Isogénie de Chen et représentation de Steinberg

François Sauvageot

Séminaire GRFA - 6 février 2003

1 Introduction

Soit E une courbe elliptique définie sur un corps de nombres K et p un nombre premier impair. La représentation mod p de E, $\rho_{\mathrm{E},p}$, est obtenue grâce l'action du groupe de Galois absolu de K sur le groupe des points de p-torsion de E. Si la courbe E est à multiplication complexe, l'image de $\rho_{\mathrm{E},p}$ dans $\mathrm{GL}_2(\mathbf{F}_p)$ est un sous-groupe propre. Mazur et Serre ont montré que si l'image n'est pas incluse dans le normalisateur d'un sous-groupe de Cartan, i.e. si $\rho_{\mathrm{E},p}$ n'est pas une représentation diédrale, alors la réciproque est vraie sauf pour un nombre fini de nombres premiers.

Par ailleurs si H est un sous-groupe de $\mathrm{GL}_2(\mathbf{F}_p)$, il opère sur la courbe modulaire $X(p)$. Notons $X_s^+(p)$ et $X_{ns}^+(p)$ les quotients de $X(p)$ par le normalisateur d'un sous-groupe de Cartan déployé ou non déployé, respectivement. La réciproque de l'assertion précédente, dans les cas restants, revient à se demander si $X_s^+(p)$ et $X_{ns}^+(p)$ ont des points rationnels en dehors des pointes et des points CM. Lorsque p est petit, le genre de ces courbes est nul et la réciproque cherchée est donc fausse. Serre a pausé la question de savoir si néanmoins la réciproque est vraie pour $p \geq 19$.

Comme $X_s^+(p)$ est isomorphe à $X_0^+(p^2)$, les méthodes de Mazur [17] peuvent s'appliquer. L'idée est d'étudier $X_0^+(p^2)$ à travers son plongement (ou plutôt de celui de son plus grand ouvert lisse sur $\mathbf{Z}$) dans sa jacobienne $J_0^+(p^2)$ puis grâce à son image dans un quotient de $J_0^+(p^2)$ (quotient d'Eisenstein, quotient d'enroulement). En utilisant ces techniques, Momose a pu étudier des cas particuliers, notamment quand $J_0^-(p)$ est de rang nul [21, 22].

Un quotient d'enroulement est un quotient maximal pour la non-annulation de la fonction L. Ainsi, via la conjecture de Birch et Swinnerton-Dyer, il teste l'existence d'un quotient de la jacobienne (d'une variété abélienne modulaire sur $\mathbf{Q}$) de groupe de Mordell-Weil fini. Si l'on croît à cette conjecture la jacobienne $J_{ns}^+(p)$ de $X_{ns}^+(p)$ n'a pas de tel quotient fini en raison d'un lien entre $J_s^+(p)$ et $J_{ns}^+(p)$, ce qui rend la méthode de Mazur inopérante. En 1996, dans son travail de thèse (sous la direction de Birch) Imin Chen [4, 5] montre que $J_0(p) \times J_{ns}^+(p)$ et $J_s^+(p)$ sont isogènes ou, ce qui revient au même, que $J_{ns}^+(p)$ est isogène à la partie nouvelle $J_s^+(p)^{\mathrm{new}}$ de $J_s^+(p)$. 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 variétés $J_{ns}^+(p)$ et $J_0^+(p^2)^{\mathrm{new}}$ ainsi qu'entre les variétés $J_{ns}(p)$ et $J_0(p^2)^{\mathrm{new}}$.

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 $\mathrm{GL}(2,\mathbf{Z})$ 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 $\mathrm{GL}(2, \mathbf{F}_p)$.

La méthode est très compliquée et obscurcit le fait que le résultat est entièrement local. Tout en gardant cette approche, on peut simplifier les calculs par une formulation adélique, 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 : la trace de $f = \otimes_v f_v$ que l'on est amené à étudier est nulle tout simplement parce que, géométriquement, la moyenne sous K_p de f_p est nulle.

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 $\mathrm{GL}(2, \mathbf{F}_p)$ (citons notamment Edixhoven [13]). Pour obtenir le résultat, il suffit d'obtenir une relation entre idempotents de l'algèbre de groupe $\mathbf{Q}[\mathrm{G}]$ ou encore une identité de caractères, comme cela a été utilisé par Kani et Rosen [14] et étendu à un cadre plus général par De Smit et Edixhoven [10]. Dans ce langage l'existence des isogénies précédentes revient à démontrer l'identité entre caractères de représentations induites

$$\mathrm{Ind}_{\mathrm{B}}^{\mathrm{G}} 1_{\mathrm{B}} - 1_G = \mathrm{Ind}_{\mathrm{N}}^{\mathrm{G}} 1_{\mathrm{N}} - \mathrm{Ind}_{\mathrm{N}'}^{\mathrm{G}} 1_{\mathrm{N}'} = \frac{1}{2}\left(\mathrm{Ind}_{\mathrm{T}}^{\mathrm{G}} 1_{\mathrm{T}} - \mathrm{Ind}_{\mathrm{T}'}^{\mathrm{G}} 1_{\mathrm{T}'}\right)$$

où T, T', N, N' et B désignent respectivement un tore déployé maximal, un tore elliptique maximal, leurs normalisateurs dans G et un sous-groupe de Borel. Sous cette forme on voit apparaître le caractère de la représentation de Steinberg de G. La seconde identité résulte facilement de résultats de la théorie de l'induction de Deligne-Lusztig [2, Corollary 7.6.7]. De la sorte ces deux relations peuvent se démontrer dans un cadre très général, à savoir celui d'un groupe algébrique réductif connexe sur un corps algébriquement clos de caractéristique $p > 0$ muni d'une application de Frobenius F, ainsi que Bhama Srinivasan l'avait obtenu, mais par des calculs explicites, il y a plus de 30 ans [26].

En utilisant la notion d'invariant de Steinberg, définie pour un groupe fini quelconque, on peut démontrer ces deux relations dans ce cadre général grâce à trois ingrédients principaux : le théorème d'induction d'Artin, une description explicite des idempotents de l'anneau de Burnside et un résultat de théorie des caractères des groupes de Weyl. Cette démonstration a l'avantage de suggérer deux nouvelles généralisations : l'une à groupe fini quelconque (par exemple les points d'un groupe algébrique sur un anneau), l'autre à des relations dans d'autres groupes de Grothendieck. En particulier si l'on substitue le théorème d'induction de Conlon à celui d'Artin, on obtient une relation dans l'anneau de Green et on peut en déduire l'existence d'isogénies de degré premier à $|\mathrm{G}^{\mathrm{F}}|_{p'}$ (la partie première à p du cardinal de G^{F}).

Lorsque G est $\mathrm{GL}_2(\mathbf{F}_p)$, on a $|\mathrm{G}^{\mathrm{F}}|_{p'} = p^2 - 1$. De Smit et Edixhoven ont remplacé $p^2 - 1$ par $p - 1$ dans le cas des normalisateurs et ont montré que ce résultat ($p - 1$ pour les normalisateurs et $p^2 - 1$ pour les tores) est optimal.

