Math 574 Spring 2011 – Arithmetic of Lie Groups

Note Title 12/30/2010

Lecture 1: Familiar concrete examples.

The idea of this lecture is to avoid the abstraction of the general theory, & to focus on some particular examples of discrete subgroups Γ of Lie groups G.

<u>Def'n</u> A Lie group is a real manifold w/ a group structure whose operations are smooth maps. A discrete subgroup Γ of a Lie group is simply a subgroup which is discrete in the relative topology.

<u>Ex1</u> $G = \mathbb{R}$, $\Gamma = \mathbb{Z}$. The most general Γ here is $s\mathbb{Z}$ for some $s \geq 0$. Already this should be convincing that the study of cts & smooth f'ns on $\Gamma \backslash G$ is analytically rich, since it subsumes the harmonic analysis of Fourier series. Also, it has a lot of interesting number theory, eg., the classical formula that $\sum_{n=1}^{\infty} \frac{1}{n^2} = \pi^2/6$ comes through this.

<u>Ex2</u> $G = SL(n, \mathbb{R})$ = $n \times n$ real matrices w/ $\det = 1$,

There are lots of discrete Γ, uncountably many because of deformations. Most famous Γ is $SL(n,\mathbb{Z})$ = $n\times n$ integral matrices w/ det = 1. Also have nice subgroups of $SL(n,\mathbb{Z})$. Can deal w/ $GL(n)$ instead of $SL(n)$, also PGL & PSL (= mod scalar matrices). $n=2$ is already a famous case. There is a lot of number theory, in fact, for $SL(2,\mathbb{Z})$ because the membership of

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) \quad , \quad ad-bc=1,$$

requires that c & d be relatively prime, & that $a \equiv d^{-1}$ (mod b or c); likewise $b \equiv -c^{-1}$ (mod a or d), though these statements are vacuous mod 1 of course.

Ex3 $G = SL(n,\mathbb{C})$, $\Gamma = SL(n,\mathcal{O})$, where $\mathcal{O}$ = the ring of integers of an imaginary quadratic number field. The case $\mathcal{O} = \mathbb{Z}[i]$ = Gaussian integers is quite interesting, e.g., to hyperbolic manifolds ($n=2$).

Ex4 $G = SL(2,\mathbb{R}) \times SL(2,\mathbb{R})$. Of course, one could simply take $\Gamma = SL(2,\mathbb{Z}) \times SL(2,\mathbb{Z})$ or something else that resembles this product situation. Instead, irreducible examples are more interesting: Γ which do not contain a finite index subgroup which is a product of discrete subgroups from each factor.

This is the first appearance of a "virtual" condition, which essentially means modulo finite index subgroups. The classic example of an irreducible $\Gamma \subseteq SL(2,\mathbb{R}) \times SL(2,\mathbb{R})$ is $SL(2,\mathcal{O})$, where now $\mathcal{O}$ is the ring of integers of a real quadratic numberfield K

$$\mathcal{O} = \mathbb{Z} + \frac{d+\sqrt{d}}{2}\mathbb{Z}, \quad d = \mathrm{disc}(K)$$

($\mathcal{O}$ = algebraic integers in K (solutions to monic polynomials))

regarded as living inside $SL(2,\mathbb{R}) \times SL(2,\mathbb{R})$ using the diagonal embedding

$$\gamma \in SL(2,\mathcal{O}) \longmapsto (\sigma_1(\gamma), \sigma_2(\gamma)),$$

where σ_1, σ_2 are the 2 real embeddings of K, extended coordinate-by-coordinate to 2×2 matrices.

In a similar way, if K is an arbitrary number field (i.e., a finite extension of $\mathbb{Q}$) of degree $d = [K:\mathbb{Q}]$, K has r_1 embeddings into $\mathbb{R}$ (distinct injective homomorphisms $K \to \mathbb{R}$) & $2r_2$ pairs of embeddings into $\mathbb{C}$. The latter come in pairs via complex conjugation. The total $r_1 + 2r_2 = d$ (a basic result in algebraic number theory). Via these embeddings

$$SL(n,\mathcal{O}_K) \hookrightarrow \underbrace{SL(n,\mathbb{R}) \times \cdots \times SL(n,\mathbb{R})}_{r_1} \times \underbrace{SL(n,\mathbb{C}) \times \cdots \times SL(n,\mathbb{C})}_{r_2}$$

Aside from $\mathbb{Z}\backslash\mathbb{R}$, none of these Γ are cocompact in G, i.e., $\Gamma\backslash G$ is not compact. They do turn out to have finite volume quotients for SL (not GL, due to center), using the natural Haar measure on G. $GL(n,\mathbb{Z})\backslash GL(n,\mathbb{R})$ parametrizes n-dimensional lattices, so these configurations come up all over the place in modern mathematics, physics, and computer science.

There are 2 basic types of other $\Gamma \subseteq G$'s to mention. The first is when $G \subseteq GL(n,\mathbb{R})$ is a matrix Lie group. Then $G \cap GL(n,\mathbb{Z})$ is a discrete subgroup of G. Alternatively, G might also be defined by some arithmetic construction, & this might induce a different notion of group of integral points. We will study this in the coming lectures as a main topic.

The other concerns Lie groups which are not matrix groups. These could be infinite-dimensional Lie groups, or, more pedestrianly, covers of matrix Lie groups. The most famous example is

$$\widetilde{SL(2,\mathbb{R})}, \text{ the double cover of } SL(2,\mathbb{R}).$$

It cannot be written as a subgroup of $GL(n,\mathbb{R})$, yet it has phenomenally interesting arithmetic. In fact, if we view it as pairs (g, ε), $g \in SL(2,\mathbb{R})$ & $\varepsilon = \pm 1$, w/ a cocycle multiplication law, then it has a discrete subgroup of the form

$$\left\{ (\gamma, \varepsilon_\gamma) \;\middle|\; \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ w/ } \begin{matrix} c \equiv 0 (4) \\ a, d \equiv 1 (4) \end{matrix} \right\}$$

where ε_γ is the Kronecker symbol $\left(\frac{c}{d}\right)$ from number theory. In a way $\widetilde{SL(2,\mathbb{R})}$ cannot help but have deep arithmetic associated to it, because it doesn't simply get subgroups by intersection like we did w/ $G \cap GL(n,\mathbb{Z})$ above.

Lecture 2: Notion of Algebraic Group.

Let us recall some basic notions from algebraic geometry. There are several different definitions; I am choosing one which will be convenient for studying automorphic forms. We will think of linear algebraic groups as defined over an algebraically-closed field, and then consider special situations when they are defined over a subfield. In order to keep some of the alphabet free for later objects, let us consider an arbitrary field k and an algebraically closed field F which contains it:

$$k \subseteq F$$

Typically we have in mind that $k = \mathbb{Q}$ & $F = \mathbb{C}$. This allows us to be more concrete, than simply taking the larger field to be the algebraic closure of k. Also, it then makes it easier to replace k by a subfield, & analyze which structures still make sense over that subfield.

We define affine n-space (over F) to be F^n, n copies of the algebraically closed field F. An affine variety is any set of common zeroes in F^n of a set of polynomials defined over F. By the Hilbert Basis Theorem, we may assume this collection is finite. These are precisely the closed subsets of F^n under the Zariski topology, which furthermore extends to affine subvarieties as the subspace topology they inherit.

An affine algebraic group over F is an affine variety in F^n which has a group structure given by polynomial operations (with coefficients in F). For example, k is itself an algebraic group under addition, called $\mathbb{G}_a$ or $\mathbb{G}_a(F)$

How would one define the multiplicative group $\mathbb{G}_m$, without being allowed to use a statement like "$x \neq 0$"? There is an important trick of adding in an extra variable, which just as well allows us to define the general linear group $GL(n, F)$. We think of the entries of an $n \times n$ matrix as variables $x_1, \cdots, x_{n^2}$; & its determinant as the polynomial $d(x_1, \cdots, x_{n^2})$. Then

$GL(n, \bar{F})$ is the vanishing set in $\bar{F}^{n^2+1}$ of the polynomial

$$p(x_1, -, x_{n^2}, x_{n^2+1}) = x_{n^2+1} \cdot d(x_1, -, x_{n^2}) - 1,$$

so that the extra variable x_{n^2+1} stands in for $\overline{\text{determinant}}^{\,1}$. Thus for $G_m(\bar{F}) = GL(1, \bar{F})$, $x_2 = x_1^{-1}$, giving us the ability to take reciprocals without division. $GL(n, \bar{F})$ is an algebraic group under the usual operations (recall the inverse of a matrix can be written in terms of minors, divided by the determinant).

An affine variety is <u>reducible</u> if it is the union of 2 proper Zariski-closed subsets. "Disconnected" (union of 2 disjoint such subsets) for algebraic matrix groups is equivalent to irreducibility. Here of course "Zariski" refers to polynomials w/ coeff. in $\bar{F}$. The connected component of an algebraic matrix group G, G^0, always has $[G(\bar{F}) : G^0(\bar{F})]$ finite. G^0 is again an algebraic matrix group, of course. If $\bar{F} = \mathbb{C}$, G is Zariski connected if & only if its complex points $G(\mathbb{C})$ form a connected Lie group in the ambient euclidean topology.

<u>Warning</u>: reducibility & connectedness refer to the Zariski topology defined w/ polynomials over $\bar{F}$. It can happen that G is connected, defined over $\mathbb{R}$, but its $\mathbb{R}$-points are not connected in the usual sense. The best example of this is the group $GL(n)$, which is connected (because its $\mathbb{C}$-points are), but its $\mathbb{R}$-points $GL(n, \mathbb{R})$ are not because $\det = \pm 1$.

An <u>algebraic matrix group</u> (a.k.a., "linear algebraic group")

is a subgroup of $GL(n, F)$, $F \supseteq \bar{k}$ = algebraic closure of k, which is the common zero set of a finite set of polynomials in the matrix entries with coefficients in F (Zariski closed). The group is said to be defined over k if a $\exists$ a basis of the ideal of $F[x_1, \cdots, x_n]$ that the group annihilates which is contained in $k[x_1, \cdots, x_n]$.
In general, this is not the same as the simpler notion of k-closed, i.e. being the zero set of polynomials with coefficients in k. However, in char $= 0$ (& more generally for k perfect) it is!

We mainly take $k = \mathbb{Q}$, $F = \mathbb{C}$. Let G = algebraic matrix group defined over k, & consider its k-rational points $G_k = G \cap GL(n, k)$. A subgroup Γ of $G_{\mathbb{Q}}$ is called "arithmetic" if $\exists$ some faithful representation $\rho: G \to GL(N)$ defined over $\mathbb{Q}$ such that $\rho(\Gamma)$ & $\rho(G) \cap GL(N, \mathbb{Z})$ are commensurable (meaning their intersection has finite index in each).

Theorem (Borel) Γ arithmetic $\Rightarrow$ $\rho(\Gamma)$ & $\rho(G) \cap GL(m, \mathbb{Z})$ are commensurable for all rationally-defined faithful rep'ns $\rho: G \to GL(m)$, not just the one with $m = N$ in the def'n.
In particular, Γ arithmetic $\Leftrightarrow$ Γ & $G \cap GL(n, \mathbb{Z})$ are commensurable.

Natural question: if you replace $\mathbb{Q}$ by a finite extension, do you get new examples of arithmetic groups? Actually not, by "restriction of scalars" and the fact that the ring of integers has an integral basis.

Another def'n (equivalent): $G_{\mathbb{R}}$ acts on a finite-dimensional real vector space $\cong \mathbb{R}^n$, which has a lattice $\cong \mathbb{Z}^n$ (under $G \hookrightarrow GL(n)$ structure). $G(\mathbb{Z})$ is defined to be the stabilizer of this lattice, the "integral points" in G. Arithmetic means commensurable to the stabilizer of a lattice, e.g., $G(\mathbb{Z})$.

<u>Theorem</u> $\Gamma \subseteq G_{\mathbb{R}}$ is discrete, under the ambient real topology.

Interestingly, Γ can be cocompact (i.e., $\Gamma \backslash G$ is compact) sometimes, & this depends very much on G. E.g., it happens if $G_{\mathbb{R}}$ is compact. There are nice examples when $G_{\mathbb{R}}$ is not compact that come from this situation, though.

In order to develop the Lie theory for this, we investigate abelian subgroups. Recall that a closed subgroup of a Lie group is itself a Lie group. So for now we will study these special, abelian examples & later see how they fit in with the general theory.

<u>Tori</u> Here k is the ground field, which we usually take to be a number field such as $\mathbb{Q}$.

An <u>(algebraic) torus</u> is an algebraic matrix group which is isomorphic to $GL(1, F)^d \cong (F_{\neq 0})^d$ for some $d \geq 0$, which is called its dimension. Since it is a matrix group, it is natural to think of it consisting of diagonal elements. In fact, in $SL(n)$

the subgroup of diagonal matrices is an (algebraic) torus of dimension n. In $GL(n)$, dimension $n+1$.

<u>Theorem</u> Let G be a Zariski-connected algebraic group. Then each element of an (algebraic) torus (which is, a priori, a matrix) can be diagonalized over $\bar{F}$. In fact, the whole (algebraic) torus can be diagonalized simultaneously.

