CIMPA-ICTP Research School **Lattices and applications to Cryptography and Coding Theory**, Ho Chi Minh City, August 1–12, 2016.

LATTICES AND LIE ALGEBRAS

LAURA GEATTI

The purpose of these lectures is to explain the connection between complex semisimple Lie algebras and root lattices. Root lattices form a special family of lattices admitting a large amount of symmetries. Among them is the lattice L_{E_8}. The link between the above two categories of objects is provided by the notion of an abstract root system, which is a combinatorial object canonically associated to a complex semisimple Lie algebra. Root systems were introduced by W. Killing around 1890 in his attempt to classify complex simple Lie algebras.

We beging by introducing the notion of an abstact root system Δ: it is a finite set of vectors in a real vector space endowed with a positive definite scalar product. In addition, it is stable under the orthogonal reflections determined by its elements and satisfies some integrality conditions.

We will show that a root system Δ admits a *base*: by definition it is a set of elements which is a basis of the ambient vector space and whose integral span contains every element of Δ, with coefficients either all positive or all negative. All such bases are conjugate under the symmetries of Δ. In this way, the integral span of Δ coincides with the integral span of any of its bases and it is indeed a lattice. Its name *root lattice* comes from being generated by a root system.

The conditions defining a root system are very restrictive. Irreducible root systems are completely classified: they fall into four infinite families and five exceptional examples. The root system E_8 is one of them, and the lattice L_{E_8} is its associated root lattice.

Later we outline the construction of the root system a complex semisimple Lie algebra. In doing that an important role is played by the Lie algebra $\mathfrak{sl}(2,\mathbb{C})$ and its finite dimensional complex representations.

1. Abstract root systems and root lattices.

Let E be an n-dimensional vector space over $\mathbb{R}$, endowed with a positive definite inner product $(\ ,\ ): E \times E \to \mathbb{R}$.

An abstract *root system* Δ in E is a finite set with the following properties:

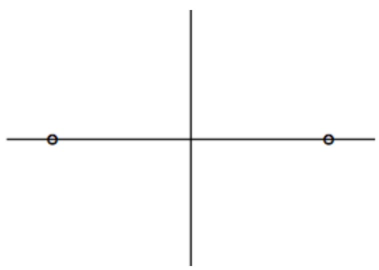
$(\mathbf{R1})$ Δ spans E and does not contain 0;
$(\mathbf{R2})$ if $\alpha \in \Delta$ and $c\alpha \in \Delta$, for some $c \in \mathbb{R}$, then $c = \pm 1$;

Date: August 11, 2016.

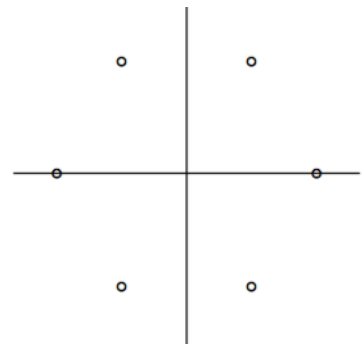
($\mathbf{R3}$) for every $\alpha \in \Delta$, the orthogonal reflection

$$s_\alpha \colon E \to E, \quad s_\alpha(x) = x - 2\frac{(x,\alpha)}{(\alpha,\alpha)}\alpha$$

maps Δ to itself;
($\mathbf{R4}$) if $\alpha, \beta \in \Delta$, then $2\frac{(\beta,\alpha)}{(\alpha,\alpha)} \in \mathbb{Z}$.



A root system in $\mathbb{R}$.



A root system in $\mathbb{R}^2$: the vertices of a regular hexagon.

The subgroup W of $GL(E)$ generated by the reflections σ_α, for $\alpha \in \Delta$, is called the *Weyl group* of the root system Δ. It is a finite group, as it is a subgroup of the permutations of the finite set Δ.

• Condition ($\mathbf{R3}$) implies that if $\alpha \in \Delta$ then also $-\alpha \in \Delta$.
• The integer $2\frac{(\beta,\alpha)}{(\alpha,\alpha)}$ is referred to as the *Cartan integer* $c_{\beta\alpha}$. Because of condition ($\mathbf{R4}$) a root system is a very rigid object. Denote by $\widehat{\alpha\beta}$ the angle between α and β (with respect to the Euclidean structure of E). Then

$$2\frac{(\beta,\alpha)}{(\alpha,\alpha)} \text{ and } 2\frac{(\alpha,\beta)}{(\beta,\beta)} \in \mathbb{Z} \qquad \Rightarrow \qquad 2\frac{(\beta,\alpha)}{(\alpha,\alpha)} \cdot 2\frac{(\alpha,\beta)}{(\beta,\beta)} = 2\frac{|\beta|}{|\alpha|}\cos\widehat{\alpha\beta} \cdot 2\frac{|\alpha|}{|\beta|}\cos\widehat{\alpha\beta} = 4(\cos\widehat{\alpha\beta})^2 \in \mathbb{Z}.$$

It follows that

$$4(\cos\widehat{\alpha\beta})^2 = 0, 1, 2, 3, 4$$

which implies

$$2\cos\widehat{\alpha\beta} = 0, \pm 1, \pm\sqrt{2}, \pm\sqrt{3}, \pm 2.$$

Let's look what we find by combining for example

$$\underbrace{\frac{|\beta|}{|\alpha|}2\cos\widehat{\alpha\beta}}_{\in\mathbb{Z}} \cdot \underbrace{\frac{|\alpha|}{|\beta|}2\cos\widehat{\alpha\beta}}_{\in\mathbb{Z}} = 2 \qquad \text{and} \qquad 2\cos\widehat{\alpha\beta} = \sqrt{2}.$$

The integers factors on the left-hand side of the first relation above must have the same sign and one of the two must have modulus 2, say $\frac{|\beta|}{|\alpha|}2\cos\widehat{\alpha\beta}$ (and the other one modulus 1). It follows that

$$\cos\widehat{\alpha\beta} = \sqrt{2}/2, \quad \widehat{\alpha\beta} = \pi/4 \qquad \text{and} \qquad |\beta| = \sqrt{2}|\alpha|.$$

In other words, the combination of the integrality conditions force the angle between α and β (which are not orthogonal nor parallel) and the ratio between their lengths.

Going through all cases, one finds that for a pair of *nonproportional roots* $\alpha, \beta \in \Delta$, up to switching them, the only possibilities are the ones listed in the next table.

Table 1

- (a) $2\frac{(\beta,\alpha)}{(\alpha,\alpha)} = 0$ $2\frac{(\alpha,\beta)}{(\beta,\beta)} = 0$ $\widehat{\alpha\beta} = \pi/2$ $|\beta|, |\alpha|$ arbitrary
- (b) $2\frac{(\beta,\alpha)}{(\alpha,\alpha)} = 1$ $2\frac{(\alpha,\beta)}{(\beta,\beta)} = 1$ $\widehat{\alpha\beta} = \pi/3$ $|\beta| = |\alpha|$
- (c) $2\frac{(\beta,\alpha)}{(\alpha,\alpha)} = -1$ $2\frac{(\alpha,\beta)}{(\beta,\beta)} = -1$ $\widehat{\alpha\beta} = 2\pi/3$ $|\beta| = |\alpha|$
- (d) $2\frac{(\beta,\alpha)}{(\alpha,\alpha)} = 1$ $2\frac{(\alpha,\beta)}{(\beta,\beta)} = 2$ $\widehat{\alpha\beta} = \pi/4$ $|\beta| = \sqrt{2}|\alpha|$
- (e) $2\frac{(\beta,\alpha)}{(\alpha,\alpha)} = -1$ $2\frac{(\alpha,\beta)}{(\beta,\beta)} = -2$ $\widehat{\alpha\beta} = 3\pi/4$ $|\beta| = \sqrt{2}|\alpha|$
- (f) $2\frac{(\beta,\alpha)}{(\alpha,\alpha)} = 1$ $2\frac{(\alpha,\beta)}{(\beta,\beta)} = 3$ $\widehat{\alpha\beta} = \pi/6$ $|\beta| = \sqrt{3}|\alpha|$
- (g) $2\frac{(\beta,\alpha)}{(\alpha,\alpha)} = -1$ $2\frac{(\alpha,\beta)}{(\beta,\beta)} = -3$ $\widehat{\alpha\beta} = 5\pi/6$ $|\beta| = \sqrt{3}|\alpha|$

Later we will use the following fact.

Lemma 1. *Let $\alpha, \beta \in \Delta$ be non-proportional roots. If $(\alpha, \beta) > 0$, then $\alpha - \beta$ is a root. Likewise if $(\alpha, \beta) < 0$, then $\alpha + \beta$ is a root.*

Proof. If $(\alpha, \beta) > 0$, then, after possibly switching α and β, we may assume $2\frac{(\beta,\alpha)}{(\alpha,\alpha)} = 1$ (see above table). Then $\alpha - \beta = -s_\alpha(\beta)$, which is a root by (**R3**). The second statement follows in a similar way. $\square$

A *base* of a root system Δ is a subset Π which is a basis of the vector space E and such that every element of Δ can be written as a linear combination of elements of Π with integer coefficients, *all non-negative or all non-positive*.

The link between root systems and *root lattices* is provided by the following theorem.

Theorem 2. *A root system Δ admits a base.*

Proof. Fix $t \in E$ with property that $(t, \alpha) \neq 0$, for every $\alpha \in \Delta$: for such t one can take any element in $E \backslash \bigcup_\alpha \alpha^\perp$.

Then $\Delta = \Delta^+ \bigcup -\Delta^+$, where $\Delta^+ = \{\alpha \ : \ (t, \alpha) > 0\}$: clearly if $\alpha \in \Delta^+$, then $-\alpha \in -\Delta^+$.

Call a root in Δ^+ *simple* or *indecomposable* if it not the sum of roots in Δ^+. We claim that every $\alpha \in \Delta^+$ can be written as a sum of indecomposable roots with non-negative integer coefficients: if α is indecomposable, we are done. Otherwise write $\alpha = \beta + \gamma$, with $\beta, \gamma \in \Delta^+$. Note that $(t, \alpha) = (t, \beta) + (t, \gamma)$, with $(t, \beta), (t, \gamma) > 0$ and strictly smaller than (t, α). Since Δ is finite, the set of numbers $\{(t, \alpha)\}_{\alpha \in \Delta^+}$ has a minimum. Hence after finitely many steps we obtain the desired decomposition.

Denote by Π the set of indecomposable roots in Δ^+. We are going to show that Π is a base of Δ. The above arguments already show that every root in Δ is a $\mathbb{Z}$-linear combination of elements of Π, with coefficients either all positive or all negative. It remains to prove that the elements of Π are linearly independent.

Observe first that $(\alpha, \beta) \leqslant 0$, for all $\alpha, \beta \in \Pi$: otherwise, if it were $(\alpha, \beta) > 0$, then $\gamma = \alpha - \beta$ would be a root by Lemma 1. If $\gamma \in \Delta^+$, then $\alpha = \gamma + \beta$; likewise, if $\gamma \in -\Delta^+$, then $\beta = \gamma + \alpha$. In both cases the indecomposability of either α or of β is contradicted.

