

LES ALGÈBRES DE HECKE

Ici nous préparons le terrain algébrique pour la construction du polynôme universel au prochain chapitre. Nous commencerons par quelques rappels de connaissances algébriques de base, concernant notamment une généralisation des ensembles de matrices carrées d'un même ordre à coefficients dans un corps fixe. Ensuite nous définirons et étudierons en détail certains objets algébriques, les *algèbres de Hecke*, qui englobent simultanément les groupes de tresses et les groupes de permutations. Pour terminer nous étendrons la notion classique de la trace d'une matrice aux éléments des algèbres de Hecke.

A. Algèbres, modules et produits tensoriels

L'étude des algèbres de Hecke demande certaines connaissances algébriques qui ne sont pas enseignées en général au premier cycle mais qui font néanmoins partie des outils quotidiens de l'algébriste.

Pour commencer nous allons préciser ce qu'est une *algèbre*, puisque les algèbres de Hecke sont, d'après leur nom, des objets de ce type. Il s'agit en fait d'abstraire et généraliser les propriétés les plus importantes des ensembles de matrices carrées.

DÉFINITION. Soit \mathbb{k} un corps quelconque. Un anneau A est une \mathbb{k} -*algèbre* s'il est également un espace vectoriel sur \mathbb{k} , de telle manière à ce que les deux structures soient compatibles dans le sens suivant.

$$\alpha(ab) = (\alpha a)b = a(\alpha b) \quad \forall a, b \in A, \alpha \in \mathbb{k}.$$

EXEMPLE. Soit V un espace vectoriel sur un corps \mathbb{k} . Alors l'ensemble $End(V)$ de toutes les application linéaires de V vers lui-même – les *endomorphismes de V* – est une algèbre, où les opérations sont définies de la manière usuelle.

La deuxième notion algébrique dont nous aurons besoin généralise la notion d'espace vectoriel.

DÉFINITION. Soit A un anneau. Un A -*module* à gauche (respectivement, à droite) consiste en un groupe abélien M , écrit additivement, et une opération qui associe à chaque couple $x \in M, a \in A$ un nouvel élément $ax \in M$ (respectivement, $xa \in M$) et qui vérifie les conditions suivantes.

- (1) $a(x + x') = ax + ax'$ (respectivement, $(x + x')a = xa + x'a$) $\forall x, x' \in M, \forall a \in A$.
- (2) $(ab)x = a(bx)$ (respectivement, $x(ab) = (xa)b$) $\forall x \in M, \forall a, b \in A$.
- (3) $(a+b)x = ax+bx$ (respectivement, $x(a+b) = xa+xb$) $\forall x \in M, \forall a, b \in A$.

Si M est un A -module à gauche et à droite simultanément et $(ax)b = a(xb)$ pour tout $x \in M$ et $a, b \in A$, alors M est un A -bimodule.

EXEMPLES.

- (1) Tout groupe abélien G est un \mathbb{Z} -bimodule, où

$$nw = \underbrace{w + \dots + w}_{n \text{ fois}} = wn.$$

Par exemple, $\mathbb{Z}/2\mathbb{Z}$ est un \mathbb{Z} -bimodule. Ainsi nous voyons que les modules ne sont pas aussi simples que les espaces vectoriels, car un A -module n'est pas toujours égal à une somme directe de copies de A .

- (2) Tout idéal de A est un A -bimodule.

Pour comprendre l'algèbre de Hecke, il nous faudra une construction algébrique, le *produit tensoriel* de deux modules, qui peut paraître assez compliquée et non-intuitive au début. D'abord nous l'expliquerons en termes d'une propriété universelle. Nous démontrerons ensuite son existence par une construction explicite, avant d'en présenter quelques exemples explicites.

DÉFINITION. Soit A un anneau. Soient M un A -module à droite et N un A -module à gauche, et soit $M \times N$ leur produit cartésien, en tant qu'ensemble. Une application ensembliste $f : M \times N \rightarrow H$, où H est un groupe abélien, est *bilinéaire* si

$$\begin{aligned} f(x_1 + x_2, y_1 + y_2) &= f(x_1, y_1) + f(x_1, y_2) \\ &\quad + f(x_2, y_1) + f(x_2, y_2) \quad \forall x_1, x_2 \in M, \forall y_1, y_2 \in N. \end{aligned}$$

Elle est A -invariant si $f(xa, y) = f(x, ay)$ pour tout $x \in M, y \in N, a \in A$.

