1. Groupes de Coxeter.

Soit W un groupe engendré par un ensemble S d'involutions. Tout élément de w est produit d'un nombre fini d'éléments de S, donc est l'image dans W d'un mot du monoïde libre S^* engendré par S. On dit que $s_1 \dots s_k \in S^*$ est une *décomposition réduite* de $w \in W$ si c'est un mot de longueur minimum d'image w, et cette longueur est appelée longueur de w et notée $l(w)$. 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.

1.1. Définition. *On dit que (W, S) comme ci-dessus 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.

Attention! Un système (W, S) ayant une telle présentation n'est 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 (cf. 2.4), mais ce n'est pas évident.

Nous utiliserons la terminologie suivante dans un système de Coxeter: les éléments de S seront appelés les *réflexions élémentaires* de W, les éléments de l'ensemble R des éléments de W conjugués à un élément de S seront appelés les *réflexions* de W.

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

1.2. Théorème. *Soit S un ensemble d'involutions engendrant un 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 $l(ws) \leq l(w)$, alors il existe i tel que $ws = s_1 \dots \hat{s}_i \dots s_k$.

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.

Preuve: 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).

1.3. Lemme. *Soit (W, S) un système de Coxeter. Si $s_1 \dots s_k$ est une décomposition réduite de $w \in W$, l'ensemble $R(s_1 \dots s_k) = \{s_k, s_k s_{k-1} s_k, \dots, s_k s_{k-1} \dots s_2 s_1 s_2 \dots s_k\}$ ne dépend que de w. Nous le noterons $R(w)$; il est formé de $l(w)$ éléments distincts de R.*

PREUVE: Notons d'abord que $R(s_1 \dots s_k)$ est bien formé de $l(w)$ éléments distincts de R. En effet, de $s_k \dots s_i \dots s_k = s_k \dots s_j \dots s_k$ avec $i < j$ on tire $s_i s_{i+1} \dots s_j = s_{i+1} s_{i+2} \dots s_{j-1}$ ce qui contredit le fait que la décomposition $s_1 \dots s_k$ soit réduite.

L'ensemble $\Phi = \{\pm 1\} \times R$ des réflexions munies d'un signe sera appelé l'ensemble des *racines* (abstraites) de W. C'est l'union des *racines positives* $(+1, t)_{t \in R}$ et des *racines négatives* $(-1, t)_{t \in R}$.

Soit $\mathfrak{S}_\Phi$ le groupe des permutations de Φ. Nous allons montrer que l'application $f : S \to \mathfrak{S}_\Phi$ définie par $f(s)(\varepsilon, t) = \begin{cases} (\varepsilon, {}^s t) & \text{si } s \neq t \\ (-\varepsilon, s) & \text{si } s = t \end{cases}$ se prolonge en un homomorphisme $W \hookrightarrow \mathfrak{S}_\Phi$. Il faut vérifier que l'homomorphisme $f : S^* \to \mathfrak{S}_\Phi$ induit par f vérifie $f(s^2) = 1$, ce qui est clair, puis qu'il vérifie $f(\Delta_{s,s'}) = f(\Delta_{s',s})$.

On a la formule: $f(s_1 \dots s_k)(\varepsilon, t) = \begin{cases} (-\varepsilon, {}^w t) & \text{si } t \in R(s_1 \dots s_k), \\ (\varepsilon, {}^w t) & \text{sinon} \end{cases}$; en effet, (ε, t) "change de signe" par $s_1 \dots s_k$ seulement s'il existe un nombre impair de j tels que ${}^{s_j \dots s_k} t = s_{j-1}$, ce qui est équivaut à ce que t apparaisse un nombre impair de fois dans $R(s_1 \dots s_k)$, d'où le résultat puisque $R(s_1 \dots s_k)$ est formé d'éléments distincts.

Il est clair par définition que $R(\Delta_{s,s'}) = R(\Delta_{s',s})$, d'où $f(\Delta_{s,s'}) = f(\Delta_{s',s})$. L'application f induit donc bien un homomorphisme $W \to \mathfrak{S}_\Phi$, et l'ensemble $R(s_1 \dots s_k)$ ne dépend donc que de w. ■

Montrons maintenant (i)⇒(ii). Si $l(ws) \leq l(w)$, alors $l(ws) < l(w)$. En effet la présentation de W montre que $s \mapsto -1$ se prolonge en un caractère de degré 1 de W donné par $w \mapsto (-1)^{l(w)}$, donc $(-1)^{l(ws)} = -(-1)^{l(w)}$. Si $l(ws) < l(w)$, alors on obtient une décomposition réduite de w en faisant suivre par s une décomposition de ws, donc on en déduit que $s \in R(w)$. 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, leurs premières lettres étant 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 est absurde.

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. ■

1.4. Exercice. Montrer que $(\mathfrak{S}_n, \{(i, i+1)\}_{i=1\ldots n-1})$ est un système de Coxeter, et qu'on a $l(w) = |\{i < j \mid w(i) > w(j)\}|$ (on montrera que l'ensemble $R(w)$ est en bijection avec cet ensemble).

Si (W, S) est un système de Coxeter, pour $I \subset S$, on note W_I le sous-groupe de W engendré par I. Nous aurons besoin de la notion suivante:

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

(i) Pour tout $v \in W_I$, on a $l(v) + l(w) = l(vw)$.
(ii) Pour tout $s \in I$, on a $l(s) + l(w) = l(sw)$.
(iii) w est l'unique élément de longueur minimum dans $W_I w$.

Preuve: Commençons par remarquer que si $v, w \in W$ et $l(v) + l(w) < l(vw)$, 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 $vw = \hat{v}\hat{w}$ où on a noté $\hat{v}$ (resp. $\hat{w}$) le produit d'une suite extraite stricte d'une décomposition réduite de v (resp. w). Si dans notre calcul on prend $v \in W_I$, on voit que si w ne vérifie pas (i) (a fortiori s'il ne vérifie pas (ii)), il n'est pas de longueur minimale dans sa classe (puisque $\hat{w}$ dans la même classe est de longueur inférieure). Réciproquement, si w' n'est pas de longueur minimum dans $W_I w'$, i.e. qu'il est de la forme vw avec $l(w) < l(w')$, alors il existe une décomposition réduite de w' de la forme $\hat{v}\hat{w}$ avec $l(\hat{w}) \leq l(w) < l(w')$ donc $l(\hat{v}) > 0$, donc il existe une décomposition réduite de w' commençant par un élément de I, donc w' ne vérifie pas (ii). On a donc vu que les négations de (i),(ii),(iii) sont équivalentes. ■

2. Groupes finis de réflexion.

Soit K un corps commutatif de caractéristique 0 et soit V un K-espace vectoriel de dimension n. Un élément $s \in \mathrm{End}(V)$ est dit une *pseudo-réflexion* si $\mathrm{rang}(\mathrm{Id}_V - s) = 1$. Si s est d'ordre fini nous dirons aussi que s est une réflexion complexe. La "justification" de cette définition est que si nous prenons $K = \mathbb{R}$, une réflexion complexe est une réflexion. Une réflexion complexe est de la forme $s(x) = x - a'(x)a$ où a' est une forme linéaire définissant l'hyperplan $H_s = \mathrm{Ker}(s - \mathrm{Id}_V)$, et a est un vecteur propre associé à la valeur propre $\xi \neq 1$ de s, ces données vérifiant $a'(a) = 1 - \xi$.

On appellera *groupe fini de réflexions complexes* un sous-groupe fini de $\mathrm{GL}(V)$ engendré par des pseudo-réflexions. Un groupe de réflexions complexes W est associé au système d'hyperplans W-invariant $\mathcal{A}_W = \{H_s\}_s$ où s parcourt les pseudo-réflexions de W.

Quand $K = \mathbb{R}$, on obtient la notion de groupe fini de réflexions réel, dont nous allons voir qu'elle coïncide avec celle de groupe de Coxeter fini (attention! il existe des groupes engendrés sur $\mathbb{C}$ par des réflexions qui ne sont pas réalisables sur $\mathbb{R}$).

Quand $K = \mathbb{R}$, on appelle *chambres* de l'arrangement $\mathcal{A} = \mathcal{A}_W$ les composantes connexes de $V - \bigcup_{H \in \mathcal{A}} H$; on appelle murs d'une chambre C les $H \in \mathcal{A}$ tels que $H \cap \overline{C}$ soit un fermé de H d'intérieur non vide.

2.1. Proposition. *Soit W un groupe de réflexion fini dans V espace vectoriel réel de dimension finie. Alors:*

(i) Pour tout $H \in \mathcal{A}$ il existe une unique réflexion que nous noterons s_H d'hyperplan H.

(ii) Soit C une chambre, $\mathcal{M}$ l'ensemble de ses murs, et soit $S = \{s_H \mid H \in \mathcal{M}\}$. Alors (W, S) est un système de Coxeter, et on a $m_{s,s'} = |\{H'' \in \mathcal{A} \mid H'' \supset H \cap H'\}|$.

(iii) Le fixateur dans W de $x \in V$ est engendré par les réflexions qui fixent x.

Preuve: Comme W est fini, on peut munir V d'un produit scalaire invariant par W, et les réflexions sont alors les réflexions orthogonales par rapport à leur hyperplan de réflexion (en effet on a alors $s(x) = x - \langle x, a' \rangle a$ où $\langle a, a' \rangle = 1 - \xi = 2$, et de $\langle s(x), s(a) \rangle = \langle x, a \rangle$ on tire $\langle x, a' \rangle = 2\frac{\langle x,a \rangle}{\langle a,a \rangle}$ i.e. $s(x) = x - 2\frac{\langle x,a \rangle}{\langle a,a \rangle}a$); ceci prouve (i).

Notons W' le sous-groupe de W engendré par S. Montrons d'abord que pour tout $x \in V$, il existe $w \in W'$ tel que $w(x) \in \overline{C}$. Choisissons $a \in C$ et soit y un point de l'orbite de x sous W' a distance minimale de a. Alors on doit nécessairement avoir $y \in \overline{C}$. En effet, si a et y sont de part et d'autre du mur H de C, alors $s_H(y)$ est plus près de a que y.

On en déduit que pour toute chambre C' il existe $w \in W'$ tel que $w(C') = C$. En effet, par ce qui précède on peut trouver w tel que $w(C') \cap \overline{C} \neq \emptyset$, et ceci implique $w(C') = C$. On en déduit aussi que toute réflexion s_H de W est dans W'. En effet, soit C' une chambre dont H est un mur. Soit $w \in W'$ tel que $w(C') = C$. Alors $w(H)$ est un mur de C, donc $ws_Hw^{-1} \in S$. Donc $W' = W$.

Pour démontrer (ii), nous utiliserons le lemme suivant:

2.2. Lemme. *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 $D_s = \{w \in W \mid l(sw) > l(w)\}$.*

Preuve: 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. ■

Nous appliquons le lemme en prenant pour H mur de C l'ensemble D_{s_H} égal à l'ensemble des w tels que $w(C)$ soit du même coté de H que C. La seule chose non triviale à vérifier est que si $w \in D_{s_H}$ et si H' est un mur de C tel que $ws_{H'} \notin D_{s_H}$, alors $ws_{H'} = s_Hw$. Par hypothèse $ws_{H'}(C)$ et $w(C)$ sont de part et d'autre de H, donc $s_{H'}(C)$ et C sont de part et d'autre de $w^{-1}(H)$. Ceci n'est possible que si $H' = w^{-1}(H)$, i.e. $s_{H'} = w^{-1}s_Hw$, d'où le résultat.

La valeur annoncée pour $m_{s_H,s_{H'}}$ se voit en se ramenant au rang 2, spécifiquement en considérant le groupe engendré par les $s_{H''}$ dans l'espace $(H \cap H')^{\perp}$. Ce groupe est un groupe diédral engendré par s_H et $s_{H'}$.

Montrons (iii). Soit C une chambre telle que $x \in \overline{C}$. Nous allons montrer par récurrence sur $l(w)$ que si $w(x) = x$ alors w appartient au sous-groupe de W engendré par les s_H où H est un mur de C contenant x. Si $w \neq 1$, il existe un mur de H de C tel que $l(s_Hw) < l(w)$ (où ici nous mesurons la longueur par rapport au système S des s_H où H est un mur de C). On a $x \in \overline{C} \cap w(\overline{C})$ puisque w fixe x; d'autre part, puisque $w \notin D_{s_H}$ (cf. notations du

lemme), $w(C)$ et C sont de part et d'autre de H, d'où $\overline{w(C)} \cap \overline{C} \subset H$ et d'où $x \in H$, ce qui permet de conclure par récurrence. ■

REMARQUE. La preuve ci-dessus peut s'étendre au cas où V est un espace affine et où W est fini modulo les translations qu'il contient (on obtient un *groupe de Weyl affine*).

2.3. EXERCICE. Montrer que dans la situation de 2.1 il existe un élément $w_0 \in W$ qui est l'unique élément ayant une des deux propriétés suivantes:

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

(ii) $w_0(C) = -C$.

(On utilisera que $-C$ est la seule chambre séparée de C par tous les hyperplans de $\mathcal{M}$).

À un système de Coxeter on associe une *matrice de Coxeter*, matrice symétrique dont le coefficient $m_{s,s'}$ est la longueur de $\Delta_{s,s'}$ quand cet élément existe (et on pose $m_{s,s} = 1$), sinon ∞.

2.4. PROPOSITION. *À toute matrice symétrique $\{m_{s,s'}\}_{s,s' \in S}$ à coefficients entiers ≥ 2 ou $+\infty$ et à coefficients diagonaux 1 on peut associer un groupe de Coxeter W qui admet cette matrice comme matrice de Coxeter, et une représentation fidèle comme groupe de réflexions de W dans un espace vectoriel réel de dimension $|S|$.*

PREUVE: On munit un espace vectoriel réel V de base $\{e_s\}_{s \in S}$ de la forme bilinéaire donnée par $\langle e_s, e_{s'} \rangle = -\cos(\pi/m_{s,s'})$ (où on pose $\pi/m_{s,s'} = 0$ si $m_{s,s'} = \infty$). On a donc $\langle e_s, e_s \rangle = 1$ et $\langle e_s, e_{s'} \rangle = -1$ si $m_{s,s'} = \infty$. On fait agir sur V le groupe W défini par la présentation $\langle s \in S \mid (ss)^{m_{s,s'}} = 1 \rangle$ en faisant agir s par $s(x) = x - 2\langle x, e_s \rangle e_s$. Alors s est une réflexion, qui préserve $\langle\ ,\ \rangle$.

Pour vérifier qu'on a une représentation de W, il faut calculer l'ordre de ss'. Posons $\lambda = \langle e_s, e_{s'} \rangle$. On obtient $ss'(e_s) = (4\lambda^2 - 1)e_s - 2\lambda e_{s'}$ et $ss'(e_{s'}) = 2\lambda e_s - e_{s'}$. Si $\lambda = -1$, on a $ss'(e_s + e_{s'}) = e_s + e_{s'}$, d'où, en itérant la première formule qui s'écrit dans ce cas $ss'(e_s) = 2(e_s + e_{s'}) + e_s$, on obtient $(ss')^m(e_s) = 2m(e_s + e_{s'}) + e_s$ et ss' est d'ordre infini. Sinon, identifions le plan engendré par e_s et $e_{s'}$ au plan complexe en identifiant e_s à 1 et $e_{s'}$ à $-e^{-i\theta}$ où $\theta = \pi/m_{s,s'}$. Alors sur ce plan $\langle\ ,\ \rangle$ s'identifie au produit scalaire usuel et on trouve $ss'(e_s) = (4\cos^2\theta - 1) - 2\cos\theta e^{-i\theta} = e^{2i\theta}$ et $ss'(e_{s'}) = -2\cos\theta + e^{-i\theta} = -e^{i\theta}$, donc ss' agit sur ce plan comme une rotation d'angle $2\pi/m_{s,s'}$. Agissant trivialement sur l'orthogonal du plan pour $\langle\ ,\ \rangle$, ss' est donc d'ordre $m_{s,s'}$.

Nous avons donc déjà vu que W possède une représentation où ss' est d'ordre $m_{s,s'}$, donc toute matrice de Coxeter correspond à un groupe de Coxeter.

En fait la représentation de réflexion que nous venons de construire est injective, et fait donc de W un groupe de réflexion. Pour démontrer cela, nous considérons la représentation de W sur le dual V^* (où $w \in W$ agit comme ${}^t\rho(w^{-1})$, si $\rho(w)$ est l'action de w sur V). Pour $I \subset S$ nous posons $C_I = \{x^* \in V^* \mid x^*(e_s) > 0 \forall s \in I\}$, et on pose $C = C_s$ (le "cône de Tits"). La fidélité de la représentation résulte alors du

2.5 LEMME (TITS). *Si $w \neq 1$, alors $w(C) \cap C = \emptyset$.*

PREUVE: Pour $I \subset S$, soit $\alpha_I(w)$ l'élément de W_I de longueur maximum tel que $l(\alpha_I(w)) + l(\alpha_I(w)^{-1}w) = l(w)$ (cf. 1.5). Nous allons montrer par récurrence sur $l(w)$ que $w(C) \subset$

$\alpha_I(w)C_I$ pour tout $I \subset S, |I| \leq 2$. Le lemme en résultera car si $w \neq 1$, il existe $s \in S$ tel que $\alpha_{\{s\}}(w) = s$, d'où $w(C) \subset sC_s = -C_s \not\supset C$.

Supposons donc l'assertion vraie pour les éléments de longueur inférieure à w, et commençons par la démontrer quand $I = \{s\}$. Si $\alpha_I(w) = s$ alors $w = sw'$ où $l(w') < l(w)$ et $\alpha_I(w') = 1$ d'où $w(C) = sw'(C) \subset sC_s$ q.e.d. Si $\alpha_I(w) = 1$ choisissons s' tel que $\alpha_{\{s'\}}(w) = s'$ et écrivons $w = \alpha_{\{s,s'\}}(w)w'$. Puisque $l(w') < l(w)$ on a par récurrence $w(C) = \alpha_{\{s,s'\}}(w)w'(C) \subset \alpha_{\{s,s'\}}(w)(C_{s,s'})$. On est donc ramené exactement à la même question pour le groupe diédral $W_{s,s'}$ où on fait un dessin: si $m_{s,s'} < \infty$ alors $\langle\, , \,\rangle$ est définie positive donc on peut identifier V à V^* au moyen de cette forme pour faire le dessin. Si $m_{s,s'} = \infty$, soit $\{e_s^*\}_{s\in S}$ la base duale de $\{e_s\}_{s\in S}$; en utilisant la définition $(se_s^*)(x) = e_s^*(sx)$ et $\langle\, x, e_s \,\rangle = e_s^*(x) - e_{s'}^*(x)$, on trouve pour l'action contragrédiente que s agit par $\begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix}$ et s' par $\begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix}$. Les éléments s et s' préservent les droites $x + y =$constante...

Enfin montrons l'assertion pour $I = \{s, s'\}$. Si $\alpha_{\{s,s'\}}(w) = 1$ alors $\alpha_{\{s\}}(w) = \alpha_{\{s'\}}(w) = 1$ et $w(C) \subset C_s \cap C_{s'} = C_{s,s'}$ q.e.d. Sinon $w = \alpha_{\{s,s'\}}(w)w'$ où $w'(C_{s,s'}) = C_{s,s'}$ d'où le résultat. ■

Remarquons que W a une image finie si et seulement si la forme bilinéaire que nous avons défini est définie positive. En effet, si l'image est finie, la représentation étant irréductible, tout produit scalaire invariant est proportionnel à $\langle\, , \,\rangle$. Réciproquement, si la forme est définie positive son groupe orthogonal est compact et un sous-groupe discret d'un groupe compact est fini (W est discret car si $x \in C$ et $w \in W$, l'ensemble $\{g \in \mathrm{GL}(V^*) \mid gw(x) \in w(C)\}$ est un voisinage ouvert de w qui ne rencontre pas ses translatés par W). ■

3. Groupes de réflexions complexes et invariants.

Nous aurons deux motivations pour nous intéresser aux groupes de réflexions complexes: d'une part, la classe des groupes de Coxeter n'est pas stable sous certaines opérations (la prise du centralisateur d'un élément régulier) — d'autre part ils interviennent naturellement lors de l'étude des *invariants polynômiaux* des groupes finis. Les groupes de réflexions complexes irréductibles ont été classifiés par Shephard et Todd, en une famille infinie a 3 paramètres (qui contient les 4 familles infinies de groupes de Coxeter), et 34 groupes "sporadiques".

Soit V un espace vectoriel sur un corps K, et soit G un sous-groupe de $\mathrm{GL}(V)$. On appelle invariants polynômiaux les invariants S^G de G dans l'algèbre symétrique S de V (la partie symétrique de l'algèbre tensorielle). Pour tout choix d'une base $x_1, \ldots, x_n$ de V, l'algèbre S s'identifie à l'algèbre de polynômes $K[x_1, \ldots, x_n]$.

Le premier résultat important est le

3.1. Théorème de Hilbert-Noether. *S^G est une algèbre de type fini sur K.*

Preuve: Notons d'abord que S est un S^G-module de rang fini car tout élément $p \in S$ (en particulier les générateurs de S sur K) est entier sur S^G, car il est racine du polynôme unitaire $\prod_{g\in G}(X - gp)$. Le théorème résultera donc de la

3.2. Proposition. *Soit S une K-algèbre de type fini et soit R une sous-algèbre telle que S soit un R-module de rang fini. Alors R est une K-algèbre de type fini.*

Preuve: S étant de rang fini sur R, les éléments de S sont finis sur R. Notons $P(s)$ le polynôme à coefficients dans R qui exprime l'intégralité de $s \in S$ sur R, et soit S' la sous-algèbre de S engendrée par les coefficients des $P(s)$ quand p décrit un ensemble de générateurs de S sur K. Les générateurs de S étant entiers sur S' par construction, S est déjà de rang fini sur S', et S' est une algèbre de type fini sur K.

L'idée essentielle pour en déduire l'engendrement fini de S^G est une définition: un module M sur un anneau commutatif A est dit *Noetherien* si toute chaîne croissante de sous-modules est stationnaire. A lui-même est dit Noetherien s'il l'est comme A-module. Il est clair que tout quotient ou sous-module d'un module Noetherien l'est, ainsi que tout somme directe de modules Noetheriens. Un module M de rang fini sur un anneau Noetherien A est Noetherien comme quotient d'une somme de copies de A; réciproquement, si M est un module Noetherien sur A il est de rang fini, sinon on pourrait construire à partir d'un ensemble de générateurs une suite non-stationnaire de sous-modules.

3.3. Théorème de la base de Hilbert. *Si A est Noetherien, $A[x]$ l'est aussi.*

Preuve: On remarque d'abord qu'un anneau A est Noetherien si et seulement si tout idéal est de type fini. En effet, si A est Noetherien un idéal=sous-module est de rang fini. Réciproquement, l'union d'une chaîne croissante d'idéaux est un idéal, donc est engendrée par un nombre fini d'éléments. Ces éléments sont tous dans un certain idéal de la chaîne, donc la chaîne stationne après un certain point.

Il suffit donc de voir que tout idéal I de $A[x]$ est de type fini. Soit I' l'idéal de A formé des coefficients de plus haut degré des éléments de I. Alors I' est de type fini comme idéal de A, engendré par disons $a_1, \ldots, a_n$; soient $f_1, \ldots, f_n$ des éléments de I de coefficients de plus haut degré $a_1, \ldots, a_n$, et soit $t = \max(\deg f_i)$ et I'' le sous-idéal de I engendré par les f_i. Alors pour tout $a \in I'$, l'idéal I'' contient un polynôme de terme directeur ax^t, donc tout élément de I est congru modulo I'' à un polynôme de degré plus petit que t. Le A-module M des polynômes de degré plus petit que t est isomorphe à $A \oplus \ldots \oplus A$ (t fois) donc est Noetherien, donc $I \cap M$ est de rang fini et $I = (I \cap M) \oplus I''$ est de type fini. ■

Il en résulte que toute A-algèbre de type fini est Noetherienne.

Dans notre cas, S' est Noetherien étant de type fini sur K. Le S'-module S est de rang fini sur S', donc Noetherien. Son S'-sous-module R est donc Noetherien, donc aussi de rang fini sur S', donc de type fini sur K. ■

■

L'action de G étant degré par degré, on peut trouver un ensemble de générateurs homogènes $f_1, \ldots, f_r$ de S^G. S étant de rang fini sur S^G, le degré de transcendance de S^G doit être le même que celui de S, à savoir n. On peut donc trouver n générateurs algébriquement indépendants parmi les f_i, i.e., quitte à renuméroter les f_i on peut supposer que $K[f_1, \ldots, f_n]$ est une algèbre de polynômes. Nous noterons d_i le degré de f_i, et nous supposerons de plus que les f_i on été choisis tels que le produit $d_1 \ldots d_n$ soit minimal. On peut montrer (avec beaucoup d'algèbre commutative) que dans cette situation S^G est un module libre sur $K[f_1, \ldots, f_n]$ mais nous ne l'utiliserons pas.

3.4. Théorème (Shephard et Todd + Springer). *Supposons K de caractéristique 0. On a toujours $|G| \leq d_1 \dots d_n$, et on a équivalence entre:*
(i) $|G| = d_1 \dots d_n$.
(ii) *G est engendré par des pseudo-réflexions d'ordre fini.*
(iii) $S^G = K[f_1, \dots, f_n]$.

Et, si ces conditions sont vérifiées et que nous notons I l'idéal gradué de S engendré par les éléments de S^G de degré strictement positif, la représentation de G sur S/I est une version graduée de la représentation régulière de G et on a un isomorphisme de KG-modules $S \simeq (S/I) \otimes_K S^G$.

Preuve: Nous commençons par (ii) $\Rightarrow$ (iii). Shephard et Todd ont démontré cette propriété cas par cas. Nous suivons une preuve générale due à Chevalley. Nous commençons par démontrer que S est libre sur S^G, et plus précisément que toute K-base homogène de l'algèbre graduée S/I se relève en une S^G-base de S (ce qui impliquera entre autres que cette base est de cardinal fini par 3.1). Soit $\{z_\alpha\}_\alpha$ une famille d'éléments homogènes de S d'image une K-base de S/I. Montrons d'abord que z_α engendre S comme S^G-module, i.e. que si l'on pose $M = \oplus_\alpha S^G z_\alpha$, alors $M = S$. Sinon, soit f un élément homogène de degré minimum de S qui n'est pas dans M. Choisissant une écriture homogène de $f \in I + \oplus_\alpha K z_\alpha$, on voit qu'il il existe $g \in I$ homogène de même degré que f, i.e. $g = \sum_i x_i f_i$ où les x_i sont des invariants de degré strictement positif. Donc $\deg f_i < \deg f$, d'où $f_i \in M$, d'où $g \in M$, une contradiction.

Nous allons maintenant montrer que les z_α sont indépendants sur S^G. Nous introduisons d'abord un opérateur S^G-linéaire Δ_s sur S, attaché à une pseudo-réflexion s qui baisse de 1 le degré des éléments. On a $sv - v = -a'(v)a$ pour $v \in V$, et comme V engendre S on en déduit que s opère trivialement sur S/Sa; donc pour tout $x \in S$, il existe $\Delta_s(x)$ tel que $sx - x = \Delta_s(x)a$. On vérifie facilement la formule $\Delta_s(xy) = x\Delta_s(y) + y\Delta_s(x) + a\Delta_s(x)\Delta_s(y)$. Comme on a clairement $\Delta_s(x) = 0$ si $x \in S^G$, on en déduit que Δ_s est S^G-linéaire. Notons le

3.5. Lemme. *Si $x \in S$ est homogène, de degré positif et que pour toute pseudo-réflexion s on a $\Delta_s(x) \in I$, alors $x \in I$.*

Preuve: En effet, si $\Delta_s(x) \in I$ alors $x \equiv sx \pmod I$, d'où, puisque G est engendré par ses pseudo-réflexions, $x \equiv gx \pmod I$ pour tout $g \in G$, d'où enfin $x \equiv p_G(x) \pmod I$ où p_G est le projecteur $p_G : S \to S^G$ donné par $x \mapsto |G|^{-1} \sum_{g \in G} g(x)$. Mais comme x est de degré positif on a $p_G(x) \in I$, d'où $x \in I$. ■

Nous montrons maintenant que tout ensemble d'éléments homogènes de S qui sont K-linéairement indépendants mod. I sont S^G-linéairement indépendants. Sinon, soit $x_1 z_1 + \dots + x_m z_m = 0$ une relation de dépendance linéaire minimale à coefficients $x_i \in S^G$ entre éléments $z_1, \dots, z_m$ qui sont K-linéairement indépendants modulo I. On peut supposer z_1 de degré minimal parmi les z_i. Puisque $z_1 \notin I$, par 3.5 il existe une suite $s_1, \dots, s_k$ telle que $\Delta_{s_1} \dots \Delta_{s_k} z_1$ soit un élément non nul de K (car puisque $z_1 \notin I$, si $z_1 \notin K$ il existe s_1 tel que $\Delta_{s_1}(z_1) \notin I$, etc...). Comme les Δ_s sont S^G-linéaires, on a $x_1 \Delta_{s_1} \dots \Delta_{s_k} z_1 + \dots + x_m \Delta_{s_1} \dots \Delta_{s_k} z_m = 0$. En posant $y_i = -p_G(\frac{\Delta_{s_1} \dots \Delta_{s_k} z_i}{\Delta_{s_1} \dots \Delta_{s_k} z_1}) \in S^G$, on a $x_1 = x_2 y_2 + \dots + x_m y_m$, d'où $x_2(z_2 + z_1 y_2) + \dots + x_m(z_m + z_1 y_m) = 0$, d'où une contradiction car c'est une relation

de dépendance linéaire entre $m-1$ éléments $z_i+z_1y_i$ qui sont K-linéairement indépendants modulo I.

On conclut maintenant (ii)⇒(iii) par la

PROPOSITION. *Soit S une K-algèbre graduée de polynômes, et soit R une sous-algèbre graduée telle que le R-module S admette une base finie formée d'éléments homogènes. Alors R est une K-algèbre de polynômes.*

PREUVE: Commençons par remarquer qu'on est sous les hypothèses de 3.2, donc R est Noetherien. L'idéal R^+ de R engendré par les éléments homogènes de degré positif est donc engendré par un nombre fini d'éléments, qu'on peut supposer homogènes. Soit $\alpha_1,\dots,\alpha_s$ un ensemble de générateurs homogènes en nombre minimal. Nous allons prouver que $R=K[\alpha_1,\dots,\alpha_s]$.

Montrons maintenant que les α_i engendrent bien R. Nous raisonnons par récurrence sur le degré. Soit $x=\sum_i r_i\alpha_i$ une écriture homogène d'un élément homogène de R^+. Alors les r_i sont dans R et de degré inférieur à x, donc par récurrence ils sont engendrés par les α_i, d'où le résultat. Montrons maintenant par l'absurde que les α_i sont algébriquement indépendants. Soit $H(X_1,\dots,X_s)$ une relation (qu'on peut supposer homogène) de dépendance algébrique de degré minimal (où l'algèbre de polynômes $K[X_1,\dots,X_s]$ a été munie du degré $\deg X_i=\deg\alpha_i$, ce dernier étant lui-même mesuré dans $S=K[x_1,\dots,x_r]$ où nous n'avons pas nécessairement supposé les x_i de degré 1). Soit J l'idéal de R engendré par les $\beta_1:=\frac{\partial H}{\partial X_i}(\alpha_1,\dots,\alpha_s)$, et soit I une partie minimale de $\{1,\dots,s\}$ telle que J soit engendré par les $\{\beta_i\}_{i\in I}$; soient donc γ_{ij} des éléments de R tels que pour $j\notin I$ on aie $\beta_j=\sum_{i\in I}\gamma_{ji}\beta_i$. Pour tout k on a:

$$\sum_{i=1}^{s}\beta_i\frac{\partial\alpha_i}{\partial x_k}=\frac{\partial}{\partial x_k}H(\alpha_1,\dots,\alpha_s)=0.$$

En remplaçant par leur valeur les $\beta_j(j\notin I)$, on obtient

$$\sum_{i\in I}\beta_i\Big(\frac{\partial\alpha_i}{\partial x_k}+\sum_{j\notin I}\gamma_{ji}\frac{\partial\alpha_j}{\partial x_k}\Big)=0 \qquad (k)$$

Notons u_{ik} le facteur de β_i dans (k). Nous allons montrer maintenant que $u_{ik}\in R^+S$. Soit $\{z_\lambda\}_{\lambda\in\Lambda}$ une base de S sur R et écrivons les u_{ik} sur cette base: $u_{ik}=\sum_{\lambda\in\Lambda}\epsilon_{ik,\lambda}z_\lambda$. À cause de l'indépendance linéaire des z_λ, (k) entraîne que pour tout λ on a $\sum_{i\in I}\beta_i\epsilon_{ik,\lambda}=0$. Si l'un des $\epsilon_{ik,\lambda}\notin R^+$, alors, prenant les termes homogènes de degré $\deg\beta_i$ d'une telle relation, on trouve une écriture d'un $\beta_i(i\in I)$ comme combinaison R-linéaire des autres $\beta_{i'}(i'\in I)$, ce qui est absurde, d'où le résultat sur les u_{ik}.