Now suppose that an $\mathbb{R}$-linear combination of the elements of Π is zero. Collecting the coefficients with the same sign, we can rewrite it as

$$\sum x_\alpha \alpha = \sum y_\beta \beta$$

with $\alpha' s$ and $\beta' s$ contained in disjoint subsets of Π and the coefficients x_α and y_β all non-negative. Set $\lambda := \sum x_\alpha \alpha = \sum y_\beta \beta$. Since $(\alpha, \beta) \leqslant 0$, for all $\alpha, \beta \in \Pi$, $\alpha \neq \beta$, one has

$$0 \leqslant (\lambda, \lambda) = (\sum x_\alpha \alpha, \sum y_\beta \beta) = \sum x_\alpha y_\beta (\alpha, \beta) \leqslant 0,$$

which implies $\lambda = 0$. Now $(t, \lambda) = \sum_\alpha x_a (t, \alpha) = 0$ and $(t, \alpha) > 0$ for all $\alpha \in \Pi$, forces $x_\alpha = 0$ for all α. In the same way one can show that $y_\beta = 0$ for all β. So the elements of Π are linearly independent and the proof of the theorem is complete. □

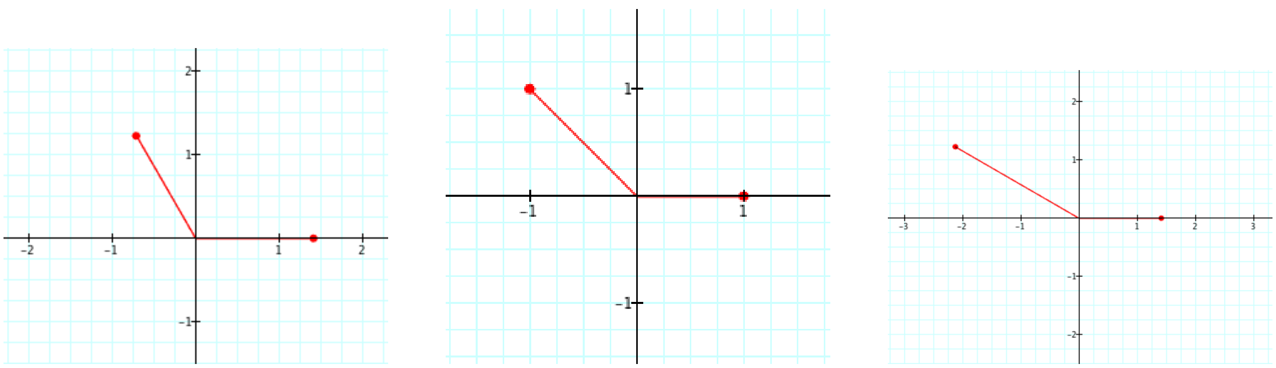
Remark 3. Since a base of a root system Δ is also a basis of the vector space E, every base has the same number of elements, equal to the dimension of E. One can show that the Weyl group acts transitively on the set of bases of Δ (cf. [Hu], Thm. 10.3, p. 51, or [Se], Thm.2, p.33).

The *root lattice* L_Δ associated to a root system Δ is by definition the integral span of the elements of Δ. By the above theorem it is indeed a lattice and by Remark 3 it coincides with the integral span of any of its bases Π

$$L_\Delta := \mathrm{Span}_{\mathbb{Z}}(\Delta) = \mathrm{Span}_{\mathbb{Z}}(\Pi).$$

We will see that different root systems may give rise to isomorphic or homothetic root lattices. Because of its definition, a root lattice L_Δ inherits all the symmetries of the root system Δ. The automorphism group of the root system Δ is given by the semidirect product of the Weyl group W and S, the group of permutations of Δ leaving the Cartan integers invariant, namely $Aut(\Delta) = W \cdot S$ (see [Se], Prop.9, p. 35). Note that, by [Se], Prop.8, p.35, the elements of S are induced by linear isomorphisms of the vecor space E.

Remark 4. The notion of a base of a root system Δ is more restrictive than the notion of a basis of the associated lattice L_Δ: the angle between arbitrary elements of a base Π of Δ is necessarily obtuse, equivalently $(\alpha, \beta) \leqslant 0$, for all $\alpha, \beta \in \Pi$, $\alpha \neq \beta$. In fact, if it were $(\alpha, \beta) > 0$ for some $\alpha, \beta \in \Pi$, then $\alpha - \beta$ would be a root by Lemma 1. This would contradict the definition of a base of a root system, which requires that every element $\alpha \in \Delta$ is an integral combination of elements of Π, with coefficients either all non-negative or all non-positive.



Bases of root systems in $\mathbb{R}^2$, corresponding to cases (c), (e) and (g) in Table 1.

Exercise 5. Let Δ be a root system in a vector space E with inner product $(\ ,\ )$. Then Δ is also a root system in E with inner product $c(\ ,\ )$, for some $c \in \mathbb{R}_{>0}$. Conversely, let Δ be a root system in a vector space E both with inner products $(\ ,\ )_1$ and $(\ ,\ )_2$. Then $(\ ,\ )_1 = c(\ ,\ )_2$, for some $c \in \mathbb{R} > 0$.

Exercise 6. Let ϕ be an orthogonal linear transformation of E preserving the root system Δ. Show that
(a) $\frac{2(\phi(\beta),\phi(\alpha))}{(\phi(\alpha),\phi(\alpha))} = \frac{2(\beta,\alpha)}{(\alpha,\alpha)}$, for all $\alpha, \beta \in \Delta$;
(b) $s_{\phi(\alpha)} = \phi \circ s_\alpha \circ \phi^{-1}$, for all $\alpha \in \Delta$.

Remark 7. Part (b) of the above excercise and the fact that every element of Δ can be mapped into a given base by some element $w \in W$ (cf. [Se], Thm.2, p. 33), implies that the Weyl group W is already generated by the reflections in the simple roots.

Example 8. (**The inverse root system**). Let Δ be a root system in E. To every $\alpha \in \Delta$ there is associated the element $\alpha^\vee := \frac{2\alpha}{(\alpha,\alpha)} \in E$. The set

$$\Delta^\vee = \{\alpha^\vee \mid \alpha \in \Delta\}$$

is another root system in E. It is called the *inverse root system*, as the map $\alpha \mapsto \frac{2\alpha}{(\alpha,\alpha)}$ is the inversion in the sphere of radius $\sqrt{2}$ in E. It is easy to see that $(\alpha^\vee)^\vee = \alpha$, for all $\alpha \in \Delta$, implying that $(\Delta^\vee)^\vee = \Delta$.
As an excercise, let us show that $\Delta^\vee$ satisfies the four axioms of a root system:
It is clear that $\Delta^\vee$ satisfies ($\mathbf{R1}$) and ($\mathbf{R4}$).
($\mathbf{R2}$): suppose that for some $\alpha, \beta \in \Delta$ and $c \in \mathbb{R}$ one has

$$c\frac{2\alpha}{(\alpha,\alpha)} = \frac{2\beta}{(\beta,\beta)} \quad \Leftrightarrow \quad c\frac{(\beta,\beta)}{(\alpha,\alpha)}\alpha = \beta.$$

Then, by ($\mathbf{R2}$) applied to Δ, one finds

$$c\frac{(\beta,\beta)}{(\alpha,\alpha)} = \pm 1 \quad \Leftrightarrow \quad c = \pm\frac{(\alpha,\alpha)}{(\beta,\beta)}.$$

This implies $\alpha = \pm\beta$, respectively, and likewise $\alpha^\vee = \pm\beta^\vee$.
($\mathbf{R3}$): we are going to show that $s_{\alpha^\vee}(\beta^\vee) = (s_\alpha(\beta))^\vee$. One has

$$s_{\alpha^\vee}(\beta^\vee) = \beta^\vee - (\beta^\vee, (\alpha^\vee)^\vee)\alpha^\vee = \frac{2\beta}{(\beta,\beta)} - (\frac{2\beta}{(\beta,\beta)}, \alpha)\frac{2\alpha}{(\alpha,\alpha)}$$

$$(s_\alpha(\beta))^\vee = \frac{2s_\alpha(\beta)}{(s_\alpha(\beta), s_\alpha(\beta))} = \frac{2(\beta - (\beta,\alpha^\vee)\alpha)}{(s_\alpha(\beta), s_\alpha(\beta))} = \frac{2(\beta - (\beta,\alpha^\vee)\alpha)}{(\beta,\beta)} = s_{\alpha^\vee}(\beta^\vee).$$

In the last equality we used the fact that each reflection s_α is an isometry for $(\ , \ )$, hence $(s_\alpha(\beta), s_\alpha(\beta)) = (\beta,\beta)$.

• If Π is a base of Δ, then $\Pi^\vee$ is a base of $\Delta^\vee$ (the proof is left as an excercise).

2. The classification of irreducible root systems.

A root system $\Delta \subset E$ is called *irreducible* if it cannot be partitioned into the union of two proper subsets $\Delta' \cup \Delta''$, such that each root in one set is orthogonal to each root in the other. If Δ is not irreducible, then E is the orthogonal direct sum of vector spaces E' and E'', with Δ' a root system in E' and Δ'' a root system in E'' (a proof is left as an excercise). Irreducible root systems are classified. They fall into four infinite families, A_n, B_n, C_n, D_n, and five sporadic examples E_6, E_7, E_8, F_4 and G_2.

For every $m \geqslant 1$, denote by e_i the i^{th} vector of the canonical basis of $\mathbb{R}^m$. The inner product $(\ , \ )$ on $\mathbb{R}^m$ is the standard one. Here is a realization of all irreducible root systems, without repetitions (see [Bou]).

• **Type** $A_n,\ n \geqslant 1$
In the space $\mathbb{R}^{n+1}$

$$A_n := \{e_i - e_j \mid 1 \leqslant i, j \leqslant n+1,\ i \neq j\};$$

a base of A_n is given by $\Pi = \{e_i - e_{i+1} \mid 1 \leqslant i \leqslant n\}$.

• **Type** $B_n,\ n \geqslant 2$
In the space $\mathbb{R}^n$

$$B_n := \{\pm e_i \pm e_j,\ \pm e_i \mid 1 \leqslant i < j \leqslant n\};$$

A base of B_n is given by $\Pi = \{e_i - e_{i+1},\ e_n \mid 1 \leqslant i \leqslant n-1\}$.

• **Type** $C_n,\ n \geqslant 3$
In the space $\mathbb{R}^n$

$$C_n := \{\pm e_i \pm e_j,\ \pm 2e_i \mid 1 \leqslant i < j \leqslant n\};$$

a base of C_n is given by $\Pi = \{e_i - e_{i+1},\ 2e_n \mid 1 \leqslant i \leqslant n-1\}$.

• **Type** $D_n,\ n \geqslant 4$
In the space $\mathbb{R}^n$

$$D_n := \{\pm e_i \pm e_j \mid 1 \leqslant i < j \leqslant n\} = \{\alpha \in \mathbb{Z}^n \mid (\alpha, \alpha) = 2\};$$

a base of D_n is given by $\Pi = \{e_i - e_{i+1},\ e_{n-1} + e_n \mid 1 \leqslant i \leqslant n-1\}$.

• **Type** G_2
In the space $\mathbb{R}^3$

$$\begin{aligned} G_2 &:= \{\pm(e_2 - e_3), \pm(e_1 - e_3), \pm(e_1 - e_2), \pm(2e_1 - e_2 - e_3), \pm(2e_2 - e_1 - e_3), \pm(2e_3 - e_1 - e_2)\} \\ &= \{\alpha \in \mathbb{Z}^3 \cap \{x_1 + x_2 + x_3 = 0 \mid (\alpha, \alpha) = 2 \text{ or } (\alpha, \alpha) = 6\}; \end{aligned}$$

a base of G_2 is given by $\Pi = \{(e_1 - e_2), (-2e_1 + e_2 + e_3)\}$.

• **Type** F_4
In the space $\mathbb{R}^4$

$$\begin{aligned} F_4 &:= \{\ \pm e_i,\ 1 \leqslant i \leqslant 4,\ \pm(e_i \pm e_j),\ 1 \leqslant i < j \leqslant 4,\ \frac{1}{2}(\pm e_1 \pm e_2 \pm e_3 \pm e_4)\} \\ &= \{\alpha \in \mathbb{Z}^4 + \mathbb{Z}(e_1 + e_2 + e_3 + e_4)/2 \mid (\alpha, \alpha) = 2\}; \end{aligned}$$

a base of F_4 is given by $\Pi = \{(e_2 - e_3), (e_3 - e_4), e_4, \frac{1}{2}(e_1 - e_2 - e_3 - e_4)\}$.

