Sur les points rationnels des groupes réductifs

Benoit Loisel

28 août 2014

Stage réalisé à l'Institut Camille Jordan, sous la direction de Bertrand Rémy

Table des matières

1 Préliminaires, définitions et notations

Le but de cette section est d'introduire les définitions et notations nécessaires dans toute la suite.

1.1 Action de Galois, action adjointe

Dans toute la suite, k désigne un corps quelconque. On note :
- k_s sa clôture séparable
- $\overline{k} = K$ sa clôture algébrique
- $\Gamma = \mathrm{Gal}(k_s/k)$
- $p = \mathrm{car}(k)$ sa caractéristique

Afin de répondre à des questions de rationalité, on utilise parfois des critères galoisiens. Définissons d'abord une action naturelle du groupe de Galois.

1.1.1 Définition (action de Galois)**.** Si V est un k-espace vectoriel, alors on peut définir une action de Γ sur $V_{k_s} = k_s \otimes V$ donnée pour $\gamma \in \Gamma, v \in V, a \in k$ par $\gamma \cdot a \otimes v = \gamma(a) \otimes v$ sur les tenseurs simples. On note $\gamma_V : V_{k_s} \to V_{k_s}$, l'application inversible $\gamma_V(w) = \gamma \cdot w$.

Si G est un groupe algébrique défini sur k dont A est l'algèbre de Hopf, alors on définit également une action de Γ sur G de la manière suivante : si $\gamma \in \Gamma$, pour toute k-algèbre R et tout $g \in G(R) = \mathrm{Hom}_{k-alg}(A, R)$, on pose $\gamma \cdot g = \gamma_R \circ g \circ \gamma_A^{-1}$.

1.1.2 Définition (Conjugaison et adjoint)**.** Soit G un groupe algébrique et H un sous-groupe de G. Le groupe G agit sur lui-même par automorphismes intérieurs. Soit $g \in G$. On définit l'application conjugaison par g par $\begin{array}{rccc} c_g : & G & \to & G \\ & h & \mapsto & ghg^{-1} \end{array}$, l'action est ainsi décrite par $g \cdot h = c_g(h)$. On note aussi $\mathrm{Int}(g) = c_g$.

On note ${}^gH$ l'image $c_g(H)$.

On définit l'application adjoint $\mathrm{Ad} : G \to gl(\mathfrak{g})$ par $\mathrm{Ad}(g) = d_e c_g : \mathfrak{g} \to \mathfrak{g}$.

La différentielle de cette application en l'identité $d_e\mathrm{Ad} = \mathrm{ad} : \mathfrak{g} \to gl(\mathfrak{g})$ correspond au crochet de Lie [Bor91, 3.14] : $\forall X \in \mathfrak{g} \forall Y \in \mathfrak{g}\, \mathrm{ad}(X)(Y) = [X, Y]$. Ce qui se vérifie par un calcul en plongeant G dans un GL_n.

Introduisons également quelques notations. Soit G un groupe algébrique et H un sous-groupe de G. On note $\mathcal{Z}_G(H) = \{g \in G\,,\, \forall h \in H\ ghg^{-1} = h\}$ le centralisateur de H dans G. On note $\mathcal{N}_G(H) = \{g \in G\,,\, {}^gH = H\}$ le normalisateur de H dans G. On note $\mathcal{Z}_G$ ou $\mathcal{C}G$ le centre de G, qui s'écrit aussi $Z_G(G)$.

1.2 Groupes diagonalisables et tores

Étant donné un groupe algébrique G, on note $X^*(G) = \mathrm{Mor}_{gr-alg}(G, \mathbb{G}_m)$ et $X_*(G) = \mathrm{Mor}_{gr-alg}(\mathbb{G}_m, G)$.

1.2.1 Définition. Un groupe algébrique G ayant A pour algèbre de Hopf est dit diagonalisable si $X^*(G)$ engendre A comme K-module.

1.2.2 Théorème ([Bor91, 8.12]). *Soit $\mathcal{A}$ la catégorie des k-groupes diagonalisables. Soit $\mathcal{B}$ la catégorie des $\mathbb{Z}$-modules de type fini, sans éléments de p-torsion et munis d'une action de Γ. Alors on a une équivalence de catégories donnée par $G \in \mathcal{A} \mapsto X^*(G) \in \mathcal{B}$*

1.2.3 Définition. Étant donné $n \in \mathbb{N}$, un tore de dimension n est un groupe algébrique isomorphe à $\mathbb{D}_n = (GL_1)^n$ ou, de manière équivalente, un groupe diagonalisable connexe de dimension n.

1.3 Sous-groupes de Borel, racines, donnée de groupes radiciels et radical

1.3.1 Définition (Radical et radical unipotent). Soit G un groupe algébrique connexe. On appelle radical de G, et on note $\mathcal{R}(G)$, le plus grand sous-groupe distingué fermé résoluble connexe de G. On appelle radical unipotent de G, et on note $\mathcal{R}_u(G)$, le plus grand sous-groupe distingué fermé unipotent connexe de G.

Soit G un groupe algébrique. On dit que G est semi-simple si $\mathcal{R}(G^\circ) = \{e\}$. On dit que G est réductif si $\mathcal{R}_u(G^\circ) = \{e\}$.

1.3.2 Définition. Soit G un groupe algébrique et B un sous-groupe de G. On dit que B est un sous-groupe de Borel de G s'il est maximal parmi les groupes sous-groupes connexes résolubles de G.

En utilisant le fait qu'un sous-groupe résoluble connexe laisse stable un drapeau (Théorème de Lie-Kolchin [Bor91, 10.5]), on peut montrer que les sous-groupes de Borel sont conjugués [Bor91, 11.1]. Tout tore maximal est un sous-groupe d'un sous-groupe de Borel, ils sont également conjugués [Bor91, 11.3].

1.3.3 Définition (Racines). Si G est un groupe algébrique connexe réductif et si T désigne un tore de G, alors T agit sur l'algèbre de Lie $\mathfrak{g}$ de G par la représentation adjointe $\mathrm{Ad} : T \to gl(\mathfrak{g})$ et on a la décomposition de $\mathfrak{g}$ en espaces propres $\mathfrak{g} = \bigoplus_{\alpha \in X^*(T)} \mathfrak{g}_\alpha$, où $\mathfrak{g}_\alpha = \{X \in \mathfrak{g}\,,\, \forall t \in T\, \mathrm{Ad}(t)(X) = \alpha(t)X\}$ [Spr98, 7.1.1].

On appelle racine de G tout élément $\alpha \in X^*(T) \setminus \{0\}$ tels que l'espace propre associé $\mathfrak{g}_\alpha$ est non nul.

On note $\Phi(G,T) \subset$ l'ensemble des racines ainsi définies.

1.3.4 Remarque. Si G n'est pas supposé réductif, on peut tout de même définir un ensemble de racines pour (G,T) en relevant celui du groupe réductif $G/\mathcal{R}_u(G)$. [Spr98, 7.4.3].

Il existe une notion abstraite de système de racines définie dans [Bou81, Chap.VI] que l'on utilisera.

1.3.5 Proposition (Systèmes de racines et groupe de Weyl). *Si G est un groupe algébrique connexe et si T est un tore maximal de G, alors $\Phi(G,T)$ est un système de racines [Spr98, 7.4.3].*

Le groupe $W(G,T) = \mathcal{N}_G(T)/\mathcal{Z}_G(T)$ est fini [Bor91, 11.19]. On peut le voir comme le groupe de Weyl du système de racines $\Phi(G,T)$ [Spr98, 8.1.3].

Si B est un sous-groupe de Borel de G contenant T, alors $\Phi(B,T)$ correspond aux racines positives $\Phi(G,T)^+$ du système de racines $\Phi(G,T)$ pour un certain ordre de système de racines [Spr98, 7.4.6]. Cela permet également de définir une base du système de racine, notée $D = D(G,T,B)$.

1.3.6 Définition et théorème (Groupes radiciels à un paramètre, d'après [Spr98, 8.1.1])**.** Soit G un groupe algébrique linéaire connexe réductif et T un tore maximal de G. Pour toute racine $\alpha \in \Phi(G,T)$, il existe un unique sous-groupe fermé normalisé par T de G, noté U_α tel qu'il existe au moins un isomorphisme $\varepsilon_\alpha : \mathbb{G}_a \to U_\alpha$ satisfaisant $\forall t \in T,\ \forall x \in K,\ t\varepsilon_\alpha(x)t^{-1} = \varepsilon_\alpha(\alpha(t)x)$.

De plus, chaque U_α est de dimension 1 et $\mathrm{Lie}(U_\alpha) = \mathfrak{g}_\alpha$. On les appelle groupes radiciels à un paramètre.

Le groupe G est engendré par T et les sous-groupes U_α.

1.3.7 Remarque. Chaque ε_α est unique à une constante de $\overline{k}$ près [Spr98, 7.3.3 (i)], une constante par racine.

1.4 Sous-groupes paraboliques

Lorsque le corps de base n'est pas algébriquement clos, l'existence d'un sous-groupe de Borel n'est pas assurée. On remplace alors ces derniers par les groupes paraboliques qui, bien que plus grand, permettent d'obtenir des résultats de point fixe d'une part, et répondent aux problèmes de corps de définition d'autre part.

1.4.1 Définition. Un sous-groupe P d'un groupe algébrique G est dit parabolique s'il est fermé et tel que la variété G/P est complète.

Soit G un groupe algébrique et L un sous-groupe fermé réductif de G. On dit que L est un sous-groupe de Levi de G si $G = L \ltimes \mathcal{R}_u(G)$ (produit semi-direct).

Deux sous-groupes paraboliques P et P^- d'un groupe algébrique G sont dit opposés si $L = P \cap P^-$ est un sous-groupe de Levi commun à P et P^-.

1.4.2 Proposition (Propriétés)**.**

- *[Tit65, 4.1] Soit G un groupe algébrique et P un sous-groupe fermé de G. Les assertions suivantes sont équivalentes :*
  - **(i)** *P est un sous-groupe parabolique*
  - **(ii)** *G/P est une variété projective*
  - **(iii)** *P contient un sous-groupe de Borel B de G*
- *[Bor91, 14.21 (i)] Soit P un sous-groupe parabolique d'un groupe algébrique G et L un sous-groupe de Levi de P. Alors il existe un unique sous-groupe parabolique P^- opposé à P ayant L comme sous-groupe de Levi commun.*

Soit G groupe réductif connexe, T tore maximal de G et B sous-groupe de Borel contenant T. Soit D la base associée à B du système de racines $\Phi(G,T)$. Pour toute partie $I \subset D$, on note $[I] = \mathbb{Z}I \cap \Phi(G,T)$ l'ensemble des racines obtenues comme combinaison linéaire à coefficients entiers d'éléments de I. On pose $\Phi(I)^+ =$

$\Phi(G,T)^+ \setminus [I]$. Soit $\Psi_I = [I] \cap \Phi(G,T)^+$. On définit $T_I = \left(\bigcap_{\alpha \in I} \ker \alpha \right)^\circ$ et $U_{\Phi(I)^+} = \prod_{\alpha \in I} U_\alpha$ (ordre du produit quelconque mais fixé). Soit $P_I = \mathcal{Z}_G(T_I) \cdot U_{\Phi(I)^+}$. C'est un sous-groupe parabolique de G et $\mathcal{Z}_G(T_I)$ en est un sous-groupe de Levi. Son radical unipotent est $\mathcal{R}_u(P_I) = U_{\Phi(I)^+}$ [Bor91, 14.17]. Son unique sous-groupe parabolique opposé par rapport à T est $P'_I = \mathcal{Z}_G(T_I) \cdot U_{-\Phi(I)^+}$ [Bor91, 14.20].

Tout sous-groupe parabolique est conjugué à un unique sous-groupe parabolique standard [Tit65, 4.3].

1.5 Données combinatoires

Les systèmes de Tits, également appelés BN-paires ont été introduit par Jacques Tits. Ils traduisent le lien avec la décomposition de Bruhat des groupes algébriques et peuvent servir à énoncer des résultats de simplicité modulo le centre du groupe.

1.5.1 Définition (Système de Tits)**.** Soit G un groupe abstrait. Considérons $\mathcal{T} = (G, B, N, S)$ un quadruplet tel que :

- B et N sont des sous-groupes de G.
- S est une partie de $W = N/T$ avec $T = N \cap B$.

On dit que $\mathcal{T}$ est un système de Tits s'il vérifie les quatre axiomes suivants :

(T1) G est engendré par B et N ; T est distingué dans N.

(T2) Les éléments de S sont d'ordre deux dans le groupe W, et l'engendrent.

(T3) $\forall w \in W \ \forall s \in S \ , sBw \subset BwB \cup BswB$

(T4) $\forall s \in S \ , sBs \neq B$

Les données radicielles indroduites par Michel Demazure constituent une généralisation des systèmes de racines. Elles permettent de déterminer un groupe réductif connexe déployé à isomorphisme près.

1.5.2 Définition (Donnée radicielle [Spr98, 7.4.1])**.** Soit $X, X^\vee$ deux groupes abéliens libres de rang fini duaux l'un de l'autre par une application $\mathbb{Z}$-linéaire, notons-la par $\langle , \rangle : X \otimes_{\mathbb{Z}} X^\vee \to \mathbb{Z}$ (on appelle couplage l'application correspondante $X \times X^\vee \to \mathbb{Z}$). Soit R et $R^\vee$ deux parties finies de X et $X^\vee$ respectivement, en bijection par une application $\iota : R \to R^\vee$. On note $\iota(\alpha) = \alpha^\vee$ pour tout $\alpha \in R$. Étant donné $\alpha \in R$, on définit les endomorphismes suivants :

$$s_\alpha : \begin{array}{ccc} X & \to & X \\ x & \mapsto & x - \langle x, \alpha^\vee \rangle \alpha \end{array} \quad \text{et} \quad s_\alpha^\vee : \begin{array}{ccc} X^\vee & \to & X^\vee \\ y & \mapsto & y - \langle \alpha, y \rangle \alpha^\vee \end{array} .$$

On dit que le quadruplet $\Psi = (X, R, X^\vee, R^\vee)$ est une donnée radicielle s'il vérifie les axiomes suivants :

(RD1) Pour tout $\alpha \in R$, on a $\langle \alpha, \alpha^\vee \rangle = 2$;

(RD2) Pour tout $\alpha \in R$, on a $s_\alpha(R) = R$ et $s_\alpha^\vee(R^\vee) = R^\vee$.

1.5.3 Exemple. Étant donné un tore T d'un groupe algébrique G, le groupe des caractères $X^*(T) = \mathrm{Hom}_{gr-alg}(T, \mathbb{G}_m)$ est naturellement en dualité avec le groupe des cocaractères $X_*(T) = \mathrm{Hom}_{gr-alg}(\mathbb{G}_m, T)$. Notons $\langle \cdot, \cdot \rangle$ le couplage correspondant. Ces deux groupes sont des candidats naturels à faire partie d'une donnée radicielle.

Le système de racines $\Phi(G,T)$ est une partie finie de $X^*(T)$. Si $\alpha \in \Phi(G,T)$, il existe un unique élément de $X_*(T)$, noté $\alpha^\vee$ tel que $\langle \alpha, \alpha^\vee \rangle = 2$. Les éléments ainsi obtenus sont appelés coracines et on note $\Phi(G,T)^\vee$ l'ensemble de ces éléments.

1.5.4 Proposition-définition (Donnée radicielle d'un groupe algébrique connexe [Spr98, 7.4.3])**.** Soit G un groupe algébrique connexe et T un tore maximal de G. Alors le quadruplet $(X^*(T), \Phi(G,T), X_*(T), \Phi(G,T)^\vee)$ est une donnée radicielle. On l'appelle donnée radicielle de G relative à T et on la note $\Psi(G,T)$.

1.5.5 Définition (Morphismes de données radicielles [Spr98, 9.6.1])**.**
Soit $\Psi_1 = (X_1, R_1, X_1^\vee, R_1^\vee)$ et $\Psi_2 = (X_2, R_2, X_2^\vee, R_2^\vee)$ des données radicielles. Soit $f : X_1 \to X_2$ un morphisme de $\mathbb{Z}$-modules. On définit par dualité un morphisme $f^\vee : X_2^\vee \to X_1^\vee$ par $\langle f(\alpha), \lambda \rangle = \langle \alpha, f^\vee(\lambda) \rangle$ pour tout $\alpha \in X_1$ et tout $\lambda \in X_2^\vee$. On dit que $f : X_1 \to X_2$ réalise un isomorphisme de Ψ_1 dans Ψ_2 si f est un isomorphisme de $\mathbb{Z}$-modules qui envoie R_1 sur R_2, et si son dual $f^\vee$ est un isomorphisme de $\mathbb{Z}$-modules qui envoie $R_2^\vee$ sur $R_1^\vee$.

