Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres

Pierre Parent

▶ **To cite this version:**

Pierre Parent. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. Journal für die reine und angewandte Mathematik, 1999, 506, pp.85-116. hal-00325661

HAL Id: hal-00325661
https://hal.science/hal-00325661

Submitted on 29 Sep 2008

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres.

Pierre Parent

18 décembre 1997

Abstract

On se propose de donner une forme effective au théorème de Mazur-Kamienny-Merel sur la torsion des courbes elliptiques sur les corps de nombres. (1991 Mathematics Subject Classification : 11-G-05, 14-G-05.)

Contents

1 Présentation des résultats. **1**
1.1 Introduction. 1
1.3 Schéma de la preuve. 2

2 Quotients de courbes elliptiques. **5**

3 L'algèbre de Hecke pour Γ_1 en niveau et poids quelconques. **6**
3.1 Rappels. 7
3.3 Cas de co-niveau qu'un seul premier p divise. 8
3.3.1 Si p divise M. 9
3.3.2 Si p ne divise pas M. 10
3.4 Cas de co-niveau quelconque. 11
3.8 Finitude du quotient d'enroulement. 14

4 Espaces tangents et cotangents. **17**
4.1 Espace tangent à $J_0(N)_{/\mathbb{Z}[1/N]}$ en zéro. 17
4.8 Espace tangent au quotient de la jacobienne. 20
4.12 Preuve de la proposition "critère de Kamienny". 21

5 Lemme combinatoire. **25**
5.1 Notations et rappels. 25
5.3 Preuve de la proposition 1.9. 27

1 Présentation des résultats.

1.1 Introduction.

La "conjecture de borne uniforme pour les courbes elliptiques", affirmant qu'il existe pour tout entier d un entier $B(d)$ tel que, pour tout corps de nombres K de degré d sur $\mathbb{Q}$ et pour toute courbe elliptique E sur K, la partie de torsion $E(K)_{\text{tors}}$ du groupe de Mordell-Weil $E(K)$ est de cardinal majoré par $B(d)$, a été démontrée dans le cas général en février 1994 par Loïc Merel. En fait, Merel (et Oesterlé) montrent que, si P est un point d'ordre p premier de $E(K)$, on a $p \leq (1+3^{d/2})^2$. Des travaux de Faltings et Frey permettent alors de conclure à l'existence des bornes $B(d)$, mais pas de manière effective : en effet, si on a bien majoré les nombres premiers pouvant diviser les groupes $E(K)_{\text{tors}}$, on ne sait pas en pratique quelles puissances de ces nombres premiers peuvent intervenir dans ces groupes. Le but de cet article est de démontrer une forme explicite de la forme forte de la conjecture de borne uniforme, en donnant une borne pour ces puissances de premiers qui peuvent diviser la torsion :

Théorème 1.2 *Soit E une courbe elliptique sur un corps K de degré d sur $\mathbb{Q}$. Si $E(K)$ possède un point P d'ordre une puissance p^n d'un nombre premier p, on a :*

1. $p^n \leq 65.(3^d-1).(2d)^6$, *si p est différent de* 2 *et* 3 ;
2. *Si* $p=3$, $p^n \leq 65.(5^d-1).(2d)^6$;
3. *et pour* $p=2$, $2^n \leq 129.(3^d-1).(3d)^6$.

Le théorème de Mordell-Weil assure que pour tous K et E comme ci-dessus, il existe deux entiers n_1 et n_2 tel que $E(K)_{\text{tors}} \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$. On borne donc ainsi le cardinal de tous les p-groupes de $E(K)_{\text{tors}}$, et avec la borne de Merel-Oesterlé pour les nombres premiers p pouvant intervenir on obtient une borne effective "globale" pour l'ensemble $\{\text{card}(E(K)_{\text{tors}}) \mid K$ est un corps de nombres de degré d et E est une courbe elliptique sur $K\}$.

Une telle borne globale semble de toute façon assez facile à améliorer en reprenant les arguments de ce papier directement en niveau N entier quelconque : les seuls endroits où on utilise que la torsion est une puissance de nombre premier est le lemme 5.2, et les calculs de la proposition 5.5 ; et notre hypothèse y paraît plus pratique que cruciale. Mais on obtiendrait de toute façon une borne qui resterait exponentielle en le degré, alors qu'on conjecture qu'il en existe de polynômiales...

1.3 Schéma de la preuve.

Soit E une courbe elliptique sur un corps de nombres K de degré d sur $\mathbb{Q}$, possédant un point K-rationnel P, tel que le cardinal du sous-groupe cyclique

de $E(K)$ engendré par P soit une puissance d'un nombre premier : $|\langle P\rangle| = p^n$. On cherche à majorer p^n en fonction de d. Soit l un nombre premier différent de 2 et de p (on prendra dans la suite le plus petit possible, *i.e.* $l = 5$ si $p = 3$, $l = 3$ dans tous les autres cas). Soit $\mathcal{L}$ un idéal maximal de $\mathcal{O}_K$ (l'anneau des entiers du corps K), contenant l. Examinons la fibre en $\mathcal{L}$ du modèle de Néron (qu'on note $\mathcal{E}$) de la courbe elliptique sur $\mathcal{O}_K$.

Proposition 1.4 *Si en $\mathcal{L}$ au-dessus de l, on a l'un des quatre cas :*

1. *$\mathcal{E}$ a bonne réduction ;*
2. *$\mathcal{E}$ a réduction additive ;*
3. *$\mathcal{E}$ a réduction multiplicative tordue ;*
4. *$\mathcal{E}$ a réduction multiplicative déployée et $\langle\widetilde{P}\rangle$ (où $\widetilde{P}$ est la réduction de P mod $\mathcal{L}$) appartient à la composante neutre,*

alors $|\langle P\rangle| \leq 2.(1 + l^d)$.