• **Type** E_8
In the space $\mathbb{R}^8$

$$E_8 = \{\pm e_i \pm e_j,\ 1 \leqslant i < j \leqslant 8, \quad \frac{1}{2}\sum_{i=1}^{8}(-1)^{\nu(i)}e_i, \quad \sum_{i=1}^{8}\nu(i) = even\};$$

a base of E_8 is given by
$\Pi = \{\frac{1}{2}(e_1+e_8)-\frac{1}{2}(e_2+e_3+e_4+e_5+e_6+e_7),\ e_1+e_2,\ e_2-e_1,\ e_3-e_2,\ e_4-e_3,\ e_5-e_4,\ e_6-e_5,\ e_7-e_6\}.$

• **Type** E_7
In the space $\mathbb{R}^8$

$$E_7 = \{\pm e_i \pm e_j,\ 1 \leqslant i < j \leqslant 6,\ \pm(e_7 - e_8),\ \pm\frac{1}{2}(e_7 - e_8 + \sum_{i=1}^{6}(-1)^{\nu(i)}e_i), \quad \sum_{i=1}^{6}\nu(i) = odd\};$$
$$= E_8 \cap \{e_8 + e_7\}^{\perp};$$

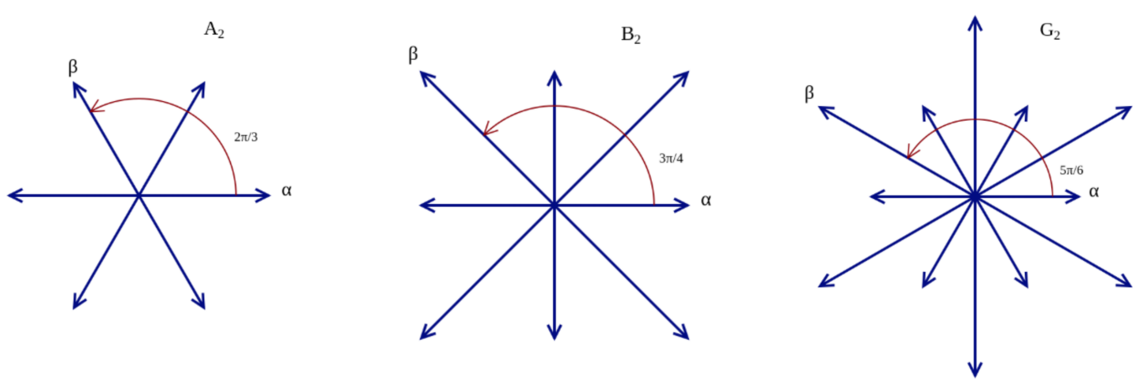
a base of E_7 is given by the first 7 vectors of the above base of E_8.

• **Type** E_6
In the space $\mathbb{R}^8$

$$E_6 = \{\pm e_i \pm e_j,\ 1 \leqslant i < j \leqslant 5,\ \pm\frac{1}{2}(e_7 - e_8 - e_6 + \sum_{i=1}^{5}(-1)^{\nu(i)}e_i), \quad \sum_{i=1}^{5}\nu(i) = even\};$$
$$= E_8 \cap \{e_8 + e_7\}^{\perp} \cap \{e_8 + e_6\}^{\perp};$$

a base of E_6 is given by the first 6 vectors of the above base of E_8.

It follows from the classification that there are three distinct irreducible root systems in the plane, namely A_2, B_2 and G_2:



All the irreducible root systems in the plane.

Example 9. Using the above description, let's show that $\mathbf{A_2}$ satisfies axioms $(R1)-(R4)$.

• It is easy to see that the elements in Π generate the plane $x_2+x_2+x_3=0$, hence $(R1)$ is satisfied.
• It is immediate from the list of elements in A_2 that also $(R2)$ is satisfied.
•To check $(R3)$, it is sufficient to show that the set of roots in A_2 is stable under the symmetries in the roots in Π (cf. Remark 7):

$$s_{e_1-e_2}(e_1-e_2)=-(e_1-e_2),\quad s_{e_1-e_2}(e_2-e_3)=(e_1-e_3),\quad s_{e_1-e_2}(e_1-e_3)=(e_2-e_3);$$
$$s_{e_2-e_3}(e_2-e_3)=-(e_2-e_2),\quad s_{e_2-e_3}(e_1-e_2)=(e_1-e_3),\quad s_{e_2-e_3}(e_1-e_3)=(e_1-e_2).$$

Obviously...if $s_\alpha(\beta)\in\Delta$, also $s_\alpha(-\beta)\in\Delta$.
• Finally, observe that $(\alpha,\alpha)=2$, for all $\alpha\in A_2$. Hence $2\frac{(\beta,\alpha)}{(\alpha,\alpha)}=(\beta,\alpha)$, which is an integer for all $\alpha,\beta\in A_2$. So also $(R4)$ is satisfied.

Exercise 10. Verify that $\mathbf{B_2}$ and $\mathbf{G_2}$ satisfy axioms $(R1)-(R4)$.

Exercise 11. Prove that
(a) $\Delta=\Delta^\vee$, for $\Delta=A_n,\ D_n,\ E_6,\ E_7,\ E_8$.
Two root systems $\Delta\subset(E,(\ ,\ ))$ and $\Delta'\subset(E',(\ ,\ )')$ are said *isomorphic* if there exists a vector space isomorphism (not necessarily an isometry) $\phi\colon E\to E'$, mapping Δ onto Δ' and such that

$$\frac{2(\phi(\beta),\phi(\alpha))}{(\phi(\alpha),\phi(\alpha))}=\frac{2(\beta,\alpha)}{(\alpha,\alpha)},\qquad\forall\ \alpha,\ \beta\in\Delta.$$

Show that
(b) $B_n^\vee\cong C_n$.
(c) $G_2^\vee\cong G_2$.
(d) $F_4^\vee\cong F_4$.

• **The Cartan matrix of Δ.** Let Δ be a root system and let $\Pi=\{\alpha_1,\ldots,\alpha_n\}$ be a base of Δ. Its associated Cartan matrix is the $n\times n$ matrix with integral entries

$$c_{ii}=c_{\alpha_i\alpha_i}=2,\ \text{for}\ i=1,\ldots,n,\qquad c_{ij}=c_{\alpha_i\alpha_j}:=(\alpha_i,\alpha_j^\vee)=\frac{2(\alpha_i,\alpha_j)}{(\alpha_j,\alpha_j)},\quad\text{for}\ i\neq j.$$

If the root system is not irreducible, the Cartan matrix is block diagonal with the Cartan matrices of the irreducible components as blocks. For example, the Cartan matrices of A_2 , G_2 and F_4 (in the description of the previous section) are given by

$$\begin{pmatrix}2&-1\\-1&2\end{pmatrix},\qquad\begin{pmatrix}2&-1\\-3&2\end{pmatrix},\qquad\begin{pmatrix}2&-1&0&0\\-1&2&-2&0\\0&-1&2&-1\\0&0&-1&2\end{pmatrix},$$

respectively. The Cartan matrix is always an invertible matrix, since its columns are multiples of the columns of the Gram matrix of the base $\alpha_1, \ldots, \alpha_n$. The Cartan matrix of the inverse root system $\Delta^\vee$ is the transpose of the Cartan matrix of Δ. In particular, the Cartan matrix is symmetric when $\Pi = \Pi^\vee$. In that case, it coincides with the Gram matrix of $\alpha_1, \ldots, \alpha_n$.

Note that by Remark 3 and Excercise 6 (a), the Cartan matrix remains the same when we transform the given base by the action of the Weyl group. Hence the Cartan matrix only depends on the labelling of the roots in Π and on the root system Δ. If we choose $\Pi' = \{(-2e_1 + e_2 + e_3), (e_1 - e_2)\}$ for G_2, the corresponding Cartan matrix is

$$\begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix}.$$

A root system Δ can be reconstructed from its Cartan matrix (see [Hu], Ch. 3, Sect.11).

Exercise 12. Compute the Cartan matrix of the root systems B_3 and C_3.

3. Root lattices

For every $m \geqslant 1$, denote by e_i the i^{th} vector of the canonical basis of $\mathbb{R}^m$, and by $\mathbb{Z}^m := \mathrm{Span}_{\mathbb{Z}}\{e_1, \ldots, e_m\}$ the integral lattice in $\mathbb{R}^m$. In this section we describe the root lattices arising from the various root systems. We will see that in some cases non-isomorphic root systems give rise to isomorphic root lattices.

Lemma 13. *The root lattice L_{A_n} is given by*

$$L_{A_n} = \mathbb{Z}^{n+1} \cap \{x_1 + \ldots + x_{n+1} = 0\} = \{\sum_{i=1}^{n+1} a_i e_i \mid a_i \in \mathbb{Z},\ \sum_{i=1}^{n+1} a_i = 0\} \subset \mathbb{R}^{n+1}.$$

Proof. By the description of A_n given in Section 2, an element $v \in L_{A_n}$ is of the form

$$v = a_1(e_1 - e_2) + \ldots + a_n(e_n - e_{n+1}) = a_1 e_1 + (a_2 - a_1)e_2 + \ldots + (a_n - a_{n-1})e_n - a_n e_{n+1},$$

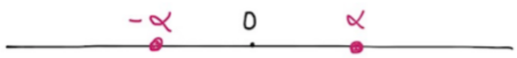
with $a_i \in \mathbb{Z}$. For such a vector the sum of the coordinates is zero

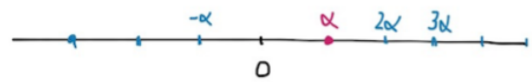
$$a_1 + (a_2 - a_1) + \ldots + (a_n - a_{n-1}) - a_n = 0.$$

Conversely, a vector $v = \sum_{i=1}^{n+1} a_i e_i$, with $\sum_{i=1}^{n+1} a_i = 0$ can be written as

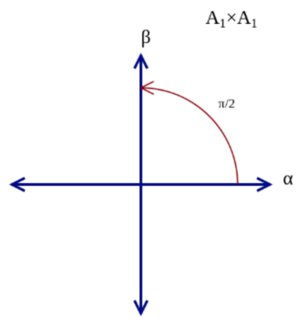
$$v = a_1(e_1 - e_2) + (a_1 + a_2)(e_2 - e_3) + \ldots + (a_1 + \ldots + a_n)(e_n - e_{n+1}) + (a_1 + \ldots + a_{n+1})e_{n+1}.$$

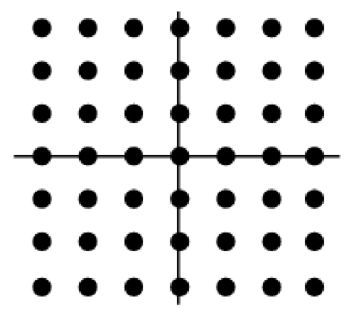
□





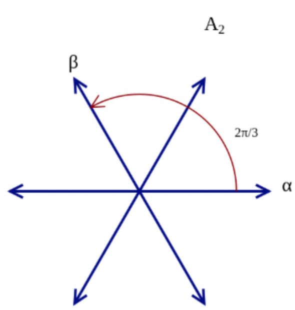
The root system A_1 and its associated root lattice.

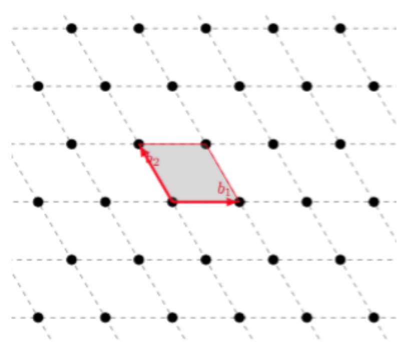




The root system $A_1 \times A_1$ and the orthogonal sum of two A_1 lattices.

The root lattice L_{A_2} coincides the hexagonal lattice in the plane $\{x_1 + x_2 + x_3 = 0\} \subset \mathbb{R}^3$.



