Cours "Groupes algébriques II"

Jean Michel

Janvier-Février 2014

1 Rappels sur les groupes algébriques affines

Une référence pour cette première section est [Szamuely]. J'aime aussi le livre [Geck] de mon ami et ancien collègue.

Notre sujet est un groupe algébrique affine connexe $\mathbf{G}$ défini sur un corps k algébriquement clos. Affine équivaut à l'existence d'un plongement de $\mathbf{G}$ comme sous-groupe fermé d'un $\mathrm{GL}_n(k)$. Les éléments *semi-simples* (resp. *unipotents*) sont ceux dont l'image l'est par un tel plongement (ceci ne dépend pas d'un plongement). Tout élément $g \in \mathbf{G}$ a une *décomposition de Jordan* $g = g_s g_u$ unique où g_s est semi-simple, g_u unipotent et ils commutent. Un groupe unipotent est nilpotent ; il est connexe en caractéristique 0 ; un groupe unipotent connexe est isomorphe à un espace affine comme variété algébrique.

Nous noterons $\mathbb{G}_a = \operatorname{Spec} k[t]$ le groupe additif k^+ vu comme groupe algébrique, et $\mathbb{G}_m = \operatorname{Spec} k[t, t^{-1}]$ le groupe multiplicatif $k^\times$ vu comme groupe algébrique.

Un *tore* est un groupe algébrique $\mathbf{T}$ isomorphe à $\mathbb{G}_m^r$; r est le *rang* de $\mathbf{T}$. On pose $X(\mathbf{T}) = \operatorname{Hom}(\mathbf{T}, \mathbb{G}_m)$; on a $X(\mathbf{T}) \simeq \mathbb{Z}^r$ car un morphisme $k[t, t^{-1}] \to k[t_1, \dots, t_r, t_1^{-1}, \dots, t_r^{-1}]$ est défini par l'image de t qui doit être inversible, donc un monôme, unitaire pour avoir un morphisme de cogèbres. On pose $Y(\mathbf{T}) = \operatorname{Hom}(\mathbb{G}_m, \mathbf{T})$, qui est en dualité naturelle avec $X(\mathbf{T})$: si $\alpha \in X(\mathbf{T}), \alpha^\vee \in Y(\mathbf{T})$ alors $\alpha \circ \alpha^\vee \in \operatorname{Hom}(\mathbb{G}_m, \mathbb{G}_m) \simeq \mathbb{Z}$.

Pour un groupe algébrique affine $\mathbf{G}$, le rang maximal d'un sous-tore est le *rang* de $\mathbf{G}$.

Les *sous-groupes de Borel* sont les sous-groupes fermés connexes résolubles maximaux.

Le *radical* $\mathrm{Rad}(\mathbf{G})$ est le plus grand sous-groupe normal fermé résoluble connexe ; $\mathbf{G}$ est *semi-simple* si $\mathrm{Rad}(\mathbf{G}) = 1$.

Le *radical unipotent* $\mathrm{R_u}(\mathbf{G})$ est le plus grand sous-groupe normal fermé unipotent connexe. $\mathbf{G}$ est *réductif* si $\mathrm{R_u}(\mathbf{G}) = 1$.

$\mathbf{G}/\mathrm{R_u}(\mathbf{G})$ est réductif. Son radical est un tore central.

Proposition 1.1 (Admise)**.** *Soit* $\mathbf{B}$ *un groupe algébrique connexe résoluble et* $\mathbf{T}$ *un tore maximal de* $\mathbf{B}$*. Alors* $\mathbf{B} = \mathbf{T} \ltimes R_u(\mathbf{B})$*.*

Il en résulte que si

Lemme 1.2. $\mathbf{S}$ *est un sous-tore de* $\mathbf{B}$ *alors* $N_{\mathbf{B}}(\mathbf{S}) = C_{\mathbf{B}}(\mathbf{S})$.

Démonstration. En effet si $n \in N_{\mathbf{B}}(\mathbf{S})$ et $s \in \mathbf{S}$ alors $[n, s] \in [\mathbf{B}, \mathbf{B}] \cap \mathbf{S} \subset \mathrm{R_u}(\mathbf{B}) \cap \mathbf{S} = 1$. □

Proposition 1.3 (Admise)**.** *Dans un sous-groupe algébrique connexe* $\mathbf{G}$*, les sous-groupes de Borel sont tous conjugués et si* $\mathbf{B}$ *est un sous-groupe de Borel alors* $N_{\mathbf{G}}(\mathbf{B}) = \mathbf{B}$ *; tout élément est dans un sous-groupe de Borel.*

Le radical étant dans au moins un sous-groupe de Borel est donc dans tous et est la composante neutre de l'intersection des sous-groupes de Borel.

Proposition 1.4. *Définissons un sous-groupe parabolique* $\mathbf{P}$ *comme un sous-groupe contenant un sous-groupe de Borel ; alors*

- $\mathbf{P}$ *est connexe et* $N_{\mathbf{G}}(\mathbf{P}) = \mathbf{P}$.
- *Deux sous-groupes paraboliques distincts contenant* le même *sous-groupe de Borel ne sont pas conjugués.*

Démonstration. Si $\mathbf{P}$ est parabolique, comme les sous-groupes de Borel sont connexes, $\mathbf{P}^0$ contient un sous-groupe de Borel $\mathbf{B}$. On a $N_{\mathbf{G}}(\mathbf{P}^0) = \mathbf{P}^0$ car ses sous-groupes de Borel sont conjugués donc $N_{\mathbf{G}}(\mathbf{P}_0) = \mathbf{P}_0 N_{\mathbf{G}}(\mathbf{B})$. Comme $\mathbf{P} \subset N_{\mathbf{G}}(\mathbf{P}^0)$ on a $\mathbf{P} = \mathbf{P}^0$. Enfin, en utilisant le fait que tous les sous-groupes de Borel d'un sous-groupe parabolique sont conjugués, on voit que deux sous-groupes paraboliques conjugués contenant le même sous-groupe de Borel $\mathbf{B}$ sont conjugués par $N_{\mathbf{G}}(\mathbf{B}) = \mathbf{B}$, donc sont égaux. □

Proposition 1.5 (Admise)**.** *Pour un tore* $\mathbf{T}$*, on a* $C_{\mathbf{G}}(\mathbf{T}) = N_{\mathbf{G}}(\mathbf{T})^0$*. Les sous-groupes de Borel de* $C_{\mathbf{G}}(\mathbf{T})$ *sont les* $\mathbf{B} \cap C_{\mathbf{G}}(\mathbf{T})$ *où* $\mathbf{B}$ *est un sous-groupe de Borel de* $\mathbf{G}$ *contenant* $\mathbf{T}$*.*

Le *groupe de Weyl* $W_{\mathbf{G}}(\mathbf{T}) = N_{\mathbf{G}}(\mathbf{T})/C_{\mathbf{G}}(\mathbf{T})$ est donc fini et s'identifie à un sous-groupe de $\mathrm{GL}(X(\mathbf{T}))$.

Proposition 1.6 (Admise)**.** *Tous les tores maximaux sont conjugués. Si* $\mathbf{T}$ *est maximal,* $C_{\mathbf{G}}(\mathbf{T})$ *est nilpotent.*

Donc si $\mathbf{T}$ est maximal, par 1.5 et 1.6, $C_{\mathbf{G}}(\mathbf{T})$ est dans l'intersection des sous-groupes de Borel contenant $\mathbf{T}$. Il résulte de ceci et de 1.2 que pour $\mathbf{T}$ maximal, $W_{\mathbf{G}}(\mathbf{T})$ est en bijection avec les sous-groupes de Borel contenant $\mathbf{T}$.

Exemples de groupes réductifs

- $\mathrm{GL}_n(k) = \mathrm{Spec}\, k[t_{i,j}, \det(t_{i,j})^{-1}], i, j \in [1 \dots n]$. un tore maximal est formé des matrices diagonales $\mathrm{diag}(t_1, \dots, t_n)$. Les matrices triangulaires supérieures forment un sous-groupe de Borel. Comme l'intersection des Borels supérieurs et inférieurs est un tore, $\mathbf{G}$ est réductif.
- $\mathrm{SL}_n(k) = \mathrm{Spec}\, k[t_{i,j}]/(\det(t_{i,j}) - 1)$. Les matrices diagonales (resp. triangulaires supérieures) forment toujours un tore maximal (resp. sous-groupe de Borel).

— $\mathrm{PGL}_n(k)$. Pour voir que c'est une variété affine, on remarque que c'est le sous-groupe de $\mathrm{GL}(M_n(k))$ formé des automorphismes d'algèbres *i.e.*, tels que $g(E_{i,j})g(E_{k,l}) = \delta_{j,k}g(E_{i,l})$ où $E_{i,j}$ est nulle sauf un coefficient 1 en position i, j. Vu comme quotient de GL_n, l'image des matrices diagonales (resp. triangulaires supérieures) est un tore maximal (resp. sous-groupe de Borel).


Le centre de SL_p en caractéristique p est $\mathrm{Spec}\, k[t]/(t^p-1) = \mathrm{Spec}\, k[t]/(t-1)^p$ qui a un seul point donc comme variété est le groupe trivial, mais pas comme schéma ! Ici SL_p et PGL_p ont les mêmes points mais ne sont pas isomorphes comme schémas en groupes.

— $\mathrm{Sp}_{2n}(k)$. Soit $V = k^{2n}$ avec base $(e_1, \ldots, e_n, e'_n, \ldots, e'_1)$, muni de la forme bilinéaire *symplectique* $\langle e_i, e_j\rangle = \langle e'_i, e'_j\rangle = 0$, $\langle e_i, e'_j\rangle = -\langle e'_j, e_i\rangle = \delta_{i,j}$. Le groupe Sp_{2n} est formé des éléments de GL_{2n} préservant cette forme. Si $j = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}$ et $J = \begin{pmatrix} & j \\ -j & \end{pmatrix}$, la forme est donnée par $\langle v, v'\rangle = {}^tvJv'$ et la condition pour une matrice symplectique est ${}^tMJM = J$. Un tore maximal est formé de $\mathrm{diag}(t_1, \ldots, t_n, t_1^{-1}, \ldots, t_n^{-1})$. Un sous-groupe de Borel **B** est formé des matrices triangulaires supérieures symplectiques ; elles sont de la forme $\begin{pmatrix} B & BjS \\ 0 & j{}^tB^{-1}j \end{pmatrix}$ où B est triangulaire supérieure et S est symétrique. Il est connexe car isomorphe à la variété des matrices triangulaire $\times$ celle des matrices symétriques ; résoluble car intersection d'un résoluble avec Sp ; maximal car contenu dans un seul Borel de GL (il stabilise un seul drapeau complet).

2 Groupes de Coxeter

Soit W un groupe engendré par un ensemble S d'involutions. Tout élément de w est l'image dans W d'un mot du monoïde libre S^* sur S. On dit que $s_1 \ldots s_k \in S^*$ est une *décomposition réduite* de $w \in W$ si c'est un mot de longueur minimum d'image w, et on pose alors $l(w) = k$.

Si $s, s' \in S$, et que le produit ss' est d'ordre fini m, on note $\Delta_{s,s'}$ le mot $\underbrace{ss'ss'\cdots}_{m \text{ termes}}$. Dans W, on a la relation $\Delta_{s,s'} = \Delta_{s',s}$ dite *relation de tresse* liant s et s' (la raison de cette terminologie apparaîtra plus tard) et les deux membres sont des décompositions réduites du même élément de W. Si l'ordre de ss' est infini, on dit que $\Delta_{s,s'}$ n'existe pas.

Définition 2.1. *On dit que (W, S) où S est un ensemble d'involutions engendrant le groupe W est un système de Coxeter si*

$$\langle s \in S \mid s^2 = 1, \Delta_{s,s'} = \Delta_{s',s} \text{ quand } \Delta_{s,s'} \text{ existe}\rangle$$

est une présentation de W.

 Une telle présentation ne définit un système de Coxeter que si la longueur du mot $\Delta_{s,s'}$ est l'ordre de ss' ; il se trouve que c'est toujours le cas, mais ce n'est pas évident. On le prouve en construisant une représentation fidèle d'un tel groupe comme groupe linéaire engendré par des réflexions.

Cette représentation de réflexion amène au vocabulaire traditionnel : les éléments de S sont appelés les *réflexions élémentaires* de W, les éléments de l'ensemble R des éléments de W conjugués à un élément de S sont appelés les *réflexions* de W.

Si W possède un ensemble S d'involutions telles que (W, S) soit un système de Coxeter, on dit que W est un groupe de Coxeter, et que S est un ensemble de générateurs de Coxeter de W.

Théorème 2.2. *Soit S un ensemble d'involutions engendrant le groupe W. Les propriétés suivantes sont équivalentes :*

(i) (W, S) est un système de Coxeter.

(ii) (Condition d'échange) Si $s_1 \dots s_k$ est une décomposition réduite de w et $s \in S$ est tel que $l(sw) \leq l(w)$, alors il existe i tel que $sw = s_1 \dots \hat{s}_i \dots s_k$.

Et sous ces conditions on a :

(iii) (Lemme de Matsumoto) Deux décompositions réduites d'un même mot sont équivalentes par relations de tresses. En d'autres termes, toute application de $f : S \to M$ dans un monoïde (induisant donc une application encore notée $f : S^* \to M$) telle que $f(\Delta_{s,s'}) = f(\Delta_{s',s})$ quand $\Delta_{s,s'}$ existe est constante sur l'ensemble des décompositions réduites d'un élément donné de W.

Sous la condition additionnelle $w \in W, s \in S \Rightarrow l(ws) \neq l(w)$ on a (iii)⇒ (i).

Démonstration. Nous allons montrer (i)⇒(ii)⇒(iii), et que sous la condition que $l(ws) \neq l(w)$ pour $w \in W, s \in S$ (qui est par exemple impliquée par (ii)), alors (iii)⇒(i).

Lemme 2.3. *Soit (W, S) un système de Coxeter, et soit N l'application de S^* dans l'ensemble des parties de R qui associe à $s_1 \dots s_k$ l'ensemble des éléments de R qui apparaissent un nombre impair de fois dans la suite*

$$\{s_k, {}^{s_k}s_{k-1} \dots, {}^{s_k s_{k-1} \dots s_2}s_1\}.$$

Alors $N(s_1 \dots s_k)$ ne dépend que de l'image w de $s_1 \dots s_k$ dans w (nous le noterons $N(w)$) et il a $l(w)$ éléments.

Démonstration. Pour voir que N ne dépend que de l'image d'un élément dans W, on utilise que W est en bijection avec l'ensemble des classes de S^* pour la relation qui est la clôture transitive des équivalences $assb = ab$ et $a\Delta_{s,s'}b = a\Delta_{s',s}b$ (cela résulte de la définition d'une présentation d'un groupe dans le cas particulier où les générateurs sont des involutions). Pour vérifier que N est compatible avec ces équivalences, on utilise le fait qui est immédiat d'après la définition que $N(xy) = N(y)\dot{+}\overline{y}^{-1}N(x)\overline{y}$ où $\dot{+}$ désigne la différence symétrique

(somme modulo 2 des fonctions caractéristiques) et où $\overline{y}$ est l'image de y dans W. En utilisant cette égalité, les relations à démontrer résultent de $N(ss) = \emptyset$ et de $N(\Delta_{s,s'}) = N(\Delta_{s',s})$, égalités qui sont immédiates à vérifier. □

Maintenant (i)⇒(ii) résulte du lemme suivant :

Lemme 2.4. *Si un groupe W engendré par des involutions S possède une fonction N de W vers les parties de l'ensemble R des conjugués de S qui vérifie $N(xy) = N(y)\dot{+}y^{-1}N(x)y$ et $N(s) = \{s\}$ pour $s \in S$ alors pour tout w on a $|N(w)| = l(w)$ et (W, S) vérifie la condition d'échange.*

Démonstration. En calculant de proche en proche $N(s_1 \dots s_n)$ à partir des formules de l'énoncé on trouve $N(s_1 \dots s_n) = \{s_k\}\dot{+}\{^{s_k}s_{k-1}\}\dot{+}\dots\dot{+}\{^{s_k s_{k-1}\cdots s_2}s_1\}$. Si la décomposition $s_1 \dots s_k$ est réduite, ces éléments sont tous distincts. En effet, s'il existe $i < j$ tels que $s_k \dots s_i \dots s_k = s_k \dots s_j \dots s_k$ alors $s_i s_{i+1} \dots s_j = s_{i+1}s_{i+2} \dots s_{j-1}$ ce qui contredit le fait que la décomposition $s_1 \dots s_k$ soit réduite ; ceci montre la première assertion du lemme.

Si $l(ws) \leq l(w)$, alors $l(ws) < l(w)$. En effet $N(ws) = \{s\}\dot{+}s^{-1}N(w)s$ donc par les propriétés de la différence symétrique $l(ws) = l(w) \pm 1$. On voit aussi que si $l(ws) < l(w)$, alors $s \in s^{-1}N(w)s$ ou de façon équivalente $s \in N(w)$. Il existe donc i tel que $s = s_k \dots s_i \dots s_k$, ce qui donne $ws = s_1 \dots \hat{s}_i \dots s_k$ c.q.f.d. □

Montrons maintenant (ii)⇒(iii). Soit $f : S^* \to M$ une application comme dans l'énoncé et montrons par récurrence sur $l(w)$ que deux décompositions réduites de w ont même image dans M. Raisonnant par l'absurde, soient $s_1 \dots s_k$ et $s'_1 \dots s'_k$ deux décompositions réduites d'image différente par f. Par la condition d'échange, on a $s'_1 s_1 \dots s_k = s_1 \dots \hat{s}_i \dots s_k$, *i.e.* $s_1 \dots s_k = s'_1 s_1 \dots \hat{s}_i \dots s_k$. Par hypothèse de récurrence (applicable car les premières lettres sont égales), on a $f(s'_1 s_1 \dots \hat{s}_i \dots s_k) = f(s'_1 \dots s'_k)$ et donc on doit avoir $i = k$ sinon toujours par hypothèse de récurrence on aurait $f(s'_1 s_1 \dots \hat{s}_i \dots s_k) = f(s_1 \dots s_k)$. On arrive donc à la conclusion que $s'_1 s_1 \dots s_{k-1}$ est une autre décomposition réduite de w telle que $f(s'_1 s_1 \dots s_{k-1}) \neq f(s_1 \dots s_k)$.

Reprenant le même raisonnement à partir de ces deux dernières décompositions, on trouve que $s_1 s'_1 s_1 \dots s_{k-2}$ est une décomposition réduite de w telle que

$$f(s_1 s'_1 s_1 \dots s_{k-2}) \neq f(s'_1 s_1 \dots s_{k-1});$$

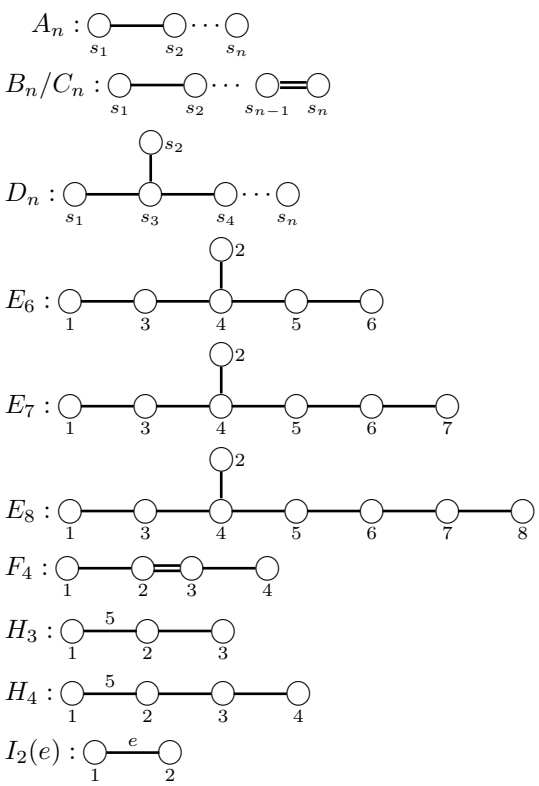
continuant ainsi de proche en proche, on trouve que $w = \Delta_{s_1,s'_1} = \Delta_{s'_1,s_1}$ et $f(\Delta_{s_1,s'_1}) \neq f(\Delta_{s'_1,s_1})$, ce qui contredit l'hypothèse.

Montrons maintenant (iii)⇒ (i) sous la condition que $l(ws) \neq l(w)$ quand $s \in S$. (i) est équivalent au fait que toute application $f : S \to G$ de S dans un groupe G (induisant donc une application encore notée $f : S^* \to G$) telle $f(s^2) = 1$ et $f(\Delta_{s,s'}) = f(\Delta_{s',s})$ induit un homomorphisme $W \to G$. On sait déjà, d'après le lemme de Matsumoto, que f induit une application bien définie $f : W \to G$. Il reste à voir que $f(w)f(w') = f(ww')$ et, puisque S engendre W, il suffit de voir que $f(s)f(w) = f(sw)$. Si $l(sw) > l(w)$ alors puisque f est définie en faisant le produit suivant une décomposition réduite le résultat est

clair. Si $l(sw) < l(w)$, alors l'égalité $f(s)^2 = 1$ permet de réécrire l'équation à démontrer $f(w) = f(s)f(sw)$ et le même raisonnement s'applique. □

On représente un groupe de Coxeter par un graphe de sommets S où on lie s et s' par une arête si l'ordre de ss' est > 2. On indique sur cette arête l'ordre de ss'. On omet toute indication si cet ordre est 3, et on met une double arête si c'est 4 et un triple arête si c'est 6.

Les groupes de Coxeter finis sont :



Un groupe de Coxeter fini est dit *groupe de Weyl* s'il a une représentation de réflexion sur $\mathbb{Q}$. C'est le cas des types A, B, D, E, F et de $I_2(e)$ pour $e \in \{2, 3, 4, 6\}$. On note G_2 pour $I_2(6)$.

Proposition 2.5. *Soit (W, S) un système de Coxeter. Alors les propriétés suivantes sont équivalentes pour un élément $w_0 \in W$:*

(i) $l(w_0 s) < l(w_0)$ pour tout $s \in S$.

(ii) $l(w_0 w) = l(w_0) - l(w)$ pour tout $w \in W$.

(iii) w_0 est de longueur maximum parmi les éléments de W.

De plus, si un tel élément existe, c'est une involution, il est unique, et W est fini.

Démonstration. Il est clair que (ii) implique (iii) et que (iii) implique (i).

Pour démontrer que (i) implique (ii), nous allons voir par récurrence sur $l(w)$ que w_0 a une expression réduite se terminant par une expression réduite de w^{-1}. Écrivons $w^{-1} = vs$ où $l(v)+l(s) = l(w)$. Par récurrence, on peut écrire $w_0 = yv$ où $l(w_0) = l(y) + l(v)$. Par le lemme d'échange, en utilisant que $l(w_0 s) < l(w_0)$ mais que vs est réduit, on voit que $w_0 s$ est de la forme $\hat{y}v$ où $\hat{y}$ représente le mot y dont on a retiré une lettre. On en déduit que $\hat{y}vs$ est une expression réduite de w_0.

Un élément vérifiant (ii) est une involution car $l(w_0^2) = l(w_0) - l(w_0) = 0$ et il est unique car un autre w_1 est de même longueur par (iii) et $l(w_0 w_1) = l(w_0) - l(w_1) = 0$ donc $w_1 = w_0^{-1} = w_0$.

Si w_0 existe alors S est fini puisque $S \subset N(w_0)$ donc W est fini par (iii). □

Systèmes de racines

Dans cette section on fixe un espace vectoriel réel V de dimension finie ; nous notons V^* le dual de V.

Notation 2.6. Une *réflexion* $s \in \mathrm{GL}(V)$ est un élément tel que $s^2 = 1$ et $\mathrm{Ker}(s - \mathrm{Id})$ est un hyperplan. Il en résulte que s a une valeur propre -1 de multiplicité 1, et que si $\alpha \in V$ est vecteur propre pour -1 et $\alpha^\vee \in V^*$ est une forme linéaire de noyau $\mathrm{Ker}(s - \mathrm{Id})$, choisie telle que $\alpha^\vee(\alpha) = 2$, alors $s(x) = x - \alpha^\vee(x)\alpha$. On appelle α *racine* attachée à la réflexion et $\alpha^\vee$ *coracine* attachée à la réflexion. Ils sont uniques à scalaires (inverses) près.

Définition 2.7. *On appellera* système de racines *des ensembles finis* $\Phi \subset V, \Phi^\vee \subset V^*$ *en bijection* $\alpha \mapsto \alpha^\vee$*, tels que* Φ *engendre* V*, et vérifiant* $\alpha^\vee(\alpha) = 2$ *et* Φ *est stable par la réflexion* s_α *de racine* α *et coracine* $\alpha^\vee$*.*

Propriétés 2.8.
- Le système est dit *cristallographique* (ou défini sur $\mathbb{Z}$) si $\alpha^\vee(\beta) \in \mathbb{Z}$ pour tous α, β.
- Le système est dit *réduit* si pour tout α on a $\Phi \cap \mathbb{R}\alpha = \{\alpha, -\alpha\}$.