So just as algebraic matrix groups are subgroups of some $GL(n)$, and just as their arithmetic subgroups are commensurable their intersection with $GL(n,\mathbb{Z})$, so too their (algebraic) tori are intersections with conjugates of the famous (algebraic) torus of $GL(n)$ that consists of diagonal matrices.

<u>Nondiagonal</u> examples of tori: Let us consider $SO(2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ ad-bc=1 \right\}$, defined over $\mathbb{Q}$. Its real points form an abelian group, which is of course compact. Regard $SO(2)$ as a subgroup of $SU(2)$ in the obvious way. Then $SO(2)$ is torus, conjugate to the diagonal subgroup:

$$\begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix}^{-1}\begin{pmatrix} e^{i\theta} & \\ & e^{-i\theta} \end{pmatrix}\begin{pmatrix} 1 & i \\ -i & -1 \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Another: $\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \;\middle|\; a^2+b^2 \neq 0 \right\}$ over any field. It is conjugate to a diagonal subgroup over $\bar{k}$.
or put a "D" here.

The $\underbrace{\text{character}}_{\mathbb{C}\text{-rational maps to } \mathbb{C}^*}$ group of the complex torus $(\mathbb{C}^*)^d$ is $\cong \mathbb{Z}^d$. This is also true over $\bar{F}$.

This motivates some definitions:

<u>Def'ns</u> A torus is split over k (a.k.a., "k-split") if it is diagonalizable over k, & defined over k. Equivalently, all characters of it are defined over k. This means that if ρ is an algebraic representation of the torus into $GL(1)$, given by rational maps defined over $\bar{F}$, it can in fact be defined over k, (I.e., all $\mathbb{Z}^d$ of these characters are defined over k.)
All tori split over some finite extension.

On the other hand, an <u>anisotropic torus over k</u> is one which has no characters at all defined over k. If $k=\mathbb{R}$, this is equivalent to its real points being compact.

These are 2 extremes. If $k=\mathbb{R}$ & $d=\dim=1$, the torus is either $\mathbb{R}^*$ (k-split) or $\cong SO(2,\mathbb{R})$ (anisotropic). The $SO(2) \subseteq SU(2)$ example shows how sensitive this is to the arithmetic of the base field.

<u>Decomposition Theorem</u>: a) Any torus defined over k can be written as the unique product of a k-split torus & an anisotropic torus over k, having finite intersection. (An "almost direct product": finite intersection of factors.)

b) Given a k-torus T & a k-subtorus S, $\exists$ a k-subtorus S' such that $T=$ almost direct product of S & S' ($T = S.S'$ & $S \cap S'$ is finite).

Over $k = \mathbb{R}$, all tori are hence almost direct products of one-dimensional ones ($\mathbb{R}^*$ or $SO(2,\mathbb{R})$).

Unipotent Groups

A matrix is nilpotent if some power of it is zero. It is unipotent if it is equal to a nilpotent matrix plus the identity matrix. Warning: linear algebraic groups of unipotent elements are "nilpotent" groups.

Famous examples: upper triangular matrices which have all zeroes (resp. ones) on the diagonal.

Theorem Any Zariski-connected unipotent algebraic matrix group is conjugate to an upper triangular one (over $\bar{F}$).

Recall that if $F = \mathbb{C}$, Zariski-connectivity is equivalent to the connectivity of its $\mathbb{C}$-points.

So, in keeping with the earlier principle, connected unipotent algebraic groups are subgroups of the unipotent upper-triangular subgroup of $GL(n)$.

Solvable Groups

Recall this means that G has a series $G = G_0 \supseteq \cdots \supseteq G_k = \{e\}$ in which each

G_{i+1} is normal in G_i, & each G_i/G_{i+1} is abelian.

Lie-Kolchin Theorem: Zariski-connected solvable algebraic groups are conjugate to an upper triangular subgroup over $\bar{F}$ (& vice-versa).

Furthermore, a solvable group has a composition series in which each successive quotient is isomorphic to either $\mathbb{G}_a$ or $\mathbb{G}_m$ (the algebraic groups of the additive, resp. multiplicative, structures of a field).

For example, the algebraic group of all upper triangular matrices in $GL(n)$ is a maximal solvable subgroup, known as a Borel subgroup.

This motivates...

Split Groups over k

A Zariski-connected solvable algebraic matrix group defined over k is said to "split over k" if it has a composition series of connected k-subgroups whose successive quotients, over k, are either $\cong$ $\mathbb{G}_a(k)$ or $GL(1,k) \cong \mathbb{G}_m(k)$.

Example All tori, Zariski-connected, solvable algebraic matrix groups that are defined over k in fact split over k.

If $\mathrm{char}(k)=0$ (usually in our applications) & all maximal tori of G that are defined over k in fact split over k, then G is also split over k.

Lecture 3: Reductive & semisimple groups

The <u>radical</u> of an algebraic matrix group is its largest normal, connected solvable subgroup.

The <u>unipotent radical</u> of an algebraic matrix group is its largest connected unipotent normal subgroup.

We denote these radicals of G by $R(G)$ & $R_u(G)$, respectively. These, too, are linear algebraic groups.

G is <u>semisimple</u>* when $R(G) = \{e\}$. The quotient $G/R(G)$ is always semisimple. Analogously, G is <u>reductive</u>* when $R_u(G) = \{e\}$, & the quotient $G/R_u(G)$ is always reductive. *Some authors require Zariski-connectivity, too.

<u>Famous Example</u> of $GL(n)$: A standard parabolic subgroup of $GL(n)$ is associated to any partition of n,

$$n = n_1 + \dots + n_r, \quad n_i > 0,$$

as the subgroup of block upper triangular matrices

$$\left\{ \begin{array}{c|cccc} & n_1 & n_2 & \cdots & n_r \\ \hline n_1 & * & * & \cdots & * \\ n_2 & 0 & * & \cdots & * \\ \vdots & & & \ddots & \vdots \\ n_r & 0 & 0 & \cdots & * \end{array} \right\}$$

Its unipotent radical is the subgroup

$$\left\{ \begin{pmatrix} I_{n_1} & * & * & * \\ 0 & I_{n_2} & * & * \\ 0 & 0 & \ddots & * \\ 0 & 0 & 0 & I_{n_r} \end{pmatrix} \right\},$$

and the reductive quotient is $\cong GL(n_1) \times \cdots \times GL(n_r)$.
However, this is not semisimple because it contains

$$\begin{pmatrix} c_1 I_{n_1} & 0 & 0 & 0 \\ 0 & c_2 I_{n_2} & 0 & 0 \\ 0 & 0 & \ddots & \\ 0 & 0 & & c_r I_{n_r} \end{pmatrix}.$$

Semisimple groups like $SL(n)$, can have a finite center (e.g., if it is disconnected). The center is in the radical, of course.

<u>Product Theorem</u> (For characteristic 0) Every algebraic matrix group over k can be written as the semidirect product of a maximal reductive k-subgroup & its unipotent radical. All reductive subgroups defined over k are k-conjugate to a subgroup of this maximal reductive k-subgroup, by an element of the unipotent radical.

If G is an algebraic group, let G^0 be the connected component of the identity in the Zariski topology. It makes to look at G^0 because the defins of semisimple & reductive involve connectivity. G^0 always has finite index in $G \subseteq GL(n, \bar{F})$, & $R(G^0) = R(G)$, $R_u(G^0) = R_u(G)$.

Theorem G^0 is reductive if & only if it is the product of the semisimple algebraic group $[G,G]$ (smallest normal subgroup w/ abelian quotient) & a central torus. In characteristic 0, this is equivalent to all rational representations being fully reducible. Furthermore, if $k=\mathbb{R}$, it is equivalent to the existence of a matrix representation of $G_{\mathbb{R}}$ which is closed under the transpose map ("self-adjoint").

Conjugacy Theorems for Tori in Connected Algebraic Groups

Thm All maximal tori are conjugate over F.

We say an element of G is semisimple if it can be diagonalized over F.

Thm All semisimple elements are contained in some maximal torus.

The centralizer of a maximal torus is a Cartan subgroup. These are all connected & conjugate over k, & their common dimension is the rank, which is also the common dimension of the maximal tori.

If G is Zariski-connected & defined over k, it has a maximal torus defined over k.

A maximal solvable, connected, & closed (in Zariski topology for F) subgroup of G is called a <u>Borel subgroup</u> (cf. earlier $GL(n)$ example). Any closed subgroup of G that contains a Borel subgroup is called a <u>parabolic subgroup</u>.

Later we will state a conjugacy theorem for these.

<u>Theorem</u> $G_k = G \cap GL(n,k)$ is Zariski-dense in $G_{\bar{k}}$ when G is reductive & k is infinite. When $\mathrm{char}(k) = 0$, this density holds without any assumptions on G.

<u>Definition</u> An <u>anisotropic reductive group</u> over k is Zariski-connected and has no nontrivial k-split tori. Eg, $SO(2)$ over $k = \mathbb{R}$. In fact when $k = \mathbb{R}$ or $\mathbb{Q}_p$, this is equivalent to the compactness of G_k in the usual topology. In an arbitrary field of characteristic zero, it is equivalent to G_k having no nontrivial unipotent elements and no nontrivial characters.

<u>Ex</u> $SU(2,\mathbb{C}) \cong SL(2,\mathbb{C})$ is not anisotropic, & has nontrivial unipotents. However, their real points, $SO(2,\mathbb{R})$ & $SL(2,\mathbb{R})$, respectively, are totally different in this respect. Such real forms exhibit a spectrum of behavior.

Way to measure this: define the k-rank of a Zariski-connected reductive group G to be the dimension of any maximal k-split torus

In fact $N(S) = N(S)_k Z(S)$, so each coset in ${}_kW(G) = N(S)/Z(S)$ has a representative in G_k.

Famous Example $SL(n)$, $k = \mathbb{R}$

$$S = \left\{ \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \middle| \ a_1 \cdots a_n = 1 \right\}$$ is a maximal $\mathbb{R}$-split torus

For general $g = (g_{ij}) \in G$, calculate

$\begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix} g \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix}^{-1}$ has (i,j)-th entry equal to $a_i g_{ij} a_j^{-1}$.

Thus $Z(S) = S$, proving it is maximal

Now consider $g \in N(S)$, which means that $\forall s_1 \in S$ $\exists s_2 \in S$ such that $gs_1 = s_2 g$, i.e.

$s_1 = \mathrm{diag}(a_1, \dots, a_n)$ etc...

$$g_{ij} a_j = g_{ij} a_i' \quad , \quad 1 \leq i,j \leq n.$$

Since we may chose s_1, we can assume the a_j are distinct. Then

$$g_{ij} \neq 0 \Rightarrow a_j = a_i'.$$

This implies for any i, $g_{ij} = 0$ for all but at most one j (exactly one, since g is invertible), $N(S)$ is stable under transpose, so it thus has exactly one nonzero entry in each row & column. We conclude $N(S) = S \times$ permutation matrices & ${}_{\mathbb{R}}W(G) \cong S_n$ as permutation

Matrices.

We now wish to define the Lie algebra in such a way that holds for general fields, i.e., not simply using Lie groups, but instead algebraically.

Recall we have set up the definition so that the algebraic group G is a Zariski closed subgroup of some $GL(n, F)$. Let I_k = the ideal of $k[x_1, \cdots, x_{n^2+1}]$ of polynomials that vanish on G for a subfield $k \subseteq F$. We furthermore said G is defined over k (aka, a "k-group") if the ideal $I_k \subseteq I_F$ generates the latter. When $\text{Char}\, k = 0$, it is equivalent to G being the zero set of polynomials with coefficients in k.

<u>Definition</u> The coordinate ring of G over k is

$$k[G] := k[x_1, \cdots, x_{n^2+1}] / I_k$$

The coordinate ring over F, $F[G]$, is an integral domain (a nontrivial commutative ring without zero divisors).

Motivation: this is basically the space of polynomial functions defined on G. One feature of the Lie algebra of a Lie group is that it differentiates functions by infinitessimal translation, e.g.,

$$(Xf)(g) := \frac{d}{dt}\Big|_{t=0} f(g e^{tX}) \quad , \quad g \in G, \ X \in \mathfrak{g}.$$

So we will try to mimic this algebraically. The above derivative satisfies Leibniz's rule (the product rule from first semester calculus),

$$X(f_1 \times f_2)(g) = \frac{d}{dt}\Big|_{t=0} f_1(ge^{tX}) f_2(ge^{tX})$$

$$= Xf_1 \times f_2 + f_1 \times Xf_2$$

(Since this is a one-variable phenomenon), So, instead, we will algebraically imitate this on functions in the coordinate ring, A key point is that the Lie algebra is identified with the tangent space at the identity, & that the differential operators just mentioned are invariant under left-translating the function:

if $\quad (\lambda(h)f)(g) = f(h^{-1}g), \qquad$ for $g, h \in G$,
$\qquad$ (so $\lambda(h_1)\lambda(h_2) = \lambda(h_1h_2)$)

$$X(\lambda(h)f) = \lambda(h)Xf.$$

Suppose K is an arbitrary field. A K-algebra A is a commutative ring containing the field K. A K-derivation is a K-linear map to some A-module M such that

$$X(ab) = (Xa)b + a(Xb), \qquad \forall a, b \in A.$$

Here we tacitly regard M as an A-bi-module with $am = ma$ by definition, which makes sense because A is commutative. We denote the set of K-derivations from

A to M as $\mathrm{Der}_k(A, M)$.