Remarque. Cette proposition classique est explicitée dans [5] par exemple, ou dans [9]. Dans le cas 2., on peut borner par 4 l'ordre du groupe des composantes de la réduction additive, donc la borne pour l'ordre de P est 1 si $p \geq 5$, 3 si $p = 3$, et 4 si $p = 2$. Dans les cas 1. et 4., la borne est en fait $(l^{d/2} + 1)^2$ (borne de Weil) et $(l^d - 1)$ (cardinal de groupe multiplicatif) respectivement, donc en l^d. Le cas 3. la porte à $(1 + l^d)$ ou à $2(1 + 3^d)$: dans ce cas en effet, soit $\widetilde{P}$ appartient à la composante neutre, et son ordre est majoré par $(1 + l^d)$; soit il est dans une composante non triviale. Le groupe de Galois d'une extension quadratique du corps résiduel $k(\mathcal{L})$ agit alors par la multiplication par (± 1) sur le groupe des composantes. Mais $\widetilde{P}$ est $k(\mathcal{L})$-rationnel, et donc la composante à laquelle il appartient égale son opposée, ce qui veut dire que $2\widetilde{P}$ est dans la composante neutre (chose qui ne peut arriver que si p est 2).

Supposons donc qu'en tout $\mathcal{L}$ au-dessus de l, $\mathcal{E}$ ait réduction multiplicative déployée et que $\widetilde{P}$ ne soit pas trivial dans le groupe des composantes de cette réduction $\mathcal{E}_{k(\mathcal{L})}$ de $\mathcal{E}_{/\mathcal{O}_K}$. Pour avoir une bonne interprétation modulaire dans la suite, comme indiqué plus bas, on aimerait que $\widetilde{P}$ soit d'ordre p^n dans le groupe des composantes de $\mathcal{E}_{k(\mathcal{L})}$: d'où l'idée d'examiner le quotient de $\mathcal{E}_{k(\mathcal{L})}$ par le plus gros sous-groupe de $\langle\widetilde{P}\rangle$ inclus dans sa composante neutre $\mathcal{E}^0_{k(\mathcal{L})}$. Soit donc $n_{\mathcal{L}}$ le plus petit entier tel que $p^{n_{\mathcal{L}}}.\widetilde{P}$ tombe dans $\mathcal{E}^0_{k(\mathcal{L})}$. Soit aussi n' le plus petit des $n_{\mathcal{L}}$, pour $\mathcal{L}$ parcourant l'ensemble des places de $\mathcal{O}_K$ au-dessus de l. Oesterlé énonce le lemme suivant (en en donnant une démonstration différente de celle qui est exposée ici, à la section 2) :

Lemme 1.5 *Soit k élément de $\mathbb{N}$; si en la place $\mathcal{L}$, $p^{k-1}.P$ ne se réduit pas dans la composante neutre de $\mathcal{E}_{k(\mathcal{L})}$, alors la réduction de $\widetilde{P}$ dans la fibre en $\mathcal{L}$ du modèle de Néron $\mathcal{E}'$ de $E/\langle p^k.P\rangle$ est d'ordre exactement p^k dans son groupe des composantes.*

On sait que $p^n/p^{n'} \leq (l^d - 1)$ (puisqu'inférieur au cardinal du groupe multiplicatif $\mathbb{G}_{m,\mathbb{F}_l}$). Quitte à remplacer notre couple $(E, \langle P\rangle)$ par $(E/\langle p^{n'}.P\rangle, \langle P\rangle)$, les arguments précédents montrent donc que ce lemme permet de ramener la preuve du théorème 1.2 à celle du :

Théorème 1.6 *Soit E une courbe elliptique sur un corps de nombres K, de degré d sur $\mathbb{Q}$, et possédant un point K-rationnel P d'ordre une puissance p^n d'un nombre premier p. Soit l un nombre premier différent de p ; supposons qu'en toute place $\mathcal{L}$ au-dessus de l, le modèle de Néron de E ait réduction multiplicative déployée et que P soit d'ordre p^n dans le groupe des composantes de E. Alors,*

$$p^n < C_p^2.(s_p.d)^6,$$

où $C_p := \sqrt{65}$, $s_p := 2$ si $p \neq 2$, et $C_2 := \sqrt{129}$, $s_2 := 3$.

Exposons dans le reste de cette section comment les arguments de Mazur et Kamienny ([9], [5]) permettent de prouver le théorème 1.6.

Soit E une courbe elliptique comme dans l'énoncé précédent. Le point $K-$rationnel j de la courbe modulaire $X_0(p^n)$ que définit le couple $(E, \langle P\rangle)$ se réduit en la pointe 0 modulo toute place $\mathcal{L}$; et l'image j' de ce point par l'involution d'Atkin-Lehner, en la pointe infinie (voir [15] , page 159).

Si les σ_i, $1 \leq i \leq d$ sont les plongements de K dans $\overline{\mathbb{Q}}$, $j'^{(d)} := (\sigma_1(j'), \sigma_2(j'),$ $..., \sigma_d(j'))$ définit un point $\mathbb{Q}$-rationnel du produit symétrique d-ième : $X_0(p^n)^{(d)}$, de $X_0(p^n)$.

