EXPOSÉ XXV

LE THÉORÈME D'EXISTENCE

par M. DEMAZURE

⁽⁰⁾ Pour être complet, nous donnons dans cet exposé une démonstration du théo- 410
rème d'existence des groupes déployés. Comme la démonstration originale de Cheval-
ley (« *Sur certains schémas de groupes semi-simples* », Séminaire Bourbaki, Mai 1961,
n°219), elle s'appuie sur l'existence de groupes algébriques semi-simples complexes de
tous les types possibles. Le principe d'une démonstration plus satisfaisante, prouvant
directement l'existence d'un $\mathbb{Z}$ -groupe semi-simple déployé simplement connexe cor-
respondant à une matrice de Cartan donnée a été donné par Cartier (non publié). ⁽¹⁾
Signalons cependant que la difficulté n'est pas de donner une construction explicite
d'un schéma en groupes, mais de vérifier que le groupe ainsi construit répond bien
aux conditions exigées, c'est-à-dire essentiellement que ses fibres sont bien lisses et
réductives.

1. Énoncé du théorème

Théorème 1.1. — Soit S un schéma non vide. Le foncteur

$$G \mapsto \mathcal{R}(G)$$

est une équivalence de la catégorie des S -groupes réductifs épinglés avec la catégorie
des données radicielles réduites épinglées.

En vertu du théorème d'unicité (Exp. XXIII, 4.1), l'énoncé précédent équivaut à : 411

Corollaire 1.2 (Existence de groupes déployés). — Pour toute donnée radicielle réduite
 $\mathcal{R}$, il existe un $\mathbb{Z}$ -groupe réductif déployé G tel que $\mathcal{R}(G) \simeq \mathcal{R}$. ⁽²⁾

⁽⁰⁾N.D.E. : Version du 13/10/2024

⁽¹⁾N.D.E. : Un tel principe a aussi été esquissé par B. Kostant [Ko66] ; une démonstration complète,
utilisant les groupes quantiques, a été donnée récemment par G. Lusztig [Lu09].

⁽²⁾N.D.E. : Signalons aussi que l'ouvrage [BT84] de F. Bruhat et J. Tits contient une variante de
la construction de Chevalley (*loc. cit.*, 2.2.3–2.2.5 et §3.2), qui fournit en particulier un $\mathbb{Z}$ -groupe
lisse affine à fibres connexes G , possédant un tore maximal déployé, et dont la fibre générique est
un $\mathbb{Q}$ -groupe réductif de type $\mathcal{R}$; le fait que les fibres géométriques de G sont réductives découle de
l'étude du radical unipotent d'une fibre spéciale faite dans *loc. cit.*, 4.6.12 et 4.6.15 (valables pour des

En particulier :

Corollaire 1.3. — *Soit k un corps. Pour tout k -groupe réductif déployable G_k , il existe un $\mathbb{Z}$ -groupe réductif G tel que $G \otimes_{\mathbb{Z}} k \simeq G_k$.*

Réciproquement, remarquons d'abord que pour prouver 1.2, il suffit par Exp. XXII 4.3.1 et Exp. XXI 6.5.10, de considérer le cas où la donnée radicielle $\mathcal{R}$ est simplement connexe (et même irréductible si on y tient, par Exp. XXI, 7.1.6).

D'autre part, sous les conditions de 1.3, le schéma en groupes G est de type constant (car $\text{Spec}(\mathbb{Z})$ est connexe) donc de type $\mathcal{R}(G_k)$; par Exp. XXIII, 5.9, il s'ensuit que la validité de 1.3 pour un groupe G_k donné entraîne l'existence d'un $\mathbb{Z}$ -groupe *déployé* de type $\mathcal{R}(G_k)$.⁽³⁾

Pour démontrer 1.2 et donc 1.1, il suffit donc de prouver 1.3 lorsque k est de caractéristique nulle (par exemple $k = \mathbb{C}$) et G_k simplement connexe (et en particulier semi-simple), ainsi que :

Proposition 1.4. — *Pour toute donnée radicielle réduite simplement connexe $\mathcal{R}$, il existe un $\mathbb{C}$ -groupe algébrique semi-simple de type $\mathcal{R}$.*

On peut prouver 1.4 de la manière suivante. On sait d'abord qu'il existe une algèbre de Lie semi-simple complexe $\mathfrak{g}$ de type $\mathcal{R}$, cf. par exemple, N. Jacobson, *Lie Algebras*, ch. VII, Th. 5.⁽⁴⁾ Alors $G = \text{Aut}(\mathfrak{g})^0$ est un $\mathbb{C}$ -groupe algébrique semi-simple de type $\text{ad}(\mathcal{R})$.⁽⁵⁾ Par *Bible*, § 23.1, prop. 1, on en déduit l'existence d'un $\mathbb{C}$ -groupe semi-simple de type $\mathcal{R}$.

Le reste de cet exposé est consacré à la démonstration de 1.3 pour k de caractéristique nulle et G_k semi-simple. Celle-ci se fera en deux temps : construction d'un « morceau de $\mathbb{Z}$ -schéma en groupes » (n°2), étude du groupe obtenu par application du « théorème de Weil » (n°3).

