j = \theta^{-1}e_i$ and $re_k = e_k$ for all $k \neq i,j$.*

Proposition 1.2.10. *The group $G(m,m,n)$ contains $m\binom{n}{2}$ reflections of order 2. If $n > 2$ or if m is odd, the reflections form a single conjugacy class. If m is even, $G(m,m,2)$ contains two conjugacy classes of reflections.*

Proposition 1.2.11. *If $m > 1$, then $G(m,p,n)$ is an imprimitive complex reflection group. It is irreducible except when $(m,p,n) = (2,2,2)$.*

What follows, instead, allows us to determine all imprimitive complex reflection groups.

Theorem 1.2.12. *Let V be a complex vector space of dimension n with inner product (-,-), and G be an irreducible imprimitive finite subgroup of $U(V)$, which is generated by reflections. Then $n > 1$ and G is conjugate to $G(m,p,n)$ for some $m > 1$ and some divisor p of m.*

Let $e_1,\ldots,e_n$ be an orthonormal basis for V and suppose that the matrices of $G(m,p,n)$ with respect to this basis are monomial. Furthermore, we note that when $G(m,p,n)$ is irreducible, the system of imprimitivity $\{\mathbb{C}e_1,\ldots,\mathbb{C}e_n\}$ consists of the distinct isotypic components of the abelian normal subgroup $A(m,p,n)$.

Theorem 1.2.13. *Suppose that $G := G(m,p,n)$ is irreducible and has more than one system of imprimitivity. Then G is one of the following groups.*

1. *$G(2,1,2) \simeq G(4,4,2)$ or $G(4,2,2)$, each of which has the same three systems of imprimitivity: $\{\mathbb{C}e_1, \mathbb{C}e_2\}, \{\mathbb{C}(e_1+e_2), \mathbb{C}(e_1-e_2)\}$ and $\{\mathbb{C}(e_1+ie_2), \mathbb{C}(e_1-ie_2)\}$.*

2. *$G(3,3,3)$ with four systems of imprimitivity: $\Pi_0 := \{\mathbb{C}e_1, \mathbb{C}e_2, \mathbb{C}e_3\}$ and, for a fixed primitive cube root of unity ω,*

$$\Pi_i := \{\mathbb{C}(e_1 + \omega_2 e_2 + \omega_3 e_3) \mid \omega_2, \omega_3 \in \{1, \omega, \omega^2\} \text{ and } \omega_2\omega_3 = \omega^i\}$$

for $i := 1, 2$ and 3.

3. *$G(2,2,4)$ with three systems of imprimitivity:*

$$\Lambda_0 := \{\mathbb{C}e_1, \mathbb{C}e_2, \mathbb{C}e_3, \mathbb{C}e_4\} \text{ and}$$

$$\Lambda_i := \{\mathbb{C}(e_1 + \epsilon_2 e_2 + \epsilon_3 e_3 + \epsilon_4 e_4) \mid \epsilon_j = \pm 1 \text{ and } \epsilon_2\epsilon_3\epsilon_4 = (-1)^i\}$$

for $i := 1$ and 2.

Corollary 1.2.14. *Suppose that $m \geq 2$ and that G is a finite reflection subgroup of $U_n(\mathbb{C})$ which contains $G(m,p,n)$ as a normal subgroup.*

1. *If $n \geq 3$ and (m,p,n) is neither $(3,3,3)$ nor $(2,2,4)$, then for some divisor q of p we have $G = G(m,q,n)$,*

2. *If $n = 2$ and $(m,p,2)$ is not $(4,2,2)$, then G is contained in $G(2m,2,2)$.*

Proposition 1.2.15. *$G(4,2,2), G(3,3,3)$ and $G(2,2,4)$ occur as normal subgroups of primitive reflection groups. On the other hand, for all divisors p of m we have $G(m,p,n) \lhd G(m,1,n)$ and when $n = 2$ we also have $G(m,p,2) \lhd G(2m,2,2)$.*

Theorem 1.2.16. *Suppose that G is a primitive complex reflection group in $U(V)$ and that W is a proper subspace of V of dimension at least two. Suppose that H is a subgroup of G that fixes $W^\perp$ pointwise and which acts on W as an irreducible imprimitive reflection group not conjugate to $G(2,1,2), G(3,3,2), G(4,4,2), G(4,2,2), G(2,2,3), G(3,3,3)$ nor $G(2,2,4)$. Then there is a reflection $r \in G$ with root $a \notin W$ such that the action of $\langle H, r\rangle$ on $W \oplus \mathbb{C}a$ is primitive.*

In order to determine minimal sets of generating reflections for the groups $G(m,p,n)$ we can do as follows. For $i := 1, \dots, n-1$ let $r_i := r_{e_i - e_{i+1}, -1}$ be the reflection of order 2 that interchanges the basis vectors e_i and e_{i+1} and fixes e_j for $j \neq i, i+1$. Let $t := r_{e_1, \zeta_m}$ be the reflection of order m that fixes $e_2, \dots, e_n$ and sends e_1 to $\zeta_m e_1$ and let $s := t^{-1} r_1 t$ be the reflection of order 2 that interchanges e_1 and $\zeta_m e_2$. For $m > 1$, the groups $G(m,m,n)$ and $G(m,1,n)$ can be generated by n reflections; however, the minimum number of reflections required to generate $G(m,p,n)$, for $p \neq 1, m$ is $n+1$. In particular, we have

- $G(1,1,n) = \langle r_1, \ldots, r_{n-1} \rangle \simeq \mathrm{Sym}(n)$,
- $G(m,m,n) = \langle s, r_1, \ldots, r_{n-1} \rangle$,
- $G(m,1,n) = \langle t, r_1, \ldots, r_{n-1} \rangle$,
- $G(m,p,n) = \langle s, t^p, r_1, \ldots, r_{n-1} \rangle$ for $p \neq 1, m$.

1.3 Polynomial invariants

Definition 1.3.1. For each $r := 0, 1, \ldots$ we let $T^r(V)$ denote the r-fold tensor power of V. That is, $T^0(V) := \mathbb{C}$, $T^1(V) := V$, $T^2(V) := V \otimes V$, and so on. The direct sum

$$T(V) := \bigoplus_{r=0}^{\infty} T^r(V)$$

is the called the tensor algebra of V. Multiplication is defined on $T(V)$ by declaring the product of $v_{i_1} \otimes \cdots \otimes v_{i_k} \in T^k(V)$ with $v_{j_1} \otimes \cdots \otimes v_{j_l} \in T^l(V)$ to be $v_{i_1} \otimes \cdots \otimes v_{i_k} \otimes v_{j_1} \otimes \cdots \otimes v_{j_l} \in T^{k+l}(V)$, and then extending this to all of $T(V)$ by linearity.

There is a natural embedding of V in $T(V)$ that identifies $v \in V$ with the element $(0, v, 0, \ldots) \in T(V)$. This makes $T(V)$ the free associative algebra on V in the sense that if A is any associative $\mathbb{C}$-algebra and if $\phi : V \to A$ is a vector space homomorphism, there is a unique algebra homomorphism $\Phi : T(V) \to A$ such that $\phi(v) = \Phi(v)$ for all $v \in V$. Given a linear transformation $f : V \to W$ there is a unique algebra homomorphism $T(f) : T(V) \to T(W)$ such that $T(f)v = f(v)$ for all $v \in V$. Thus $T(f)(v_{i_1} \otimes \cdots \otimes v_{i_k}) = f(v_{i_1}) \otimes \cdots \otimes f(v_{i_k})$. Moreover, $T(1_V) = 1_{T(V)}$ and if $g : W \to U$ is another linear transformation, then $T(gf) = T(g)T(f)$. These properties are usually expressed by saying that T is a *functor* from vector spaces to associative algebras.

Definition 1.3.2. Let I be the two-sided ideal of $T(V)$ generated by the elements $v \otimes w - w \otimes v$ for all $v, w \in V$. Define the symmetric algebra of V to be the quotient $S(V) := T(V)/I$. It is the free commutative algebra on V. The product of $\xi := u + I$ and $\eta := v + I$ in $S(V)$ is $\xi\eta := u \otimes v + I$, where $u \otimes v$ is the product of u and v in $T(V)$.

We have $V \cap I = \{0\}$ and therefore V may be identified with its image in $S(V)$. If $v_1, \ldots, v_n$ is a basis for V, then $S(V)$ is isomorphic to the algebra of polynomials in the symbols $v_1, \ldots, v_n$. That is, $S(V) \simeq \mathbb{C}[v_1, \ldots, v_n]$. We let $X_1, \ldots, X_n$ be the basis of V^* dual to the basis $v_1, \ldots, v_n$ of V. The linear maps $X_1, \ldots, X_n$ are the coordinate functions of V and $S := S(V^*) \simeq \mathbb{C}[X_1, \ldots, X_n]$ is the coordinate ring of V. Thus S may be identified with the ring of polynomial functions on V.

Lemma 1.3.3. *Let $w_1, \ldots, w_s$ be distinct elements of V, and let $a_1, \ldots, a_s$ be arbitrary elements of $\mathbb{C}$. Then there is a polynomial $P \in S$ such that $P(w_i) = a_i$ for $i = 1, \ldots, s$.*

The *degree* of the monomial $X_1^{m_1} \cdots X_n^{m_n}$ is $m_1 + \cdots + m_n$. A polynomial P is *homogeneous* of degree r, and we write deg $P := r$, if P is a linear combination of monomials of degree r. The ring S has a natural grading by degree. That is, if S_r denotes the subspace of homogeneous polynomials of degree r, then $S = \bigoplus_{r=0}^{\infty} S_r$ and $S_r S_t \subset S_{r+t}$. Note that there are $\binom{n+r-1}{r}$ distinct monomials of degree r and therefore dim $S_r = \binom{n+r-1}{r}$.

The above remarks about grading apply equally to the non-commutative tensor algebra

$$T(V) = \bigoplus_{r=0}^{\infty} T^r(V)$$

and we clearly have dim $T_r(V) = n^r$. If I is any homogeneous ideal of $T(V)$, i.e., if I is an ideal which contains the homogeneous components of all its elements, then the quotient algebra $T_r(V)/I$ inherits a grading, and the example $S(V)$ above is a special case of this construction.

The group GL(V) acts on V^* and hence on S. That is, for $g \in$ GL(V) and for a polynomial function $P \in S$ we define gP by

$$gP(v) := P(g^{-1}v)$$

for all $v \in V$.

This is a linear action that preserves both the degree and algebra structure of S, i.e. $gS_r = S_r$ and $g(PQ) = (gP)(gQ)$. If the matrix of g with respect to the basis $v_1, \ldots, v_n$ is $A := (a_{ij})$, where $gv_j = \sum_i a_{ij} v_i$, then the matrix of the action of g on V^* with respect to the basis $X_1, \ldots, X_n$ is A^{-t}, the inverse transpose of A. Thus for a polynomial $P(X_1, \ldots, X_n)$ we have $gP(X_1, \ldots, X_n)$=$P(X_1', \ldots, X_n')$, where

$$\begin{bmatrix} X_1' \\ \vdots \\ X_n' \end{bmatrix} = A^{-1} \begin{bmatrix} X_1 \\ \vdots \\ X_n \end{bmatrix}$$

For example, if $n = 2$ and the matrix of g is $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, then the action of g on S is given by

$$g(X_1^i X_2^j) = (X_1 - X_2)^i X_2^j$$

.

From now on, let G be a subgroup of GL(V). We say that $P \in S$ is G-*invariant* if $gP = P$ for all $g \in G$. If M is a G-module, then M^G denotes the isotypic component corresponding to the trivial representation; in other words $M^G := \{m \in M \mid gm = m$ for all $g \in G\}$ is the submodule of G-invariant elements, also known as the space of fixed points of G.

Definition 1.3.4. The *algebra of invariants* of G is the algebra of G-invariant polynomial functions $J := S^G$.

If $P \in J$, then P is constant on each G-orbit of V and therefore J may be interpreted as an algebra of polynomial functions on the set V/G of all G-orbits on V. A useful direct connection between the action of G and the algebra of invariants is given in the next result, which is due to E. Noether.

Theorem 1.3.5. *Suppose that $v, w \in V$. Then there exists $g \in G$ such that $g(v) = w$ if and only if $P(v) = P(w)$ for all $P \in J$.*

Theorem 1.3.6 (Hilbert-Noether)**.** *Consider a finite dimensional vector space V over $\mathbb{C}$ and let G be a finite subgroup of $\mathrm{GL}(V)$. Then the algebra $S(V^*)^G$ of invariants is finitely generated.*

Theorem 1.3.7 (Chevalley-Shephard-Todd)**.** *If G is a complex reflection group on the vector space V of dimension n, then the ring J of G-invariant polynomials is a polynomial algebra, i.e. it is generated by a collection of algebraically independent homogeneous polynomials.*

Theorem 1.3.8. *Let G be a finite group acting on the complex vector space V of dimension n. Suppose that $f_1, \ldots, f_n$ are homogeneous algebraically independent elements of $J := S(V^*)^G$ and set $d_i := \deg f_i$ for $i := 1, \ldots, n$. Then*

1. *$|G| \leq d_1 \cdots d_n$;*
2. *if $|G| = d_1 \cdots d_n$ then G is a reflection group in V and J is generated by $f_1, \cdots f_n$ as an algebra;*
3. *if J is generated by $f_1, \ldots, f_n$ as an algebra, then equality holds in 1. and G is a reflection group.*

Definition 1.3.9. A set of algebraically independent homogeneous polynomials that generate the algebra J of G-invariant polynomials is called a set of *fundamental* (or *basic*) invariants for G.

Theorem 1.3.10. *A set of fundamental invariants of G is not unique, however their number and their degrees are uniquely determined by G.*

Definition 1.3.11. For ℓ being the rank of G, the degrees $d_1 \leq \cdots \leq d_\ell$ of the generators of the ring of invariants are called the *degrees* of G.

Theorem 1.3.12. *The following results hold.*

- *The centre of an irreducible reflection group is cyclic of order equal to the greatest common divisor of the degrees.*
- *The order of a complex reflection group is the product of its degrees.*
- *The number of reflections is the sum of the degrees minus the rank.*
- *An irreducible complex reflection group comes from a real reflection group if and only if it has an invariant of degree 2.*
- *The degrees di satisfy the formula* $\prod_{i=1}^{l}(q + d_i - 1) = \sum_{g \in G} q^{\dim(V^g)}$.

Definition 1.3.13. For ℓ being the rank of the reflection group, the *codegrees* $d_1^* \geq \cdots \geq d_\ell^*$ of G can be defined by $\prod_{i=1}^{\ell}(q - d_i^* - 1) = \sum_{g \in G} \det(g) q^{\dim(V^g)}$.

1.4 Classification

Proposition 1.4.1. *Any complex reflection group is a product of irreducible complex reflection groups, acting on the sum of the corresponding vector spaces.*

The complete classification of complex reflection groups is then obtained once having just classified the irreducible ones. This work was made in 1954 by G. C. Shephard and J. A. Todd. I conclude the chapter by reporting their standard list. In that:

- **ST** is the Shephard-Todd number of the reflection group;
- **Rank** is the dimension of the complex vector space the group acts on;
- **Structure** describes the structure of the group;
- **Order** is the number of elements of the group;
- **Reflections** describes the number of reflections: $2^6 4^{12}$ means that there are 6 reflections of order 2 and 12 of order 4.
- **Degrees** gives the degrees of the fundamental invariants of the ring of polynomial invariants. For example, the invariants of group number 4 form a polynomial ring with 2 generators of degrees 4 and 6.

Table 1.1: List of irreducible complex reflection groups.

ST	Rank	Structure and names	Order	Reflections	Degrees	Codegrees
1	$n-1$	Symmetric group $G(1,1,n)=\mathrm{Sym}(n)$	$n!$	$2^{n(n-1)/2}$	$2,3,\ldots,n$	$0,1,\ldots,n-2$
2	n	$G(m,p,n)$ $m>1,\ n>1,\ p\mid m$ ($G(2,2,2)$ is reducible)	$m^n n!/p$	$2^{mn(n-1)/2},\ d^{n\phi(d)}$ $(d\mid m/p,\ d>1)$	$m,2m,\ldots,(n-1)m;$ mn/p	$0,m,\ldots,(n-1)m$ if $p<m$; $0,m,\ldots,(n-2)m,$ $(n-1)m-n$ if $p=m$
3	1	Cyclic group $G(m,1,1)=\mathbf{Z}_m$	m	$d^{\phi(d)}$ $(d\mid m,d>1)$	m	0
4	2	$\mathbf{Z}_2.T=3[3]3$	24	3^8	4,6	0,2
5	2	$\mathbf{Z}_6.T=3[4]3$	72	3^{16}	6,12	0,6
6	2	$\mathbf{Z}_4.T=3[6]2$	48	$2^6 3^8$	4,12	0,8
7	2	$\mathbf{Z}_{12}.T=\langle 3,3,3\rangle_2$	144	$2^6 3^{16}$	12,12	0,12
8	2	$\mathbf{Z}_4.O=4[3]4$	96	$2^6 4^{12}$	8,12	0,4
9	2	$\mathbf{Z}_8.O=4[6]2$	192	$2^{18} 4^{12}$	8,24	0,16
10	2	$\mathbf{Z}_{12}.O=4[4]3$	288	$2^6 3^{16} 4^{12}$	12,24	0,12
11	2	$\mathbf{Z}_{24}.O=\langle 4,3,2\rangle_{12}$	576	$2^{18} 3^{16} 4^{12}$	24,24	0,24
12	2	$\mathbf{Z}_2.O=\mathrm{GL}_2(\mathbf{F}_3)$	48	2^{12}	6,8	0,10
13	2	$\mathbf{Z}_4.O=\langle 4,3,2\rangle_2$	96	2^{18}	8,12	0,16
14	2	$\mathbf{Z}_6.O=3[8]2$	144	$2^{12} 3^{16}$	6,24	0,18
15	2	$\mathbf{Z}_{12}.O=\langle 4,3,2\rangle_6$	288	$2^{18} 3^{16}$	12,24	0,24
16	2	$\mathbf{Z}_{10}.I=5[3]5$	600	5^{48}	20,30	0,10
17	2	$\mathbf{Z}_{20}.I=5[6]2$	1200	$2^{30} 5^{48}$	20,60	0,40
18	2	$\mathbf{Z}_{30}.I=5[4]3$	1800	$3^{40} 5^{48}$	30,60	0,30
19	2	$\mathbf{Z}_{60}.I=\langle 5,3,2\rangle_{30}$	3600	$2^{30} 3^{40} 5^{48}$	60,60	0,60
20	2	$\mathbf{Z}_6.I=3[5]3$	360	3^{40}	12,30	0,18
21	2	$\mathbf{Z}_{12}.I=3[10]2$	720	$2^{30} 3^{40}$	12,60	0,48
22	2	$\mathbf{Z}_4.I=\langle 5,3,2\rangle_2$	240	2^{30}	12,20	0,28
23	3	$\mathrm{W(H_3)}=\mathbf{Z}_2\times\mathrm{PSL}_2(5)$, Coxeter	120	2^{15}	2,6,10	0,4,8
24	3	$\mathrm{W(J_3(4))}=\mathbf{Z}_2\times\mathrm{PSL}_2(7)$ Klein	336	2^{21}	4,6,14	0,8,10
25	3	$\mathrm{W(L_3)}=\mathrm{W(P_3)}=3^{1+2}.\mathrm{SL}_2(3)$ Hessian	648	3^{24}	6,9,12	0,3,6
26	3	$\mathrm{W(M_3)}=\mathbf{Z}_2\times 3^{1+2}.\mathrm{SL}_2(3)$ Hessian	1296	$2^9 3^{24}$	6,12,18	0,6,12
27	3	$\mathrm{W(J_3(5))}=\mathbf{Z}_2\times(\mathbf{Z}_3.\mathrm{Alt}(6))$ Valentiner	2160	2^{45}	6,12,30	0,18,24

Irreducible complex reflection groups.						
28	4	$W(F_4)=(SL_2(3)^*SL_2(3)).(\mathbf{Z}_2\times\mathbf{Z}_2)$ Weyl	1152	2^{12+12}	2,6,8,12	0,4,6,10
29	4	$W(N_4)=(\mathbf{Z}_4{}^*2^{1+4}).\mathrm{Sym}(5)$	7680	2^{40}	4,8,12,20	0,8,12,16
30	4	$W(H_4)=(SL_2(5)^*SL_2(5)).\mathbf{Z}_2$	14400	2^{60}	2,12,20,30	0,10,18,28
31	4	$W(EN_4)=W(O_4)=(\mathbf{Z}_4{}^*2^{1+4}).Sp_4(2)$	46080	2^{60}	8,12,20,24	0,12,16,28
32	4	$W(L_4)=\mathbf{Z}_3\times Sp_4(3)$	155520	3^{80}	12,18,24,30	0,6,12,18
33	5	$W(K_5)=\mathbf{Z}_2\times\Omega_5(3)=$ $\mathbf{Z}_2\times PSp_4(3)=\mathbf{Z}_2\times PSU_4(2)$	51840	2^{45}	4,6,10,12,18	0,6,8,12,14
34	6	$W(K_6)=\mathbf{Z}_3.\Omega_6^-(3).\mathbf{Z}_2$, Mitchell	39191040	2^{126}	6,12,18,24, 30,42	0,12,18,24, 30,36
35	6	$W(E_6)=SO_5(3)=O_6^-(2)=$ $PSp_4(3).\mathbf{Z}_2=PSU_4(2).\mathbf{Z}_2$ Weyl	51840	2^{36}	2,5,6,8, 9,12	0,3,4,6, 7,10
36	7	$W(E_7)=\mathbf{Z}_2\times Sp_6(2)$ Weyl	2903040	2^{63}	2,6,8,10, 12,14,18	0,4,6,8, 10,12,16
37	8	$W(E_8)=\mathbf{Z}_2.O_8^+(2)$ Weyl	696729600	2^{120}	2,8,12,14, 18,20,24,30	0,6,10,12, 16,18,22,28

For more information, including diagrams, presentations, and codegrees of complex reflection groups, see the tables in [2].

Chapter 2

Simple Lie algebras

In this chapter I introduce the general concept of complex Lie algebra, and then investigate the specific properties of the *semisimple* Lie algebras. These include the *simple* Lie algebras for which I show, in essential lines, the steps for getting their classification, following directly from the one of the irreducible *root systems*. For references see [11], [12], [9] and [23].

Throughout, all vector spaces (so, in particular, Lie algebras) are always intended finite-dimensional over $\mathbb{C}$.