We now take $K = F$, $A = F[G]$, & $M = F[G]$ & set

$$\mathrm{Lie}(G) := \{D \in \mathrm{Der}_F(A, A) \mid D \text{ commutes w/ left translation by } G\}$$

whose k-points are

$$\mathrm{Lie}(G)_k = \{D \in \mathrm{Lie}(G) \mid D(k[G]) \subseteq k[G]\}.$$

This is a finite-dimensional vector space over the respective base field F or k.

Remarks 1) $\mathrm{Lie}(G) = \mathrm{Lie}(G^0)$ = connected component of identity)

2) $\mathrm{Lie}(G)_k \otimes F = \mathrm{Lie}(G)$

3) $\mathrm{Lie}(G)$ is in fact a Lie algebra over F, & likewise $\mathrm{Lie}(G)_k$ is one over k. The Lie bracket is $[X, Y] = XY - YX$. (Recall that a Lie algebra is a finite-dimensional vector space over a ground field endowed with a k-bilinear bracket $[\,,\,]$ such that

$$[X, X] = 0$$

& $$[X,[Y,Z]] + [Y,[Z,X]] + [Z,[X,Y]] = 0 \quad (\text{"Jacobi Identity"}).$$

Of course, for k a number field & $F = \mathbb{C}$, $\mathrm{Lie}(G)$ is a complex Lie algebra — which have been completely classified dating back to Killing & Cartan classification of root systems etc. We will describe this later.

The group G acts on $Lie(G)$ by the adjoint action

$$Ad(g)X := gXg^{-1}, \qquad g \in G \;\&\; X \in Lie(G)$$

which acts on $f \in F[G]$ by first translating the argument by g, applying X, then translating back by g^{-1}.

<u>Example</u> $G = GL(2,\mathbb{C})$, $\mathfrak{g} = Lie(G) = M_2(\mathbb{C})$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} w & x \\ y & z \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}.$$

This is conjugation, & leaves scalars $\begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix}$ invariant. In fact, it decomposes into a 3-dimensional rep'n & this one-dimensional representation. In particular, the adjoint action of its maximal torus $\left\{\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}\right\}$ is noteworthy:

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}\begin{pmatrix} w & x \\ y & z \end{pmatrix}\begin{pmatrix} a^{-1} & 0 \\ 0 & d^{-1} \end{pmatrix} = \begin{pmatrix} w & \frac{a}{d}x \\ \frac{d}{a}y & z \end{pmatrix}.$$

Under this action, $M_2(\mathbb{R})$ decomposes as the direct sum of subspaces spanned by

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

respect., under which the torus acts by the characters

$$1, \quad 1, \quad \frac{a}{d}, \quad \& \quad \frac{d}{a},$$

respectively. This is an important phenomenon which motivates the following crucial definitions.

<u>Definition</u>: Let G be a reductive linear algebraic group with a torus $S \subseteq G$. The image of S under $Ad(S)$ is diagonalizable in $GL(Lie(G))$. If α is a nonzero character of S's action on $\mathfrak{g} = Lie(G)$, its <u>root space</u>

$$\mathfrak{g}_\alpha^{(S)} := \{ X \in \mathfrak{g} = Lie(G) \mid Ad(s)X = s^\alpha X, \ \forall s \in S \},$$

provided this space is nontrivial, in which case α is called a root of G relative to S. (We use additive notation for the character.) We let $\Phi(G,S)$ denote the set of such α. It is finite, & the Lie algebra is the direct sum

$$\mathfrak{g} = \mathfrak{g}_0^{(S)} \oplus \bigoplus_{\alpha \in \Phi(G,S)} \mathfrak{g}_\alpha^{(S)},$$

where $\mathfrak{g}_0^{(S)} = \{ X \in \mathfrak{g} \mid Ad(s)X = X, \ \forall s \in S \}$.

In the special case that S is a maximal torus, we say $\Phi(G) = \Phi(G,S)$ consists of all roots of G, & write $\mathfrak{g}_\alpha$ for $\mathfrak{g}_\alpha^{(S)}$. The set Φ is independent of the choice of maximal torus, because their respective Ad actions are conjugate, & have the same eigenvalues. It is therefore an important invariant of the algebraic matrix group G.

Returning to the previous example, w/ S as the full torus, the eigenspace for the trivial character is 2-dimensional.

If $X \in \mathfrak{g}_\alpha$ & $Y \in \mathfrak{g}_\beta$, then $[X,Y] = XY - YX$ is clearly in $\mathfrak{g}_{\alpha+\beta}$. If this latter space is zero, it reflects the commutativity of the 2 root spaces. There are only finitely many roots, and their structure is encoded nicely as a root system, the subject of the next lecture.

All of this has been for F, but one can define the notions restricted to k. It should be expected that there are more roots & root spaces over F, & that the dimensions of root spaces over k are larger. Also, the Weyl group clearly acts on the root spaces.

Note: One can treat roots via actions on one-parameter subgroups, without reference to the Lie algebra.

Lecture 5: Root Systems

In the previous lecture, we considered root spaces & the relation

$$[\mathfrak{g}_\alpha, \mathfrak{g}_\beta] \subseteq \mathfrak{g}_{\alpha+\beta}.$$

One of the most effective ways of understanding the roots is via the notion of root system. They live in a finite-dimensional vector space (of characters), which has a metric invariant under the (finite) Weyl group. Thus it is an example of.....

Definition Let V = finite dimensional real vector space with a nondegenerate, positive inner product (essentially this is $\mathbb{R}^n$). A finite subset $\Phi \subseteq V$ is a root system if it satisfies these axioms,

1) The $\mathbb{R}$-span of Φ is V.
2) $\Phi = -\Phi$
3) $s_\alpha(v) := v - 2\alpha\langle\alpha, v\rangle/\langle\alpha,\alpha\rangle$ preserves Φ
   (reflection in plane $\perp$ to α, e.g., $s_\alpha(\alpha) = -\alpha$)
4) $\underbrace{\dfrac{2\langle\alpha,\beta\rangle}{\langle\alpha,\alpha\rangle}}_{\text{called "Cartan integers"}} \in \mathbb{Z}$ for any $\alpha, \beta \in \Phi$.

The Weyl group of a root system is the finite group generated by $\{s_\alpha \mid \alpha \in \Phi\}$. It is finite, since Φ is finite.

The root system is furthermore reduced if
5) $\alpha, r\alpha \in \Phi \Rightarrow r = \pm 1$.

It is <u>irreducible</u> if not the direct sum of 2 sub-root systems. Every root system is a sum of irreducibles, so we mainly study those.

<u>Example</u> Let $G = SL(3,\mathbb{R})$
$\mathfrak{g} = \mathrm{Lie}(G)$ = traceless, real 3×3 matrices.
Clearly $S = \{$diagonal matrices$\}$ constitute a torus. If $g \in G$ commutes w/ all diagonal matrices, the formula

$$\begin{pmatrix} a_1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & a_3 \end{pmatrix}\begin{pmatrix} g_{11} & g_{12} & g_{13} \\ g_{21} & g_{22} & g_{23} \\ g_{31} & g_{32} & g_{33} \end{pmatrix}\begin{pmatrix} a_1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & a_3 \end{pmatrix}^{-1} = \begin{pmatrix} g_{11} & \frac{a_1}{a_2} g_{12} & \frac{a_1}{a_3} g_{13} \\ \frac{a_2}{a_1} g_{12} & g_{22} & \frac{a_2}{a_3} g_{23} \\ \frac{a_3}{a_1} g_{13} & \frac{a_3}{a_2} g_{32} & g_{33} \end{pmatrix}$$

shows that g is diagonal & hence already in S. Hence S is a maximal torus. The same calculation shows that $\mathfrak{g}$ is the direct sum of the Lie algebra of S = traceless diagonal matrices, & root spaces

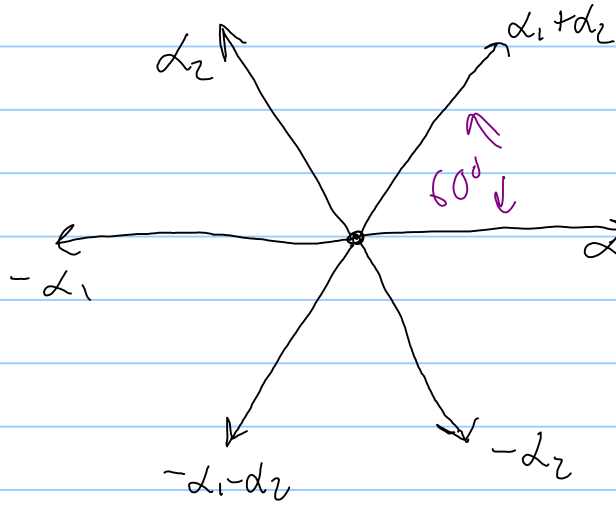
$$\left\{\begin{pmatrix} 0 & * & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\right\}, \quad \left\{\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & * \\ 0 & 0 & 0 \end{pmatrix}\right\}, \quad \left\{\begin{pmatrix} 0 & 0 & * \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\right\}, \quad \left\{\begin{pmatrix} 0 & 0 & 0 \\ * & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\right\}$$

for $\alpha_1 = \frac{a_1}{a_2}$, $\quad \alpha_2 = \frac{a_2}{a_3}$, $\quad \alpha_1 + \alpha_2 = \frac{a_1}{a_3}$, $\quad -\alpha_1 = \frac{a_2}{a_1}$,

$$\left\{\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ * & 0 & 0 \end{pmatrix}\right\}, \quad \& \quad \left\{\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & * & 0 \end{pmatrix}\right\}.$$

$-\alpha_1 - \alpha_2 = \frac{a_1}{a_3}$ $\qquad\qquad$ $-\alpha_2 = \frac{a_3}{a_2}$

Here is a diagram of its root system



The "A_2 root system"

Later we will explain the geometry – it has to do with the fact the Weyl group is S_3.

<u>Another example</u>: $G = Sp(4,\mathbb{R}) = \{ g \in SL(4,\mathbb{R}) \mid gJg^t = J \}$, where $J = \begin{pmatrix} 0&0&0&1 \\ 0&0&1&0 \\ 0&-1&0&0 \\ -1&0&0&0 \end{pmatrix}$.

Note! often $J = \begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix}$ is used instead, which gives a different group. This is better suited for some purposes because it is a split real form.

The Lie algebra $\mathrm{Lie}(G) = \mathfrak{sp}(4,\mathbb{R})$ consists of all $X \in \mathfrak{sl}(4,\mathbb{R})$ such that $XJ + JX^t = 0$. (This is derived by taking $g = e^{tX}$, $t \in \mathbb{R}$, & differentiating at $t=0$.) Thus

$$\mathfrak{sp}(4,\mathbb{R}) = \left\{ \begin{pmatrix} t_1 & x_1 & x_3 & x_2 \\ y_1 & t_2 & x_2 & x_4 \\ y_3 & y_2 & -t_2 & -x_1 \\ y_2 & y_4 & -y_1 & -t_1 \end{pmatrix} \in M_4(\mathbb{R}) \right\}.$$

For the same reason as for $SL(3)$, diagonal matrices constitute a maximal torus

$$T = \left\{ \begin{pmatrix} a_1 & 0 & 0 & 0 \\ 0 & a_2 & 0 & 0 \\ 0 & 0 & a_2^{-1} & 0 \\ 0 & 0 & 0 & a_1^{-1} \end{pmatrix} \middle| \; a_1, a_2 \neq 0 \right\}.$$

Here $\mathfrak{sp}(4,\mathbb{R})$ is the direct sum of S's Lie algebra, & the following 8 root spaces:

(variable x_1) $\begin{pmatrix} 0&1&0&0\\ 0&0&0&0\\ 0&0&0&-1\\ 0&0&0&0 \end{pmatrix}$ $\alpha_1 = \dfrac{a_1}{a_2}$

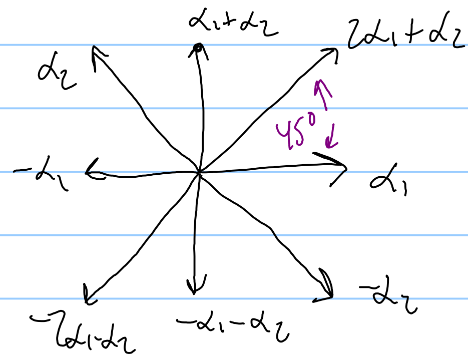
(variable x_2) $\begin{pmatrix} 0&0&0&0\\ 0&0&1&0\\ 0&0&0&0\\ 0&0&0&0 \end{pmatrix}$ $\alpha_2 = a_2^2$

(variable x_3) $\begin{pmatrix} 0&0&1&0\\ 0&0&0&1\\ 0&0&0&0\\ 0&0&0&0 \end{pmatrix}$ $\alpha_1+\alpha_2 = a_1 a_2$

(variable x_4) $\begin{pmatrix} 0&0&0&1\\ 0&0&0&0\\ 0&0&0&0\\ 0&0&0&0 \end{pmatrix}$ $2\alpha_1+\alpha_2 = a_1^2$

In each case, can replace "x" w/ "y", matrix w/ transpose, "α" w/ "$-\alpha$", & character formula with inverse.

