LECTURE 17

Results from SGA3, §XX.2: construction of $\alpha^\vee$

The goal of this lecture is to explain the proof of Demazure's crucial theorem 2.1 in Exp. XX, and the subsequent construction of a root datum for a split reductive group scheme.

43. Demazure's construction of $\alpha^\vee$

We keep the notation of Lecture 15: Z_α is a reductive S-scheme with a split maximal torus $T = D_S(M)$ and, setting $\mathfrak{g} = \mathrm{Lie}(G)$ and $\mathfrak{t} = \mathrm{Lie}(T)$, there exists $\alpha \in M$ such that

$$\mathrm{Lie}(Z_\alpha) = \mathfrak{t} \oplus \mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha}$$

where $\mathfrak{g}_\alpha$ and $\mathfrak{g}_{-\alpha}$ are line bundles over S, and there exist closed subgroups U_α and $U_{-\alpha}$, normalised by T, and T-equivariant group isomorphisms $\exp_\alpha : \mathfrak{g}_\alpha \xrightarrow{\sim} U_\alpha$ and $\exp_{-\alpha} : \mathfrak{g}_{-\alpha} \xrightarrow{\sim} U_{-\alpha}$. Further, the multiplication map m induces an isomorphism of S-schemes

$$U_{-\alpha} \times T \times U_\alpha \xrightarrow{\sim} \Omega_\alpha$$

where Ω_α is an open subscheme of Z_α, called the big cell.[1] Consider the following map, where we take the product $U_\alpha \times U_{-\alpha}$ in the "wrong order" w.r.t. to the choice of the big cell Ω:

$$f = m \circ (\exp_\alpha, \exp_{-\alpha}) : \qquad \mathfrak{g}_\alpha \times \mathfrak{g}_{-\alpha} \longrightarrow U_\alpha \times U_{-\alpha} \xrightarrow{m} G.$$

Theorem 43.1. *There exists a unique $\mathcal{O}_S$-linear pairing $\langle\ ,\ \rangle : \mathfrak{g}_\alpha \otimes \mathfrak{g}_{-\alpha} \to \mathcal{O}_S$ such that $f^{-1}(\Omega)$ is the complement $\mathcal{U}$ of the hypersurface $\langle X, Y\rangle = 1$ in $\mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha}$.*

Further, there exists a unique morphism of S-groups $\alpha^\vee : \mathbb{G}_{m,S} \to T$ such that for every $S' \to S$ and $(X, Y) \in \mathcal{U}(S')$, one has the equality:

$$f(X,Y) = \exp_{-\alpha}\Big(\frac{Y}{1 - \langle X, Y\rangle}\Big)\alpha^\vee\big(1 - \langle X, Y\rangle\big)\exp_\alpha\Big(\frac{X}{1 - \langle X, Y\rangle}\Big). \tag{43.1}$$

Moreover, $\langle\ ,\ \rangle$ is an isomorphism and one has $\alpha \circ \alpha^\vee = 2$.

Proof. By the uniqueness, which will be proved in the course of the proof, it suffices to prove existence in the case where $\mathfrak{g}_\alpha$ and $\mathfrak{g}_{-\alpha}$ have global sections X_α and $X_{-\alpha}$. Then, for every $S' \to S$ and $u, v \in \mathbb{G}_a(S')$, write

$$p_\alpha(u) = \exp_\alpha(uX_\alpha) \qquad \text{and} \qquad p_{-\alpha}(v) = \exp_{-\alpha}(vX_{-\alpha}).$$

Let $\mathcal{U}$ be the open subscheme of $\mathbb{G}^2_{a,m}$ which is the inverse image of the big cell Ω_α under the morphism :

$$f : \mathbb{G}^2_{a,S} \xrightarrow{p_\alpha \times p_{-\alpha}} U_\alpha \times U_{-\alpha} \xrightarrow{m} Z_\alpha.$$

---

[0] Lecture of Aug. 20 and 22, 2024. Version of Aug. 23. Thanks to Vikraman Balaji and Sukhendu Mehrotra for useful questions, which lead to improvements in the exposition.

[1] Later on, G will be a reductive S-scheme with a split maximal torus $T = D_S(M)$; then replacing S by an open subset we may assume that there exists a subset R of M such that $\mathrm{Lie}(G) = \mathfrak{t} \oplus \bigoplus_{\beta \in R} \mathfrak{g}_\beta$ where each $\mathfrak{g}_\beta$ is a line bundle. The point is that one needs to prove results over any given pair of opposite roots $\pm\alpha$. This is achieved by considering the subgroup $\mathrm{Ker}(\alpha) \subset T$ and its centraliser $Z_\alpha = \underline{\mathrm{Cent}}_G(\mathrm{Ker}(\alpha))$; it has the properties stated above, see Lect. 15, §40.2.

