Algèbres de Hecke

Notes d'exposés au groupe de travail de topologie algébrique

Nantes/Angers

Aurélien DJAMENT

Décembre 2013

Résumé

Le but de cet exposé est de présenter l'essentiel des définitions et résultats (qui sont élémentaires et classiques) de la section 4 (ainsi qu'un petit calcul de la section 6 qui en découle) de la prépublication [Kuh] de Kuhn, avec quelques digressions de culture générale en guise de motivation.

Table des matières

1 Groupes symétriques, tresses et algèbres de Hecke

Pour tout entier $n \geq 1$, le *monoïde des tresses* sur n brins est le monoïde Br_n^+ (on note dans cet exposé Br au lieu de B pour les monoïdes ou groupes de tresses afin d'éviter la confusion avec les groupes de matrices triangulaires B_n dont on aura également besoin — cf. section suivante) est le monoïde engendré par $n-1$ générateurs σ_i $(1 \leq i \leq n-1)$ soumis aux relations suivantes :

$$\sigma_i\sigma_j = \sigma_j\sigma_i \qquad \text{si} \quad |i-j| > 1 \ ;$$

$$\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \qquad \text{si} \quad |i-j| = 1.$$

Le *groupe des tresses* sur n brins est la complétion en groupes Br_n de ce monoïde (c'est donc le groupe défini par $n-1$ générateurs soumis aux mêmes relations). Un résultat important et non trivial est que le morphisme de monoïdes canonique $Br_n^+ \to Br_n$ est injectif (voir [KT08], § 6.5.4) ; nous n'en aurons pas usage.

Ces groupes sont intimement liés aux groupes symétriques ; de fait, on dispose d'un épimorphisme de groupes fondamental $Br_n \twoheadrightarrow \Sigma_n$ obtenu en constatant que les transpositions $s_i := (i \quad i+1)$ (pour $1 \leq i < n$) engendrent Σ_n

et vérifient les relations de tresses précédentes. Un résultat classique (élémentaire pas immédiat ; voir par exemple [KT08], §4.1.1 et 4.1.2) dit plus, à savoir qu'on obtient une *présentation* de Σ_n à l'aide des s_i soumis aux relations de tresses et aux relations $s_i^2 = 1$. On peut dire davantage : les écritures réduites des éléments du groupe symétrique comme produit des générateurs s_i possèdent de nombreuses propriétés qui font (ou, selon le point de vue, sont dues au fait) que Σ_n est un *groupe de Coexeter* (voir par exemple [Bou68], chap. IV, ou [KT08] § 4.1 pour le seul cas des groupes symétriques).

On dispose d'un diagramme commutatif évident de groupes

$$\begin{tikzcd} Br_n \arrow[r] \arrow[d] & Br_{n+1} \arrow[d] \\ \Sigma_n \arrow[r] & \Sigma_{n+1} \end{tikzcd}$$

dont les flèches verticales sont épi et les flèches horizontales sont mono (pour le cas des groupes de tresses, ce n'est pas une évidence ; voir par exemple [KT08], corollaire 1.14).

Les groupes ou monoïdes de tresses n'interviendront pas directement dans cet exposé (ni dans les investigations de la prépublication de Kuhn utilisant les algèbres de Hecke mais dont nous ne parlerons pas) ; ils semblent en revanche indispensables à motiver l'introduction des algèbres de Hecke. Mentionnons à ce sujet la *représentation de Burau*, l'une des familles les plus importantes de représentations des groupes de tresses.

Soient A un anneau commutatif et t un élément de A. Pour tout entier $n > 0$, on munit le A-module libre A^n d'une action du monoïde de tresses Br_n^+ en faisant agir le générateur σ_i par $1_{i-1} \oplus M \oplus 1_{n-i-1}$ où

$$M = \begin{pmatrix} 1-t & t \\ 1 & 0 \end{pmatrix}.$$

On note que la matrice M (donc l'action des σ_i) vérifie la relation quadratique

$$M^2 = (1-t)M + t.$$

Si t est inversible dans A, M est une matrice inversible de sorte qu'on obtient même une représentation du groupe de tresses Br_n (pour Burau on prend généralement $A = \mathbb{Z}[t, t^{-1}]$). Noter que pour $t = 1$, la représentation obtenue se factorise par l'épimorphisme canonique $Br_n \twoheadrightarrow \Sigma_n$; c'est l'image inverse par ce morphisme de la représentation de permutations usuelle A^n de Σ_n.