Root system



The "C_2 root system"

<u>Another Example:</u> $G = SO(4,\mathbb{R})$, but the split real form which is defined with

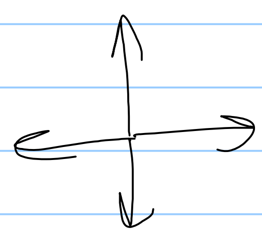
$$J = \begin{pmatrix} 0&0&0&1\\ 0&0&1&0\\ 0&1&0&0\\ 1&0&0&0 \end{pmatrix},$$ not the identity matrix.

This is noncompact, as we will see. Similar computation shows

$$\mathfrak{so}(4,\mathbb{R}) = \{ X \in \mathfrak{sl}(4,\mathbb{R}) \mid XJ = -JX^t \}$$

$$= \left\{ \begin{pmatrix} t_1 & x_1 & x_2 & 0 \\ y_1 & t_2 & 0 & -x_2 \\ y_2 & 0 & -t_2 & -x_1 \\ 0 & -y_2 & -y_1 & -t_1 \end{pmatrix} \in \mathfrak{sl}(4,\mathbb{R}) \right\}.$$

It has the same maximal torus as $Sp(4,\mathbb{R})$, using the exact same logic. It has only 2 roots, & infact the root system is reducible, being a copy of 2 $\mathfrak{sl}(2,\mathbb{R})$'s:



The "D_2 root system"

Infact, it is isogeneous to $SL(2,\mathbb{R}) \times SL(2,\mathbb{R})$. This causes the following issue: sometimes in math one gets interesting constructions for $SL(2,\mathbb{R}) \times SL(2,\mathbb{R})$ that do not generalize to $SL(n,\mathbb{R}) \times SL(n,\mathbb{R})$, but to $SO(2n,\mathbb{R})$ (cf. Fergan's talk in the number theory seminar last year, which explained limitations about L-function special values).

Another Example: $G = SO(5,\mathbb{R})$, again, split real form w/ Lie algebra

$$\mathfrak{so}(5,\mathbb{R}) = \left\{ \begin{pmatrix} t_1 & x_1 & x_3 & x_4 & 0 \\ y_1 & t_2 & x_2 & 0 & -x_4 \\ y_3 & y_2 & 0 & -x_2 & -x_3 \\ y_4 & 0 & -y_2 & -t_2 & -x_1 \\ 0 & -y_4 & -y_3 & -y_1 & -t_1 \end{pmatrix} \in \mathfrak{sl}(5,\mathbb{R}) \right\}$$

(Note position of 0's reflects differences

between SO(odd) & SO(even)).
The maximal torus is

$$S = \left\{ \begin{pmatrix} a_1 & & & \\ & a_2 & & \\ & & a_2^{-1} & \\ & & & a_1^{-1} \end{pmatrix} \right\}$$

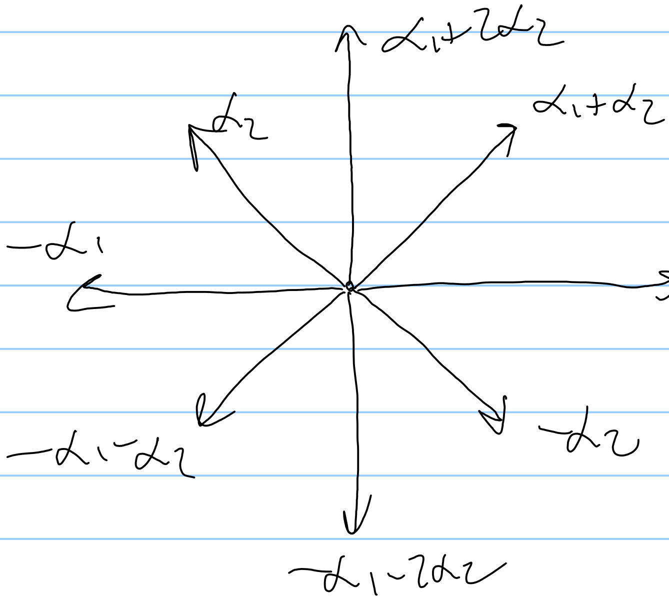
and the roots are

(variable x_1) $\quad \alpha_1 = \frac{a_1}{a_2}$ $\qquad$ (variable x_3) $\alpha_1+\alpha_2 = a_1$

(variable x_2) $\quad \alpha_2 = a_2$ $\qquad$ (variable x_4) $\alpha_1+2\alpha_2 = a_1 a_2$

In each case, the root vector is the coefficient matrix of the "x" variable & transposing the matrix is the same as replacing "x" with "y" is the same as negating "α" is the same as taking the inverse character.

The root system is



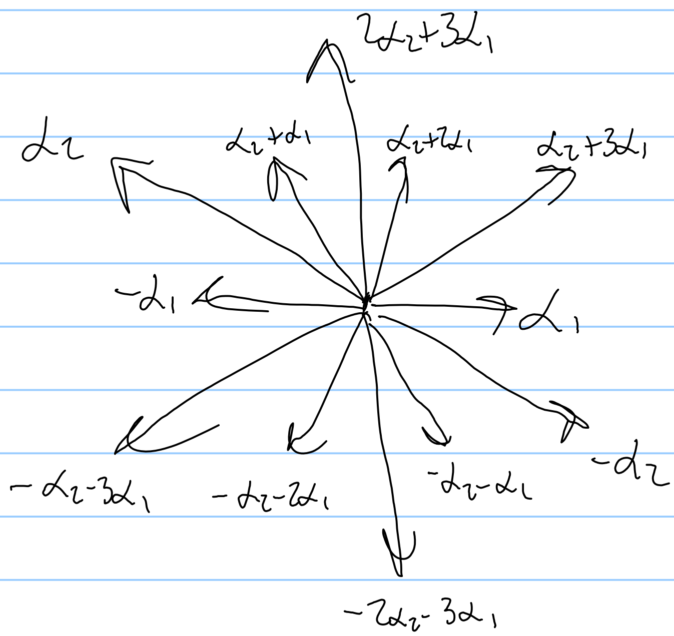
The "C_2 root system."

Note: it's really B_2, rotated! Thus these have the same root system, & in fact $Sp(4,\mathbb{R})$ & $SO(5,\mathbb{R})$

are isogeneous, split real rank 2 Lie groups.

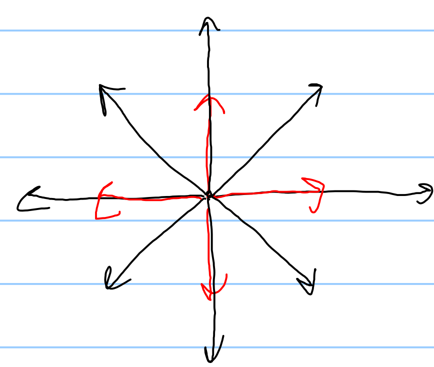
Last Example $G = G_2(\mathbb{R})$, split real group, will not define here, as it is complicated. It can be realized as a subgroup of $SO(7,\mathbb{R})$ (again, the split real form).

Root system:



The "G_2 root system"

These root systems A_2, $B_2 \cong C_2$, & G_2 are precisely all reduced root systems of $\mathbb{R}^2$. There is additionally a single nonreduced root system, BC_2, which is the union of B_2 & C_2.



Lecture 6: Some nonsplit orthogonal groups

So far we have looked at some maximally split examples, which are in some sense as noncompact as possible. On the other extreme are rank 0 groups which are compact (at least as real Lie groups). There is a general phenomenon of "forms" of algebraic groups: inequivalent algebraic groups which are isomorphic over $\bar{F}$.

Let us now take a detailed look at some orthogonal groups. For example, our (very noncompact) $SO(2)$ before has an inner form $SO(2,\mathbb{R})$ which is famously compact (the usual one we know). In general, $SO(n)$ has numerous intermediate nonsplit, noncompact forms, $SO(p,q)$ – isometries of $x_1^2+\cdots+x_p^2-x_{p+1}^2-\cdots-x_{p+q}^2$, $q=n-p$. Here is another type of construction.

To start, let Q_0 be a nondegenerate quadratic form over a field k in $n-2q$ variables. We assume that Q_0 does not represent 0 (i.e., it takes nonzero values on nonzero inputs. A good example of this is the diagonal form $x_1^2+\cdots+x_{n-2q}^2$ over $\mathbb{R}$ or $\mathbb{Q}$. Let $SO(Q_0)$ be the algebraic group defined over k which is the stabilizer of this form in $SL(n-2q)$. Also, assume $\operatorname{char} k \neq 2$ (often made for quadratic forms).

Lemma $SO(Q_0)$ is anisotropic over k

(obvious for our example over $\mathbb{R}$, since it is then compact).

Converse is easy: if $Q_0(v)=0$, we can scale v to preserve Q_0 by a split, one-dimensional torus.

Sketch of Proof An earlier result says a k-torus is the almost-direct product of a k-split torus & an anisotropic torus (over k). If the lemma is false, then there exists a k-split torus $S \subseteq G$, which by earlier results we can assume is diagonal. So there exists a vector $v \neq 0$ such that for all $s \in S$

$$sv = \chi(s) v \quad , \text{ for some character } \chi \text{ of } S.$$

Since the character group of S is a free abelian group, χ^2 is nontrivial (unless S is trivial).

Since $s \in SO(Q_0)$, $Q_0(sv) = Q_0(v)$

$$\underset{Q_0(\chi(s)v) = \chi(s)^2 Q_0(v).}{\overset{Q_0(sv)}{\shortparallel}}$$

This implies that $Q_0(v)$ vanishes. $\square$

Let $Q(x_1, \dots, x_n) = x_1 x_n + x_2 x_{n-1} + \dots + x_q x_{n-q+1} + Q_0(x_{q+1}, \dots, x_{n-q})$

Remarks: 1) If $q = n$, this is our split $SO(n)$ from before.

2) The most general nondegenerate quadratic form over k can be transformed into this form using a change of basis. Recall $\mathrm{char}(k) \neq 2$.

We study $G = SO(Q)$ now. Its maximal k-split torus is

$$S = \left\{ \begin{pmatrix} s_1 & & & & & & \\ & \ddots & & & & & \\ & & s_q & & & & \\ & & & I_{n-2q} & & & \\ & & & & s_q^{-1} & & \\ & & & & & \ddots & \\ & & & & & & s_1^{-1} \end{pmatrix} \right\},$$

where the map $\lambda_i : s \mapsto s_i$ is a character (& all characters of S have the form $s_1^{n_1} \cdots s_q^{n_q}$, for some $n_i \in \mathbb{Z}$). Its maximality follows from earlier arguments for the nonsplit $SO(n)$, using the fact $SO(F_0)$ — which sits in the middle $n-2q$ block — is anisotropic. In fact, this logic shows that

$$Z(S) = S \times SO(F_0).$$

Thus it splits if & only if $q = \lfloor n/2 \rfloor$.

It has the following minimal k-parabolic

$$P = \left\{ \begin{pmatrix} A_0 & A_1 & A_2 \\ 0 & B & A_3 \\ 0 & 0 & A_4 \end{pmatrix} \;\middle|\; \begin{array}{l} A_0, A_4 \text{ upper triangular,} \\ B \in SO(F_0) \end{array} \right\}$$

The unipotent radical of P is its subgroup defined by A_0 & A_4 unipotent, & $B = I$.

Let us now analyze the root spaces. The matrix positions corresponding to A_0, A_2, & A_4 decompose into one-dimensional root spaces for

$$\begin{array}{lll} & \lambda_i - \lambda_j, & 1 \le i < j \le q \\ \text{and} & \lambda_i + \lambda_j, & 1 \le i, j \le q \end{array} \quad (\text{multiplicity } 1).$$

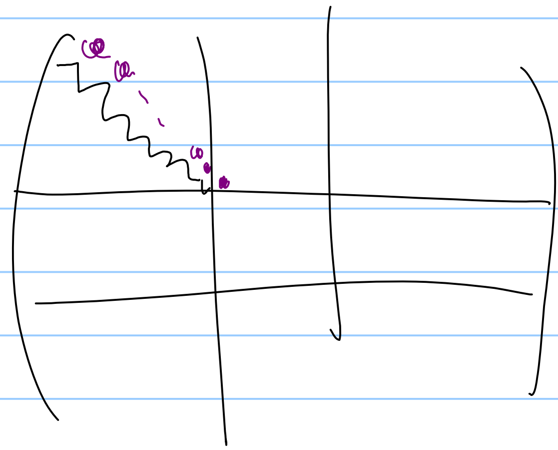
In addition, positions A_1 & A_3 give

$$\lambda_i, \quad 1 \le i \le q \quad \text{w/ multiplicity } n-2q,$$

In particular, this is a good example of where $\dim \mathfrak{g}_\alpha > 1$.