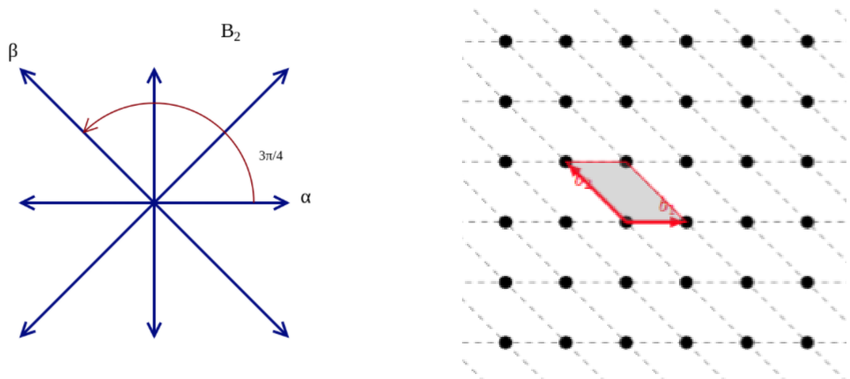


The root system A_2 and its associated root lattice.

Lemma 14. *The root lattice L_{B_n} ($n \geqslant 2$) coincides with the integral lattice*

$$L_{B_n} = \{\sum_{i=1}^{n} a_i e_i \mid a_i \in \mathbb{Z}\} = \mathbb{Z}^n \subset \mathbb{R}^n.$$

Proof. The proof is left as an excercise. □



The root system B_2 and its associated root lattice.

Lemma 15. *The root lattice L_{C_n} ($n \geqslant 3$)) is given by*

$$L_{C_n} = \{\sum_{i=1}^{n} a_i e_i \mid a_i \in \mathbb{Z},\ \sum_{i=1}^{n} a_i \in 2\mathbb{Z}\}.$$

Proof. By the description of C_n given in Section 2, an element $v \in L_{C_n}$ is of the form

$$v = a_1(e_1 - e_2) + \ldots + a_{n-1}(e_{n-1} - e_n) + a_n 2e_n$$

$$= a_1 e_1 + (a_2 - a_1)e_2 + \ldots + (a_{n-1} - a_{n-2})e_{n-1} + (2a_n - a_{n-1})e_n,$$

with $a_i \in \mathbb{Z}$. For such a vector the sum of the coordinates is even

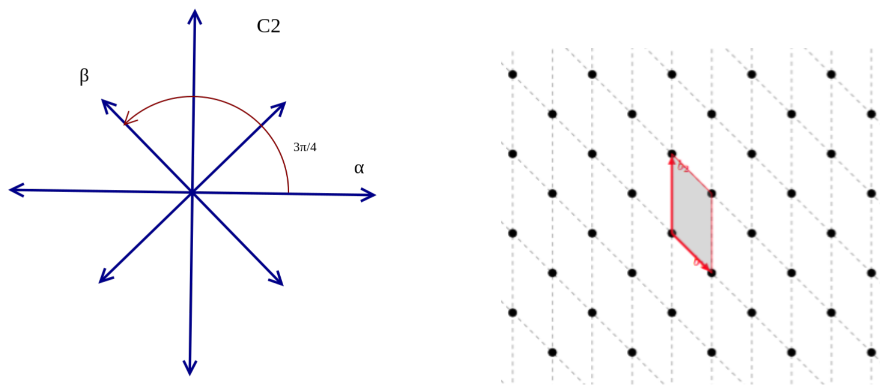
$$a_1 + (a_2 - a_1) + \ldots + (a_{n-1} - a_{n-2}) + (2a_n - a_{n-1}) = 2a_n \in 2\mathbb{Z}.$$

Conversely, a vector $v = \sum_{i=1}^{n+1} a_i e_i$, with $\sum_{i=1}^{n+1} a_i \in 2\mathbb{Z}$ can be written as

$$v = a_1(e_1 - e_2) + (a_1 + a_2)(e_2 - e_3) + \ldots + (a_1 + \ldots + a_{n-1})(e_{n-1} - e_n) + \frac{1}{2}(a_1 + \ldots + a_n)2e_n.$$

Since $(a_1 + \ldots + a_n)$ is even, $v \in L_{C_n}$. □

Remark 16. For $n = 2$ the root lattice L_{C_2} is isomorphic to $\sqrt{2}\mathbb{Z}^2$. However for $n \geqslant 3$, the lattices $\sqrt{2}\mathbb{Z}^n$ and C_n are distinct. This can be seen for example by counting shortest vectors.



The root system C_2 and its associated root lattice.

Lemma 17. *The root lattice L_{D_n} is given by*

$$L_{D_n} = \{\sum_{i=1}^{n} a_i e_i \mid a_i \in \mathbb{Z},\ \sum_{i=1}^{n} a_i \in 2\mathbb{Z}\}.$$

Proof. By the description of D_n given in Section 2, an element $v \in L_{D_n}$ is of the form

$$v = a_1(e_1 - e_2) + \ldots + a_{n-1}(e_{n-1} - e_n) + a_n(e_{n-1} + e_n)$$

$$= a_1 e_1 + (a_2 - a_1)e_2 + \ldots + (a_{n-1} - a_{n-2} + a_n)e_{n-1} + (a_n - a_{n-1})e_n,$$

with $a_i \in \mathbb{Z}$. For such a vector the sum of the coordinates is even

$$a_1 + (a_2 - a_1) + \ldots + (a_{n-1} - a_{n-2} + a_n) + (a_n - a_{n-1}) = 2a_n \in 2\mathbb{Z}.$$

Conversely, a vector $v = \sum_{i=1}^{n+1} a_i e_i$, with $\sum_{i=1}^{n+1} a_i \in 2\mathbb{Z}$ can be written as

$$v = a_1(e_1-e_2)+(a_1+a_2)(e_2-e_3)+\ldots+\frac{1}{2}(a_1+\ldots+a_{n-1}-a_n)(e_{n-1}-e_n)+\frac{1}{2}(a_1+\ldots+a_n)(e_{n-1}+e_n).$$

Note that $(a_1+\ldots+a_n)$ is even, hence $\frac{1}{2}(a_1+\ldots+a_n)$ is an integer. Moreover $\frac{1}{2}(a_1+\ldots+a_{n-1}-a_n) = (a_1 + \ldots + a_{n-1}) - \frac{1}{2}(a_1 + \ldots + a_n)$ is an integer as well. Hence $v \in L_{D_n}$. □

Proposition 18. *All irreducible distinct root lattices are:*
1. L_{A_n}, $n \geqslant 1$;
2. L_{D_n}, $n \geqslant 4$;
3. L_{E_6};
4. L_{E_7};
5. L_{E_8}.

Proof. The proof consists of showing that all lattices in the list are distinct and that the remaining root lattices are isomorphic to lattices in the list. For the first part, it is sufficient to count the number of shortest vectors in each case of the list:
we find

$$n(n+1),\ (n \geqslant 1) \quad 2n(n-1),\ (n \geqslant 4), \quad 72, \quad 126, \quad 240,$$

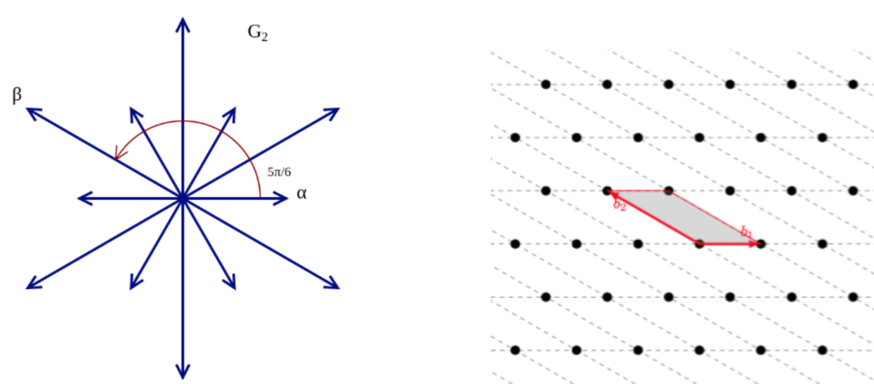
respectively.

For the second part it remains to show that
- L_{C_3} is isometric to L_{A_3},
- L_{G_2} coincides with L_{A_2},
- L_{F_4} can be mapped into to L_{D_4} by the composition of an homothety with an isometry (see the Excercises below). $\square$

Exercise 19. Prove that L_{C_3} is isomorphic L_{A_3}. In other words, for $n = 3$ the "sum of coordinates zero" lattice in $\mathbb{R}^4$ and the "sum of coordinates even" in $\mathbb{R}^3$ are isomorphic.
Suggestion: consider the map

$$\phi\colon \mathbb{R}^4 \to \mathbb{R}^3, \qquad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \mapsto \begin{pmatrix} x_1 + x_4 \\ x_2 + x_4 \\ x_1 + x_2 \end{pmatrix}.$$

Exercise 20. Prove that $L_{G_2} = L_{A_2}$. In other words L_{G_2}, like L_{A_2}, coincides with the hexagonal lattice in the plane $x_1 + x_2 + x_3 = 0$ in $\mathbb{R}^3$.



The root system G_2 and its associated root lattice.

Exercise 21. Prove that L_{F_4} can be mapped into to L_{D_4} by the composition of an homothety with an isometry.
Sugg.: consider the map

$$\phi\colon \mathbb{R}^4 \to \mathbb{R}^4, \quad \phi(e_1) = e_1 + e_2,\ \phi(e_2) = e_1 - e_2,\ \phi(e_3) = e_3 + e_4,\ \phi(e_4) = e_3 - e_4.$$

Remark 22. For every irreducible root lattice L_Δ listed in of Proposition 18, one has that:
(a) L_Δ is integral, namely $(v,w) \in \mathbb{Z}$, for all $v, w \in L_\Delta$;
(b) L_Δ is even, namely $(v,v) \in 2\mathbb{Z}$, for all $v \in L_\Delta$.

Part (a) follows from the fact that all elements of $\Delta = A_n, D_n, E_6, E_7, E_8$ have the same length squared equal to 2. In particular the Cartan matrix of any base of Δ (which has integral entries) is symmetric and coincides with the Gram matrix. Part (b) follows from the fact that all elements on the diagonal of the Gram matrix are equal to 2.

Even without using the classification of Proposition 18, one can prove that root lattices are rational, namely $(v,w) \in \mathbb{Z}$, for all $v, w \in L_\Delta$:

$$\frac{2(\beta,\alpha)}{(\alpha,\alpha)} \in \mathbb{Z}, \quad \forall \alpha, \beta \in \Delta \qquad \Rightarrow \qquad (\beta,\alpha) \in \mathbb{Q}, \forall \alpha, \beta \in \Delta.$$

The argument is the one used in [Hu], Sect.8.5, p.39.

Exercise 23. Let L be a lattice in a vector space E with inner product $(\ ,\ )$.
If L is even and $L \cap \{(v,v) = 2\}$ spans E, then $L \cap \{(v,v) = 2\}$ is a root system in E.

Remark 24. In an irreducible root lattice L_Δ (see Proposition 18) the shortest vectors are exactly the vectors of Δ.

More about the lattice L_{E_8}.
Since it is so special, let's compute some of the relevant quantities for this lattice.

• The *covolume* $covol(L_{E_8})$ of L_{E_8} is the volume of the "parallelepiped" spanned by an arbitrary basis of the lattice. We choose the base of L_{E_8} given in Section 2, we have

$$B_{E_8} = \begin{pmatrix} 1/2 & 1 & -1 & 0 & 0 & 0 & 0 & 0 \\ -1/2 & 1 & 1 & -1 & 0 & 0 & 0 & 0 \\ -1/2 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\ -1/2 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ -1/2 & 0 & 0 & 0 & 0 & 1 & -1 & 0 \\ -1/2 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ -1/2 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1/2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and $covol(L_{E_8}) := |\det(B_{E_8})| = |-1| = 1$. Hence L_{E_8} is *unimodular*. In particular, it coincides with its dual lattice $L_{E_8}^* = \{\lambda \in \mathbb{R}^8 \mid (\lambda, X) \in \mathbb{Z},\ \forall X \in L_{E_8}\}$

$$L_{E_8} = L_{E_8}^*.$$

• The *Gram matrix* $G(L_{E_8})$ of the above basis, i.e. the matrix whose entries G_{ij} are the inner products of the i^{th} and the j^{th} vectors, is given by

$$G(L_{E_8}) = {}^tB_{E_8} \cdot B_{E_8} = \begin{pmatrix} 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}.$$

As we already mentioned, $G(L_{E_8})$ coincides with the Cartan matrix of the root system E_8. One has

$$covol(L_{E_8}) = \sqrt{\det(G(B_{E_8}))} = 1.$$

• The *kissing number*, which coincides the number of shortest vectors in L_{E_8}, is equal to $|E_8| = 240$ (cf. Excercise 23). The norm squared of the shortest vectors is equal to 2.

