REPRESENTATION THEORY
An Electronic Journal of the American Mathematical Society
Volume 10, Pages 1–20 (January 6, 2006)
S 1088-4165(06)00185-3

ALGÈBRES DE HECKE AFFINES GÉNÉRIQUES

MARIE-FRANCE VIGNÉRAS

Résumé. Soit H l'algèbre de Hecke du groupe de Weyl W d'une donnée radicielle basée $(X, X^\vee, R, R^\vee, B)$, et d'un poids générique $(q_w)_{w\in W}$. Nous montrerons que H est un module de type fini sur son centre, et que le centre est une algèbre à engendrement fini. Ceci était connu après inversion du poids, mais il est essentiel de ne pas inverser le poids, dans l'étude des modules des algèbres de Hecke affines qui apparaissent naturellement dans la théorie des représentations des groupes réductifs p-adiques sur un corps p-adique ou de caractéristique p. Des applications de ces théorèmes de finitude à la théorie des modules sont donnés dans une seconde partie. Dans une troisième partie, on explicitera les résultats pour le groupe $GL(n)$, et l'on introduira pour ce groupe, les modules supersinguliers.

Introduction

Chapitre 1. L'algèbre de Hecke générique H est un module libre sur l'algèbre de polynômes générique $\mathbf{Z}[q_w, w \in W]$ (notée $\mathbf{Z}[q_*]$ dans la suite), ayant une base naturelle $(T_w)_{w\in W}$, appelée la "base de Iwahori-Matsumoto". Le groupe de Weyl fini W_o du système de racines R agit naturellement sur X. Le groupe de Weyl W de la donnée radicielle est le produit semi-direct $W = W_oX$. Les éléments T_w sont inversibles dans l'algèbre $H[q_*^{-1}]$ obtenue après inversion des poids $q_w, w \in W$. Suivant Bernstein et Lusztig, il existe une application $x \to \tilde\theta_x$ de X dans l'algèbre de Hecke $H[q_*^{-1/2}]$ obtenue après addition des inverses des racines carrées des poids, identifiant l'algèbre de groupe $\mathbf{Z}[q_*^{\pm 1/2}][X]$ à une sous-algèbre commutative A de $H[q_*^{-1/2}]$. Pour un élément $w = (w_o, x)$ de W, nous posons $E_w := q_w^{1/2}\tilde T_{w_o}\tilde\theta_x$. Nous montrons, sans utiliser la théorie de Bernstein-Lusztig, en étudiant le développement de $T_wT_{v^{-1}}^{-1}$ sur la base de Iwahori-Matsumoto pour tout $w, v \in W$, le résultat fondamental suivant:

Théorème 1. *$(E_w)_{w\in W}$ est une base de l'algèbre de Hecke générique H sur $\mathbf{Z}[q_*]$, et la matrice de passage avec la base de Iwahori-Matsumoto $(T_w)_{w\in W}$ est triangulaire, de coefficients diagonaux* 1*, pour l'ordre de Chevalley-Bruhat.*

La base $(E_w)_{w\in W}$ de H sur $\mathbf{Z}[q_*]$ a des propriétés remarquables qui permettent de montrer que:

- *$H \cap A$ est un $\mathbf{Z}[q_*]$-module libre de base $(E_x = q_x^{1/2}\tilde\theta_x)_{x\in X}$,*
- *H est un $H \cap A$-module à droite de type fini.*

Received by the editors January 22, 2003 and, in revised form, March 20, 2004.
2000 *Mathematics Subject Classification.* Primary 22E50, 11F33.

Comme $x \mapsto q_x$ est constante sur toute W_o-orbite de X, l'algèbre commutative $H \cap A$ est stable par l'action naturelle de W_o sur A, et le centre de H est $(H \cap A)^{W_o}$. Nous obtiendrons le théorème structural suivant:

Théorème 2. *L'algèbre de Hecke générique H est un module de type fini sur son centre $Z(H) = (H \cap A)^{W_o}$, le centre et $H \cap A$ sont des algèbres commutatives de type fini, et*

$$H = \bigoplus_{w_o \in W_o} T_{w_o} J(w_o)$$

pour des idéaux fractionnaires $J(w_o)$ de $A \cap H$.

En général les $A \cap H$-modules $J(w_o)$ ne sont plats, i.e. projectifs puisque $A \cap H$ est un anneau noetherien. Des contre-exemples ont été donnés par Rachel Ollivier pour les algèbres associées au groupe $GL(3)$.

Chapitre 2. Il contient des applications des théorèmes de finitude du chapitre 1 à la théorie des modules. On fixe un morphisme d'anneau commutatif $\phi : \mathbf{Z}[q_*] \to R$ et l'on note H_ϕ l'algèbre de Hecke spécialisée. Pour tout morphisme d'anneau $\chi : A \cap H \to R$ prolongeant ϕ, le module induit de χ,

$$I(\chi) := H \otimes_{A \cap H, \chi} R$$

(le H-module universel engendré par le caractère χ de $A \cap H$) est appelé un module standard (à gauche) de H_ϕ. Si les images des poids $q_s,\ s \in S$, sont inversibles et ont des racines carrées dans R (on peut se passer des racines carrées), c'est simplement le module induit de l'unique morphisme d'anneau $\chi_A : A \to R$ prolongeant χ,

$$I(\chi_A) = H[q_*^{-1/2}] \otimes_{A, \chi_A} R.$$

Le théorème 2 implique que:

- $I(\chi)$ est un R-module de type fini.
- Lorsque R est un corps algébriquement clos, un H_ϕ-module simple est de dimension finie si et seulement si $Z(H)$ agit par un caractère, appelé le caractère central.

Théorème 3. *Si R est un corps algébriquement clos, un H_ϕ-module simple de dimension finie est quotient d'un H_ϕ-module standard.*

Dans le cas classique, le théorème est aussi vrai avec *sous-module* au lieu de quotient. Je ne sais pas si cela reste vrai dans le cas où $\phi(q_s) = 0$ pour tout $s \in S$ de longueur non nulle, apparaissant dans l'étude des représentations modulo p des groupes réductifs p-adiques.

Soit $\overline{\mathbf{Q}}_p$ une clôture algébrique du corps des nombres p-adiques, $\overline{\mathbf{Z}}_p$ son anneau d'entiers de corps résiduel $\overline{\mathbf{F}}_p$. On note $i_p : \overline{\mathbf{Z}}_p \to \overline{\mathbf{Q}}_p$ l'inclusion et $r_p : \overline{\mathbf{Z}}_p \to \overline{\mathbf{F}}_p$ la réduction. On fixe un morphisme d'anneau $\phi : \mathbf{Z}[q_*] \to \overline{\mathbf{Z}}_p$ tel que $\phi(q_s) \neq 0$ pour tout $s \in S$. La finitude de l'algèbre de Hecke générique H permettra de transférer certaines propriétés de la théorie classique des $H_{i_p\phi}$-modules à celle des $H_{r_p\phi}$-modules, par réduction.

Un $H_{i_p\phi}$-module V sera appelé entier s'il est engendré sur $\overline{\mathbf{Q}}_p$ par un sous-$\overline{\mathbf{Z}}_p$-module libre L stable par H_ϕ, appelé une structure entière de V. Pour un $H_{i_p\phi}$-module simple de dimension finie, la propriété d'être entier se voit sur le caractère central.

Théorème 4. *Un $H_{i_p\phi}$-module simple de dimension finie est entier si et seulement si son caractère central est entier.*

Tout caractère $\chi : A \cap H \to \overline{\mathbf{Q}}_p$ prolongeant ϕ s'étend en un caractère χ_A de A et s'identifie à un caractère χ_X de X en posant $\chi_A(\tilde{\theta}_x) = \chi_X(x)$ pour tout $x \in X$. L'isomorphisme de Bernstein-Lusztig $\tilde{\theta} : \mathbf{Z}[q_*^{\pm 1/2}][X] \simeq A$ n'est pas compatible aux structures entières naturelles puisque une $\mathbf{Z}[q_*]$-base de $A \cap H$ est $(E_x = q_x^{1/2}\tilde{\theta}_x)_{x\in X}$.

Théorème 4 (suite)**.** *Soit $\chi_X : X \to \overline{\mathbf{Q}}_p$ un caractère de X. Le $H_{i_p\phi}$-module standard $I(\chi_A)$ associé est entier si et seulement si $\chi_X(x)\phi(q_x)^{-1/2} \in \overline{\mathbf{Z}}_p$ pour tout $x \in X$.*

Comme q_x est constant sur une W_o-orbite de X, la condition est W_o-invariante. Le module standard est de dimension $|W_o|$ sur $\overline{\mathbf{Q}}_p$ et admet une base canonique: l'image canonique de $(T_{w_o})_{w_o\in W_o}$.

Théorème 5. *Soit $\chi : A \cap H \to \overline{\mathbf{Z}}_p$ un morphisme d'anneau prolongeant ϕ. Alors*

(i) *Le module standard $I(\chi, \overline{\mathbf{Q}}_p) := H \otimes_{i_p\chi} \overline{\mathbf{Q}}_p = I(\chi) \otimes_{i_p} \overline{\mathbf{Q}}_p$ admet une structure entière canonique contenant la base canonique, isomorphe au quotient de $I(\chi)$ par son sous-groupe de torsion $I(\chi)_{tor}$.*

(ii) *Les propriétés suivantes sont équivalentes:*
   - a) *Le module standard $I(\chi, \overline{\mathbf{F}}_p) := H \otimes_{r_p\chi} \overline{\mathbf{F}}_p = I(\chi) \otimes_{r_p} \overline{\mathbf{F}}_p$ est de dimension $|W_o|$ sur $\overline{\mathbf{F}}_p$.*
   - b) *La réduction de la structure entière canonique $M(\chi) := I(\chi)/I(\chi)_{tor}$ de $I(\chi, \overline{\mathbf{Q}}_p)$ est isomorphe au module standard $I(\chi, \overline{\mathbf{F}}_p)$.*
   - c) *Le $\overline{\mathbf{Z}}_p$-module $I(\chi)$ est sans torsion.357*

Elles sont vérifiées si le $A \cap H$-module à droite H est plat.

Lorsque $r_p\phi(q_s) = 0$ pour $s \in S$, les propriétés (ii) sont vérifiées pour $GL(2)$ mais pas pour $GL(3)$, d'après les résultats de Rachel Ollivier. Donc en général, le $A \cap H$-module à droite de type fini H n'est pas plat. Il serait intéressant de savoir s'il existe un caractère $\chi' : A \cap H \to \overline{\mathbf{Z}}_p$ de même réduction que χ mais tel que la réduction $r_pM(\chi')$ n'ait pas la même semi-simplifiée que $r_pM(\chi)$, et s'il existe un caractère χ tel que le noyau du morphisme canonique

$$I(\chi, \overline{\mathbf{F}}_p) \to \prod_{\chi', r_p(\chi')=r_p(X)} r_pM(\chi')$$

n'est pas nul.

Chapitre 3. Il contient une étude détaillée de l'algèbre de Hecke générique du groupe linéaire $GL(n)$, et l'introduction de ses modules supersinguliers.