En utilisant que l'on a $\alpha_i=\sum_k\frac{\deg x_k}{\deg\alpha_i}x_k\frac{\partial\alpha_i}{\partial x_k}$, on trouve $\alpha_i+\sum_{j\notin I}\frac{\deg\alpha_j}{\deg\alpha_i}\gamma_{ji}\alpha_j=\sum_k\frac{\deg x_k}{\deg\alpha_i}x_ku_{ik}\in R^+S^+$; en d'autres termes on a $\alpha_i+\sum_{j\notin I}\frac{\deg\alpha_j}{\deg\alpha_i}\gamma_{ji}\alpha_j=\sum_k y_k\alpha_k$ où les $y_k\in S$ sont homogènes de degré positif. En prenant la composante homogène de degré $\deg\alpha_i$ de cette égalité, on voit que α_i est combinaison S-linéaire des autres α_j. Mais S étant R-libre, cela implique que α_i est combinaison R-linéaire des autres (écrire par exemple les y_k sur z_λ pour le voir), une absurdité . ■

Montrons maintenant le fait que sous l'hypothèse (ii) ou (iii) la représentation de G sur S/I est une version graduée de la représentation régulière de G. Par le théorème de Mashke, I admet un supplémentaire G-stable R dans S. Toute K-base de R est, on l'a vu, une S^G-base de S (i.e. $S = R \otimes_K S^G$), donc une base de $\mathrm{Frac}(S)$ sur $\mathrm{Frac}(S^G)$. Or $\mathrm{Frac}(S^G) = \mathrm{Frac}(S)^G$ (si $x/y \in \mathrm{Frac}(S)^G$ on obtient un élément de $\mathrm{Frac}(S^G)$ en multipliant numérateur et dénominateur par les G-transformés de y). Mais $\mathrm{Frac}(S)/\mathrm{Frac}(S)^G$ est une extension Galoisienne de groupe G, donc G agit par la représentation régulière sur R.

Pour démontrer le reste du théorème, ici encore l'idée essentielle est une définition: soit M un K-espace vectoriel gradué par $\mathbb{N}$ (tel que chaque M_i soit de dimension finie). On appelle *série de Poincaré* de M la série formelle en t donnée par $P_M = \sum_{n=0}^{\infty} \dim M_i t^i$. On vérifie facilement qu'on a $P_{M\oplus M'} = P_M + P_{M'}$, et $P_{M\otimes M'} = P_M \times P_{M'}$ (si on gradue $M\otimes M'$ par le degré total). On a $P_{K[f_1,\dots,f_n]} = \prod_{i=1}^{i=n}(1-t^{d_i})^{-1}$. En effet, on a $K[f_1,\dots,f_n] \simeq K[f_1]\otimes\dots\otimes K[f_n]$ et $P_{K[f_i]} = \sum_{j=0}^{\infty} t^{jd_i} = (1-t^{d_i})^{-1}$. De même on a $P_S = (1-t)^{-n}$.

3.6. Lemme (Molien). *On a* $P_{S^G} = |G|^{-1}\sum_{g\in G}\det(1-gt \mid V)^{-1}$.

Preuve: On peut généraliser la notion de série de Poincaré: si $g \in \mathrm{End}(M)$ agit degré par degré, on définit sa *trace graduée* $P_M(g) = \sum_{i=0}^{\infty}\mathrm{Trace}(g \mid M_i)t^i$; on a $P_M(\mathrm{Id}) = P_M$. Pour calculer la trace graduée de $g\in G$ sur S, choisissons une base de V formée de vecteurs propres $x_1,\dots,x_n$ de g et soient $\lambda_1,\dots,\lambda_n$ les valeurs propres associées. On a clairement $P_S(g) = \prod_i P_{K[x_i]}(g)$ et $P_{K[x_i]}(g) = \sum_{j=0}^{\infty}(\lambda_i t)^j = (1-\lambda_i t)^{-1}$ donc $P_S(g) = \det(1-gt \mid V)^{-1}$. Maintenant, p_G est un projecteur sur S^G, donc $P_S(p_G) = P_{S^G}$, d'où le lemme. ■

Sur la formule 3.6, on voit que la série P_{S^G} converge pour t réel tel que $0 \le t < 1$, et que P_{S^G} a un développement en série de Laurent au voisinage de 1 qui commence par $\frac{1}{|G|(1-t)^n} + \frac{N}{2|G|(1-t)^{n-1}} + \dots$ où N est le nombre de réflexions complexes de G. En effet, seul l'identité contribue au terme en $(1-t)^{-n}$, et seules les réflexions complexes de G contribuent au terme en $(1-t)^{1-n}$; de plus pour chaque réflexion complexe de valeur propre λ non réelle on a $\frac{1}{1-\lambda} + \frac{1}{1-\lambda^{-1}} = 1$, et pour $\lambda = -1$ on a $\frac{1}{1-(-1)} = 1/2$, d'où le facteur $\frac{1}{2}$.

D'autre part, le développement en série de Laurent de $P_{K[f_1,\dots,f_n]}$ au voisinage de 1 est $\frac{1}{(1-t)^n d_1\dots d_n} + \frac{\sum_{i=1}^{i=n}(d_i-1)}{(1-t)^{n-1}2d_1\dots d_n} + \dots$ (pour trouver le second terme, on multiplie par $(1-t)^n$, on dérive et on fait $t=1$). Comme $K[f_1,\dots,f_n] \subset S^G$, les coefficients de la série $P_{K[f_1,\dots,f_n]}$ sont inférieurs ou égaux à ceux de la série P_{S^G}, donc pour $0 \le t < 1$ on a $P_{K[f_1,\dots,f_n]}(t) \le P_{S^G}$. En particulier, le premier coefficient du développement de Laurent de la première série en 1 doit être inférieur au premier coefficient de Laurent de la deuxième série, i.e. $|G| \le d_1\dots d_n$.

Si $|G| = d_1\dots d_n$ on peut comparer de même le deuxième coefficient des développements de Laurent et on obtient $N \ge \sum_{i=1}^{i=n}(d_i-1)$.

Soit H le sous-groupe engendré par les réflexions complexes de G. Alors, par $(ii) \Rightarrow (iii)$ il existe $h_1,\dots,h_n$ algébriquement indépendants tels que $S^H = K[h_1,\dots,h_n]$. Soient $l_1,\dots l_n$ les degrés des h_i et supposons qu'on ait choisi l'ordre des f_i et des h_i tel que $d_1 \le \dots \le d_n$ et $l_1 \le \dots \le l_n$. Puisque $K[f_1,\dots,f_n] \subset S^G \subset S^H$ il existe des polynômes $p_1,\dots,p_n$ tels que $f_i = p_i(h_1,\dots,h_n)$. On a $\deg f_i \ge \deg h_i$, sinon $f_1,\dots,f_i$ ne feraient intervenir que $h_1,\dots,h_{i-1}$ ce qui est absurde puisqu'ils sont algébriquement indépendants.

On a donc $d_i \geq l_i$. Notons que puisque toute réflexion complexe de G est dans H on a $N = \sum_{i=1}^{i=n}(l_i - 1)$.

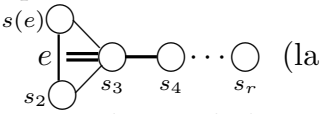
Nous pouvons maintenant conclure. Si $|G| = d_1 \dots d_n$, alors $\sum_{i=1}^{i=n}(l_i - 1) = N \geq \sum_{i=1}^{i=n}(d_i - 1)$, ce qui impose $d_i = l_i$ puisque $d_i \geq l_i$. Dans l'inégalité $\dim(K[f_1, \dots, f_n])_i \leq \dim(S^G)_i \leq \dim(K[h_1, \dots, h_n])_i$ les termes extrêmes coïncident donc les trois modules $K[f_1, \dots, f_n]$, S^G et $K[h_1, \dots, h_n]$ sont égaux.

Réciproquement, si S^G est une algèbre de polynômes $K[s_1, \dots, s_n]$ où les degrés des s_i sont $m_1, \dots, m_n$ ordonnés de façon croissante, le raisonnement ci-dessus (appliqué avec f_i et s_i au lieu de f_i et h_i) montre que $d_i \geq m_i$. Vu le choix de la minimalité de $d_1 \dots d_n$ on doit avoir $d_i = m_i$, et ayant même série de Poincaré les modules $K[f_1, \dots, f_n]$ et $K[s_1, \dots, s_n]$ doivent être tous deux égaux (à S^G); et $|G| = d_1 \dots d_n$. ∎

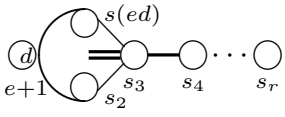
On appelle *degré fantôme* la multiplicité graduée d'un caractère irréductible de G dans S/I. On a $P_{S/I} = P_S/P_{S^G}$ et le degré fantôme de χ est donné par $P_S(p_\chi)/P_{S^G}$ où p_χ est donné par $|G|^{-1}\sum_{g\in G}\chi(g)g$ ($\chi(1)p_\chi$ est le projecteur sur la partie $\overline{\chi}$-isotypique).

3.7 Exemple. La famille (triplement) infinie de groupes engendrés par des pseudo-réflexions est $G(de, e, r) \subset \mathrm{Gl}_r(\mathbb{Q}(\zeta_{de}))$ défini comme l'ensemble des matrices monômiales à coefficients dans μ_{de} et dont le produit des coefficients est dans μ_d. Si D est le sous-groupe des matrices diagonales de $G(de, e, r)$ alors il est clair que $|D| = (de)^r/e$ et $G(de, e, r) = D \rtimes \mathfrak{S}_r$.

Appelons s_i la matrice de la permutation $(i-1, i)$, $s(e)$ la matrice $\begin{pmatrix} 0 & \zeta_e & 0 \\ \zeta_e^{-1} & 0 & 0 \\ 0 & 0 & \mathrm{Id} \end{pmatrix}$, et $t(d)$ la matrice $\mathrm{diag}(\zeta_d, 1, \dots, 1)$. Toutes ces matrices sont des réflexions sauf la dernière qui n'est qu'une pseudo-réflexion quand $d > 2$. On vérifie aisément que:

- $G(e, e, r)$ est engendré par $s(e), s_2, \dots, s_r$ avec présentation 

(la double barre signifie relation de tresse double entre $s(e)s_2$ et s_3; quand $e = 2$ la barre verticale et la double barre horizontale sautent et on retrouve D_r; quand $r = 2$ on trouve le groupe de Coxeter $I_2(e)$).
- $G(d, 1, r)$ est engendré par $t, s_2, \dots, s_r$ avec présentation: 

. Quand $d = 2$ on retrouve B_r. Il faut aussi mentionner le cas particulier dégénéré $G(1, 1, r) = \mathfrak{S}_r$ qui est engendré par $r - 1$ réflexions $s_2, \dots, s_r$ mais qui est en fait un groupe de réflexions de dimension $r - 1$.
- Les cas ci-dessus sont les seuls cas où $G(de, e, r)$ est engendré par r réflexions dans les autres cas il en faut $r + 1$ (de même, 8 des 34 groupes sporadiques nécessitent $r + 1$ réflexions (r pour les autres)). $G(de, e, r)$ est engendré par $t(d), s(ed), s_2, \dots, s_r$ avec présentation 

, ce qui signifie que $\underbrace{s_2t(d)s(ed)s_2s(ed)s_2\dots}_{e+1 \text{ termes}} = \underbrace{t(d)s(ed)s_2s(ed)s_2\dots}_{e+1 \text{ termes}}$, que $t(d)$ commute à $s(ed)s_2$ et à s_3, et mêmes relations que

$G(e,e,r)$.

Si nous choisissons une base $v_1,\dots,v_r$ de V, des générateurs algébriquement indépendants de l'anneau des invariants de $G(ed,e,r)$ sont: $f_k=\sum_{j_1<\dots<j_k} v_{j_1}^{de}\dots v_{j_k}^{de}$ pour $k=1,\dots,r-1$ et $f_r=(v_1\dots v_r)^d$. En effet: il est clair que ce sont des invariants, ils sont algébriquement indépendants car $v_1,\dots,v_r$ sont algébriques sur $f_1,\dots,f_r$ (les v_i^{de} sont zéros de $x^r-f_1x^{r-1}+\dots+(-1)^{r-1}f_{r-1}x+(-1)^rf_r^e$) et le produit de leurs degrés: $de,2de,\dots,(r-1)(de),rd$ est l'ordre de $G(de,e,r)$.

3.8.Exercice. Soit G le groupe d'ordre 2 plongé dans $\mathrm{GL}_2(K)$ en envoyant son élément non trivial sur $\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$. Montrer que la série de Poincaré de ses invariants est $P_{S^G}=\sum_{i=0}^{\infty}(2i+1)t^{2i}$. En déduire que, dans la base de K^2 donnée par $x=(1,0)$, $y=(0,1)$, l'algèbre S^G est engendrée par x^2, xy et y^2. Montrer que $S^G\simeq K[\alpha.\beta,\gamma]/(\alpha\gamma-\beta^2)$ (où dans l'isomorphisme $\alpha=x^2$, $\beta=xy$ et $\gamma=y^2$).

4. Rappels sur les groupes algébriques.

Soit k un corps algébriquement clos. Nous noterons $\mathbb{G}_a$ (resp $\mathbb{G}_m$) le groupe additif k^+ (resp. le groupe multiplicatif $k^\times$) vu comme groupe algébrique.

Soit $\mathbf{G}$ un groupe algébrique connexe sur k. Tous les *sous-groupes de Borel* (= sous-groupe fermés connexes résolubles maximaux) sont conjugués. Un *tore* de $\mathbf{G}$ est un sous-groupe isomorphe à $\mathbb{G}_m^r$. Le r maximal est le *rang* de $\mathbf{G}$. Tous les tores maximaux sont conjugués. Le *radical unipotent* $R_u(\mathbf{G})$ est le plus grand sous-groupe normal fermé unipotent. $\mathbf{G}$ est *réductif* si $R_u(\mathbf{G})=1$.

Étant donné un espace vectoriel réel V, nous appelons système de racines des données $\Phi\subset V,\check{\Phi}\subset V^*$ en bijection $\alpha\mapsto\check{\alpha}$, telles que Φ est fini, engendre V, et vérifiant $\check{\alpha}(\Phi)\in\mathbb{Z}$, $\check{\alpha}(\alpha)=2$ et Φ est stable par la réflexion $s_\alpha\in\mathrm{GL}(V)$ définie par $x\mapsto x-\check{\alpha}(x)\alpha$. Le système est *réduit* si une droite de V contient au plus 2 racines.

Étant donné un ordre sur V tel que toute racine soit positive ou négative, on note Φ^+ (resp Φ^-) les racines positives (resp. négatives) et base Π associée à l'ordre les racines positives indécomposables comme somme de 2 racines positives (alors toute racine est combinaison entièrement positive ou entièrement négative des éléments de Π).

4.1 Rappel. *Soit $\mathbf{G}$ un groupe algébrique réductif connexe sur k, et soit $\mathbf{T}$ un tore maximal de $\mathbf{G}$. Alors*

(i) Les sous-groupes unipotents fermés normalisés par $\mathbf{T}$ minimaux de $\mathbf{G}$ sont isomorphes à $\mathbb{G}_a$, l'action de conjugaison par $t\in\mathbf{T}$ devenant par cet isomorphisme la multiplication par $\alpha(t)$ pour un certain $\alpha\in X(\mathbf{T}):=\mathrm{Hom}(\mathbf{T},\mathbb{G}_m)$. Les α obtenus sont distincts, ce qui permet d'appeler $\mathbf{U}_\alpha$ un tel groupe unipotent minimal. Tout sous-groupe fermé connexe $\mathbf{H}$ de $\mathbf{G}$ normalisé par $\mathbf{T}$ est engendré par $(\mathbf{T}\cap\mathbf{H})^0$ et les $\mathbf{U}_\alpha$ qu'il contient (si $\mathbf{H}$ est unipotent, sa connexité est automatique et on a $\mathbf{H}=\prod_{\mathbf{U}_\alpha\in\mathbf{H}}\mathbf{U}_\alpha$ dans n'importe quel ordre).

(ii) Les α obtenus dans (i) forment un système de racines réduit Φ dans $X(\mathbf{T})\otimes\mathbb{R}$. On a $C_{\mathbf{G}}(\mathbf{T})=\mathbf{T}=N_{\mathbf{G}}(\mathbf{T})^0$ 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 Weyl de Φ (ceci définit la réflexion $s_\alpha\in W$ pour $\alpha\in\Phi$, et on a donc ${}^{s_\alpha}\mathbf{U}_\beta=\mathbf{U}_{s_\alpha(\beta)}$).

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

(iv) *Il y a bijection entre les sous-groupes de Borel contenant* $\mathbf{T}$*, les ordres sur* Φ*, et les systèmes de Coxeter pour* W *(avec* $S = \{s_\alpha\}_{\alpha\in\Pi}$*). Si* $\mathbf{B}$ *correspond à l'ordre* Φ^+*, alors* $R_u(\mathbf{B}) = \prod_{\alpha\in\Phi^+} \mathbf{U}_\alpha$ *(produit des variétés dans n'importe quel ordre sur* Φ^+*) et* $\mathbf{B} = R_u(\mathbf{B}) \rtimes \mathbf{T}$.

(v) *Pour tout* $\alpha \in \Phi$*, il existe un homomorphisme* $\phi : \mathrm{SL}_2 \to \mathbf{G}$ *d'image* $\langle \mathbf{U}_\alpha, \mathbf{U}_{-\alpha}\rangle$ *et de noyau* 1 *ou* $Z(\mathrm{SL}_2)$*, tel que*

$$\phi\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} = \mathbf{U}_\alpha, \quad \phi\begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix} = \mathbf{U}_{-\alpha},$$
$$\phi\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} = \check{\alpha}(k), \quad \phi\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \text{ un représentant de } s_\alpha.$$

5. (B, N)-paires.

5.1. Définition. *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 (5.5(iv)) que S est défini par (B, N).

5.2. Exemple. $\mathrm{GL}_n(k)$ pour k un corps; N=matrices monômiales, T= matrices diagonales, B=matrices triangulaires supérieures, S=matrices de permutation $(i, i+1)$.

Montrons que B et N engendrent G. L'effet de multiplier une matrice à droite par un élément de B est de rajouter à une colonne une combinaison linéaire des colonnes précédentes, et l'effet de multiplier à gauche est de rajouter à une ligne une combinaison linéaire des lignes suivantes. Quitte à multiplier par un élément de N on peut supposer que le coefficient $(n, 1)$ d'une matrice est non nul et alors en multipliant par B des deux côtés on annule la dernière ligne et la première colonne sauf le coefficient $(n, 1)$. En continuant ainsi, on amène la matrice à la matrice anti-diagonale qui est dans N.

La condition (ii) est claire par 1.4.

Démontrons (iii). Pour $s = (i, i+1) \in S$, posons $G_s = \mathrm{GL}_2$ pris aux places $i, i+1$. Posons $B_s = G_s \cap B$. Alors on vérifie que $G_s \cap {}^wB = \begin{cases} B_s & \text{si } w(i) < w(i+1) \\ sB_s s & \text{sinon} \end{cases}$, et dans les deux cas un calcul dans GL_2 montre que $G_s \subset (G_s \cap B)(G_s \cap {}^wB) \cup (G_s \cap B)s(G_s \cap {}^wB)$. Multipliant par B à gauche et utilisant $G_s \cap {}^wB \subset {}^wB$ on obtient $BG_s \subset B\,{}^wB \cup Bs\,{}^wB$. Utilisant $BG_s = G_sB$, d'où $BsB \subset BG_s$, et multipliant à droite par wB, on obtient (iii).

(iv) est évident.

5.3. Exemple. Nous allons montrer que les propriétés 4.1 impliquent que si $\mathbf{T} \subset \mathbf{B}$ 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 4.1 (iv) cela revient à voir que $R_u(\mathbf{B}) \cap N_{\mathbf{G}}(\mathbf{T}) = 1$. Mais si $v \in R_u(\mathbf{B}) \cap N_{\mathbf{G}}(\mathbf{T})$, alors pour tout $t \in \mathbf{T}$, on a $[v,t] \in R_u(\mathbf{B}) \cap \mathbf{T} = 1$, donc $v \in C_{\mathbf{G}}(\mathbf{T}) = \mathbf{T}$ (par 4.1 (ii)) donc $v \in R_u(\mathbf{B}) \cap \mathbf{T} = 1$.

Montrons que $\mathbf{G}$ est engendré par $\mathbf{B}$ et $N_{\mathbf{G}}(\mathbf{T})$. Par 4.1 (v), s_α conjugue $\mathbf{U}_\alpha$ sur $\mathbf{U}_{-\alpha}$. Donc le groupe engendré par $\mathbf{B}$ et $N_{\mathbf{G}}(\mathbf{T})$ contenant $\mathbf{T}$ et $\mathbf{U}_\alpha (\alpha \in \Phi^+)$ par 4.1 (iv), et s_α, contient tous les $\mathbf{U}_\alpha$ et par 4.1 (i) 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) on procède de façon analogue à l'exemple 5.2. Si $s = s_\alpha$ on pose $G_s = \langle \mathbf{T}, \mathbf{U}_\alpha, \mathbf{U}_{-\alpha} \rangle$. Un calcul dans SL_2 montre que $G_s = \mathbf{U}_{-\alpha}\mathbf{T}\mathbf{U}_\alpha \coprod s\mathbf{T}\mathbf{U}_\alpha$. On a ${}^w\mathbf{B} \cap s\mathbf{T}\mathbf{U}_\alpha = \emptyset$, car ceci équivaut à $\mathbf{B} \cap w^{-1}s\mathbf{T}\mathbf{U}_\alpha w = \emptyset$ et $w^{-1}s\mathbf{T}\mathbf{U}_\alpha w = w^{-1}sw\mathbf{T}\mathbf{U}_{w^{-1}(\alpha)} = \mathbf{T}\mathbf{U}_{sw^{-1}(\alpha)}w^{-1}sw$ est dans $w^{-1}sw\mathbf{B}$ ou dans $\mathbf{B}w^{-1}sw$ suivant que $w^{-1}(\alpha) \in \Phi^+$ ou $w^{-1}(\alpha) \in \Phi^-$, et en tout cas ne rencontre pas $\mathbf{B}$. Par 4.1 (ii) et (iv) on en déduit que $G_s \cap {}^w\mathbf{B} = \begin{cases} G_s \cap \mathbf{B} & \text{si } w(\alpha) < 0 \\ G_s \cap s\mathbf{B}s & \text{sinon} \end{cases}$, et on conclut comme dans l'exemple 5.2.

5.4. Exemple. $\mathrm{GL}_n(\mathbb{Q}_p)$; N=matrices monômiales, B=matrices à coefficients dans $\mathbb{Z}_p$ et à coefficients sous la diagonale divisibles par p (c'est un *sous-groupe d'Iwahori*). Alors W est de type $\tilde{A}_n$. On pourra voir que pour $n = 2$, W est le groupe diédral infini engendré par $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 0 & p \\ -p^{-1} & 0 \end{pmatrix}$.

5.5. Théorème. *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) des (B,N)-paires 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 $t \in R(w)$ (cf. 1.3), on a $BtB \subset Bw^{-1}BwB$.

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

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

Preuve: Montrons (i). Puisque B et N engendrent B, on a $G = \cup_i (BWB)^i$. Par la propriété (iii) appliquée de proche en proche (avec $s = s_k$, puis $s = s_{k-1}$, etc...), si $w = s_1 \dots s_k$ on a $BwBw'B \subset Bs_1Bs_2B \dots Bs_kBwB \subset BWB$ d'où $BWBWB = BWB$ et $G = BWB$. Il reste à voir que deux doubles classes BwB et $Bw'B$ ne sont pas égales 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 2.2 en prenant $D_s = \{w \in W \mid BsBBwB = BswB\}$ (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 comme ${}^sB \neq B$ on doit avoir $BsB.BsB = BsB \coprod B$.

Il reste à voir $w \in D_s, ws' \notin D_s \Rightarrow ws' = sw$. L'hypothèse 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 $Bws'B.Bs'B \subset BwB \coprod Bws'B$. Donc $BswB = BsBwB$ est égal à soit $Bws'B$, soit à BwB. Cette dernière possibilité étant exclue, on en déduit le résultat.

On a aussi démontré (iii) au passage.

Démontrons (iv). Si $w = s_1 \dots s_k$ est une décomposition réduite, pour tout i on a

$$\begin{aligned} Bw^{-1}B.BwB &= Bs_kB \dots Bs_1Bs_1B \dots Bs_kB \\ &\supset Bs_kB \dots Bs_{i+1}Bs_iBs_iBs_{i+1}B \dots Bs_kB \\ &\supset Bs_kB \dots Bs_{i+1}Bs_iBs_{i+1}B \dots Bs_kB \\ &\supset Bs_k \dots s_{i+1}s_is_{i+1} \dots s_kB \end{aligned}$$

où on a utilisé $BsBsB \supset B$, puis $Bs_iBs_iB \supset Bs_iB$, puis $BsBwB \supset BswB$; d'où le résultat.

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

(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 $w = 1$. ■

6. Algèbres de Hecke.

6.1. Définition. *Soient (W, S) un système de Coxeter et A un anneau commutatif, et soient $\{q_s, q'_s\}_{s\in S} \in A$ une famille de paramètres ne dépendant que de la classe de conjugaison de s dans W. Alors l'algèbre de Hecke $\mathcal{H}_{\{q_s,q'_s\}_{s\in S}}(W, A)$ est la A-algèbre unitaire définie par générateurs et relations*

$$\langle \{T_s\}_{s\in S} \mid \Delta_{T_s,T'_s} = \Delta_{T'_s,T_s}, (T_s - q_s)(T_s - q'_s) = 0 \rangle.$$

6.2. Proposition. *Une autre présentation de $\mathcal{H}_{\{q_s,q'_s\}_{s\in S}}(W, A)$ est*

$$\langle \{T_w\}_{w\in W} \mid T_sT_w = \begin{cases} T_{sw} & \text{si } l(sw) > l(w) \\ (q_s + q'_s)T_w - q_sq'_sT_{sw} & \text{sinon} \end{cases} \rangle.$$

Preuve: Montrons que 6.1⇒6.2. On pose $T_w := T_{s_1} \dots T_{s_n}$ où $s_1 \dots s_n$ est une décomposition réduite de w. Alors T_w ne dépend pas de la décomposition réduite choisie par 1.2(iii). Les relations 6.2 viennent de la condition d'échange 1.2(ii).

Montrons 6.2⇒6.1. Le premier cas de la relation montre que $T_w = T_{s_1} \dots T_{s_n}$ si $s_1 \dots s_n$ est une décomposition réduite de w. En particulier l'algèbre est engendrée par les T_s et $\Delta_{T_s,T'_s} = \Delta_{T'_s,T_s}$. En prenant $w = s$ dans la relation on a la relation quadratique. ■

La présentation 6.2 montre que les T_w engendrent $\mathcal{H}_{\{q_s,q'_s\}_{s\in S}}(W,A)$ comme A-module. En fait on a

6.3. Théorème. *$\mathcal{H}_{\{q_s,q'_s\}_{s\in S}}(W,A)$ est un A-module libre de base T_w.*

Preuve: Le problème est de démontrer l'indépendance linéaire des T_w. Pour ce faire, nous allons construire une représentation $L : \mathcal{H}_{\{q_s,q'_s\}_{s\in S}}(W,A) \to A^W$ où nous pourrons prouver que les opérateurs $L(T_w) \in \mathrm{End}_A(A^W)$ sont linéairement indépendants. Si $\{e_w\}_{w\in W}$ est la base canonique de A^W, nous posons

$$L_s(e_w) = \begin{cases} e_{sw} & \text{si } l(sw) > l(w) \\ (q_s + q'_s)e_w - q_s q'_s e_{sw} & \text{sinon} \end{cases}\rangle.$$

Pour montrer que $L(T_s) = L_s$ est une représentation et que les $L(T_w)$ sont linéairement indépendants, nous utilisons le

Lemme. *Si λ est un élément de la sous-algèbre de $\mathrm{End}(A^W)$ engendré par les L_s, alors on a $\lambda = 0$ si et seulement si $\lambda(e_1) = 0$.*

Preuve: Pour $t \in S$, nous définissons un opérateur R_t par

$$R_t(e_w) = \begin{cases} e_{wt} & \text{si } l(wt) > l(w) \\ (q_t + q'_t)e_w - q_t q'_t e_{wt} & \text{sinon} \end{cases}\rangle.$$

Le point essentiel de la preuve sera que les R_t et les L_s commutent. Pour ne pas faire 4 calculs, définissons l_s, l'_s, r_t, r'_t par $L_s(e_w) = l'_s(w)e_w + l_s(w)e_{sw}$ et $R_t(e_w) = r'_t(w)e_w + r_t(w)e_{wt}$. Alors on trouve

$$\begin{aligned} R_t L_s(e_w) &= r'_t(w)l'_s(w)e_w + r_t(w)l'_s(w)e_{wt} + r'_t(sw)l_s(w)e_{sw} + r_t(sw)l_s(w)e_{swt} \\ L_s R_t(e_w) &= r'_t(w)l'_s(w)e_w + r_t(w)l'_s(wt)e_{wt} + r'_t(w)l_s(w)e_{sw} + r_t(w)l_s(wt)e_{swt}. \end{aligned}$$

Les coefficients de e_w dont égaux. Ceux de e_{wt} sont égaux sauf si $l'_s(w) \neq l'_s(wt)$ ce qui arrive quand soit $l(sw) > l(w)$ et $l(swt) < l(wt)$, soit $l(sw) < l(w)$ et $l(swt) > l(wt)$. Dans le premier cas on a par le lemme d'échange $wt = s\widehat{wt}$ où $\widehat{wt}$ doit être égal à w (sinon, s'il était égal à $\hat{w}t$ on aurait $w = s\hat{w}$ qui contredit $l(sw) > l(w)$). On a donc dans ce cas $wt = sw$. Dans le deuxième cas, on a $w = s\hat{w}$, et la deuxième condition devient $l(\hat{w}t) > l(s\hat{w}t)$. En raisonnant comme dans le premier cas, on a $\hat{w}t = s\hat{w}$, d'où encore $sw = wt$.

Les coefficients de e_{sw} sont égaux sauf si $r'_t(sw) \neq r'_t(w)$ où un raisonnement symétrique nous amène à la même conclusion $sw = wt$. Enfin les coefficients de e_{swt} sont égaux sauf si $r_t(sw) \neq r_t(w)$ ou $l_s(w) \neq l_s(wt)$ où on aboutit encore à la même conclusion.

Il reste donc à voir le cas $sw = wt$; mais alors, puisque s et t sont conjugués, on a $r_t(w) = l_s(w)$, $r'_t(w) = l'_s(w)$, $r_t(sw) = l_s(wt)$, $r'_t(sw) = l'_s(wt)$ d'où égalité (en rassemblant les termes relatifs à $e_{sw} = e_{wt}$).

Le lemme résulte immédiatement de la commutation des R_t avec λ. En effet si $l(wt) > l(w)$ alors $\lambda(e_{wt}) = \lambda(R_t(e_w)) = R_t(\lambda(e_w))$ donc par récurrence sur $l(w)$, l'égalité $\lambda(e_1) = 0$ entraîne $\lambda(e_w) = 0$. ■

Le théorème résulte immédiatement du lemme. En effet, les relations quadratiques sur les L_s résultent du calcul de $L_s^2(e_1)$. Les relations de tresse résultent du calcul $\Delta_{L_s,L_t}(e_1) = e_{\Delta_{s,t}}$. Et l'indépendance linéaire des $L(T_w)$ résulte de $L(T_w)(e_1) = e_w$ qu'on voit en prenant une décomposition réduite $w = s_1 \dots s_n$ et en appliquant $L_{s_1} \dots L_{s_n}$ à e_1. ■

Exercice.

(i) Soit (W, S) un système de Coxeter. Montrer que $s, s' \in S$ sont conjugués sous W si et seulement si il existe une suite $s = s_1, s_2, \dots s_k = s'$ d'éléments de S telle que tous les $m_{s_i,s_{i+1}}$ soient impairs (on étudiera les homomorphismes $W \to \mathbb{Z}/2\mathbb{Z}$).

(ii) Soit $\mathcal{H}$ l'algèbre définie par la présentation 6.2, mais sans supposer $q_s = q_t$ (resp. $q'_s = q'_t$) quand s et t sont conjugués. Montrer que, quand A est intègre, ces égalités (à l'échange près de q_s et q'_s) sont imposées par l'indépendance linéaire des T_w (on démontrera et utilisera l'égalité $T_s\Delta_{T_s,T_t} = \Delta_{T_t,T_s}T_t$ quand $m_{s,t}$ est impair).

7. Algèbre commutante de $\mathrm{Ind}_B^G \mathrm{Id}$.

Soit A un anneau commutatif. Nous voulons, dans un groupe G qui a une (B, N)-paire, étudier la représentation $\mathrm{Ind}_B^G A$. Nous rappelons qu'en général, si $\rho : B \to E$ est une représentation d'un sous-groupe B d'un groupe G, on note $\mathrm{Ind}_B^G E$ la représentation de G sur l'espace des fonctions $f : G \to E$ telles que $f(gb) = \rho(b)f(g)$ pour $b \in B$ où $h \in G$ agit par $(hf)(g) = f(hg)$. Ici nous allons nous intéresser à l'induit $\mathrm{Ind}_B^G A$ "à support fini", i.e. formé des fonctions qui s'annulent en dehors d'un nombre fini de classes gB (dans le cas où G est un groupe p-adique et B un sous-groupe d'Iwahori, c'est l'induit "à support compact"). Alors $\mathrm{Ind}_B^G A$ s'identifie à $A[G/B]$, en identifiant la classe gB à sa fonction caractéristique.