G plus généraux, associés à une donnée radicielle valuée), mais il est plus simple de le déduire de la description de $\mathfrak{g} = \text{Lie}(G)$, de Exp. XIX 1.12 (iii) et de l'existence des éléments $w_\alpha(X)$ de Exp. XX 3.1 (iv) (cf. [BT84], 3.2.1).

⁽³⁾N.D.E. : En fait, Exp. XXIII, 5.9 n'est pas nécessaire car le présent exposé construit, pour tout $\mathbb{Q}$ -groupe semi-simple $G_{\mathbb{Q}}$, un $\mathbb{Z}$ -groupe semi-simple G de même type que $G_{\mathbb{Q}}$ et muni d'un tore maximal déployé T ; donc, d'après Exp. XXII 2.2, G est déployé.

⁽⁴⁾N.D.E. : Soient Δ une base de R et $\tilde{\mathfrak{g}}$ la $\mathbb{C}$ -algèbre de Lie engendrée par des générateurs $(e_\alpha, f_\alpha, h_\alpha)_{\alpha \in \Delta}$ soumis aux relations $[h_\alpha, h_\beta] = 0$, $[e_\alpha, f_\beta] = h_\alpha$ si $\beta = \alpha$ et $= 0$ sinon, $[h_\alpha, e_\beta] = (\alpha^*, \beta)e_\beta$ et $[h_\alpha, f_\beta] = -(\alpha^*, \beta)f_\beta$. Dans *loc. cit.*, $\mathfrak{g}$ est définie comme le quotient de $\tilde{\mathfrak{g}}$ par l'intersection des noyaux des représentations irréductibles de dimension finie de $\tilde{\mathfrak{g}}$; dans [Se66], § VI.5, Th. 9 (voir aussi [BLie], VIII, § 4.3, Th. 1) il est montré que $\mathfrak{g}$ est le quotient de $\tilde{\mathfrak{g}}$ par les relations $\text{ad}(e_\alpha)^{1-(\alpha^*, \beta)}(e_\beta) = 0$ et $\text{ad}(f_\alpha)^{1-(\alpha^*, \beta)}(f_\beta) = 0$. Pour une description explicite des constantes de structure (en particulier le choix des signes), voir Exp. XXIII 6.5 et 6.7 ainsi que [Ti66], § 4, Th. 1 et (pour les types A,D,E) [Sp98], 10.2.5.

⁽⁵⁾N.D.E. : On peut supposer $\mathcal{R}$ irréductible, donc $\mathfrak{g}$ simple. Par un argument général, on sait que $\text{Lie}(G)$ est la $\mathbb{C}$ -algèbre de Lie des dérivations de $\mathfrak{g}$ (cf. [DG70], § II.4, Prop. 2.3), or celles-ci sont toutes intérieures (cf. [BLie], I § 6.1, cor. 3 de la prop. 1), donc $\text{Lie}(G) = \mathfrak{g}$; par conséquent G n'a pas de sous-groupe invariant de dimension > 0 , donc G est semi-simple. Son système de racines est alors le même que celui de $\mathfrak{g}$; de plus le centre de G agit à la fois trivialement et fidèlement sur $\mathfrak{g}$, donc est trivial, donc G est adjoint.

Pour éviter des confusions, nous n'utiliserons pas dans le numéro 2 la notation abrégée X_k pour désigner le k -schéma $X \otimes_{\mathbb{Z}} k$, où X est un $\mathbb{Z}$ -schéma. 412

2. Théorème d'existence : construction d'un morceau de groupe

2.1. — Choisissons une fois pour toutes un déploiement de G_k , noté

$$(G_k, T_k, M, R)$$

(cf. Exp. XXII, 1.13), un système de racines simples Δ de R (définissant le système de racines positives R_+), un système de Chevalley $(X_{\alpha,k})_{\alpha \in R}$ de G_k (Exp. XXIII, 6.1 et 6.2) vérifiant la condition supplémentaire suivante (cf. XX 2.6) : pour tout $\alpha \in R$, on a

$$X_{\alpha,k} X_{-\alpha,k} = 1.$$

Choisissons enfin sur le sous-groupe de M engendré par R une relation d'ordre total compatible avec la structure de groupe, telle que les racines > 0 soient les éléments de R_+ . On note alors les racines

$$-\alpha_n < -\alpha_{n-1} < \dots < -\alpha_1 < \alpha_1 < \alpha_2 < \dots < \alpha_n.$$

Pour $\alpha \in R$, on note $U_{\alpha,k}$ le groupe vectoriel correspondant à la racine α et

$$p_{\alpha,k} : \mathbb{G}_{a,k} \xrightarrow{\sim} U_{\alpha,k}$$

l'isomorphisme de groupes vectoriels défini par $X_{\alpha,k}$.