1.5.6 Remarque. Soit G_1 et G_2 deux groupes réductifs connexes, ayant des tores maximaux notés T_1 et T_2 respectivement. S"il existe un isomorphisme de groupes algébriques $\varphi : G_1 \to G_2$ tel que $\varphi(T_1) = T_2$, alors $\begin{array}{ccc} X^*(T_2) & \to & X^*(T_1) \\ \alpha & \mapsto & \alpha \circ \varphi|_{T_1} \end{array}$ réalise un isomorphisme de données radicielles entre $\Psi(G_2, T_2)$ et $\Psi(G_1, T_1)$.

2 Théorème d'isomorphisme : le cas algébriquement clos

Ici on suppose que $k = \overline{k}$.

2.1 Énoncés et notations

Le but de cette section est donner une démonstration du théorème suivant :

2.1.1 Théorème. *Soit G et G' deux groupes algébriques semi-simples, T et T' des tores maximaux de G et G' respectivement et $\varphi_T : T \to T'$ un isomorphisme qui induit un isomorphisme de systèmes de racines* $\begin{array}{rccc} f : & \Phi(G',T') & \to & \Phi(G,T) \\ & \alpha & \mapsto & \alpha \circ \varphi_T \end{array}$. *Alors φ_T s'étend en un isomorphisme $\varphi : G \to G'$.*

On doit pouvoir raffiner en

2.1.2 Théorème. *[Spr98, 9.6.2] Soit G et G' deux groupes algébriques réductifs connexes, T et T' des tores maximaux de G et G' respectivement, Ψ et Ψ' les données radicielles correspondantes. On suppose qu'il existe $f : \Psi' \to \Psi$ un isomorphisme de données radicielles. Alors il existe un isomorphisme de groupes algébriques $\varphi : G \to G'$ tel que $\varphi(T) = T'$ et que f est un isomorphisme de données radicielles induit par φ.*

De plus, si φ' est un autre isomorphisme ayant de telles propriétés, alors il existe $t \in T$ tel que $\forall g \in G\ \varphi'(g) = \varphi(tgt^{-1})$.

Idée : on va étendre φ_T à des sous-groupes de G qui engendrent G et s'assurer que ces extensions soient cohérentes entre elles vis-à-vis des lois de groupes.

Mise en place des sous-groupes auxquels on va étendre les flèches initiales :

Comme G est réductif, on a $\mathcal{Z}_G(T) = T$ par [Spr98, 7.6.4 (ii)]. On note les normalisateurs $N = \mathcal{N}_G(T)$ et $N' = \mathcal{N}_{G'}(T')$.

On fixe un sous-groupe de Borel B de G contenant T, ce qui détermine une unique base, notée $D = D(G,T,B)$, de $\Phi(G,T)$. On pose $U = B_u$. On fixe un sous-groupe de Borel B' de G' contenant T', ce qui détermine une unique base, notée $D' = D(G',T',B')$, de $\Phi(G',T')$.

On note $W = W(G,T) = N/T$ (resp. $W' = W(G',T')$) ; on a des symétries s_α (resp. s'_α) telles que $W =< s_\alpha\ ,\ \alpha \in D >$. Pour α parcourant D, on fixe une famille $(n_\alpha)_\alpha$ d'éléments de N vérifiant $n_\alpha T = s_\alpha$ (resp. $s'_{\alpha'} = n'_{\alpha'}$).

Pour $\alpha, \beta \in D$, on note $m(\alpha,\beta)$ l'ordre de $s_\alpha s_\beta$ dans W. On pose $t_{\alpha\beta} = (n_\alpha n_\beta)^{m(\alpha,\beta)}$. On a $t_{\alpha\beta} \in Z_G(T) = T$. On pose $\forall \alpha \in D\ t_\alpha = t_{\alpha\alpha} = n_\alpha^2 \in T$.

Pour $\alpha \in \Phi(G,T)$, le groupe $T_\alpha = (\ker \alpha)^\circ$ est un sous-tore de codimension 1 de T. On pose $G_\alpha = Z_G(T_\alpha)$.

Les paramétrages des groupes radiciels ε_α [1.3.6] peuvent être choisis de sorte que pour tout $\alpha \in \Phi(G,T)$, l'élément $\varepsilon_\alpha(1)\varepsilon_{-\alpha}(-1)\varepsilon_\alpha(1) = n_\alpha \in N$ [Spr98, 8.1.4].

Pour toutes racines simples $\alpha, \beta \in D$, on note $G_{\alpha\beta} = \mathcal{Z}_G((T_\alpha \cap T_\beta)^\circ)$ et $U_{\alpha\beta} = U \cap G_{\alpha\beta}$. Les $G_{\alpha\beta}$ sont des groupes réductifs de rang semi-simple égal à 2, de système de racines noté $\Phi_{\alpha\beta}$ engendré par α et β [Hum98, 26.2 Cor.A]. On note $W_{\alpha,\beta}$ le groupe de Weyl correspondant.

2.2 Extension aux normalisateurs de tores maximaux

2.2.1 Proposition (d'après [Hum98, 32.2]). *Soit H un groupe algébrique. Soit $\psi : T \to H$ un homomorphisme de groupes abstraits. Soit $(h_\alpha)_{\alpha\in D}$ une famille d'éléments de H.*

Alors les assertions suivantes sont équivalentes :
(i) $\exists\widetilde{\psi} : \mathcal{N}_G(T) \to H$ *tel que* $\widetilde{\psi}|_T = \psi$ *et* $\forall\alpha \in D\ \widetilde{\psi}(n_\alpha) = h_\alpha$.
(ii) $\forall\alpha,\beta \in D\ (h_\alpha h_\beta)^{m(\alpha,\beta)} = \psi(t_{\alpha\beta})$.

Démonstration. « $\Rightarrow$ » :

$$\begin{array}{rcl} \forall\alpha,\beta \in D\ \psi(t_{\alpha\beta}) & = & \widetilde{\psi}((n_\alpha n_\beta)^{m(\alpha,\beta)}) \\ & = & (\widetilde{\psi}(n_\alpha)\widetilde{\psi}(n_\beta))^{m(\alpha,\beta)} \\ & = & (h_\alpha h_\beta)^{m(\alpha,\beta)} \end{array} .$$

« $\Leftarrow$ » :

Considérons W^* le groupe libre engendré par des éléments notés n^*_α , $\alpha \in D$. On a un homomorphisme de groupes $\begin{array}{rccc} \rho : & W^* & \to & \mathrm{Aut}(T) \\ & n^*_\alpha & \mapsto & (t \mapsto n_\alpha t n_\alpha^{-1}) \end{array}$. On peut donc définir le produit semi-direct pour cette action : $N^* = W^* \ltimes T$. On identifie T au sous-groupe $T^* = \{(1,t)\ ,\ t \in T\} \leq N^*$ par l'isomorphisme $j : t \mapsto (1,t)$; on pose $t^*_{\alpha\beta} = j(t_{\alpha\beta})$.

Considérons K^* le plus petit sous-groupe distingué de N^* contenant l'ensemble $\{(t^*_{\alpha\beta})^{-1}(n^*_\alpha n^*_\beta)^{m(\alpha,\beta)}\ ;\ \alpha,\beta \in D\} \subset N^*$ et le groupe quotient $\widetilde{N} = N^*/K^*$.

Le morphisme $\psi \circ j^{-1} : T^* \to H$ s'étend de manière unique en un morphisme $\psi^* : N^* \to H$ tel que $\forall\alpha \in D\ \phi^*(n^*_\alpha) = h_\alpha$. Les $(t^*_{\alpha\beta})^{-1}(n^*_\alpha n^*_\beta)^{m(\alpha,\beta)}$ sont dans $\ker\psi^*$ qui est distingué dans N^*, donc $K^* \leq \ker\psi^*$. On peut passer au quotient pour former un morphisme $\widetilde{\psi} : \widetilde{N} \to H$ tel que $\forall\alpha \in D\ \widetilde{\psi}(\widetilde{n_\alpha}) = h_\alpha$ où $\widetilde{n_\alpha}$ désigne la classe de n^*_α.

Il reste à montrer que $\begin{array}{rccc} \iota : & N & \to & \widetilde{N} \\ & n_\alpha & \mapsto & \widetilde{n_\alpha} \end{array}$ est un isomorphisme. Pour cela, il suffit alors de montrer que le morphisme surjectif entre $\widetilde{W} = \widetilde{N}/\widetilde{T}$ et $W = N/T$ est un isomorphisme. Le groupe $\widetilde{W}$ est engendré par les éléments $\widetilde{n_\alpha}\widetilde{T}$ pour α parcourant D. Ces éléments vérifient les mêmes relations que celles des éléments s_α de W correspondant. Or, (W,S) étant un système de Coxeter [Hum98, 29.4], ces groupes sont nécessairement fini, de même cardinal. Donc il s'agit bien d'un isomorphisme.

Ceci permet de conclure en considérant l'isomorphisme $\widetilde{\psi} \circ \iota : N \to H$ □

On choisira alors $H = G'$ et en étudiant les groupes ayant un système de racines de rang 2, on pourra choisir une telle famille d'éléments de G'.

2.3 Extension aux sous-groupes de rang semi-simple égal à 1

2.3.1 Proposition. *Soit $\alpha \in \Phi(G,T)$ et $\alpha' \in \Phi(G',T')$. Soit $\varphi_T : T \to T'$ un isomorphisme de tores tel que $\begin{array}{rccc} f : & X^*(T') & \to & X^*(T) \\ & \beta' & \mapsto & \beta' \circ \varphi_T \end{array}$ envoie α' sur α.*

Alors φ_T s'étend en un unique isomorphisme de groupes algébriques $\varphi_{G_\alpha} : G_\alpha \to G'_{\alpha'}$ tel que $\forall x \in \mathbb{G}_a\ \varphi_{G_\alpha}(\varepsilon_\alpha(x)) = \varepsilon'_{\alpha'}(x)$ et $\varphi_{G_\alpha}(n_\alpha) = n'_{\alpha'}$

Démonstration. Les G_α sont des groupes réductifs de rang semi-simple égal à 1 [Bor91, 13.18 (4)].

Quitte à considérer les groupes dérivés, on peut supposer que G_α et $G'_{\alpha'}$ sont semi-simples de rang 1 [Spr98, 7.3.2].

L'unicité provient du fait que T, n_α et U_α engendrent G_α [Spr98, 7.2].

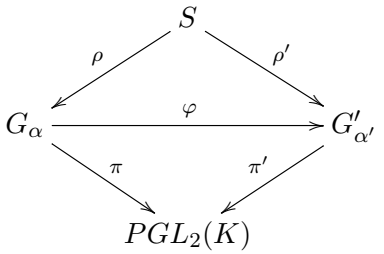
Existence :

On note $\Omega_\alpha = U_{-\alpha} \cdot T \cdot U_\alpha$ la grosse cellule de G_α pour le choix du sous-groupe de Borel $B_\alpha = T \cdot U_\alpha$. C'est un ouvert (dense) de G_α [Hum98, 28.5]. On note également $\Omega'_{\alpha'} = U'_{-\alpha} \cdot T' \cdot U'_{\alpha'}$.

Pour tout α, on sait que Ω_α est isomorphe à $U_{-\alpha} \times T \times U_\alpha$ comme variété, donc on peut définir l'isomorphisme de variétés $\varphi_{\Omega_\alpha} : \Omega_\alpha \to \Omega'_{\alpha'}$ par
$\forall x, y \in \mathbb{G}_a \ \forall t \in T \ \varphi_{\Omega_\alpha}(\varepsilon_{-\alpha}(x) t \varepsilon_\alpha(y)) = \varepsilon'_{-\alpha'}(x) \varphi_T(t) \varepsilon'_{\alpha'}(y)$.

On dispose de deux épimorphismes $\pi : G_\alpha \to PGL_2(K)$ et $\pi' : G'_{\alpha'} \to PGL_2(K)$ [Hum98, 25.3].

On cherche un recouvrement S de G_α et $G'_{\alpha'}$ tel que le diagramme suivant commute :



Précisément, posons $R = \left\{(z, z') \in G_\alpha \times G'_{\alpha'} \ , \ \pi(z) = \pi'(z')\right\}$. C'est un sous-groupe fermé par construction.

Soit $S = R^\circ$, et $\begin{array}{rccc} \rho : & S & \to & G_\alpha \\ & (z,z') & \mapsto & z \end{array}$ et $\begin{array}{rccc} \rho' : & S & \to & G'_{\alpha'} \\ & (z,z') & \mapsto & z' \end{array}$. On a alors $\pi \circ \rho = \pi' \circ \rho'$ par définition de S.

Soit $\begin{array}{rccc} \psi : & T & \to & S \\ & t & \mapsto & (t, \varphi_T(t)) \end{array}$. Le groupe $\psi(T)$ est un tore maximal de S, pour lequel $\rho : \widetilde{\Omega_\alpha}(\psi(T)) \to \Omega_\alpha(T)$ et $\rho' : \widetilde{\Omega_{\alpha'}}(\psi(T)) \to \Omega'_{\alpha'}(T')$ sont des isomorphismes.

φ est alors définie sur Ω_α, ouvert de G_α. En fait, φ est définie partout et est un homomorphisme de groupes. Montrons-le. Soit $x \in S$. On pose $z = \rho(x)$ et $z' = \rho'(x)$. On pose $\begin{array}{rccc} \lambda_0 : & S & \to & S \\ & y & \mapsto & xy \end{array}$, $\begin{array}{rccc} \lambda : & G_\alpha & \to & G_\alpha \\ & u & \mapsto & zu \end{array}$, $\begin{array}{rccc} \lambda' : & G'_{\alpha'} & \to & G'_{\alpha'} \\ & v & \mapsto & z'v \end{array}$.
Lorsque ceci est bien défini (dépend de φ), on a $\lambda' \circ \varphi \circ \rho = \lambda' \circ \rho' = \rho' \circ \lambda_0 = \varphi \circ \rho \circ \lambda_0 = \varphi \circ \lambda \circ \rho$. Comme ρ est surjective, on a $\lambda' \circ \varphi = \varphi \circ \lambda$. Donc si φ est définie en $y \in G_\alpha$, alors on peut définir $\varphi(zy) = z'\varphi(y)$, et donc définir φ sur G_α entier.

On a $\varphi \circ \rho = \rho'$ et $\lambda' \circ \varphi = \varphi \circ \lambda$, ce qui assure que φ est un homomorphisme de groupes. De plus, on constate que $\varphi(n_\alpha) = n'_{\alpha'}$.

En permutant les rôles de G et G', on obtient l'isomorphisme. □

2.4 Extension aux groupes radiciels

Pour $\alpha \in D$, on pose $h_\alpha = \varphi_{G_\alpha}(n_\alpha)$. Cela a du sens car $n_\alpha \in G_\alpha$.

Pour $\alpha \in D$, on pose $\varphi_\alpha = \varphi_{G_\alpha}|_{U_\alpha}$.

En effectuant des calculs dans les 3 types de systèmes de racines de rang 2, on pourrait démontrer la proposition suivante :

2.4.1 Proposition ([Hum98, 33]).

(A) *Pour toutes racines simples $\alpha, \beta \in D$, on a $\varphi_T(t_{\alpha\beta}) = (h_\alpha h_\beta)^{m(\alpha,\beta)}$.*

(B) *Pour toutes racines simples $\alpha, \beta \in D$, il existe un isomorphisme $\varphi_{\alpha\beta}$ de $U_{\alpha\beta}$ dans un sous-groupe de G' tel que $\varphi_{\alpha\beta}|_{U_\alpha} = \varphi_\alpha$ et $\varphi_{\alpha\beta}|_{U_\beta} = \varphi_\beta$*

(C) *Pour toutes racines simples $\alpha, \beta \in D$, on a les égalités :*
$\forall \gamma \in \Phi^+_{\alpha\beta} \setminus \{\alpha\}$ $(\mathrm{Int}\ h_\alpha) \circ \varphi_{\alpha\beta}|_{U_\gamma} = \varphi_{\alpha\beta} \circ (\mathrm{Int}\ n_\alpha)|_{U_\gamma}$

On utilise

2.4.2 Proposition ([Hum98, 32.4]). *Il existe une famille d'isomorphismes $(\varphi_\alpha)_\alpha$, pour α parcourant $\Phi(G,T)$, telle que :*

(a) $\forall \alpha \in D$ $\varphi_\alpha = \varphi_{G_\alpha}|_{U_\alpha}$ *et* $\varphi_{-\alpha} = \varphi_{G_\alpha}|_{U_{-\alpha}}$

(b) $\forall \alpha, \beta \in D$ $\forall \gamma \in \Phi^+_{\alpha\beta}$ $\varphi_\gamma = \varphi_{\alpha\beta}|_{U_\gamma}$

(c) $\forall n \in N$ $\forall \alpha, \beta \in \Phi(G,T)$ $(n(\alpha) = \beta) \Rightarrow \mathrm{Int}(\varphi_N(n)) \circ \varphi_\alpha = \varphi_\beta \circ \mathrm{Int}(n)|_{U_\alpha}$

Démonstration. Les points (a) et (b) définissent certains éléments de la famille cherchée.

Il s'agit d'une part de vérifier (c) pour ces éléments et, d'autre part, de construire les φ_α qui ne sont pas prescrits par (a) et (b).