Définissons comme Merel le quotient d'enroulement ([19]). On considère les premiers groupes d'homologie singulière absolue : $H_1(X_0(p^n)\,;\,\mathbb{Z})$ et relative aux pointes : $H_1(X_0(p^n)$, pointes$\,;\,\mathbb{Z})$, de $X_0(p^n)$, le premier étant vu comme un sous-groupe du second. Si a et b sont deux éléments de $\mathbb{P}^1(\mathbb{Q})$, le *symbole modulaire* $\{a, b\}$ est l'élément de $H_1(X_0(p^n)$, pointes$\,;\,\mathbb{Z})$ défini par l'image de n'importe quel chemin continu reliant a à b sur le demi-plan de Poincaré auquel on a ajouté l'ensemble $\mathbb{P}^1(\mathbb{Q})$ de ses pointes. L'intégration définit un isomorphisme classique d'espaces vectoriels réels :

$$\begin{cases} H_1(X_0(p^n)\,;\,\mathbb{Z}) \otimes \mathbb{R} \to \mathrm{Hom}_{\mathbb{C}}\left(H^0(X_0(p^n)\,;\,\Omega^1),\ \mathbb{C}\right) \\ \gamma \otimes 1 \mapsto \left(\omega \mapsto \int_\gamma \omega\right). \end{cases}$$

Selon un théorème de Manin et Drinfeld, l'image réciproque de la forme linéaire $\omega \mapsto \int_{\{0,\infty\}} \omega$ dans $H_1(X_0(p^n)\,;\,\mathbb{R})$ est en réalité dans $H_1(X_0(p^n)\,;\,\mathbb{Q})$. C'est *l'élément d'enroulement*, qu'on note e (comme d'habitude). Notons (toujours comme d'habitude) $\mathbb{T}$ l'algèbre engendrée sur $\mathbb{Z}$ par les opérateurs de Hecke T_i ($i \geq 1$, entier), agissant fidèlement entre autres sur $H_1(X_0(p^n)\,;\,\mathbb{Q})$ et sur la jacobienne $J_0(p^n)$ de la courbe modulaire. Soit $\mathcal{A}_e$ l'idéal annulateur dans $\mathbb{T}$ de e (*idéal d'enroulement*) ; on définit alors le *quotient d'enroulement* J_0^e comme la variété abélienne quotient $J_0(p^n)/\mathcal{A}_e J_0(p^n)$. Un théorème de Kolyvagin-Logachev nous permet de montrer dans la section 3 le :

Théorème 1.7 *$J_0^e(\mathbb{Q})$ est fini.*

Soit maintenant l'application naturelle $f_d : X_0(p^n)^{(d)}_{\text{lisse}} \to J_0^e$, qu'on a normalisée par $\infty^{(d)} \mapsto 0$; la section $j'^{(d)}$ croise $\infty^{(d)}$ au-dessus de l, donc $f_d(j'^{(d)})_{\mathbb{F}_l} = 0_{\mathbb{F}_l}$. La finitude de $J_0^e(\mathbb{Q})$ implique alors que $f_d(j'^{(d)})_{/\mathbb{Z}} = 0_{/\mathbb{Z}} = f_d(\infty^{(d)})_{/\mathbb{Z}}$. Mais ceci montre que f_d ne peut être une immersion formelle en $\infty^{(d)}_{\mathbb{F}_l}$ (cela impliquerait en effet que $j'^{(d)}_{\mathbb{Q}}$ serait la pointe infinie) (voir la sous-section 4.12). Or on a le "critère de Kamienny" :

Théorème 1.8 *On a équivalence entre :*

1. *f_d est une immersion formelle en $\infty^{(d)}_{\mathbb{F}_l}$, et*
2. *$T_1 e, ..., T_d e$ sont $\mathbb{F}_l$-linéairement indépendants dans $\mathbb{T}e/l\mathbb{T}e$.*

De plus, ces deux conditions sont satisfaites si l'est :

3. *$T_1\{0,\infty\}, ..., T_{d.s_p}\{0,\infty\}$ sont $\mathbb{F}_l$-linéairement indépendants dans l'espace vectoriel $H_1(X_0(p^n), \text{pointes}\,; \mathbb{Z}) \otimes \mathbb{F}_l$ (où s_p désigne le plus petit nombre premier différent de p, comme en 1.6).*

(Le fait que la dernière condition implique les précédentes est une remarque d'Oesterlé en niveau premier, utilisée déjà par Merel ; ce théorème sera démontré dans la section 4). Il suffit donc maintenant de prouver :

Proposition 1.9 *Soit C_p, s_p comme dans le théorème 1.6. Supposons $d > 2$. Si $p^n \geq C_p^2.(s_p d)^6$, alors les $T_i\{0,\infty\}$, $1 \leq i \leq sd$ sont $\mathbb{F}$-linéairement indépendants (dans le $\mathbb{F}$-espace vectoriel $H_1(X_0(p^n), \text{pointes}\,; \mathbb{Z}) \otimes \mathbb{F}$) pour tout corps $\mathbb{F}$.*

Cette proposition, dont la démonstration occupe la section 5, implique en effet le théorème 1.6, et donc le théorème principal 1.2. (Pour des raisons techniques contingentes qui apparaissent dans la preuve à la section 5, on suppose $d > 2$: ce qui est sans incidence sur les théorèmes 1.6 et 1.2, puisqu'ils donnent en degré 1 et 2 des bornes supérieures (!) aux cardinaux des groupes de torsion possibles (que Mazur et Kamienny ont explicitement déterminés) pour ces degrés.)

