Essays on the structure of reductive groups

Bill Casselman
University of British Columbia
cass@math.ubc.ca

Finite root systems

This essay discusses some elementary points concerning finite integral root systems. These are a crucial tool in representation theory, because they describe the structure of reductive groups, and in all characteristics.

My approach will slightly different from the standard one in [Bourbaki:1968], which does not distinguish carefully between roots and coroots, and does not deal with root systems that are invariant under translations, such as those arising from parabolic subgroups.

Contents

1. Introduction

In this section I'll motivate what's to come by a well known example.

Let F be an arbitrary field, and

$$\begin{aligned} G &= \mathrm{GL}_n \\ T &= \text{ subgroup of diagonal matrices in } G \\ \mathfrak{g}, \mathfrak{t} &= \text{ the Lie algebras of } G(F), T(F)\,. \end{aligned}$$

Here G is considered as an algebraic group defined over F. The Lie algebra $\mathfrak{g}$ may be identified with $M_n(F)$, with Lie bracket $[X, Y] = XY - YX$. The group T is isomorphic to the algebraic torus $\mathbb{G}_m^n$, $T(F)$ is isomorphic to $(F^\times)^n$, and the Lie algebra $\mathfrak{t}$ is isomorphic to F^n. The character group $X^*(T)$ is the lattice of algebraic homomorphisms $T \to \mathbb{G}_m$, the cocharacter group that of algebraic homomorphisms $\mathbb{G}_m \to T$. These are free $\mathbb{Z}$-modules of rank n, and are canonically dual. I express them additively. If x has diagonal entries x_i, we have the characters ε_i

$$x \longmapsto x^{\varepsilon_i} = x_i\,,$$

that make up a basis of $X^*(T)$. The group $T(F)$ acts by conjugation on $\mathfrak{g}$, which decomposes into the direct sum of $\mathfrak{t}$ and $n(n-1)$ eigenspaces of dimension one, on which T acts by the multiplicative characters

$$x^{\varepsilon_i - \varepsilon_j} \quad (x_i/x_j \text{ in multiplicative notation}) \quad (1 \le i, j \le n,\ i \ne j)\,.$$

These make up the set Σ of **roots** $\alpha_{i,j} = \varepsilon_i - \varepsilon_j$ of (G, T), which lie in $X^*(T)$. Corresponding to each of these pairs $i \ne j$ is an embedding $\varphi_{i,j}$ of $\mathrm{SL}_2(F)$ into G. For example, if $n = 3$, $i = 1$, $j = 3$:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \longmapsto \begin{bmatrix} a & 0 & b \\ 0 & 1 & 0 \\ c & 0 & d \end{bmatrix}\,.$$

If

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

then its image $\sigma_{i,j}$ with respect to $\varphi_{i,j}$ lies in the normalizer $N_G(T)$ of T, which consists of the monomial matrices. The quotient $N_G(T)/T$ is isomorphic to $\mathfrak{S}_n$. This embedding of SL_2 also gives rise to embeddings of $\mathbb{G}_m$ through composition

$$x \longmapsto \begin{bmatrix} x & 0 \\ 0 & 1/x \end{bmatrix} \longrightarrow T \subset G\,.$$

These make up the set $\Sigma^\vee$ of **coroots** $x^{\alpha^\vee_{i,j}} = x^{\varepsilon^\vee_i - \varepsilon^\vee_j}$, lying in $X_*(T)$. For every root α,

$$\langle \alpha, \alpha^\vee \rangle = 2\,,$$

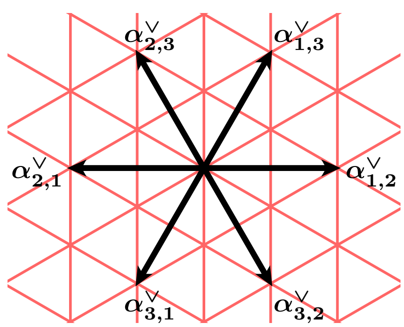
in effect since

$$\begin{bmatrix} x & 0 \\ 0 & 1/x \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x & 0 \\ 0 & 1/x \end{bmatrix}^{-1} = \begin{bmatrix} 1 & x^2 \\ 0 & 1 \end{bmatrix}.$$

The matrices $\sigma_{i,j}$ act as reflections on $X^*(T)$, swapping x_i and x_j. This can be formulated in more general terms:

$$\sigma_{i,j}\colon\ \lambda \longrightarrow \lambda - \langle \lambda, \alpha^\vee_{i,j} \rangle \alpha_{i,j}\,.$$

The group SL_n embeds into GL_n. Its subgroup S of diagonal matrices satisfy $\prod x_i = 1$, or $\sum \varepsilon_i = 0$. The $\alpha^\vee_{i,j}$ make up a basis of $X_*(S)$. The restrictions of the ε_i to S span $X^*(S)$, although the restrictions of the roots have index n in it. In the figure below are drawn the coroots for SL_3 as vectors in the plane $\varepsilon_1 + \varepsilon_2 + \varepsilon_3 = 0$ and the level lines $\alpha_{i,j} = k$ for integers k.