Le groupe $X \simeq \mathbf{Z}^n$ s'identifie au groupe $Mor(GL(1), GL(n))$ des cocaractères sur lequel le groupe de Weyl fini W_o identifié à S_n, agit naturellement. Le groupe de Weyl W est isomorphe au produit semi-direct naturel $S_n\mathbf{Z}^n$. On a $q_s = q$ pour tout $s \in S$. L'algèbre de Hecke générique H est une $\mathbf{Z}[q]$-algèbre. On donnera (3.1-2) une description explicite de $A \cap H$ et de ses caractères dont on en déduira les résultats suivants. On fixe une spécialisation $\phi : \mathbf{Z}[q] \to \overline{\mathbf{Z}}_p$ telle que $\phi(q) \neq 0$ n'est pas une unité p-adique.

Théorème 6. *Pour $GL(n)$, tout caractère $\chi : A \cap H \to \overline{\mathbf{F}}_p$ nul sur q, se relève en un caractère $\tilde{\chi} : A \cap H \to \overline{\mathbf{Z}}_p$ tel que $\tilde{\chi}(q) = \phi(q)$.*

Il existe des $\overline{\mathbf{F}}_p$-représentations irréductibles de $GL(2, \mathbf{Q}_p)$ qui ne sont pas des sous-quotients d'induites paraboliques propres, appelées supersingulières. Par le foncteur des invariants par le sous-groupe d'Iwahori, elles sont en bijection avec des $H_{r_p\phi}$-modules simples standards. Une généralisation naturelle de ces modules est celle-ci:

Définition. Pour $GL(n)$, on dira qu'un $H_{r_p\phi}$-module ayant un caractère central ω est supersingulier, si ω se prolonge en un (unique) caractère de $A \cap H$ fixe par S_n.

Pour un caractère de $A \cap H$ nul sur q, *être fixe par S_n signifie être nul sur E_x pour tout $x \in X$ qui n'est pas une puissance du plongement diagonal δ de $GL(1)$ dans $GL(n)$*. La valeur en E_δ est toujours inversible car $E_\delta = T_\delta$ est inversible dans H. Pour $z \in \overline{\mathbf{F}}_p^*$, le caractère $A \cap H \to \overline{\mathbf{F}}_p$ nul sur q, fixe par S_n, tel que $\chi(E_\delta) = z$ sera noté χ_z, et sa restriction au centre sera notée ω_z. Le $H_{r_p\phi}$-module standard $I(\chi_z)$ est l'unique module standard supersingulier de caractère central ω_z.

Proposition 7. *Pour $GL(n)$, un module standard supersingulier $I(\chi_z)$ est de longueur $\geq 2^{n-2}$. Tout $H_{r_p\phi}$-module simple supersingulier de caractère central ω_z est quotient de $I(\chi_z)$. Pour $n = 2$, $I(\chi_z)$ est irréductible de dimension 2.*

Le cas $n = 2$ est traité dans un article précédent [Vignéras]. Le cas $n = 3$ est traité dans un article de Rachel Ollivier à paraitre au Journal of Algebra.

Les outils actuels de la théorie des représentations s'adaptent mal aux représentations lisses modulo p des groupes réductifs p-adiques pour lesquelles on ne sait pour ainsi dire rien. Ce travail est le premier pas vers une classification des modules simples modulo p de leurs algèbres de Hecke-Iwahori, problème qui semble plus accessible et qui est relié au précédent par le foncteur des invariants par un sous-groupe d'Iwahori. La situation est très différente de celle des groupes réductifs finis sur un corps de caractéristique p, où tous ces problèmes sont résolus: les modules simples modulo p sont classés par la théorie du plus haut poids, le foncteur des invariants par un sous-groupe de Borel respecte l'irréductibilité là où il ne s'annule pas, et les modules simples modulo p des algèbres de Hecke-Iwahori sont tous de dimension 1.

L'auteur remercie Rachel Ollivier dont les travaux sur les modules standards de type A_2 ont confirmé la possibilité d'une théorie intéressante des algèbres de Hecke affines de paramètre $q = 0$ et qui ont permis de corriger une version précédente du théorème 5, Jean-Francois Dat pour son étude parallèle des représentations entières p-adiques des groupes réductifs p-adiques, Peter Schneider et les participants de la conférence "Fonctorialité de Langlands: progrès recents" (Luminy, CIRM, 21/29 juin 2002) dans laquelle ces résultats furent exposés, l'Institut de Mathématiques de Jussieu pour un environnement de recherche remarquable, et le C.N.R.S. pour son soutien financier.

Chapitre 1

Soit $(X, X^\vee, R, R^\vee, B)$ une donnée radicielle basée réduite [Lusztig1 1 pp. 600-601]. Le groupe de Weyl fini W_o est le système de Coxeter avec $S_o = \{s_\alpha \mid \alpha \in B\}$ comme ensemble de réflexions simples; le produit semi-direct $W = W_o.X$ est le groupe de Weyl de la donnée radicielle; le groupe de Weyl affine est $W_{\mathit{aff}} :=$

$W_o.Q(R)$ où $Q(R)$ est le sous-$\mathbf{Z}$-module de X engendré par R. Il existe un sous-groupe commutatif Ω de W formé d'éléments tel que $W_{\mathit{aff}} \cap \Omega = \{1\}$ et $W = \Omega W_{\mathit{aff}}$.

Traditionellement la notation pour le produit est additive dans le $\mathbf{Z}$-module libre X et multiplicative dans les groupes W_o et dans W. Pour cette raison on notera e^x l'élément $x \in X$ plongé dans W qui s'écrira dorénavant

$$W = W_o e^X = \Omega W_{\mathit{aff}}.$$

Un élément général de W s'écrira donc $w = w_o e^x = u w_{\mathit{aff}}$ avec $w_o \in W_o,\ x \in X,\ u \in U,\ w_{\mathit{aff}} \in W_{\mathit{aff}}$, uniques. La valeur en e^x d'une fonction $w \to f_w$ sur W sera aussi notée f_x.

Soit R_m l'ensemble des racines $\alpha \in R$ telles que $\alpha^\vee$ est minimal pour l'ordre partiel $\preceq$ défini sur les coracines $R^\vee$ par: $\alpha_1^\vee \preceq \alpha_2^\vee$ si $\alpha_2^\vee - \alpha_1^\vee \in \sum_{\alpha \in B} \mathbf{N}\alpha^\vee$. Le groupe de Weyl affine W_{aff} est un système de Coxeter avec

$$S = S_o \cup \{s_\alpha e^\alpha \mid \alpha \in R_m\}$$

comme ensemble de réflexions simples. Le groupe Ω normalise S. On note $\leq$ l'ordre de Chevalley-Bruhat, ℓ la longueur de W, définis par extension de l'ordre et de la longueur de (W_{aff}, S), et X_{dom} le monoide de type fini formé par les éléments dominants x de X, i.e. $(x, \alpha^\vee) \geq 0$ pour toute racine positive α. Les définitions et rappels ci-dessus sont détaillés dans l'appendice.

Algèbre de Hecke générique

L'algèbre de Hecke générique du groupe de Weyl de la donnée radicielle basée sera définie "à la Iwahori-Matsumoto" en utilisant la décomposition en produit semi-direct $W = \Omega W_{\mathit{aff}}$. Lorsque la donnée radicielle est torale, $W = \Omega = X$, l'algèbre de Hecke générique est simplement l'algèbre du groupe $\mathbf{Z}[X]$.

Poids générique. Lorsque la donnée radicielle basée est non torale, soient $(q_s)_{s \in S}$ des *indéterminées telles que* $q_s = q_{s'}$ *si* $s, s' \in S$ *sont conjugués dans* W.

La $\mathbf{Z}$-algèbre de polynômes engendrée par ces indéterminées est notée $\mathbf{Z}[q_*]$. On connait un critère pour que deux éléments de S soient conjugués dans W_{aff} [Bourbaki GAL, IV.1, proposition 3, p. 12]. Deux éléments de S peuvent être conjugués dans W sans l'être dans W_{aff}, et l'algèbre de polynômes associée à W est une spécialisation de celle associée à W_{aff}.

Pour tout $n \in \mathbf{N}^S$ on dit que $q_n := \prod_{s \in S} q_s^{n(s)}$ est un monôme en q_*. Si n est la fonction "multiplicité de s dans une décomposition réduite" de $w_{\mathit{aff}} \in W_{\mathit{aff}}$, alors le fait que $q_s = q_{s'}$ si s, s' sont conjuguées dans W, montre que le monôme q_n ne dépend pas de la décomposition réduite, et sera noté $q_{w_{\mathit{aff}}}$. On ne risque pas de contresens en posant $q_w = q_{w_{\mathit{aff}}}$ pour tout $w \in \Omega w_{\mathit{aff}} \Omega$. On a $q_w = q_{w^{-1}}$. On a $q_w = q_{w'}$ pour deux éléments conjugués w, w' de W. On notera $q_x = q_{e^x}$ pour $x \in X$. La fonction $x \to q_x$ est constante sur les W_o-orbites de X puisque $e^{w_o(x)} = w_o e^x w_o^{-1}$.

On dit que $(q_w)_{w \in W}$ est un poids générique de W.

1.1. Définition. L'algèbre de Hecke générique H est la $\mathbf{Z}[q_*]$-algèbre, libre de base $(T_w)_{w \in W}$ comme $\mathbf{Z}[q_*]$-module, de produit vérifiant les relations

- $(T_s + 1)(T_s - q_s) = 0$ pour tout $s \in S$,
- $T_{ww'} = T_w T_{w'}$ si $\ell(ww') = \ell(w) + \ell(w')$ pour tout $w, w' \in W$.

Remarque. Dans [Lusztig 1, 3.1, p. 606], l'algèbre $\mathbf{Z}[q_*]$ est remplacée par l'anneau des polynômes de Laurent $\mathbf{Z}[v^{\pm 1}]$, que l'on peut voir comme une localisation d'une spécialisation $\phi_L : \mathbf{Z}[q_*] \to \mathbf{Z}[v]$ définie par $\phi_L(q_s) = v^{2n_s}$ pour des entiers $(n_s \geq 0)_{s\in S}$ tels que $n_s = n_{s'}$ si s, s' sont conjuguées dans W. La $\mathbf{Z}[v]$-algèbre spécialisée H_{ϕ_L} est moins générale que H mais est suffisante pour les applications à la théorie des représentations des groupes réductifs p-adiques. La $\mathbf{Z}[v^{\pm 1}]$-algèbre $H_{\phi_L}[v^{-1}]$ est considérée dans [Lusztig 1, 3.2, p. 607] ou [Lusztig 3, 3, si $W = W_{\mathit{aff}}$].

Le groupe Ω se plonge dans H par $u \to T_u$, le $\mathbf{Z}[q_*]$-module libre de base $(T_w)_{w\in W_{\mathit{aff}}}$ est une sous-algèbre H_{aff} de H normalisée par $T_u, u \in \Omega$, et

$$H \simeq \mathbf{Z}[\Omega].H_{\mathit{aff}}.$$

L'algèbre H_{aff} est l'algèbre de Hecke générique de W_{aff}.