Rappelons que si A est un corps algébriquement clos et E est une représentation semi-simple de G, sa décomposition en composantes isotypiques est de la forme $E = \oplus_i V_i \otimes E_i$, où les E_i sont des représentations simples de G et où G agit sur $V_i \otimes E_i$ par des opérateurs de la forme $\mathrm{Id} \otimes \rho_i(g)$; on a $\mathrm{End}_G(E) \simeq \prod_i \mathrm{End}_A(V_i)$, et il y a bijection entre les représentations irréductibles de G apparaissant dans E et les $\mathrm{End}_G(E)$-modules simples. Sous des hypothèses plus générales il y a bijection entre les G-sous-modules indécomposables de E et les projectifs indécomposables pour $\mathrm{End}_G(E)$. Pour étudier la décomposition de $\mathrm{Ind}_B^G A$, nous allons donc étudier son algèbre commutante.

Avant d'énoncer la proposition suivante, nous avons besoin d'une notation. Soit W un ensemble de représentants des doubles classes $B\backslash G/B$; alors les orbites de G dans $G/B \times G/B$ (où g agit par $g(g_1B, g_2B) = (gg_1B, gg_2B)$) sont aussi indexées par w en associant à BwB l'orbite de (B, wB); nous noterons $\mathcal{O}_w$ cette orbite.

7.1. Proposition. *Soit B un sous-groupe d'un groupe G. Alors $\mathrm{End}_G \mathrm{Ind}_B^G A$ (où on a pris "l'induit à support fini") est libre de base les opérateurs T_w définis par $T_w(gB) = \sum_{\{g'B|(gB,g'B)\in\mathcal{O}_w\}} g'B$ où w parcourt les représentants des doubles classes $B\backslash G/B$ telles que $|BwB/B|$ soit fini. On a $T_w.T_{w'} = \sum_{w''} |(BwB \cap w''Bw'^{-1}B)/B| T_{w''}$.*

PREUVE: L'image de gB par un élément T de l'algèbre commutante est de la forme $T(gB) = \sum_{g'B} \lambda_{gB,g'B} g'B$. Le fait que $hT = Th$ pour $h \in G$ se traduit par

$$\sum_{g'B} \lambda_{gB,g'B} hg'B = \sum_{g'B} \lambda_{hgB,g'B} g'B,$$

i.e. $\lambda_{gB,g'B} = \lambda_{hgB,hg'B}$, i.e. λ est constante sur les orbites de G dans $G/B \times G/B$. Comme la somme doit être finie, il faut se limiter aux orbites $\mathcal{O}_w$ telles qu'il y ait un nombre fini de $g'B$ tels $(gB, g'B) \in \mathcal{O}_w$, ce qui revient à demander que $|BwB/B|$ soit fini; on obtient une base en prenant pour λ la fonction caractéristique d'une telle orbite, d'où la première partie de l'énoncé.

Pour calculer les coefficients du produit $T_w.T_{w'}$, écrivons $T_w.T_{w'} = \sum_{w''} a_{w,w'}^{w''} T_{w''}$ et appliquons les deux membres à gB. On obtient

$$\sum_{\{g'B, g''B | (gB,g'B) \in \mathcal{O}_w, (g'B,g''B) \in \mathcal{O}_{w'}\}} g''B = \sum_{\{w'', g''B | (gB,g''B) \in \mathcal{O}_{w''}\}} a_{w,w'}^{w''} g''B.$$

En comparant les coefficients (il suffit de prendre $(gB, g''B) = (B, w''B)$) on trouve

$$\begin{aligned} a_{w,w'}^{w''} &= |\{g'B \mid (B, g'B) \in \mathcal{O}_w \text{ et } (g'B, w''B) \in \mathcal{O}_{w'}\}| \\ &= |\{g'B \mid Bg'B = BwB \text{ et } Bg'^{-1}w''B = Bw'B\}|. \end{aligned}$$

Or $Bg'^{-1}w''B = Bw'B \Leftrightarrow Bw''^{-1}g'B = Bw'^{-1}B \Leftrightarrow w''^{-1}g'B \subset Bw'^{-1}B \Leftrightarrow g'B \subset w''Bw'^{-1}B$, d'où l'énoncé. ■

7.2. PROPOSITION. *Si G admet une (B, N)-paire telle que pour tout $s \in S$, $q_s := |BsB/B|$ soit fini, alors $\mathrm{End}_G \mathrm{Ind}_B^G A \simeq \mathcal{H}_{\{q_s,-1\}}(W, A)$, l'isomorphisme identifiant le T_w de 7.1 et celui de 6.2.*

PREUVE: Il suffit de voir que les opérateurs de 7.1 vérifient
(1) $T_s^2 = (q_s - 1)T_s + q_s T_1$
(2) $T_s T_w = T_{sw}$ si $l(sw) > l(w)$.

En effet (2) prouve par récurrence sur $l(w)$ que T_w existe (i.e. que $|BwB/B|$ est fini) pour tout w; on sait déjà que les T_w sont linéairement indépendants et la preuve de 6.3 montre alors que $\mathrm{End}_G \mathrm{Ind}_B^G A$ est isomorphe à la représentation $\mathcal{H}_{\{q_s,-1\}}(W, A)$ qui apparaît dans 6.3 ("représentation régulière").

Pour vérifier (1), calculons $|(BsB \cap wBsB)/B|$; c'est 0 sauf si $w \in BsBsB$ i.e., $w \in \{1, s\}$. Si $w = 1$ on trouve q_s, si $w = s$ on trouve $|(BsB \cap sBsB)/B|$; or on a $BsB \coprod B = sBsB \coprod sB$ (en effet le membre de droite est celui de gauche multiplié par s; et le membre de gauche est un groupe contenant s). Donc la seule classe $gB \subset BsB$ qui ne soit pas dans $sBsB$ est sB, et on trouve $q_s - 1$.

Pour vérifier (2) il faut calculer $|(BsB \cap w'Bw^{-1}B)/B|$ pour chaque w'; on trouve 0 sauf si $w' \in BsBwB$, ce qui implique $w' = sw$. Il reste donc à calculer $|(BsB \cap swBw^{-1}B)/B| = |(w^{-1}sBsB \cap Bw^{-1}B)/B|$. Or $w^{-1}sBsB \cap Bw^{-1}B = w^{-1}B$; en effet $w^{-1}B$ est clairement inclus dans cet ensemble, et $w^{-1}sBsB \subset w^{-1}(B \cup BsB) \subset w^{-1}B \cup Bw^{-1}sB$ dont l'intersection avec $Bw^{-1}B$ est $w^{-1}B$. On trouve donc $|w^{-1}B/B|$ ce qui vaut 1. ■

8. Théorème de déformation de Tits.

8.1. Théorème-définition. *Soit $\mathcal{H}$ une algèbre de dimension finie sur un corps K. Alors on appelle radical de $\mathcal{H}$ l'idéal bilatère défini par une des conditions suivantes:*
(i) Le plus grand idéal bilatère qui annule tous les $\mathcal{H}$-modules simples.
(ii) Le plus petit idéal à gauche J_2 tel que $\mathcal{H}/J_2$ soit semi-simple.
(iii) L'intersection des idéaux à gauche maximaux de $\mathcal{H}$.
(iv) Le plus grand idéal bilatère nilpotent de $\mathcal{H}$.

Preuve: Soit J_1 (resp. J_2, J_3, J_4) l'idéal défini par (i) (resp. (ii),(iii),(iv)). Il est clair que la somme de deux idéaux nilpotents est nilpotente, donc J_4 existe. Si S est un $\mathcal{H}$-module simple, on a $J_4S = 0$. En effet, sinon $J_4S = S$ donc $J_4^iS = S$ pour tout i ce qui contredit J_4 nilpotent. Donc $J_4 \subset J_1$. Maintenant, si $N \subset J_1^i$ tel que J_1^i/N soit simple (ce qui est toujours possible si $J_1^i \neq 0$; tout $\mathcal{H}$-module possède un quotient simple), alors $J_1^{i+1} = J_1.J_1^i \subset N$ (puisque J_1 annule J_1^i/N) donc la suite J_1^i ne peut stationner et doit converger vers 0. Donc $J_1 = J_4$.

Si $N_1, \ldots N_r$ sont des idéaux à gauche de $\mathcal{H}$ tels que $\mathcal{H}/N_i$ soit semi-simple, alors $\mathcal{H}/(N_1 \cap \ldots \cap N_r)$ s'injecte dans $\mathcal{H}/N_1 \oplus \ldots \oplus \mathcal{H}/N_r$, donc est semi-simple, donc J_2 existe; et si on prend pour N_i des idéaux maximaux tels que $J_3 = N_1 \cap \ldots \cap N_r$, alors on obtient $J_3 \supset J_2$. Réciproquement, si $\mathcal{H}/J_2 = N_1/J_2 \oplus \ldots \oplus N_r/J_2 = (\sum_i N_i)/J_2$ est une décomposition en modules simples, alors si $M_i = \sum_{j \neq i} N_j$ on a $\mathcal{H}/M_i \simeq (\mathcal{H}/J_2)/(\oplus_{j \neq i} N_i/J_2) \simeq N_i/J_2$ est simple donc M_i est maximal, et $J_2 = M_1 \cap \ldots \cap M_r$. Donc $J_2 = J_3$.

Si M est un idéal à gauche maximal alors $\mathcal{H}/M$ est simple donc $J_1\mathcal{H}/M = 0$. Ceci implique $J_1 \subset M$. En effet, si $x \in J_1$ alors $x(h + M) = M$ pour tout $h \in \mathcal{H}$, en particulier $x(1 + M) = M$ d'où $x \in M$. Donc $J_1 \subset J_3$. Réciproquement, si $J_3 \not\subset J_1$, il existe S simple tel que $J_3S \neq 0$, donc il existe $s \in S$ tel que $J_3s = S$; en particulier il existe $j \in J_3$ tel que $js = -s$, i.e. $(j + 1)s = 0$; donc $j + 1$ est dans un idéal à gauche propre, l'annulateur de s, donc est dans un certain idéal maximal M. Mais j aussi est dans M une contradiction (car alors $1 \in M$). ■

Le théorème 8.1 est en fait généralement valable pour les anneaux Artiniens (avec une preuve plus compliquée).

8.2. Théorème-définition. *Soit $\overline{K}$ une clôture algébrique de K. Alors $\mathcal{H}$ est dite séparable si elle vérifie une des conditions équivalentes suivantes:*
(i) $\mathcal{H} \otimes \overline{K}$ est semi-simple.
(ii) $\mathcal{H} \otimes \overline{K}$ est une somme $\oplus_i M_{n_i}(\overline{K})$ d'algèbres de matrices.
(iii) Pour toute extension E de K, l'algèbre $\mathcal{H} \otimes E$ est semi-simple.

Preuve: Démontrons (i) $\Rightarrow$ (ii). Supposons K algébriquement clos et montrons qu'une algèbre $\mathcal{H}$ semi-simple est isomorphe à une somme d'algèbres de matrices. On a $\mathcal{H} \simeq \mathrm{End}_{\mathcal{H}}(\mathcal{H})^{\mathrm{opp}}$. En effet, un élément $\rho \in \mathrm{End}_{\mathcal{H}}(\mathcal{H})$ s'identifie à la multiplication à droite par $\rho(1)$ car $a.\rho(1) = \rho(a.1) = \rho(a)$. Maintenant, $\mathcal{H}$ étant semi-simple, $\mathrm{End}_{\mathcal{H}}(\mathcal{H})^{\mathrm{opp}}$ est la somme directe des endomorphismes des composantes isotypiques. Soit $\oplus_{i=1}^{i=n} S$ une telle composante. K étant algébriquement clos, on a $\mathrm{End}_A(S) \simeq K$ par le lemme de Schur (un élément $\rho \in \mathrm{End}_A(S)$ a au moins une valeur propre λ sur K et $\rho - \lambda\,\mathrm{Id}$ n'étant pas surjectif doit être nul). On en déduit que $\mathrm{End}_A(\oplus_{i=1}^{i=n} S) \simeq M_n(K)$.

Réciproquement, comme module sur elle-même, $M_n(K)$ est somme pour $i \in [1..n]$ des modules simples formés des matrices qui ont tous les coefficients nuls hors d'une colonne, donc est semi-simple (on voit aussi que dans les composantes isotypiques on a $\dim S = n$).

On a clairement (iii) $\Rightarrow$ (i). Pour voir la réciproque, on remarque que si $\mathcal{H} \otimes E$ a un radical N non trivial, alors $N \otimes_E \overline{K}$ donne un idéal nilpotent non trivial de $\mathcal{H} \otimes \overline{K}$, ce qui contredit le fait que le radical de cette dernière algèbre soit trivial. ■

Si $\mathcal{H}$ est séparable, les n_i du (ii) du théorème ci-dessus sont appelés les *invariants numériques* de $\mathcal{H}$. Deux algèbres sur $\overline{K}$ sont isomorphes si et seulement si elles ont mêmes invariants numériques. Si K est parfait, séparable équivaut à semi-simple.

8.3. Proposition. *Soit $\mathcal{H}$ une algèbre de dimension finie sur un corps K.*

(i) Si la forme bilinéaire $(a,b) \mapsto \mathrm{Trace}_{\mathcal{H}/K}(ab)$ est non-dégénérée (où $\mathrm{Trace}_{\mathcal{H}/K}(a)$ est la trace de la matrice de la multiplication par a), alors l'algèbre $\mathcal{H} \otimes E$ est séparable.

(ii) Si K est de caractéristique 0 et $\mathcal{H}$ est séparable, alors la forme bilinéaire $(a,b) \mapsto \mathrm{Trace}_{\mathcal{H}/K}(ab)$ est non dégénérée.

Preuve: Montrons (i). La forme $(a,b) \mapsto \mathrm{Trace}_{\mathcal{H}/K}(ab)$ reste non dégénérée sur toute extension. Il suffit donc de voir que sa non-dégénérescence implique que le radical de $\mathcal{H}$ est nul. Mais un élément du radical est nilpotent, donc sa matrice a une trace nulle.

Montrons (ii). Il suffit de faire le calcul pour un algèbre de matrices $M_n(K)$, en prenant par exemple pour base les matrices $E_{i,j}$ dont seul le coefficient (i,j) est non nul et vaut 1. Pour la matrice m, on trouve $\mathrm{Trace}_{\mathcal{H}/K}(m) = n\,\mathrm{Trace}(m)$. D'où le résultat. ■

8.4. Théorème de déformation de Tits. *Soit $f : A \to k$ un morphisme d'anneaux où A est un anneau intègre et k un corps. Soit $\mathcal{H}$ une A-algèbre qui soit un A-module libre de dimension finie. Soit K le corps des fractions de A.*

(i) Supposons que sur $\mathcal{H} \otimes_A k$ (défini par f) la forme $(a,b) \mapsto \mathrm{Trace}_{\mathcal{H}\otimes_A k/k}(ab)$ soit non-dégénérée. Alors $\mathcal{H} \otimes_A K$ est séparable.

(ii) Supposons que $\mathcal{H} \otimes_A k$ et $\mathcal{H} \otimes_A K$ soient séparables. Alors elles ont mêmes invariants numériques.

(iii) Soit $\overline{A}$ la clôture intégrale de A dans une clôture algébrique $\overline{K}$ de K; alors il existe une extension $\overline{f} : \overline{A} \to \overline{k}$ de f (où $\overline{k}$ est une clôture algébrique de k). Si $\overline{f}$ est une telle extension, sous les hypothèses de (ii), pour tout caractère irréductible χ de $\mathcal{H} \otimes_A \overline{K}$ et pour tout $a \in A$ on a $\chi(a) \in \overline{A}$ et $\overline{f} \circ \chi$ est un caractère irréductible de $\mathcal{H} \otimes_A k$.

Preuve: Pour abréger, notons $\mathcal{H}(K)$ (resp. $\mathcal{H}(\overline{K})$, $\mathcal{H}(k)$) pour $\mathcal{H} \otimes_A K$ (resp. $\mathcal{H} \otimes_A \overline{K}$, $\mathcal{H} \otimes_A k$). Remarquons d'abord que sous l'hypothèse de (i) $\mathcal{H}(K)$ est séparable. En effet une base de $\mathcal{H}$ sur A donne après tensorisation une base de $\mathcal{H}(k)$ sur k, et la forme bilinéaire $\mathrm{Trace}_{\mathcal{H}(K)/K}(ab)$ se spécialise en $\mathrm{Trace}_{\mathcal{H}(k)/k}(ab)$ qui par hypothèse est non dégénérée. Ces deux considérations impliquent que $\mathrm{Trace}_{\mathcal{H}(K)/K}(ab)$ est non dégénérée.

Plaçons-nous maintenant sous les hypothèses de (ii). Notons $b_1, \ldots, b_n$ une base de $\mathcal{H}$ sur A, et soient $x_1, \ldots, x_n$ des indéterminées. Soit $P(t)$ le polynôme caractéristique de la multiplication par "l'élément général" $\sum_i x_i b_i$ dans $\mathcal{H}(A[x_1, \ldots, x_n])$, et soit $\prod_j P_j^{p_j}$ sa décomposition en facteurs irréductibles sur $\overline{K}(x_1, \ldots, x_n)$. Alors p_j est le degré de P_j, et les p_j sont les invariants numériques de $\mathcal{H}(\overline{K})$. En effet $\mathcal{H}(\overline{K}) \simeq \oplus_i M_{n_i}(\overline{K})$, d'où

$\mathcal{H}(\overline{K}(x_1,\dots,x_n)) \simeq \oplus_i M_{n_i}(\overline{K}(x_1,\dots,x_n))$. Changer de base b_i dans $\mathcal{H}(\overline{K})$ revient à remplacer les x_i par des formes linéaires en les x_i donc ne change rien à la factorisation de $P(t)$. Pour calculer celle-ci, on peut donc se ramener à calculer $P(t)$ pour une algèbre de matrices $M_n(\overline{K}(x_1,\dots,x_n))$ en prenant pour base les matrices $E_{i,j}$ dont seul le coefficient (i,j) est non nul et vaut 1. Alors on trouve que la matrice de la multiplication par $\sum_i x_{i,j}E_{i,j}$ est n copies sur la diagonale de la matrice $(x_{i,j})_{i,j}$, et donc $P(t) = \det(t\,\mathrm{Id} - (x_{i,j})_{i,j})^n$. Les facteurs $\det(t\,\mathrm{Id} - (x_{i,j})_{i,j})$ sont irréductibles (car par exemple ils se spécialisent en le polynôme général de degré n), d'où le résultat annoncé sur la factorisation de $P(t)$. Notons aussi pour référence future que si χ est le caractère irréductible de $\mathcal{H}(\overline{K}(x_1,\dots,x_n))$ sur M_n, alors $\chi(\sum_j x_j b_j)$ est le coefficient du terme de degré $n-1$ d'un facteur irréductible de P.

Maintenant, $\overline{A}[x_1,\dots,x_n]$ est la clôture intégrale de $A[x_1,\dots,x_n]$ dans $\overline{K}(x_1,\dots,x_n)$ (Bourbaki, algèbre commutative ch V prop.13). Les coefficients des P_i sont entiers sur les racines des P_i, donc sur les coefficients de P, donc sur $A[x_1,\dots,x_n]$, donc ils sont dans $\overline{A}[x_1,\dots,x_n]$. Pour voir qu'on peut étendre f en $\overline{f} : \overline{A} \to \overline{k}$, il suffit de le faire pour une extension par un élément $A[\alpha]$ et on peut clairement le faire. Par $\overline{f}$, la décomposition $P = \prod_i P_i^{p_i}$ se spécialise en une décomposition du polynôme caractéristique de l'élément général de $\mathcal{H}(k[x_1,\dots,x_n])$. Mais un polynôme $\prod_i P_i^{p_i}$ ne peut avoir qu'une décomposition où les facteurs irréductibles sont à la puissance leur degré (si un tel facteur n'est pas irréductible, ses facteurs irréductibles seront élevés à plus que leur degré). Donc les invariants numériques de $\mathcal{H}(K)$ et de $\mathcal{H}(k)$ sont les mêmes.

La remarque ci-dessus sur le fait que les caractères apparaissent comme coefficients des P_i prouve aussi que leurs valeurs sont dans $\overline{A}$ et qu'un caractère se déforme en un caractère. ■

Corollaire. *Soit (W,S) un système de Coxeter fini et soit k un corps dont la caractéristique de divise pas $|W|$.*

(i) Soient $\{q_s, q'_s\}_{s\in S}$ des indéterminées qui ne dépendent que de la classe de conjugaison de s sous W. Alors $\mathcal{H}_{\{q_s,q'_s\}}(W, k(q_s,q'_s))$ est séparable et a mêmes invariants numériques que kW.

(ii) Soit G un groupe fini admettant une (B,N)-paire de groupe de Weyl W, et supposons k algébriquement clos et que sa caractéristique ne divise pas l'ordre de G. Alors $\mathrm{End}_G \mathrm{Ind}_B^G k \simeq kW$.

Preuve: Pour (i) on utilise la spécialisation $q_s \mapsto 1, q'_s \mapsto -1$ et 8.4 (i) puis (ii); ici $\mathcal{H}(k) \simeq kW$; la forme bilinéaire $\mathrm{Trace}_{\mathcal{H}(k)/k}$ est non-dégénérée car les dimensions des représentations irréductibles de W divisent $|W|$ donc sont inversibles dans k.

Pour (ii) on utilise le fait qu'un algèbre commutante d'une représentation semi-simple est semi-simple; puis on utilise 8.4 (ii) en partant de l'algèbre générique (qui est séparable par (i)) et en spécialisant en $\{q_s, -1\}$. ■

9. Algèbres symétriques, degrés génériques.

Soit $\mathcal{H}$ une algèbre de dimension finie sur un corps K. Une forme linéaire $\tau : \mathcal{H} \to K$ est dite une *fonction centrale* ou une *trace* si $\tau(hh') = \tau(h'h)$ pour tous $h, h' \in \mathcal{H}$.

9.1. Définition. *L'algèbre $\mathcal{H}$ est dite symétrique si elle possède une fonction centrale τ telle que la forme bilinéaire $(a,b)\mapsto\tau(ab)$ soit non-dégénérée; la trace τ est dite forme symétrisante pour $\mathcal{H}$.*

Cela revient au même de demander un isomorphisme de $\mathcal{H}$-module-$\mathcal{H}$ entre $\mathcal{H}$ et son dual $\mathcal{H}^*$. En effet $h\mapsto(x\mapsto\tau(hx))$ donne un tel isomorphisme. Réciproquement, si i est un tel isomorphisme, posons $\tau(h)=i(h)(1)$. Alors, en utilisant la structure de $\mathcal{H}$-module-CH sur $\mathcal{H}^*$: $(x.\phi)(y)=\phi(yx)$ et $(\phi.x)(y)=\phi(xy)$ pour $\phi\in\mathcal{H}^*$ et $x,y\in\mathcal{H}$, on trouve $\tau(xy)=i(xy)(1)=(x.i(y))(1)=i(y)(x)=(i(y).x)(1)=i(yx)(1)=\tau(yx)$.

Si $\{b_i\}_i$ est une base de $\mathcal{H}$, nous noterons $\{\check{b}_i\}_i$ la base duale définie par $\tau(b_i\check{b}_j)=\delta_{i,j}$. Le fait que la forme bilinéaire associée à τ soit non dégénérée est évidemment équivalente au fait qu'il existe une base qui ait (ou que toute base ait) une base duale.

9.2. Exemple. On a vu (8.3 (ii)) qu'une algèbre séparable sur un corps de caractéristique 0 est symétrique (en fait ceci reste vrai en caractéristique finie en remplaçant la $\mathrm{Trace}_{\mathcal{H}/K}$ par la trace réduite qui consiste à prendre la trace et non n fois la trace pour $M_n(K)$; plus généralement, une combinaison $\tau=\sum_i\lambda_i\chi_i$ où χ_i sont les caractères irréductibles convient si aucun des λ_i n'est nul).

9.3 Exemple. Si G est un groupe fini et K un corps, KG est symétrique (même quand la caractéristique de K divise $|G|$ où elle n'est pas semi-simple). On prend $\tau=$ coefficient sur 1, et on constate que $\{g\}_{g\in G}$ et $\{g^{-1}\}_{g\in G}$ sont duales.

9.4. Exemple. Sous les conditions de 7.1, si K est un corps de caractéristique 0 et G/B est fini, l'algèbre $\mathrm{End}_G\mathrm{Ind}_B^G K$ est symétrique pour la forme $\tau(h)=\mathrm{Trace}(h\mid\mathrm{Ind}_B^G A)$: on commence par remarquer que $\mathrm{Trace}(T_w\mid\mathrm{Ind}_B^G A)=0$ si $w\neq1$, et $\mathrm{Trace}(T_1)=|G/B|$. On en déduit que $\tau(T_wT_{w'})=|G/B|(T_wT_{w'}\mid T_1)=|G/B||BwB\cap Bw'^{-1}B/B|=|G/B||BwB/B|\delta_{w,w'^{-1}}$. Donc dans la base T_w la matrice de la forme bilinéaire associée à τ est inversible.

9.5. Exemple. Cet exemple a un rapport avec le précédent. Si $\{q_s,q'_s\}$ sont des éléments inversibles du corps K, alors $\mathcal{H}_{\{q_s,q'_s\}}(K,W)$ est symétrique pour $\tau=$coefficient sur T_1. En effet, si on pose $q_w=q_{s_1}\dots q_{s_n}$ si $w=s_1\dots s_n$ est une décomposition réduite, et qu'on définit de même q'_w, alors on a:

Lemme. *Le coefficient de $T_wT_{w'^{-1}}$ sur T_1 est nul sauf si $w=w'$ auquel cas il vaut $q_wq'_w(-1)^{l(w)}$.*

Preuve: On procède par récurrence sur $l(w)$. C'est clair si $l(w)=0$. Sinon on écrit $w=w_1s$ où $s\in S$ et $l(w)=l(w_1)+1$. Si $l(w's)>l(w')$ alors $T_wT_{w'^{-1}}=T_{w_1}T_{(w's)^{-1}}$ dont par récurrence le coefficient sur T_1 est 0 car $w_1\neq w's$ (s s'ajoute à w_1 et se retranche à $w's$), ce qui est le résultat voulu car aussi $w\neq w'^{-1}$. Sinon on a $T_wT_{w'^{-1}}=(q_s+q'_s)T_{w_1}T_{w'^{-1}}-q_sq'_sT_{w_1}T_{(w's)^{-1}}$. Le coefficient sur 1 de $T_{w_1}T_{w'^{-1}}$ est nul par récurrence, et celui de $T_{w_1}T_{(w's)^{-1}}$ est nul sauf si $w's=w_1$ (ce qui équivaut à $w=w'$) et vaut dans ce dernier cas $q_{w_1}q'_{w_1}(-1)^{l(w_1)}$, d'où le résultat. ■

On voit aussi que $\{T_w\}_{w\in W}$ et $\{q_w^{-1}q'^{-1}_w(-1)^{l(w)}T_{w^{-1}}\}_{w\in W}$ sont des bases duales. On voit aussi, en comparant les formules de 9.4 et de 9.5, que si G possède une (B,N)-paire telle que $q_s=|BsB/B|$, on a $|BwB/B|=q_w$ dans 9.4.

9.6. Proposition. *Soit $\mathcal{H}$ une algèbre symétrique sur un corps K, et soient $\{b_i\}_i, \{\check{b}_i\}_i$ deux bases duales. Alors l'élément $I = \sum_i b_i \otimes \check{b}_i$ de $\mathcal{H} \otimes_K \mathcal{H}^{op}$ vérifie $(h \otimes 1)I = (1 \otimes h)I$ pour $h \in \mathcal{H}$ et ne dépend pas de la base choisie pour le construire.*

Preuve: Pour $h, h', x, y \in H$, calculons $\tau \otimes \tau((h \otimes h')I(x \otimes y))$. On trouve

$$\sum_i \tau(hb_ix)\tau(y\check{b}_ih') = \sum_i \tau(b_ixh)\tau(\check{b}_ih'y) = \sum_i (xh \mid \check{b}_i)(h'y \mid b_i) = \tau(xhh'y).$$

La forme bilinéaire $\tau \otimes \tau$ étant non dégénérée, ceci montre les deux assertions de l'énoncé. ■

Notons que l'image de I par l'isomorphisme $\mathcal{H} \otimes \mathcal{H}^{op} \xrightarrow{\sim} \mathrm{Hom}(\mathcal{H}^*, \mathcal{H})$ donné par $x \otimes y \mapsto (\phi \mapsto \phi(x)y)$ est l'inverse de l'isomorphisme $i : \mathcal{H} \xrightarrow{\sim} \mathcal{H}^*$ donné par τ. En d'autres termes on a $i^{-1}(\phi) = \sum_i \phi(b_i)\check{b}_i$.

9.7 Corollaire. *Sous les hypothèses ci-dessus, soient M et N deux $\mathcal{H}$-modules, et soit $\phi \in \mathrm{Hom}_K(M, N)$. Alors $I\phi \in \mathrm{Hom}_H(M, N)$.*

Preuve: Ici l'action de $\mathcal{H} \otimes_K \mathcal{H}^{op}$ sur $\mathrm{Hom}_K(M, N)$ est par $(h \otimes h')(\phi)(x) = h\phi(h'x)$. Le résultat est une conséquence évidente de la proposition précédente. ■

On définit le produit scalaire de deux fonctions centrales χ et ψ par $\langle \chi, \psi \rangle_\tau = (\chi \otimes \psi)(I) = \chi(i^{-1}(\psi)) = \psi(i^{-1}(\chi))$ (dans l'exemple 9.3, on a $|G|$ fois le produit scalaire usuel pour des caractères irréductibles. Mais on a étendu linéairement ici et non semi-linéairement). On a:

9.8. Proposition. *Si χ et ψ sont les caractères de deux modules simples non isomorphes, alors $\langle \chi, \psi \rangle_\tau = 0$.*

Preuve: Soit $v_1, \ldots, v_m$ une K-base du module M dont χ est le caractère, et $v'_1, \ldots, v'_n$ une K-base du module N dont ψ est le caractère. Soit $E_{k,k'} \in \mathrm{Hom}_K(M, N)$ qui envoie v_k sur $v'_{k'}$ et les autres vecteurs de base sur 0. On applique 9.7 à $E_{k,k'}$ et on trouve que tous les coefficients de $\sum_i b_i E_{k,k'} \check{b}_i$ son nuls. En l'écrivant pour le coefficient k, k' cela donne $\sum_i (b_i)_{k,k} (\check{b}_i)_{k',k'} = 0$ où ici (b_i) représente la matrice de b_i dans M et $(\check{b}_i)$ la matrice de $\check{b}_i$ dans N. En sommant sur k, k' on obtient la proposition.

Proposition. *Soit G un groupe fini muni d'une BN-paire, et soit K un corps de caractéristique ne divisant pas $|G|$. Soit $\mathcal{H} = \mathrm{End}_G \mathrm{Ind}_B^G K$, soit $\chi \in \mathrm{Irr}(\mathcal{H})$ et soit ρ_χ le caractère irréductible de G correspondant (tel que le caractère de $\mathrm{Ind}_B^G K$ soit $\sum_\chi \chi \otimes \rho_\chi$). Soit τ la forme symétrisante "coefficient sur T_1" dans $\mathcal{H}$. Alors on a $\rho_\chi(1) = \chi(1)|G/B|/\langle \chi, \chi \rangle_\tau$.*

Preuve: On calcule le produit scalaire de caractères de $\mathcal{H}$-modules $\langle \mathrm{Ind}_B^G K, \chi \rangle_\tau = \langle \sum_\chi \rho_\chi(1)\chi, \chi \rangle_\tau = \rho_\chi(1)\langle \chi, \chi \rangle_\tau$, la dernière égalité par 9.8. Mais en utilisant la définition et les bases duales $\{T_w\}_{w \in W}$ et $\{q_w^{-1} T_{w^{-1}}\}_{w \in W}$ (ici $q'_s = -1$), on a $\langle \mathrm{Ind}_B^G K, \chi \rangle_\tau = \sum_w \mathrm{Trace}(T_w \mid \mathrm{Ind}_B^G K)\chi(q_w^{-1} T_{w^{-1}}) = |G/B|\chi(1)$, la dernière égalité d'après les calculs de 9.4. ■

Notons que $|G/B| = \sum_{w \in W} |BwB/B| = \sum_{w \in W} q_w$, et que

$$\langle \chi, \chi \rangle_\tau = \sum_{w \in W} \chi(T_w)\chi(T_{w^{-1}})q_w^{-1}.$$

Exercice. Calculer $\rho_\chi(1)$ pour $\chi(T_w) = q_w$ et pour $\chi(T_w) = (-1)^{l(w)}$ (pour ce dernier cas on utilisera l'élément w_0 de 2.3).

10. Rappels de topologie algébrique.

Pour des détails ou démonstrations, voir [Godbillon].

Soient X, Y deux espaces topologiques. On note I l'espace topologique que constitue le segment $[0,1] \subset \mathbb{R}$. Deux applications continues $f, g : X \to Y$ sont dites *homotopes* (noté $f \sim g$) s'il existe une application continue $h : X \times I \to Y$ telle que $h(x,0) = f(x)$ et $h(x,1) = g(x)$ pour tout $x \in X$ (on peut imaginer I comme le "temps", et imaginer une déformation de f en g quand le temps va de 0 à 1).

L'homotopie est une relation d'équivalence (pour voir la transitivité, on coupe I en deux parties homéomorphes à lui-même, et on fait la première homotopie dans un premier temps, la seconde dans le deuxième), compatible à la composition des applications.