Soient q et z deux éléments d'un anneau commutatif A. Suivant [KT08], § 4.2.1 (à la différence près qu'on ne suppose pas que q soit inversible), on définit l'algèbre de Hecke $\mathcal{H}_n(A; q, z)$ (les décorations auront tendance à disparaître des notations) comme la A-algèbre (associative, unitaire) engendrée par des générateurs T_i pour $1 \leq i < n$ soumis aux relations de tresses et à la relation quadratique

$$T_i^2 = zT_i + q$$

(autrement dit, c'est le quotient de l'algèbre de monoïde $A[Br_n^+]$ par l'idéal bilatère engendré par ces relations). Si q est inversible dans A, les T_i sont inversibles dans $\mathcal{H}_n(A; q, z)$, qui est donc le quotient de l'algèbre de groupe $A[Br_n]$

par les mêmes relations quadratiques. On se restreint le plus souvent au cas $z = q - 1$. La représentation de Burau montre l'importance de ce choix : la relation quadratique précédente sur la matrice M montre que cette représentation définit en fait une représentation de $\mathcal{H}_n(A; t, 1-t)$; cette algèbre est isomorphe à $\mathcal{H}_n(A; t, t-1)$ via l'application envoyant T_i sur $-T_i$.

Bien sûr, l'algèbre $\mathcal{H}_n(A; 1, 0)$ n'est autre que l'algèbre $A[\Sigma_n]$. Il est remarquable que les algèbres de Hecke jouissent d'une manière générale d'un certain nombre de propriétés favorables de cette algèbre de groupe qu'on ne peut attendre ni de $A[Br_n]$ ni de $A[Br_n^+]$. Cela est dû à ce que, pour $n \geq 2$, Br_n est un groupe infini (de surcroît, « méchamment » non commutatif pour $n \geq 3$), ses représentations ne bénéficient donc pas de celles des propriétés usuelles de celles des groupes finis. En revanche, on peut montrer que, si K est un corps commutatif de caractéristique nulle (ou de caractéristique ne divisant par $n!$), alors l'algèbre de Hecke $\mathcal{H}_n(K; q)$ est semi-simple sauf pour un nombre fini de valeurs de q ; on peut de plus classifier ses représentations simples par une combinatoire de diagrammes Young analogue à celle bien connue pour les groupes symétriques (voir [KT08] § 4.6 et chap. 5). Tout cela ne nous sera toutefois pas utile ici.

Signalons aussi qu'on peut définir les algèbres de Hecke dans un contexte plus général : il s'agit ici seulement des algèbres de Hecke de type A.

2 Algèbre de Hecke et représentations de $GL_n(\mathbb{F}_p)$

Ce qu'on présente ici, suivant notamment [Kuh85] (ou [KP85]), peut être exposé sans grand changement dans le cadre général des systèmes de Tits (voir [Bou68], chap. IV à leur sujet ; ils sont appelés en anglais *BN-pairs*), on pourra se référer à [CIK71] pour cette présentation axiomatique.

À partir de maintenant, on fixe un nombre premier p. Les liens sont notoires entre le groupe linéaire $G := GL_n(\mathbb{F}_p)$ et le groupe symétrique $W := \Sigma_n$ — W est le *groupe de Weyl* du groupe de Chevalley G muni du système de Tits standard.

Le point de départ est la proposition complètement générale suivante (voir [CR81], proposition (11.34)).

Proposition 2.1. *Soient G un groupe fini, B un sous-groupe de G et A un anneau commutatif. La A-algèbre $\mathrm{End}_{A[G]}(A[B\backslash G])$ est un A-module libre possédant une base $(t(X))$ indexée par les éléments X de l'ensemble de doubles classes $B\backslash G/B$ et satisfaisant la table de multiplication*

$$t(X)t(Y) = \sum_{Z \subset X.Y} \mu(X, Y, Z)t(Z)$$

(noter que $X.Y$ est une réunion de doubles classes) où

$$\mu(X, Y, Z) = \frac{|Y \cap X^{-1}z|}{|B|}$$

où z est un élément de Z (ce cardinal ne dépend pas du choix de z, et est non nul si et seulement si $Z \subset X.Y$).