Les éléments de la base $(T_w)_{w\in W}$ deviennent inversibles si l'on inverse les paramètres, i.e., T_w est inversible dans la $\mathbf{Z}[q_*^{\pm 1}]$-algèbre $H[q_*^{-1}]$ qui contient H.

1.2. Lemme fondamental. *Soient $w, v \in W$. Alors*

1) $q_{wv}q_w^{-1}q_v = c_{w,v}^2$ *est le carré d'un monôme $c_{w,v}$ en q_* divisant q_v,*

2) *Soient $u \in \Omega$, $s_1, \dots, s_n \in S$ tels que $v \in W_{\mathit{aff}}u$ et $vu^{-1} = s_1 \dots s_n$ soit une décomposition réduite. Alors*

$$\begin{aligned} c_{w,v}T_wT_{v^{-1}}^{-1} = \ & T_{wv} \\ & + \sum T_{ws_1\dots\hat{s}_{i_1}\dots\hat{s}_{i_2}\dots\hat{s}_{i_q}\dots s_n u}\ \lambda_{s_{i_1}}\lambda_{s_{i_2}}\dots\lambda_{s_{i_q}} \prod_{j\in\{1,\dots,n\}-\{i_1,i_2,\dots,i_q\}} q_{s_j}^{k_j} \end{aligned}$$

où $\lambda_s := 1 - q_s$ pour $s \in S$, les k_j sont des entiers ≥ 0, et la somme est prise sur les suites $(s_{i_1}, s_{i_2}, \dots, s_{i_q})$ de longueur ≥ 1 extraites de la suite $(s_1, \dots, s_n)$ qui sont w-distinguées au sens suivant:

$\sigma_{i_1-1} := ws_1 \dots s_{i_1-1} < \sigma_{i_1-1}s_{i_1}$

$\sigma_{i_2-1} := \sigma_{i_1-1}s_{i_1+1}\dots s_{i_2-1} < \sigma_{i_2-1}s_{i_2}$,

$\dots$

$\sigma_{i_q-1} := \sigma_{i_{q-1}-1}s_{i_{q-1}+1}\dots s_{i_q-1} < \sigma_{i_q-1}s_{i_q}$.

3) $ws_1 \dots \hat{s}_{i_1} \dots \hat{s}_{i_2} \dots \hat{s}_{i_q} \dots s_n u < wv$ *pour toute suite $(s_{i_1}, s_{i_2}, \dots, s_{i_q})$ de longueur ≥ 1 extraite de la suite $(s_1, \dots, s_n)$, qui est w-distinguée.*

Il est pratique d'introduire de nouvelles indéterminées $(q_s^{1/2})_{s\in S}$ égales si s, s' sont conjugués dans W, dont les carrés sont $(q_s)_{s\in S}$. Pour tout $s \in S$ on note $\tilde{\lambda}_s := q_s^{-1/2}\lambda_s$, et pour tout $w \in W$ on note $\tilde{T}_w := q_w^{-1/2}T_w$. Le lemme fondamental résulte essentiellement des relations

$$\tilde{T}_s^{-1} = \tilde{T}_s + \tilde{\lambda}_s,$$
$$\tilde{T}_w\tilde{T}_s^{-1} = \tilde{T}_{ws} \ \text{ si } \ ws < w, \ \text{et} \ \tilde{T}_w\tilde{T}_s^{-1} = \tilde{T}_{ws} + \tilde{\lambda}_s\tilde{T}_w \ \text{si} \ w < ws.$$

Preuve. La démonstration de 3) est faite dans ([Haines, prop. 5.5]). On y démontre l'inégalité au sens large $ws_1 \dots \hat{s}_{i_1} \dots \hat{s}_{i_2} \dots \hat{s}_{i_q} \dots s_n \leq wv$, l'égalité impliquerait en simplifiant $\hat{s}_{i_1} \dots \hat{s}_{i_2} \dots \hat{s}_{i_q} = s_{i_1} \dots s_{i_q}$ ce qui est faux si $q \neq 0$. On a donc l'inégalité stricte.

Montrons 1).

a) Si $v = s \in S$ on a $q_{ws} = q_wq_s^{\varepsilon}$ où $\ell(ws) = \ell(w) + \varepsilon$; donc 1) est vérifié pour (w, s) avec $c_{w,s} = q_s$ si $ws > w$ et 1 si $ws < w$.

b) Si $v \in W_{\mathit{aff}}$ et $v = s_1 \dots s_n$ est une décomposition réduite, on a par induction $q_{wv} = q_w q_{s_1}^{\varepsilon_1} \dots q_{s_v}^{\varepsilon_n}$ où $\ell(ws_1) = \ell(w) + \varepsilon_1,\ \ell(ws_1s_2) = \ell(ws_1) + \varepsilon_2,\ \dots,\ \ell(wv) = \ell(ws_1 \dots s_{n-1}) + \varepsilon_n$. On a $q_v = q_{s_1} \dots q_{s_n}$ et 1) est vérifié pour (w, v) avec

$$c_{w,v} = \prod_{1 \le i \le n, \varepsilon_i = 1} q_{s_i}$$

c) Si $v = v_{\mathit{aff}} u, v_{\mathit{aff}} \in W_{\mathit{aff}}, u \in \Omega$, on a $q_{wv} = q_{wv_{\mathit{aff}}}, q_v = q_{v_{\mathit{aff}}}$. Donc par b), le lemme est vérifié pour (w, v) avec $c_{w,v} = c_{w,v_{\mathit{aff}}}$.

Montrons 2). Il est immédiat que le lemme fondamental est vérifié si $v = s \in S$. Soient $s_1, \dots, s_n \in S$ tels que $v = s_1 \dots s_n$ soit une décomposition réduite. En appliquant la relation précédente plusieurs fois, on obtient

$$\tilde{T}_w \tilde{T}_{v^{-1}}^{-1} = \tilde{T}_{wv} + \sum \tilde{T}_{ws_1 \dots \hat{s}_{i_1} \dots \hat{s}_{i_2} \dots \hat{s}_{i_q} \dots s_n} \tilde{\lambda}_{s_{i_1}} \tilde{\lambda}_{s_{i_2}} \dots \tilde{\lambda}_{s_{i_q}}$$

où la somme est prise sur les suites $(s_{i_1}, s_{i_2}, \dots, s_{i_q})$ de longueur ≥ 1 extraites de la suite $(s_1, \dots, s_n)$ qui sont w-distinguées. Le lemme fondamental pour $v \in W_{\mathit{aff}}$ est alors équivalent à l'assertion suivante sur les fonctions q_w. $\square$

Soit $w \in W, s_1, \dots, s_n \in S$ tels que $s_1 \dots s_n$ soit une décomposition réduite. Pour une suite $(s_{i_1}, s_{i_2}, \dots, s_{i_q})$ extraite de la suite $(s_1, \dots, s_n)$ et w-distinguée, on a

$$q_{ws_1 \dots s_n} = q_{ws_1 \dots \hat{s}_{i_1} \dots \hat{s}_{i_2} \dots \hat{s}_{i_q} \dots s_n}\ q_{s_{i_1}} q_{s_{i_2}} \dots q_{s_{i_q}} \prod_{j \in \{1, \dots, n\} - \{i_1, i_2, \dots, i_q\}} q_{s_j}^{2k_j}$$

où les k_j sont des entiers naturels.

La preuve se fait pas récurrence sur n. Lorsque $n = 1$ c'est évident. Supposons cette propriété vraie pour $n - 1$ et montrons la pour n. Si $i_1 > 1$, la suite $(s_{i_1}, s_{i_2}, \dots, s_{i_q})$ est extraite de la suite $(s_2, \dots, s_n)$ et elle est ws_1-distinguée. L'assertion est vraie pour $(ws_1, s_2, \dots, s_n)$ par hypothèse de récurrence, et l'on obtient le résultat, avec $k_1 = 0$. Supposons que $i_1 = 1$. La suite $(s_{i_2}, \dots, s_{i_q})$ est extraite de la suite $(s_2, \dots, s_n)$ et elle est w-distinguée. L'assertion est vraie pour $(w, s_2, \dots, s_n)$ par hypothèse de récurrence, et l'on obtient

$$q_{ws_2 \dots s_n} = q_{ws_2 \dots \hat{s}_{i_2} \dots \hat{s}_{i_q} \dots s_n}\ q_{s_{i_2}} \dots q_{s_{i_q}} \prod_{j \in \{2, \dots, n\} - \{i_2, \dots, i_q\}} q_{s_j}^{2t_j}$$

pour des entiers $t_j \ge 0$. L'assertion pour $i_1 = 1$ résulte alors du lemme suivant.

1.3. Lemme. *Soit $w \in W$ et $s_1, s_2, \dots s_n \in S$ tels que $w < ws_1$ et $s_1 \dots s_n$ est une décomposition réduite. Alors*

a) $ws_2 \dots s_n < ws_1 s_2 \dots s_n$,

b)

$$q_{ws_1 \dots s_n} q_{ws_2 \dots s_n}^{-1} = q_{s_1} \prod_{j \in \{2, \dots, n\}} q_{s_j}^{2k_j}$$

pour des entiers $0 \le k_j \le 1$.

Le lemme 1.3 termine la démonstration du lemme fondamental lorsque $v \in W_{\mathit{aff}}$. Le cas général s'en déduit, car si $v = v_{\mathit{aff}} u, v_{\mathit{aff}} \in W_{\mathit{aff}}, u \in \Omega$, et si $w, w' \in W$, on a $\tilde{T}_w \tilde{T}_{v^{-1}}^{-1} = \tilde{T}_w \tilde{T}_{v_{\mathit{aff}}^{-1}}^{-1} T_u,\ T_{w'} T_u = T_{w'u},\ q_{w'u} = q_{w'},\ w' < wv_{\mathit{aff}}$ implique $w'u < wv$. La démonstration du lemme fondamental sera donc achevée, après la preuve de 1.3.

Preuve du lemme 1.3. La partie a) est démontrée dans ([Haines, lemma 5.6]). Elle implique que le membre de gauche de b) est un monôme $c_n \in Q$ différent de 1. On montre b) par récurrence sur n. Pour $n = 1$ on a $c_1 = q_{s_1}$ donc b) est vrai. Montrons que si b) est vrai pour $n-1$, alors il est vrai pour n. On a

$q_{ws_1\dots s_n} = q_{ws_1\dots s_{n-1}} q_{s_n}^{\varepsilon_1}$,
$q_{ws_2\dots s_n} = q_{ws_2\dots s_{n-1}} q_{s_n}^{\varepsilon_2}$

avec $\varepsilon_1, \varepsilon_2 \in \{\pm 1\}$. On a donc

$c_n = c_{n-1}, c_{n-1}q_{s_n}^2, c_{n-1}q_{s_n}^{-2}$ selon que $\varepsilon_1 = \varepsilon_2$, $(\varepsilon_1, \varepsilon_2) = (1,-1)$, $(\varepsilon_1, \varepsilon_2) = (-1, 1)$.