Les classes d'homotopie d'applications continues $I \to X$ forment ce qu'on appelle le *groupoïde fondamental* de X. Un telle application est appelé un *chemin* et son image un *arc*. Un groupoïde est une catégorie où toutes les flèches sont inversibles; ici les objets de la catégorie sont les points de X et les flèches de x à y les chemins de x à y (applications $\gamma : I \to X$ telles que $\gamma(0) = x$, $\gamma(1) = y$). On compose deux chemins en "divisant les temps par 2". L'inverse de γ est le chemin $\gamma'(t) = \gamma(1-t)$; le composé $\gamma'' = \gamma' \circ \gamma$, qui vaut $\gamma(2t)$ si $t \leq 1/2$ et $\gamma'(2t-1)$ sinon, est homotope au chemin trivial $I \to x$ par l'homotopie $h(t,t') = \gamma''(tt')$.

Étant donné $x \in X$, les chemins d'origine et d'extrémité x (qu'on appelle les *lacets* de base x) forment un groupe $\Pi_1(X,x)$ appelé *groupe fondamental* de base x. À isomorphisme près, ce groupe ne dépend que de la composante connexe par arcs du point base (un espace est *connexe par arcs* s'il existe un arc reliant deux points arbitraires).

Une application $f : X \to Y$ induit une application $f^* : \Pi_1(X,x) \to \Pi_1(Y, f(x))$ par composition. S'il existe $g : Y \to X$ telle que $f \circ g \sim \mathrm{Id}_Y$ et $g \circ f \sim \mathrm{Id}_X$ on dit que f est une *équivalence d'homotopie* et que X et Y ont même *type d'homotopie*. On dit que X est *contractile* s'il a même type d'homotopie qu'un point. Une partie convexe d'un espace affine est contractile (on peut la contracter sur un de ses points). Un équivalence d'homotopie induit un isomorphisme de Π_1 (car $g \circ f$ induit clairement un isomorphisme $\Pi_1(X,x) \simeq \Pi_1(X, g \circ f(x))$).

Une application $p : E \to B$ a la *propriété de relèvement des homotopies* si pour tout diagramme commutatif

$$\begin{array}{ccc} X \times \{0\} & \longrightarrow & E \\ \downarrow & \overset{h}{\nearrow} & \downarrow p \\ X \times I & \longrightarrow & B \end{array}$$

il existe h qui rend le diagramme commutatif. C'est le cas par exemple si p est une *fibration*, c'est-à-dire qu'il existe un espace F et un recouvrement ouvert $\{U_\alpha\}_\alpha$ de B tel que $p^{-1}(U_\alpha) \simeq U_\alpha \times F$, sur lequel p s'identifie à la première projection, et B est paracompact (i.e. séparé, et pour tout recouvrement ouvert il existe un recouvrement ouvert localement fini plus fin). Un *revêtement* est une fibration qui est un *homéomorphisme local* (tout point de E possède un voisinage où la restriction de p devient un homéomorphisme). Alors nécessairement F est discret. Le revêtement est galoisien si E est connexe et p est le quotient par l'action d'un groupe discret G agissant librement et proprement (tout point possède

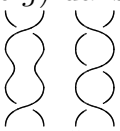
un voisinage dont tous les translatés sont disjoints). Alors (cf. [Godbillon, IX, 4.5]) on a une suite exacte:

$$1 \to \Pi_1(E, e) \to \Pi_1(B, p(e)) \to G \to 1.$$

10.1. Exemple. $\mathbb{R} \to \mathbb{U} : x \mapsto e^{2i\pi x}$ est un revêtement galoisien du cercle unité de $\mathbb{C}$ de groupe $\mathbb{Z}$ (réalisé comme les translations entières). L'espace $\mathbb{R}$ étant contractile, on en déduit $\Pi_1(\mathbb{U}) \simeq \mathbb{Z}$.

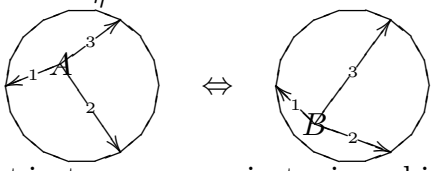
10.2. Exemple. Soit V un $\mathbb{C}$-espace vectoriel, et soit W un groupe fini de réflexions complexes associé à l'arrangement $\mathcal{A}$ d'hyperplans. Soit $\mathcal{M} = V - \cup_{H \in \mathcal{A}} H$. Alors W agit proprement et librement sur $\mathcal{M}$ (le fait qu'il n'y ait pas de point fixe en dehors des hyperplans est donné par 2.1(iii) quand V possède une structure réelle; c'est un théorème assez difficile dû à Steinberg dans le cas général). On en déduit, si on choisit $x \in \mathcal{M}$, une suite exacte $1 \to \Pi_1(\mathcal{M}, x) \to \Pi_1(\mathcal{M}/W, \overline{x}) \to W \to 1$. Le groupe $\Pi_1(\mathcal{M}, x)$ est appelé le *groupe de tresses pures* associé à (V, W), et $\Pi_1(\mathcal{M}/W, \overline{x})$ le *groupe de tresses* associé à (V, W).

Nous allons nous intéresser particulièrement dans la suite à l'exemple 10.2 dans le cas où W est le groupe $\mathfrak{S}_n$ agissant par permutation des coordonnées dans $\mathbb{C}^n$. Alors $\mathcal{A} = \{H_{ij}\}_{i,j}$ où H_{ij} est défini par l'équation $x_i = x_j$, donc $\mathcal{M} = \{(x_1, \ldots, x_n) \in \mathbb{C}^n \mid x_i \neq x_j \forall i, j\}$. La variété $\mathcal{M}/W$ s'identifie à l'espace X_n des parties à n éléments de $\mathbb{C}$. Si γ est un lacet de base x dans X_n, un argument de continuité montre que γ définit une application continue $f : x \times I \to \mathbb{C}$ (où $\gamma(t) = f(x \times \{t\})$), i.e. qu'on peut "suivre l'image de chaque élément de x" par γ (l'image d'un élément donné de x est appelé un *brin* de la tresse). Dans cette correspondance, $f(., 0)$ est l'identité sur x, mais $f(., 1)$ peut réaliser une permutation non triviale de x. À cette application f on peut associer à son tour un plongement $g : x \times I \hookrightarrow \mathbb{C} \times I$ par $g(., t) = (f(., t), t)$.

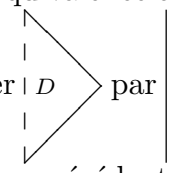
Ceci amène à la façon traditionnelle de dessiner une tresse (l'image de g) dans $\mathbb{C} \times I$ (une tresse à 4 brins avec le point-base traditionnel $x = \{1, \ldots, 4\} \subset \mathbb{C}$: ).

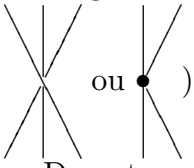
Un homotopie de lacets dans $\Pi_1(\mathcal{M}/W, \overline{x})$ est dans ce cadre devenu une "isotopie à niveau constant" entre g et g', i.e. une application continue $I \times (x \times I) \to \mathbb{C} \times I$ qui à tout $t \in I$ associe un plongement g_t, avec $g_0 = g$ et $g_1 = g'$. Ici le "à niveau constant" se réfère au fait qu'on demande $g_t(., t') \in \mathbb{C} \times \{t'\}$ pour tout t (une isotopie générale n'est pas soumise à cette condition).

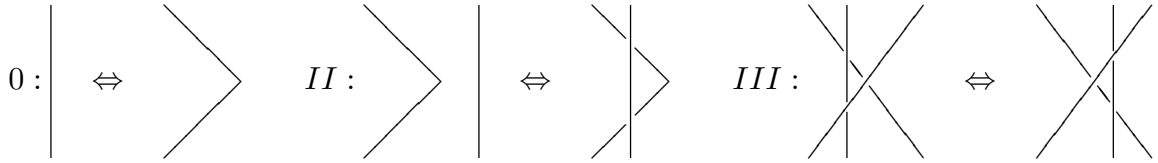
Toute tresse g est isotope à une tresse g' PL ("piecewise linear", i.e. linéaire par morceaux) par une isotopie ambiante à niveau constant (c'est-à-dire une application $h : I \times (\mathbb{C} \times I) \to \mathbb{C} \times I$ telle que si on note h_t pour $h(t, .)$, pour tout t l'application h_t soit un homéomorphisme, $h_0 = \mathrm{Id}$, $h_1 \circ g = g'$ et le niveau constant correspond à la condition $\forall t, h_t(., t') \in \mathbb{C} \times \{t'\}$; "tout l'espace" se déforme pour amener une tresse sur l'autre). Pour le voir, on utilise le fait qu'en tout t, l'image $g(x, t)$ est formée de n éléments distincts. Si $x = \{x_1, \ldots, x_n\}$, on choisit $\epsilon > 0$ tel que les "brins" $f_i(t) = g(x_i, t)$ soient toujours séparés de 2ϵ. La continuité uniforme de la fonction f_i nous donne qu'il existe η tel que $|t - t'| < \eta \Rightarrow |f_i(t) - f_i(t')| < \epsilon$ pour tout i. Alors la tresse g est dans une union de voisinages de la forme $V_{i,t} = \{y, t' \mid t \leq t' \leq t + \eta, |y - f_i(t)| \leq \epsilon\}$ qui ne rencontrent chacun qu'un seul brin. Dans chacun de ces voisinages le brin f_i est homotope par une

isotopie ambiante à la droite qui D qui relie $f_i(t)$ à $f_i(t+\eta)$: si $t' \in [t, t+\eta]$, et si dans le plan $P = \mathbb{C} \times \{t'\}$ on pose $A = f_i(t')$ et $B = P \cap D = f_i(t) + \frac{t'-t}{\eta}(f_i(t+\eta) - f_i(t))$ l'isotopie a l'aspect suivant dans le disque $|y - f_i(t)| \leq \epsilon$ de P: 

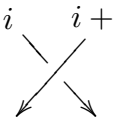
(les points notés 1, 2, 3 se correspondent); donc la tresse g est isotope par une isotopie ambiante à une tresse PL.

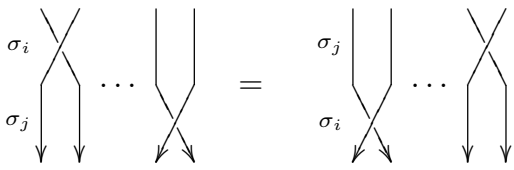
Pour les tresses PL, les notions d'"isotopie à niveau constant", d'"isotopie ambiante à niveau constant", et d'"équivalence combinatoire" coïncident, où une équivalence combinatoire consiste à remplacer 

par où D ne rencontre pas la tresse (par un raisonnement de continuité analogue au précédent, on montre que deux tresses PL isotopes le sont par une isotopie PL). Une tresse PL est déterminée à isotopie près par une *projection régulière*, c'est-à-dire une projection orthogonale sur un plan $P_\theta = \{(z,t) \in \mathbb{C} \times I \mid \arg(z) = \theta\}$ telle que chaque point de la projection n'appartienne qu'à un brin ou n'appartienne qu'à l'intérieur de deux segments de droites appartenant à des brins distincts (i.e. pas d'accidents du genre  ou); de plus, à chaque croisement on indique quel est le segment qui est au-dessus. Deux tresses isotopes ont des projections régulières équivalentes par des mouvements de Reidemeister d'un des types

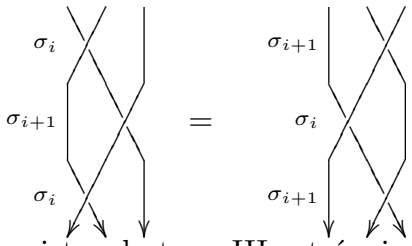


(0 résulte d'une équivalence combinatoire, et II et III peuvent résulter aussi bien d'une équivalence combinatoire que d'une projection différente).

Une tresse est isotope à une autre où, dans la projection régulière, tous les brins se croisent à des hauteurs différentes. Le groupe $B(A_n)$ des tresses à n brins est donc engendré par les générateurs σ_i : 

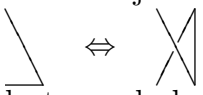
qui croisent le i-ième et $(i+1)$-ième brins. On a les relations: $\sigma_i\sigma_j = \sigma_j\sigma_i$ si $|i-j| > 1$ 

et

$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ 

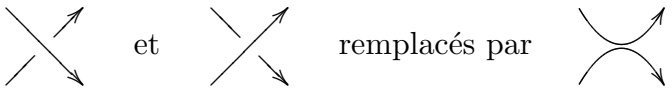
. Ces relations sont les seules, car le mouvement de Reidemeister de type III est équivalent à la seconde relation, et le mouvement de Reidemeister de type II est équivalent à la relation $\sigma_i\sigma_i^{-1} = 1$. On a des plongements naturels $B(A_{n-1}) \subset B(A_n)$ (en "rajoutant un brin").

11. Tresses et entrelacs.

Un *entrelacs orienté* est un plongement orienté $(S_1)^n \hookrightarrow \mathbb{R}^3$ à isotopie ambiante près (ce qui revient, si $x = \{x_1, \ldots, x_n\} \in \mathbb{C}^n$, à une application $f : x \times I \to \mathbb{R}^3$ telle que $f(x,0) = f(x,1)$; l'orientation se réfère au sens de parcours de 0 à 1). L'entrelacs est un noeud si $n = 1$. On s'intéresse aux entrelacs PL (il existe des entrelacs "sauvages" qui ne sont isotopes à aucun entrelacs PL). Cette fois pour l'équivalence des entrelacs il faut rajouter sur les projections régulières les mouvements de Reidemeister de type I:  . À une tresse, on associe un entrelacs, sa *fermeture*, obtenue en "repliant la tresse le long d'un cylindre" jusqu'à identifier $g(x,0)$ et $g(x,1)$. Il est clair que deux éléments conjugués de $B(A_n)$ ont même fermeture, et que si $g \in B(A_{n-1}) \subset B(A_n)$ alors g, $g\sigma_n$ et $g\sigma_n^{-1}$ ont même fermeture. Les deux théorèmes qui permettent de ramener la classification des entrelacs à une question sur les tresses sont:

11.1. Théorème (Alexander). *Tout entrelacs orienté est la fermeture d'une tresse.*

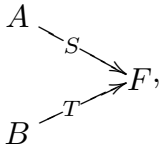
Preuve: Nous suivons une preuve due à P.Vogel, "Representation of links by braids: a new algorithm", *Comm. Math. Helv.* **65** (1990), 104–113. À la projection régulière d'un entrelacs, on associe son *diagramme de Seifert*, union de ses *cercles de Seifert* (topologiques) disjoints en remplaçant chaque croisement de la projection comme suit:



Au diagramme de Seifert, on associe un arbre orienté dont les sommets sont les faces du diagramme (les composantes connexes du complémentaire dans le plan du diagramme) et un arête va du sommet A au sommet B s'il existe un cercle tel que A soit immédiatement à gauche et B immédiatement à droite: 

. On dit qu'un arbre orienté est *une chaîne* si c'est une suite d'arcs orientés mis bout à bout. L'algorithme de Vogel repose sur le

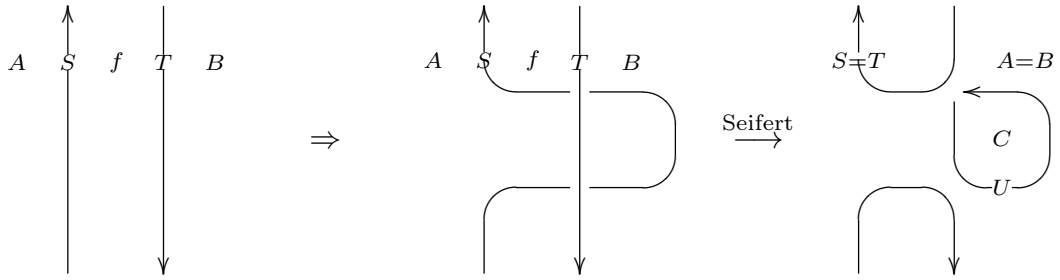
11.2. Lemme. *Si l'arbre décrit ci-dessus n'est pas une chaîne, il existe une face f de la projection régulière et deux arcs α et β bordant cette face de même orientation et appartenant à des cercles de Seifert différents.*

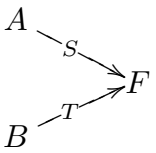
PREUVE: Puisque l'arbre n'est pas une chaîne, quitte à renverser toutes les orientations, on peut supposer qu'il contient un sommet sur lequel deux arêtes aboutissent: 

c'est-à-dire dans le diagramme de Seifert 

(deux cercles distincts S et T de même orientation bordant la face F). Le bord de la face F contient donc au moins deux cercles S, T de même orientation. Soient $f_1, \ldots, f_k$ les faces de la projection régulière dont F est l'union. En regardant au voisinage d'une intersection, on voit que chaque f_i contient dans son bord au moins un cercle de Seifert de chaque orientation. Si le lemme est faux, elle contient exactement un cercle de chaque orientation dans son bord. En regardant au voisinage de chaque intersection on voit que ces cercles sont les mêmes dans chaque f_i, ce qui impliquerait que F ne contient qu'un cercle de chaque orientation, une contradiction. ■

L'algorithme utilise alors le fait que si l'arbre est une chaîne le diagramme de Seifert est homotope à un ensemble de cercles concentriques de même orientation, et l'entrelacs est naturellement tressé autour du cercle le plus intérieur. Sinon, sur une face de la projection régulière répondant aux conditions du lemme, on pratique un mouvement de Reidemeister de type II:



On remplace ainsi le sous-arbre 

par $C \xrightarrow{U} A = B \xrightarrow{S=T} F$. Ceci amène éventuellement l'arbre à être linéaire; il suffit de vérifier qu'un invariant approprié augmente à chaque opération, par exemple le nombre de sous-chaînes. ■

11.3. THÉORÈME (MARKOV). *Soit $B_\infty = \coprod_{n\geq 0} B(A_n)$. Les classes d'isotopies d'entrelacs orientés obtenus par fermeture d'éléments de B_∞ sont en bijection avec les classes d'équivalence pour la relation sur B_∞ clôture transitive de: $g \sim g'$ si $g, g' \in B(A_n)$ et y sont conjuguées ou $g \in B(A_{n-1}), g' \in B(A_n)$ et $g' = g\sigma_n$ ou $g' = g\sigma_n^{-1}$.*

PREUVE: Il est possible de démontrer ce théorème en analysant plus en détail la preuve du précédent. Mais la démonstration est longue, nous ne la ferons pas ici. ■

Nous allons maintenant présenter les résultats de Jones sur les invariants des noeuds. Pour plus de détails, voir V.F.R.Jones, "Hecke algebra representations of braid groups and link polynomials", *Ann. of Math.* **126** (1987) 335–388. Fixons un corps k et des indéterminées q', q'' et posons $H_n = \mathcal{H}_{q',q''}(W(A_n), k(q', q''))$; H_n est un quotient de l'algèbre du groupe $B(A_n)$, donc fournit une représentation de ce groupe. On note h cette représentation, et on pose $T_n = h(\sigma_n)$. On appelle *trace de Markov* une collection de fonctions centrales $\tau_n : H_n \to k(q', q'')$ telles que pour $T \in H_{n-1}$ on ait $\tau_n(TT_n) = \tau_n(TT_n^{-1}) = \tau_{n-1}(T)$. D'après le théorème de Markov, si τ est une trace de Markov, alors la fonction qui à $g \in B(A_n)$, tresse dont la fermeture est un entrelacs e, associe $\tau_n(h(g))$ est un invariant d'isotopie de e. Posons $P = q'q''$ et $S = q' + q''$. Alors on a:

11.4. Théorème (Jones). *Il existe une unique trace de Markov telle que $\tau_0(1) = 1$. Ses valeurs sur un élément de la forme $h(b)$, où $b \in B(A_n)$, sont des polynômes de Laurent en S et P.*

Preuve: On utilise le fait qu'il n'existe que deux éléments $W(A_{n-1})$-réduits-$W(A_{n-1})$ dans $W(A_n)$, à savoir s_n et 1. Pour le voir, on calcule le cardinal de la double classe $|W(A_{n-1})s_nW(A_{n-1})| = |W(A_{n-1})|^2/|W(A_{n-1}) \cap {}^{s_n}W(A_{n-1})| = n.n!$, cette dernière égalité car $W(A_{n-1}) \cap {}^{s_n}W(A_{n-1}) = W(A_{n-2})$— en effet une permutation de $\mathfrak{S}_n$ qui n'a pas n dans son support est dans l'intersection; si elle a n dans son support elle est envoyée par conjugaison par s_n sur une permutation qui a $n+1$ dans son support, donc qui n'est pas dans $W(A_{n-1})$. On en déduit un isomorphisme $H_{n+1} \simeq H_n \oplus (H_n \otimes_{H_{n-1}} H_n)$ donné par $a \oplus (b \otimes c) \mapsto a + bT_{n+1}c$. En effet il est clair que cette application est surjective et un calcul de dimension basé sur le calcul de cardinal ci-dessus montre qu'elle est injective. On en déduit une construction récursive de τ_n: si τ_n est déjà définie, on définit τ_{n+1} sur H_{n+1} par $\tau_{n+1}(a + bT_{n+1}c) = \frac{1+P}{S}\tau_n(a) + \tau_n(bc)$ pour $a, b, c \in H_n$. Il faut voir que l'on a $\tau_{n+1}(TT_{n+1}^{-1}) = \tau_n(T)$ pour $T \in H_n$ et $\tau_{n+1}(AB) = \tau_{n+1}(BA)$. La première égalité résulte de $T_{n+1}^{-1} = (S - T_{n+1})/P$. Pour voir la seconde égalité, il suffit de considérer le cas d'un A de la forme T_i et B de la forme x ou $xT_{n+1}y$ où $x, y \in H_n$. Le seul cas qui n'est pas une conséquence triviale des propriétés de τ_n est $\tau_{n+1}(xT_{n+1}yT_{n+1}) = \tau_{n+1}(T_{n+1}xT_{n+1}y)$ (pour $i = n+1$). En utilisant à son tour $H_n = H_{n-1} \oplus H_{n-1} \otimes_{H_{n-2}} H_{n-1}$ on peut supposer x de la forme a ou aT_nb et y de la forme c ou cT_nd où $a, b, c, d \in H_{n-1}$. Le cas $x = a$, $y = c$ est trivial puisque T_{n+1} commute avec H_{n-1}. Si $x = aT_nb$, $y = c$ on trouve

$$\begin{aligned}\tau_{n+1}(aT_nbT_{n+1}yT_{n+1}) &= \tau_{n+1}(aT_nT_{n+1}^2by) = \tau_{n+1}(aT_n(ST_{n+1} - P)by)\\ &= S\tau_n(aT_nby) + \frac{-P(1+P)}{S}\tau_n(aT_nby) = S\tau_n(aT_nby) + \frac{-P(1+P)}{S}\tau_{n-1}(aby)\\ &= S\tau_n(aT_nby) - P\tau_n(aby) = \tau_n(aT_n^2by) = \tau_{n+1}(aT_nT_{n+1}T_nby)\\ &= \tau_{n+1}(aT_{n+1}T_nT_{n+1}by) = \tau_n(T_{n+1}aT_nbT_{n+1}y).\end{aligned}$$

On traite symétriquement le cas $x = a$, $y = cT_nd$. Enfin si $x = aT_nb$ et $y = cT_nd$ on trouve

$$\begin{aligned}\tau_{n+1}(aT_nbT_{n+1}cT_ndT_{n+1}) &= \tau_{n+1}(aT_nbcT_{n+1}T_nT_{n+1}d) = \tau_{n+1}(aT_nbcT_nT_{n+1}T_nd)\\ &= \tau_n(aT_nbcT_n^2d) = S\tau_n(aT_nbcT_nd) - P\tau_{n-1}(abcd)\\ &= S\tau_n(aT_nbcT_nd) - P\tau_{n-1}(abcT_nd) = \tau_n(aT_n^2bcT_nd)\\ &= \tau_{n+1}(aT_nT_{n+1}T_nbcT_nd) = \tau_{n+1}(aT_{n+1}T_nT_{n+1}bcT_nd) = \tau_{n+1}(T_{n+1}aT_nbT_{n+1}cT_nd)\end{aligned}$$

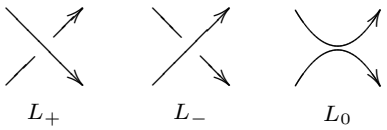
q.e.d. ■

On obtient un invariant défini pour toute spécialisation telle que S et P soient inversibles. Pour avoir le polynôme HOMFLY $P_b(t,x)$ comme il est donné dans la littérature, il faut faire dans $\tau_n(h(b))$ le changement de variables $P=-t^2$, $S=tx$.

11.5. Exemple. Le noeud de trèfle  est la fermeture de la tresse σ_1^3 de $B(A_1)$.

On trouve $\tau_1(h(\sigma_1^3))=\tau_1(T_1^3)=\tau_1((ST_1-P)T_1)=\tau_1((S^2-P)T_1-SP)=\tau_0(S^2-P)-\frac{1+P}{S}\tau_0(SP)=S^2-2P-P^2=t^2x^2+2t^2-t^4$.

Le polynôme HOMFLY vérifie une "skein relation" qui permet de le définir aussi par récurrence: soient 3 entrelacs L_+, L_- et L_0 dont les projections régulières ne diffèrent qu'en un croisement comme suit:



11.6. Proposition. *Dans la situation ci-dessus, on a* $t^{-1}P_{L_+}-tP_{L_-}=xP_{L_0}$.

Preuve: Il existe n,i et $a,b\in B(A_n)$ tels que L_+, L_- et L_0 soient respectivement la clôture des tresses $a\sigma_i b$, $a\sigma_i^{-1}b$ et ab. La trace de Markov étant une fonction centrale, il suffit donc de vérifier que $\tau_n(cT_i^2)-t^2\tau_n(c)=xt\tau_n(cT_i)$ (en prenant $c=h(ba\sigma_i^{-1})$), ce qui est un calcul immédiat. ■

Mentionnons deux autres invariants découverts antérieurement et qui sont cas particuliers du polynôme HOMFLY: le *polynôme d'Alexander* obtenu pour la spécialisation $q'=t^{1/2}$, $q''=-t^{-1/2}$, et le *polynôme de Jones* obtenu pour la spécialisation $q'=t^{-1/2}$, $q''=-t^{-3/2}$.

12. 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 $N_G(T)/T$. On appelle sous-groupes de Borel les conjugués de B, sous-groupes paraboliques les sous-groupes contenant un sous-groupe de Borel, et tores les conjugués de T.

12.1 Proposition.

(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 $g\in P_I$. En particulier deux sous-groupes paraboliques différents contenant B ne sont pas conjugués, et les sous-groupes paraboliques sont leur propre normalisateur.

(iii) L'intersection de deux sous-groupes de Borel contient toujours un tore.

Preuve: Soit P un groupe contenant B et soit $w\in W$ tel que $BwB\subset P$. Alors $BwBw^{-1}B\subset B$ donc par 5.5 (iv), on a $\dot t\subset P$ pour tout $t\in R(w)$, où on a noté $\dot t$ un représentant de t dans $N_G(T)$. Si $s_1\dots s_k$ est une décomposition réduite de W, on

a donc $\dot{s}_k \in P, \dot{s}_k\dot{s}_{k-1}\dot{s}_k \in P, \ldots$ d'où $\dot{s}_i \in P$ pour tout i; finalement $P \supset BW_IB$ où $I = \{s_1, \ldots, s_k\}$; d'où (i).

Démontrons (ii). Soit $w \in W$ tel que $g \in BwB$. Alors $B^gBB = BwBw^{-1}B \subset P_I$ d'où par le raisonnement ci-dessus $w \in W_I$ donc $g \in P_I$.

Enfin (iii) vient de ce que tout couple de sous-groupes de Borel est conjugué à un couple de la forme $(B, {}^wB)$ où $w \in W$. ■

12.2 Lemme-Définition. *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_IwW_J.

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

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

Preuve: 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 $x^{-1}w' = wy$, d'où en utilisant les définitions de I-réduit et réduit-J et $l(y^{-1}) = l(y)$, $l(x^{-1}) = l(x)$ on obtient $l(w')+l(y) = l(x)+l(w)$ et $l(x)+l(w') = l(w)+l(y)$, d'où le résultat.

Montrons maintenant (ii)⇒(iii). Soit w vérifiant (ii); Il suffit de montrer qu'un élément $v \in W_IwW_J$ qui est réduit-J vérifie (iii) avec $y = 1$. Soit xwy une écriture de v où on a choisi $l(x) + l(y)$ minimal. Comme dans 1.5, 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 $\hat{x} = x$ et $\hat{y} = y$ vu l'hypothèse de minimalité de $l(x)+l(y)$, et on a donc $l(x)+l(w)+l(y) = l(xwy)$; on a donc $y = 1$ puisque xwy est l'élément de longueur minimum de $xwyW_J$.

Enfin on a clairement (iii)⇒ (i). ■

Attention! Il est à noter que toute écriture xwy ne satisfait pas (iii) (la situation est moins bonne de ce point de vue que dans le cas I-réduit).

12.3 Lemme. *On a $P_I\backslash G/P_J \simeq W_I\backslash W/W_I \simeq \{$Élements de W qui sont I-réduits-$J\}$ par les applications naturelles entre ces ensembles.*

Preuve: Considérons une double classe P_IgP_J. D'après la décomposition de Bruhat, on a $g \in BwB$ pour un certain $w \in W$, et donc $P_IgP_J = P_IwP_J$. Comme les représentants de W_I et W_J sont respectivement dans P_I et P_J, on a finalement $P_IgP_J = P_IW_IwW_JP_J$, d'où une application bien définie surjective de $W_I\backslash W/W_J$ sur $P_I\backslash G/P_J$. Elle est injective: supposons $P_IwP_J = P_Iw'P_J$, c'est-à-dire $BW_IBwBW_JB = BW_IBw'BW_JB$, où w et w' ont été choisis I-réduits-J. Par 5.1(iii) et un raisonnement analogue à la preuve de 12.2(iii) on obtient que pour tout $x \in W_I$ et $y \in W_J$, $BxBwByB$ est union de $B\hat{x}w\hat{y}B$ où $l(\hat{x}w\hat{y}) = l(\hat{x})+l(w)+l(\hat{y})$ d'où $BW_IBwBW_JB \subset BW_IwW_JB$, et de même avec w', d'où l'égalité des doubles classes W_IwW_J et $W_Iw'W_J$. La deuxième bijection de l'énoncé est le lemme 12.2. ■

13. Sous-groupes de Levi, parties closes et quasi-closes.

On appelle *isogénie* un morphisme surjectif de groupes algébriques, de noyau fini. Nous reprenons les hypothèses de 4.1: $\mathbf{G}$ est un groupe algébrique réductif, et $\mathbf{T}$ un tore maximal de $\mathbf{G}$. On appelle p-morphisme (où $p = \operatorname{car} k$) un endomorphisme de $X(\mathbf{T})$ vérifiant $f(\alpha) = q_\alpha \tau(\alpha)$ et $f^*(\check{\alpha}) = q_{\tau^{-1}(\alpha)}\tau^{-1}(\check{\alpha})$ où q_α est une puissance de p ($q_\alpha = 1$ si k est de caractéristique 0) et où τ est une permutation des racines. Nous aurons besoin du rappel supplémentaire suivant:

13.1 Théorème. *Toute isogénie $\phi : \mathbf{G} \to \mathbf{G}$ stabilisant $\mathbf{T}$ induit un p-morphisme sur $X(\mathbf{T})$ (par la formule $\phi(x_\alpha(\xi)) = x_{\tau(\alpha)}(\xi^{q_\alpha})$ si x_α est le sous-groupe à un paramètre d'image $\mathbf{U}_\alpha$). Réciproquement, tout p-morphisme sur $X(\mathbf{T})$ est induit par une isogénie (déterminée uniquement à conjugaison par $\mathbf{T}$ près).*

Preuve: Voir par exemple [Springer, 11.4.9]. ■

Nous avons besoin de quelques rappels supplémentaires sur les systèmes de racines. Si $I \subset \Pi$, on note $\Phi_I = \Phi \cap <I>$; c'est le système de racines de W_I (où on a noté W_I pour $W_{\{s_\alpha\}_{\alpha\in I}}$), et I est une base de Φ_I. On dit que $\Psi \subset \Phi$ est *clos* si $\mathbb{N}\Psi \cap \Phi = \Psi$ (c'est équivalent à $\alpha, \beta \in \Psi, \alpha + \beta \in \Phi \Rightarrow \alpha + \beta \in \Psi$; l'intersection de deux parties closes est clairement close). On dit que Ψ est *symétrique* si $\Psi = -\Psi$, donc Ψ est clos et symétrique si $\mathbb{Z}\Psi \cap \Phi = \Psi$. Par [Bourbaki, VI 1.8 prop.23] si Ψ est clos et symétrique c'est un système de racines pour le sous-groupe W_Ψ de W engendré par les réflexions par rapport aux racines de Ψ. Il est clair que Φ_I est clos et symétrique, et que $\Phi^+ - \Phi_I$ et $\Phi^+ \cup \Phi_I$ sont clos. Par [Bourbaki, VI 1.7 prop. 22] si Ψ est clos et $\Psi \cap -\Psi = \emptyset$, alors il existe un ordre sur Φ tel que $\Psi \supset \Phi^+$. On dit que Ψ est parabolique si Ψ est clos et $\Psi \cup -\Psi = \Phi$; alors par [Bourbaki VI 1.7 prop.20] il existe un ordre sur Φ tel que $\Psi \supset \Phi^+$, et Ψ est de la forme $\Phi^+ \cup \Phi_I$ pour un certain I (en particulier le complémentaire d'une partie parabolique est clos).

Si $\Psi \subset \Phi$ on pose $\mathbf{G}^*_\Psi = <\mathbf{U}_\alpha \mid \alpha \in \Psi>$ et $\mathbf{G}_\Psi = <\mathbf{T}, \mathbf{U}_\alpha \mid \alpha \in \Psi>$. Par 4.1(i), tout sous-groupe fermé connexe contenant $\mathbf{T}$ est de la forme $\mathbf{G}_\Psi$.