If $V = \mathbb{R} \otimes X^*(T)$, then V, Σ and the map from Σ to the dual space $V^\vee$ taking $\alpha_{i,j}$ to $\alpha^\vee_{i,j}$ define what is called a **root system**.

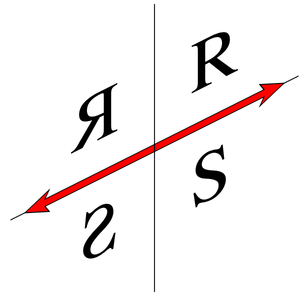
I'll now look at this notion systematically.

2. Reflections

A **reflection** in a finite-dimensional vector space is a linear transformation that fixes vectors in a hyperplane, and acts on a complementary line as multiplication by -1. Every reflection can be written as

$$s_{f,f^\vee}\colon\ v \longmapsto v - \langle f, v \rangle f^\vee$$

for some linear function $f \neq 0$ and vector $f^\vee$ with $\langle f, f^\vee \rangle = 2$. The function f is unique up to non-zero scalar, and if f is replaced by cf then $f^\vee$ is replaced by $f^\vee/c$.



If V is given a Euclidean norm, a reflection is **orthogonal** if it is of the form

$$v \longmapsto v - 2\left(\frac{v \bullet r}{r \bullet r}\right) r$$

for some non-zero r. Why? The vector

$$v_{\|} = \left(\frac{v \bullet r}{r \bullet r}\right) r$$

is the orthogonal projection onto the line through r. Then $v_{\perp} = v - v_{\|}$ lies in the reflection hyperplane, $v = v_{\perp} + v_{\|}$ is an orthogonal decomposition, and $v_{\perp} - v_{\|}$ is the mirror image of v.

If $(f^{\vee}, f)$ is a pair defining a reflection, then so is $(f, f^{\vee})$.

2.1. Lemma. *If λ, $\lambda^{\vee}$ are any vectors in V, $V^{\vee}$ with $\langle \lambda, \lambda^{\vee} \rangle = 2$, the contragredient of $s_{\lambda^{\vee},\lambda}$ is $s_{\lambda,\lambda^{\vee}}$.*

Proof. It has to be shown that

$$\langle s_{\lambda} u, v \rangle = \langle u, s_{\lambda^{\vee}} v \rangle \ .$$

The first is

$$\langle u - \langle u, \lambda^{\vee} \rangle \lambda, v \rangle = \langle u, v \rangle - \langle u, \lambda^{\vee} \rangle \langle \lambda, v \rangle$$

and the second is

$$\langle u, v - \langle \lambda, v \rangle \lambda^{\vee} \rangle = \langle u, v \rangle - \langle \lambda, v \rangle \langle u, \lambda^{\vee} \rangle \ .$$

2.2. Lemma. *If g is any element in $\mathrm{GL}(V)$ then*

$$g \cdot s_{\lambda^{\vee},\lambda} \cdot g^{-1} = s_{g\lambda^{\vee}, g\lambda} \ .$$

This is immediate.

3. Root systems

Definition. *A* **finite root system** *is*

- *a quadruple $(V, \Sigma, V^{\vee}, \Sigma^{\vee})$ where V is a finite-dimensional vector space over $\mathbb{R}$, $V^{\vee}$ its linear dual, Σ a finite subset of $V - \{0\}$, $\Sigma^{\vee}$ a finite subset of $V^{\vee} - \{0\}$;*
- *a bijection $\lambda \mapsto \lambda^{\vee}$ of Σ with $\Sigma^{\vee}$*

subject to these conditions:

- *for each λ in Σ, $\langle \lambda, \lambda^{\vee} \rangle = 2$;*
- *for each λ and μ in Σ, $\langle \lambda, \mu^{\vee} \rangle$ lies in $\mathbb{Z}$;*
- *for each λ in Σ the reflection*
$$s_{\lambda^{\vee},\lambda} \colon \ v \longmapsto v - \langle v, \lambda^{\vee} \rangle \lambda$$
takes Σ to itself;
- *for each λ in Σ the reflection*
$$s_{\lambda,\lambda^{\vee}} \colon \ v \longmapsto v - \langle \lambda, v \rangle \lambda^{\vee}$$

in $V^\vee$ preserves $\Sigma^\vee$.

The last condition is not redundant. For example, consider a vector space of dimension 2 with basis ε, δ and in $\widehat{V}$ the dual basis $\widehat{\varepsilon}$, $\widehat{\delta}$. Set

$$\begin{aligned} \alpha &= 2\varepsilon \\ \beta &= -2\varepsilon \\ \alpha^\vee &= \widehat{\varepsilon} \\ \beta^\vee &= -\widehat{\varepsilon} + \widehat{\delta}\,. \end{aligned}$$

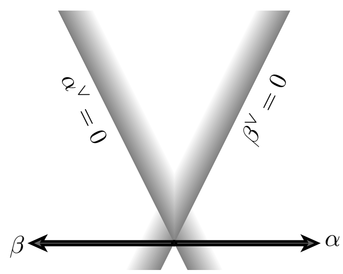
This satisfies the first three conditions, but expressing reflections as matrices in the basis ε, δ:

$$\begin{aligned} s_{\alpha,\alpha^\vee} &= \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \\ s_{\beta,\beta^\vee} &= \begin{bmatrix} -1 & 0 \\ 2 & 1 \end{bmatrix}. \end{aligned}$$

The product is

$$\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix},$$

which is a shear that cannot preserve any finite set not contained in the line spanned by $\widehat{\delta}$.