Démonstration. Le foncteur $\mathrm{Hom}_{A[G]}(A[B\backslash G], -)$ des $A[G]$-modules à droite vers les groupes abéliens est canoniquement isomorphe au foncteur des invariants sous l'action de B. Comme G est un groupe fini, on a $A[B\backslash G]^B \simeq A[B\backslash G/B]$. Explicitement, l'isomorphisme de A-modules

$$A[B\backslash G/B] \xrightarrow{\simeq} \mathrm{End}_{A[G]}(A[B\backslash G])$$

déduit de ces observations associe à $X \in B\backslash G/B$ l'endomorphisme

$$[Bg] \mapsto \sum_{b \in B/(B\cap x^{-1}Bx)} [Bxbg]$$

où x est un élément de X (le quotient par le sous-groupe $B \cap x^{-1}Bx$ provient de ce que la condition $Bxb = Bxb'$ équivaut à $bb'^{-1} \in x^{-1}Bx$), et b désigne par abus (cet abus sera répété dans la suite), dans le terme de la somme, un représentant dans B de la classe modulo $B \cap x^{-1}Bx$ (le terme ne dépend pas du choix). Ceci n'est qu'une reformulation de la formule classique de Mackey pour la composée d'une restriction et d'une induction.

Le produit $t(X)t(Y)$ est caractérisé par le fait qu'il envoie $[B]$ sur

$$\sum_{\substack{b_1 \in B/(B\cap x^{-1}Bx) \\ b_2 \in B/(B\cap y^{-1}By)}} [Bxb_1yb_2].$$

Les termes qui apparaissent dans cette somme sont les $[Bt]$ pour t appartenant à $BxByB = XY$, mais ils peuvent apparaître plusieurs fois. L'occurrence d'un terme $[Bz]$ est exactement le nombre de (b_1, b_2) tel que $Bxb_1yb_2 = Bz$, relation équivalente à $b_1yb_2 \in x^{-1}Bz$. On en déduit que $|B|\mu(X, Y, Z)$ égale le nombre de (b_1, b_2) tels que $b_1yb_2 \in X^{-1}z$, qui est exactement le cardinal de $Y \cap X^{-1}z$ (on rappelle que les couples sont pris sur les ensembles quotients appropriés, de sorte qu'à un élément de $X^{-1}z$ correspond au plus un couple (b_1, b_2), il en correspond un si et seulement cet élément appartient aussi à $Y = ByB$). $\square$

Remarque 2.2. Le lemme de Yoneda montre que l'algèbre $\mathrm{End}_{A[G]}(A[B\backslash G])$ s'identifie à l'algèbre opposée de l'algèbre des endomorphismes du foncteur $M \mapsto M^B$ (des $A[G]$-modules à droite vers les groupes abéliens). Une variante duale montre que notre algèbre s'identifie aussi à l'algèbre des endomorphismes du foncteur des coïnvariants $M \mapsto M_B$, c'est le lemme 4.2 de [Kuh]. On utilisera plusieurs fois librement ce point de vue.

Revenons au groupe $G = G_n = GL_n(\mathbb{F}_p)$ et à son sous-groupe $B = B_n$ des matrices triangulaires supérieures. La *décomposition de Bruhat* dit que l'inclusion du sous-groupe $W = W_n$ des matrices de permutation de G induit une bijection $W \xrightarrow{\simeq} B\backslash G/B$. Ceci constitue une partie des propriétés qui font qu'on dispose sur G d'un système de Tits dont le sous-groupe de Borel standard est B et le groupe de Weyl W. Un autre propriété fondamentale décrit les produits de doubles classes Bs_iB (où $1 \le i < n$; on conserve les notations de la première section) et BwB : on a $Bs_iBwB = Bs_iwB$ si $l(s_iw) \ge l(w)$, où l désigne la fonction longueur sur le groupe W muni de l'ensemble de générateurs $\{s_1, \dots, s_{n-1}\}$ tandis que $Bs_iBwB = Bs_iwB \cup BwB$ sinon. En combinant ces propriétés avec la proposition 2.1, on peut montrer que la A-algèbre $\mathrm{End}_{A[G]}(A[B\backslash G])$ (A est un anneau commutatif quelconque) est un A-module libre possédant une base $\{a_w\}_{w\in W}$ telle que $a_{s_i}a_w = a_{s_iw}$ si $l(s_iw) > l(w)$ et $a_{s_i}a_w = pa_{s_iw} + (p-1)a_w$ sinon. On en déduit en particulier un morphisme de A-algèbres surjectif $\mathcal{H}_n(A;p) \twoheadrightarrow \mathrm{End}_{A[G_n]}(A[B_n\backslash G_n])$ envoyant T_i sur a_{s_i} ; on peut montrer que c'est un *isomorphisme*. On pourra trouver une démonstration de ces résultats, qui remontent pour l'essentiel à Iwahori, dans [CR87], § 67.A par exemple.