Remarque. Notons au passage que ce qui précède permet de minorer la dimension du quotient d'enroulement en niveau p^n par $(p^n/C_p^2.s_p^6)^{\frac{1}{6}}$ (voir la preuve du théorème 1.7). Dans le cas du niveau premier p, Kowalski et Michel ont une borne linéaire en p (non publiée), et on conjecture que ceci est généralisable en tout niveau. Ce qui montre qu'il "n'y a pas d'objection" à ce que la condition 2. du théorème 1.8 soit satisfaite pour $p^n \geq \alpha.d$, i.e. que les bornes du théorème 1.2 soient en $d.l^d$ au lieu de $d^6.l^d$ ($l = 3$ ou 5). Mais encore une fois, on espère en fait des bornes polynômiales.

La preuve dans son ensemble ayant été esquissée, nous allons montrer dans la suite, dans l'ordre indiqué, les différentes propositions utilisées.

2 Quotients de courbes elliptiques.

On prouve le lemme 1.5 :

Proposition 2.1 *Soit E une courbe elliptique sur un corps de nombres K, notons $\mathcal{E}$ son modèle de Néron sur $\mathcal{O}_K$, et soit P un point K-rationnel de E, d'ordre une puissance p^n d'un nombre premier p. Soit encore k un entier, et $\mathcal{L}$ une place de $\mathcal{O}_K$ qui ne soit pas au-dessus de p. Supposons qu'en $\mathcal{L}$, $\mathcal{E}$ ait réduction multiplicative déployée, et que $p^{k-1}.P$ ne se réduise pas dans la composante neutre de $\mathcal{E}_{k(\mathcal{L})}$. Alors la réduction de P dans la fibre en $\mathcal{L}$ du modèle de Néron $\mathcal{E}'$ de $E/\langle p^k.P\rangle$ est d'ordre exactement p^k dans son groupe de composantes.*

Preuve. Pour simplifier les notations, écrivons $\mathcal{O}_K$ pour ce qui sera son localisé en $\mathcal{L}$, et F son corps résiduel (isomorphe à $k(\mathcal{L})$, donc dont la caractéristique est $l \neq p$). On a la suite exacte de schémas en groupes sur F (comme faisceaux f.p.p.f.) :

$$\mathbb{G}_{m,F} \rightarrowtail \mathcal{E}_F \twoheadrightarrow (\mathbb{Z}/N\mathbb{Z})_F.$$

Soit a l'entier positif tel que $\langle p^a.P\rangle_F = \langle p^a.\widetilde{P}\rangle = \langle \widetilde{P}\rangle \cap \mathcal{E}_F^0\,(\subseteq \langle p^k.\widetilde{P}\rangle)$, où on a noté $\mathcal{E}_F^0$ la composante neutre de la fibre spéciale du modèle de Néron de E. On a $a \geq k$, et p^a divise N. Il suffit de montrer que $\mathcal{E}_F/\langle p^k.P\rangle_F$ est un ouvert de $\mathcal{E}'_F$, car alors le lemme est évident : on peut travailler dans $\mathcal{E}_F/\langle p^k.P\rangle_F$, où il est clair par le choix de k que l'image de P est d'ordre p^k dans le groupe des composantes.

Première étape. Montrons qu'on a $\mathcal{E}_F/\langle p^k.P\rangle_F = (\mathcal{E}/\langle p^k.P\rangle)_F$. Le groupe fini $G := (\mathbb{Z}/p^{n-k}\mathbb{Z})$ agit sur $\mathcal{E}_{/\mathcal{O}_K}$ par addition de $p^k.P$. Comme $\mathcal{E}_{/\mathcal{O}_K}$ est quasi-projectif, l'orbite sous G de chaque point est contenue dans un affine. Donc on sait que tout ouvert affine $\mathrm{Spec}(A)$, stable par G, de $\mathcal{E}_{/\mathcal{O}_K}$ donne les ouverts $\mathrm{Spec}(A^G \otimes_{\mathcal{O}_K} F)$ et $\mathrm{Spec}((A\otimes_{\mathcal{O}_K} F)^G)$ de $(\mathcal{E}/\langle p^k.P\rangle)_F$ et $\mathcal{E}_F/\langle p^k.P\rangle_F$ respectivement (voir [26], III §12, [20], III §12). On a donc juste à vérifier que le morphisme canonique entre les deux anneaux ci-dessus est un isomorphisme. Il suffit pour cela de remarquer que, $|G|$ étant inversible dans A, le projecteur $A \to A^G$ qui envoie x sur $\frac{1}{|G|}\sum_G g(x)$ commute au changement de base.

Deuxième étape. Pour pouvoir déduire de la propriété universelle des modèles de Néron un prolongement à tout $\mathrm{Spec}(\mathcal{O}_K)$ du morphisme sur la fibre générique $(\mathcal{E}/\langle p^k.P\rangle)_K \to {\mathcal{E}'}_K$, on doit vérifier que le premier schéma est lisse sur $\mathrm{Spec}(\mathcal{O}_K)$. Considérons la suite exacte de schémas :

$$\langle p^k.P\rangle_{/\mathcal{O}_K} \simeq (\mathbb{Z}/p^{n-k}\mathbb{Z})_{/\mathcal{O}_K} \rightarrowtail \mathcal{E}_{/\mathcal{O}_K} \twoheadrightarrow (\mathcal{E}/\langle p^k.P\rangle)_{/\mathcal{O}_K}\ ;$$

ils sont tous ici localement de présentation finie, puisque localement de type fini sur un anneau noethérien. De plus, le premier schéma de la suite est étale sur $\mathcal{O}_K$; puisque $(\mathbb{Z}/p^{n-k}\mathbb{Z})$ agit librement sur $\mathcal{E}_{/\mathcal{O}_K}$, la seconde flèche est finie étale (voir [11], théorème A7.1.1). Étant données nos hypothèses, la lissité sur