• The *Hermite constant* is given by

$$\gamma_{L_{E_8}} = 2/(covol(L_{E_8}))^{2/8} = 2.$$

• The lattice L_{E_8} has a large group of *isometries* $Aut(L_{E_8})$, namely linear orthogonal transformations which take the lattice to itself: $Aut(L_{E_8})$ contains the Weyl group W of the root system E_8, which is generated by reflections in the simple roots, and has order $2^{14}3^55^27 = 696.729.600$.

4. Complex semisimple Lie algebras.

A complex *Lie algebra* $\mathfrak{g}$ is a complex algebra whose "product", called Lie bracket and usually denoted by $[\cdot,\cdot]$, is bilinear, skew-symmetric, and satisfies the Jacobi identity

$$[X,[Y,Z]]+[Z,[X,Y]]+[Y,[Z,X]]=0,\quad \forall X,Y,Z\in\mathfrak{g}.$$

A *subalgebra* of a Lie algebra $\mathfrak{g}$ is a vector subspace closed under the Lie bracket. An *ideal* $\mathfrak{l}$ of $\mathfrak{g}$ is a subalgebra such that $[\mathfrak{g},\mathfrak{l}]\subset\mathfrak{l}$. A Lie algebra is called *simple* if it is non-abelian and its only ideals are $\{0\}$ and itself; it is called *semisimple* if it is the direct sum of simple ideals. In particular, a semisimple Lie algebra has trivial center. The direct sum of Lie algebras $\mathfrak{g}_1\oplus\mathfrak{g}_2$, with Lie bracket given by $[X_1+X_2,Y_1+Y_2]:=[X_1,Y_1]+[X_2,Y_2]$, for $X_1,Y_1\in\mathfrak{g}_1$ and $X_2,Y_2\in\mathfrak{g}_2$, is a Lie algebra. Moreover, $\mathfrak{g}_1\oplus\{0\}$ and $\{0\}\oplus\mathfrak{g}_2$ are ideals of $\mathfrak{g}_1\oplus\mathfrak{g}_2$.

Example 25. An important example of a Lie algebra is given by $\mathfrak{gl}(V)$, the Lie algebra of endomorphims of a complex n-dimensional vector space V, with the Lie bracket $[f,g]=f\circ g-g\circ f$, where $\circ$ denotes the composition of maps. If a basis of V is fixed, then $\mathfrak{gl}(V)$ can be identified with the $n\times n$ complex matrices $\mathfrak{gl}(n,\mathbb{C})$ with Lie bracket $[X,Y]=XY-YX$, where XY is the usual matrix product in $\mathfrak{gl}(n,\mathbb{C})$. Let's check the Jacobi identity: for all $X,Y,Z\in\mathfrak{g}$ one has

$$[X,[Y,Z]]+[Z,[X,Y]]+[Y,[Z,X]]$$

$$=X(YX-ZY)-(YX-ZY)X+Z(XY-YX)-(XY-YX)Z+Y(ZX-XZ)-(ZX-XZ)Y=\ldots=0.$$

The Lie algebra $\mathfrak{gl}(n,\mathbb{C})$ is not simple. It is the direct sum of two non-trivial ideals: the center, given by the scalar matrices $Z(\mathfrak{g})=\{\lambda Id,\ \lambda\in\mathbb{C}\}$, and the simple ideal $\mathfrak{sl}(n,\mathbb{C})$ consisting of the $n\times n$ complex matrices with zero trace.

Let us verify that $\mathfrak{sl}(n,\mathbb{C})$ is an ideal of $\mathfrak{gl}(n,\mathbb{C})$:
let $X\in\mathfrak{gl}(n,\mathbb{C})$ and $Y\in\mathfrak{sl}(n,\mathbb{C})$. The trace of the bracket of X and Y is given by

$$\mathrm{tr}[X,Y]=\mathrm{tr}(XY-YX)=\mathrm{tr}(XY)-\mathrm{tr}(YX)=0.$$

Hence $[X,Y]\in\mathfrak{sl}(n,\mathbb{C})$, as claimed.

Exercise 26. Show that
(a) a 1-dimensional Lie algebra is necessarily abelian, that is $[X,Y]=0$, for all $X,Y\in\mathfrak{g}$;
(b) there are no 2-dimensional simple Lie algebras.

Exercise 27. Show that the space $\mathfrak{so}(n,\mathbb{C})$ of complex skew symmetric matrices is a Lie subalgebra of $\mathfrak{sl}(n,\mathbb{C})$.

Exercise 28. Show that the space $\mathfrak{sp}(n,\mathbb{C})$ of complex $2n\times 2n$ matrices satisfying ${}^tXJ+JX=O$, where $J=\begin{pmatrix}O&-I_n\\ I_n&O\end{pmatrix}$, is a Lie algebra subalgebra of $\mathfrak{sl}(2n,\mathbb{C})$ (here I_n denotes the identity matrix of order n).

A *Lie algebra homomorphism* $\phi\colon (\mathfrak{g}_1, [\ ,\ ]_1) \to (\mathfrak{g}_2, [\ ,\ ]_2)$ is a linear map satisfying the condition $\phi([X,Y]_1) = [\phi(X), \phi(Y)]_2$. A *representation* of a Lie algebra $\mathfrak{g}$ is a Lie algebra homomorphism

$$\rho\colon \mathfrak{g} \to \mathfrak{gl}(V)$$

from $\mathfrak{g}$ to the endomorphisms of some vector space V. An important representation of a Lie algebra is the *adjoint representation*,

$$ad\colon \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g}), \quad X \mapsto ad_X,$$

where ad_X denotes the linear endomorphism of $\mathfrak{g}$

$$ad_X(Y) := [X,Y], \quad \forall Y \in \mathfrak{g}.$$

Exercise 29. (a) Prove that the map $ad_Z\colon \mathfrak{g} \to \mathfrak{g}$ is a linear endomorphism of $\mathfrak{g}$; moreover the map ad_Z is a derivation of $\mathfrak{g}$, namely

$$ad_Z([X,Y]) = [ad_Z(X), Y] + [X, ad_Z(Y)], \qquad \forall X, Y, Z \in \mathfrak{g}.$$

(b) Prove that the map $\mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$, defined by $X \mapsto ad_X$, is a Lie algebra homomorphism.
(c) Prove that the adjoint representation of a semisimple Lie algebra is *faithful*, that is has zero kernel.

Via the adjoint representation, to every complex Lie algebra there is associated an intrinsic complex symmetric bilinear form, the *Killing form*, defined by

$$B\colon \mathfrak{g} \times \mathfrak{g} \to \mathbb{C}, \quad B(X,Y) := \mathrm{tr}(ad_X ad_Y).$$

The Killing form satisfies

$$B([Z,X],Y) = -B(X,[Z,Y]), \quad \forall X, Y, Z \in \mathfrak{g}. \tag{4·1}$$

(see Excercise 30). The non-degeneracy of the Killing form characterizes semisimple Lie algebras: *A Lie algebra $\mathfrak{g}$ is semisimple if and only if its Killing form is non-degenerate* (cf. [Hu], Thm. 5.1, p. 22).

Exercise 30. Verify that the Killing form satisfies equation (4·1).

Exercise 31. Let $\mathfrak{g} = \mathfrak{g}_1 \oplus \mathfrak{g}_2$ be a Lie algebra decomposition into a direct sum of ideals. Prove that:
(a) $[X_1, X_2] = 0$, for all $X_1 \in \mathfrak{g}_1 \oplus \{0\}$ and $X_2 \in \{0\} \oplus \mathfrak{g}_2$.
(b) the Killing form of $\mathfrak{g}$ satisfies $B(X_1, X_2) = 0$, for all $X_1 \in \mathfrak{g}_1 \oplus \{0\}$ and $X_2 \in \{0\} \oplus \mathfrak{g}_2$.
(c) if $\mathfrak{h} \subset \mathfrak{g}$ is an ideal, then the Killing form of $\mathfrak{h}$ coincides with the restriction of the Killing form of $\mathfrak{g}$ to $\mathfrak{h}$.

In the remaining part of this section we discuss the main tools for the construction of the root system of a complex semisimple Lie algebra: *Cartan subalgebras* of a semisimple Lie algebra and the *classification of all finite dimensional irreducible complex representations of* $\mathfrak{sl}(2,\mathbb{C})$.

A *Cartan subalgebra* $\mathfrak{h}$ of a complex semisimple Lie algebra $\mathfrak{g}$ is a maximal abelian subalgebra consisting of semisimple elements, namely elements for which the map $ad_X : \mathfrak{g} \to \mathfrak{g}$ is diagonalizable (in a complex semisimple Lie algebra the notion of a Cartan subalgebra coincides with that of a *maximal toral subalgebra* [Hu], Sect.8.1 and Sect.15.3). All Cartan subalgebras of $\mathfrak{g}$ are conjugate under inner automorphisms of $\mathfrak{g}$. Therefore they all have the same dimension, which is by definition the *rank* of $\mathfrak{g}$ (for a proof of these statements about Cartan subalgebras, we refer to [Hu], Sections 16.2–16.4).

As a consequence of the abstract Jordan decomposition in a Lie algebra (cf. [Hu], Sect. 5.4, p. 24) and its preservation under Lie algebra homomorphisms (cf. [Hu], Sect. 6.4, p. 29), the image of a Cartan subalgebra under any representation $\mathfrak{g} \to \mathfrak{gl}(V)$ is a commuting family of diagonalizable endomorphisms of V.

Example 32. • Let $\mathfrak{g} = \mathfrak{sl}(n, \mathbb{C})$ (cf. Example 25). A Cartan subalgebra of $\mathfrak{g}$ is given by the diagonal matrices.

• Let $\mathfrak{g} = \mathfrak{so}(2n+1, \mathbb{C})$ (resp. $\mathfrak{g} = \mathfrak{so}(2n, \mathbb{C})$). A Cartan subalgebra of $\mathfrak{g}$ is given by

$$\mathfrak{h} = \begin{pmatrix} B_1 & \dots & O \\ \vdots & \ddots & \vdots \\ O & \dots & -B_n \end{pmatrix}, \qquad (\text{resp. } \mathfrak{h} = \begin{pmatrix} B_1 & \dots & O & 0 \\ \vdots & \ddots & \vdots & \vdots \\ O & \dots & -B_n & \vdots \\ 0 & \dots & \dots & 0 \end{pmatrix}), \quad \text{where } B_i = \begin{pmatrix} 0 & \theta_i \\ -\theta_i & 0 \end{pmatrix},$$

for $i = 1, \dots, n$.

• Let $\mathfrak{g} = \mathfrak{sp}(n, \mathbb{C})$. A Cartan subalgebra of $\mathfrak{g}$ is given by $\mathfrak{h} = \begin{pmatrix} D & O \\ O & -D \end{pmatrix}$, where D is an $n \times n$ diagonal matrix.

The Lie algebra $\mathfrak{sl}(2, \mathbb{C})$.