2.1 Basic concepts

Definition 2.1.1. A *(complex) Lie algebra* $\mathfrak{g}$ is a vector space over $\mathbb{C}$ endowed with a *bilinear* operation

$$\begin{aligned} [\ ,\ ]\colon \mathfrak{g} \times \mathfrak{g} &\longrightarrow \mathfrak{g} \\ (x, y) &\longmapsto [x, y] \end{aligned}$$

called *bracket* or *commutator*, verifying the axioms:

(L_1) $[x, x] = 0$ for all $x \in \mathfrak{g}$;

(L_2) $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ for all $x, y, z \in \mathfrak{g}$ (*Jacobi identity*).

The equivalence of (L_1) and

$$(L_1') \ \ [x, y] = -[y, x] \text{ for all } x, y \in \mathfrak{g}$$

immediately follows, from bilinearity, by

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

When $[x, y] = 0$ for all $x, y \in \mathfrak{g}$, the structure is called *abelian*.

Throughout $\mathfrak{g}$ will always denote a Lie algebra.

Remark 2.1.2 (Structure constants)**.** Let $\{x_1, \dots, x_n\}$ be a basis of $\mathfrak{g}$ and consider two elements $a = \sum_{i=1}^{n} a_i x_i$, $b = \sum_{j=1}^{n} b_j x_j$. From bilinearity of commutator it follows

$$[a, b] = \sum_{i=1}^{n} \sum_{j=1}^{n} a_i b_j [x_i, x_j]$$

On the other hand

$$[x_i, x_j] = \sum_{k=1}^{n} c_{ij}^k x_k$$

Then

$$[a, b] = \sum_{i=1}^{n} \sum_{j=1}^{n} a_i b_j c_{ij}^k x_k$$

In other words, the commutator is defined when the n^3 *structure constants* c_{ij}^k relative to the basis $\{x_1, \dots, x_n\}$ of $\mathfrak{g}$ are given. By the axioms $(L_1), (L_2)$, they satisfy the relations:

$$c_{ii}^k = 0 = c_{ij}^k + c_{ji}^k$$

$$\sum_{k=1}^{n} (c_{ij}^k c_{kl}^m + c_{jl}^k c_{ki}^m + c_{li}^k c_{kj}^m) = 0$$

Definition 2.1.3. A subspace A of $\mathfrak{g}$ such that

$$[x, y] \in A$$

for all $x, y \in A$ is called a *subalgebra* of $\mathfrak{g}$.

Definition 2.1.4. The smallest subalgebra including $X \subset \mathfrak{g}$ is called the subalgebra *generated* by X.

We can note that, owing to (L_1), every $x \in \mathfrak{g}$ defines a subalgebra with trivial commutator.

Example 2.1.5. Let V be a vector space of dimension n, and consider the set $\mathrm{End}(V)$ of linear trasformations $V \to V$. $\mathrm{End}(V)$ is a vector space of dimension n^2, and becomes a Lie algebra with the new operation given by $[a, b] = ab - ba$ for all $a, b \in \mathrm{End}(V)$. It is called the *general linear algebra* and denoted by $\mathfrak{gl}(V)$. Every subalgebra of $\mathfrak{gl}(V)$ is called a *linear Lie algebra*. An important example of linear Lie algebra is given by

$$\mathfrak{sl}(V) := \{a \in \mathfrak{gl}(V) \mid \mathrm{Tr}(a) = 0\}$$

called the *special linear algebra*.

Definition 2.1.6. Let $\mathfrak{g}$ and $\mathfrak{g}'$ be Lie algebras. A linear transformation $\phi : \mathfrak{g} \to \mathfrak{g}'$ such that
$$[\phi(x), \phi(y)] = \phi([x, y])$$
for all $x, y \in \mathfrak{g}$ is called a *homomorphism.*

The homomorphism ϕ is called a *monomorphism* if it is injective (or, what is the same, $\mathrm{Ker}(\phi) = 0$), an *epimorphism* if its image is $\mathfrak{g}'$, an *isomorphism* if it is invertible. If there exists an isomorphism between $\mathfrak{g}$ and $\mathfrak{g}'$ the two Lie algebras are called *isomorphic.* An isomorphism of a Lie algebra $\mathfrak{g}$ onto itself is called an *automorphism* of $\mathfrak{g}$. The set of all the automorphisms of $\mathfrak{g}$ with respect to the function composition is a group, denoted by $\mathrm{Aut}(\mathfrak{g})$.

Example 2.1.7. Relatively to any fixed basis of V, $\mathfrak{gl}(V)$ is canonically isomorphic to the Lie algebra $\mathfrak{gl}(n, \mathbb{C})$ consisting of the vector space $M_n(\mathbb{C})$ of the matrices $n \times n$ over $\mathbb{C}$ endowed with the commutator given by
$$[a, b] := ab - ba$$
for all $a, b \in M_n(\mathbb{C})$. In the same way, an isomorphism between $\mathfrak{sl}(V)$ and a certain matrix Lie algebra $\mathfrak{sl}(n, \mathbb{C})$ follows.

Definition 2.1.8. A subspace I of a Lie algebra $\mathfrak{g}$ such that
$$[x, y] \in I$$
for all $x \in \mathfrak{g}$ and for all $y \in I$ is called an *ideal* of $\mathfrak{g}$.

$\mathfrak{g}$ and 0 are trivial examples of ideals of $\mathfrak{g}$. A less trivial example is given by the *centre* $Z(\mathfrak{g}) := \{z \in \mathfrak{g} \mid [x, z] = 0 \text{ for all } x \in \mathfrak{g}\}$.

Definition 2.1.9. Let I, J ideals of $\mathfrak{g}$.
$$I + J := \{i + j \in \mathfrak{g} \mid i \in I, j \in J\}$$
is called the *sum* of I and J.

Definition 2.1.10. Let I, J ideals of $\mathfrak{g}$. The set $[I, J]$ of all linear combinations of commutators $[i, j]$ with $i \in I$ and $j \in J$ is called the *commutator* of I and J. In particular, $[\mathfrak{g}, \mathfrak{g}]$ is called the *derived algebra* of $\mathfrak{g}$.

Remark 2.1.11. It is straightforward to see that $[\mathfrak{g}, \mathfrak{g}] = 0$ means $\mathfrak{g}$ to be abelian.

Proposition 2.1.12. *$[I, J]$ and $I + J$ are ideals of $\mathfrak{g}$.*

Definition 2.1.13. A Lie algebra $\mathfrak{g}$ is called *simple* if $[\mathfrak{g}, \mathfrak{g}] \neq 0$ and its only ideals are the trivial ones.

The introduction of ideals allows us to define direct sum and quotient structure for Lie algebras.

Definition 2.1.14. A Lie algebra $\mathfrak{g}$ is said to be *direct sum* of ideals $I_1, \dots, I_t$ when it is $\mathfrak{g} = I_1 \oplus \cdots \oplus I_t$ as direct sum of subspaces.

Remark 2.1.15. When $\mathfrak{g} = I_1 \oplus \cdots \oplus I_t$, necessarily $[I_i, I_j] \subset I_i \cap I_j$ if $i \neq j$.

Definition 2.1.16. Let I be an ideal of a Lie algebra $\mathfrak{g}$. The (partition) set

$$\mathfrak{g}/I := \{x + I \mid x \in \mathfrak{g}\}$$

endowed with the (well defined) operations:

1. $(x + I) + (y + I) := (x + y) + I$ for all $x, y \in \mathfrak{g}$
2. $\alpha(x + I) := \alpha x + I$ for all $x \in \mathfrak{g}$, for all $\alpha \in \mathbb{C}$
3. $[x + I, y + I] := [x, y] + I$ for all $x, y \in \mathfrak{g}$

is a Lie algebra, called the *quotient algebra* of $\mathfrak{g}$ on I.

To any ideal I of $\mathfrak{g}$ the *canonical map*

$$\begin{aligned} \pi\colon \mathfrak{g} &\longrightarrow \mathfrak{g}/I \\ x &\longmapsto x + I \end{aligned}$$

is associated. It is straightforward to see that π is an epimorphism.

Lemma 2.1.17. *Let $\phi : \mathfrak{g} \to \mathfrak{g}'$ be a homomorphism. Then* $\mathrm{Ker}(\phi)$ *is an ideal of* $\mathfrak{g}$ *and* $\mathrm{Im}(\phi)$ *is a subalgebra of* $\mathfrak{g}'$

Also for Lie algebras, standard results about homomorphisms hold.

Theorem 2.1.18. *Let $\phi : \mathfrak{g} \to \mathfrak{g}'$ an homomorphism. Then* *(a)* $\mathfrak{g}/\mathrm{Ker}(\phi) \simeq \mathrm{Im}(\phi)$*. Moreover, if* I *is an ideal of* $\mathfrak{g}$ *included in* $\mathrm{Ker}(\phi)$*, there exists a unique homomorphism* $\psi : \mathfrak{g}/I \to \mathfrak{g}'$ *such that* $\phi = \psi \circ \pi$*.*

(b) If I *and* J *are ideals of* $\mathfrak{g}$ *and* $I \subset J$*, then* J/I *is an ideal of* $\mathfrak{g}/I$ *and* $(\mathfrak{g}/I)/(J/I)$ *is naturally isomorphic to* $\mathfrak{g}/J$*.*

(c) If I, J *are ideals of* $\mathfrak{g}$*, then* $(I + J)/J \simeq I/(I \cap J)$*.*

Now, another important notion.

Definition 2.1.19. Let $\mathfrak{g}$ be a Lie algebra and V a vector space. A homomorphism $\phi : \mathfrak{g} \to \mathfrak{gl}(V)$ is called a *representation* of $\mathfrak{g}$.

Let $x \in \mathfrak{g}$ and consider the map

$$\begin{aligned} \mathrm{ad}_{\mathfrak{g}}x \colon \mathfrak{g} &\longrightarrow \mathfrak{g} \\ y &\longmapsto [x, y] \end{aligned}$$

By the Jacoby identity, $\mathrm{ad}_{\mathfrak{g}}x \in \mathfrak{gl}(\mathfrak{g})$. Moreover, the consequent map

$$\begin{aligned} \mathrm{ad}_{\mathfrak{g}} \colon \mathfrak{g} &\longrightarrow \mathfrak{gl}(\mathfrak{g}) \\ x &\longmapsto \mathrm{ad}_{\mathfrak{g}}x \end{aligned}$$

is a homomorphism.

$\mathrm{ad}_{\mathfrak{g}}$ is called the *adjoint representation* of $\mathfrak{g}$, and it's easy to check that $\mathrm{Ker}(\mathrm{ad}_{\mathfrak{g}}) = Z(\mathfrak{g})$. From Theorem 2.1.18 (a), if $Z(\mathfrak{g}) = 0$ (as in simple Lie algebras) then $\mathfrak{g}$ is isomorphic to a linear algebra.

Actually we know that every complex Lie algebra is isomorphic to some linear algebras (and then to some matrix Lie algebras) for a general theorem due to Ado and Iwasawa.

I conclude this section by giving two further notions.

Definition 2.1.20. Let $\mathfrak{g}$ be a Lie algebra and K a subspace of $\mathfrak{g}$. The set

$$N_{\mathfrak{g}}(K) := \{x \in \mathfrak{g} \mid [x, K] \subset K\}$$

is called the *normaliser* of K in $\mathfrak{g}$.

By the Jacobi identity, $N_{\mathfrak{g}}(K)$ is a subalgebra of $\mathfrak{g}$; it is the largest subalgebra of $\mathfrak{g}$ contained K as ideal when K is a subalgebra.

Every subspace (in particular, subalgebra) $K = Z_{\mathfrak{g}}(K)$ is called *self-normalsing.*

Definition 2.1.21. For any subset X of a Lie algebra $\mathfrak{g}$

$$C_{\mathfrak{g}}(X) := \{x \in \mathfrak{g} \mid [x, X] = 0\}$$

is called the *centraliser* of X in $\mathfrak{g}$.

Again by the Jacobi identity, $C_{\mathfrak{g}}(X)$ is a subalgebra of $\mathfrak{g}$. It is straightforward to see that $Z(\mathfrak{g}) = C_{\mathfrak{g}}(\mathfrak{g})$.

Definition 2.1.22. An element x of a Lie algebra $\mathfrak{g}$ is called *regular* if the dimension of $C_{\mathfrak{g}}(x) := C_{\mathfrak{g}}(\{x\})$ is minimal among all centralisers of elements in $\mathfrak{g}$.

2.2 Semisimple Lie algebras

Let $\mathfrak{g}$ be a Lie algebra and consider the sequence of ideals recursively defined by:

- $\mathfrak{g}^{(1)} = \mathfrak{g}$;
- $\mathfrak{g}^{(n)} = [\mathfrak{g}^{(n-1)}, \mathfrak{g}^{(n-1)}]$ for $n > 1$

and called the *derived series* of $\mathfrak{g}$.

Definition 2.2.1. $\mathfrak{g}$ is said to be *solvable* if $\mathfrak{g}^{(n)} = 0$ for some n.

Proposition 2.2.2. *The following statements hold.*

(a) If $\mathfrak{g}$ is solvable, then so are all subalgebras and homomorphic images of $\mathfrak{g}$.

(b) If I is a solvable ideal of $\mathfrak{g}$ such that $\mathfrak{g}/I$ is solvable, then $\mathfrak{g}$ itself is solvable.

(c) If I, J are solvable ideals of $\mathfrak{g}$, then so is $I + J$.

Corollary 2.2.3. *There exists a unique maximal solvable ideal of $\mathfrak{g}$.*

The above ideal is called the *radical* of $\mathfrak{g}$. It is denoted by $\mathrm{Rad}(\mathfrak{g})$.

Definition 2.2.4. $\mathfrak{g}$ is called a *semisimple Lie algebra* if $\mathrm{Rad}(\mathfrak{g}) = 0$

We can note that every simple Lie algebra $\mathfrak{g}$ is semisimple. Indeed, the only ideals of $\mathfrak{g}$ are $\mathfrak{g}$ itself and 0, while $\mathfrak{g}$ is not solvable by definition ($\mathfrak{g}^1 \neq 0$ and then $\mathfrak{g}^{(n)} = \mathfrak{g}$ for all n, for $\mathfrak{g}$ being the only non-zero ideal of $\mathfrak{g}$).

Definition 2.2.5. Let $\mathfrak{g}$ be any Lie algebra. The map

$$\begin{aligned} \kappa\colon \mathfrak{g} \times \mathfrak{g} &\longrightarrow \mathbb{C} \\ (x, y) &\longmapsto \mathrm{Tr}(\mathrm{ad}_{\mathfrak{g}} x \; \mathrm{ad}_{\mathfrak{g}} y) \end{aligned}$$

is a symmetric bilinear form on $\mathfrak{g}$, called *Killing form*.

Lemma 2.2.6. *κ is associative (i.e., $\kappa([x,y],z) = \kappa(x,[y,z])$). Moreover, for any ideal I of $\mathfrak{g}$ it results $\kappa_I = \kappa_{|I\times I}$.*

In general, a bilinear form $\beta(x,y)$ on $\mathfrak{g}$ is called *nondegenerate* if its *radical* S is 0, where $S := \{x \in \mathfrak{g} \mid \beta(x,y) = 0 \text{ for all } y \in \mathfrak{g}\}$.

Semisimple Lie algebras are related to the Killing form and to simple ideals by the following results.

Theorem 2.2.7. *A Lie algebra is semisimple if, and only if, its Killing form is nondegenerate.*

Theorem 2.2.8. *Let $\mathfrak{g}$ be semisimple. Then there exist ideals $I_1,\dots,I_t$ of $\mathfrak{g}$ which are simple (as Lie algebras), such that $\mathfrak{g} = I_1 \oplus \cdots \oplus I_t$. Every simple ideal of $\mathfrak{g}$ coincides with one of the I_i. Moreover, the Killing form of I_i is the restriction of κ to $I_i \times I_i$.*

Corollary 2.2.9. *If $\mathfrak{g}$ is semisimple, then $\mathfrak{g} = [\mathfrak{g},\mathfrak{g}]$, and all ideals and homomorphic images of $\mathfrak{g}$ are semisimple. Moreover, each ideal of $\mathfrak{g}$ is a sum of certain simple ideals of $\mathfrak{g}$.*

2.3 Abstract Jordan decomposition

Definition 2.3.1. Let V be a finite dimensional vector space (over $\mathbb{C}$), $\mathrm{End}(V)$ the vector space of linear transformations $V \to V$, $a \in \mathrm{End}(V)$. Then a is said to be *semisimple* if it is diagonalizable, i.e., $\mathfrak{g}$ admits a basis of eigenvectors of a. $\mathfrak{g}$ is instead said to be *nilpotent* if $a^n = 0$ for some $n \in \mathbb{N}$.

Consider now a semisimple Lie algebra $\mathfrak{g}$. I recall that $\mathrm{ad}_{\mathfrak{g}} x \in \mathfrak{gl}(V)$ for all $x \in \mathfrak{g}$. The following result holds.

Proposition 2.3.2. *Let $x \in \mathfrak{g}$. There are unique $x_s, x_n \in \mathfrak{g}$ satisfying the conditions:*

- $\mathrm{ad}_{\mathfrak{g}} x = \mathrm{ad}_{\mathfrak{g}} x_s + \mathrm{ad}_{\mathfrak{g}} x_n$,
- $\mathrm{ad}_{\mathfrak{g}} x_s$ *semisimple,*
- $\mathrm{ad}_{\mathfrak{g}} x_n$ *nilpotent,*
- $[x_s, x_n] = 0$.

x_s and x_n are respectively called the *semisimple part* and the *nilpotent part* of x.

Remark 2.3.3. When $\mathfrak{g}$ is a linear Lie algebra, every $x \in \mathfrak{g}$ is semisimple (resp. nilpotent) if, and only if, $\mathrm{ad}_{\mathfrak{g}} x$ is semisimple (resp. nilpotent) in the sense of a linear transformation. So, in any case, the following definition doesn't present ambiguity of interpretation.

Definition 2.3.4. Let $\mathfrak{g}$ be a Lie algebra and $x \in \mathfrak{g}$. x is said to be *semisimple* (resp. *nilpotent*) if $\mathrm{ad}_{\mathfrak{g}}x$ is semisimple (resp. nilpotent).

Remark 2.3.5 (Nilpotent Lie algebras)**.** A particular class of solvable Lie algebras is given by the *nilpotent* Lie algebras, characterised by having all the elements nilpotent.

2.4 Root spaces decomposition

In the sequel, except when explicitally declared, Lie algebras are always intended to be semisimple.

Definition 2.4.1. A subalgebra of $\mathfrak{g}$, only consisting of semisimple elements, is called *toral*.

If $\mathfrak{g}$ is non-nilpotent, then it admits an element x whose semisimple part x_s is nonzero; so, the subspace spanned by x_s is a subalgebra (with trivial commutator) whose elements are all semisimple. Therefore there is always at least one toral subalgebra of $\mathfrak{g}$.

An important fact is given by

Proposition 2.4.2. *Every toral subalgebra is abelian.*

Definition 2.4.3. A maximal toral subalgebra of $\mathfrak{g}$ is called a *Cartan subalgebra*.

Remark 2.4.4. For any Lie algebra $\mathfrak{g}$ (not necessarily semisimple) a *Cartan subalgebra* is defined as a nilpotent, self-normalised subalgebra of $\mathfrak{g}$. However, in the case of semisimple Lie algebras the two definitions are equivalent.

Proposition 2.4.5. *Two Cartan subalgebras of the same Lie algebra are conjugated under the automorphism group* $\mathrm{Aut}(\mathfrak{g})$*.*

Proposition 2.4.6. *For any Cartan subalgebra* $\mathfrak{h}$ *of* $\mathfrak{g}$ *results* $C_{\mathfrak{g}}(\mathfrak{h}) = \mathfrak{h}$*.*

Let $\mathfrak{h}$ be a Cartan subalgebra of $\mathfrak{g}$. As $\mathfrak{h}$ is abelian, the set $\mathrm{ad}_{\mathfrak{g}}\mathfrak{h}$ consists of commuting semisimple endomorphisms of $\mathfrak{g}$; so, according to a standard result in linear algebra, $\mathrm{ad}_{\mathfrak{g}}\mathfrak{h}$ is *simultaneously diagonalizable*. In other words, $\mathfrak{g}$ is the direct sum of the subspaces

$$\mathfrak{g}_\alpha = \{x \in \mathfrak{g} \mid [h,x] = \alpha(h)x \text{ for all } h \in \mathfrak{g}\}$$

where α ranges over $\mathfrak{h}^*$. Every $\mathfrak{g}_\alpha$ is called the *root space* of α.

We can note that $\mathfrak{g}_0$ coincides with $C_{\mathfrak{g}}(\mathfrak{h})$ and then with $\mathfrak{h}$ for the last proposition. The set of all nonzero $\alpha \in \mathfrak{h}^*$ for which $\mathfrak{g}_\alpha \neq 0$ is denoted by Φ; the elements of Φ are called the *roots* of $\mathfrak{g}$ relative to $\mathfrak{h}$; they are finite in number. In this way, we have a *root space decomposition* (or *Cartan decomposition*):

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha\in\Phi} \mathfrak{g}_\alpha$$

Proposition 2.4.7. *The restriction of the Killing form to* $\mathfrak{h}$ *is nondegenerate.*

The last proposition allows to identify $\mathfrak{h}$ with $\mathfrak{h}^*$ by mapping $\mu \in \mathfrak{h}^*$ to the unique elements $\hat{\mu} \in \mathfrak{h}$ satisfying $\kappa(h, \hat{\mu}) = \mu(h)$ for all $h \in \mathfrak{h}$. Using this bijection, κ induces a non-degenerate bilinear form $(\ , \ )$ on $\mathfrak{h}^*$. For $\mu \in \mathfrak{h}^*$ we set

$$\mu^\vee = \frac{2\hat{\mu}}{(\mu, \mu)}$$

Before going on I recall some general notions that will be fundamental in the sequel.

Definition 2.4.8. We call *euclidean vector space* E a finite dimensional vector space over $\mathbb{R}$ endowed with a positive definite symmetric bilinear form $(\ , \ )$ called *inner product*.

Definition 2.4.9. $a, b \in E$ are said to be *ortogonal* if $(a, b) = 0$.

Definition 2.4.10. An invertible linear transformation of a euclidean vector space E, leaving pointwise fixed some *hyperplane* (subspace of codimension one) and sending any vector orthogonal to that hyperplane into its negative, is called a *reflection* in E.