Pour conclure, pour mener une étude plus fine, on peut chercher à réaliser explicitement l'isogénie obtenue ou, en termes de théorie des représentations, à trouver un élement conjugant dans l'algèbre de groupe. Loïc Mérel [20] a suggéré que l'isogénie est obtenue à partir des projections de $X(p)$ sur les courbes modulaires étudiées. Chen [6] a démontré que cette construction est correcte pour $X_{ns}^+(p)$ et $X_0^+(p^2)^{\mathrm{new}}$ bien qu'elle soit trivialement inopérante pour $X_{ns}(p)$ et $X_0(p^2)^{\mathrm{new}}$.

2 Digression adélique

Rappelons que l'on peut écrire [3, p. 111]

$$\Gamma\backslash\mathcal{H} \simeq \mathrm{G}(\mathbf{Q})\backslash\mathrm{G}(\mathbf{A})/\mathrm{Z}_\infty\mathrm{K}_\infty\mathrm{K}\ .$$

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

Dans ce formalisme une forme modulaire correspond à une représentation automorphe de $\mathrm{G}(\mathbf{A})$, 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 $\underline{\mathrm{K}} = \mathrm{K}\Pi_{v\nmid N}\underline{\mathrm{K}}_v$ 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

$$tr\,(T_n \mid S_k(\Gamma)) = tr\left(f_\infty^{(k)} \otimes e_{\mathrm{K}} \otimes h_n \mid L_0^2\,(\mathrm{G}(\mathbf{Q})\backslash\mathrm{G}(\mathbf{A}))\right)$$

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

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

Chen démontre le théorème suivant [4, 5] :

Théorème 1 (Chen) *Pour n premier à p, on a*

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

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 $\mathrm{GL}(2, \mathbf{Z})$.

Rappelons que la théorie d'Atkin-Lehner permet de décomposer $S_k\,(\Gamma_0(p^n))$ 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 $S_k\,(\Gamma_0(p^m))$, 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 dans $S_k\,(\Gamma_0(p^n))$ et v_n cette même trace mais dans la partie nouvelle seulement, on a

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

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 est ramené à montrer que la trace de $f_\infty^{(2)} \otimes f_p \otimes h_n$ dans $L_0^2(\mathrm{G}(\mathbf{Q})\backslash\mathrm{G}(\mathbf{A}))$ est nulle pour

$$f_p = e_{\mathrm{K}_{ns}} - (e_{\mathrm{K}_s} - 2e_{\mathrm{K}_0} + e_{\mathrm{K}}) - e_{\mathrm{K}} = e_{\mathrm{K}_{ns}} - e_{\mathrm{K}_s} + 2e_{\mathrm{K}_0} - 2e_{\mathrm{K}}$$

et

$$f_p^+ = e_{\mathrm{K}_{ns}^+} - e_{\mathrm{K}_s^+} + e_{\mathrm{K}_0} - e_{\mathrm{K}} \ .$$

Remarque 1 *Le fait que* $\det(\mathrm{K}_{ns}) = \mathbf{Z}_p$ *résulte du théorème de Chevalley-Warning.*

Comme le montre 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

$$tr\,\pi_p(f_p) = tr\,\pi_p(f_p^+) = 0$$

pour toute représentation π_p de G_p. Cet argument a été utilisé par Edixhoven [13], qui a évalué ces caractères en utilisant un calcul explicite.

On peut encore simplifier cette approche. En effet, si on note, pour f une fonction lisse à support compact sur G_p, f^{K} la fonction moyennée sur K, on a $tr\,\pi_p(f^{\mathrm{K}}) = vol(\mathrm{K})\,tr\,\pi_p(f)$ puisque la trace est invariante par conjugaison. Le résultat de Chen découle immédiatement de l'observation suivante

Proposition 1 *Si f est soit f_p, soit f_p^+, alors la moyenne de f sous K est nulle.*

Pour démontrer ce fait, il suffit d'étudier la réduction modulo p. On a en effet, en notant $\bar{\mathrm{G}} = \mathrm{GL}_2(\mathbf{F}_p)$,

$$\forall \mathrm{H} < \mathrm{K} \quad \forall \gamma \in \mathrm{K} \qquad e_{\mathrm{H}}^{\mathrm{K}}(\gamma) = [\bar{\mathrm{G}} : \bar{\mathrm{H}}] \frac{Card(\mathcal{O}_{\bar{\gamma}} \cap \bar{\mathrm{H}})}{Card(\mathcal{O}_{\bar{\gamma}})}$$

et on pourrait donc conclure avec l'argument de comptage suivant, résultant de la classification des éléments de $\mathrm{GL}_2(\mathbf{F}_p)$:

Lemme 1 *Pour tout x dans $\bar{\mathrm{G}}$:*

$$\begin{aligned} Card(\mathcal{O}_x) \quad = \quad & [\bar{\mathrm{G}} : \mathrm{B}]\, Card(\mathcal{O}_x \cap \mathrm{B}) - [\bar{\mathrm{G}} : \mathrm{N}]\, Card(\mathcal{O}_x \cap \mathrm{T}) \\ & + [\bar{\mathrm{G}} : \mathrm{N}']\, Card(\mathcal{O}_x \cap \mathrm{T}') \end{aligned}$$

et

$$[\bar{\mathrm{G}} : \mathrm{N}]\, Card\left(\mathcal{O}_x \cap (\mathrm{N} \setminus \mathrm{T})\right) = [\bar{\mathrm{G}} : \mathrm{N}']\, Card\left(\mathcal{O}_x \cap (\mathrm{N}' \setminus \mathrm{T}')\right) \ .$$

Remarque 2

1. *Le lemme précédent indique un phénomène général : l'identité sur les normalisateurs s'obtient en utilisant celle sur les tores et en la couplant avec un argument purement géométrique. Il s'agit de décrire comment une orbite rencontre différents objets.*
2. *Un lemme similaire a été dégagé par Prasad et Rajan [23]. Si deux sous-groupes H_1 et H_2 rencontrent toutes les orbites autant de fois et si π est une représentation de G, alors π^{H_1} et π^{H_2} sont isomorphes et l'isomorphisme commute avec tout endomorphisme de π commutant avec l'action de G. On peut en déduire le théorème de Sunada : si G opère isométriquement et sans point fixe sur une variété Riemannienne X alors $\mathrm{X}^{\mathrm{H}_1}$ et $\mathrm{X}^{\mathrm{H}_2}$ sont isospectrales. Ou encore, si X est une variété algébrique projective, les jacobiennes de X/H_1 et de X/H_2 sont isogènes. Si X est définie sur un corps de nombres k et si $\bar{\mathrm{X}}$ est son changement de base à la clôture séparable de k, les fonctions L associées aux groupes de cohomologie étale de $\bar{\mathrm{X}}/\mathrm{H}_1$ et $\bar{\mathrm{X}}/\mathrm{H}_2$ sont identiques. En particulier cela donne des corps de nombres non-conjugués ayant même fonction ζ.*

3. *Prasad et Rajan utilisent cette remarque pour formuler une conjecture : si deux surfaces de Riemann compactes sont isospectrales pour la métrique de Kahler de courbure constante -1, alors leurs jacobiennes sont isogènes, quitte à prendre la conjuguée complexe de l'une d'elles. Ils vérifient cette conjecture sur les variétés isospectrales construites par Vignéras.*

3 Identités de projecteurs

On peut reformuler ces résultats en termes d'identités de projecteurs. On pose $\mathrm{G} = \mathrm{GL}_2(\mathbf{F}_q)$. À tout sous-groupe H de G, on fait correspondre le projecteur $e_\mathrm{H} = \frac{1}{|\mathrm{H}|}\sum_{h\in\mathrm{H}} h$ de l'algèbre de groupe $\mathbf{Q}[\mathrm{G}]$.