Considérons d'abord le cas de deux racines simples $\alpha, \beta \in D$ distinctes. Soit $n \in \mathcal{N}_{G_{\alpha,\beta}}(T)$. On écrit $n = n_{\gamma_j} \dots n_{\gamma_1} t$ avec j entier, $\gamma_i \in \{\alpha, \beta\}$ et $t \in T$. On veut montrer par récurrence sur l'entier j que si $nT \cdot \alpha = \beta$ alors on a l'égalité (c), à savoir $\mathrm{Int}(\varphi_N(n)) \circ \varphi_\alpha = \varphi_\beta \circ \mathrm{Int}(n)|_{U_\alpha}$.

Remarquons au préalable que si $n(\alpha) = \alpha$, alors par construction de φ_α, on a $\mathrm{Int}(\varphi_N(n)) \circ \varphi_\alpha = \varphi_\alpha \circ \mathrm{Int}(n)|_{U_\alpha}$.

Si $j = 0$, alors $n \in T$. Comme φ_N et φ_α prolongent φ_T, on a l'égalité $\mathrm{Int}(\varphi_N(n)) \circ \varphi_\alpha = \varphi_\alpha \circ \mathrm{Int}(n)$.

Si $j = 1$, alors $\gamma_1 = \beta$ (car $n_\alpha \cdot \alpha = -\alpha$) et l'égalité (c) est donnée par 2.4.1(C).

Hérédité : Notons $\alpha_i = n_{\gamma_{i-1}} \dots n_{\gamma_1} \cdot \alpha$. On peut supposer que j est minimal dans l'écriture de n de sorte qu'en particulier $\alpha_i \neq \alpha$ pour tout $0 < i < j$. Pour $i < j$, lorsque $\alpha_i \in \Phi^+_{\alpha,\beta} \setminus \{\alpha\}$ on a l'égalité $\mathrm{Int}(\varphi_N(n_{\gamma_i})) \circ \varphi_{\alpha,\beta}|_{U_{\alpha_i}} = \varphi_{\alpha,\beta} \circ \mathrm{Int}(n_{\gamma_i})|_{U_{\alpha_i}}$.

Si pour tout $0 < i < j$, on a $\alpha_i \Phi^+_{\alpha,\beta}$, alors les égalités ci-dessus se combinent pour donner le résultat.

Sinon, considérons un entier $0 < i < j$ tel que $\alpha_i \in \Phi^+_{\alpha,\beta}$ et $\alpha_{i+1} \notin \Phi^+_{\alpha,\beta}$. Posons $n' = n_{\gamma_{i-1}} \dots n_{\gamma_1} t$ et $n'' = n_{\gamma_j} \dots n_{\gamma_i}$. Comme n_{γ_i} préserve $\Phi^+_{\alpha,\beta}\{\gamma_i\}$, on a donc $\alpha_i \in \{\alpha, \beta\}$. Si $\alpha_i = \alpha$, alors $n'(\alpha) = \alpha$ et $n''(\alpha) = n(\alpha) = \beta$. Par hypothèse de récurrence appliquée à n'', on a $\mathrm{Int}(\varphi_N(n'')) \circ \varphi_\alpha = \varphi_\beta \circ \mathrm{Int}(n'')|_{U_\alpha}$. On a aussi $\mathrm{Int}(\varphi_N(n')) \circ \varphi_\alpha = \varphi_\alpha \circ \mathrm{Int}(n')|_{U_\alpha}$. Ces deux égalités se combinent pour donner le résultat. Si $\alpha_i = \beta$, alors $n'(\alpha) = \beta$ et $n''(\beta) = \beta$. On procède de même en appliquant cette fois-ci l'hypothèse de récurrence à n'.

On veut généraliser l'égalité pour $n \in N$. On suppose à nouveau que $\alpha, \beta \in D$ vérifient $n(\alpha) = \beta$. Alors un lemme sur les systèmes de racines donne l'existence

d'une famille $(\gamma_i)_i$ d'éléments de D tels que $\gamma_0 = \alpha$, $\gamma_j = \beta$ d'une famille d'éléments de N, notons-la $(n_i)_i$, telle que $n = n_{j-1} \dots n_0$ et $n_i(\gamma_i) = \gamma_{i+1}$ pour tout i. De plus, pour tout i, il existe un $\delta_i \in D$ tel que $n_i \in W_{\gamma_i,\delta_i}$ le groupe de Weyl engendré par n_{γ_i} et n_{δ_i} et on a $\gamma_{i+1} \in \{\gamma_i, \delta_i\}$ [Hum98, A12]. On peut alors appliquer le résultat de la récurrence successivement aux n_i et on obtient (c) pour $\alpha, \beta \in D$.

On veut désormais définir les φ_α pour α racine quelconque. Soit $\alpha \in \Phi(G,T)$ et $n, n' \in N$. Soit $\beta = n(\alpha)$ et $\beta' = n'(\beta)$. Supposons que $\beta, \beta' \in D$. On a $n'n^{-1}(\beta) = \beta'$. Donc par ce qui précède, on $\mathrm{Int}(\varphi_N(n'n^{-1})) \circ \varphi_\beta = \varphi_{\beta'} \circ \mathrm{Int}(n'n^{-1})|_{U_\beta}$. En composant par $\mathrm{Int}(\varphi_N(n')^{-1}))$ à gauche et $\mathrm{Int}(n)$ à droite on obtient $\mathrm{Int}(\varphi_N(n)^{-1}) \circ \varphi_\beta \circ \mathrm{Int}(n)|_{U_\alpha} = \mathrm{Int}(\varphi_N(n')^{-1}) \circ \varphi_{\beta'} \circ \mathrm{Int}(n')|_{U_\alpha}$.

Étant donné $\alpha \in \Phi(G,T)$, il existe $\beta \in D$ et $n \in N$ tels que $n(\alpha) = \beta$ [Hum98, A.4]. On peut poser $\varphi_\alpha = \mathrm{Int}(\varphi_N(n)^{-1}) \circ \varphi_\beta \circ \mathrm{Int}(n)|_{U_\alpha}$ et on a montré que cela ne dépend ni du n, ni du β choisi. De plus, φ_α est un isomorphisme par composition. Pour cette définition, 2.4.1(B) donne (b).

Soit $\alpha, \beta \in \Phi(G,T)$ et $n \in N$ tels que $n(\alpha) = \beta$. Il existe $n', n'' \in N$ et $\gamma, \delta \in D$ tels que $n'(\alpha) = \gamma$ et $n''(\beta) = \delta$ de sorte que l'on peut appliquer les résultats précédents pour $n''nn'^{-1}(\gamma) = \delta$ et ainsi obtenir (c). □

2.5 Extension à un sous-groupe de Borel

On sait réaliser un sous-groupe de Borel comme le produit d'un tore maximal qu'il contient et des sous-groupes radiciels correspondants. On a déjà défini des morphismes de groupes algébriques de ces sous-groupes radiciels. Afin de vérifier que les choix de construction des φ_α permettent de définir un morphisme de groupes algébrique, on s'appuie sur le lemme suivant faisant intervenir des constantes dites « constantes de structure ».

2.5.1 Lemme. *Soit $\alpha, \beta \in \Phi(G,T)^+$. Soit $\mathcal{I} = \{(i,j) \in (N^*)^2 \ , \ i\alpha + j\beta \in \Phi(G,T)\}$. On munit $\Phi(G,T)^+$ d'un ordre total arbitraire afin de pouvoir écrire des produits (non commutatifs) sur cet ensemble suivant cet ordre.*

Pour chaque couple $\forall (i,j) \in \mathcal{I}$, il existe une constante $c_{\alpha\beta;ij} \in K$ telle que ces constantes vérifient l'égalité :
$\forall x, y \in \mathbb{G}_a \ [\varepsilon_\alpha(x), \varepsilon_\beta(y)] = \prod_{\substack{\gamma \in \Phi(G,T)^+ \\ \gamma = i\alpha + j\beta}} \varepsilon_\gamma(c_{\alpha\beta;ij} x^i y^j)$.

En particulier, on retrouve le fait que le commutateur de deux groupes radiciels est le produit des groupes radiciels qu'il contient.

Démonstration. Soit $m = \mathrm{Card}(\Phi(G,T)^+)$. Numérotons les racines positives $\alpha_i \in \Phi(G,T)^+$ de sorte que cela corresponde à l'ordre total fixé sur $\Phi(G,T)^+$. On rappelle que $\begin{array}{ccc} U_{\alpha_1} \times \dots \times U_{\alpha_m} & \to & U \\ (x_1, \dots, x_m) & \mapsto & x_1 \dots x_m \end{array}$ est un isomorphisme de variétés algébriques [Spr98, 8.2.1].

Soit $\begin{array}{rccc} \psi : & \mathbb{G}_a \times \mathbb{G}_a & \to & U \\ & (x,y) & \mapsto & [\varepsilon_\alpha(x), \varepsilon_\beta(y)] \end{array}$

Les morphismes ε_α sont réguliers et ψ l'est aussi, donc il existe des polynômes $p_k = \sum_{i,j} a_{k;ij} X^i Y^j \in K[X,Y]$ tels que $\forall x, y \ \psi(x,y) = u_{\alpha_1}(p_1(x,y)) \dots u_{\alpha_m}(p_m(x,y))$. On a $\forall x \in \mathbb{G}_a \ \psi(x,0) = [\varepsilon_\alpha(x), 1] = 1$. De même, $\forall y \in \mathbb{G}_a \ \psi(0,y) = 1$. Donc XY divise p_k pour tout $k \in [[1,m]]$. Donc lorsque $a_{k;ij} \neq 0$, on a $i, j > 0$.

Conjuguons $\psi(x,y)$ par $t \in T$ et exprimons le résultat de deux façons.

D'une part,

$$\begin{aligned} t\psi(x,y)t^{-1} &= t\varepsilon_\alpha(x)\varepsilon_\beta(y)\varepsilon_\alpha(-x)\varepsilon_\beta(-y)t^{-1} \\ &= t\varepsilon_\alpha(x)t^{-1}t\varepsilon_\beta(y)t^{-1}t\varepsilon_\alpha(-x)t^{-1}t\varepsilon_\beta(-y) \\ &= [\varepsilon_\alpha(\alpha(t)x, \varepsilon_\beta(\beta(t)y)] \\ &= \prod_{k=1}^{m} \varepsilon_{\alpha_k}(p_k(\alpha(t)x, \beta(t)y)) \end{aligned}$$

D'autre part,

$$\begin{aligned} t\psi(x,y)t^{-1} &= \prod_{k=1}^{m} t\varepsilon_{\alpha_k}(p_k(x,y))t^{-1} \\ &= \prod_{k=1}^{m} \varepsilon_{\alpha_k}(\alpha_k(t)p_k(x,y)) \end{aligned}$$

Donc $\forall k \in [[1,m]] \ \forall t \in T \ \forall x, y \ \alpha_k(t)p_k(x,y) = p_k(\alpha(t)x, \beta(t)y)$.

Donc $\forall k \in [[1,m]] \ \forall i, j > 0 \ \alpha_k a_{k;ij} = \alpha^i \beta^j a_{k;ij}$ (notation multiplicative des racines vues comme caractères)

Donc $\alpha_k \neq i\alpha + j\beta \Rightarrow a_{k;ij} = 0$ (notation additive des racines vues comme éléments du $\mathbb{Z}$-module $X^*(T)$). □

2.5.2 Proposition. *φ_T s'étend en un homomorphisme de groupes algébriques $\varphi_B : B \to G'$*

Démonstration. On a un isomorphisme de variétés $\iota : B \simeq T \times U_{\alpha_1} \times \dots U_{\alpha_m}$ où les α_i sont une numérotation des racines de $\Phi(G,T)^+$ [Spr98, 6.3.5 et 8.2.1].

On pose $\varphi_B = (\varphi_T \times \varphi_{\alpha_1} \times \cdots \times \varphi_{\alpha_m}) \circ \iota$. C'est un isomorphisme de variétés par composition et son image est un sous-groupe de Borel de G'.

Il faut alors vérifier que les choix réalisés pour définir les φ_α en font un morphisme de groupes.

Le lemme montre qu'il suffit de vérifier que c'est un homomorphisme de groupes pour les groupes engendrés par deux groupes radiciels.

Soit $\alpha, \beta \in \Phi(G,T)^+$. D'après [Hum98, A.4], il existe $n \in N$ et $\gamma, \delta \in D$ tels que $n(\alpha) = \gamma$ et $n(\beta) \in \Phi^+_{\gamma,\delta}$. En utilisant 2.4.1(B), on sait que $\varphi_{\gamma\delta} = \varphi_B|_{U_{\gamma\delta}}$. En utilisant les formules données par 2.4.2(c), on obtient que φ_B préserve la formule du commutateur pour α et β donnée par le lemme. Ainsi, $\varphi_B|U$ est un morphisme de groupes.

Par 2.4.2(c), φ_B préserve l'action de T par conjugaison sur chaque U_α. Donc φ_B est un morphisme de groupes.

Comme φ_B est un isomorphisme de variétés, c'est donc un isomorphisme de groupes algébriques. □

2.6 Extension au groupe tout entier

On part des morphismes φ_N et φ_B définis précédemment.

2.6.1 Lemme ([Hum98, 28.4]). *On se donne une famille d'éléments $(n_w)_{w\in W}$ relevant les éléments du groupe de Weyl W. Alors tout élément $x \in G$ s'écrit de manière unique sous la forme $x = u'n_wtu$ avec $w \in W$, $t \in T$, $u' \in U \cap wU^-w^{-1}$ et $u \in U$.*

De plus, $n = n_wt$ ne dépend que de $x \in G$ et pas du choix des représentants n_w.

On peut donc définir une application $\varphi : G \to G'$ telle que $\varphi(x) = \varphi_B(u')\varphi_N(n)\varphi_B(u)$.

Il faut vérifier que c'est un isomorphisme de groupes algébriques.

2.6.2 Proposition. *L'application φ précédemment construite vérifie $\varphi(xy) = \varphi(x)\varphi(y)$ pour tout $x, y \in \Omega$ tels que $xy \in \Omega$.*

Démonstration. On a des homomorphismes de groupes : $\varphi|_{G_\alpha}$, φ_N, $\varphi|_U$ et $\varphi|_{U^-}$.

1ère étape : Soit w_0 l'élément le plus long de W et $n_0 \in N$ représentant cet élément. Il permute racines positives et négatives donc $n_0Un_0^{-1} = U^-$ et $n_0U^-n_0^{-1} = U$.

$\forall u \in U$ $\varphi(n_0un_0^{-1}) = \varphi(n_0)\varphi(u)\varphi(n_0)^{-1}$ par une proposition précédente.

2ème étape : Soit $u \in B$, $v \in B^-$, $x \in \Omega$.

On écrit $v = v_1t_1$ avec $v_1 \in U^-$, $t \in T$;
$x = v_2t_2u_2$ avec $v_2 \in U^-$, $t_2 \in T$ et $u_2 \in U$;
$u = t_3u_3$ avec $t_3 \in T$ et $u_3 \in U$.

Alors on a d'une part, $\varphi(v)\varphi(x)\varphi(u) = \varphi(v_1)\varphi(t_1)\varphi(v_2)\varphi(t_2)\varphi(u_2)\varphi(t_3)\varphi(u_3)$;
et d'autre part $\varphi(vxu) = \varphi(v_1t_1v_2t_1^{-1}t_1t_2t_3t_3^{-1}u_2t_3u_3) = \varphi(v_1t_1v_2t_1^{-1})\varphi(t_1t_2t_3)\varphi(t_3^{-1}u_2t_3u_3)$.
En utilisant que $t_1v_2t_1^{-1} \in U^-$ et $\varphi|_{U^-}$, on a $\varphi(t_1v_2t_1^{-1}) = \varphi(t_1)\varphi(v_2)\varphi(t_1^{-1})$. On procède de même pour le membre de droite et l'on obtient que $\varphi(vxu) = \varphi(v)\varphi(x)\varphi(u)$.

3ème étape : Soit $\alpha \in D$ et $x \in \Omega$ tels que $n_\alpha xn_\alpha^{-1} \in \Omega$. On veut montrer que $\varphi(n_\alpha xn_\alpha^{-1}) = \varphi(n_\alpha)\varphi(x)\varphi(n_\alpha^1)$.

On écrit $x = vx_{-\alpha}tx_\alpha u$ avec $t \in T$, $x_{-\alpha} \in U_{-\alpha}$, $x_\alpha \in U_\alpha$, $v \in \prod_{\beta\in\Phi^+\setminus\{\alpha\}} U_{-\beta}$, $u \in \prod_{\beta\in\Phi^+\setminus\{\alpha\}} U_\beta$, où ces deux derniers produits sont normalisés par n_α car s_α est représenté par n_α et permute les racines de $\Phi^+ \setminus \{\alpha\}$ pour α racine simple.

Si $x = u$ ou v, alors le résultat est vrai.

Sinon, par la 2ème étape, il suffit de le vérifier pour $x = x_{-\alpha}tx_\alpha \in G_\alpha$ et c'est le cas car $\varphi|_{G_\alpha}$ est un morphisme de groupes.