Par hypothèse de récurrence,

$c_{n-1} = q_{s_1} \prod_{j\in\{2,\dots,n-1\}} q_{s_j}^{2t_j}$ pour des entiers $0 \le t_j \le 1$.

Donc c_n vérifie b) si $c_n = c_{n-1}$ ou $c_{n-1}q_{s_n}^2$. Pour terminer la démonstration il suffit de remarquer que si $c_n q_{s_n}^2 = c_{n-1}$ alors il existe j tel que $t_j = 1$ et $q_{s_n} = q_{s_j}$. Donc c_n vérifie aussi b).

Le lemme 1.3 est démontré. □

Décomposition de Bernstein. D'après Bernstein-Lusztig, la décomposition de W en produit semi-direct $W = W_o e^X$ se généralise à l'algèbre de Hecke $H_{\phi_L}[q_*^{-1/2}]$.

On notera $?_x := ?_{e^x}$ pour $x \in X$, et A l'image du morphisme de $\mathbf{Z}[q_*^{\pm 1/2}]$-modules

$$\tilde{\theta} : \mathbf{Z}[q_*^{\pm 1/2}][X] \to H[q_*^{-1/12}]$$

qui envoie $x \in X$ sur $\tilde{\theta}_x := \tilde{T}_y \tilde{T}_z^{-1} = q_y^{-1/2} q_z^{1/2} T_y T_z^{-1}$ où $x = y - z$ pour deux éléments dominants y, z de X (bien défini car la longueur étant un morphisme de monoide sur les éléments dominants).

Soit $\alpha \in B$ une racine simple de réflexion associée $s \in S_o$. Si $\alpha^\vee \in 2X^\vee$, soit $\tilde{s} \in S_o$ la réflexion définie comme en [Lusztig 1, 2.4, p. 604]. On définit deux éléments $a_s, b_s \in A$ par:

$$a_s = q_s - 1, \quad b_s = 1 - \tilde{\theta}_{-\alpha}, \quad \text{si } \alpha^\vee \notin 2X^\vee,$$
$$a_s = q_s - 1 + q_s^{1/2}(q_{\tilde{s}}^{1/2} - q_{\tilde{s}}^{-1/2})\tilde{\theta}_{-\alpha}, \quad b_s = 1 - \tilde{\theta}_{-2\alpha}, \quad \text{si } \alpha^\vee \in 2X^\vee.$$

1.4. Théorème (Bernstein-Lusztig). 1) *Le morphisme* $\tilde{\theta} : \mathbf{Z}[q_*^{\pm 1/2}][X] \to H[q_*^{-1/12}]$ *est injectif et respecte le produit.*

2) $\tilde{\theta}_x T_s - T_s \tilde{\theta}_{s(x)} = (\tilde{\theta}_x - \tilde{\theta}_{s(x)}) a_s b_s^{-1}$ *pour tout* $(s, x) \in S_o \times X$.

3) $(T_{w_o})_{w_o \in W_o}$ *est une base de* $H[q_*^{-1/2}]$ *comme* A*-module, à droite ou à gauche.*

4) *Le centre de* $H[q_*^{-1/2}]$ *est l'algèbre* A^{W_o} *des éléments* W_o*-invariants de* A. *C'est un* $\mathbf{Z}[q_*^{\pm 1/2}]$*-module libre de base* $\tilde{z}_x = \sum_{x' \in W_o e^x} \tilde{\theta}_{x'}$ *pour tout* $x \in X_{dom}$.

Les références que je connais concernent seulement la $\mathbf{Z}[v^{\pm 1}]$-algèbre $H_{\phi_L}[v^{-1}]$. Ce sont [Lusztig 1, 3.3 à 3.11, pp. 607-610], [Lusztig 2, 7.1, p. 216; 8.1, p. 222]. L'algèbre $H_{\phi_L}[v^{-1}]$ suffit pour les applications en vue, et il me semble que les démonstrations restent valables pour $H[q_*^{-1/2}]$, modulo des modifications triviales.

Par le théorème, $H[q_*^{-1/2}]$ est un A-module à droite ou à gauche libre de rang fini égal au cardinal $|W_o|$ de W_o. *Si de plus,* X *contient tous les poids dominants pour le système de racines* R*, alors* $\mathbf{Z}[X]$ *est libre sur* $\mathbf{Z}[X]^{W_o}$ *de rang* $|W_o|$ [Steinberg, th. 2.2, p. 173] *et* $H[q_*^{-1/2}]$ *est un module libre de rang* $|W_o|^2$ *sur son centre.*

A-t-on des résultats analogues pour la $\mathbf{Z}[q_*]$-algèbre H?

- Le $\mathbf{Z}[q_*]$-module $A \cap H$ est-il libre?
- L'algèbre commutative $A \cap H$ est-elle de type fini?
- Le centre $Z(H) = A^{W_o} \cap H$ de H est-il une algèbre de type fini?
- Le $Z(H)$-module $A \cap H$ est-il de type fini?
- Le $(A \cap H)$-module H **à droite**, est-il de type fini?

Toutes ces questions seront résolues avec l'aide du théorème suivant qui se déduit du lemme fondamental appliqué à $\tilde{T}_{w_o}\tilde{\theta}_{y-z} = \tilde{T}_{w_o e^y}\tilde{T}_{e^z}^{-1}$ pour tout $w_o \in W_o,\ y, z \in X_{dom}$ (l'égalité vient de $\ell(w_o e^y) = \ell(w_o) + \ell(e^y)$).

1.5. Théorème. *Pour $w_o \in W_o,\ x \in X$, posons*

$$E_{w_o e^x} := q_{w_o e^x}^{1/2}\tilde{T}_{w_o}\tilde{\theta}_x.$$

Pour tout $w \in W$, le développement de E_w dans la base de Iwahori-Matsumoto $(T_w)_{w \in W}$ est

$$E_w = T_w + \sum_{w' < w} a_{w'}\ T_{w'}$$

pour des polynômes $a_{w'} \in \mathbf{Z}[q_*]$.

Le théorème 1 s'en déduit par un argument général.

Le théorème 2 résulte des des propriétés remarquables ci-dessous de la nouvelle base $(E_w)_{w \in W}$ de l'algèbre de Hecke générique H.

1.6. Propriétés de $(E_w)_{w \in W}$.

(1.6.1) *Le $\mathbf{Z}[q_*]$-module libre de base $(E_x)_{x \in X}$ est égal à la sous-algèbre commutative $A \cap H$.*

C'est immédiat puisque $E_x = q_x^{1/2}\tilde{\theta}_x$.

(1.6.2) *On a $H = \bigoplus_{w_o \in W_o} H(w_o)$ où $H(w_o)$ est le $\mathbf{Z}[q_*]$-module libre de base $(E_{w_o e^x})_{x \in X}$.*

En effet, $\tilde{T}_{w_o}\tilde{\theta}_x\tilde{\theta}_{x'} = \tilde{T}_{w_o}\tilde{\theta}_{x+x'}$ pour tout $x, x' \in X$, car $\tilde{\theta}$ respecte le produit (1.4.1).

(1.6.3) *$H(w_o) = T_{w_o} J(w_o)$, où $J(w_o)$ est un idéal fractionnaire de type fini de $A \cap H$.*

En effet,

$$E_{w_o e^x} E_{x'} = q(w_o e^x, e^{x'}) E_{w_o e^{x+x'}}, \quad q(w_o e^x, e^{x'}) := (q_{w_o e^x} q_{x'} q_{w_o e^{x+x'}}^{-1})^{1/2}.$$

Le produit $q(w_o e^x, e^{x'}) \in \mathbf{Z}[q_*]$ est un monôme puisque $(E_w)_{w \in W}$ est une base de H sur $\mathbf{Z}[q_*]$. On montre avec la formule des longueurs:

Il existe un ensemble fini $X(w_o) = \{x_1, \ldots, x_r\} \subset X$ dépendant de w_o, tel que

$$X = \bigcup_{i=1}^{r} X(w_o, x_i)$$

où $X(w_o, x_i)$ est l'ensemble des $x \in X$ vérifiant $\ell(w_o e^x) = \ell(w_o e^{x_i}) + \ell(e^{x - x_i})$.

Si $x \in X(w_o, x_i)$, on a

$$E_{w_o e^x} = E_{w_o e^{x_i}} E_{x - x_i}, \quad q(w_o, e^{x_i}) E_{w_o e^{x_i}} = T_{w_o} E_{x_i}, \quad E_{w_o e^x} = c(w_o, e^x) T_{w_o} E_x,$$

où $q(w_o, e^{x_i}) \in \mathbf{Z}[q_*]$ est un monôme et $c(w_o, e^x) = q(e^{x_i}, e^{x-x_i})q(w_o, e^{x_i})^{-1}$ est un monôme de Laurent. On a $q(w_o, e^{x_i})E_{w_o e^{x_i}} = T_{w_o}E_{x_i}$.

- Le $A \cap H$-module à droite $H(w_o)$ est engendré par $(E_{w_o e^x})_{x \in X(w_o)}$,

- $H(w_o) = T_{w_o}J(w_o)$ où $J(w_o)$ est le $A \cap H$-module de type fini engendré par $(q(w_o, e^x)^{-1}E_x)_{x \in X(w_o)}$ dans $A \cap H(q_*^{-1})$.

(1.6.4) On a $E_x E_{x'} = E_{x+x'}$ s'il existe $w_o \in W_o$ tel que $w_o(x), w_o(x') \in X_{dom}$ car la longueur est W_o-invariante sur e^X et un morphisme de monoide sur $e^{X_{dom}}$. Le monoide X_{dom} est de type fini. On choisit un système générateur fini M_{dom} de X_{dom}. Alors $M_X := W_o(M_{dom})$ est un ensemble fini.

La $\mathbf{Z}[q_*]$-algèbre $A \cap H$ est de type fini engendrée par $(E_x)_{x \in M_X}$.

(1.6.5) Le centre $Z(H)$ de H est $A^{W_o} \cap H$. Comme $q_x = q_{w_o(x)}$ pour tout $(w_o, x) \in W_o \times X$, on a $q_x^{1/2}\tilde{z}_x = \sum_{x' \in W_o(x)} E_{x'}$. On déduit alors de (1.4.3):

Le centre $Z(H)$ de H est égal à $(A \cap H)^{W_o}$; c'est un $\mathbf{Z}[q_*]$-module libre de base $Z_x := \sum_{x' \in W_o(x)} E_{x'}$ pour $x \in X_{dom}$.

(1.6.6) Des arguments généraux [Bourbaki AC, V 1.9, théorème 2, p. 29] permettent de déduire:

$A \cap H$ est un $(A \cap H)^{W_o}$-module de type fini, car c'est une $\mathbf{Z}[q_*]$-algèbre de type fini (1.6.4).

$(A \cap H)^{W_o}$ est une $\mathbf{Z}[q_*]$-algèbre de type fini, car $\mathbf{Z}[q_*]$ est un anneau noetherien.