Remarquons que deux idempotents e_1 et e_2 de $\mathbf{Q}[\mathrm{G}]$ sont conjugués si et seulement si leurs images, par $f \mapsto \sum_{g\in\mathrm{G}} g^{-1}fg$, dans le centre de $\mathbf{Q}[\mathrm{G}]$, sont identiques. On obtient donc

Corollaire 1 (Chen–Edixhoven) *Les projecteurs $e_{\mathrm{T}'} + e_\mathrm{B} - 2e_\mathrm{G}$ et $e_\mathrm{T} - e_\mathrm{B}$ de $\mathbf{Q}[\mathrm{G}]$ sont conjugués de même que $e_{N'} + e_\mathrm{B} - e_\mathrm{G}$ et e_N. Donc*

$$\mathbf{Q}[\mathrm{G/T}] \oplus \mathbf{Q} \oplus \mathbf{Q} \simeq \mathbf{Q}[\mathrm{G/T'}] \oplus \mathbf{Q}[\mathrm{G/B}] \oplus \mathbf{Q}[\mathrm{G/B}]$$

et

$$\mathbf{Q}[\mathrm{G/N}] \oplus \mathbf{Q} \simeq \mathbf{Q}[\mathrm{G/N'}] \oplus \mathbf{Q}[\mathrm{G/B}]$$

Cette relation entraîne l'existence de l'isogénie de Chen, en raison de résultats généraux de Kani et Rosen [14].

Soit en effet C une courbe lisse, projective et géométriquement connexe définie sur un corps K, J_C sa variété jacobienne et G un groupe fini d'automorphismes de C. Si H est un sous-groupe de G, on note e_H l'idempotent de $\mathbf{Q}[\mathrm{G}]$ associé et π_H le revêtement galoisien $C \to C/\mathrm{H}$. On a un homomorphisme canonique de $\mathbf{Q}$-algèbres de $\mathbf{Q}[\mathrm{G}]$ dans $\mathcal{A}_C = \mathbf{Q} \otimes_\mathbf{Z} \mathrm{End}_\mathrm{K}(J_C)$ envoyant e_H sur l'idempotent $\varepsilon_\mathrm{H} = \frac{1}{\deg(\pi_\mathrm{H})}\pi_\mathrm{H}^*\pi_{\mathrm{H}*}$.

Par le théorème de complète réductibilité de Poincaré, J_C est isogène à un produit $\times_{1\le i\le r} A_i^{n_i}$ où les A_i sont des variétés abéliennes K-simples, de sorte que $\mathcal{A}_C$ est isomorphe à $\prod_{1\le i\le n} M_{n_i}(S_i)$ avec $S_i = \mathbf{Q} \otimes_\mathbf{Z} \mathrm{End}_\mathrm{K}(A_i)$. Le caractère du $\mathcal{A}_C$-module $M_{n_i}(S_i)$ s'écrit $n_i\chi_i$ et alors, pour tout idempotent ε de $\mathcal{A}_C$, $\varepsilon(J_C)$ est isogène à $\times_{1\le i\le r} A_i^{m_i}$ avec $m_i = \chi_i(\varepsilon)/\dim_\mathbf{Q}(S_i)$.

Dès lors si $\sum_i e_{\mathrm{H}_i}$ et $\sum_j e_{H_j}$ ont la même évaluation sur tous les caractères de $\mathbf{Q}[\mathrm{G}]$ (par exemple s'ils sont conjugués), la même propriété est vraie pour $\sum_i \varepsilon_{\mathrm{H}_i}$ et $\sum_j \varepsilon_{H_j}$ relativement aux caractères de $\mathcal{A}_C$. Le résultat précédent implique donc une isogénie entre $\times_i J_{C/\mathrm{H}_i}$ et $\times_j J_{C/\mathrm{H}_j}$.

Si l'on part maintenant d'une identité dans $\mathbf{Q}[G] : h^{-1}e_1h = e_2$, avec e_1 et e_2 des idempotents, on en tire une identité dans $\mathcal{A}_C$ et donc une isogénie explicite entre $\varepsilon_1(J_C)$ et $\varepsilon_2(J_C)$.

4 Représentation de Steinberg

Sous la forme précédente, le théorème de Chen-Edixhoven est totalement général. Soient G un groupe algébrique réductif connexe sur un corps algébriquement clos de caractéristique $p > 0$, F une application de Frobenius sur G et

T_0 un tore maximal F-stable quasi-déployé de G. Notons (S) l'hypothèse : p ne divise pas $|\mathrm{W}|$ et G est un groupe de Chevalley (ou une forme tordue) de type A_n, B_n, C_n, D_n, F_4 ou G_2 ou encore un groupe de Suzuki ou un groupe de Ree.

On note $r(\mathrm{G})$ le F-rang de G, $\mathrm{St}_{\mathrm{G}^\mathrm{F}}$ la représentation de Steinberg de G^F, $\mathrm{W} = \mathrm{W}(\mathrm{T}_0)$ le groupe de Weyl de T_0 dans G, $\mathcal{T}$ l'ensemble des tores maximaux F-stables de G, $[\mathcal{T}/\mathrm{G}^\mathrm{F}]$ un ensemble de représentants de classes de conjugaison de $\mathcal{T}$ sous G^F et $R_{\mathbf{C}}(\mathrm{G}^\mathrm{F})$ le groupe de Grothendieck de la catégorie semi-simple des G^F-modules complexes.

On pose $\varepsilon_\mathrm{G} = (-1)^{r(\mathrm{G})}$. Dans [26, section 5], Bhama Srinivasan introduit explicitement des familles de caractères $(\psi_{\mathrm{T}^\mathrm{F}})_{\mathrm{T}\in\mathcal{T}}$ des normalisateurs $\mathrm{N}_\mathrm{G}(\mathrm{T})^\mathrm{F}$, triviaux sur T^F. À l'exception de la 2-partie, ces caractères sont les moins dégénérés possibles.

Exemple – Sur $\mathbf{Z}/m\mathbf{Z} \int \mathfrak{S}_n$, on prend un caractère d'ordre $m/(m,2)$ et sur $\mathfrak{S}_n$ on prend le caractère signature si m est impair et le caractère trivial sinon.