However, as we shall see later, in case V is spanned by Σ the condition that $\Sigma^\vee$ be reflection-invariant is redundant.

The elements of Σ are called the **roots** of the system, those of $\Sigma^\vee$ its **coroots**. The **rank** of the system is the dimension of V, and the **semi-simple rank** is that of the subspace $V(\Sigma)$ of V spanned by Σ. The system is called **semi-simple** if $V = V(\Sigma)$. The **Weyl group** W of the system is the group W generated by the reflections $s_{\lambda^\vee,\lambda}$. Because of Lemma 2.1, it is isomorphic to the dual group generated by the $s_{\lambda,\lambda^\vee}$

The root system is said to be **reducible** if Σ is the union of two subsets Σ_1 and Σ_2 with $\langle \lambda, \mu^\vee \rangle = 0$ whenever λ and μ belong to different components. Otherwise it is **irreducible**.

Remark. There are many slightly differing definitions of root systems in the literature. Sometimes the extra condition that Σ span V is imposed, for example in Chapitre VI of the standard reference [Bourbaki:1968]. But often in this subject one is interested in subsets of Σ which again give rise to root systems that do not possess this property even if the original one does.

Sometimes the vector space V is assumed to be Euclidean and the reflections orthogonal, but there may be several possible choices of metric, so I prefer not to make it part of the basic data. The definition I have given is one that arises most directly in the theory of reductive Lie and algebraic groups, but there is some justification in that theory for something like a Euclidean structure as well, since a semi-simple Lie algebra possesses a canonical invariant quadratic form (its Killing form). Another virtue of not starting off with a Euclidean structure is that it allows one to keep in view generalizations, relevant to Kac-Moody algebras, where the root system is not finite and no canonical inner product, let alone a Euclidean one, exists.

4. Simple properties

If λ is in Σ, so is $-\lambda = s_\lambda \lambda$.

The definition is self-dual. If $(V, \Sigma, V^\vee, \Sigma^\vee)$ is a root system, so is its **dual** $(V^\vee, \Sigma^\vee, V, \Sigma)$.

4.1. Lemma. *If $\lambda = c\mu$ for roots λ, μ, then c is either ± 2, ± 1, or $\pm 1/2$.*

Proof. From integrality of $\langle \lambda, \mu^\vee \rangle$ and $\langle \mu, \lambda^\vee \rangle$. ∎

SEMI-SIMPLE SYSTEMS.

4.2. Theorem. *If V is spanned by Σ, then the fourth condition is redundant.*

That is to say, if $(V, \sigma, V^\vee, \Sigma^\vee)$ satisfies the first three conditions and V is spanned by Σ, it also satisfies the fourth.

Proof. In a series of steps.

Step 1. *Suppose Ω to be a finite subset of a vector space V that spans V, and ω arbitrary in V. There exists at most one reflection taking ω to $-\omega$, and Ω to itself.*

Suppose that r, s were two such reflections, say fixing points on hyperplanes H_r, H_s. They both fix all vectors on the intersection $H_r \cap H_s$, which is of codimension two. The product rs fixes in addition the vector ω. The vector ω does not lie in either H_r nor H_s, so ω and $H_r \cap H_s$ span a hyper-plane H. Since $\det(rs) = 1$, rs acts as the identity on V/H, and rs must therefore be a shear. But since $rs(\Omega) = \Omega$ and Ω is not contained in H, this shear must be trivial, and $r = s$.

Step 2. Assume now that $V = V(\Sigma)$. Apply the previous step to Σ and any λ in Σ. The result of the previous step implies that $\lambda^\vee$ *is the unique vector v in $V^\vee$ such that (a) $\langle \lambda, v \rangle = 2$ and (b) $s_{\lambda,v}$ takes Σ to itself.*

From now on, I can refer to s_λ without ambiguity. Because of Lemma 2.1, I can also refer to $s_{\lambda^\vee}$ without ambiguity.

Step 3. Finally:

$$s_\lambda(\mu^\vee) = (s_\lambda \mu)^\vee \, .$$

Let $v = s_\lambda(\mu^\vee)$. We must verify that (a) $\langle s_\lambda(\mu), v \rangle = 2$ and (b) $s_{v, s_\lambda \mu}$ takes Σ to itself.