Then there exist S-morphisms $A, C : \mathcal{U} \to \mathbb{G}_{a,S}$ and $B : \mathcal{U} \to T$ such that for $(u, v) \in \mathcal{U}(S')$ we can write uniquely:

$$p_\alpha(u)p_{-\alpha}(v) = p_{-\alpha}\big(A(u,v)\big) \cdot B(u,v) \cdot p_\alpha\big(C(u,v)\big). \tag{43.2}$$

Obviously, denoting by e_T the unit element of $T(S')$, one has

$$p_\alpha(0)p_{-\alpha}(v) = p_{-\alpha}(v) \cdot e_T \cdot p_\alpha(0) \qquad \text{and} \qquad p_\alpha(u)p_{-\alpha}(0) = p_{-\alpha}(0) \cdot e_T \cdot p_\alpha(u).$$

This shows that $\mathcal{U}$ contains a neighborhood of the coordinate axes in $\mathbb{G}^2_{a,S}$, hence is schematically dense relative to S, and that one has the equalities:

$$\begin{cases} \text{if } u = 0 \text{ then} & A(0,v) = v, \quad B(0,v) = e_T, \quad C(0,v) = 0, \\ \text{if } v = 0 \text{ then} & A(u,0) = 0, \quad B(u,0) = e_T, \quad C(u,0) = u. \end{cases} \tag{43.3}$$

We want to prove that there exists $a \in \mathbb{G}_m(S)$ such that $\mathcal{U}$ is the complement of the hypersurface $auv = 1$ and that for every $S' \to S$ and $(u, v) \in \mathcal{U}(S')$, one has:

$$A(u,v) = \frac{v}{1 - auv}, \qquad C(u,v) = \frac{u}{1 - auv}, \qquad B(u,v) = \alpha^\vee(1 - auv), \tag{43.4}$$

for some uniquely defined morphism of S-groups $\alpha^\vee : \mathbb{G}_{m,S} \to T$. The proof has several steps.

43.1. Reduction to functions of the single variable $x = uv$. The first step is to prove the following lemma:

Lemma 43.2. *There exist an open subset W of $\mathbb{G}_{a,S}$, containing the zero section hence universally schematically dense relative to S, and morphisms $E, F : W \to \mathbb{G}_{m,S}$ and $H : W \to T$ with $F(0) = 1 = E(0)$ and $H(0) = e_T$ such that, for any $S' \to S$, if $(u, v) \in \mathcal{U}(S')$ and $uv \in W(S')$ then*

$$p_\alpha(u)p_{-\alpha}(v) = p_{-\alpha}\Big(\frac{v}{F(uv)}\Big) \cdot H(uv) \cdot p_\alpha\Big(\frac{u}{E(uv)}\Big). \tag{43.5}$$

Proof. Firstly, define the open subscheme $\mathcal{V}$ of $\mathcal{U}$ by

$$\mathcal{V}(S') = \{(u,v) \in \mathcal{U}(S') \mid (uv, 1) \text{ and } (1, uv) \text{ belong to } \mathcal{U}(S')\}$$

for every $S' \to S$.

Since f is T-equivariant (for the adjoint action of T), one has for any $S' \to S$ and $t \in T(S')$:

$$f\big(\alpha(t)u, \alpha(t)^{-1}v\big) = tf(u,v)t^{-1} = p_{-\alpha}\big(\alpha(t)^{-1}A(u,v)\big) \cdot B(u,v) \cdot p_\alpha\big(\alpha(t)C(u,v)\big).$$

Since $\alpha \neq 0$, the morphism $\alpha : T \to \mathbb{G}_{m,S}$ is faithfully flat. It follows that for every $S' \to S$ and $(z, u, v) \in \mathbb{G}_m(S') \times \mathcal{U}(S')$ one has the equalities below, because the corresponding morphisms become equal after the faithfully flat base change to $T \times_S \mathcal{U}$:

$$A(u,v) = zA(zu, z^{-1}v), \qquad C(u,v) = z^{-1}C(zu, z^{-1}v), \qquad B(u,v) = B(zu, z^{-1}v).$$

If follows that if $(u, v) \in \mathcal{U}(S')$ and $u, v \in \mathbb{G}_m(S')$ then $(u, v) \in \mathcal{V}(S')$ and one has the equalities:

$$A(u,v) = vA(uv,1), \qquad C(u,v) = uC(1,uv), \qquad B(u,v) = B(uv,1) = B(1,uv). \tag{43.6}$$

In particular, these equalities are true on $\mathcal{V} \cap \mathbb{G}^2_{m,S}$. Since $\mathbb{G}^2_{m,S}$ is schematically dense in $\mathbb{G}^2_{a,S}$, they hold true on $\mathcal{V}$.