13.2. Définition. *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 un tore, donc tout $\mathbf{U}_\alpha$ est dans le noyau de ce quotient, donc dans $\mathbf{G}^*_\Psi$. Il est clair que l'intersection de deux parties quasi-closes est quasi-close, car $(\mathbf{G}_\Psi \cap \mathbf{G}_{\Psi'})^0 = \mathbf{G}_{\Psi\cap\Psi'}$.

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 $\mathbf{P} = R_u(\mathbf{P}) \rtimes \mathbf{L}$ ($\mathbf{L}$ est donc réductif).

13.3. Proposition. *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 $\mathbf{G}^*_{\Psi_u} = R_u(\mathbf{G}_\Psi)$).*

Preuve: 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 13.1).

Montrons maintenant que $\mathbf{G}_{\Psi_s} \cap R_u(\mathbf{G}_\Psi) = 1$. Cette intersection étant normalisée par $\mathbf{T}$ et unipotente, est le produit des $\mathbf{U}_\alpha$ qu'il contient. Mais pour un tel α, comme $\mathbf{U}_{-\alpha} \in \mathbf{G}_\Psi$, le groupe $\mathbf{U}_{-\alpha}$ normalise $R_u(\mathbf{G}_\Psi)$ donc $[\mathbf{U}_{-\alpha}, \mathbf{U}_\alpha] \subset R_u(\mathbf{G}_\psi)$ ce qui est absurde car cet ensemble contient des éléments non unipotents.

Étant unipotent normalisé par $\mathbf{T}$, le groupe $R_u(\mathbf{G}_\Psi)$ est de la forme $\mathbf{G}^*_{\Psi'}$ pour une certaine partie $\Psi' \subset \Psi$. On vient de voir que $\Psi' \subset \Psi_u$. Réciproquement si $\alpha \notin \Psi'$ pour $\alpha \in \Psi$ alors $\mathbf{U}_\alpha \cap R_u(\mathbf{G}_\Psi) = 1$ car cette intersection est normalisée par $\mathbf{T}$ et ne contient aucun $\mathbf{U}_\beta$. Donc $\mathbf{U}_\alpha$ s'envoie injectivement sur un groupe radiciel du groupe $\mathbf{G}_\Psi/R_u(\mathbf{G}_\Psi)$; 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 unipotente donc produit des $\mathbf{U}_\beta$ qu'elle contient et $\mathbf{U}_{-\alpha}$ doit être l'un d'entre eux). Donc $\alpha \in \Psi_s$. En fin de compte on a bien $\Psi' = \Psi_u$ ce qui montre aussi que Ψ_u est quasi-clos; et $\mathbf{G}_{\Psi_s}$ est un complément de Levi de $R_u(\mathbf{G}_\Psi)$.

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

Preuve: Soit $\Psi \subset \Phi$ close et définissons Ψ_s et Ψ_u comme dans la preuve de 13.3. 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 $\Psi_u \subset \Phi^+$. Par 4.1 (iii) il est alors clair que $\prod_{\alpha\in\Psi_u} \mathbf{U}_\alpha$ est un groupe (donc égal à $\mathbf{G}^*_{\Psi_u}$ et Ψ_u est quasi-clos). 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 $\mathbf{G}_{\Psi_s}$.

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; en effet $<\mathbf{U}_\alpha, \mathbf{U}_{-\alpha}>$ 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 4.1(ii). Montrons maintenant que $\mathbf{G}_{\Psi_s} = \mathbf{U}_{\Psi_s^+} W_{\Psi_s} \mathbf{T} \mathbf{U}_{\Psi_s^+}$. Pour cela, il suffit de voir que le membre de droite est un groupe; il faut voir qu'il est stable par translation à gauche par un élément de $\mathbf{T}$ (clair), par un $\mathbf{U}_\alpha$ où $\alpha \in \Psi^+$ est simple (clair) et par un élément de $\mathbf{U}_{-\alpha}$ où $\alpha \in \Psi_s^+$ est simple. Ce dernier point demande un calcul. Puisque α est simple par 4.1(iii) $\mathbf{U}_{-\alpha}$ 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 dans $<\mathbf{U}_\alpha, \mathbf{U}_{-\alpha}>$ montre que $\mathbf{U}_{-\alpha}\mathbf{U}_\alpha \subset \mathbf{U}_\alpha \mathbf{T} \cup \mathbf{U}_\alpha s_\alpha \mathbf{T} \mathbf{U}_\alpha$. On a $\mathbf{U}_\alpha \mathbf{T} W_{\Psi_s} \mathbf{T} \mathbf{U}_{\Psi_s^+} = \mathbf{U}_\alpha W_{\Psi_s} \mathbf{T} \mathbf{U}_{\Psi_s^+}$ donc il nous suffit d'étudier $\mathbf{U}_\alpha s_\alpha \mathbf{T} \mathbf{U}_\alpha W_{\Psi_s} \mathbf{T} \mathbf{U}_{\Psi_s^+} = \mathbf{U}_\alpha s_\alpha \mathbf{U}_\alpha W_{\Psi_s} \mathbf{T} \mathbf{U}_{\Psi_s^+}$. Pour $w \in W_{\Psi_s}$ on a $\mathbf{U}_\alpha s_\alpha \mathbf{U}_\alpha w \mathbf{T} \mathbf{U}_{\Psi_s^+} = \mathbf{U}_\alpha s_\alpha w \mathbf{T} \mathbf{U}_{w^{-1}(\alpha)} \mathbf{U}_{\Psi_s^+}$; si $w^{-1}(\alpha) \in \Psi^+$ alors $\mathbf{U}_\alpha s_\alpha w \mathbf{T} \mathbf{U}_{w^{-1}(\alpha)} \mathbf{U}_{\Psi_s^+} = \mathbf{U}_\alpha s_\alpha w \mathbf{T} \mathbf{U}_{\Psi_s^+}$ c.q.f.d. Sinon, $w^{-1}(\alpha) = -\beta \in \Psi^-$ et

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

enfin $\mathbf{U}_\alpha s_\alpha w \mathbf{T} \mathbf{U}_\beta s_\beta \mathbf{U}_{\Psi_s^+} = \mathbf{U}_\alpha s_\alpha \mathbf{U}_{-\alpha} w s_\beta \mathbf{T} \mathbf{U}_{\Psi_s^+} = \mathbf{U}_\alpha s_\alpha w s_\beta \mathbf{T} \mathbf{U}_{\Psi_s^+}$.

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 pour $w \in W_{\Psi_s}$ on a $\mathbf{U}_{\Psi_s^+} w \mathbf{T} \mathbf{U}_{\Psi_s^+} \subset \mathbf{U} w \mathbf{T} \mathbf{U}$ la décomposition de Bruhat de $\mathbf{G}$ montre qu'on doit avoir $\mathbf{U}_\gamma \subset \mathbf{T} \mathbf{U}_{\Psi_s^+}$. La propriété 4.1 (iv) montre alors que l'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 $\alpha \notin \Psi$ et $\mathbf{U}_\alpha \subset \mathbf{G}_\Psi$ alors $\mathbf{U}_\alpha$ s'envoie isomorphiquement dans le quotient $\mathbf{G}_{\Psi_s}$ donc par ce qui précède $\alpha \in \Psi_s$, une contradiction. ■

REMARQUE. Sauf en caractéristique 2 ou 3 la réciproque de 13.4 a lieu: une partie quasi-close est close.

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

PREUVE: C'est une conséquence immédiate de 13.3 si nous montrons que $\mathbf{P}_I = \mathbf{G}_\Psi$ où $\Psi = \Phi^+ \cup \Phi_I$. Mais c'est clair car $\mathbf{P}_I$ est engendré par W_I et $\mathbf{B}$, et s_α pour $\alpha \in I$ est dans le groupe engendré par $\mathbf{U}_\alpha$ et $\mathbf{U}_{-\alpha}$. ■

13.6. PROPOSITION. *Soit $\mathbf{P}$ un sous-groupe parabolique de $\mathbf{G}$. Il y a un unique sous-groupe de Levi de $\mathbf{P}$ contenant un tore maximal de $\mathbf{P}$. Deux sous-groupes de Levi de $\mathbf{P}$ sont conjugués par un unique élément de $R_u(\mathbf{P})$.*

PREUVE: Soit $\mathbf{T}$ un tore maximal de $\mathbf{P}$, et $\mathbf{B}$ un sous-groupe de Borel de $\mathbf{P}$ le contenant. Alors, puisque $\mathbf{P}$ contient un sous-groupe de Borel de $\mathbf{G}$, $\mathbf{B}$ en est un, et $\mathbf{P}$ est de la forme $\mathbf{P}_I$ pour ce Borel et $\mathbf{L}_I$ contient $\mathbf{T}$. 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 $R_u(\mathbf{P})$, il ne contient que des $\mathbf{U}_\alpha$ qui sont dans $\mathbf{L}_I$, 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 $R_u(\mathbf{P})$. L'unicité de l'élément qui les conjugue équivaut à $R_u(\mathbf{P}) \cap N_\mathbf{G}(\mathbf{L}) = 1$; ceci résulte de ce que si $v \in R_u(\mathbf{P}) \cap N_\mathbf{G}(\mathbf{L})$ alors pour tout $l \in \mathbf{L}$ on a $[v, l] \in R_u(\mathbf{P}) \cap \mathbf{L} = 1$; donc $v \in C_\mathbf{G}(\mathbf{L})$. Mais $C_\mathbf{G}(\mathbf{L}) \subset \mathbf{L}$ (par ex. puisque par 4.1 (ii) on a $C_\mathbf{G}(\mathbf{T}) = \mathbf{T}$) d'où $v \in \mathbf{L} \cap R_u(\mathbf{P}) = 1$. ■

13.7. PROPOSITION. *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 $\mathbf{U}_{-\alpha} \subset \mathbf{P}$.*

PREUVE: 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 $\Psi \cup -\Psi = \Phi$. Montrons que $\mathbf{P}^0$ contient un sous-groupe de Borel. Soit $\mathbf{B}$ un sous-groupe de Borel de $\mathbf{G}$ contenant $\mathbf{T}\mathbf{G}^*_{\Psi_u}$ et soit $\mathbf{U}_\alpha \subset \mathbf{B}$. Il suffit de voir que $\alpha \in \Psi$. Si $\alpha \notin \Psi$, alors $-\alpha \in \Psi_u$ d'où $\mathbf{U}_{-\alpha} \subset \mathbf{G}^*_{\Psi_u} \subset \mathbf{B}$ ce qui est absurde car un sous-groupe de Borel ne contient pas deux sous-groupes radiciels correspondant à des racines opposées. Donc $\mathbf{P}^0$ est parabolique, et par 12.1(ii) on a $N_\mathbf{G}(\mathbf{P}^0) = \mathbf{P}^0$ ce qui implique $\mathbf{P} = \mathbf{P}^0$. ■

13.8 PROPOSITION. *Soient $\mathbf{P}$ et $\mathbf{Q}$ deux sous-groupes paraboliques de $\mathbf{G}$ de radicaux unipotents respectifs $\mathbf{U}$ et $\mathbf{V}$, et soient $\mathbf{L}$ et $\mathbf{M}$ des sous-groupes de Levi respectifs de $\mathbf{P}$ et $\mathbf{Q}$ contenant un même tore maximal $\mathbf{T}$ de $\mathbf{G}$; alors*

(i) Le groupe $(\mathbf{P} \cap \mathbf{Q}).\mathbf{U}$ est un sous-groupe parabolique de $\mathbf{G}$ inclus dans $\mathbf{P}$ ayant même intersection que $\mathbf{Q}$ avec $\mathbf{L}$ et dont $\mathbf{L} \cap \mathbf{M}$ est un sous-groupe de Levi.

(ii) $\mathbf{P} \cap \mathbf{Q}$ est connexe ainsi que $\mathbf{L} \cap \mathbf{M}$ et on a la décomposition de Levi $\mathbf{P} \cap \mathbf{Q} = (\mathbf{L} \cap \mathbf{M}) \rtimes ((\mathbf{L} \cap \mathbf{V}).(\mathbf{M} \cap \mathbf{U}).(\mathbf{U} \cap \mathbf{V}))$; c'est une décomposition comme produit de 4

variétés (la décomposition correspondante d'un élément de $\mathbf{P} \cap \mathbf{Q}$ *suivant ce produit est unique).*

PREUVE: 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 $\mathbf{Q} = \mathbf{G}_{\Psi''}$). Montrons que pour tout $\alpha \subset \Phi$, soit $\mathbf{U}_\alpha$ soit $\mathbf{U}_{-\alpha}$ est inclus dans le groupe $(\mathbf{P} \cap \mathbf{Q}).\mathbf{U}$ (c'est un groupe car $\mathbf{P}$ normalise $\mathbf{U}$). Si $\mathbf{U}_\alpha$ n'est pas dans $\mathbf{U}$, alors $\mathbf{U}_\alpha$ et $\mathbf{U}_{-\alpha}$ sont tous les deux dans $\mathbf{L}$. Comme l'un des deux est dans $\mathbf{Q}$, l'un des deux est dans $\mathbf{L} \cap \mathbf{Q}$, donc dans $(\mathbf{P} \cap \mathbf{Q}).\mathbf{U}$. La proposition 13.7 montre alors que $(\mathbf{P} \cap \mathbf{Q}).\mathbf{U}$ est un sous-groupe parabolique de $\mathbf{G}$, d'où la première assertion de (i). En particulier $(\mathbf{P} \cap \mathbf{Q}).\mathbf{U}$ est connexe, et donc égal à $\mathbf{G}_{(\Psi' \cap \Psi'') \cup \Psi'_u}$ (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 13.4). Maintenant, $\Psi'_u - \Psi''$ est clos comme intersection de deux parties closes (Ψ'_u et le complémentaire de Ψ''), donc on a $(\mathbf{P} \cap \mathbf{Q}).\mathbf{U} = (\mathbf{P} \cap \mathbf{Q}).\mathbf{G}^*_{\Psi'_u - \Psi''}$. 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 $\mathbf{P} \cap \mathbf{Q}$ l'est et est égal à $\mathbf{G}_{\Psi' \cap \Psi''}$. Les groupes $(\mathbf{P} \cap \mathbf{Q}).\mathbf{U}$ et $\mathbf{P} \cap \mathbf{Q}$ admettent tous deux pour groupe de Levi $(\mathbf{L} \cap \mathbf{M})^0$ 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 $-\alpha \notin (\Psi' \cap \Psi'') \cup \Psi'_u$).

Montrons (ii). Soit $\alpha \in \Psi' \cap \Psi''$. Examinons les diverses possibilités pour $-\alpha$:

- $-\alpha$ n'est ni dans Ψ' ni dans Ψ''. Dans ce cas $\mathbf{U}_\alpha$ est dans $\mathbf{U} \cap \mathbf{V}$.
- $-\alpha$ est dans $\Psi' - \Psi''$ (resp. dans $\Psi'' - \Psi'$). Alors $\mathbf{U}_\alpha$ est dans $\mathbf{L} \cap \mathbf{V}$ (resp. $\mathbf{M} \cap \mathbf{U}$).
- $-\alpha \in \Psi' \cap \Psi''$. Alors $\mathbf{U}_\alpha$ est dans $\mathbf{L} \cap \mathbf{M}$.

On voit donc que $\mathbf{P} \cap \mathbf{Q} = <\mathbf{U} \cap \mathbf{V}, \mathbf{L} \cap \mathbf{V}, \mathbf{M} \cap \mathbf{U}, \mathbf{L} \cap \mathbf{M}>$. Or $\mathbf{U} \cap \mathbf{V}$ est normal dans $\mathbf{P} \cap \mathbf{Q}$. De même, $\mathbf{L} \cap \mathbf{M}$ normalise $\mathbf{L} \cap \mathbf{V}$ et $\mathbf{M} \cap \mathbf{U}$. Donc

$$\mathbf{P} \cap \mathbf{Q} = (\mathbf{L} \cap \mathbf{M}).<\mathbf{L} \cap \mathbf{V}, \mathbf{M} \cap \mathbf{U}>.(\mathbf{U} \cap \mathbf{V}).$$

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

$$\mathbf{P} \cap \mathbf{Q} = (\mathbf{L} \cap \mathbf{M}).(\mathbf{L} \cap \mathbf{V}).(\mathbf{M} \cap \mathbf{U}).(\mathbf{U} \cap \mathbf{V}),$$

Supposons maintenant que $x = l_{\mathbf{M}} l_{\mathbf{V}} m_{\mathbf{U}} u_V \in \mathbf{P} \cap \mathbf{Q}$, où $l_{\mathbf{M}} \in \mathbf{L} \cap \mathbf{M}$, $l_{\mathbf{V}} \in \mathbf{L} \cap \mathbf{V}$, *etc.*... Alors $l_{\mathbf{M}} l_{\mathbf{V}}$ est l'image de x par la projection $\mathbf{P} \to \mathbf{L}$ et $l_{\mathbf{M}}$ (resp. $m_{\mathbf{U}}$) est l'image de $l_{\mathbf{M}} l_{\mathbf{V}}$ (resp. $m_{\mathbf{U}} u_{\mathbf{V}}$) par le morphisme $\mathbf{Q} \to \mathbf{M}$. Donc la décomposition de x est unique, et l'application produit $(\mathbf{L} \cap \mathbf{M}) \times (\mathbf{L} \cap \mathbf{V}) \times (\mathbf{M} \cap \mathbf{U}) \times (\mathbf{U} \cap \mathbf{V}) \to \mathbf{P} \cap \mathbf{Q}$ est un isomorphisme de variétés; et les 4 termes sont connexes puisque le produit l'est donc $\mathbf{L} \cap \mathbf{M}$ est bien connexe. ■

14. $\mathbb{F}_q$-structures et endomorphisme de Frobenius.

14.1. DÉFINITION.

Une variété algébrique $\mathbf{V}$ *sur* $\overline{\mathbb{F}}_q$ *est dite définie sur* $\mathbb{F}_q$*, ou munie d'une* $\mathbb{F}_q$*-structure* $\mathbf{V}_0$*, s'il existe une variété* $\mathbf{V}_0$ *sur* $\mathbf{F}_q$ *telle que* $\mathbf{V} = \mathbf{V}_0 \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$*. 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* $\mathbf{V}_0$ *qui élève les fonctions sur* $\mathbf{V}_0$ *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.*

Explicitons ces définitions en termes d'anneaux des fonctions pour une variété affine ou projective. Une variété affine (resp. projective) sur un corps 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 variété $\mathbf{V}$ affine ou projective est définie sur $\mathbb{F}_q$ si et seulement si la $\overline{\mathbb{F}}_q$-algèbre correspondante est de la forme $A = A_0 \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ où A_0 est un $\mathbb{F}_q$-algèbre de type fini. On dit que A_0 est une $\mathbb{F}_q$-structure sur A. L'endomorphisme de Frobenius $F : \mathbf{V} \to \mathbf{V}$ associé à cette $\mathbb{F}_q$-structure correspond à l'endomorphisme de $A = A_0 \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ donné par $a \otimes \lambda \mapsto a^q \otimes \lambda$ (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 Φ envoie $a \otimes \lambda$ sur $a \otimes \lambda^q$. 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 $\mathbf{V}$.

14.2. Exemple. La droite affine sur $\overline{\mathbb{F}}_q$ est la variété $\mathbf{V}$ définie par la $\overline{\mathbb{F}}_q$-algèbre $\overline{\mathbb{F}}_q[T]$. La droite affine sur $\mathbb{F}_q$, variété $\mathbf{V}_0$ définie par la $\mathbb{F}_q$-algèbre $\mathbb{F}_q[T]$, est une $\mathbb{F}_q$-structure sur $\mathbf{V}$ puisque $\overline{\mathbb{F}}_q[T] = \mathbb{F}_q[T] \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$. L'endomorphisme de Frobenius géométrique envoie un polynôme $P(T)$ sur $P(T^q)$, tandis que l'endomorphisme de Frobenius arithmétique envoie $\sum_i a_i T^i$ sur $\sum_i a_i^q T^i$; donc $F \circ \Phi$ envoie $P(T)$ sur $P(T)^q$. Un point de $\mathbf{V}$ sur $\overline{\mathbb{F}}_q$ correspond à un élément $a \in \overline{\mathbb{F}}_q$ (l'idéal correspondant est le noyau du morphisme $P \mapsto P(a) : \overline{\mathbb{F}}_q[T] \to \overline{\mathbb{F}}_q$); l'image du point a par $F \circ \Phi$ est défini par le noyau de $P \mapsto P(a)^q$ qui est le même.

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 omettrons par défaut le mot "géométrique" et dirons que F est "l'endomorphisme de Frobenius". On dit qu'un morphisme (resp. une sous-variété, *etc.*...) est rationnel ou défini sur $\mathbb{F}_q$ s'il est stable par l'endomorphisme de Frobenius. Rappelons quelques résultats sur les variétés définies sur $\mathbb{F}_q$.

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

(i) Soit F *un morphisme surjectif de* A *sur* A^q*; alors* F *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 $\mathbf{V}$ *est munie d'une* $\mathbb{F}_q$*-structure* A_0 *et que* F *est l'endomorphisme de Frobenius correspondant.*

(ii) On a $A_0 = \{x \in A \mid x^q = F(x)\}$.

(iii) Une sous-variété fermée de $\mathbf{V}$ *est stable par* F *si et seulement si l'idéal qui la définit est de la forme* $I_0 \otimes \overline{\mathbb{F}}_q$ *où* I_0 *est un idéal de* A_0*. Dans ce cas la sous-variété est définie sur* $\mathbb{F}_q$ *et 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 $\mathbf{V}^F$ des points rationnels de $\mathbf{V}$ (encore noté $\mathbf{V}(\mathbb{F}_q)$).

PREUVE: Voir [Digne-Michel]. ■

Le (iii) ci-dessus montre qu'une sous-variété rationnelle fermée est définie sur $\mathbb{F}_q$ comme variété. Cette propriété s'étend à toute sous-variété, ce qui rend la terminologie cohérente.

14.4 PROPOSITION. *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 $\mathbf{V}$.*

PREUVE: On peut en donner une preuve élémentaire compliquée. C'est une conséquence immédiate des propriétés de la cohomologie l-adique. ■

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.

EXEMPLE(S). 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.*... Un plongement d'un groupe algébrique $\mathbf{G}$ dans GL_n du type ci-dessus définit un endomorphisme de Frobenius **standard** sur $\mathbf{G}$ associé à ce plongement: $(x_{ij}) \mapsto (x_{ij}^q)$. Mais un groupe $\mathbf{G}^F$ n'est pas nécessairement obtenu de cette façon; par exemple le groupe unitaire est $\mathrm{GL}_n^{F'}$ où F' est l'endomorphisme de Frobenius défini par $F'(x) = F({}^t x^{-1})$ (où F est l'endomorphisme de Frobenius standard sur GL_n élévation des coefficients à la puissance q).

Si $\mathbf{G}$ est un groupe réductif défini sur $\mathbb{F}_q$, et $\mathbf{T}$ est un tore maximal de $\mathbf{G}$ défini sur $\mathbb{F}_q$ (nous verrons (15.2) qu'il existe toujours un tel tore maximal), alors $X(\mathbf{T}) = \mathrm{Hom}(\mathbf{T}, \mathbb{G}_m)$ est muni d'une action naturelle que nous noterons τ du générateur $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ induite par le Frobenius arithmétique sur $\mathbf{T}$ et sur $\mathbb{G}_m$. Pour $\alpha \in X(\mathbf{T})$ on a $(\tau\alpha)({}^F t) = (\alpha(t))^q$. L'endomorphisme F est une isogénie stabilisant $\mathbf{T}$, telle que τ induit la permutation des racines décrite dans 13.1, et le p-morphisme défini par F est égal à $q\tau$. De même que la donnée radicielle $(X(\mathbf{T}), Y(\mathbf{T}), \Phi, \check{\Phi})$ et le corps $\overline{\mathbb{F}}_q$ déterminent $\mathbf{G}$ à isomorphisme près, la donnée supplémentaire de q et de τ détermine le couple $(\mathbf{G}, F)$ (donc $\mathbf{G}^F$) à isomorphisme près. Nous verrons (remarque après 15.11) que pour $w \in W$, τ et $w\tau$ déterminent le même couple $(\mathbf{G}, F)$ ("vu" depuis un tore F-stable différent). À actions près de W, on peut donc supposer que τ fixe une chambre du système d'hyperplans associé à W, ou encore un système de racines positives.

Alors τ est classifié 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): $A_n (n \geq 1)$

— Groupe projectif spécial linéaire $\mathrm{PSL}_n \simeq \mathrm{PGL}_n$ (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; voir 15.5; de plus 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); ${}^2A_n (n \geq 2)$ — Groupe projectif spécial unitaire $\mathrm{PSU}_n \simeq \mathrm{PU}_n$ (même remarque sur PSU_n^F; de plus pour $q=2$ le groupe obtenu 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}^-); ${}^3D_4$ — Groupe de la trialité; 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; ${}^2E_6$; E_7; E_8.

15. Théorème de Lang-Steinberg.

Soit $\mathbf{G}$ un groupe algébrique réductif sur $\overline{\mathbb{F}}_q$, et soit $F : \mathbf{G} \to \mathbf{G}$ une isogénie ayant un nombre fini de points fixes. Alors le groupe des points fixes $\mathbf{G}^F$ est ce qu'on appelle un *groupe fini de type de Lie*. En général, une telle isogénie est un endomorphisme de Frobenius correspondant à une $\mathbb{F}_q$-structure pour un certain q, et $\mathbf{G}^F = \mathbf{G}(\mathbb{F}_q)$; il existe des exceptions, les groupes de Ree et de Suzuki, correspondant à des isogénies exceptionnelles associées aux automorphismes ${}^2B_2$, ${}^2F_4$ (resp. ${}^2G_2$) des diagrammes de Coxeter en caractéristique 2 (resp. 3); par exemple, pour B_2 (resp. G_2), si on note α, β les racines simples (où α est courte), et si q est une puissance de $p=2$ (resp. $p=3$), alors il existe un p-morphisme f tel que $f(\alpha) = q\beta$ et $f(\beta) = 2q\alpha$ (resp. $f(\beta) = 3q\alpha$); le carré de l'isogénie F associée est un endomorphisme de Frobenius, associé à une $\mathbb{F}_{q^2p}$-structure. 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 dans la section précédente ces séries de groupes (découvertes par Ree et Suzuki) et les groupes alternés, on obtient toutes les séries infinies de groupes simples finis.

Le théorème fondamental pour l'étude des groupes de type de Lie est le

15.1 Théorème de Lang-Steinberg. *Soit $\mathbf{G}$ un groupe algébrique affine* **connexe**, *et F un endomorphisme de $\mathbf{G}$ surjectif et ayant un nombre fini de points fixes. Alors l'application (dite application de Lang) $\mathcal{L} : g \mapsto g^{-1}.{}^F g$ de $\mathbf{G}$ sur lui-même est surjective.*

Indications sur la preuve: On démontre d'abord qu'un tel endomorphisme a une différentielle en 1 nilpotente. On en déduit que la différentielle en 1 de $\mathcal{L}$ est surjective, ce qui implique que $\mathcal{L}$ est dominant, c'est-à-dire que son image contient un ouvert dense. On en déduit ensuite que pour x fixé, l'application $g \mapsto g^{-1}.x.{}^F g$ a aussi une différentielle surjective donc son image contient aussi un ouvert dense. Ces deux ouverts doivent se rencontrer; donc il existe $\mathbf{G}$ et h tels que $g^{-1}.{}^F g = h^{-1}.x.{}^F h$, donc $x = \mathcal{L}(gh^{-1})$ (voir [Steinberg, "Endomorphisms of algebraic groups", memoirs of AMS 80] pour une preuve complète). ■

Dans la suite de cette section $\mathbf{G}$ sera un groupe algébrique connexe sur $\overline{\mathbb{F}}_q$ et F un endomorphisme surjectif de $\mathbf{G}$ ayant un nombre fini de points fixes.

15.2 Corollaire. *Soit* $\mathbf{V}$ *une variété sur* $\overline{\mathbb{F}}_q$ *sur laquelle* $\mathbf{G}$ *agit, et supposons* $\mathbf{V}$ *muni d'un endomorphisme encore noté* F *tel que l'action de* $\mathbf{G}$ *commute à* F*. Soit* $\mathcal{O}$ *une* $\mathbf{G}$*-orbite* F*-stable dans* $\mathbf{V}$

(i) $\mathcal{O}^F$ *est non vide.*

(ii) Soient $x \in \mathcal{O}^F$ *et* $g \in \mathbf{G}$*; on a* $gx \in \mathcal{O}^F$ *si et seulement si* $g^{-1}Fg \in \mathrm{Stab}_{\mathbf{G}}(x)$*.*

(iii) Étant donné $x \in \mathcal{O}^F$*, l'application qui à l'orbite sous* $\mathbf{G}^F$ *de* $gx \in \mathcal{O}^F$ *associe la classe de* F*-conjugaison de l'image de* $g^{-1}Fg$ *dans* $\mathrm{Stab}_{\mathbf{G}}(x)/\mathrm{Stab}_{\mathbf{G}}(x)^0$ *est bien définie et est bijective.*

Rappelons qu'on appelle F-conjugaison dans un groupe K muni d'un automorphisme F l'action d'un élément $k \in K$ définie par $x \mapsto kxFk^{-1}$.

Preuve: Prouvons (i). Soit $v \in \mathcal{O}$. On a donc ${}^Fv = {}^gv$ pour un certain $g \in \mathbf{G}$. Utilisons le théorème de Lang pour écrire $g^{-1} = h^{-1}Fh$ pour un certain $h \in \mathbf{G}$. Alors ${}^hv \in \mathcal{O}^F$.

(ii) résulte d'un calcul immédiat.

Prouvons (iii). Pour $x \in \mathcal{O}^F$ soient $h, g \in \mathbf{G}$ tels que $hx, gx \in \mathcal{O}^F$. Remarquons que $hx = gx$ si et seulement si h et g diffèrent d'un élément de $\mathrm{Stab}_{\mathbf{G}}(x)$, et alors $h^{-1}Fh$ et $g^{-1}Fg$ sont F-conjugués dans $\mathrm{Stab}_{\mathbf{G}}(x)$. On a donc une application bien définie de l'ensemble $\mathcal{O}^F$ sur les F-classes de $\mathrm{Stab}_{\mathbf{G}}(x)$. 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 $\mathcal{O}^F$ dans les F-classes de $\mathrm{Stab}_{\mathbf{G}}(x)$. Supposons que $g^{-1}Fg$ et $h^{-1}Fh$ soient des éléments F-conjugués par $n \in \mathrm{Stab}_{\mathbf{G}}(x)$, alors gnh^{-1} est un élément de $\mathbf{G}^F$ qui envoie hx sur gx. L'application est donc injective. Comme, d'après le théorème de Lang, un élément de $\mathrm{Stab}_{\mathbf{G}}(x)$ s'écrit $g^{-1}Fg$ avec $g \in \mathbf{G}$, on voit que l'application est surjective. Il reste à voir que le passage au quotient de $\mathrm{Stab}_{\mathbf{G}}(x)$ à $\mathrm{Stab}_{\mathbf{G}}(x)/\mathrm{Stab}_{\mathbf{G}}(x)^0$ induit une bijection sur les F-classes, ce qui est une conséquence du:

15.3 Lemme. *Soit* $\mathbf{H}$ *un sous-groupe fermé normal* F*-stable de* $\mathbf{G}$*, alors le passage au quotient induit une bijection des* F*-classes de* $\mathbf{H}$ *sur celles de* $\mathbf{H}/\mathbf{H}^0$*.*

Preuve: Il est clair que deux éléments F-conjugués de $\mathbf{H}$ ont des images F-conjuguées. Réciproquement, si h et h' sont F-conjugués modulo $\mathbf{H}^0$, on a $h_0h = xh'Fx^{-1}$, avec $x \in \mathbf{H}$ et $h_0 \in \mathbf{H}^0$. Comme $\mathbf{H}^0$ est connexe, on peut lui appliquer le théorème de Lang avec l'application $\mathrm{ad}\, hF$; en effet si on écrit $h = k^{-1}Fk$, alors les points fixes z de hF vérifient ${}^{k^{-1}Fk}Fz = z \Leftrightarrow {}^F({}^kz) = {}^kz$ donc sont en nombre fini. Il existe donc y tel que $h_0 = y^{-1}hFy$, donc $h_0h = y^{-1}hFy$, et $h = (yx)h'F(yx)^{-1}$. Donc h et h' sont F-conjugués dans $\mathbf{H}$. ■

■

15.4 Proposition. *Si* $\mathbf{H}$ *est un sous-groupe fermé connexe* F*-stable de* $\mathbf{G}$*, alors on a* $(\mathbf{G}/\mathbf{H})^F = \mathbf{G}^F/\mathbf{H}^F$*.*

Preuve: Par 15.2(i), toute classe F-stable $x\mathbf{H}$ contient un élément F-stable, donc l'application naturelle $\mathbf{G}^F/\mathbf{H}^F \to (\mathbf{G}/\mathbf{H})^F$ est surjective. Elle est injective car si $x, y \in \mathbf{G}^F$ sont dans la même classe de $\mathbf{H}$, alors $x^{-1}y \in \mathbf{H}^F$.