For (a):

$$\langle s_\lambda(\mu), v \rangle = \langle s_\lambda(\mu), s_\lambda(\mu^\vee) \rangle = \langle \mu, \mu^\vee \rangle = 2 \, .$$

For (b): Let ν be in Σ. Then

$$\begin{aligned} s_{v, s_\lambda \mu}(\nu) &= \nu - \langle \nu, s_\lambda(\mu^\vee) \rangle s_\lambda \mu \\ &= \nu - \langle s_\lambda \nu, \mu^\vee \rangle s_\lambda \mu \\ &= s_\lambda\big(s_\lambda(\nu) - \langle s_\lambda \nu, \mu^\vee \rangle \mu\big) \\ &= s_\lambda s_\mu s_\lambda(\nu) \, . \end{aligned}$$

But since s_λ and s_μ take Σ to itself, the whole right hand side lies in Σ.

This concludes the proof of the Proposition. ∎

THE CANONICAL METRIC. Next I introduce a semi-Euclidean structure on V, with respect to which the root reflections will be orthogonal. The existence of such a structure is important, especially for the classification of root systems (and reductive groups). The construction of some reflection-invariant Euclidean norm is straightforward, but the one introduced here is canonical.

Define the linear map

$$\rho \colon V \longrightarrow V^\vee, \quad v \longmapsto \sum_{\lambda \in \Sigma} \langle v, \lambda^\vee \rangle \lambda^\vee$$

and define a symmetric dot product on V by the formula

$$u \bullet v = \big\langle u, \rho(v) \big\rangle = \sum_{\lambda \in \Sigma} \langle u, \lambda^\vee \rangle \langle v, \lambda^\vee \rangle \, .$$

The semi-norm

$$\|v\|^2 = v\bullet v = \sum_{\lambda\in\Sigma} \langle v, \lambda^\vee\rangle^2$$

is positive semi-definite, vanishing precisely on

$$\mathrm{RAD}(V) = (\Sigma^\vee)^\perp .$$

In particular $\|\lambda\| > 0$ for all roots λ. Since $\Sigma^\vee$ is W-invariant, the semi-norm $\|v\|^2$ is also W-invariant. That $\|v\|^2$ vanishes on $\mathrm{RAD}(V)$ mirrors the fact that the Killing form of a reductive Lie algebra vanishes on the radical of the algebra.

4.3. Proposition. *For every root λ*

$$\|\lambda\|^2\,\lambda^\vee = 2\rho(\lambda) .$$

Thus although the map $\lambda \mapsto \lambda^\vee$ is not the restriction of a linear map, it is simply related to such a restriction.

Proof. For every μ in Σ

$$\begin{aligned}
s_{\lambda^\vee}\mu^\vee &= \mu^\vee - \langle\lambda, \mu^\vee\rangle\lambda^\vee \\
\langle\lambda, \mu^\vee\rangle\lambda^\vee &= \mu^\vee - s_{\lambda^\vee}\mu^\vee \\
\langle\lambda, \mu^\vee\rangle^2\,\lambda^\vee &= \langle\lambda, \mu^\vee\rangle\mu^\vee - \langle\lambda, \mu^\vee\rangle s_{\lambda^\vee}\mu^\vee \\
&= \langle\lambda, \mu^\vee\rangle\mu^\vee + \langle s_\lambda\lambda, \mu^\vee\rangle s_{\lambda^\vee}\mu^\vee \\
&= \langle\lambda, \mu^\vee\rangle\mu^\vee + \langle\lambda, s_{\lambda^\vee}\mu^\vee\rangle s_{\lambda^\vee}\mu^\vee
\end{aligned}$$

But since $s_{\lambda^\vee}$ is a bijection of $\Sigma^\vee$ with itself, we can conclude by summing over μ in Σ.

4.4. Corollary. *For every v in V and root λ*

$$\langle v, \lambda^\vee\rangle = 2\left(\frac{v\bullet\lambda}{\lambda\bullet\lambda}\right) .$$

Thus the formula for the reflection s_λ is that for an orthogonal reflection

$$s_\lambda v = v - 2\left(\frac{v\bullet\lambda}{\lambda\bullet\lambda}\right)\lambda .$$

4.5. Corollary. *The semi-simple ranks of a root system and of its dual are equal.*

Proof. The map

$$\lambda \longmapsto \|\lambda\|^2\,\lambda^\vee$$

is the same as the linear map 2ρ, so ρ is a surjection from $V(\Sigma)$ onto $V^\vee(\Sigma^\vee)$. Apply the same reasoning to the dual system to see that $\rho^\vee\circ\rho$ must be an isomorphism on $V(\Sigma)$, hence $\rho|V(\Sigma)$ an injection as well.

4.6. Corollary. *The space $V(\Sigma)$ spanned by Σ is complementary to $\mathrm{RAD}(V)$.*

So we have a direct sum decomposition

$$V = \mathrm{RAD}(V) \oplus V(\Sigma) .$$

This allows us to reduce properties of arbitrary systems to semi-simple ones.

Proof. Because the kernel of ρ is $\mathrm{RAD}(V)$.

