REPRÉSENTATION DE STEINBERG ET IDENTITÉS DE PROJECTEURS

par

François Sauvageot

1. Introduction

En 1996, dans son travail de thèse Imin Chen [**2**] montre une isogénie entre les jacobiennes de deux courbes modulaires. Pour cela il démontre une identité de traces pour les opérateurs de Hecke opérant dans les espaces de formes modulaires paraboliques de poids 2. Il en déduit, grâce à la correspondance d'Eichler-Shimura une égalité de fonctions L locales, puis, grâce au théorème de Faltings, une isogénie entre les courbes $X_{ns}(p)$ et $X_0(p^2)^{new}$ ainsi qu'entre les courbes $X^+_{ns}(p)$ et $X^+_0(p^2)^{new}$.

L'ingrédient principal est la formule des traces de Selberg pour $\Gamma\backslash\mathcal{H}$ où $\mathcal{H}$ est le demi-plan de Poincaré et Γ est un sous-groupe discret inclus dans $GL(2,\mathbf{Z})$ et de co-volume fini. Les sous-groupes de congruence étudiés sont $\Gamma_0(p^2)$ et $\Gamma_{ns}(p)$ (le groupe des matrices congrues modulo p à un tore non-déployé de $GL(2,\mathbf{F}_p)$.

La méthode est très compliquée et obscurcit le fait que le résultat est entièrement local. À la lecture de son papier [**3**], il semblait clair que la formulation adélique est bien mieux adaptée à la résolution de ce problème que l'approche «classique». On s'aperçoit alors qu'il n'est nul besoin de formule de traces. Autrement dit 150 des 160 pages de sa thèse, conduite sous la direction de Birch, ne servent à rien ...

Il existe maintenant des démonstrations « élémentaires » du résultat de Chen en ce sens qu'elles n'utilisent que la théorie des représentations du groupe fini $GL(2,\mathbf{F}_p)$ (citons notamment Bas Edixhoven [**7**]). Dans une prépublication [**4**], Chen a même démontré qu'une construction géométrique explicite proposée par Loïc Merel dans [**10**] fournissait l'isogénie voulue dans le cas des normalisateurs.

2. Digression adélique

Rappelons que l'on peut écrire [**1**, p. 111]

$$\Gamma\backslash\mathcal{H} \simeq G(\mathbf{Q})\backslash G(\mathbf{A})/Z_\infty K_\infty K \ .$$

où G le groupe $GL(2)$, $\mathcal{H}$ le demi-plan de Poincaré, K un sous-groupe compact ouvert de $G(\mathbf{A}_f)$ tel que $\det(K) = \mathbf{Z}^\times$ avec Γ, sous-groupe discret de G_∞ égal à $pr_{G_\infty}(G(\mathbf{Q}) \cap (G^+_\infty \times K))$.

Dans ce formalisme une forme modulaire correspond à une représentation automorphe de $G(\mathbf{A})$, les formes de poids k correspondant aux représentations $\pi = \otimes_v \pi_v$ dont la partie à l'infini π_∞ est D_k, la série discrète de G_∞ de poids k.

Si Γ est un sous-groupe de congruence modulo N, correspondant à K_N et si T_n est un opérateur de Hecke au sens classique avec n premier à N, il lui correspond une fonction h_n dans l'algèbre de Hecke de

G, de sorte que

$$\mathrm{trace}\left(f_\infty^{(k)} \otimes e_N \otimes h_n \parallel L_0^2\left(G(\mathbf{Q})\backslash G(\mathbf{A})\right)\right)$$

où $S_k(\Gamma)$ est l'espace des formes modulaires paraboliques de poids k relativement à Γ et $f_\infty^{(k)}$ est un pseudo-coefficient (ou une fonction d'Euler-Poincaré, pour $GL(2)$ cela revient au même) pour la série disrète D_k, c'est-à-dire que, pour toute représentation tempérée π_∞ de G_∞, on a

$$\mathrm{trace}\,\pi_\infty(f_\infty^{(k)}) = \begin{cases} 1 & \text{si } \pi_\infty \simeq D_k \\ 0 & \text{sinon.} \end{cases}$$

Imin Chen démontre le théorème suivant :

***Théorème* 2.1 (Chen).** — *Pour n premier à p, on a*

$$\mathrm{trace}\left(T_n \mid S_2(\Gamma_{ns}(p))\right) - \mathrm{trace}\left(T_n \mid S_2(\Gamma_0(p^2))^{new}\right) = \mathrm{trace}\left(T_n \mid S_2(\Gamma(1))\right) = 0\ ,$$

où l'exposant new indique que l'on se restreint aux formes modulaires paraboliques nouvelles au sens d'Atkin-Lehner.