4ème étape : Pour $n \in N$ quelconque et $x \in \Omega$ tels que $nxn^{-1} \in \Omega$, on veut montrer que $\varphi(nxn^{-1}) = \varphi(n)\varphi(x)\varphi(n^{-1})$.

Si $n \in T$, c'est vrai.

Si $n = n_\alpha$ pour un certain $\alpha \in D$, c'est vrai par la 3ème étape.

Sinon, on cherche un ouvert V_n de Ω tel que $\mathrm{Int}(n)(V_n) \subset \Omega$ et $\varphi \circ \mathrm{Int}(n)|_{V_n} = \mathrm{Int}(\varphi(n)) \circ \varphi|_{V_n}$. On procède par récurrence en écrivant n comme un produit de n_α pour $\alpha \in D$ et d'un élément $t \in T$. On suppose que alors qu'on a un n' pour lequel un tel $V_{n'}$ existe et que $n = n'n_\alpha$ avec $\alpha \in D$. Posons $V_n = \Omega \cap \mathrm{Int}(n_\alpha)^{-1}(V_{n'})$. Ainsi, $\mathrm{Int}(n)(V_n) \subset \mathrm{Int}(n')(V_{n'}) \subset \Omega$.

Si $x \in V_n$, alors $\mathrm{Int}(n)(x) = \mathrm{Int}(n') \circ \mathrm{Int}(n_\alpha)(x)$. Comme $\mathrm{Int}(n_\alpha)(x) \in V_{n'}$, on a $\varphi(\mathrm{Int}(n)(x)) = \mathrm{Int}(\varphi(n_\alpha))(\varphi(x))$. D'où le résultat.

5ème étape : Soit $x, x' \in \Omega$, que l'on écrit $x = vtu$, $x' = v't'u'$ avec $v, v' \in U^-$, $t, t' \in T$, $u, u' \in U$. On suppose de plus que $xx' \in \Omega$. Comme $\Omega = U^-\Omega U$, on a donc également $uv' \in \Omega$. Au regard de ce qui précède, il suffit de montrer que $\varphi(uv') = \varphi(u)\varphi(v')$. On considère la décomposition $uv' = n_0^{-1}(n_0un_0^{-1})(n_0v'n_0^{-1})n_0$.

Par la 1ère étape, on a les égalités $\varphi(u) = \varphi(n_0)^{-1}\varphi(n_0un_0^{-1})\varphi(n_0)$ et $\varphi(v') = \varphi(n_0)^{-1}\varphi(n_0v'n_0^{-1})\varphi(n_0)$. On a donc l'égalité $\varphi(u)\varphi(v') = \varphi(n_0)^{-1}\varphi(n_0un_0^{-1})\varphi(n_0v'n_0^{-1})\varphi(n_0)$

Par la 4ème étape, on a $\varphi(n_0uv'n_0^{-1}) = \varphi(n_0)\varphi(uv')\varphi(n_0^{-1})$

Comme $n_0Un_0^{-1} = U^-$ et $n_0U^-n_0^{-1} = U$, par la 2ème étape, on a donc $\varphi(n_0uv'n_0^{-1}) = \varphi(n_0un_0^{-1})\varphi(n_0vn_0^{-1})$.

En combinant ces égalités, on obtient alors le résultat attendu. □

2.6.3 Lemme. *Soit G_1 et G_2 des groupes algébriques connexes. Soit U un ouvert non vide de G_1. Soit $\psi : U \to G_2$ morphisme de variétés tel que $\forall x, y \in U$ $xy \in U \Rightarrow \psi(xy) = \psi(x)\psi(y)$. Alors $\exists!$ $\psi' : G_1 \to G_2$ morphisme de groupes algébriques prolongeant ψ.*

Démonstration. Notons $\mu_1 : G_1 \times G_1 \to G_1$ et $\mu_2 : G_2 \times G_2 \to G_2$ les morphismes de multiplication. Notons $V = \{(x, x') \in U \times U\,,\ xx' \in U\} = U \times U \cap \mu_1^{-1}(U)$. C'est un ouvert de $G_1 \times G_1$. On sait que $G_1 = U \cdot U$ [Bor91, 1.3]. On veut alors prolonger ψ à l'ensemble des éléments de $\mu_1(V)$, et pour cela on veut montrer que pour tout $(w, x, y, z) \in U^4$ on a $wx = yz \Rightarrow \psi(w)\psi(x) = \psi(y)\psi(z)$. Posons $f = \mu_1 \times \mu_1$ et $g = (\mu_2 \times \mu_2) \circ (\psi \times \psi \times \psi \times \psi)$. Soit $D_1 = \{(x, x)\,,\ x \in G_1\}$, c'est un fermé de $G_1 \times G_1$. De même $D_2 = \{(y, y)\,,\ y \in G_2\}$ est un fermé de $G_2 \times G_2$. Notons $\mathcal{O}_1 = f^{-1}(D_1) \cap U^4$ et $\mathcal{O}_2 = f^{-1}(D_2) \cap U^4$ Ce que l'on cherche à montrer se traduit par l'inclusion $\mathcal{O}_1 \subset \mathcal{O}_2$.

On a un isomorphisme de variétés $\begin{array}{ccc} f^{-1}(D_1) & \to & G_1 \times G_1 \times G_1 \\ (w, x, y, z) & \mapsto & (w, x, y) \end{array}$ d'inverse $(w, x, y) \mapsto (w, x, y, y^{-1}wx)$. Comme G_1 est irréductible, G_1^3 l'est donc $f^{-1}(D_1)$ aussi par isomorphisme [Hum98, 1.3 Prop. A (b)]. Par construction, $\mathcal{O}_1 = f^{-1}(D_1) \cap U^4$ est un ouvert de $f^{-1}(D_1)$, donc $\mathcal{O}_1$ est irréductible. En effet, si $\mathcal{O}_1 \neq f^{-1}(D_1)$, supposons par l'absurde qu'il s'écrive comme union de deux fermés propres $F \cap \mathcal{O}_1 \cup F' \cap \mathcal{O}_1$ avec F, F' fermés dans $f^{-1}(D_1)$, alors $f^{-1}(D_1)$ est l'union de $f^{-1}(D_1) \setminus \mathcal{O}_1$ qui est un fermé propre, et de $(F \cup F')$ qui est non vide. Donc $F \cup F' = f^{-1}(D_1)$. Donc F ou F' est $f^{-1}(D_1)$, ce qui contredit la supposition. Comme $\mathcal{O}_1$ est irréductible, l'ouvert $(V \times V) \cap \mathcal{O}_1$ est dense dans $\mathcal{O}_1$. Soit $(w, x, y, z) \in (V \times V) \cap \mathcal{O}_1$, on a $wx = yz$ et $\psi(wx) = \psi(w)\psi(x)$ et $\psi(yz) = \psi(y)\psi(z)$. Donc $\psi(wx) = \psi(yz)$. Donc $(w, x, y, z) \in \mathcal{O}_2$. Comme $(V \times V) \cap \mathcal{O}_1$ est dense dans $\mathcal{O}_1$ et comme $\mathcal{O}_1$ et $\mathcal{O}_2$ sont des fermés de U^4, on a $\mathcal{O}_1 \subset \mathcal{O}_2$.

On peut donc définir un morphisme $\psi' : G_1 \to G_2$ de la manière suivante : si $x \in G_1$ s'écrit $x = yz$ avec $y, z \in U$, on pose $\psi'(x) = \psi(y)\psi(z)$. Cela ne dépend pas du choix de y, z. Il reste à montrer que le morphisme de variétés ψ' est multiplicatif. Posons $\chi(x, y) = \psi'(xy)\psi'(y)^{-1}\psi'(x)^{-1}$ pour tout $x, y \in G_1$. $\chi : G_1 \times G_1 \to G_2$ est un morphisme de variété qui vaut l'identité sur V, qui est ouvert donc dense dans

$G_1 \times G_1$. Donc χ est trivial sur $G_1 \times G_1$ tout entier. Donc ψ' est un morphisme de groupes algébriques. □

On applique ce lemme au morphisme φ, aux groupes G et G' et à l'ouvert Ω de G. L'application $\varphi|_\Omega$ s'étend de manière unique en un morphisme de groupes $\varphi' : G \to G'$. De plus, pour toute racine $\alpha \in \Phi$, les applications φ et φ' coïncident sur l'ouvert $\Omega \cap G_\alpha$ de G_α. Donc φ et φ' sont égales sur chaque groupe G_α. Comme ces groupes engendrent G, on a nécessairement $\varphi = \varphi'$ et donc l'application φ est en fait un morphisme de groupes algébrique.

Ce morphisme est injectif par construction et on a $\varphi(U_\alpha) = U'_{\alpha'}$ pour chaque $\alpha \in \Phi$. Comme on dispose d'un isomorphisme de systèmes de racines entre $\Phi(G,T)$ et $\Phi(G',T')$, l'image de φ contient les $U'_{\alpha'}$ et T'. Ces groupes engendrent G', donc φ réalise un isomorphisme de groupes algébriques comme annoncé dans le théorème d'isomorphisme.

3 Existence de k-tores maximaux et densité des points rationnels des groupes réductifs

3.1 Éléments réguliers des algèbres de Lie

Afin de répondre à des problèmes de définition sur le corps de base, une solution est de construire des objets comme centralisateurs d'éléments semi-simple du groupe ou de l'algèbre de Lie sous certaines action ; la plus naturelle étant donnée par automorphismes intérieurs et leurs dérivées (action adjointe).

3.1.1 Définition. Soit $\mathfrak{g}$ l'algèbre de Lie d'un groupe algébrique G. Soit $X \in \mathfrak{g}$. Considérant l'application linéaire $\operatorname{ad} X : \mathfrak{g} \to \mathfrak{g}$, on définit $\operatorname{nil}(X)$ comme étant la multiplicité de la valeur propre 0 de $\operatorname{ad} X$.

Pour toute sous-algèbre de Lie $\mathfrak{h}$ de $\mathfrak{g}$, on pose $\operatorname{nil}(\mathfrak{h}) = \min_{X \in \mathfrak{h}} \operatorname{nil}(X)$.

On dit que X est régulier si $\operatorname{nil}(X) = \operatorname{nil}(\mathfrak{g})$, singulier sinon.

Les éléments réguliers semi-simples seront les bons candidats, il s'agit d'en trouver sur le corps de base.

3.1.2 Lemme (d'après [Bor91, 18.1])**.** *Si k est infini et si $\mathfrak{h}$ est une sous-algèbre de Lie propre de $\mathfrak{g}$, alors il existe un élément $Y \in \mathfrak{g}(k)$ qui est régulier et semi-simple et tel que $z_{\mathfrak{g}}(Y) \not\subset \mathfrak{h}$.*

Démonstration. Soit $n = \dim G$ et $\mathbf{e} = (e_1, \dots, e_n)$ une base de $\mathfrak{g}(k)$. On définit des coefficients $c_l^{i,j} \in k$ par $\operatorname{ad} e_i(e_j) = \sum_l c_l^{i,j} e_l$. On a $\operatorname{Mat}_{\mathbf{e}}(\operatorname{ad} X) = \left(\sum_l X_l c_j^{l,i}\right)_{i,j}$ pour $X = \sum_l X_l e_l$.

Donc, $\det(\operatorname{ad} X - T) = T^{\operatorname{nil}(\mathfrak{g})} \left(P_0(X) + \cdots + P_{n-\operatorname{nil}(\mathfrak{g})}(X) T^{n-\operatorname{nil}(\mathfrak{g})}\right)$, où les P_i sont des polynômes homogènes en les X_l, à coefficients dans k.

Par définition, $X \in \mathfrak{g}$ est régulier si et seulement si $P_0(X) \neq 0$, et un tel X existe par définition de $\operatorname{nil}(\mathfrak{g})$. En particulier, $P_0 \neq 0$ vu comme polynôme dans $K[T]$. Comme k est supposé infini, il existe donc $X \in \mathfrak{g}(k)$ tel que $P_0(X) \neq 0$, et donc X est régulier. On peut de plus imposer $X \notin \mathfrak{h}$ dès lors que $\mathfrak{h}$ est une sous-algèbre de Lie propre de $\mathfrak{g}$.

On a $\operatorname{ad} X_s = (\operatorname{ad} X)_s$ et $\operatorname{ad} X_n = (\operatorname{ad} X)_n$ [Spr98, 4.4.20]. Par définition, X_n et X_s commutent et 0 est la seule valeur propre de X_n, donc X et X_n ont les mêmes valeurs propres avec les mêmes multiplicités, donc $\operatorname{nil}(X) = \operatorname{nil}(X_s)$. De plus, on sait que $X_s \in \mathfrak{g}(k^{p^{-\infty}})$ [Bor91, 4.2 (5)].

Si $p = 0$, alors k est parfait donc $Y = X_s \in \mathfrak{g}(k)$ est régulier et semi-simple.

Désormais, on suppose $p > 0$. Dans ce cas, $\mathfrak{g}$ est une algèbre de Lie restreinte (ou p-algèbre de Lie) en tant qu'algèbre de Lie d'un groupe algébrique défini sur k [Spr98, 4.4.3], c'est-à-dire qu'il existe une application $[p] : \mathfrak{g} \to \mathfrak{g}$ telle que :

$$\begin{cases} \forall X \in \mathfrak{g} & \operatorname{ad}[p](X) = (\operatorname{ad} X)^p \\ \forall X, Y \in \mathfrak{g} & [p](X+Y) = [p](X) + [p](Y) \\ \forall X \in \mathfrak{g}\, \forall a \in k & [p](aX) = F_p(a)[p](X) \end{cases}$$

On note aussi $X^{[p]}$ au lieu de $[p](X)$ et $\forall n \in \mathbb{N}^*\ [p^n] = [p]^n$.

Il existe une puissance q de p telle que $\operatorname{ad}(X_n)^q = 0$. Ainsi, $(X_n)^{[q]} = 0$ (injectivité de ad). Soit $Y = X^{[q]}$. On a $Y \in \mathfrak{g}(k)$, car $X \in \mathfrak{g}(k)$. On sait aussi

que Y est régulier car $[p]$ ne change pas la multiplicité de la valeur propre 0 de $\operatorname{ad} Y$ Il s'agit de montrer que Y est semi-simple. L'élément $\operatorname{ad}({X_s}^{[q]}) = (\operatorname{ad} X_s)^q = ((\operatorname{ad} X)_s)^q \in gl(\mathfrak{g})$ est semi-simple, donc [Bor91, 4.3 (2)] ${X_s}^{[q]}$ est semi-simple. $Y = (X_s + X_n)^{[q]} = X_s^{[q]}$ car ${X_n}^{[q]} = 0$, donc $Y = (X_s)^{[q]} = X^{[q]}$ est semi-simple.

Il reste à voir $z_{\mathfrak{g}}(Y) \not\subset \mathfrak{h}$. On sait que X et X_s commutent, donc X et Y aussi, donc $X \in z_{\mathfrak{g}}(Y)$ permet de conclure car on a pris soin de choisir X hors de $\mathfrak{h}$. □

3.2 Existence de tores maximaux définis sur k

3.2.1 Théorème (d'après [Bor91, 18.2 i], résultat dû à Rosenlicht et Grothendieck)**.** *Soit G un groupe algébrique connexe défini sur k. Alors G contient un tore maximal qui est défini sur k.*

Démonstration du théorème. On distingue le cas des corps finis (donc parfaits) de celui des corps infinis.

Cas des corps finis : Notons $p = \operatorname{car} k$ et $q = \operatorname{Card} k$. On note F_q l'automorphisme de corps $\begin{array}{rccc} F_q : & \overline{k} & \to & \overline{k} \\ & x & \mapsto & x^q \end{array} \in \operatorname{Gal}(\overline{k}/k)$ fixant k.

Considérons les morphismes de groupes algébriques $\begin{array}{rccc} f_h : & G & \to & G \\ & g & \mapsto & (F_q \cdot g)hg^{-1} \end{array}$, pour $h \in G$ définissant une action de G sur lui-même par $g \cdot h = f_h(g)$. Les images $\operatorname{Im} f_h = G \cdot h$ sont des orbites. Calculons les différentielles de ces morphismes en l'identité. Comme produit, on a $\forall X \in \mathfrak{g}\ d(f_h)_e(X) = -X \cdot h + h \cdot d(F_q)_e(X)$ Or $d(F_q) = 0$, donc $d(f_h)_e$ est surjective, donc f_h est séparable donc dominant (ce résultat est un théorème de Lang). En particulier, $\operatorname{Im} f_h$ contient un ouvert non vide U_0 de G [Bor91, AG 10.1 (2)]. Par homogénéité (en tant qu'orbite d'une action), $\operatorname{Im} f_h$ est ouvert dans G. Pour cette action, on a montré que toutes les orbites sont ouvertes, elles sont donc aussi fermées. En particulier, f_e est surjective par connexité.

Soit T un tore maximal, a priori défini sur $\overline{k}$. On note $T^{[q]} = F_q \cdot T$, c'est aussi un tore maximal de G. Les tores maximaux sont G-conjugués [Bor91, 11.3 (1)]. Soit $g \in G$ tel que $T^{[q]} = {}^gT$. Soit $h \in G$ tel que $f_e(h^{-1}) = g$. Alors $F_q \cdot {}^hT = {}^{F_q \cdot h}T^{[q]} = {}^hT$. Donc ${}^hT$ est un tore maximal de G qui est F_q-stable. Donc ce tore maximal est défini sur k.