Dans l'article [Kuh85] (§ 4), Kuhn étudie l'algèbre $\mathrm{End}_{A[G_n]}(A[B_n\backslash G_n])$ pour $A = \mathbb{Z}_{(p)}$ (localisé de $\mathbb{Z}$ où l'on inverse les entiers premiers à p) ; dans [Kuh] Kuhn a seulement besoin de la réduction modulo p. Changeant légèrement de notation pour suivre Kuhn, on s'intéresse donc à $\mathrm{End}_{\mathbb{F}_p[G_n]}(\mathbb{F}_p[B_n\backslash G_n]) \simeq \mathcal{H}_n(\mathbb{F}_p;0)$, engendré par des générateurs *idempotents* $e(i)$ (ce sont les opposés des T_i ou a_{s_i}) pour $1 \leq i < n$ soumis aux relations de tresses.

Si l'on définit $\hat{e}(i) = 1 - e(i)$ dans $\mathcal{H}_n = \mathcal{H}_n(\mathbb{F}_p;0)$ (ou $\hat{e}(i) = p + 1 - e(i)$ dans $\mathcal{H}_n(\mathbb{Z}_{(p)};p)$), un calcul simple montre que ces éléments vérifient les mêmes relations que les $e(i)$. On en déduit une involution $x \mapsto \hat{x}$ sur l'algèbre de Hecke qu'utilise copieusement Kuhn.

La construction fondamentale dans $\mathcal{H}_n$, dans le travail de Kuhn, est celle d'un idempotent remarquable, qui est démontrée en détails (y compris sur $\mathbb{Z}_{(p)}$) dans [Kuh85].

Proposition 2.3. *Il existe un unique idempotent non nul e_n de $\mathcal{H}_n$ tel que $e(i)e_n = e_n = e_ne(i)$ pour tout i. De plus, pour tout $\mathcal{H}_n$-module M, on a*

$$e_nM = \bigcap_{i=1}^{n-1} e(i)M.$$

Indication de démonstration de l'existence. On utilise une permutation qui joue un rôle particulier dans la théorie, à savoir $w_0 := (i \mapsto n + 1 - i)$ (la double classe modulo B_n correspondante est celle de la décomposition LU, c'est l'unique double classe ouverte (et dense) pour la topologie de Zariski). Cette permutation est de longueur maximale $n(n-1)/2$ et c'est la seule. Cette longueur peut se réaliser par la décomposition

$$\begin{aligned} w_0 &= (1 \quad 2 \quad \ldots \quad n)(1 \quad 2 \quad \ldots \quad n-1)\ldots(1 \quad 2 \quad 3)(1 \quad 2) \\ &= (s_1s_2\ldots s_{n-1})(s_1\ldots s_{n-2})\ldots(s_1s_2)s_1 \end{aligned}$$

(cf. [KT08] § 4.1.6 par exemple). On pose $e_n = -a_{w_0}$. La propriété de longueur maximale entraîne $l(s_iw_0) < l(w_0)$ pour tout i, d'où

$$e(i)e_n = e_n.$$

Montrons que $e_ne(1) = e_n$: le fait que la décomposition précédente fournisse une écriture réduite montre que

$$e_n = (e(1)e(2)\ldots e(n-1))((e(1)e(2)\ldots e(n-2))\ldots(e(1)e(2))e(1)\ ;$$

en particulier $e_n \in \mathcal{H}_ne(1)$ et $e_ne(1) = e_n$ puisque $e(1)$ est idempotent. On montre que même que $e_ne(i) = e_n$ pour tout i (w_0 possède une écriture réduite qui se termine par s_i — cela se voit soit à la main, soit en utilisant que $l(w_0s_i) < l(w_0)$ par la propriété de minimalité).

Ce qui précède montre en particulier que $e_n \in e(i)\mathcal{H}_n$ pour tout i, d'où l'on tire

$$e_n M \subset \bigcap_{i=1}^{n-1} e(i)M.$$

L'inclusion inverse découle également de la discussion précédente, puisqu'elle montre que e_n est un produit des idempotents $e(i)$. □

Remarque 2.4. Comme l'algèbre $\mathcal{H}_n$ est engendrée par les $e(i)$, e_n en est un idempotent *central*. Ce phénomène est à rapprocher de la description du centre du groupe de tresses Br_n, qui est cyclique infini engendré par le carré de l'élément donné par le même mot que w_0 en remplaçant les s_i par les σ_i (cf. [KT08], théorème 1.24).

Remarque 2.5. Une propriété similaire vaut dans l'algèbre de Hecke $\mathrm{End}_{\mathbb{Z}_{(p)}[G_n]}(\mathbb{Z}_{(p)}[B_n\backslash G_n])$ (voir [Kuh85]), mais la formule donnant l'idempotent est plus compliquée (les générateurs naturels $e(i)$ de cette algèbre de Hecke ne sont plus idempotents, il faut tenir compte des facteurs supplémentaires qui apparaissent dans la table de multiplication).