Define temporarily the open subset $\widetilde{W}$ of $\mathbb{G}_{a,S}$ by $\widetilde{W}(S') = \{x \in \mathbb{G}_a(S') \mid (x, 1) \in \mathcal{V}(S')\}$, and define morphisms $A_1, C_1 : \widetilde{W} \to \mathbb{G}_{a,S}$ and $H : \widetilde{W} \to T$ by $A_1(x) = A(x, 1)$, $C_1(x) = C(1, x)$ and $H(x) = B(x, 1) = B(1, x)$. Then, for $(u, v) \in \mathcal{V}(S')$ one has

$$A(u,v) = vA_1(uv), \qquad C(u,v) = uC_1(uv), \qquad B(u,v) = H(uv). \tag{43.7}$$

By (43.3), one has $A_1(0) = 1$ and $C_1(0) = 1$. Therefore, the open subscheme W of $\widetilde{W}$ defined for every $S' \to S$ by

$$W(S') = \{x \in WS') \mid A_1(x) \in \mathbb{G}_m(S'), \quad C_1(x) \in \mathbb{G}_m(S')\} \tag{43.8}$$

is still an open neighborhood of the zero section, hence schematically dense in $\mathbb{G}_{a,S}$ relative to S. We define morphisms $F, E : W \to \mathbb{G}_{m,S}$ by:

$$F(x) = A_1(x)^{-1} \quad \text{and} \quad E(x) = C_1(x)^{-1}. \tag{43.9}$$

Now, if $(u, v) \in \mathcal{U}(S')$ and $uv \in W(S')$ then $(u, v) \in \mathcal{V}(S')$ and taking (43.2), (43.7) and (43.9) into account one obtains the desired equality (43.5). [2] $\square$

43.2. Functional equations. Now, take $u = 1$ and multiply (43.5) on the right by $p_{-\alpha}(w)$. On the one hand, provided that $(E(v)^{-1}, w) \in \mathcal{U}(S')$ and $wE(v)^{-1} \in W(S')$, we can apply (43.5) to the product $p_\alpha\big(E(v)^{-1}\big)p_{-\alpha}(w)$ and then the equality $H(x)p_{-\alpha}(y) = p_{-\alpha}\big(\alpha(H(x)^{-1})y\big)H(x)$ to find the "coordinates" of the RHS as an element of Ω.

On the other hand, since $p_{-\alpha}(v)p_{-\alpha}(w) = p_{-\alpha}(v+w)$, we obtain another expression, provided that $(1, v + w) \in \mathcal{U}(S')$ and $v + w \in W(S')$. Therefore, making the change of variables $x = v$ and $y = wE(v)^{-1}$, we obtain that there exists an open neighborhood $\mathcal{W}$ of the zero section of $\mathbb{G}^2_{a,S}$ such that if $(x, y) \in \mathcal{W}(S')$ then x, y and $x + yE(x)$ belong to $W(S')$ and one has:

$$E(x + yE(x)) = E(x)E(y) \tag{43.10}$$

$$H(x + yE(x)) = H(x)H(y) \tag{43.11}$$

$$\frac{x + yE(x)}{F(x + yE(x))} = \frac{x}{F(x)} + \alpha(H(x))^{-1}\,\frac{yE(x)}{F(y)} \tag{43.12}$$

Similarly, take $v = 1$ and multiply (43.5) on the left by $p_\alpha(t)$. Making another change of variables and replacing the previous $\mathcal{W}$ by a *smaller* neighborhood of the zero section of $\mathbb{G}^2_{a,S}$, still denoted by $\mathcal{W}$, one obtains that if $(x, y) \in \mathcal{W}(S')$ then x, y and $x + yF(x)$ belong to $W(S')$ and one has:

$$F(x + yF(x)) = F(x)F(y) \tag{43.13}$$

$$H(x + yF(x)) = H(x)H(y) \tag{43.14}$$

$$\frac{x + yF(x)}{E(x + yF(x))} = \frac{x}{E(x)} + \alpha(H(x))^{-1}\,\frac{yF(x)}{E(y)} \tag{43.15}$$

Set $W_1(S') = \{x \in W(S') \mid (x, 0) \in \mathcal{W}(S')\}$ and define W_2 similarly. Then, one has the following lemma ([**SGA3**$_3$], XX, Lemma 2.3).

LEMMA 43.3. *Consider the functional equation* (43.13)*. Then:*

(i) *If $S = \mathrm{Spec}(k)$, with k a field, one has $F(x) = 1 + ax$, where a is the derivative $F'(0)$.*
(ii) *For S arbitrary, consider the section $a = F'(0)$ of $\mathcal{O}_S$. If $a \in \mathbb{G}_m(S)$ then $F(x) = 1+ax$.*

SKETCH OF PROOF. By derivating (43.13) with respect to x at $x = 0$, and with respect to y at $y = 0$, and recalling that $F(0) = 1$, ones obtains:

$$\begin{cases} F'(y)(1 + yF'(0)) = F'(0)F(y) & \text{for } y \in W_2(S') \\ F'(x)F(x) = F(x)F'(0) & \text{for } x \in W_1(S'). \end{cases}$$

As F take its values in $\mathbb{G}_m$, the second equality gives

$$F'(x) = F'(0) \qquad \text{for } x \in W_1(S') \tag{43.16}$$

[2] In fact, the proof will show that $\mathcal{U}(S') = \{(u, v) \in \mathbb{G}_a(S')^2 \mid uv \in W(S')\}$. In particular, one has $\mathcal{V} = \mathcal{U}$.

and hence the first gives:

$$F'(0)(1 + yF'(0)) = F'(0)F(y) \quad \text{for } y \in (W_1 \cap W_2)(S').$$

If $a = F'(0)$ is invertible, this gives (ii) as well as (i) in the case where $a \neq 0$.