Cas des corps infinis : On procède par récurrence sur $\dim G$.

Si G admet un tore maximal central (éventuellement trivial), alors G est nilpotent [Bor91, 11.5 (3)]. Par [Ros57, Prop. 9 p. 37], ce tore maximal est défini sur k en tant que tore maximal d'un groupe connexe nilpotent.

On suppose désormais que G est non nilpotent, donc qu'il admet un tore maximal non trivial et non central. On cherche dans G un sous-groupe de dimension strictement inférieure et défini sur k susceptible de contenir un tore maximal de G, comme centralisateur d'un élément de l'algèbre de Lie. On va trouver un tel élément non central, quitte à travailler dans un groupe plus gros que G.

Si tous les éléments de $\mathfrak{g}$ sont centraux, on s'appuie sur la proposition suivante dont on reprend les notations par la suite [Bor91, 17.8] :

3.2.2 Proposition (d'après [Bor91, 17.8]). *Si G est un groupe algébrique connexe, non nilpotent, tel que tout élément semi-simple de $\mathfrak{g}$ est central, et si T est un tore maximal de G, alors il existe un k-groupe G' tel que $\mathfrak{g}'$ contient des éléments semi-simples non centraux, et une k-isogénie purement inséparable $\pi : G \to G'$ telle que* $\ker d\pi = \mathfrak{t}$ *et pour tout tore maximal T' de G',* $\operatorname{Im} d\pi \oplus \mathfrak{t}' = \mathfrak{g}'$.

Sinon, si $\mathfrak{g}$ admet un élément non central, on pose $G' = G$ et $\pi = \mathrm{id}_G$.

Ainsi, $\mathfrak{g}'$ contient des éléments semi-simples non centraux. On a $\mathrm{nil}(\mathfrak{g}') < \dim \mathfrak{g}'$, car sinon $\mathfrak{g}'$ ne contiendrait que des éléments nilpotents. Soit $Y \in \mathfrak{g}'(k)$ un élément régulier semi-simple, ce qui existe [3.1.2]. On a $\dim z_{\mathfrak{g}'}(Y) = \dim \ker \mathrm{ad}\, Y \leq \mathrm{nil} Y < \dim \mathfrak{g}'$. Donc Y n'est pas central.

On fait agir G sur $\mathfrak{g}'$ par $g \cdot X = \mathrm{Ad}(\pi(g))(X)$. Soit $G_Y = \mathrm{Stab}_G(Y) = \{g \in G\,,\, \mathrm{Ad}(\pi(g))(Y) = Y\}$. On a $\pi(G_Y) = \{g' \in G'\,,\, \pi^{-1}(\{g'\}) \neq \emptyset$ et $\mathrm{Ad}(g')(Y) = Y\}$. Par surjectivité de π, on a alors $\pi(G_Y) = \mathcal{Z}_{G'}(Y)$.

Comme $Y \in \mathfrak{g}'(k)$ est semi-simple, par [Bor91, 9.1], on sait que $\mathcal{Z}_{G'}(Y)$ est défini sur k. On sait également qu'il existe un tore maximal de G', disons S, tel que $Y \in \mathrm{Lie}(S) = \mathfrak{s}$ [Bor91, 11.8].

Dans le cas où $\pi = \mathrm{id}_G$, on sait donc que G_Y est défini sur k.

Dans le cas où π est donné par la proposition [3.2.2], notons $\begin{array}{rccc} f : & G & \to & \mathfrak{g}' \\ & g & \mapsto & \mathrm{Ad}(\pi(g))(Y) \end{array}$. On a $G_Y = f^{-1}(\{Y\})$. De plus, $\mathrm{ad}\,(Y)(\mathfrak{s}) = 0$, et comme $d\pi_e(\mathfrak{g})$ est un supplémentaire de $\mathfrak{s}$ d'après la proposition [3.2.2], on a $\mathrm{ad}\,(Y)(\mathfrak{g}') = \mathrm{ad}\,(Y)(d\pi_e(\mathfrak{g}))$. On a $T_Y\mathfrak{g}' = Y + \mathrm{ad}\,(Y)(\mathfrak{g}')$ et $df_e(X) = Y - \mathrm{ad}\,(Y)(d\pi_e(X))$. Donc df_e est surjective. Donc f est séparable et par [Bor91, 6.7], G_Y est défini sur k.

Ainsi, $(G_Y)^\circ$ est défini sur k comme composante neutre d'un tel groupe [Bor91, 1.2 (b)].

On a $S \subset \mathcal{Z}_{G'}(Y) = \pi(G_Y)$, donc $(G_Y)^\circ$ contient $T = \pi^{-1}(S)^\circ$. Comme π est une isogénie, T est isomorphe à un sous-groupe de S donc, par caractérisation des groupes diagonalisables [Bor91, 8.4], T est diagonalisable. De plus, il est connexe par construction. Donc c'est un tore de G. L'image par π d'un tore maximal de G contenant T est un tore de G' contenant S, donc égal par maximalité de S. Ainsi, T est un tore maximal de G.

Par conjugaison des tores maximaux [Bor91, 11.3 (1)], les tores maximaux de $(G_Y)^\circ$ sont des tores maximaux de G. Si $G_Y = G$, alors $\pi(G_Y) = G' = \mathcal{Z}_{G'}(Y)$, ce qui est exclu car $\dim z_{\mathfrak{g}'}(Y) < \dim \mathfrak{g}'$. Donc $\dim(G_Y)^\circ = \dim G_Y < \dim G$. Par récurrence sur la dimension, comme le groupe $(G_Y)^\circ$ est connexe et défini sur k, il contient un tore maximal T défini sur k, et T est un tore maximal de G, d'où le résultat. □

Une conséquence immédiate est l'existence de sous-groupes de Cartan définis sur k puisque ces sous-groupes sont par définition les centralisateurs des tores maximaux [Bor91, 11.13] et que le centralisateur d'un tore défini sur k est lui-même défini sur k [Ros57, prop. 9 p37].

3.3 Unirationalité et densité des points rationnels des groupes réductifs

3.3.1 Définition (rationalité et unirationalité sur k)**.** Soit V une k-variété irréductible représentée par $k[V]$, et $k(V)$ son corps des fractions.

On dit que V est rationnelle sur k si l'extension $k(V)/k$ est purement transcendante, c'est-à-dire qu'il existe une base de transcendance S de $k(V)$ sur k telle que $k(V) = k(S)$.

On dit que V est unirationnelle sur k si $k(V)$ est un sous-corps d'une extension purement transcendante de k.

3.3.2 Lemme. *Soit $V_1, \dots, V_m$ et V des k-variétés irréductibles. On suppose que $V_1, \dots, V_m$ sont unirationnelles sur k et qu'il existe un k-morphisme dominant $f : V_1 \times \cdots \times V_m \to V$. Alors V est unirationnelle sur k.*

Démonstration. Comme f est dominant, le comorphisme $f^* : k(V) \to k(V_1 \times \cdots \times V_n)$ est injectif et fait de $k(V)$ une sous-extension de $k(V_1 \times \cdots \times V_n)$. Pour $1 \leq i \leq n$, par unirationnalité de V_i, on a une extension $L_i/k(V_i)$ et une base de transcendance S_i telle que $k(S_i) = L_i/k$ soit une extension purement transcendante. Soit $S = \bigcup_i S_i$, c'est une base de transcendance pour une extension $L = k(S)/k$ purement transcendante, dont $k(V_1 \times \cdots \times V_n)$ est une sous-extension, et donc aussi $k(V)$. Ainsi, V est unirationnelle sur k. □

3.3.3 Lemme (d'après [Spr98, 13.2.6])**.** *Soit V une k-variété irréductible. On suppose que k est infini et que V est unirationnelle sur k. Alors $V(k)$ est dense dans V.*

Démonstration. On écrit la suite d'extensions $k \subset k(V) \subset k(S)$ où $k(S)/k$ est purement transcendante et S est une base de transcendance de $k(S)$, et $j : k(V) \to k(S)$ l'injection canonique. $\mathrm{Hom}_{k-alg}(k[S], \cdot) = \mathbb{A}^n$ pour un certain n. Il existe un ouvert Zariski-dense U de $\mathbb{A}^n$ et un morphisme dominant $\alpha : U \to V$ [Bor91, AG 8.2]. Comme k est infini, $\mathbb{A}^n(k)$ est dense dans $\mathbb{A}^n$, donc $U(k)$ est dense dans U, donc $V(k) = \alpha(U(k))$ est dense dans V. □

3.3.4 Théorème. *Soit G un groupe réductif connexe défini sur k supposé infini. Alors G est unirationnel sur k et $G(k)$ est dense dans G.*

3.3.5 Remarque. Si l'on suppose à l'inverse que le corps k est fini, alors l'unirationalité demeure mais ne permet pas de conclure à la densité des points rationnels.

Démonstration. On procède par récurrence sur $\dim G$ pour démontrer que G est unirationnel sur k.

Si $\dim G = 0$, alors $G = \{e\} = \mathrm{Hom}_{k-alg}(k, \cdot)$ où l'extension triviale k/k est purement transcendante.

Si $\dim G = 1$, alors ou bien $G \simeq \mathbb{G}_a = \mathrm{Hom}_{k-alg}(k[T], \cdot)$, ou bien $G \simeq \mathbb{G}_m = \mathrm{Hom}_{k-alg}(k[T, T^{-1}], \cdot)$, donc $k(G) \simeq k(T)$ est purement transcendante sur k.

Hérédité : Si $G = T$ est un tore défini sur k, on va construire un k-groupe diagonalisable T' unirationnel sur k et une surjection $T' \twoheadrightarrow T$. On sait que Γ est muni d'une topologie de groupe profini qui le rend compact [Dou05, 5.9.2] et Γ agit continument sur $N = X^*(T)$ vu comme $\mathbb{Z}$-module de type fini. Donc il existe un sous-groupe U ouvert distingué de $\Gamma = \mathrm{Gal}(k_s/k)$ qui agit trivialement sur $X^*(T)$. Soit $\Gamma' = \Gamma/U$, c'est donc un groupe fini et $X^*(T)$ est un Γ'-module, donc une $\mathbb{Z}$-représentation libre de rang fini de Γ'. On considère un $\mathbb{Z}[\Gamma']$-module bidual de N, à savoir $M = \mathrm{Hom}_{\mathbb{Z}-mod}(\mathrm{Hom}_{\mathbb{Z}-mod}(N, \mathbb{Z}[\Gamma']), \mathbb{Z}[\Gamma'])$. C'est un $\mathbb{Z}[\Gamma']$-module. On pose $\begin{array}{rccc} \alpha_0 : & N & \to & M \\ & n & \mapsto & (f \mapsto f(n)) \end{array}$. On veut s'assurer qu'il s'agit d'un monomorphisme. Pour tout $\mathbb{Z}$-module P, et tous $f, g \in \mathrm{Hom}_{\mathbb{Z}-mod}(P, N)$, on a pour tout $p \in P$ $\alpha_0 \circ f(p) = \alpha_0 \circ g(p)$. Donc $\forall h \in \mathrm{Hom}_{\mathbb{Z}-mod}(N, \mathbb{Z}[\Gamma'])\, h \circ f(p) = h \circ g(p)$, Ce qui impose $f(p) = g(p)$. Donc α_0 est un monomorphisme. α_0 admet alors un dual α qui est un épimorphisme $\alpha : T' \to T$ où T' est un k-groupe diagonalisable tel que $X^*(T') = M$ donné par l'équivalence de catégories [1.2.2]. Son comorphisme $\alpha^* : k(T) \to k(T')$ est injectif. Il reste à voir que l'extension $k(T')/k$ est purement transcendante, autrement dit que T' est rationnel sur k. On pose $A = K[M]$, de sorte que $T' = \mathrm{Hom}_{K-alg}(A, \cdot)$. $A_k = k_s[M]^\Gamma$ est une k-structure pour A. Pour toute k-algèbre R, on définit une action de Γ sur $k_s \underset{k}{\otimes} R$ par $\forall \gamma \in \Gamma\, \forall a \in k_s\, \forall r \in R\, \gamma \cdot (a \otimes r) = \gamma(a) \otimes r$. On a alors $((k_s \otimes R)^\times)^U = (L \otimes R)^\times$ où $L = {k_s}^U/k$ est une extension finie. $T'(R) = \mathrm{Hom}_{K-alg}(A, K \otimes R) = \mathrm{Hom}_{k-alg}(A_k, R) = \mathrm{Hom}_{k_s-alg}(k_s \otimes A_k, k_s \otimes R)^\Gamma = \mathrm{Hom}_{\mathbb{Z}-mod}(M, (k_s \otimes R)^\times)^\Gamma = ((k_s \otimes R)^\times)^U = (L \otimes R)^\times = \mathbb{G}_{m,L}(R)$ Comme $T' = \mathbb{G}_{m,L}$ est k-rationnel [Bor91, 1.6 (9)], on peut alors conclure que T est unirationnel sur k.

Si G n'est pas un tore, alors on peut reprendre les notations de la démonstration du théorème [3.2.1]. On note H le plus petit sous-groupe fermé de G contenant les $((G_Y)^\circ)_{Y \in \mathfrak{g}(k), Y \text{ régulier et semi-simple}}$. On a déjà vu que les $(G_Y)^\circ$ sont définis sur k et que $\dim(G_Y)^\circ < \dim G$. On sait que $G' = \pi(G)$ est réductif comme image d'un groupe réductif par une isogénie donc $\pi(G_Y) = \mathcal{Z}_{G'}(Y)^\circ$ est réductif [Bor91, 13.19]. Donc G_Y est réductif, et a fortiori, $(G_Y)^\circ$ l'est aussi. Ainsi, par hypothèse de récurrence, les $(G_Y)^\circ$ sont unirationnels sur k.

On va montrer que $H = G$. Supposons par l'absurde $H \neq G$. On a $\dim H < \dim G$. Notons $H' = \pi(H)$. Les isogénies préservant la dimension, on a $\dim H' = \dim H < \dim G = \dim G'$, donc $\mathfrak{h}' = \mathrm{Lie}(H')$ est une sous-algèbre de Lie propre de $\mathfrak{g}'$. Soit Y donné par le lemme [3.1.2]. On sait que $z_{\mathfrak{g}'}(Y) = \mathrm{Lie}(\mathcal{Z}_{G'}(Y)^\circ)$ [Bor91, 9.1]. Donc $(G_U)^\circ \not\subset H$, ce qui contredit la définition de H.

En utilisant [Bor91, 2.2], on trouve un ensemble fini $(Y_i)_{1 \leq i \leq m}$ tel que G est engendré par les $({G_{Y_i}}^\circ)_i$. En particulier, on a un k-morphisme surjectif $f : {G_{Y_1}}^\circ \times \cdots \times {G_{Y_m}}^\circ \to G$ Par le lemme [3.3.2], on sait alors que G est unirationnel sur k. D'où le résultat d'unirationalité.

On peut alors conclure, en utilisant le lemme [3.3.3], que $G(k)$ est dense dans G. □

4 Groupes réductifs, déploiement

4.1 Définition et énoncés

4.1.1 Définition. Soit G un groupe algébrique connexe réductif défini sur k. On dit que G est déployé sur k s'il existe un tore maximal T de G qui est k-déployé ainsi que des isomorphismes $\varepsilon_\alpha : \mathbb{G}_a \to U_\alpha$ définis sur k pour tout $\alpha \in \Phi(G,T)$.

Le couple $(T, (\varepsilon_\alpha)_{\alpha\in\Phi(G,T)})$ est appelé une donnée de déploiement pour G.

4.1.2 Théorème ([Bor91, 18.7])**.** *Soit G un groupe algébrique connexe réductif. Si G admet un tore maximal T qui est k-déployé. Alors G est déployé sur k.*

4.1.3 Corollaire. *Soit G un groupe algébrique connexe réductif. Alors G est déployé sur une extension finie séparable de k.*

Démonstation du corollaire. Si G est connexe réductif, alors par [3.2.1], G admet un tore maximal T qui est défini sur k. Or T se déploie sur une extension finie séparable disons L/k [Bor91, 8.11]. Donc G se déploie sur L d'après le théorème [4.1.2]. □

4.2 Démonstration du théorème de déploiement des groupes réductifs connexes

Il s'agit en fait de montrer qu'un tore maximal qui est k-déployé fait partie d'une donnée de déploiement pour G. Les racines α étant alors imposés par le choix de T, les U_α le sont aussi par le théorème [1.3.6] Il s'agit uniquement de montrer que les U_α sont définis sur k pour chaque $\alpha \in \Phi(G,T)$ et d'exhiber une famille d'isomorphismes définis sur k correspondante.

Première étape : on se ramène au cas d'un groupe réductif de rang semi-simple égal à 1.