Un *produit tensoriel* de M et N sur A , consiste en une application bilinéaire et A -invariant $\mathfrak{p} : M \times N \rightarrow G$ tel que pour tout autre application bilinéaire et A -invariant $f : M \times N \rightarrow H$ il existe un unique homomorphisme de groupes abéliens $\hat{f} : G \rightarrow H$ tel que le diagramme suivant commute.

$$\begin{array}{ccc} M \times N & \xrightarrow{\mathfrak{p}} & G \\ & \searrow f & \downarrow \hat{f} \\ & & H \end{array}$$

Puisque nous avons défini le produit tensoriel par une propriété universelle, la même démonstration que toujours montre que si le produit tensoriel de deux modules existe, alors il est unique. Voyons ce qu'il en est de son existence.

LEMME 1. Soit A un anneau. Soient M un A -module à droite et N un A -module à gauche. Le produit tensoriel de M et N sur A existe.

PREUVE. Définir une relation d'équivalence sur $M \times N$ par

$$(x, y) \sim (x', y') \Leftrightarrow \exists a \in A \text{ t.q. } x' = xa, y = ay'.$$

Poser $Z = M \times N / \sim$, l'ensemble des classes d'équivalence sous cette relation. Considérer $(\mathcal{F}(Z))_{ab}$, l'abélienisation du groupe libre engendré par Z , que nous écrivons additivement. Soit

$$R = \{[(x_1 + x_2, y_1 + y_2)] = \sum_{i,j=1}^2 [(x_i, y_j)] \mid x_i \in M, y_j \in N, i, j = 1, 2\},$$

et notons $Q(R)$ le plus petit sousgroupe de $(\mathcal{F}(Z))_{ab}$ qui contient R . Définir

$$\mathfrak{p} : M \times N \rightarrow \frac{(\mathcal{F}(Z))_{ab}}{Q(R)} : (m, n) \rightarrow [(m, n)].$$

Il est maintenant une conséquence immédiate de la propriété universelle du groupe libre et de celle de l'abélienisation que \mathfrak{p} vérifie la propriété universelle du produit tensoriel. \square

NOTATION. Etant donné que le produit tensoriel sur A de deux modules M et N existe toujours et est unique, nous pouvons fixer une notation, $M \otimes_A N$, pour désigner cet objet. Nous écrirons également $x \otimes y$ pour désigner le générateur qui est la classe du couple (x, y) , ce qui veut dire que

$$(xa) \otimes y = x \otimes (ay) \quad \text{et} \quad (x_1 + x_2) \otimes (y_1 + y_2) = \sum_{i,j=1}^2 x_i \otimes y_j$$

pour tout $x \in M$, $y \in N$, et $a \in A$.

REMARQUE. Si M (respectivement, N) est un A -bimodule, alors $M \otimes_A N$ est doté d'une structure naturelle de A -module à gauche (respectivement, à droite) définie par $a(x \otimes y) = (ax) \otimes y$ (respectivement, $(x \otimes y)a = x \otimes (ya)$).

Le produit tensoriel est une construction dont l'importance en algèbre et topologie serait difficile de surestimer. Les algébristes et topologues sont toujours en train de calculer des produits tensoriels. Voici quelques exemples de ces calculs.

EXEMPLES.

- (1) Il est facile de voir que $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z} = 0$ pour tout $p \in \mathbb{Z}$. En effet, pour tout $q \in \mathbb{Q}$ et $x \in \mathbb{Z}/p\mathbb{Z}$,

$$q \otimes x = \frac{q}{p} \cdot p \otimes x = \frac{q}{p} \otimes \underbrace{px}_{=0} = 0.$$