The simple roots are

$$\lambda_1 - \lambda_2,\ \lambda_2 - \lambda_3,\ \cdots,\ \lambda_{q-1} - \lambda_q,\ \begin{cases} \lambda_q & \text{if } n \neq 2q \\ \lambda_{q-1} + \lambda_q, & n = 2q,\ (\text{Split } SO(n)) \end{cases}$$



This is the D_q root system when $n = 2q$, but the B_q root system if $n > 2q$. A Hermitian variant is BC_q.

So the root system corresponds more uniquely to the group (i.e., $\dim \mathfrak{g}_\alpha$ closer to 1) when it is split.

Lecture 7: Dynkin diagrams

In this lecture we explain the importance of the ambient geometry of the root system. Ultimately this stems from the examples of $GL(n)$ & $SL(n)$, so we start there.

__Definition__ The Bilinear form

$$B(X,Y) = tr(XY)$$

on $\mathfrak{gl}(n) \times \mathfrak{gl}(n)$ is called the Killing form.

The basic idea is that all algebraic matrix groups embed into some $GL(n)$, & obtain a Killing form by restriction. However, it is most interesting for reductive groups. For example, consider the algebraic group $\mathbb{G}_a$ as the unipotent upper triangular subgroup of $SL(2)$. Then the restriction of the Killing form to its Lie algebra is trivial:

$$\mathrm{tr}\left(\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & y \\ 0 & 0 \end{pmatrix}\right) = 0.$$

The restriction of the Killing form to diagonal matrices is, however nondegenerate. This gives an inner product on the root spaces. Let us take $n=3$ & $G = SL(3)$ to be more concrete. Recall that

$$S = \left\{ \begin{pmatrix} a_1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & a_3 \end{pmatrix} \middle| \, a_1 a_2 a_3 \right\} \text{ is a maximal torus}$$

& its Lie algebra is the additive algebraic group

$$\mathrm{Lie}(S) = \left\{ \begin{pmatrix} h_1 & 0 & 0 \\ 0 & h_2 & 0 \\ 0 & 0 & h_3 \end{pmatrix} \middle| \, h_1 + h_2 + h_3 = 0 \right\}.$$

We endow S w/ the inner product given by the Killing form. This makes its dual isometric with it (at least the real points), & so the roots α have dual coroots $\alpha^\vee \in H$:

For each root α, $\exists\, \alpha^\vee \in \mathrm{Lie}(S)$ s.t.

$$\alpha(H) = \langle \alpha^\vee, H \rangle = B(\alpha^\vee, H) \text{ for all } H \in \mathrm{Lie}(S).$$

The inner product is Weyl-group invariant.
This is one way to understand the specific

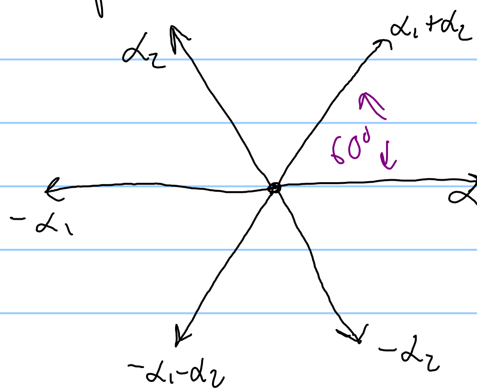
geometry that is involved in the root system.
Here is a table for $\mathfrak{sl}(3)$:

	$\alpha\begin{pmatrix} h_1 & 0 & 0 \\ 0 & h_2 & 0 \\ 0 & 0 & h_3 \end{pmatrix}$	$\alpha^\vee$
α_1	$h_1 - h_2$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$
α_2	$h_2 - h_3$	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$
$\alpha_1+\alpha_2$	$h_1 - h_3$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$
$-\alpha_1$	$h_2 - h_1$	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$
$-\alpha_2$	$h_3 - h_2$	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
$-\alpha_1-\alpha_2$	$h_3 - h_1$	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Inner products: each $\langle \alpha_i, \alpha_i^\vee \rangle = 2$

$\langle \alpha_1, \alpha_2 \rangle = -1$ etc....

So this explains the 60° angle picture described earlier:



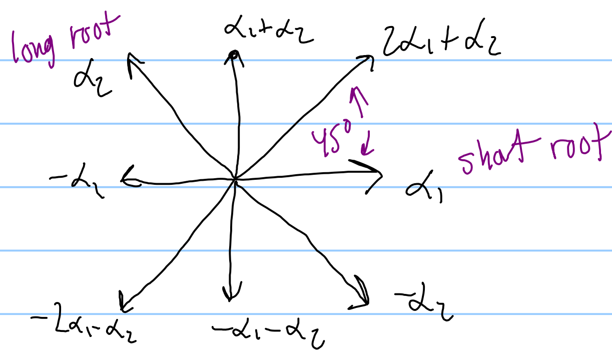
Next we will explain the $Sp(4)$ picture from before.
Here are the roots & coroots:

$\alpha \begin{pmatrix} h_1 & 0 & 0 & 0 \\ 0 & h_2 & 0 & 0 \\ 0 & 0 & -h_2 & 0 \\ 0 & 0 & 0 & -h_1 \end{pmatrix}$	$\alpha^\vee$
$\alpha_1 = h_1 - h_2$	$\frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$
$\alpha_2 = 2h_2$	$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$
$\alpha_1 + \alpha_2 = h_1 + h_2$	$\frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$
$2\alpha_1 + \alpha_2 = 2h_1$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$

$\langle \alpha_1^\vee, \alpha_1^\vee \rangle = 1$

$\langle \alpha_1, \alpha_2 \rangle = -1$

$\langle \alpha_2, \alpha_2 \rangle = 2$



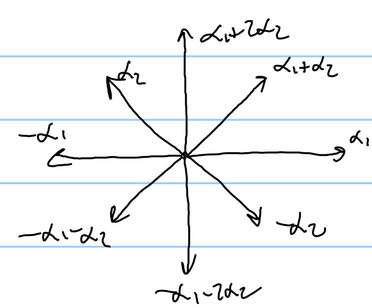
For $SO(5)$:

	$\alpha \begin{pmatrix} h_1 & & & & \\ & h_2 & & & \\ & & 0 & & \\ & & & -h_2 & \\ & & & & -h_1 \end{pmatrix}$	$\alpha^\vee$
α_1	$h_1 - h_2$	$\frac{1}{2}\begin{pmatrix} 1 & & & & \\ & -1 & & & \\ & & 0 & & \\ & & & 1 & \\ & & & & -1 \end{pmatrix}$
α_2	h_2	$\frac{1}{2}\begin{pmatrix} 0 & & & & \\ & 1 & & & \\ & & 0 & & \\ & & & -1 & \\ & & & & 0 \end{pmatrix}$
$\alpha_1 + \alpha_2$	h_1	$\frac{1}{2}\begin{pmatrix} 1 & & & & \\ & 0 & & & \\ & & 0 & & \\ & & & 0 & \\ & & & & -1 \end{pmatrix}$
$\alpha_1 + 2\alpha_2$	$h_1 + h_2$	$\frac{1}{2}\begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & 0 & & \\ & & & -1 & \\ & & & & -1 \end{pmatrix}$

$\langle \alpha_1^\vee, \alpha_1^\vee \rangle = 1$

$\langle \alpha_2^\vee, \alpha_2^\vee \rangle = \frac{1}{2}$

$\langle \alpha_1^\vee, \alpha_2^\vee \rangle = -1/2$



A fundamental role is played by the reflection about a simple root in a root system:

$$S_\alpha(v) = v - 2\frac{\langle v,\alpha\rangle}{\langle \alpha,\alpha\rangle}\alpha.$$

Since $s_\alpha(v)$ leaves the root system invariant,

$$S_\alpha(\beta) = \beta - \alpha\boxed{\frac{2\langle \beta,\alpha\rangle}{\langle\alpha,\alpha\rangle}}$$

by definition, this "Cartan integer $n_{\beta\alpha}$" is an integer (part 4) in the root system definition).

<u>Fundamental Integrality Theorem for Reduced Root Systems:</u>

$$n_{\beta,\alpha} = \frac{2\langle\beta,\alpha\rangle}{\langle\alpha,\alpha\rangle} \in \{-3,-2,-1,0,1,2,3\}$$

(We have seen all these possibilities indeed do occur.)

<u>Pf</u> Cauchy-Schwartz says

$$n_{\alpha,\beta}\, n_{\beta,\alpha} = \frac{4\langle\alpha,\beta\rangle^2}{\langle\alpha,\alpha\rangle\langle\beta,\beta\rangle}$$

is bounded by 4 in absolute value. Hence these integers are bounded by 4 in absolute value. If it is exactly 4 α & β are colinear, & $\alpha = \pm\beta$ (since we are assuming it is reduced). Thus $n_{\beta,\alpha}$ cannot equal 4. $\square$

In any root system, choosing a vector in general position in the ambient vector space gives a notion of positive & negative roots (as long as none of the roots are orthogonal to this vector). Among the positive roots, let Σ^+ denote the subset of those which are not nontrivial combinations of positive roots that has coefficients in $\mathbb{Z}_{\geq 0}$. These are called positive simple roots, a crucial notion due to E. Dynkin. Their ~~negatives are~~ negatives are negative simple roots

Lemma 1. Every positive root is a sum of elements of Σ^+ w/ $\mathbb{Z}_{\geq 0}$ coefficients.

Pf By definition, either a vector lies in Σ^+, or else ~~it~~ it is the sum of 2 positive roots. The same can be said of these 2 vectors. Repeating — & using the ~~fact that there~~ only a finite number of roots — we see that every root is an integral combination of the elements in Σ^+, with coefficients in $\mathbb{Z}_{\geq 0}$. $\square$

Suppose that $\langle\alpha,\beta\rangle > 0$, which is of course equivalent to the positivity of $n_{\beta\alpha}$ & $n_{\alpha\beta}$. We saw above that if α & β are not colinear, then one of these must be 1. If $n_{\beta\alpha} = 1$, then

$$S_\alpha(\beta) = \beta - \frac{2\langle\alpha,\beta\rangle}{\langle\alpha,\alpha\rangle}\alpha = \beta - \alpha,$$

so both $\alpha - \beta$ & $\beta - \alpha$ are roots.

Lemma 2 If $\alpha, \beta \in \Sigma^+$, then $\langle \alpha, \beta \rangle \leq 0$ unless $\alpha = \beta$.

Proof: Otherwise $\alpha - \beta$ & $\beta - \alpha$ are roots. One of these is positive, say $\alpha - \beta$ without loss of generality. Then $\alpha = (\alpha - \beta) + \beta$ is a sum of 2 positive roots, contradicting the simplicity of α. $\square$

$\square$

Lemma 3 Σ^+ is a basis of the root space.

Proof: In view of lemma 1, it suffices to show linear independence. Suppose $\sum_{\alpha \in \Sigma^+} c_\alpha \alpha = 0$. Separating the positive & negative coefficients, it suffices to rule out the existence of a vector v which can be written 2 separate ways as a positive (real) combination of disjoint subsets of simple roots:

$$v = \sum_{\alpha \in S} c_\alpha \alpha = \sum_{\alpha \in T} d_\alpha \alpha, \quad S \cap T = \emptyset.$$

The norm^2 of this vector is

$$\langle v, v\rangle = \langle \sum_S c_\alpha \alpha, \sum_T d_\beta \beta\rangle$$

$$= \sum c_\alpha d_\beta \langle \alpha, \beta\rangle,$$

which is ≤ 0 since $c_\alpha, d_\beta > 0$ & $\langle \alpha, \beta\rangle \leq 0$. Hence $\|v\| = 0$ & $v = 0$. $\square$

Lemma 4 No root can be written as a linear combination of simple roots with mixed signs.

Proof Lemma 1 shows each root has at least one expression, & Lemma 3 shows it is unique. $\square$

Definition The Dynkin diagram of a root system is the directed multigraph on its simple positive roots which has $n_{\alpha,\beta} n_{\beta,\alpha}$ lines between α & β, & an arrow from the larger root to the smaller root if their lengths differ.

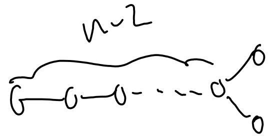
We have not yet demonstrated this is independent of our choice of "positive." Here is the famous classification of irreducible, reduced root systems,

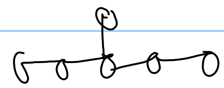
Theorem. Every Dynkin diagram is of the form

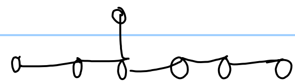
A_n $\quad \overbrace{\circ - \circ - \circ - \cdots - \circ - \circ}^{n}$, $n \geq 1$,

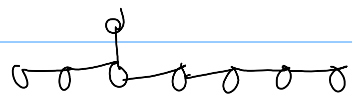
B_n $\quad \overbrace{\circ - \circ - \circ - \cdots - \circ - \circ \Rightarrow \circ}^{n}$, $n \geq 2$,

C_n $\quad \overbrace{\circ - \circ - \circ \cdots\cdots - \circ - \circ \Leftarrow \circ}^{n}$, $n \geq 3$ $\quad (C_2 = B_2)$,

D_n  , $n \geq 4$ $(C_3 = A_3)$,

E_6  ,

E_7  ,

E_8  ,

F_4  ,

or

G_2  .