Nous différons de Bourbaki en ce que nous ne supposons pas *à priori* le système cristallographique. On peut attacher un tel système à tout groupe de Coxeter fini, mais les groupes de Weyl des groupes algébriques réductifs correspondent à des systèmes de racines cristallographiques.

On se fixe maintenant un système de racines et on note W le groupe engendré par les s_α. Il est fini car ses éléments sont déterminés par la permutation de Φ qu'ils définissent. Il existe donc un produit scalaire $(,)$ invariant par W.

Lemme 2.9. *Si on identifie* V *à* V^* *par* $(,)$ *alors* $\alpha^\vee = \frac{2\alpha}{(\alpha,\alpha)}$.

Démonstration. Puisque le produit scalaire est invariant par s_α, on a $(s_\alpha \alpha, s_\alpha v) = (\alpha, v)$ pour tout $v \in V$, c'est-à-dire $(-\alpha, v - \alpha^\vee(v)\alpha) = (\alpha, v)$ ce qui s'écrit $\alpha^\vee(v) = \frac{2(\alpha,v)}{(\alpha,\alpha)}$. □

Utilisant cette identification on peut travailler dans un espace V euclidien et se dispenser de $\Phi^\vee$ mais cela empêche de considérer des systèmes infinis.

Nous supposerons toujours Φ réduit ; ce n'est pas essentiel, mais simplifie les énoncés et les preuves (un système non réduit, BC_n joue un rôle dans certains aspects de la théorie des groupes algébriques que nous n'aborderons pas).

Théorème 2.10. *Soit Φ un système de racines (réduit). Étant donné un ordre sur V tel que toute racine soit positive ou négative (c'est-à-dire une forme linéaire ne s'annulant pas sur Φ), ce qui donne une partition $\Phi = \Phi^+ \sqcup -\Phi^+$, il existe une unique base $\Pi \subset \Phi^+$ de V telle que $\Phi^+ = \Phi \cap \mathbb{R}_{\geq 0}\Pi$.*

Démonstration. Remarquons qu'on peut obtenir une partie minimale Π de Φ^+ telle que $\Phi^+ = \Phi \cap \mathbb{R}_{\geq 0}\Pi$, en supprimant de façon répétée les éléments combinaison positive d'autres éléments de Π.

Lemme 2.11. *Pour Π comme ci-dessus, $(\alpha, \beta) \leq 0$ pour $\alpha, \beta \in \Pi, \alpha \neq \beta$.*

Démonstration. Supposons au contraire $(\alpha, \beta) > 0$. Alors $s_\alpha(\beta) = \beta - c\alpha$ où $c = \frac{2(\alpha,\beta)}{\alpha,\alpha} > 0$. On a soit $s_\alpha(\beta) \in \Phi^+$, soit $-s_\alpha(\beta) \in \Phi^+$.

Dans le premier cas, par hypothèse $s_\alpha(\beta) = \sum_{\gamma\in\Pi} c_\gamma\gamma$ avec $c_\gamma \geq 0$. Il vient $\sum_{\gamma\in\Pi-\{\beta\}} c_\gamma\gamma + c\alpha + (c_\beta - 1)\beta = 0$. Il serait absurde que $c_\beta - 1 \geq 0$ car une somme non nulle de vecteurs positifs ne peut être nulle. Mais alors on a exprimé β comme élément de $\mathbb{R}_{\geq 0}(\Pi - \{\beta\})$ ce qui contredit la minimalité de Π.

Dans le deuxième cas, écrivant $-s_\alpha(\beta) = \sum_{\gamma\in\Pi} c_\gamma\gamma$ avec $c_\gamma \geq 0$, il vient $\sum_{\gamma\in\Pi-\{\alpha\}} c_\gamma\gamma + \beta + (c_\alpha - c)\alpha = 0$, et de même on doit avoir $c_\alpha - c < 0$ ce qui exprime α comme élément de $\mathbb{R}_{\geq 0}(\Pi - \{\alpha\})$, contredisant la minimalité de Π. □

Voyons maintenant que les éléments de Φ sont linéairement indépendants. Sinon, on peut écrire une relation de dépendance linéaire sous la forme $v = \sum_{\alpha\in\Pi_1} c_\alpha\alpha = \sum_{\beta\in\Pi_2} c_\beta\beta$ où v est un vecteur non nul, où $c_\alpha, c_\beta \geq 0$ et où $\Pi = \Pi_1 \sqcup \Pi_2$. Mais alors on a $0 < (v, v) = (\sum_{\alpha\in\Pi_1} c_\alpha\alpha, \sum_{\beta\in\Pi_2} c_\beta\beta) \leq 0$, une contradiction.

Voyons enfin que Π est unique : s'il y a 2 bases $\Pi \neq \Pi'$ on peut trouver $\alpha \in \Pi - \Pi'$; exprimé sur Π' : $\alpha = \sum_{\beta\in\Pi'} c_\beta\beta$, puis ré-exprimons chaque β dans Π : les β étant différents de α vont faire intervenir une racine différente de α (on utilise ici que le système est réduit) et cette racine va rester en effectuant la somme car les coefficients sont positifs ; d'où une contradiction. □

Un Φ^+ comme ci-dessus est appelé un *système de racines positives* et un Π comme ci-dessus un *système de racines simples*.

On notera que dans la base Π les coefficients de la matrice de s_α sont 1 ou $-\alpha^\vee(\beta)$ donc W agit par des matrices à coefficients entiers si le système est cristallographique.

Proposition 2.12. *Deux systèmes de racines positifs (resp. simples) sont conjugués sous W.*

Démonstration.

Lemme 2.13. *Soit $\alpha \in \Pi$. Alors α est la seule racine positive dont s_α change le signe.*

Démonstration. Si $\beta \in \Phi^+ - \{\alpha\}$ alors $\beta = \sum_{\gamma\in\Pi} c_\gamma\gamma$ où au moins un $c_\gamma > 0$ pour $\gamma \neq \alpha$, sinon $\beta \in \Phi^+ \cap \mathbb{R}_{\geq 0}\alpha = \{\alpha\}$. Mais alors $s_\alpha(\beta) = \beta - \alpha^\vee(\beta)\alpha$ a même coefficient sur l'élément γ de la base Π, et comme toute racine a tous ses coefficients sur Π non nuls de même signe, $s_\alpha(\beta)$ doit être positif. □

Nous utilisons le lemme pour conjuguer par W un système Φ_1^+ sur Φ^+ en procédant par récurrence sur $|\Phi^+ \cap -\Phi_1^+|$. Si ce cardinal est non nul, alors on ne peut avoir $\Pi \cap -\Phi_1^+ = \emptyset$. Soit α dans ce dernier ensemble. Alors, comme $s_\alpha(\Phi^+) = \Phi^+ - \{\alpha\} + \{-\alpha\}$, l'ensemble $s_\alpha(\Phi^+)$ est un système de racines positif tel que $|s_\alpha(\Phi^+) \cap -\Phi_1^+| = |\Phi^+ \cap -\Phi_1^+| - 1$. □

Du lemme 2.13 on tire le

Corollaire 2.14. *Toute racine est dans l'orbite de Π sous W.*

Démonstration. Il suffit de le voir pour Φ^+ puisqu'une racine α change de signe par s_α. Soit $\alpha = \sum_{\gamma\in\Pi} c_\gamma\gamma \in \Phi^+ - \Pi$; comme $0 < (\alpha,\alpha) = \sum_{\gamma\in\Pi} c_\gamma(\alpha,\gamma)$ il existe γ tel que $(\alpha,\gamma) > 0$. Alors $\alpha' = s_\gamma(\alpha)$ est positif par 2.13 et est obtenu en retirant un multiple positif de γ à α. Donc si on pose $h(\alpha) = \sum_\gamma c_\gamma$ on a $h(\alpha') < h(\alpha)$. Tant que $\alpha' \notin \Pi$, on peut continuer. Comme Φ^+ est fini ce processus doit s'arrêter, sur un élément de Π. □

Il résulte de la preuve du corollaire que toute racine est conjuguée à une racine de Π par une suite de $s_\gamma, \gamma \in \Pi$. En particulier tout s_α est dans le groupe engendré par les $\{s_\gamma\}_{\gamma\in\Pi}$, donc W est engendré par les $\{s_\gamma\}_{\gamma\in\Pi}$.

Nous allons montrer que W est un groupe de Coxeter à l'aide du lemme suivant :

Lemme 2.15. *Soit W un groupe engendré par un ensemble d'involutions S et soit $\{D_s\}_{s\in S}$ un ensemble de parties de W contenant 1, telles que $D_s \cap sD_s = \emptyset$ pour tout $s \in S$, et telles que pour $s, s' \in S$ on ait $w \in D_s, ws' \notin D_s \Rightarrow ws' = sw$. Alors (W,S) est un système de Coxeter, et on a $D_s = \{w \in W \mid l(sw) > l(w)\}$.*

Démonstration. Soit $s_1 \dots s_k$ une décomposition réduite de $w \notin D_s$ et soit i minimal tel que $s_1 \dots s_i \notin D_s$ ($i > 0$ puisque $1 \in D_s$). Alors de $s_1 \dots s_{i-1} \in D_s$ et $s_1 \dots s_i \notin D_s$ on tire $ss_1 \dots s_{i-1} = s_1 \dots s_i$, d'où $sw = s_1 \dots \hat{s}_i \dots s_k$ (et $l(sw) < l(w)$). Si $w \in D_s$ alors $sw \notin D_s$ et appliquant le même raisonnement à sw on a $l(w) < l(sw)$. Au total on a donc vérifié la condition d'échange, d'où le résultat. □

Proposition 2.16. *(W,S) où $S = \{s_\alpha \mid \alpha \in \Pi\}$ est un système de Coxeter.*

Démonstration. On utilise 2.15 avec $D_{s_\alpha} = \{w \in W \mid w^{-1}(\alpha) > 0\}$. La condition $D_{s_\alpha} \cap s_\alpha D_{s_\alpha} = \emptyset$ est claire. Supposons maintenant que $w \in D_{s_\alpha}$ et $ws_{\alpha'} \notin D_{s_\alpha}$, c'est-à-dire $w^{-1}(\alpha) > 0$ et $s_{\alpha'}w^{-1}(\alpha) < 0$. Comme s'_α ne change le signe que de α', on doit avoir $w^{-1}(\alpha) = \alpha'$. Comme w préserve le produit scalaire, il conjugue $s_{\alpha'}$ sur s_α, d'où le résultat. □

Lemme 2.17. *(i) L'ensemble $N(w)$ de 2.3 est $\{s_\alpha \mid \alpha \in \Phi^+, w(\alpha) < 0\}$.*

(ii) L'élément w_0 de 2.5 vérifie $w_0(\Phi^+) = \Phi^-$.

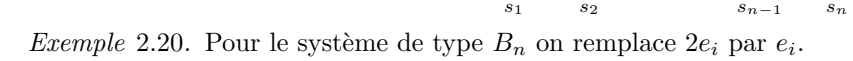
Démonstration. Si on pose $N'(w) = \{s_\alpha \mid \alpha \in \Phi^+, w(\alpha) < 0\}$ et que $N(w)$ est comme en 2.3 on montre que $N(w) = N'(w)$ par récurrence sur la longueur de w : si $w = vs$ avec $s \in S, l(w) > l(v)$ il résulte de la définition aussi bien pour N que pour N' que $N(w) = s \cup sN(v)s$ et $N'(w) = s \cup sN'(v)s$.

Pour (ii), si $w \in W$ et $N(w) \neq \Phi^+$ il existe $\alpha \in \Pi$ tel que $w(\alpha) > 0$. Alors par 2.16 et 2.15 on a $l(s_\alpha w) > l(w)$. Ce processus s'arrête quand on tombe sur w_0 tel que $N(w_0) = \Phi^+$. □

Exemple 2.18. Système de racines de type A_{n-1}. Soit $\{e_1, \ldots, e_n\}$ une base orthonormée de $\mathbb{R}^n$. Alors $\Phi = \{e_i - e_j\}_{i,j\in[1,\ldots n],i\neq j}$ est un système de $n(n-1)$ racines dans l'espace V de dimension $n-1$ qu'il engendre. Les vecteurs avec $i > j$ sont un système positif pour la forme linéaire $x \mapsto (x, ne_1 + (n-1)e_2 + \ldots + e_n)$. On a $\Pi = \{e_i - e_{i+1}\}_{i=1,\ldots,n-1}$. Si on pose $\alpha_i = e_i - e_{i+1}$, on a $e_i - e_j = \alpha_i + \alpha_{i+1} + \ldots + \alpha_j$ pour $i < j$. Le groupe W s'identifie au groupe symétrique permutant les e_i : $s_{e_i-e_j}$ échange e_i et e_j et fixe les autres vecteurs de base. Le graphe de Coxeter de A_n est 

.

Exemple 2.19. Système de racines de type C_n.

Cette fois il y a $2n^2$ racines dans $\mathbb{R}^n$, les $\pm 2e_i$ et $\pm e_i \pm e_j$. Pour la même forme linéaire qu'avant on a $\Phi^+ = \{2e_i\}_i \cup \{e_i \pm e_j\}_{i<j}$ et on a $\Pi = \{e_1 - e_2, \ldots, e_{n-1} - e_n, 2e_n\}$. Ici $s_{e_i-e_j}$ échange e_i et e_j, $s_{e_i+e_j}$ échange e_i et $-e_j$ et s_{2e_i} échange e_i et $-e_i$; le groupe W est le groupe *hyperoctaédral* qui permute les $\pm e_i$. Le graphe de Coxeter de C_n est 

.

Exemple 2.20. Pour le système de type B_n on remplace $2e_i$ par e_i.

3 Structure des groupes réductifs

Propriétés 3.1 (Structure des groupes réductifs). Soit $\mathbf{G}$ un groupe algébrique affine réductif connexe sur k, et soit $\mathbf{T}$ un tore maximal de $\mathbf{G}$. Alors

(i) Les sous-groupes unipotents de $\mathbf{G}$ fermés normalisés par $\mathbf{T}$ minimaux sont isomorphes à $\mathbb{G}_a$. Pour un tel groupe à un paramètre $x \mapsto \mathbf{u}(x)$ il existe $\alpha \in X(\mathbf{T})$ tel que pour $t \in \mathbf{T}$ on a $t\mathbf{u}(x)t^{-1} = \mathbf{u}(\alpha(t)x)$. Les α obtenus sont distincts ; donc si Φ est leur ensemble, $\alpha \in \Phi$ détermine $\mathbf{U}_\alpha \simeq \mathbb{G}_a$.

(ii) Pour tout $\alpha \in \Phi$, il existe un homomorphisme $\phi_\alpha : \mathrm{SL}_2 \to \mathbf{G}$ d'image $\langle \mathbf{U}_\alpha, \mathbf{U}_{-\alpha} \rangle$ et injectif ou de noyau $\pm \mathrm{Id} = Z(\mathrm{SL}_2)$, tel que

$$\phi_\alpha \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} = \mathbf{U}_\alpha, \quad \phi_\alpha \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix} = \mathbf{U}_{-\alpha}$$

On pose

$$\check{\alpha}(x) = \phi_\alpha \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}, \quad \dot{s}_\alpha = \phi_\alpha \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

(iii) Φ est un système de racines réduit dans $X(\mathbf{T}) \otimes \mathbb{R}$. On a $C_{\mathbf{G}}(\mathbf{T}) = \mathbf{T}$ et l'application naturelle $W := N_{\mathbf{G}}(\mathbf{T})/\mathbf{T} \to \mathrm{GL}(X(\mathbf{T}) \otimes \mathbb{R})$ identifie W au groupe de réflexions défini par Φ ; s_α est l'image de $\dot{s}_\alpha$.

(iv) Un sous-groupe fermé connexe $\mathbf{H}$ de $\mathbf{G}$ contenant $\mathbf{T}$ est engendré par $\mathbf{T}$ et les $\mathbf{U}_\alpha$ qu'il contient.

(v) Un sous-groupe unipotent $\mathbf{H}$ de $\mathbf{G}$ normalisé par $\mathbf{T}$ est égal à $\prod_{\mathbf{U}_\alpha \subset \mathbf{H}} \mathbf{U}_\alpha$ dans n'importe quel ordre.

(vi) Il y a bijection entre les sous-groupes de Borel contenant $\mathbf{T}$ et les ordres sur Φ : si $\mathbf{B}$ correspond à l'ordre Φ^+, alors $\mathrm{R_u}(\mathbf{B}) = \prod_{\alpha \in \Phi^+} \mathbf{U}_\alpha$.

(vii) Si $\alpha \neq -\beta$ alors $[\mathbf{U}_\alpha, \mathbf{U}_\beta] \subset \prod_{\{\lambda,\mu \in \mathbb{N}^\times \mid \lambda\alpha+\mu\beta \in \Phi\}} \mathbf{U}_{\lambda\alpha+\mu\beta}$.

sketch de preuve. [Springer, pages 114–141] Soit $\mathbf{T}$ un tore maximal de $\mathbf{G}$. Pour $\alpha \in X(\mathbf{T})$ on pose $\mathbf{G}_\alpha = C_{\mathbf{G}}(\mathrm{Ker}(\alpha)^0)$. Alors, en utilisant l'action adjointe de $\mathbf{T}$ sur l'algèbre de Lie $\mathfrak{G}$ de $\mathbf{G}$, on montre :

— Il y a un nombre fini de α tels que $\mathbf{G}_\alpha \neq C_{\mathbf{G}}(\mathbf{T})$ [α doit être un poids de $\mathbf{T}$ agissant sur $\mathfrak{G}$].

— Les $\mathbf{G}_\alpha$ engendrent $\mathbf{G}$ [le groupe engendré par les $\mathbf{G}_\alpha$ a même algèbre de Lie que $\mathbf{G}$].

Ensuite, on démontre que si $\mathbf{G}_\alpha$ n'est pas résoluble, alors $\mathbf{G}_\alpha/\mathrm{Rad}(\mathbf{G}_\alpha)$ est isomorphe à SL_2 ou PGL_2, car un groupe semi-simple dont le tore maximal est de dimension 1 est un de ces groupes (on voit immédiatement que le groupe de Weyl de G_α est $\mathbb{Z}/2$ car $\mathrm{GL}(\mathbb{Z}) = \pm 1$ — la preuve du reste est un peu longue).

On pose $\Phi = \{\alpha \mid \mathbf{G}_\alpha \text{ est non résoluble}\}$. On démontre, ce qui n'est pas évident, que $\mathbf{G}_\alpha/\mathrm{Rad}(\mathbf{G}_\alpha)$ se relève ce qui définit ϕ_α. Alors chaque $\mathbf{G}_\alpha$ pour $\alpha \in \Phi$ contribue une réflexion $s_\alpha \in W$ (image dans W de $\dot{s}_\alpha \in N_{\mathbf{G}}(\mathbf{T})$), et un groupe $\mathbf{U}_\alpha$ normalisé par $\mathbf{T}$ et où $\mathbf{T}$ agit par α. On a aussi $\alpha^\vee \in Y(\mathbf{T})$ qui est la restriction de ϕ_α au tore.

Φ est un système de racines réduit cristallographique : la stabilité par les s_α résulte de la construction, et le système est réduit car par construction $\mathbf{G}_{n\alpha} = \mathbf{G}_\alpha$ (la composante neutre du noyau est la même pour $n\alpha$ et α) et $\mathbf{G}_\alpha$ n'a que 2 racines $\pm\alpha$.

On montre que les s_α engendrent W par récurrence sur le rang de $\mathbf{G}$. Pour cela on utilise que W étant fini préserve un produit scalaire sur $X(\mathbf{T}) \otimes \mathbb{R}$ et le lemme :

Lemme 3.2. *Soit V un espace réel Euclidien de dimension finie et w, s deux éléments du groupe orthogonal où w n'a pas de valeur propre 1 et où s est une réflexion. Alors sw a une valeur propre 1.*

Démonstration. Puisque w n'a pas de valeur propre 1 alors $w - \mathrm{Id}$ est surjectif. Soit α une racine de s, de telle sorte que $s = x \mapsto x - \frac{2(x,\alpha)}{(\alpha,\alpha)}\alpha$ (voir lemme 2.9), et soit x tel que $(w - \mathrm{Id})(x) = \alpha$. Alors $(x, x) = (w(x), w(x)) = (x + \alpha, x + \alpha)$ implique $\frac{2(x,\alpha)}{(\alpha,\alpha)} = -1$ d'où $s(x) = x + \alpha = w(x)$. □

À cause du lemme on peut supposer que $w \in W$ a une valeur propre 1. Alors w a un point fixe dans $X(\mathbf{T})$ (car $w - \mathrm{Id}$ a un noyau dans $X(\mathbf{T}) \otimes \mathbb{Q}$) et $\mathbf{S} = \mathrm{Ker}(t \mapsto [w, t])^0$ est un sous-tore non-trivial centralisé par w. On peut alors travailler dans $C_{\mathbf{G}}(\mathbf{S})/\mathbf{S}$ qui est de rang plus petit.

Par 1.5 les $\mathbf{G}_\alpha$ résolubles sont dans l'intersection C des sous-groupes de Borel contenant $\mathbf{T}$. On démontre que $\mathrm{R_u}(C)$ est normal dans $\mathbf{G}$ d'où $\mathrm{R_u}(C) = \mathrm{R_u}(\mathbf{G})$ ([Luna] montre à partir des seuls éléments rappelés au §1 que l'intersection des $\mathrm{R_u}(\mathbf{B})$ où $\mathbf{B}$ parcourt les sous-groupes de Borel contenant $\mathbf{T}$ est $R_u(\mathbf{G})$). Donc si $\mathbf{G}$ est réductif, il n'y a pas de $\mathbf{G}_\alpha$ résolubles, $C_{\mathbf{G}}(\mathbf{T}) = \mathbf{T}$ (voir 1.6) et les $\mathbf{G}_\alpha$ sont engendrés par $\mathbf{U}_\alpha$, $\mathbf{U}_{-\alpha}$ et $\mathbf{T}$ (l'image de ϕ_α est engendrée par $\mathbf{U}_\alpha$ et $\mathbf{U}_{-\alpha}$).

On déduit (iv) de ce que $\mathbf{H}$ comme dans (iv) est engendré par les $\mathbf{G}_\alpha$ qu'il contient.

Pour (v) on démontre un théorème général sur un groupe résoluble $\mathbf{T} \rtimes \mathbf{U}$ où $\mathbf{U}$ contient des $\mathbf{U}_\alpha$ isomorphes à $\mathbb{G}_a$ sur lesquels $\mathbf{T}$ agit par des caractères α distincts qui sont tous les poids de $\mathbf{T}$ dans l'algèbre de Lie de $\mathbf{U}$: alors $\mathbf{U}$ est produit des $\mathbf{U}_\alpha$ dans n'importe quel ordre.

Pour (vi) le point essentiel est qu'un sous-groupe de Borel $\mathbf{B}$ contenant $\mathbf{T}$ définit une forme linéaire sur $X(\mathbf{T})$: on utilise une représentation rationnelle de $\mathbf{G}$ où $\mathbf{B}$ est le stabilisateur d'une droite. Cette représentation définit un élément $\chi \in X(\mathbf{T})$ (l'action de $\mathbf{T}$ sur cette droite) ; en composant avec l'action de $\mathbf{U}_\alpha \subset \mathbf{B}$ on démontre que $\langle \chi, \alpha \rangle \geq 0$.

Pour (vii) comme $\alpha \neq -\beta$ on peut les supposer positives, *i.e* dans un $R_u(\mathbf{B})$. Si on note $x \mapsto \mathbf{u}_\alpha(x)$ l'isomorphisme $k^+ \to \mathbf{U}_\alpha$, dans l'isomorphisme de (v) la multiplication est donnée par des polynômes donc il existe des polynômes P_γ tels que $[\mathbf{u}_\alpha(x), \mathbf{u}_\beta(y)] = \prod_\gamma \mathbf{u}_\gamma(p_\gamma(x, y))$. Alors pour $t \in \mathbf{T}$ on a $p_\gamma(\alpha(t)x, \beta(t)y) = \gamma(t)p_\gamma(x, y)$ ce qui vu l'indépendance linéaire des caractères force γ à être $\lambda\alpha+\mu\beta$ et $p_\gamma = c_\gamma x^\lambda y^\mu$. On ne peut avoir par ex. $\mu = 0$ car alors en prenant $y = 0, x = 1$ on aurait une égalité $1 = \mathbf{u}_\alpha(c_\alpha)$. □

On notera qu'il résulte du (i) de 3.1 que pour $w \in W$ et $\alpha \in \Phi$, on a ${}^w\mathbf{U}_\alpha = \mathbf{U}_{w(\alpha)}$.

Exemple 3.3. Pour GL_n et le tore des matrices diagonales, $N_{\mathbf{G}}(\mathbf{T})$ est formé des matrices monomiales. Les matrices de permutation sont une section (représentant W) du quotient $N_{\mathbf{G}}(\mathbf{T})/\mathbf{T}$. On a $X(\mathbf{T}) \simeq \mathbb{Z}^n$. L'ensemble $\Phi = e_i - e_j$ forme un système de racines pour le produit scalaire naturel (qui n'engendre pas $X(\mathbf{T})$ mais seulement les vecteurs de somme nulle). Le groupe $\mathbf{U}_{e_i - e_j}$ est formé des

matrices de la forme $\mathrm{Id} + \lambda E_{i,j}$. Pour l'ordre de 2.18 le sous-groupe de Borel correspondant est formé des matrices triangulaires supérieures. L'image de $\Phi_{e_i - e_j}$ est formé d'un SL_2 en lignes et colonnes i, j.