So, suppose that $S = \operatorname{Spec}(k)$, with k a field, and that $F'(0) = 0$. Then, by (43.16), F' vanishes on the schematically dense open subset W_1, hence $F' = 0$. If $\operatorname{char}(k) = 0$ this gives immediately that F is constant, hence equal to $F(0) = 1$. So assume that $\operatorname{char}(k) = p > 0$ and that $F \in k(X)$ is not constant. Then there exists $F_1 \in k(X)$ such that $F_1' \neq 0$ and $n \in \mathbb{N}^*$ such that

$$F(X) = F_1(X^{p^n}) = F_1(X)^{p^n}.$$

Note then that $F_1(0) = F(0) = 1$. Plugging this into the functional equation (43.13) one obtains:

$$F_1(x + yF_1(x)^{p^n}) = F_1(x)F_1(y).$$

Derivating this with respect to x at $x = 0$, and with respect to y at $y = 0$, and using that $F_1(0) = 1$, ones obtains:

$$\begin{cases} F_1'(y) = F_1'(0)F_1(y) & \text{for } y \in W_2(S') \\ F_1'(x)F_1(x)^{p^n} = F_1(x)F_1'(0) & \text{for } x \in W_1(S'). \end{cases}$$

Together, these equalities give $F_1'(x)F_1(x)^{p^n} = F_1'(x)$ for $x \in (W_1 \cap W_2)(S')$, hence by (schematic) density, we have

$$F_1'(X)F_1(X)^{p^n} = F_1'(X).$$

in the field $k(X)$. By assumption, F_1' is a non-zero element of $k(X)$, hence we obtain that $F_1(X)^{p^n} = 1$, whence $F_1 = 1$, contradicting the initial hypothesis. This shows that F is constant, and equal to $F(0) = 1$. This completes the proof of the lemma. $\square$

43.3. Determination of E and F. Suppose first that $S = \operatorname{Spec}(k)$, with k a field, and that $F'(0) = 0$. Then we have seen that $F = 1$ and hence (43.14) gives $H(x + y) = H(x)H(y)$ for all $x, y \in W(S')$ such that $x + y \in W(S')$. By Prop. 42.12, it follows that H extends to a homomorphism of k-groups $\mathbb{G}_{a,k} \to T$, which is necessarily constant with value e, the neutral element of T.

On the other hand, by the previous lemma, we also have $E(x) = 1 + bx$ for some $b \in k$. But then (43.10) gives:[3]

$$\frac{x + y}{1 + b(x + y)} = \frac{x}{1 + bx} + \frac{y}{1 + by}$$

which gives $0 = xyb(2 + (x + y)b)$, whence $b(2 + (x + y)b) = 0$ and finally $b = 0$. Thus, F, H, E are constant with values $1, e, 1$ on a neighborhood of 0, hence on $\mathbb{G}_{a,k}$, and therefore

$$p_\alpha(u)p_{-\alpha}(v) = p_{-\alpha}(v)p_\alpha(u)$$

for all u, v, which is a contradiction since U_α and $U_{-\alpha}$ do not commute on any fiber.

Coming back to arbitrary S, this shows that the section $F'(0)$ of $\mathcal{O}_S$ vanishes nowhere, hence is invertible. By the previous lemma, again, there exist $a, b \in \mathbb{G}_m(S)$ such that

$$F(x) = 1 + ax, \qquad E(x) = 1 + bx$$

for all $x \in W(S')$. Plugging this into (43.12), one obtains:[4]

$$y\,\alpha(H(x))\,(1 + ay) = y\Big(1 + ax + ay(1 + bx)\Big)(1 + ax).$$

[3]Note a typo in [**SGA3**$_3$], XX, first displayed formula on p.40: on the RHS $E(x)$ should be $E(x)^{-1}$.

[4]Note a typo in [**SGA3**$_3$], XX, p.40, §E: on the right of 3 formulas, $(1 + bx)$ should be replaced by $(1 + ax)$.

Since $\mathbb{G}_{m,S}$ is schematically dense in $\mathbb{G}_{a,S}$, one obtains:

$$\alpha(H(x))\,(1+ay) = \Big(1+ax+ay(1+bx)\Big)(1+ax). \tag{43.17}$$

Then, taking $y=0$ gives:

$$\alpha(H(x)) = (1+ax)^2, \qquad \forall x \in W(S') \tag{43.18}$$

and plugging this into (43.17) and using that the open subset $\{1+ax \neq 0\}$ is schematically dense, one obtains

$$1+ax+ay+a^2xy = (1+ax)(1+ay) = 1+ax+ay+abxy$$

whence $\boxed{a=b.}$ Finally, since $a \in \mathbb{G}_m(S)$ the pairing $\mathfrak{g}_\alpha \otimes_{\mathcal{O}_S} \mathfrak{g}_{-\alpha} \to \mathcal{O}_S$, $uX_\alpha \otimes vX_{-\alpha} \mapsto -auv$ is an isomorphism.