Remarks 1) Arrows occur exactly when there are multiple lines. This is because

$$n_{\alpha,\beta} = n_{\beta,\alpha} \iff \frac{2\langle\alpha,\beta\rangle}{\langle\alpha,\alpha\rangle} = \frac{2\langle\alpha,\beta\rangle}{\langle\beta,\beta\rangle}$$

$$\Updownarrow$$

$$\|\alpha\| = \|\beta\|,$$

& $n_{\alpha,\beta} = n_{\beta,\alpha}$ forces these integers to be < 2 in absolute value (or else the product $n_{\alpha\beta} n_{\beta\alpha}$ is illegally > 3).

2) If S is a subset of Σ^+, the roots in its span constitute a root system (all axioms are immediately satisfied).

3) We have constructed A_n, B_n, C_n, D_n, & will later describe the "exceptional" E_6, E_7, E_8, F_4, & G_2.

[See Barry Simon's book, pp. 187–189: All we use is the roots' $\mathbb{R}$-span is the whole ambient vectorspace, & the $n_{\alpha,\beta} \in \mathbb{Z}_{\le 0}$ satisfy $n_{\alpha\beta} n_{\beta\alpha} \le 3$]

Proof that the list is complete: Perhaps the most striking feature is that none of them have loops. If one did, it would mean roots

$$\alpha_1, \cdots, \alpha_m \quad \text{with} \quad n_{\alpha_1\alpha_2}, n_{\alpha_2\alpha_3}, \cdots, n_{\alpha_{m-1}\alpha_m}, \text{ and } n_{\alpha_m,\alpha_1} \le -1.$$

Hence

$$\langle \alpha_j, \alpha_{j+1} \rangle \le -\frac{\|\alpha_j\|^2}{2} \;\&\; -\frac{\|\alpha_{j+1}\|^2}{2}$$

$$\langle \alpha_1, \alpha_m \rangle \le -\frac{\|\alpha_1\|^2}{2} \;\&\; -\frac{\|\alpha_m\|^2}{2}.$$

In particular, each is bounded by the means of the objects on the right: $\langle \alpha_j, \alpha_{j+1 (\mathrm{mod}\, m)} \rangle \le -\frac{1}{4}\|\alpha_j\|^2 - \frac{1}{4}\|\alpha_{j+1(\mathrm{mod}\, m)}\|^2$.

So their sum is $\le -\frac{1}{2}\sum_{j\le m}\|\alpha_j\|^2$.

Now we consider the norm-squared of $\alpha_1 + \cdots + \alpha_m$:

$$\|\alpha_1 + \cdots + \alpha_m\|^2 = \sum_{j=1}^m \|\alpha_j\|^2 + 2\sum_{j=1}^m \langle \alpha_j, \alpha_{j+1(\mathrm{mod}\, m)}\rangle + \text{other } \langle \alpha_i, \alpha_j \rangle, \text{ which are always } \le 0$$

$$\le 0$$

$\Rightarrow \alpha_1 + \cdots + \alpha_m = 0$, a contradiction since Σ^+ is a linearly independent set. This proves the Dynkin diagram is indeed contractible.

Next, suppose α_0 has neighbors $\alpha_1, \cdots, \alpha_m$, which $\ell_1, \cdots, \ell_m$ lines, respectively from α_0. We have that

$$\ell_j = n_{\alpha_0,\alpha_j} n_{\alpha_j,\alpha_0} = \frac{4\langle \alpha_0,\alpha_j\rangle^2}{\|\alpha_0\|^2\|\alpha_j\|^2}.$$

There are no loops, so none of the $\alpha_1,\cdots,\alpha_m$ are directly linked to each other; that is, $\langle \alpha_i,\alpha_j\rangle = 0$ for $i\neq j$. Using Parseval for this orthogonal set

$$\|\alpha_0\|^2 > \sum_{j=1}^m \frac{\langle \alpha_0,\alpha_j\rangle^2}{\|\alpha_j\|^2} = \sum_{j=1}^m \frac{\|\alpha_0\|^2 \ell_j}{4}.$$

strict, because α_0 is not in the span of $\alpha_1,\cdots,\alpha_m$.

Hence $\sum \ell_j < 4$, & thus it is ≤ 3 since it is a nonnegative integer. So at most 3 lines come out of any vertex in the Dynkin diagram. G_2 is the unique one w/ a triple bond.

We have one more main ingredient, that single bonds can be "fused" $\Rightarrow$ if the 2 nodes are identified & the bond removed, it is still a Dynkin diagram. Indeed, this reflects the following transformation of root systems: take 2 simple roots α & β w/ $\langle\alpha,\beta\rangle = -\|\alpha\|^2/2 = -\|\beta\|^2/2$, & replace them by $\gamma = \alpha+\beta$. Of course we replace the ambient vector space by the $\mathbb{R}$-span of γ & the other roots. We compute

$$\|\gamma\|^2 = \|\alpha\|^2 + \|\beta\|^2 + 2\langle\alpha,\beta\rangle = \|\alpha\|^2 = \|\beta\|^2$$

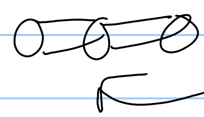
& if δ is any othe simple root, then

$$\langle\gamma,\delta\rangle = \langle\alpha,\delta\rangle + \langle\beta,\delta\rangle.$$

Recall we are working w/ Simon's weaker setup.

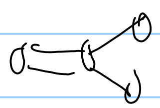
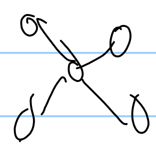
Since there are no loops, δ cannot be a neighbor of both α & β, so one of $\langle\alpha,\delta\rangle$, $\langle\beta,\delta\rangle$ vanishes, & $\langle\gamma,\delta\rangle$ equals the other. This means that for δ next to α in the original Dynkin diagram, $n_{\alpha,\delta} = n_{\gamma,\delta}$ & $n_{\delta,\alpha} = n_{\delta,\gamma}$. So the new Dynkin diagram indeed has the bond between α & β removed, & the 2 nodes fused (as claimed).

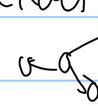
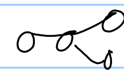
We cannot have a subconfiguration



since this has degree 4.

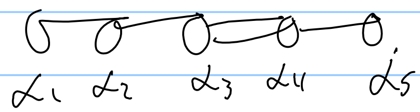
Hence if there are 2 $\circ\!=\!\circ$'s in the diagram, they are separated by single bonds. But removing those as in the last step returns us to the forbidden $\circ\!=\!\circ\!=\!\circ$ configuration. So there is at most one double bond. Likewise, since

 &  are forbidden subconfigurations

due to having valence 4, the exact same argument says we cannot have 2 's or both a $\circ\!=\!\circ$ & a .

Thus all diagrams are contractible, w/ few trivalent vertices (satisfying these constraints).

Next we show a double bond can only be in the middle of F_4. Indeed, suppose there is a subconfiguration of the form



This means $\|\alpha_1\| = \|\alpha_2\| = \|\alpha_3\|$, & $\|\alpha_4\| = \|\alpha_5\|$,
Also

$$\frac{2\langle \alpha_1, \alpha_2\rangle}{\|\alpha_1\|^2} = -1 \Rightarrow \langle \alpha_1, \alpha_2\rangle = -\frac{\|\alpha_1\|^2}{2}.$$

Likewise $\langle \alpha_2, \alpha_3\rangle = -\|\alpha_1\|^2/2$,

& $\langle \alpha_4, \alpha_5\rangle = -\|\alpha_4\|^2/2$,

Consider the following 3 inner products:

$$\langle \alpha_1 + 2\alpha_2 + 3\alpha_3, \alpha_1 + 2\alpha_2 + 3\alpha_3\rangle$$
$$= \|\alpha_1\|^2 + 4\|\alpha_2\|^2 + 9\|\alpha_3\|^2 + 4\langle \alpha_1, \alpha_2\rangle + 6\langle \alpha_1, \alpha_3\rangle + 12\langle \alpha_2, \alpha_3\rangle$$
$$= 14\|\alpha_1\|^2 - 8\|\alpha_1\|^2 = 6\|\alpha_1\|^2,$$

$$\langle 2\alpha_4 + \alpha_5, 2\alpha_4 + \alpha_5\rangle = 4\|\alpha_4\|^2 + \|\alpha_5\|^2 + 4\langle \alpha_4, \alpha_5\rangle$$
$$= 5\|\alpha_4\|^2 - 2\|\alpha_4\|^2 = 3\|\alpha_4\|^2,$$

and

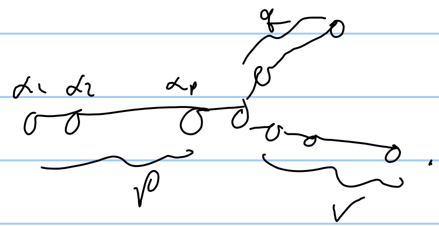
$$\langle \alpha_1 + 2\alpha_2 + 3\alpha_3, 2\alpha_4 + \alpha_5\rangle$$
$$= 2\langle \alpha_1, \alpha_4\rangle + \langle \alpha_1, \alpha_5\rangle + 4\langle \alpha_2, \alpha_4\rangle + 2\langle \alpha_2, \alpha_5\rangle + 6\langle \alpha_3, \alpha_4\rangle + 3\langle \alpha_3, \alpha_5\rangle$$
$$= 6\langle \alpha_3, \alpha_4\rangle$$
$$= 3\sqrt{\frac{4\langle \alpha_3, \alpha_4\rangle^2}{\|\alpha_3\|^2\|\alpha_4\|^2}}\,\|\alpha_3\|\,\|\alpha_4\|$$
$$= 3\sqrt{n_{\alpha,\beta}\, n_{\beta,\alpha}}\,\|\alpha_3\|\,\|\alpha_4\| = 3\sqrt{2}\,\|\alpha_3\|\,\|\alpha_4\|$$

Since the square of the latter $= (8\|\alpha_3\|^2\|\alpha_4\|^2$ is the product of the first 2, we see that

$\alpha_1 + 2\alpha_2 + 3\alpha_3$ & $2\alpha_4 + \alpha_5$ are colinear,

violating the linear independence of Σ^+.

So a double bond must occur at the end.
Now we consider a subdiagram of the form

$T_{p,q,r}$ 

Let $\alpha_0 =$ central node, & let

$V_p = \alpha_1 + 2\alpha_2 + \cdots + p\alpha_p$

V_q, V_r analogously for other legs.
We must have that V_p, V_q & V_r are mutually perpendicular. We compute

$$\langle V_p, V_p\rangle = \sum_{j=1}^{p} j^2\|\alpha_j\|^2 + \sum_{j=1}^{p-1} 2j(j+1)\langle\alpha_j, \alpha_{j+1}\rangle \quad (\text{others} = 0)$$

$$= \|\alpha_1\|^2\left(\sum_{j=1}^{p} j^2 - \sum_{j=1}^{p-1} j(j+1)\right)$$

since each have same length, & the inner products $= -\|\alpha_1\|^2/2$.

$$= \|\alpha_1\|^2\left(p^2 - \sum_{j=1}^{p-1} j\right)$$

$$= \|\alpha_1\|^2\left(p^2 - \frac{p(p-1)}{2}\right) = \|\alpha_1\|^2\left(\frac{p^2+p}{2}\right) = \frac{1}{2}\|\alpha_1\|^2 p(p+1).$$

Meanwhile, $\langle v_p, \alpha_0 \rangle = p \langle \alpha_p, \alpha_0 \rangle = -p\frac{\|\alpha_p\|^2}{2} = -p\|\alpha_1\|^2/2$,
Using Parseval again for the projection of α_0 onto the span of the orthogonal vectors v_p, v_q, & v_r (which does not contain α_0, so that there is strict inequality)

$$\|\alpha_0\|^2 \geq \frac{\langle \alpha_0, v_p\rangle^2}{\|v_p\|^2} + \frac{\langle \alpha_0, v_q\rangle^2}{\|v_q\|^2} + \frac{\langle \alpha_0, v_r\rangle^2}{\|v_r\|^2}$$

$$= \frac{p^2\|\alpha_1\|^4}{4\frac{1}{2}\|\alpha_1\|^2 p(p+1)} + \text{similar}$$

since $\|\alpha_1\| = \|\alpha_0\|$

$$= \|\alpha_0\|^2 \left[\frac{p}{2(p+1)} + \frac{q}{2(q+1)} + \frac{r}{2(r+1)}\right]$$

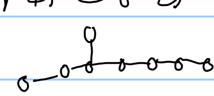
$$\Longrightarrow \quad \frac{p}{p+1} + \frac{q}{q+1} + \frac{r}{r+1} < 2,$$

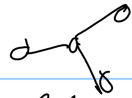
It is clear there are only finitely many sol'ns since $n/n+1 \to 1$ as $n \to \infty$. Rewriting $\frac{x}{x+1} = 1 - \frac{1}{x+1}$, this is equivalent to

$$\frac{1}{p+1} + \frac{1}{q+1} + \frac{1}{r+1} > 1.$$

If $p=1$: $\frac{1}{q+1} + \frac{1}{r+1} > \frac{1}{2}$. Since $q \leq r$, $\frac{1}{q+1} \geq \frac{1}{r+1}$ & $\frac{2}{q+1} > \frac{1}{2} \Rightarrow q+1 < 4$
$\Rightarrow q \leq 2$

The case $q=1$ is allowed (D_n series),
If $q=2$, $\frac{1}{r+1} > \frac{1}{2} - \frac{1}{3} = \frac{1}{6}$ & $r+1 < 6 \Rightarrow r \leq 4$


Gives $E_6, E_7, \& E_8$.