Evidently a reflection is *ortogonal*, i.e., preserves the inner product on E. Any nonzero vector α determines a reflection σ_α, with *reflecting hyperplane* $P_\alpha := \{\beta \in E \mid (\beta, \alpha) = 0\}$. Certainly, nonzero vectors proportional to α yield the same reflection. Finally, we have the explicit formula:

$$\sigma_\alpha(\beta) = \beta - \frac{2(\beta, \alpha)}{(\alpha, \alpha)}\alpha$$

for all $\beta \in E$. In order to abbreviate we put

$$\langle \beta, \alpha^\vee \rangle := \frac{2(\beta, \alpha)}{(\alpha, \alpha)}$$

Definition 2.4.11. Let E be an euclidean vector space and $\Psi \subset E$, verifying the following properties:

(a) Ψ is finite, spans E, and does not contains 0.

(b) If $\alpha \in \Psi$ the only multiples of α in Ψ are $\pm\alpha$.

(c) If $\alpha \in \Psi$, the reflection σ_α leaves Ψ invariant.

(d) If $\alpha, \beta \in \Psi$, then $\langle \beta, \alpha^\vee \rangle \in \mathbb{Z}$

The pair (Ψ, E) is called a *root system.*

Now, let's turn to $\mathfrak{h}$ and $\mathfrak{h}^*$.

Proposition 2.4.12. *Let* $\mathrm{E}_\mathbb{Q}$ *be the* $\mathbb{Q}$*-subspace of* $\mathfrak{h}^*$ *spanned by all the roots. Then*

1. $\mathrm{E}_\mathbb{Q}$ *has the same dimension of* $\mathfrak{h}^*$ *over* $\mathbb{C}$.
2. $(\alpha, \beta) \in \mathbb{Q}$ *for all* $\alpha, \beta \in \mathrm{E}_\mathbb{Q}$*. So* $(\ ,\ )$ *is also a form on* $\mathrm{E}_\mathbb{Q}$.
3. $(\ ,\ )$ *on* $\mathrm{E}_\mathbb{Q}$ *is positive definite.*

Now let E be the real vector space E obtained by extending the base field from $\mathbb{Q}$ to $\mathbb{R}$, i.e., $\mathrm{E} := \mathbb{R} \otimes_\mathbb{Q} \mathrm{E}_\mathbb{Q}$. The form $(\ ,\ )$ on $\mathrm{E}_\mathbb{Q}$ canonically extended to E is positive definite too. We conclude that E is a euclidean vector space.

Theorem 2.4.13. *Let* $\mathfrak{g}, \mathfrak{h}, \Psi, \mathrm{E}$ *be as above. Then* (Ψ, E) *is a root system.*

Theorem 2.4.14. *The correspondence* $(\mathfrak{g}, \mathfrak{h}) \mapsto (\Psi, \mathrm{E})$ *is 1 - 1. Moreover, different choices of Cartan subalgebras bring to root systems that are isomorphic (see next section).*

Root systems (and then, as we will see, all simple Lie algebras) are completely classified in next section.

2.5 Root systems

Let (Ψ, E) (or simply Φ if it is implicit the referred space E) be a *root system* (see Definition 2.4.11). We say that the *rank* of (Ψ, E) is l if $\dim(E) = l$.

Proposition 2.5.1. *Let* (Ψ, E) *be a root system and* $\alpha \in \Psi$*. Then the reflection* s_α *is a permutation of* Ψ*.*

Let (Ψ, E) be a root system and suppose that $\Psi = \Psi_1 \cup \Psi_2$ with $(\alpha_1, \alpha_2) = 0$ for all $\alpha_1 \in \Psi_1$ and $\alpha_2 \in \Psi_2$. Let $W_i \subset E_i$ be the subspace of E_i spanned by Ψ_i $(i = 1, 2)$. It is straightforward to verify that Ψ_i is a root system in W_i. Then (Ψ, E) is called *direct sum* of (Ψ_1, W_1) and (Ψ_2, W_2).

Definition 2.5.2. A root system is said to be *irreducible* if it is not direct sum of two other root systems.

Definition 2.5.3. The root systems (Ψ_1, E_1) e (Ψ_2, E_2) are said to be *isomorphic* if there exists a bijective linear map $f : E_1 \to E_2$ with $f(\Psi_1) = \Psi_2$ and $\langle \alpha, \beta^\vee \rangle = \langle f(\alpha), f(\beta)^\vee \rangle$, for all $\alpha, \beta \in \Psi_1$. In this case we write $(\Psi_1, E_1) \simeq (\Psi_2, E_2)$ (or $\Psi_1 \simeq \Psi_2$).

The following theorem is very important for allowing to classify all simple Lie algebras from the classification of irreducible root system.

Theorem 2.5.4. *The root system of any simple Lie algebra is irreducible. Conversely, for any irreducible root system Ψ there exist a simple Lie algebra having Ψ as own root system.*

Let (Ψ, E) be now a root system. Since Ψ spans E, we can select, in many ways, a subset $\Delta \in \Psi$ that is a basis of E. We focus our attention to so-called *root bases*, having rather convenient properties.

Definition 2.5.5. Let $<$ a partial order on E. We say that $(E, <)$ is a *root order* if the following properties hold:

1. every root $\alpha \in \Psi$ is comparable to zero (i.e., either $\alpha < 0$ or $\alpha > 0$),
2. if $v \in E$ is such that $v > 0$, then for $\lambda \in \mathbb{R}$ then $\lambda v < 0$ if $\lambda < 0$ and $\lambda v > 0$ if $\lambda > 0$,
3. if $u, v \in E$ and $u < v$ then $u + w < v + w$ for all $w \in E$.

Example 2.5.6. To give an example (and, contestually, to prove the existence) of a root order in any given root system (E, Ψ), let choose a basis $\{v_1, \ldots v_n\}$ of E. So, any $v \in E$ can be written as a linear combination:

$$\sum_{i=1}^{l} \lambda_i v_i \quad \text{where } \lambda_1, \ldots, \lambda_n \in \mathbb{R}.$$

We set $v > 0$ if the first non-zero λ_i is positive. Also, for $v, w \in E$ we set $v > w$ if $v - w > 0$. We have that $>$ is a total order on E and it is clearly a root order. We call $<$ the *lexicographical order* relative to $v_1, \ldots, v_n$.

Let $<$ be now a root order in (E, Ψ). The root $\alpha \in \Psi$ is said to be *positive* if $\alpha > 0$, and *negative* if $\alpha < 0$. By Ψ^+ we denote the set of positive roots and by Ψ^- the set of negative roots. Since roots are either positive or negative, $\Psi = \Psi^+ \cup \Psi^-$. Note that $\Psi^- = -\Psi^+$.

Definition 2.5.7. A root α is said to be *simple* if it is positive and it is not sum of other two positive roots.

Proposition 2.5.8. *Let $\Delta = \{\alpha_1, \dots, \alpha_l\}$ be the set of simple roots. Let β be a root and write $\beta = \sum_{i=1}^{l} k_i \alpha_i$. Thet k_i is an integer for $1 \le i \le l$ and either all $k_i \ge 0$ or all $k_i \le 0$.*

Δ is then a basis of E, called the *root basis* relative to $<$ of the root system Ψ. We can note that Ψ has no unique root basis, depending the simpleness of a roots on the choice of the root order and, in general, two different root orders determine two different root bases. However, the statement of the last proposition does characterises the root bases in the sense of the following result.

Proposition 2.5.9. *Let $\alpha_1, \dots, \alpha_l \in \Psi$, where l is the rank of Ψ, be such that every element of Ψ can be written as a $\mathbb{Z}$-linear combination of the α_i such that the coefficients are either all non-negative or all non-positive. Then there exists a root order $<$ such that $\{\alpha_1, \dots, \alpha_l\}$ is the root basis of Ψ relative to $<$.*

Definition 2.5.10. Let $\Delta = \{\alpha_1, \dots, \alpha_l\}$ be a root basis. An element $\lambda \in E$ is called a *weight* if $\langle \lambda, \alpha_i^\vee \rangle \in \mathbb{Z}$ for all $1 \le i \le l$.

Definition 2.5.11. Let β be a positive root and write β as an integral linear combination of simple roots,

$$\sum_{i=1}^{l} k_i \alpha_i$$

where all $k_i \ge 0$. Then the number $\mathrm{ht}(\beta) = \sum_{i=1}^{l} k_i$ is called the *height* of β.

Definition 2.5.12. A $l \times l$ matrix C with entries in $\mathbb{Z}$ is called a *Cartan matrix* if

1. $C(i,i) = 2$ for $1 \le i \le l$,
2. $C(i,j) \le 0$ for $i \ne j$,
3. there is a matrix $D = \mathrm{diag}(d_1, \dots, d_l)$ with $d_i \in \mathbb{Z}_{>0}$, $\gcd(d_1, \dots, d_l) = 1$ such that $B = CD$ is a positive definite symmetric matrix.

Definition 2.5.13. Let C_1, C_2 Cartan matrices. We say that the they are *equivalent*, and write $C_1 \sim C_2$ if there exists a permutation σ of $\{1, \dots, l\}$ such that $C_1(i,j) = C_2(\sigma(i), \sigma(j))$.

Proposition 2.5.14. *Let* (Ψ, E) *a root system and* $\Delta = \{\alpha_1, \ldots, \alpha_l\}$ *a root basis. The matrix* $C = (\langle \alpha_i, \alpha_j^\vee \rangle)$ *is a Cartan matrix, called the Cartan matrix of* (Ψ, E) *relative to* Δ.

Proposition 2.5.15. *Let* E *a real euclidean space of dimension* l, $\Delta = \{\alpha_1, \ldots, \alpha_l\}$ *a basis of* E *and* C *a Cartan matrix. Then there exists an unique root system* $\Psi \subset E$ *having* Δ *as root basis and such that* $C = (\langle \alpha_i, \alpha_j^\vee \rangle)$.

The following fundamental result holds:

Proposition 2.5.16. *Let* $(\Psi_1, E_1), (\Psi_2, E_2)$ *be root system. Let* Δ_1 *and* Δ_2 *be root bases of respectively* Ψ_1 *and* Ψ_2 *and let* C_1 *and* C_2 *be their respective Cartan matrices. We have* $(\Psi_1, E_1) \simeq (\Psi_2, E_2)$ *if, and only if,* $C_1 \sim C_2$.

Remark 2.5.17. Let $\Psi = \Psi_1 \oplus \Psi_2$ be the direct sum of root systems Ψ_1 and Ψ_2, and $\Delta_1 = \{\alpha_1, \ldots, \alpha_m\}$, $\Delta_2 = \{\beta_1, \ldots, \beta_n\}$ root bases of Ψ_1 and Ψ_2 respectively. Then

$$\Delta = \{\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n\}$$

is a root basis of Ψ. Furthermore, the Cartan matrix of Ψ relative to Δ is

$$\begin{pmatrix} C_1 & 0 \\ 0 & C_2 \end{pmatrix}$$

Cartan matrices can be conveniently displayed by so-called *Dynkin diagrams*. Actually it is often much easier to work with these diagrams than with the corresponding matrices.

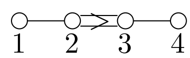
Lemma 2.5.18. *Let* C *be an* $l \times l$ *Cartan matrix. Let* $i \neq j$*; then* $C(i,j)C(j,i) = 0, 1, 2, 3$. *Furthermore, if* $C(i,j)C(j,i) \neq 0$ *then at least one of* $C(i,j), C(j,i)$ *is* -1.

Let C be a Cartan matrix. We define the *Dynkin diagram* of C to be the graph on l points with labels $1, \ldots, l$.Two points i and j are connected by $C(i,j)C(j,i) = 0, 1, 2, 3$ lines. If this number is > 0 then we put an arrow towards j if $|C(i,j)| > 1|$, and we put an arrow towards i if $|C(j,i)| > 1$.

Example 2.5.19. Let

$$C = \begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -2 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix}$$

Then the Dynkin diagram of C is



Let us show now that from the Dynkin diagram it can be recovered the Cartan matrix. Let $i \neq j \in \{1, \ldots, l\}$ and k be the numbers of lines connecting ii and j in the Dynkin diagram. If $k = 0$, then $C(i,j) = C(j,i) = 0$, and if $k = 1$, then $C(i,j) = C(j,i) = -1$. If $k \geq 2$, then there is an arrow. Suppose that the arrow points towards j. Then $C(i,j) = -k$ and $C(j,i) = -1$. So, from the Dynkin diagram we can determine the off-diagonal elements of the Cartan matrix. The conclusion is that the Dynkin diagrams determines the Cartan matrix.

Lemma 2.5.20. *Let Ψ be a root system with Dynkin diagram D. Then Ψ is the direct sum of Ψ_1 and Ψ_2 if, and only if, D can be decomposed as the union of two components D_1 and D_2 that are not connected and such that D_i is the Dynkin diagram of Ψ_i for $i = 1, 2$.*

The classification of all possible Dynkin diagrams, allows to classify all possible root system. From the previous lemma it is clear that we may restrict our attention to connected Dynkin diangrams. In this way we classify all the irreducible root systems. All other root systems are direct sums of these.

Theorem 2.5.21. *All connected Dynkin diagrams belong to the following list:*

A_l :

B_l :

C_l :

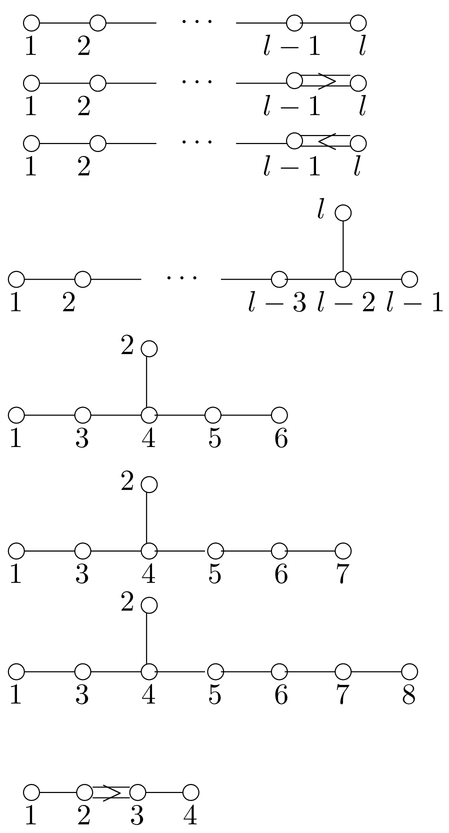
D_l :

E_6 :

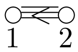
E_7 :

E_8 :

F_4 :



G_2 :



I conclude this section by giving a further notion.

Definition 2.5.22. The subgroup of $\mathrm{Aut}(E)$ generated by the set of reflections $\{s_\alpha : E \to E \mid \alpha \in \Psi\}$ is called the *Weyl group* of the root system (Ψ, E). It is usually denoted by $W(\Psi)$, or simply W if it is clear the root system of reference.

Theorem 2.5.23. $W(\Psi) = \Psi$

Corollary 2.5.24. *W is a finite group.*

2.6 Automorphisms

Let $\mathfrak{g}$ be a Lie algebra, and $x \in \mathfrak{g}$ a nilpotent element. Said $n \in \mathbb{N}$ such that $(\mathrm{ad}_{\mathfrak{g}} x)^n = 0$, we can define the *exponential* of $\mathrm{ad}_{\mathfrak{g}} x$ as

$$\exp(\mathrm{ad}_{\mathfrak{g}} x) := 1 + \mathrm{ad}_{\mathfrak{g}} x + (\mathrm{ad}_{\mathfrak{g}} x)^2/2! + \ldots + (\mathrm{ad}_{\mathfrak{g}} x)^{n-1}/(n-1)!$$

An important fact is that $\exp(\mathrm{ad}_{\mathfrak{g}} x) \in \mathrm{Aut}(\mathfrak{g})$. This allows the following

Definition 2.6.1. The elements of the subgroup of $\mathrm{Aut}(\mathfrak{g})$ generated by the set of all the exponentials of nilpotent maps $\mathrm{ad}_{\mathfrak{g}} x$ are called the *inner automorphisms* of $\mathfrak{g}$. The group of the inner automorphisms of $\mathfrak{g}$ is denoted by $\mathrm{Int}(\mathfrak{g})$.

An automorphism that is not inner, is said to be an *outer* automorphism.

Proposition 2.6.2. $\mathrm{Int}(\mathfrak{g}) \lhd \mathrm{Aut}(\mathfrak{g})$.

Let $\mathfrak{g}$ be a semisimple Lie algebra and $\mathfrak{h}$ a Cartan subalgebra. Consider then the root system Φ of $\mathfrak{h}^*$ and let $\Delta = \{\alpha_1, \ldots \alpha_n\}$ be a root basis. We call a *canonical* set of generators of $\mathfrak{g}$ corresponding to Δ, a set of the elements $x_1, \ldots, x_n, y_1, \ldots, y_n, h_1, \ldots, h_n$, such that $x_i \in \mathfrak{g}_{\alpha_i}$, $y_i \in \mathfrak{g}_{-\alpha_i}$, the $h_i \in \mathfrak{h}$ form a basis of $\mathfrak{h}$ and

- $[h_i, h_j] = 0$
- $[x_i, y_j] = \delta_{ij} h_i$
- $[h_i, x_j] = \langle \alpha_j, \alpha_i^\vee \rangle x_j$
- $[h_i, y_j] = -\langle \alpha_j, \alpha_i^\vee \rangle y_j$

Lemma 2.6.3. *Let $\{\tilde{\alpha_1}, \ldots, \tilde{\alpha_l}\}$ be a basis of Φ and $\tilde{x}_i$ be a nonzero element of $\mathfrak{g}_{\tilde{\alpha}_i}$. Then there is a nonzero $\tilde{y}_i \in \mathfrak{g}_{-\tilde{\alpha}_i}$ such that, setting $\tilde{h}_i = [\tilde{x}_i, \tilde{y}_i]$, we have $[\tilde{h}_i, \tilde{x}_i] = 2\tilde{x}_i$. Moreover, the $\tilde{x}_i$, $\tilde{y}_i$, $\tilde{h}_i$ form a canonical set of generators of $\mathfrak{g}$.*

An automorphism of $\mathfrak{g}$ can be described by giving the images of the elements of a canonical set of generators. Conversely, given any canonical set of generators x'_i, y'_i, h'_i corresponding to Δ, the map sending x_i to x'_i, y_i to y'_i, h_i to h'_i is an automorphism of $\mathfrak{g}$.

Remark 2.6.4. Let $w \in W$; then

$$w(h_i) = w(\alpha_i^\vee) = w(\alpha_i)^\vee$$

. Let x'_i be a nonzero element of $g_{w(\alpha_i)}$, and let $y'_i \in g_{w(\alpha_i)}$ be such that $[[x'_i, y'_i], x'_i] = 2x'_i$. Set $h'_i = [x'_i, y'_i]$. Then by Lemma 2.6.3 the x'_i, y'_i, h'_i form a canonical generating set of $\mathfrak{g}$. Hence the map sending $x_i \mapsto x'_i$, $y_i \mapsto y'_i$, $h_i \mapsto h'_i$ extends to an automorphism σ_w of $\mathfrak{g}$. Moreover, $h'_i = w(\alpha_i^\vee) = w(h_i)$. Hence σ_w is an automorphism of $\mathfrak{g}$, stabilising $\mathfrak{h}$, and such that its restriction to $\mathfrak{h}$ coincides with w.

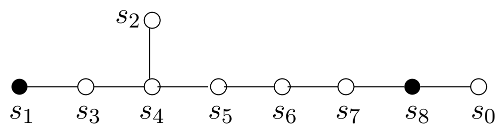
Let D be the Dynkin diagram of Φ with respect to Δ. We call *diagram automorphism* a $\phi \in \mathrm{Aut}(\mathfrak{g})$ inducing a permutation on Δ such that:

1. the number of lines connecting α_i and α_j in D is equal to the number of lines connecting $\phi(\alpha_i)$ and $\phi(\alpha_j)$,
2. if α_i and α_j are connected in D by more than one line then there is an arrow pointing from α_i to α_j if and only if the same is true for $\phi(\alpha_i)$ and $\phi(\alpha_j)$, for $1 \leq i, j \leq l$.

The conjugacy classes of the finite order automorphisms in $\mathrm{Aut}(\mathfrak{g})$ have been classified by Kac in terms of so-called *Kac diagrams* (see [13] [9]) which we are going to illustrate for inner and outer automorphisms. In any case, a black node means that the corresponding label (throughout denoted by s_i) is 1; a non-black node means that the corresponding lable is 0.

2.6.1 Kac diagrams of inner automorphisms

Let α_0 denote the lowest root of Φ. Then, the Dynkin diagram of the roots $\alpha_0, \alpha_1, \ldots, \alpha_n$ is called the *extended* Dynkin diagram of Φ (or of $\mathfrak{g}$). Let $n_i \in \mathbb{Z}$ be such that $\alpha_0 = -\sum_{i=i}^{l} n_i\alpha_i$ and set $n_0 = 1$. Let $s_0, \ldots, s_l$ be non-negative integers with $\gcd(s_0, \ldots, s_l) = 1$, and set $m = \sum_{i=0}^{l} n_i s_i$. Let $\omega \in \mathbb{C}$ be a primitive m-th root of unity. Let x_0 be a nonzero element of $\mathfrak{g}_{\alpha_0}$. Then $x_0, \ldots, x_l$ generate $\mathfrak{g}$. Moreover $x_i \mapsto \omega^{s_i} x_i$ $(1 \leq i \leq l)$ defines an inner automorphism of $\mathfrak{g}$, of order m. The *Kac diagram* of this automorphism is then the extended Dynkin diagram with labels $s_0, s_1 \ldots, s_l$. In terms of canonical generating set, the automorphism is given by $x_i \mapsto \omega^{s_i} x_i$, $y_i \mapsto \omega^{-s_i} x_i$, $h_i \mapsto h_i$ $(1 \leq i \leq l)$. An example of Kac diagram of (conjugacy class of) an inner automorphism of E_8 of order 4 follows.



2.6.2 Kac diagrams of outer automorphisms

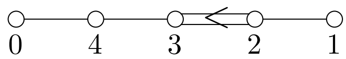
We restrict, for semplicity, to the simple Lie algebra of type E_6.