Théorème 2 (Srinivasan [26]) *Dans* $\mathbf{Q}\otimes_\mathbf{Z} R_\mathbf{C}(\mathrm{G}^\mathrm{F})$, *on a*

$$\mathrm{St}_{\mathrm{G}^\mathrm{F}} = \sum_{\mathrm{T}\in[\mathcal{T}/\mathrm{G}^\mathrm{F}]} \frac{\varepsilon_\mathrm{G}\varepsilon_\mathrm{T}}{|\mathrm{W}(\mathrm{T})^\mathrm{F}|}\mathrm{Ind}_{\mathrm{T}^\mathrm{F}}^{\mathrm{G}^\mathrm{F}} 1_{\mathrm{T}^\mathrm{F}} = \frac{1}{|\mathrm{G}^\mathrm{F}|}\sum_{\mathrm{T}\in\mathcal{T}} \varepsilon_\mathrm{G}\varepsilon_\mathrm{T}|\mathrm{T}^\mathrm{F}|\mathrm{Ind}_{\mathrm{T}^\mathrm{F}}^{\mathrm{G}^\mathrm{F}} 1_{\mathrm{T}^\mathrm{F}} .$$

Si on se place dans l'hypothèse (S), *alors on a de plus*

$$\mathrm{St}_{\mathrm{G}^\mathrm{F}} = \sum_{\mathrm{T}\in[\mathcal{T}/\mathrm{G}^\mathrm{F}]} \varepsilon_\mathrm{G}\varepsilon_\mathrm{T}\mathrm{Ind}_{\mathrm{N}_\mathrm{G}(\mathrm{T})^\mathrm{F}}^{\mathrm{G}^\mathrm{F}}\psi_{\mathrm{T}^\mathrm{F}} = \frac{1}{|\mathrm{G}^\mathrm{F}|}\sum_{\mathrm{T}\in\mathcal{T}} \varepsilon_\mathrm{G}\varepsilon_\mathrm{T}|\mathrm{N}_\mathrm{G}(\mathrm{T})^\mathrm{F}|\mathrm{Ind}_{\mathrm{N}_\mathrm{G}(\mathrm{T})^\mathrm{F}}^{\mathrm{G}^\mathrm{F}}\psi_{\mathrm{T}^\mathrm{F}} .$$

Une démonstration de l'identité pour les tores, utilisant la théorie de Deligne-Lusztig, est donnée par Carter [2, Corollary 7.6.7]. On se place dans le groupe de Grothendieck des représentations de G à valeurs dans $\overline{\mathbf{Q}_l}$. Pour w dans W, soit T_w un tore de type w (i.e. $\mathrm{T}_w = g^{-1}\mathrm{T}_0 g$ avec $\sigma(g)g^{-1} = w$) et $R_{\mathrm{T}_w}^\mathrm{G}$ le foncteur d'induction de Lusztig de T_w à G. Partons de la formule [11, (12.13)] :

$$1_\mathrm{G} = \frac{1}{|\mathrm{W}|}\sum_{w\in\mathrm{W}} R_{\mathrm{T}_w}^\mathrm{G} 1_{\mathrm{T}_w} \qquad \text{on obtient} \qquad \mathrm{St}_{\mathrm{G}^\mathrm{F}} = \frac{1}{|\mathrm{W}|}\sum_{w\in\mathrm{W}} R_{\mathrm{T}_w}^\mathrm{G} 1_{\mathrm{T}_w}.\mathrm{St}_{\mathrm{G}^\mathrm{F}} .$$

La formule recherchée résulte de [11, (12.18)]

$$\varepsilon_\mathrm{G} R_{\mathrm{T}_w}^\mathrm{G} 1_{\mathrm{T}_w}\mathrm{St}_{\mathrm{G}^\mathrm{F}} = \varepsilon_{\mathrm{T}_w}\mathrm{Ind}_{\mathrm{T}_w}^\mathrm{G} 1_{\mathrm{T}_w}$$

en regroupant les tores selon leur classe de conjugaison.

Remarque 3

1. *On peut faire un choix de caractères moins dégénérés que ceux de Srinivasan et garder le résultat. Dans l'exemple précédent ceci consiste à prendre un caractère primitif mod m et le caractère signature.*
2. *Il serait intéressant de comprendre les caractères précédents et ceux introduits par Srinivasan dans le cadre de la théorie de Deligne-Lusztig.*
3. *Les isomorphismes du corollaire 1 sont donc valides dès que* G^F *n'a que deux classes de conjugaison de tores maximaux rationnels* F*-stables. Par contre la propriété de conjugaison des projecteurs résulte des propriétés* $\mathrm{T}\subset\mathrm{B}$ *et* $\mathrm{T}'\mathrm{B} = \mathrm{G}$ *et cette dernière est spécifique à* GL_2.

5 Extension à l'anneau de Green

On note $B(\mathrm{G}^\mathrm{F})$ l'anneau de Burnside de G^F, i.e. le groupe de Grothendieck de la catégorie des G^F-ensembles pour les relations données par l'union disjointe, la multiplication étant induite par le produit direct. Une conséquence du théorème fondamental de Burnside (caractérisant les G-ensembles isomorphes par le cardinal de leurs points fixes sous les sous-groupes de G) est l'isomorphisme

$$\mathbf{Q} \otimes_\mathbf{Z} B(\mathrm{G}^\mathrm{F}) \simeq \prod_{H \in [s_{\mathrm{G}^\mathrm{F}}]} \mathbf{Q}$$

où $[s_{\mathrm{G}^\mathrm{F}}]$ désigne un ensemble de représentants des sous-groupes de G^F à conjugaison près. On construit ainsi, pour tout sous-groupe H de G^F, un idempotent $e_\mathrm{H}^{\mathrm{G}^\mathrm{F}}$ de $\mathbf{Q} \otimes_\mathbf{Z} B(\mathrm{G}^\mathrm{F})$ associé au G^F-ensemble $\mathrm{G}^\mathrm{F}/\mathrm{H}$. Cet idempotent peut se calculer explicitement. Pour cela on introduit μ la fonction de Möbius de l'ensemble partiellement ordonné (poset) des sous-groupes de G^F (la somme sur H, sous-groupe de G^F contenant K, de $\mu(\mathrm{K},\mathrm{H})$ vaut $[\mathrm{G}^\mathrm{F} : \mathrm{K}]$ si $\mathrm{K} = \mathrm{G}^\mathrm{F}$ et 0 sinon). Gluck [1, Theorem 3.3.2] donne une description explicite des idempotents $e_\mathrm{H}^{\mathrm{G}^\mathrm{F}}$:

$$e_\mathrm{H}^{\mathrm{G}^\mathrm{F}} = \sum_{\mathrm{K} \subset \mathrm{H}} \frac{|\mathrm{K}|}{|\mathrm{N}_{\mathrm{G}^\mathrm{F}}(\mathrm{H})|} \mu(\mathrm{K},\mathrm{H}) \, \mathrm{Ind}_\mathrm{K}^{\mathrm{G}^\mathrm{F}} 1_\mathrm{K}$$

Soit X un poset muni d'une action de G^F par conjugaison. Par exemple $\mathrm{X} = s_p(\mathrm{G}^\mathrm{F})$ l'ensemble des p-sous-groupes non triviaux de G^F. Pour n entier naturel on note $C_n(\mathrm{X},\mathbf{Z})$ le $\mathbf{Z}$-module libre engendré par les éléments de $C_n(\mathrm{X})$, i.e. les chaînes strictement croissantes de $n+1$ éléments de X. On pose $C_{-1}(\mathrm{X},\mathbf{Z}) = \mathbf{Z}$ et on obtient un complexe $C_*(\mathrm{X},\mathbf{Z})$ (la différentielle d'une chaîne est la somme alternée des chaînes obtenues en éliminant un élément de la chaîne de départ). L'invariant de Lefschetz (réduit) est l'élément de $B(\mathrm{G}^\mathrm{F})$ défini par

$$\Lambda_\mathrm{X} = \sum_{n \in \mathbf{N}} (-1)^n C_n(\mathrm{X}) - \mathrm{G}^\mathrm{F}/\mathrm{G}^\mathrm{F}$$

et on appelle caractéristique d'Euler-Poincaré réduite l'entier relatif

$$\widetilde{\chi}(\mathrm{X}) = |\Lambda_\mathrm{X}| = \sum_{n \geq -1} (-1)^n \mathrm{rang}_\mathbf{Z} C_n(\mathrm{X},\mathbf{Z}) \; .$$