Soit $\alpha \in \Phi(G,T)$. Soit $T_\alpha = (\ker\alpha)^\circ \leq T$. C'est un sous-tore de T de codimension 1 [Bor91, 13.2], déployé sur k car T l'est [Bor91, Cor. 8.4].

On considère $G_\alpha = \mathcal{Z}_G(T_\alpha)$ qui est un groupe réductif de rang semi-simple 1 [Bor91, 13.18]. On choisit de considérer deux sous-groupes de Borel opposés par rapport à T qui sont $B_\alpha = T \cdot U_\alpha$ et $B_{-\alpha} = T \cdot U_{-\alpha}$ de ce groupe G_α. D'une part, G_α vérifie les hypothèses du théorème et, d'autre part, si tous les G_α sont déployés sur k alors G l'est aussi car il suffit de vérifier que les U_α sont définis sur k et k-isomorphes à $\mathbb{G}_a$. On travaille désormais dans $G = G_\alpha$.

Deuxième étape : les B_α sont k-fermés.

On sait par [Bor91, 13.18] que $\mathrm{Lie}(G_\alpha) = \mathfrak{t} \oplus \mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha}$, que $\mathfrak{b}_\alpha := \mathrm{Lie}(B_\alpha) = \mathfrak{t} \oplus \mathfrak{g}_\alpha$, et que $\mathfrak{b}_{-\alpha} := \mathrm{Lie}(B_{-\alpha}) = \mathfrak{t} \oplus \mathfrak{g}_{-\alpha}$.

On sait que l'algèbre de Lie $\mathfrak{t} = \mathrm{Lie}(T)$ est définie sur k car T l'est.

On veut montrer que les $\mathfrak{g}_\alpha$ sont définis sur k. Comme G est défini sur k, son algèbre de Lie $\mathfrak{g}$ l'est aussi et on a une action de Γ sur $\mathfrak{g}$. La racine α vue comme morphisme $T \to \mathbb{G}_m$ est un k-morphisme de k-groupes algébriques car T est k-déployé, donc est aussi définie sur k_s. Ainsi, pour tout $t \in T(k_s)$, l'équation $\mathrm{Ad}(t)(X) = \alpha(t)X$ est à coefficients dans k_s. Comme $T(k_s)$ est dense dans

T [Bor91, AG 13.3], $\mathfrak{g}_\alpha$ est défini sur k_s. On veut alors vérifier que $\mathfrak{g}_\alpha$ est Γ-stable. Soit $X \in \mathfrak{g}_\alpha$. Par définition, pour tout $t \in T$, on a $\mathrm{Ad}(t)(X) = \alpha(t)X$. Comme Ad et α sont définis sur k, ces morphismes sont Γ-équivariants. Ainsi, pour tout $t \in T$, $\gamma^{-1}(\mathrm{Ad}(\gamma(t)))(X) = \gamma^{-1}(\alpha(\gamma(t)))(X)$. Par semi-linéarité, on a alors $\gamma^{-1}(\mathrm{Ad}(\gamma(t))(\gamma(X))) = \gamma^{-1}(\alpha(\gamma(t))\gamma(X))$. En composant par γ, on a finalement $\mathrm{Ad}(\gamma(t))(\gamma(X)) = \alpha(\gamma(t))\gamma(X)$, et ce pour tout $t \in T$, où T est Γ-stable. Donc $\gamma(X) \in \mathfrak{g}_\alpha$ quel que soit $\gamma \in \Gamma$. Comme $\mathfrak{g}_\alpha$ est définie sur k_s et est Γ-stable, par [Bor91, AG 14.4], $\mathfrak{g}_\alpha$ est définie sur k. Par conséquent, les algèbres de Lie $\mathfrak{b}_\alpha$ et $\mathfrak{b}_{-\alpha}$ sont aussi définies sur k.

Par [Bor91, 14.1 Cor.2], on a $B_\alpha = \mathcal{N}_G(\mathfrak{b}_\alpha)$ et $B_{-\alpha} = \mathcal{N}_G(\mathfrak{b}_{-\alpha})$.

On utilise alors le lemme suivant pour conclure

4.2.1 Lemme (issu de [Bor91, 1.7]). *Soit G un k-groupe, V une k-variété et $\alpha : G \times V \to V$ une action de G sur V définie sur k. Si W est une partie k-fermée de V, et X une partie quelconque de V, alors $\mathrm{Tran}_G(X, W)$ est k-fermé. En particulier $\mathcal{N}_G(W)$ est k-fermé.*

Démonstration.
Rappelons que $\mathrm{Tran}_G(X, V) \underset{\text{déf}}{=} \{g \in G \ , \ g \cdot X \subset V\}$
Soit $x \in V(k)$ et $\begin{array}{rccc} \alpha_x : & G & \to & V \\ & g & \mapsto & g \cdot x \end{array}$. C'est un morphisme défini sur k car l'action l'est, donc $\alpha_x^{-1}(W) = \mathrm{Tran}_G(\{x\}, V)$ est k-fermé.
Donc $\bigcap_{x \in X} \alpha_x^{-1}(W) = \mathrm{Tran}_G(X, W)$ est k-fermé.
En particulier, prenant $X = W$, on a $\mathrm{Tran}_G(W, W) = \mathcal{N}_G(W)$ qui est donc k-fermé. □

On applique le lemme pour $V = \mathfrak{g}$ et $W = \mathfrak{b}_\alpha$ (resp. $\mathfrak{b}_{-\alpha}$) pour finir la deuxième étape.

Troisième étape : les B_α sont définis sur k

Si k est parfait, les notions « être k-fermé » et « être défini sur k » coïncident [Hum98, 34.1]. On suppose désormais que k est un corps imparfait, donc infini de caractéristique positive. Pour la démonstration de cette étape, on distingue les cas suivant que $\mathfrak{t}$ est central ou non.

Considérons le cas où $\mathfrak{t}$ n'est pas central dans $\mathfrak{g}$. Sous cette hypothèse, on a nécessairement $[\mathfrak{t}, \mathfrak{g}_\alpha] \neq 0$ ou $[\mathfrak{t}, \mathfrak{g}_{-\alpha}] \neq 0$. Quitte à échanger les rôles de α et $-\alpha$, on peut supposer $[\mathfrak{t}, \mathfrak{g}_{-\alpha}] \neq 0$. Comme $[\mathfrak{t}, \mathfrak{g}_{-\alpha}] \subset \mathfrak{g}_{-\alpha}$ et que $\mathfrak{g}_{-\alpha}$ est de dimension 1, on a $[\mathfrak{t}, \mathfrak{g}_{-\alpha}] = \mathfrak{g}_{-\alpha}$. En écrivant l'action de $\mathfrak{t}$ sur $\mathfrak{g}$, on a donc aussi $[\mathfrak{t}, \mathfrak{g}_\alpha] = \mathfrak{g}_\alpha$. On constate que $n_\mathfrak{g}(\mathfrak{b}_\alpha) = \mathfrak{b}_\alpha$. En effet, si $X \in n_\mathfrak{g}(\mathfrak{b}_\alpha)$ s'écrit $X = X_0 + X_\alpha + X_{-\alpha}$, avec $X_0 \in \mathfrak{t}$, $X_\alpha \in \mathfrak{g}_\alpha$ et $X_{-\alpha} \in \mathfrak{g}_{-\alpha}$. alors $X_{-\alpha} = 0$ car sinon, on aurait $[\mathfrak{t}, X_{-\alpha}] = \mathfrak{g}_{-\alpha}$ et donc $[\mathfrak{b}_\alpha, X] \not\subset \mathfrak{b}_\alpha$, ce qui contredit $X \in n_\mathfrak{g}(\mathfrak{b}_\alpha)$. On applique alors le :

4.2.2 Lemme ([Bor91, 18.5]). *Soit G un groupe algébrique connexe réductif. Soit $H \leq G$ un sous-groupe fermé. On note $\mathfrak{g} = \mathrm{Lie}(G)$ et $\mathfrak{h} = \mathrm{Lie}(H)$.*

Si $\mathfrak{h}$ est définie sur k et si $\mathfrak{h} = n_\mathfrak{g}(\mathfrak{h})$, alors on a les résultats suivants :

- *$\mathcal{N}_G(\mathfrak{h})$ est défini sur k ;*
- *$H \leq \mathcal{N}_G(\mathfrak{h})$ est un sous-groupe d'indice fini ;*

– *H° est défini sur k.*

Démonstration. Posons $N = \mathcal{N}_G(\mathfrak{h}) \supset H$. On a $\mathrm{Lie}(N) \supset \mathrm{Lie}(H)$ et $\mathrm{Lie}(N) \subset n_{\mathfrak{g}}(\mathfrak{h})$. Donc, par hypothèse, $\mathrm{Lie}(N) = \mathfrak{h}$. Donc N et H ont même dimension. Comme $H \subset N$, on a l'égalité $N^\circ = H^\circ$, et H est d'indice fini dans N.

On veut réaliser N comme un stabilisateur d'un vecteur dans une représentation bien choisie. Soit $d = \dim \mathfrak{h}$, soit $E = \bigwedge^d \mathfrak{g}$ et $\pi = \bigwedge^d \mathrm{Ad} : G \to GL(E)$. On note $D = \bigwedge^d \mathfrak{h}$ la droite représentant $\mathfrak{h}$ dans E. On a $N = \mathrm{Stab}_G(D)$. En effet, $N \subset \mathrm{Stab}_G(D)$ est clair. Pour montrer l'autre inclusion, considérons $g \in \mathrm{Stab}_G(D)$. Il existe une base $(e_1, \dots, e_n)$ de $\mathfrak{g}$ telle que $(e_1, \dots, e_d)$ est une base de $\mathfrak{h}$ et $(e_{m+1}, \dots, e_{m+d})$ base de $\mathrm{Ad}(g)(\mathfrak{h})$. On a donc $D = ke_1 \wedge \cdots \wedge e_d$;
$D = \pi(g)(D) = \bigwedge^d \mathrm{Ad}(g)(\mathfrak{h}) = ke_{m+1} \wedge \cdots \wedge e_{m+d}$.
Donc $m = 1$, et ainsi $g \in N_G(\mathfrak{h})$.

On montre de même que $\mathrm{Lie}(N) = \mathrm{Stab}_{\mathfrak{g}}(D)$.

Soit $\begin{array}{rccc} f : & G & \to & G \cdot D \subset \mathbb{P}(E) \\ & g & \mapsto & g \cdot D = \pi(g)(D) \end{array}$.

$\mathfrak{h}$ est définie sur k donc $D = \bigwedge^d \mathfrak{h}$ l'est. G est défini sur k donc [Bor91, 3.13] Ad l'est. Donc π, puis f sont définies sur k elles aussi.

Montrons que f est séparable.
Le noyau de sa différentielle en l'identité $\ker d_e f = \{X \in \mathfrak{g} \ , \ \bigwedge^d \mathrm{ad}(X)(D) = D\} = \mathrm{Stab}_{\mathfrak{g}}(D) = \mathrm{Lie}(N)$ est de dimension d, donc l'image de $d_e f$ est de dimension $\dim \mathfrak{g} - d$. On sait que $\dim T_D \mathbb{P}(E) = \dim E = \dim \mathfrak{g} - d$. Pour des raisons de dimension, df est surjective. Par [Bor91, AG 17.3], f est séparable car sa différentielle en un point est surjective.

En appliquant [Bor91, 6.7], on obtient que $\mathrm{Stab}_G(D) = N$ est défini sur k. Par [Bor91, 1.2 (b)], $H^\circ = N^\circ$ est défini sur k car N l'est. □

On conclut donc que B_α est défini sur k dans le cas où $\mathfrak{t}$ est non central dans $\mathfrak{g}$.

Cas où $\mathfrak{t}$ est central dans $\mathfrak{g}$:

On reprend les notations de la proposition [3.2.2].

On pose $T' = \pi(T)$, $B' = \pi(B_\alpha)$ et $B'_- = \pi(B_{-\alpha})$. En appliquant [Bor91, 11.14] au morphisme π surjectif, on remarque que T' est un tore maximal de G' et que B' et B'_- sont deux sous-groupes de Borel de G' contenant T', oppposés par rapport à T'. D'après [Bor91, 8.4], T' est défini sur k en tant qu'image d'un tore k-déployé par un morphisme défini sur k. L'hypothèse sur $\mathfrak{g}'$ permet de se ramener au cas où $\mathfrak{t}'$ n'est pas central dans $\mathfrak{g}'$ et, en appliquant le cas précédent, on obtient que B' est défini sur k. De plus, le quotient G'/B' existe et est défini sur k ; la projection canonique $\sigma : G' \twoheadrightarrow G'/B'$ est définie sur k et surjective [Bor91, 15.7].

On pose $\tau = \sigma \circ \pi : G \twoheadrightarrow G'/B'$, définie sur k. On note $V = G'/B'$ et $x = e \cdot B' \in V$. On a une action de G sur V par $g \cdot v = \pi(g)v$, et $\tau(g) = g \cdot x$. Vérifions que τ est séparable :
$\mathrm{Stab}_G(x) = \{g \in G \ , \ \pi(g)B' = B'\} = \pi^{-1}(B') = B_\alpha$.
$X \in \ker d\tau \Leftrightarrow d\pi(X) \in \ker d\sigma = \mathfrak{b}' \Leftrightarrow X \in \mathfrak{b}_\alpha = \mathrm{Lie}(\mathrm{Stab}_G(x))$.
En appliquant [Bor91, 6.7], on obtient alors que B_α est défini sur k. Il en est de même pour $B_{-\alpha}$.

Quatrième étape : U_α est défini sur k.

En effet, $[B_\alpha, B_\alpha] = U_\alpha$ est défini sur k comme groupe dérivé [Bor91, 2.3].

Cinquième étape : U_α est k-isomorphe à $\mathbb{G}_a$

Si $\mathfrak{t}$ n'est pas central dans $\mathfrak{g}$, on pose $G' = G$ et $\pi = \mathrm{id}$. Sinon, on se donne à nouveau l'isogénie de la proposition [3.2.2]. Considérons quel que soit le cas la restriction $\widetilde{\pi} : U_\alpha \to \pi(U_\alpha)$. C'est un k-morphisme surjectif. Dans le premier cas, on a $\ker d\widetilde{\pi} = 0$. Dans le second cas, on a $\ker d\widetilde{\pi} = \mathfrak{t} \cap \mathfrak{g}_\alpha = 0$. Donc $\widetilde{\pi}$ est un k-isomorphisme.

Il reste à montrer que $\pi(U_\alpha)$ est k-isomorphe à $\mathbb{G}_a$, et il suffit de le voir lorsque $\mathfrak{t}$ n'est pas central dans $\mathfrak{g}$ quitte à composer par $\widetilde{\pi}$.

Si k est parfait, sachant que U_α et $\mathbb{G}_a$ sont isomorphes, la remarque [Bor91, 10.9] assure qu'il existe un tel isomorphisme défini sur $k^{p^{-\infty}} = k$.

On suppose k infini. Il existe donc $Y \in \mathfrak{t}(k)$ tel que $d_e\alpha(Y) \neq 0$ car c'est une équation linéaire à coefficients dans k. On a $z_{\mathfrak{g}}(Y) = \{Z \in \mathfrak{g} \ , \ [Z, Y] = 0\} = \mathfrak{t}$ car $\mathfrak{g} = \mathfrak{t} \oplus \mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha}$ et $\mathfrak{t}$ n'est pas central dans $\mathfrak{g}$. Y est semi-simple, donc par [Bor91, 9.1], on sait que $\mathcal{Z}_G(Y)$ est défini sur k et que $\mathrm{Lie}(\mathcal{Z}_G(Y)) = \mathfrak{t}$.

On sait que $T \subset \mathcal{Z}_G(Y)$ et que $\mathcal{Z}_G(Y)^\circ$ est un tore contenant T tore maximal, on a donc $\mathcal{Z}_G(Y)^\circ = T$. Par [Bor91, 10.6], on a l'isomorphisme de variétés $B_\alpha = T \ltimes U_\alpha$ (produit semi-direct). De plus, le choix de Y donne $\mathcal{Z}_{U_\alpha}(Y) = \{e\}$. Donc $\mathcal{Z}_B(Y) = B \cap \mathcal{Z}_G(Y) = T$.

Soit $\begin{array}{rccc} f : & U_\alpha & \to & \mathfrak{g}_\alpha \\ & u & \mapsto & \mathrm{Ad}\, u(Y) - Y \end{array}$. On a $f(u) = f(v) \Leftrightarrow f(v^{-1}u) = 0$. De plus, si $f(u) = 0$, alors $u \in \mathcal{Z}_{U_\alpha}(Y) = U_\alpha \cap \mathcal{Z}_B(Y) = \{e\}$. Donc l'application f est injective.

On se donne maintenant $X \in \mathfrak{g}_\alpha(k) \setminus \{0\}$ et on définit l'application $\theta : U_\alpha \to \mathbb{G}_a$ telle que $\mathrm{Ad}\, u(Y) = Y + \theta(u)X$ (i.e. $\theta(u)X = f(u)$). θ est un k-morphisme de groupes, injectif car f l'est, donc nécessairement bijectif.