- (2) Soit \mathbb{k} un corps, et soit G un groupe quelconque. Alors \mathbb{k} et $\mathbb{Z}[G]$ ont tous les deux une structure sous-jacente de groupe abélien, i.e., ce sont des \mathbb{Z} -bimodules. Nous pouvons donc former leur produit tensoriel

$$\mathbb{k}[G] = \mathbb{k} \otimes_{\mathbb{Z}} \mathbb{Z}[G],$$

qui est même une \mathbb{k} -algèbre, dont la structure d'anneau est donnée par

$$(q \otimes \sigma)(q' \otimes \sigma') = qq' \otimes \sigma\sigma'$$

et la structure d'espace vectoriel par

$$q(r \otimes \sigma) = (qr) \otimes \sigma.$$

Observer que $\{1 \otimes w \mid w \in G\}$ est une base de $\mathbb{k}[G]$, ce qui nous permet d'écrire

$$\mathbb{k}[G] \cong \left\{ \sum_{i=1}^n q_i \cdot w_i \mid q_i \in \mathbb{k}, w_i \in G, n \in \mathbb{N} \right\}.$$

D'ailleurs, si V est un \mathbb{k} -espace vectoriel et $f : G \rightarrow V$ est une application ensembliste, alors f possède une unique extension linéaire

$$\hat{f} : \mathbb{k}[G] \rightarrow V : \sum_{i=1}^n q_i \cdot w_i \rightarrow \sum_{i=1}^n q_i \cdot f(w_i).$$

Ce deuxième exemple nous sera très utile par la suite, car il nous permet de présenter des algèbres, de la même manière que nous avons présenté des groupes auparavant. Ainsi nous aurons un moyen compact pour spécifier les algèbres, en particulier les algèbres de Hecke.

DÉFINITION. Une *présentation* d'une \mathbb{k} -algèbre A consiste en un ensemble \mathbf{x} , un sousensemble $\mathbf{r} \subseteq \mathbb{k}[\mathcal{F}(\mathbf{x})]$ et un isomorphisme

$$\frac{\mathbb{k}[\mathcal{F}(\mathbf{x})]}{\langle \mathbf{r} \rangle} \xrightarrow{\cong} A.$$

B. La structure des algèbres de Hecke

Nous sommes enfin prêts à étudier les objets algébriques qui sont au coeur de la construction du polynôme universel – les algèbres de Hecke.

Nous commençons par spécifier la structure d'algèbre des algèbres de Hecke, ce qui sera vite fait, grâce à la notion de présentation d'algèbre. Ensuite nous consacrerons beaucoup de temps à l'étude de leur structure d'espace vectoriel. Plus précisément, nous leur construirons une belle base explicite.

DÉFINITION. Soient \mathbb{k} un corps, $q \in \mathbb{k}$, et $n \geq 2$, un entier. La (n, q) ^{ième}-algèbre de Hecke, notée $\mathcal{H}_n(q)$, est la \mathbb{k} -algèbre dont une présentation est

$$\left(\begin{array}{l} \tau_i \tau_j = \tau_j \tau_i : |i - j| > 1 \\ \tau_1, \dots, \tau_{n-1} : \tau_i \tau_{i+1} \tau_i = \tau_{i+1} \tau_i \tau_{i+1} : 1 \leq i < n - 1 \\ \tau_i^2 = (q - 1) \tau_i + q : 1 \leq i < n \end{array} \right).$$

Cette présentation doit nous rappeler deux choses: la présentation de \mathcal{S}_n , aussi bien que celle de \mathcal{B}_n . Une comparaison des présentations montre que $\mathbb{k}[\mathcal{S}_n] = \mathcal{H}_n(1)$ pour tout n , où τ_i correspond à la permutation $(i \ i + 1)$, tandis que tout $\mathcal{H}_n(q)$ est un quotient de $\mathbb{k}[\mathcal{B}_n]$. Par la suite, nous explorerons plus en détail les liens fascinants et révélateurs entre ces trois algèbres.

Avant de commencer notre étude de la structure d'espace vectoriel de $\mathcal{H}_n(q)$, il est important d'observer que la suite d'inclusions d'ensemble

$$\{\tau_1\} \hookrightarrow \{\tau_1, \tau_2\} \hookrightarrow \dots \hookrightarrow \{\tau_1, \dots, \tau_{n-1}\} \hookrightarrow \{\tau_1, \dots, \tau_n\} \hookrightarrow \dots$$

induit une suite d'inclusions d'algèbre

$$\mathcal{H}_2(q) \hookrightarrow \mathcal{H}_3(q) \hookrightarrow \dots \hookrightarrow \mathcal{H}_n(q) \hookrightarrow \mathcal{H}_{n+1}(q) \hookrightarrow \dots$$

Par conséquent, $\mathcal{H}_{n+1}(q)$ est clairement un $\mathcal{H}_n(q)$ -bimodule, pour tout n .