Exemple 3.4. Pour SL_n les principales différences sont : Les éléments de $\mathbf{T}$ vérifient $t_1 \dots t_n = 1$. Les coracines engendrent $Y(\mathbf{T})$ (mais il y a toujours un centre, noyau des racines, formé de $\mathrm{diag}(\zeta, \dots, \zeta)$ où $\zeta^n = 1$). Le groupe de Weyl n'a pas de section car $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 = -\mathrm{Id}$.

Exemple 3.5. Pour PGL_n les racines engendrent $X(\mathbf{T})$; les images de ϕ_α sont des PGL_2.

Exemple 3.6. Pour Sp_{2n}, avec nos coordonnées $1, \dots, n, n', \dots, 1'$, il y a 3 types de groupes $\mathbf{U}_\alpha$, correspondant aux morphismes $\mathbb{G}_a \to \mathbf{G}$ donnés par :

— $\lambda \mapsto \mathrm{Id} + \lambda E_{i,j} - \lambda E_{j',i'}$ pour $\alpha = e_i - e_j$
— $\lambda \mapsto \mathrm{Id} + \lambda E_{i,j'} + \lambda E_{j,i'}$ pour $\alpha = e_i + e_j$
— $\lambda \mapsto \mathrm{Id} + \lambda E_{i,i'}$ pour $\alpha = 2e_i$

4 (B, N)-paires

Définition 4.1. *On dit que deux sous-groupes B et N d'un groupe G forment une (B, N)-paire pour G (ou un système de Tits pour G) si*

(i) B et N engendrent G et $T := B \cap N$ est normal dans N.

(ii) Le groupe $W := N/T$ est engendré par un ensemble S d'involutions.

(iii) Pour $s \in S$, $w \in W$ on a $BsB.BwB \subset BwB \cup BswB$.

(iv) Pour $s \in S$, on a $sBs \neq B$.

On verra que sous les hypothèses 4.1 on a $S = \{w \in W \mid B \cup BwB \text{ est un groupe}\}$ donc S est défini par (B, N).

Exemple 4.2. Nous allons montrer que les propriétés 3.1 impliquent que si $\mathbf{G}$ est un groupe algébrique linéaire réductif connexe et que $\mathbf{T} \subset \mathbf{B}$ est un couple formé d'un sous-groupe de Borel inclus dans un tore maximal, alors $(\mathbf{B}, N_{\mathbf{G}}(\mathbf{T}))$ est une (B, N)-paire pour $\mathbf{G}$.

Montrons d'abord que $\mathbf{B} \cap N_{\mathbf{G}}(\mathbf{T}) = \mathbf{T}$. Par 1.2 on a $N_{\mathbf{B}}(\mathbf{T}) = C_{\mathbf{B}}(\mathbf{T}) \subset C_{\mathbf{G}}(\mathbf{T}) = \mathbf{T}$.

Montrons que $\mathbf{G}$ est engendré par $\mathbf{B}$ et $N_{\mathbf{G}}(\mathbf{T})$. L'élément s_α conjugue $\mathbf{U}_\alpha$ sur $\mathbf{U}_{s_\alpha(\alpha)} = \mathbf{U}_{-\alpha}$. Donc le groupe engendré par $\mathbf{B}$ et $N_{\mathbf{G}}(\mathbf{T})$ contenant $\mathbf{T}$ et $\mathbf{U}_\alpha (\alpha \in \Phi^+)$ par 3.1 (vi), et s_α, contient tous les $\mathbf{U}_\alpha$ et par 3.1 (iv) engendre $\mathbf{G}$.

Le (ii) des axiomes des (B, N)-paires vient de ce que les s_α engendrent W et le (iv) de ce que ${}^s\mathbf{U}_\alpha = \mathbf{U}_{-\alpha}$ n'est pas dans $\mathbf{B}$.

Pour le (iii), si $s = s_\alpha$, comme $\mathbf{B} = \mathbf{T} \prod_{\beta \in \Phi^+} \mathbf{U}_\beta$, que s normalise $\mathbf{T}$ et que ${}^s\mathbf{U}_\beta = \mathbf{U}_{s_\alpha(\beta)}$ et que $s_\alpha \in \Phi^+$ si $\beta \in \Phi^+ - \{\alpha\}$, on a $\mathbf{B}s\mathbf{B}w\mathbf{B} = \mathbf{B}s\mathbf{U}_\alpha w\mathbf{B}$. Si $w^{-1}(\alpha) \in \Phi^+$ c'est égal à $\mathbf{B}sw\mathbf{B}$. Sinon on écrit $\mathbf{B}s\mathbf{U}_\alpha ssw\mathbf{B}$ où $(sw)^{-1}(\alpha) \in \Phi^+$ et, si $\mathbf{G}_\alpha = \langle \mathbf{T}, \mathbf{U}_\alpha, \mathbf{U}_{-\alpha} \rangle$ et $\mathbf{B}_\alpha = \mathbf{T}\mathbf{U}_\alpha = \mathbf{G}_\alpha \cap \mathbf{B}$, on utilise la "décomposition

de Bruhat dans $\mathbf{G}_\alpha$" : $\mathbf{G}_\alpha = \mathbf{B}_\alpha s \mathbf{B}_\alpha \cup \mathbf{B}_\alpha$ (la preuve est un calcul dans SL_2 ou PGL_2). On en déduit $s\mathbf{U}_\alpha s \subset \mathbf{B}_\alpha s \mathbf{U}_\alpha \cup \mathbf{B}_\alpha$ d'où $\mathbf{B}s\mathbf{U}_\alpha ssw\mathbf{B} \subset \mathbf{B}s\mathbf{U}_\alpha sw\mathbf{B} \cup \mathbf{B}sw\mathbf{B}$ où le premier terme est égal à $\mathbf{B}w\mathbf{B}$.

Théorème 4.3. *Si G admet une (B,N)-paire, alors*

(i) $G = \coprod_{w\in W} BwB$ ("décomposition de Bruhat").

(ii) (W,S) est un groupe de Coxeter.

(iii) La condition (iii) de 4.1 peut être raffinée en

$$BsB.BwB = \begin{cases} BswB & \text{si } l(sw) = l(w)+1 \\ BswB \cup BwB & \text{sinon} \end{cases}.$$

(iv) Pour tout $t \in N(w)$ (cf. 2.3), on a $BtB \subset Bw^{-1}BwB$.

(v) $S = \{w \in W \mid B \cup BwB$ est un groupe$\}$.

(vi) On a $N_G(B) = B$.

Démonstration. Montrons (i). Puisque B et N engendrent B, on a $G = \cup_i (BNB)^i$, et $BNB = BWB$. Si $w = s_1 \dots s_k$ avec $s_i \in S$, on a $BwB \subset Bs_1Bs_2B \dots Bs_kB$, et par 4.1(iii) on a $Bs_iB \cdot BWB \subset BWB$ d'où $BwB \cdot BWB \subset BWB$ d'où $(BWB)^2 = BWB$ d'où $G = BWB$. Il reste à voir que $BwB \neq Bw'B$ si $w \neq w'$. Montrons le résultat par récurrence sur $\inf(l(w), l(w'))$ et supposons par exemple $l(w) \leq l(w')$. Le point de départ est $l(w) = 0$ et le résultat vient de $w' \notin B$. Sinon, prenant $s \in S$ tel que $l(sw) < l(w)$, par l'hypothèse de récurrence $BswB$ ne peut être égal à $Bw'B$ ni à $Bsw'B$ donc $BswB \cap BsB.Bw'B = \emptyset$; comme on a par ailleurs $BswB \subset BsB.BwB$ on doit avoir $BwB \neq Bw'B$.

Pour montrer (ii), nous utilisons le Lemme 2.15 ; on prend $D_s = \{w \in W \mid BsBBwB = BswB\}$ (notons que la seule autre possibilité est $BsBBwB = BswB \coprod BwB$). La condition $D_s \ni 1$ est claire.

Si on avait à la fois $w \in D_s$ et $sw \in D_s$, alors de $BsB.BwB = BswB$ et $BsB.BswB = BwB$ on tire $BsB.BsB.BwB = BwB$ ce qui est absurde car $BsB.BsB = BsB \coprod B$ (sinon, si $BsB.BsB = B$, on aurait ${}^sB \subset B$ ce qui contredit 4.1(iv)).

Il reste à voir $w \in D_s, ws' \notin D_s \Rightarrow ws' = sw$. L'hypothèse $ws' \notin D_s$ implique $BsB.Bws'B = Bsws'B \coprod Bws'B$; en particulier $BsBws'$ rencontre $Bws'B$; en multipliant par $s'B$ à droite on en déduit que $BsBwB$ rencontre $Bws'Bs'B \subset (BwB \coprod Bws'B)$ (pour cette dernière inclusion, on se sert de 4.1 (iii) "à l'envers" ce qui s'obtient en prenant les inverses des éléments dans 4.1(iii)). Donc $BswB = BsBwB$ (puisque $w \in D_s$) est égal à soit $Bws'B$, soit à BwB. Cette dernière possibilité étant exclue puisque $w \neq sw$, on en déduit le résultat $sw = ws'$.

On a aussi démontré (iii) au passage.

Démontrons (iv). Si $w = s_1 \dots s_k$ est une décomposition réduite, pour tout i par (iii) on a $BwB = Bs_1 \dots s_{i-1}Bs_iBs_{i+1} \dots s_kB$ et de même pour $Bw^{-1}B$

d'où

$$\begin{aligned} Bw^{-1}B.BwB &= Bs_k \dots s_{i+1}Bs_iBs_{i-1} \dots s_1Bs_1 \dots s_{i-1}Bs_iBs_{i+1} \dots s_kB \\ &\supset Bs_k \dots s_{i+1}Bs_iBs_iBs_{i+1} \dots s_kB \\ &\supset Bs_k \dots s_{i+1}Bs_iBs_{i+1} \dots s_kB \\ &\supset Bs_k \dots s_{i+1}s_is_{i+1} \dots s_kB \end{aligned}$$

d'où le résultat.

(v) Résulte immédiatement de (iv), qui implique que $B \cup BwB$ ne peut être un groupe que si $|N(w)| = 1$.

(vi) en résulte aussi. Si $g \in BwB$, on a ${}^gB = B \Leftrightarrow {}^wB = B \Leftrightarrow BwBw^{-1}B = B$ ce qui par (iv) ne se produit que pour $w = 1$. □

Remarque 4.4. Dans un groupe muni d'une (B, N)-paire, on appelle sous-groupes de Borel les conjugués de B. Un autre façon d'exprimer la décomposition de Bruhat est de dire que toute paire de sous-groupes de Borel est conjuguée à une paire $(B, {}^wB)$ pour $w \in W$. On dit que la paire est *en position relative* w.

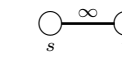
Il en résulte que, si on appelle tores les conjugués de T, l'intersection de deux sous-groupes de Borel contient toujours un tore (car la paire $(B, {}^wB)$ en contient un).

Exemple 4.5. Dans le cas de GL_n une matrice m est dans BwB si et seulement si elle a les mêmes rangs de mineurs que la matrice de permutation w parmi les mineurs "en bas à gauche", c'est-à-dire les rangs des sous-matrices $m_{i,j}$ données par les lignes $i, \dots, n$ et les colonnes $1, \dots, j$. En effet, on voit :

— Les rangs des $m_{i,j}$ sont invariants par multiplication à droite ou à gauche de m par une matrice triangulaire supérieure.

— La matrice m d'une permutation w est caractérisée par les rangs des $m_{i,j}$ qui sont égaux à $|\{k <= j \mid w(k) \geq i\}|$.

Si $\{F_i\}$ et $\{F'_i\}$ sont deux drapeaux complets, $m_{i,j} = \dim \frac{F_i \cap F'_j}{F_{i-1} \cap F'_j + F_i \cap F'_{j-1}}$ est une matrice de permutation qui donne leur position relative.

Exemple 4.6. Une (B, N)-paire "exotique" : $G = \mathrm{GL}_n(\mathbb{Q}_p)$; N=matrices monomiales, B=matrices à coefficients dans $\mathbb{Z}_p$ dans la partie triangulaire supérieure (incluant la diagonale) et à coefficients sous la diagonale dans $p\mathbb{Z}_p$ (B est un *sous-groupe d'Iwahori* : un sous-groupe dans $\mathrm{GL}_n(\mathbb{Z}_p)$ qui tombe en réduction dans un sous-groupe de Borel de $\mathrm{GL}_n(\mathbb{F}_p)$). Alors W est de type $\tilde{A}_n$ ("affine" A_n). Pour $n = 2$, W est le groupe diédral infini, de diagramme de Coxeter 

, engendré par $s = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et $t = \begin{pmatrix} 0 & p \\ -p^{-1} & 0 \end{pmatrix}$.

5 Sous-groupes Paraboliques

Soit G un groupe muni d'une (B, N)-paire, et soit $T = B \cap N$ et (W, S) le système de Coxeter de 4.3(ii). On appelle sous-groupes paraboliques les sous-groupes contenant un sous-groupe de Borel, et tores les conjugués de T.

Dans un système de Coxeter (W, S), pour $I \subset S$, on note W_I le sous-groupe de W engendré par I — par la condition d'échange (ii) du théorème 2.1 il est clair que (W_I, I) est un système de Coxeter.

Proposition 5.1. *(i) Les sous-groupes paraboliques contenant B sont les $P_I := BW_IB$ pour $I \subset S$.*

(ii) Si $g \in G$ est tel que ${}^gB \subset P_I$ alors $g \in P_I$.

Il résulte de (ii) que deux sous-groupes paraboliques différents contenant B ne sont pas conjugués, et que $N_{\mathbf{G}}(P_I) = P_I$.

Démonstration. Soit P un groupe contenant B et soit $w \in W$ tel que $BwB \subset P$. Alors $Bw^{-1}BwB \subset B$ donc par 4.3 (iv), on a $BtB \subset P$ pour tout $t \in N(w)$. Si $s_1 \dots s_k$ est une décomposition réduite de W, on a donc $Bs_kB \subset P$, $Bs_ks_{k-1}s_k \subset P, \dots$ ce qui implique de proche en proche $Bs_iB \subset P$ pour tout i ; d'où $P \supset BW_IB$ où $I = \{s_1, \dots, s_k\}$; d'où (i).

Démontrons (ii). Supposons ${}^gB \subset P_I$ et soit $w \in W$ tel que $g \in Bw^{-1}B$. Alors $P_I \supset BgBg^{-1}B = BwBw^{-1}B$ d'où par le raisonnement de (i) $w \in W_I$ donc $g \in P_I$. □

Nous aurons besoin des notions suivantes dans un système de Coxeter (W, S) avec $I \subset S$:

Lemme-Définition 5.2. *$w \in W$ est dit I-réduit s'il vérifie une des conditions équivalentes suivantes :*

(i) Pour tout $v \in W_I$, on a $l(vw) = l(v) + l(w)$.

(ii) Pour tout $s \in I$, on a $l(sw) > l(w)$.

(iii) w est de longueur minimum dans W_Iw.
Il y a un seul élément I-réduit dans W_Iw.

Démonstration. Il est clair que (iii)⇒(ii) car (iii) implique que $l(sw) \geq l(w)$. Montrons que non (iii)⇒ non (ii). Si w' n'est pas de longueur minimum dans W_Iw', c'est-à-dire que $w' = vw$ avec $v \in W_I$ et $l(w) < l(w')$, en ajoutant un à un les termes d'une décomposition réduite de v à w et en appliquant à chaque fois le lemme d'échange, on trouve une décomposition réduite $\hat{v}\hat{w}(= vw = w')$ où on a noté $\hat{v}$ (resp. $\hat{w}$) le produit d'une suite extraite stricte d'une décomposition réduite de v (resp. w). Comme $l(\hat{w}) \leq l(w) < l(w')$, on a $l(\hat{v}) > 0$, donc il existe une décomposition réduite de w' commençant par un élément de I, donc w' ne vérifie pas (ii).

Il est clair que (i)⇒(iii). On a non (i)⇒ non (iii) car si $l(vw) < l(v) + l(w)$ alors une décomposition réduite de vw est de la forme $\hat{v}\hat{w}$ où $l(\hat{w}) < l(w)$. Donc $\hat{w} \in W_Iw$ et est de longueur inférieure à celle de w.

Enfin un élément vérifiant (i) est clairement unique dans W_Iw. □

On a évidemment la notion de réduit-I qui vérifie le lemme symétrique.

Corollaire 5.3. *On a $P_I\backslash G/B \simeq W_I\backslash W \simeq \{w \in W \mid w \text{ est } I\text{-réduit}\}$.*

Démonstration. C'est clair : la classe $P_I g B$ pour $g \in BvB$ est $P_I w B$ où w est l'élément de longueur minimale de $W_I v$. □

Lemme-Définition 5.4. *Soient I et J deux parties de S. Un élément $w \in W$ est dit I-réduit-J s'il vérifie une des propriétés équivalentes suivantes :*

(i) w est à la fois I-réduit et réduit-J.

(ii) w est de longueur minimale dans $W_I w W_J$.

(iii) Tout élément de $W_I w W_J$ s'écrit de façon unique sous la forme xwy avec $x \in W_I$, $y \in W_J$, $l(x) + l(w) + l(y) = l(xwy)$ et xw réduit-J.

Par (iii) il y a un unique élément I-réduit-J dans une double classe, qui est de longueur minimum ; par symétrie on a l'énoncé analogue en remplaçant dans (iii) la condition que xw est réduit-J par celle que wy est I-réduit.

Démonstration. Montrons d'abord que deux éléments w et w' d'une même double classe et vérifiant (i) sont de même longueur. Écrivons $w' = xwy$ avec $x \in W_I$ et $y \in W_J$; on a donc $w'y^{-1} = xw$ et $x^{-1}w' = wy$; en utilisant les définitions de I-réduit et réduit-J et $l(y^{-1}) = l(y)$, $l(x^{-1}) = l(x)$ on en déduit $l(w') + l(y) = l(x) + l(w)$ et $l(x) + l(w') = l(w) + l(y)$, d'où $l(x) = l(y)$ et $l(w) = l(w')$. Comme clairement (ii)⇒(i) cette longueur unique doit être la longueur minimale, donc (i)⇔(ii).

Montrons maintenant (ii)⇒(iii). Soit w vérifiant (ii) ; Soit xwy une écriture de $v \in W_I w W_J$ où on a choisi $l(x)$ minimal. En appliquant le lemme d'échange on peut écrire une décomposition réduite de xwy sous la forme $\hat{x}\hat{w}\hat{y}$ où $\hat{x}$ (resp. $\hat{w}$, $\hat{y}$) est extrait d'une décomposition réduite de x (resp. w, y). On a nécessairement $\hat{w} = w$ sinon w ne serait pas de longueur minimum dans sa double classe. Mais alors on a nécessairement $\hat{x} = x$ vu l'hypothèse de minimalité de $l(x)$, d'où $\hat{y} = y$ et donc $l(x) + l(w) + l(y) = l(xwy)$. L'élément xw est réduit sinon on peut écrire $xw = v'y'$ où $v' \in W_I w W_J$, $y' \in W_J - \{1\}$ et $l(v') + l(y') = l(xw)$. En appliquant ce qu'on vient de démontrer on a $v' = x''wy''$ avec $l(x'') + l(w) + l(y'') + l(y') = l(x) + l(w)$ ce qui implique $l(x'') < l(x)$ contredisant la minimalité de $l(x)$. On a unicité puisque xw est unique comme élément J-réduit.

Enfin on a clairement (iii)⇒(ii). □


Il est à noter que toute écriture xwy ne satisfait pas (iii) ; considérer par exemple le cas $w = 1$ et $I = J$; la situation est moins bonne de ce point de vue que dans le cas I-réduit.

Corollaire 5.5. *On a $P_I \backslash G / P_J \simeq W_I \backslash W / W_J \simeq \{w \in W \mid w \text{ est } I\text{-réduit-}J\}$ par les applications naturelles entre ces ensembles.*

Démonstration. Considérons une double classe $P_I g P_J$. D'après la décomposition de Bruhat, on a $g \in BwB$ pour un certain $w \in W$, et donc $P_I g P_J = P_I w P_J$. Comme les représentants de W_I et W_J sont respectivement dans P_I et P_J, on

a finalement $P_I g P_J = P_I W_I w W_J P_J$, d'où une application bien définie surjective de $W_I \backslash W / W_J$ sur $P_I \backslash G / P_J$. Pour montrer qu'elle est injective, il suffit de démontrer que $P_I w P_J = B W_I w W_J B$. A priori, on a $P_I w P_J = B W_I B w B W_J B$ où on peut choisir w de longueur minimum dans sa double classe. Alors w est I-réduit donc $B W_I B w B W_J B = B W_I w B W_J B$ par 4.3(iii). Par application répétée du symétrique de 4.1(iii) on voit que pour $y \in W_J$ on a $B W_I w B y B \subset B W_I w W_J B$.

La deuxième bijection de l'énoncé est le lemme 5.4. □

6 Parties closes

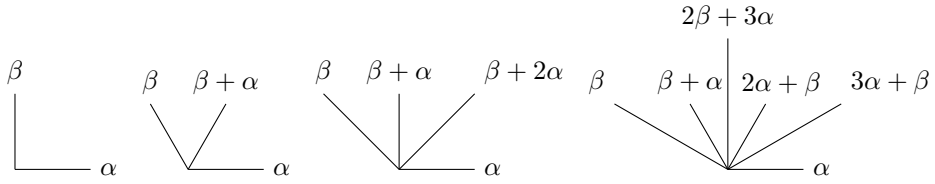
Nous avons besoin de quelques rappels supplémentaires sur les systèmes de racines cristallographiques. Soit Φ un système de racines réduit cristallographique, Π une base des racines, et (W, S) le système de Coxeter correspondant, où $S = \{s_\alpha\}_{\alpha \in \Pi}$.

Pour $I \subset \Phi$ nous noterons W_I le sous-groupe engendré par $\{s_\alpha\}_{\alpha \in I}$. Si $I \subset \Pi$, c'est le groupe de Coxeter associé au système $\Phi_I = \Phi \cap \langle I \rangle$; en effet, Φ_I est clairement un sous-système ; et I en est une base, car l'écriture d'une racine de Φ_I sur Π ne fait intervenir que des éléments de I.

On dit que $\Psi \subset \Phi$ est *clos* si $\alpha, \beta \in \Psi, \alpha + \beta \in \Phi \Rightarrow \alpha + \beta \in \Psi$; l'intersection de deux parties closes est clairement close.

On dit que Ψ est *symétrique* si $\Psi = -\Psi$.

Lemme 6.1. *Les systèmes de racines cristallographiques de rang 2 sont $A_1 \times A_1$, A_2, $C_2 = B_2$ et G_2.*



Démonstration. Pour 2 racines α, β on a $\alpha^\vee(\beta)\beta^\vee(\alpha) = 4\frac{(\alpha,\beta)^2}{(\alpha,\alpha)(\beta,\beta)} = 4\cos(\theta)^2$ où θ est l'angle entre α et β. Si nous choisissons des vecteurs voisins l'angle est $\leq \pi/2$ et l'intégralité de ce cosinus force un des angles $\pi/2, \pi/3, \pi/4$ ou $\pi/6$. Le rapport entre les longueurs des racines est donné par le fait que si par exemple $\alpha^\vee(\beta)\beta^\vee(\alpha) = 2$ où $\alpha, \beta \in \Pi$ à symétrie près la solution unique est $\alpha^\vee(\beta) = -1$ et $\beta^\vee(\alpha) = -2$ d'où $2(\beta, \beta) = (\alpha, \alpha)$. Pour $A_1 \times A_1$ le rapport des longueurs est arbitraire, nous l'avons choisi égal à 1. □

Un corollaire de 6.1 est

Corollaire 6.2. *(i) Si $\alpha, \beta \in \Phi$, $\alpha \neq -\beta$ et $(\alpha, \beta) < 0$ alors $\alpha + \beta \in \Phi$.*

(ii) Si $\alpha, \beta \in \Phi$ et $\alpha + n\beta \in \Phi$ pour $n \in \mathbb{N}$, alors $\alpha + m\beta \in \Phi$ aussi pour tout entier $0 \leq m \leq n$.

(iii) Soient $\alpha_1, \ldots, \alpha_k \in \Phi^+$ telles que $\alpha = \alpha_1 + \ldots + \alpha_k \in \Phi^+$. Alors si $k > 1$ il existe i tel que $\alpha - \alpha_i \in \Phi^+$.

Démonstration. Pour (i) et (ii) : α et β engendrent un sous-système de rang 2. On vérifie les propriétés de l'énoncé sur les systèmes de rang 2.