43.4. The morphism $\alpha^\vee : \mathbb{G}_{m,S} \to T$. Since $a \in \mathbb{G}_m(S)$, the image by $x \mapsto 1+ax$ of the neighborhood W of 0 in $\mathbb{G}_{a,S}$ is a neighborhood W' of 1 in $\mathbb{G}_{m,S}$. Consider the morphism $P : W' \to T$ defined by $P(1+ax) = H(x)$.

Using (43.11) one obtains that for (x,y) in some schematically dense open subset, one has

$$P(1+ax+ay) = P\Big(\frac{1+ax+ay}{1+ax}\Big)P(1+ax).$$

Using Prop. 42.12, it follows that P extends to a S-group morphism $\alpha^\vee : \mathbb{G}_{m,S} \to T$. By (43.18) one has $\alpha\circ\alpha^\vee(z) = z^2$ for $z \in W'(S')$. Since W' is schematically dense, it follows that $\alpha\circ\alpha^\vee = 2$.

43.5. Description of $\mathcal{U} = f^{-1}(\Omega_\alpha)$. So, replacing the previous a by $-a$ we have proved that there exist $a \in \mathbb{G}_m(S)$ and $\alpha^\vee \in \mathrm{Hom}_{S\text{-Gr}}(\mathbb{G}_{m,S}, T)$ with $\alpha\circ\alpha^\vee = 2$, such that, whenever $(u,v) \in \mathcal{U}(S')$ and $uv \in W(S')$, one has that $1-auv$ is invertible and the equality:

$$p_\alpha(u)p_{-\alpha}(v) = p_{-\alpha}\Big(\frac{v}{1-auv}\Big)\alpha^\vee(1-auv)p_\alpha\Big(\frac{u}{1-auv}\Big). \tag{43.19}$$

Consider now the open subset $\mathcal{U}'$ of $\mathbb{G}^2_{a,S}$ defined by $1-auv$ invertible, i.e. $\mathcal{U}' = (\mathbb{G}^2_{a,S})_g$, where $g(u,v) = 1-auv$. The two sides of the above equality define morphisms from $\mathcal{U}'$ to G, which coincide on $\mathcal{U}'\cap\mathcal{U}$. Since $\mathcal{U}$ is schematically dense, it follows that they coincide on $\mathcal{U}'$, and hence we have $\mathcal{U}' \subset \mathcal{U}$.

To prove that $\mathcal{U}' = \mathcal{U}$, it suffices to check equality on each fiber. But, over a field k, the domain of definition of rational map $A : \mathbb{G}^2_{a,k} \to \mathbb{G}_{a,k}$, $(u,v) \mapsto \dfrac{v}{1-auv}$ is the open subset defined by $1-auv$ invertible, i.e. , A cannot be extended as a morphism on a strictly larger open subset. This proves that $\mathcal{U} = \mathcal{U}'$. It follows that the open subset $\mathcal{V} \subset \mathcal{U}$ considered in the proof is actually equal to $\mathcal{U}$, and that for $(u,v) \in \mathcal{U}(S')$ one has $uv \in W(S')$.

43.6. Uniqueness of a and $\alpha^\vee$, existence of the perfect pairing $\langle\ ,\ \rangle$. Suppose that a' and $\beta^\vee$ have the same properties as a and $\alpha^\vee$. Then, for every $u \in W(S')$ one hase $(u,1) \in \mathcal{U}(S')$ and

$$\frac{1}{1-au} = A(u,1) = \frac{1}{1-a'u}$$

hence $1-au = 1-a'u$ for $u \in W(S')$, which gives $a' = a$. This proves the uniqueness of $a \in \mathbb{G}_m(U)$ corresponding to an arbitrary choice of trivializing sections $X_\alpha, X_{-\alpha}$ of the line bundles $\mathfrak{g}_\alpha$ and $\mathfrak{g}_{-\alpha}$ over an open subset U of S.[5]

[5] Note that the a itself has not significance, but the uniqueness result show that the perfect pairing $\mathfrak{g}_\alpha\times\mathfrak{g}_{-\alpha} \to \mathcal{O}_S$ defined over U by $(uX_\alpha, vX_{-\alpha}) \mapsto auv$ extends uniquely to a perfect pairing over S, which makes $\mathfrak{g}_\alpha$ and $\mathfrak{g}_{-\alpha}$ dual line bundles. One this is known, over any subset U where $\mathcal{L} = \mathfrak{g}_\alpha$ is trivial, we can choose arbitrarily a trivializing section $X = X_\alpha$; then if we chose for $X_{-\alpha}$ the dual section X^{-1}, i.e. the unique section of $\mathcal{L}^{-1} = \mathfrak{g}_{-\alpha}$ over U such that $\rangle X^{-1}, X\rangle = 1$, we have that $\rangle uX_\alpha, vX_{-\alpha}\rangle = uv$, i.e. the constant a has become 1.