Comme nous le montrerons par la suite, il y a une base de $\mathcal{H}_n(q)$ qui consiste en éléments du type défini ci-dessous.

DÉFINITION. Pour tout $k \geq 1$, poser $T_k = \{1, \tau_k, \tau_k \tau_{k-1}, \dots, \tau_k \tau_{k-1} \cdots \tau_2 \tau_1\}$. Un élément $a \in \mathcal{H}_{n+1}(q)$ est *normal* si $a = a_1 a_2 \cdots a_n$, où $a_k \in T_k$ pour tout $1 \leq k \leq n$.

NOTATION. L'ensemble de tous les éléments normaux de $\mathcal{H}_{n+1}(q)$ sera dénoté \mathcal{N}_n . Puisque cet ensemble est indépendant de q , le q n'apparaît pas dans la notation. Observer également que $\mathcal{N}_{n-1} \subset \mathcal{N}_n$ pour tout n .

Puisque $\#T_k = k + 1$ pour tout k , il existe $(n + 1)!$ éléments normaux dans $\mathcal{H}_n(q)$.

THÉORÈME 2. *L'ensemble \mathcal{N}_n est une \mathbb{k} -base de $\mathcal{H}_{n+1}(q)$.*

Nous démontrerons ce théorème par une suite de lemmes. Les deux premiers lemmes servent à montrer que tout élément de $\mathcal{H}_{n+1}(q)$ est égal à une combinaison linéaire d'éléments normaux. Nous établirons d'abord une première approximation à ce résultat, que nous raffinerons ensuite dans le deuxième lemme.

Le but du troisième lemme est de nous permettre d'utiliser notre connaissance de \mathcal{S}_n pour démontrer l'indépendance linéaire de l'ensemble des éléments normaux. Ainsi, nous aurons démontré le théorème.

LEMME 3. *L'algèbre $\mathcal{H}_{n+1}(q)$ est engendrée en tant qu'espace vectoriel par les monômes dans lesquels τ_n apparaît au plus une fois.*

PREUVE. Cette preuve se fait par récurrence sur n .

Puisque $(\tau_1 : \tau_1^2 = (q - 1) \cdot \tau_1 + q)$ est une présentation de $\mathcal{H}_2(q)$, on a que

$$\tau_1^k = (q - 1) \cdot \tau_1^{k-1} + q \cdot \tau_1^{k-2}$$

pour tout $k \geq 2$, i.e., toute puissance plus grande que 1 de τ_1 s'exprime comme une combinaison linéaire de puissances strictement inférieures du même élément. Appliquant cette substitution $k - 1$ fois à τ_1^k , nous obtenons une combinaison linéaire de τ_1 et de 1 qui est égale à τ_1^k .

Ainsi, le lemme est vrai pour $n = 1$.

Supposons que le lemme soit vrai pour n , et vérifions-le pour $n + 1$. Soit $a \in \mathcal{H}_{n+1}(q)$. Nous allons exprimer a comme une combinaison linéaire de monômes de $\mathcal{H}_{n+1}(q)$ dans lesquels τ_n apparaît moins de fois que dans a .

Ecrire $a = b \tau_n c \tau_n d$, où $b, d \in \mathcal{H}_{n+1}(q)$ et $c \in \mathcal{H}_n(q)$. Par l'hypothèse de récurrence nous pouvons supposer que soit $c \in \mathcal{H}_{n-1}(q)$, soit $c = c' \tau_{n-1} c''$, où $c', c'' \in \mathcal{H}_{n-1}(q)$.

Dans le premier cas

$$a = bc\tau_n^2 d = (q-1) \cdot bc\tau_n d + q \cdot bcd,$$

ce qui est la combinaison linéaire recherchée.

Dans le deuxième cas,

$$\begin{aligned} a &= b\tau_n c' \tau_{n-1} c'' \tau_n d \\ &= bc' \tau_n \tau_{n-1} \tau_n c'' d \\ &= bc' \tau_{n-1} \tau_n \tau_{n-1} c'' d, \end{aligned}$$

ce qui nous permet de conclure. \square

LE CAS $q = 1$. Observer que l'argument ci-dessus montre que tout monôme de $\mathcal{H}_{n+1}(1)$ est égal à un *monôme* où τ_n n'apparaît qu'une seule fois.