Let $\nu : \mathfrak{g} \to \mathfrak{g}$ a diagram automorphism (so, of order 2) and $\mathfrak{g}_0^\nu \oplus \mathfrak{g}_1^\nu$ the corresponding grading. Let then $\mathfrak{h}$ be a Cartan subalgebra of $\mathfrak{g}$ fixed by ν. Then:

$$\mathfrak{h}_0^\nu = \{h \in \mathfrak{h} \mid \nu(h) = h\}$$

is a Cartan subalgebra of $\mathfrak{g}_0^\nu$. Moreover $\mathfrak{g}_0^\nu$ is a simple Lie algebra (precisely, of type F_4). Let Ψ be a root system of $\mathfrak{g}_0^\nu$ corresponding to the Cartan subalgebra $\mathfrak{h}_0^\nu$ and $\Pi = \{\beta_1, \ldots, \beta_n\}$ a basis of simple roots. Let X_i, Y_i, H_i $(1 \leq i \leq n)$ be a canonical generating set of $\mathfrak{g}_0^\nu$.

$\mathfrak{g}_0^\nu$ acts on $\mathfrak{g}_1^\nu$. Let β_0 be the lowest weight of $\mathfrak{g}_1^\nu$ and let $X_0 \in (\mathfrak{g}_1^\nu)_{\beta_0}$, $X_0 \neq 0$. Let $(s_0, s_1, \ldots, s_n)$ be integers with $s_i \geq 0$ and $\gcd(s_0, s_1, \ldots, s_n) = 1$. The roots $\beta_0, \beta_1, \ldots, \beta_n$ have Dynkin diagram

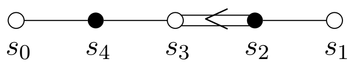


With $a_0 = 1$, $a_1 = 2$, $a_2 = 3$, $a_3 = 2$, $a_4 = 1$, we have $\sum_{i=0}^n a_i \beta_i = 0$.

Set $m = 2 \sum_{i=0}^n a_i s_i$, and let $\omega \in \mathbb{C}$ be a primitive m-th root of unity. Then:

- $X_0, X_1, \ldots, X_n$ generate $\mathfrak{g}$ and by $\sigma(X_i) = \omega^{s_i} X_i$ we uniquely define an automorphism of $\mathfrak{g}$ of order m.
- Every outer automorphism of $\mathfrak{g}$ of order m is obtained in this way (up to conjugation).

An example of Kac diagram of (conjugacy class of) an outer automorphism of E_6 of order 8 follows.



Chapter 3

Algebraic groups and θ-representations

In this chapter I introduce general notions of the theory of algebraic groups over $\mathbb{C}$, once presented the algebraic-geometrical context where these objects arise from. The notion of Lie algebra associated to an algebraic group, finally, lead me to introduce the so called θ-groups, about which my research is concerned. For references see [4], [20], [15], [22]

3.1 Algebraic varieties

Let n be a positive integer, and consider the *n-dimensional affine space* $\mathbb{A}^n := \mathbb{C}^n$. The polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$ is then called the *coordinate ring* of $\mathbb{A}^n$, and is also denoted by $\mathbb{C}[\mathbb{A}^n]$. Every $f \in \mathbb{C}[\mathbb{A}^n]$ can be obviously viewed as a function $f : \mathbb{A}^n \to \mathbb{C}$ by $f(v) = f(v_1, \ldots, v_n)$, where $v = (v_1, \ldots, v_n)$.

We say that a set $X \subset \mathbb{A}^n$ is an *algebraic variety* over $\mathbb{C}$ if there exists a subset A of $\mathbb{C}[\mathbb{A}^n]$ so that $X = \{v \in \mathbb{A}^n \mid f(v) = 0 \text{ for all } f \in A\}$.

The following results hold.

Proposition 3.1.1. *The ideal generated by A defines the same algebraic variety defined by A.*

Theorem 3.1.2 (Hilbert's basis theorem)**.** *Let k be a subfield of $\mathbb{C}$ (eventually, $k = \mathbb{C}$). Every ideal of $k[x_1, \ldots, x_n]$ is finite generated.*

Corollary 3.1.3. *There is no infinite series of strictly increasing ideals in $k[x_1, \ldots, x_n]$*

The set of algebraic varieties of $\mathbb{A}^n$ verifies the axioms of the closed sets of a topology that is called the *topology of Zariski* on $\mathbb{A}^n$. So, throughout, we refer to algebraic varieties as to *closed sets*.

Hence, a subset of $\mathbb{A}^n$ is called *open* if it is the complement of a closed set. More generally, if $X \subset \mathbb{A}^n$ is closed, then a $Y \subset X$ is called open in X if $X - Y$ is a closed set.

Definition 3.1.4. Let $U \in \mathbb{A}^n$. The smallest closed containing U is called the *closure* of U and is denoted by $\overline{U}$. $U \subset X$ is said to be *dense* in X if $\overline{U} = X$.

Proposition 3.1.5. *Any polynomial which is zero on a dense subset of X, must be zero on X.*

Now, let $U \subset \mathbb{A}^n$ and consider the set

$$\mathcal{I}(U) = \{f \in \mathbb{C}[x_1, \ldots, x_n] \mid f(u) = 0 \text{ for all } u \in U\}$$

Proposition 3.1.6. *$\mathcal{I}(U)$ is an ideal of $\mathbb{C}[x_1, \ldots, x_n]$, called the* vanishing ideal *of U.*

Conversely, given an ideal $I \subset \mathbb{C}[x_1, \ldots, x_n]$, we can construct the closed set

$$\mathcal{V}(I) = \{v \in \mathbb{A}^n \mid f(v) = 0 \text{ for all } f \in I\}.$$

Proposition 3.1.7. *For a given $U \subset \mathbb{A}^n$ the set $\mathcal{V}(\mathcal{I}(U))$ is the smallest closed set containing U; i.e., the closure of U.*

Definition 3.1.8. Let $I \subset \mathbb{C}[x_1, \ldots, x_n]$ an ideal. We call the *radical* of I the ideal

$$\sqrt{I} = \{f \in \mathbb{C}[x_1, \ldots, x_n] \mid \exists m > 0 : f^m \in I\}$$

As $\mathbb{C}$ is algebrically closed, the following famous result holds.

Theorem 3.1.9 (Hilbert's Nullstellensatz)**.** *Let $I \subset \mathbb{C}[x_1, \ldots, x_n]$ be an ideal. Then $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$.*

Let $X \subset \mathbb{A}^n$ be closed. The ring

$$\mathbb{C}[X] := \mathbb{C}[x_1, \ldots, x_n]/\mathcal{I}(X)$$

is called the *coordinate ring* of X. Its elements can be naturally identified by the restrictions to X of all $f \in \mathbb{C}[x_1, \ldots, x_n]$. The functions $f : X \to \mathbb{C}$ associated to the elements of $\mathbb{C}[X]$ are called *regular functions*. Now, let $Y \subset \mathbb{A}^m$ be closed, and $h_1, \ldots, h_m \in \mathbb{C}[X]$ be such that $(h_1(v), \ldots, h_m(v)) \in Y$ for all $v \in X$. Then $h : X \to Y$ defined by $h(v) = (h_1(v), \ldots, h_m(v))$ is called a *regular map*. If the h_i have coefficients in a subfield $k \subset \mathbb{C}$, then h is said to be defined over k.

Let $h : X \to Y$ be a regular map. We define a corresponding map $h^* : \mathbb{C}[Y] \to \mathbb{C}[X]$ by

$$h^*(f)(v) = f(h(v))$$

This map is called the *pullback*, or *comorphism* of h.

Proposition 3.1.10. *h^* is a homomorphism of algebras. Moreover it is is injective if and only if $h(X)$ is dense in Y.*

A regular map $h : X \to Y$ that has a regular inverse is called an *isomorphism*.

Definition 3.1.11 (Irreducible closed sets)**.** A closed set $X \subset \mathbb{A}^n$ is called *irreducible* if it is not the union of two other closed sets.

Let $X \subset \mathbb{A}^n$ be closed. If X is not irreducible, we can write $X = X_1 \cup X_2$, where $X_1, X_2 \subset X$ are two proper nonempty closed sets. With X_1, X_2 we can continue this process. It has to terminate, otherwise we can construct an infinite sequence of closed sets $X \supsetneq Y_1 \supsetneq Y_2 \supsetneq \ldots$, that is impossible because $\mathbb{C}[x_1, \ldots, x_n]$ has no strictly increasing sequence of ideals, as consequence of Hilbert's basis theorem. It follows that X is a finite union of irreducible closed subsets $X = X_1 \cup \ldots \cup X_r$. If there are $i \neq j$ such that $X_i \subset X_j$, then we discard X_i. In this way we obtain a union $X = X_1 \cup \ldots \cup X_s$ such that $X_i \subset X_j$ for $i \neq j$. It is not difficult to see that, up to order, these X_i are uniquely determined. They are called the *irreducible components* of X.

Theorem 3.1.12. *Let $X \subset \mathbb{A}^n$ be closed. X is irreducible if and only if $\mathcal{I}(X)$ is prime.*

Proposition 3.1.13. *Let $f : \mathbb{A}^n \to \mathbb{A}^m$ be a regular map. Let $X \subset \mathbb{A}^n$ be an irreducible closed set. Then $\overline{f(X)}$ is irreducible as well.*

Proposition 3.1.14. *Let $X \subset \mathbb{A}^n$ be closed and irreducible. Let $U \subset X$ be open in X. Then U is dense in X.*

Consider now the set of *dual numbers*

$$D = \{a + b\epsilon \mid a, b \in \mathbb{C}, \epsilon^2 = 0\}$$

that becomes a 2-dimensional associative algebra over $\mathbb{C}$ by putting

$$(a + b\epsilon)(c + d\epsilon) = ac + (ad + bc)\epsilon$$

Let $X \subset \mathbb{A}^n$ a closed set and consider $v \in X$. Let $\mathfrak{m}_v = \{f \in \mathbb{C}[X] \mid f(v) = 0\}$. Then a map $\phi : \mathbb{C}[X] \to \mathbb{C}$ of the form $\phi(f) = f(v) + L(f)\epsilon$ is a $\mathbb{C}$-homomorphism of algebras if and only if

1. $\phi(\alpha) = \alpha$ for all $\alpha \in \mathbb{C}$,
2. $L : \mathbb{C}[X] \to \mathbb{C}$ is a linear map whose kernel includes $\mathfrak{m}_v^2$ and $\mathbb{C}$.

Definition 3.1.15. Every $\mathbb{C}$-algebra homomorphism $\phi : \mathbb{C}[X] \to D$ of the form $\phi(f) = f(v) + L(f)\epsilon$ is called a *close point* to v on X.

Proposition 3.1.16. *If ϕ is a close point to v on X then*

1. *$L(\alpha) = 0$ for all $\alpha \in \mathbb{C}$,*
2. *L(fg)=g(v)L(f)+f(v)L(g).*

Definition 3.1.17. A linear map $L : \mathbb{C}[X] \to \mathbb{C}$ so that $L(fg) = g(v)L(f) + f(v)L(g)$ is called a *tangent vector* on X at v.

Proposition 3.1.18. *The natural correspondence, between close points to v on X and tangent vectors on X at v, is one to one.*

The space of all tangent vectors on X at v is called the *tangent space* at v, and is denoted by $T_v(X)$.

Remark 3.1.19. $L \in T_v(X)$ is completely determined by the values $L(x_i)$ for $1 \leq i \leq n$. Indeed, any $f \in \mathbb{C}[X]$ can be written $f = a_0 + \sum_{i=1}^{n} a_i(x_i - v_i) + h$, where $a_i \in \mathbb{C}$ and $h \in \mathfrak{m}_v^2$. Furthermore, $L(x_i - v_i) = L(x_i)$. Hence $L(f) = \sum_{i=1}^{n} a_i L(x_i)$.

Let $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ be closed sets, and $\sigma : X \to Y$ a regular map. Let $v \in X$, and $w = \sigma(v) \in Y$. Let ϕ be a close point to v on X, and define $\psi : \mathbb{C}[X] \to \mathbb{C}$ by $\psi(f) = \phi(\sigma^*(f))$. Then ψ is a close point to w on Y. Let L_ϕ, L_ψ be the elements of respectively T_v, T_w corresponding to respectively ϕ, ψ. Then

$$L_\psi(f) = L_\phi(\sigma^*(f))$$

Definition 3.1.20. The linear map $\mathrm{d}_v\sigma : T_v \to T_w$ defined by $\mathrm{d}_v\sigma(f) = L(\sigma^*(f))$ is called the *differential* of σ at v.

Lemma 3.1.21. *Let $X \subset \mathbb{A}_n, Y \subset \mathbb{A}^m$ be closed sets, and $\sigma : X \to Y, \pi : Y \to Z$ regular functions. Let $u \in X$ and $v = \sigma(u) \in Y$. Then $\mathrm{d}_v\sigma : T_v \to T_w$ is an isomorphism.*

Corollary 3.1.22. *Let $X \subset \mathbb{A}^n, Y \subset \mathbb{A}^m$ be closed sets. Let $\sigma : X \to Y$ be a regular function, and suppose that it has a regular inverse. Let $v \in X$ and $w = \sigma(v)$. Then $\mathrm{d}_v\sigma : T_v \to T_w$ is an isomorphism.*

Now consider the closed set $\mathbb{A}^n$, and let $v \in \mathbb{A}^n$. Then the $x_i - v_i$ mod $\mathfrak{m}_v^2$ form a basis of $\mathfrak{m}_v/\mathfrak{m}_v^2$. For $(a_1, \dots, a_n) \in \mathbb{C}^n$ there is a unique $L \in T_v(\mathbb{A}^n)$ with $L(x_i) = L(x_i - v_i) = a_i$. This implies that $T_v(\mathbb{A}^n) \simeq \mathbb{C}^n$.

Proposition 3.1.23. *Let $X \subset \mathbb{A}^n$ be a closed set, and $v \in X$. Let $\sigma : X \to \mathbb{A}^n$ be the identity map. Then $\mathrm{d}_v\sigma$ maps $T_v(X)$ injectively into $T_v(\mathbb{A}^n)$. This identifies $T_v(X)$ with a subspace of $T_v(\mathbb{A}^n)$. Moreover, for $L \in T_v(\mathbb{A}^n)$ we have $L \in T_v(X)$ if and only if $L(f) = 0$ for all $f \in \mathcal{I}(X)$. In fact, it is enough to have this condition for a set of generators of $\mathcal{I}(X)$.*

Proposition 3.1.24. *Let $X \subset \mathbb{A}^n$ be a closed set. Let $F_1, \dots, F_r \in \mathbb{C}[\mathbb{A}^n]$ be generators of $\mathcal{I}(X)$. Identify $T_v(\mathbb{A}^n)$ with $\mathbb{C}^n$. Then $T_v(X)$ corresponds to the subspace consisting of $(a_1, \dots, a_n)$ such that $\sum_{i=1}^{n} (D_iF_j)(v)a_i = 0$ for $1 \le j \le r$, where D_iF_j the partial derivative of F_j with respect to x_i.*

We can note that the last condition is also equivalent to $F_j(v_1 + a_1\epsilon, \dots, v_n + a_n\epsilon) = 0$ for $1 \le j \le r$.

Let $X \subset \mathbb{A}^n, Y \subset \mathbb{A}^m$ two closed sets. We identify the product $\mathbb{A}^n \times \mathbb{A}^m$ with $\mathbb{A}^{n+m}$. We write $\mathbb{C}[\mathbb{A}^n \times \mathbb{A}^m] = \mathbb{C}[x_1, \dots, x_n, y_1, \dots, y_m]$ and we have natural inclusions $\mathbb{C}[\mathbb{A}^n], \mathbb{C}[\mathbb{A}^m] \subset \mathbb{C}[\mathbb{A}^n \times \mathbb{A}^m]$. Moreover, if X is defined by the equations $f_i(v) = 0$, and Y by $g_j(w) = 0$, then $X \times Y$ is defined by the equations $f_i(v, w) = g_j(v, w) = 0$ (where now f_i, g_j are viewed as elements of $\mathbb{C}[\mathbb{A}^n \times \mathbb{A}^m]$. It follows that $X \times Y$ is a closed set.

Lemma 3.1.25. *We have $\mathbb{C}[\mathbb{A}^n \times \mathbb{A}^m] \simeq \mathbb{C}[\mathbb{A}^n] \otimes \mathbb{C}[\mathbb{A}^m]$.*

Throughout we identify $\mathbb{C}[\mathbb{A}^n \times \mathbb{A}^m]$ and $\mathbb{C}[\mathbb{A}^n] \otimes \mathbb{C}[\mathbb{A}^m]$.

Let $\pi_1 : X \times Y \to X$ be the projection onto X; i.e, $\pi_1(v, w) = v$. Similarly π_2 will be the projection onto Y. Then $\pi_1^*(f) = f \otimes 1$, and $\pi_2^*(g) = 1 \otimes g$ for $f \in \mathbb{C}[X], g \in \mathbb{C}[Y]$.

Proposition 3.1.26. *Let $v \in X$ and $w \in Y$. Then $L \mapsto (\mathrm{d}_{(v,w)}\pi_1(L), \mathrm{d}_{(v,w)}\pi_2(L))$ is an isomorphism $T_{(v,w)} \to T_v \oplus T_w$.*

Theorem 3.1.27. *Let $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$ be irreducible closed sets. Then $X \times Y$ in $\mathbb{A}^{n+m}$ is irreducible as well.*

Let $X \subset \mathbb{A}^n$ be an irreducible closed set. Then $\mathcal{I}(X)$ is a prime ideal, and therefore the algebra $\mathbb{C}[X] = \mathbb{C}[x_1, \ldots, x_n]/\mathcal{I}(X)$ has no zero divisors. Hence, we can consider the field of fraction

$$\mathbb{C}(X) = \{f/g \mid f, g \in \mathbb{C}[X], g \neq 0\}$$

that is called the *field of rational function on X*.

We can note that, by definition, taken $f/g, f_1/g_1 \in \mathbb{C}(X)$, it is $f/g = f_1/g_1$ if and only if $fg_1 - gf_1 = 0$

Definition 3.1.28 (Dimension of a closed set)**.** Let $X \subset \mathbb{A}^n$ be an irreducible closed set. Then the *dimension* of X is defined as the transcendence degree of $\mathbb{C}(X)$ over $\mathbb{C}$.

Let X be as above and let s be the minimal dimension of a $T_v(X)$ as V ranges over X. Then a point v is called *singular* if $\dim T_v(X) > s$, otherwise it is nonsingular. The set of nonsingular points forms a nonempty open set in X. The set of singular points is therefore a closed subset. Furthermore, the number s equals the dimension of X.

3.2 Linear algebraic groups and Lie algebras

Proposition 3.2.1. *Let $G \subset \mathbb{C}^n$ be a closed set endowed with a group structure. Then G is called a (linear) algebraic group if the group operations $\cdot : G \times G \to G$ and $\iota : G \to G$ are regular maps. (here ι denotes inversion).*

Example 3.2.2. Let $G = \{x \in G \mid x^n - 1 = 0\}$. Then the product and the inverse are respectively given by $(x, y) \mapsto xy$ and $x \mapsto x^{n-1}$. Both are clearly regular maps. Hence G is algebraic.

Example 3.2.3. Let V be an n-dimensional vector space over $\mathbb{C}$. Let $\mathrm{GL}(V)$ be the group of invertible linear transformations of V. We denote an element of $\mathbb{C}^{n^2+1}$ by (a_{ij}, b), where $1 \leq i, j \leq n$. Correspondingly we consider the polynomial ring $\mathbb{C}[x_{ij}, d]$. We embed $\mathrm{GL}(V)$ into $\mathbb{C}^{n^2+1}$ by $g \mapsto (g_{ij}, 1/det(g))$, where (g_{ij}) is the matrix of g with respect to a fixed basis of V. The image of this map is clearly a group. It consists of the zeros of the polynomial $d\det((x_{ij})) - 1$. Hence it is a closed set. We have $\mathbb{C}[\mathrm{GL}(V)] = \mathbb{C}[x_{ij}, d]/(d\det((x_{ij})) - 1$. The multiplication map is clearly regular. Inversion is regular as well because $d = 1/\det((x_{ij}))$ on $\mathrm{GL}(V)$.

Proposition 3.2.4. *An algebraic group G has no singular points.*

Lemma 3.2.5. *Let G be an algebraic group, and $A, B \subset G$ with A nonempty and open and B dense. Then $G = AB$.*

Lemma 3.2.6. *Let G be an algebraic group. Let H be a subgroup (not necessarily closed). Then the closure $\overline{H}$ is an algebraic subgroup of G.*

Proposition 3.2.7. *Let $\alpha : G \to H$ be a morphism of algebraic groups. Then $\alpha(G)$ is an algebraic subgroup of H. Moreover, if G and α are defined over k, so is $\alpha(G)$.*

Proposition 3.2.8. *Let G_i for $i \in I$ be connected algebraic subgroups of the algebraic group G. Let $G' \subset G$ be the subgroup generated by all the G_i. Then G' is a connected algebraic group. Moreover, there is a finite subset $J \subset I$ and a $k > 0$ such that every element of G' can be written as a product of k elements, each from one of the G_j where $j \in J$.*

Theorem 3.2.9. *Let G an algebraic group, and let $X_1, \ldots, X_n$ be its irreducible components. There is exactly one component containing e. This component is a normal subgroup of finite index in G.*

Definition 3.2.10. The irreducible component of G containing e is called the *connected component of the identity of G*, and denoted by G^{o}.

With an algebraic group G is associated a Lie algebra, that is, roughly speaking, the tangent space at the identity e, witch we equip with a Lie algebra structure.

Definition 3.2.11. We call the Lie algebra of G the space

$$\mathrm{Lie}(G) = \{\delta \in \mathbb{C}[G]^* \mid \delta(fg) = f(e)\delta(g) + g(e)\delta(f) \text{ for all } f, g \in \mathbb{C}[G]\}$$

where $\mathbb{C}[G]^*$ is the dual space of $\mathbb{C}[G]$; i.e, the space of linear maps $\mathbb{C}[G] \to \mathbb{C}$.

Now we want to equip $\mathrm{Lie}(G)$ with a Lie algebra structure. In order to do it we first define a multiplication on $\mathbb{C}[G]^*$ with respect to which $\mathrm{Lie}(G)$ is an associative algebra. Then we show that $\mathrm{Lie}(G)$ is closed under taking commutators, by identifying it with an algebra of derivations. This then immediately implies that it is a Lie algebra. So, having identified $\mathbb{C}[G \times G]$ with $\mathbb{C}[G] \otimes \mathbb{C}[G]$, we define a map $\Delta : \mathbb{C}[G] \to \mathbb{C}[G] \otimes \mathbb{C}[G]$ by $\Delta(f)(a, b) = f(ab)$, for $a, b \in G$. This is the cohomomorphism of the multiplication map $G \times G \to G$. So if $\Delta(f) = \sum_i f_i \otimes g_i$ then $f(ab) = \sum_i f_i(a)g_i(b)$ for all $a, b \in G$.