Then one has also:

$$\alpha^\vee(1-au) = p_{-\alpha}\Big(\frac{-1}{1-au}\Big)p_\alpha(u)p_{-\alpha}(1)p_\alpha\Big(\frac{-u}{1-au}\Big) = \beta^\vee(1-au)$$

and it follows that $\beta^\vee = \alpha^\vee$. This completes the proof of Theorem 43.1.

REMARK 43.4. Applying $g \mapsto g^{-1}$ to both sides of (43.1) and replacing $-X, -Y$ by X, Y, one obtains:

$$\exp_{-\alpha}(Y)\exp_\alpha(X) = \exp_\alpha\Big(\frac{X}{1-\langle X,Y\rangle}\Big)\alpha^\vee\big(1-\langle X,Y\rangle\big)^{-1}\exp_{-\alpha}\Big(\frac{Y}{1-\langle X,Y\rangle}\Big).$$

This shows that $\langle Y,X\rangle = \langle X,Y\rangle$ and that, in additive notation, $(-\alpha)^\vee = -\alpha^\vee$.

44. Consequences. Root data and split reductive group schemes

Now, as in Lect. 15, Lemma 40.7, assume that G is a reductive S-group scheme with a *split* maximal torus $T = D_S(M)$ and that there exists a set R of constant sections of M_S, i.e. of elements of M, such that $\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\beta\in R}\mathfrak{g}_\beta$.

44.1. The elements $m_\alpha \in N_G(T)$. The normaliser $N_G(T)$ is represented by a closed subgroup scheme of G. We want to define local sections m_α of $N_G(T)$, for every pair of opposite roots $\pm\alpha$.

DEFINITION 44.1. We say that two local sections X_α and $X_{-\alpha}$ of $\mathfrak{g}_\alpha$ and $\mathfrak{g}_{-\alpha}$ over an open subset U of S are *paired*[6] if $\langle X_\alpha, X_{-\alpha}\rangle = 1$, i.e. if $\exp_\alpha(X_\alpha)\exp_{-\alpha}(X_{-\alpha})$ is "universally out of the big cell Ω_α"; in this case, we write $X_{-\alpha} = X_\alpha^{-1}$ and we set:

$$m_\alpha = \exp_\alpha(X_\alpha)\exp_{-\alpha}(X_\alpha^{-1})\exp_\alpha(X_\alpha).$$

Note also that in this case formula (43.19) becomes:

$$p_\alpha(u)p_{-\alpha}(v) = p_{-\alpha}\Big(\frac{v}{1-uv}\Big)\alpha^\vee(1-uv)p_\alpha\Big(\frac{u}{1-uv}\Big). \tag{44.1}$$

PROPOSITION 44.2. (i) m_α *depends only on the pair* $\pm\alpha$ (*and the choice of* X_α), *i.e. setting* $X_{-\alpha} = X_\alpha^{-1}$ *we have*

$$m_\alpha = \exp_\alpha(X_\alpha)\exp_{-\alpha}(X_\alpha^{-1})\exp_\alpha(X_\alpha) = \exp_{-\alpha}(X_{-\alpha})\exp_\alpha(X_{-\alpha}^{-1})\exp_{-\alpha}(X_{-\alpha}). \tag{44.2}$$

(ii) $m_\alpha^2 = \alpha^\vee(-1)$; *in particular,* m_α^2 *is a section of* T.

(iii) m_α *belongs to* $N_G(T)$. *More precisely, for any* $S' \to S$ *and* $t \in T(S')$, *one has*

$$m_\alpha\, t\, m_\alpha^{-1} = t\cdot\alpha^\vee\big(\alpha(t)^{-1}\big) = m_\alpha^{-1}\, t\, m_\alpha.$$

(iv) *The induced action of* m_α *on* $X(T)$ *and* $X^\vee(T)$ *are given respectively by:*

$$m_\alpha(\lambda) = \lambda - \langle\lambda,\alpha^\vee\rangle\alpha \qquad \textit{and} \qquad m_\alpha(\eta) = \eta - \langle\alpha,\eta\rangle\alpha^\vee. \tag{44.3}$$

PROOF. For (i) we refer to the proof of Exp. XX, Th. 3.1 (vi). (We did this computation for SL_2 in Lect. 15.[7])

[6] In French: appariées.

[7] With the choice $X_\alpha = E_{12}$ one has $X_{-\alpha} = -E_{21}$ and $m_\alpha = \begin{pmatrix} 0 & 1 \\ -1 & 0\end{pmatrix}$. More symmetrically, in the adjoint representation $\mathfrak{sl}_2$ with basis $(X_\alpha, H_\alpha, X_{-\alpha})$, where $H_\alpha = [X_{-\alpha}, X_\alpha]$, the matrix of m_α is $\begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0\end{pmatrix}$.