Pour (iii) comme $(\alpha, \alpha) > 0$ un des $(\alpha, \alpha_i) > 0$ donc par (i) $\alpha - \alpha_i \in \Phi$. □

Corollaire 6.3. *Si Ψ est clos et symétrique c'est un sous-système de racines de groupe de Coxeter W_Ψ.*

Démonstration. Si on prend deux racines α et β, par 6.2 (ii) on voit de proche en proche (commençant par $\alpha + \beta$, $\alpha + 2\beta$, etc...) que Ψ clos et symétrique contenant α et β contient $\alpha + n\beta$ pour tout n tel que ce soit une racine, en particulier contient $s_\alpha(\beta)$ et est donc un sous-système. □

Pour $I \subset \Pi$ il est clair que Φ_I est clos et symétrique, et que $\Phi^+ - \Phi_I$ et $\Phi^+ \cup \Phi_I$ sont clos.

Exemple 6.4. Des exemples de parties closes et symétriques qui ne sont pas de la forme Φ_I sont données par les racines de longues de B_2 (un système de type $A_1 \times A_1$) ou celles de G_2 (un sous-système de type A_2).

Proposition 6.5. *Si Ψ est clos et $\Psi \cap -\Psi = \emptyset$, alors il existe un ordre sur Φ tel que $\Psi \supset \Phi^+$.*

Démonstration. Montrons par récurrence sur k que toute somme de $k \geq 1$ éléments de Ψ est non nulle. C'est clair pour $k = 1$. Si $0 = \alpha_1 + \ldots + \alpha_k$ alors $(-\alpha_1, \alpha_2 + \ldots + \alpha_k)$ est le carré scalaire de α_1 donc est positif et il existe $i \neq 1$ tel que $(\alpha_1, \alpha_i) < 0$. Comme $\alpha_1 \neq -\alpha_i$ car $-\alpha_i \notin \Psi$ par 6.2(i) on a $\alpha_1 + \alpha_i$ racine donc dans Ψ et la somme est somme de $k - 1$ éléments.

Considérons maintenant $\gamma_k \in \Psi$ qui est somme de k éléments de Ψ. S'il existe $\alpha \in \Psi$ tel que $(\gamma_k, \alpha) < 0$ alors $\gamma_{k+1} = \alpha + \gamma_k \in \Psi$. La suite γ_k a tous ses termes distincts (car sinon on aurait une somme nulle d'éléments de Ψ) donc par finitude de Ψ doit s'arrêter sur un élément γ_k tel que $(\gamma_k, \alpha) \geq 0$ pour tout $\alpha \in P$. La forme linéaire $(\gamma_k, -)$ définit presque un ordre : il faut la modifier sur $\gamma_k^\perp$. Mais $\gamma_k^\perp \cap \Psi$ vérifie les mêmes hypothèses sur un sous-espace et on procède par récurrence. □

On dit que Ψ est parabolique si Ψ est clos et $\Psi \cup -\Psi = \Phi$; alors

Proposition 6.6. *Si Ψ est parabolique il existe un ordre sur Φ tel que $\Psi \subset \Phi^+$*

Démonstration. Soit Φ^+ un ordre qui maximise $|\Psi \cap \Phi^+|$. Montrons par l'absurde que $\Phi^+ \subset \Psi$. Sinon, il existe un élément α de la base Π associée telle $\alpha \notin \Psi$, donc $-\alpha \in \Psi$. Puisque $\alpha \notin \Psi$ on a $s_\alpha(\Psi \cap \Phi^+) \subset \Phi^+$; en appliquent s_α à nouveau on a $\Psi \cap \Phi^+ \subset s_\alpha(\Phi^+)$. Mais alors pour l'ordre $s_\alpha(\Phi^+)$ qui contient $-\alpha$ le cardinal $|\Psi \cap s_\alpha(\Phi^+)|$ a grandi, une contradiction. □

Proposition 6.7. *Si Ψ est parabolique il est de la forme $\Phi^+ \cup \Phi_I$ pour un certain I.*

Démonstration. On fixe un ordre Φ^+ de base Π tel que $\Psi \supset \Phi^+$. On pose $I = -\{-\Pi \cap \Psi\}$. Montrons que $\Psi \cap \Phi^- = \Phi_I^-$. Notons que par 2.14 toute racine positive est somme d'un nombre fini de racines de Π ; de même toute racine de Φ_I^- est somme de racines de $-I$. Montrons par récurrence sur k qu'une racine de Φ_I^- somme de k racines de $-I$ est dans Ψ. C'est vrai par hypothèse si k=1 ; sinon par 6.2(iii) la somme est $\alpha + \beta$ où $\alpha \in -I$ et $\beta \in \Phi_I^-$ est somme de $k-1$ racines de $-I$; par récurrence on a $\beta \in \Psi$ et comme $\alpha \in \Psi$ on a $\alpha + \beta \in \Psi$.

Pour la réciproque on procède de même par récurrence : un $\gamma \in \Psi \cap \Phi^-$ est somme de k racines de $-\Pi$. On écrit $\gamma = \alpha + \beta$ où $\alpha \in -\Pi$ et $\beta \in \Phi$ somme de $k-1$ racines de $-\Pi$. Comme $-\beta \in \Phi^+ \subset \Psi$ on a $\alpha = \gamma + (-\beta) \in \Psi$. Donc $\alpha \in -I$, d'où $-\alpha \in \Psi$ et d'où $\beta \in \Psi$ et on continue... □

Il résulte en particulier de cette proposition que le complémentaire d'une partie parabolique est clos.

7 Sous-groupes de rang maximum, parties quasi-closes

Si $\Psi \subset \Phi$ on pose $\mathbf{G}_\Psi^* = \langle \mathbf{U}_\alpha \mid \alpha \in \Psi \rangle$ et $\mathbf{G}_\Psi = \langle \mathbf{T}, \mathbf{U}_\alpha \mid \alpha \in \Psi \rangle$. Ces groupes sont connexes comme produit de groupes connexes, et par 3.1(iv), tout sous-groupe fermé connexe contenant $\mathbf{T}$ est de la forme $\mathbf{G}_\Psi$.

Définition 7.1. *Une partie $\Psi \subset \Phi$ est dite quasi-close si $\mathbf{G}_\Psi^*$ ne contient pas de $\mathbf{U}_\alpha$ avec $\alpha \notin \Psi$.*

Notons qu'il est équivalent que $\mathbf{G}_\Psi$ ne contienne pas de $\mathbf{U}_\alpha$ avec $\alpha \notin \Psi$, car $\mathbf{G}_\Psi / \mathbf{G}_\Psi^*$ est quotient de $\mathbf{T}$, donc un tore, donc tout $\mathbf{U}_\alpha$ est dans le noyau de ce quotient, donc dans $\mathbf{G}_\Psi^*$. L'intersection de deux parties quasi-closes est quasi-close (clair par l'absurde), et $(\mathbf{G}_\Psi \cap \mathbf{G}_{\Psi'})^0 = \mathbf{G}_{\Psi \cap \Psi'}$.

On dit qu'un groupe algébrique $\mathbf{P}$ possède une *décomposition de Levi* s'il existe un sous-groupe fermé $\mathbf{L} \subset \mathbf{P}$ (dit *sous-groupe de Levi*) tel que $\mathbf{P} = \mathrm{R_u}(\mathbf{P}) \rtimes \mathbf{L}$ ($\mathbf{L}$ est donc réductif).

Proposition 7.2. *Soit $\Psi \subset \Phi$ une partie quasi-close. Alors $\Psi_s = \{\alpha \in \Psi \mid -\alpha \in \Psi\}$ et $\Psi_u = \{\alpha \in \Psi \mid -\alpha \notin \Psi\}$ sont quasi-closes, et $\mathbf{G}_\Psi$ possède une décomposition de Levi $\mathbf{G}_\Psi = \mathbf{G}_{\Psi_u}^* \rtimes \mathbf{G}_{\Psi_s}$ (où $\mathbf{G}_{\Psi_u}^* = \mathrm{R_u}(\mathbf{G}_\Psi)$).*

Démonstration. Commençons par montrer que Ψ_s est quasi-clos L'intersection de deux parties quasi-closes étant quasi-close, il suffit de voir que $-\Psi$ est quasi-clos. Mais ceci est conséquence de l'existence de l'automorphisme d'opposition de $\mathbf{G}$ (qui induit -1 sur $X(\mathbf{T})$ et dont l'existence est garantie par 8.1).

Étant unipotent normalisé par $\mathbf{T}$, le groupe $\mathrm{R_u}(\mathbf{G}_\Psi)$ est de la forme $\mathbf{G}_{\Psi'}^*$ pour une certaine partie $\Psi' \subset \Psi$ que nous supposerons maximale donc quasi-close. Montrons que $\Psi' \subset \Psi_u$. Si $\alpha \in \Psi_s \cap \Psi'$, comme $\mathbf{U}_{-\alpha} \in \mathbf{G}_\Psi$, le groupe $\mathbf{U}_{-\alpha}$ normalise $\mathrm{R_u}(\mathbf{G}_\Psi)$ donc $[\mathbf{U}_{-\alpha}, \mathbf{U}_\alpha] \subset \mathrm{R_u}(\mathbf{G}_\psi)$ ce qui est absurde car cet ensemble contient des éléments non unipotents.

Réciproquement il suffit de voir $\Psi - \Psi' \subset \Psi_s$. Si $\alpha \in \Psi - \Psi'$ alors $\mathbf{U}_\alpha \cap \mathrm{R_u}(\mathbf{G}_\Psi) = 1$ car cette intersection étant normalisée par $\mathbf{T}$ contient $\mathbf{U}_\alpha$ si elle en contient un élément. Donc $\mathbf{U}_\alpha$ s'envoie injectivement sur un groupe radiciel du groupe $\mathbf{G}_\Psi/\mathrm{R_u}(\mathbf{G}_\Psi)$; ce groupe étant réductif a un ensemble de racines symétriques et son groupe $\mathbf{U}_{-\alpha}$ se remonte (l'image réciproque de $\mathbf{U}_{-\alpha}$ est un groupe unipotent normalisé par $\mathbf{T}$ donc produit des $\mathbf{U}_\beta$ qu'il contient et $\mathbf{U}_{-\alpha}$ doit être l'un d'entre eux). Donc $\alpha \in \Psi_s$.

On a vu que $\mathbf{G}_{\Psi_s}$ est un complément de Levi de $\mathrm{R_u}(\mathbf{G}_\Psi)$. □

Proposition 7.3. *Une partie close est quasi-close.*

Démonstration. Soit $\Psi \subset \Phi$ close et définissons Ψ_s et Ψ_u comme dans la preuve de 7.2. Il est clair que Ψ_s est clos. Remarquons aussi que si $\alpha \in \Psi$, $\beta \in \Psi_u$ et $\alpha + \beta \in \Phi$ alors $\alpha + \beta \in \Psi_u$ (sinon $\alpha + \beta \in \Psi_s$ d'où $-\alpha - \beta \in \Psi_s$ donc $\alpha + (-\alpha - \beta) = -\beta \in \Psi$ ce qui contredit $\beta \in \Psi_u$). On en déduit que Ψ_u est clos. Il existe donc un ordre tel que $\Psi_u \subset \Phi^+$. Il est claire qu'une partie positive close (ici Ψ_u) est quasi-close. En effet par 3.1(vii) il est clair que $\prod_{\alpha\in\Psi_u} \mathbf{U}_\alpha$ est un groupe, donc égal à $\mathbf{G}^*_{\Psi_u}$. De plus la propriété $\alpha \in \Psi_s$, $\beta \in \Psi_u$ et $\alpha + \beta \in \Phi \Rightarrow \alpha + \beta \in \Psi_u$ montre que $\mathbf{G}^*_{\Psi_u}$ est normalisé par $\mathbf{G}_{\Psi_s}$ (on voit par 6.2(iii) que $n\alpha + m\beta \in \Psi_u$ pour $n, m \geq 1$).

Remarquons maintenant que $\mathbf{G}_{\Psi_s}$ est déjà engendré par $\mathbf{T}$, et les $\mathbf{U}_\alpha$ tels que $\pm\alpha$ soit une racine simple de Ψ_s (pour l'ordre Φ^+ choisi) ; en effet $\langle \mathbf{U}_\alpha, \mathbf{U}_{-\alpha}\rangle$ contient s_α donc ce groupe contient W_{Ψ_s}, et toute racine de Ψ_s est conjuguée à une racine simple par W_{Ψ_s}, d'où le résultat par 3.1(iii). Montrons maintenant que $\mathbf{G}_{\Psi_s} = \mathbf{U}_{\Psi_s^+} W_{\Psi_s} \mathbf{T}\mathbf{U}_{\Psi_s^+}$ (pour n'importe quel ordre sur Φ). Pour cela, il suffit de voir que le membre de droite est un groupe ; comme il est stable par translation à gauche par $\mathbf{T}$ et $\mathbf{U}_\alpha$ où $\alpha \in \Psi_s^+$ il suffit de voir qu'il est stable par un élément de $\mathbf{U}_{-\alpha}$ où $\alpha \in \Psi_s^+$ est simple. Écrivant $\mathbf{U}_{\Psi_s^+} = \mathbf{U}_{\Psi_s^+ - \{\alpha\}}\mathbf{U}_\alpha$, puisque α est simple par 3.1(vii) $\mathbf{U}_{-\alpha}$ normalise le groupe $\mathbf{U}_{\Psi_s^+ - \{\alpha\}}$, donc il suffit de voir que $\mathbf{U}_\alpha W_{\Psi_s} \mathbf{T}\mathbf{U}_{\Psi_s^+}$ est stable par translation par $\mathbf{U}_{-\alpha}$. La décomposition de Bruhat $\langle \mathbf{T}, \mathbf{U}_\alpha, \mathbf{U}_{-\alpha}\rangle = \mathbf{U}_\alpha\mathbf{T} \cup \mathbf{U}_\alpha s_\alpha \mathbf{T}\mathbf{U}_\alpha$ montre que $\mathbf{U}_{-\alpha}\mathbf{U}_\alpha \subset \mathbf{U}_\alpha\mathbf{T} \cup \mathbf{U}_\alpha s_\alpha \mathbf{T}\mathbf{U}_\alpha$. Il suffit d'étudier le deuxième terme

$$\mathbf{U}_\alpha s_\alpha \mathbf{T}\mathbf{U}_\alpha W_{\Psi_s} \mathbf{T}\mathbf{U}_{\Psi_s^+} = \bigcup_{w\in\Psi_s} \mathbf{U}_\alpha s_\alpha \mathbf{U}_\alpha w \mathbf{T}\mathbf{U}_{\Psi_s^+}.$$

Si $w^{-1}(\alpha) \in \Psi^+$ alors $\mathbf{U}_\alpha w = w\mathbf{U}_{w^{-1}(\alpha)}$ et on obtient un terme cherché. Sinon, posant $\beta = -w^{-1}(\alpha) \in \Psi_s^+$ on obtient

$$\begin{aligned}&\mathbf{U}_\alpha s_\alpha w \mathbf{T}\mathbf{U}_{w^{-1}(\alpha)}\mathbf{U}_{\Psi_s^+} = \mathbf{U}_\alpha s_\alpha w \mathbf{T}\mathbf{U}_{-\beta}\mathbf{U}_\beta \mathbf{U}_{\Psi_s^+ - \{\beta\}}\\ &\subset \mathbf{U}_\alpha s_\alpha w \mathbf{T}(\mathbf{U}_\beta \cup \mathbf{U}_\beta s_\beta \mathbf{U}_\beta)\mathbf{U}_{\Psi_s^+ - \{\beta\}} = \mathbf{U}_\alpha s_\alpha w \mathbf{T}\mathbf{U}_{\Psi_s^+} \cup \mathbf{U}_\alpha s_\alpha w \mathbf{T}\mathbf{U}_\beta s_\beta \mathbf{U}_{\Psi_s^+}\end{aligned}$$

il suffit de considérer le terme de droite mais $s_\alpha w\mathbf{U}_\beta = s_\alpha \mathbf{U}_{-\alpha} w = \mathbf{U}_\alpha s_\alpha w$ d'où le résultat.

Montrons maintenant que Ψ_s est quasi-clos. Soit γ tel que $\mathbf{U}_\gamma \subset \mathbf{G}_{\Psi_s}$, et choisissons un ordre tel que $\gamma \in \Phi^+$ donc $\mathbf{U}_\gamma \subset \mathbf{U}$. Comme chaque terme

$\mathbf{U}_{\Psi_s^+} w \mathbf{T} \mathbf{U}_{\Psi_s^+}$ rencontre une seule cellule de Bruhat de $\mathbf{G}$ on doit avoir $\mathbf{U}_\gamma \subset \mathbf{T}\mathbf{U}_{\Psi_s^+}$. Par la remarque du début de la preuve sur Ψ_u (une partie positive close est quasi-close) on doit avoir $\gamma \in \Psi_s^+$.

Le groupe $\mathbf{G}_\Psi$ a donc une décomposition en produit semi-direct $\mathbf{G}^*_{\Psi_u} \rtimes \mathbf{G}_{\Psi_s}$. Enfin Ψ est quasi-clos car si $\alpha \notin \Psi_u$ et $\mathbf{U}_\alpha \subset \mathbf{G}_\Psi$ alors $\mathbf{U}_\alpha$ s'envoie isomorphiquement dans le quotient $\mathbf{G}_{\Psi_s}$ donc $\alpha \in \Psi_s$. □

Remarque 7.4. Sauf en caractéristique 2 ou 3 la réciproque de 7.3 a lieu : une partie quasi-close est close ; cela résulte de ce que pour les autres caractéristiques le groupe engendré par $\mathbf{U}_\alpha$ et $\mathbf{U}_\beta$ contient tous les $\mathbf{U}_{n\alpha+m\beta}$ pour $n, m \in \mathbb{N}$ tels que $n\alpha + m\beta$ soit une racine, par les valeurs explicites des coefficients (voir la preuve de 3.1(vii)).

Exemple 7.5. Le sous-groupe réductif de Sp_4 correspondant au sous-système clos de type $A_1 \times A_1$ est $\begin{pmatrix} a & 0 & 0 & b \\ 0 & a' & b' & 0 \\ 0 & c' & d' & 0 \\ c & 0 & 0 & d \end{pmatrix}$ où chacune des matrices données par a, b, c, d ou a', b', c', d' est dans SL_2. C'est le centralisateur de l'élément $\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$

Proposition 7.6. *Le groupe $\mathbf{P}_I$ possède une décomposition de Levi $\mathbf{P}_I = \mathrm{R_u}(\mathbf{P}) \rtimes \mathbf{L}_I$ où $\mathrm{R_u}(\mathbf{P}_I) = \prod_{\alpha \in \Phi^+ - \Phi_I} \mathbf{U}_\alpha$ et où $\mathbf{L}_I = \langle \mathbf{T}, \{\mathbf{U}_\alpha\}_{\alpha \in \Phi_I} \rangle$ est réductif.*

Démonstration. $\Psi = \Phi^+ \cup \Phi_I$ est quasi-clos car clos. La proposition résulte alors de 7.2 si nous montrons que $\mathbf{P}_I = \mathbf{G}_\Psi$. On a $\mathbf{P}_I \supset \mathbf{G}_\Psi$ car $\mathbf{P}_I$ contient $\mathbf{T}$, $\mathbf{U}_\alpha$ pour $\alpha \in \Psi$; et $\mathbf{G}_\psi$ contient $\mathbf{P}_I$ car $\langle \mathbf{U}_\alpha, \mathbf{U}_{-\alpha} \rangle \ni s_\alpha$. □

Proposition 7.7. *Soit $\mathbf{P}$ un sous-groupe parabolique de $\mathbf{G}$ contenant $\mathbf{T}$. Il y a un unique sous-groupe de Levi de $\mathbf{P}$ contenant $\mathbf{T}$. Deux sous-groupes de Levi de $\mathbf{P}$ sont conjugués par un unique élément de $\mathrm{R_u}(\mathbf{P})$.*

Démonstration. Soit $\mathbf{B}$ un sous-groupe de Borel de $\mathbf{P}$ (donc de $\mathbf{G}$) contenant $\mathbf{T}$. Alors, par 5.1 $\mathbf{P}$ est de la forme $\mathbf{P}_I$ pour ce Borel et 7.6 donne l'existence de $\mathbf{L}_I \supset \mathbf{T}$. Réciproquement, un sous-groupe de Levi contenant $\mathbf{T}$ est engendré par $\mathbf{T}$ et les $\mathbf{U}_\alpha$ qu'il contient. Comme tous les $\mathbf{U}_\alpha$ où $\alpha \in \Phi^+ - \Phi_I$ sont dans $\mathrm{R_u}(\mathbf{P})$, il ne contient que des $\mathbf{U}_\alpha$ où $\alpha \in \Phi_I$, donc il est inclus dans $\mathbf{L}_I$ donc doit lui être égal.

Deux sous-groupes de Levi de $\mathbf{P}$ sont conjugués, car un élément qui conjugue un tore maximal de l'un sur un tore maximal de l'autre les conjugue. Modulo un de ces Levis, on peut choisir l'élément dans $\mathrm{R_u}(\mathbf{P})$. L'unicité de l'élément qui les conjugue équivaut à $\mathrm{R_u}(\mathbf{P}) \cap N_\mathbf{G}(\mathbf{L}) = 1$; ceci résulte de ce que si $v \in \mathrm{R_u}(\mathbf{P}) \cap N_\mathbf{G}(\mathbf{L})$ alors pour tout $l \in \mathbf{L}$ on a $[v, l] \in \mathrm{R_u}(\mathbf{P}) \cap \mathbf{L} = 1$; donc $v \in C_\mathbf{G}(\mathbf{L})$. Mais $C_\mathbf{G}(\mathbf{L}) \subset \mathbf{L}$ (par ex. puisque $C_\mathbf{G}(\mathbf{T}) = \mathbf{T}$) d'où $v = 1$. □

Proposition 7.8. *Un sous-groupe fermé $\mathbf{P} \supset \mathbf{T}$ de $\mathbf{G}$ est parabolique si et seulement si pour tout $\alpha \in \Phi$, on a $\mathbf{U}_\alpha \subset \mathbf{P}$ ou $\mathbf{U}_{-\alpha} \subset \mathbf{P}$.*

Démonstration. Un sous-groupe parabolique vérifie cette condition. Réciproquement, soit un groupe $\mathbf{P}$ comme dans l'énoncé ; alors $\mathbf{P}^0$ est de la forme $\mathbf{G}_\Psi$ où Ψ est une partie quasi-close telle que $\Psi \cup -\Psi = \Phi$. Montrons que $\mathbf{P}^0$ contient un sous-groupe de Borel. Par 7.2 il existe un ordre Φ^+ tel que $\Phi^+ \supset \Psi_u$. Soit $\alpha \in \Phi^+$; alors $\alpha \in \Psi$ sinon $-\alpha \in \Psi_u \subset \Phi^+$, une contradiction. Donc $\Phi^+ \subset \Psi$. □

Lemme 7.9. *Soient $\mathbf{T} \subset \mathbf{B}$ une tore maximal et un sous-groupe de Borel de $\mathbf{G}$. Une cellule de Bruhat $\mathbf{B}w\mathbf{B}$ est égale au produit direct $\mathbf{U}\mathbf{T}w\mathbf{U}_w$ où $\mathbf{U}_w = \prod_{\{\alpha\in\Phi^+ | w(\alpha)<0\}} \mathbf{U}_\alpha$.*

Démonstration. Remarquons d'abord que $\mathbf{U}_w$ est un groupe car $\{\alpha \in \Phi^+ \mid w(\alpha) < 0\}$ est clos. D'autre part si $\mathbf{U} = \mathrm{R_u}(\mathbf{B})$ on a $\mathbf{U} = \mathbf{U}'\mathbf{U}_w$ où $\mathbf{U}' = \prod_{\{\alpha\in\Phi^+ | w(\alpha)>0\}} \mathbf{U}_\alpha$, donc ${}^w\mathbf{U}' \subset \mathbf{U}$; donc $\mathbf{B}w\mathbf{B} = \mathbf{U}\mathbf{T}w\mathbf{U}'\mathbf{U}_w = \mathbf{U}\mathbf{T}{}^w\mathbf{U}'w\mathbf{U}_w = \mathbf{U}\mathbf{T}w\mathbf{U}_w$. Il reste à voir que la décomposition est unique, ce qui revient à voir que si $u\mathbf{T}wu' = \mathbf{T}w$ avec $u \in \mathbf{U}, u' \in \mathbf{U}_w$ alors $u = u' = 1$. La condition se réécrit $u \cdot {}^wu' \in \mathbf{T}$; en particulier ${}^wu' \in \mathbf{B}$. Mais ${}^w\mathbf{U}_w \cap \mathbf{B} = 1$ car ce groupe unipotent normalisé par $\mathbf{T}$ ne contient pas de $\mathbf{U}_\alpha$. Donc $u' = 1$, d'où $u = 1$. □

Proposition 7.10. *Pour $s \in \mathbf{T}$ posons $\Psi_s = \{\alpha \in \Phi \mid \alpha(s) = 1\}$. Alors*

(i) $C_\mathbf{G}(s)^0 = \mathbf{G}_{\Psi_s}$.

(ii) $C_\mathbf{G}(s)$ est engendré par $C_\mathbf{G}(s)^0$ et $\{n \in N_\mathbf{G}(\mathbf{T}) \mid {}^ns = s\}$.