We also define a map $\Delta \otimes 1 : \mathbb{C}[G] \otimes \mathbb{C}[G] \to \mathbb{C}[G] \otimes \mathbb{C}[G] \otimes \mathbb{C}[G]$ by $(\Delta \otimes 1)(f \otimes g) = \Delta(f) \otimes g$. Similarly we have a map $1 \otimes \Delta$.

Lemma 3.2.12. $(\Delta \otimes 1) \circ \Delta = (1 \otimes \Delta) \circ \Delta$.

The map Δ is called the *comultiplication*, while the property expressed by the previous lemma is called *coassociativity*.

Now let $\gamma, \delta \in \mathbb{C}[G]^*$. We define their product by $\gamma\delta = (\gamma \otimes \delta \otimes \epsilon) \circ (\Delta \otimes 1) \circ \Delta$. In other words, if $\Delta(f) = \sum_i f_i \otimes g_i$ then $\gamma\delta(f) = \sum_i \gamma(f_i)\delta(g_i)$. From the previous lemma the associativity of this multiplication follows.

Now consider the function $\epsilon : \mathbb{C}[G] \to \mathbb{C}$ given by $\epsilon(f) = f(e)$. Then ϵ is identity element for the multiplication on $\mathbb{C}[G]^*$. Indeed, for $f \in \mathbb{C}[G]$ and $g \in G$ we have $f(g) = (1 \otimes \epsilon) \circ \Delta(f)(g)$. So

$$\delta\epsilon(f) = \delta \circ (1 \otimes \epsilon) \circ \Delta(f) = \delta(f)$$

and, similarly, $\epsilon\delta(f) = \delta(f)$.

We now consider derivations of $\mathbb{C}[G]$; i.e., linear maps $D : \mathbb{C}[G] \to \mathbb{C}[G]$ so that $D(f_1 f_2) = D(f_1)f_2 + f_1 D(f_2)$. Given two derivations D_1, D_2 we can form their commutator by $[D_1, D_2] = D_1 D_2 - D_2 D_1$, that is a derivation again, as one can see by executing of a short calculation. Hence all derivations of $\mathbb{C}[G]$ form a Lie algebra.

Proposition 3.2.13. *Let* $\gamma, \delta \in \mathrm{Lie}(G)$. *Then it is* $[\gamma, \delta] \in \mathrm{Lie}(G)$ *too.*

Last result implies that $\mathrm{Lie}(G)$ is a Lie algebra.

Example 3.2.14. Consider the Lie algebra $\mathrm{GL}(V)$, where V is an n-dimensional complex vector space. Then G can be viewed as a closed subset of $\mathbb{C}^{n^2+1}$ and we have $\mathbb{C}[G] = \mathbb{C}[d, x_{ij} \mid 1 \leq i, j, \leq n]/(d\det((x_{ij}) - 1)$. Let $\delta \in \mathrm{Lie}(G)$; then δ has $\mathfrak{m}_e^2$ in its kernel. Moreover, $\det((x_{ij})) = x_{11} \cdots x_{nn} \mod \mathfrak{m}_e^2$ (as $x_{ij} \in \mathfrak{m}_e^2$ if $i \neq j$). Also, by induction, we have $\delta(x_{11} \cdots x_{nn}) = \sum_{i=1}^{n} \delta(x_{ii})$. So we get $0 = \delta(\det((x_{ij})d - 1) = \delta(x_{11} \cdots x_{nn} d) = \sum_{i=1}^{n} \delta(x_{ii}) + \delta(d)$. Hence $\delta(d)$ is determined once we know the $\delta(x_{ii})$. There are no algebraic relations between the x_{ij}; so we can choose $a_{ij} \in \mathbb{C}$ and define $\delta \in \mathrm{Lie}(G)$ by $\delta(x_{ij}) = a_{ij}$. Now, let $\gamma, \delta \in \mathrm{Lie}(G)$ be defined by $\gamma(x_{ij}) = a_{ij}$ and $\delta(x_{ij}) = b_{ij}$. We want to compute c_{ij} such that $\gamma\delta(x_{ij}) = c_{ij}$. For this we need $\Delta(x_{ij})$. As element of $\mathbb{C}[G \times G]$ we have $\Delta(x_{ij})(g, g') = x_{ij}(g, g') = \sum_k g_{ik} g'_{kj}$. To this there corresponds a unique element of $\mathbb{C}[G] \otimes \mathbb{C}[G]$. Hence we get $\Delta(x_{ij}) = \sum_k x_{ik} \otimes x_{kj}$. Therefore $c_{ij} = \sum_k a_{ik} b_{kj}$. We conclude that, if we identify γ, δ with their matrices $(a_{ij}), (b_{ij})$, then the product $\gamma\delta$ corresponds to the product of the matrices. Therefore, the Lie algebra of G is the Lie algebra of $n \times n$ matrices with the commutator as bracket operation. This Lie algebra is denoted $\mathfrak{gl}(n, \mathbb{C})$.

Theorem 3.2.15. *Let* G *be an algebraic group with algebraic subgroups* H_1, H_2. *Then*

1. *If* $\mathrm{Lie}(H_1) \subset \mathrm{Lie}(H_2)$ *then* $H_1 \subset H_2$. *In particular, if both* H_1, H_2 *are connected then* $H_1 = H_2$ *if and only if* $\mathrm{Lie}(H_1) = \mathrm{Lie}(H_2)$,

2. $\mathrm{Lie}(H_1 \cap H_2) = \mathrm{Lie}(H_1) \cap \mathrm{Lie}(H_2)$.

Theorem 3.2.16. *Let* G, H *and* $\alpha : G \to H$ *a morphism, i.e a regular map and a group homomorphism too. Then* $\mathrm{d}_e\alpha : \mathrm{Lie}(G) \to \mathrm{Lie}(H)$ *is a homomorphism of Lie algebras.*

Throughout we indicate $\mathrm{d}_e\alpha$ simply by $\mathrm{d}\alpha$.

Definition 3.2.17. A morphism $\rho : G \to \mathrm{GL}(V)$ is called a *rational representation* of G.

Theorem 3.2.18. *Let* G *be a connected algebraic group, and* $\rho : G \to \mathrm{GL}(V)$ *a rational representation. Let* U *be a subspace of* V. *Then* U *is stable under* $\rho(G)$ *if and only if* U *is stable under* $\mathrm{d}\rho(\mathrm{Lie}(G))$.

Definition 3.2.19. Let G be an algebraic group and write $\mathfrak{g} = \mathrm{Lie}(G)$. For $g \in G$ consider the isomorphism $\phi_g : g' \in G \mapsto gg'g^{-1}$. Then its differential in e $\mathrm{Ad}(g) : \mathfrak{g} \to \mathfrak{g}$ is an automorphism of $\mathfrak{g}$. The consequent map $\mathrm{Ad} : G \to \mathrm{GL}(\mathfrak{g})$ is called the *adjoint representation* of G.

Theorem 3.2.20. *Let* G *be an algebraic group. Then the adjoint representation* Ad *is a rational representation of* G, *and* $\mathrm{d}\,\mathrm{Ad}(\delta)(\gamma) = [\delta, \gamma]$ *for* $\gamma, \delta \in \mathrm{Lie}(G)$.

I recall that a G-module is said to be *simple*, or *irreducible*, if its G-submodules are just the trivial ones. It is said to be *semisimple* if it is direct sum of simple G-submodules.

Definition 3.2.21. An algebraic group G is called (*linearly*) *reductive* if every finite-dimensional rational G-module is semisimple.

Theorem 3.2.22. *Let* V *be a complex vector space of finite dimension. An algebraic group* $G \subset \mathrm{GL}(V)$ *is reductive if and only if* $\mathrm{Lie}(G) = \mathfrak{s} \oplus \mathfrak{t}$, *where* $\mathfrak{s}$ *is a semisimple ideal, and* $\mathfrak{t}$ *is an abelian ideal consisting of semisimple elements.*

3.3 Reductive Lie algebras and their inner automorphisms

Definition 3.3.1. A complex Lie algebra $\mathfrak{g}$ is said to be *reductive* if $\mathfrak{g} = \mathfrak{s} \oplus \mathfrak{c}$, where $\mathfrak{s}$ is semisimple and $\mathfrak{c}$ is the centre.

Lemma 3.3.2. *Let* $\mathfrak{g}$ *be reductive. Then* $\mathrm{Int}(\mathfrak{g})$ *is a connected algebraic subgroup of* $\mathrm{GL}(\mathfrak{g})$*, with Lie algebra* $\mathrm{ad}\mathfrak{g}$*.*

Corollary 3.3.3. *The Lie algebra* $\mathrm{ad}\mathfrak{g} \subset \mathfrak{gl}(\mathfrak{g})$ *is algebraic. Moreover, the unique connected algebraic subgroup of* $\mathrm{GL}(\mathfrak{g})$ *with Lie algebra* $\mathrm{ad}\mathfrak{g}$ *is* $\mathrm{Int}(\mathfrak{g})$*.*

Proposition 3.3.4. *If* $\mathfrak{g}$ *is semisimple, then* $\mathrm{Int}(\mathfrak{g})$ *is the connected component of the identity of* $\mathrm{Aut}(\mathfrak{g})$*.*

3.4 The Weyl group

Let $\mathfrak{g}$ be a semisimple Lie algebra and $\mathfrak{h} \subset \mathfrak{g}$ be a Cartan subalgebra, with corresponding root system $\Phi \subset \mathfrak{h}^*$.

Consider then the Weyl group W of Φ having Δ as its root basis. I recall that (see §2.4), for being the Killing form κ not degenerate, we get a natural bijective linear map $\mu \in \mathfrak{h}^* \mapsto \hat{\mu} \in \mathfrak{h}$ by means of which κ induces a a scalar product $(\ ,\ )$ on $\mathfrak{h}^*$ that is W-invariant. Moreover, W acts on $\mathfrak{h}^*$. We can use the bijection between $\mathfrak{h}^*$ and $\mathfrak{h}$ to let W also act on $\mathfrak{h}$. This means that $w(\hat{\mu}) = \widehat{w(\mu)}$. A short calculation shows that this implies that $s_\alpha(h) = h - \alpha(h)\alpha^\vee$.

In the sequel we identify W with its image in $\mathrm{GL}(\mathfrak{h})$.

Lemma 3.4.1. *Let* $w \in W$*; then there is* $\sigma \in \mathrm{Int}(\mathfrak{g})$ *such that* σ *maps* $\mathfrak{h}$ *onto itself, and* $\sigma|_{\mathfrak{h}} = w$*.*

Now let G be an algebraic group with Lie algebra $\mathfrak{g}$ (for example, $G = \mathrm{Int}(\mathfrak{g})$) and let $N_G(\mathfrak{h})$ be the set of $\sigma \in G$ that map $\mathfrak{h}$ onto itself. Morever, let $Z_G(\mathfrak{h})$ be the set of $\sigma \in N_G(\mathfrak{h})$ that are the identity on $\mathfrak{h}$. Then we get a natural map $\psi : N_G(\mathfrak{h})/Z_G(\mathfrak{h}) \to \mathrm{GL}(\mathfrak{h})$.

Theorem 3.4.2. *The image of* ψ *is* W*.*

Corollary 3.4.3. $W \simeq N_G(\mathfrak{h})/Z_G(\mathfrak{h})$*.*

Proposition 3.4.4. *Two elements of* $\mathfrak{h}$ *are* G*-conjugate if and only if they are* W*-conjugate.*

Proof. One direction is obvious. For the other, suppose that $\sigma(h_1) = h_2$, for some $\sigma \in G$, $h_1, h_2 \in \mathfrak{h}$. Then $\sigma(\mathfrak{h})$ is also a Cartan subalgebra of $\mathfrak{g}$, which contains h_2. Now $\mathfrak{h}$ and $\sigma(\mathfrak{h})$ are Cartan subalgebras of $Z_{\mathfrak{g}}(h_2)$. So there is a $\theta \in \mathrm{Int}(Z_{\mathfrak{g}}(h_2))$ with $\theta\sigma(\mathfrak{h}) = \mathfrak{h}$. Note that $\theta(h_2) = h_2$. So $\theta\sigma(h_1) = h_2$ and $\theta\sigma \in N_G(\mathfrak{h})$. $\square$

3.5 θ-groups

Let $\mathfrak{g}$ be a semisimple Lie algebra, and $G = \mathrm{Ad}\mathfrak{g}$. We consider $\mathbb{Z}/m\mathbb{Z}$-gradings of $\mathfrak{g}$:

$$\mathfrak{g} = \bigoplus_{i \in \mathbb{Z}/m\mathbb{Z}} \mathfrak{g}_i$$

This means that $[\mathfrak{g}_i, \mathfrak{g}_j] \subset \mathfrak{g}_{i+j}$. Also $m = 1$ is allowed; then by convention, the grading is a $\mathbb{Z}$-grading.

A $\mathbb{Z}/m\mathbb{Z}$-grading, for $m \neq \infty$, yields an automorphism of $\mathfrak{g}$ of order m by setting $\theta(x) = \omega^i x$, for $x \in g_i$, where ω is a primitive m-th root of unity. Conversely, if $\theta \in \mathrm{Aut}(\mathfrak{g})$ has order m, then the eigenvalues of θ are ω^i, and the decomposition of $\mathfrak{g}$ into eigenspaces of θ gives a $\mathbb{Z}/m\mathbb{Z}$-grading. A $\mathbb{Z}$-grading of $\mathfrak{g}$ corresponds to a subgroup $\{\theta_t \mid t \in \mathbb{C}\}$ of $\mathrm{Aut}(\mathfrak{g})$, where $\theta_t(x) = t^i x$ for $x \in \mathfrak{g}_i$.

Consider the group $H = \{g \in \mathrm{GL}(\mathfrak{g}) \mid \theta g = g\theta\}$. Since the equations that define H are linear, $\mathrm{Lie}(H) = \{X \in \mathrm{GL}(\mathfrak{g}) \mid \theta X = X\theta\}$. Let G_0 be the connected component of the identity of $H \cap G$. Then by Theorem 3.2.15

$$\mathrm{Lie}(G_0) = \mathrm{Lie}(H) \cap \mathrm{Lie}(G) = \{\mathrm{ad}\mathfrak{g}x \mid x \in \mathfrak{g} \text{ and } \mathrm{ad}_{\mathfrak{g}}\theta(x) = \mathrm{ad}x\}$$

(as $\theta(\mathrm{ad}x)\theta^{-1} = \mathrm{ad}\theta(x)$). But the latter is isomorphic to $\mathfrak{g}_0$. It follows that $\mathrm{ad}\mathfrak{g}_0$ is algebraic and G_0 is the unique connected subgroup of G with Lie algebra $\mathrm{ad}\mathfrak{g}_0$. Moreover, $\mathrm{ad}\mathfrak{g}_0(\mathfrak{g}_1) \subset \mathfrak{g}_1$. Therefore, by Theorem 3.2.18 $G_0 \cdot \mathfrak{g}_1 = \mathfrak{g}_1$. The group G_0, together with its action on $\mathfrak{g}_1$ is called a θ-group.

Remark 3.5.1 (Vinberg)**.** It is also possible to consider the action of G_0 on $\mathfrak{g}_k$, for $k \neq 1$. However this arises also in the above manner by considering the graded Lie algebra $\tilde{\mathfrak{g}}$ with components $\tilde{\mathfrak{g}}_i = \mathfrak{g}_{ik}$ for $0 \le i \le l$, where $l = m/\gcd(m,k)$.

Let κ denote the Killing form of $\mathfrak{g}$. Let $x \in \mathfrak{g}_i$, $y \in \mathfrak{g}_j$, then $(\mathrm{ad}x)(\mathrm{ad}y)$ maps $\mathfrak{g}_k$ to $\mathfrak{g}_{k+i+j}$. So if $i + j \neq 0$ then $\kappa(x,y) = 0$. So since κ is non-degenerate, its restrictions to $\mathfrak{g}_i \times \mathfrak{g}_{-i}$ have to be non-degenerate as well. In particular, its restriction to $\mathfrak{g}_0$ is non-degenerate. So if $\mathfrak{g}_0 \neq 0$, then it is reductive.

Lemma 3.5.2. *Let $\mathfrak{h}_0$ be a Cartan subalgebra of $\mathfrak{g}_0$. Then the centraliser of $\mathfrak{h}_0$ in $\mathfrak{g}$ is a Cartan subalgebra of $\mathfrak{g}$. In particular, $\mathfrak{g}_0 \neq 0$.*

Let $\mathfrak{h}$ be a Cartan subalgebra of $\mathfrak{g}$ with corresponding root system Φ. Then we can define a $\mathbb{Z}$-grading of $\mathfrak{g}$ by assigning a non-negative degree to the simple roots. Moreover, by $\deg(\alpha + \beta) = \deg(\alpha) + \deg(\beta)$ and $\deg(-\alpha) = -\deg(\alpha)$, every root gets a degree. Now we let $\mathfrak{g}_0$ be spanned by $\mathfrak{h}$, along with all $\mathfrak{g}_\alpha$ where $\deg(\alpha) = 0$. Furthermore, $\mathfrak{g}_i$, for $i \neq 0$, is spanned by all $\mathfrak{g}_\alpha$ where $\deg(\alpha) = i$. Then $\mathfrak{g} = \oplus \mathfrak{g}_i$ is a $\mathbb{Z}$-grading of $\mathfrak{g}$. We call this a standard $\mathbb{Z}$-grading. Now consider a $\mathbb{Z}$-grading of $\mathfrak{g}$. Let $\mathfrak{h}_0$ be a Cartan subalgebra of $\mathfrak{g}_0$, and $\mathfrak{h}_0$ its centraliser. Then $\mathfrak{h}_0$ contains the homogeneous components of its elements. So since $\mathfrak{g}_i$ for $i \neq 0$ consists of nilpotent elements only, we infer that $\mathfrak{h}' \subset \mathfrak{g}_0$ (and $\mathfrak{h}' = \mathfrak{h}_0$). Let Φ be the root system of $\mathfrak{g}$ with respect to $\mathfrak{h}_0$. Let $x_\alpha \in \mathfrak{g}_\alpha$ and write $x_\alpha = \sum_{i\in\mathbb{Z}} x_i$ with $x_i \in \mathfrak{g}_i$. Then for $h \in \mathfrak{h}_0$,

$$\sum_{i\in\mathbb{Z}} [h, x_i] = [h, x_\alpha] = \sum_{i\in\mathbb{Z}} \alpha(h)x_i$$

from which it follows that $x_\alpha \in \mathfrak{g}_i$ for a certain i. We say that i is the degree of α. Now write $\alpha > 0$ if its degree if is positive. Then $\{\alpha \in \Phi' \mid \alpha > 0\}$ is a system of positive roots, with corresponding root basis. Moreover, the degree of the simple roots determines the degrees of the other roots. It follows that the given $\mathbb{Z}$-grading can be mapped by an inner automorphism to a standard $\mathbb{Z}$-grading.

Consider a standard $\mathbb{Z}$-grading of $\mathfrak{g}$. Let $h_0 \in \mathfrak{h}$ be defined by $\alpha(h_0) = \deg(\alpha)$, where α runs over the simple roots. Then $\mathfrak{g}_k = \{x \in \mathfrak{g} \mid [h_0, x] = kx\}$. This h_0 is called the *defining element* of the $\mathbb{Z}$-graded algebra $\mathfrak{g}$.

Now consider a $\mathbb{Z}/m\mathbb{Z}$-grading of $\mathfrak{g}$ with corresponding automorphism θ of order m. Then θ maps nilpotent (respectively semisimple) elements of $\mathfrak{g}$ to nilpotent (respectively semisimple) elements of $\mathfrak{g}$. (Indeed: the minimal polynomial of ad$x$ is the same as the minimal polynomial of ad $\theta(x)$). Let $x \in \mathfrak{g}_i$, and let $x = x_s + x_n$ be its Jordan decomposition. Then $\theta(x) = \theta(x_s) + \theta(x_n)$ is the Jordan decomposition of $\theta(x)$. But $\theta(x) = \omega^i x$, and $\omega^i x = \omega^i x_s + \omega^i x_n$ is the Jordan decomposition of $\omega^i x$. So $\theta(x_s) = \omega^i x_s$ and $\theta(x_n) = \omega^i x_n$. We conclude that $\mathfrak{g}_i$ contains the nilpotent and semisimple parts of all of its elements.

3.6 Cartan subspaces

Let the notation be as in last section. We consider a $\mathbb{Z}/m\mathbb{Z}$-grading of $\mathfrak{g}$ with corresponding automorphism θ of order m. A subspace $\mathfrak{c} \subset \mathfrak{g}_1$ is said to be a Cartan subspace if it consists of commuting semisimple elements, and it is maximal with that property. Cartan subspaces obviously exist. In the first part of this section we show that all Cartan subspaces are conjugate under G_0.

Let $\mathfrak{c} \subset \mathfrak{g}_1$ be a Cartan subspace. Let $\mathfrak{h} \supset \mathfrak{c}$ be a Cartan subagebra of $\mathfrak{g}$, with corresponding root system Φ. Then $\mathfrak{h} \subset Z_{\mathfrak{g}}(\mathfrak{c})$. So

$$Z_{\mathfrak{g}}(\mathfrak{c}) = \mathfrak{h} \oplus \bigoplus_{\substack{\alpha\in\Phi \\ \alpha(\mathfrak{c})=0}} \mathfrak{g}_\alpha = \mathfrak{t} \oplus \mathfrak{s}$$

where $\mathfrak{t} \subset \mathfrak{h}$ and $\mathfrak{s}$ is semisimple. Since $\mathfrak{c}$ commutes with $\mathfrak{s}$, we see that $\mathfrak{c} \subset \mathfrak{t}$. Now $Z_{\mathfrak{g}}(\mathfrak{c})$ is θ-stable, so $\mathfrak{s}$ is as well (as it is the derived subalgebra of the former), and therefore it is graded (where the grading is inherited from $\mathfrak{g}$). As $\mathfrak{c} \subset \mathfrak{t}$ we get that $\mathfrak{s}_1$ has no semisimple elements. Let $t \in \mathfrak{t}$, $s \in \mathfrak{s}$. As $\mathfrak{t}$ and $\mathfrak{s}$ are both θ-stable, we get that $t + s \in \mathfrak{g}_1$ if and only if $t \in \mathfrak{t}_1$ and $s \in \mathfrak{s}_1$. So with $U_{\mathfrak{c}} = Z_{\mathfrak{g}}(\mathfrak{c}) \cap \mathfrak{g}_1$, we get $U_{\mathfrak{c}} = \mathfrak{c} \oplus \mathfrak{s}_1$. Furthermore, if we write $u \in U_{\mathfrak{c}}$ according this decomposition, $u = c + s$, then this is also the Jordan decomposition of u, i.e., the semisimple part is $\mathfrak{c}$ and the nilpotent part is $\mathfrak{s}$. Now decompose $\mathfrak{g}$ into simultaneous eigenspaces with respect to $\mathfrak{c}$, and let the set of nonzero weights be denoted $\Sigma \subset \mathfrak{c}^*$. Then for an $x \in \mathfrak{c}$ the following statements are equivalent

1. $\sigma(x) \neq 0$ for all $\sigma \in \Sigma$,
2. $Z_{\mathfrak{g}}(x) = Z_{\mathfrak{g}}(\mathfrak{c})$.