The Lie algebra $\mathfrak{g} = \mathfrak{sl}(2, \mathbb{C}) = \{\begin{pmatrix} a & b \\ c & -a \end{pmatrix}, \ a, b, c \in \mathbb{C}\}$ is the lowest dimensional complex simple Lie algebra. Let us check that the set of diagonal matrices $\mathfrak{h} = \{\begin{pmatrix} h & 0 \\ 0 & -h \end{pmatrix}, \ h \in \mathbb{C}\}$ is a Cartan subalgebra of $\mathfrak{g}$.

- It is easy to verify that $\mathfrak{h}$ is an abelian subalgebra of $\mathfrak{g}$ and that $[H, X] = HX - XH = 0$, for all $H \in \mathfrak{h}$, implies $X \in \mathfrak{h}$. Hence it is a maximal abelian subalgebra of $\mathfrak{g}$.

- To see that $ad_H : \mathfrak{g} \to \mathfrak{g}$ is diagonalizable for all $H \in \mathfrak{h}$, we show that $\mathfrak{g}$ decomposes into the direct sum of ad_H-eigenspaces. For $H = \begin{pmatrix} h & 0 \\ 0 & -h \end{pmatrix}$, one has

$$ad_H(\begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}) = \begin{pmatrix} h & 0 \\ 0 & -h \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix} - \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix} \begin{pmatrix} h & 0 \\ 0 & -h \end{pmatrix} \equiv 0,$$

$$ad_H(\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}) = \begin{pmatrix} h & 0 \\ 0 & -h \end{pmatrix}\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} h & 0 \\ 0 & -h \end{pmatrix} = 2h\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix};$$
$$ad_H(\begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix}) = \begin{pmatrix} h & 0 \\ 0 & -h \end{pmatrix}\begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix}\begin{pmatrix} h & 0 \\ 0 & -h \end{pmatrix} = -2h\begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix}.$$

The above computation shows that

$$\mathfrak{g} = \underbrace{\begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}}_{\mathfrak{g}_0} \oplus \underbrace{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}}_{\mathfrak{g}_\alpha} \oplus \underbrace{\begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix}}_{\mathfrak{g}_{-\alpha}}$$

is an ad_H-eigenspace decomposition of $\mathfrak{g}$ for every $H \in \mathfrak{h}$: the subalgebra $\mathfrak{h}$ coincides with the 0-eigenspace, namely it coincides with its own centralizer; the subspace $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$, $b \in \mathbb{C}$, is the eigenspace of eigenvalue $\alpha(H) = 2h$ and the subspace $\begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix}$, $c \in \mathbb{C}$, is the eigenspace of eigenvalue $\alpha(H) = -2h$. In other words, the eigenspace decomposition of $\mathfrak{g}$ is the same for every $H \in \mathfrak{h}$, but the eigenvalues are functions of H, namely $\pm\alpha \colon \mathfrak{h} \to \mathbb{C}$, where

$$\alpha(\begin{pmatrix} h & 0 \\ 0 & -h \end{pmatrix}) = 2h.$$

Remark 33. The Lie algebra $\mathfrak{sl}(2, \mathbb{C})$ admits a basis A, X, Y satisfying

$$A = [X, Y], \quad [A, X] = 2X, \quad [A, Y] = -2Y; \tag{4·2}$$

for example

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

A 3-dimensional Lie algebra which admits a basis satisfying relations (4·2) is necessarily isomorphic to $\mathfrak{sl}(2, \mathbb{C})$.

Irreducible finite dimensional representations of $\mathfrak{sl}(2, \mathbb{C})$.

Recall that a representation of a Lie algebra $\mathfrak{g}$ is a Lie algebra homomorphism $\rho \colon \mathfrak{g} \to \mathfrak{gl}(V)$ to the endomorphisms of some vector space V. It is called *irreducible* if V does not decompose into the direct sum of non-trivial stable subspaces. Two representations $\rho_1 \colon \mathfrak{g} \to \mathfrak{gl}(V_1)$ and $\rho_2 \colon \mathfrak{g} \to \mathfrak{gl}(V_2)$ are said to be *equivalent* if there exists a linear isomorphism $\phi \colon V_1 \to V_2$ which commutes with the actions of $\mathfrak{g}$ on V_1 and V_2, namely $\phi(\rho_1(X)v) = \rho_2(X)\phi(v)$, for all $X \in \mathfrak{g}$ and $v \in V_1$. Finite dimensional *irreducible* representations of $\mathfrak{sl}(2, \mathbb{C})$ are classified (cf. [Se], Ch. IV).

Theorem 34. *For every $n \geqslant 0$ there is a unique (up to equivalence) irreducible representation V_n of $\mathfrak{sl}(2, \mathbb{C})$, of dimension $n + 1$.*

Construction of V_n:
consider a $n+1$-dimensional complex vector space $V_n = \mathrm{Span}_{\mathbb{C}}\{e_0, e_1, \dots, e_n\}$, with basis $e_0, e_1, \dots, e_n$. We define a representation $\rho_n \colon \mathfrak{sl}(2,\mathbb{C}) \to \mathfrak{gl}(V_n)$ by assigning it on the matrices A, X, Y:

$$(4{\cdot}3) \qquad \rho_(A) \cdot e_i := (n-2i)e_i, \quad \rho_n(X) \cdot e_i := (n-i+1)e_{i-1}, \quad \rho_n(X) \cdot v_i := (i+1)e_{i+1}$$

(by convention $e_{-1} = e_{n+1} = 0$). To see that it is a representation, we need to check that the above rules are compatible with the Lie brackets, namely

(i) $\rho_n([X,Y]) \cdot e_i = \rho_n(X) \cdot (\rho_n(Y) \cdot e_i) - \rho_n(Y) \cdot (\rho_n(X) \cdot e_i) = \rho_n(A) \cdot e_i$;
(ii) $\rho_n([A,X]) \cdot e_i = \rho_n(A) \cdot (\rho_n(X) \cdot e_i) - \rho_n(X) \cdot (\rho_n(A) \cdot e_i) = 2\rho_n(X) \cdot e_i$;
(iii) $\rho_n([A,Y]) \cdot e_i = \rho_n(A) \cdot (\rho_n(Y) \cdot e_i) - \rho_n(Y) \cdot (\rho_n(A) \cdot e_i) = -2\rho_n(Y) \cdot e_i$,
for all $i = 0, \dots, n$.

Let's prove that (i) is satisfied: we have

$$\rho_n(X) \cdot (\rho_n(Y) \cdot e_i) - \rho_n(Y) \cdot (\rho_n(X) \cdot e_i) = (i+1)\rho_n(X) \cdot e_{i+1} - (n-i+1)\rho_n(Y) \cdot e_{i-1}$$

$$= (i+1)(n-i)e_i - (n-i+1)ie_i = (n-2i)e_i = \rho_n(A) \cdot e_i,$$

as required. We leave (ii) and (iii) as an excercise.

Exercise 35. Show that for $n = 0$, the 1-dimensional representation of $\rho_0 \colon \mathfrak{sl}(2,\mathbb{C}) \to \mathfrak{gl}(\mathbb{C})$ is the trivial representation, that is $\rho_0(M) = 0$, for all $M \in \mathfrak{sl}(2,\mathbb{C})$.

Example 36. • For $n = 1$, fix the basis v_0, v_1 of V_1. By (4·3), the elements

$$X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

act on V_1 via the matrices

$$\rho_1(X) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \rho_1(A) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \rho_1(Y) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

So rules (4·3) determine the natural matrix multiplication on $\mathbb{C}^2$.

• For $n = 2$, fix the basis v_0, v_1, v_2 of V_2. By (4·3), the elements

$$X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

act on V_2 via the matrices

$$\rho_2(X) = \begin{pmatrix} 0 & 2 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad \rho_2(A) = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -2 \end{pmatrix}, \quad \rho_2(Y) = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix},$$

respectively. If write a generic element of $\mathfrak{sl}(2,\mathbb{C})$ as $M = bX + aA + cY$, for $a, b, c \in \mathbb{C}$, then it acts on $V_2 \cong \mathbb{C}^3$ by the matrix

$$\rho_2(M) = \begin{pmatrix} 2a & 2b & 0 \\ c & 0 & b \\ 0 & 2c & -2a \end{pmatrix}, \qquad a, b, c \in \mathbb{C}.$$

Remark 37. By Theorem 34, there is a unique (up to equivalence) 3-dimensional irreducible representation of $\mathfrak{sl}(2,\mathbb{C})$. So ρ_2 is equivalent to the adjoint representation of $\mathfrak{sl}(2,\mathbb{C})$ on itself. Fix the basis X, A, Y of $\mathfrak{sl}(2,\mathbb{C})$. Then the representative matrices of ad_X, ad_A, ad_Y in this basis are given by

$$\begin{pmatrix} 0 & -2 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -2 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 \\ -1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix},$$

respectively and the representative matrix of ad_M, for $M = bX + aA + cY$, is given by

$$\begin{pmatrix} 2a & -2b & 0 \\ -c & 0 & b \\ 0 & 2c & -2a \end{pmatrix}, \qquad a, b, c \in \mathbb{C}.$$

Example 38. In order to give a concrete realization of the irreducble $\mathfrak{sl}(2,\mathbb{C})$ representations V_n for all $n \geqslant 1$, we take a different realization of $\mathfrak{sl}(2,\mathbb{C})$. Consider the differential operators

$$\mathbf{x} = u\frac{\partial}{\partial v} \qquad \mathbf{a} = u\frac{\partial}{\partial u} - v\frac{\partial}{\partial v} \qquad \mathbf{y} = v\frac{\partial}{\partial u}, \qquad \text{for } u, v \in \mathbb{C}.$$

One can check that they satisfy

$$[\mathbf{x}, \mathbf{y}] = u(\frac{\partial}{\partial v}v)\frac{\partial}{\partial u} - v(\frac{\partial}{\partial u}u)\frac{\partial}{\partial v} = \mathbf{a}, \qquad [\mathbf{a}, \mathbf{x}] = 2\mathbf{x}, \qquad [\mathbf{a}, \mathbf{y}] = -2\mathbf{y}.$$

So they generate a 3-dimensional Lie algebra isomorphic to $\mathfrak{sl}(2,\mathbb{C})$.

For $n \geqslant 1$, denote by V_n the $(n+1)$-dimensional complex vector space generated by the complex homogeneous monomials of degree n in the two variables $\{u, v\}$

$$V_n = \mathrm{Span}\{u^n,\ u^{n-1}uv,\ \ldots, u^{n-i}v^i, \ldots, v^n\}, \qquad i = 0, \ldots, n.$$

Then we obtain the relations

$\mathbf{x} \cdot u^{n-i}v^i = iu^{n-i+1}v^{i-1}$
$\mathbf{a} \cdot u^{n-i}v^i = (n-2i)u^{n-i}v^i$
$\mathbf{y} \cdot u^{n-i}v^i = (n-i)u^{n-i-1}v^{i+1}.$

Now let's examine the eigenspace decomposition of V_n under the action of the Cartan subalgebra $\mathfrak{h} = \mathbb{C}\mathbf{a}$:

• the eigenspaces, which in this context are called *weight spaces*, are all 1-dimensional;
• they are generated by the monomials $u^{n-i}v^i$, for $i = 0, \dots, n$;
• the corresponding eigenvalues $\lambda \in \mathfrak{h}^*$, which in this context are called *weights*, are given by

$$\lambda(z\mathbf{a}) = (n-2i)z, \quad z \in \mathbb{C},$$

respectively. So the weights are parametrized by the complete strip of integers between $-n$ and n, with successive differences 2:

$$\begin{array}{ccccccccccl} -n & -n+2 & \dots & -2 & 0 & 2 & \dots & n-2 & n & & \text{for } n+1 = \dim V_n \text{ odd} \\ -n & -n+2 & \dots & -1 & & 1 & \dots & n-2 & n & & \text{for } n+1 = \dim V_n \text{ even.} \end{array}$$