4.7. Corollary. *The canonical map from $V(\Sigma)$ to the dual of $V^\vee(\Sigma^\vee)$ is an isomorphism.*

4.8. Corollary. *The set Σ is contained in a lattice of $V(\Sigma)$.*

Proof. Because it is contained in the lattice of v such that $\langle v, \lambda^\vee\rangle$ is integral for all $\lambda^\vee$ in some linearly independent subset of $\Sigma^\vee$.

4.9. Corollary. *The Weyl group is finite.*

Proof. It fixes all v annihilated by $\Sigma^\vee$ and therefore embeds into the group of permutations of Σ.

CHARACTERIZING COROOTS. The formula for s_λ as an orthogonal reflection remains valid for any W-invariant Euclidean norm on $V(\Sigma)$ and its associated inner product. If we are given such an inner product, then we may set

$$\lambda^\vee = \left(\frac{2}{\lambda\bullet\lambda}\right)\lambda\,,$$

and then necessarily $\lambda^\vee$ is uniquely determined in $V^\vee(\Sigma^\vee)$ by the formula

$$\langle \mu, \lambda^\vee\rangle = \mu\bullet\lambda^\vee\,.$$

But there is another way to specify $\lambda^\vee$ in terms of λ, one which works even for most infinite root systems. The following, which I first saw in [Tits:1966], is surprisingly useful.

4.10. Corollary. *The coroot $\lambda^\vee$ is the unique element of $V^\vee$ satisfying these conditions:*

(a) $\langle \lambda, \lambda^\vee\rangle = 2$;
(b) it lies in the subspace of $V^\vee$ spanned by $\Sigma^\vee$;
(c) for any μ in Σ, the sum $\sum_\nu \langle \nu, \lambda^\vee\rangle$ over the affine line $(\mu + \mathbb{Z}\,\lambda)\cap\Sigma$ vanishes.

An advantage of this formulation is that it makes no reference to reflections.

Proof. (a) and (b) are immediate; (c) is true because the reflection s_λ preserves $(\mu+\mathbb{Z}\,\lambda)\cap\Sigma$ and $\langle s_\lambda v, \lambda^\vee\rangle = -\langle v, \lambda^\vee\rangle$.

To prove that it is unique, suppose $\ell^\vee$ another vector satisfying the same conditions. Suppose μ to be a root and m its projection onto the hyperplane $\lambda = 0$. Since the the affine line $(\mu+\mathbb{Z}\,\lambda)\cap\Sigma$ is invariant under $s_{\lambda^\vee}$, that sum is equal to some positive integral multiple of m. Thus $\langle \lambda^\vee - \ell^\vee, v\rangle = 0$ when $v = \lambda$ and also when v is the projection of a root onto the hyperplane $\lambda = 0$. Since these v span the dual of $V(\Sigma^\vee)$, $\lambda^\vee - \ell^\vee = 0$.

4.11. Corollary. *For all roots λ and μ*

$$(s_\lambda\mu)^\vee = s_{\lambda^\vee}\mu^\vee\,.$$

Proof. We have already seen a proof of this when the system is semi-simple, but here I'll use Tits' criterion instead. According to that criterion, it must be shown that

(a) $\langle s_\lambda\mu, s_{\lambda^\vee}\mu^\vee\rangle = 2$;
(b) $s_{\lambda^\vee}\mu^\vee$ is in the linear span of $\Sigma^\vee$;
(c) for any root τ we have

$$\sum_\nu \langle \nu, s_{\lambda^\vee}\mu^\vee\rangle = 0$$

where the sum is over roots in over ν in $(\tau + \mathbb{Z}\,s_\lambda\mu)$.

(a) is immediate, since $s_{\lambda^\vee}$ is the contragredient of s_λ. (b) is trivial. As for (c), we know that

$$\sum_{\nu\in(\chi+\mathbb{Z}\mu)\cap\Sigma} \langle \nu, \mu^\vee\rangle = 0$$

for all roots χ. But

$$\langle \nu, \mu^\vee\rangle = \langle s_\lambda\nu, s_{\lambda^\vee}\mu^\vee\rangle$$

and and if we replace χ by $s_\lambda\tau$ we obtain equation (c).

4.12. Corollary. *For any roots λ, μ we have*

$$s_{s_\lambda\mu} = s_\lambda s_\mu s_\lambda\,.$$

Proof. The algebra becomes simpler if one separates this into two halves: (a) both transformations take $s_\lambda\mu$ to $-s_\lambda\mu$; (b) if $\langle v, (s_\lambda\mu)^\vee\rangle = 0$, then both take v to itself. Verifying these, using the previous formula for $(s_\lambda\mu)^\vee$, is straightforward.

4.13. Proposition. *The quadruple $(V(\Sigma), \Sigma, V^\vee(\Sigma^\vee), \Sigma^\vee)$ is a root system.*

It is called the **semi-simple root system** associated to the original.

Any set of roots Σ is the union of mutually orthogonal subsets Σ_i, each irreducible.

