Lecture 12-4: The Existence Theorem, part 1

December 4, 2023

Last time we gave the outline of the proof that any two reductive groups G, G' over a fixed $\mathbf{k}$ with isomorphic root data are isomorphic; for this last week we will sketch the proof that there exists an algebraic group with any given root datum. For simplicity we will confine attention to data $D = (X, R, \check{X}, \check{R})$ such that X is exactly the $\mathbb{Z}$-span of R, so that the groups G we construct will be semisimple and of adjoint type. (There is a supplementary argument in the text to deal with the general case, which will be omitted here.)

The first step is to define the Lie algebra $\mathfrak{g}$ of G, using only the root system R. First we define (abstract) Lie algebras $\mathfrak{h}$ (over arbitrary fields F) in general: such an $\mathfrak{h}$ is a finite-dimensional vector space over F endowed with a bilinear product $[x, y]$ (called the bracket of x and y) such that $[x, x] = 0$ for all x (so that also $[x, y] = -[y, x]$ for all x, y) and the *Jacobi identity* holds, so that $[x, [y, z]] - [y, [x, z]] = [[x, y], z]$ for all x, y, z, or equivalently $[[x, y], z] + [[z, x], y] + [[y, z], x] = 0$. The main example to keep in mind is that of any finite-dimensional associative F-algebra A, taking $[xy]$ to be the commutator $xy - yx$; an easy calculation shows that the Jacobi identity indeed holds in this case. Now, given R, set $\mathfrak{t} = \mathbf{k} \otimes \check{X}$ and define $\mathfrak{g}$ as a vector space as $\mathfrak{t} \oplus \sum_{\alpha \in R} \mathbf{k} e_\alpha$ (see p. 179). Note that this decomposition is similar to, but much simpler than, the analogous one observed earlier for an algebraic group G with a given root system.

To define the bracket in general, it is enough by bilnearity to define $[x, y]$ for x, y lying either in $\mathfrak{t}$ or equal to one of the *root vectors* e_α. We decree that $[u, u'] = 0$ for $u, u' \in \mathfrak{t}, [u, e_\alpha] = \langle \alpha, u \rangle e_\alpha, [e_\alpha, e_{-\alpha}] = 1 \otimes \check{\alpha}, [e_\alpha, e_\beta] = c_{\alpha,\beta} e_{\alpha+\beta}$ if $\alpha, \beta, \alpha + \beta \in R, [e_\alpha, e_\beta] = 0$ if $\alpha, \beta \in R, \alpha + \beta \notin R$ (p. 179). Here the $c_{\alpha,\beta} \in \mathbf{k}^*$ are certain *structure constants* to be specified below; note that these are similar to, but significantly simpler than, the structure constants introduced earlier for groups.

To define the $c_{\alpha,\beta}$, we restrict for now to the *simply laced* case, where all roots in R have the same length; recall that this holds if and only if there are no multiple bonds in the Dynkin diagram of R, in which case we may take $(\alpha, \alpha) = 2$ for all $\alpha \in R$. It is easy to check that *for* $\alpha, \beta \in R$ *and* $\epsilon = \pm 1$ *we have* $\alpha + \epsilon\beta \in R$ *if and only if* $\langle \alpha, \check{\beta} \rangle = -\epsilon$ (Lemma 10.2.2 (i), p. 177). Now let f be a $\mathbb{Z}$-valued bilinear function on X such that $(x, y) \equiv f(x, y) + f(y, x) \mod 2$, $\frac{1}{2}(x, x) \equiv f(x, x) \mod 2$ for all $x, y \in X$; for example, fixing a $\mathbb{Z}$-basis $(e_i)_{1 \leq i \leq n}$ of X, we could set $f(e_i, e_j) = (e_i, e_j)$ if $1 \leq i < j \leq n$, $f(e_i, e_j) = 0$ if $i > j$, $f(e_i, e_i) = \frac{1}{2}(e_i, e_i)$.

Now fix a choice R^+ of positive roots, put $\epsilon(\alpha) = \pm 1$, according as $\alpha \in R$ lies in R^+ or $-R^+$, and define $c_{\alpha,\beta} = \epsilon(\alpha)\epsilon(\beta)\epsilon(\alpha+\beta)(-1)^{f(\alpha,\beta)}$ if $\alpha, \beta, \alpha+\beta \in R$. Also define $c_{\alpha\beta} = 0$ if any of $\alpha, \beta, \alpha+\beta$ fail to lie in R. Then we have

Lemma 10.2.4, p. 178

- $c_{\alpha,\beta} = -c_{\beta,\alpha}$ and $c_{-\alpha,\beta}c_{\alpha,-\alpha+\beta} + c_{\beta,\alpha}c_{-\alpha,\alpha+\beta} = \langle \beta, \check{\alpha} \rangle$;
- If $\alpha, \beta, \gamma \in R$ are linearly independent we have $c_{\alpha,\beta}c_{\alpha+\beta,\gamma} + c_{\beta,\gamma}c_{\beta+\gamma,\alpha} + c_{\gamma,\alpha}c_{\gamma+\alpha,\beta} = 0$.