15.5 (Contre)-Exemple. *Un piège.* 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 $\mathrm{SL}_n(\mathbb{F}_q)$ par son centre (ce phénomène ne se produit

que si l'on fait le quotient par un sous-groupe non connexe). En effet, le centre de SL_n, formé des matrices scalaires multiples de l'identité par un élément du groupe μ_n des racines n-ième de l'unité, s'identifie à μ_n. L'image de $x \in \mathrm{SL}_n$ est dans PSL_n^F si et seulement si $x.{}^F x^{-1} \in \mu_n$. Si n est premier à $q-1$ alors l'application $z \mapsto z.{}^F z^{-1} = z^{1-q}$ est une bijection de μ_n sur μ_n et, comme dans la preuve de 15.2, on conclut que x diffère par un élément de μ_n d'un élément de SL_n^F; pour ces n le centre μ_n^F de SL_n^F est trivial, mais pour d'autres valeurs de n le groupe PSL_n^F contient des éléments qui ne sont pas dans SL_n^F/μ_n^F (La "suite exacte de cohomologie Galoisienne" montre qu'à la suite exacte $1 \to \mu_n \to \mathrm{SL}_n \to \mathrm{PSL}_n \to 1$ correspond la suite exacte $1 \to \mu_n^F \to \mathrm{SL}_n^F \to \mathrm{PSL}_n^F \to H^1(F,\mu_n) \to 1$ où $H^1(F,\mu_n) = \mu_n/\operatorname{Im}(x \mapsto x^{1-q})$ s'identifie à l'ensemble des F-classes de μ_n).

15.6 Applications.

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

(ii) Supposons $\mathbf{G}$ réductif. Tout sous-groupe parabolique F-stable $\mathbf{P}$ admet une décomposition de Levi F-stable, et deux sous-groupes de Levi F-stables sont conjugués sous $(R_u(\mathbf{P}))^F$.

(iii) Toute classe de conjugaison F-stable de $\mathbf{G}$ a des représentants F-stables. Les classes sous $\mathbf{G}^F$ d'éléments de $\mathbf{G}^F$ conjugués à $x \in \mathbf{G}^F$ donné sous $\mathbf{G}$ sont paramétrées par les F-classes de $C_{\mathbf{G}}(x)/C_{\mathbf{G}}(x)^0$ (deux éléments de $\mathbf{G}^F$ conjugués sous $\mathbf{G}$ sont dits **géométriquement** *conjugués).*

Preuve: Prouvons (i). On peut se ramener au cas $\mathbf{G}$ réductif en quotientant par $R_u(\mathbf{G})$. L'existence vient de 15.2(i) et du fait que tous les sous-groupes de Borel sont conjugués. Le fait qu'il y ait une seule orbite sous $\mathbf{G}^F$ vient de 15.2(iii) et de $N_{\mathbf{G}}(\mathbf{B}) = \mathbf{B}$ si $\mathbf{B}$ est un sous-groupe de Borel.

Prouvons (ii). Par 13.6 deux sous-groupes de Levi sont conjugués sous $R_u(\mathbf{P})$, qui est F-stable, d'où l'existence de sous-groupes de Levi F-stables. Il y en a une seule orbite car (cf. preuve de 13.6) $N_{R_u(\mathbf{P})}(\mathbf{L}) = 1$ ce qui est connexe.

Pour (iii) il suffit d'appliquer 15.2 avec $\mathbf{V} = \mathbf{G}$ sur lequel $\mathbf{G}$ agit par conjugaison. ■

On voit d'après (i) et (ii) que les tores maximaux F-stables des sous-groupes de Borel F-stables sont conjugués sous $\mathbf{G}^F$.

Donnons maintenant des caractérisations des éléments semi-simples et unipotents "en termes de groupes finis".

15.7 Proposition.

(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 $\mathbf{G}$.

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

Soit s un élément semi-simple; considérons le groupe algébrique connexe $C^0_{\mathbf{G}}(s)$. Il contient s car tout élément semi-simple est dans un tore maximal de $\mathbf{G}$, qui est donc dans $C^0_{\mathbf{G}}(s)$. Comme s est central dans son centralisateur, 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 $\mathbf{G}$. ■

15.8 Proposition. *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* $W^F = N_{\mathbf{G}}(\mathbf{T})^F/\mathbf{T}^F$*.*

(ii) Soient $\mathbf{T}$ *et* $\mathbf{B} \supset \mathbf{T}$ *un tore maximal et un sous-groupe de Borel* F*-stables de* $\mathbf{G}$*. Alors On a la "décomposition de Bruhat relative"* $\mathbf{G}^F = \coprod_{w\in W^F} \mathbf{B}^F w\mathbf{B}^F$ *(c'est la décomposition de Bruhat associée à la "*(B,N)*-paire relative" de* $\mathbf{G}^F$ *— cf. 15.10 ci-dessous).*

(iii) Supposons que F *est l'endomorphisme de Frobenius attaché à une* $\mathbb{F}_q$*-structure. Alors on a* $|\mathbf{G}^F| = q^{|\Phi^+|}|\mathbf{T}^F|(\sum_{w\in W^F} q^{l(w)})$ *où* Φ^+ *est l'ensemble des racines positives et où* $\mathbf{T}$ *est un tore maximal inclus dans un sous-groupe de Borel* F*-stable. Les* p*-sous-groupes de Sylow de* $\mathbf{G}^F$ *sont les* $\mathbf{U}^F$ *où* $\mathbf{U}$ *est le radical unipotent d'un sous-groupe de Borel* F*-stable de* $\mathbf{G}$*.*

Preuve: (i) vient de 15.4 (qui s'applique même quand $\mathbf{G}$ n'est pas connexe, pourvu que $\mathbf{H}$ le soit).

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 ce qu'une double classe de la décomposition de Bruhat s'écrit $\mathbf{B}w\mathbf{B} = \mathbf{B}w\mathbf{U}_w$ où on a posé $\mathbf{U}_w = \prod_{\{\alpha\in\Phi^+|w(\alpha)<0\}} \mathbf{U}_\alpha$; en effet on a par 4.1(iv) $\mathbf{U} = (\mathbf{U}\cap {}^{w^{-1}}\mathbf{U})\mathbf{U}_w$. Le produit à droite est direct car $\mathbf{B}\cap {}^w\mathbf{U}_w = 1$ par construction de $\mathbf{U}_w$. On en déduit bien qu'un élément F-stable de $\mathbf{B}w\mathbf{B}$ est dans $\mathbf{B}^F w\mathbf{B}^F$.

Montrons (iii). Par ce qui précède $|\mathbf{G}^F/\mathbf{B}^F| = \sum_{w\in W^F} |\mathbf{U}_w^F|$ où $\mathbf{U}_w^F$ est un espace affine de dimension $l(w)$, donc par 14.4 on a $|\mathbf{U}_w^F| = q^{l(w)}$. On en déduit (ii) car on a $|\mathbf{B}^F| = |\mathbf{T}^F||\mathbf{U}^F|$ et, toujours d'après 14.4, $|\mathbf{U}^F| = q^{|\Phi^+|}$. 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 $\mathbf{G}^F$ (remarquons que comme $N_{\mathbf{G}^F}(\mathbf{U}^F) = \mathbf{B}^F$, $\sum_{w\in W^F} q^{l(w)}$ est le nombre de p-sous-groupes de Sylow de $\mathbf{G}^F$). ■

Remarquons que le fait que les points rationnels du radical unipotent d'un sous-groupe de Borel forment un p-sous-groupe de Sylow de $\mathbf{G}(\mathbb{F}_q)$ s'étend aux groupes non réductifs, car $R_u(\mathbf{G})$ est un p-groupe d'après 15.7(i), il est inclus dans tous les radicaux unipotents des sous-groupes de Borel, et $R_u(\mathbf{G})$ étant connexe $|\mathbf{G}^F| = |(\mathbf{G}/R_u(\mathbf{G}))^F||R_u(\mathbf{G})^F|$.

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

15.9. Proposition. *Soit* (W,S) *un système de Coxeter et soit* σ *un automorphisme de* W *qui stabilise* S*. Soit* $(S/\sigma)_{<\infty}$ *l'ensemble des orbites* $\mathcal{O}$ *de* σ *dans* S *telles que le sous-groupe parabolique* $W_{\mathcal{O}}$ *soit fini. Alors* $(W^\sigma, \{w_{\mathcal{O}}\}_{\mathcal{O}\in(S/\sigma)_{<\infty}})$*, est un système de Coxeter, où* W^σ *est le sous-groupe des points fixes de* σ*, et où* $w_{\mathcal{O}}$ *est l'élément de plus grande longueur de* $W_{\mathcal{O}}$ *(cf. 2.3). De plus, si* $w_{\mathcal{O}_1}\dots w_{\mathcal{O}_k}$ *est la décomposition réduite d'un élément* w *dans le système de Coxeter ci-dessus, on a* $l(w) = \sum_{i=1}^{i=k} l(w_{\mathcal{O}_i})$ *(où* l *est la fonction longueur du système* (W,S)*).*

Preuve: Voir, par exemple J.-Y. Hée, "Systèmes de racines sur un anneau commutatif totalement ordonné", *Geom. Dedicata* **37**, 65–102 (1991). La preuve utilise la représentation géométrique considérée en 2.4. ■

15.10. Corollaire. *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*.*

Preuve: C'est une conséquence immédiate de la définition des (B,N)-paires, de 15.8(ii) et de 15.9. Le point essentiel est que si I est une orbite de F dans S, on a $\mathbf{B}^F w_I \mathbf{B}^F w_I \mathbf{B}^F \subset \mathbf{B}^F \cup \mathbf{B}^F w_I \mathbf{B}^F$, ce qui résulte de ce que 1 est w_I sont les seuls éléments F-stables de W_I (cette propriété résulte elle-même de ce que l'ensemble des racines qui changent de signe par un élément de W_I^F contient une racine simple s'il n'est pas vide, donc contient toutes les racines simples puisqu'il est F-stable, donc contient toutes les racines positives puisqu'il est clos). ■

La (B,N)-paire de 15.10 permet d'étendre le (iii) de 15.8 au cas où F n'est pas un endomorphisme de Frobenius, sous la forme $|\mathbf{G}^F| = q_{w_0} |\mathbf{T}^F| (\sum_{w \in W^F} q_w)$ où q_w est comme dans 9.4. En effet on a $|\mathbf{U}_w^F| = |\mathbf{B}^F w \mathbf{B}^F / \mathbf{B}^F| = q_w$ où la dernière égalité résulte de de la remarque avant 9.6.

15.11 Proposition. *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* F*-classes de* $N_{\mathbf{G}}(\mathbf{T})/N_{\mathbf{G}}(\mathbf{T})^0 = W(\mathbf{T})$ *(On appelle* **type** *du tore* ${}^g\mathbf{T}$ *par rapport au tore* $\mathbf{T}$ *la* F*-classe de* $W(\mathbf{T})$ *définie par l'élément* $g^{-1}\,{}^F g$*).*

Preuve: On applique 15.2 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 ${}^g\mathbf{T}$.

On peut démontrer que les centralisateurs de tous les éléments de GL_n sont connexes, donc les classes géométriques ne se scindent pas. Par contre

Exercice.

(i) Montrer que les classes géométriques de $\mathrm{SL}_n(\mathbb{F}_q)$ sont l'intersection avec SL_n des classes géométriques de $\mathrm{GL}_n(\mathbb{F}_q)$.

(ii) Soit $u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{F}_q)$. Calculer ses centralisateurs dans GL_2 et dans SL_2; montrer qu'en caractéristique différente de 2 ce dernier a deux composantes connexes.

(iii) Le (ii) montre qu'il y a deux classes rationnelles conjuguées géométriquement à u. Pour les identifier, montrer que la matrice $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ où $a \in \mathbb{F}_q$ est conjuguée géométriquement à u mais n'est conjuguée rationnellement à u que si a est un carré.

(iv) De même, soit $s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{F}_q)$. Montrer qu'en caractéristique différente de 2 son centralisateur dans PGL_2 a deux composantes connexes.

(v) Montrer que $\begin{pmatrix} 0 & \lambda^{-1} \\ \lambda & 0 \end{pmatrix}$ où λ est un élément de $\mathbb{F}_{q^2}$ tel que $\lambda^{q-1} = -1$ est un élément de $\mathrm{PGL}_2(\mathbb{F}_q)$, et que cet élément est conjugué géométriquement mais non rationnellement à s.

Cet exercice illustre un phénomène général: dans SL_n, les centralisateurs des éléments semi-simples sont connexes mais pas toujours ceux des éléments unipotents, tandis que dans PGL_n, ce sont les éléments semi-simples qui ont parfois un centralisateur non connexe.

16. Induction de Harish-Chandra; 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_G^H; 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 $\mathbf{G}$.

16.1 Proposition.

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

(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) $\mathbf{M}$ est un sous-groupe de Levi d'un sous-groupe parabolique de $\mathbf{L}$.

(b) $\mathbf{M}$ est un sous-groupe de Levi d'un sous-groupe parabolique de $\mathbf{G}$, et $\mathbf{M}\subset\mathbf{L}$.

Preuve: Démontrons (i); soit $\mathbf{T}$ un tore maximal de $\mathbf{M}$ et soit $\mathbf{L}$ l'unique sous-groupe de Levi de $\mathbf{P}$ contenant $\mathbf{T}$ (*cf.* 13.6). Il suffit de voir qu'alors $\mathbf{L}\supset\mathbf{M}$; c'est un conséquence immédiate de 13.8(i). Démontrons (ii); si $\mathbf{M}$ est un sous-groupe de Levi de $\mathbf{Q}_0$, sous-groupe parabolique de $\mathbf{L}$, alors $\mathbf{Q}_0R_u(\mathbf{P})$ est un sous-groupe parabolique de $\mathbf{G}$ (c'est un groupe car $\mathbf{L}$, donc $\mathbf{Q}_0$, normalise $R_u(\mathbf{P})$ et il contient clairement $\mathbf{U}_\alpha$ ou $\mathbf{U}_{-\alpha}$ pour tout $\alpha\in\Phi$) Borel) dont $\mathbf{M}$ est un sous-groupe de Levi (car $R_u(\mathbf{Q}_0).R_u(\mathbf{P})$ est unipotent normal dans $\mathbf{Q}_0.R_u(\mathbf{P})$). Donc (a) implique (b). Pour voir la réciproque, soit $\mathbf{Q}$ un sous-groupe parabolique de $\mathbf{G}$ dont $\mathbf{M}$ est un sous-groupe de Levi, et appliquons 13.8 à $\mathbf{P}\cap\mathbf{Q}$. Par 13.8(ii), $\mathbf{M}\rtimes(\mathbf{L}\cap\mathbf{V})$ est une décomposition de Levi de $\mathbf{L}\cap\mathbf{Q}$ et ce dernier groupe est parabolique par 13.7. ■

Dans la situation (ii) ci-dessus on dira par abus de langage que "$\mathbf{M}$ est un sous-groupe de Levi de $\mathbf{L}$".

Quand $\mathbf{L}$ est un sous-groupe de Levi F-stable de $\mathbf{G}$, on pourrait essayer de construire des représentations de $\mathbf{G}^F$ à partir de celles $\mathbf{L}^F$ en considérant $\mathrm{Ind}_{\mathbf{L}^F}^{\mathbf{G}^F}$. En fait les représentations obtenues n'ont pas de bonnes propriétés; il faut utiliser "l'induction de Harish-Chandra" que nous allons étudier dans les prochains paragraphes; nous allons la définir comme induction généralisée associée à un bimodule.

On considère deux groupes finis G et H et un bimodule M sur lequel $\mathbb{C}[G]$ opère à gauche et $\mathbb{C}[H]$ opère à droite. Un tel module sera appelé un G-module-H. Il permet de définir un foncteur $R_H^G : E \mapsto M\otimes_{\mathbb{C}[H]} E$ de la catégorie des $\mathbb{C}[H]$-modules à gauche

dans celle des $\mathbb{C}[G]$-modules à gauche, où G opère par son action sur M. Le module dual M^* définit clairement le foncteur adjoint, qui sera noté ${}^*R_H^G$. L'associativité du produit tensoriel donne:

16.2 Proposition (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. Donnons, sous cette hypothèse la formule de l'induction généralisée pour les caractères.

16.3 Proposition. *Si M est de dimension finie, et E est un H-module de dimension finie, alors pour $g \in G$ on a* $\mathrm{Trace}(g \mid R_H^G E) = |H|^{-1} \sum_{h \in H} \mathrm{Trace}((g, h^{-1}) \mid M) \mathrm{Trace}(h \mid E)$.

Preuve: Considérons l'élément idempotent $|H|^{-1} \sum_h h^{-1} \otimes h$ de l'algèbre $\mathbb{C}[H \times H] = \mathbb{C}[H] \otimes \mathbb{C}[H]$. Son image dans la représentation de $H \times H$ sur le produit tensoriel $M \otimes_{\mathbb{C}} E$ est un projecteur de noyau engendré par les éléments $mh \otimes x - m \otimes hx$. En effet si $\sum_i \sum_h m_i h^{-1} \otimes h x_i = 0$, alors

$$\sum_i m_i \otimes x_i = |H|^{-1} \sum_h \sum_i (m_i \otimes x_i - m_i h^{-1} \otimes h x_i).$$

Comme $M \otimes_{\mathbb{C}[H]} E$ est le quotient de $M \otimes_{\mathbb{C}} E$ par l'espace engendré par les éléments $mh \otimes x - m \otimes hx$, la trace de $g \in G$ sur $R_H^G E$ est la trace sur $M \otimes_{\mathbb{C}} E$ de $|H|^{-1} \sum_h (g, h^{-1}) \otimes h$, d'où la formule de l'énoncé. ■

16.4 Exemple. Induction et restriction. On suppose H sous-groupe de G et l'on prend pour M l'algèbre du groupe G sur laquelle G opère à gauche et H opère à droite, par translations; alors R_H^G est l'induction et son adjoint la restriction.

16.5 Exemple. *Induction et restriction de Harish-Chandra.* Soit $\mathbf{G}$ un groupe de type de Lie et soit $\mathbf{P}$ un sous-groupe parabolique F-stable de $\mathbf{G}$ et $\mathbf{L}$ un sous-groupe de Levi F-stable de $\mathbf{P}$; on a $\mathbf{P} = \mathbf{LU}$. On considère le $\mathbf{G}^F$-module-$\mathbf{L}^F$ $\mathbb{C}[\mathbf{G}^F/\mathbf{U}^F]$ sur lequel $\mathbf{G}^F$ opère par translations à gauche et $\mathbf{L}^F$ opère par translations à droite (possible car $\mathbf{L}$ normalise $\mathbf{U}$). On obtient l'induction de Harish-Chandra. Le foncteur adjoint appelé restriction de Harish-Chandra, noté ${}^*R_{\mathbf{L}}^{\mathbf{G}}$ correspond au $\mathbf{L}^F$-module-$\mathbf{G}^F$ $\mathbb{C}[\mathbf{U}^F \backslash \mathbf{G}^F]$ où $\mathbf{G}^F$ opère par translations à droite et $\mathbf{L}^F$ par translations à gauche. D'après la formule du caractère 16.3 appliquée à la restriction de Harish-Chandra, la valeur de ${}^*R_{\mathbf{L}}^{\mathbf{G}}(\chi)(l)$, où χ est un caractère de $\mathbf{G}^F$ et l un élément de $\mathbf{L}^F$ est donc

$${}^*R_{\mathbf{L}}^{\mathbf{G}}(\chi)(l) = |\mathbf{G}^F|^{-1} \sum_{g \in \mathbf{G}^F} \#\{\, x\mathbf{U}^F \in \mathbf{G}^F/\mathbf{U}^F \mid x^{-1} g x \in l\mathbf{U}^F \,\} \chi(g) = |\mathbf{U}^F|^{-1} \sum_{u \in \mathbf{U}^F} \chi(lu),$$

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

Notation. Nous avons noté $R_{\mathbf{L}}^{\mathbf{G}}$ et ${}^*R_{\mathbf{L}}^{\mathbf{G}}$ l'induction et la restriction de Harish-Chandra pour abréger; on les notera $R_{\mathbf{L}^F}^{\mathbf{G}^F}$ et ${}^*R_{\mathbf{L}^F}^{\mathbf{G}^F}$ s'il y a ambiguïté possible sur F. Le sous-groupe parabolique n'intervient pas dans la notation car nous verrons que $R_{\mathbf{L}}^{\mathbf{G}}$ et ${}^*R_{\mathbf{L}}^{\mathbf{G}}$

ne dépendent pas du sous-groupe parabolique utilisé dans la construction. Si nous devons spécifier le sous-groupe parabolique, nous noterons $R^{\mathbf{G}}_{\mathbf{L}\subset\mathbf{P}}$.

NOTE. Nous n'avons ici défini un foncteur $R^{\mathbf{G}}_{\mathbf{L}}$ que quand $\mathbf{L}$ est un sous-groupe de Levi F-stable d'un sous-groupe parabolique F-stable $\mathbf{P}$ de $\mathbf{G}$; nous construirons plus tard l'induction de Deligne-Lusztig qui est définie même si $\mathbf{P}$ n'est pas F-stable.

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

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

16.6 PROPOSITION Transitivité de $R^{\mathbf{G}}_{\mathbf{L}}$. *Soit $\mathbf{G}$ un groupe réductif défini sur $\mathbb{F}_q$, soit $\mathbf{P}$ un sous-groupe parabolique F-stable de $\mathbf{G}$, soit $\mathbf{Q}$ 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 $\mathbf{M}$ un sous-groupe de Levi F-stable de $\mathbf{Q}$ inclus dans $\mathbf{L}$. Alors on a $R^{\mathbf{G}}_{\mathbf{L}\subset\mathbf{P}} \circ R^{\mathbf{L}}_{\mathbf{M}\subset\mathbf{L}\cap\mathbf{Q}} = R^{\mathbf{G}}_{\mathbf{M}\subset\mathbf{Q}}$.*

PREUVE: Nous noterons $\mathbf{U}$ le radical unipotent de $\mathbf{P}$ et $\mathbf{V}$ celui de $\mathbf{Q}$. On a $\mathbf{V} = \mathbf{U}(\mathbf{L}\cap\mathbf{V})$ par 13.8 (iii) et la propriété d'unicité dans cette décomposition montre que $\mathbf{V}^F = \mathbf{U}^F(\mathbf{L}^F \cap \mathbf{V}^F)$. D'après 16.2, pour montrer la proposition il faut montrer que

$$\mathbb{C}[\mathbf{G}^F/\mathbf{U}^F] \otimes_{\mathbb{C}[\mathbf{L}^F]} \mathbb{C}[\mathbf{L}^F/(\mathbf{L}\cap\mathbf{V})^F] \tilde{\to} \mathbb{C}[\mathbf{G}^F/\mathbf{V}^F]$$

en tant que $\mathbf{G}^F$-module-$\mathbf{M}^F$. Cela résulte clairement de l'isomorphisme d'ensembles munis de l'action de $\mathbf{G}^F \times \mathbf{M}^F$: $\mathbf{G}^F/\mathbf{U}^F \times^{\mathbf{L}^F} \mathbf{L}^F/(\mathbf{L}\cap\mathbf{V})^F \tilde{\to} \mathbf{G}^F/\mathbf{V}^F$ qui est induit par l'application $(g\mathbf{U}^F, l(\mathbf{L}\cap\mathbf{V})^F) \mapsto gl\mathbf{V}^F$ de $\mathbf{G}^F/\mathbf{U}^F \times \mathbf{L}^F/(\mathbf{L}\cap\mathbf{V})^F$ dans $\mathbf{G}^F/\mathbf{V}^F$; cette application est bien définie car l normalise $\mathbf{U}$ et $\mathbf{U} \subset \mathbf{V}$; il est facile de voir qu'elle se factorise par le produit amalgamé et définit un isomorphisme en utilisant la décomposition $\mathbf{V}^F = \mathbf{U}^F(\mathbf{L}\cap\mathbf{V})^F$. ■

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, dont une conséquence sera l'indépendance de cette induction par rapport au sous-groupe parabolique utilisé dans la définition.

16.7 THÉORÈME. *Soient $\mathbf{P}$ et $\mathbf{Q}$ deux sous-groupes paraboliques F-stables de $\mathbf{G}$ et $\mathbf{L}$ et $\mathbf{M}$ des sous-groupes de Levi F-stables respectivement de $\mathbf{P}$ et de $\mathbf{Q}$. Alors, si $\mathrm{ad}\, x$ dénote l'action de x par conjugaison sur les représentations, on a:*

$${}^*R^{\mathbf{G}}_{\mathbf{L}\subset\mathbf{P}} \circ R^{\mathbf{G}}_{\mathbf{M}\subset\mathbf{Q}} = \sum_x R^{\mathbf{L}}_{\mathbf{L}\cap{}^x\mathbf{M}\subset\mathbf{L}\cap{}^x\mathbf{Q}} \circ {}^*R^{{}^x\mathbf{M}}_{\mathbf{L}\cap{}^x\mathbf{M}\subset\mathbf{P}\cap{}^x\mathbf{M}} \circ \mathrm{ad}\, x,$$

où x parcourt des représentants de $\mathbf{L}^F\backslash\mathcal{S}(\mathbf{L},\mathbf{M})^F/\mathbf{M}^F$, où $\mathcal{S}(\mathbf{L},\mathbf{M}) = \{x \in \mathbf{G} \mid \mathbf{L} \cap {}^x\mathbf{M}$ contient un tore maximal de $G\}$.

PREUVE: Donnons d'abord une conséquence de 12.3.

16.8 Lemme. *Avec les notations de 16.7,*

(i) L'application naturelle $\mathcal{S}(\mathbf{L},\mathbf{M}) \to \mathbf{P}\backslash\mathbf{G}/\mathbf{Q}$ *induit un isomorphisme*

$$\mathbf{L}\backslash\mathcal{S}(\mathbf{L},\mathbf{M})/\mathbf{M}\xrightarrow{\sim}\mathbf{P}\backslash\mathbf{G}/\mathbf{Q}.$$

(ii) $\mathbf{P}^F\backslash\mathbf{G}^F/\mathbf{Q}^F$ *s'identifie aux points fixes sous* F *de* $\mathbf{P}\backslash\mathbf{G}/\mathbf{Q}$, *et* $\mathbf{L}^F\backslash\mathcal{S}(\mathbf{L},\mathbf{M})^F/\mathbf{M}^F$ *aux points fixes sous* F *de* $\mathbf{L}\backslash\mathcal{S}(\mathbf{L},\mathbf{M})/\mathbf{M}$.

Preuve: Montrons d'abord (ii). D'après 15.2 comme $\mathbf{P}\times\mathbf{Q}$ ainsi que 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 doubles classes $\mathbf{P}^F\backslash\mathbf{G}^F/\mathbf{Q}^F$ s'identifient aux doubles classes F-stables de $\mathbf{P}\backslash\mathbf{G}/\mathbf{Q}$. De même, comme, si $\mathbf{L}\cap {}^x\mathbf{M}$ contient un tore maximal, il est connexe, les doubles classes $\mathbf{L}^F\backslash\mathcal{S}(\mathbf{L},\mathbf{M})^F/\mathbf{M}^F$ s'identifient aux doubles classes F-stables de $\mathbf{L}\backslash\mathcal{S}(\mathbf{L},\mathbf{M})/\mathbf{M}$.

Montrons(i). On peut conjuguer $\mathbf{Q}$ par un élément $g\in\mathbf{G}$ pour 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 en commun. Alors $\mathbf{P}x\mathbf{Q}=(\mathbf{P}xg^{-1}{}^g\mathbf{Q})g$ pour tout $x\in\mathbf{G}$, c'est-à-dire que les doubles classes par rapport à $\mathbf{P}$ et $\mathbf{Q}$ sont les translatées des doubles classes par rapport à $\mathbf{P}$ et ${}^g\mathbf{Q}$. De même $\mathcal{S}(\mathbf{L},\mathbf{M})=\mathcal{S}(\mathbf{L},{}^g\mathbf{M})g$. Donc on peut remplacer $\mathbf{Q}$ par ${}^g\mathbf{Q}$ pour démontrer le lemme, c'est-à-dire supposer que $\mathbf{P}$ et $\mathbf{Q}$ sont standards et que $\mathbf{L}$ et $\mathbf{M}$ sont des sous-groupes de Levi standards, *i.e.*$\mathbf{P}=\mathbf{P}_I$, $\mathbf{Q}=\mathbf{P}_J$, $\mathbf{L}=\mathbf{L}_I$, et $\mathbf{M}=\mathbf{L}_J$. D'après le lemme 12.3, on peut trouver des représentants des doubles classes par rapport à $\mathbf{P}_I$ et $\mathbf{P}_J$ dans $N(\mathbf{T})$. Donc toute double classe a un représentant dans $\mathcal{S}(\mathbf{L},\mathbf{M})$. Donc l'application naturelle de $\mathcal{S}(\mathbf{L},\mathbf{M})$ dans $\mathbf{P}\backslash\mathbf{G}/\mathbf{Q}$ est surjective. Réciproquement, si $\mathbf{L}\cap {}^x\mathbf{M}$ contient un tore maximal avec $x\in\mathbf{G}$, alors ce tore est de la forme ${}^l\mathbf{T}$ et aussi ${}^{xm}\mathbf{T}$, avec $l\in\mathbf{L}$ et $m\in\mathbf{M}$, car les tores maximaux d'un groupe algébrique sont conjugués. Mais alors $l^{-1}xm$ normalise $\mathbf{T}$ et est dans la même double classe par rapport à $\mathbf{L}$ et $\mathbf{M}$, et on peut encore modifier cet élément par $\mathbf{L}$ à gauche et $\mathbf{M}$ à droite pour qu'il soit I,J-réduit. Soient maintenant x et y deux éléments de $\mathcal{S}(\mathbf{L},\mathbf{M})$ tels que $\mathbf{P}x\mathbf{Q}=\mathbf{P}y\mathbf{Q}$. D'après ce qu'on vient de voir, on peut modifier x et y par des éléments de $\mathbf{L}$ et $\mathbf{M}$ pour les ramener sur des éléments de $N_{\mathbf{G}}(\mathbf{T})$ qui ont des images I,J-réduites dans le groupe de Weyl. D'après le lemme 12.3, les images de x et y sont égales, donc x et y représentent la même double classe par rapport à $\mathbf{L}$ et $\mathbf{M}$. ■

Démontrons maintenant le théorème 16.7. Notons $\mathbf{U}$ et $\mathbf{V}$ les radicaux unipotents respectifs de $\mathbf{P}$ et $\mathbf{Q}$. Le premier membre de la formule de Mackey correspond au $\mathbf{L}$-module-$\mathbf{M}$ donné par $\mathbb{C}[\mathbf{U}^F\backslash\mathbf{G}^F]\otimes_{\mathbb{C}[\mathbf{G}^F]}\mathbb{C}[\mathbf{G}^F/\mathbf{V}^F]$ qui est clairement isomorphe à $\mathbb{C}[\mathbf{U}^F\backslash\mathbf{G}^F/\mathbf{V}^F]$. Décomposons $\mathbf{G}^F$ suivant ses doubles classes modulo $\mathbf{P}^F$ et $\mathbf{Q}^F$. On a

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

Or:

16.9 Lemme. *Pour tout* $x\in\mathcal{S}(\mathbf{L},\mathbf{M})^F$ *l'application* $l(\mathbf{L}\cap {}^x\mathbf{V})^F\times({}^x\mathbf{M}\cap\mathbf{U})^F.{}^xm\mapsto\mathbf{U}^FlxmV^F$ *est un isomorphisme du produit amalgamé* $\mathbf{L}^F/(\mathbf{L}\cap {}^x\mathbf{V})^F\times_{(\mathbf{L}\cap {}^x\mathbf{M})^F}({}^x\mathbf{M}\cap\mathbf{U})^F\backslash{}^x\mathbf{M}^F$ *sur* $\mathbf{U}^F\backslash\mathbf{P}^Fx\mathbf{Q}^F/\mathbf{V}^F$.