4.14. Corollary. *If Σ is the union of mutually orthogonal subsets Σ_i, then $V(\Sigma) = \oplus V(\Sigma_i)$.*

4.15. Proposition. *Suppose U to be a vector subspace of V, $\Sigma_U = \Sigma \cap U$, $\Sigma_U^\vee = (\Sigma_U)^\vee$. Then $(V, \Sigma_U, V^\vee, \Sigma_U^\vee)$ is a root system.*

Proof. If λ lies in $\Sigma_U = U \cap \Sigma$ then the reflection s_λ certainly preserves Σ_U. The same is true for $\Sigma_U^\vee$ by Corollary 4.11.

METRIC AXIOMS. The metric $\|v\|^2$ vanishes on $(\Sigma^\vee)^\perp$, but any extension of it from $V(\Sigma)$ to a semi-Euclidean metric on all of V for which Σ and this space are orthogonal will be W-invariant. Thus we arrive at a Euclidean structure on V such that for every λ in Σ:

(a) $2(\lambda\bullet\mu)/(\lambda\bullet\lambda)$ is integral;
(b) the subset Σ is stable under the orthogonal reflection

$$s_\lambda \colon v \longmapsto v - 2\left(\frac{v\bullet\lambda}{\lambda\bullet\lambda}\right)\lambda\,.$$

Conversely:

4.16. Proposition. *Suppose V to be a Euclidean space on it, suppose Σ to be a finite subset with the properties (a) and (b) above for every λ in Σ. Define for every λ in Σ a vector $\lambda^\vee$ in $V^\vee$ by the formula*

$$\langle\lambda^\vee, v\rangle = 2\left(\frac{v\bullet\lambda}{\lambda\bullet\lambda}\right)\,.$$

Then $(V, \Sigma, V^\vee, \Sigma^\vee)$ is a root system.

This follows from Theorem 4.2.

SATURATION. In practice, root systems can be constructed from a very small amount of data. Suppose V to be a Euclidean space, S is a finite set of orthogonal reflections and Λ a finite subset of V. The **saturation** of Λ with respect to S is the smallest subset of V containing Λ and stable under S.

For any vector v in the Euclidean space V define $v^\vee$ to be the element of $V^\vee$ such that

$$\langle v^\vee, u\rangle = 2\left(\frac{u\bullet v}{v\bullet v}\right)\,.$$

Then

$$s_v \colon u \longmapsto u - \langle u, v^\vee\rangle v$$

is an orthogonal reflection.

4.17. Proposition. *Suppose Λ to be a finite subset of the Euclidean space V containing a basis of V. Let S be the set of s_λ. Assume that $\Lambda^\vee$ contains a basis of $V^\vee$, and that $\langle\lambda, \mu^\vee\rangle$ lies in $\mathbb{Z}$ for all λ, μ in Λ. Then the saturation Σ of Λ with respect to S is finite and determines a root system $(V, \Sigma, V^\vee, \Sigma^\vee)$.*

Proof. Let L be the subgroup of all v in V such that $\langle\lambda^\vee, v\rangle$ lies in $\mathbb{Z}$ for all λ in Λ. Since $\Lambda^\vee$ contains a basis of $V^\vee$, it is contained in a lattice. Since Λ contains a basis of V, it contains a basis of V, so it is actually a lattice.

We construct Σ by starting with Λ and applying elements of S repeatedly until we don't get anything new. This process will to stop with Σ finite, as we shall see.

So define $\Lambda_0 = \Lambda$, and

$$\Lambda_{n+1} = \Lambda \cup \{ s_\lambda \mu \,|\, \lambda \in \Lambda, \mu \in \Lambda_n \} .$$

Since

$$\langle s_\lambda \mu, \nu^\vee \rangle = \langle \mu, \nu^\vee \rangle - \langle \mu, \lambda^\vee \rangle \langle \lambda, \nu^\vee \rangle$$

the set Λ_{n+1} is contained in L if Λ_n is. Apply induction to conclude all the Λ_{n+1} are contained in L. But since the reflections are orthogonal, elements of all Λ_n are also bounded in length. Therefore the process has to stop.

5. Examples

Suppose $(V, \Sigma, \lambda \mapsto \lambda^\vee)$ to be a root system.

RANK ONE SYSTEMS. Suppose λ to be in Σ. Then $-\lambda$ also lies in Σ. Any other root must be a multiple of λ, say $\mu = c\lambda$. As we have seen, $c = \pm 1/2$, ± 1, or ± 2. All cases can occur—in dimension one both

$$\{\pm\lambda\} \;\text{ or }\; \{\pm\lambda, \pm 2\lambda\}$$

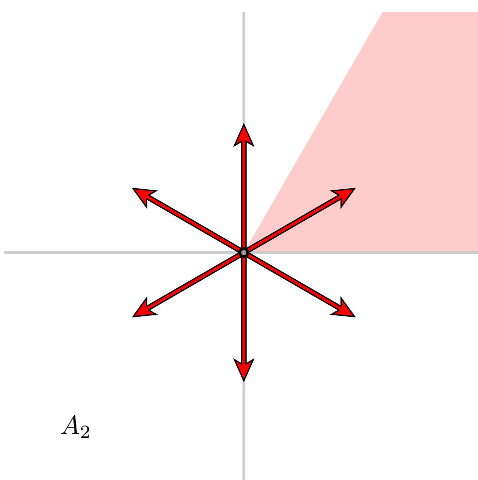
are possible root systems. To summarize:

5.1. Lemma. *If λ and $c\lambda$ are both roots, then $c = \pm 1$, $\pm 1/2$, or ± 2.*

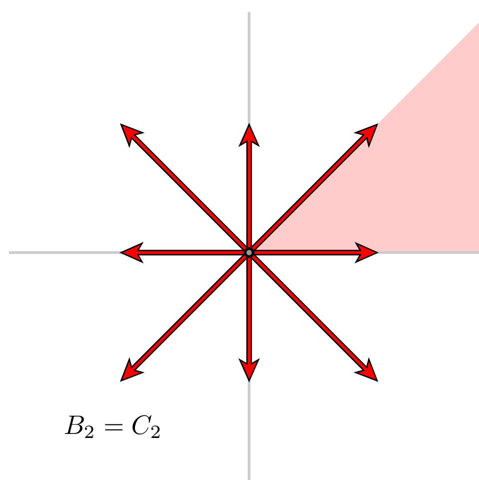
A root λ is called **indivisible** if $\lambda/2$ is not a root. It is easy to see that:

5.2. Proposition. *The indivisible roots in any root system also make up a root system.*

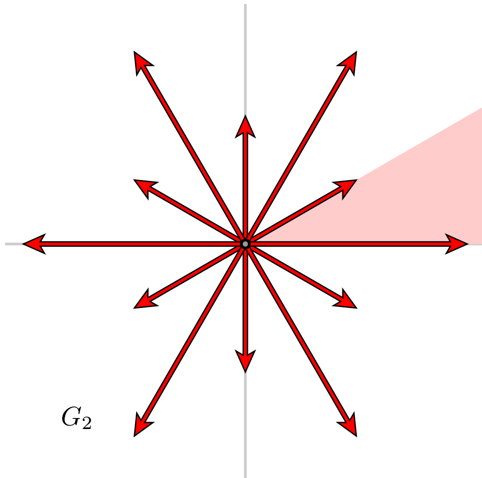
RANK TWO SYSTEMS. Suppose α, β to be linearly independent vectors in a Euclidean plane whose reflections generate a finite group preserving the lattice they span. The product $s_\alpha s_\beta$ is a rotation preserving the lattice, and must therefore have order 2, 3, 4, or 6. In the first case they commute. The other possibilities are shown in the following diagrams. The last is not reduced.

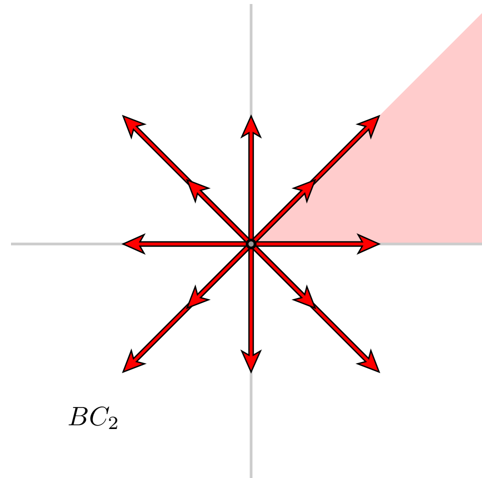


A_2



$B_2 = C_2$





6. Bases

In this section I'll summarize without proof further important developments. Suppose given a root system $(V, \Sigma, V^\vee, \Sigma^\vee)$.

The connected components of the complement in $V^\vee$ of the root hyperplanes $\lambda = 0$ for λ in Σ are called the **chambers** of the system.

6.1. Proposition. *The chambers are simplicial cones.*

This means that a chamber is defined by inequalities $\alpha > 0$ as α ranges over a set of linearly independent linear functions in V.

Fix one of these, say C. It is open in $V^\vee$. Define Δ to be the indivisible roots defining the walls of C. The elements of Δ are called the **simple roots** determined by the choice of C. As already noted, they are linearly independent. By definition, no root hyperplane intersects C. Those roots that are positive on C are called **positive**, and the rest negative.

6.2. Proposition. *Every positive root is a non-negative, integral, linear combination of simple roots.*

The chamber is a strong fundamental domain for W. The group W is generated by the elementary reflections s_α for α in Δ. Because C is simplicial, its closed faces of are all of the form

$$\overline{C}_\Theta = \{ v \in V \mid \langle \alpha, v \rangle = 0 \text{ for all } \alpha \in \Theta \}$$

for some subset $\Theta \subseteq \Delta$. Let C_Θ be the relative interior of $\overline{C}_\Theta$.

6.3. Proposition. *The closed face $\overline{C}_\Theta$ is exactly the points of C fixed by the subgroup W_Θ generated by the s_α with α in Θ.*

Let S be the set of elementary reflections s_α. An expression

$$w = s_{\alpha_1} \dots s_{\alpha_n} \quad (\alpha_i \in \Delta)$$

is called **reduced** if it is of minimal length among all such expressions. This minimal length $\ell(w)$ is called the **length** of w.