Elements $x \in \mathfrak{c}$ with these properties are said to be in general position. From 1. we see that the set of elements in general position form a nonempty open subset of $\mathfrak{c}$. We let $U_{\mathfrak{c}}^{\mathrm{gp}}$ be the set of all $c+s$, where $c \in \mathfrak{c}$ is in general position and $s \in \mathfrak{s}_1$. This then is a nonempty open subset of $U_{\mathfrak{c}}$.

Proposition 3.6.1. *The set $G_0 \cdot U_{\mathfrak{c}}^{\mathrm{gp}}$ is open in $\mathfrak{g}_1$.*

Corollary 3.6.2. *Let $\mathfrak{c}, \mathfrak{c}'$ be two Cartan subspaces of $\mathfrak{g}_1$. Then there is a $g \in G_0$ such that $g(\mathfrak{c}) = \mathfrak{c}'$.*

Now let $\mathfrak{c} \subset \mathfrak{g}_1$ be a Cartan subspace. Set

- $N_{G_0}(\mathfrak{c}) = \{g \in G_0 \mid \mathfrak{g}(\mathfrak{c}) = \mathfrak{c}\}$,
- $Z_{G_0}(\mathfrak{c}) = \{g \in G_0 \mid g(x) = x \text{ for all } x \in \mathfrak{c}\}$,
- $W_0 = N_{G_0}(\mathfrak{c})/Z_{G_0}(\mathfrak{c})$.

If $\mathfrak{c}'$ is a second Cartan subspace, then by the previous theorem, there is a $g \in G_0$ such that $N_{G_0}(\mathfrak{c}') = gN_{G_0}(\mathfrak{c})g^{-1}$ and $Z_{G_0}(\mathfrak{c}') = gZ_{G_0}(\mathfrak{c})g^{-1}$. So W_0, and its action on $\mathfrak{c}$, do not depend on the choice of Cartan subspace. The group W_0 is called the *little Weyl group.*

Proposition 3.6.3. *Two elements of $\mathfrak{c}$ lie in the same G_0-orbit if and only if they lie in the same W_0-orbit.*

Let $\mathfrak{t}$ be the unique minimal algebraic subalgebra of $\mathfrak{g}$ containing $\mathfrak{c}$. Then $\mathfrak{t}$ consists of commuting semisimple elements. In the sequel we set $\mathfrak{s} = Z_{\mathfrak{g}}(\mathfrak{c})$ (the centraliser of $\mathfrak{c}$ in $\mathfrak{g}$). Then $\mathfrak{s}$ is a reductive subalgebra. Moreover, it is θ-stable and hence graded, $\mathfrak{s}_k = \mathfrak{s} \cap \mathfrak{g}_k$.

Lemma 3.6.4. *Let $\mathfrak{t}_\mathfrak{o}$ be a Cartan subalgebra of $\mathfrak{s}_0$. Then $h = Z_{\mathfrak{g}}(\mathfrak{t}_\mathfrak{o}+\mathfrak{t})$ is a θ-stable Cartan subalgebra of $\mathfrak{g}$ containing $\mathfrak{c}$.*

Let $\mathfrak{h}$ be as in the previous lemma. Let $W = N_G(\mathfrak{h})/Z_G(\mathfrak{h})$ be the corresponding Weyl group. Since $\mathfrak{h}$ is θ-stable we can consider the centraliser W^θ of θ in W. Let $w \in W^\theta$ and $x \in \mathfrak{c}$. Then $w(x) \in \mathfrak{h} \cap \mathfrak{g}_1 = \mathfrak{c}$. So w stabilises $\mathfrak{c}$, and we get a map

$$\pi : W^\theta \to \mathrm{GL}(\mathfrak{c})$$

by restriction, $\pi(w) = w|_{\mathfrak{c}}$.

Proposition 3.6.5. *$W_0 \subset \pi(W^\theta)$.*

Proof. Let $a \in W_0$, and let $g \in N_{G_0}(\mathfrak{c})$ be a representative of it. Set $L = Z_G(\mathfrak{t})$, which is a subgroup of G with Lie algebra $\mathfrak{l} = Z_{\mathfrak{g}}(\mathfrak{t})$. Now $g(\mathfrak{t})$ is an algebraic torus of $\mathfrak{g}$ containing $\mathfrak{c}$; hence $g(\mathfrak{t}) = \mathfrak{t}$. This implies that $g^{-1}Lg = L$, and $g(\mathfrak{l}) = \mathfrak{l}$.

Furthermore, $\mathfrak{l}$ is θ-stable, hence it is graded, and $\mathfrak{l}_0$ contains $\mathfrak{t}_0$. Hence $\mathfrak{t}_0$ is a Cartan subalgebra of $\mathfrak{l}_0$. Since g lies in $G_0 = G^\theta$, it leaves the grading invariant, and hence $g(\mathfrak{t}_0)$ is a Cartan subalgebra of $\mathfrak{l}_0$. So there is a $h \in L_0 \subset G_0$ with $hg(\mathfrak{t}_0) = (\mathfrak{t}_0)$ (where L_0 denotes the connected subgroup of G with Lie algebra $\mathfrak{l}_0$).

Since $h \in L$ also $hg(\mathfrak{t}) = \mathfrak{t}$. But $\mathfrak{h}$ is the centraliser of $\mathfrak{t}_0 + \mathfrak{t}$. It follows that $hg(\mathfrak{h}) = \mathfrak{h}$. Also $hg \in G_0 \subset G^\theta$, hence $(hg)|_{\mathfrak{h}} \in W^\theta$. Moreover, $(hg)|_{\mathfrak{c}} = g|_{\mathfrak{c}}$ as $h \in L$. So if we write $w = (hg)|_{\mathfrak{h}}$, then $\pi(w) = a$. □

Corollary 3.6.6. *W_0 is finite.*

Theorem 3.6.7 (Vinberg)**.** *W_0 is a complex reflection group.*

Chapter 4

Computing the little Weyl group

Finally, I consider the problem of classifying the semisimple orbits of a θ-group. The computational approach consists of an algorithm to compute a Cartan subspace, and of methods to determine the little Weyl group on the base of theoretical results.

4.1 Constructing a Cartan subspace

In this section $\mathfrak{g}$ is a reductive Lie algebra with a $\mathbb{Z}_m$-grading, $\mathfrak{g} = \oplus_{i=0}^{m-1} \mathfrak{g}_i$. The algorithm I'm going to describe, computes a Cartan subspace of $\mathfrak{g}_1$. This requires to compute the Jordan decomposition of elements of semisimple Lie algebras. Let $x \in \mathfrak{s}$, with $\mathfrak{s}$ a semisimple Lie algebra. Compute the Jordan decomposition of the adjoint map $\mathrm{ad}_{\mathfrak{s}} x = S + N$, with S semisimple and N nilpotent. As we know, there are unique $x_s, x_n \in \mathfrak{s}$ such that $S = \mathrm{ad}_{\mathfrak{s}} x_s$ and $N = \mathrm{ad}_{\mathfrak{s}} x_n$ and we can find these elements by solving systems of linear equations. Furthermore, the Jordan decomposition of x is $x = x_s + x_n$.

In the algorithm a parameter R is used. It is a positive integer, fixed throughout. The behaviour of the algorithm depends on it. The explanation of the algorithm is reported in the proof of Proposition 4.1.1.

Algorithm 1.

Input: a reductive $\mathbb{Z}_m$-graded Lie algebra $\mathfrak{g}$.
Output: a Cartan subspace of $\mathfrak{g}_1$.

(1) Let $\mathfrak{s} = [\mathfrak{g}, \mathfrak{g}]$ and let $\mathfrak{r}$ be the centre of $\mathfrak{g}$. Let $\mathfrak{s}_1 = \mathfrak{s} \cap \mathfrak{g}_1$.

(2) If $\mathfrak{s}_1 = 0$ then return $\mathfrak{g}_1$.

(3) Let $x_1, \ldots, x_m$ be a basis of $\mathfrak{s}_1$, and set $x = \sum_{i=1}^{m} c_i x_i$ where the c_i are drawn randomly

uniformly and indipendently from the set $\Omega = \{0, \dots, R\}$.

(4) If x is not nilpotent, then execute Step 4(a). Otherwise execute Step 4(b).

(a) (x not nilpotent) Compute the Jordan decomposition $x = x_s + x_n$. Let $\tilde{\mathfrak{g}}$ be the centraliser of x_s in $\mathfrak{g}$. Return the output of the algorithm when applied recursively to $\tilde{\mathfrak{g}}$, with the grading induced by the grading of $\mathfrak{g}$.

(b) (x is nilpotent) Set $\mathfrak{s}_0 = \mathfrak{s} \cap \mathfrak{g}_0$. Compute $[\mathfrak{s}_0, x]$; if the dimension of this space is equal to the dimension of $\mathfrak{s}_1$ then return $\mathfrak{g}_1 \cap \mathfrak{r}$. Otherwise return to Step 3.

Proposition 4.1.1. *If Algorithm 1. terminates, then it returns a Cartan subspace of* $\mathfrak{g}_1$. *Moreover, the probability that the algorithm terminates tends to 1 as R tends to* ∞.

Proof. We note that since $\mathfrak{g}$ is reductive, $\mathfrak{g} = \mathfrak{s} \oplus \mathfrak{r}$, with $\mathfrak{s}$ semisimple. Let θ be the automorphism corresponding to the grading of $\mathfrak{g}$, i.e., $\theta(x) = \omega^i x$ for $x \in \mathfrak{g}_i$, where ω is a primitive m-th root of unity. Then θ stabilises $\mathfrak{s}$ and $\mathfrak{r}$. Hence $\mathfrak{s}$ is also graded, where the grading is induced by the grading of $\mathfrak{g}$. Furthermore, $\mathfrak{g}_1 = \mathfrak{g}_1 \cap \mathfrak{s} \oplus \mathfrak{g}_1 \cap \mathfrak{r}$. Note that $\mathfrak{g}_1 \cap \mathfrak{r}$ is always contained in a Cartan subspace. So if $\mathfrak{g}_1 \cap \mathfrak{s} = 0$ then $\mathfrak{g}_1 \subset \mathfrak{r}$ and hence $\mathfrak{g}_1$ is a Cartan subspace of $\mathfrak{g}_1$.

If the x found in Step 3 is not nilpotent, then its semisimple part, x_s, also lies in $\mathfrak{s}$. Therefore, its centraliser, $\tilde{\mathfrak{g}}$, is strictly contained in $\mathfrak{g}$. Furthermore, it is reductive as x_s is semisimple. Hence by induction the algorithm, with input $\tilde{\mathfrak{g}}$, computes a Cartan subspace, $\mathfrak{c}$ of $\tilde{\mathfrak{g}_1}$. Then $\mathfrak{c}$ is a Cartan subspace of $\mathfrak{g}$. Indeed, x_s is contained in a Cartan subspace $\mathfrak{c}'$ of $\mathfrak{g}_1$. But $\mathfrak{c}'$ is also contained in $\tilde{\mathfrak{g}}$. Now x_s is an eigenvector of θ, so it is also an eigenvector of θ^{-1}. This implies that $\tilde{\mathfrak{g}}$ is θ-stable. Therefore, $\tilde{\mathfrak{g}}_1 = \mathfrak{g}_1 \cap \tilde{\mathfrak{g}}$. Now a $y \in \tilde{\mathfrak{g}}$ is semisimple as element of $\tilde{\mathfrak{g}}$ if and only if it is semisimple as element in $\mathfrak{g}$. It follows that $\mathfrak{c}'$ is a maximal commutative subspace of $\tilde{\mathfrak{g}}_1$ consisting of semisimple elements. In other words, it is a Cartan subspace of $\tilde{\mathfrak{g}}_1$. So $\mathfrak{c}'$ is $\widetilde{G}_0$-conjugate to $\mathfrak{c}$ (where $\widetilde{G}_0$ is the subgroup of G corresponding to $\tilde{\mathfrak{g}}_0$). Hence $\mathfrak{c}$ is a Cartan subspace of $\mathfrak{g}_1$.

If, on the other hand, x is nilpotent, then $[\mathfrak{s}_0, x]$ is the tangent space to the orbit $S_0 \cdot x$, where $S_0 \subset G_0$ is the group corresponding to $\mathfrak{s}_0$. If the dimension of this orbit equals the dimension of $\mathfrak{s}_1$, then $\mathfrak{s}_1$ contains an open nilpotent orbit (namely $S_0 \cdot x$). This implies that $\mathfrak{s}_1$ consists entirely of nilpotent elements. Indeed, the set of non-nilpotent elements in $\mathfrak{s}_1$ is open. If it is non-empty then it has to have a non-empty intersection with the open nilpotent orbit, which is not possible. Hence in this case $\mathfrak{g}_1 \cap \mathfrak{r}$ is a Cartan subspace of $\mathfrak{g}_1$.

If the algorithm does not terminate, then it enters an infinite loop in steps 3 to 5. This means that the element found in Step 3 is always nilpotent. But for large R that means that $\mathfrak{s}_1$ consists of nilpotent elements, as the set of non-nilpotent elements is open (and therefore dense, when non-empty). By [22] this implies that $\mathfrak{s}_1$ has an open nilpotent orbit. Again for large R that means that at some point a random x is found that lies in the open nilpotent orbit. But that contradicts the assumption that we have an infinite loop.

□

Remark 4.1.2. The previous proposition ensures that the algorithm works when R is large enough. In practice however, it turns out that it is enough to take a small R. In my implementation I have used $R = 2$, and hence $\Omega = \{0, 1\}$. On some occasions this makes it necessary to perform more iterations; but this is payed back by the fact that the coefficients of the elements involved are much nicer. Of course, with such a small R it is not guaranteed that the algorithm terminates. This can be remedied by increasing R if, after a few rounds of the iteration, no "good" element has been found (i.e., a semisimple element, or a nilpotent element lying in a dense orbit).

4.2 Determination of W_0

We consider the case where $\mathfrak{g}$ is a simple Lie algebra with a finite order automorphism θ. We let G be a connected and simply connected algebraic group with Lie algebra $\mathfrak{g}$. Then there exists an automorphism $\hat{\theta}$ of G, with differential equal to θ. Also, G_0 (which is defined to be the connected algebraic subgroup of G with Lie algebra $\mathfrak{g}_0$) is equal to $G^\theta = \{g \in G \mid \hat{\theta}(g) = g\}$. This follows from a theorem of Steinberg that says that the centraliser of a semisimple element in a simply connected algebraic group is connected (see [3], Theorem 3.5.6). Let $\mathfrak{c}$ be a Cartan subspace of $\mathfrak{g}_1$. I recall that $W_0 = N_{G_0}(\mathfrak{c})/Z_{G_0}(\mathfrak{c})$. According to Theorem 3.6.7 this group is generated by complex refections that act on the space $\mathfrak{c}$. We want to find a set of complex refections, given by their matrices with respect to a fixed basis of $\mathfrak{c}$, that generate W_0. Here we focus on the Lie algebras $\mathfrak{g}$ of exceptional type; however, the same methods work when $\mathfrak{g}$ is of classical type.

Let Φ be the root system of $\mathfrak{g}$ with respect to a fixed Cartan subalgebra $\mathfrak{h}$. Let $\Delta = \{\alpha_1, \dots, \alpha_l\}$ be a fixed basis of Φ. I recall (see §3.4) that W is isomorphic to the Weyl group of Φ, which is generated by the simple refections $s_i = s_{\alpha_i}$. Such a reflections acts on $\mathfrak{h}$ by $s_i(h) = h - \alpha_i(h)\alpha_i^\vee$, where

$$\alpha_i^\vee = \frac{2\hat{\alpha}_i}{(\alpha_i, \alpha_i)}$$

Now an element of W permutes the set $\{\alpha^\vee \mid \alpha \in \Phi\}$. This yields a faithful (i.e., injective) permutation representation of W. So if θ is an inner automorphism, then $\theta \in W$ and hence we can compute a generating set of W^θ by using permutation group algorithms ([10] [19]). If θ is an outer automorphism then it does not lie in W, but it still permutes the $\alpha^\vee$. So also in this case we can compute W^θ by permutation group algorithms.

Set $\mathcal{C} = \pi(W^\theta)$. Then we have the following scheme

$$N_G(\mathfrak{h}) \xrightarrow{\psi} W \supset W^\theta \xrightarrow{\pi} \mathcal{C} \supset W_0$$

(Here $\psi : N_G(\mathfrak{h}) \to N_G(\mathfrak{h})/Z_G(\mathfrak{h}) = W$ is the projection). Let $a \in \mathcal{C}$. Then $a \in W_0$ if and only if there is a $g \in N_G(\mathfrak{h})$ such that

- $\phi(g) \in W^\theta$ and $\pi(\psi(g)) = a$,

- $g \in G_0$ or, equivalently, $\hat{\theta}(g) = g$.

So, in order to construct W_0, we need to decide whether, for a given $a \in \mathcal{C}$, there exists a $g \in N_G(\mathfrak{h})$ with the above properties. For this we need an explicit realisation of G. How to obtain it depends on $\mathfrak{g}$. First we suppose that $\mathrm{Int}(\mathfrak{g}) = \mathrm{Aut}(\mathfrak{g})^o$ is simply connected as, for example, when $\mathfrak{g}$ is of type E_8, F_4, G_2. In these cases we take $G = \mathrm{Aut}(\mathfrak{g})$ and identify $\mathfrak{g}$ and the Lie algebra of G (which is $\mathrm{ad}(\mathfrak{g})$). The reason for taking this particular realisation is that we know well how to work with automorphisms of $\mathfrak{g}$. In these cases $\theta \in G = \mathrm{Aut}(\mathfrak{g})$. Hence we can define $\hat{\theta}$ by $\hat{\theta}(g) = \theta g \theta^{-1}$. So it is easy to decide whether a given $g \in G$ lies in G_0.

Let $a \in \mathcal{C}$, and $K_a = \pi^{-1}(a) = \{w \in W^\theta \mid \pi(w) = a\}$. (Note that this is a finite set.) Let $w \in K_a$, and let $\sigma_w \in G$ be an automorphism of $\mathfrak{g}$ stabilising $\mathfrak{h}$, and such that its restriction to $\mathfrak{h}$ is equal to w. Then the set of $g \in N_G(\mathfrak{h})$ such that $\psi(g) = w$ is equal to $\sigma_w Z_G(\mathfrak{h})$. Let's see how $Z_G(\mathfrak{h})$ can be described. Take $g_0 \in Z_G(\mathfrak{h})$ and consider a set of canoincal generators x_i, y_i, h_i $(1 \leq i \leq l)$ of $\mathfrak{g}$ (see §2.6). Then $g_0(h_i) = h_i$. Morover, the $g_0(x_i)$, $g_0(y_i)$, lie in $\mathfrak{g}_{\alpha_i}$,$\mathfrak{g}_{-\alpha_i}$ respectively. So $g_0(x_i) = \lambda_i x_i$, $g_0(y_i) = \mu_i y_i$. Since $[x_i, y_i] = h_i$ we get that $\lambda_i \mu_i = 1$. Conversely, if we take arbitrarily $\lambda_i \in \mathbb{C}$, $\lambda_i \neq 0$, and set $\mu_i = 1/\lambda_i$, then the h_i, $\lambda_i x_i$, $\mu_i y_i$ form a canonical set of generating set of $\mathfrak{g}$. In this way we get a corresponding automorphism of $\mathfrak{g}$ that is the identity on $\mathfrak{h}$, and so we have an explicit description of the automorphisms that are the identity on $\mathfrak{h}$ by means of $2l$ parameters $\lambda_1, \dots, \lambda_l, \mu_1, \dots \mu_l$. On the other hand g_0 is represented by its matrix relative to a fixed basis of $\mathfrak{g}$, which in this way becomes a matrix depending on the $2l$ parameters above. Now set $g = \sigma_w g_0$. Then $g \in G_0$ if and only if $\theta g = g\theta$, and this is equivalent to a system of polynomial equations in the λ_i, μ_i. Computing a Gröbner basis we can check whether this system has a solution over $\mathbb{C}$. Here it is important to note that we do not need to solve the equations. If the reduced Gröbner basis is not $\{1\}$, then the system has a solution, and hence $a \in W_0$. We perform this for all $w \in K_a$; if the resulting reduced Gröbner basis is always equal to $\{1\}$, then $a \notin W_0$.

Now suppose that $\mathrm{Aut}(\mathfrak{g})$ is not simply connected, as for example for $\mathfrak{g}$ of type E_6, E_7. Then we consider a finite dimensional irreducible representation $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$, and we let G be the connected subgroup of $\mathrm{GL}(V)$ with Lie algebra $\sigma(\mathfrak{g})$. We choose V such that G is simply connected. For types E_6, E_7 we can take the smallest dimensional representation, where V is of dimension 27 and 56 respectively. Furthermore, as σ is irreducible, the centraliser of $\sigma(g)$ in $\mathfrak{gl}(V)$ is 1-dimensional, spanned by the identity transformation. In the sequel we identify the Lie algebras $\mathfrak{g}$ and $\sigma(\mathfrak{g})$. Note that G acts on $\sigma(\mathfrak{g})$ by automorphisms $\mathrm{Ad}(g)(\rho(x)(x)) = g\rho(x)g^{-1}$. This yields a surjective map $\phi : G \to \mathrm{Int}(\mathfrak{g})$, with kernel equal to the centre of G. (In type E_6, E_7, with σ as before, this is the group of scalar matrices, with a third, respectively second, root of unity on the diagonal).

Now let $\sigma \in \mathrm{Int}(\mathfrak{g})$. Let U_σ be the space of $u \in \mathrm{End}(V)$ such that $u\rho(x) = \rho(\sigma(x))u$, for x in a basis of $\mathfrak{g}$. We can compute a basis of U_σ by solving a set of linear equations.

