Lecture 5-30: Root systems

May 30, 2025

In this last lecture I conclude my very brief (and rather idiosyncratic) treatment of linear algebraic groups by defining a purely combinatorial object that is used to classify a large number of the most important such groups. I will not give any proofs, only statements of results. Throughout the basefield k is algebraically closed and of characteristic 0.

I begin with an important characterization: a group G is linear algebraic if and only if it is a closed subgroup of $GL_n(k)$ for some n. This fact, which is not difficult to prove, justifies the adjective "linear" in the name of these groups. I mention that there are non-affine algebraic groups as well that do not embed in any general linear group; the most important of these are the elliptic curves, which live on projective varieties of dimension one.

An $n \times n$ matrix M is called unipotent if $M - I$ is nilpotent, so that $(M - I)^n = 0$. Thus the group U_n of upper triangular matrices with ones on the diagonal mentioned in the last lecture consists of unipotent matrices; accordingly, it too is called unipotent. In fact every subgroup of GL_n consisting of unipotent matrices is conjugate to a subgroup of U_n. Accordingly, every such subgroup is solvable as an abstract group; more generally, the solvable subgroups of GL_n are exactly those that are conjugate to a subgroup of B_n, the group of all upper triangular matrices. A linear algebraic group G is called reductive if it does not have any proper normal subgroup consisting of unipotent matrices. This last criterion makes sense because (as mentioned above) every linear algebraic group is isomorphic to a subgroup of GL_n; it turns out to be independent of the choice of isomorphism and even of the value of n.

Reductive algebraic groups over a fixed basefield k, unlike most objects in mathematics, can be completely classified; in fact the classification is discrete rather than continuous. It relies on the classification of certain kind of finite subset of the ordinary Euclidean space $\mathbb{R}^n$ called a *root system*. Such subsets arise in the context of reductive groups as follows. Any such group is generated by a maximal torus T together with finitely many subgroups isomorphic to the additive group G_a, each normalized by T. For example, if $G = GL_n(k)$, then the maximal torus can be taken to be group D_n of diagonal matrices, Here the subgroups correspond to the off-diagonal entries of the matrices in G; given indices i, j with $i \neq j$, the group of matrices in G equal to the identity apart from their ij-entries form a one-dimensional subgroup isomorphic to G_a. Conjugating an element of this group by a diagonal matrix, say with diagonal entries $d_1, \ldots, d_n$, multiplies its ij-entry by the scalar $d_i d_j^{-1}$.

Accordingly, the subset arising in this case consists of all differences $e_i - e_j$ of distinct unit coordinate vectors in $\mathbb{R}^n$. In general, a finite subset R of $\mathbb{R}^n$ is called a root system if

1. R spans $\mathbb{R}^n$;
2. If $v \in R$, then the only multiples of v in R are $\pm v$; in particular, $0 \notin R$;
3. If $\alpha, \beta \in R$ then $s_\alpha \beta = \beta - \frac{2(\beta,\alpha)}{(\alpha,\alpha)}\alpha$, the reflection of β by α, lies in R and $\frac{2(\beta,\alpha)}{(\alpha,\alpha)} \in \mathbb{Z}$; here (v, w) denotes the usual dot product of $v, w \in \mathbb{R}^n$.

The condition that $\frac{2(\beta,\alpha)}{(\alpha,\alpha)} \in \mathbb{Z}$ is called the crystallographic condition; it is easy to check that it limits the possible angles between any $\alpha, \beta \in R$ to integer multiples of $\pi/6$ or $\pi/4$. Here the linear transformation s_α is the reflection by α: it sends α to its negative while fixing any vector orthogonal to α. If $\alpha = e_i$, a unit coordinate vector, then the reflection s_α acts on $\mathbb{R}^n$ by changing the sign of the ith coordinate. If $\alpha = e_i - e_j$, then s_α flips the ith and jth coordinates; if $\alpha = e_i + e_j$, then s_α flips the ith and jth coordinates and changes both their signs.

A root system $R \subset \mathbb{R}^{n+m}$ is said to be irreducible if it is not the disjoint union of two subsystems R_1, R_2 living in $\mathbb{R}^n, \mathbb{R}^m$, respectively, embedding these last two spaces into $\mathbb{R}^{n+m}$ in the obvious way (so that in particular all roots in R_1 are orthogonal to all roots in R_2). Any root system is then the orthogonal union of irreducible subsystems, so that to classify the root systems it suffices to classify the irreducible ones. We identify any two root systems $R, R' \subset \mathbb{R}^n$ if there is some $M \in O_n(\mathbb{R})$ sending R onto R'.