Let us prove (ii). One has $m_\alpha^2 = p_\alpha(1)p_{-\alpha}(1)p_\alpha(2)p_{-\alpha}(1)p_\alpha(1)$. Applying (44.1) to the product $p_\alpha(2)p_{-\alpha}(1)$, one obtains:

$$\begin{aligned} m_\alpha^2 &= p_\alpha(1)p_{-\alpha}(1)p_{-\alpha}\Big(\frac{1}{1-2}\Big)\alpha^\vee(1-2)p_\alpha\Big(\frac{2}{1-2}\Big)p_\alpha(1) \\ &= p_\alpha(1)\alpha^\vee(-1)p_\alpha(-1) = \alpha^\vee(-1)p_\alpha\Big((-1)^{\langle\alpha,\alpha^\vee\rangle}\Big)p_\alpha(-1) = \alpha^\vee(-1). \end{aligned}$$

Let us prove (iii). Using the T-equivariance of p_α and $p_{-\alpha}$, one has

$$\begin{aligned} m_\alpha\, t\, m_\alpha^{-1} &= p_\alpha(1)p_{-\alpha}(1)p_\alpha(1)\, t\, p_\alpha(-1)p_{-\alpha}(-1)p_\alpha(-1) \\ &= p_\alpha(1)p_{-\alpha}(1)p_\alpha\big(1-\alpha(t)\big)p_{-\alpha}\big(-\alpha(t)^{-1}\big)p_\alpha(-\alpha(t))\, t \end{aligned}$$

Next, (44.1) gives:[8]

$$\begin{aligned} p_\alpha\big(1-\alpha(t)\big)p_{-\alpha}\big(-\alpha(t)^{-1}\big) &= p_{-\alpha}\Big(\frac{-\alpha(t)^{-1}}{1+\alpha(t)^{-1}-1}\Big)\alpha^\vee\big(\alpha(t)^{-1}\big)p_\alpha\Big(\frac{1-\alpha(t)}{\alpha(t)^{-1}}\Big) \\ &= p_{-\alpha}(-1)\alpha^\vee\big(\alpha(t)^{-1}\big)p_\alpha\big(\alpha(t)-\alpha(t)^2\big) \end{aligned}$$

and plugging this into the previous equality gives

$$\begin{aligned} m_\alpha\, t\, m_\alpha^{-1} &= p_\alpha(1)\alpha^\vee\big(\alpha(t)^{-1}\big)p_\alpha\big(-\alpha(t)^2\big)\, t \\ &= \alpha^\vee\big(\alpha(t)^{-1}\big)p_\alpha\Big(\alpha\circ\alpha^\vee(\alpha(t))\Big)p_\alpha\big(-\alpha(t)^2\big)\, t = \alpha^\vee\big(\alpha(t)^{-1}\big)\, t \end{aligned}$$

where in the last equality we used that $\alpha\circ\alpha^\vee = 2$. This proves the first equality of (iii). The second one follows since $m_\alpha^{-1} = m_\alpha\alpha^\vee(-1)$ by (ii).

Let us prove (iv). Let $\lambda \in X(T)$ and $\eta \in X^\vee(T)$. Firstly, $m_\alpha(\lambda)$ is defined by $m_\alpha(\lambda)(t) = \lambda(m_\alpha^{-1}\, t\, m_\alpha)$, for any $S' \to S$ and $t \in T(S')$. Since, by (ii), the adjoint action of m_α and m_α^{-1} on T are the same, one obtains:

$$m_\alpha(\lambda)(t) = \lambda(m_\alpha\, t\, m_\alpha^{-1}) = \lambda(t)\lambda\big(\alpha^\vee(\alpha(t))^{-1}\big) = \lambda(t)\alpha(t)^{-\langle\lambda,\alpha^\vee\rangle}$$

and, in additive notation, the RHS is $(\lambda - \langle\lambda,\alpha^\vee\rangle\alpha)(t)$. Similarly, for $z \in \mathbb{G}_m(S')$ one has:

$$m_\alpha(\eta(z)) = \eta(z)\cdot(\alpha^\vee\circ\alpha\circ\eta)(z)^{-1} = \eta(z)\cdot\alpha^\vee(z)^{-\langle\alpha,\eta\rangle}$$

and in additive notation the RHS is $(\eta - \langle\alpha,\eta\rangle\alpha^\vee)(z)$. This proves (iv). $\square$

44.2. Split reductive group schemes. We follow Exp. XXII, Def. 1.13, with a grain of salt added by Conrad ([**Co14**], Example 5.1.2).

DEFINITION 44.3. Let G be a reductive S-group scheme and $\mathfrak{g} = \mathrm{Lie}(G)$. We say that G is **split** if there exists a maximal torus T equipped with an isomorphism $T \simeq D_S(M)$ for a finite free abelian group M such that, setting $M^\vee = \mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Z})$, one has:

(1) there exist a system of roots R of (G,T) given by constant sections of M_S, i.e. elements of M,
(2) each root space $\mathfrak{g}_\alpha$ is a *trivial* line bundle, i.e. isomorphic to $\mathcal{O}_S$,
(3) for each $\alpha \in R$, the coroot $\alpha^\vee \in \underline{\mathrm{Hom}}_{S\text{-}\mathrm{Gr}}(\mathbb{G}_{m,S},T) \simeq M_S^\vee$ constructed in §43 is given by a *constant* section of $M_S^\vee$, i.e. an element of $M^\vee$.