2.2. — Le déploiement de G_k comporte en particulier un isomorphisme de k -groupes

$$T_k \simeq D_k(M).$$

Posons $T = D(M)$; c'est un $\mathbb{Z}$ -tore, et on peut considérer l'isomorphisme précédent comme un isomorphisme 413

$$T_k \simeq T \otimes_{\mathbb{Z}} k.$$

On a

$$\text{Hom}_{\mathbb{Z}\text{-gr.}}(T, \mathbb{G}_m) = M,$$

et on considérera les éléments de $R \subset M$ comme des caractères de T . On considérera de même les éléments de R^* comme des morphismes de $\mathbb{Z}$ -groupes $\mathbb{G}_m \rightarrow T$.

2.3. — Pour chaque $\alpha \in R_+$, soit $\mathbb{G}_a(\alpha)$ une copie du groupe $\mathbb{G}_a$; considérons le $\mathbb{Z}$ -schéma

$$U = \mathbb{G}_a(\alpha_1) \times \dots \times \mathbb{G}_a(\alpha_n).$$

Si U_k désigne la partie unipotente du groupe de Borel B_k de G_k défini par R_+ , notons

$$a : U \otimes_{\mathbb{Z}} k \xrightarrow{\sim} U_k$$

l'isomorphisme de k -schémas défini par

$$a(x_1, \dots, x_n) = p_{\alpha_1,k}(x_1) \cdots p_{\alpha_n,k}(x_n).$$

2.4. — La loi de groupe de U_k se traduit par des relations de la forme

$$a(x_1, \dots, x_n) \cdot a(y_1, \dots, y_n) = a(z_1, \dots, z_n),$$

où chaque z_h ($h = 1, \dots, n$) s'exprime comme un polynôme

$$z_h = x_h + y_h + Q_h(x_1, \dots, x_{h-1}, y_1, \dots, y_{h-1}),$$

les coefficients de Q_h étant *entiers* (Exp. XXII, 5.5.8 et Exp. XXIII, 6.4). De plus $Q_h(x_1, \dots, x_{h-1}, 0, \dots, 0) = 0$.

414 Munissons U de la loi composition définie par les formules précédentes (qui sont bien « définies sur $\mathbb{Z}$ »). Comme cette loi induit sur U_k sa loi de groupe, elle est associative, et (0) en est un élément unité (en effet, les deux assertions précédentes s'expriment par des relations entre les polynômes Q_h , et $\mathbb{Z} \rightarrow k$ est injectif). Montrons que c'est une loi de groupe : si (x_i) est une section de U (sur un S quelconque), on calcule l'inverse (y_i) de (x_i) par les formules récurrentes :

$$y_i = -x_i - Q_i(x_i, \dots, x_{i-1}, y_1, \dots, y_{i-1})$$

qui sont encore « définies sur $\mathbb{Z}$ ».

En résumé, nous avons construit sur U une loi de groupe telle que l'isomorphisme a précédent soit un isomorphisme de groupes.

Pour chaque $\alpha \in R_+$, considérons le morphisme

$$p_\alpha : \mathbb{G}_a \longrightarrow U$$

défini par $p_\alpha(x) = (x_i)$ où $\begin{cases} x_i = x & \text{si } \alpha_i = \alpha \\ x_i = 0 & \text{si } \alpha_i \neq \alpha. \end{cases}$

C'est une immersion fermée et un homomorphisme de groupes ; on note U_α son image. On a $(x_i) = p_{\alpha_1}(x_1) \cdots p_{\alpha_n}(x_n)$, ce qui prouve que U s'identifie au produit

$$U = U_{\alpha_1} \cdot U_{\alpha_2} \cdots U_{\alpha_n}.$$

2.5. — Faisons opérer $T = D(M)$ sur chaque U_α par l'intermédiaire du caractère α ; on vérifie aussitôt que cela définit une opération de T sur le groupe U et on peut construire le produit semi-direct $B = T \cdot U$. On a un isomorphisme canonique de k -groupes

$$B \otimes_{\mathbb{Z}} k \xrightarrow{\sim} B_k.$$

415 Si nous prenons maintenant un ordre *quelconque* sur R_+ , le morphisme

$$\prod_{\alpha \in R_+} U_\alpha \longrightarrow U$$

défini par le produit dans U est encore un isomorphisme. En effet, comme les deux membres sont des $\mathbb{Z}$ -schémas plats et de présentation finie, on peut se contenter de vérifier l'assertion sur les fibres géométriques ; on est alors ramené à la théorie de Lazard (*Bible*, § 13.1, prop. 1) : on considère U comme groupe à opérateurs T , et on utilise le fait que les U_α sont deux à deux non isomorphes comme groupes à opérateurs (car les caractères $\alpha \in R_+$ de T sont deux à deux distincts sur chaque fibre).

2.6. — Remplaçant R_+ par $R_- = -R_+$, on construit de même des groupes U^-, B^-, U_α ($\alpha \in R_-$) et des isomorphismes

$$p_\alpha : \mathbb{G}_a \xrightarrow{\sim} U_\alpha, \quad \alpha \in R_-.$$

Introduisons enfin le schéma produit

$$\Omega = U^- \times T \times U;$$

on a un isomorphisme canonique de k -schémas

$$\Omega \otimes_{\mathbb{Z}} k \xrightarrow{\sim} U_k^- \times_k T_k \times_k U_k \simeq \Omega_k,$$

où Ω_k est la « grosse cellule » de G_k (Exp. XXII, 4.1.2).