Consider the group

$$\widetilde{G} = N_{\mathrm{GL}(V)}(\rho(\mathfrak{g})) = \{g \in \mathrm{GL}(V) \mid g\rho(\mathfrak{g})g^{-1} = \rho(\mathfrak{g})\}$$

Then $\widetilde{G}$ acts on $\mathfrak{g}$ by automorphisms; we let $\phi : \widetilde{G} \to \mathrm{Int}(\mathfrak{g})$ be the corresponding map. (Note that $G \subset \widetilde{G}$). Then $U_\sigma \cap \mathrm{GL}(V)$ is equal to the fibre $\phi^{-1}(\sigma)$. If we let σ be the identity, then this fibre is an algebraic subgroup whose Lie algebra is $Z_{\mathfrak{gl}(V)}(\rho(\mathfrak{g}))$. Since ρ is irreducible, this is 1-dimensional. Hence, since all fibres are of the same dimension, we get that U_σ is a 1-dimensional space. However, also G has a nontrivial intersection with U_σ. Therefore, taking a basis vector u of U_σ, there is a nonzero $\lambda \in \mathbb{C}$ such that $g = \lambda u$ lies in G. The conclusion is that, up to multiplication by nonzero scalars, we can find an element of G that maps to a given $\sigma \in \mathrm{Int}(\mathfrak{g})$. Now suppose that θ is an inner automorphism. Then by the above we can compute a $\bar{\theta} \in \mathrm{GL}(V)$ such that $\lambda\bar{\theta} \in G$, for some nonzero scalar λ, and $\bar{\theta}\rho(x)\bar{\theta}^{-1} = \rho(\theta((x))$ for all $x \in \mathfrak{g}$. So we can define an automorphism $\tilde{\theta}$ of G by $\tilde{\theta}(g) = \bar{\theta}g\bar{\theta}^{-1}$. The differential of $\tilde{\theta}$ is equal to θ (after identifying $\mathfrak{g}$ and $\rho(\mathfrak{g})$). So $G_0 = \{g \in G \mid \bar{\theta}g = g\bar{\theta}\}$.

Let σ_0 be a generic automorphism of $\mathfrak{g}$, stabilising $\mathfrak{h}$, such that its restriction to $\mathfrak{h}$ is the identity. As seen before, σ_0 can be represented (with respect to a fixed basis of $\mathfrak{g}$) by a matrix whose entries are polynomials in $2l$ parameters, $\lambda_1, \dots, \lambda_l, \mu_1, \dots, \mu_l$, with $\lambda_i\mu_i = 1$. Now we take the λ_i to be the generators of a rational function field F in l indeterminates, and $\mu_i = \lambda_i^{-1}$. Then we compute a basis vector of the space U_{σ_0}, by solving a set of linear equations over F. Taking a basis vector of U_{σ_0}, we get (up to scalar multiples) a generic element of $Z_G(\mathfrak{h})$. We denote this element by g_0.

Again consider $a \in \mathcal{C}$, $K_a = \pi^{-1}(a) = \{w \in W^\theta \mid \pi(w) = a\}$, and $w \in K_a$. Let $\sigma_w \in \mathrm{Int}(\mathfrak{g})$ be such that it normalises $\mathfrak{h}$ and its restriction to $\mathfrak{h}$ coincides with w. We can compute a $g_w \in \mathrm{GL}(V)$, such that, after multiplication by a nonzero scalar, $g_w \in G$, and $g_w\rho(x)g_w^{-1} = \rho(\sigma_w(x))$ for all $x \in \mathfrak{g}$. Then $g_wZ_G(\mathfrak{h})$ is the set of elements of G that map to $w \in W$. We have $a \in W_0$ if and only if $gZ_G(\mathfrak{h}) \cap G_0$ is not empty for at least one $w \in K_a$. Consider g_wg_0: we have that $g_wZ_G(\mathfrak{h}) \cap G_0$ is not empty if and only if the polynomial equations that correspond to $\tilde{\theta}g_wg_0 = g_wg_0\tilde{\theta}$ have a solution over $\mathbb{C}$. (Note that we know g, g_0 only up to multiplication by nonzero scalars. These, however, do not affect the equations). Again by Gröbner basis calculations we can check whether these equations have a solution. Performing this for all $w \in K_a$, we can check whether a given $a \in \mathcal{C}$ lies in W_0.

Remark 4.2.1. In practice I compute g_0 slightly differently. Let $\mathfrak{h}'$ be the *standard* Cartan subalgebra (i.e., the Cartan subalgebra that is part of the Chevalley basis appearing in the construction of $\mathfrak{g}$). We get a matrix u_0 depending on parameters, that is the general form of an element in $Z_G(\mathfrak{h}')$. Secondly, we construct an automorphism σ of $\mathfrak{g}$, mapping $\mathfrak{h}$ to $\mathfrak{h}$. Then we get a $g_\sigma \in G$ such that $g_\sigma\rho(x)g_\sigma^{-1}$. We do this because the equations for u_0 are easier to solve than the ones that arise when computing a generic element of $Z_G(\mathfrak{h})$ directly.

I briefly summarise the procedure described in this section. Given a Cartan subspace $\mathfrak{c} \subset \mathfrak{g}_1$ we perform the following steps:

- Calculate (bases of) $\mathfrak{s} = Z_{\mathfrak{g}}(\mathfrak{c})$, $\mathfrak{t} = \bigoplus_{\gcd(k,m)=1} \mathfrak{g}_k \cap Z(\mathfrak{s})$, $\mathfrak{t}_0$ (which is a Cartan subalgebra of $\mathfrak{s}_0$ and $\mathfrak{h} = Z_{\mathfrak{g}}(\mathfrak{t} + \mathfrak{t}_0)$.
- Compute the root system Φ of $\mathfrak{g}$ with respect to $\mathfrak{h}$. And let W be the corresponding Weyl group.
- Compute generators of W^θ by permutation group algorithms. Set $\mathcal{C} = \pi(W^\theta)$.
- For all $a \in \mathcal{C}$ decide whether a *lifts* to an element of G_0. The elements that lift generate W_0.

Remark 4.2.2. In the last step, of course, one may restrict to a that are complex reflections. Also, once I find a set of $a \in \mathcal{C}$ that do lift to G_0, and generate a subgroup of $\mathcal{C}$ of prime index, and at the same time I have found a $b \in \mathcal{C}$ that does not lift to G_0, then I can stop.

Remark 4.2.3. I remark that for the constructions described in this section it is necessary to compute the root system of $\mathfrak{g}$ with respect to $\mathfrak{h}$. However, this Cartan subalgebra may not be split over $\mathbb{Q}$. In fact, that happens quite often. In these cases we have to work over algebraic extensions of $\mathbb{Q}$. Fortunately, MAGMA can handle these well. However, if the degree of the extension increases, then the computations tend to become much more difficult.

Remark 4.2.4. The automorphism θ is said to be N-regular if g_1 contains a regular nilpotent element. It is known that, up to conjugacy, there is exactly one N-regular inner automorphism of any given order ([17]). Also, Panyushev proved ([17]) that for N-regular θ we have that W_0 coincides with $\mathcal{C} = \pi(W^\theta)$. Finally, I remark that for the exceptional types the N-regular automorphisms have been determined in [8].

Remark 4.2.5. We can compute the degrees of the invariants that generate $\mathbb{C}[\mathfrak{c}]^{W_0}$ directly. Indeed, this last ring is isomorphic to $\mathbb{C}[\mathfrak{c}]^{G_0}$ ([22]). The space of homogeneous elements of degree k of $\mathbb{C}[\mathfrak{g}_1]^{G_0}$ is isomorphic, as G_0-module, to $\mathrm{Sym}^k(\mathfrak{g}_1)$. Now in MAGMA there are algorithms implemented for computing the decomposition of this last module into irreducibles, given such a decomposition of $\mathfrak{g}_1$. Write $\mathfrak{g}_0 = \mathfrak{s} \oplus \mathfrak{t}$, where $\mathfrak{s}$ is semisimple and $\mathfrak{t}$ a central torus. Then there is an invariant of degree k if and only if there is a 1-dimensional submodule of $\mathrm{Sym}^k(\mathfrak{g}_1)$, on which $\mathfrak{t}$ acts trivially.

Moreover, the product of the degrees of the generating invariants is equal to the order of W_0 (Theorem 1.3.8). So if this product equals the order of $\mathcal{C}$, then we can conclude $\mathcal{C} = W_0$.

This approach works well if the degrees of the generating invariants are relatively small. For higher degrees it becomes difficult to execute it, due to the complexity of the algorithm for finding the decomposition of the module $\mathrm{Sym}^k(\mathfrak{g}_1)$. However it has been fruitful (except in one case) for θ-groups corresponding to automorphisms of rank 1.

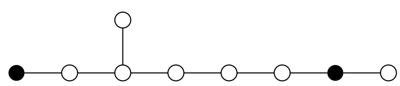
I have implemented the algorithms described above in the language of the computer algebra system MAGMA ([1]). With the help of these implementations I have computed the little Weyl groups for θ-groups corresponding to inner automorphisms of the Lie algebras of exceptional type. For the outer automorphisms of the Lie algebra of type E_6, the little Weyl group was in all cases proved to be equal to $\mathcal{C}$, using the method of Remark 4.2.5. As an example, I report the lines in MAGMA for getting W_0 in a case of outer automorphism of rank 1.

```
>R:= RootDatum( "A2A2" : Isogeny:= "SC" );
>d:= LieRepresentationDecomposition( R, [ [ 0, 1, 1, 0 ] ] , [ 1 ]);
> 0 in Weights(d);
false
> S2:= SymmetricPower( d, 2 ); > 0 in Weights(S2);
false
> S3:= SymmetricPower( d, 3 ); > 0 in Weights(S3);
true
```

In the tables I concentrate on the Lie algebras of type E because for the other types the little Weyl groups have been determined by Vinberg([22], classic types) and Levy ([15], classic types, also in characteristic $p > 0$, and [16], for G_2 and F_4, also in characteristic $p > 0$. For $\mathfrak{g}$ of type F_4 and G_2, my results agree with those of Levy ([16]). I would like to stess, however, that I have obtained all little Weyl groups explicitly, not just their isomorphism types.

In the sequel, I describe some examples. In the first one we see a case where $W_0 \neq \mathcal{C}$. The second one illustrates the use of the method outlined in Remark 4.2.5. The third one reports, at least in one case, the matrices representing the generating reflections of W_0 with respect to a certain basis.

Example 4.2.6. Let $\mathfrak{g}$ be the Lie algebra of type E_8, and θ the automorphism of order 4 with Kac diagram



The following table contains eight roots of the root system of $\mathfrak{g}$, given by their coefficients relative to a set of simple roots:

	2		0		1		1
α_1	2454321	α_2	0000001	α_3	1232110	α_4	1222210
	2		1		1		0
β_1	2343211	β_2	1121000	β_3	1111100	β_4	0111111

A Cartan subspace of $\mathfrak{g}_1$ is spanned by $x_{-\alpha_1} + x_{\alpha_2} + x_{\alpha_3} + x_{\alpha_4}$, $x_{-\beta_1} + x_{\beta_2} + x_{\beta_3} + x_{\beta_4}$.

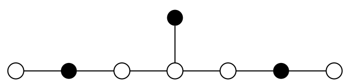
Let $i \in \mathbb{C}$ be the usual imaginary unit. Then the little Weyl group W_0 is generated by the matrices (with respect to the above basis):

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}$$

Here W_0 is strictly smaller than $\mathcal{C}$; we have $|W_0| = 32$ and $|\mathcal{C}| = 96$. The little Weyl group W_0 is isomorphic to the group $G(4, 1, 2)$ in the list of Shephard-Todd.

The invariant ring $\mathbb{C}[\mathfrak{c}]^{W_0}$ is generated by $x_1^4 + x_2^4$, $x_1^8 + x_2^8$.

Example 4.2.7. Let θ be the automorphism of order 6 of the Lie algebra of type E_7, with Kac diagram



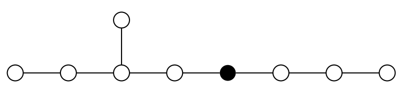
In this case the rank is 2, and $\mathcal{C} = \pi(W^\theta)$ is a complex reflection group isomorphic to $G(6, 2, 2)$. The degrees of the generating invariants of this group are 6, 6.

Here $\mathfrak{g}_0$ is isomorphic to the Lie algebra of type $A_1 + A_1 + A_3 + T_2$, where T_2 denotes a 2-dimensional central torus. As $\mathfrak{g}_0$-module G_1 decomposes as a sum of three irreducible modules with heighest weights

$$(0, 1, 0, 0, 1, -1, -1), (0, 0, 0, 1, 0, 2, -2), (1, 0, 1, 0, 0, -1, 3)$$

(here the first two coordinates correspond to the two copies of A_1, the next three coordinates to A_3 and the last two coordinates to the torus). Now with MAGMA it is possible to compute the decomposition of the modules $\mathrm{Sym}^k(\mathfrak{g}_1)$. Doing that I find that for $k \leq 5$ there are two of them. From this it follows that $\mathbb{C}[\mathfrak{c}]^{W_0}$ is generated by two invariants of degree 6. We conclude that $W_0 = \mathcal{C}$.

Example 4.2.8. Let θ be the automorphism of order 4 of the Lie algebra of type E_8, with Kac diagram



θ is realised in MAGMA as a matrix group over the number field with defining polynomial $x^4 - 2x^2 + 9$ over $\mathbb{Q}$.

In the basis

$$\{v_4+v_{176}+v_{187}+v_{193},\ v_7+v_{155}-v_{167}+v_{209},\ v_{18}+v_{157}+v_{173}-v_{177},\ v_{21}+v_{164}+v_{166}+v_{169}\}$$

the found generating reflections are given by the matrices:

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & \frac{1}{6}(-y^3-y) & 0 & 0 \\ \frac{1}{6}(y^3+y) & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

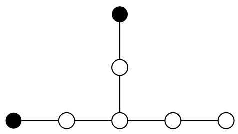
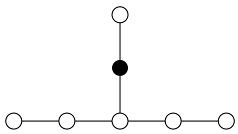
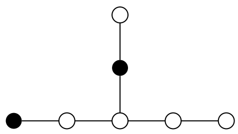
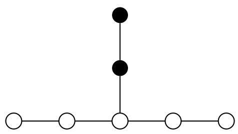
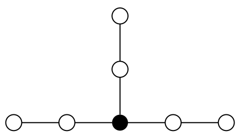
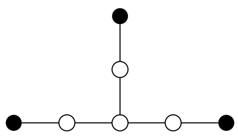
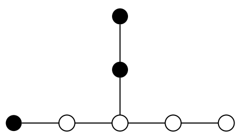
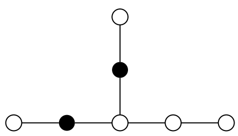
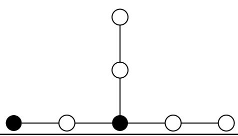
$$\begin{pmatrix} 0 & 0 & \frac{1}{12}(-y^3+3y^2+5y-3) & 0 \\ 0 & 1 & 0 & 0 \\ \frac{1}{12}(-y^3-3y^2+5y+3) & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & \frac{1}{24}(y^3+3y^2-5y-3) & \frac{1}{24}(y^3+3y^2-5y-3) \\ -\frac{1}{2} & \frac{1}{2} & \frac{1}{24}(y^3+3y^2-5y-3) & \frac{1}{24}(y^3+3y^2-5y-3) \\ \frac{1}{24}(y^3-3y^2-5y+3) & \frac{1}{24}(y^3-3y^2-5y+3) & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{24}(y^3-3y^2-5y+3) & \frac{1}{24}(y^3-3y^2-5y+3) & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

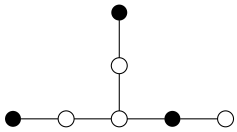
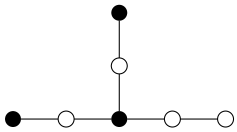
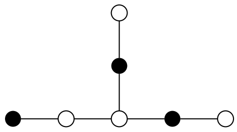
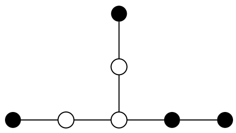
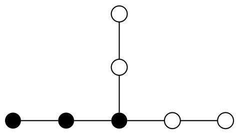
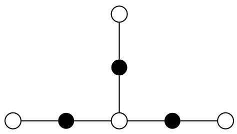
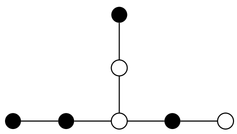
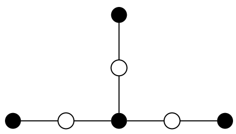
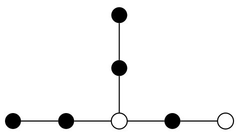
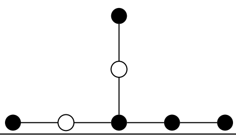
4.3 Tables

This section contains the tables of the little Weyl groups corresponding to the positive rank automorphisms of the Lie algebras of exceptional type. They agree with the results already determined by Vinberg [22], except for one case in each of the types E_6, E_7 and E_8. In those cases I find the group with number 8, wheras Vinberg found the group with number 13. In these cases the correct groups were also found by Panyushev ([17], Example 5.3, together with the inclusions in [22], §9.3) and Pervushin ([18], for the one in type E_7).

Table 4.1: Inner automorphisms of E_6 of positive rank.

order	Kac diagram	rank	N-reg	W_0
2		2	N	$G(2,1,2)$
2		4	Y	28
3		1	N	$\mathcal{C}_6$
3		1	N	$\mathcal{C}_6$
3		3	Y	25
3		2	N	$G(3,1,2)$
4		1	N	$\mathcal{C}_4$
4		1	N	$\mathcal{C}_4$
4		2	Y	8

Inner automorphisms of E_6.

4		2	N	$G(4,1,2)$
5		1	Y	$\mathcal{C}_5$
5		1	N	$\mathcal{C}_5$
5		1	N	$\mathcal{C}_5$
6		1	N	$\mathcal{C}_6$
6		1	N	$\mathcal{C}_6$
6		1	N	$\mathcal{C}_6$
6		2	Y	5
8		1	N	$\mathcal{C}_8$
8		1	Y	$\mathcal{C}_8$

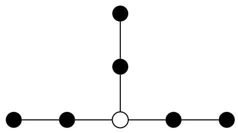
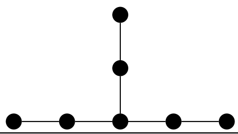
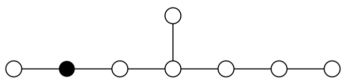
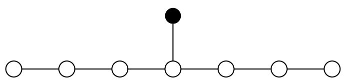
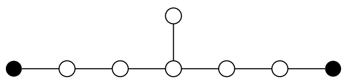
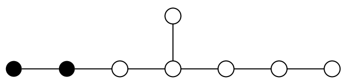
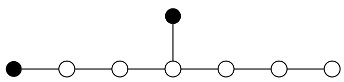
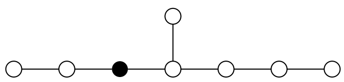
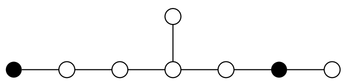
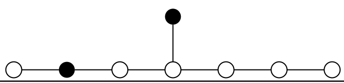
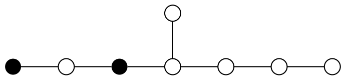
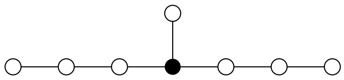
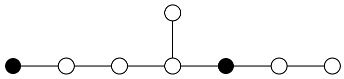
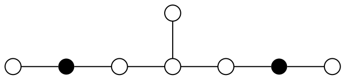
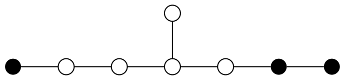
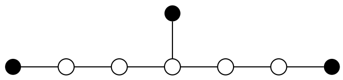
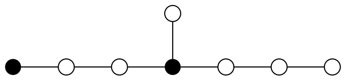
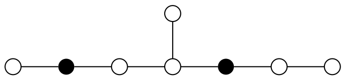
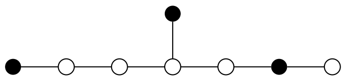
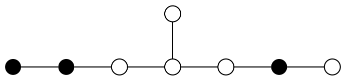
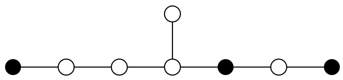
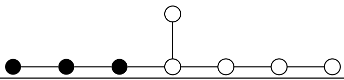
Inner automorphisms of E_6.				
9		1	Y	$\mathcal{C}_9$
12		1	Y	$\mathcal{C}_{12}$

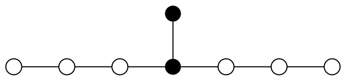
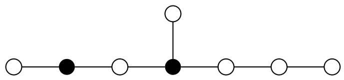
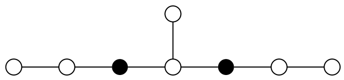
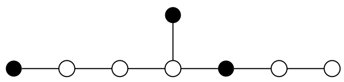
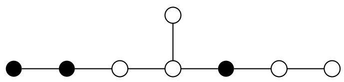
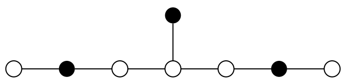
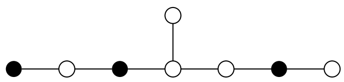
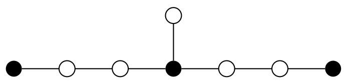
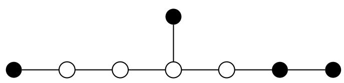
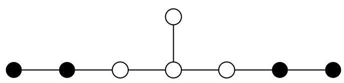
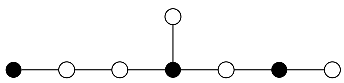
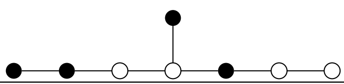
Table 4.2: Inner automorphisms of E_7 of positive rank.

order	Kac diagram	rank	N-reg	W_0
2		4	N	28
2		7	Y	36
2		3	N	$G(2,1,3)$
3		1	N	$\mathcal{C}_6$
3		1	N	$\mathcal{C}_6$
3		3	Y	26
3		2	N	$G(6,2,2)$
4		1	N	$\mathcal{C}_4$

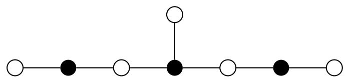
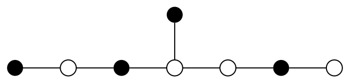
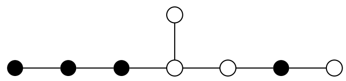
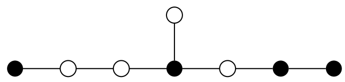
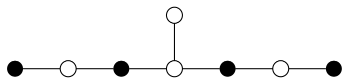
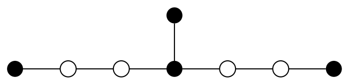
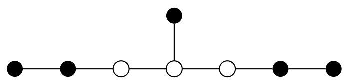
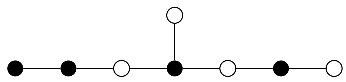
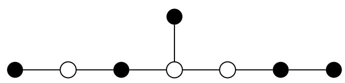
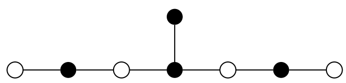
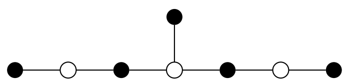
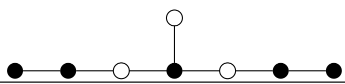
Inner automorphisms of E_7.