We had shown in earlier lectures that for any $s \in S$, there exists an open neighborhood V of S and a surjective étale map $U \to V$ such that G_U possesses a maximal torus T which is split, i.e. $T \simeq D_S(M)$ for some M. Then we showed in Lect. 15, Lemma 40.7, that conditions (i) and (ii) are satisfied Zariski-locally, and for each $\alpha \in R$ we just proved in §43 the existence of the coroot $\alpha^\vee \in \underline{\mathrm{Hom}}_{U\text{-}\mathrm{Gr}}(\mathbb{G}_{m,U},T) \simeq M_U^\vee$, which is therefore a locally constant section of $M^\vee$ over

[8] In [**SGA3**$_3$], Exp. XX, proof of Th. 3.1 (iii), formula (43.5) for $-\alpha$ is applied to $p_{-\alpha}(1)p_\alpha(1-\alpha(t))$.

U. Then, for any $s' \in U$ there exists a clopen subset U' containing s' such that all $\alpha^\vee$ are given by constant sections over U', hence $G_{U'}$ is split.

Thus, we have obtained the following proposition ([**SGA3**$_3$], Exp. XXII, Prop. 2.1 or [**Co14**], Lemma 5.1.3):

PROPOSITION 44.4. *Let G be a reductive S-group scheme.*

(1) *Étale-locally on S, G possesses a split maximal torus T.*

(2) *If G possesses a split maximal torus T over S, then G is split Zariski-locally on S.*

REMARK 44.5. Note that if G possesses a split maximal torus T and if S is connected and $\mathrm{Pic}(S) = \{0\}$, for example if $S = \mathrm{Spec}(A)$ where A is a PID or a local ring, then G is split.

REMARK 44.6. Let us record here the following example by Conrad ([**Co14**], Example 5.1.2). Let $S = S_1 \coprod S_2$, with each S_i a copy of $\mathrm{Spec}(\mathbb{C})$, and let G be the S-group scheme which is $\mathrm{PGL}_2 \times \mathbb{G}_m$ over S_1 and GL_2 over S_2. We can choose as maximal torus $T = \mathbb{G}_{m,S}^2$, where the isomorphism from T to the diagonal matrices in G is given over S_1 by $(z, z') = (\overline{\varepsilon}_1(z), z')$, using the notation of Lect. 15, 41.3, and by $(z, z') \mapsto \mathrm{diag}(zz', z')$ over S_2. Set $M = \mathrm{Hom}_{S\text{-}\mathrm{Gr}}(T, \mathbb{G}_{m,S}) \simeq \mathbb{Z}^2$ and let $M^\vee = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$. Then $\mathfrak{g} = \mathfrak{t} \oplus \mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha}$ where α is the constant element of M given by $(z, z') \mapsto z$. Further, $\mathfrak{g}_\alpha$ and $\mathfrak{g}_{-\alpha}$ are free modules over $\mathcal{O}(S) = \mathbb{C} \times \mathbb{C}$. However, the coroot $\alpha^\vee$ is given over S_1 by $\alpha^\vee(z) = (\overline{\varepsilon}_1(z^2), 1)$ and over S_2 by $\alpha^\vee(z) = (z^2, z^{-1})$; it is *not* a constant section of $M_S^\vee$. This shows that over a non-connected base S, condition (iii) does not follow from conditions (i) and (ii) of Def. 44.3, so that replacing S by some clopen subset on which $\alpha^\vee$ is constant may be needed to obtain condition (iii).

We also have the following proposition (see [**SGA3**$_3$], Exp. XXII, Prop. 1.14 or [**Co14**], Prop. 5.1.6)

PROPOSITION 44.7. *Let (G, T) be a split reductive S-group scheme, with $T = D_S(M)$, and let $R \subset M$ and $R^\vee \subset M^\vee$ be the sets of roots and coroots respectively. Then the quadruple $\mathcal{R} = (M, R, M^\vee, R^\vee)$ is a root datum. It is called the* type *of G.*

PROOF. This follows from the results in Th. 43.1 and Prop. 44.2, just as in the case where S is the spectrum of an algebraically closed field. $\square$

REMARK 44.8. So far, we have achieved part of Grothendieck's 1960 program mentioned in Section 39: taking the "weaker" definition of reductive group schemes, we have proved that they are étale-locally isomorphic to a group $\mathcal{G}(\mathcal{R})$ possessing a root datum $\mathcal{R}$. We will see in the next lecture that $\mathcal{G}(\mathcal{R})$ is unique up to isomorphism and comes from a "split Chevalley group" defined over $\mathbb{Z}$.