Nous allons maintenant raffiner les arguments de cette dernière preuve, montrant que l'on peut se restreindre à ne considérer que les éléments normaux.

LEMME 4. *L'ensemble \mathcal{N}_n engendre $\mathcal{H}_{n+1}(q)$ en tant que \mathbb{k} -espace vectoriel.*

PREUVE. De nouveau la preuve se fait par récurrence sur n .

Puisque $\mathcal{N}_1 = \{1, \tau_1\}$, le lemme 4 est équivalent au lemme 3 pour $n = 1$.

Supposons que le lemme soit vrai pour n , et vérifions-le pour $n + 1$. Grâce au lemme 3, nous savons que $\mathcal{H}_{n+1}(q)$ est engendré par $\mathcal{H}_n(q) \cup \{a\tau_n b \mid a, b, \in \mathcal{H}_n(q)\}$. Or par l'hypothèse de récurrence, $\mathcal{H}_n(q)$ est engendré par \mathcal{N}_{n-1} , donc $\mathcal{H}_{n+1}(q)$ est engendré par $\mathcal{N}_{n-1} \cup \{a\tau_n b \mid a, b, \in \mathcal{H}_n(q)\}$.

Considérer $a\tau_n b$, où $a, b, \in \mathcal{H}_n(q)$. Grâce à l'hypothèse de récurrence, on peut supposer que $b \in \mathcal{N}_{n-1}$. Ecrire $b = b_1 \cdots b_{n-1}$, où $b_i \in T_i$. Alors

$$a\tau_n b = \underbrace{ab_1 \cdots b_{n-2}}_{\in \mathcal{H}_n(q)} \underbrace{\tau_n b_{n-1}}_{\in T_n}.$$

Par l'hypothèse de récurrence, $ab_1 \cdots b_{n-2} = \sum_{i=1}^k q_i \cdot c_i$, où $q_i \in \mathbb{k}$, $c_i \in \mathcal{N}_{n-1}$ pour tout i . Donc

$$a\tau_n b = \sum_{i=1}^k q_i \cdot \underbrace{c_i \tau_n b_{n-1}}_{\in \mathcal{N}_n},$$

i.e., $a\tau_n b$ est égal à une combinaison linéaire d'éléments normaux. \square

LE CAS $q = 1$. Dans ce cas nous pouvons même montrer que tout monôme de $\mathcal{H}_{n+1}(1)$ est égal à un monôme normal, à cause de la version spéciale du lemme 3 dans ce même cas.

Faisons maintenant un pas critique vers la démonstration de l'indépendance linéaire de \mathcal{N}_n dans $\mathcal{H}_{n+1}(q)$.

LEMME 5. *Pour tout $q \in \mathbb{k}$, il existe une application linéaire*

$$\psi : \mathcal{H}_{n+1}(q) \rightarrow \mathcal{H}_{n+1}(1) = \mathbb{k}[\mathcal{S}_{n+1}]$$

qui est l'identité sur \mathcal{N}_n .

PREUVE. Puisque nous ne connaissons pas encore de base explicite de $\mathcal{H}_{n+1}(q)$, nous ne pouvons pas définir ψ sur une base et puis étendre linéairement, comme cela se fait souvent. Nous sommes obligés de définir ψ indirectement.

Nous définirons une application linéaire $\widehat{\Psi} : \mathcal{H}_{n+1}(q) \rightarrow \text{End}(\mathcal{H}_{n+1}(1))$ telle que $\widehat{\Psi}(a)(1) = a$ pour tout $a \in \mathcal{N}_n$. Nous pourrons ensuite définir ψ par $\psi(a) = \widehat{\Psi}(a)(1)$ pour tout $a \in \mathcal{H}_{n+1}(q)$.