À partir de maintenant, nous identifions $\Omega \otimes_{\mathbb{Z}} k$ à Ω_k par l'isomorphisme précédent ; nous considérons U^-, T, U comme des sous-schémas de Ω , par l'intermédiaire des sections unités. On note $\underline{e} = ((0), e, (0))$ la « section unité » de Ω .

Notre but est maintenant de mettre une loi de morceau de groupe sur Ω .

Lemme 2.7. — Soit $\alpha \in \Delta$, et soit $w_{\alpha,k}$ l'élément de $\text{Norm}_{G_k}(T_k)(k)$ défini par $X_{\alpha,k}$ 416 (rappelons que l'on a par définition

$$w_{\alpha,k} = p_{-\alpha,k}(-1)p_{\alpha,k}(1)p_{-\alpha,k}(-1).$$

Il existe un ouvert V_α de Ω , contenant la section $\underline{e}$, et un morphisme

$$h_\alpha : V_\alpha \longrightarrow \Omega,$$

vérifiant les conditions suivantes :

- (i) $h_\alpha(\underline{e}) = \underline{e}$,
- (ii) $(h_\alpha) \otimes_{\mathbb{Z}} k$ coïncide avec la restriction de $\text{int}(w_{\alpha,k})$ à $V_\alpha \otimes_{\mathbb{Z}} k \subset G_k$.
- (iii) On a $T \subset V_\alpha$ et h_α envoie T dans T . Pour tout $\beta \in R$, on a $U_\beta \subset V_\alpha$ et h_α envoie U_β dans $U_{s_\alpha(\beta)}$.

En vertu de la définition d'un système de Chevalley (Exp. XXIII, 6.1), il existe pour chaque $\beta \in R$ un entier $e_\beta = \pm 1$ tel que

$$\text{int}(w_{\alpha,k})p_{\beta,k}(x) = p_{s_\alpha(\beta),k}(e_\beta x)$$

pour tout $x \in \mathbb{G}_a(S)$, $S \rightarrow \text{Spec}(k)$.

Soit S un schéma quelconque, écrivons un élément quelconque de $\Omega(S)$ sous la forme

$$u = \left(\left(\prod_{\substack{\beta \in R_- \\ \beta \neq -\alpha}} p_\beta(x_\beta) \right) \cdot p_{-\alpha}(x_{-\alpha}), \quad t, \quad p_\alpha(x_\alpha) \cdot \left(\prod_{\substack{\beta \in R_+ \\ \beta \neq \alpha}} p_\beta(x_\beta) \right) \right),$$

où on a choisi un ordre (quelconque) sur $R_- - \{-\alpha\}$ et $R_+ - \{\alpha\}$ (cf. 2.5).

On définit un morphisme $d : \Omega \rightarrow \text{Spec}(\mathbb{Z})$ par

$$d(u) = \alpha(t) + x_\alpha x_{-\alpha}.$$

Soit V_α l'ouvert Ω_d (c'est-à-dire l'ouvert de Ω défini par « $d(u)$ inversible »); il contient $\underline{e}$, T , et chaque U_β , $\beta \in R$. Soit

$$h_\alpha : V_\alpha \longrightarrow \Omega$$

le morphisme défini par $h_\alpha(u) = (a(u), b(u), c(u))$ où

$$a(u) = \left(\prod_{\substack{\beta \in R_- \\ \beta \neq -\alpha}} p_{s_\alpha(\beta)}(e_\beta x_\beta) \right) \cdot p_{-\alpha}(-x_\alpha d(u)^{-1})$$

$$b(u) = t \cdot \alpha^*(d(u)),$$

$$c(u) = p_\alpha(-x_{-\alpha} d(u)^{-1}) \cdot \left(\prod_{\substack{\beta \in R_+ \\ \beta \neq \alpha}} p_{s_\alpha(\beta)}(e_\beta x_\beta) \right).$$

Comme s_α permute les racines positives (resp. négatives) distinctes de α (resp. $-\alpha$), alors $c(u)$ (resp. $a(u)$) est une section de U (resp. U^-) et le morphisme précédent est bien défini. Il vérifie trivialement (i) et (iii). Quant à (ii), cela résulte aussitôt de la définition des e_β , $\beta \in R$, et de Exp. XX, 3.12.

Lemme 2.8. — *Il existe des ouverts V et V' de Ω et des morphismes*

$$h : V \longrightarrow \Omega, \quad h' : V' \longrightarrow \Omega,$$

vérifiant les conditions suivantes :

- (i) V et V' contiennent $\underline{e}$, et $h(\underline{e}) = h'(\underline{e}) = \underline{e}$.
- 418 (ii) *Le morphisme induit par $h' \circ h : h^{-1}(V') \rightarrow \Omega$ est la restriction du morphisme identique.*
- (iii) *Les k -morphismes $h \otimes_{\mathbb{Z}} k$ et $h' \otimes_{\mathbb{Z}} k$ sont la restriction à $V \otimes_{\mathbb{Z}} k$ et $V' \otimes_{\mathbb{Z}} k$ d'automorphismes du groupe G_k .*
- (iv) V et V' contiennent U , T et U^- ; h et h' envoient U dans U^- , U^- dans U , et T dans T .