Chapitre 2. Caractères de $A \cap H$ et modules standards

Soit R un anneau commutatif intègre de corps des fractions K et $i : R \to K$ l'inclusion. Soient un morphisme d'anneau de $\phi : \mathbf{Z}[q_*] \to R$ et $\chi : A \cap H \to R$ un morphisme d'anneau prolongeant ϕ. On note ω la restriction de χ au centre $Z(H)$ de H.

Pour les applications que nous avons en vue, il ne serait pas gênant de supposer que ϕ se prolonge à $\mathbf{Z}[q_*^{1/2}]$. On notera $B_\phi := B \otimes_\phi R$ la ϕ-spécialisation d'une $\mathbf{Z}[q_*]$-algèbre B et f_ϕ la ϕ-spécialisation d'un morphisme f de $\mathbf{Z}[q_*]$-algèbre.

On identifie χ à un morphisme d'anneau $\chi_\phi : (A \cap H)_\phi \to R$, et aussi en posant $\chi_X(x) := \chi(E_x)$, à une application $\chi_X : X \to R$ vérifiant

$$\chi_X(x)\chi_X(x') = \phi((q_x q_{x'} q_{x+x'}^{-1})^{1/2})\chi_X(x + x')$$

pour tout $x, x' \in X$, par la formule $E_x E_{x'} = (q_x q_{x'} q_{x+x'}^{-1})^{1/2} E_{x+x'}$ cas particulier de (1.6.2).

Lorsque $\phi(q_s) \subset R^*$ est inversible pour tout $s \in S$, et que ϕ se prolonge à $\mathbf{Z}[q_*^{1/2}]$, en posant pour $x \in X$,

$$\chi_X(x) = \chi_A(\tilde{\theta}_x) := \phi(q_x)^{-1/2}\chi(E_x),$$

on identifie χ à un morphisme d'anneau $\chi_A : A \to R$ et à un morphisme de groupe $\chi_X : X \to R^*$.

On dit que ω est le caractère central d'un H-module V, lorsque $Z(H)$ agit sur V par multiplication par ω. Le caractère ω s'identifie à un caractère de $Z(H)_\phi$. Le centre de la ϕ-spécialisation H_ϕ de H peut être plus gros que $Z(H)_\phi$. La R-algèbre H_ϕ est un R-module libre de rang infini puisque W est infini. La R-algèbre

$H_\omega = H \otimes_\omega R$ est de type fini sur R, car H est un module de rang fini sur son centre. On en déduit:

2.1. Proposition. *Si R est un corps algébriquement clos, un H_ϕ-module simple est de dimension finie si et seulement s'il a un caractère central.*

2.2. Définition. *Le H_ϕ-module à gauche induit de χ,*

$$I(\chi) := H \otimes_\chi R$$

de caractère central ω est appelé un module standard à gauche de H_ϕ.

Lorsque $\phi(q_s) \subset R^*$ est inversible pour tout $s \in S$, et que ϕ se prolonge à $\mathbf{Z}[q_*^{1/2}]$, le module standard $I(\chi)$ est le module standard $I(\chi_A)$ induit du caractère $\chi_A : A \to R$ prolongeant χ. Il est libre sur R de rang $|W_o|$ et admet une base canonique: l'image canonique de $(T_{w_o})_{w_o \in W_o}$.

2.3. Premières propriétés. Le module standard $I(\chi)$ satisfait les propriétés suivantes.

(2.3.1) *Il est de type fini comme R-module,* car H est de type fini comme $A \cap H$-module (théorème 2).

(2.3.2) *Il est cyclique, avec un générateur canonique $1 \otimes 1$ propre pour $A \cap H$ de valeur propre χ. Un H_ϕ-module à gauche engendré par un vecteur propre pour $A \cap H$ de valeur propre χ est quotient de $I(\chi)$.*

Le théorème 3 se déduit de ce résultat et de (2.1). Comme la R-algèbre de type fini H_ω admet un module simple à gauche, on obtient aussi:

(2.3.3) *Si R est un corps algébriquement clos, tout morphisme de R-algèbre $\omega : Z(H) \to R$ se prolonge en un morphisme d'anneau $\chi : A \cap H \to R$.*

Supposons $\chi(q_s) \neq 0$ pour tout $s \in S$. Par définition, une structure entière du module standard $I(\chi, K) = I(\chi) \otimes_R K$ est un sous-R-module de type fini stable par H et contenant une base de $I(\chi, K)$. Le noyau du morphisme canonique $I(\chi) \to I(\chi, K)$ est le sous-groupe de torsion $I(\chi)_{tor}$.

(2.3.4) *L'image de $I(\chi)$ dans $I(\chi, K)$ est une structure entière $M(\chi) \simeq I(\chi)/I(\chi)_{tor}$ contenant la base canonique.*

Le morphisme $I(\chi) \to I(\chi, K)$ est le produit tensoriel avec H de l'inclusion $i : R \to K$, vue comme une inclusion de $A \cap H$-modules via le caractère χ. Si H est un $A \cap H$-module à droite plat, alors le morphisme est injectif et $I(\chi)$ n'a pas de torsion. La classification des R-modules de type fini implique que si R est un anneau principal, le rang du R-module $I(\chi)$ est $|W_o|$ et le R-module $M(\chi)$ est libre de rang $|W_o|$.

2.4. Proposition. *Supposons $\chi(q_s) \neq 0$ pour tout $s \in S$ et que R est un anneau de valuation discrète de corps résiduel k_R, et de réduction $r : R \to k_R$. Alors les propriétés suivantes sont équivalentes:*

a) *Le module standard $I(\chi, k_R) := H \otimes_{r\chi} k_R = I(\chi) \otimes_r k_R$ est de dimension $|W_o|$ sur k_R,*
b) *La réduction de la structure entière canonique de $I(\chi, K)$ est le le module standard $I(\chi, k_R) \simeq M(\chi) \otimes_{R,r} k_R$,*
c) *Le R-module $I(\chi)$ est sans torsion.*

Le théorème 5 résulte de cette proposition, car le cas $R = \overline{\mathbf{Z}}_p$ se ramène au cas de l'anneau des entiers d'une extension finie de $\mathbf{Q}_p$.

2.5. Remarques. (i) Avec les hypothèses de la proposition, il existe une application $f : W_o \to X$, non unique et dépendant de χ, telle que $M(\chi)$ admet comme base sur R l'image canonique de $(E_{w_o e^{x_o}})_{w_o \in W_{w_o}}$. Lorsque le R-module $I(\chi)$ est sans torsion (par exemple si $r\phi(q_s) \neq 0$ pour tout $s \in S$), l'on peut probablement montrer par réduction, en utilisant sur R les arguments classiques [Rogawski], [Cherednik, proposition 1.5, p. 416], que pour tout $w_o \in W_o$,

- $I(\chi, k_R)$ et $I(\chi w_o, k_R)$ ont les mêmes suites de Jordan-Hölder,
- $I(\chi, k_R)$ contient un vecteur propre pour $A \cap H$ de valeur propre χw_o, ou ce qui est équivalent, il existe un R-morphisme H-équivariant (un opérateur d'entrelacement) de $I(\chi w_o, k_R)$ dans $I(\chi, k_R)$.

(ii) Supposons que $R = \overline{\mathbf{Z}}_p$ et que la réduction de $\phi(q_s)$ est nulle pour tout $s \in S$. Que peut-on dire sur la réduction du sous-module de torsion $I(\chi)_{tor}$? Est-ce que tout caractère $A \cap H \to \overline{\mathbf{F}}_p$ nul sur q_s pour tout $s \in S$, se relève?

Chapitre 3. Exemple du groupe linéaire

Soient $n > 1$ un entier et q une indéterminée. On note A_n la $\mathbf{Z}[q]$-algèbre commutative engendrée par les éléments $(e_I)_{I \subset \{1,\dots,n\}}$ vérifiant les relations

$$e_\emptyset = 1, \quad e_I e_J = q^{yz} e_{I\cup J} e_{I \cap J}, \quad |I \cap J| = x, |I| = x + y, \ |J| = x + z,$$

en notant $|I|$ le nombre d'éléments de I. L'identité polynômiale

$$(X+Y)(X+Y-1)+(X+Z)(X+Z-1)+2YZ = (X+Y+Z)(X+Y+Z-1)+X(X-1)$$

permet de vérifier que *les relations sont équivalentes à*

$$e_\emptyset = 1, \quad e_{i_1} e_{i_2} \dots e_{i_t} = q^{t(t-1)/2} e_{\{i_1,\dots,i_t\}}.$$

Le groupe S_n des permutations de $\{1,\dots,n\}$, permute les parties de $\{1,\dots,n\}$ de même cardinal, et agit naturellement sur A_n en fixant $e_{\{1,\dots,n\}}$. L'algèbre $A_n^{s_n}$ fixe par S_n est engendrée par $z_t := \sum_{|I|=t} e_I$ pour $1 \le t \le n$.

On pose $z := z_n = e_{\{1,\dots,n\}}$.

3.1. Proposition. *Pour la donnée radicielle basée correspondant au groupe $GL(n)$, l'algèbre commutative $A \cap H$ est isomorphe à $A_n[z^{-1}]$. Le centre de H est isomorphe à $A_n^{S_n}[z^{-1}]$.*

Preuve. La donnée radicielle se décrit avec le groupe $GL(n, \mathbf{C})$. Soit $e \in \mathbf{C}$ un élément transcendant. Le groupe abélien $X = \mathbf{Z}^n$ s'identifie au groupe des diagonales $e^x := \mathrm{diag}(e^{x_1}, \dots, e^{x_n})$ pour $x = (x_1, \dots, x_n) \in X$. La base $B = (\alpha_i)_{1 \le i \le n-1}$ est telle que

$$e^{\alpha_i} = (1, \dots, 1, e^{-1}, e, 1, \dots, 1), \quad \alpha_i^\vee \ (x) \ = \ x_{i+1} - x_i$$

pour $1 \le i \le n-1$, où e^{-1} est à la place i. Le groupe de Weyl fini W_o s'identifie au groupe symétrique S_n engendré par les réflexions $s_i = (i, i+1)$ pour $1 \le i \le n-1$ associées aux racines α_i. Le groupe de Weyl W de la donnée radicielle est isomorphe au produit semi-direct $S_n.e^X$. Le sous-groupe $\Omega \subset W$ des éléments de longueur 0 s'identifie au groupe $t^{\mathbf{Z}}$ où

$$t = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \\ 0 & 1 & 0 & 0 & \dots & 1 \\ e & 0 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

Le groupe de Weyl affine W_{aff} est engendré par les réflexions $s_o, s_1, \dots, s_{n-1}$, avec $s_o t = t s_1, s_1 t = t s_2, \dots, s_{n-2} t = t s_{n-1}$. Les poids fondamentaux dans X sont $\omega_i = (0^i, 1^{n-i})$, i premiers termes égaux à 0 et $n-i$ derniers termes égaux à 1, pour $1 \leq i \leq n-1$. Il est pratique d'introduire $\omega_n := (0^n)$, $\omega_o := (1^n)$. On a $X \cap \Omega = \omega_o \mathbf{Z}$ et le centre de $GL(n, \mathbf{Q}_p)$ est $p^{\omega_o \mathbf{Z}}$. La longueur de ω_i est le nombre $(n-i)i$ de racines positives contenant α_i si $1 \leq i \leq n-1$. Elle est nulle si $i = 0, n$. Les conjugués de ω_{n-1} par S_n sont $y_i := \omega_{i-1} - \omega_i$ $(1 \leq i \leq n)$, avec un seul coefficient 1 différent de 0 à la place i. $\square$

Une base du monoide X^+ est $(w_i)_{1 \leq i \leq n}$. L'algèbre $A \cap H$ est donc engendrée par $E_{w_o(w_i)}$ pour $w_o \in S_n$, $1 \leq i \leq n$. On a $y_n = \omega_{n-1}$ et $y_j = s_j \dots s_{n-1}(\omega_{n-1})$ pour $1 \leq j \leq n-1$. Plus généralement, les S_n-conjugués de ω_{n-t} sont $y_I := \sum_{i \in I} y_i$ pour toutes les parties I à t éléments de $\{1, \dots, n\}$. On note pour simplifier $E_I = E_{y_I}, \tilde{\theta}_I = \tilde{\theta}_{y_I}$. L'algèbre $A \cap H$ est engendrée par E_I pour les parties non vides de $\{1, \dots, n\}$.