$\mathcal{O}_K$ du dernier schéma résulte par exemple de la proposition 17.7.7 de [6].
Troisième étape. On considère donc le morphisme prolongé $(\mathcal{E}/\langle p^k.P\rangle)_{/\mathcal{O}_K} \to \mathcal{E}'_{/\mathcal{O}_K}$. Le premier schéma est clairement séparé sur la base. On peut donc appliquer la proposition 3.2 de l'exposé IX de [25] : et dire que ce morphisme est une immersion ouverte. En se restreignant à la fibre spéciale, et en se servant de la première étape, on peut bien voir comme on le voulait plus haut $\mathcal{E}_F/\langle p^k.P\rangle_F$ comme un ouvert de $\mathcal{E}'_F$. □

3 L'algèbre de Hecke pour Γ_1 en niveau et poids quelconques.

On a introduit dans le "schéma de la preuve" l'algèbre de Hecke sur $\mathbb{Z}$ pour Γ_0. On va maintenant se placer dans un cadre un peu plus général : ce qu'on notera dans cette section $\mathbb{T}_\mathbb{Z}$ ou simplement $\mathbb{T}$ désignera l'algèbre de Hecke "pour Γ_1, en niveau et poids quelconques" comme intitulé (pour plus de détails, voir la sous-section suivante). On notera $\mathbb{T}_\mathbb{Q}$ et $\mathbb{T}_\mathbb{C}$ les tensorisations de $\mathbb{T}$ avec $\mathbb{Q}$ et $\mathbb{C}$ respectivement. Le but de ce qui suit est d'expliciter matriciellement l'action de $\mathbb{T}_\mathbb{Q}$ sur l'espace des formes paraboliques de poids λ pour $\Gamma_1(N)$, où N est un entier quelconque. Pour cela, on se sert des résultats de [1] généralisés (voir par exemple [4] ; ces références seront constamment utilisées). On en déduira la forme de $\mathbb{T}_\mathbb{Q}$ comme $\mathbb{Q}$-algèbre abstraite, ce qui permettra ensuite, en se restreignant au cas de poids 2 et de caractère trivial (*i.e.*, formes modulaires sur $\Gamma_0(N)$), de prouver la finitude du quotient d'enroulement sur $\mathbb{Q}$ en niveau quelconque (théorème 3.9) - même si on n'a besoin pour le théorème 1.7 que des niveaux puissance d'un nombre premier.

3.1 Rappels.

On commence par fixer les notations : soit $f = \sum_{n\geq 1} a_n x^n$ une série formelle à coefficients dans un corps, en une variable ; soit λ et N deux entiers, et ε l'extension à $\mathbb{Z}$ d'un caractère de Dirichlet sur $(\mathbb{Z}/N\mathbb{Z})^\times$ (on pose $\varepsilon(n) = 0$ si $(n \wedge N) \neq 1$). On note t_p, U_q, B_d (p, q, premiers, d entier quelconque), les opérateurs définis formellement (voir [1]) par :

$$\begin{cases} t_p(f) = \sum_{n\geq 1}(a_{np} + \varepsilon(p)p^{\lambda-1}\, a_{n/p})x^n \ ; \\ U_q(f) = \sum_{n\geq 1} a_{np}\, x^n \ ; \\ B_d(f) = \sum_{n\geq 1} a_n x^{nd} = \sum_{n\geq 1} a_{n/d} x^n \ , \end{cases}$$

où on pose $a_{n/m} = 0$ si m ne divise pas n. On a les relations de commutation suivantes :

$$\begin{cases} B_d \circ B_{d'} = B_{d'} \circ B_d, \text{ pour tous } d, d' \text{ dans } \mathbb{N} ; \\ t_p \circ B_d = B_d \circ t_p, \text{ si } p \text{ et } d \text{ sont premiers entre eux ;} \\ t_p \circ t_{p'} = t_{p'} \circ t_p \text{ pour tous } p \text{ et } p' \text{ premiers ;} \\ t_p \circ U_q = U_q \circ t_p \text{ si } p \neq q ; \\ U_q \circ U_{q'} = U_{q'} \circ U_q , \text{ pour tous } q \text{ et } q' \text{ premiers ;} \\ U_q \circ B_d = B_d \circ U_q, \text{ si } d \text{ et } q' \text{ sont premiers entre eux.} \end{cases}$$

De plus,

$$U_q \circ B_{q^k} = B_{q^{k-1}}.$$

Considérons maintenant l'espace des formes modulaires de poids λ pour $\Gamma_1(N)$ à coefficients dans $\mathbb{Z}$, $S_\lambda(\Gamma_1(N))$, et sa tensorisation par $\mathbb{Q}$, $S_\lambda(\Gamma_1(N))\otimes_{\mathbb{Z}}\mathbb{Q}$, qu'on écrira $S_\lambda(\Gamma_1(N))_{\mathbb{Q}}$ (de même, $S_\lambda(\Gamma_1(N))_{\mathbb{C}}$). On peut définir l'algèbre de Hecke d'endomorphismes de ce $\mathbb{Q}$-espace, comme on le disait précédemment, qui est engendrée par les opérateurs T_p (p premier), et les opérateurs diamants $\langle n\rangle$ (pour les n premiers au niveau N). Un élément de $S_\lambda(\Gamma_1(N))_{\mathbb{Q}} \subset S_\lambda(\Gamma_1(N))_{\mathbb{C}}$ peut être vu comme une fonction $f(z)$ holomorphe sur le demi-plan de Poincaré, et on peut écrire son développement de Fourier en l'infini pour arriver à l'expression :

$$f(x) = \sum_{n\geq 1} a_n\, x^n \ ,$$

où $x = e^{2i\pi z}$, et les a_n sont dans $\mathbb{Q}$. L'action des opérateurs de Hecke T_p sur $S_\lambda(\Gamma_1(N))_{\mathbb{Q}}$ est alors précisément celle décrite plus haut par opérateurs t_p, si p ne divise pas N, et U_q si q divise N ; on conserve désormais cette notation "mixte" pour nous des $T_p\,, U_q$, qui est celle d'Atkin-Lehner. On rappelle alors le théorème principal de leur théorie (voir [4]) :