Le théorème étant encore valable si on remplace les sous-groupes Γ par leurs normalisteurs Γ^+ dans $GL(2,\mathbf{Z})$.

Rappelons que la théorie d'Atkin-Lehner permet de décomposer $S_k\left(\Gamma_0(p^n)\right)$ en deux parties une nouvelle et une ancienne. Cette dernière étant engendrée par les formes modulaires $z \mapsto f(p^d z)$ pour f dans $S_k\left(\Gamma_0(p^m)\right)$, pour $0 \leq m \leq n$ et d variant entre 0 et $n-m$. En particulier, si on note w_n la trace d'un opérateur de Hecke T dans $S_k\left(\Gamma_0(p^n)\right)$ et v_n cette même trace mais dans la partie nouvelle seulement, on a

$$w_n = \sum_{m=0}^{n} v_m(n-m+1) \qquad \text{d'où} \qquad \sum w_n t^n = \frac{\sum v_n t^n}{(1-t)^2} \qquad \text{et} \qquad v_n = w_n - 2w_{n-1} + w_{n-2}$$

avec $w_m = 0$ si $m < 0$.

Avec ces remarques et le fait que $\Gamma_0(p^2)$ est conjugé (via diag(p,1)) à $\Gamma_s(p)$ on voit qu'on est ramené à montrer que la trace de $f_\infty^{(2)} \otimes f_p \otimes h_n$ dans $L_0^2(G(\mathbf{Q})\backslash G(\mathbf{A}))$ est nulle pour

$$f_p = e_{K_{ns}} - (e_{K_s} - 2e_{K_0} + e_K) - e_K = e_{K_{ns}} - e_{K_s} + 2e_{K_0} - 2e_K\ .$$

Remarque : le fait que $det(K_{ns} = \mathbf{Z}_p$ résulte du théorème de Chevalley-Warning.

Les normalisateurs de K_s et K_{ns} sont respectivement $K_s^+ = K_s \cup w_s K_s$ et $K_{ns}^+ = K_{ns} \cup w_{ns} K_{ns}$ où

$$w_s = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad w_{ns} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\ .$$

L'identité de traces démontrée par Chen s'interprète de la même façon en remplaçant f_p par f_p^+ avec

$$f_p^+ = e_{K_{ns}^+} - e_{K_s^+} + e_{K_0} - e_K\ .$$

Comme le montre Imin Chen c'est un problème local et la trace s'annule encore si on remplace le poids 2 par un poids quelconque. On montre en effet

$$\mathrm{trace}\,\pi_p(f_p) = \mathrm{trace}\,\pi_p(f_p^+) = 0$$

pour toute représentation π_p de G_p. En fait, si on note, pour f une fonction lisse à support compact sur G_p, f^K la fonction moyennée sur K, on a $\mathrm{trace}\,\pi_p(f^K) = \mathrm{vol}(K)\,\mathrm{trace}\,\pi_p(f)$ puisque la trace est invariante par conjugaison. Le résultat de Imin Chen découle immédiatement de l'observation suivante

***Théorème* 2.2**. — *Si f est soit f_p, soit F_p, alors la moyenne de f sous K est nulle, i.e.*

$$f^K = 0 \ .$$

Pour démontrer ce fait, il suffit d'étudier la réduction modulo p. On a en effet

$$\forall K_1 < H < K \quad \forall \gamma \in K \qquad e_H^K(\gamma) = [\overline{G} : \overline{H}] \frac{\operatorname{card}(\mathcal{O}_{\overline{\gamma}} \cap \overline{H})}{\operatorname{card}(\mathcal{O}_{\overline{\gamma}})}$$

et on pourrait donc conclure avec l'argument de comptage suivant :

***Lemme* 2.3**. — *Pour tout x dans $\overline{G}$:*

$$[\overline{G} : T_s] \operatorname{card}(\mathcal{O}_x \cap T_s) - 2[\overline{G} : \overline{B}] \operatorname{card}(\mathcal{O}_x \cap \overline{B}) + 2 \operatorname{card}(\mathcal{O}_x) - [\overline{G} : T_{ns}] \operatorname{card}(\mathcal{O}_x \cap T_{ns}) = 0$$

et

$$[\overline{G} : T_s] \operatorname{card}(\mathcal{O}_x \cap w_s T_s = [\overline{G} : T_{ns}] \operatorname{card}(\mathcal{O}_x \cap w_{ns} T_{ns}) \ .$$

3. Reformulation en termes d'identités de projecteurs

En fait toute la problématique est locale et on peut se placer dans l'algèbre de groupe de $GL(2, \mathbf{F}_p)$.