Par définition l'invariant de Steinberg $\mathrm{St}_p(\mathrm{G}^\mathrm{F})$ de G^F en p est l'invariant de Lefschetz réduit de $s_p(\mathrm{G}^\mathrm{F})$. Au signe près le caractère de permutation virtuel attaché à $\mathrm{St}_p(\mathrm{G}^\mathrm{F})$ est le caractère de Steinberg de G^F mais $\mathrm{St}_p(\mathrm{G}^\mathrm{F})$ est défini pour tout groupe fini.

Soit $\mathcal{O}$ un anneau commutatif local noethérien complet de caractéristique résiduelle ℓ première à $|\mathrm{G}^\mathrm{F}|_{p'}$ et $A_\mathcal{O}(\mathrm{G}^\mathrm{F})$ l'anneau de Green de G^F sur $\mathcal{O}$, i.e. le groupe de Grothendieck de la catégorie des $\mathcal{O}\mathrm{G}^\mathrm{F}$-réseaux ($\mathcal{O}\mathrm{G}^\mathrm{F}$-modules de type fini et $\mathcal{O}$-libres), pour les relations données par les décompositions en sommes directes.

Théorème 3 *L'image de* $\mathrm{St}_p(\mathrm{G}^\mathrm{F})$ *dans* $\mathbf{Q} \otimes_\mathbf{Z} A_\mathcal{O}(\mathrm{G}^\mathrm{F})$ *est*

$$\frac{1}{|\mathrm{G}^\mathrm{F}|} \sum_{\mathrm{T} \in \mathcal{T}} \varepsilon_\mathrm{G} \varepsilon_\mathrm{T} |\mathrm{T}^\mathrm{F}| \mathrm{Ind}_{\mathrm{T}^\mathrm{F}}^{\mathrm{G}^\mathrm{F}} 1_{\mathrm{T}^\mathrm{F}} = \sum_{\mathrm{T} \in [\mathcal{T}/\mathrm{G}^\mathrm{F}]} \varepsilon_\mathrm{G} \varepsilon_\mathrm{T} \frac{1}{|\mathrm{W}(\mathrm{T})^\mathrm{F}|} \mathrm{Ind}_{\mathrm{T}^\mathrm{F}}^{\mathrm{G}^\mathrm{F}} 1_{\mathrm{T}^\mathrm{F}} \; .$$

Si X est un G^{F}-ensemble, par définition des idempotents $e_{\mathrm{H}}^{\mathrm{G}^{\mathrm{F}}}$, on a l'identité

$$\mathrm{X} = \sum_{\mathrm{H}\in[s_{\mathrm{G}^{\mathrm{F}}}]} \left|\mathrm{X}^{\mathrm{H}}\right| e_{\mathrm{H}}^{\mathrm{G}^{\mathrm{F}}}$$

dans $\mathbf{Q}\otimes_{\mathbf{Z}} B(\mathrm{G}^{\mathrm{F}})$. Par conséquent

$$\mathrm{St}_p(\mathrm{G}^{\mathrm{F}}) = \sum_{\mathrm{H}\in[s_{\mathrm{G}^{\mathrm{F}}}]} \widetilde{\chi}\left(s_p(\mathrm{G}^{\mathrm{F}})^{\mathrm{H}}\right) e_{\mathrm{H}}^{\mathrm{G}^{\mathrm{F}}}$$

Pour P dand $s_p(\mathrm{G}^{\mathrm{F}})$, on pose $\mathrm{K} = \mathrm{N}_{\mathrm{G}^{\mathrm{F}}}(\mathrm{P})/\mathrm{P}$. D'après [1, Lemma 4.3.7], $\mathrm{St}_p(\mathrm{G}^{\mathrm{F}})^{\mathrm{P}}$ est nul dans $B(\mathrm{K})$. En effet, si

$$\begin{array}{ccccccccc} f & : & [\mathrm{P},.[_{s_p(\mathrm{G}^{\mathrm{F}})} & \hookrightarrow & s_p(\mathrm{G}^{\mathrm{F}})^{\mathrm{P}} & \text{et} & g & : & s_p(\mathrm{G}^{\mathrm{F}})^{\mathrm{P}} & \to & [\mathrm{P},.[_{s_p(\mathrm{G}^{\mathrm{F}})} \\ & & \mathrm{H} & \mapsto & \mathrm{H} & & & & \mathrm{H} & \mapsto & \mathrm{HP} \end{array},$$

on a $g\circ f = Id_{[\mathrm{P},.[_{s_p(\mathrm{G}^{\mathrm{F}})}}$ et $f\circ g \geq Id_{s_p(\mathrm{G}^{\mathrm{F}})^{\mathrm{P}}}$, de sorte que, par équivalence d'homotopie entre $C_*(s_p(\mathrm{G}^{\mathrm{F}})^{\mathrm{P}},\mathbf{Z})$ et $C_*([\mathrm{P},.[_{s_p(\mathrm{G}^{\mathrm{F}})},\mathbf{Z})$

$$\mathrm{St}_p(\mathrm{G}^{\mathrm{F}})^{\mathrm{P}} = \Lambda_{s_p(\mathrm{G}^{\mathrm{F}})^{\mathrm{P}}} = \Lambda_{[\mathrm{P},.[_{s_p(\mathrm{G}^{\mathrm{F}})}}$$

et ce dernier invariant est nul puisqu'un intervalle est contractile. En particulier

$$0 = \mathrm{St}_p(\mathrm{G}^{\mathrm{F}})^{\mathrm{P}} = \sum_{\mathrm{H}\in[\mathrm{K}]} \widetilde{\chi}\left(\left(s_p(\mathrm{G}^{\mathrm{F}})^{\mathrm{P}}\right)^{\mathrm{H}}\right) e_{\mathrm{H}}^{\mathrm{K}} = \sum_{[\mathrm{P}\subset\mathrm{H}\subset\mathrm{N}_{\mathrm{G}^{\mathrm{F}}}(\mathrm{P})]} \widetilde{\chi}\left(s_p(\mathrm{G}^{\mathrm{F}})^{\mathrm{H}}\right) e_{\mathrm{H}/\mathrm{P}}^{\mathrm{K}}$$

et donc $\widetilde{\chi}\left(s_p(\mathrm{G}^{\mathrm{F}})^{\mathrm{H}}\right)$ est nul pour tout sous-groupe H de G^{F} admettant un p-sous-groupe normal non trivial.