Kuhn a besoin aussi de l'idempotent $\hat{e}_n$ obtenu en appliquant l'involution « chapeau » :

Corollaire 2.6. *Pour tout $\mathbb{F}_p[GL_n]$-module M, l'endomorphisme de M_{B_n} obtenu en évaluant sur M l'idempotent $\hat{e}_n$ (on voit ici l'algèbre $\mathcal{H}_n$ comme algèbre des endomorphismes du foncteur $M \mapsto M_{B_n}$) coïncide avec la composée*

$$M_{B_n} \twoheadrightarrow M_{GL_n} \to M_{B_n}$$

où la première flèche est l'application canonique et la seconde le transfert.

Ce corollaire se déduit (cf. [Kuh]) de la proposition 2.3 en utilisant l'unicité de e_n et la description de la transformation naturelle $M_{B_n} \to M_{B_n}$ associée à $\hat{e}(i)$ comme composée

$$M_{B_n} \twoheadrightarrow M_{P_i} \to M_{B_n}$$

(la deuxième flèche étant encore le transfert) où P_i est le sous-groupe (parabolique) de GL_n engendré par B_n et s_i.

Kuhn a également besoin de considérer, k et n étant deux entiers naturels, les images des éléments construits précédemment par le morphisme d'algèbres (injectif) $\mathcal{H}_k \times \mathcal{H}_n \to \mathcal{H}_{n+k}$ qui envoie les $e(i)$ de h_k sur les $e(i)$ de h_{n+k} et les $e(i)$ de $\mathcal{H}_n$ sur $e(i+k)$. En général, pour $i \le m$, on note $e_i^{(1)}$ (resp. $e_i^{(2)}$) l'image de $e_i \in \mathcal{H}_i$ dans $\mathcal{H}_m$ par le morphisme d'algèbre $\mathcal{H}_i \hookrightarrow \mathcal{H}_i \times \mathcal{H}_{m-i} \to \mathcal{H}_m$ (resp. $\mathcal{H}_i \hookrightarrow \mathcal{H}_{m-i} \times \mathcal{H}_i \to \mathcal{H}_m$). Autrement dit :

$$e_i^{(1)} = \big(e(1)e(2)\dots e(i-1)\big)\dots\big(e(1)e(2)\big)e(1),$$

$$e_i^{(2)} = \big(e(n-i+1)e(n-i+2)\dots e(n-1)\big)\dots\big(e(n_i+1)e(n-i+2)\big)e(n-i+1).$$

On utilisera aussi les analogues avec des chapeaux.

Proposition 2.7. *On a les identités suivantes dans $\mathcal{H}_{n+k}$:*

1. *(corollaire 4.12 de [Kuh], corollaire 2.8 de [KP85])*

$$e_k^{(1)}e(k)e_k^{(1)} = e_{k+1}^{(1)} \quad \textit{et} \quad \hat{e}_n^{(2)}\hat{e}(k)\hat{e}_n^{(2)} = \hat{e}_{n+1}^{(2)}\ ;$$

2. *(proposition 6.9 de [Kuh], corollaire 2.9 de [KP85])*

$$\hat{e}_n^{(2)} e_{k+1}^{(1)} \hat{e}_n^{(2)} + e_k^{(1)} \hat{e}_{n+1}^{(2)} e_k^{(1)} = \hat{e}_n^{(2)} e_k^{(1)},$$

de plus $\hat{e}_n^{(2)} e_{k+1}^{(1)} \hat{e}_n^{(2)}$ *et* $e_k^{(1)} \hat{e}_{n+1}^{(2)} e_k^{(1)}$ *sont des idempotents orthogonaux.*

Démonstration. 1. En utilisant plusieurs fois la propriété $e_k^{(1)} = e(i) e_k^{(1)}$ pour $i < k$ (proposition 2.3), on voit que $e_k^{(1)} = e_{k-1}^{(1)} e_k^{(1)}$. Comme $e_{k-1}^{(1)}$ commute à $e(k)$, on en tire

$$e_{k+1}^{(1)} = e(1) \dots e(k-1) e(k) e_k^{(1)} = e(1) \dots e(k-1) e(k) e_{k-1}^{(1)} e_k^{(1)}$$

$$= e(1) \dots e(k-1) e_{k-1}^{(1)} e(k) e_k^{(1)} = e_k^{(1)} e(k) e_k^{(1)}.$$

La deuxième identité du premier point s'en déduit formellement.