Démonstration. Appliquons le lemme 7.9 pour voir quand un élément $uwtu' \in \mathbf{B}w\mathbf{B}$ avec $u \in \mathbf{U}$, $u' \in \mathbf{U}_w$ et $t \in \mathbf{T}$ centralise s. Comme s normalise $\mathbf{U}$, $\mathbf{U}_w$ et $w\mathbf{T}$ il faut que chacun des 3 termes centralise s. De plus, écrivant $u = \prod_{\alpha\in\Phi^+} \mathbf{u}_\alpha(x_\alpha)$ cette décomposition étant unique on doit avoir $x_\alpha = 0$ si $\alpha(s) \neq 1$. Finalement on trouve $u, u' \in \mathbf{G}_{\Psi_s}$ et ${}^ws = s$. Donc $\mathbf{G}_{\Psi_s} \subset C_\mathbf{G}(s)$ et $C_\mathbf{G}(s)$ est engendré par $\mathbf{G}_\Psi$ et $W(s)$ si on pose $W(s) = \{w \in W \mid {}^ws = s\}$. De plus $\mathbf{G}_{\Psi_s}$ est normal dans $C_\mathbf{G}(s)$ car si $w \in W(s)$ et $\alpha(s) = 1$ alors ${}^w\alpha(s) = \alpha({}^{w^{-1}}s) = \alpha(s) = 1$. Donc étant d'indice fini le groupe connexe $\mathbf{G}_{\Psi_s}$ doit être la composante neutre. □

Exemple 7.11. Les centralisateurs de tous les éléments de GL_n sont connexes, donc les classes géométriques ne se scindent pas. En effet, le centralisateur d'une matrice dans M_n est un espace affine ; et un ouvert d'un espace affine est connexe.

Par contre le centralisateur de $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ n'est pas connexe dans PGL_2 car il contient $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in W$.

Rappelons (voir 4.4) que deux sous-groupes de Borel (donc deux sous-groupes paraboliques) ont toujours un tore maximal en commun.

Proposition 7.12. *Soient* $\mathbf{P}$ *et* $\mathbf{P}'$ *deux sous-groupes paraboliques de* $\mathbf{G}$ *et soient* $\mathbf{L}$ *et* $\mathbf{L}'$ *des sous-groupes de Levi respectifs de* $\mathbf{P}$ *et* $\mathbf{P}'$ *contenant un même tore maximal* $\mathbf{T}$ *de* $\mathbf{G}$*. On pose* $\mathbf{U} = \mathrm{R_u}(\mathbf{P})$ *et* $\mathbf{U}' = \mathrm{R_u}(\mathbf{P}')$*. Alors* $(\mathbf{P} \cap \mathbf{P}').\mathbf{U}$ *est un sous-groupe parabolique de* $\mathbf{G}$ *inclus dans* $\mathbf{P}$ *ayant même intersection que* $\mathbf{P}'$ *avec* $\mathbf{L}$ *et dont* $\mathbf{L} \cap \mathbf{L}'$ *est un sous-groupe de Levi.* $\mathbf{P} \cap \mathbf{P}'$ *est connexe ainsi que* $\mathbf{L} \cap \mathbf{L}'$ *et on a la décomposition de Levi* $\mathbf{P} \cap \mathbf{P}' = (\mathbf{L} \cap \mathbf{L}') \ltimes ((\mathbf{L} \cap \mathbf{U}').(\mathbf{L}' \cap \mathbf{U}).(\mathbf{U} \cap \mathbf{U}'))$*; c'est une décomposition comme produit de 4 variétés (la décomposition correspondante d'un élément de* $\mathbf{P} \cap \mathbf{P}'$ *suivant ce produit est unique).*

Démonstration. Soit Φ l'ensemble des racines de $\mathbf{G}$ par rapport à $\mathbf{T}$ et soit $\Psi \subset \Phi$ (resp. $\Psi' \subset \Phi$) tel que $\mathbf{P} = \mathbf{G}_\Psi$ (resp $\mathbf{P}' = \mathbf{G}_{\Psi'}$). Montrons que pour tout $\alpha \subset \Phi$, soit $\mathbf{U}_\alpha$ soit $\mathbf{U}_{-\alpha}$ est inclus dans le groupe $(\mathbf{P} \cap \mathbf{P}') \cdot \mathbf{U}$ (c'est un groupe car $\mathbf{P}$ normalise $\mathbf{U}$). On a $(\mathbf{P} \cap \mathbf{P}')^0 \cdot \mathbf{U} = \mathbf{G}_{\Psi \cap \Psi'} \cdot \mathbf{G}^*_{\Psi_u}$. Si α et $-\alpha$ ne sont pas dans Ψ_u alors α et $-\alpha$ sont tous les deux dans Ψ. Comme l'un des deux est dans Ψ', l'un des deux est dans $\Psi \cap \Psi'$. La proposition 7.8 montre alors que $(\mathbf{P} \cap \mathbf{P}').\mathbf{U}$ est un sous-groupe parabolique de $\mathbf{G}$, d'où la première assertion, et $(\mathbf{P} \cap \mathbf{P}').\mathbf{U} = \mathbf{G}_{(\Psi \cap \Psi') \cup \Psi_u}$ (cet ensemble est clos car la somme d'une racine de Ψ et d'une racine de Ψ_u qui est une racine est dans Ψ_u, cf. preuve de 7.3). Maintenant, $\Psi_u - \Psi'$ est clos comme intersection de deux parties closes (qui sont Ψ_u et le complémentaire $-\Psi'_u$ de Ψ'), donc on a $(\mathbf{P} \cap \mathbf{P}').\mathbf{U} = (\mathbf{P} \cap \mathbf{P}').\mathbf{G}^*_{\Psi_u - \Psi'}$. Le produit est un produit direct de variétés car l'intersection est un groupe unipotent normalisé par $\mathbf{T}$ (donc connexe) et ne contient aucun $\mathbf{U}_\alpha$. Le produit étant connexe, chacun des termes l'est donc $\mathbf{P} \cap \mathbf{P}'$ l'est et est égal à $\mathbf{G}_{\Psi \cap \Psi'}$. Les groupes $(\mathbf{P} \cap \mathbf{P}').\mathbf{U}$ et $\mathbf{P} \cap \mathbf{P}'$ admettent tous deux pour groupe de Levi $(\mathbf{L} \cap \mathbf{L}')^0$ car $((\Psi \cap \Psi') \cup \Psi_u)_s = (\Psi \cap \Psi')_s = \Psi_s \cap \Psi'_s$ (c'est clair car si $\alpha \in \Psi_u$ alors $-\alpha \notin \Psi$ donc $-\alpha \notin (\Psi \cap \Psi') \cup \Psi_u$).

La décomposition $\Psi \cap \Psi' = (\Psi_s \cap \Psi'_s) \coprod (\Psi_s \cap \Psi'_u) \coprod (\Psi_u \cap \Psi'_s) \coprod (\Psi_u \cap \Psi'_u)$ montre que $\mathbf{P} \cap \mathbf{P}' = \langle \mathbf{L} \cap \mathbf{L}', \mathbf{L} \cap \mathbf{U}', \mathbf{L}' \cap \mathbf{U}, \mathbf{U} \cap \mathbf{U}' \rangle$. Utilisant que $\mathbf{U} \cap \mathbf{U}'$ est normal dans $\mathbf{P} \cap \mathbf{P}'$, puis que $\mathbf{L} \cap \mathbf{L}'$ normalise $\mathbf{L} \cap \mathbf{U}'$ et $\mathbf{L}' \cap \mathbf{U}$, on a

$$\mathbf{P} \cap \mathbf{P}' = (\mathbf{L} \cap \mathbf{L}').\langle \mathbf{L} \cap \mathbf{U}', \mathbf{L}' \cap \mathbf{U} \rangle.(\mathbf{U} \cap \mathbf{U}').$$

De plus le commutateur d'un élément de $\mathbf{L} \cap \mathbf{U}'$ avec un élément de $\mathbf{L}' \cap \mathbf{U}$ est dans $\mathbf{U} \cap \mathbf{U}'$. Donc on a

$$\mathbf{P} \cap \mathbf{P}' = (\mathbf{L} \cap \mathbf{L}').(\mathbf{L} \cap \mathbf{U}').(\mathbf{L}' \cap \mathbf{U}).(\mathbf{U} \cap \mathbf{U}'),$$

Supposons maintenant que $x = lu'uv \in \mathbf{P} \cap \mathbf{P}'$, où $l \in \mathbf{L} \cap \mathbf{L}'$, $u' \in \mathbf{L} \cap \mathbf{U}'$, $u \in \mathbf{L}' \cap \mathbf{U}$, $v \in \mathbf{U} \cap \mathbf{U}'$. Alors lu' est l'image de x par la projection $\mathbf{P} \to \mathbf{L}$ et l (resp. u) est l'image de lu' (resp. uv) par le morphisme $\mathbf{P}' \to \mathbf{L}'$. Donc la décomposition de x est unique, et l'application produit $(\mathbf{L} \cap \mathbf{L}') \times (\mathbf{L} \cap \mathbf{U}') \times (\mathbf{L}' \cap \mathbf{U}) \times (\mathbf{U} \cap \mathbf{U}') \to \mathbf{P} \cap \mathbf{P}'$ est un isomorphisme de variétés ; et les 4 termes sont connexes puisque le produit l'est donc $\mathbf{L} \cap \mathbf{L}'$ est bien connexe. □

Proposition 7.13. *(i) Soient* $\mathbf{P}'$ *et* $\mathbf{P}$ *deux sous-groupes paraboliques de* $\mathbf{G}$ *tels que* $\mathbf{P}' \subset \mathbf{P}$*, alors* $\mathrm{R_u}(\mathbf{P}') \supset \mathrm{R_u}(\mathbf{P})$ *et pour tout sous-groupe de Levi* $\mathbf{L}'$ *de* $\mathbf{P}'$*, il existe un unique sous-groupe de Levi* $\mathbf{L}$ *de* $\mathbf{P}$ *tel que* $\mathbf{L} \supset \mathbf{L}'$*.*

(ii) Soit $\mathbf{L}$ *un sous-groupe de Levi d'un sous-groupe parabolique* $\mathbf{P}$ *de* $\mathbf{G}$*. Alors on a équivalence entre*
   (a) $\mathbf{L}'$ *est un sous-groupe de Levi d'un sous-groupe parabolique de* $\mathbf{L}$*.*
   (b) $\mathbf{L}'$ *est un sous-groupe de Levi d'un sous-groupe parabolique de* $\mathbf{G}$*, et* $\mathbf{L}' \subset \mathbf{L}$*.*

Démonstration. Démontrons (i) ; soit $\mathbf{T}$ un tore maximal de $\mathbf{L}'$ et soit $\mathbf{L}$ l'unique sous-groupe de Levi de $\mathbf{P}$ contenant $\mathbf{T}$ (*c.f.* 7.7). Alors 7.12 dit que $\mathbf{L}' \cap \mathbf{L}$ est un sous-groupe de de Levi de $\mathbf{P}' = \mathbf{P} \cap \mathbf{P}'$ donc $\mathbf{L} \cap \mathbf{L}' = \mathbf{L}'$. D'autre part $\mathrm{R_u}(\mathbf{P})$ est dans tout sous-groupe de Borel de P, donc dans $\mathbf{P}'$ d'où $\mathrm{R_u}(\mathbf{P}) \subset \mathrm{R_u}(\mathbf{P}')$.

Démontrons (ii) ; si $\mathbf{L}'$ est un sous-groupe de Levi de $\mathbf{P_L}$, sous-groupe parabolique de $\mathbf{L}$, alors $\mathbf{P_L}\mathrm{R_u}(\mathbf{P})$ est un sous-groupe parabolique de $\mathbf{G}$ (c'est un groupe car $\mathbf{L}$, donc $\mathbf{P_L}$, normalise $\mathrm{R_u}(\mathbf{P})$ et il contient clairement $\mathbf{U}_\alpha$ ou $\mathbf{U}_{-\alpha}$ pour tout $\alpha \in \Phi$) dont $\mathbf{L}'$ est un sous-groupe de Levi (car $\mathrm{R_u}(\mathbf{P_L}).\mathrm{R_u}(\mathbf{P})$ est unipotent normal dans $\mathbf{P_L}.\mathrm{R_u}(\mathbf{P})$). Donc (a) implique (b). Pour voir la réciproque, soit $\mathbf{P}'$ un sous-groupe parabolique de $\mathbf{G}$ dont $\mathbf{L}'$ est un sous-groupe de Levi ; par 7.12 on a $\mathbf{P} \cap \mathbf{P}' = \mathbf{L}'.(\mathbf{L} \cap \mathbf{U}').(\mathbf{U} \cap \mathbf{U}')$ donc $\mathbf{L}' \rtimes (\mathbf{L} \cap \mathbf{U}')$ est une décomposition de Levi de $\mathbf{L} \cap \mathbf{P}'$ et ce dernier groupe est parabolique par 7.8. □

8 Isogénies ; présentation de G

Si $\mathbf{G}$ est un groupe réductif connexe avec un tore maximal $\mathbf{T}$, on appelle *donnée radicielle* de $\mathbf{G}$ le quadruplet $(X, Y, \Phi, \Phi^\vee)$ où $X = X(\mathbf{T})$, $Y = Y(\mathbf{T})$ et Φ (resp. $\Phi^\vee$) sont les racines (resp. coracines) relatives à ce tore. Nous allons voire que cette donnée détermine $\mathbf{G}$ à isomorphisme près.

Isogénies

On appelle *isogénie* un morphisme surjectif de groupes algébriques, de noyau fini. Le noyau de f étant fini et normal est central dans $\mathbf{G}$ (la conjugaison par $\mathbf{G}$ est continue donc triviale sur un groupe fini), donc sous-groupe de $\mathbf{T}$.

On appelle p-morphisme (où $p = \mathrm{car}\, k$) entre les données radicielles $(X, Y, \Phi, \Phi^\vee)$ et $(X_1, Y_1, \Phi_1, \Phi_1^\vee)$ un morphisme $X_1 \xrightarrow{f} X$ de conoyau fini associé à une bijection $\Phi \xrightarrow{\tau} \Phi_1$ telle que $f(\tau(\alpha)) = q_\alpha \alpha$ et $f^\vee(\alpha^\vee) = q_\alpha \tau(\alpha)^\vee$ où q_α est une puissance de p ($q_\alpha = 1$ si k est de caractéristique 0) — et où $f^\vee : Y \to Y_1$ est la transposée de f.

Théorème 8.1. *Pour toute isogénie* $\phi : \mathbf{G} \to \mathbf{G}_1$ *si on pose* $\mathbf{T}_1 = \phi(\mathbf{T})$ *alors* ϕ *induit un p-morphisme entre* $(X(\mathbf{T}), Y(\mathbf{T}), \Phi, \Phi^\vee)$ *et* $(X_1(\mathbf{T}_1), Y_1(\mathbf{T}_1), \Phi_1, \Phi_1^\vee)$ *associé à la bijection* τ *et les facteurs* q_α *définis par la formule* $\phi(\mathbf{u}_\alpha(\xi)) = \mathbf{u}_{\tau(\alpha)}(\xi^{q_\alpha})$*. Réciproquement, tout p-morphisme entre les données radicielles est induit par une isogénie (déterminée uniquement à conjugaison par* $\mathbf{T}$ *près).*

preuve de la partie directe, sketch de la réciproque. L'isogénie ϕ induit un morphisme $X(\mathbf{T}_1) \xrightarrow{f} X(\mathbf{T})$ donné par $\alpha \mapsto \alpha \circ \phi$ et de même $Y(\mathbf{T}) \xrightarrow{f^\vee} Y(\mathbf{T}_1)$ donné par $\alpha^\vee \mapsto \phi \circ \alpha^\vee$. Si $\mathbf{u}_\alpha$ est un sous-groupe radiciel, alors $\phi(\mathbf{u}_\alpha)$ en est

un autre $\mathbf{u}_{\tau(\alpha)}$ pour une certaine bijection τ. On a $\phi(\mathbf{u}_\alpha(\xi)) = \mathbf{u}_{\tau(\alpha)}(p(\xi))$ pour un certain polynôme p ; la compatibilité avec l'action de $\mathbf{T}$ donne $p(\alpha(t)\xi) = \tau(\alpha)(\phi(t))p(\xi)$ donc p doit être un monôme ; de plus, pour être compatible à la loi de $\mathbb{G}_a$, on a $p(x+y) = p(x)+p(y)$. La seule possibilité est $\lambda\xi^{q_\alpha}$ où q_α est une puissance de $p = \operatorname{car} k$ et λ une constante ($q_\alpha = 1$ si k de caractéristique 0). Ces constantes λ reflètent le fait que le p-morphisme définit l'isogénie à $\operatorname{ad}\mathbf{T}$ près.

La réciproque est plus compliquée : classiquement, on utilise la présentation de la sous-section suivante pour montrer que la formule de l'isogénie est bien un morphisme de groupes algébriques. [Steinberg] donne une preuve utilisant seulement les propriétés de 3.1, qui commence par le cas des groupes de rang semi-simple 1, et en déduit le cas général. □

Exemple 8.2. Automorphisme d'opposition : on choisit $q_\alpha = 1$ et $\tau(\alpha) = -\alpha$ pour tout α.

Exemple 8.3. Automorphisme du système de racines τ. On choisit $q_\alpha = 1$.

Exemple 8.4. Frobenius déployé : on choisit $q_\alpha = q$ une puissance de $p = \operatorname{car} k$ et $\tau(\alpha) = \alpha$ pour tout α. Si $k = \overline{\mathbb{F}}_p$, ceci définit une isogénie $\mathbf{G} \xrightarrow{F} \mathbf{G}$ tel que $\mathbf{G}^F = \mathbf{G}(\mathbb{F}_q)$.

Exemple 8.5. Pour un système de type C_2, avec base des racines $\{\alpha = e_1 - e_2, \beta = 2e_2\}$, en caractéristique 2 les formules $\phi(\mathbf{u}_\alpha(x)) = \mathbf{u}_\beta(x^2), \phi(\mathbf{u}_{\alpha+\beta}(x)) = \mathbf{u}_{2\alpha+\beta}(x^2)), \phi(\mathbf{u}_\beta(x)) = \mathbf{u}_\alpha(x), \phi(\mathbf{u}_{2\alpha+\beta(x)}) = \mathbf{u}_{\alpha+\beta}(x)$ définissent une isogénie. Pour $t = \operatorname{diag}(t_1, t_2, t_2^{-1}, t_1^{-1}) \in \mathbf{T}$ on a $\phi(t) = \operatorname{diag}(t_1t_2, t_1t_2^{-1}, t_1^{-1}t_2, t_1^{-1}t_2^{-1})$. On vérifie que ϕ^2 élève toutes les coordonnées au carré : c'est le Frobenius F sur le corps $\mathbb{F}_2$. Alors $\phi \circ F^r$ a $2^{2r+1} - 1$ points fixes sur le tore. Les points fixes $\mathbf{G}^\phi$ sont le *groupe de Suzuki*.

Le théorème montre que des groupes qui ont des données radicielles isomorphes sont isomorphes, d'où la classification — Il manque l'existence qui se montre d'abord en rang 2, et est obtenue ensuite en recollant les sous-groupes de rang 2.

Présentation de G

Nous allons donner une présentation de $\mathbf{G}$ à partir de la donnée radicielle $(X, Y, \Phi, \Phi^\vee)$ et du corps k. On pose d'abord $\mathbf{T} = \operatorname{Hom}(X, k^\times)$ ($\alpha(t)$ est l'image de α par t). Un $\alpha^\vee \in Y$ définit $\alpha^\vee : k^\times \to \mathbf{T}$ par $\alpha^\vee(x)(\beta) = x^{\alpha^\vee(\beta)}$. Pour chaque $\alpha \in \Phi$ on se donne un groupe $\mathbf{U}_\alpha$ avec un isomorphisme fixé $k^+ \to \mathbf{U}_\alpha : x \mapsto \mathbf{u}_\alpha(x)$. Les générateurs sont $\{t \in \mathbf{T}\}, \{\mathbf{u}_\alpha(x)\}_{\alpha\in\Phi, x\in k}$. Si on pose

$s_\alpha = \mathbf{u}_\alpha(1)\mathbf{u}_{-\alpha}(1)^{-1}\mathbf{u}_\alpha(1)$, les relations sont

$$\begin{aligned}
\mathbf{u}_\alpha(x)\mathbf{u}_\alpha(y) &= \mathbf{u}_\alpha(x+y)\\
s_\alpha \mathbf{u}_\alpha(x) s_\alpha^{-1} &= \mathbf{u}_{-\alpha}(x)^{-1}\\
\mathbf{u}_\alpha(x)\mathbf{u}_{-\alpha}(x^{-1})^{-1}\mathbf{u}_\alpha(x) &= \alpha^\vee(x)s_\alpha\\
t\mathbf{u}_\alpha(x)t^{-1} &= \mathbf{u}_\alpha(\alpha(t)x)\\
s_\alpha^2 \in \mathbf{T}, \beta(s_\alpha^2) &= (-1)^{\alpha^\vee(\beta)}\\
s_\alpha s_\beta \ldots &= s_\beta s_\alpha \ldots\\
[\mathbf{u}_\alpha(x), \mathbf{u}_\beta(y)] &= \prod_{i\alpha+j\beta\in\Phi, i,j>0} \mathbf{u}_{i\alpha+j\beta}(c_{\alpha,\beta,i,j}x^i y^j)
\end{aligned}$$

où les constantes $c_{\alpha,\beta,i,j}$ sont entières ; elles dépendent d'un choix (d'une partie de $\Phi^+\times\Phi^+$) qui peut faire varier leur signe mais à part ça dépendent uniquement de Φ.

9 Rationalité

Soit k_0 un sous-corps de k.

Définition 9.1. *Une variété algébrique* $\mathbf{V}$ *sur* k *est dite définie sur* k_0*, ou munie d'une* k_0*-structure* $\mathbf{V}(k_0)$*, s'il existe une variété* $\mathbf{V}(k_0)$ *sur* k_0 *telle que* $\mathbf{V} = \mathbf{V}(k_0)\otimes_{k_0} k$.

Explicitons cette définition en termes d'anneaux des fonctions pour une variété affine ou projective. Une variété affine (resp. projective) sur k est définie par un k-algèbre de type fini (resp. une k-algèbre graduée réduite engendrée par ses éléments de degré 1). Une sous-variété fermée correspond à un idéal (resp. un idéal homogène).

Une k_0-structure sur un espace vectoriel V est un sous-k_0-espace $V(k_0)$ tel que $V = V(k_0)\otimes_{k_0} k$. Une k_0-structure sur une k-algèbre si et seulement si la k-algèbre correspondante est de la forme $A = A(k_0)\otimes_{k_0} k$ où $A(k_0)$ est une k_0-algèbre de type fini. On dit que $A(k_0)$ est une k_0-structure sur A. Une variété $\mathbf{V}$ affine ou projective est définie sur k_0 si et seulement si la k-algèbre correspondante a une k_0-structure.

Si k/k_0 est Galoisienne, par exemple si k est la clôture séparable de k_0, un élément de $\sigma \in \mathrm{Gal}(k/k_0)$ agit alors sur $\mathbf{V}$ par $x\otimes\lambda \mapsto x\otimes\sigma(\lambda)$. On peut retrouver $V(k_0)$ comme les points fixes de l'action de $\mathrm{Gal}(k/k_0)$. Plus généralement, on peut démontrer

Proposition 9.2. *Si on se donne une* k*-algèbre* A *ou un* k*-espace vectoriel et une action continue de* $\mathrm{Gal}(k/k_0)$ *(comme groupe profini, ce qui veut dire que* $A = \cup_U A^U$ *où* U *parcourt les sous-groupes d'indice fini) compatible à la structure d'algèbre, les points fixes de cette action définissent une* k_0*-structure.*

Démonstration. Voir [Springer, 11.1.6] ; [Digne-Michel, 3.5] quand $k = \overline{\mathbb{F}}_q$. □

Proposition 9.3. *Une sous-variété (sous-algèbre, sous-espace vectoriel) est définie sur k_0 (possède une k_0-structure qui est une sous-variété (resp. sous-algèbre, sous-espace)) si elle est fixe par l'action de* $\mathrm{Gal}(k/k_0)$.

Démonstration. Voir [Springer, 11.1.4]. □

Exemple 9.4. La droite affine sur k est la variété définie par la k-algèbre $k[T]$. La droite affine sur k_0, variété définie par la k_0-algèbre $k_0[T]$, est une k_0-structure puisque $k[T] = k_0[T] \otimes_{k_0} k$. Un élément $\sigma \in \mathrm{Gal}(k/k_0)$ envoie $\sum_i a_i T^i$ sur $\sum_i \sigma(a_i) T^i$. Un point de la droite affine sur k correspond à un élément $a \in k$ (l'idéal correspondant est le noyau du morphisme $P \mapsto P(a) : k[T] \to k$) ; le point est défini sur k_0 si $a \in k_0$

Endomorphisme de Frobenius

Nous considérons maintenant le cas de $k = \overline{\mathbb{F}}_q$, une clôture algébrique de $\mathbb{F}_p$. On a $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) = \hat{\mathbb{Z}}$; en effet un élément de ce groupe agit sur $\mathbb{F}_{q^n}$ par $x \mapsto x^{q^{k_n}}$ où la suite d'entiers k_n est soumise à la seule condition $k_n \equiv k_m \pmod m$ si m divise n. On a $\hat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p$.