Commençons la construction de $\widehat{\Psi}$ en définissant une application ensembliste

$$\omega : \mathcal{S}_{n+1} \rightarrow \mathbb{N}$$

où $\omega(\tau)$ est la longueur du plus petit mot de $\mathcal{F}(\{\tau_1, \dots, \tau_n\})$ qui est un représentant de τ . Ensuite, pour tout $1 \leq i \leq n$, soit

$$\Psi_i : \mathbb{k}[\mathcal{S}_{n+1}] \rightarrow \mathbb{k}[\mathcal{S}_{n+1}]$$

l'application linéaire précisée par

$$\Psi_i(\tau) = \begin{cases} (i \ i + 1)\tau & : \omega((i \ i + 1)\tau) > \omega(\tau) \\ q \cdot (i \ i + 1)\tau + (q - 1) \cdot \tau & : \text{sinon.} \end{cases}$$

(Voir l'exemple (2) dans le paragraphe A.)

Enfin, considérer l'application ensembliste

$$\Psi : \{\tau_1, \dots, \tau_n\} \rightarrow \text{End}(\mathbb{k}[\mathcal{S}_{n+1}]) : \tau_i \mapsto \Psi_i.$$

Affirmation: Ψ s'étend en un homomorphisme d'algèbres

$$\widehat{\Psi} : \mathcal{H}_{n+1}(q) \rightarrow \text{End}(\mathcal{H}_{n+1}(1)).$$

Preuve de l'affirmation: Il faut vérifier les trois égalités suivantes.

- (1) $\Psi_i \Psi_j = \Psi_j \Psi_i \quad \forall |i - j| > 1.$
- (2) $\Psi_i \Psi_{i+1} \Psi_i = \Psi_{i+1} \Psi_i \Psi_{i+1} \quad \forall 1 \leq i < n.$
- (3) $\Psi_i \Psi_i = (q - 1) \cdot \Psi_i + q \quad \forall 1 \leq i \leq n.$

Ici nous vérifierons la dernière, laissant les deux autres comme exercices.

Soit $\tau \in \mathcal{S}_{n+1}$. Si $\omega((i \ i + 1)\tau) > \omega(\tau)$, alors

$$\begin{aligned} \Psi_i \circ \Psi_i(\tau) &= \Psi_i((i \ i + 1)\tau) \\ &= q \cdot (i \ i + 1)^2 \tau + (q - 1) \cdot (i \ i + 1)\tau \\ &= q \cdot \tau + (q - 1) \cdot (i \ i + 1)\tau \\ &= ((q - 1) \cdot \Psi_i + q)(\tau). \end{aligned}$$

Par contre, si $\omega((i \ i + 1)\tau) < \omega(\tau)$, alors

$$\begin{aligned} \Psi_i \circ \Psi_i(\tau) &= \Psi_i(q \cdot (i \ i + 1)\tau + (q - 1) \cdot \tau) \\ &= q \cdot (i \ i + 1)^2 \tau + (q - 1) \cdot \Psi_i(\tau) \\ &= (q + (q - 1) \cdot \Psi_i)(\tau). \end{aligned}$$

Ainsi l'égalité (3) est vérifiée.

Ayant établi l'existence de l'homomorphisme d'algèbres $\widehat{\Psi}$, il faut montrer que $\widehat{\Psi}(a)(1) = a$ pour tout $a \in \mathcal{N}_n$. Écrire $a = a_1 \cdots a_n$, où $a_i = \tau_i \cdots \tau_{i-k_i} \in T_i$. Observer d'abord que

$$\begin{aligned} \widehat{\Psi}(a_i)(1) &= \Psi_{i-k_i} \circ \cdots \circ \Psi_i(1) \\ &= (i - k_i \ i - k_i + 1)(i - k_i + 1 \ i - k_i + 2) \cdots (i - 1 \ i)(i \ i + 1) \\ &= a_i, \end{aligned}$$

puisque

$$\omega((i - j \ i - j + 1) \cdots (i \ i + 1)) < \omega((i - j - 1 \ i - j)(i - j \ i - j + 1) \cdots (i \ i + 1))$$

pour tout $0 \leq j < i$. Plus généralement, $\widehat{\Psi}(a)(1) = a$, car seule la relation $\tau_i^2 = 1$ dans la présentation de \mathcal{S}_n réduit la longueur d'un mot. Or un élément normal ne contient aucun carré de générateur. \square

Voyons maintenant pourquoi l'existence de ψ entraîne l'indépendance linéaire de \mathcal{N}_n dans $\mathcal{H}_{n+1}(q)$.