Soit $\bar{w}_0$ l'élément du groupe de Weyl de G_k qui transforme R_+ en R_- . Écrivons

$$\bar{w}_0 = s_{\alpha_n} \cdots s_{\alpha_1}, \quad \alpha_i \in \Delta$$

(aucun rapport avec la numérotation de 2.1). Posons

$$w_0 = w_{\alpha_n, k} \cdots w_{\alpha_1, k} \in \underline{\text{Norm}}_{G_k}(\Gamma_k)(k).$$

Définissons par récurrence sur $i \leq n$ un ouvert V_i de Ω et un morphisme $h_i : V_i \rightarrow \Omega$ par $V_0 = \Omega$, $h_0 = \text{id}$, et, pour $i = 0, \dots, n-1$,

$$V_{i+1} = h_i^{-1}(V_{\alpha_{i+1}}), \quad h_{i+1} = h_{\alpha_{i+1}} \circ h_i,$$

où les notations V_{α_j} et h_{α_j} sont celles de 2.7.

Prenons $V = V_n$ et $h = h_n$. Les conditions de (i), (iii) et (iv) portant sur V et h sont bien vérifiées ; pour (i) et (iii) cela résulte aussitôt de 2.8, pour (iv), de ce que $h \otimes_{\mathbb{Z}} k$ est la restriction de $\text{int}(w_0)$ à $V \otimes_{\mathbb{Z}} k$.

Comme $(\bar{w}_0)^2 = 1$, on a aussi

$$\bar{w}_0 = s_{\alpha_1} \cdots s_{\alpha_n} = (s_{\alpha_1}^3) \cdots (s_{\alpha_n}^3).$$

Posant

$$w'_0 = (w_{\alpha_1, k})^3 \cdots (w_{\alpha_n, k})^3,$$

419

et effectuant la même construction que ci-dessus, on en déduit un ouvert V' et un morphisme h' vérifiant également (i), (iii), (iv). De plus, $h' \otimes_{\mathbb{Z}} k$ est la restriction de $\text{int}(w'_0)$ à $V' \otimes_{\mathbb{Z}} k$. Mais pour chaque racine simple $\alpha \in \Delta$, on a $(w_{\alpha, k})^4 = e$ (cf. Exp. XX, 3.1), donc $w'_0 \cdot w_0 = e$, ce qui montre que $h' \circ h$ induit le morphisme identique dans un ouvert non vide de $\Omega \otimes_{\mathbb{Z}} k$. Mais Ω étant lisse et de présentation finie sur $\mathbb{Z}$, $\Omega \otimes_{\mathbb{Z}} k$ est schématiquement dense dans Ω , ce qui prouve (ii).

Proposition 2.9. — *Il existe un ouvert V_1 de $\Omega \times \Omega$, un ouvert V_2 de Ω , des morphismes*

$$\pi : V_1 \longrightarrow \Omega, \quad \sigma : V_2 \longrightarrow \Omega,$$

possédant les propriétés suivantes :

(i) *Si $x \in \Omega(S)$, alors $(\underline{e}, x)$ et $(x, \underline{e})$ sont des sections de V_1 et*

$$\pi(\underline{e}, x) = \pi(x, \underline{e}) = x.$$

(ii) *V_2 contient $\underline{e}$ et $\sigma(\underline{e}) = \underline{e}$.*

(iii) *π_k et σ_k sont la restriction des morphismes $G_k \times_k G_k \rightarrow G_k$ et $G_k \rightarrow G_k$ définis par le produit (resp. l'inverse).*

Démonstration. Soient (v, t, u) et (v', t', u') deux sections de Ω . Alors $h(u)$ est une section de U^- , $h(v')$ est une section de U par 2.8 (iv) et on peut donc considérer $(h(u), e, h(v'))$ comme une section de Ω . Soit V_1 l'ouvert de $\Omega \times \Omega$ défini par la condition :

$$((v, t, u), (v', t', u')) \in V_1(S) \iff (h(u), e, h(v')) \in V'(S)$$

(notations de 2.8). Si $((v, t, u), (v', t', u'))$ est une section de V_1 , alors $h'(h(u), e, h(v'))$ est défini ; c'est une section de Ω que l'on peut décomposer : 420

$$h'(h(u), e, h(v')) = (v'', t'', u'').$$

On pose alors

$$\pi((v, t, u), (v', t', u')) = (v \cdot tv''t^{-1}, tt''t', t'^{-1}u''t' \cdot u').$$