2. Comme les idempotents $e_k^{(1)}$ et $\hat{e}_n^{(2)}$ commutent, on déduit de ce qui précède les égalités suivantes :

$$\hat{e}_n^{(2)} e_{k+1}^{(1)} \hat{e}_n^{(2)} + e_k^{(1)} \hat{e}_{n+1}^{(2)} e_k^{(1)} = \hat{e}_n^{(2)} e_k^{(1)} e(k) e_k^{(1)} \hat{e}_n^{(2)} + e_k^{(1)} \hat{e}_n^{(2)} \hat{e}(k) \hat{e}_n^{(2)} e_k^{(1)}$$

$$= \hat{e}_n^{(2)} e_k^{(1)} \big(e(k) + \hat{e}(k)\big) \hat{e}_n^{(2)} e_k^{(1)} = \big(\hat{e}_n^{(2)} e_k^{(1)}\big)^2 = \hat{e}_n^{(2)} e_k^{(1)}.$$

Ainsi, $\hat{e}_n^{(2)} e_{k+1}^{(1)} \hat{e}_n^{(2)}$ et $e_k^{(1)} \hat{e}_{n+1}^{(2)} e_k^{(1)}$ sont deux éléments de l'algèbre $\hat{e}_n^{(2)} e_k^{(1)} \mathcal{H}_{n+k} \hat{e}_n^{(2)} e_k^{(1)}$ dont la somme est l'unité (de cette algèbre), il suffit donc de montrer que leur produit d'un côté est nul pour conclure que ce sont des idempotents orthogonaux. Pour le voir on calcule :

$$(\hat{e}_n^{(2)} e_{k+1}^{(1)} \hat{e}_n^{(2)})(e_k^{(1)} \hat{e}_{n+1}^{(2)} e_k^{(1)}) = \hat{e}_n^{(2)} e_{k+1}^{(1)} e_k^{(1)} \hat{e}_n^{(2)} \hat{e}_{n+1}^{(2)} e_k^{(1)} = \hat{e}_n^{(2)} e_{k+1}^{(1)} \hat{e}_{n+1}^{(2)} e_k^{(1)}$$

(en utilisant l'observation du début de la démonstration ainsi que sa variante avec un chapeau et l'exposant (2) au lieu de (1)). Or $e_{k+1}^{(1)} = e_{k+1}^{(1)} e(k)$ (par la proposition 2.3) et $\hat{e}_{n+1}^{(2)} = \hat{e}(k) \hat{e}_{n+1}^{(2)}$ (pour la même raison) ; comme $e(k)\hat{e}(k) = 0$, cela termine la démonstration.

□

3 L'idempotent de Steinberg

Notons $\bar{B}_n$ (resp. $\tilde{W}_n$) la somme (resp. la somme alternée) des éléments de B_n (resp. W_n) dans l'anneau de groupe $\mathbb{Z}[GL_n]$. L'élément

$$st_n := \frac{1}{(p^n - 1)(p^{n-1} - 1) \dots (p - 1)} \tilde{W}_n \bar{B}_n$$

(le dénominateur est l'indice des p-Sylow dans GL_n, dont le groupe des matrices triangulaires supérieures strictes $U_n \subset B_n$ est un exemple) de $\mathbb{Z}_{(p)}[GL_n]$ est idempotent, c'est l'idempotent de Steinberg. (Pour la démonstration, voir [Ste57], lemme 2.) Signalons qu'il existe bien d'autres manières d'introduire la représentation projective correspondante (notamment comme l'homologie en dimension maximale du GL_n-ensemble ordonné des sous-groupes paraboliques propres de notre groupe de Chevalley GL_n — voir par exemple [CR87], § 66C) et que la représentation de Steinberg joue un rôle fondamental dans toute la théorie des représentations du groupe linéaire (et des autres groupes qui en possèdent une).

Le lien avec les considérations précédentes est donné par la proposition suivante :

Proposition 3.1 (Proposition 4.14 de [Kuh], [Kuh85], proposition 4.15). *Soit M un $\mathbb{F}_p[GL_n]$-module. La multiplication par la réduction modulo p de st_n induit une application linéaire $M_{B_n} \to M$; sa composée avec la projection canonique $M \twoheadrightarrow M_{B_n}$ coïncide avec l'application $M_{B_n} \to M_{B_n}$ évaluation sur M de la transformation naturelle correspondant à $e_n \in \mathcal{H}_n$.*