$d_e\theta(X) = -[Y, X] = -\alpha(Y)X \neq 0$. Donc $d\theta$ est surjectif car $\mathrm{Lie}(\mathbb{G}_a)$ est de dimension 1, donc θ est séparable. Ainsi, θ réalise le k-isomorphisme souhaité, à savoir celui noté ε_α^{-1}, entre U_α et $\mathbb{G}_a$.

Conclusion : On a trouvé des k-isomorphismes $\varepsilon_\alpha : \mathbb{G}_a \to U_\alpha$ pour toute racine $\alpha \in \Phi(G, T)$. L'unicité de tels isomorphismes à une constante près [Spr98, 7.3.3 (i)] assure que $(T, (\varepsilon)_\alpha)$ constitue une donnée de déploiement pour le groupe G.

5 Conjugaison des k-sous-groupes paraboliques minimaux et des tores k-déployés maximaux par les points rationnels

Dans toute cette partie, G désigne un groupe connexe réductif et $\Gamma = \mathrm{Gal}(k_s/k)$.

5.1 Points rationnels des sous-groupes paraboliques

On se pose ici essentiellement des questions de corps de définition.

5.1.1 Lemme ([Bor91, 20.3]). *Si T est un tore maximal de G défini sur k, si H est un sous-groupe fermé connexe de G normalisé par T, alors sont équivalents :*

(i) *H est défini sur k.*

(ii) *H est k-fermé.*

(iii) *$(H \cap T)^\circ$ est k-fermé et $\Phi(H,T)$ est Γ-invariant.*

Démonstration. (i) $\Rightarrow$ (ii) est clair.

(ii) $\Rightarrow$ (iii) : $(H \cap T)^\circ$ est k-fermé comme composante neutre d'une intersection de k-fermés. Soit $\alpha \in \Phi(H,T)$ et $\gamma \in \Gamma$, alors $\gamma \cdot \alpha \in X^*(T)$. Soit $X \in \mathfrak{h}_\alpha \setminus \{0\}$ et $Y = \gamma \cdot X$. Alors pour tout $t \in T$, on a $\mathrm{Ad}(t)(Y) = \gamma(\mathrm{Ad}(\gamma^{-1} \cdot t)(X)) = \gamma(\alpha(\gamma^{-1} \cdot t)X) = (\gamma \cdot \alpha)(t)Y$. Donc $Y \in \mathfrak{h}_{\gamma\cdot\alpha}$. Donc $\gamma \cdot \alpha \in \Phi(H,T)$.

(iii) $\Rightarrow$ (i) : On rappelle que H est engendré par $(H \cap T)^\circ$ et les U_α, pour $\alpha \in \Phi(H,T)$ [Bor91, 13.20]. Travaillons tout d'abord sur k_s.

On sait que T est déployé sur k_s [Bor91, 8.11]. Donc d'une part, les U_α sont définis sur k_s [Théorème 4.1.2], et d'autre part $T \cap H$ est k_s-déployé en tant que tore [Bor91, 8.11], donc $(T \cap H)^\circ$ est défini sur k_s en tant que composante irréductible d'un tel groupe [Bor91, 1.2 (b)].

Observons l'invariance sous Γ. Comme par hypothèse $\Phi(H,T)$ est Γ-stable, de par leur unicité, les $U_\alpha(k_s)$, pour α parcourant $\Phi(H,T)$ sont permutés par Γ. Le tore $(T \cap H)^\circ(k_s)$ est Γ-stable car il est défini sur k_s. Les $U_\alpha(k_s)$ et $(T \cap H)^\circ(k_s)$ engendrent un sous-groupe dense et Γ-stable de H, donc par [Bor91, AG 14.4], H est défini sur k. □

5.1.2 Proposition ([Bor91, 20.5] et [Tit65, 3.14]). *Soit P un sous-groupe parabolique de G défini sur k. Alors*

1. *$\mathcal{R}(P)$ et $\mathcal{R}_u(P)$ sont définis sur k.*
2. *Les k-sous-groupes de Levi de P sont exactement les $\mathcal{Z}_G(S)$ où S est un tore maximal de $\mathcal{R}(P)$ défini sur k.*
3. *Deux k-sous-groupes de Levi de P sont $\mathcal{R}(P)(k)$ conjugués.*
4. *Soit L un k-sous-groupe de Levi de P. Alors l'unique sous-groupe parabolique P^- opposé à P contenant L est défini sur k.*
5. *La projection canonique $\pi : G \to G/P$ définit un morphisme de k-variétés surjectif sur k : $\pi_k : G(k) \twoheadrightarrow (G/P)(k)$.*

Démonstration. Comme P est un sous-groupe parabolique, il est connexe [Bor91, 11.16]. Donc [Théorème 3.2.1] P contient un tore maximal T qui est défini sur k. En fait, T est un tore maximal de G. (Oubliant le corps de base, T est inclus dans un sous-groupe de Borel qui est inclus dans P [Bor91, 11.3 et 11.2]).

1. $\mathcal{R}(P)$ est k-fermé, donc par [Bor91, 4.5] $\mathcal{R}_u(P)$ l'est aussi. Ces groupes sont normalisés par T. Par le lemme [5.1.1 (ii) $\Rightarrow$ (i)], on sait alors que $\mathcal{R}(P)$ et $\mathcal{R}_u(P)$ sont définis sur k.

2. D'après [Tit65, 3.13] P admet une décomposition de Levi, notons-la $P = L \cdot \mathcal{R}_u(P)$, choisie de telle sorte que L soit défini sur k. On peut choisir T tel qu'il soit en fait un tore maximal de L. On a $\mathcal{R}(P) = \mathcal{Z}_L^\circ \cdot \mathcal{R}_u(P)$. En effet, si $x \in \mathcal{R}(P)$ s'écrit $x = lu$ avec $l \in L$ et $u \in \mathcal{R}_u(P)$, alors $l = xu^{-1} \in \mathcal{R}(P)$ distingué dans P, donc en particulier pour tout $l' \in L$, $l'xu^{-1}l'^{-1} = xu^{-1}$. Donc $l \in \mathcal{Z}_L$. Comme $\mathcal{R}(H)$ est connexe, on a alors $l \in \mathcal{Z}_L^\circ$.

   On veut montrer que $L = \mathcal{Z}_P(\mathcal{Z}_L^\circ)$.

   L'inclusion $L \subset \mathcal{Z}_P(\mathcal{Z}_L^\circ)$ est immédiate par définition.

   Le groupe $\mathcal{Z}_P(\mathcal{Z}_L^\circ) \cap \mathcal{R}_u(P)$ est normalisé par T donc c'est le produit des U_α, pour $\alpha \in \Phi(G,T)$ qu'il contient [Tit65, 2.3]. Donc [Tit65, 3.6] $\mathcal{Z}_P(\mathcal{Z}_L^\circ) \cap \mathcal{R}_u(P) = \{e\}$. Pour des raisons de dimension, on a donc l'égalité.

   On sait que les sous-groupes de Levi de P sont les centralisateurs des tores maximaux de $\mathcal{R}(P)$ [Bor91, 14.19]. Donc $\mathcal{Z}_L^\circ$ est un tore maximal de $\mathcal{R}(P)$ défini sur k. Et réciproquement, si S est un tore maximal de $\mathcal{R}(P)$ défini sur k. Alors [4.2.1] assure que $\mathcal{Z}_G(S)$ est k-fermé. De plus ce groupe est connexe (rigidité des tores [Bor91, 8.10]) et fermé dans G. Donc par le lemme [5.1.1], $\mathcal{Z}_G(S)$ est défini sur k.

3. Soit $L_1 = \mathcal{Z}_G(S_1) = L$ le k-sous-groupe de Levi précédemment choisi et $L_2 = \mathcal{Z}_G(S_2)$ un autre k-sous-groupes de Levi de P, où S_1 et S_2 sont des tores maximaux de $\mathcal{R}(P)$ définis sur k. On a vu précédemment que $S_1 = \mathcal{Z}_{L_1}^\circ$ et $S_2 = \mathcal{Z}_{L_2}^\circ$. S_1 et S_2 sont conjugués par un unique élément de $\mathcal{R}_u(P)$ [Bor91, 11.23 (ii)]. On cherche à montrer qu'ils le sont en fait par un élément rationnel, c'est-à-dire dans $\mathcal{R}_u(P)(k)$.

   Dans une certaine extension séparable k' de k, le tore maximal T est k'-déployé, et donc fait partie d'une donnée de déploiement de G sur k' [théorème 4.1.2].

   Le groupe $\mathcal{R}_u(P)$ est normalisé par T. En appliquant [Tit65, 2.10] à $V = \mathcal{R}_u(P)$ et au tore T défini sur k, on obtient l'existence d'un élément $v \in T \cdot V(k)$ pour lequel ${}^vS_2$ est un sous-tore de T Comme T est inclus dans $\mathcal{R}(P) \cap L = \mathcal{Z}_{\mathcal{R}(P)}(\mathcal{Z}_L^\circ)$ qui est égal à $\mathcal{Z}_L^\circ = S_1$, on obtient que ${}^vS_2$ est un sous-tore de S_1. Ces tores sont donc égaux car ils sont choisis maximaux.

   Par conséquent, ${}^vL_2 = L_1$.

4. L'existence et l'unicité du groupe parabolique, noté P^-, opposé à P ayant L pour sous-groupe de Levi commun est admise [Bor91, 14.20 (i)]. L'enjeu est de montrer que celui-ci est défini sur k. On peut mettre sur $\Phi(G,T)$ un ordre tel que P soit le sous-groupe parabolique standard P_I et $P^- = P'_I$

pour une partie $I \subset D$, où D est une base de $\Phi(G,T)$ pour cet ordre. On a également $L = \mathcal{Z}_G(T_I)$. Le lemme [5.1.1] s'applique aux groupes définis sur k suivants : G, P et $L = \mathcal{Z}_G(T_I)$. Ainsi, les systèmes de racines $\Phi(G,T)$, $\Phi(P,T) = \Phi(G,T)^+ \cup [I]$ et $\Phi(L,T) = [I]$ sont Γ-stables (notations définies en [1.4]). Donc $-\Phi(I)^+ = \Phi(G,T) \setminus \Phi(P,T)$ et $\Phi(P^-,T) = [I] \cup -\Phi(G,T)^+$ sont Γ-stables. Donc le lemme [5.1.1] s'applique à P^- sous-groupe connexe fermé de G normalisé par T. Donc P^- est défini sur k.

5. On distingue le cas des corps finis de celui des corps infinis.

   Si k est un corps fini à q éléments, soit $x \in (G/P)(k)$ et $V = \pi^{-1}(x)$. Alors V est une k-variété munie d'une k-action transitive de P par translation à droite. Soit $y \in V$, on a alors $F_q(y) \in V$ donc il existe $g \in P$ tel que $y = F_q(y)g$. Or (théorème de Lang vu précédemment dans la démonstration de 3.2.1), il existe $h \in G$ tel que $g = F_q(h)h^{-1}$. Donc $yh = F_q(yh)$. Donc $yh \in V(k)$ est un antécédent de x pour π_k.

   On suppose désormais que k est infini. Par [5.1.2 4], il existe un k-sous-groupe parabolique opposé à P, considérons P^- un tel sous-groupe. Par [5.1.2 1], $\mathcal{R}_u(P^-)$ est défini sur k . Alors par [Bor91, 14.21 (iii)], π induit un isomorphisme de k-variétés $\mathcal{R}_u(P^-) \to \mathcal{U}$ où $\mathcal{U} = P^- \cdot P/P$ est un ouvert (non vide) de G/P défini sur k en tant que quotient de tels groupes. Donc $\pi_k : \mathcal{R}_u(P^-)(k) \twoheadrightarrow \mathcal{U}(k)$ est surjective.

   Soit $\Omega = \bigcup_{g \in G(k)} g\mathcal{U}$. C'est un ouvert de G/P qui est $G(k)$-invariant. De plus, $\Omega(k) \subset \pi_k(G(k))$. Soit F le complémentaire de Ω dans G/P. F est aussi $G(k)$-invariant. Comme k est infini et G connexe réductif, $G(k)$ est Zariski-dense dans G par le théorème [3.3.4]. Donc $F = G(k) \cdot F = G \cdot F$ car F est fermé. Si F était non vide, alors on aurait $G \cdot F = G$, ce qui est exclu. Donc $\Omega = G/P$. D'où le résultat.

□

5.2 Théorèmes de conjugaison

5.2.1 Théorème. *Les k-sous-groupes paraboliques minimaux de G sont conjugués par des éléments de $G(k)$.*

Démonstration. On distingue le cas des corps finis de celui des corps infinis.

Si k est fini, alors [Bor91, 16.6] G admet des sous-groupes de Borel définis sur k et ils sont $G(k)$-conjugués. Donc les k-sous-groupes paraboliques minimaux sont des sous-groupes de Borel de G et sont donc $G(k)$-conjugués.

On suppose k infini. Soit P et Q deux sous-groupes paraboliques minimaux. Par [Bor91, 20.8], $M(P,Q) = \{g \in G\,,\, {}^gP$ et Q contiennent des sous-groupes de Borel opposés$\}$ est un ouvert dense de G (on montre que cet ensemble contient un translaté d'une grosse cellule, donc un ouvert de G). Comme G est réductif et k est infini, par unirationalité [3.3.4], $G(k)$ est Zariski-dense. Ainsi, il existe $g \in G(k) \cap M(P,P) \cap M(Q,P)$ car c'est une intersection finie d'ouverts denses avec une partie dense et non vide. Les groupes ${}^gP$ et P contiennent des sous-groupes de

Borel opposés par définition, donc [Bor91, 20.7 (ii)] et [Bor91, 14.20], $L_1 = {}^gP \cap P$ est un sous-groupe de Levi commun à ces deux sous-groupes. De même, on a $L_2 = {}^gQ \cap P$ sous-groupe de Levi commun à ${}^gQ$ et P. Par [Bor91, 20.7 (i)], L_1 et L_2 sont définis sur k. Comme L_1 et L_2 sont deux k-sous-groupes de Levi de P, ils sont conjugués par un élément $x \in \mathcal{R}_u(P)(k)$ [5.1.2 3)], disons $L_1 = {}^xL_2$. Alors $L_1 = {}^{xg}Q \cap {}^xP = {}^{xg}Q \cap P$. Par unicité du sous-groupe parabolique opposé contenant un sous-groupe de Levi donné [Bor91, 14.21 (i)], on a ${}^{xg}Q = {}^gP$. Donc P et Q sont conjugués par $g^{-1}xg \in G(k)$. □

5.2.2 Théorème. *Les tores k-déployés maximaux de G sont conjugués par des éléments de $G(k)$.*

Démonstration. Soit S et S' deux tores k-déployés maximaux. Soit $L = \mathcal{Z}_G(S)$ et $L' = \mathcal{Z}_G(S')$. Par [Bor91, 20.4], L et L' sont des sous-groupes de Levi de groupes paraboliques dans G notés respectivement P et P'. On peut supposer que P et P' sont propres. En effet, si $P = G$, alors S est central donc $S \subset S'$ et maximal donc $S = S'$ et le résultat est vrai. Par [Bor91, 20.6], comme S et S' sont des tores k-déployé maximaux de G, les k-sous-groupes paraboliques correspondant P et P' sont donc minimaux. Par [5.2.1], il existe $g \in G(k)$ tel que ${}^gP' = P$. Soit $S'' = {}^gS'$. Le centre de $\mathcal{Z}_G(S)$ admet un unique plus grand sous-tore k-déployé (par commutativité) ; il s'agit de S car celui-ci est supposé maximal. Or, S'' est aussi un sous-tore k-déployé maximal de $\mathcal{CZ}_G(S)$. Par unicité, $S = S'' = {}^gS'$. □

6 Un système de Tits des groupes réductifs isotropes

6.1 Énoncé du théorème

6.1.1 Définition. On dit qu'un groupe réductif est isotrope s'il admet un tore k-déployé maximal non trivial, et qu'il est anisotrope dans le cas contraire.

On va donner une démonstration du théorème suivant.

6.1.2 Théorème ([Bor91, 21.15]). *Soit G un groupe réductif isotrope et S un tore k-déployé maximal de G. Soit P un k-sous-groupe parabolique minimal de G contenant $\mathcal{Z}_G(S)$. Soit $N = \mathcal{N}_G(S)$. On note $U = \mathcal{R}_u(P)$.*

(1) On a $G(k) = U(k) \cdot N(k) \cdot U(k) = \bigsqcup_{w \in {}_kW} P(k) \cdot w \cdot P(k)$.

(2) On définit $R = \{s_\alpha\,,\ \alpha \in {}_k\Delta\}$ et ${}_k\mathcal{T} = (G(k), P(k), N(k), R)$ (où ${}_k\Delta$ est une base d'un système de racines décrit par la suite). Alors ${}_k\mathcal{T}$ est un système de Tits.

6.2 k-racines et groupe de Weyl relatif

6.2.1 Définition. On appelle k-racines, et on note ${}_k\Phi$, l'ensemble $\Phi(G,S) \subset X^*(S)$.

On appelle groupe de Weyl relatif à k de G le quotient ${}_kW = \mathcal{N}_G(S)/\mathcal{Z}_G(S)$.