D'après le théorème d'induction de Conlon [1, Theorem 3.5.5], l'image de $e_{\mathrm{H}}^{\mathrm{G}^{\mathrm{F}}}$ dans $\mathbf{Q}\otimes_{\mathbf{Z}} A_{\mathcal{O}}(\mathrm{G}^{\mathrm{F}})$ est nulle sauf si H est cyclique mod ℓ, i.e. sauf si le quotient de H par son plus grand ℓ-sous-groupe normal est cyclique.

Par conséquent, vu l'hypothèse faite sur ℓ, l'image de $\mathrm{St}_p(\mathrm{G}^{\mathrm{F}})$ dans $\mathbf{Q}\otimes_{\mathbf{Z}} A_{\mathcal{O}}(\mathrm{G}^{\mathrm{F}})$ est celle de

$$\sum_{[s_{\mathrm{G}^{\mathrm{F}}}]\ni \mathrm{H}\ p'-cyclique} \widetilde{\chi}\left(s_p(\mathrm{G}^{\mathrm{F}})^{\mathrm{H}}\right) e_{\mathrm{H}}^{\mathrm{G}^{\mathrm{F}}} = \sum_{\mathrm{H}\ p'-cyclique} \frac{|\mathrm{N}_{\mathrm{G}^{\mathrm{F}}}(\mathrm{H})|}{|\mathrm{G}^{\mathrm{F}}|} \widetilde{\chi}\left(s_p(\mathrm{G}^{\mathrm{F}})^{\mathrm{H}}\right) e_{\mathrm{H}}^{\mathrm{G}^{\mathrm{F}}}$$

ou encore, puisque $\mu(\mathrm{K},\mathrm{H}) = \mu(\mathrm{H}/\mathrm{K})$ où μ est la fonction de Möbius,

$$\sum_{\mathrm{K}\subset\mathrm{H}\subset\mathrm{G}^{\mathrm{F}}\ |\ \mathrm{H}\ p'-cyclique} \frac{|\mathrm{K}|}{|\mathrm{G}^{\mathrm{F}}|} \mu\left(\mathrm{H}/\mathrm{K}\right) \widetilde{\chi}\left(s_p(\mathrm{G}^{\mathrm{F}})^{\mathrm{H}}\right) \mathrm{Ind}_{\mathrm{K}}^{\mathrm{G}^{\mathrm{F}}} 1_{\mathrm{K}} .$$

Par ailleurs, si T est un tore maximal F-stable de G, le même raisonnement conduit à l'égalité, dans $\mathbf{Q}\otimes_{\mathbf{Z}} A_{\mathcal{O}}(\mathrm{T}^{\mathrm{F}})$,

$$\begin{aligned} 1_{\mathrm{T}^{\mathrm{F}}} &= \sum_{\mathrm{H}\in[s_{\mathrm{T}^{\mathrm{F}}}]} e_{\mathrm{H}}^{\mathrm{T}^{\mathrm{F}}} = \sum_{\mathrm{H}\in[s_{\mathrm{T}^{\mathrm{F}}}]\ |\ \mathrm{H}\ cyclique} e_{\mathrm{H}}^{\mathrm{T}^{\mathrm{F}}} \\ &= \sum_{\mathrm{K}\subset\mathrm{H}\subset\mathrm{T}^{\mathrm{F}}\ |\ \mathrm{H}\ cyclique} \frac{|\mathrm{K}|}{|\mathrm{T}^{\mathrm{F}}|} \mu\left(\mathrm{H}/\mathrm{K}\right) \mathrm{Ind}_{\mathrm{K}}^{\mathrm{T}^{\mathrm{F}}} 1_{\mathrm{K}} . \end{aligned}$$

Si maintenant H est un p'-sous-groupe cyclique de G^{F}, d'après [16, Corollary 1.12], on a

$$\begin{aligned}\sum_{\mathrm{T}\in\mathcal{T}\mid \mathrm{T}\supset\mathrm{H}} \varepsilon_{\mathrm{G}}\varepsilon_{\mathrm{T}} &= \sum_{\mathrm{T}\in\mathcal{T}\mid \mathrm{T}\subset C_{\mathrm{G}^{\mathrm{F}}}(\mathrm{H})^0} \varepsilon_{\mathrm{G}}\varepsilon_{\mathrm{T}} = \varepsilon_{\mathrm{G}}\varepsilon_{C_{\mathrm{G}^{\mathrm{F}}}(\mathrm{H})^0}|C_{\mathrm{G}^{\mathrm{F}}}(\mathrm{H})^0|_p \\ &= \varepsilon_{\mathrm{G}}\varepsilon_{C_{\mathrm{G}^{\mathrm{F}}}(\mathrm{H})^0}\widetilde{\chi}\left(s_p(C_{\mathrm{G}^{\mathrm{F}}}(\mathrm{H})^0)\right) = \widetilde{\chi}\left(s_p(\mathrm{G}^{\mathrm{F}})^{\mathrm{H}}\right)\end{aligned}$$

où $C_{\mathrm{G}^{\mathrm{F}}}(\mathrm{H})^0$ désigne la composante connexe de l'identité du centralisateur de H dans G^{F}.

Remarque 4 *1. Si on veut étudier l'image de* $\mathrm{St}_p(\mathrm{G}^{\mathrm{F}})$ *dans* $R_{\mathbf{C}}(\mathrm{G}^{\mathrm{F}})$*, on utilise le théorème d'induction d'Artin au lieu du théorème d'induction de Conlon dans la démonstration précédente, à savoir que l'image de* $e_{\mathrm{H}}^{\mathrm{G}^{\mathrm{F}}}$ *est nulle dans* $R_{\mathbf{C}}(\mathrm{G}^{\mathrm{F}})$ *sauf si* H *est cyclique. On retrouve ainsi le résultat de Srinivasan.*

2. Le résultat de Lehrer repose sur la théorie des caractères de W*. On note* V *l'espace vectoriel réel* $Y(\mathrm{T}_0)\otimes_{\mathbf{Z}}\mathbf{R}$ *où* $Y(\mathrm{T}_0)$ *désigne le groupe des cocaractères de* T_0*. On écrit l'action de l'application de Frobenius sur* V *sous la forme* $\mathrm{F} = q\mathrm{F}_0$*. On désigne par* S *l'algèbre symétrique sur* V *et par* J *l'idéal de* S *engendré par les* W*-invariants de degré positif. On peut alors écrire*

$$\sum_{\mathrm{T}\in\mathcal{T}} \varepsilon_{\mathrm{T}} = q^{2N}P_{S/J}(q^{-1};\mathrm{F}_0^{-1}\varepsilon_{\mathrm{W}})$$

où $\varepsilon_{\mathrm{W}} = \frac{1}{|\mathrm{W}|}\sum_{w\in W}\varepsilon(w)w$ *est le projecteur associé à la signature sur* W*,* N *désigne le nombre de racines positives dans* G^{F}*, et où, pour un* W*-module* $\mathbf{Z}$*-gradué* $M = \oplus_{i\in\mathbf{Z}}M_i$*, on a noté* $P_M(t;w) = \sum_{i\in\mathbf{Z}} tr(w|M_i)t^i$*. En fait* ε_{W} *est le projecteur sur la composante de degré* N *de* S/J*. Cette dernière est de dimension 1, engendrée par le produit des racines positives, et* F_0 *y opère trivialement (puisqu'il préserve l'ensemble des racines positives). On obtient donc* q^N*, i.e.* $|\mathrm{G}^{\mathrm{F}}|_p$*, pour la quantité étudiée.*