Soit G un groupe fini et k un anneau commutatif, on note $k[G]$ l'algèbre du groupe G et $k(G)^0 \subset k[G]$ son centre. Si A est une partie de G, on note $[A] \subset k[G]$ l'élément $\sum_{a \in A} a \in k[G]$ et $p_A = [A]/|A|$. Ce dernier est un projecteur si A est un sous-groupe de G.

On définit aussi un homomorphisme

$$\varphi : k[G] \to k(G)^0, \quad f \mapsto \sum_{g \in G} g^{-1} f g.$$

Si f et f' sont deux éléments de $k[G]$, on notera $f \equiv f'$ pour dire que $\varphi(f) = \varphi(f')$. Le fait fondamental est que, si $\operatorname{card} G$ est inversible dans k, deux idempotents p_1 et p_2 de $k[G]$ sont conjugués si et seulement si $\varphi(p_1) = \varphi(p_2)$.

On applique ces considérations au cas du groupe $G = \mathrm{GL}(2)$ sur un corps fini $\mathbf{F}$. Soit B un sous-groupe de Borel de $\mathrm{GL}(2)$, $T \subset B$ son tore déployé maximal, $U \subset B$ son radical unipotent. Soit enfin T' un tore elliptique maximal. Par abus de langage, on notera les $\mathbf{F}$-points de ces groupes algébriques par la même lettre. On notera également N et N' les normalisateurs $N_G(T)$ et $N_G(T')$ et W et W' les groupes de Weyl N/T et N'/T'.

On peut démontrer une sorte d'analogue de la formule d'intégration de Weyl pour G

$$[G] = \frac{1}{\operatorname{card} N_G(T)} \varphi([T_{\text{rég}}]) + \frac{1}{\operatorname{card} N_G(T')} \varphi([T'_{\text{rég}}]) + \frac{1}{\operatorname{card} N_G(U)} \varphi([ZU_{\text{rég}}]) + \frac{1}{\operatorname{card} G} \varphi([Z])$$

et en combinant le résultat analogue pour B (où T' n'apparaît donc plus), il vient

***Corollaire* 3.1 (Chen–Edixhoven)**. — *Si $\operatorname{card} G$ est inversible dans k, les projecteurs $p_{T'} + p_B - 2p_G$ et $p_T - p_B$ de $k[G]$ sont conjugués. En particulier les deux $\mathbf{Q}[G]$-modules*

$$\mathbf{Q}[G/T] \oplus \mathbf{Q} \oplus \mathbf{Q} \qquad \textit{et} \qquad \mathbf{Q}[G/T'] \oplus \mathbf{Q}[G/B] \oplus \mathbf{Q}[G/B]$$

ont même caractère et sont donc isomorphes.

4. Représentation de Steinberg

Sous la forme précédente, le théorème de Chen–Edixhoven est totalement général. Soit donc F un corps fini, q son cardinal et p sa caractéristique et G un groupe algébrique réductif connexe défini sur F. En général on notera r et r_s les F-rang et F-rang semi-simple des groupes algébriques définis sur F. On note 1_H la représentation triviale d'un groupe H. Enfin on fixe B un sous-groupe de Borel rationnel de G.

Soit St_G la représentation de Steinberg de $G(F)$, c'est-à-dire que, dans le groupe de Grothendieck $R(G)$ des représentations complexes de G, on a

$$St_G = \sum_{P \supset B} (-1)^{r_s(P)} Ind_P^G 1_P$$

où la somme est prise sur tous les sous-groupes paraboliques rationnels de G contenant B.

***Théorème* 4.1**. — *On a la formule*

$$St_G = \sum_T \frac{1}{|W(T)|} (-1)^{r(G)-r(T)} Ind_T^G 1_T$$

où la somme est prise sur un ensemble de représentants de classes de conjugaison de tores maximaux rationnels de G.

Cette formule peut s'interpréter comme la conjugaison de deux projecteurs dans l'algèbre de groupe de G dès que G n'a que deux classes de conjugaisons de tores rationnels comme $G = SL(2)$ ou $G = U(2)$. On retrouve en particulier des résultats pour $SL(2)$ de Kani et Rosen [**8, 9**], démontrés par des voies compliquées.

Pour la démonstration, nous aurons besoin de notations. Fixons donc B un sous-groupe de Borel rationnel de G et T un tore maximal rationnel quasi-déployé de G inclus dans B. Notons σ l'élément de Frobenius dans la groupe de Galois $Gal(\overline{F}/F)$, où $\overline{F}$ est une clôture algébrique de F.

Comme tous les tores maximaux sont conjugués dans $G(\overline{F})$, on trouve tous les tores maximaux rationnels en considérant les $g^{-1}Tg$ pour g dans $G(\overline{F})$. Un tel tore est rationnel si et seulement si $\sigma(g)g^{-1}$ normalise T. D'après le théorème de Hilbert 90, on en conclut que l'on obtient toutes les classes de conjugaison de tores maximaux rationnels en considérant les tores T_w pour w dans $W(T)$ en notant T_w un tore $g^{-1}Tg$ tel que $\sigma(g)g^{-1} = w$.