COROLLAIRE 6. *L'ensemble \mathcal{N}_n est linéairement indépendant dans $\mathcal{H}_{n+1}(q)$.*

PREUVE. L'existence de $\widehat{\Psi}$ implique que si \mathcal{N}_n est linéairement indépendant dans $\mathcal{H}_{n+1}(1)$, alors il l'est également dans $\mathcal{H}_{n+1}(q)$.

L'indépendance linéaire de \mathcal{N}_n dans $\mathcal{H}_{n+1}(1)$ est évidente, car les éléments normaux de $\mathcal{H}_{n+1}(1)$ sont des éléments de \mathcal{S}_{n+1} . Or nous avons déjà vu que $\{1 \otimes w \mid w \in G\}$ est linéairement indépendant dans $\mathbb{k}[G]$ pour tout groupe G . \square

Le lemme 4 et le corollaire 6 pris ensemble entraînent le théorème 2.

C. La trace sur $\mathcal{H}_n(q)$

Avant de pouvoir définir le polynôme universel, il faut mettre en place un dernier morceau purement algébrique du puzzle: une fonction analogue à la fonction trace sur l'ensemble des matrices carrées. Il s'agit d'une famille d'applications linéaires

$$Tr : \mathcal{H}_n(q) \rightarrow \mathbb{k}, \quad n \geq 2$$

compatibles avec les inclusions $\mathcal{H}_n(q) \hookrightarrow \mathcal{H}_{n+1}(q)$ et vérifiant des propriétés intéressantes. Parmi ces propriétés se trouve une qui rappelle la propriété clé de la trace d'une matrice, justifiant ainsi le choix de terminologie.

THÉORÈME 7. *Soit \mathbb{k} un corps, et soient $q, z \in \mathbb{k}$. Alors il existe une famille d'applications linéaires*

$$Tr : \mathcal{H}_n(q) \rightarrow \mathbb{k}, \quad n \geq 2$$

compatibles avec les inclusions $\mathcal{H}_n(q) \hookrightarrow \mathcal{H}_{n+1}(q)$, vérifiant les propriétés suivantes.

- (1) $Tr(1) = 1$.
- (2) $Tr(ab) = Tr(ba) \quad \forall a, b \in \mathcal{H}_n(q)$.
- (3) $Tr(a\tau_n b) = z \cdot Tr(ab) \quad \forall a, b \in \mathcal{H}_n(q)$.

REMARQUE. Les propriétés de la trace nous permettent de calculer $Tr(a)$ pour tout $a \in \mathcal{H}_n(q)$, sachant que a s'exprime comme une combinaison linéaire d'éléments normaux. Par exemple,

$$Tr(\tau_1) = Tr(1 \cdot \tau_1 \cdot 1) = z \cdot Tr(1) = z,$$

donc

$$Tr(\tau_1 \tau_2) = z \cdot Tr(\tau_1) = z^2,$$

et

$$Tr(\tau_1 \tau_2 \tau_1) = z Tr(\tau_1^2) = z Tr((q-1)\tau_1 + q) = (q-1)z^2 + qz.$$

PREUVE. Nous définirons Tr par récurrence sur les éléments normaux de $\mathcal{H}_n(q)$ et l'étendrons ensuite par linéarité à toute l'algèbre. Nous avons déjà amorcé la récurrence dans l'exemple précédent, lorsque nous avons montré que l'on a forcément $Tr(\tau_1) = z$, car $\mathcal{N}_1 = \{1, \tau_1\}$. Nous complétons cette base de la récurrence en posant $Tr(1) = 1$, pour être en accord avec la condition (1).

Supposons que Tr soit définie sur \mathcal{N}_{n-1} et que son extension linéaire à $\mathcal{H}_n(q)$ satisfasse aux conditions (1) – (3). Soit $a \in \mathcal{N}_n \setminus \mathcal{N}_{n-1}$. Alors $a = b\tau_n c$, où $b \in \mathcal{N}_{n-1}$ et $c \in T_{n-1} \subset \mathcal{N}_{n-1}$. Poser

$$Tr(a) = z \cdot Tr(bc).$$

La trace ainsi définie satisfait à la condition (3) par construction. Vérifions qu'elle satisfasse également à la condition (2).