If $p > 1$, $\frac{1}{p+1} \leq \frac{1}{3}$, & $\frac{1}{q+1} + \frac{1}{r+1} > 2/3 \Longrightarrow \frac{2}{q+1} > 2/3 \Rightarrow \underset{\substack{\shortparallel \\ p}}{2} \leq q < 2$, impossible, Thus we get that  is either in the D_n or E_n series. This completes the argument $\square$

Remark: the $\frac{1}{p+1} + \frac{1}{q+1} + \frac{1}{r+1}$ calculation appears many places in geometric group theory.

We did not show that the Dynkin diagram is independent of our choice of positive root system. This can be shown, but the fact that the root system is independent of the choice of maximal torus can be used as a substitute as far as applications to classifying Lie algebras go.

Lecture 8: Serre relations for complex Lie algebras

Let us now withdraw to the easier world of complex Lie algebras. We begin by recalling the notions of simple & semisimple Lie algebras, the latter of which were classified by Cartan & Killing over $\mathbb{C}$. We describe a neat presentation of these Lie algebras due to J.-P. Serre in terms of the Cartan matrix of the Lie algebra, which encodes its Dynkin diagram. We conclude with a discussion of the classification of the real forms of these semisimple Lie algebras, which thereby gives a classification of semisimple real Lie algebras.

Let us now list some terminology for structures of Lie algebras that are analogous to ones we have already seen for algebraic groups. We will work over an arbitrary field of characteristic 0. We also look only at finite-dimensional ones. An ideal by definition contains the Lie bracket of anything with a member of it.

A Lie algebra $\mathfrak{g}$ is said to be <u>nilpotent</u> if the chain of ideals $\mathfrak{g}, [\mathfrak{g},\mathfrak{g}], [\mathfrak{g},[\mathfrak{g},\mathfrak{g}]], [\mathfrak{g},[\mathfrak{g},[\mathfrak{g},\mathfrak{g}]]], \ldots$ eventually terminates to $\{0\}$ in a finite number of steps. This sequence is called the "lower central series" of $\mathfrak{g}$. The Lie algebra $\mathfrak{g}$ is said to be solvable if its "derived series"

$$\mathfrak{g}, [\mathfrak{g},\mathfrak{g}], [[\mathfrak{g},\mathfrak{g}],[\mathfrak{g},\mathfrak{g}]], [[[\mathfrak{g},\mathfrak{g}],[\mathfrak{g},\mathfrak{g}]], [[\mathfrak{g},\mathfrak{g}],[\mathfrak{g},\mathfrak{g}]]], \ldots$$

eventually terminates to $\{0\}$ in a finite number of steps. Nilpotent in fact implies solvable, but not vice versa.

The radical $\mathfrak{r}$ of $\mathfrak{g}$ is its largest solvable ideal, & $\mathfrak{g}$ is semisimple if this is $\{0\}$. For example, $\mathfrak{sl}(n)$ is semisimple. The quotient $\mathfrak{g}/\mathfrak{r}$ is always semisimple & $\mathfrak{g}$ is always a semidirect product of a semisimple Lie algebra & a solvable ideal. This is known as a Levi decomposition.

<u>Cartan-Killing Theorem</u> $\mathfrak{g}$ is semisimple if & only if its Killing form is nondegenerate.

A Lie algebra is <u>simple</u> if it is not abelian & has no proper ideals. The semisimple Lie algebras are precisely the products of simple Lie algebras.

For example, $[\mathfrak{g},\mathfrak{g}]=\mathfrak{g}$ if $\mathfrak{g}$ is simple, & hence if it is semisimple too.

Over $k=\mathbb{C}$, the complex simple Lie algebras are precisely the A_n, B_n, C_n, D_n, E_n ($n=6,7,8$), F_4, & G_2 Lie algebras. All semisimple ones are products of these

Over $k=\mathbb{R}$, if $\mathfrak{g}$ is a Lie algebra, $\mathfrak{g}\otimes_{\mathbb{R}}\mathbb{C}$ is then classified above, so $\mathfrak{g}$ is a real form of one of these families (by defn, one which equals it after tensoring w/ $\mathbb{C}$). However, simplicity itself is a little more complicated: a real Lie algebra is simple if & only if its complexification is either simple, or of the form $\mathfrak{s}\times\bar{\mathfrak{s}}$, $\mathfrak{s}$ simple & $\bar{\mathfrak{s}}$ related by conjugation.

We will now describe how to create one of these simple complex Lie algebras from its Dynkin diagram, passing through its Cartan matrix and root system. We work with connected Dynkin diagrams, which correspond to reduced root systems & simple Lie algebras.

Dynkin Diagram to Cartan matrix (Easy)

The Cartan integers were defined above when we introduced the notion of root system, as

$$n_{\beta\alpha} := \frac{2\langle\alpha,\beta\rangle}{\langle\alpha,\alpha\rangle}, \quad \alpha, \beta \text{ roots}$$

which are integral as part of the definition of root system.

The Cartan matrix for a root system in $\mathbb{R}^n$ is the $n \times n$ matrix of $n_{\beta\alpha}$ where α & β range over positive simple roots.

The Dynkin diagram has $n_{\alpha\beta} n_{\beta\alpha} = \frac{4\langle\alpha,\beta\rangle^2}{\|\alpha\|^2\|\beta\|^2}$ edges between 2 simple roots, & a directed arrow from the longer to shorter root.

We can reconstruct the lengths of simple roots from the Dynkin diagram as follows. We have already seen that a single line connects vectors of equal length. Thus all roots in the simply laced Dynkin diagrams have the same length, which is $\sqrt{2}$. Thus for $\alpha, \beta \in \Sigma^+$

$$n_{\alpha\beta} = n_{\beta\alpha} = \langle \alpha, \beta \rangle = \begin{cases} 2, & \alpha = \beta \\ -1, & \alpha \text{ connected to } \beta \text{ by an edge} \\ 0 & \text{otherwise.} \end{cases}$$

This handles A_n, D_n, & E_n's Cartan matrices.
A double line means

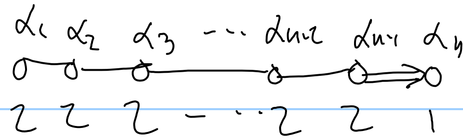
$$n_{\beta\alpha} = \frac{2\langle\alpha,\beta\rangle}{\|\alpha\|^2} = \pm 2 \quad \& \quad n_{\alpha\beta} = \frac{2\langle\alpha,\beta\rangle}{\|\beta\|^2} = \pm 1,$$

where $\|\beta\|$ must be the longer root, & in fact have

$$\|\beta\| = \sqrt{2}\,\|\alpha\| \quad \text{in order to get}$$

the correct ratio.

So for B_n

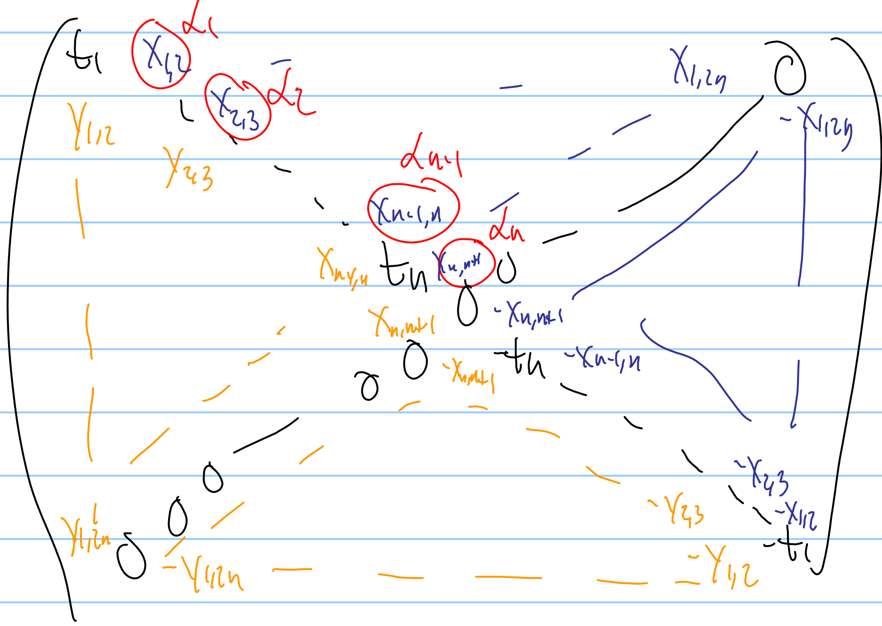


the lengths are

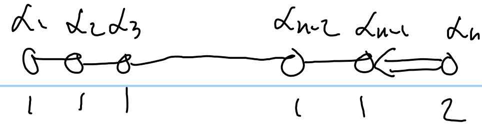
$$\|\alpha_i\| = \begin{cases} \sqrt{2}, & i<n \\ 1, & i=n \end{cases}$$

& $$\langle \alpha_i, \alpha_j \rangle = \begin{cases} -1, & |i-j|=1 \\ 0, & \text{otherwise} \end{cases}$$

We can check this with the explicit Matrix representation of B_n from the split $SO(2n+1)$, $SO(n+1,n)$



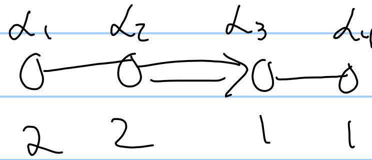
Recall $n=2$:
$$\begin{pmatrix} t_1 & X_1 & X_3 & X_4 & 0 \\ Y_1 & t_2 & X_2 & 0 & -X_4 \\ Y_3 & Y_2 & 0 & -X_2 & -X_3 \\ Y_4 & 0 & -Y_2 & -t_2 & -X_1 \\ 0 & -Y_4 & -Y_3 & -Y_1 & -t_1 \end{pmatrix}$$

For C_n 

, $|\alpha_i| = \begin{cases} \sqrt{2}, & i=n \\ 1, & i<n \end{cases}$

&

$$\langle \alpha_i, \beta \rangle = \begin{cases} -1/2, & |i-j| \;\&\; i,j<n \\ -1, & (i,j) = (n-1,n) \text{ or } (n,n-1) \\ 0, & \text{otherwise.} \end{cases}$$

For F_4 

The Cartan matrix is
$$\begin{bmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -2 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{bmatrix}$$

(i,j)-th entry is $n_{\alpha_i \alpha_j} = \dfrac{2\langle \alpha_i, \alpha_j \rangle}{\|\alpha_j\|^2}$

So the inner products are
$$(\langle \alpha_i, \alpha_j \rangle)_{ij} = \begin{bmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 1 & -1/2 \\ 0 & 0 & -1/2 & 1 \end{bmatrix}$$

The remaining example G_2  is the only one with a triple line. By the same logic the simple root lengths are $\sqrt{3}$ & 1

$\|\alpha_1\|^2 = 3$, $\|\alpha_2\| = 1$

$\langle \alpha_1, \alpha_2 \rangle = -3/2$

Cartan Matrix to Root system

First, we can easily find n explicit vectors in $\mathbb{R}^n$ whose inner products are those of our root system. To do this, let M = the symmetric matrix of inner products determined above, & diagonalize it by an orthogonal matrix Q:

$$M = Q^t D Q, \quad \text{with } D > 0 \text{ since } M \text{ is a matrix of inner products.}$$

Let $P = D^{1/2} Q$, so $M = P^t P$, & P's columns have the correct inner products.

Then reconstructing the root system amounts to determining which integral combinations of the simple roots are roots. The simple reflections (= reflections S_α for $\alpha \in \Sigma^+$) generate the Weyl group, & the Weyl group maps any root to some simple root. Thus we need only keep applying the simple Weyl reflections until we generate no more.

This is done efficiently by noting that for each $\alpha, \beta \in \Sigma^+$, $S_\alpha(\beta) = \beta - n_{\beta\alpha}\alpha$ is determined by the Cartan matrix (note how this takes place in a 2-dimensional root system). Then it is easy to work this out using Σ^+ as a basis.