Proof.

If $\alpha, \beta, \alpha+\beta \in R$ then we see from Lemma 10.2.2 (i) that $f(\alpha,\beta) + f(\beta < \alpha) \equiv (\alpha,\beta) \equiv 1 \mod 2$, implying the first assertion in (i). If $(\beta, \check{\alpha}) = -1$ then $\alpha+\beta \in R, -\alpha+\beta \notin R$, and $c_{-\alpha,\beta} = 0$. Hence $c_{\beta,\alpha} c_{-\alpha,\alpha+\beta} = -(-1)^{f(\beta,\alpha)+f(-\alpha,\alpha+\beta)} = -1$ and the second part of (i) follows. If $(\beta,\check{\alpha}) = 1$ the proof is similar. To prove part (ii) we may assume that $c_{\alpha,\beta} c_{\alpha+\beta,\gamma} \neq 0$. Then $(\alpha,\beta) = (\alpha+\beta,\gamma) = -1$, whence either $(\alpha,\gamma) = 0, (\beta,\gamma) = -1$ or $(\alpha,\gamma) = -1, (\beta,\gamma) = 0$; by symmetry we may assume that the first alternative holds. Then what we must show follows from

$$f(\alpha,\beta)+f(\alpha+\beta,\gamma)+f(\beta,\gamma)+f(\beta+\gamma,\alpha) \equiv (\alpha,\beta)+(\alpha,\gamma)+2f(\beta,\gamma) \equiv 1 \mod 2.$$

The proof is complete. □

As a consequence the Jacobi identity holds on basis vectors of $\mathfrak{g}$, so by linearity holds in general.

By analogy with associative algebras, we define a *derivation* on a general Lie algebra $\mathfrak{h}$ to be a linear map Δ on $\mathfrak{h}$ such that $\Delta[x, y] = [\Delta x . y] + [x, \Delta y]$ (the Leibniz rule). The Jacobi identity shows at once for any fixed $z \in \mathfrak{h}$ that ad z, sending any $x \in \mathfrak{h}$ to $[z, x]$, is a derivation; such derivations are called *inner*.

Lemma 10.2.6, p. 179

Any derivation Δ on the Lie algebra $\mathfrak{g}$ constructed above from a root datum is ad a for a unique $a \in \mathfrak{g}$, so that it is inner.

Proof.

Given Δ, write $\Delta u = d(u) + \sum_{\alpha \in R} \ell_\alpha(u) e_\alpha$ for $u \in \mathfrak{t}$, where d is a linear map from $\mathfrak{g}$ to $\mathfrak{t}$ and the ℓ_α are linear functions on $\mathfrak{g}$. By the Leibniz rule on $\mathfrak{t}$ we get $\langle \alpha, u \rangle \ell_\alpha(u') = \langle \alpha, u' \rangle \ell_\alpha(u)$ for all $\alpha \in R, u, u' \in \mathfrak{t}$, whence there is $c_\alpha \in \mathbf{k}$ with $\ell_\alpha(u) = c_\alpha \langle \alpha, u \rangle$ for $u \in \mathfrak{t}, \alpha \in R$. Then Δ+ad$(\sum c_\alpha e_\alpha)$ is a derivation Δ' mapping $\mathfrak{t}$ into itself. The Leibniz rule applied to $\mathfrak{t}$ and e_α then shows that there is $d_\alpha \in \mathbf{k}$ with $\Delta' e_\alpha = d_\alpha e_\alpha$; applying this rule to e_α and e_β we get $d_{\alpha+\beta} = d_\alpha + d_\beta$ if $\alpha, \beta\, \alpha + \beta \in R$, $d_{-\alpha} = -d_\alpha$. □

Proof.

Now let D be the choice of simple roots corresponding to R^+. Given $\beta \in R^+, \beta = \sum_{\alpha \in D} n_\alpha \alpha$, there must be some $\alpha \in D$ such that $n_\alpha > 0, (\beta, \alpha) > 0$, whence either $\beta = \alpha$ or $\beta - \alpha \in R^+$. Continuing in this way, we see that we can write any $\beta \in R^+$ as a sum $\alpha_1 + \ldots + \alpha_m$ of not necessarily distinct simple roots such that every partial sum $\alpha_1 + \ldots \alpha_i$ is a root. It follows that the d_α for $\alpha \in R^+$ and thus for $\alpha \in R$ are completely determined by the d_α for $\alpha \in D$, and finally that $\Delta' =$ad u_0 for some $u_0 \in \mathfrak{t}$, as desired. This u_0 is unique as it is easily seen that the only $x \in \mathfrak{g}$ with ad $x = 0$ is $x = 0$. □

If Δ is a derivation on a general Lie algebra $\mathfrak{h}$, then an easy calculation with the power series $\exp \Delta = \sum_{n=0}^{\infty} \frac{\Delta^n}{n!}$ defines an automorphism of $\mathfrak{h}$ whenever this series is well defined, taking Δ^0 to be the identity map. This is not always the case (even for say the algebraically closed field of algebraic complex numbers), but it does hold if Δ is nilpotent (and $\mathbf{k}$ has characteristic 0), so that Δ^m is identically 0 on $\mathfrak{h}$ for some fixed m.