Théorème 3.2 (Atkin-Lehner) *L'espace $S_\lambda(\Gamma_1(N))_{\mathbb{C}}$ se décompose en une somme directe :*

$$S_\lambda(\Gamma_1(N))_{\mathbb{C}} = \bigoplus_{\varepsilon} S_\lambda(N,\varepsilon),$$

où $S_\lambda(N,\varepsilon)$ désigne l'espace propre correspondant au caractère de Dirichlet ε, et la somme est prise sur tous les tels ε vérifiant $\varepsilon(-1) = (-1)^\lambda$.

Chaque espace $S_\lambda(N,\varepsilon)_{\mathbb{C}}$ possède à son tour une base $\mathcal{B}^\varepsilon$ composée de sous-bases $\mathcal{B}^\varepsilon_f$ du type suivant :

$$\mathcal{B}^\varepsilon_f = \{f(kz),\ k|(N/M)\} = \{B_k(f),\ k|(N/M)\} \ ,$$

où f est une newform en niveau M, de caractère χ (sur $(\mathbb{Z}/M\mathbb{Z})^\times$) tel que l'extension de χ à $(\mathbb{Z}/N\mathbb{Z})^\times$ égale ε ; si C est le conducteur de ε (ou de χ), on a : $C|M|N$. Si $N = M$, alors $\mathcal{B}^\varepsilon_f$ ne comporte qu'un élément, et on l'appelle

une newclass *; sinon, $\mathcal{B}_f^\varepsilon$ est une* oldclass. *On note E_f^ε le sous $\mathbb{C}$-espace de $S_\lambda(N,\varepsilon)_\mathbb{C} \subset S_\lambda(\Gamma_1(N))_\mathbb{C}$ engendré par $\mathcal{B}_f^\varepsilon$.*

Pour p premier à M, (respectivement, q premier divisant M), f est un vecteur propre de T_p (respectivement U_q), et la valeur propre associée est le p-ième coefficient a_p de f, (qui, puisque newform, est supposée normalisée par $a_1 = 1$).

Dans le cas où ε est trivial (formes modulaires pour $\Gamma_0(N)$), si q^2 divise M, on a $U_q(f) = 0$, tandis que si q - mais pas son carré - divise M (ce qu'on note $q||M$), $U_q(f) = \pm f$.

On va donc maintenant décrire l'action de l'algèbre de Hecke $\mathbb{T}_\mathbb{C}$ sur $S_\lambda(\Gamma_1(N))_\mathbb{C}$, en écrivant cet espace comme somme de facteurs $S_\lambda(N,\varepsilon)_\mathbb{C}$, qu'on décompose à leur tour en somme des E_f^ε qui correspondent aux classes du théorème. (On en déduira à chaque fois l'action de $\mathbb{T}_\mathbb{Q}$ sur $S_\lambda(\Gamma_1(N))_\mathbb{Q}$, en le décomposant en sous-$\mathbb{Q}$-espaces $\mathcal{E}_f^\varepsilon$ dont la tensorisation avec $\mathbb{C}$ donne la somme des conjugués sous Galois des E_f^ε.) On commencera d'abord (3.3) par étudier le cas de "co-niveau" puissance de premier, c'est-à-dire le cas où, avec les notations du théorème, $(N/M) = p^k$ pour p premier - (et c'est encore une fois le seul cas dont on ait besoin dans le reste du papier). Puis on traitera le cas général en 3.4.

3.3 Cas de co-niveau qu'un seul premier p divise.

Soit donc $f \in S_\lambda(N,\varepsilon)_\mathbb{C}$, qui est une newform en niveau M, avec $N/M = p^k$. On a alors $\mathcal{B}_f = \{(f(z),\, f(pz),\, f(p^2z),\, \ldots, f(p^kz)\} = \{f, B_p(f),\, \ldots, B_{p^k}(f)\}$. Examinons l'action des différents opérateurs de Hecke sur E_f : d'après les résultats précédents, les opérateurs T_l, l ne divisant pas N, et U_q, q divisant M et différent de p, de même que les opérateurs diamants, agissent diagonalement sur E_f, puisqu'ils ont f comme vecteur propre et qu'ils commutent avec les B_{p^j}, $0 \leq j \leq k$. Puisque $\mathbb{T}_\mathbb{Z}$ opère sur $S_\lambda(\Gamma_1(N))_\mathbb{Z}$, qui est un $\mathbb{Z}$-module libre de rang fini, les valeurs propres des T_l sont des entiers algébriques. Et il existe un corps de nombre K_f contenant tous les a_p (car l'algèbre de Hecke est un $\mathbb{Z}$-module de type fini).