Example G_2: We had $\langle \alpha_1, \alpha_1 \rangle = 3$
and $\langle \alpha_2, \alpha_2 \rangle = 1$,

so

$$n_{\alpha_1 \alpha_2} = \frac{2 \langle \alpha_1, \alpha_2 \rangle}{\langle \alpha_2, \alpha_2 \rangle} = -3$$

& $n_{\alpha_2 \alpha_1} = -1$.

Shorthand: $s_1 = s_{\alpha_1}$, $s_2 = s_{\alpha_2}$

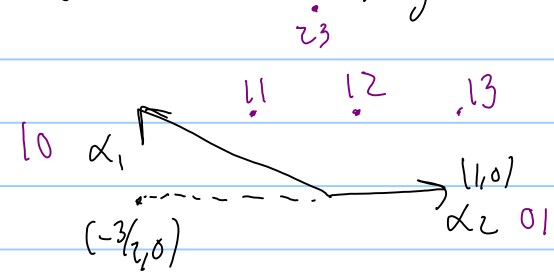
We start w/ 2 roots, 10 & 01, plus negatives. Then

$$s_1 \alpha_1 = -\alpha_1 \quad , \quad s_1 \alpha_2 = \alpha_1 + \alpha_2$$
$$s_2 \alpha_1 = \alpha_1 + 3\alpha_2 \quad , \quad s_2 \alpha_2 = -\alpha_2.$$

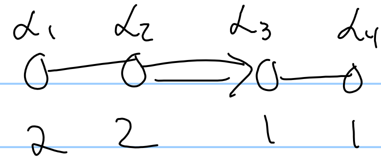
This gives us roots $13 = \alpha_1 + 3\alpha_2$ & $11 = \alpha_1 + \alpha_2$. Applying again,

$$s_1 13 = s_1 \alpha_1 + 3 s_1 \alpha_2 = -\alpha_1 + 3\alpha_1 + 3\alpha_2$$
$$= 2\alpha_1 + 3\alpha_2 =: 23$$
$$s_2 11 = s_2 \alpha_1 + s_2 \alpha_2 = \alpha_1 + 2\alpha_2 =: 12$$

In fact, these & their negatives give all roots:



Example F_4

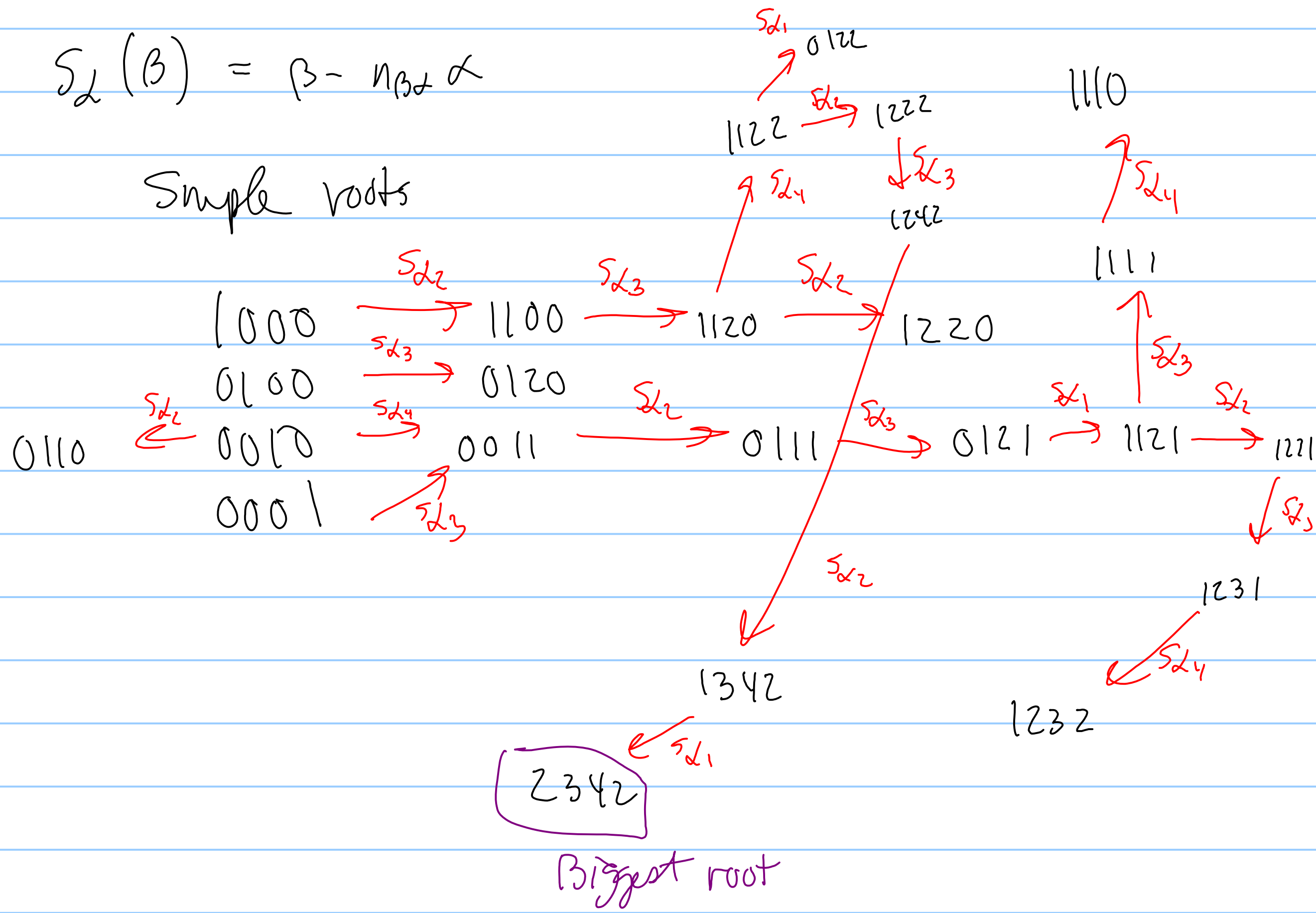


Cartan matrix

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

$$S_\alpha(\beta) = \beta - n_{\beta\alpha}\alpha$$

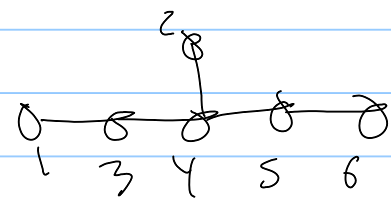
Simple roots



These are all 24 positive roots of F_4.

Example E_6, which is simply laced, so easier. Then $s_\alpha \beta = \beta$ if the nodes are not connected (after all, the sub-Dynkin diagram is like a product of 2 $SL(2)$'s, which commute)

Bourbaki numbering:



Write 6 simple roots as

$$\alpha_1 = 1\,0\,\overset{0}{0}\,0\,0 \xrightarrow{s_{\alpha_3}} 1\,1\,\overset{0}{0}\,0\,0 \xrightarrow{s_{\alpha_4}} 1\,1\,\overset{0}{1}\,0\,0 \xrightarrow{s_{\alpha_5}} 1\,1\,\overset{0}{1}\,1\,0 \xrightarrow{s_{\alpha_6}} 1\,1\,\overset{0}{1}\,1\,1$$

$$\alpha_3 = 0\,1\,\overset{0}{0}\,0\,0 \xrightarrow{s_{\alpha_4}} 0\,1\,\overset{0}{1}\,0\,0$$

$$\alpha_4 = 0\,0\,\overset{0}{1}\,0\,0$$

$$\alpha_5 = 0\,0\,\overset{0}{0}\,1\,0 \xrightarrow{s_{\alpha_4}} 0\,0\,\overset{0}{1}\,1\,0$$

$$\alpha_6 = 0\,0\,\overset{0}{0}\,0\,1 \xrightarrow{s_{\alpha_5}} 0\,0\,\overset{0}{0}\,1\,1 \xrightarrow{s_{\alpha_4}} 0\,0\,\overset{0}{1}\,1\,1 \xrightarrow{s_{\alpha_2}} 0\,0\,\overset{1}{1}\,1\,1$$

$$0\,0\,\overset{0}{1}\,1\,1 \xrightarrow{s_{\alpha_3}} 0\,1\,\overset{0}{1}\,1\,1$$

$$\alpha_2 = 0\,0\,\overset{1}{0}\,0\,0$$

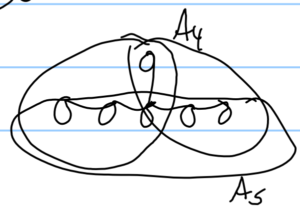
$$1\,1\,\overset{0}{1}\,0\,0 \xrightarrow{s_{\alpha_2}} 1\,1\,\overset{1}{1}\,0\,0 \xrightarrow{s_{\alpha_5}} 1\,1\,\overset{1}{1}\,1\,0 \xrightarrow{s_{\alpha_6}} 1\,1\,\overset{1}{1}\,1\,1 \xrightarrow{s_{\alpha_4}} 1\,1\,\overset{1}{2}\,1\,1$$

$$1\,1\,\overset{1}{2}\,1\,1 \xrightarrow{s_{\alpha_3}} 1\,2\,\overset{1}{2}\,1\,1 \qquad 1\,1\,\overset{1}{2}\,1\,1 \xrightarrow{s_{\alpha_5}} 1\,1\,\overset{1}{2}\,2\,1$$

$$1\,2\,\overset{1}{2}\,1\,1 \xrightarrow{s_{\alpha_5}} 1\,2\,\overset{1}{2}\,2\,1 \xrightarrow{s_{\alpha_4}} 1\,2\,\overset{1}{3}\,2\,1 \xrightarrow{s_{\alpha_2}} \boxed{1\,2\,\overset{2}{3}\,2\,1}$$

Biggest root
(others come by descent)

So far this is not a complete list. However, we can obviously get all roots for any Dynkin sub-diagram:



So the A_5 roots ($GL(6)$, will have 15 of these)

$$\begin{array}{ccc}
1\,0\,\overset{0}{0}\,0\,0 & 0\,1\,\overset{0}{0}\,0\,0 & 0\,0\,\overset{0}{1}\,1\,0 \\
1\,1\,\overset{0}{0}\,0\,0 & 0\,1\,\overset{0}{1}\,0\,0 & 0\,0\,\overset{0}{1}\,1\,1 \\
1\,1\,\overset{0}{1}\,0\,0 & 0\,1\,\overset{0}{1}\,1\,0 & 0\,0\,\overset{0}{0}\,1\,0 \\
1\,1\,\overset{0}{1}\,1\,0 & 0\,1\,\overset{0}{1}\,1\,1 & 0\,0\,\overset{0}{0}\,1\,1 \\
1\,1\,\overset{0}{1}\,1\,1 & 0\,0\,\overset{0}{1}\,0\,0 & 0\,0\,\overset{0}{0}\,0\,1
\end{array}$$

Embedded A_4's ($GL(5)$, has 10, but with overlap - omit common A_3)

$$\begin{array}{cc}
0\,0\,\overset{1}{0}\,0\,0 & \\
0\,0\,\overset{1}{1}\,0\,0 & \\
0\,1\,\overset{1}{1}\,0\,0 & 0\,0\,\overset{1}{1}\,1\,0 \\
1\,1\,\overset{1}{1}\,0\,0 & 0\,0\,\overset{1}{1}\,1\,1
\end{array}$$

$$0\,0\,\overset{1}{1}\,1\,0 \xrightarrow{s_{\alpha_3}} 0\,1\,\overset{1}{1}\,1\,0$$

From above, also $1\,1\,\overset{1}{1}\,1\,0$, $0\,1\,\overset{1}{1}\,1\,1$, & $1\,1\,\overset{1}{1}\,1\,1$

$$\begin{tikzcd}
& 1\,1\,\overset{1}{1}\,1\,0 \arrow[d, "s_{\alpha_4}"] & 0\,1\,\overset{1}{1}\,1\,1 \arrow[d, "s_{\alpha_4}"] & 1\,1\,\overset{1}{1}\,1\,1 \arrow[d, "s_{\alpha_4}"] & & 0\,1\,\overset{1}{1}\,1\,0 \arrow[d, "s_{\alpha_4}"] \\
& 1\,1\,\overset{1}{2}\,1\,0 \arrow[dl, "s_{\alpha_3}"] & 0\,1\,\overset{1}{2}\,1\,1 \arrow[d, "s_{\alpha_5}"] & 1\,1\,\overset{1}{2}\,1\,1 \arrow[d, "s_{\alpha_3}"] \arrow[dr, "s_{\alpha_5}"] & & 0\,1\,\overset{1}{2}\,1\,0 \\
1\,2\,\overset{1}{2}\,1\,0 & & 0\,1\,\overset{1}{2}\,2\,1 & 1\,2\,\overset{1}{2}\,1\,1 \arrow[d, "s_{\alpha_5}"] & 1\,1\,\overset{1}{2}\,2\,1 \arrow[dl, "s_{\alpha_3}"] & \\
& & & 1\,2\,\overset{1}{2}\,2\,1 \arrow[d, "s_{\alpha_4}"] & & \\
& & & 1\,2\,\overset{1}{3}\,2\,1 \arrow[r, "s_{\alpha_2}"] & 1\,2\,\overset{2}{3}\,2\,1 &
\end{tikzcd}$$

These are all 36.