If the characteristic of $\mathbf{k}$ is positive, then we must also make sure that we never divide by 0 in forming the series. Returning now to the above Lie algebra $\mathfrak{g}$, we find that $\Delta_{x,\alpha} =$ad $\mathbf{x}e_\alpha$ satisfies $D^3_{x,\alpha} = 0$ on $\mathfrak{g}$ for any $\alpha \in R, x \in \mathbf{k}$, since the only root β such that $\beta + 2\alpha$ is a root is $\beta = -\alpha$ and then $\beta + 3\alpha$ is not a root. Moreover we have (ad $e_\alpha)^2(e_{-\alpha}) = \check{\alpha}(\alpha)e_\alpha = 2e_\alpha$, so exp ke_α is defined on $\mathfrak{g}$ even if $\mathbf{k}$ has characteristic 2. We also have the law of exponents (exp ad ke_α)(exp ad ℓe_α) =exp ad $(k+\ell)e_\alpha$ for $k, \ell \in \mathbf{k}$. The set U_α of all automorphisms of $\mathfrak{g}$ of this type is then a one-dimensional group isomorphic to G_a and acting on $\mathfrak{g}$ by automorphisms; its Lie algebra may be identified with $\mathbf{k}e_\alpha$, since the action of U_α on $\mathfrak{g}$ has as differential the adjoint action of $\mathbf{k}e_\alpha$.

Now let T be a torus with character group X; let T act on $\mathfrak{g}$ via $t.u = u$ for $u \in \mathfrak{t}$, $t.e_\alpha = \alpha(t)e_\alpha$ for $\alpha \in R$. Finally, let G be the subgroup of $GL(\mathfrak{g}$ generated by T and all the groups U_α. Then we have

Proposition 10.2.8, p. 180

With notation as above, G is reductive, T is a maximal torus of it, and the root system of G relative to T is R.

Indeed, G acts on $\mathfrak{g}$ by automorphisms by the construction; as the differential of an automorphism is a derivation by Lemma 4.4.14, the Lie algebra of G is contained in $\mathfrak{g} = \mathfrak{t} + \sum_\alpha \mathbf{k}e_\alpha$ by the previous result. But $\mathfrak{g}$ is also contained in the Lie algebra $L(G)$ by the construction, whence $\mathfrak{g} = L(G)$ and $\dim G = \dim \mathfrak{g} = \dim T + |R|$.

It is easy to check that the roots of T are exactly the elements of R; since the minimal nontrivial normal subgroups of G correspond to the connected components of the Dynkin diagram of R by Theorem 8.1.5, G has no nontrivial normal unipotent subgroups and it is reductive. Identifying X with its dual $\check{X}$ via the bilinear form $(\cdot,\cdot)$, we have $\check{\alpha} = \alpha$ for all $\alpha \in R$ and thus $\check{R} = R$. Thus the root datum of G is $(X, R, \check{X}, \check{R})$. For $\alpha \in R$, the map sending $k \in \mathbf{k}$ to exp ad ke_α provides a realization of R in G. The structure constants $c_{\alpha,\beta;i,j}$ turn out to equal $c_{\alpha,\beta}$ if $\alpha, \beta \in R$ and $i = j = 1$; they are 0 otherwise. The quasisimple groups that are realized in this way are $PSL(n, \mathbf{k})$ (type A), $PSO(2n, \mathbf{k})$ (type D), and of types E_6, E_7, and E_8 (type E).

We conclude by remarking that another construction of the *simply connected* group G having a given root system R arises as the universal covering of G as an abstract topological group, bearing in mind that any such covering always has a topological group structure and that its deck transformations all arise from elements of its center (which turns out for algebraic groups to be isomorphic to the quotient of the weight lattice of R by its root lattice, as previously noted). The other groups having root system R, including the adjoint group, are then all quotients of this one by a finite central subgroup. We also observe that the non-semisimple adjoint group G' corresponding to a datum $(X, R, \check{X}, \check{R})$ for which X is not spanned by R but is instead the direct product of the abelian subgroup Q spanned by R and its orthogonal under the form $(\cdot, \cdot)$ is easily constructed from the group G with datum $(Q, R, \check{Q}, \check{R})$ by taking the direct product of this group and a suitable torus.