La vérification de (i) est immédiate (par 2.8 (ii)). Pour vérifier la condition de (iii) portant sur π , on voit que

$$h'(h(u), e, h(v')) = uv' = v''t''u''$$

lorsque $u \in U(S)$, $v \in U^-(S)$, $S \rightarrow k$, en vertu de 2.8 (iii) et (ii). On construit σ de manière semblable : si (v, t, u) est une section de Ω , $h(u^{-1})$ est une section de U^- ,

$h(v^{-1})$ une section de U , $h(t^{-1})$ une section de T , donc $(h(u^{-1}), h(t^{-1}), h(v^{-1}))$ est une section de Ω et on peut définir un ouvert V_2 de Ω par

$$(v, t, u) \in V_2(S) \iff (h(u^{-1}), h(t^{-1}), h(v^{-1})) \in V'(S)$$

et un morphisme $\sigma : V_2 \rightarrow \Omega$ par

$$\sigma(v, t, u) = h'(h(u^{-1}), h(t^{-1}), h(v^{-1})).$$

On vérifie les conditions sur σ comme ci-dessus.

Corollaire 2.10. — π est « génériquement associatif » et σ est un « inverse générique » : si $x, y, z \in \Omega(S)$ et si les expressions ci-dessous sont définies (ce qui se produit toujours au-dessus d'un ouvert de Ω contenant la section unité), on a :

$$\pi(x, \pi(y, z)) = \pi(\pi(x, y), z), \quad \pi(x, \sigma(x)) = \underline{e} = \pi(\sigma(x), x).$$

421 En effet, les deux membres de chacune de ces formules définissent des morphismes entre $\mathbb{Z}$ -schémas lisses et de présentation finie, qui coïncident sur les fibres génériques, par 2.10 (iii).

Corollaire 2.11. — Soit $\alpha \in \mathbb{R}$. Pour tout S et tous $x, y \in \mathbb{G}_\alpha(S)$ tels que $(p_\alpha(x), p_{-\alpha}(y)) \in V_1(S)$ et $1+xy \in \mathbb{G}_m(S)$ (ce qui définit un ouvert de $\mathbb{G}_{\alpha,S}^2$ contenant la section $(0, 0)$), on a :

$$\pi(p_\alpha(x), p_{-\alpha}(y)) = \left(p_{-\alpha} \left(\frac{y}{1+xy} \right), \alpha^*(1+xy), p_\alpha \left(\frac{x}{1+xy} \right) \right).$$

La démonstration est la même que précédemment, par Exp. XX, 2.1.

3. Théorème d'existence : fin de la démonstration

Posons pour simplifier le langage la définition suivante.

Définition 3.1. — Soient S un schéma et G un S -schéma en groupes. On dit que G est *admissible* s'il existe une immersion ouverte de S -schémas $i : \Omega_S = \Omega \times S \rightarrow G$ vérifiant les conditions suivantes :

(i) Le diagramme

$$\begin{array}{ccc} (V_1)_S & \longrightarrow & \Omega_S \times_S \Omega_S \xrightarrow{i \times_S i} G \times_S G \\ \downarrow \pi & & \downarrow \pi_G \\ \Omega_S & \xrightarrow{i_S} & G, \end{array}$$

où l'on note π_G le morphisme de multiplication dans G , est commutatif.

(ii) Il existe un ensemble fini de sections $a_j \in \Omega(S)$ tel que les $i(a_j) \cdot i(\Omega_S)$ recouvrent G .

422 Par le « théorème de Weil » (Exp. XVIII, 3.13 (iii) et (iv)), on a :

Lemme 3.2. — Si pour tout schéma S étale et de type fini sur $\mathbb{Z}$, tout S -groupe admissible est affine, alors il existe un $\mathbb{Z}$ -groupe admissible et affine.

Or on a :

Lemme 3.3. — *Soient S un schéma et G un S -groupe admissible. Alors G est lisse et de présentation finie sur S , à fibres affines connexes et semi-simples.*

Comme Ω_S est lisse et de présentation finie sur S , à fibres connexes, il en est de même pour G , en vertu de la condition (ii). Pour vérifier 3.3, on peut donc supposer que S est le spectre d'un corps K . Identifions Ω_K à son image dans G . Il est clair que Ω_K est le produit

$$\prod_{\alpha \in \mathbb{R}_-} U_{\alpha, K} \cdot T_K \cdot \prod_{\alpha \in \mathbb{R}_+} U_{\alpha, K}$$

des sous-groupes T_K et $U_{\alpha, K}$ ($\alpha \in \mathbb{R}$) de G . L'algèbre de Lie de G s'identifie donc à la somme directe

$$\text{Lie}(T_K) \oplus \prod_{\alpha \in \mathbb{R}} \text{Lie}(U_{\alpha, K}).$$