There is a basic relationship between combinatorics in W and geometry:

6.4. Proposition. *If α is a simple root, then $\ell(ws_\alpha) = \ell(w) + 1$ if and only if $w\alpha > 0$.*

A **Cartan matrix** is an integral square matrix $C = (c_{\alpha,\beta})$, indexed by a finite set $\Delta \times \Delta$, with these properties:

(a) all diagonal entries $c_{\alpha,\alpha}$ are equal to 2;
(b) $c_{\alpha,\beta} \le 0$ for $\alpha \ne \beta$;
(c) there exists a positive diagonal matrix D such that CD is positive definite symmetric.

6.5. Proposition. *The matrix $(\langle \alpha, \beta^\vee \rangle)$ is a Cartan matrix. Every Cartan matrix is that attached to a finite root system.*

If α and β are two elements of Δ, then the product $s_\alpha s_\beta$ is a two-dimensional rotation of finite order $m = m_{\alpha,\beta}$. Define

$$n_{\alpha,\beta} = \langle \alpha, \beta^\vee \rangle \langle \beta, \alpha^\vee \rangle .$$

It must be a positive integer, and since W preserves a lattice then the only cases that occur are 0, 1, 2, or 3.

$$m = \begin{cases} 2 & \text{if } n_{\alpha,\beta} = 0; \\ 3 & \quad n_{\alpha,\beta} = 1; \\ 4 & \quad n_{\alpha,\beta} = 2; \\ 6 & \quad n_{\alpha,\beta} = 3. \end{cases}$$

In other words, we recover the reduced systems of rank 2 described earlier.

Let S be the set of reflections s_α for α in Δ.

6.6. Proposition. *The group W is a Coxeter group with generating set S and relations*

$$s_\alpha^2 = I, \quad (s_\alpha s_\beta)^{m_{\alpha,\beta}} = I .$$

7. Root data

A **root datum** is a quadruple $(L, \Sigma, L^\vee, \Sigma^\vee)$ in which
(a) L is a free $\mathbb{Z}$-module of finite rank;
(b) $L^\vee = \mathrm{Hom}(L, \mathbb{Z})$;
(c) Σ is a finite subset of L;
(d) $\lambda \mapsto \lambda^\vee$ is a map from Σ to $L^\vee$ such that $\langle lambda, \lambda^\vee \rangle = 2$;
(e) Every reflection $s_{\lambda,\lambda^\vee}$ takes Σ to itself, and every $s_{\lambda^\vee,\lambda}$ takes $\Sigma^\vee$ to itself.

Root data determine reductive groups over an algebraically closed field just as root systems determine reductive Lie algebras. The asignment of a datum to a reductive group is classical. The converse assignment is not covered all that well in the literature—there does not seem to be a simple construction of the group from the datum. [Lusztig:2009] incorporates a promising idea of [Kostant:1966], but is also concerned with some elaboration that makes the argument much more complicated.

The simplest examples of root data are the **toric data**, in which $\Delta = \emptyset$.

For a slightly more interesting example, look at

$$\begin{aligned} G &= \mathrm{SL}_n \\ B &= \text{ upper triangular matrices in } G \\ T &= \text{ diagonal matrices in } B \ . \end{aligned}$$

Take $L = X^*(T)$, Δ the set of characters

$$\alpha_i \colon \mathrm{diag}(x_i) \longmapsto x^{\varepsilon_i - \varepsilon_{i+1}} = x_i / x_{i+1} \quad (1 \le i < n) .$$

The positive roots are those of the form x_i/x_j with $i < j$, which are those that occur in the eigenspace decomposition of the adjoint action of T on the Lie algebra of $\mathfrak{b}$. The lattice $L^\vee$ may be identified with the co-character group $X_*(T)$.

There is an analogue of Corollary 4.6 valid for root data. Suppose $\mathcal{L}_1$ and $\mathcal{L}_2$ to be two root data of the same rank. An isogeny from the first to the second is a map from $L_1^\vee$ to $L_2^\vee$ such that (a) the quotiemt of L_2 by the image of $L_1^\vee$ is finite; (b) $\Delta_1^\vee$ is mapped to $\Delta^\vee$; (c) under the dual map, Δ_2 is taken to Δ_1.

A root datum is called simply connected if $\Delta^\vee$ is a basis of $L^\vee$. For example, the root datum of SL_n is simply connected.

7.1. Proposition. *Any root datum is an isogeny quotient of a direct product of a toric lattice and a simply connected root datum.*

8. References

1. N. Bourbaki, Chapitres IV, V, et VI of **Groupes et algèbres de Lie**, Hermann, 1968.

2. Bertram Kostant, ‘Groups over $\mathbb{Z}$’, pp. 90–98 in [Borel-Mostow:1966].

3. George Lusztig, ‘Study of a $\mathbb{Z}$-form of the coordinate ring of a reductive group’, *Journal of the American Mathematical Society* **22** (2009), 739–769.