Soit maintenant L un sous-groupe de Levi rationnel d'un sous-groupe parabolique P non nécessairement rationnel de G. Lusztig a introduit un foncteur d'induction R_L^G de L à G qui n'est autre que l'induction parabolique (au sens de Harish-Chandra) lorsque P est rationnel.

Démonstration. — Nous allons appliquer des résultats établis dans [**6**] concernant l'induction de Lusztig et démontrer (ce qui est équivalent) le résultat dans le groupe de Grothendieck des représentations de G à valeurs dans $\overline{\mathbf{Q}_l}$. Pour w dans $W = W(T)$, soit T_w un tore de type w. Partons de la formule (12.13) :

$$1_G = \frac{1}{|W|} \sum_{w \in W} R_{T_w}^G 1_{T_w} \qquad \text{on obtient} \qquad St_G = \frac{1}{|W|} \sum_{w \in W} R_{T_w}^G 1_{T_w} . St_G \ .$$

Comme, d'après (12.18) et (12.10),

$$(-1)^{r(G)} R_{T_w}^G 1_{T_w} St_G = (-1)^{r(T_w)} Ind_{T_w}^G 1_{T_w} \qquad \text{et} \qquad (-1)^{r(G)}(-1)^{r(T_w)} = (-1)^{l(w)} \ ,$$

$$\text{on a} \qquad St_G = \frac{1}{|W|} \sum_{w \in W} (-1)^{l(w)} Ind_{T_w}^G 1_{T_w} \ .$$

Ce qui est bien la formule recherchée en regroupant les tores selon leur classe de conjugaison. □

5. Éléments conjugants ($G = GL(2)$)

On vient de voir que, dans le cas de $GL(2)$, les projecteurs $p_T - p_B$ et $p_{T'} + p_B - 2p_G$ sont conjugués dans $\mathbf{Q}[G]$. Le problème est donc de savoir par quoi ils le sont.

Concrètement cela revient à se poser la question de comment réaliser une isogénie entre les jacobiennes des courbes X/T et X/T', où X est la courbe modulaire $X(p)$. En fait cette dernière question est un peu moins exigeante puisqu'elle revient à chercher $p_T h p_{T'}$ avec h dans $\mathbf{Q}[G]$, inversible, tel que $(p_T - p_B)h = h(p_{T'} + p_B - 2p_G)$.

La première idée naturelle, suggérée par Loïc Mérel, est de tester si l'on peut trouver un tel h de sorte que $p_T h p_{T'} = p_T p_{T'}$. Comme il est expliqué dans [**3**], la question est donc de savoir si

$$\pi(p_T)\pi(p_{T'}) \neq 0$$

dans toute représentation irréductible π de $G(F)$ ayant des vecteurs fixes sous $T(F)$ et $T'(F)$.

Cette condition est manifestement invariante par conjugaison sur le couple (T, T') et il est donc licite de fixer pour T le tore diagonal.

L'usage est de considérer un tore elliptique $T' = T'_\varepsilon$ tel que $T'_\varepsilon(F)$ soit formé de matrices de la forme

$$t'(a,b) = \begin{pmatrix} a & \varepsilon b \\ b & a \end{pmatrix}$$

pour a et b dans F non simultanément nuls et ε un élément de F qui n'est pas un carré.

Le fait est que ces tores sont très spéciaux puisque ce sont les tores elliptiques tels que $N(T)(F) \cap T'(F)$ contient des éléments non centraux de $G(F)$ (et de même pour $N(T')(F) \cap T(F)$). Notons w un tel élément (par exemple $t'(0,1)$). Soit π une représentation irréductible de $G(F)$; on voit que $\pi(p_T)\pi(p_{T'_\varepsilon})$ est nul dès que $\pi(w)$ n'est pas l'identité.

Autrement dit, si π a un vecteur invariant sous $T(F)$ mais pas sous $N(T)(F)$, la propriété désirée est impossible. Comme de telles représentations existent, le choix «naturel» n'est donc pas le bon dans ce cas.

Lq première question qui se pose en rapport avec cette constatation est de savoir s'il existe un couple (T, T') tel que les projecteurs $p_T - p_B$ et $p_{T'} + p_B - 2p_G$ sont conjugués par un élément h de $\mathbf{Q}[G]$ satisfaisant $p_T h p_{T'} = p_T p_{T'}$.