Comme l'automorphisme intérieur défini par une section de T_K opère dans $U_{\alpha, K}$, et donc dans $\text{Lie}(U_{\alpha, K})$, par l'intermédiaire du caractère

$$\alpha \in \mathbb{R} \subset M \simeq \text{Hom}_{K\text{-gr.}}(T_K, \mathbb{G}_m, K),$$

la décomposition précédente de $\text{Lie}(G)$ est exactement la décomposition sous l'opération adjointe de T . Les racines de $\mathbb{G}_K$ par rapport à T_K sont donc les $\alpha \in \mathbb{R}$. Appliquons Exp. XIX, 1.13. Soit T_α le tore maximal de $\text{Ker}(\alpha) \subset T_K$ et soit $Z_\alpha = \underline{\text{Centr}}_G(T_\alpha)$; il nous suffit de prouver que chaque Z_α est réductif. Or $Z_\alpha \cap \Omega_K$ n'est autre que

$$\prod_{\substack{\beta \in \mathbb{R}_- \\ \beta|_{T_\alpha} = e}} U_{\beta, K} \cdot T_K \cdot \prod_{\substack{\beta \in \mathbb{R}_+ \\ \beta|_{T_\alpha} = e}} U_{\beta, K};$$

mais les racines nulles sur T_α sont les multiples rationnels de α , donc α et $-\alpha$; ce qui 423 prouve

$$Z_\alpha \cap \Omega_K = U_{-\alpha, K} \cdot T_K \cdot U_{\alpha, K}.$$

Pour prouver que Z_α est réductif il suffit, en vertu de Exp. XX 3.4, de prouver que $U_{\alpha, K}$ et $U_{-\alpha, K}$ ne commutent pas, ce qui résulte aussitôt de 2.11.

Il résulte de 3.2 et 3.3 que la démonstration sera achevée si nous prouvons :

Lemme 3.4. — *Si S est un schéma localement noethérien de dimension ≤ 1 , et si G est un S -groupe lisse et de type fini, à fibres affines connexes et semi-simples, alors G est affine (et donc semi-simple).*

Nota. — Dans Exp. XVI, on a vu que 3.4 est vrai sans hypothèse sur S , mais la démonstration est relativement délicate; comme ici nous n'avons besoin que du cas particulier 3.4, nous en donnons une démonstration directe.

Considérons l'algèbre de Lie $\mathfrak{g}$ de G , qui est un $\mathcal{O}_S$ -module localement libre, et la représentation adjointe de G

$$\text{Ad} : G \longrightarrow \text{GL}_{\mathcal{O}_S}(\mathfrak{g}).$$

Pour prouver que G est affine sur S , il suffit de prouver que le morphisme Ad est affine. Comme G est lisse et à fibres connexes, il est séparé sur S (VI_B 5.5) donc le morphisme Ad est séparé. Utilisant un résultat démontré en appendice (voir 4.1), il suffit de prouver que le morphisme Ad est quasi-fini. On est donc ramené au cas où S est le spectre d'un corps ; en ce cas G est affine, donc semi-simple, et on est ramené à Exp. XXII 5.7.14.

4. Appendice

424

Nous avons utilisé en cours de démonstration la proposition suivante :

Proposition 4.1. — Soient S un schéma localement noethérien de dimension ≤ 1 , G et H deux S -schémas en groupes de type fini, $f : G \rightarrow H$ un morphisme de groupes quasi-fini et séparé. Si G est plat sur S , ⁽⁶⁾ alors f est affine.

Nous ne ferons la démonstration que dans le cas où G est lisse sur S , hypothèse qui est bien vérifiée dans l'application que nous avons faite de la proposition.

4.2. — Par EGA II, 1.6.4, on peut supposer S réduit. Par les techniques habituelles de passage à la limite, ⁽⁷⁾ on peut supposer S local. Si $\dim(S) = 0$, l'assertion est triviale, ⁽⁸⁾ supposons $\dim(S) = 1$. Par descente fidèlement plate, on peut supposer que S est complet à corps résiduel algébriquement clos. Quitte à remplacer S par son normalisé $\tilde{S}$, on peut (EGA II, 6.7.1 et EGA 0_{IV} 23.1.5) supposer S normal. ⁽⁹⁾ On est donc ramené au cas où S est le spectre d'un anneau de valuation discrète complet A à corps résiduel algébriquement clos.

4.3. — Soit η (resp. s) le point générique (resp. fermé) de S . Considérons l'image $f_\eta(G_\eta)$ de G_η dans H_η . C'est un sous-schéma en groupes fermé de H_η . Soit H' l'adhérence schématique dans H de $f_\eta(G_\eta)$. Comme $H' \rightarrow H$ est affine (c'est une immersion fermée), on peut remplacer H par H' et donc supposer H plat sur S et f_η surjectif. Comme f_η est fini, G et H plats sur S , on a

$$\dim(G_s) = \dim(G_\eta) = \dim(H_\eta) = \dim(H_s).$$

425

4.4. — Soient $H_s^0, \dots, H_s^n$ les composantes irréductibles de H_s , où H_s^0 désigne la composante neutre, et soient $z_0, \dots, z_n$ leurs points génériques. Comme chaque anneau local $\mathcal{O}_{H, z_i}$ est de dimension ≤ 1 , le morphisme $G \times_H \mathcal{O}_{H, z_i} \rightarrow \mathcal{O}_{H, z_i}$ est affine car quasi-fini et séparé (cf. Exp. XVI, lemme 4.2), donc G est affine sur H au voisinage de z_i . Notant V le plus grand ouvert de H tel que $G|_V$ soit affine sur V , il en résulte

⁽⁶⁾N.D.E. : Nous avons ajouté l'hypothèse de platitude qui avait été omise.