Les relations entre les E_I se déduisent de celles entre les $\tilde{\theta}_I$. On a $q_{\omega_{n-t}} = q_I = q^{t(n-t)}$ pour $I \subset \{1, \dots, n\}$ avec t elements, ainsi:

$$\tilde{\theta}_i = q^{-i+(n+1)/2} T_{\omega_{i-1}} T_{\omega_i}^{-1}, \quad E_i = q^{n-i} T_{\omega_{i-1}} T_{\omega_i}^{-1} \quad , \quad \tilde{\theta}_I = \prod_{i \in I} \tilde{\theta}_i, \quad E_I = q^{t(n-t)/2} \tilde{\theta}_I.$$

L'élément central inversible $E_{\{1,\dots,n\}} = T_{\omega_o}$ est noté plus simplement Z. On a

$$E_\emptyset = 1, \quad \prod_{i \in I} E_i = q^{t(t-1)/2} E_I.$$

La $\mathbf{Z}[q_*]$-algèbre engendrée par $Z_t := \sum_{|I|=t} E_I$ $(1 \leq t \leq n-1), Z^{\pm 1}$ est égale au centre $Z(H)$.

On en déduit la proposition 3.1.

Soit R un anneau intègre. Un morphisme d'anneau $\chi : A \cap H \to R$ vérifie

$$\prod_{i \in I} \chi(E_i) = \chi(q)^{t(t-1)/2} \chi(E_I),$$

pour tout $I \subset \{1, \dots, n\}$ avec $t \geq 1$ éléments. Si $\chi(q)$ est inversible dans R, alors χ est déterminé par les n éléments non nuls $(\chi(E_i))_{1 \leq i \leq n}$ de produit $\prod_{1 \leq i \leq n} \chi(E_i)$ inversible, et inversement. Lorsque $\chi(q) = 0$, la situation est bien différente.

3.2. Lemme. *Soit $\chi : A \cap H \to R$ un morphisme d'anneau tel que $\chi(q) = 0$.*

1) *Les parties non vides $I \subset \{1, \dots, k\}$ telles que $\chi(E_I) \neq 0$ forment une suite croissante*

$$\emptyset \neq I_1 \subset I_2 \subset \dots \subset I_r = \{1, \dots, n\}.$$

2) *Inversement, étant donné une suite croissante comme ci-dessus et des éléments non nuls* $x_{I_1}, \dots, x_{I_r} \in R$, *il existe un unique morphisme d'anneau* $\chi : A \cap H \to R$ *tel que* $\chi(E_{I_j}) = x_{I_j}$ *et* $\chi(E_I) = 0$ *si* $I \neq I_j$ *pour tout* $1 \leq j \leq r$.

Preuve. On choisit $x_I \in R$ pour toute partie non vide I de $\{1, \dots, n\}$. Il existe un caractère $\chi : A \cap H \to R$ tel que $\chi(q) = 0$ et $\chi(E_I) = x_I$ pour tout I, si et seulement si $x_{\{1 \dots, n\}} \in R^*$ est une unité et $x_I x_J = 0$ lorsque $yz \neq 0$ où $|I| = x + y, |J| = x + z, |I \cap J| = x$, i.e. lorsque I n'est pas contenu dans J et J n'est pas contenu dans I.

Deux parties I, J tels que $x_I x_J \neq 0$ doivent donc vérifier $I \subset J$ ou $J \subset I$. Les parties I non vides telles que $x_I \neq 0$ doivent former une suite croissante, se terminant par $\{1 \dots, n\}$. Il n'y a aucune autre condition sur les valeurs non nulles x_I ni sur la suite croissante.

Le morphisme χ est évidemment déterminé par les x_I, lorsqu'il existe.

On en déduit le lemme 3.2. $\square$

Applications. 1) Le nombre de S_n-conjugués de χ est

$$\frac{n!}{t_1!(t_2 - t_1)! \dots (n - t_{r-1})!}$$

si t_j est le nombre d'éléments de I_j pour $1 \leq j \leq r$.

2) La restriction de χ au centre $Z(H)$ est le caractère ω tel que

$$\omega(Z_{t_j}) = \chi(E_{I_j}) \quad \text{pour tout} \quad 1 \leq j \leq r,$$

et $\omega(Z_t) = 0$ pour les autres valeurs possibles de t.

3.3. Définition. Soit R un anneau intègre. On dit qu'un R-caractère χ de $A \cap H$ nul sur q, ou que sa restriction ω au centre $Z(H)$, est

- régulier, si le stabilisateur de χ dans S_n est trivial, i.e., $\omega(Z_t) \neq 0$ pour tout $1 \leq t \leq n$,
- singulier, s'il n'est pas régulier,
- supersingulier, si χ est fixe par S_n, i.e. $\chi(E_I) = 0$ pour tout $\emptyset \neq I \subset \{1, \dots, n\}$, i.e. $\omega(Z_t) = 0$ sauf si $t = n$.

Un $H_{r_p \phi}$-module ayant un caractère central est appelé régulier, ou singulier, ou supersingulier, si son caractère central a cette propriété.

La terminologie "supersingulier"est analogue à celle introduite par Barthel et Livne dans leur étude des $\overline{\mathbf{F}}_p$-représentations de $GL(2, F)$ sur un corps p-adique F. Un caractère ω, χ supersingulier est déterminé par sa valeur $z := \chi(Z) = \omega(Z) \in R^*$ en Z, et sera noté ω_z, χ_z.

3.4. Preuve du théorème 6. Soit $\phi(q) \in \overline{\mathbf{Z}}_p$ non nul de réduction nulle $r_p \phi(q) = 0$. Démontrons que tout morphisme d'anneau $\chi : A \cap H \to \overline{\mathbf{F}}_p$ tel que $\chi(q) = 0$ se relève en un morphisme d'anneau $\tilde{\chi} : A \cap H \to \overline{\mathbf{Z}}_p$ tel que $\tilde{\chi}(q) = \phi(q)$.

On choisit un système compatible de racines n-ièmes $\phi(q)^{1/n}$ de $\phi(q)$ dans $\overline{\mathbf{Z}}_p$, pour tout entier $n \geq 1$. Tout élément λ_i de $\overline{\mathbf{Z}}_p$ s'écrit de facon unique $\lambda_i = x_i \phi(q)^{e_i}$ pour un nombre rationnel $e_i \geq 0$ et une unité $x_i \in \overline{\mathbf{Z}}_p^*$.

On associe au morphisme χ un drapeau $(I_j)_{1 \leq j \leq r}$ comme en (3.2).

Le morphisme $\tilde{\chi}$ tel que $\tilde{\chi}(E_i) = x_i\phi(q)^{e_i}$, $x_i \in \overline{\mathbf{Z}}_p^*, e_i \in \mathbf{Q}_{\geq 0}$, pour $1 \leq i \leq n$ relève χ si et seulement si $(e_i, x_i)_{1\leq i\leq n}$ vérifient:

$$e_{I_j} = t_j(t_j-1)/2, \quad r_p(x_{I_j}) = \chi(E_{I_j})$$

pour tout $1 \leq j \leq r$, et si I de cardinal t n'appartient pas au drapeau $(I_j)_{1\leq j\leq r}$,

$$e_I > t(t-1)/2,$$

où l'on pose

$$x_I = \prod_{i\in I} x_i, \quad e_I = \sum_{i\in I} e_i.$$

Le théorème 6 dit qu'il existe $(e_i, x_i)_{1\leq i\leq n}$ satisfaisant ces conditions. Il suffit de choisir des relèvements arbitraires $y_{I_j} \in \overline{\mathbf{Z}}_p^*$ de $\chi(E_{I_j})$ pour $1 \leq j \leq r$, et de prendre

$e_i = (t_1-1)/2$, $x_i = y_{I_1}^{1/t_1}$, pour $i \in I_1$,

$e_i = (t_{j+1}+t_j-1)/2$, $x_i = (y_{I_{j+1}}(y_{I_j}\dots y_{I_j})^{-1})^{1/(t_{j+1}-t_j)}$, pour $i \in I_{j+1} - I_j$ si $1 \leq j \leq r-1$.

On vérifie immédiatement les conditions sur les x_i. Vérifions les conditions sur les e_I. Soit $I \subset \{1,\dots,n\}$ non vide avec $t = |I|$. Posons $x_j := |I \cap I_j|$ pour $1 \leq j \leq r$. Donc $t = \sum x_i$ et

$$2e_I = x_1(t_1-1) + (x_2-x_1)(t_2+t_1-1) + \ldots + (x_r - x_{r-1})(n + x_{r-1} - 1).$$

La suite (x_j) est croissante et $x_j \leq t_j$ pour tout j, donc

$$2e_I \leq x_1(x_1-1) + (x_2-x_1)(x_2+x_1-1) + \ldots + (x_r - x_{r-1})(x_r + x_{r-1} - 1).$$

avec égalité si et seulement si I appartient au drapeau $(I_j)_{1\leq j\leq r}$. Les propriétés voulues des e_I résultent de l'identité polynômiale

$$X(X-1) + (Y-X)(Y+X-1) = Y(Y-1).$$

qui implique que le membre de droite de l'inégalité est $t(t-1)$.

3.5. Preuve de la proposition 7. Nous allons démontrer que la longueur d'un module standard supersingulier sur $\overline{\mathbf{F}}_p$ est $\geq 2^{n-2}$. Il suffit de montrer qu'un caractère supersingulier quelconque de $A \cap H$ à valeurs dans $\overline{\mathbf{F}}_p$ possède un relèvement $\chi : A \cap H \to \overline{\mathbf{Z}}_p$, tel que le module standard $I(\chi, \overline{\mathbf{Q}}_p)$ admette 2^{n-2} sous-quotients simples et d'appliquer le théorème 5. La théorie de Rogawski-Zelevinski permet de décrire les sous-quotients simples d'un module standard $I(\chi, \overline{\mathbf{Q}}_p)$ sur $\overline{\mathbf{Q}}_p$ en fonction de χ lorsque $\chi(q) = q$. Maintenant que le principe est établi, il reste à exhiber le relèvement. Le relèvement décrit en 3.4 ne convient pas, mais sa forme est analogue à celui que l'on va exhiber.