Remarque. Le corps de nombres engendré par les valeurs propres associées à f de $\mathbb{T}_\mathbb{Q}$ n'est pas plus grand que K_f : en effet, même s'il contient, en plus des a_n, les valeurs propres des opérateurs diamants, la relation $p^{\lambda-1}\langle p\rangle = T_p^2 - T_{p^2}$ (pour tout p premier ne divisant pas le niveau) montre que ces valeurs propres appartiennent à K_f.

En caractère trivial, les U_q sont triviaux, puisque leurs valeurs propres en f sont soit 0, soit 1, soit -1 ; dans ce cas encore, les coefficients a_n de f sont de plus totalement réels : en effet, les opérateurs de Hecke sont auto-adjoints pour le produit scalaire de Petersson :

$$\langle f, g\rangle = \int\int_{z=x+iy\,\in D} f(z)\,\overline{g(z)}\,y^{\lambda-2}\,dx\,dy\ ,$$

qui fait de $S_2(N)_{\mathbb{C}}$ un espace de Hilbert (on a désigné par D dans l'intégrale un domaine fondamental du demi-plan de Poincaré pour $\Gamma_0(N)$). (En fait, on définit un produit scalaire de Petersson pour tout $S_\lambda(\Gamma_1(N))_{\mathbb{C}}$, pour lequel les T_l sont normaux (sinon auto-adjoints), et pour lequel la décomposition en E_f^ε est orthogonale - voir la preuve de 3.7.)

Revenant au cas général, on considère maintenant l'action de U_p. Pour cela, on distingue deux cas : selon que p divise ou non M.

3.3.1 Si p divise M.

L'opérateur U_p de l'algèbre de Hecke en niveau N est le même que celui de niveau M, et donc avec le lemme plus haut,

$$\begin{cases} U_p(f) = a_p\, f, \text{ et} \\ U_p(B_{p^j}(f)) = B_{p^{j-1}}(f) \text{ si } j \geq 1\ . \end{cases}$$

Si $a_p = 0$, U_p n'a qu'un bloc de Jordan, et la restriction R_f de l'algèbre de Hecke $\mathbb{T}_{\mathbb{Q}}$ au $\mathbb{Q}$-espace $\mathcal{E}_f^\varepsilon$ qu'on a défini plus haut (correspondant sur $\mathbb{C}$ à la somme des conjugués par Galois de E_f^ε), est de forme :

$$R_f = K_f[U_p] \simeq K_f[X]/(X^{k+1}).$$

Sinon, U_p se réduit en deux blocs de Jordan, un petit correspondant à la valeur propre a_p, et un gros, correspondant à 0 ; en tant que $\mathbb{Q}$-algèbres, on a donc l'isomorphisme

$$R_f \simeq K_f \times K_f[X]/(X^k).$$

Remarque. Le fait que le corps du deuxième facteur de R_f soit bien tout K_f, malgré l'absence de la valeur propre a_p, peut se voir par un argument de dimension des espaces cotangents ; ou bien avec les résultats d'Atkin-Lehner, qui disent moralement qu'une newform est caractérisée par "tous ses coefficients de Fourier moins un nombre fini".

Application au cas de caractère trivial. Dans ce cas, si p^2 divise M, $a_p = 0$, et $R_f \simeq K_f[X]/(X^{k+1})$; la base $\mathcal{B}_f^\varepsilon$ diagonalise U_p. Si en revanche p - mais pas son carré - divise M, on a $a_p = \pm 1$, donc $R_f \simeq K_f \times K_f[X]/(X^k)$, et on voit facilement que la nouvelle base de E_f^ε :

$$\mathcal{B}'_f = \{f,\, B_p(f) - a_p f,\, B_{p^2}(f) - f,\, \dots\ ,\, B_{p^{2j}}(f) - f,\, B_{p^{2j+1}}(f) - a_p f, \dots\}$$

est de Jordan pour U_p et donc triangulise toute la restriction de l'algèbre de Hecke à E_f^ε.

3.3.2 Si p ne divise pas M.

Le fait nouveau par rapport au cas précédent est que l'algèbre de Hecke en niveau N, $\mathbb{T}_{N,\mathbb{C}}$, qu'on fait agir sur E_f^ε, n'est plus la restriction à cet espace de l'algèbre de Hecke en niveau M : le "bon" p-ième opérateur de Hecke, celui pour lequel f est un vecteur propre, est T_p, mais puisqu'on s'intéresse à $\mathbb{T}$ en niveau N, on doit considérer à la place l'opérateur U_p.

Puisque f est propre pour T_p, on a :

$$T_p(f) = \sum_{n\geq 1} (a_{np} + \varepsilon(p)\, p^{\lambda-1}\, a_{n/p})\, x^n \ = a_p\, f \ ,$$

et les coefficients de f vérifient donc pour tout n les relations :

$$a_p\, a_n = a_{np} + \varepsilon(p)\, p^{\lambda-1}\, a_{n/p}.$$

On calcule alors :

$$\begin{aligned} U_p(f) &= \sum_{n\geq 1} a_{np}\, x^n \\ &= \sum_{n\geq 1} (a_p a_n \ - \varepsilon(p)\, p^{\lambda-1}\, a_{n/p})\, x^n \\ &= a_p f - \varepsilon(p)\, p^{\lambda-1}\, B_p(f). \end{aligned}$$

Le polynôme caractéristique de la restriction de U_p à E_f^ε est donc

$$P_{U_p}(X) = (X^2 - a_p X + \varepsilon(p)\, p^{\lambda-1}).X^{k-1} \ ,$$

et les racines α_p et $\overline{\alpha}_p$ du premier facteur sont simples si ${a_p}^2 \neq 4\varepsilon(p)\, p^{\lambda-1}$, doubles (valant $\pm\sqrt{\varepsilon(p)}p^{\frac{\lambda-1}{2}}$) sinon ; dans ce deuxième cas on voit sur le rang de U_p qu'il se réduit en deux blocs de Jordan, un pour chaque valeur propre (0 et $\pm\sqrt{\varepsilon(p)}p^{\frac{\lambda-1}{2}}$).