⁽⁷⁾N.D.E. : cf. EGA IV₃, 8.10.5 (viii).

⁽⁸⁾N.D.E. : En effet, si $S = \text{Spec}(k)$ (k un corps), alors f est la composée de la projection $p : G \rightarrow G/\text{Ker}(f)$ et d'une immersion fermée i , et comme $\text{Ker}(f)$ est fini sur k , alors p est fini (VI_B 9.2).

⁽⁹⁾N.D.E. : En effet, les composantes irréductibles $S_1, \dots, S_r$ de S sont des schémas locaux noethériens intègres complets donc, d'après un théorème de Nagata (cf. EGA 0_{IV}, 23.1.5) le normalisé $\tilde{S}_i$ est fini sur S_i , et donc $\tilde{S}$ est fini sur S . Alors, d'après un théorème de Chevalley (cf. EGA II, 6.7.1), si $f \times_S \tilde{S}$ est un morphisme affine, il en est de même de f .

que V contient tous les z_i ,⁽¹⁰⁾ donc contient au moins un point fermé $y_i \in H_s^i$ (et on a $\kappa(y_i) = \kappa(s)$ puisque $\kappa(s)$ est algébriquement clos).

D'autre part, V est évidemment stable par la translation définie par un élément quelconque $g \in G(S)$. Mais on a $\dim(G_s) = \dim(H_s)$ et f_s est fini, donc

$$f(s) : G_s^0(s) \longrightarrow H_s^0(s)$$

est surjectif. Comme A est complet et G lisse sur S , l'application canonique $G^0(S) \rightarrow G_s^0(s)$ est surjective; comme $H_s^0(s)$ opère transitivement dans chaque $H_s^i(s)$, il en résulte que $V \supset H_s(s)$, donc ($\kappa(s)$ étant algébriquement clos) $V \supset H_s$.⁽¹¹⁾

Comme on a évidemment $V \supset H_\eta$, puisque f_η est fini, on a donc $V = H$. C.Q.F.D.

Bibliographie

(12)

- [BLie] N. Bourbaki, *Groupes et algèbres de Lie*, Chap. I et VII-VIII, Hermann, 1960 et 1975.
- [BT84] F. Bruhat, J. Tits, *Groupes réductifs sur un corps local II. Schémas en groupes. Existence d'une donnée radicielle valuée*, Publ. Math. I.H.É.S. **60** (1984), 5-184.
- [DG70] M. Demazure, P. Gabriel, *Groupes algébriques*, Masson & North-Holland, 1970.
- [Ko66] B. Kostant, *Groups over $\mathbb{Z}$* , pp. 90-98 in : Algebraic groups and their discontinuous subgroups (eds. A. Borel & G. D. Mostow), Proc. Symp. Pure Math. IX, Amer. Math. Soc., 1966.
- [Lu09] G. Lusztig, *Study of a $\mathbb{Z}$ -form of the coordinate ring of a reductive group*, J. Amer. Math. Soc. **22** (2009), n°3, 739-769.
- [Se66] J.-P. Serre, *Algèbres de Lie semi-simples complexes*, Benjamin, 1966.
- [Sp98] T. A. Springer, *Linear algebraic groups*, 2nd ed., Birkhäuser, 1998.
- [Ti66] J. Tits, *Sur les constantes de structure et le théorème d'existence des algèbres de Lie semi-simples*, Publ. Math. I.H.É.S. **31** (1966), 21-58.

⁽¹⁰⁾N.D.E. : On a ajouté la phrase qui suit.

⁽¹¹⁾N.D.E. : Lorsque G n'est pas supposé lisse sur S , on peut procéder comme suit. Soient h_0 un point rationnel de H_s^0 et g_0 un point rationnel de G_s^0 tel que $f(g_0) = h_0$. D'après VI_B 5.6.1, il existe un diagramme commutatif

$$\begin{array}{ccc} S'' & \xrightarrow{g} & G \\ \pi \downarrow & \searrow \phi & \downarrow \\ S' & \xrightarrow{w} & S \end{array}$$

où w est étale et surjectif, π fini et surjectif, et $\phi^{-1}(s)$ est formé d'un seul point s'' tel que $g(s'') = g_0$. Alors le morphisme $G_{S''} \rightarrow H_{S''}$ est affine au-dessus d'un voisinage de $h_0 y_i$, et il en est de même de $G_{S'} \rightarrow H_{S'}$ (EGA II, 6.7.1) puis de $G \rightarrow H$ par descente fidèlement plate (EGA IV₂, 2.7.1 (xiii)). Donc $h_0 y_i \in V$, et il en résulte que V contient $H_s(s)$ et donc H_s .

⁽¹²⁾N.D.E. : références additionnelles citées dans cet Exposé.