4		2	N	8
4		2	N	8
4		2	Y	8
4		2	N	$G(4,1,2)$
4		1	N	$\mathcal{C}_4$
4		2	N	$G(4,1,2)$
5		1	Y	$\mathcal{C}_{10}$
5		1	N	$\mathcal{C}_{10}$
5		1	N	$\mathcal{C}_5$
5		1	N	$\mathcal{C}_{10}$
5		1	N	$\mathcal{C}_5$
6		1	N	$\mathcal{C}_6$

Inner automorphisms of E_7.

6		1	N	$\mathcal{C}_6$
6		1	N	$\mathcal{C}_6$
6		1	N	$\mathcal{C}_6$
6		1	N	$\mathcal{C}_6$
6		1	N	$\mathcal{C}_6$
6		2	N	$G(6,2,2)$
6		2	N	5
6		3	Y	26
6		1	N	$\mathcal{C}_6$
6		1	N	$\mathcal{C}_6$
7		1	Y	$\mathcal{C}_{14}$
8		1	N	$\mathcal{C}_8$

Inner automorphisms of E_7.

8		1	N	$\mathcal{C}_8$
8		1	N	$\mathcal{C}_8$
8		1	N	$\mathcal{C}_8$
8		1	Y	$\mathcal{C}_8$
8		1	N	$\mathcal{C}_8$
8		1	N	$\mathcal{C}_8$
8		1	N	$\mathcal{C}_8$
9		1	Y	$\mathcal{C}_{18}$
9		1	N	$\mathcal{C}_9$
10		1	N	$\mathcal{C}_{10}$
10		1	Y	$\mathcal{C}_{10}$
10		1	N	$\mathcal{C}_{10}$

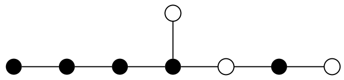
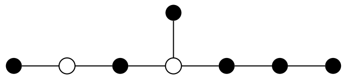
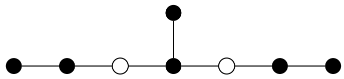
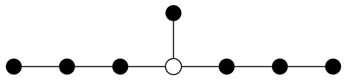
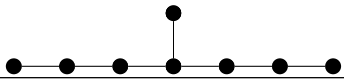
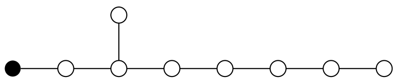
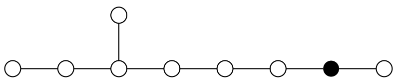
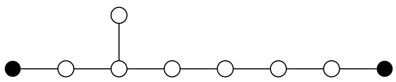
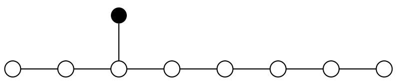
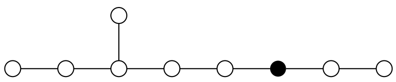
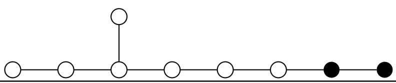
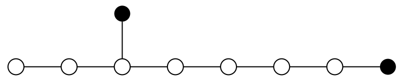
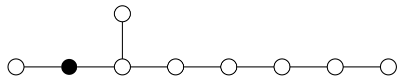
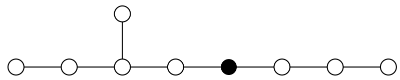
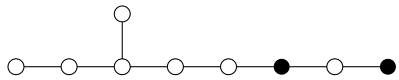
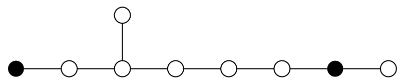
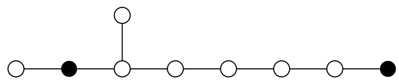
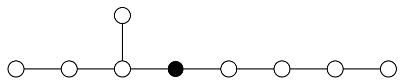
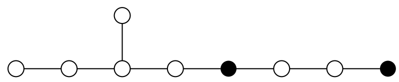
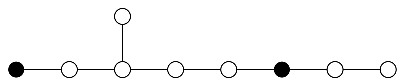
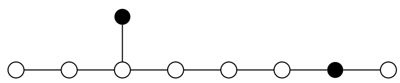
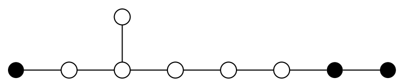
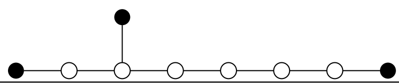
Inner automorphisms of E_7.				
12		1	N	$\mathcal{C}_{12}$
12		1	Y	$\mathcal{C}_{12}$
12		1	N	$\mathcal{C}_{12}$
14		1	Y	$\mathcal{C}_{14}$
18		1	Y	$\mathcal{C}_{18}$

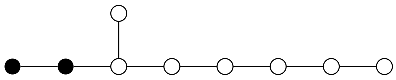
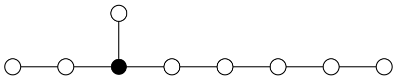
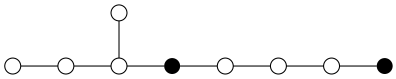
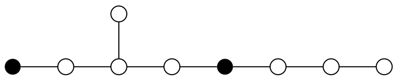
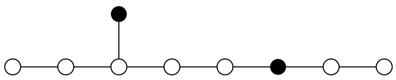
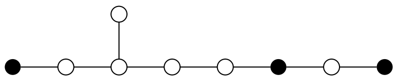
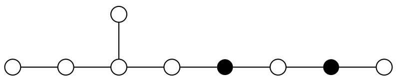
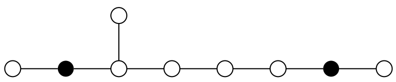
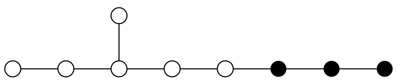
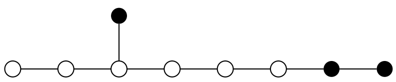
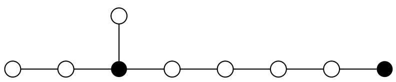
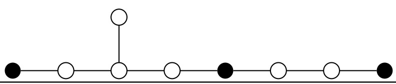
Table 4.3: Inner automorphisms of E_8 of positive rank.

order	Kac diagram	rank	N-reg	W_0
2		8	Y	37
2		4	N	28
3		2	N	$G(6,1,2)$
3		4	Y	32
3		3	N	26
3		1	N	$\mathcal{C}_6$

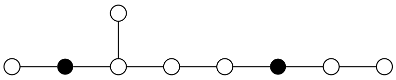
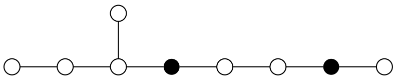
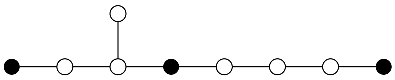
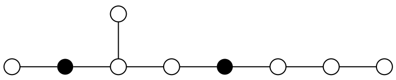
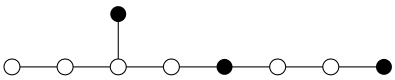
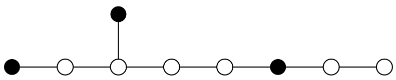
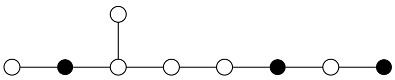
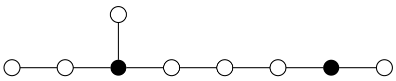
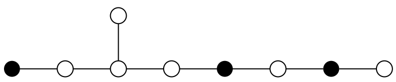
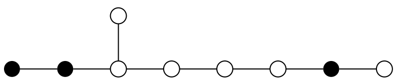
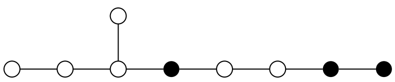
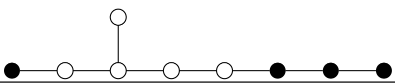
Inner automorphisms of E_8.

4		2	N	8
4		2	N	8
4		4	Y	31
4		2	N	8
4		2	N	$G(4,1,2)$
5		1	N	$\mathcal{C}_{10}$
5		2	Y	16
5		1	N	$\mathcal{C}_{10}$
5		1	N	$\mathcal{C}_{10}$
5		1	N	$\mathcal{C}_{10}$
5		1	N	$\mathcal{C}_{10}$
6		1	N	$\mathcal{C}_6$

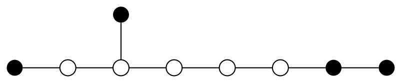
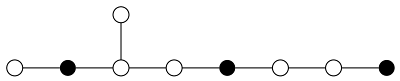
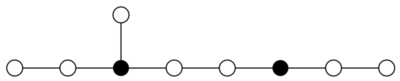
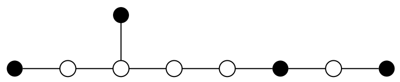
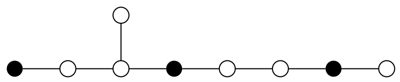
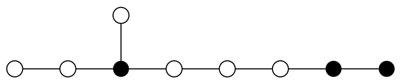
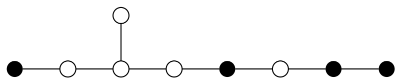
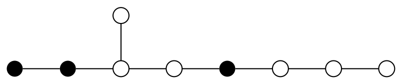
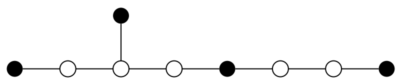
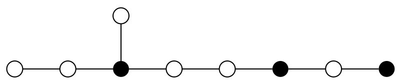
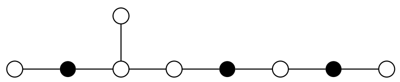
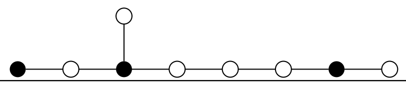
Inner automorphisms of E_8.

6		1	N	$\mathcal{C}_6$
6		1	N	$\mathcal{C}_6$
6		4	Y	32
6		2	N	$G(6,1,2)$
6		2	N	5
6		2	N	5
6		1	N	$\mathcal{C}_6$
6		3	N	5
6		1	N	$\mathcal{C}_6$
6		1	N	$\mathcal{C}_6$
7		1	N	$\mathcal{C}_{14}$
7		1	N	$\mathcal{C}_{14}$

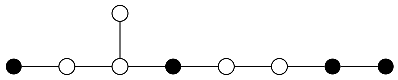
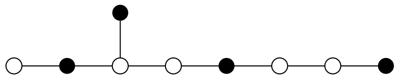
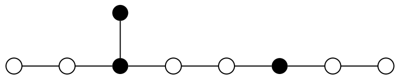
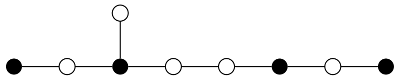
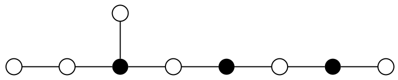
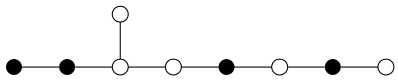
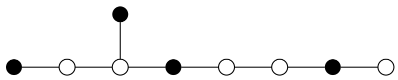
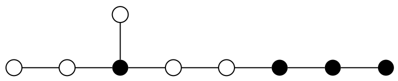
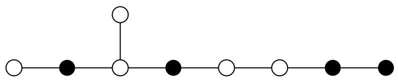
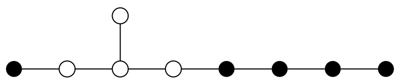
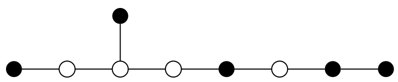
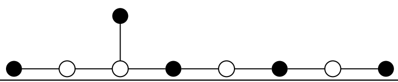
Inner automorphisms of E_8.

7		1	N	$\mathcal{C}_{14}$
7		1	Y	$\mathcal{C}_{14}$
8		1	N	$\mathcal{C}_8$
8		1	N	$\mathcal{C}_8$
8		1	N	$\mathcal{C}_8$
8		1	N	$\mathcal{C}_8$
8		1	N	$\mathcal{C}_8$
8		2	Y	9
8		1	N	$\mathcal{C}_8$
8		1	N	$\mathcal{C}_8$
8		1	N	$\mathcal{C}_8$
8		1	N	$\mathcal{C}_8$

Inner automorphisms of E_8.

8		1	N	$\mathcal{C}_8$
9		1	N	$\mathcal{C}_{18}$
9		1	N	$\mathcal{C}_{18}$
9		1	N	$\mathcal{C}_9$
9		1	N	$\mathcal{C}_{18}$
9		1	Y	$\mathcal{C}_{18}$
9		1	N	$\mathcal{C}_{18}$
10		1	N	$\mathcal{C}_{10}$
10		1	N	$\mathcal{C}_{10}$
10		2	Y	16
10		1	N	$\mathcal{C}_{10}$
10		1	N	$\mathcal{C}_{10}$

Inner automorphisms of E_8.

10		1	N	$\mathcal{C}_{10}$
12		1	N	$\mathcal{C}_{12}$
12		1	N	$\mathcal{C}_{12}$
12		2	Y	10
12		1	N	$\mathcal{C}_{12}$
12		1	N	$\mathcal{C}_{12}$
12		1	N	$\mathcal{C}_{12}$
12		1	N	$\mathcal{C}_{12}$
12		1	N	$\mathcal{C}_{12}$
12		1	N	$\mathcal{C}_{12}$
12		1	N	$\mathcal{C}_{12}$
14		1	N	$\mathcal{C}_{14}$

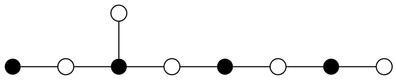
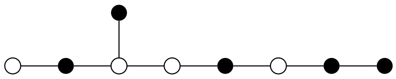
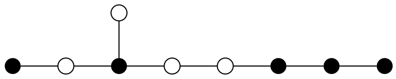
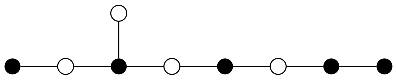
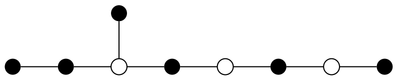
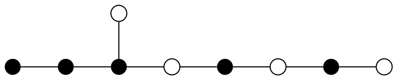
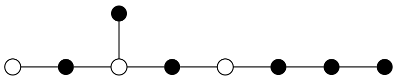
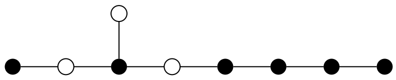
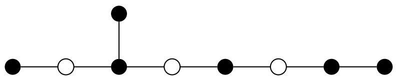
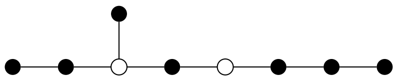
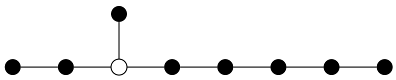
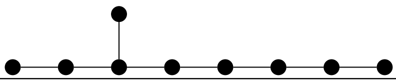
Inner automorphisms of E_8.				
14		1	N	$\mathcal{C}_{14}$
14		1	N	$\mathcal{C}_{14}$
14		1	Y	$\mathcal{C}_{14}$
15		1	Y	$\mathcal{C}_{30}$?
18		1	Y	$\mathcal{C}_{18}$
18		1	N	$\mathcal{C}_{18}$
18		1	N	$\mathcal{C}_{18}$
18		1	N	$\mathcal{C}_{18}$
18		1	N	$\mathcal{C}_{18}$
20		1	Y	$\mathcal{C}_{20}$
24		1	Y	$\mathcal{C}_{24}$
30		1	Y	$\mathcal{C}_{30}$

Table 4.4: Inner automorphisms of F_4 of positive rank.

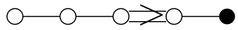
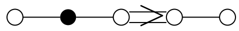
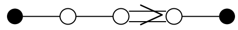
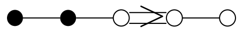
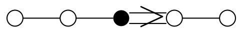
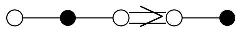
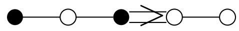
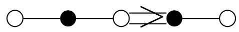
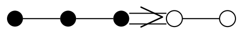
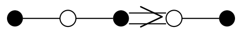
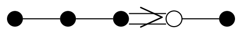
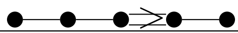
order	Kac diagram	rank	W_0
2		1	$\mathcal{C}_2$
2		4	4
3		1	$\mathcal{C}_6$
3		1	$\mathcal{C}_6$
3		2	5
4		1	$\mathcal{C}_4$
4		2	8
6		1	$\mathcal{C}_6$
6		1	$\mathcal{C}_6$
6		2	5
8		1	$\mathcal{C}_8$
12		1	$\mathcal{C}_{12}$

Table 4.5: Inner automorphisms of G_2 of positive rank.

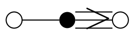
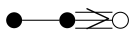
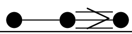
order	Kac diagram	rank	W_0
2		2	$G(6,6,2)$
3		1	$\mathcal{C}_6$
6		1	$\mathcal{C}_6$

Table 4.6: Outer automorphisms of E_6 of positive rank.

order	Kac diagram	rank	W_0
2	●—○—○⇐○—○	2	$G(3,3,2)$
2	○—○—○⇐○—●	6	35
4	○—○—○⇐●—○	2	8
4	○—●—○⇐○—○	1	$\mathcal{C}_4$
4	●—○—○⇐○—●	1	$\mathcal{C}_4$
6	●—○—○⇐●—○	3	25
6	○—●—○⇐○—●	2	$G(3,1,2)$
6	○—○—○⇐●—●	1	$\mathcal{C}_6$
6	○—○—●⇐○—○	1	$\mathcal{C}_3$
6	●—●—○⇐○—○	1	$\mathcal{C}_3$
8	●—○—○⇐●—●	1	$\mathcal{C}_8$
8	○—●—○⇐●—○	1	$\mathcal{C}_8$
10	●—○—●⇐○—●	1	$\mathcal{C}_5$
10	●—●—○⇐●—○	1	$\mathcal{C}_5$
10	○—●—○⇐●—●	1	$\mathcal{C}_5$

Bibliography

[1] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[2] Michel Broué, Gunter Malle, and Raphaël Rouquier. Complex reflection groups, braid groups, Hecke algebras. *J. Reine Angew. Math.*, 500:127–190, 1998.

[3] R. W. Carter. *Finite Groups of Lie Type, conjugacy classes and complex characters.* John Wiley & Sons, Chichester, 1985.

[4] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Springer Verlag, New York, Heidelberg, Berlin, 1992.

[5] Harm Derksen and Gregor Kemper. *Computational Invariant Theory.* Springer-Verlag, Berlin Heidelberg New York, 2002.

[6] L. Yu. Galitski and D. A. Timashev. On classification of metabelian Lie algebras. *J. of Lie Theory*, 9:125–156, 1999.

[7] W. A. de Graaf. *Lie Algebras: Theory and Algorithms*, volume 56 of *North-Holland Mathematical Library.* Elsevier Science, 2000.

[8] Willem A. de Graaf. Computing representatives of nilpotent orbits of θ-groups. *J. Symbolic Comput.*, 46:438–458, 2011.

[9] Sigurdur Helgason. *Differential geometry, Lie groups, and symmetric spaces*, volume 80 of *Pure and Applied Mathematics.* Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, 1978.

[10] Derek F. Holt, Bettina Eick, and Eamonn A. O'Brien. *Handbook of computational group theory.* Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2005.

[11] J. E. Humphreys. *Introduction to Lie Algebras and Representation Theory.* Springer Verlag, New York, Heidelberg, Berlin, 1972.

[12] N. Jacobson. *Lie Algebras.* Dover, New York, 1979.

[13] V. G. Kac. Automorphisms of finite order of semisimple Lie algebras. *Funkcional. Anal. i Priložen.*, 3(3):94–96, 1969.

[14] Gustav I. Lehrer and Donald E. Taylor. *Unitary reflection groups*, volume 20 of *Australian Mathematical Society Lecture Series.* Cambridge University Press, Cambridge, 2009.

[15] Paul Levy. Vinberg's θ-groups in positive characteristic and Kostant-Weierstrass slices. *Transform. Groups*, 14(2):417–461, 2009.

[16] Paul Levy. KW-sections for exceptional type Vinbergâs θ-groups. `arXiv:0805.2064v2 [math.RA]`, 2010.

[17] Dmitri I. Panyushev. On invariant theory of θ-groups. *J. Algebra*, 283(2):655–670, 2005.

[18] D. D. Pervushin. Invariants and orbits of the standard $(\mathrm{SL}_4(\mathbf{C}) \times \mathrm{SL}_4(\mathbf{C}) \times \mathrm{SL}_2(\mathbf{C}))$-module. *Izv. Ross. Akad. Nauk Ser. Mat.*, 64(5):133–146, 2000. English translation in Izv. Math. 64 (2000), no. 5, 1003–1015.

[19] Ákos Seress. *Permutation group algorithms*, volume 152 of *Cambridge Tracts in Mathematics.* Cambridge University Press, Cambridge, 2003.

[20] Igor R. Shafarevich. *Basic Algebraic Geometry 1.* Springer-Verlag, Heidelberg, New York, 1994.

[21] Bernd Sturmfels. *Algorithms in Invariant Theory.* Springer-Verlag, Wien, second edition, 2008.

[22] È. B. Vinberg. The Weyl group of a graded Lie algebra. *Izv. Akad. Nauk SSSR Ser. Mat.*, 40(3):488–526, 1976. English translation: Math. USSR-Izv. 10, 463–495 (1976).

[23] È. B. Vinberg, editor. *Lie groups and Lie algebras, III*, volume 41 of *Encyclopaedia of Mathematical Sciences.* Springer-Verlag, Berlin, 1994. Structure of Lie groups and Lie algebras, A translation of ıt Current problems in mathematics. Fundamental directions. Vol. 41 (Russian), Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1990, Translation by V. Minachin, Translation edited by A. L. Onishchik and È. B. Vinberg.

[24] È. B. Vinberg and A. G. Èlašvili. A classification of the three-vectors of nine-dimensional space. *Trudy Sem. Vektor. Tenzor. Anal.*, 18:197–233, 1978. English translation: Selecta Math. Sov., 7, 63-98, (1988).