Remark 39. Since all the weight spaces of any irreducible $\mathfrak{sl}(2,\mathbb{C})$-representation are1-dimensional and the weight 0 (resp. the weight 1) only appears in odd dimensional representations (resp. in even dimensional representations), the number of irreducible components of a finite dimensional $\mathfrak{sl}(2,\mathbb{C})$-representation is given by

$$\dim V_0 + \dim V_1.$$

5. Root system of a semisimple Lie algebra

Let $\mathfrak{g}$ be an arbitrary semisimple Lie algebra and let $\mathfrak{h}$ be a Cartan subalgebra of $\mathfrak{g}$. Consider the family of endomorphisms $ad_H \colon \mathfrak{g} \to \mathfrak{g}$, where H varies in $\mathfrak{h}$: since they are all diagonalizable and commute with each other, they are *simultaneously diagonalizable*. The eigenvalues α, which depend on H, define elements of $\mathfrak{h}^*$, i.e. *linear* maps $\alpha \colon \mathfrak{h} \to \mathbb{C}$. In other words $\mathfrak{g}$ admits a simultaneous eigenspace decomposition

$$\mathfrak{g} = \bigoplus_{\alpha \in \mathfrak{h}^*} \mathfrak{g}^\alpha$$

which is stable under ad_H, for all $H \in \mathfrak{h}$. Only finitely many of the α-eigenspaces

$$\mathfrak{g}^\alpha = \{X \in \mathfrak{g} \mid ad_H(X) = \alpha(H)X,\ H \in \mathfrak{h}\}$$

are non-zero. Let Δ denote the non-zero $\alpha \in \mathfrak{h}^*$ for which $\mathfrak{g}^\alpha \neq \{0\}$. The elements of Δ are called the *roots* of $\mathfrak{g}$ and the eigenspaces $\mathfrak{g}^\alpha$ the *root spaces*. We have

$$\mathfrak{g} = Z_{\mathfrak{g}}(\mathfrak{h}) \oplus \bigoplus_{\alpha \in \Delta} \mathfrak{g}^\alpha, \tag{5·1}$$

where

$$Z_{\mathfrak{g}}(\mathfrak{h}) = \{X \in \mathfrak{g} \mid Ad_X(H) = [X,H] = 0\}$$

denotes the centralizer of $\mathfrak{h}$ in $\mathfrak{g}$, which is just the 0-eigenspace, and contains the Cartan subagebra $\mathfrak{h}$.

• It is a *non-trivial fact* that a Cartan subalgebra $\mathfrak{h}$ coincides with its own centralizer

$$Z_{\mathfrak{g}}(\mathfrak{h}) = \mathfrak{h}$$

(cf. [Hu], Prop.8.2, p. 36). In particular, decomposition (5·1) becomes

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha\in\Delta} \mathfrak{g}^{\alpha}. \tag{5·2}$$

We are going to prove the following claim:

Claim *The $\mathbb{R}$-linear span of the roots in Δ is a real vector subspace of $\mathfrak{h}^*$, of real dimension equal to the complex dimension of $\mathfrak{h}^*$. On such a subspace there is a positive definite bilinear form $(\ ,\ )$ and the elements of Δ form a root system therein.*

Before we are able to show that the roots in Δ satisfy the axioms of an abstract root system, we need some preparation. The fact that the endomorphisms ad_H act on a semisimple Lie algebra, and not just on a vector space, puts restrictions on their common eigenvalues and eigenspaces.

Lemma 40.
- (a) $\mathrm{Span}_{\mathbb{C}}\{\alpha\}_{\alpha\in\Delta} = \mathfrak{h}^*$. *(cf.* **(R1)***)*
- (b) *For all $\alpha, \beta \in \Delta$, one has $[\mathfrak{g}^{\alpha}, \mathfrak{g}^{\beta}] \subset \mathfrak{g}^{\alpha+\beta}$, with $\mathfrak{g}^{\alpha+\beta}$ possibly zero.*
- (c) *The decomposition (5·2) is "almost" orthogonal with respect to the Killing form: for all $\alpha, \beta \in \Delta$, one has*

$$B(\mathfrak{g}^{\alpha}, \mathfrak{g}^{\beta}) \equiv 0, \quad \text{if } \alpha + \beta \neq 0.$$

- (d) *For every root α, also $-\alpha$ is a root.*

Proof. (a) This is a consequence of the fact that $Z(\mathfrak{g}) = \{0\}$. Suppose that $\mathrm{Span}_{\mathbb{C}}\{\alpha\}_{\alpha\in\Delta} \subsetneq \mathfrak{h}^*$. Then there exists $H \in \mathfrak{h}$ such that $\alpha(H) = 0$, for all $\alpha \in \Delta$. This implies that $[H, X_\alpha] = \alpha(H)X_\alpha = 0$, for all $\alpha \in \Delta$. In other words, H commutes with every element of $\mathfrak{g}$. Then $H \in Z(\mathfrak{g})$, contradicting the semisimplicity of $\mathfrak{g}$.

(b) This is a consequence of the Jacobi identity. Assume $X \in \mathfrak{g}^{\alpha}$ and $Y \in \mathfrak{g}^{\beta}$. Then

$$[H, [X, Y]] = [[H, X], Y] + [X, [H, Y]] = (\alpha(H) + \beta(H))[X, Y].$$

This means that $[X, Y]$ lies in $\mathfrak{g}^{\alpha+\beta}$. In particular, if $[X, Y] \neq 0$, then $\alpha + \beta \in \Delta$.

(c) This follows from the property (4·1) of the Killing form. Assume $X \in \mathfrak{g}^{\alpha}$ and $Y \in \mathfrak{g}^{\beta}$. Then for all $H \in \mathfrak{h}$ one has

$$\alpha(H)B(X, Y) = -B(X, [H, Y]) = B([H, X], Y) = -\beta(H)B(X, Y) \quad \Leftrightarrow \quad (\alpha(H)+\beta(H))B(X, Y) = 0.$$

It follows that $\alpha(H) + \beta(H) \neq 0$ implies $B(X, Y) = 0$.

(d) This is a consequence nondegeneracy of the Killing form. If $\alpha \in \Delta$ and $-\alpha \notin \Delta$, then by (b) there exists $X \neq 0$ in $\mathfrak{g}^{\alpha}$ such that $B(X, \mathfrak{g}) \equiv 0$. The nondegeneracy of the Killing form forces $X = 0$, yielding a contradiction. □

An immediate consequence of (c) is that the restriction of the Killing form to $\mathfrak{h}$ is *non-degenerate* and provides an identification of $\mathfrak{h}$ and its dual $\mathfrak{h}^*$: to every root $\alpha \in \Delta$ there is associated a unique vector $t_\alpha \in \mathfrak{h}$ such that

$$\alpha(H) = B(H, t_\alpha), \qquad \forall H \in \mathfrak{h}. \tag{5·3}$$

Moreover, a *complex valued* non-degenerate symmetric bilinear form can be defined on $\mathfrak{h}^*$ by posing

$$(\alpha, \beta) := B(t_\alpha, t_\beta) = \beta(t_\alpha) = \alpha(t_\beta). \tag{5·4}$$

The next result says that for every root α in Δ, a root vector $X \in \mathfrak{g}^\alpha$ can be embedded in a subalgebra of $\mathfrak{g}$ isomorphic to $\mathfrak{sl}(2, \mathbb{C})$. We denote it by $\mathfrak{sl}_2(\alpha)$. Such a subalgebra acts on $\mathfrak{g}$ by the restriction of the adjoint representation. In other words, $\mathfrak{g}$ contains several copies of $\mathfrak{sl}(2, \mathbb{C})$ and several $\mathfrak{sl}(2, \mathbb{C})$-modules.

Lemma 41. *Given $X \in \mathfrak{g}^\alpha$, there exists $Y \in \mathfrak{g}^{-\alpha}$ such that $\{X,\ Y,\ A := [X, Y]\}$ generate a Lie subalgebra of $\mathfrak{g}$ isomorphic to $\mathfrak{sl}(2, \mathbb{C})$.*

Proof. Fix $X \in \mathfrak{g}^\alpha$. To prove the Lemma we need to show that there exists $Y \in \mathfrak{g}^{-\alpha}$ such that $X,\ Y,\ A := [X, Y]$ satisfy the conditions of Remark 4·2. We do this in several steps.

(a) for all $X \in \mathfrak{g}^\alpha$ and $Y \in \mathfrak{g}^{-\alpha}$, one has $[X, Y] = B(X, Y)t_\alpha \subset \mathbb{C}t_\alpha$, where t_α is the dual root defined in (5·3):

by Lemma 40 (a), we already know that

$$[\mathfrak{g}^\alpha, \mathfrak{g}^{-\alpha}] \subset \mathfrak{g}^0 = \mathfrak{h}.$$

By (4·1) and (5·3), one has

$$B(H, [X, Y]) = B([H, X], Y) = \alpha(H)B(X, Y) = B(H, t_\alpha)B(X, Y) = B(H, t_\alpha B(X, Y)),$$

for every $H \in \mathfrak{h}$. Then (a) follows by the non-degeneracy of the Killing form on $\mathfrak{h}$.

(b) for every $X \in \mathfrak{g}^\alpha$, there exists $Z \in \mathfrak{g}^{-\alpha}$ such that $[X, Z] \neq 0$:

suppose by contradiction that $B(X, Z) = 0$, for all $Z \in \mathfrak{g}^{-\alpha}$. Then by Lemma 40(c) it follows that $B(X, \mathfrak{g}) \equiv 0$, contradicting the non-degeneracy of the Killing form. Hence (b) holds.

(c) One has $\alpha(t_\alpha) = B(t_\alpha, t_\alpha) \neq 0$; equivalently $(\alpha, \alpha) \neq 0$:

if $\alpha(t_\alpha) = 0$, then $[t_\alpha, X] = [t_\alpha, Y] = 0$ and X, Y, t_α generate a 3-dimensional solvable subalgebra $\mathfrak{s}$ of $\mathfrak{g}$. The operator ad_{t_α} is a nilpotent endomorphism of $\mathfrak{s}$ and a therefore a nilpotent endomorphism of $\mathfrak{g}$ (see [Hu], Sect. 3.2). But this, together with the semisimplicity of ad_{t_α} as an endomorphism of $\mathfrak{g}$, implies $t_\alpha = 0$, a contradiction.

As a consequence of (a), (b) and (c), one can normalize the triple $\{X, Y, A = [X, Y]\}$ so that it satisfies conditions (4·2) and generates a subalgebra isomorphic to $\mathfrak{sl}(2, \mathbb{C})$:
X is given;
$A = \frac{2t_\alpha}{B(t_\alpha, t_\alpha)}$;
for Y take $\frac{2t_\alpha}{B(X,Y)B(t_\alpha,t_\alpha)} Z$, where Z is the vector from (b). □

In the next proposition we prove a "complex version" of axioms $(R1) - (R4)$ for Δ, viewed as a subset of the complex vector space $\mathfrak{h}^*$, with the non-degenerate bilinear form $(\, , \,)$ defined in (5·4). We do it by identifying appropriate $\mathfrak{sl}_2(\alpha)$-modules inside $\mathfrak{g}$ and applying to them the results on the weight system of $\mathfrak{sl}(2, \mathbb{C})$-representations.

Proposition 42. *The roots in Δ, viewed in the complex vector space $\mathfrak{h}^*$ with the non-degenerate bilinear form $(\, , \,)$ defined in (5·4), satisfy axioms $(R1) - (R4)$*

Proof. • $(\mathbf{R1})$: by definition, Δ does not contain 0. The spanning property was proved in Lemma 40(a).