Définition 9.5. *Soit* $\mathbf{V}$ *une variété algébrique sur* $\overline{\mathbb{F}}_q$ *qui possède une* $\mathbb{F}_q$*-structure* $\mathbf{V}(\mathbb{F}_q)$. *L'* endomorphisme de Frobenius géométrique $F : \mathbf{V} \to \mathbf{V}$ *associé à cette* $\mathbb{F}_q$*-structure est* $F_0 \otimes \mathrm{Id}$ *où* F_0 *est l'endomorphisme de* $\mathbf{V}(\mathbb{F}_q)$ *qui élève les fonctions sur* $\mathbf{V}(\mathbb{F}_q)$ *à la puissance* q.

L'endomorphisme Φ de $\mathbf{V}$ induit par l'élément $\lambda \mapsto \lambda^q$ de $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ est appelé l'*endomorphisme de Frobenius arithmétique*.

Sur une algèbre $A = A(\mathbb{F}_q) \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ l'endomorphisme de Frobenius correspond à un morphisme $F^* : a \otimes \lambda \mapsto a^q \otimes \lambda$ (dans un système de coordonnées pour la variété, le morphisme de Frobenius se traduit par l'élévation de chaque coordonnée à la puissance q). L'endomorphisme de Frobenius arithmétique est donné par $\Phi : a \otimes \lambda \mapsto a \otimes \lambda^q$. Le composé $F^* \otimes \Phi$ élève chaque élément de A à la puissance q-ième, ce qui induit l'identité sur les points sur $\overline{\mathbb{F}}_q$ de $\mathrm{Spec}\, A$.

Exemple 9.6. Sur la droite affine, l'endomorphisme de Frobenius géométrique est donné par $F^* : P(T) \mapsto P(T^q)$; donc $F^* \circ \Phi$ envoie $P(T)$ sur $P(T)^q$. Considérons un point donné par $a \in \overline{\mathbb{F}}_q$; l'image du point a par $F^* \circ \Phi$ est défini par le noyau de $P \mapsto P(a)^q$ qui est le même que celui de $P \mapsto P(a)$.

Notons que l'endomorphisme de Frobenius géométrique est un endomorphisme de $\overline{\mathbb{F}}_q$-variétés, mais que l'endomorphisme de Frobenius arithmétique n'est qu'un endomorphisme de $\mathbb{F}_q$-variétés. Dans la suite nous ne considérerons que l'endomorphisme géométrique que nous appellerons "l'endomorphisme de Frobenius".

Proposition 9.7. *Soit* $\mathbf{V}$ *une variété affine ou projective sur* $\overline{\mathbb{F}}_q$, *et soit* A *son algèbre.*

(i) Un morphisme surjectif de $A \xrightarrow{F^*} A^q$ est l'endomorphisme de Frobenius associé à une $\mathbb{F}_q$-structure sur $\mathbf{V}$ si et seulement si pour tout $x \in A$ il existe n tel que $F^{*n}(x) = x^{q^n}$.

Dans la suite de l'énoncé, nous supposons que A est munie d'une $\mathbb{F}_q$-structure $A(\mathbb{F}_q)$ et que F est l'endomorphisme de Frobenius correspondant.

(ii) On a $A(\mathbb{F}_q) = \{x \in A \mid x^q = F^*(x)\}$.

(iii)Une sous-variété de $\mathbf{V}$ est définie sur $\mathbb{F}_q$ si et seulement si elle est F-stable ; l'endomorphisme de Frobenius correspondant est la restriction de F.

(iv)Soit φ un automorphisme de $\mathbf{V}$ tel que $(\varphi F)^n = F^n$ pour un entier n positif ; alors φF est l'endomorphisme de Frobenius correspondant à une autre $\mathbb{F}_q$-structure sur $\mathbf{V}$.

(v)Si F' est un endomorphisme de Frobenius correspondant à une autre $\mathbb{F}_q$-structure sur $\mathbf{V}$, alors il existe un entier $n > 0$ tel que $F^n = F'^n$.

(vi) F^n est l'endomorphisme de Frobenius correspondant à une $\mathbb{F}_{q^n}$-structure sur $\mathbf{V}$.

(vii)Toute sous-variété fermée d'une variété définie sur $\mathbb{F}_q$ est définie sur une extension finie de $\mathbb{F}_q$. Tout morphisme entre variétés définies sur $\mathbb{F}_q$ est défini sur une extension finie de $\mathbb{F}_q$.

(viii) Les orbites de F sur l'ensemble des points de $\mathbf{V}$ sont finies, ainsi que l'ensemble $\mathbf{V}^F$ (encore noté $\mathbf{V}(\mathbb{F}_q)$, formé des points rationnels de $\mathbf{V}$).

Démonstration. Pour (i) : si F est un Frobenius et $A = A(\mathbb{F}_q \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q) \ni x = \sum_i x_i \otimes \lambda_i$ alors $x^{q^n} = \sum_i x_i^{q^n} \otimes \lambda_i^{q^n}$ donc $x^{q^n} = F^{*n}(x)$ si tous les λ_i sont dans $\mathbb{F}_{q^n}$. Réciproquement comme $x \mapsto x^{q^n}$ est injectif F^{*n} doit l'être aussi, donc F^* est bijectif et on peut définir ϕ par $\phi(x) = F^{*-1}(x^q)$; alors si on fait agir le générateur de $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ par ϕ on est dans la situation de 9.2. On a aussi (ii) par la même proposition.

(iii) vient de 9.3.

(iv) vient de ce que φF vérifie encore (i).

(v) vient de ce que A étant de type fini, il existe n tel que $F^{*n}(x) = F'^{*n}(x) = x^{q^n}$ pour tout générateur de A.

(vi) résulte encore de (i).

(vii) vient d'un raisonnement analogue à (v) : il existe n tel que pour tout élément a d'un ensemble fini de générateurs de l'idéal (resp. tout coefficient a d'une équation du morphisme) on ait $F^{*n}a = a^{q^n}$.

Prouvons (vii). Soient $\{a_1, \ldots, a_n\}$ des générateurs de $A(\mathbb{F}_q)$. Un point $x \in \mathbf{V}$ est un morphisme $x : A \to \overline{\mathbb{F}}_q$. Il est fixe par F^{*n} si pour tout i on $x(a_i) \in \mathbb{F}_{q^n}$ ce qui est possible pour n assez grand. Il est fixe par F^* si $x(a_i) \in \mathbb{F}_q$, c'est à-dire qu'on a un morphisme $A(\mathbb{F}_q) \to \mathbb{F}_q$; il y a un nombre fini de tels morphismes. □

Proposition 9.8. *Soit $\mathbf{V} \simeq \mathbb{A}^n$ un espace affine de dimension n sur $\overline{\mathbb{F}}_q$. Alors $|\mathbf{V}^F| = q^n$ pour toute $\mathbb{F}_q$-structure sur $\mathbf{V}$.*

Démonstration. Voir [Geck, 4.2.4] pour une preuve élémentaire compliquée dans le cas des groupes unipotents. C'est une conséquence immédiate des propriétés de la cohomologie l-adique. □

10 Théorème de Lang-Steinberg

Un groupe algébrique est dit défini sur $\mathbb{F}_q$ s'il est muni d'un endomorphisme de Frobenius qui est un morphisme de groupe.

Soit $\mathbf{G}$ un groupe algébrique réductif sur $\overline{\mathbb{F}}_q$, et soit $F : \mathbf{G} \to \mathbf{G}$ une isogénie dont une puissance est un endomorphisme de Frobenius (un endomorphisme de Frobenius étant bijectif et de noyau trivial est une isogénie ; mais pas un isomorphisme : il n'est pas inversible comme morphisme de variétés). Alors le groupe des points fixes $\mathbf{G}^F$ est ce qu'on appelle un *groupe fini de type de Lie.* Le théorème fondamental pour l'étude des groupes de type de Lie est le

Théorème 10.1. *(Lang-Steinberg) Soit* $\mathbf{G}$ *un groupe algébrique affine* **connexe**, *et* F *une isogénie dont une puissance est un endomorphisme de Frobenius. Alors l'application (dite* application de Lang*)* $\mathcal{L} : g \mapsto g^{-1}.{}^F g$ *de* $\mathbf{G}$ *sur lui-même est surjective.*

Démonstration. L'application $\mathcal{L}$ a toutes ses fibres isomorphes à $\mathbf{G}^F$ donc finies, donc la dimension de son image est celle de $\mathbf{G}$, et comme $\mathbf{G}$ est irréductible elle est dominante ($\mathbf{G}$ est l'adhérence de son image), donc son image contient un ouvert non vide de $\mathbf{G}$.

Pour x fixé, l'application $g \mapsto g^{-1}.x.{}^F g$ a aussi des fibres finies car une fibre a même cardinal que les solutions de $g^{-1}x^F g = x$, c'est-à-dire $g = {}^{xF}g$; or xF a une puissance égale à une puissance de F : on a $(xF)^n = yF^n$ où $y = x^F x \dots {}^{F^{n-1}}x$; si on choisit n tel que x soit F^n-stable alors y l'est aussi et si e est l'ordre de y alors $(xF)^{ne} = F^{ne}$. Donc l'image de $g \mapsto g^{-1}.x.{}^F g$ contient aussi un ouvert, donc rencontre celle de $\mathcal{L}$, donc il existe g et h tels que $g^{-1}.{}^F g = h^{-1}.x.{}^F h$, donc $x = \mathcal{L}(gh^{-1})$. □

[Steinberg68] montre ce théorème sous la seule hypothèse que F est un endomorphisme surjectif tel que $\mathbf{G}^F$ soit fini.

Suite exacte de cohomologie Galoisienne.

En général [Serre, §5] si F est un groupe profini opérant continûment sur un ensemble E on définit $H^0(F, E) = E^F$ et si E est un groupe (sur lequel F opère de façon compatible avec l'opération de groupe) on définit $H^1(F, E)$. Si $A \subset B$ est une inclusion de groupes on a la "suite exacte de cohomologie Galoisienne"

$$1 \to H^0(F, A) \to H^0(F, B) \to H^0(F, B/A) \xrightarrow{p} H^1(F, A) \xrightarrow{i} H^1(F, B) \qquad (*)$$

Si le groupe est $\hat{\mathbb{Z}}$ de générateur F, on notera $H^i(F, E)$ pour $H^i(\hat{\mathbb{Z}}, E)$. Alors $H^1(F, E)$ est formé des F-classes de E, égales aux E-orbites pour la conjugaison

dans $E.F$, ou encore aux orbites de E sur lui-même pour la "conjugaison tordue" $e \mapsto e'eF(e'^{-1})$. Les applications dans (*) sont évidentes sauf p qui associe à une classe F-stable bA la F-classe de $b^{-1}F(b)$ (un élément de A puisque bA est stable) ; noter que $H^0(F,B) = B^F$ agit naturellement sur $H^0(F,B/A) = (B/A)^F$ et les éléments d'une même orbite ont même image dans $H^1(F,A)$. Pour les ensembles qui interviennent qui ne sont pas des groupes, on a affaire à une "suite exactes d'ensembles pointés" : l'image d'une application est égale à l'image réciproque par l'application suivante de l'élément neutre.

Le théorème de Lang peut se reformuler :

Proposition 10.2. *Si $\mathbf{G}$, F sont comme en 10.1, on a $H^1(F,\mathbf{G}) = 1$.*

Proposition 10.3. *Soient $\mathbf{G}, F$ comme en 10.1 et soit $\mathbf{V}$ une variété munie d'une action de F sur laquelle $\mathbf{G}$ agit transitivement, de façon compatible à F. Alors $\mathbf{V}^F$ est non vide.*

Démonstration. Pour $v \in \mathbf{V}$, il existe $g \in \mathbf{G}$ tel que ${}^F v = gv$. Écrivons $g^{-1} = h^{-1\,F}h$. Alors ${}^F(hv) = {}^F hgv = hg^{-1}gv = hv$. □

Lemme 10.4. *Soient $A \subset B$ deux sous-groupes fermés F-stables de $\mathbf{G}$ où A est connexe. Alors*

(i) On a $(B/A)^F = B^F/A^F$.

(ii) Si de plus A est normal dans B, le passage au quotient induit une bijection $H^1(F,B) \to H^1(F,A/B)$.

Démonstration. (i) est la suite exacte (*) puisque $H^1(F,A) = 1$ mais prouvons-le. Par 10.3, toute classe F-stable bA contient un élément F-stable, donc l'application naturelle $B^F/A^F \to (B/A)^F$ est surjective. Elle est injective car si $x, y \in B^F$ sont dans la même classe de A, alors $x^{-1}y \in A^F$.

Prouvons (ii). La surjectivité est claire. Réciproquement, si $b, b' \in B$ sont F-conjugués modulo A, on a $ab = xb'^{F}x^{-1}$, avec $x \in B$ et $a \in A$. Il faut voir que ab est F-conjugué à b, c'est-à-dire qu'il existe y tel que $yab^F y^{-1} = b$ ou encore $a = y^{-1\,bF}y$. Cela résulte de ce que, comme remarqué dans la preuve de 10.1, $\mathrm{ad}\, bF$ est encore une isogénie sur A dont une puissance est un Frobenius. □

Proposition 10.5. *Soient $\mathbf{G}, F, \mathbf{V}$ comme en 10.3. Alors*

(i) Soient $x \in \mathbf{V}^F$ et $g \in \mathbf{G}$; on a $gx \in \mathbf{V}^F$ si et seulement si $g^{-1\,F}g \in C_{\mathbf{G}}(x)$.

(ii) Étant donné $x \in \mathbf{V}^F$, l'application qui à l'orbite sous $\mathbf{G}^F$ de $gx \in \mathbf{V}^F$ associe la classe de F-conjugaison de l'image de $g^{-1\,F}g$ dans $C_{\mathbf{G}}(x)/C_{\mathbf{G}}(x)^0$ est bien définie et est bijective.

Démonstration. La proposition traduit la suite exacte (*) pour l'inclusion $C_{\mathbf{G}}(x) \subset \mathbf{G}$, qui donne $1 \to C_{\mathbf{G}}(x)^F \to \mathbf{G}^F \to \mathbf{V}^F \to H^1(F, C_{\mathbf{G}}(x)) \to 1$ en tenant compte de $H^1(F, C_{\mathbf{G}}(x)) = H^1(F, C_{\mathbf{G}}(x)/C_{\mathbf{G}}(x)^0)$ donné par 10.4(ii). Mais nous allons le démontrer explicitement.

(i) résulte d'un calcul immédiat. Prouvons (ii). Pour $x \in \mathbf{V}^F$ soient $h, g \in \mathbf{G}$ tels que $hx, gx \in \mathbf{V}^F$. Remarquons que $hx = gx$ si et seulement si h et g diffèrent

d'un élément de $C_{\mathbf{G}}(x)$, et alors $h^{-1}Fh$ et $g^{-1}Fg$ sont F-conjugués dans $C_{\mathbf{G}}(x)$. On a donc une application bien définie de l'ensemble $\mathbf{V}^F$ sur les F-classes de $C_{\mathbf{G}}(x)$. D'autre part si h est un élément de $\mathbf{G}^F$, les éléments gx et hgx donnent le même élément $g^{-1}Fg = (hg)^{-1}F(hg)$. Donc l'application est bien définie des orbites sous $\mathbf{G}^F$ dans $\mathbf{V}^F$ dans les F-classes de $C_{\mathbf{G}}(x)$. Supposons que $g^{-1}Fg$ et $h^{-1}Fh$ soient des éléments F-conjugués par $n \in C_{\mathbf{G}}(x)$, alors gnh^{-1} est un élément de $\mathbf{G}^F$ qui envoie hx sur gx. L'application est donc injective. Comme, $\mathbf{G}$ étant connexe, un élément de $C_{\mathbf{G}}(x)$ s'écrit $g^{-1}Fg$ avec $g \in \mathbf{G}$, on voit que l'application est surjective. On termine par 10.4(ii). □

Corollaire 10.6.

(i) Les sous-groupes de Borel F-stables forment une seule orbite non vide sous la $\mathbf{G}^F$-conjugaison.

(ii) Supposons $\mathbf{G}$ réductif, et soit $\mathbf{P}$ un sous-groupe parabolique F-stable. Alors les sous-groupes de Levi F-stable de $\mathbf{P}$ forment une seule orbite non-vide sous la $(\mathrm{R_u}(\mathbf{P}))^F$-conjugaison.

(iii)On appelle classe de conjugaison géométrique *l'intersection avec $\mathbf{G}^F$ d'une classe de conjugaison F-stable de $\mathbf{G}$. Une classe géométrique C est non vide et se scinde sous $\mathbf{G}^F$ en classes paramétrées par $H^1(F, C_{\mathbf{G}}(x)/C_{\mathbf{G}}(x)^0)$ pour $x \in C$.*

Démonstration. (i) résulte de 10.5 en prenant pour $\mathbf{V}$ la variété des sous-groupes de Borel, et utilisant que pour un tel sous-groupe $N_{\mathbf{G}}(\mathbf{B}) = \mathbf{B}$ est connexe.

De même, pour (ii), par 7.7 on peut identifier les sous-groupes de Levi de $\mathbf{P}$ à $\mathrm{R_u}(\mathbf{P})$, avec des stabilisateurs triviaux.

Pour (iii) il suffit d'appliquer 10.5 en prenant pour $\mathbf{V}$ la classe, sur laquelle $\mathbf{G}$ agit par conjugaison. □

Exemple 10.7.

Soit $s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{F}_q)$; par 7.11, si $q \not\equiv 0 \pmod 2$ alors $C_{\mathrm{PGL}_2}(s)$ a deux composantes connexes et $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in C_{\mathrm{PGL}_2}(s) - C_{\mathrm{PGL}_2}(s)^0$. Si $\lambda \in \mathbb{F}_{q^2}, \lambda^{q-1} = -1$ alors $m = \begin{pmatrix} 0 & \lambda^{-1} \\ \lambda & 0 \end{pmatrix}$ vérifie ${}^F m = -m$ dans GL_2 donc $m \in \mathrm{PGL}_2^F$ et si $x = \begin{pmatrix} 1 & 1 \\ \lambda & -\lambda \end{pmatrix}$ alors $xsx^{-1} = m$ et $x^{-1}Fx = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ donc m est conjugué géométriquement mais non rationnellement à s.

On voit d'après (i) et (ii) que les tores maximaux F-stables des sous-groupes de Borel F-stables existent et sont conjugués sous $\mathbf{G}^F$. On peut trouver donc un couple $\mathbf{T} \subset \mathbf{B}$ qui sont F-stables.

Il y a une $\mathbb{F}_q$-structure naturelle sur $X(\mathbf{T}) = \mathrm{Hom}(\mathbf{T}, \mathbb{G}_m)$ donnée par la $\mathbb{F}_q$-structure $F(x) = x^q$ sur $\mathbb{G}_m$ (la seule compatible à la structure de groupe) : pour cette $\mathbb{F}_q$-structure F induit une permutation τ des racines telle que pour

$\alpha \in X(\mathbf{T})$ on a $(\tau\alpha)({}^F t) = (\alpha(t))^q$. On en déduit que $F(\mathbf{u}_\alpha(x)) = u_{\tau(\alpha)}(\lambda x^q)$ donc F est une isogénie associée à τ et telle que $q_\alpha = q$ pour tout α.

Notons que par le théorème de Lang, si $g \in \mathbf{G}$, l'isogénie $\operatorname{ad} gF$ définit un groupe $\mathbf{G}^{\operatorname{ad} gF}$ isomorphe à $\mathbf{G}^F$. En effet, si on écrit $g = h^{-1}F(h)$ alors x est $\operatorname{ad} gF$-fixe si et seulement si ${}^h x$ est F-fixe.

Exemple 10.8. Considérons le groupe GL_n sur $\overline{\mathbb{F}}_q$. Il est défini sur $\mathbb{F}_q$ car son algèbre est égale à $\overline{\mathbb{F}}_q[T_{i,j}, \det(T_{i,j})^{-1}]$, qui est isomorphe à $\mathbb{F}_q[T_{i,j}, \det(T_{i,j})^{-1}] \otimes \overline{\mathbb{F}}_q$. Ses points sur $\mathbb{F}_q$ forment le groupe $\mathrm{GL}_n(\mathbb{F}_q)$. On peut faire le même raisonnement avec SL_n, les groupes symplectiques, orthogonaux, *etc...* On obtient le Frobenius déployé sur $\mathbb{F}_q$ où $\tau = 1$. Ce Frobenius élève tous les coefficients d'une matrice à la puissance q. Un exemple de Frobenius non déployé est le groupe unitaire $\mathrm{GL}_n^{F'}$ où F' est l'endomorphisme de Frobenius défini par $F'(x) = F({}^t x^{-1})$, où F est l'endomorphisme de Frobenius déployé. Ici $\tau(\alpha) = -\alpha$.

La permutation τ stabilise l'ordre défini par le sous-groupe de Borel F-stable $\mathbf{B}$ et la donnée radicielle $(X(\mathbf{T}), Y(\mathbf{T}), \Phi, \check{\Phi})$ plus la donnée de de q et de τ détermine le couple $(\mathbf{G}, F)$ (donc $\mathbf{G}^F$) à isomorphisme près. Les possibilités pour τ sont classifiées par les automorphismes du diagramme de Dynkin associé à la donnée radicielle.

De tels automorphismes non-triviaux τ sur un système de racines irréductible sont ${}^2A_n (n \geq 2)$, ${}^2D_n$, ${}^3D_4$ et ${}^2E_6$ où l'exposant à gauche indique l'ordre de τ. On obtient donc la liste suivante pour les couples $(\mathbf{G}, F)$ à isomorphisme près où $\mathbf{G}$ est un groupe algébrique simple (adjoint) sur $\overline{\mathbb{F}}_q$, et F un endomorphisme de Frobenius associé à une $\mathbb{F}_q$-structure (alors $\mathbf{G}^F$ est un groupe fini simple sauf indication contraire) :

Dans le cas déployé ($\tau = 1$) :

— $A_n (n \geq 1)$ — le groupe algébrique simple est le groupe projectif spécial linéaire $\mathrm{PSL}_n \simeq \mathrm{PGL}_n$

Remarque 10.9. Le groupe fini simple est $\mathrm{SL}_n^F / Z(\mathrm{SL}_n^F)$, qui n'est pas égal à PSL_n^F mais est son dérivé. Considérons le groupe PSL_n sur $\overline{\mathbb{F}}_q$, c'est-à-dire le quotient de SL_n par son centre. Ce groupe est défini sur $\mathbb{F}_q$, mais si n n'est pas premier à $q-1$, PSL_n^F n'est pas le quotient de SL_n^F par son centre (on a fait le quotient par un sous-groupe non connexe). En effet, le centre de SL_n s'identifie au groupe μ_n des racines n-ième de l'unité. La suite exacte (*) appliquée à l'inclusion $\mu_n \subset \mathrm{SL}_n$ donne $1 \to \mu_n^F \to \mathrm{SL}_n^F \to \mathrm{PSL}_n^F \to H^1(F, \mu_n) \to 1$ où $H^1(F, \mu_n) = \mu_n / \mu_n^{q-1}$ d'où un défaut de surjectivité si $\mu_n^{q-1} \neq \mu_n$.
Notons aussi que pour $q = 2$ (resp. 3) on a $\mathrm{SL}_n^F / Z(\mathrm{SL}_n^F) = \mathfrak{S}_3$ (resp. $\mathfrak{A}_4$) et n'est pas simple.

— $C_n (n \geq 2)$ — Groupe projectif symplectique PSp_{2n}.

— $B_2 (n \geq 2)$ — Groupe orthogonal SO_{2n+1} (B_2 et C_2 donnent des groupes isomorphes ; le groupe ainsi obtenu est isomorphe à $\mathfrak{S}_6$ pour $q = 2$ et n'est donc pas simple dans ce cas).

— D_n (resp. ${}^2D_n$)$(n \geq 4)$ — Groupe projectif orthogonal PSO_{2n}^+ (resp. PSO_{2n}^-).

— G_2 (pour $q = 2$ le groupe obtenu n'est pas simple ; son dérivé, qui est d'indice 2, l'est).
— F_4, E_6, E_7, E_8.

Dans le cas non déployé :
— ${}^2A_n (n \geq 2)$ — Groupe projectif spécial unitaire $\mathrm{PSU}_n \simeq \mathrm{PU}_n$ (même remarque sur PSU_n^F que sur PSL_n^F) ; de plus pour $q = 2$ le groupe obtenu n'est pas simple) ;
— ${}^2D_n) (n \geq 4)$ — Groupe projectif orthogonal PSO_{2n}^-.
— ${}^3D_4$ — Groupe de la trialité.
— ${}^2E_6$.