Il résulte de la décomposition de Bruhat et de $T' \cap B = Z$ que $G(F) = T(F)U(F)T'_\varepsilon(F)$. Par conséquent les tores elliptiques sont de la forme $T' = tuT'_\varepsilon u^{-1}t^{-1}$ pour t dans $T(F)$ et u dans $U(F)$ et donc

$$p_T p_{T'} = p_T u p_{T'_\varepsilon} u^{-1} t^{-1} \ .$$

Par conséquent $\pi(p_T)\pi(p_{T'})$ est non nul si et seulement si $\pi(p_T)\pi(u)\pi(p_{T'_\varepsilon})$ est non nul. Le tore $T' = tuT'_\varepsilon u^{-1}t^{-1}$ étant fixé, il existe un élément h convenable si et seulement si pour toute représentation irréductible π de $G(F)$ ayant des vecteurs fixes non nuls sous $T(F)$ et $T'(F)$, $\pi(p_T u p_{T'_\varepsilon}) \neq 0$. La première question peut finalement se reformuler ainsi : existe-t-il un unipotent $u \in U(F)$ tel que pour toute représentation irréductible π de $G(F)$ ayant des vecteurs fixes non nuls sous $T(F)$ et $T'_\varepsilon(F)$, $\pi(p_T u p_{T'_\varepsilon}) \neq 0$.

Cette question semble ardue et nous nous contenterons de signaler que pour F le corps à 3 éléments, tout u non trivial convient (autrement dit le choix naturel est l'unique mauvais choix !). En effet $U(F)$ est formé de trois éléments, disons 1, u et u^2 et, on a

$$p_T p_{T'_\varepsilon} + p_T u p_{T'_\varepsilon} + p_T u^2 p_{T'_\varepsilon} = 3 p_T p_U p_{T'_\varepsilon} = 3 p_G \ .$$

Par conséquent dans toute représentation irréductible non triviale de $G(F)$ la somme des trois opérateurs $\pi(p_T)\pi(p_{T'_\varepsilon})$, $\pi(p_T)\pi(u)\pi(p_{T'_\varepsilon})$ et $\pi(p_T)\pi(u^2)\pi(p_{T'_\varepsilon})$ est nulle. Mais u et u^2 sont conjugués par un élément

w' de $T(F)$ qui normalise $T'_\varepsilon(F)$ et donc les deux opérateurs sont reliés par la formule

$$\pi(p_T)\pi(u^2)\pi(p_{T'_\varepsilon}) = \pi(p_T)\pi(u)\pi(p_{T'_\varepsilon})\pi(w')$$

et ils sont simultanément nuls ou non nuls. Par conséquent si $\pi(p_T)\pi(u)\pi(p_{T'_\varepsilon})$ est nul, les trois opérateurs précédents sont nuls et ceci contredit l'existence d'un conjugant. Donc $\pi(p_T)\pi(u)\pi(p_{T'_\varepsilon})$ est non nul dès que π a des vecteurs invariants sous $T(F)$ et $T'_\varepsilon(F)$.

Par des calculs sur ordinateur, nous avons vérifié qu'un tel u existe toujours pour q inférieur à 1000 ; néanmoins, tous les u non triviaux ne conviennent pas toujours.

Signalons enfin qu'on peut toujours trouver h' dans $\mathbf{Q}[U]$ tel que $p_T h p_{T'_\varepsilon} = p_T h' p_{T'_\varepsilon}$. Trouver $T' = u^{-1}T'_\varepsilon u$ répondant à la question précédente est en fait équivalent au fait de pouvoir prendre $h' = u$.

6. Passage aux normalisateurs

A-t-on une relation entre p_N et $p_{N'}$ et, si oui, que peut-on dire de $p_N p_{N'}$? I. Chen a répondu positivement a cette question en démontrant les projecteurs p_N et $p_{N'} + p_B - p_G$ sont conjugués dans $\mathbf{Q}[G]$ et que $\pi(p_N)\pi(p_{N'})$ est non nul dans toute représentation irréductible π de $G(F)$ ayant des vecteurs invariants sous $N(T)(F)$ et $N(T')(F)$.

Remarquons que le passage aux normalisateurs correspond pour les jacobiennes de courbes modulaires à se restreindre à la partie fixée par l'involution d'Atkin-Lehner et que l'on construit donc explicitement une isogénie entre les jacobiennes de X/N et de X/N' grâce à ce résultat.

Il est naturel, avec notre approche, de traduire le résultat de I. Chen et de chercher à le généraliser à des groupes généraux (au moins pour la première partie). Avec notre point de vue, son énoncé se traduit par l'identité (dans $R(G)$ avec $G = GL(2)$)

$$St_G = \sum_T (-1)^{r(G)-r(T)} Ind_{N(T)}^G 1_{N(T)}$$

où la somme est prise sur l'ensemble des (classes de conjugaisons de) tores maximaux rationnels de G.