On obtient un isomorphisme de $\mathcal{O}\mathrm{G}^{\mathrm{F}}$-réseaux en regroupant les termes affectés d'un même signe dans l'identité :

$$|\mathrm{G}^{\mathrm{F}}|\mathrm{St}_p(\mathrm{G}^{\mathrm{F}}) = \sum_{\mathrm{T}\in\mathcal{T}} \varepsilon_{\mathrm{G}}\varepsilon_{\mathrm{T}}|\mathrm{T}^{\mathrm{F}}|\mathrm{Ind}_{\mathrm{T}^{\mathrm{F}}}^{\mathrm{G}^{\mathrm{F}}}1_{\mathrm{T}^{\mathrm{F}}} .$$

Par ailleurs, on peut remplacer $\mathcal{O}$ par $\mathbf{Z}_{(\ell)}$ pour ℓ premier à $|\mathrm{G}^{\mathrm{F}}|_{p'}$, d'après [7, Proposition 30.17]. Lorsque G est GL(2), ce théorème est l'un des résultats de Bart De Smit et Bas Edixhoven [10]. Dans le cas des groupes SL(2) ou PSL(2), on affine les résultats de Ernst Kani et Michael Rosen [14].

On obtient également une identité similaire pour les normalisateurs :

Théorème 4 *Si on se place dans l'hypothèse* (S)*, l'image de* $\mathrm{St}_p(\mathrm{G}^{\mathrm{F}})$ *dans* $\mathbf{Q}\otimes_{\mathbf{Z}} A_{\mathcal{O}}(\mathrm{G}^{\mathrm{F}})$ *est égale à*

$$\sum_{\mathrm{T}\in[\mathcal{T}/\mathrm{G}^{\mathrm{F}}]} \varepsilon_{\mathrm{G}}\varepsilon_{\mathrm{T}}\mathrm{Ind}_{\mathrm{N}_{\mathrm{G}}(\mathrm{T})^{\mathrm{F}}}^{\mathrm{G}^{\mathrm{F}}}\psi_{\mathrm{T}^{\mathrm{F}}} .$$

En effet un $\mathcal{O}\mathrm{G}^{\mathrm{F}}$-module induit à partir d'un p'-sous-groupe est projectif. Par conséquent, pour démontrer que les $\mathcal{O}\mathrm{G}^{\mathrm{F}}$-modules

$$\sum_{\mathrm{T}\in\mathcal{T}} \varepsilon_{\mathrm{G}}\varepsilon_{\mathrm{T}}|\mathrm{T}^{\mathrm{F}}|\mathrm{Ind}_{\mathrm{T}^{\mathrm{F}}}^{\mathrm{G}^{\mathrm{F}}} 1_{\mathrm{T}^{\mathrm{F}}} \qquad \text{et} \qquad \sum_{\mathrm{T}\in\mathcal{T}} \varepsilon_{\mathrm{G}}\varepsilon_{\mathrm{T}}|\mathrm{N}_{\mathrm{G}}(\mathrm{T})^{\mathrm{F}}|\mathrm{Ind}_{\mathrm{N}_{\mathrm{G}}(\mathrm{T})^{\mathrm{F}}}^{\mathrm{G}^{\mathrm{F}}} \psi_{\mathrm{T}^{\mathrm{F}}}$$

sont isomorphes, il suffit de les étudier après extension des scalaires au corps des fractions de $\mathcal{O}$ d'après [7, Theorem 32.1]. L'assertion résulte donc du théorème 2.

6 Éléments conjugants dans GL(2)

Revenons au cas GL(2). On a montré que certains projecteurs sont conjugués dans $\mathbf{Q}[\mathrm{G}^{\mathrm{F}}]$. Le problème est donc de savoir par quoi ils le sont. Une réponse explicite permet également de réaliser l'isogénie entre jacobiennes déjà évoquée.

Loïc Mérel a suggéré [20] que l'isogénie provienne des deux morphismes quotients obtenus à partir de $X(p)$. En fait si h est un inversible de $\mathbf{Q}[\mathrm{G}]$ tel que $h^{-1}e_{\mathrm{N}}h = e_{\mathrm{N}'} + e_{\mathrm{B}} - e_{\mathrm{G}}$, la question de Mérel revient à demander si l'on peut choisir h de sorte que, pour toute représentation irréductible π de G (a priori distincte de la représentation de Steinberg, mais c'est en fait inutile), on a rang $\pi(e_{\mathrm{N}}he_{\mathrm{N}'}) =$ rang $\pi(e_{\mathrm{N}}e_{\mathrm{N}'})$. Il faut noter que la réponse à cette question dépend a priori des tores T et T' choisis. En effet le tore T étant fixé il existe une unique classe de T-conjugaison de tores elliptiques tels que que $\mathrm{N}\cap\mathrm{T}'$ contient des éléments non centraux de G (et de même pour $\mathrm{N}'\cap\mathrm{T}$).

Choisissons T et T' standard, de sorte que $\mathrm{N}\cap\mathrm{T}'$ contienne effectivement des éléments non centraux. Notons B le parabolique standard contenant T et U son radical unipotent. Comme $e_{\mathrm{N}}e_{\mathrm{N}'} = e_{\mathrm{T}}e_{\mathrm{T}'}$, on peut tout de suite noter que l'analogue de la question de Mérel pour les tores a une réponse négative. Néanmoins il résulte de la décomposition de Bruhat et de $\mathrm{T}'\cap\mathrm{B} = \mathrm{Z}$ que $\mathrm{G} = \mathrm{TUT}'$. Par conséquent les tores elliptiques sont de la forme $tu\mathrm{T}'u^{-1}t^{-1}$ pour t dans T et u dans U et donc on peut formuler la question ainsi : existe-t-il un unipotent $u\in\mathrm{U}$ tel que pour toute représentation irréductible π de G ayant des vecteurs fixes non nuls sous T', $\pi(e_{\mathrm{T}}ue_{\mathrm{T}'})\neq 0$.

Cette question semble ardue et je me contenterai de signaler que pour F le corps à 3 éléments, tout u non trivial convient. En effet U est formé de trois éléments, disons 1, u et u^2 et, on a

$$e_{\mathrm{T}}e_{\mathrm{T}'} + e_{\mathrm{T}}ue_{\mathrm{T}'} + e_{\mathrm{T}}u^2e_{\mathrm{T}'} = 3e_{\mathrm{G}}\ .$$

Mais u et u^2 sont conjugués par un élément w de W qui normalise T' et donc

$$\pi(e_{\mathrm{T}})\pi(u^2)\pi(e_{\mathrm{T}'}) = \pi(e_{\mathrm{T}})\pi(u)\pi(e_{\mathrm{T}'})\pi(w)$$

et ils sont simultanément nuls ou non nuls. L'assertion en découle.

Par ailleurs, par des calculs sur ordinateur, Antoine Chambert-Loir et moi-même avons vérifié qu'un tel u existe toujours pour q inférieur à 1000 ; néanmoins, tous les u non triviaux ne conviennent pas toujours.