De plus il y a des isogénies exceptionnelles correspondant à des automorphismes du système de racines "à homothéthie près par $\sqrt{2}$" (resp. $\sqrt{3}$) dont le carré est un Frobenius sur un corps de caractéristique 2 (resp. 3). Cela donne les groupes de Suzuki et de Ree, de type ${}^2B_2$, ${}^2F_4$ (resp. ${}^2G_2$) en caractéristique 2 (resp. 3). Le groupe $\mathbf{G}^F$ obtenu est simple sauf ${}^2B_2$ pour $q = 2$ (qui est résoluble), ${}^2G_2$ pour $q = 3$ (dont le dérivé est le groupe simple $\mathrm{SL}_2(\mathbb{F}_8)$), et ${}^2F_4$ pour $q = 2$ dont le dérivé, d'indice 2, est simple. En ajoutant aux groupes décrits ci-dessus ces groupes et les groupes alternés, on obtient toutes les séries infinies de groupes simples finis.

Proposition 10.10.

(i) Les éléments semi-simples de $\mathbf{G}$ *sont les* p'*-éléments de* $\mathbf{G}$ *et les éléments unipotents sont les* p*-éléments de* $\mathbf{G}$*, où* p *est la caractéristique de* $\overline{\mathbb{F}}_q$*.*

(ii) Tout élément semi-simple F*-stable est dans un tore maximal* F*-stable de* $\mathbf{G}$*.*

Démonstration. (i) s'obtient immédiatement en plongeant $\mathbf{G}$ dans un GL_n convenable.

Soit s un élément semi-simple ; on a $s \in C^0_{\mathbf{G}}(s)$, et y étant central il est dans tous les tores maximaux de $C^0_{\mathbf{G}}(s)$, donc en particulier dans les tores maximaux F-stables de $C^0_{\mathbf{G}}(s)$ qui sont aussi des tores maximaux F-stables de $\mathbf{G}$. □

Proposition 10.11. *Supposons* $\mathbf{G}$ *réductif.*

(i)Soit $\mathbf{T}$ *un tore maximal* F*-stable de* $\mathbf{G}$*, l'endomorphisme* F *agit sur le groupe de Weyl* W *de* $\mathbf{T}$*, et l'on a* $W^F = N_{\mathbf{G}}(\mathbf{T})^F/\mathbf{T}^F$*.*

Soient maintenant $\mathbf{T} \subset \mathbf{B}$ *un tore maximal et un sous-groupe de Borel* F*-stables de* $\mathbf{G}$*. Alors*

(ii) On a la décomposition de Bruhat associée à la (B, N)-paire relative *de* $\mathbf{G}^F$ *(voir 10.14 ci-dessous) :* $\mathbf{G}^F = \coprod_{w \in W^F} \mathbf{B}^F w \mathbf{B}^F$*.*

(iii) $|\mathbf{G}^F| = q^{l(w_0)} |\mathbf{T}^F| (\sum_{w \in W^F} q^{l(w)})$ *où* $q \in \mathbb{R}_{>0}$ *est défini par le fait qu'il existe* $a \in \mathbb{N}$ *tel que* F^a *soit un Frobenius associé à une* $\mathbb{F}_{q^a}$*-structure.*

(iv) $\mathrm{R_u}(\mathbf{B})^F$ *est un* p*-sous-groupe de Sylow de* $\mathbf{G}^F$*.*

Démonstration. (i) vient de 10.4(i).

Soit $\mathbf{B} = \mathbf{U} \rtimes \mathbf{T}$ une décomposition de Levi F-stable d'un sous-groupe de Borel F-stable de $\mathbf{G}$. Le (ii) vient de la "décomposition de Bruhat unique" $\mathbf{B}w\mathbf{B} = \mathbf{U}\mathbf{T}w\mathbf{U}_w$, qui implique qu'un élément F-stable de $\mathbf{B}w\mathbf{B}$ est dans $\mathbf{B}^F n\mathbf{B}^F = \mathbf{B}^F n\mathbf{U}_w^F$ où $n \in N_{\mathbf{G}}(\mathbf{T})^F$ a pour image w dans W.

Montrons (iii). Par ce qui précède $|\mathbf{G}^F/\mathbf{B}^F| = \sum_{w\in W^F} |\mathbf{U}_w^F|$ où $\mathbf{U}_w^F$, et utilisant $|\mathbf{B}^F| = |\mathbf{T}^F||\mathbf{U}^F|$ on en déduit la formule annoncée si on montre que $|\mathbf{U}_w| = q^{l(w)}$ (car $\mathbf{U} = \mathbf{U}_{w_0}$). Comme $\mathbf{U}_w$ est un espace affine de dimension $l(w)$, si F est un Frobenius sur $\mathbb{F}_q$ par 9.8 on a $|\mathbf{U}_w^F| = q^{l(w)}$. On admettra la formule dans les autres cas — elle résulte de ce que $|\mathbf{U}_w^F| = \prod_{\{\alpha\in\Phi^+|w(\alpha)<0\}} q_\alpha$ et de la description de W^F donnée en 10.12 ci-dessous.

Comme $|\mathbf{G}^F/\mathbf{U}^F| = |\mathbf{T}^F|(\sum_{w\in W^F} q^{l(w)})$ est premier à p (car $\mathbf{T}$ est un p'-groupe, et $\sum_{w\in W^F} q^{l(w)} \equiv 1 \bmod. q$) on voit que $\mathbf{U}^F$ est un p-sous groupe de Sylow de $\mathbf{G}^F$ (on peut voir que $N_{\mathbf{G}^F}(\mathbf{U}^F) = \mathbf{B}^F$, donc $\sum_{w\in W^F} q^{l(w)}$ est le nombre de p-sous-groupes de Sylow de $\mathbf{G}^F$). □

Remarquons que le fait que $\mathrm{R_u}(\mathbf{B})^F$ est un p-sous-groupe de Sylow de $\mathbf{G}^F$ s'étend aux groupes non réductifs, car $\mathrm{R_u}(\mathbf{G})$ est un p-groupe d'après 10.10(i), il est inclus dans tous les radicaux unipotents des sous-groupes de Borel, et $\mathrm{R_u}(\mathbf{G})$ étant connexe $|\mathbf{G}^F| = |(\mathbf{G}/\mathrm{R_u}(\mathbf{G}))^F||\mathrm{R_u}(\mathbf{G})^F|$.

La proposition suivante nous permettra de décrire la (B, N)-paire relative de $\mathbf{G}^F$:

Proposition 10.12. *Soit σ un automorphisme du système de Coxeter (W, S), c'est-à-dire un automorphisme de W qui stabilise S. Soit $(S/\sigma)_{<\infty}$ l'ensemble des orbites I de σ dans S telles que le sous-groupe parabolique W_I soit fini. Alors $(W^\sigma, \{w_I\}_{I\in(S/\sigma)_{<\infty}})$, est un système de Coxeter, où W^σ est le sous-groupe des points fixes de σ, et où w_I est l'élément de plus grande longueur de W_I (cf. 2.5). De plus, si $w_{I_1}\dots w_{I_k}$ est la décomposition réduite d'un élément w dans le système de Coxeter ci-dessus, on a $l(w) = \sum_{i=1}^{i=k} l(w_{I_i})$ (où l est la fonction longueur du système (W, S)).*

Démonstration. Commençons par démontrer que W^σ est engendré par les w_I. Puisque σ est un automorphisme de (W, S), pour $w \in W^\sigma$ l'ensemble des $s \in S$ tels que $l(sw) < l(w)$ est une union d'orbites. Si I est l'une d'entre elles, écrivons $w = vw'$ où w' est I-réduit et $v \in W_I$. Alors $l(sv) < l(s)$ pour tout $s \in I$ n'est possible que si W_I est fini et $v = w_I$ (voir 2.5). De proche en proche on trouve $w = w_{I_1}\dots w_{I_k}$ où $l(w) = \sum_{i=1}^{i=k} l(w_{I_i})$.

Soit S_σ l'ensemble des w_I pour $I \in (S/\sigma)_{<\infty}$ et R_σ l'ensemble de leurs conjugués dans W^σ. Nous allons utiliser le critère 2.15 pour voir que (W^σ, S_σ) est un système de Coxeter, mais en retournant la gauche et la droite. Pour $w_I \in S_\sigma$, on pose $D_{w_I} = \{w \in W^\sigma \mid w \text{ est réduit-}I\}$. On a manifestement $D_{w_I} \ni 1$ et $D_{w_I} \cap D_{w_I} w_I = \emptyset$. Étudions le cas où $w \in D_{w_I}$ et $w_J w \notin D_{w_I}$. Il faut montrer que $w_J w = w w_I$. On a $N(w_J w) = N(w_J)^w \dot{+} N(w)$. Nous aurons besoin du lemme :

Lemme 10.13. *Sous les hypothèses de 2.4, pour $r \in R$ la condition $r \in N(w)$ implique $l(wr) < l(w)$.*

Démonstration. En effet si $w = s_1 \dots s_n$ est une expression réduite il existe i tel que $r = s_n \dots s_i \dots s_n$ d'où $wr = s_1 \dots \hat{s}_i \dots s_n$. □

On déduit du lemme que si $r \in W_I$ et pour $w \in W^\sigma$ on a $r \in N(w)$, alors $N(w_I) \subset N(w)$. En effet si $l(wr) < l(w)$ alors w ne peut être I-réduit et il a donc une décomposition $w_{I_1} \dots w_{I_k}$ où les longueurs s'ajoutent et $I_k = I$.

Comme par hypothèse dans notre situation on a $N(w) \cap N(w_I) = \emptyset$ et $N(w_J w) \supset N(w_I)$, on en déduit $N(w_J)^w \supset N(w_I)$. Il faut en déduire $w_J^w = w_I$. Si w n'est pas J-réduit on peut le remplacer par $w_J w$, les prémisses et conclusions étant équivalents pour w et $w_J w$. On écrit alors $N(w_I w^{-1}) = {}^w N(w_I) + N(w^{-1})$. Comme w est J-réduit, $N(w^{-1}) \cap N(w_J) = \emptyset$, et comme ${}^w N(w_I)$ rencontre $N(w_J)$, alors tout $N(w_J)$ doit être dans $N(w_I w^{-1})$ donc dans ${}^w N(w_I)$. De l'égalité $N(w_I) = x^{-1} N(w_J) x$ on déduit $W_I = x^{-1} W_J x$ d'où $w_I = x^{-1} w_J x$ car $x^{-1} w_J x$ est un élément σ-stable non trivial de w_I. □

Notons au passage que 1 et w_I sont les seuls éléments σ-stables de W_I.

Corollaire 10.14. *Supposons* $\mathbf{G}$ *réductif. Soit* $\mathbf{T} \subset \mathbf{B}$ *un couple formé d'un tore maximal* F*-stable inclus dans un sous-groupe de Borel* F*-stable de* $\mathbf{G}$*. Alors* $(\mathbf{B}^F, N_{\mathbf{G}}(\mathbf{T})^F)$ *est une* (B, N)*-paire pour* $\mathbf{G}^F$ *de groupe de Weyl* W^F*. L'ensemble de réflexions élémentaires de* W^F *est formé des* w_I *où* I *parcourt les orbites de* F *dans* S *et où* w_I *est l'élément de plus grande longueur de* W_I*.*

Démonstration. C'est une conséquence immédiate de la définition des (B, N)-paires, de 10.11(ii) et de 10.12. Il faut voir que si I est une orbite de F dans S, et $w \in W^F$, on a $\mathbf{B}^F w \mathbf{B}^F w_I \mathbf{B}^F \subset \mathbf{B}^F w \mathbf{B}^F \cup \mathbf{B}^F w w_I \mathbf{B}^F$. On utilise que soit $l(w) + l(w_I) = l(w w_I)$, auquel cas $\mathbf{B}^F w \mathbf{B}^F w_I \mathbf{B}^F = \mathbf{B}^F w w_I \mathbf{B}^F$, soit $w = w' w_I$ où $l(w') + l(w_I) = l(w' w_I)$ auquel cas $\mathbf{B}^F w \mathbf{B}^F w_I \mathbf{B}^F \subset \mathbf{B}^F w' \mathbf{B}^F w_I \mathbf{B}^F w_I \mathbf{B}^F$, et $\mathbf{B}^F w_I \mathbf{B}^F w_I \mathbf{B}^F \subset \mathbf{B}^F \cup \mathbf{B}^F w_I \mathbf{B}^F$ car 1 et w_I sont les seuls éléments F-stables de W_I. □

Proposition 10.15. *Soit* $\mathbf{T}$ *un tore maximal* F*-stable fixé de* $\mathbf{G}$*, groupe algébrique réductif connexe défini sur* $\mathbb{F}_q$*. Les classes de conjugaison sous* $\mathbf{G}^F$ *de tores* F*-stables sont paramétrées par les* $H^1(F, W_{\mathbf{G}}(\mathbf{T}))$ *— on appelle* **type** *du tore* ${}^g\mathbf{T}$ *par rapport au tore* $\mathbf{T}$ *la* F*-classe de* w*, image dans* $W_{\mathbf{G}}(\mathbf{T})$ *de l'élément* $g^{-1\,F} g \in N_{\mathbf{G}}(\mathbf{T})$*.*

Démonstration. On applique 10.5 en prenant pour $\mathbf{V}$ l'ensemble des tores maximaux de $\mathbf{G}$ sur lequel $\mathbf{G}$ agit par conjugaison. □

Remarquons que le tore ${}^g\mathbf{T}$, muni de l'action de F est identifié par conjugaison par g^{-1} au tore $\mathbf{T}$ muni de wF, si w est le type de ${}^g\mathbf{T}$.

Proposition 10.16. *Soit* $\mathbf{T}_w$ *un tore de type* w *par rapport au tore* $\mathbf{T}$*. Alors* $|\mathbf{T}_w^F| = \det(wF - 1 \mid X(\mathbf{T}))$*.*

Démonstration. Il suffit de démontrer cette formule pour $\mathbf{T}$. En appliquant $\mathrm{Hom}(-, \mathbb{G}_m)$ à la suite exacte $1 \to \mathbf{T}^F \to \mathbf{T} \xrightarrow{F-1} \mathbf{T} \to 1$ (où la surjectivité provient du théorème de Lang) on obtient $1 \to X(\mathbf{T}) \xrightarrow{F-1} X(\mathbf{T}) \xrightarrow{p} \mathrm{Irr}(\mathbf{T}^F)$ où

on a posé $\mathrm{Irr}(\mathbf{T}^F) = \mathrm{Hom}(\mathbf{T}^F, \mathbb{G}_m)$ et il faut voir la surjectivité de la restriction des caractères p. Cela résulte de ce que l'application duale $\mathrm{Hom}(\mathrm{Irr}(\mathbf{T}^F) \to \mathrm{Hom}(X(\mathbf{T}), \mathbb{G}_m)$ est l'injection $\mathbf{T}^F \hookrightarrow \mathbf{T}$ (peut identifier l'algèbre de $\mathbf{T}$ à $\overline{\mathbb{F}}_q(X(\mathbf{T}))$. Cela résulte par produit du cas où $\mathbf{T}$ est de dimension 1). □

11 Induction parabolique ; formule de Mackey

Pour construire des représentations irréductibles d'un groupe fini G, une heuristique qui marche "souvent" est de considérer une famille $\mathcal{F}$ de sous-groupes de G "de même type que G" et de construire des représentations de G "par récurrence" à partir de celles de $H \in \mathcal{F}$ (par exemple en utilisant Ind_H^G ; un exemple typique est la construction des représentations des groupes symétriques $\mathfrak{S}_n$ comme combinaison de $\mathrm{Ind}_{\mathfrak{S}_{n_1} \times \ldots \times \mathfrak{S}_{n_k}}^{\mathfrak{S}_n}$ quand $n_1 + \ldots + n_k = n$).

Dans le cas d'un groupe de type de Lie, une famille $\mathcal{F}$ convenable de sous-groupes de $\mathbf{G}^F$ est constituée des groupes $\mathbf{L}^F$ où $\mathbf{L}$ est un sous-groupe de Levi F-stable d'un sous-groupe parabolique F-stable de $\mathbf{G}$. Mais ici $\mathrm{Ind}_{\mathbf{L}^F}^{\mathbf{G}^F}$ ne convient pas, ayant une décomposition en irréductibles "trop compliquée" ; il faut utiliser "l'induction parabolique" appelée aussi "l'induction de Harish-Chandra", définie comme induction généralisée associée à un bimodule.

Soient G et L deux groupes finis et M un G-module-L. On définit $R_L^G : \lambda \mapsto M \otimes_{\mathbb{C}L} \lambda$ de la catégorie des $\mathbb{C}L$-modules à gauche dans celle des $\mathbb{C}G$-modules à gauche, où G opère par son action sur M. Le foncteur ${}^*R_L^G : \gamma \mapsto M^* \otimes_{\mathbb{C}G} \gamma$ est adjoint, où $M^* = \mathrm{Hom}(M, \mathbb{C})$ est le module dual, car $\mathrm{Hom}_{\mathbb{C}L}(M^* \otimes_{\mathbb{C}G} \gamma, \lambda) \simeq \gamma^* \otimes_{\mathbb{C}G} M \otimes_{\mathbb{C}L} \lambda \simeq \mathrm{Hom}_{\mathbb{C}G}(\gamma, M \otimes_{\mathbb{C}L} \lambda)$.

L'associativité du produit tensoriel donne :

Proposition 11.1. *(Transitivité) Soient G, H, et K des groupes finis ; soit M un G-module-H et N un H-module-K, alors le foncteur composé $R_H^G \circ R_K^H$ est égal au foncteur R_K^G défini par $M \otimes_{\mathbb{C}H} N$ considéré comme G-module-K.*

Dans la suite, les modules considérés seront toujours des $\mathbb{C}$-espaces vectoriels de dimension finie. Sous ces hypothèses on a

Proposition 11.2. *Pour $g \in G$ on a*

$$\mathrm{Trace}(g \mid R_L^G \lambda) = |L|^{-1} \sum_{l \in L} \mathrm{Trace}((g, l^{-1}) \mid M) \, \mathrm{Trace}(l \mid \lambda).$$

Démonstration. L'idempotent $p = |L|^{-1} \sum_l l^{-1} \otimes l$ est un projecteur de $M \otimes_{\mathbb{C}} \lambda$ sur $M \otimes_{\mathbb{C}L} \lambda$. La trace de $g \in G$ sur $R_L^G \lambda$ est donc la trace sur $M \otimes_{\mathbb{C}} \lambda$ de gp, d'où la formule de l'énoncé. □

Exemple 11.3. Induction et restriction. On suppose L sous-groupe de G et l'on prend $M = \mathbb{C}G$ où G opère à gauche et L à droite, par translations ; alors R_L^G est l'induction et son adjoint la restriction.

Exemple 11.4. *Induction et restriction de Harish-Chandra.* Soit $\mathbf{G}$ un groupe de type de Lie et soit $\mathbf{L} \subset \mathbf{P}$ un sous-groupe de Levi F-stable d'un sous-groupe parabolique F-stable de $\mathbf{G}$. On note $R_{\mathbf{L}\subset\mathbf{P}}^{\mathbf{G}}$ l'induction associée à $\mathbb{C}[\mathbf{G}^F/\mathbf{U}^F]$ où $\mathbf{U} = \mathrm{R_u}(\mathbf{P})$, un $\mathbf{G}^F$-module-$\mathbf{L}^F$ sur lequel $\mathbf{G}^F$ opère par translation à gauche et $\mathbf{L}^F$ opère par translation à droite. L'adjoint noté ${}^*R_{\mathbf{L}\subset\mathbf{P}}^{\mathbf{G}}$ correspond à $\mathbb{C}[\mathbf{U}^F\backslash\mathbf{G}^F]$, un $\mathbf{L}^F$-module-$\mathbf{G}^F$ où $\mathbf{G}^F$ opère à droite et $\mathbf{L}^F$ à gauche. La formule du caractère 11.2 donne pour χ le caractère d'une représentation de $\mathbf{G}^F$ et $l \in \mathbf{L}^F$:

$$\begin{aligned}
{}^*R_{\mathbf{L}\subset\mathbf{P}}^{\mathbf{G}}(\chi)(l) &= |\mathbf{G}^F|^{-1} \sum_{g\in\mathbf{G}^F} \#\{\mathbf{U}^F x \in \mathbf{U}^F\backslash\mathbf{G}^F \mid \mathbf{U}^F x = l\mathbf{U}^F xg\}\chi(g^{-1}) \\
&= |\mathbf{G}^F|^{-1} \sum_{g\in\mathbf{G}^F} \#\{\mathbf{U}^F x \in \mathbf{U}^F\backslash\mathbf{G}^F \mid xg^{-1}x^{-1} \in l\mathbf{U}^F\}\chi(g^{-1}) \\
&= |\mathbf{U}^F|^{-1} \sum_{u\in\mathbf{U}^F} \chi(lu),
\end{aligned}$$

cette dernière égalité car χ étant une fonction centrale sur $\mathbf{G}^F$ vérifie $\chi(g^{-1}) = \chi(xg^{-1}x^{-1})$.

$R_{\mathbf{L}\subset\mathbf{P}}^{\mathbf{G}}$ admet aussi comme description "l'extension triviale" de $\mathbf{L}$ à $\mathbf{P}$ à travers le quotient $\mathbf{P}/\mathbf{U} = \mathbf{L}$ suivie de l'induction $\mathrm{Ind}_{\mathbf{P}^F}^{\mathbf{G}^F}$. De même, ${}^*R_{\mathbf{L}\subset\mathbf{P}}^{\mathbf{G}}$ est la restriction $\mathrm{Res}_{\mathbf{P}^F}^{\mathbf{G}^F}$ suivie de la prise des co-invariants sous $\mathbf{U}^F$.

Remarque 11.5. Nous verrons que $R_{\mathbf{L}\subset\mathbf{P}}^{\mathbf{G}}$ ne dépend pas de $\mathbf{P}$, ce qui nous permettra de noter $R_{\mathbf{L}}^{\mathbf{G}}$. Nous n'avons ici défini un tel foncteur que quand $\mathbf{L}$ est un sous-groupe de Levi F-stable d'un sous-groupe parabolique F-stable $\mathbf{P}$ de $\mathbf{G}$; l'induction de Deligne-Lusztig est une généralisation définie même si $\mathbf{P}$ n'est pas F-stable.

Les propriétés fondamentales de l'induction de Harish-Chandra sont analogues à celles de l'induction ordinaire :

Proposition 11.6. *(Transitivité de $R_{\mathbf{L}}^{\mathbf{G}}$) Soit $\mathbf{G}$ un groupe réductif défini sur $\mathbb{F}_q$, soit $\mathbf{P}$ un sous-groupe parabolique F-stable de $\mathbf{G}$, soit $\mathbf{P}'$ un sous-groupe parabolique F-stable inclus dans $\mathbf{P}$. On note $\mathbf{L}$ un sous-groupe de Levi F-stable de $\mathbf{P}$ et $\mathbf{L}'$ un sous-groupe de Levi F-stable de $\mathbf{P}'$ inclus dans $\mathbf{L}$. Alors on a $R_{\mathbf{L}\subset\mathbf{P}}^{\mathbf{G}} \circ R_{\mathbf{L}'\subset\mathbf{L}\cap\mathbf{P}'}^{\mathbf{L}} = R_{\mathbf{L}'\subset\mathbf{P}'}^{\mathbf{G}}$.*

Démonstration. On pose $\mathbf{U} = \mathrm{R_u}(\mathbf{P}), \mathbf{U}' = \mathrm{R_u}(\mathbf{P}')$. D'après 11.1, pour montrer la proposition il faut montrer que

$$\mathbb{C}[\mathbf{G}^F/\mathbf{U}^F] \otimes_{\mathbb{C}\mathbf{L}^F} \mathbb{C}[\mathbf{L}^F/(\mathbf{L}\cap\mathbf{U}')^F] \simeq \mathbb{C}[\mathbf{G}^F/\mathbf{U}'^F]$$

en tant que $\mathbf{G}^F$-module-$\mathbf{M}^F$. Cela résulte de l'isomorphisme de $\mathbf{G}^F$-ensembles-$\mathbf{M}^F$ de $\mathbf{G}^F/\mathbf{U}^F \times_{\mathbf{L}^F} \mathbf{L}^F/(\mathbf{L}\cap\mathbf{U}')^F$ vers $\mathbf{G}^F/\mathbf{U}'^F$ donné par $(g\mathbf{U}^F, l(\mathbf{L}\cap\mathbf{U}')^F) \mapsto gl\mathbf{U}'^F$; cette application est bien définie car $\mathbf{U}' = \mathbf{U}(\mathbf{L}\cap\mathbf{U}')$ par 7.12 et 7.13(i) et la propriété d'unicité dans cette décomposition montre que $\mathbf{U}'^F = \mathbf{U}^F(\mathbf{L}^F \cap \mathbf{U}'^F)$; donc $g\mathbf{U}^F l(\mathbf{L}\cap\mathbf{U}')^F = gl\mathbf{U}^F(\mathbf{L}\cap\mathbf{U}')^F = gl\mathbf{U}'^F$ où dans la première égalité on a utilisé que l normalise $\mathbf{U}^F$. Il est clair que cette application se factorise par le produit amalgamé, fournissant un isomorphisme. □

Nous allons maintenant démontrer la propriété la plus importante de l'induction de Harish-Chandra, qui est un analogue de la formule de Mackey sur la composition d'une restriction et d'une induction.