Nous ne pourrons pas entrer dans les détails de la démonstration (voir [Kuh84]), mais mentionnons le rôle fondamental de la représentation de Steinberg pour relier algèbre de Hecke et algèbre de $GL_n(\mathbb{F}_p)$ sur $\mathbb{F}_p$ (Kuhn et Priddy notent dans [KP85] qu'on peut étendre la plupart des résultats de [Kuh84] à l'anneau de base $\mathbb{Z}_{(p)}$). Remarquons d'abord que l'algèbre de Hecke, telle que définie au début de la section 2 comme anneau d'endomorphismes sur $A[G]$ de $A[H\backslash G]$ où H est un sous-groupe d'un groupe fini G, est trivialement une sous-algèbre (avec une unité différente) de $A[G]$ lorsque l'ordre de H est inversible dans A : en effet, $e_H := \frac{1}{|H|}\sum_{h\in H}[h] \in A[G]$ est idempotent et

$$\mathrm{End}_{A[G]}(A[H\backslash G]) \simeq e_H A[G] e_H.$$

Mais lorsque l'ordre de H n'est pas inversible dans G (comme c'est le cas pour B_n dans G_n dès que $n > 1$), il n'existe plus aucun plongement évident de $\mathrm{End}_{A[G]}(A[H\backslash G])$ dans $A[G]$.

Dans [Kuh84], Kuhn commence par remarquer (théorème 1.1) que, pour $n = 2$, la sous-algèbre unitaire de $\mathbb{F}_p[GL_2]$ engendrée par l'idempotent de Steinberg est isomorphe à l'algèbre de Hecke $\mathcal{H}_2$, ce qui fournit en particulier un morphisme (unifère) d'algèbres injectif $\mathcal{H}_2 \to \mathbb{F}_p[GL_2]$. En utilisant les différentes inclusions de petits GL_2 dans GL_n (par choix de deux éléments de la base canonique de $\mathbb{F}_p^n$), on en déduit un morphisme injectif $\mathcal{H}_n \to \mathbb{F}_p[GL_n]$ pour tout n (théorème 3.1 de [Kuh84], valable dans le cadre général d'un système de Tits *scindé* — notion pour laquelle on pourra par exemple se référer à [CR87], § 69). Cette construction repose sur la présentation explicite de l'algèbre de Hecke que nous avons présentée dans la section 2. Cela fait, la proposition 3.1 devient pour l'essentiel une reformulation de résultats de la section précédente.

4 Utilisation homotopique

On commence par rappeler la définition de l'espace de Thom associé à un fibré vectoriel. Il s'agit ici de fibrés vectoriels localement triviaux, de rang fini, réels (on pourrait remplacer $\mathbb{R}$ par un autre corps topologique localement compact). Si V est un $\mathbb{R}$-espace vectoriel de dimension finie (qu'on munira toujours de la topologie usuelle), on note $\mathbf{S}(V)$ le compactifié d'Alexandroff de V. On définit ainsi un foncteur des $\mathbb{R}$-espaces vectoriels de dimension finie avec *injections* linéaires vers les espaces topologiques pointés. (En particulier, si V est une représentation réelle d'un groupe G, $\mathbf{S}(V)$ hérite d'une action continue de G.) Pour un fibré trivial $X \times V \twoheadrightarrow X$ sur X, l'espace de Thom est

$$\mathrm{Th}(X \times V \to X) := X \rtimes \mathbf{S}(V)(= X_+ \wedge \mathbf{S}(V)).$$

On rappelle la notation $X \rtimes Y$ (produit semi-contracté de X par Y) où X est un espace topologique et Y un espace topologique pointé (de point de base y) : c'est l'espace pointé $(X \times Y)/(X \times \{y\})$. La fonctorialité de cette construction permet de l'étendre en un foncteur Th de la catégorie des fibrés vectoriels (réels, de dimension finie, localement triviaux), les morphismes étant les morphismes usuels *injectifs entre les fibres*, vers les espaces topologiques pointés.

Si V est une représentation (réelle, de dimension finie) d'un groupe G, le morphisme de groupes $G \to GL(V)$ correspondant induit une application continue $BG \to BGL(V)$, donc un fibré vectoriel de fibres isomorphes (comme $\mathbb{R}$-espaces vectoriels) à V. On peut également le décrire comme la projection

$$EG \underset{G}{\times} V \twoheadrightarrow EG \underset{G}{\times} * = BG.$$

Son espace de Thom s'identifie donc à

$$EG \underset{G}{\rtimes} \mathbf{S}(V).$$

Si G est un groupe fini et V la représentation régulière (sur $\mathbb{R}$) de G, cet espace est muni d'une action naturelle du groupe $\mathrm{Aut}\,(G)$, puisque celui-ci opère sur ladite représentation. On note aussi que cet espace est une suspension parce que la représentation régulière contient une copie de la représentation triviale (utiliser les homéomorphismes pointés naturels $\mathbf{S}(V \oplus W) \simeq \mathbf{S}(V) \wedge \mathbf{S}(W)$).