Malheureusement ce théorème n'a aucune chance de se généraliser tel quel, comme on peut le voir dans le cas $G = GL(3)$ en évaluant le caractère de ces représentations sur un élément de la forme wt avec t elliptique régulier et w non-trivial dans le groupe de Weyl du centralisateur de t. Néanmoins nous proposons la généralisation suivante, dans le cas du groupe $GL(n)$. Pour cela nous définirons en 6.2 pour tout tore maximal rationnel T de G un caractère $\chi_{N(T)}$ déduit d'un caractère de $W(T)$.

***Théorème* 6.1**. — *Pour $G = GL(n)$ avec p strictement supérieur à n , on a*

$$St_G = \sum_T (-1)^{r(G)-r(T)} Ind_{N(T)}^G \chi_{N(T)}$$

où la somme est prise sur l'ensemble des classes de conjugaisons de tores maximaux rationnels de G.

Dans le cas de $GL(2)$ le caractère $\chi_{N(T)}$ est l'unique caractère non trivial de $N(T)$ trivial sur T et le théorème s'obtient par différence des deux formules obtenues par I. Chen.

Plaçons-nous maintenant dans le groupe $G = GL(n)$ pour un entier n quelconque supérieur ou égal à 2. Soit T le tore diagonal ; $W = W(T)$ n'est autre que $\mathfrak{S}_n$ et tout w dans W admet une décomposition unique en cycles à supports disjoints $w = \prod_{m=1}^n \prod_{k\in I_m} w_{m,k}$ où les $w_{m,k}$ sont des cycles de longueur m et où les I_m sont des ensembles éventuellement vides. Remarquons que cette décomposition revient à inclure w dans un sous-groupe de Levi rationnel minimal L_w.

Un tore maximal rationnel peut être choisi de la forme T_v pour v dans W et $W(T_v)$ s'identifie alors au centralisateur W_v de v dans W.

Si deux éléments w et v commutent, v permute entre eux les cycles $(w_{m,k})_{k\in I_m}$ pour tout m, si bien que v normalise L_w. Notons W'_w le sous-groupe de W_w formé des v fixant tous les cycles $(w_{m,k})_{m,k}$. On a une décomposition en produit semi-direct

$$W_w \simeq W'_w \rtimes S_w \ .$$

On a en fait $L_w \simeq \prod_{1\leq m\leq n} GL(m)^{I_m}$ et avec cet isomorphisme

$$W'_w \simeq \prod_{m=1}^{n} (\mathbf{Z}/m\mathbf{Z})^{I_m} \qquad \text{et} \qquad S_w \simeq \prod_{m=1}^{n} \mathfrak{S}_{I_m} \ ,$$

de sorte que W_w est isomorphe à un produit direct de produits en couronne.

En choisissant un point $x_{m,k}$ dans le support de $w_{m,k}$ pour tout (m,k) on peut relever S_w dans W : tout entier x entre 1 et n s'écrit de façon unique $w^a.x_{m,k}$ pour un couple (m,k) et a entre 0 et $m-1$ et pour $s=\prod_m s_m$ dans $\prod_m \mathfrak{S}_{I_m}$ on peut poser $s.x = w^a.x_{m,s_m(k)}$.

***Définition* 6.2**. — *Fixons une fois pour toute un caractère primitif χ de $\mathbf{Z}/n!\mathbf{Z}$. Pour tout entier naturel non nul m inférieur à n, on en déduit un caractère primitif χ_m de $\mathbf{Z}/m\mathbf{Z}$ induit par $\chi^{n!/m}$.*

Pour w dans W et v dans W_w, on écrit v sous la forme

$$v = \prod_{m=1}^{n} \left(\prod_{k\in I_m} w_{m,k}^{\alpha_{m,k}} \right) s_m$$

pour des $\alpha_{m,k}$ dans $\mathbf{Z}/m\mathbf{Z}$ et pour un relèvement fixé (mais a priori dépendant de w) de S_w dans W comme expliqué ci-dessus.

On note alors χ_w le caractère de W_w défini par

$$\chi_w(v) = \prod_{m=1}^{n} \left(\prod_{k\in I_m} \chi_m(\alpha_{m,k}) \right) \varepsilon_m(s_m)$$

où ε_m est le caractère signature sur $\mathfrak{S}_{I_m}$.

Lorsque T est un tore de type w, le caractère χ_w définit naturellement un caractère sur $N(T)$, trivial sur T, noté $\chi_{N(T)}$.

Remarquons que l'on a bien défini un caractère de W_w car on a choisi le même caractère sur chacune des composantes $\mathbf{Z}/m\mathbf{Z}$ de W_w. De plus ce caractère ne dépend pas du choix du relèvement de S_w.