Preuve: On voit facilement que l'application est bien définie. Comme pour tout x, le stabilisateur $\mathbf{U}\cap {}^x\mathbf{V}$ d'un point de $\mathbf{G}$ sous l'action de $\mathbf{U}\times\mathbf{V}$ est connexe (*cf.* 4.1 (i)), 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 la propriété analogue au niveau des groupes algébriques, car l'application analogue sur les groupes algébriques est clairement compatible à F. L'application est surjective car tout élément de $\mathbf{P}x\mathbf{Q}$ s'écrit $ulxmv$. Montrons l'injectivité. Si $\mathbf{U}lxm\mathbf{V} = \mathbf{U}l'xm'\mathbf{V}$, alors $lxm = l'uxvm'$ avec $u \in \mathbf{U}$ et $v \in \mathbf{V}$ car l' normalise $\mathbf{U}$ et m' normalise $\mathbf{V}$. Donc

$$u^{-1}{l'}^{-1}l = {}^x(vm'm^{-1}), \tag{1}$$

et cet élément est dans $\mathbf{P}\cap {}^x\mathbf{Q}$. Or d'après 13.8 (iii), on a

$$\mathbf{P}\cap {}^x\mathbf{Q} = (\mathbf{L}\cap {}^x\mathbf{M}).(\mathbf{L}\cap {}^x\mathbf{V}).({}^x\mathbf{M}\cap\mathbf{U}).(\mathbf{U}\cap {}^x\mathbf{V}),$$

avec décomposition unique. Dans cette décomposition, la composante dans $\mathbf{L}\cap {}^x\mathbf{M}$ du premier membre de (1) est celle de ${l'}^{-1}l$, et la composante dans $\mathbf{L}\cap {}^x\mathbf{M}$ du deuxième membre de (1) est celle de ${}^x(m'm^{-1})$. Cela résulte du lemme:

16.10 Lemme. *Soient* $\mathbf{P}$ *et* $\mathbf{Q}$ *deux sous-groupes paraboliques et* $\mathbf{L}$ *et* $\mathbf{M}$ *des sous-groupes de Levi respectifs ayant un tore maximal commun. Si* $ul = vm \in \mathbf{P}\cap\mathbf{Q}$*, alors* $u_{\mathbf{M}} = m_{\mathbf{U}}$*,* $l_{\mathbf{V}} = v_l$ *et* $l_{\mathbf{M}} = m_{\mathbf{L}}$*, où* $u_{\mathbf{M}}$ *est la composante de* u *dans* $\mathbf{U}\cap\mathbf{M}$ *etc...*

Preuve: On a $u_{\mathbf{V}}u_{\mathbf{M}}l_{\mathbf{V}}l_{\mathbf{M}} = v_{\mathbf{U}}v_{\mathbf{L}}m_{\mathbf{U}}m_{\mathbf{L}} = v_{\mathbf{U}}(v_{\mathbf{L}}, m_{\mathbf{U}})m_{\mathbf{U}}v_{\mathbf{L}}m_{\mathbf{L}}$ et le commutateur qui apparaît dans cette formule est dans $\mathbf{V}\cap\mathbf{U}$. L'unicité de la décomposition dans 13.8 (iii) donne le résultat. ■

Donc $l(\mathbf{L}\cap {}^x\mathbf{V})\times({}^x\mathbf{M}\cap\mathbf{U})^xm$ et $l'(\mathbf{L}\cap {}^x\mathbf{V})\times({}^x\mathbf{M}\cap\mathbf{U})^xm'$ sont égaux dans le produit amalgamé, d'où l'injectivité et le lemme 16.9. ■

En prenant alors l'union sur les x, on obtient donc

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

et cette bijection est compatible à l'action de $\mathbf{L}^F$ par multiplication à gauche et à celle de $\mathbf{M}^F$ par multiplication à droite dans le premier membre et par le composé de la multiplication à gauche et de $\operatorname{ad} x$ sur le terme indexé par x dans le second membre. On a donc un isomorphisme de $\mathbf{L}^F$-module-$\mathbf{M}^F$:

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

où l'action de $\mathbf{M}^F$ dans le deuxième membre est composée avec $\operatorname{ad} x$ comme expliqué ci-dessus. Le module qui apparaît dans le membre de droite ci-dessus est donc exactement celui qui donne le deuxième membre de la formule de Mackey, d'où le théorème. ■

17. Théorie de Harish-Chandra.

Nous exposons ici la théorie des représentations "cuspidales", due à Harish-Chandra. Commençons par démontrer comme promis:

17.1 Proposition. *Le foncteur $R^{\mathbf{G}}_{\mathbf{L}\subset\mathbf{P}}$ ne dépend pas de $\mathbf{P}$.*

Ceci nous autorisera à omettre $\mathbf{P}$ de la notation.

Preuve: Nous allons procéder par récurrence sur le *rang semi-simple* de $\mathbf{G}$, qui défini comme le rang du système de racines de $\mathbf{G}$ (le nombre de racines simples). Notons qu'un sous-groupe de Levi d'un sous-groupe parabolique propre de $\mathbf{G}$ a un rang semi-simple strictement plus petit que celui de $\mathbf{G}$ (cf. 13.5). Si $\mathbf{L}=\mathbf{G}$ le résultat est trivial, donc on peut supposer le rang semi-simple de $\mathbf{L}$ strictement plus petit que celui de $\mathbf{G}$. En écrivant la formule de Mackey avec le même sous-groupe de Levi $\mathbf{L}$ et deux sous-groupes paraboliques $\mathbf{P}$ et $\mathbf{Q}$, on a:

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

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 $f(\mathbf{P})=R^{\mathbf{G}}_{\mathbf{L}\subset\mathbf{P}}\lambda$, on a:

$$\langle f(\mathbf{P}), f(\mathbf{P})\rangle_{\mathbf{G}^F} = \langle f(\mathbf{P}), f(\mathbf{Q})\rangle_{\mathbf{G}^F} = \langle f(\mathbf{Q}), f(\mathbf{Q})\rangle_{\mathbf{G}^F} = \langle f(\mathbf{Q}), f(\mathbf{P})\rangle_{\mathbf{G}^F}$$

d'où $\langle f(\mathbf{P})-f(\mathbf{Q}), f(\mathbf{P})-f(\mathbf{Q})\rangle_{\mathbf{G}^F}=0$ et donc $f(\mathbf{P})=f(\mathbf{Q})$. ■

17.2 Exemple. Soit $RGL=\bigoplus_{n>=0}R[\mathrm{GL}_n(\mathbb{F}_q)]$ (où, pour un groupe fini H, on note $R(H)$ le groupe de Grothendieck des caractères de H). On munit RGL d'une loi d'algèbre en posant, pour deux caractères irréductibles $\chi\in\mathrm{Irr}(\mathrm{GL}_n(\overline{\mathbb{F}}_q))$ et $\psi\in\mathrm{Irr}(\mathrm{GL}_m(\overline{\mathbb{F}}_q))$, $\chi\circ\psi=R^{\mathrm{GL}_{n+m}}_{\mathrm{GL}_n\times\mathrm{GL}_m\subset\mathbf{P}_{n,m}}\chi\otimes\psi$ où on a plongé $\mathrm{GL}_n\times\mathrm{GL}_m$ comme groupe de matrices diagonales par bloc dans GL_{n+m}:

$$\begin{pmatrix}\mathrm{GL}_n & 0\\ 0 & \mathrm{GL}_m\end{pmatrix}$$

et où on a pris pour $\mathbf{P}_{n,m}$ les matrices triangulaires par bloc:

$$\begin{pmatrix}\mathrm{GL}_n & \dots\\ 0 & \mathrm{GL}_m\end{pmatrix}$$

Par la proposition 17.1, cette loi d'algèbre est commutative. Remarquons néanmoins que, si $\mathrm{GL}_n\times\mathrm{GL}_m$ est conjugué à $\mathrm{GL}_m\times\mathrm{GL}_n$ dans GL_{n+m}, il n'en est pas de même pour $\mathbf{P}_{n,m}$ et $\mathbf{P}_{m,n}$ et en fait cette commutativité est difficile à vérifier directement.

De même on peut munir RGL d'un co-produit co-commutatif: $RGL\to RGL\otimes RGL$: $\chi\in\mathrm{Irr}(\mathrm{GL}_n(\mathbb{F}_q))\mapsto\bigoplus_{i+j=n}{}^*R^{\mathrm{GL}_n}_{\mathrm{GL}_i\times\mathrm{GL}_j}\chi$, et on peut vérifier que la formule de Mackey implique que ces deux lois munissent RGL d'une structure d'algèbre de Hopf.

Vu la transitivité de $R^{\mathbf{G}}_{\mathbf{L}}$ (*cf.* 16.6), on peut définir une relation d'ordre partiel sur l'ensemble des couples $(\mathbf{L},\lambda)$ formés d'un sous-groupe de Levi rationnel d'un sous-groupe parabolique rationnel de $\mathbf{G}$ et de $\lambda\in\mathrm{Irr}(\mathbf{L}^F)$, en posant $(\mathbf{L}',\lambda')\le(\mathbf{L},\lambda)$ si $\mathbf{L}'\subset\mathbf{L}$ et $\langle\lambda, R^{\mathbf{L}}_{\mathbf{L}'}\lambda'\rangle_{\mathbf{L}^F}\neq 0$.

17.3 Définition-Théorème. *On dit que la représentation λ de $\mathbf{L}^F$ 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 rationnel $\mathbf{L}'$ d'un sous-groupe parabolique rationnel de $\mathbf{L}$, on a ${}^*R^{\mathbf{L}}_{\mathbf{L}'}\lambda = 0$.

Preuve: 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. ■

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

Preuve:

17.5 Lemme. *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 rationnels de $\mathbf{G}$, alors:*

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

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

Preuve: Par la "formule de Mackey", on a:

$$\begin{aligned} \langle R^{\mathbf{G}}_{\mathbf{L}}\lambda, R^{\mathbf{G}}_{\mathbf{M}}\mu \rangle_{\mathbf{G}^F} = \langle \lambda, {}^*R^{\mathbf{G}}_{\mathbf{L}} R^{\mathbf{G}}_{\mathbf{M}}\mu \rangle_{\mathbf{L}^F} &= \langle \lambda, \sum_{x \in \mathbf{L}^F \backslash \mathcal{S}(\mathbf{L},\mathbf{M})/\mathbf{M}^F} \mathrm{ad}\, x^{-1} R^{{}^x\mathbf{L}}_{{}^x\mathbf{L}\cap\mathbf{M}} {}^*R^{\mathbf{M}}_{{}^x\mathbf{L}\cap\mathbf{M}}\mu \rangle_{\mathbf{L}^F} \\ &= \langle \lambda, \sum_{\{x \in \mathbf{L}^F \backslash \mathcal{S}(\mathbf{L},\mathbf{M})/\mathbf{M}^F \mid {}^x\mathbf{L} \supset \mathbf{M}\}} \mathrm{ad}\, x^{-1} R^{{}^x\mathbf{L}}_{\mathbf{M}}\mu \rangle_{\mathbf{L}^F} \end{aligned},$$

cette dernière égalité car, puisque μ est cuspidal, on a ${}^*R^{\mathbf{M}}_{{}^x\mathbf{L}\cap\mathbf{M}}\mu = 0$ si ${}^x\mathbf{L} \cap \mathbf{M} \neq \mathbf{M}$. De même:

$$\begin{aligned} \langle \lambda, \sum_{\{x \in \mathbf{L}^F \backslash \mathcal{S}(\mathbf{L},\mathbf{M})/\mathbf{M}^F \mid {}^x\mathbf{L} \supset \mathbf{M}\}} \mathrm{ad}\, x^{-1} R^{\mathbf{L}}_{\mathbf{M}}\mu \rangle_{\mathbf{L}^F} &= \langle \sum_{\{x \in \mathbf{L}^F \backslash \mathcal{S}(\mathbf{L},\mathbf{M})/\mathbf{M}^F \mid {}^x\mathbf{L} \supset \mathbf{M}\}} {}^*R^{{}^x\mathbf{L}}_{\mathbf{M}}\, {}^x\lambda, \chi \rangle_{\mathbf{M}^F} \\ &= \langle \sum_{\{x \in \mathbf{L}^F \backslash \mathcal{S}(\mathbf{L},\mathbf{M})/\mathbf{M}^F \mid {}^x\mathbf{L} = \mathbf{M}\}} {}^x\lambda, \chi \rangle_{\mathbf{M}^F}, \end{aligned}$$

cette dernière égalité car λ (donc ${}^x\lambda$) est cuspidal, d'où le lemme. ■

Le théorème 17.4 est une conséquence immédiate du lemme 17.5, car si $\langle \chi, R^{\mathbf{G}}_{\mathbf{L}}\lambda \rangle_{\mathbf{G}^F}$, et $\langle \chi, R^{\mathbf{G}}_{\mathbf{M}}\mu \rangle_{\mathbf{G}^F}$ sont non nuls, alors $\langle R^{\mathbf{G}}_{\mathbf{L}}\lambda, R^{\mathbf{G}}_{\mathbf{M}}\mu \rangle_{\mathbf{G}^F}$ est évidemment non nul. ■

Si λ est cuspidale, on a par 17.5: $\langle R^{\mathbf{G}}_{\mathbf{L}}\lambda, R^{\mathbf{G}}_{\mathbf{L}}\lambda \rangle_{\mathbf{G}^F} = |W_{\mathbf{G}^F}(\mathbf{L},\lambda)|$. En fait, par un théorème fondamental de Howlett et Lehrer, $\mathrm{End}_{\mathbf{G}^F}(R^{\mathbf{G}}_{\mathbf{L}}(\lambda))$ est une algèbre de Hecke associée au groupe $W_{\mathbf{G}^F}(\mathbf{L},\lambda)$ (le résultat initial de Howlett et Lehrer (1980) obtenait une telle algèbre tordue par un cocycle; Lusztig (1984) quand $\mathbf{G}$ est à centre connexe, puis Geck (1993) 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 $\langle \rho_\chi, R_{\mathbf{L}}^{\mathbf{G}}\lambda \rangle_{\mathbf{G}^F} = \dim \chi$.

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 $\{\rho_\chi \mid \chi \in \mathrm{Irr}(W_{\mathbf{G}^F}(\mathbf{L},\lambda))\}$ est appelé la **série de Harish-Chandra** associée à $(\mathbf{L},\lambda)$. On appelle aussi parfois l'union de telles séries quand λ parcourt l'ensemble des représentations cuspidales de $\mathbf{L}^F$ la série de Harish-Chandra associée à $\mathbf{L}$. Quand $\mathbf{L} = \mathbf{T}$, un tore maximal inclus dans un sous-groupe de Borel rationnel, 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.

18. Cohomologie l-adique.

Soit $\mathbf{X}$ une variété algébrique sur $\overline{\mathbb{F}}_q$ et soit ℓ un nombre premier différent de la caractéristique p de $\overline{\mathbb{F}}_q$. Les travaux de Grothendieck permettent d'associer à $\mathbf{X}$ des groupes de cohomologie l-adique à support compact $H_c^i(\mathbf{X},\overline{\mathbb{Q}}_\ell)$ qui sont des $\overline{\mathbb{Q}}_\ell$-espaces vectoriels de dimension finie possédant de nombreuses propriétés intéressantes. Ces groupes de cohomologie nous serviront à définir l'induction de Deligne et Lusztig. Pour rester dans le cadre du chapitre 12, nous supposerons ci-dessous que les variétés sont quasi-projectives (ouverts d'une variété projective). On parle aussi de cohomologie "à support propre". Un morphisme *propre* est le pendant en géométrie algébrique d'un morphisme compact: c'est un morphisme séparé, de type fini, et universellement fermé (i.e. il reste fermé par tout changement de base). Un morphisme fini est propre, et si $f \circ g$ est propre et f séparé, alors g est propre. En particulier, un endomorphisme d'ordre fini, ou dont une puissance est un endomorphisme de Frobenius, est propre. Énonçons une première série de propriétés essentielles de la cohomologie ℓ-adique.

18.1 Proposition.

(i) *On a* $H_c^i(\mathbf{X},\overline{\mathbb{Q}}_\ell) = 0$ *si* $i \notin [0,\dots,2\dim \mathbf{X}]$.

(ii) *Tout morphisme propre* $f : \mathbf{X} \to \mathbf{X}$ *induit une application linéaire* f^* *sur* $H_c^i(\mathbf{X},\overline{\mathbb{Q}}_\ell)$ *et cette correspondance est fonctorielle.*

(iii) *Si* F *est un endomorphisme de Frobenius pour une* $\mathbb{F}_q$*-structure sur* $\mathbf{X}$*, alors* F^* *est inversible et on a on a* $|\mathbf{X}^F| = \sum_i (-1)^i \,\mathrm{Trace}(F^* \mid H_c^i(\mathbf{X},\overline{\mathbb{Q}}_\ell))$.

Notons que par (i) la somme de (iii) est finie. On notera $H_c^*(\mathbf{X}) = \sum_i (-1)^i H_c^i(\mathbf{X},\overline{\mathbb{Q}}_\ell)$ qui est donc un $\overline{\mathbb{Q}}_\ell$-espace vectoriel virtuel de dimension finie. La propriété (iii) est appelée "formule de traces" ou "théorème de Lefschetz", et est fondamentale. Si $g \in \mathrm{Aut}(\mathbf{X})$ est d'ordre fini, on pose $\mathcal{L}(g,\mathbf{X}) = \mathrm{Trace}(g^* \mid H_c^*(\mathbf{X}))$ et on l'appelle *nombre de Lefschetz* de g sur $\mathbf{X}$. Par 14.3 (vii) et (iv), g commute à une puissance de F, donc pour n assez divisible gF^n ayant une puissance égale à la même puissance de F^n est un endomorphisme de Frobenius, et vérifie (iii).

18.2 Corollaire. *Soit $g \in \mathrm{Aut}(\mathbf{X})$ d'ordre fini. Définissons une série formelle $R(t) = -\sum_n |\mathbf{X}^{gF^n}| t^n$ où la somme porte sur les $n > 0$ tels que F^n commute à g. Alors $\mathcal{L}(g, \mathbf{X}) = R(t)|_{t=\infty}$, et est un entier rationnel indépendant de ℓ.*

(On voit ici la puissance de la cohomologie l-adique, qui affirme que $R(t)|_{t=\infty}$ représente la valeur d'un caractère de tout sous-groupe fini de $\mathrm{Aut}(\mathbf{X})$, ce qu'on ne sait pas démontrer autrement).

Preuve: Soit n_0 le plus petit entier tel que g commute à F^{n_0}; il existe une base de $H_c^*(\mathbf{X})$ où g et F^{n_0} sont simultanément triangularisés. Soient $\lambda_1, \ldots, \lambda_k$ les valeurs propres de F^{n_0} et $x_1, \ldots, x_k$ celles de g dans cette base. Puisque gF^n est encore un endomorphisme de Frobenius pour tout n tel que F^n commute à g, on a par 18.1(iii)

$$R(t) = -\sum_{n_0 | n} \sum_{i=1}^{k} \lambda_i^{n/n_0} x_i t^n = \sum_{i=1}^{k} x_i \frac{-\lambda_i t^{n_0}}{1 - \lambda_i t^{n_0}}$$

L'indépendance de ℓ de $R(t)$ résulte de cette formule car il n'y apparaît pas; cette formule montre aussi que $R(t)$ est une fraction rationnelle, et que $R(t)|_{t=\infty} = \sum_{i=1}^k x_i$. Étant une série formelle à coefficients entiers, $R(t)$ est une fraction rationnelle à coefficients entiers. Donc $\mathcal{L}(g, \mathbf{X})$ est un nombre rationnel, mais c'est un entier algébrique en tant que $\sum_{i=1}^k x_i$ car les x_i sont des racines de l'unité du même ordre que g, donc c'est un entier. ■

Nous allons maintenant donner une série de propriétés des nombres de Lefschetz. Quand ces propriétés peuvent se démontrer directement à partir de 18.2 nous le ferons; nous indiquerons aussi à chaque fois sans preuve le théorème correspondant sur la cohomologie l-adique quand il existe.

18.3 Proposition.

(i) Soit $\mathbf{X} = \mathbf{X}_1 \coprod \mathbf{X}_2$ une partition de $\mathbf{X}$ en deux sous-variétés où $\mathbf{X}_1$ est ouvert (donc $\mathbf{X}_2$ fermé). On a une suite exacte longue de cohomologie

$$\ldots \to H_c^i(\mathbf{X}_1, \overline{\mathbb{Q}}_\ell) \to H_c^i(\mathbf{X}, \overline{\mathbb{Q}}_\ell) \to H_c^i(\mathbf{X}_2, \overline{\mathbb{Q}}_\ell) \to H_c^{i+1}(\mathbf{X}_1, \overline{\mathbb{Q}}_\ell) \to \ldots,$$

et en particulier $H_c^*(\mathbf{X}) = H_c^*(\mathbf{X}_1) + H_c^*(\mathbf{X}_2)$ comme espaces vectoriels virtuels. Les morphismes de connexion sont nuls si $\mathbf{X}_1$ est aussi fermé.

(ii) Soit $\mathbf{X} = \coprod_j \mathbf{X}_j$ une partition finie de $\mathbf{X}$ en sous variétés localement fermées; alors si $g \in \mathrm{Aut}\,\mathbf{X}$ d'ordre fini stabilise cette partition on a $\mathcal{L}(g, \mathbf{X}) = \sum_{\{j \mid {}^g\mathbf{X}_j = \mathbf{X}_j\}} \mathcal{L}(g, \mathbf{X}_j)$.

Preuve de (ii): Soit F un endomorphisme de Frobenius commutant à g et stabilisant $\mathbf{X}_j$ pour tout j (*cf.* 14.3 vii). L'assertion (ii) est immédiate à partir de 18.2 et de l'égalité $|\mathbf{X}^{gF^n}| = \sum_j |\mathbf{X}_j^{gF^n}|$. ■

18.4 Proposition. *Soit $\mathbf{X}$ une variété sur $\overline{\mathbb{F}}_q$ réduite à un ensemble fini de points. Alors:*

(i) $H_c^i(\mathbf{X}, \overline{\mathbb{Q}}_\ell) = 0$ si $i \neq 0$ et $H_c^0(\mathbf{X}, \overline{\mathbb{Q}}_\ell) \simeq \overline{\mathbb{Q}}_\ell[\mathbf{X}]$.

(ii) Toute bijection g sur l'ensemble fini $\mathbf{X}$ induit un automorphisme de la variété $\mathbf{X}$, et agit de façon naturelle sur $H_c^*(\mathbf{X}) \simeq \overline{\mathbb{Q}}_\ell[\mathbf{X}]$ comme module de permutation; on a $\mathcal{L}(g, \mathbf{X}) = |\mathbf{X}^g|$.

Preuve: C'est une conséquence immédiate de 18.1 et de 18.3. ■

18.5 Proposition. *Soient $\mathbf{X}$ et $\mathbf{X}'$ deux variétés. On a:*
(i) $H_c^k(\mathbf{X}\times\mathbf{X}',\overline{\mathbb{Q}}_\ell)\simeq\bigoplus_{i+j=k}H_c^i(\mathbf{X},\overline{\mathbb{Q}}_\ell)\otimes_{\overline{\mathbb{Q}}_\ell}H_c^j(\mathbf{X}',\overline{\mathbb{Q}}_\ell)$ *("Théorème de Kunneth").*
(ii) Soit $g\in\operatorname{Aut}\mathbf{X}$ *(resp.* $g'\in\operatorname{Aut}\mathbf{X}'$*) d'ordre fini. On a alors* $\mathcal{L}(g\times g',\mathbf{X}\times\mathbf{X}')=\mathcal{L}(g,\mathbf{X})\mathcal{L}(g',\mathbf{X}')$.

Preuve de (ii): Notons $f*g=\sum_{i\geq0}a_ib_it^i$ le produit de Hadamard de deux séries formelles $f=\sum_{i\geq0}a_it^i$ et $g=\sum_{i\geq0}b_it^i$. Il faut montrer que les séries $f=\sum_{n\geq1}|\mathbf{X}^{gF^n}|t^n$ et $g=\sum_{n\geq1}|\mathbf{X}'^{g'F^n}|t^n$ vérifient $-(f*g)|_{t=\infty}=-f|_{t=\infty}\times-g|_{t=\infty}$. On voit que c'est le cas en suivant la preuve de 18.2, car ces séries sont combinaison linéaires de séries de la forme $\frac{t}{1-\lambda t}$ qui ont cette propriété. ■

18.6 Proposition. *Soit $H\subset\operatorname{Aut}\mathbf{X}$ un groupe fini tel que le quotient $\mathbf{X}/H$ existe (c'est toujours le cas si $\mathbf{X}$ est quasi-projective), et soit $g\in\operatorname{Aut}\mathbf{X}$ d'ordre fini commutant à tous les éléments de H; alors:*
(i) On a un isomorphisme de $\overline{\mathbb{Q}}_\ell[g]$-modules: $H_c^i(\mathbf{X})^H\simeq H_c^i(\mathbf{X}/H)$.
(ii) $\mathcal{L}(g,\mathbf{X}/H)=|H|^{-1}\sum_{h\in H}\mathcal{L}(gh,\mathbf{X})$.

Preuve de (ii): Cela résulte de ce que, si on choisit un endomorphisme de Frobenius F de telle sorte que g et tous les éléments de H soient rationnels, alors on a clairement:

$$|(\mathbf{X}/H)^{gF^n}|=|H|^{-1}\sum_{h\in H}|\mathbf{X}^{ghF^n}|$$

■

18.7 Proposition. *Soit $\mathbf{X}$ un espace affine de dimension n. Alors:*
(i) $\dim H_c^i(\mathbf{X},\overline{\mathbb{Q}}_\ell)=\begin{cases}1, & \text{si } i=2n\\ 0, & \text{sinon}\end{cases}$.
(ii) Si F est l'endomorphisme de Frobenius associé à une $\mathbb{F}_q$-structure quelconque sur $\mathbf{X}$, on a $|\mathbf{X}^F|=q^n$.
(iii) Pour tout $g\in\operatorname{Aut}(\mathbf{X})$ d'ordre fini, on a $\mathcal{L}(g,\mathbf{X})=1$.

Preuve de (ii) et (iii): Soit λ le scalaire par lequel F agit sur $H_c^{2n}(\mathbf{X},\overline{\mathbb{Q}}_\ell)$; pour tout $m>0$ on a $|\mathbf{X}^{F^m}|=\lambda^m$ donc λ est un entier. D'autre part, si $A=A_\circ\otimes_{\mathbb{F}_q}\overline{\mathbb{F}}_q$ est la $\mathbb{F}_q$-structure associée à F, alors il existe n_0 tel que $A_0\otimes_{\mathbb{F}_q}\mathbb{F}_{q^{n_0}}\simeq\mathbb{F}_{q^{n_0}}[T_1,\dots,T_n]$; en effet, $A\simeq\overline{\mathbb{F}}_q[T_1,\dots,T_n]$ et si $A_\circ$ est engendrée par $t_1,\dots,t_k$ il existe n_0 tel que $t_i\in\mathbb{F}_{q^{n_0}}[T_1,\dots,T_n]$ et alors $A_\circ\otimes_{\mathbb{F}_q}\mathbb{F}_{q^{n_0}}\subset\mathbb{F}_{q^{n_0}}[T_1,\dots,T_n]$ donc on a égalité puisque ce sont deux $\mathbb{F}_{q^{n_0}}$-espaces vectoriels qui deviennent égaux après tensorisation par $\overline{\mathbb{F}}_q$. Donc pour m multiple de n_0, on a $|\mathbf{X}^{F^m}|=q^{mn}$, donc $\lambda=q^n$, ce qui prouve (ii); (iii) s'en déduit immédiatement. ■

18.8 Proposition. *Soit $\mathbf{X}\xrightarrow{\pi}\mathbf{X}'$ un épimorphisme dont toutes les fibres sont isomorphes à un espace affine de dimension n. Soit $g\in\operatorname{Aut}\mathbf{X}$ (resp. $g'\in\operatorname{Aut}\mathbf{X}'$) tels que $g'\pi=\pi g$, alors:*
(i) $H_c^i(\mathbf{X},\overline{\mathbb{Q}}_\ell)\simeq H_c^{i-2n}(\mathbf{X}',\overline{\mathbb{Q}}_\ell)(-n)$*, (un "Tate twist", c'est-à-dire que le $\overline{\mathbb{Q}}_\ell[g]$-module $H_c^i(\mathbf{X},\overline{\mathbb{Q}}_\ell)$ est isomorphe au $\overline{\mathbb{Q}}_\ell[g']$-module $H_c^{i-2n}(\mathbf{X}',\overline{\mathbb{Q}}_\ell)$ par $g\mapsto g'$, et que pour toute structure rationnelle sur $\mathbf{X}$ (resp. $\mathbf{X}'$) compatible avec π,g,g' l'action de F sur $H_c^i(\mathbf{X},\overline{\mathbb{Q}}_\ell)$ est q^n fois celle de F sur $H_c^{i-2n}(\mathbf{X}',\overline{\mathbb{Q}}_\ell)$).*

(ii) $\mathcal{L}(g,\mathbf{X}) = \mathcal{L}(g',\mathbf{X}')$.

PREUVE DE (ii): Choisissons des structures rationnelles sur $\mathbf{X}$ et $\mathbf{X}'$ définies sur le même corps $\mathbb{F}_q$ et compatibles avec π, g et g'. Notons F l'endomorphisme de Frobenius sur $\mathbf{X}$ et sur $\mathbf{X}'$. D'après 18.7 on a $|\mathbf{X}^{gF^m}| = \sum_{y\in\mathbf{X}'^{g'F^m}} |\pi^{-1}(y)^{gF^m}| = |\mathbf{X}'^{g'F^m}|q^{mn}$, d'où le résultat. ■

18.9 PROPOSITION. *Soit* $\mathbf{G}$ *un groupe algébrique connexe agissant sur* $\mathbf{X}$. *Alors:*
(i) $\mathbf{G}$ *agit trivialement sur* $H_c^i(\mathbf{X},\overline{\mathbb{Q}}_\ell)$ *pour tout* i.
(ii) Pour tout $g\in\mathbf{G}$ *on a* $\mathcal{L}(g,\mathbf{X}) = \mathcal{L}(1,\mathbf{X})$.

PREUVE DE (ii): Choisissons des structures rationnelles sur $\mathbf{G}$ et sur $\mathbf{X}$ de façon que l'action de $\mathbf{G}$ soit rationnelle, *i.e.*$F(gx) = F(g)F(x)$ pour tout $(g,x)\in\mathbf{G}\times\mathbf{X}$. Pour tout n, par le théorème de Lang il existe $h\in\mathbf{G}$ tel que $h.^{F^n}h^{-1} = g$; alors $x\mapsto h^{-1}x$ est une bijection de $\mathbf{X}^{gF^n}$ sur $\mathbf{X}^{F^n}$, donc $|\mathbf{X}^{gF^n}| = |\mathbf{X}^{F^n}|$, d'où le résultat. ■

18.10 PROPOSITION. *Soit* $g = su$ *la décomposition en* p'*-partie et en* p*-partie de* $g\in\operatorname{Aut}\mathbf{X}$ *d'ordre fini. Alors* $\mathcal{L}(g,\mathbf{X}) = \mathcal{L}(u,\mathbf{X}^s)$.

PREUVE: Cette proposition ne peut pas se démontrer par une manipulation des nombres de Lefschetz; il faut utiliser directement les propriétés de la cohomologie l-adique. ■

19. L'induction de Deligne et Lusztig; formule de Mackey.

Nous nous plaçons toujours dans le cadre d'un groupe réductif $\mathbf{G}$ sur $\overline{\mathbb{F}}_q$ muni d'une isogénie F ayant un nombre fini de points fixes. On veut étendre la construction du foncteur $R_{\mathbf{L}}^{\mathbf{G}}$ au cas où $\mathbf{L}$ est un sous-groupe de Levi F-stable de $\mathbf{G}$ qui n'est le sous-groupe de Levi d'aucun sous-groupe parabolique F-stable.

19.1. EXEMPLE. On voudrait généraliser l'exemple 17.2 au cas des groupes unitaires, mais la construction qui y est utilisée ne marche pas, car l'image par l'endomorphisme de Frobenius de $\mathbf{U}_{n+m}$ du sous-groupe parabolique $\begin{pmatrix}\mathbf{U}_n & *\\ 0 & \mathbf{U}_m\end{pmatrix}$ est le sous-groupe parabolique $\begin{pmatrix}\mathbf{U}_n & 0\\ * & \mathbf{U}_m\end{pmatrix}$ qui est différent. En fait, si $n\neq m$, le sous-groupe de Levi rationnel $\begin{pmatrix}\mathbf{U}_n & 0\\ 0 & \mathbf{U}_m\end{pmatrix}$ n'est sous-groupe de Levi d'aucun sous-groupe parabolique rationnel.

L'idée de Deligne et Lusztig est d'associer à un sous-groupe parabolique quelconque $\mathbf{P}$ admettant $\mathbf{L}$ comme sous-groupe de Levi, une variété algébrique $\mathbf{X}$ sur $\overline{\mathbb{F}}_q$, munie d'actions de F, et de $\mathbf{G}^F\times\mathbf{L}^F$ qui commutent, et telle que, si $\mathbf{P} = {}^F\mathbf{P}$, alors $H_c^*(\mathbf{X},\overline{\mathbb{Q}}_\ell)\simeq\overline{\mathbb{Q}}_\ell[\mathbf{G}^F/\mathbf{U}^F]$. On définira alors $R_{\mathbf{L}}^{\mathbf{G}}$ à l'aide du $\mathbf{G}^F$-module-$\mathbf{L}^F$ défini par $H_c^*(\mathbf{X},\overline{\mathbb{Q}}_\ell)$.

19.2 DÉFINITION. *On définit le foncteur de Lusztig* $R_{\mathbf{L}\subset\mathbf{P}}^{\mathbf{G}}$ *comme le foncteur d'induction généralisée associé au* $\mathbf{G}^F$*-module-*$\mathbf{L}^F$ *donné par* $H_c^*(\mathcal{L}^{-1}(\mathbf{U}),\overline{\mathbb{Q}}_\ell)$, *où* $\mathcal{L}:\mathbf{G}\to\mathbf{G}$ *est l'application de Lang* $x\mapsto x^{-1\,F}x$, *et où* $\mathbf{P} = \mathbf{L}\mathbf{U}$ *est une décomposition de Levi de* $\mathbf{P}$.

L'action de $\mathbf{G}^F \times \mathbf{L}^F$ *provient de l'action sur* $\mathcal{L}^{-1}(\mathbf{U})$ *définie pour* $(g,l) \in \mathbf{G}^F \times \mathbf{L}^F$ *par* $x \mapsto gxl$ *pour tout* $x \in \mathcal{L}^{-1}(\mathbf{U})$.

Notons que, si $\mathbf{P}$ est F-stable, alors $\mathbf{U}$ aussi; et si $x \in \mathcal{L}^{-1}(\mathbf{U})$ alors ux aussi pour $u \in \mathbf{U}$. Donc on a un morphisme $\mathcal{L}^{-1}(\mathbf{U}) \to \mathbf{G}/\mathbf{U}$ donné par $x \mapsto x\mathbf{U}$, d'image $(\mathbf{G}/\mathbf{U})^F \simeq \mathbf{G}^F/\mathbf{U}^F$ et dont les fibres sont isomorphes à $\mathbf{U}$ qui est un espace affine, donc en appliquant 18.8 on obtient un isomorphisme de $\mathbf{G}^F$-modules-$\mathbf{L}^F$: $H_c^*(\mathbf{X}, \overline{\mathbb{Q}}_\ell) \simeq \overline{\mathbb{Q}}_\ell[\mathbf{G}^F/\mathbf{U}^F]$. Donc l'induction de Lusztig généralise celle de Harish-Chandra.