Théorème 11.7. *Soit* $\mathbf{L}$ *(resp.* $\mathbf{M}$*) un sous-groupe de Levi* F*-stable du sous-groupe parabolique* F*-stable* $\mathbf{P}$ *(resp.* $\mathbf{Q}$*) de* $\mathbf{G}$*. Alors, si* $\operatorname{ad} x$ *dénote l'action de* x *par conjugaison sur les représentations, on a :*

$$ {}^*R^{\mathbf{G}}_{\mathbf{L}\subset\mathbf{P}} \circ R^{\mathbf{G}}_{\mathbf{M}\subset\mathbf{Q}} = \sum_{x\in\mathbf{L}^F\backslash\mathcal{S}(\mathbf{L},\mathbf{M})^F/\mathbf{M}^F} R^{\mathbf{L}}_{\mathbf{L}\cap{}^x\mathbf{M}\subset\mathbf{L}\cap{}^x\mathbf{Q}} \circ {}^*R^{{}^x\mathbf{M}}_{\mathbf{L}\cap{}^x\mathbf{M}\subset\mathbf{P}\cap{}^x\mathbf{M}} \circ \operatorname{ad} x, $$

où $\mathcal{S}(\mathbf{L},\mathbf{M}) = \{x\in\mathbf{G} \mid \mathbf{L}\cap{}^x\mathbf{M}$ *contient un tore maximal de* $\mathbf{G}\ \}$.

Démonstration. Donnons d'abord une conséquence de 5.5.

Lemme 11.8. *Avec les notations de 11.7,*

(i) L'inclusion $\mathcal{S}(\mathbf{L},\mathbf{M})\hookrightarrow\mathbf{G}$ *induit un isomorphisme* $\mathbf{L}\backslash\mathcal{S}(\mathbf{L},\mathbf{M})/\mathbf{M}\xrightarrow{\sim}\mathbf{P}\backslash\mathbf{G}/\mathbf{Q}$.

(ii) $\mathbf{P}^F\backslash\mathbf{G}^F/\mathbf{Q}^F = (\mathbf{P}\backslash\mathbf{G}/\mathbf{Q})^F$*, et* $\mathbf{L}^F\backslash\mathcal{S}(\mathbf{L},\mathbf{M})^F/\mathbf{M}^F = (\mathbf{L}\backslash\mathcal{S}(\mathbf{L},\mathbf{M})/\mathbf{M})^F$.

Démonstration. Montrons d'abord (ii). D'après 10.5 comme $\mathbf{P}\times\mathbf{Q}$ ainsi que par 7.12 le stabilisateur $\mathbf{P}\cap{}^x\mathbf{Q}$ d'un point $x\in\mathbf{G}$ sous l'action de $\mathbf{P}\times\mathbf{Q}$ sont connexes, les orbites $\mathbf{P}^F\backslash\mathbf{G}^F/\mathbf{Q}^F$ sous $\mathbf{P}^F\times\mathbf{Q}^F$ s'identifient aux orbites F-stables $(\mathbf{P}\backslash\mathbf{G}/\mathbf{Q})^F$. De même, comme $\mathbf{L}\cap{}^x\mathbf{M}$ contient un tore maximal, il est connexe par 7.12, donc les orbites $\mathbf{L}^F\backslash\mathcal{S}(\mathbf{L},\mathbf{M})^F/\mathbf{M}^F$ sous $\mathbf{L}^F\times\mathbf{M}^F$ s'identifient aux orbites F-stables $(\mathbf{L}\backslash\mathcal{S}(\mathbf{L},\mathbf{M})/\mathbf{M})^F$.

Montrons(i). Il existe $g\in\mathbf{G}$ tel que $\mathbf{P}$ et ${}^g\mathbf{Q}$ aient un sous-groupe de Borel F-stable commun et que $\mathbf{L}$ et ${}^g\mathbf{M}$ aient un tore maximal commun. La formule $\mathbf{P}x\mathbf{Q} = (\mathbf{P}xg^{-1}{}^g\mathbf{Q})g$ montre que les doubles $\mathbf{P}\backslash\mathbf{G}/\mathbf{Q}$ sont translatées des doubles classes $\mathbf{P}\backslash\mathbf{G}/{}^g\mathbf{Q}$. De même $\mathcal{S}(\mathbf{L},\mathbf{M}) = \mathcal{S}(\mathbf{L},{}^g\mathbf{M})g$. Ceci permet, pour démontrer (i), de se placer dans le cas "standard" où $\mathbf{P}=\mathbf{P}_I$, $\mathbf{Q}=\mathbf{Q}_J$, $\mathbf{L}=\mathbf{L}_I$, et $\mathbf{M}=\mathbf{L}_J$. D'après le lemme 5.5, on peut choisir des représentants de $\mathbf{P}_I\backslash\mathbf{G}/\mathbf{P}_J$ dans $N(\mathbf{T})$, donc dans $\mathcal{S}(\mathbf{L}_I,\mathbf{M}_J)$. Donc l'application (i) est surjective. Réciproquement, si $\mathbf{L}\cap{}^x\mathbf{M}$ contient un tore maximal, alors ce tore est de la forme ${}^l\mathbf{T}$ et aussi ${}^{xm}\mathbf{T}$, avec $l\in\mathbf{L}$ et $m\in\mathbf{M}$. Mais alors $w = l^{-1}xm\in N_{\mathbf{G}}(\mathbf{T})$ est dans la même double classe $\mathbf{L}\backslash\mathcal{S}(\mathbf{L},\mathbf{M})/\mathbf{M}$ que x. On peut encore modifier y par W_I à gauche et W_J à droite pour qu'il soit I,J-réduit. Donc $|\mathbf{L}\backslash\mathcal{S}(\mathbf{L},\mathbf{M})/\mathbf{M}|\le|W_I\backslash W/W_J|$ et par 5.5, l'application (i) est injective. □

Posons $\mathbf{U}=\mathrm{R_u}(\mathbf{P})$ et $\mathbf{V}=\mathrm{R_u}(\mathbf{Q})$. Le premier membre de la formule de Mackey correspond au $\mathbf{L}^F$-module-$\mathbf{M}^F$

$$ \mathbb{C}[\mathbf{U}^F\backslash\mathbf{G}^F]\otimes_{\mathbb{C}\mathbf{G}^F}\mathbb{C}[\mathbf{G}^F/\mathbf{V}^F]\simeq\mathbb{C}[\mathbf{U}^F\backslash\mathbf{G}^F/\mathbf{V}^F]. $$

Combinant (i) et (ii) du lemme on a

$$ \mathbf{U}^F\backslash\mathbf{G}^F/\mathbf{V}^F = \coprod_{x\in\mathbf{L}^F\backslash\mathcal{S}(\mathbf{L},\mathbf{M})^F/\mathbf{M}^F} \mathbf{U}^F\backslash\mathbf{P}^F x\mathbf{Q}^F/\mathbf{V}^F. $$

Lemme 11.9. *Pour tout $x \in \mathcal{S}(\mathbf{L},\mathbf{M})^F$ on a un isomorphisme*

$$\mathbf{L}^F/(\mathbf{L}\cap {}^x\mathbf{V})^F \times_{(\mathbf{L}\cap {}^x\mathbf{M})^F} ({}^x\mathbf{M}\cap\mathbf{U})^F\backslash {}^x\mathbf{M}^F \xrightarrow{\sim} \mathbf{U}^F\backslash\mathbf{P}^F x\mathbf{Q}^F/\mathbf{V}^F$$

donné par $(l(\mathbf{L}\cap {}^x\mathbf{V})^F, ({}^x\mathbf{M}\cap\mathbf{U})^F.{}^xm) \mapsto \mathbf{U}^F lxm\mathbf{V}^F$.

Démonstration. On voit facilement que l'application est bien définie. Comme le stabilisateur $\mathbf{U}\cap {}^x\mathbf{V}$ de tout $x \in \mathbf{G}$ sous l'action de $\mathbf{U}\times\mathbf{V}$ est connexe (*c.f.* 3.1 (v)), et que le stabilisateur d'un point de $\mathbf{L}^F/(\mathbf{L}\cap {}^x\mathbf{V})^F \times ({}^x\mathbf{M}\cap\mathbf{U})^F\backslash {}^x\mathbf{M}^F$ sous l'action diagonale de $\mathbf{L}\cap {}^x\mathbf{M}$ est réduit à 1 donc connexe, il suffit de démontrer que $l(\mathbf{L}\cap {}^x\mathbf{V})\times({}^x\mathbf{M}\cap\mathbf{U}).{}^xm \mapsto \mathbf{U}lxm\mathbf{V}$ induit un isomorphisme au niveau des algébriques. Cette application est clairement surjective. Montrons l'injectivité. Si $\mathbf{U}lxm\mathbf{V} = \mathbf{U}l'xm'\mathbf{V}$, alors $lxm = l'uxvm'$ pour certains $u \in \mathbf{U}, v \in \mathbf{V}$. Donc

$$u^{-1}l'^{-1}l = {}^x(vm'm^{-1}) \in \mathbf{P}\cap {}^x\mathbf{Q} = (\mathbf{L}\cap {}^x\mathbf{M}).(\mathbf{L}\cap {}^x\mathbf{V}).({}^x\mathbf{M}\cap\mathbf{U}).(\mathbf{U}\cap {}^x\mathbf{V}).$$

L'unicité de cette décomposition force l'existence de $y \in \mathbf{L}\cap {}^x\mathbf{M}$ tel que $y \in l'^{-1}l(\mathbf{L}\cap {}^x\mathbf{V})$ et $y \in {}^x(m'm^{-1})({}^x\mathbf{M}\cap\mathbf{U})$. Cela donne l'égalité

$$l(\mathbf{L}\cap {}^x\mathbf{V})\times_{\mathbf{L}\cap {}^x\mathbf{M}} ({}^x\mathbf{M}\cap\mathbf{U})^xm = l'(\mathbf{L}\cap {}^x\mathbf{V})\times_{\mathbf{L}\cap {}^x\mathbf{M}} ({}^x\mathbf{M}\cap\mathbf{U})^xm'$$

car elle équivaut à

$$l'^{-1}l(\mathbf{L}\cap {}^x\mathbf{V})\times_{\mathbf{L}\cap {}^x\mathbf{M}} ({}^x\mathbf{M}\cap\mathbf{U}) = (\mathbf{L}\cap {}^x\mathbf{V})\times_{\mathbf{L}\cap {}^x\mathbf{M}} ({}^x\mathbf{M}\cap\mathbf{U})^x(m'm^{-1}),$$

ce qui s'écrit encore $(\mathbf{L}\cap {}^x\mathbf{V})y\times_{\mathbf{L}\cap {}^x\mathbf{M}} ({}^x\mathbf{M}\cap\mathbf{U}) = (\mathbf{L}\cap {}^x\mathbf{V})\times_{\mathbf{L}\cap {}^x\mathbf{M}} y({}^x\mathbf{M}\cap\mathbf{U})$, d'où l'injectivité. □

Par le lemme, on obtient donc un isomorphisme de $\mathbf{L}^F$-modules-$\mathbf{M}^F$

$$\mathbf{U}^F\backslash\mathbf{G}^F/\mathbf{V}^F \simeq \coprod_{x\in\mathbf{L}^F\backslash\mathcal{S}(\mathbf{L},\mathbf{M})^F/\mathbf{M}^F} \mathbf{L}^F/(\mathbf{L}\cap {}^x\mathbf{V})^F \times_{(\mathbf{L}\cap {}^x\mathbf{M})^F} ({}^x\mathbf{M}\cap\mathbf{U})^F\backslash {}^x\mathbf{M}^F,$$

où $\mathbf{L}^F$ agit par multiplication à gauche sur les deux membres et $\mathbf{M}^F$ agit par multiplication à droite dans le premier membre et par le composé de la multiplication à droite et de $\mathrm{ad}\, x$ sur le terme indexé par x dans le second membre. On a donc un isomorphisme de $\mathbf{L}^F$-modules-$\mathbf{M}^F$:

$$\mathbb{C}[\mathbf{U}^F\backslash\mathbf{G}^F/\mathbf{V}^F] \simeq \bigoplus_{x\in\mathbf{L}^F\backslash\mathcal{S}(\mathbf{L},\mathbf{M})^F/\mathbf{M}^F} \mathbb{C}[\mathbf{L}^F/(\mathbf{L}\cap {}^x\mathbf{V})^F]\otimes_{\mathbb{C}[(\mathbf{L}\cap {}^x\mathbf{M})^F]}\mathbb{C}[({}^x\mathbf{M}\cap\mathbf{U})^F\backslash {}^x\mathbf{M}^F],$$

Le membre de droite ci-dessus est exactement celui de la formule de Mackey, d'où le théorème. □

12 Théorie de Harish-Chandra

Nous exposons ici la théorie des représentations "cuspidales", due à Harish-Chandra. Ici $\mathbf{G}$ est toujours un groupe de type de Lie. Commençons par démontrer comme promis :

Proposition 12.1. *Le foncteur $R_{\mathbf{L}\subset\mathbf{P}}^{\mathbf{G}}$ ne dépend pas de $\mathbf{P}$.*

Démonstration. Nous procédons par récurrence sur $\dim \mathbf{G}$. Si $\mathbf{L} = \mathbf{G}$ le résultat est trivial, donc on peut supposer $\dim \mathbf{L} < \dim \mathbf{G}$. La formule de Mackey avec le même sous-groupe de Levi $\mathbf{L}$ et deux sous-groupes paraboliques $\mathbf{P}$ et $\mathbf{Q}$ donne, pour λ une fonction de classe sur $\mathbf{L}^F$:

$$\langle R_{\mathbf{L}\subset\mathbf{P}}^{\mathbf{G}}\lambda, R_{\mathbf{L}\subset\mathbf{Q}}^{\mathbf{G}}\lambda\rangle_{\mathbf{G}^F} = \sum_{x\in\mathbf{L}^F\backslash\mathcal{S}(\mathbf{L},\mathbf{L})^F/\mathbf{L}^F} \langle {}^*R_{\mathbf{L}\cap {}^x\mathbf{L}\subset\mathbf{P}\cap {}^x\mathbf{L}}^{\mathbf{L}}\, {}^x\lambda,\, {}^*R_{\mathbf{L}\cap {}^x\mathbf{L}\subset\mathbf{L}\cap {}^x\mathbf{Q}}^{\mathbf{L}}\lambda\rangle_{\mathbf{L}^F\cap {}^x\mathbf{L}^F}$$

Vu l'hypothèse de récurrence, le membre de droite ne dépend pas des paraboliques $\mathbf{P}$ et $\mathbf{Q}$ qui y apparaissent, donc il en est de même pour le membre de gauche ; en d'autres termes, si on pose $f = R_{\mathbf{L}\subset\mathbf{P}}^{\mathbf{G}}\lambda$, $f' = R_{\mathbf{L}\subset\mathbf{Q}}^{\mathbf{G}}\lambda$, on a : $\langle f, f\rangle_{\mathbf{G}^F} = \langle f, f'\rangle_{\mathbf{G}^F} = \langle f', f'\rangle_{\mathbf{G}^F}$ d'où $\langle f-f', f-f'\rangle_{\mathbf{G}^F} = 0$ et donc $f = f'$. □

La transitivité de $R_{\mathbf{L}}^{\mathbf{G}}$ (*c.f.* 11.6) permet de définir une relation d'ordre partiel sur l'ensemble des couples $(\mathbf{L}, \lambda)$ formés d'un sous-groupe de Levi F-stable d'un sous-groupe parabolique F-stable de $\mathbf{G}$ et de $\lambda \in \mathrm{Irr}(\mathbf{L}^F)$, en posant $(\mathbf{L}', \lambda') \leq (\mathbf{L}, \lambda)$ si $\mathbf{L}' \subset \mathbf{L}$ et $\langle \lambda, R_{\mathbf{L}'}^{\mathbf{L}}\lambda'\rangle_{\mathbf{L}^F} \neq 0$.

Définition-Théorème 12.2. *On dit que la $\lambda \in \mathrm{Irr}(\mathbf{L}^F)$ est* cuspidale *si elle vérifie une des conditions équivalentes :*

(i) Le couple $(\mathbf{L}, \lambda)$ est minimal pour l'ordre décrit ci-dessus.

(ii) Pour tout sous-groupe de Levi F-stable $\mathbf{L}'$ d'un sous-groupe parabolique F-stable de $\mathbf{L}$, on a ${}^*R_{\mathbf{L}'}^{\mathbf{L}}\lambda = 0$.

Démonstration. Le couple $(\mathbf{L}, \lambda)$ est minimal si et seulement si pour tout $\mathbf{L}' \subset \mathbf{L}$ et tout $\lambda' \in \mathrm{Irr}(\mathbf{L}'^F)$, on a $\langle \lambda, R_{\mathbf{L}'}^{\mathbf{L}}\lambda'\rangle_{\mathbf{L}^F} = \langle {}^*R_{\mathbf{L}'}^{\mathbf{L}}\lambda, \lambda'\rangle_{\mathbf{L}'^F} = 0$, ce qui est équivalent à la condition (ii), d'où le résultat. □

Théorème 12.3. *Soit $\gamma \in \mathrm{Irr}(\mathbf{G}^F)$; alors il existe un unique couple minimal $(\mathbf{L}, \lambda)$ tel que $(\mathbf{L}, \lambda) \leq (\mathbf{G}, \gamma)$ à $\mathbf{G}^F$-conjugaison près.*

Démonstration.

Lemme 12.4. *Si $\lambda \in \mathrm{Irr}(\mathbf{L}^F)$, et $\mu \in \mathrm{Irr}(\mathbf{M}^F)$ sont deux représentations cuspidales de sous-groupes de Levi de sous-groupes paraboliques F-stables de $\mathbf{G}$, alors :*

$$\langle R_{\mathbf{L}}^{\mathbf{G}}\lambda, R_{\mathbf{M}}^{\mathbf{G}}\mu\rangle_{\mathbf{G}^F} = \begin{cases} |W_{\mathbf{G}^F}(\mathbf{L}, \lambda)| & \text{si } (\mathbf{L}, \lambda) \text{ et } (\mathbf{M}, \mu) \text{ sont } \mathbf{G}^F\text{-conjugués} \\ 0 & \text{sinon} \end{cases}$$

où on a posé $W_{\mathbf{G}^F}(\mathbf{L}, \lambda) = \{w \in N_{\mathbf{G}^F}(\mathbf{L})/\mathbf{L}^F \mid {}^w\lambda = \lambda\}$.

Démonstration. Par la "formule de Mackey", on a :

$$\begin{aligned}
\langle R_{\mathbf{L}}^{\mathbf{G}}\lambda, R_{\mathbf{M}}^{\mathbf{G}}\mu\rangle_{\mathbf{G}^F} &= \langle \lambda, {}^*R_{\mathbf{L}}^{\mathbf{G}} R_{\mathbf{M}}^{\mathbf{G}}\mu\rangle_{\mathbf{L}^F} \\
&= \langle \lambda, \sum_{x\in\mathbf{L}^F\backslash\mathcal{S}(\mathbf{L},\mathbf{M})^F/\mathbf{M}^F} R_{\mathbf{L}\cap{}^x\mathbf{M}}^{\mathbf{L}}\, {}^*R_{\mathbf{L}\cap{}^x\mathbf{M}}^{{}^x\mathbf{M}}\, {}^x\mu\rangle_{\mathbf{L}^F} \\
&= \langle \lambda, \sum_{\{x\in\mathbf{L}^F\backslash\mathcal{S}(\mathbf{L},\mathbf{M})^F/\mathbf{M}^F \mid {}^x\mathbf{M}\subset\mathbf{L}\}} R_{{}^x\mathbf{M}}^{\mathbf{L}}\, {}^x\mu\rangle_{\mathbf{L}^F} \qquad (i) \\
&= \sum_{\{x\in\mathbf{L}^F\backslash\mathcal{S}(\mathbf{L},\mathbf{M})^F/\mathbf{M}^F \mid {}^x\mathbf{M}=\mathbf{L}\}} \langle \lambda, {}^x\mu\rangle_{\mathbf{L}^F}, \qquad (ii)
\end{aligned}$$

où (i) utilise que μ (donc ${}^x\mu$) est cuspidal et (ii) que λ est cuspidal. □

Le théorème 12.3 est une conséquence immédiate du lemme 12.4, car si $\langle\gamma, R_{\mathbf{L}}^{\mathbf{G}}\lambda\rangle_{\mathbf{G}^F}$, et $\langle\gamma, R_{\mathbf{M}}^{\mathbf{G}}\mu\rangle_{\mathbf{G}^F}$ sont non nuls, alors $\langle R_{\mathbf{L}}^{\mathbf{G}}\lambda, R_{\mathbf{M}}^{\mathbf{G}}\mu\rangle_{\mathbf{G}^F}$ est évidemment non nul. □

Si λ est cuspidale, on a par 12.4 : $\langle R_{\mathbf{L}}^{\mathbf{G}}\lambda, R_{\mathbf{L}}^{\mathbf{G}}\lambda\rangle_{\mathbf{G}^F} = |W_{\mathbf{G}^F}(\mathbf{L},\lambda)|$. En fait, par [Howlett-Lehrer1980] l'algèbre $\mathrm{End}_{\mathbf{G}^F}(R_{\mathbf{L}}^{\mathbf{G}}(\lambda))$ est une algèbre de Hecke associée au groupe $W_{\mathbf{G}^F}(\mathbf{L},\lambda)$ (le résultat initial de [Howlett-Lehrer1980] obtenait une telle algèbre tordue par un cocycle ; [Lusztig1984, 8.6] quand $\mathbf{G}$ est à centre connexe, puis [Geck1993] dans le cas général ont montré que ce cocycle est trivial). Donc les composantes irréductibles de $R_{\mathbf{L}}^{\mathbf{G}}\lambda$ sont paramétrées par $\mathrm{Irr}(W_{\mathbf{G}^F}(\mathbf{L},\lambda))$, et si ρ_χ est la composante associée à $\chi \in \mathrm{Irr}(W_{\mathbf{G}^F}(\mathbf{L},\lambda))$, on a $\langle\rho_\chi, R_{\mathbf{L}}^{\mathbf{G}}\lambda\rangle_{\mathbf{G}^F} = \dim\chi$. La théorie des algèbres de Hecke fournit aussi une formule pour $\dim\rho_\chi$ comme "degré générique" déterminé par l'algèbre de Hecke.

Les résultats qui précèdent donnent une première approche pour classifier $\mathrm{Irr}(\mathbf{G}^F)$, due initialement à Harish-Chandra (qui travaillait dans le cadre des groupes de Lie p-adiques). La classification de $\mathrm{Irr}(\mathbf{G}^F)$ est ramenée à celle des représentations cuspidales ; l'ensemble $\mathcal{E}(\mathbf{L},\lambda) = \{\gamma \in \mathrm{Irr}(\mathbf{G}^F) \mid \langle\gamma, R_{\mathbf{L}}^{\mathbf{G}}(\lambda)\rangle_{\mathbf{G}^F} \neq 0\}$ est appelé la **série de Harish-Chandra** associée à $(\mathbf{L},\lambda)$. On appelle **série de Harish-Chandra** associée à $\mathbf{L}$ l'union des $\mathcal{E}(\mathbf{L},\lambda)$ quand λ parcourt l'ensemble des représentations cuspidales de $\mathbf{L}^F$. Quand $\mathbf{L} = \mathbf{T}$, un tore maximal inclus dans un sous-groupe de Borel F-stable, toutes les représentations de $\mathbf{T}^F$ sont évidemment cuspidales ; la série associée à $\mathbf{T}$ est appelée la série principale. L'ensemble des représentations cuspidales de $\mathbf{G}^F$ coïncident avec la série associée à $\mathbf{G}$, qu'on appelle la série discrète. Ainsi le premier problème de la théorie est l'étude de la série discrète.

Références

[Digne-Michel] François Digne et Jean Michel, "Representations of finite groups of Lie type", *London math. soc. student texts* **21**, Cambridge university press (1991).

[Geck1993] "A note on Harish-Chandra induction" *Manuscripta Math.* **80** (1993) 393–401.

[Geck] Meinolf Geck, "An introduction to algebraic geometry and algebraic groups", Clarendon press (2003).

[Howlett-Lehrer1980] B. Howlett et G. Lehrer, "Induced cuspidal representations and generalized Hecke rings", *Inventiones* **58** (1980) 37–64.

[Luna] Domingo Luna, "Retour sur un théorème de Chevalley", *L'enseignement mathématique* **45** (1999) 317–320.

[Lusztig1984] "Characters of reductive groups over a finite field" *Ann. Math. Studies* **107**, Princeton UP (1984) 384p.

[Serre] Jean-Pierre Serre, "Cohomologie Galoisienne", (1964) 5ième édition Springer (1994).

[Springer] Tonny Springer, "Linear algebraic groups", *Progress in mathematics* **9**, Birkhauser (1998).

[Steinberg68] Robert Steinberg, "Endomorphisms of algebraic groups", *memoirs of AMS* **80**, (1968).

[Steinberg] Robert Steinberg, "The isomorphism and isogeny theorems for reductive algebraic groups", *J. Algebra* **216** (1999), 366–383.

[Szamuely] Tamás Szamuely. "Lectures on linear algebraic groups", disponible sur la page web de `www.renyi.hu/ szamuely/lag.pdf` de l'auteur