Afin de comprendre la géométrie de la situation, commençons par étudier le cas élémentaire où w est de la forme $w_1 \dots w_r$ pour des m-cycles $(w_i)_{i\in\mathbf{Z}/r\mathbf{Z}}$. On écrit v sous la forme $w_1^{\alpha_1}\dots w_r^{\alpha_r}s$ pour des $(\alpha_i)_{i\in\mathbf{Z}/r\mathbf{Z}}$ dans $\mathbf{Z}/m\mathbf{Z}$ et on suppose que s est un r-cycle, i.e. s est tel que $s^{-1}w_{i+1}s = w_i$ pour tout i dans $\mathbf{Z}/r\mathbf{Z}$. Identifions T au produit $\prod_{i\in\mathbf{Z}/r\mathbf{Z}} T_i$ en le considérant comme sous-groupe de L_w. Notons enfin σ l'élément de Frobenius dans le groupe de Galois $Gal(\overline{F}/F)$, où $\overline{F}$ est une clôture algébrique de F.

***Lemme* 6.3**. — *Soit g dans $G(\overline{F})$ tel que $g^\sigma g^{-1} = v$. Soit t dans $T(\overline{F})$, l'élément $g^{-1}wtg$ est rationnel si et seulement si t appartient au σ-centralisateur T_v^σ de v dans T et alors wt s'écrit dans L_w comme un produit $wt = \prod_{i\in\mathbf{Z}/r\mathbf{Z}} \nu_i$ d'éléments dont le polynôme caractéristique est de la forme $X^n - a^{\sigma^i}$ pour a de degré r sur F.*

Réciproquement tout produit $\nu = \prod_{i\in\mathbf{Z}/r\mathbf{Z}} \nu_i$ ayant cette propriété est conjugué à un wt pour t dans T_v^σ. De plus le nombre de ses conjugués ne dépend pas de ν.

Démonstration. — Soit t dans $T(\overline{F})$, $g^{-1}wtg$ est rationnel si et seulement si wt appartient au σ-centralisateur de v. La première assertion résulte donc du fait que w est rationnel et centralise v.

On écrit wt comme produit, dans L_w, $wt = \prod_{i\in\mathbf{Z}/r\mathbf{Z}} w_i t_i$ où t_i est une matrice diagonale $(\lambda_i^k)_{1\leq k\leq n}$ et w_i une matrice de permutation correspondant à un m-cycle. On a donc $(w_i t_i)^m = \det(t_i)$. Comme $p > n$, le polynôme $X^m - \det(t_i)$ est séparable donc est le polynôme caractéristique de $w_i t_i$. La classe de conjugaison de wt est donc caractérisée par la famille des déterminants $(\det(t_i))_{i\in\mathbf{Z}/r\mathbf{Z}}$.

Soit $\alpha = \alpha_1 + \ldots + \alpha_r$ et d l'ordre de α modulo m, la condition de rationnalité précédente s'écrit

$$\forall k \in \left[1; \frac{m}{d}\right] \qquad (\lambda_1^k)^{\sigma^{rd}} = \lambda_1^k$$

et les autres λ_i^k se déduisent de cette famille par les relations

$$\forall k \in \mathbf{Z}/m\mathbf{Z} \qquad \lambda_1^{k+\alpha} = (\lambda_1^k)^{\sigma^r}$$

et

$$\forall k \in \mathbf{Z}/m\mathbf{Z} \qquad \forall i \in [2; r] \qquad \lambda_i^{k+\alpha_1+\ldots+\alpha_{i-1}} = (\lambda_1^k)^{\sigma^i} \ .$$

En conséquence $\det(t_i) = \det(t_1)^{\sigma^i}$. Lorsque t varie, $\det(t_1)$ décrit les éléments de degré r sur F (obtenus comme produit de n/m normes d'éléments de degré rm). Comme les fibres de l'application norme ont même cardinal, la dernière assertion en résulte. □

Nous en déduisons la situation générale :

***Proposition* 6.4**. — *Soit w et v dans W deux éléments qui commutent. La valeur en w du caractère de $Ind_{N(T_v)}^G \chi_{N(T_v)}$ ne dépend que de la classe de v modulo W'_w.*

Démonstration. — Pour s fixé, sa décomposition en cycles à supports disjoints et la décomposition de L_w en produit permettent d'exprimer wt comme un produit d'éléments de la forme étudiée au lemme précédent. Il en résulte que le support du caractère de $Ind_{N(T_v)}^G \chi_{N(T_v)}$ ne dépend que de la classe de v modulo W'_w et que ce caractère prend la même valeur en tout élément de son support. La proposition en découle. □

On peut donc ramener la démonstration du théorème à une étude dans W. La proposition suivante achève la démonstration.