It turns out that all irreducible root systems arise from the following construction. let L be a lattice in a real vector space V, that is, the $\mathbb{Z}$-span of an $\mathbb{R}$-basis of V. Then one takes the vectors of one or two specified square lengths in L (usually 2, or 1 and 2). Specifically, first let V be the hyperplane in $\mathbb{R}^n$ consisting of all vectors whose coordinates sum to 0 and let L be the intersection of $\mathbb{Z}^n$ and V. Taking vectors of square length 2, we get exactly the differences $e_i - e_j$ of distinct unit coordinate vectors e_i, e_j. Next let $V = \mathbb{R}^n, L = \mathbb{Z}^n$, and take all vectors of square length 1 or 2 in L; this yields the vectors $\pm e_i$ and $\pm e_i \pm e_j$ for $i \neq j$. Next, in a small variation of the previous construction, replace the vectors $\pm e_i$ in the previous root system by $\pm 2e_i$, leaving the other vectors unchanged. Finally, take only the vectors of square length 2 in L, yielding the vectors $\pm e_i \pm e_j$ for $i \neq j$.

The preceding four root systems are said to be of types A_{n-1}, B_n, C_n, and D_n, respectively (the subscript in type A is $n-1$ rather than n because the ambient space has dimension $n-1$). They correspond to the respective algebraic groups $SL_n(k), SO_{2n+1}(k), Sp_{2n}(k)$, and $SO_{2n}(k)$. Note that orthogonal groups in even and odd dimensions have to be treated separately here and that a strange similarity is exhibited between $SO_{2n+1}(k)$ and $Sp_{2n}(k)$ that one would never have suspected from the definitions of these groups. Next take $V = \mathbb{R}^8$ and let L be the lattice spanned by the $e_i + e_j$, the $e_i - e_j$, and $(1/2, \ldots, 1/2)$. Taking the vectors of square length 2 in in L, one gets all the sums $\pm e_i \pm e_j$ as before plus the vectors $(\pm 1/2, \ldots, \pm 1/2)$ involving an *even* number of $+$ signs (this is because the vectors in L all have coordinate sums lying in $2\mathbb{Z}$). This is the root system of type E_8.

There are two other irreducible root systems of type E, namely E_7 and E_6; they are obtained from E_8 by restricting to the subspaces V', V'' of V consisting of vectors orthogonal to $e_7 + e_8$ or to $e_7 + e_8$ and $e_6 + e_8$, respectively. Finally, we have the root systems of types F_4 and G_2. The first is obtained by setting $V = \mathbb{R}^4$ and taking L to be the vectors of square length 1 or 2 in the lattice L spanned by the e_i and $(1/2, \ldots, 1/2)$; it consists of the $\pm e_i, \pm e_i \pm e_j$ and $(\pm 1/2, \ldots, \pm 1/2)$, where this time the signs are chosen with no constraints. The second, of type G_2, is obtained by defining V and L as for the root system A_2 above, but this time taking the vectors of square length 2 or 6. This yields the $e_i - e_j$ together with all vectors (a, b, c) where a, b, c are a permutation of either $1, 1, -2$ or $-1, -1, 2$. The root systems of types E through G (and the algebraic groups corresponding to them) are called exceptional.

Irreducible root systems correspond to connected algebraic groups G that are not just reductive but actually almost simple, in the sense that all proper normal subgroups of G are finite. The group G can be explicitly constructed from its root system by generators and relations. General root systems R correspond to semisimple groups G: these are products $G_1 G_2 \ldots G_m$ of normal almost simple subgroups G_i such that the intersection of any G_i and the product of the G_j for $j \neq i$ is finite. Each G_i corresponds to an irreducible subsystem of R. Finally, a general reductive group G is the product $G_s T$ of a semisimple group G_s and a torus T such that the intersection of G_s and T is finite.

The correspondence between connected semisimple groups and root systems is not one-to-one; it turns out that (finitely many) groups can share the same root system. For example, $SL_n(k)$ and the quotient $PSL_n(k)$of this group by its center (cyclic of order n) both have root systems of type A_{n-1}. A slight elaboration of a root system called a root datum, consisting of the root system together with a pair of lattices in its underlying Euclidean space, turns out to correspond bijectively to a connected almost simple linear algebraic group. The family of algebraic groups with a fixed root system is such that all members of it are quotients of one of them by a finite central subgroup.

I hope this whirlwind tour is enough to whet your appetite to learn more about algebraic groups at some point in the future. There is a second-year graduate algebra sequence offered every other year in which you can learn about Lie algebras, which are closely related to algebraic groups (in fact every algebraic group has a Lie algebra). Reductive and semisimple Lie algebras over algebraically closed fields of characteristic 0 can be classified by their root systems, in much the same manner as algebraic groups, but a little easier.