Il suffit de vérifier la condition (2) pour un produit de deux éléments de la base, car la multiplication dans $\mathcal{H}_{n+1}(q)$ et la trace sont des applications linéaires. Soient $a, b \in \mathcal{N}_n$. Si ni a , ni b n'a de facteur de τ_n , alors l'hypothèse de récurrence implique que $Tr(ab) = Tr(ba)$. Supposons donc que a possède un facteur de τ_n , i.e., $a = a'\tau_n a''$, où $a', a'' \in \mathcal{N}_{n-1}$, tandis que $b \in \mathcal{N}_{n-1}$. Alors

$$\begin{aligned} Tr(ab) &= Tr(a'\tau_n a''b) \\ &= z \cdot Tr(a'a''b) \\ &= z \cdot Tr(ba'a'') \quad \text{par l'hypothèse de récurrence} \\ &= Tr(ba'\tau_n a'') \\ &= Tr(ba). \end{aligned}$$

Ainsi, la condition (2) est vérifiée si $a \in \mathcal{H}_{n+1}(q)$ et $b \in \mathcal{H}_n(q)$.

Considérer l'affirmation suivante.

Affirmation: $Tr(a\tau_n b\tau_n) = Tr(\tau_n a\tau_n b)$ pour tout $a, b \in \mathcal{H}_n(q)$.

Si cette affirmation est juste, nous pourrions conclure la démonstration du théorème, car pour tout $a, b, a', b' \in \mathcal{H}_n(q)$, nous aurons que

$$\begin{aligned} Tr(a\tau_n b a' \tau_n b') &= Tr(b' a \tau_n b a' \tau_n) \quad \text{par le cas précédent} \\ &= Tr(\tau_n b' a \tau_n b a') \quad \text{par l'affirmation} \\ &= Tr(a' \tau_n b' a \tau_n b) \quad \text{par le cas précédent.} \end{aligned}$$

Preuve de l'affirmation: Il y a quatre cas à traiter.

- (1) $a, b, \in \mathcal{N}_{n-2}$.
- (2) $a \in \mathcal{N}_{n-2}$ et $b \in \mathcal{N}_{n-1} \setminus \mathcal{N}_{n-2}$.
- (3) $a \in \mathcal{N}_{n-1} \setminus \mathcal{N}_{n-2}$ et $b \in \mathcal{N}_{n-2}$.
- (4) $a \in \mathcal{N}_{n-1} \setminus \mathcal{N}_{n-2}$ et $b \in \mathcal{N}_{n-1} \setminus \mathcal{N}_{n-2}$.

Nous en verrons des preuves des cas (1) et (2), les deux autres étant largement semblables.

Le cas (1): Ce cas est vite réglé, car

$$a\tau_n b\tau_n = a\tau_n^2 b = \tau_n a\tau_n b.$$

Le cas (2): Cette fois $b = b'\tau_{n-1}b''$, où $b', b'' \in \mathcal{N}_{n-2}$. Alors

$$\begin{aligned} \text{Tr}(a\tau_n b\tau_n) &= \text{Tr}(a\tau_n b'\tau_{n-1}b''\tau_n) \\ &= \text{Tr}(ab'\tau_n\tau_{n-1}\tau_n b'') \\ &= \text{Tr}(ab'\tau_{n-1}\tau_n\tau_{n-1}b'') \\ &= z \cdot \text{Tr}(ab'\tau_{n-1}^2 b'') \\ &= z \cdot ((q-1) \cdot \text{Tr}(ab'\tau_{n-1}b'') + q \cdot \text{Tr}(ab'b'')) \\ &= (z^2(q-1) + zq) \cdot \text{Tr}(ab'b''), \end{aligned}$$

et

$$\begin{aligned} \text{Tr}(\tau_n a\tau_n b) &= \text{Tr}(\tau_n a\tau_n b'\tau_{n-1}b'') \\ &= \text{Tr}(\tau_n^2 ab'\tau_{n-1}b'') \\ &= (q-1) \cdot \text{Tr}(\tau_n ab'\tau_{n-1}b'') + q \cdot \text{Tr}(ab'\tau_{n-1}b'') \\ &= (q-1)z \cdot \text{Tr}(ab'\tau_{n-1}b'') + q \cdot \text{Tr}(ab'\tau_{n-1}b'') \\ &= ((q-1)z^2 + qz) \cdot \text{Tr}(ab'b''). \end{aligned}$$

Nous obtenons donc l'égalité voulue. \square