Dans le cas du p-groupe abélien élémentaire de rang k $E_k = (\mathbb{Z}/p)^k$, on obtient ainsi un espace pointé muni d'une action de $GL_k(\mathbb{F}_p)$, qui est une suspension (et ce de façon compatible à l'action), espace que Kuhn note $BE_k^{\rho_k}$ dans [Kuh]. Plus précisément, l'espace que considère Kuhn est le p-complété de cet espace (il n'y a pas de souci avec cette procédure : suspension d'un espace connexe, l'espace est simplement connexe). Le fait qu'on ait affaire à une suspension, donc à un co-H-espace, permet d'additionner les applications continues $BE_k^{\rho_k} \to BE_k^{\rho_k}$; comme on a p-complété l'espace on peut même en faire des combinaisons linéaires à coefficients dans $\mathbb{Z}_{(p)}$. Par conséquent, tout élément de l'algèbre $\mathbb{Z}_{(p)}[GL_k(\mathbb{F}_p)]$ induit une application continue (pointée) de $BE_k^{\rho_k}$ dans lui-même. Les éléments idempotents de l'algèbre agissent d'une façon idempotente à homotopie près. L'espace $L_1(k)$ de la prépublication de Kuhn est le téléscope de $BE_k^{\rho_k}$ pour l'idempotent de Steinberg de $\mathbb{Z}_{(p)}[GL_k(\mathbb{F}_p)]$, c'est-à-dire la colimite de la suite de morphismes répétant indéfiniment cette application idempotente. (L'effet en homologie à coefficients dans $\mathbb{F}_p$, par exemple, consiste simplement à appliquer l'idempotent de Steinberg à l'homologie de $BE_k^{\rho_k}$, homologie qui hérite d'une action du groupe linéaire.)

L'intervention fondamentale de l'algèbre de Hecke dans le travail de Kuhn provient du théorème suivant, établi dans la section 6 de la prépublication qu'on étudie, et qui fera l'objet d'un exposé ultérieur.

Théorème 4.1 (Théorème 6.3 de [Kuh]). *L'algèbre des endomorphismes de $H_*(BE_k^{\rho_k};\mathbb{F}_p)_{B_k}$ linéaires sur l'algèbre de Steenrod est isomorphe à l'algèbre de Hecke $\mathcal{H}_k$.*

(L'énoncé de Kuhn est plus précis : l'isomorphisme est explicité.)

Références

[Bou68] N. Bourbaki – *Éléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Chapitre IV : Groupes de Coxeter et systèmes de Tits. Chapitre V : Groupes engendrés par des réflexions. Chapitre VI : systèmes de racines*, Actualités Scientifiques et Industrielles, No. 1337, Hermann, Paris, 1968.

[CIK71] C. W. Curtis, N. Iwahori & R. Kilmoyer – « Hecke algebras and characters of parabolic type of finite groups with (B, N)-pairs », *Inst. Hautes Études Sci. Publ. Math.* (1971), no. 40, p. 81–116.

[CR81] C. W. Curtis & I. Reiner – *Methods of representation theory. Vol. I*, John Wiley & Sons Inc., New York, 1981, With applications to finite groups and orders, Pure and Applied Mathematics, A Wiley-Interscience Publication.

[CR87] — , *Methods of representation theory. Vol. II*, Pure and Applied Mathematics (New York), John Wiley & Sons Inc., New York, 1987, With applications to finite groups and orders, A Wiley-Interscience Publication.

[KP85] N. J. Kuhn & S. B. Priddy – « The transfer and Whitehead's conjecture », *Math. Proc. Cambridge Philos. Soc.* **98** (1985), no. 3, p. 459–480.

[KT08] C. Kassel & V. Turaev – *Braid groups*, Graduate Texts in Mathematics, vol. 247, Springer, New York, 2008, With the graphical assistance of Olivier Dodane.

[Kuh] N. J. Kuhn – « The Whitehead conjecture, the tower of S^1 conjecture, and Hecke algebras of type A », Disponible sur http ://front.math.ucdavis.edu/1308.4441.

[Kuh84] — , « The modular Hecke algebra and Steinberg representation of finite Chevalley groups », *J. Algebra* **91** (1984), no. 1, p. 125–141, With an appendix by Peter Landrock.

[Kuh85] — , « Chevalley group theory and the transfer in the homology of symmetric groups », *Topology* **24** (1985), no. 3, p. 247–264.

[Ste57] R. Steinberg – « Prime power representations of finite linear groups. II », *Canad. J. Math.* **9** (1957), p. 347–351.