6.2.2 Remarque. ${}_k\Phi$ est un système de racines, mais n'est pas réduit en général car S n'est pas nécessairement un tore maximal de G. Étant donné une partie $\psi \subset {}_k\Phi$, on note $\psi_{nd} = \{\alpha \in \psi\,,\ \frac{1}{2}\alpha \notin \psi\}$ ses racines non divisibles. Ce système de racines est unique à isomorphisme près car les tores k-déployé maximaux de G sont conjugués [théorème 5.2.2], [Tit65, 5.1].

Soit T un tore maximal de G contenant S. On peut définir $j : X^*(T) \to X^*(S)$ l'homomorphisme restriction. Si on munit $\Phi = \Phi(G,T)$ et ${}_k\Phi$ d'ordres (en tant que systèmes de racines), alors on dit que ces ordres sont compatibles si ${}_k\Phi^+ \subset j(\Phi) \subset {}_k\Phi^+ \cup \{0\}$. Étant donné un ordre sur ${}_k\Phi$, il existe toujours un ordre qui lui est compatible sur Φ. Étant donné des bases ${}_kD$ et D de ${}_k\Phi$ et Φ respectivement, on a toujours ${}_kD \subset j(D) \subset {}_kD \cup \{0\}$ [Bor91, 21.8]. On dit que ${}_kD$ est une k-base de ${}_k\Phi$.

Le $\mathbb{R}$-espace vectoriel $X^*(S) \otimes_{\mathbb{Z}} \mathbb{R}$ peut être muni d'un produit scalaire ${}_kW$-invariant [Tit65, 5.1]. Pour un tel produit scalaire, le groupe ${}_kW$ vu comme groupe d'automorphismes de $X^*(S) \otimes_{\mathbb{Z}} \mathbb{R}$ est engendré par les symétries par rapport aux hyperplans annulant une k-racine. On peut se restreindre aux réflexions induites par une k-base pour engendrer ${}_kW$ [Tit65, 5.3].

6.2.3 Proposition-définition ([Bor91, 21.9]). **(i)** Soit α une k-racine. Alors il existe un unique k-sous groupe unipotent connexe fermé de G normalisé par $\mathcal{Z}_G(S)$ ayant pour algèbre de Lie $\mathfrak{g}_{(\alpha)} = \bigoplus_{\beta \in \eta(\alpha)} \mathfrak{g}_\beta$ où $\eta(\alpha) = j^{-1}(\alpha) \cap {}_k\Phi$.

(ii) Soit ψ une partie fermée de ${}_k\Phi^+$. Il existe un unique k-sous-groupe unipotent connexe fermé de G normalisé par $\mathcal{Z}_G(S)$ ayant $\bigoplus_{\alpha \in \psi} \mathfrak{g}_{(\alpha)}$ pour algèbre de Lie. C'est l'ensemble des produits, pour un ordre arbitraire fixé, d'éléments pris respectivement dans les groupes $U_{(\alpha)}$ pour $\alpha \in \psi_{nd}$.

6.3 Utilisation des k-sous-groupes paraboliques standard

On fixe P un k-sous-groupe parabolique minimal contenant $\mathcal{Z}_G(S)$ comme sous-groupe de Levi. On note P^- k-sous-groupe parabolique opposé à P contenant $\mathcal{Z}_G(S)$. On note $U = \mathcal{R}_u(P)$ et $U^- = \mathcal{R}_u(P^-)$. Il existe un ordre sur ${}_k\Phi$ tel que U est engendré par les $U_{(\alpha)}$, pour $\alpha \in {}_k\Phi^+_{nd}$ et U^- est engendré par les $U_{(\alpha)}$, pour $\alpha \in -{}_k\Phi^+_{nd}$[Bor91, 21.11].

Pour toute partie $I \subset {}_kD$, par [Bor91, 21.9 (ii)] $\mathcal{Z}_G(S_I)$ est engendré par $\mathcal{Z}_G(S)$ et les $U_{(\alpha)}$ pour $\alpha \in [I]$. Le produit semi-direct ${}_kP_I = \mathcal{Z}_G(S_I) \cdot U_{\Psi(I)}$ est un k-sous-groupe parabolique de G et c'en est une décomposition de Levi sur k.

6.4 Décomposition de Bruhat

Soit $w \in {}_kW$. On pose ${}_k\Phi_w = \{\alpha \in {}_k\Phi^+_{nd}, w^{-1}(\alpha) \in {}_k\Phi^+\}$ et ${}_k\Phi'_w = \{\alpha \in {}_k\Phi^+_{nd}, w^{-1}(\alpha) \in -{}_k\Phi^+\}$. Ce sont des parties fermées de ${}_k\Phi^+$ et ${}_k\Phi^+_{nd} = {}_k\Phi_w \sqcup {}_k\Phi'_w$. Par [Bor91, 21.9 (ii)], on a des k-sous-groupes unipotents connexes fermés normalisés par $\mathcal{Z}_G(S)$ uniquement déterminés, notés $U_w = U_{{}_k\Phi_w}$ et $U'_w = U_{{}_k\Phi'_w}$, d'algèbres de Lie respectives $\bigoplus_{\alpha \in {}_k\Phi_w} \mathfrak{g}_{(\alpha)}$ et $\bigoplus_{\alpha \in {}_k\Phi'_w} \mathfrak{g}_{(\alpha)}$. De plus, $U_w = \prod_{\alpha \in {}_k\Phi_w} U_{(\alpha)}$ et $U'_w = \prod_{\alpha \in {}_k\Phi'_w} U_{(\alpha)}$.

On a $U = U_w \cdot U'_w$, ${}^wU_w \subset U$ et ${}^wU'_w \subset U^-$. Donc $U_w \subset U \cap {}^wU$ et $U'_w \subset U \cap {}^wU^-$.

6.4.1 Lemme. *Pour tous $n, n' \in \mathcal{N}_G(S)$, notant $w = nS \in {}_kW$, on a :*

(1) $U \cdot n \cdot U$ est une variété lisse localement fermé dans G.

(2) L'application produit $\phi : U'_w \times \{n\} \times U \to U \cdot n \cdot U$ est un isomorphisme de variétés.

(3) Si n est un point rationnel (i.e. $n \in \mathcal{N}_G(S)(k)$) alors ϕ est définie sur k.

(4) $U \cdot n \cdot U = U \cdot n' \cdot U \Leftrightarrow n = n'$

Démonstration. On considère l'action naturelle de $U \times U$ sur G par translation à gauche et à droite.

(1) $U \cdot n \cdot U$ est une orbite de cette action, donc [Bor91, 1.8] assure que c'est une variété lisse, ouverte dans son adhérence (i.e. localement fermée).

(2) On a $U \cdot n \cdot U = U'_w \cdot U_w \cdot n \cdot U$. Comme ${}^wU_w \subset U$, on a donc $U \cdot n \cdot U = U'_w \cdot n \cdot U$. Soit $\widetilde{\phi} : U^- \times U \to U^- \cdot U$ l'application produit. C'est un isomorphisme de variétés car $U^- \cap U = \{e\}$ et $\mathrm{Lie}(U^-) \cap \mathrm{Lie}(U) = \{0\}$.

${}^wU'_w \subset U^-$ est fermé par définition, donc $\widetilde{\phi}$ se restreint en un isomorphisme de variété $\{n^{-1}\} \times U'_w \times \{n\} \times U \to n^{-1} \cdot U'_w \cdot n \cdot U = n^{-1} \cdot U \cdot n \cdot U$. En composant par une translation par n à gauche, on obtient que ϕ est un isomorphisme de variétés.

(3) D'après [5.1.2 1], U et U^- sont définis sur k. Si de plus $n \in \mathcal{N}_G(S)(k)$, alors ϕ est défini sur k.

(4) Montrons que $\mathcal{N}_G(S) \cap U^- \cdot U = \{e\}$. Soit $n \in \mathcal{N}_G(S) \cap U^- \cdot U$. On écrit $n = vu$ avec $v \in U^-$ et $u \in U$. Soit $v_1 = v^{-1}(nsn^{-1})v(nsn^{-1})^{-1}$, $n_1 = nsn^{-1}s^{-1}$ et $u_1 = sus^{-1}u^{-1}$. Comme U^- et U sont normalisés par S et $n \in \mathcal{N}_G(S)$, on a $v_1 \in U^-$, $n_1 \in S$ et $u_1 \in U$.

On a par [Bor91, 20.6] que $P = \mathcal{Z}_G(S) \cdot U$. On a par [Bor91, 14.21 (iii)] que l'application produit : $U^- \times P \to P^- \cdot P = U^- \cdot \mathcal{Z}_G(S) \cdot U$ est un isomorphisme de variétés. Donc $v_1 = 1 = n_1 = u_1$. Donc $v, n, u \in \mathcal{Z}_G(S)$. Comme $U^- \cap \mathcal{Z}_G(S) = \{e\} = U \cap \mathcal{Z}_G(S)$, on a $v = 1 = u$. Donc $n = 1$.

On a $\mathcal{N}_G(S) \cap U^- \cdot U = \{1\}$ donc $\mathcal{N}_G(S) \cap U'_w \cdot n \cdot U = \{n\}$ donc $\mathcal{N}_G(S) \cap U \cdot n \cdot U = \{n\}$. D'où le résultat.

□

On peut désormais montrer l'assertion (1) du théorème.

Démonstration de l'assertion (1) du théorème. Soit $g \in G(k)$. On veut l'écrire $g = u_1 n u_2$ avec $u_1, u_2 \in U(k)$ et $n \in N$. Comme P et ${}^gP$ sont des k-sous-groupes paraboliques (minimaux) de G, par [Bor91, 20.7 (i)], $P \cap {}^gP$ est défni sur k et contient un $\mathcal{Z}_G(S')$ avec S' tore k-déployé maximal. Comme S et S' sont des tores k-déployés maximaux de G, par [5.2.2], ils sont $G(k)$ conjugués. Par [5.1.22 et 3], $\mathcal{Z}_G(S)$ et $\mathcal{Z}_G(S')$ sont des k-sous-groupes de Levi de P, et ils sont conjugués par un élément $x \in \mathcal{R}_u(P)(k) = U(k)$, de sorte que ${}^x\mathcal{Z}_G(S') = \mathcal{Z}_G(S)$. Comme $\mathcal{Z}_G(S') \subset {}^gP$, on a $\mathcal{Z}_G(S) \subset {}^{xg}P$. On peut donc appliquer [Bor91, 21.3] (action simplement transitive de ${}_kW$ par automorphismes intérieurs sur les sous-groupes paraboliques contenant $\mathcal{Z}_G(S)$) à P et ${}^{xg}P$ pour trouver $w \in {}_kW$ représenté par $n \in N(k)$ envoyant ${}^{xg}P$ sur P, donc ${}^{nxg}P = P$. Or P étant parabolique, il est son propre normalisateur dans G [Bor91, 11.16]. Donc $nxg \in P(k) = U(k) \cdot \mathcal{Z}_G(S)(k)$, donc $g \in U(k) \cdot N(k) \cdot U(k)$.

On a ainsi montré que $G(k) = \bigcup_{w \in {}_kW} P(k) w P(k)$. Il reste à voir la disjonction des classes. Soit $w, w' \in {}_kW$ représentés par $n, n' \in N(k)$ tels que $P(k)wP(k) \cap P(k)w'P(k) \neq \emptyset$, autrement dit $n' \in P(k)nP(k)$. Alors il existe $u, v \in U(k)$ et $a, b \in \mathcal{Z}_G(S)$ tels que $n' = uanbv$, donc $U(k)n'U(k) = U(k)anbU(k)$. Par le lemme (4), on a $n' = anb$, donc $w' = w$. □

6.5 Système de Tits

Démonstration du point (2) du théorème. On a vu que N est défini sur k. Donc $P(k)$ et $N(k)$ sont des sous-groupes de $G(k)$. On pose $T = N(k) \cap P(k)$. Comme S est k-déployé, et P parabolique minimal contenant $\mathcal{Z}_G(S)$, on a par [5.1.2] et [Bor91, 20.6 (iv)] que $T = \mathcal{Z}_G(S)(k)$.

On a aussi vu que $({}_kW, R)$ est un système de Coxeter. Donc ${}_k\mathcal{T}$ est un quadruplet candidat à être un système de Tits. Vérifions les axiomes.

(T1) : Sont déjà vus $T \triangleleft N(k)$ et par définition $N(k)/T = {}_kW$. Par (1), on a $G(k) = P(k) \cdot N(k) \cdot P(k)$. Donc $G(k)$ est engendré par $P(k)$ et $N(k)$.

(T2) : On l'a déjà vu, à savoir $({}_kW, R)$ est un système de Coxeter.

(T3) : On doit montrer que $\forall r \in R \, \forall w \in {}_kW \, rP(k)w \subset P(k)\{w, rw\}P(k)$. Soit $r \in R$ et $\alpha \in {}_k\Delta$ tel que $r = s_\alpha$. Soit $w \in {}_W$. Si (T3) est vrai pour w, il l'est aussi pour rw. Comme $(rw)^{-1}(\alpha) = -w^{-1}(\alpha)$, on peut supposer que $rw^{-1}(\alpha) \in {}_k\Phi^+$.

Étudions l'action de $r \in {}_kW = \mathcal{N}_G(S)/\mathcal{Z}_G(S)$.
On a $r\mathcal{Z}_G(S)r^{-1} = \mathcal{Z}_G(S)$.

Posons $V = \prod_{\beta\in\Psi(\alpha)} U_{(\beta)}$. On a $rV(k)r^{-1} = V(k)$.
En effet, $rV(k)r^{-1} = \prod_{\beta\in\Psi(\alpha)} rU_{(\beta)}(k)r^{-1} = \prod_{\beta\in\Psi(\alpha)} U_{(r(\beta))}(k)$.
Comme $\Psi(\alpha)$ est stable par r par construction, on a donc $\prod_{\beta\in\Psi(\alpha)} U_{(r(\beta))}(k) = \prod_{\beta\in\Psi(\alpha)} U_{(\beta)}(k) = V(k)$.

On a $rU_{(\alpha)}r^{-1} \subset \mathcal{Z}_G(S_\alpha)$. On écrit $P(k) = \mathcal{Z}_G(k)\cdot U(k) = \mathcal{Z}_G(k)\cdot V(k)\cdot U_{(\alpha)}(k)$. Alors $rP(k)wP(k) = \mathcal{Z}_G(k)\cdot V(k)rU_{(\alpha)}(k)wP(k) \subset P(k)\mathcal{Z}_G(S_\alpha)rwP(k)$.

Posons $Q = P \cap \mathcal{Z}_G(S_\alpha) = \mathcal{Z}_G(S)\cdot U_{(\alpha)}$ [Bor91, 21.11] Comme P est minimal dans G, par [Bor91, 21.13 (i)], Q est minimal dans $\mathcal{Z}_G(S_\alpha)$ (sous-groupe de Levi d'un groupe parabolique [Bor91, 20.4] — et en fait de $P_{\{\alpha\}}$). Remarquons que ${}_kW(\mathcal{Z}_G(S_\alpha)) = \{1, r\}$. En appliquant (1), on obtient $\mathcal{Z}_G(S_\alpha)(k) = Q(k)\{1,r\}Q(k) = \mathcal{Z}_G(S)(k)U_{(\alpha)}(k)\{1,r\}U_{(\alpha)}(k)$.

On a donc :

$$\begin{aligned} rP(k)wP(k) &\subset P(k)\cdot\mathcal{Z}_G(S)(k)\cdot U_{(\alpha)}(k)\{1,r\}U_{(\alpha)}(k)rwP(k) \\ &= P(k)\{1,r\}rw^{rw}U_{(\alpha)}(k)P(k) \\ &= P(k)\{w,rw\}P(k) \end{aligned} .$$

En effet, $rw(\alpha) \in {}_k\Phi^+$ donne ${}^{rw}U_{(\alpha)} \subset P$. D'où le résultat.

(T4) : rUr contient $rU_{(\alpha)}r = U_{(-\alpha)}$. Donc $rUr \neq U$. □

Références

[Bor91] Armand Borel. *Linear algebraic groups.* Graduate texts in mathematics 126. Springer, 2nd edition, 1991.

[Bou81] Nicolas Bourbaki. *Éléments de Mathématique. Groupes et algèbres de Lie. Chapitres 4 à 6.* Dunod, 1981.

[Dou05] R. Douady. *Algèbre et théories galoisiennes.* Cassini, 2005.

[Hum98] James E. Humphreys. *Linear algebraic groups.* Graduate texts in mathematics 21. Springer, 4th edition, 1998.

[Ros57] Maxwell Rosenlicht. Some rationality questions on algebraic groups. *Annali di Matematica Pura ed Applicata*, 43, 1957.

[Spr98] T.A. Springer. *Linear algebraic groups.* Progress in Mathematics. Birkhäuser Boston, 2nd edition, 1998.

[Tit65] Armand Borel ; Jacques Tits. Groupes réductifs. *Publications Mathématiques de L'IHÉS*, 27, 1965.