Soit $z \in \overline{\mathbf{F}}_p^*$ quelconque. On choisit deux unités $a, b \in \overline{\mathbf{Z}}_p^*$ telles que $r_p(a^{n-1}b) = z$ et un nombre rationnel $u \in \mathbf{Q}$ tel que $0 < u < 1/n$. Un caractère $\chi : A \cap H \to \overline{\mathbf{Q}}_p$ tel que $\chi(q) = q$ est déterminé par les valeurs $\chi(E_i)$ pour tous les entiers $1 \leq i \leq n$. On peut prendre ses valeurs quelconques. On prend

$$\chi(E_i) = aq^{u+i-1} \quad (1 \leq i \leq n-1), \quad \chi(E_n) = bq^{(n-1)(1-u)}.$$

On vérifie d'abord que χ est entier. Cela est équivalent à

$$\chi(E_I) = q^{t(1-t)/2} \prod_{i\in I} \chi(E_i) \in \overline{\mathbf{Z}}_p, \quad \chi(E_{1,\dots,n}) \in \overline{\mathbf{Z}}_p^*,$$

pour toute partie I de $\{1,\ldots,n\}$ d'après la description de $A \cap H$ par générateurs et relations (proposition 3.1). Ceci est presque évident: on minore la somme $\sum_{i\in I}(u+i-1)$ par $tu+t(t-1)/2$ donc

$$\chi(E_I) \in a^t q^{tu+\mathbf{N}}$$

est entier. On a $\chi(E_{1,\ldots,n}) = a^{n-1}b$. Donc le caractère χ est entier. Comme $u > 0$ et $r_p(a^{n-1}b) = z$, la réduction de χ est le caractère supersingulier égal à z sur l'él'ement central $E_{1,\ldots,n}$. Comme la longueur de y_i ne dépend pas du choix de i, on voit que le caractère de X associé est χ contient un "segment de Zelevinski" de longueur $n-1$. On déduit de que le module standard associé contient 2^{n-2} sous-quotients irréductibles distincts [Rogawski, 5.2, p. 456].

Cas $n = 2$**.** La décomposition des modules standards, donc la classification des modules simples sur $\overline{\mathbf{F}}_p$ est connue [Vignéras]. On a:

$\tilde\theta_1 = q^{1/2}T_{w_o}T_{\omega_1}^{-1}, \tilde\theta_2 = q^{-1/2}T_{\omega_1},\ E_i = q^{1/2}\tilde\theta_{y_i}$ pour $1 \le i \le 2$, avec la relation $E_1E_2 = qZ$.

L'algèbre commutative $A \cap H = \mathbf{Z}[q,\ Z^{\pm 1},\ E_1, E_2]$,

Le centre $Z(H) = \mathbf{Z}[q,\ Z^{\pm 1}, Z_1 = E_1 + E_2]$.

Les module standards sont de dimension 2.

Les modules standards supersinguliers sont irréductibles.

Les modules standards réguliers de caractère central ω tel que $\omega(Z_1)^2 \ne \omega(Z)$, sont irréductibles.

Les modules standards réguliers de caractère central ω tel que $\omega(Z_1)^2 = \omega(Z)$, sont indécomposables de longueur 2, contenant caractère trivial (i.e. $T_s \to 0$) et un caractère signe (i.e. $T_s \to -1$) comme sous-quotient.

Les modules simples se relèvent.

Bibliographie

[Bourbaki AC] Nicolas Bourbaki, *Algèbre commutative, Chapitre 5 à 7*, Masson, 1985.

[Bourbaki GAL] Nicolas Bourbaki, *Groupes et algèbres de Lie Chapitres 4, 5 et 6* Hermann, 1968. MR0240238 (39 #1590)

[Cherednik] Ivan Cherednik, *A unification of Knizhnik-Zamolodchikov and Dunkl operators via affine Hecke algebras*, Invent. Math. 106, 411-431 (1991). MR1128220 (93b:17040)

[Haines] Thomas J. Haines, *The combinatorics of Bernstein functions*, Trans. Amer. Math. Soc. 353, no. 3 (2001), 1251-1278. MR1804418 (2002j:20012)

[Lusztig 1] George Lusztig, *Affine Hecke algebras and their graded version*, J. Amer. Math. Soc. Vol. 2, No. 3, 1989. MR0991016 (90e:16049)

[Lusztig 2] George Lusztig, *Singularities, character formulas, and a q-analog of weight multiplicities*, Astérisque 101-102 pp. 208-229, Soc. Math. France, Paris, 1984. MR0737932 (85m:17005)

[Lusztig 3] George Lusztig, *Hecke algebras with unequal parameters*, CRM Monograph Series, 18, American Mathematical Society, Providence, RI, 2003. MR1974442 (2004k:20011)

[Ollivier] Rachel Ollivier, *Modules simples en caractéristique p des algèbres de Hecke affines de type A_1, A_2*, DEA Institut de Mathématiques de Jussieu, 28 Juin 2002.

[Rogawski] J. D. Rogawski, *On modules over the Hecke algebra of a p-adic group*, Invent. Math. 79, (1985), 443-465. MR0782228 (86j:22028)

[Steinberg] R. Steinberg, *On a theorem of Pittie*, Topology 14 (1975), 173-177. MR0372897 (51 #9101)

[Vignéras] Marie-France Vignéras, *Representations modulo p of the p-adic group $GL(2,F)$*, Compos. Math. 140 (2004), 333–358. MR2027193 (2004m:22028)

Appendice

Définitions. [Springer T.A. Reductive groups. Proceedings of Symposia in Pure Mathematics. Vol. 33 (1979), part 1, pp. 3-27] Une donnée radicielle basée est un quintuplet $(X, X^\vee, R, R^\vee, B)$ où

- $X, X^\vee$ sont des groupes libres abéliens de rang fini ≥ 1, en forte dualité par un forme bilinéaire $(\ ,\ ) : X \times X^\vee \to \mathbf{Z}$, R et $R^\vee$ sont des sous-ensembles finis non vides de X et de $X^\vee$ dont les éléments sont appelés "racines" et "coracines", B est une base de R.

- Une bijection $\alpha \leftrightarrow \alpha^\vee$ est donnée entre les racines et les coracines telle que $(\alpha, \alpha^\vee) = 2$,

- les reflexions s_α dans $GL(X)$ et dans $GL(X^\vee)$ définies par $s_\alpha(x) = x - (x, \alpha^\vee)\alpha$ et $s_\alpha(x^\vee) = x^\vee - (\alpha, x^\vee)\alpha^\vee$ pour tout $\alpha \in R, \alpha^\vee \in R^\vee, x \in X, x^\vee \in X^\vee$, permutent les racines $s_\alpha(R) = R$, et les coracines $s_{\alpha^\vee}(R^\vee) = R^\vee$.

On supposera le système de racines R réduit.

Le groupe de Weyl fini W_o est le sous-groupe de $GL(X)$ engendré par les réflexions $s_\alpha,\ \alpha \in R$. Le système $(W_o, \{s_\alpha,\ \alpha \in B\})$ est un système de Coxeter. Il est isomorphe canoniquement au sous-groupe de $GL(X^\vee)$ engendré par les réflexions $s_{\alpha^\vee},\ \alpha^\vee \in R^\vee$, et la forme bilinéaire $(\ ,\ )$ sur $X \times X^\vee$ est W_o-invariante.

Le groupe de Weyl W est le produit semi-direct de W_o et de X. On notera e^x l'élément $x \in X$ plongé dans W; on écrira $W = W_o.e^X$. On a $w_o e^x = e^{w_o(x)} w_o$ pour $(w_o, x) \in W_o \times X$.

Le groupe de Weyl affine W_{aff} est le produit semidirect de W_o et du sous-groupe $Q(R)$ de X engendré par R; on écrira $W_{aff} = W_o e^{Q(R)}$.

On définit un ordre partiel $\preceq$ dans $R^\vee$ tel que $\alpha_1^\vee \preceq \alpha_2^\vee$ si $\alpha_2^\vee - \alpha_1^\vee = \sum_{\beta \in B} n_\beta \beta^\vee$ pour des entiers $n_\beta \geq 0$. On note R_m les racines $\alpha \in R$ telles que les coracines $\alpha^\vee \in R^\vee$ sont minimales pour l'ordre $\preceq$ et

$$S = \{s_\beta,\ \beta \in B\} \cup \{e^{-\alpha} s_\alpha,\ \alpha \in R_m\}.$$

Le système (W_{aff}, S) est un système de Coxeter.

Toute racine est combinaison linéaire à coefficients entiers de même signe d'éléments de B. Si le signe est ≥ 0 la racine est dite positive, et négative sinon. On note R^+ l'ensemble des racines positives et R^- celui des racines négatives. Un élément $x \in X$ tel que $(x, \beta^\vee) \geq 0$ pour tout $\beta \in B$ est dit dominant.

Le monoide X_{dom} des éléments dominants de X est de type fini.

Longueur. La longueur ℓ de $W = \Omega.W_{aff}$ prolonge celle du système de Coxeter (W_{aff}, S) [Bourbaki GAL, IV.1.1, p. 9], de sorte que la longueur est constante sur $\Omega w_{aff} \Omega$ pour tout $w_{aff} \in W_{aff}$, ce qui a un sens car Ω normalise S. La longueur vérifie les propriétés:

- Le groupe Ω est formé par les éléments de longueur 0.

- La longueur est invariante par passage à l'inverse $\ell(w) = \ell(w^{-1})$ pour tout $w \in W$.

- La longueur de $W = W_o e^X$ s'exprime par une somme d'entiers naturels indexée par les racines positives [Iwahori-Matsumoto IHES 25, section I.10], généralisant celle pour le groupe de Weyl fini W_o [Bourbaki GAL, VI, 1.6, p. 157]. Pour $w_o \in W_o, x \in X$,

$$\ell(w_o e^x) = \sum_{\alpha\in R^+, w_o(\alpha)\in R^+} |(x,\alpha^\vee)| + \sum_{\alpha\in R^+, w_o(\alpha)\in R^-} |1+(x,\alpha^\vee)|.$$

- La longueur de $w_o \in W_o$ est donc le nombre de racines positives $\alpha \in R^+$ telles que $w_o(\alpha) \in R^-$.

- La longueur sur e^X est W_o-invariante:

$$\ell(w_o(e^x)) = \ell(e^x), \quad w_o \in W_o, x \in X.$$

En effet, il suffit de le vérifier pour une réflexion s_β définie par une racine simple $\beta \in B$, et dans ce cas d'utiliser que:

a) $(s_\beta(x), \alpha^\vee) = (x, s_\beta(\alpha)^\vee)$ pour $\alpha \in R$,

b) la réflexion s_β permute les racines positives différentes de β [Bourbaki GAL, VI, 1.6, Cor. 1, p. 157].