• $(\mathbf{R2})$: fix $\alpha \in \Delta$ and $X \in \mathfrak{g}^\alpha$. Denote by $\mathfrak{sl}_2(\alpha)$ the associated subalgebra of $\mathfrak{g}$ determined in Lemma 41. By Lemma 40 (b), the subspace

$$\mathfrak{h} \oplus \bigoplus_{c \in \mathbb{C}^*} \mathfrak{g}^{c\alpha} = \ker \alpha \oplus \underbrace{\mathbb{C}A \oplus \mathfrak{g}^{\alpha} \oplus \mathfrak{g}^{-\alpha}}_{\mathfrak{sl}_2(\alpha)} \oplus \bigoplus_{\substack{c \in \mathbb{C}^* \\ c \neq \pm 1}} \mathfrak{g}^{\pm c\alpha}. \tag{5·5}$$

is an $\mathfrak{sl}_2(\alpha)$-submodule inside $\mathfrak{g}$. It contains the trivial $\mathfrak{sl}_2(\alpha)$-module given by the hyperplane $\ker \alpha \subset \mathfrak{h}$ and $\mathfrak{sl}_2(\alpha)$ itself, which is irreducible of dimension three. Since the dimension of the 0-weight space in

$$\mathbb{C}A \oplus \mathfrak{g}^{\alpha} \oplus \mathfrak{g}^{-\alpha} \oplus \bigoplus_{\substack{c \in \mathbb{C}^* \\ c \neq \pm 1}} \mathfrak{g}^{\pm c\alpha} \tag{5·6}$$

is equal to 1, by Remark 39 the subspace (5·6) contains a unique odd dimensional irreducible submodule, namely $\mathfrak{sl}_2(\alpha)$ itself.
It follows that:

$$\dim \mathfrak{g}^{\pm\alpha} = 1, \quad \text{for all } \alpha \in \Delta;$$

$$\forall\, \alpha \in \Delta \quad \Rightarrow \quad 2\alpha \notin \Delta.$$

The latter statement in turn implies that $\alpha/2$ cannot be a root either, because α is already a root. By applying Remark 39 once more, one sees that the subspace (5·6) contains no even dimensional $\mathfrak{sl}_2(\alpha)$-submodule and the space (5·5) is the direct sum of an $(n-1)$-dimensional trivial $\mathfrak{sl}_2(\alpha)$-module and one copy of $\mathfrak{sl}_2(\alpha)$. Summarizing,

$$\mathfrak{g}^{c\alpha} \subset \mathfrak{g} \quad \Rightarrow \quad c = \pm 1. \qquad ((\mathbf{R2})) \tag{5·7}$$

• (**R4**): Fix $\beta, \alpha \in \Delta$ be two non-proportional roots and consider the subspace of $\mathfrak{g}$ given by

$$\bigoplus_{j \in \mathbb{Z}} \mathfrak{g}^{\beta + j\alpha}, \tag{5·8}$$

where we understand that $\mathfrak{g}^{\beta+j\alpha} = 0$, if $\mathfrak{g}^{\beta+j\alpha} \not\subset \mathfrak{g}$. By Lemma 40 (b), the subalgebra $\mathfrak{sl}_2(\alpha)$ acts on the space (5·8), which we know to be a direct sum of 1-dimensional root spaces. By Theorem 34, the space (5·8) consists of *all* the root spaces

$$\bigoplus_{-r \leqslant j \leqslant q} \mathfrak{g}^{\beta + j\alpha},$$

for some $r, q \in \mathbb{Z}_{\geqslant 0}$, and the eigenvalues of ad_A on the above space

$$(\beta + j\alpha)(A) = \beta(A) + j\alpha(A) = \beta(A) + 2j$$

consist of *all the integers* of an interval $[-M, M]$, for $M \in \mathbb{Z}$, with successive differences 2. This forces

$$\beta(A) = \frac{2(\beta, \alpha)}{(\alpha, \alpha)} \in \mathbb{Z}, \qquad \forall \alpha, \beta \in \Delta. \qquad ((\mathbf{R4})) \tag{5·9}$$

• (**R3**): More precisely,

$$\beta(A) - 2r = -(\beta(A) + 2q) \quad \Rightarrow \quad \beta(A) = r - q.$$

Since $q - r$ is an integer between $-r$ and q, it follows that

$$s_\alpha(\beta) = \beta - \frac{2(\beta, \alpha)}{(\alpha, \alpha)}\alpha = \beta - \beta(A)\alpha = \beta + (q - r)\alpha \in \Delta. \qquad ((\mathbf{R3}))$$

□

The next lemma concludes the proof of Claim (*).

Lemma 43. *From $2\frac{(\beta,\alpha)}{(\alpha,\alpha)} \in \mathbb{Z}$, for all $\alpha, \beta \in \Delta$, it follows that the roots of Δ are contained in a real vector subspace of $\mathfrak{h}^*$. Moreover*

$$(\alpha, \beta) \in \mathbb{Q}, \quad \textit{and} \quad (\alpha, \alpha) > 0, \quad \textit{for all } \alpha, \beta \in \Delta.$$

Proof. Since Δ generates $\mathfrak{h}^*$ over $\mathbb{C}$, there exist roots $\alpha_1, \ldots, \alpha_n$ such that every $\alpha \in \Delta$ can be written as

$$\alpha = \sum_j c_j \alpha_j, \qquad c_j \in \mathbb{C}.$$

We first prove that

• $c_j \in \mathbb{Q}$, for all $j = 1, \ldots, n$.

Taking the inner product of α with $\alpha_j^\vee = 2\frac{\alpha_j}{(\alpha_j,\alpha_j)}$, for $j = 1, \ldots, n$, we obtain

$$\begin{aligned}(\alpha, \alpha_1^\vee) &= c_1(\alpha_1, \alpha_1^\vee) + \ldots + c_n(\alpha_n, \alpha_1^\vee)\\ \vdots \quad &\quad \vdots \qquad\qquad\qquad \vdots\\ (\alpha, \alpha_n^\vee) &= c_1(\alpha_1, \alpha_n^\vee) + \ldots + c_n(\alpha_n, \alpha_n^\vee)\end{aligned}$$

So the coefficients $c_1, \ldots, c_n$ are solutions of a linear system whose coefficient matrix is an invertible matrix with integer entries. As a consequence they are rational numbers.

Next we prove that

• $(\alpha, \beta) \in \mathbb{Q}$, for all $\alpha, \beta \in \Delta$.

Recall that for every element of $H \in \mathfrak{h}$ the adjoint action ad_H respects the root decomposition (5·2). Hence the trace of ad_H is the sum of all roots evaluated at H. From the definition of $(\cdot, \cdot)$ we have then

$$(\alpha, \beta) = B(t_\alpha, t_\beta) = trace(ad_{t_\alpha} ad_{t_\beta})$$

$$= trace\left(\begin{pmatrix} \ddots & 0 & 0 \\ 0 & \lambda(t_\alpha) & 0 \\ 0 & 0 & \ddots \end{pmatrix}\begin{pmatrix} \ddots & 0 & 0 \\ 0 & \lambda(t_\beta) & 0 \\ 0 & 0 & \ddots \end{pmatrix}\right) = \sum_{\lambda \in \Delta} (\lambda, \alpha)(, \lambda, \beta).$$

Taking $\alpha = \beta$ and dividing the resulting expression by $(\alpha, \alpha)^2$ (we know from step (c) in the proof of Lemma 41 that $(\alpha, \alpha) \neq 0$) we obtain

$$\frac{1}{(\alpha, \alpha)} = \sum_{\lambda \in \Delta} \frac{(\lambda, \alpha)^2}{(\alpha, \alpha)^2} = \frac{1}{4} \sum_{\lambda \in \Delta} (\lambda, \frac{2\alpha}{(\alpha, \alpha)})^2.$$

Since each $(\lambda, \frac{2\alpha}{(\alpha,\alpha)})^2$ is the square of an integer, it follows that (α, α) is a positive rational number. It also follows that

$$(\beta, \alpha) \in \mathbb{Z}\frac{(\alpha, \alpha)}{2}$$

is a rational number, all roots $\alpha, \beta \in \Delta$. □

Example 44. As an example we work out the root system of the 10-dimensional complex Lie algebra $\mathfrak{sp}(2, \mathbb{C})$

$$\mathfrak{g} = sp(2, \mathbb{C}) = \{\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in M(2, 2, \mathbb{C}) \,|\, {}^tA = -D,\ {}^tC = C,\ {}^tB = B\} = \{\begin{pmatrix} A & B \\ C & -{}^tA \end{pmatrix} \,|\, {}^tB = B,\ {}^tC = C\}.$$

A Cartan subalgebra of $\mathfrak{g}$ is given by

$$\mathfrak{h} = \left\{ \begin{pmatrix} a_1 & 0 & 0 & 0 \\ 0 & a_2 & 0 & 0 \\ 0 & 0 & -a_1 & 0 \\ 0 & 0 & 0 & -a_2 \end{pmatrix}, \quad a_1, a_2 \in \mathbb{C} \right\}.$$

Hence $\mathfrak{g}$ is of rank 2. The family of operators $\{ad_H\}_{H\in\mathfrak{h}}$ decomposes $\mathfrak{g}$ as

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha\in\Delta^+} \mathfrak{g}^{\pm\alpha},$$

where the root spaces are generated by the matrices

$$Z_{\alpha_1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \quad Z_{-\alpha_1} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad Z_{\alpha_2} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad Z_{-\alpha_2} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix},$$

$$Z_{\alpha_1+\alpha_2} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad Z_{-(\alpha_1+\alpha_2)} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix},$$

$$Z_{2\alpha_1+\alpha_2} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad Z_{-(2\alpha_1+\alpha_2)} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

The corresponding roots are given by

$$\Delta = \pm\{\alpha_1,\ \alpha_2,\ \alpha_1+\alpha_2,\ 2\alpha_1+\alpha_2\},$$

where

$$\alpha_1(H) = a_1 - a_2, \quad \text{and} \quad \alpha_2(H) = 2a_2,$$

are simple roots and

$$(\alpha_1+\alpha_2)(H) = a_1 + a_2, \qquad (2\alpha_1+\alpha_2)(H) = 2a_1, \qquad H \in \mathfrak{h}.$$

The Killing form of $\mathfrak{g}$ is given by

$$B(X,Y) = 6tr(XY), \qquad \text{for } X, Y \in \mathfrak{g}.$$

Using B, identify $\mathfrak{h}^*$ and $\mathfrak{h}$ as in (5·3): the vectors $t_\alpha \in \mathfrak{h}$, corresponding to the roots $\alpha \in \Delta$, are given by

$$t_{\alpha_1} = \frac{1}{12}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad t_{\alpha_2} = \frac{1}{6}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix},$$

$$t_{\alpha_1+\alpha_2} = t_{\alpha_1} + t_{\alpha_1} = \frac{1}{12}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \qquad t_{2\alpha_1+\alpha_2} = 2t_{\alpha_1} + t_{\alpha_1} = \frac{1}{6}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

From the expression for the restriction of the Killing form to $\mathfrak{h} = \mathrm{Span}_{\mathbb{R}}\{t_{\alpha_1}, t_{\alpha_2}\}$

$$\begin{aligned} & B(at_{\alpha_1} + bt_{\alpha_2}, at_{\alpha_1} + bt_{\alpha_2}) \\ = & a^2 B(t_{\alpha_1}, t_{\alpha_1}) + b^2 B(t_{\alpha_2}, t_{\alpha_2}) + 2ab B(t_{\alpha_1}, t_{\alpha_2}) \\ = & \frac{1}{6}a^2 + \frac{1}{3}b^2 - \frac{1}{6}2ab, \end{aligned}$$

we can see that the vectors $\{t_\alpha\}_{\alpha\in\Delta}$ generate a real vector subspace in $\mathfrak{h}$ on which the Killing form is positive definite. Moreover, on such space they form a root system of type C_2: compare the first two entries on the diagonal of the matrices t_α with the description of the root system C_2 give in Section 2.

References

[Bou] Bourbaki, *Groupes et Algèbres de Lie, Ch. 4,5,6*, Masson, Paris, 1981.

[Hu] J. E. Humphreys, *Introduction to Lie algebras and Representation theory*, Graduate Texts in Mathematics, Springer Verlag, New York, 1972.

[Se] J.-P. Serre, *Complex semisimple Lie algebras*, Springer Verlag, New York, 1966.