Tout comme l'induction de Harish-Chandra, l'induction de Lusztig vérifie:

19.3 Transitivité. *Soient* $\mathbf{P} \subset \mathbf{Q}$ *deux sous-groupes paraboliques de* $\mathbf{G}$, *tels qu'il existe un sous-groupe de Levi* F*-stable* $\mathbf{L}$ *de* $\mathbf{P}$ *et un sous-groupe de Levi* $\mathbf{M}$ *de* $\mathbf{Q}$ *avec* $\mathbf{M} \subset \mathbf{L}$. *Alors* $R^{\mathbf{G}}_{\mathbf{L}\subset\mathbf{P}} \circ R^{\mathbf{L}}_{\mathbf{M}\subset\mathbf{L}\cap\mathbf{Q}} = R^{\mathbf{G}}_{\mathbf{M}\subset\mathbf{Q}}$.

Preuve: Il faut démontrer (*cf.* 16.6) qu'on a un isomorphisme de $\mathbf{G}^F$-modules-$\mathbf{M}^F$

$$H_c^*(\mathcal{L}^{-1}(\mathbf{U})) \otimes_{\overline{\mathbb{Q}}_\ell[\mathbf{L}^F]} H_c^*(\mathcal{L}^{-1}(\mathbf{V}\cap\mathbf{L})) \simeq H_c^*(\mathcal{L}^{-1}(\mathbf{V}))$$

où $\mathbf{P} = \mathbf{L}\mathbf{U}$ et $\mathbf{Q} = \mathbf{M}\mathbf{V}$ sont les décompositions de Levi de $\mathbf{P}$ et $\mathbf{Q}$. Si $\mathbf{X}$ et $\mathbf{Y}$ sont des variétés algébriques sur lesquelles un groupe fini G agit, nous noterons $\mathbf{X} \times_G \underline{Y}$ le quotient de $\mathbf{X}\times\mathbf{Y}$ par l'action de G définie en faisant opérer $g \in G$ par (g, g^{-1}). Avec cette notation, de façon analogue à 16.6, le résultat vient de l'isomorphisme de variétés respectant l'action de $\mathbf{L}^F \times \mathbf{M}^F$ donné par $(x,l) \mapsto xl : \mathcal{L}^{-1}(\mathbf{U}) \times_{\mathbf{L}^F} \mathcal{L}^{-1}(\mathbf{V}\cap\mathbf{L}) \xrightarrow{\sim} \mathcal{L}^{-1}(\mathbf{V})$ et des propriétés 18.5 et 18.6 de la cohomologie. ■

Il est conjecturé que l'induction de Lusztig vérifie toujours la "formule de Mackey":

19.4 Conjecture/Théorème. *Soient* $\mathbf{P}$ *et* $\mathbf{Q}$ *deux sous-groupes paraboliques de* $\mathbf{G}$ *et* $\mathbf{L}$ *et* $\mathbf{M}$ *des sous-groupes de Levi* F*-stables respectivement de* $\mathbf{P}$ *et de* $\mathbf{Q}$. *Alors, si* $\operatorname{ad} x$ *dénote l'action de* x *par conjugaison sur les représentations, on a conjecturalement:*

$$^*R^{\mathbf{G}}_{\mathbf{L}\subset\mathbf{P}} \circ R^{\mathbf{G}}_{\mathbf{M}\subset\mathbf{Q}} = \sum_x R^{\mathbf{L}}_{\mathbf{L}\cap {}^x\mathbf{M}\subset\mathbf{L}\cap {}^x\mathbf{Q}} \circ {}^*R^{{}^x\mathbf{M}}_{\mathbf{L}\cap {}^x\mathbf{M}\subset\mathbf{P}\cap {}^x\mathbf{M}} \circ \operatorname{ad} x,$$

où x *parcourt des représentants de* $\mathbf{L}^F\backslash\mathcal{S}(\mathbf{L},\mathbf{M})^F/\mathbf{M}^F$, *où* $\mathcal{S}(\mathbf{L},\mathbf{M}) = \{x \in \mathbf{G} \mid \mathbf{L} \cap {}^x\mathbf{M}$ *contient un tore maximal de* $G\}$. *Cette formule est démontrée dans les cas suivants:*

(i) Quand $\mathbf{L}$ *ou* $\mathbf{M}$ *est un tore maximal.*

(ii) Quand q *est assez grand (par exemple,* $q > |W|^3$*).*

Preuve: La preuve de chacune des assertions est assez compliquée. Pour (i), voir [Digne-Michel], 11.13. Pour (ii), voir C. Bonnafé "formule de Mackey pour q grand", *J. Algebra* **201** (1998), 207–232. ■

Comme dans 17.1, le (i) montre l'indépendance de $R^{\mathbf{G}}_{\mathbf{T}\subset\mathbf{B}}$ du sous-groupe de Borel $\mathbf{B}$ utilisé, quand $\mathbf{L} = \mathbf{T}$ est un tore maximal. Les caractères $R^{\mathbf{G}}_{\mathbf{T}}(\theta)$ pour $\theta \in \operatorname{Irr}(\mathbf{T}^F)$ obtenus ainsi sont appelés *caractères de Deligne-Lusztig* (ils furent introduits en 1976 par ces deux auteurs). Une fonction de classe sur $\mathbf{G}^F$ est dite *uniforme* si elle est combinaison linéaire de ces caractères (cette notion est importante, car "presque toute" fonction est uniforme; en particulier Lusztig a montré que la fonction caractéristique des points F-stables d'une

classe géométrique l'est). On peut montrer comme conséquence de (i) que la formule de Mackey a lieu pour des fonctions uniformes, et donc qu'elle a lieu dans les groupes linéaires et unitaires (où on peut montrer que toute fonction est uniforme).

Explicitions la formule de Mackey dans le cas des caractères de Deligne-Lusztig.

19.5 Corollaire. *Soient T et T' deux tores maximaux F-stables. Alors*
(i) Pour $\theta \in \mathrm{Irr}(\mathbf{T}^F)$ (resp. $\theta' \in \mathrm{Irr}(\mathbf{T}'^F)$) on a

$$\langle R_{\mathbf{T}}^{\mathbf{G}}(\theta), R_{\mathbf{T}'}^{\mathbf{G}}(\theta') \rangle = \begin{cases} |W_{\mathbf{G}^F}(\mathbf{T},\theta)|, & \text{si } (\mathbf{T},\theta) \text{ et } (\mathbf{T}',\theta') \text{ sont } \mathbf{G}^F\text{-conjugués} \\ 0, & \text{sinon} \end{cases}$$

(où $W_{\mathbf{G}^F}(\mathbf{T},\theta)$ est comme dans 17.5).
(ii) En particulier, soient $\mathbf{T}_w$ (resp. $\mathbf{T}_{w'}$) des tores de type (cf. 15.11) la F-classe de $w \in W$ (resp. celle de w') par rapport à un tore $\mathbf{T}$ fixé de groupe de Weyl W, alors

$$\langle R_{\mathbf{T}_w}^{\mathbf{G}}(\mathrm{Id}), R_{\mathbf{T}_{w'}}^{\mathbf{G}}(\mathrm{Id}) \rangle = \begin{cases} |C_W(wF)|, & \text{si } w \text{ et } w' \text{ sont } F\text{-conjugués} \\ 0, & \text{sinon} \end{cases}.$$

Preuve: L'assertion (i) est une conséquence immédiate de la formule de Mackey. Le cas de nullité dans (ii) en résulte ainsi que de la définition du type d'un tore. La valeur $|C_W(wF)|$ vient de ce que $(\mathbf{T}_w, F)$ est conjugué à $(\mathbf{T}, wF)$. ■

20. Application des caractères de Deligne-Lusztig — l'ordre de $\mathbf{G}^F$.

Introduisons quelques définitions pour donner la dimension des caractères (virtuels) $R_{\mathbf{L}}^{\mathbf{G}}(\varphi)$. Soit $\mathbf{T}$ un tore maximal F-stable de $\mathbf{G}$ inclus dans un sous-groupe de Borel F-stable $\mathbf{B}$ et soit (W,S) le système de Coxeter sur $W = W(\mathbf{T})$ associé à ce sous-groupe de Borel. Alors (cf. 15.10) $(\mathbf{B}^F, N_{\mathbf{G}}(\mathbf{T})^F)$ est une (B,N)-paire pour $\mathbf{G}^F$ de système de Coxeter $(W^F, S/F)$. Tout sous-groupe parabolique F-stable de $\mathbf{G}$ est conjugué à un sous-groupe parabolique $\mathbf{P}_I \supset \mathbf{B}$ où I est une partie F-stable de S.

Définition. *Soit $\mathbf{P}$ un sous-groupe parabolique F-stable de $\mathbf{G}$. On définit le rang relatif $r(\mathbf{P})$ de $\mathbf{P}$ comme étant $|I/F|$ quand $\mathbf{P}$ est conjugué à $\mathbf{P}_I$ (c'est le rang de $\mathbf{P}^F$ dans la (B,N)-paire relative). Soit $\mathbf{T}'$ un tore maximal F-stable de $\mathbf{G}$. Alors on pose $r(\mathbf{T}',\mathbf{G}) = \min(r(\mathbf{P}))$ où $\mathbf{P}$ parcourt les sous-groupes paraboliques F-stables contenant $\mathbf{T}'$, et $\varepsilon(\mathbf{T}',\mathbf{G}) = (-1)^{r(\mathbf{T}',\mathbf{G})}$.*

On a donc $\varepsilon(\mathbf{T},\mathbf{G}) = 1$. La définition de ε s'étend naturellement à tous les sous-groupes réductifs de rang maximum de $\mathbf{G}$. Pour un tel sous-groupe $\mathbf{H}$, on pose $\varepsilon(\mathbf{H},\mathbf{G}) = (-1)^{\min(r(\mathbf{T}',\mathbf{G}))}$ où le minimum porte sur tous les tores maximaux F-stables de $\mathbf{H}$. On a alors:

20.1 Proposition. *Soit $\mathbf{L}$ un sous-groupe de Levi de $\mathbf{G}$, et soit φ un caractère de $\mathbf{L}^F$, alors* $\dim(R_{\mathbf{L}}^{\mathbf{G}}\varphi) = \varepsilon(\mathbf{L},\mathbf{G})|\mathbf{G}^F/\mathbf{L}^F|_{p'} \dim(\varphi)$.

Preuve: La preuve utilise la "dualité de Curtis", que nous n'avons pas abordé ici, donc nous ne pouvons pas la donner. Voir [Digne-Michel], 12.17 pour le cas où F est un endomorphisme de Frobenius. ■

20.2 PROPOSITION. *Si $\mathbf{T}_w$ est un tore maximal F-stable de type $w \in W(\mathbf{T})$ par rapport à un tore $\mathbf{T}$ inclus dans un sous-groupe de Borel F-stable, on a $\varepsilon(\mathbf{T}_w, \mathbf{G}) = (-1)^{l(w)}$, où $l(w)$ est la longueur de w dans le groupe de Weyl.*

PREUVE: Notons que l'énoncé a bien un sens, ce qui n'est pas évident car le type w de $\mathbf{T}_w$ n'est défini qu'à F-conjugaison près: mais $(-1)^{l(w)}$ est invariant par F-conjugaison. Soit V la représentation de réflexion de $W = W(\mathbf{T})$ définie en 2.4. On peut définir un endomorphisme τ de V normalisant W par $\tau(e_s) = e_{Fs}$. Nous allons d'abord démontrer que $r(\mathbf{T}_w, \mathbf{G}) = \dim V^\tau - \dim V^{w\tau}$ (ce qui a un sens car $\dim V^{w\tau}$ est invariant par F-conjugaison de w). Il y a bijection entre les sous-groupes paraboliques de $\mathbf{G}$ contenant $\mathbf{B}$ (donc de la forme $\mathbf{P}_I$) et les facettes de l'arrangement d'hyperplans correspondant à W de la forme $\mathcal{F}_{\mathbf{P}_I} = \{x \in V \mid \langle e_s, x \rangle > 0 \text{ si } s \notin I \text{ et } \langle e_s, x \rangle = 0 \text{ si } s \in I\}$ (cette bijection est par exemple donnée par le fait que $\mathrm{Stab}_W(\mathcal{F}_{\mathbf{P}_I}) = W_I$), et on a $r(\mathbf{P}_I) = \mathrm{codim}_{V^\tau}(\mathcal{F}_{\mathbf{P}_I} \cap V^\tau)$. En effet, τ étant défini par une permutation de la base e_s, une base de V^τ est donné par les $e_{\mathcal{O}} = \sum_{s \in \mathcal{O}} e_s$ où $\mathcal{O}$ parcourt les orbites de F dans S. En fait, si e_s^* est la base duale de e_s (considérée comme base de V en identifiant V à V^* via la forme $\langle\ ,\ \rangle$ qui est définie positive), on peut prendre comme base de V^τ les $e_{\mathcal{O}}$ pour $\mathcal{O} \subset I$ et les $e^*_{\mathcal{O}} = \sum_{s \in \mathcal{O}} e_s^*$ pour $\mathcal{O} \not\subset I$: en effet les premiers vecteurs sont dans $<e_s \mid s \in I>$ (donc orthogonaux à $\mathcal{F}_{\mathbf{P}_I}$), les seconds dans l'orthogonal, et ils sont en nombre voulu. Quand $\mathcal{O} \not\subset I$ les vecteurs $\sum_{\mathcal{O}' \not\subset I}(1 + \delta_{\mathcal{O},\mathcal{O}'})e^*_{\mathcal{O}'}$ sont dans $\mathcal{F}_{\mathbf{P}_I}$, d'où $\dim(\mathcal{F}_{\mathbf{P}_I} \cap V^\tau) = |(S - I)/F|$, d'où le résultat. Montrons maintenant que $r(\mathbf{T}_w, \mathbf{G}) \geq \dim V^\tau - \dim V^{w\tau}$. Soit $\mathbf{P}$ un sous-groupe parabolique F-stable de $\mathbf{G}$ contenant $\mathbf{T}_w$. Quitte à conjuguer $\mathbf{P}$ et $\mathbf{T}_w$ sous $\mathbf{G}^F$, on peut supposer que $\mathbf{P} = \mathbf{P}_I \supset \mathbf{B}$. Alors $\mathbf{T}_w$ et $\mathbf{T}$ sont $\mathbf{P}$-conjugués, donc quitte à remplacer w par un F-conjugué on peut supposer $w \in \mathbf{P}_I$, i.e. $w \in W_I$; alors w agit trivialement sur $\mathcal{F}_{\mathbf{P}_I}$, et $r(\mathbf{P}) = \dim V^\tau - \dim(\mathcal{F}_{\mathbf{P}} \cap V^\tau) = \dim V^\tau - \dim(\mathcal{F}_{\mathbf{P}} \cap V^{w\tau}) \geq \dim V^\tau - \dim V^{w\tau}$. Réciproquement, toute facette rencontrant $V^{w\tau}$ est $w\tau$-stable; il existe une telle facette qui rencontre $V^{w\tau}$ suivant un ouvert de cet espace. Quitte à F-conjuguer w, on peut supposer cette facette de la forme $\mathcal{F}_{\mathbf{P}_I}$. Notons que si $\mathbf{P}_I$ est wF-stable, il est à la fois w-stable et F-stable, car les deux sous-groupes paraboliques $\mathbf{P}_I$ et ${}^F\mathbf{P}_I$ contenant $\mathbf{B}$ ne peuvent être conjugués s'ils sont distincts. Donc $w \in W_I$; prenant $x \in \mathbf{P}_I$ tel que $x^{-1\,F}x = w$, le tore ${}^x\mathbf{T}$ est de type w et est dans $\mathbf{P}_I$, donc $r(\mathbf{T}_w, \mathbf{G}) \leq r(\mathbf{P}_I) = \dim V^\tau - \dim(\mathcal{F}_{\mathbf{P}_I} \cap V^\tau) = \dim V^\tau - \dim(\mathcal{F}_{\mathbf{P}_I} \cap V^{w\tau}) = \dim V^\tau - \dim(V^{w\tau})$. Observons maintenant que si f est un automorphisme d'ordre fini d'un espace vectoriel réel, alors $(-1)^{\dim V - \dim V^f} = \det(f)$. En effet les valeurs propres de f qui ne sont pas égales à 1 ou -1 viennent par paires de racines de l'unité conjuguées. On en déduit $(-1)^{\dim V^\tau - \dim(V^{w\tau})} = \det(\tau)\det(w\tau) = \det(w) = (-1)^{l(w)}$. ■

Notons que si F est un endomorphisme de Frobenius attaché à une $\mathbb{F}_q$-structure, on peut aussi prendre à la place de V dans la preuve ci-dessus l'espace $X(\mathbf{T}) \otimes \mathbb{R}$, sur lequel F agit par un endomorphisme de la forme $q\tau$.

Nous pouvons aussi donner une formule pour l'ordre $|\mathbf{T}_w^F|$.

20.3. PROPOSITION. *Soit $\mathbf{T}$ un tore F-stable, et choisissons un plongement $i : \overline{\mathbb{F}}_q{}^\times \hookrightarrow \overline{\mathbb{Q}}_\ell{}^\times$. Alors*

(i) La suite $0 \to X(\mathbf{T}) \xrightarrow{F-1} X(\mathbf{T}) \to \mathrm{Irr}(\mathbf{T}^F) \to 1$ est exacte, où $\mathrm{Irr}(\mathbf{T}^F)$ représente les caractères irréductibles de $\mathbf{T}^F$ dans $\overline{\mathbb{F}}_q$.

(ii) On a $|\mathbf{T}^F| = |\det(F-1 \mid X(\mathbf{T})\otimes\mathbb{R})|$.

PREUVE: On a une suite exacte $1 \to \mathbf{T}^F \to \mathbf{T} \xrightarrow{F-1} \mathbf{T} \to 1$. On en déduit la suite exacte de l'énoncé en appliquant le foncteur X, qui est exact (*cf.* par exemple [Borel, "Linear algebraic groups", 8.3]).

Le (ii) en résulte immédiatement: pour tout endomorphisme ϕ de conoyau fini du réseau $X(\mathbf{T})$, le théorème de la base adaptée montre que l'indice du sous-réseau $\phi(X(\mathbf{T}))$ est $|\det\phi|$. ■

20.4 PROPOSITION. *La projection orthogonale sur les fonctions uniformes est donnée par l'opérateur* $p_u = |W|^{-1}\sum_{w\in W} R^{\mathbf{G}}_{\mathbf{T}_w} \circ {}^*R^{\mathbf{G}}_{\mathbf{T}_w} = \sum_{\mathbf{T}} |W(\mathbf{T})^F|^{-1} R^{\mathbf{G}}_{\mathbf{T}} \circ {}^*R^{\mathbf{G}}_{\mathbf{T}}$ *où la deuxième somme porte sur des représentants des* $\mathbf{G}^F$*-classes de tores maximaux rationnels.*

PREUVE: L'égalité des deux expressions pour p_u est un calcul immédiat. L'image de p_u étant clairement uniforme, il suffit de vérifier que pour tout $\chi \in \mathrm{Irr}(\mathbf{G}^F)$, tout tore maximal rationnel $\mathbf{T}$ et tout $\theta \in \mathrm{Irr}(\mathbf{T}^F)$, on a $\langle \chi, R^{\mathbf{G}}_{\mathbf{T}}(\theta)\rangle_{\mathbf{G}^F} = \langle p_u(\chi), R^{\mathbf{G}}_{\mathbf{T}}(\theta)\rangle_{\mathbf{G}^F}$. Utilisant la deuxième expression pour p_u on trouve

$$\begin{aligned}\langle p_u(\chi), R^{\mathbf{G}}_{\mathbf{T}}(\theta)\rangle_{\mathbf{G}^F} &= \langle \sum_{\mathbf{T}'} |W(\mathbf{T}')^F|^{-1} R^{\mathbf{G}}_{\mathbf{T}'} {}^*R^{\mathbf{G}}_{\mathbf{T}'}\chi, R^{\mathbf{G}}_{\mathbf{T}}(\theta)\rangle_{\mathbf{G}^F} \\ &= \sum_{\mathbf{T}'} \langle |W(\mathbf{T}')^F|^{-1} {}^*R^{\mathbf{G}}_{\mathbf{T}'}\chi, {}^*R^{\mathbf{G}}_{\mathbf{T}'} R^{\mathbf{G}}_{\mathbf{T}}(\theta)\rangle_{\mathbf{G}^F}\end{aligned}$$

or, par 19.5 on a:

$${}^*R^{\mathbf{G}}_{\mathbf{T}'} R^{\mathbf{G}}_{\mathbf{T}}(\theta) = \begin{cases} \sum_{w\in W(\mathbf{T})^F} {}^w\theta & \text{si } \mathbf{T} = \mathbf{T}' \\ 0 & \text{si } \mathbf{T} \text{ et } \mathbf{T}' \text{ ne sont pas } \mathbf{G}^F\text{-conjugués}\end{cases}$$

donc

$$\langle p_u(\chi), R^{\mathbf{G}}_{\mathbf{T}}(\theta)\rangle_{\mathbf{G}^F} = \langle {}^*R^{\mathbf{G}}_{\mathbf{T}}(\chi), |W(\mathbf{T})^F|^{-1} \sum_{w\in W(\mathbf{T})^F} {}^w\theta\rangle_{\mathbf{G}^F} = \langle \chi, R^{\mathbf{G}}_{\mathbf{T}}(\theta)\rangle_{\mathbf{G}^F}$$

(la dernière égalité utilise $R^{\mathbf{G}}_{\mathbf{T}}({}^w\theta) = R^{\mathbf{G}}_{\mathbf{T}}(\theta)$). ■

Montrons maintenant que l'identité est une fonction uniforme.

20.5 PROPOSITION. $\mathrm{Id}_{\mathbf{G}} = |W|^{-1}\sum_{w\in W} R^{\mathbf{G}}_{\mathbf{T}_w}(\mathrm{Id}_{\mathbf{T}_w})$

PREUVE: On a en général ${}^*R^{\mathbf{G}}_{\mathbf{L}}(\mathrm{Id}_{\mathbf{G}}) = \mathrm{Id}_{\mathbf{L}}$: en effet, par définition ${}^*R^{\mathbf{G}}_{\mathbf{L}}(\mathrm{Id}_{\mathbf{G}})$ est le caractère du $\mathbf{L}^F$-module $H^*_c(\mathcal{L}^{-1}(\mathbf{U}))^{\mathbf{G}^F}$; ce module est isomorphe à $H^*_c(\mathcal{L}^{-1}(\mathbf{U})/\mathbf{G}^F)$ (*cf.* 18.6); or l'application de Lang définit un isomorphisme de $\mathcal{L}^{-1}(\mathbf{U})/\mathbf{G}^F$ sur $\mathbf{U}$, d'où l'assertion par 18.7. L'expression de la proposition vaut donc $p_u(\mathrm{Id}_{\mathbf{G}})$. Il suffit alors de vérifier que $\mathrm{Id}_{\mathbf{G}}$ a même produit scalaire avec cette expression qu'avec elle-même. On trouve

$$\langle \mathrm{Id}_{\mathbf{G}}, |W|^{-1}\sum_{w\in W} R^{\mathbf{G}}_{\mathbf{T}_w}(\mathrm{Id}_{\mathbf{T}_w})\rangle_{\mathbf{G}^F} = |W|^{-1}\sum_{w\in W} \langle {}^*R^{\mathbf{G}}_{\mathbf{T}_w}(\mathrm{Id}_{\mathbf{G}}), \mathrm{Id}_{\mathbf{T}_w}\rangle_{\mathbf{T}_w^F} = 1$$

en utilisant encore que ${}^*R^{\mathbf{G}}_{\mathbf{T}_w}(\mathrm{Id}_{\mathbf{G}}) = \mathrm{Id}_{\mathbf{T}_w}$. ■

Nous pouvons en déduire une nouvelle formule pour $|\mathbf{G}^F|_{p'}$, à comparer avec 15.8(iii). Nous supposerons soit que F est un endomorphisme de Frobenius associé à une $\mathbb{F}_q$-structure, soit que $\mathbf{G}$ est un groupe semi-simple de type B_2 (resp. F_4, G_2) sur $\overline{\mathbb{F}}_p$ (où $p = 2$ (resp. 2, 3)) muni d'une isogénie F telle que $\mathbf{G}^F$ soit un groupe de Ree ou de Suzuki. Soit $\mathbf{T}$ un tore maximal F-stable d'un sous-groupe de Borel F-stable, et posons $V = X(\mathbf{T}) \otimes \mathbb{C}$. Si F est un endomorphisme de Frobenius, alors F détermine un endomorphisme de V de la forme $q\tau$, où τ est un automorphisme d'ordre fini de V normalisant $W \subset \mathrm{GL}(V)$. Dans le cas des groupes de Ree et Suzuki, si F^2 est un endomorphisme de Frobenius associé à une $\mathbb{F}_{q'^2p}$-structure, la même conclusion $F = q\tau$ a lieu en posant $q = q'\sqrt{p}$ (τ est alors une involution de V normalisant W et induisant sur ce dernier l'automorphisme non-trivial du diagramme de Coxeter). Il en résulte qu'on peut trouver des invariants homogènes algébriquement indépendants de degré minimal $f_1, \dots, f_r$ (où r est le rang de $\mathbf{G}$) dans l'algèbre symétrique S de V qui soient vecteurs propres de τ.

20.6. Théorème. *Soient $\varepsilon_1, \dots, \varepsilon_r$ les valeurs propres de τ sur $f_1, \dots, f_r$. Alors on a $|\mathbf{G}^F| = q^{\sum_i (d_i - 1)} \prod_{i=1}^r (q^{d_i} - \varepsilon_i)$ où d_i est le degré de f_i.*

Preuve: Prenant la valeur en 1 des deux membres de 20.5, de 20.1 et 20.2 on tire: $1 = |W|^{-1} \sum_{w \in W} (-1)^{l(w)} |\mathbf{G}^F|_{p'} / |\mathbf{T}^F_w|$, ce qui en tenant compte de 20.3(ii) donne $\frac{1}{|\mathbf{G}^F|_{p'}} = |W|^{-1} \sum_{w \in W} \frac{(-1)^{l(w)}}{|\det(wF - 1|V)|}$ (on a utilisé l'isomorphisme $(\mathbf{T}_w, F) \simeq (\mathbf{T}, wF)$). Utilisant que $F = q\tau$, le membre de droite se ré-écrit $|\mathbf{G}^F|^{-1}_{p'} = |W|^{-1} \sum_{w \in W} \frac{(-1)^{l(w)}}{|\det(qw\tau - 1|V)|}$ Mais $|\det(qw\tau - 1)| = \det(q - \tau^{-1}w^{-1})$, car $|\det w| = |\det \tau| = 1$ et le membre de droite est positif (car q est plus grand que les valeurs propres réelles de $\tau^{-1}w^{-1}$). On en déduit $(-1)^{l(w)} |\det(wF - 1)| = (-1)^{l(w)} \det(q - \tau^{-1}w^{-1}) = \det(w) \det(q - \tau^{-1}w^{-1}) = \det(\tau)^{-1} \det(qw\tau - 1)$. Mais (*cf.* preuve de 3.6) $(-1)^r \det(qw\tau - 1)^{-1} = \det(1 - qw\tau)^{-1}$ est égal à la valeur en q de la trace graduée $P_S(w\tau)$. On obtient en fin de compte $|\mathbf{G}^F|^{-1}_{p'} = \det \tau (-1)^r (|W|^{-1} \sum_{w \in W} P_S(w\tau)(q)) = \det \tau (-1)^r P_S(p_W \tau)(q)$ où p_W est le projecteur sur les invariants par W. Mais $P_S(p_W\tau) = P_{S^W}(\tau) = P_{\otimes_i \mathbb{C}[f_i]}(\tau) = \prod_i P_{\mathbb{C}[f_i]}(\tau)$, et clairement $P_{\mathbb{C}[f_i]}(\tau) = 1/(1 - \varepsilon_i t^{d_i})$. En mettant tout ensemble, on a le résultat pour $|\mathbf{G}^F|_{p'}$.

Pour la puissance de q, notons que $\sum_i (d_i - 1)$ est le nombre de réflexions de W, égal aussi à $l(w_0)$ ou au nombre de racines positives; cette puissance vient donc de 15.8(iii) dans le cas où F est un endomorphisme de Frobenius. Dans le cas des groupes de Ree et de Suzuki, elle résulte d'un calcul des nombres q_w que nous ne ferons pas ici. ■

21. Compléments sur les caractères de Deligne-Lusztig.

Pour tirer un parti maximum des caractères de Deligne-Lusztig, il faut:
- donner une façon de les calculer.
- Les décomposer en caractères irréductibles.

Pour le premier problème, on se ramène au cas des éléments unipotents:

21.1 Définition. *Soit $\mathbf{T}$ un tore maximal F-stable de $\mathbf{G}$. On appelle fonction de Green $Q_{\mathbf{T}}^{\mathbf{G}}$ la fonction définie sur l'ensemble $\mathbf{G}_u^F$ des éléments unipotents de $\mathbf{G}^F$ par: $u \mapsto R_{\mathbf{T}}^{\mathbf{G}}(\mathrm{Id})(u)$.*

21.2 Proposition (formule du caractère pour $R_{\mathbf{T}}^{\mathbf{G}}$ et ${}^*R_{\mathbf{T}}^{\mathbf{G}}$). *Soit $\mathbf{T}$ un tore maximal F-stable et soit ψ (resp. χ) un caractère de $\mathbf{G}^F$ (resp. $\mathbf{T}^F$), alors si $g = su$ est la décomposition de Jordan de $g \in \mathbf{G}^F$ on a:*

$$(R_{\mathbf{T}}^{\mathbf{G}}\chi)(g) = |C_{\mathbf{G}}^0(s)^F|^{-1} \sum_{\{\, h \in \mathbf{G}^F \mid s \in {}^h\mathbf{T}\,\}} Q_{{}^h\mathbf{T}}^{C_{\mathbf{G}}^0(s)}(u)\, {}^h\chi(s) \qquad (i)$$

et si $t \in \mathbf{T}^F$ on a:

$$({}^*R_{\mathbf{T}}^{\mathbf{G}}\psi)(t) = |\mathbf{T}^F||C_{\mathbf{G}}^0(t)^F|^{-1} \sum_{u \in C_{\mathbf{G}}^0(t)_u^F} Q_{\mathbf{T}}^{C_{\mathbf{G}}^0(t)}(u)\psi(tu) \qquad (ii)$$

Preuve: Voir [Digne-Michel, 12.2]. ■

On est ainsi ramené au calcul des fonctions de Green, qui est un problème compliqué, résolu par la théorie de la "correspondance de Springer". Mentionnons juste que $Q_{\mathbf{T}}^{\mathbf{G}}(1) = \dim R_{\mathbf{T}}^{\mathbf{G}}(\mathrm{Id})$ est donné par 20.1, et que si u est un élément unipotent régulier (une définition possible est qu'il existe un seul sous-groupe de Borel de $\mathbf{G}$ contenant u), alors $Q_{\mathbf{T}}^{\mathbf{G}}(u) = 1$.

On peut justifier que "presque toutes" les fonctions sont uniformes en donnant une formule qui montre que les fonctions caractéristiques des classes semi-simples sont uniformes (les éléments semi-simples sont denses dans $\mathbf{G}$):

21.3 Proposition. *Soit s un élément semi-simple de $\mathbf{G}^F$, et soit $\pi_s^{\mathbf{G}^F}$ la fonction sur $\mathbf{G}^F$ qui vaut $|C_{\mathbf{G}}(s)^F|$ sur la classe de conjugaison de s et 0 ailleurs, alors*

$$\pi_s^{\mathbf{G}^F} = \varepsilon_{C_{\mathbf{G}}^0(s)^F} |C_{\mathbf{G}}^0(s)^F|_p^{-1} \sum_{\mathbf{T} \ni s, \theta} \varepsilon_{\mathbf{T}}\theta(s^{-1}) R_{\mathbf{T}}^{\mathbf{G}}(\theta),$$

où la somme porte sur les tores maximaux F-stables $\mathbf{T}$ contenant s et pour chaque tore sur les caractères θ de $\mathbf{T}^F$. En particulier la représentation régulière $\mathrm{reg}_{\mathbf{G}}$ de $\mathbf{G}^F$ est une fonction uniforme, et vaut

$$\mathrm{reg}_{\mathbf{G}} = |\mathbf{G}^F|_p^{-1} \sum_{\mathbf{T},\theta} \varepsilon_{\mathbf{G}}\varepsilon_{\mathbf{T}} R_{\mathbf{T}}^{\mathbf{G}}(\theta).$$

Preuve: Voir [Digne-Michel], 12.20. ■

La décomposition des caractères de Deligne-Lustig en caractères irréductibles est un autre problème compliqué, qui a été résolu par Lusztig en 1988 (dans le cas des groupes à centre connexe, en 1984 dans le livre "Characters of reductive groupes over a finite field", Annals of math. studies N^0**107**, Princeton university press). Mentionnons juste que si $\mathbf{G} = \mathrm{GL}_n$, et que $\chi \in \mathrm{Irr}(W)$, alors $R_\chi = |W|^{-1}\sum_{w \in W} \chi(w) R_{\mathbf{T}_w}^{\mathbf{G}}(\mathrm{Id})$ est un caractère irréductible. Dans les autres groupes, R_χ est une "approximation" d'un caractère irréductible, et les R_χ (dont la dimension est le "degré fantôme" χ, évalué en q), sont reliés au caractères irréductibles par une "transformée de fourier non-commutative".