- La longueur de e^x pour $x \in X_{dom}$ est $\ell(e^x) = (x, 2\rho^\vee)$ où

$$2\rho^\vee := \sum_{\alpha\in R^+} \alpha^\vee = 2\sum_{\beta\in B} \omega_{\beta^\vee}$$

est deux fois la somme des poids fondamentaux $\omega_{\beta^\vee}$ tels que

$$(\alpha, \omega_{\beta^\vee}) = \delta_{\alpha,\beta}, \quad \alpha, \beta \in B$$

[Bourbaki GAL, VI, 1.10, prop. 29, p. 168]. En particulier,

- $\ell(w_o e^x) = \ell(w_o) + \ell(e^x)$ si x est dominant.

- Soient $x, x' \in X$ et $w_o \in W_o$. Posons $n(\alpha, w_o e^x) = (\alpha^\vee, x)$ si $w_o(\alpha) \in R^+$ et $n(\alpha, w_o e^x) = 1 + (x, \alpha^\vee)$ si $w_o(\alpha) \in R^-$. Si les entiers $n(\alpha, w_o e^x)$ et $n(\alpha, e^{x'})$ ont le même signe au sens large pour tout $\alpha \in R^+$, alors

$$\ell(w_o e^{x+x'}) = \ell(w_o e^x) + \ell(e^{x'}).$$

En particulier,

- $\ell(w_o e^{2x}) = \ell(w_o e^x) + \ell(e^x)$.

- $\ell(e^{x+x'}) = \ell(e^x) + \ell(e^{x'})$ pour tout $w_o \in W_o$ et tout $x, x' \in w_o(X_{dom})$.

(Ap.1) On vérifie:

Soient $u, v \in W_o$ et $x \in X$. Alors,

a) $\ell(u) + \ell(v) - \ell(uv)$ *est deux fois le nombre de racines $\alpha \in R^+$ telles que*

$$v(\alpha) \in R^-, \ uv(\alpha) \in R^+.$$

b) $\ell(u) + \ell(ve^x) - \ell(uve^x)$ est deux fois le nombre de racines $\alpha \in R^+$ telles que

$$1) \qquad v(\alpha) \in R^-, \ uv(\alpha) \in R^+, \ (x, \alpha^\vee) \geq 0,$$

ou

$$2) \qquad v(\alpha) \in R^+, \ uv(\alpha) \in R^-, \ (x, \alpha^\vee) < 0.$$

En particulier,

- si $\alpha, \beta \in B$, alors $\ell(s_\alpha e^\beta) = 1$ si et seulement si $(\beta, \alpha^\vee) < 0$.

(Ap.2) On va démontrer:

Soit $x \in X$. Notons $\ell(x)$ le nombre de racines positives $\alpha \in R^+$ telles que $(x, \alpha^\vee) < 0$.

1) *La longueur d'un élément $w_o \in W_o$ tel que $w_o(x)$ est dominant est $\geq \ell(x)$. Il existe un unique $u \in W_o$ de longueur $\ell(x)$ tel que $y = u(x)$ est dominant.*

On a $(x,\alpha^\vee)<0$ *si et seulement si* $u_o(\alpha)\in R^-$, *pour tout* $\alpha\in R^+$.

2) *Pour tout* t *tel que* $1\le t\le \ell(x)$, *soit* $\beta_t\in B$ *une racine simple de réflexion associée* s_t, *telle que* $u=s_{\ell(x)}\dots s_2s_1$ *soit une décomposition réduite; posons* $u_t:=s_t\dots s_2s_1$ *et* $u_o:=1$.

Pour tout $w_o\in W_o$, *on a*

$$\ell(w_o)=\ell(w_ou_t^{-1})+\ell(u_t)$$

si $w_o(\alpha)\in R^-$ *pour tout* $\alpha\in\{\beta_1,\ s_1(\beta_2),\ \dots,\ s_1\dots s_{t-1}(\beta_t)\}$, *et*

$$\ell(w_oe^x)=\ell(w_ou_t^{-1})+\ell(u_te^x)$$

si $w_o(\alpha)\in R^+$ *pour tout* $\alpha\in\{s_1\dots s_t(\beta_{t+1}),\ \dots,\ s_1\dots s_{\ell(x)-1}(\beta_{\ell(x)})\}$.

En particulier, $\ell(ue^x)=\ell(e^x)-\ell(x)$.

Preuve. 1) Soit $(w_o,x)\in W_o\times X$. On a $(w_o(x),w_o(\alpha)^\vee)=(x,\alpha^\vee)$ pour toute racine $\alpha\in R$. On voit que $w_o(x)$ *est dominant, i.e.* $\ell(w_o(x))=0$, *si et et seulement si* $w_o(\alpha)\in R^-$ *est une racine négative pour toute racine positive* $\alpha\in R^+$ *telle que* $(x,\alpha^\vee)<0$. Donc si $w_o(x)$ est dominant, la longueur de w_o est $\ge\ell(x)$ (on rappelle que $\ell(x)$ n'est pas la longueur de e^x).

Supposons que x n'est pas dominant, i.e. $\ell(x)>0$. On construit un élément $u\in W_o$ de longueur minimale $\ell(x)$ tel que $u(x)$ est dominant de la façon suivante.

Il existe au moins une racine simple β telle que $(x,\beta^\vee)<0$.

On a $\ell(s_\beta(x))=\ell(x)-1$ car $(s_\beta(x),\alpha^\vee)=(x,s_\beta(\alpha^\vee))$ et s_β permute les racines positives différentes de β.

Posons $\beta_1=\beta,u_1=s_{\beta_1},x_1=s_\beta(x)$.

On recommence en partant de x_1. Au bout de $\ell(x)$ étapes on obtient un élément dominant. On a ainsi choisi une suite de $\ell(x)$ racines simples β_t, d'éléments $u_t=s_{\beta_t}\dots s_{\beta_2}s_{\beta_1}$ de W_o, d'éléments $x_t=u_t(x)$ de X, tels que

$$(x_{t-1},\beta_t^\vee)<0,\quad \ell(x_t)=\ell(x)-t$$

pour tout $1\le t\le\ell(x)$. On prend $u=u_{\ell(x)}$.

Les racines $\alpha\in R^+$ telles que $u(\alpha)\in R^-$ sont [Bourbaki GAL, VI, §1, 1.6, Cor. 2]:

$$\text{(S)}\qquad \beta_1,\ s_{\beta_1}(\beta_2),\ \dots,\ s_{\beta_1}\dots s_{\beta_{\ell(x)-1}}(\beta_{\ell(x)}).$$

Ce sont les $\ell(x)$ racines telles que $(x,\alpha^\vee)<0$ car $(x_{t-1},\beta_t^\vee)=(x,s_{\beta_1}\dots s_{\beta_{t-1}}(\beta_t)^\vee)$.

L'unicité de u provient de ce que l'ensemble des racines positives $\alpha\in R^+$ telles que $u(\alpha)\in R^-$ est indépendant de u. Cet ensemble détermine u (introduire l'ensemble noté T_u comme dans [Bourbaki GAL, VI, 1.4, pp. 13-14] qui détermine u, puis appliquer [Bourbaki GAL, VI, 1.6, prop.17, p. 157]).

2) Soit $w_o\in W_o$. Si $t\ge1$, les racines $\alpha\in R^+$ telles que $u_t(\alpha)\in R^-$ sont les t premiers termes de la suite (S). On applique (Ap.1.1) pour obtenir les deux premières égalités sur la longueur.

Le cas particulier s'obtient en prenant $w_o=1,t=\ell(x)$ dans la seconde égalité. □

Ordre de Chevalley-Bruhat sur W. C'est un ordre partiel $\le$ sur W qui prolonge l'ordre de Chevalley-Bruhat usuel sur le système de Coxeter (W_{aff},S). Les propriétés suivantes pour $w,w'\in W_{\mathit{aff}}$ sont équivalentes [Lusztig 3], voir aussi le lemme 8.11 dans [Bernstein I.N., Gelfand I.M. and Gelfand S.I., Schubert cells and cohomology of the spaces G/P, Russ. Math. Surv. 28 (1973), 1-26]:

- il existe une expression réduite de w telle qu'en omettant certains termes on obtient une expression de w',

- pour toute expression réduite de w, en omettant certains termes on obtient une expression de w',

- il existe une suite d'éléments $w_o = w', w_1, \ldots, w_k = w$ dans W_{aff} telle que

$$\ell(w_1) - \ell(w_o) = \ldots = \ell(w_k) - \ell(w_{k-1}^{-1}) = 1, \quad w_1 w_o^{-1}, \ldots, w_k w_{k-1}^{-1} \in T,$$

- il existe une suite d'éléments $w_o = w', w_1, \ldots, w_k = w$ dans W_{aff} telle que

$$\ell(w_1) - \ell(w_o) = \ldots = \ell(w_k) > \ell(w_{k-1}), \quad w_1 w_o^{-1}, \ldots, w_k w_{k-1}^{-1} \in T.$$

où T est l'ensemble des conjugués de S dans W_{aff}.

Par définition de l'ordre de Chevalley-Bruhat, $w' \leq w$ si ces conditions sont réalisées.

La propriété d'échange des systèmes de Coxeter [Bourbaki GAL, IV, §1, 1.5, p. 15] montre que dans W_{aff}:

$$\ell(w) + \ell(w') = \ell(ww') \text{ implique } w \leq ww'.$$

L'ordre de Chevalley-Bruhat de W_{aff} est invariant par conjugaison par Ω, car Ω normalise S.

On prolonge naturellement l'ordre de Chevalley-Bruhat de W_{aff} à $W = \Omega W_{aff}$. Par définition $uw_{aff} \leq u'w'_{aff}$ si et seulement si $u = u', w_{aff} \leq w'_{aff}$, pour tout $u, u' \in \Omega, w_{aff}, w'_{aff} \in W_{aff}$. On a les propriétés équivalentes suivantes:

- $w_{aff} \leq w'_{aff}$ si et seulement si $w_{aff} u \leq w'_{aff} u$ pour tout $u \in \Omega, w_{aff}, w'_{aff} \in W_{aff}$,

- $w_{aff} \leq w'_{aff}$ si et seulement si $uw_{aff} \leq uw'_{aff}$ pour tout $u \in \Omega, w_{aff}, w'_{aff} \in W_{aff}$,

- $w_{aff} \leq w'_{aff}$ si et seulement si $uw'_{aff}u' \leq uw_{aff}u'$ pour tout $u, u' \in \Omega, w_{aff}, w'_{aff} \in W_{aff}$. On vérifie que:

Si $w, w' \in W, w' \leq w$, alors ${w'}^{-1} \leq w^{-1}$ et $\ell(w') \leq \ell(w)$.

Institut de Mathematiques de Jussieu, 175 rue du Chevaleret, Paris 75013 France