Revenons au cas des normalisateurs. On a vu qu'une classe de conjugaison dans G rencontre $\mathrm{N}\setminus\mathrm{T}$ si et seulement si elle recontre $\mathrm{N}'\setminus\mathrm{T}$. Ceci ne veut pas dire, loin de là, que $\mathrm{N}\setminus\mathrm{T}$ et $\mathrm{N}'\setminus\mathrm{T}'$ sont conjugués : seuls leurs éléments le sont. En fait si E est une extension quadratique qui déploie T', T et T' sont conjugués sur E tandis que N et N' sont à la fois conjugués et σ-conjugués sur

E. L'effet de la σ-conjugaison (la seule pertinente pour étudier le changement de base) est d'échanger les composantes neutres et non-neutres de N et N', i.e. ce sont T et $\mathrm{N}' \setminus \mathrm{T}'$ ainsi que T' et $\mathrm{N} \setminus \mathrm{T}$ qui sont σ-conjugués. Tout ceci résulte l'égalité $H^1(\Gamma, \mathrm{N}_E) = H^1(\Gamma, \mathrm{W}) = \mathrm{W}$, qui provient du théorème de Hilbert 90.

Chen a répondu positivement à la question de Mérel, dans le cas standard, mais ses calculs semblent un peu miraculeux. Aussi les lignes qui suivent n'ont pour seul objectif que de dégager des idées « naturelles »derrière ces calculs.

Puisque $\pi(e_{\mathrm{N}} e_{\mathrm{N}'})$ est un opérateur de rang au plus 1, on peut espérer que sa trace soit non nulle dès qu'il n'est pas nul. Cette dernière propriété est équivalente à la non nullité de $\pi(e_{\mathrm{T}} e_{\mathrm{T}'} e_{\mathrm{T}})$.

Comme les tores algébriques T et T' sont conjugués sur E on peut obtenir des renseignements sur eux par des considérations de changement de base. Comme on étudie TT'T, il semble naturel d'étudier $\mathrm{T_E T'_E T_E}$ et de se demander quels sont les points qui fournissent une contribution rationnelle, i.e. chercher quand le tore $t^{-1}\mathrm{T}'t$ est défini sur F, pour t dans $\mathrm{T_E}$.

C'est le cas si et seulement si, pour σ l'élément non trivial du groupe de Galois Γ de E sur F, $t^\sigma t^{-1}$ normalise T' ; comme c'est un élément de $\mathrm{T_E}$, ce n'est possible que si T et N' ont des points communs non triviaux. On retrouve ici le caractère très particulier du cas envisagé par Chen et Mérel.

Ainsi apparaît dans l'histoire une nouvelle classe de conjugaison de tores, déployés. Explicitons-la : on a

$$w' = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

et donc on peut choisir (en prenant une racine carrée quelconque de ε)

$$t = \begin{pmatrix} 1 & 0 \\ 0 & \varepsilon^{-1/2} \end{pmatrix} .$$

Comme $\mathrm{T_E}$ et $\mathrm{T'_E}$ sont conjugués et que $t^{-1}\mathrm{T}'t$ est déployé, le plus simple pour reconnaître ce tore est de définir l'élément x qui le conjugue à T. Comme

$$g^{-1}\mathrm{T_E}g = \mathrm{T'_E} \qquad \text{pour} \qquad g = \begin{pmatrix} 1 & \varepsilon^{1/2} \\ 1 & -\varepsilon^{1/2} \end{pmatrix}$$

on a

$$x = gt = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

et $x^{-1}\mathrm{T}x$ n'est rien d'autre que le tore T" considéré par Chen.

Un calcul élémentaire montre alors l'identité dans $\mathbf{Q}[\mathrm{G^F}]$:

$$e_{\mathrm{T}} e_{\mathrm{T}'} e_{\mathrm{T}} + (e_{\mathrm{T}} x e_{\mathrm{T}})^2 = 4q e_{\mathrm{N}} + {*e_{\mathrm{B}}} + {*e_{\mathrm{G}}}$$

ce qui, par un argument de non ramification de p, montre que $\pi(e_{\mathrm{T}} e_{\mathrm{T}'} e_{\mathrm{T}})$ ne peut être nul dès que $\pi(e_{\mathrm{N}})$ ne l'est pas, pour π distincte de la représentation triviale et de la représentation de Steinberg.

Références

[1] Serge Bouc, *Burnside Rings, in* Handbook of algebra, volume 2, Elsevier, 2000

[2] Roger Carter, *Finite groups of Lie type,* Wiley-Interscience, 1985

[3] Bill Casselman, *On representations of* GL_2 *ans the arithmetic of modular curves, in* Modular functions of one variable II, Lecture Notes in Mathematics 349, Spinger-Verlag, 1973

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

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

[6] Imin Chen, *On relations between jacobians of certain modular curves*, Journal of algebra 231, pages 414-448, 2000

[7] Charles W. Curtis et Irving Reiner, *Methods of representation theory with applications to finite groups and orders,* Wiley-Interscience, 1981 et 1987

[8] Henri Darmon, *The equations* $x^n+y^n=z^2$ *and* $x^n+y^n=z^3$*,* International Mathematical Research Notices 72, pages 263-273, 1993

[9] Henri Darmon et Loïc Mérel, *Winding quotients and some variants of Fermat's Last Theorem,* Journal für die reine und angewandte Mathematik 490, pages 81-100, 1997

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

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

[12] Bas Edixhoven, *Rational torsion points on elliptic curves over number fields (after Kamienny and Mazur),* Séminaire Bourbaki n°782, mars 1994

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

[14] Ernst Kani et Michael Rosen, *Idempotent relations and factors of jacobians,* Mathematische Annalen, 284(2), pages 307-327, 1989

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

[16] Gus Lehrer, *Rational tori, semisimple orbits and the topology of hyperplane complements,* Commentarii Mathematici Helveticæ 67 (2), pages 226-251, 1992

[17] Barry Mazur, *Modular curves and the Eisenstein ideal,* Publications mathématiques de l'IHES 47, pages 33-186, 1977

[18] Barry Mazur, *Rational isogenies of prime degree,* Inventiones Mathematicæ 44, pages 129-162, 1978

[19] Loïc Mérel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres,* Inventiones Mathematicæ 124, pages 437-449, 1996

[20] Loïc Mérel, *Arithmetic of elliptic curves and diophantine equations,* Journal de théorie des nombres de Bordeaux 11, pages 173-200, 1999

[21] Fumiyuki Momose, *Rational points on the modular curves* $X_{split}(p)$*,* Compositio Mathematicæ 52, pages 115-137, 1984

[22] Fumiyuki Momose, *Rational points on the modular curves $X_0^+(N)$,* Journal of the mathematical society of Japan 39, pages 269-286, 1987

[23] Dinakar Prasad, C. S. Rajan, *On an archimedean analogue of Tate's conjecture*, Algebraic Number Theory electronic preprint archives 342, 2002, `http ://www.math.uiuc.edu/Algebraic-Number-Theory`

[24] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques,* Inventiones Mathematicæ 15, pages 259-331, 1972

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

[26] Bhama Srinivasan, *On the Steinberg character of a finite simple group of Lie type,* Journal of the Australian Mathematical Society 12, pages 1-14, 1971