***Proposition* 6.5**. — *Soit w dans W, non trivial, et s dans S_w, on a*

$$\sum_{v\in W'_w s} (-1)^{l(v)} \chi_v(w) = 0 \ .$$

Démonstration. — On est encore une fois dans une situation produit et on peut donc se ramener au cas du lemme précédent : w est un produit de r m-cycles, $w = w_1 \ldots w_r$ et v s'écrit $v = w_1^{\alpha_1} \ldots w_r^{\alpha_r} s$ pour des $(\alpha_k)_{1\leq k\leq r}$ dans $\mathbf{Z}/m\mathbf{Z}$ et s insuisant un r-cycle sur les cycles $(w_k)_{1\leq k\leq r}$. Puisque w est non trivial, on peut supposer m distinct de 1.

Soit V le sous-groupe de W engendré par v et w. Le cas étudié est exactement le cas où V opère transitivement sur l'ensemble $[1; n]$ des entiers entre 1 et n (avec ici $n = mr$). Remarquons que dans ce cas r est l'ordre de v dans le quotient $V/\langle w\rangle$, $v^r = w^\alpha$ avec $\alpha = \alpha_1 + \ldots + \alpha_r$ et

$$\chi_w(v) = (-1)^{r-1} \chi_m(\alpha) \ .$$

Soit maintenant $v = v_1 \ldots v_d$ la décomposition en cycles disjoints de v. Comme V opère transitivement sur $[1; n]$, la projection de w dans S_v est un cycle de longueur maximale et donc tous les v_i sont des cycles de même longueur. L'ordre de w dans le quotient $V/\langle v\rangle$ est $pgcd(m, \alpha)$ et donc $d = pgcd(m, \alpha)$ et les cycles

v_i sont de longeur n/d. Soit maintenant k un entier entre 1 et m/d, premier à m/d, tel que $k\alpha \equiv d\ [m]$, on a $w^d = w^{\alpha k} = v^{rk}$ et donc

$$\chi_v(w) = (-1)^{d-1}\chi_{n/d}(rk) = (-1)^{d-1}\chi_n(rkd) = (-1)^{d-1}\chi_{n/r}(kd) = (-1)^{d-1}\chi_m(kd)\ .$$

D'où

$$(-1)^{l(v)}\chi_v(w) = (-1)^{(n/d-1)d}(-1)^{d-1}\chi_m(kd) = (-1)^{n-1}\chi_m(kd)$$

et cette quantité ne dépend que de α. À d fixé, quand α varie k décrit exactement l'ensemble des entiers premiers à m/d et compris entre 1 et m/d et donc kd décrit exactement l'ensemble des entiers compris entre 1 et m dont le pgcd avec m est d. Ainsi, lorsque v varie, kd décrit l'ensemble des entiers entre 1 et m.

Il en résulte

$$\sum_{v\in W'_w s}(-1)^{l(v)}\chi_v(w) = (-1)^{n-1}m^{r-1}\sum_{1\le j\le m}\chi_m(j) = 0$$

et la proposition suit. □

Remarque. — Seul le cas de $GL(n)$ peut se traiter avec des arguments géométriques aussi simples ...

Références

[1] Bill Casselman

[2] Imin Chen, The jacobian of modular curves associated to Cartan subgroups, Ph. D thesis, University of Oxford, 1996

[3] Imin Chen, *The jacobian of non-split Cartan modular curves,* Proceedings of the London mathematical society (3) 77, pages 1-38, 1998

[4] Imin Chen, *On relations between jacobians of certain modular curves*, Journal of algebra (à paraître ?)

[5] Bart De Smit et Bas Edixhoven, *Sur un résultat d'Imin Chen,* Mathematical Research Letters 7, pages 147-153, 2000

[6] François Digne et Jean Michel, *Representations of finite groups of Lie type,* London Mathematical Society Student texts 21, Cambridge University Press, 1991

[7] Bas Edixhoven, *On a result of Imin Chen,* arXiv `alg-geom/9604008`, mai 1996

[8] E. Kani et M. Rosen, *Idempotent relations and factors of jacobians,* Mathematische Annalen, 284(2), pages 307-327, 1989

[9] E. Kani et M. Rosen, *Idempotent relations among arithmetical invariants attached to number fields and algebraic varieties,* Journal of number theory 46, pages 230-254, 1994

[10] Loïc Mérel, Arithmetic of elliptic curves and diophantine equations, preprint, november 1996

[11] Jean-Pierre Serre, Représentations linéaires des groupes finis, Hermann, Paris, 1978

François Sauvageot, Institut de mathématiques de Jussieu, Université Paris 7, 2 place Jussieu, 75251 Paris Cedex 5
E-mail : `sauvageo@math.jussieu.fr`