Remarque. En caractère trivial et poids 2, ce dernier cas, (qui correspond à une valeur maximale de a_p selon la borne de Weil, qui dit que $|a_p| \leq 2\sqrt{p}$), est en fait exclu, par un théorème de Coleman et Edixhoven, en cours de publication ([3]) ; on l'explicite quand même - en attendant.

Si ${a_p}^2 \neq 4\varepsilon(p)\, p^{\lambda-1}$. Posons $K_f' = K_f[X]/(X^2 - a_p X + \varepsilon(p)\, p^{\lambda-1})$, (qui n'est pas nécéssairement un corps) ; une triangulisation de U_p montre que la restriction de $\mathbb{T}_\mathbb{Q}$ à $\mathcal{E}_f^\varepsilon$ est

$$R_f \simeq K_f' \times K_f[X]/(X^{k-1}).$$

On note (cela servira dans la suite) qu'un vecteur propre associé à la valeur propre 0 est $(B_{p^2}(f) - \frac{a_p}{\varepsilon(p)\, p^{\lambda-1}} B_p(f) + \frac{1}{\varepsilon(p)\, p^{\lambda-1}} f)$.

Si ${a_p}^2 = 4\varepsilon(p)\, p^{\lambda-1}$, on voit que la restriction de U_p à $\mathrm{Ker}(U_p^2 - a_p U_p + \varepsilon(p) p^{\lambda-1}\mathrm{Id})$ n'est pas diagonale, et qu'avec les notations précédentes,

$$R_f \simeq K_f[X]/(X^2) \times K_f[Y]/(Y^{k-1}).$$

Une base de $\mathrm{Ker}(U_p - \alpha_p \mathrm{\ Id})$ est $\{a_p f - 2\varepsilon(p)p^{\lambda-1}B_p(f)\}$, et bien sûr le même vecteur $(B_{p^2}(f) - \frac{a_p}{\varepsilon(p)\,p^{\lambda-1}}B_p(f) + \frac{1}{\varepsilon(p)\,p^{\lambda-1}}f)$ que précédemment engendre $\mathrm{Ker}(U_p)$.

3.4 Cas de co-niveau quelconque.

Soit maintenant $f \in S_\lambda(N,\varepsilon)_{\mathbb{C}}$, qui est une newform en niveau M, avec $N/M = n$ quelconque cette fois. On a alors $\mathcal{B}_f = \{B_d(f), d|n\}$. On examine à nouveau l'action des différents opérateurs de Hecke : les opérateurs T_l, l ne divisant pas N, et U_q, q ne divisant pas n, agissent toujours diagonalement sur E_f^ε, comme en co-niveau premier. Soit q un premier divisant n. Notons m la valuation en q de n : $q^m||n$. Alors, on constuit pour U_q une base qui lui est appropriée, en ordonnant partiellement la base $\mathcal{B}_f$ ainsi : pour d parcourant les diviseurs de n/q^m, on note $\mathcal{B}_f^{q,d} = \{B_d(f),\, B_{dq}(f),\, B_{dq^2}(f),\, \dots,\, B_{dq^m}(f)\}$, et on écrit

$$\mathcal{B}_f^q = \{f, B_q(f), B_{q^2}(f), \dots, B_{q^m}(f), B_d(f), B_{dq}(f), B_{dq^2}(f), \dots, B_{dq^m}(f), \dots\}$$

comme la réunion sur d de ces $\mathcal{B}_f^{q,d}$. (Il y a donc $\sigma_0(n/q^m)$ différentes bases $\mathcal{B}_f^{q,d}$ (nombre de diviseurs de n/q^m).) On déduit des relations de commutation entre les opérateurs considérés et de ce qui précède que, dans la base $\mathcal{B}_f^q$, U_q se décompose en une somme directe de $\sigma_0(n/q^m)$ copies : $B_q \oplus B_q \oplus \cdots \oplus B_q$, où chaque B_q correspond à la restriction de U_q à chaque espace engendré par un $\mathcal{B}_f^{q,d}$. (Si q divise M, alors B_q a la forme indiquée dans la sous-section 3.3.1 ; sinon, on est dans l'un des deux cas de 3.3.2.) On peut encore écrire que, si on note E_q^f le sous-espace de $S_\lambda(N,\varepsilon)_{\mathbb{C}}$ engendré par $\mathcal{B}_f^{q,1} = \{f, B_q(f),\, B_{q^2}(f),\, \dots,\, B_{q^m}(f)\}$, alors on peut considérer E_f^ε comme le produit tensoriel sur $\mathbb{C}$:

$$E_f^{q_1} \otimes E_f^{q_2} \otimes \cdots \otimes E_f^{q_m},$$

où les q_i sont les nombres premiers divisant n. Et $S_\lambda(N,\varepsilon)_{\mathbb{C}}$, à son tour, est la somme directe sur les f des tels E_f^ε.

On résume tout ça :

Théorème 3.5 *Soit N un entier naturel quelconque. L'algèbre de Hecke $\mathbb{T}_{\mathbb{Q}}$, vue comme sous-algèbre des endomorphismes de $\mathbb{Q}$-espace vectoriel de $S_\lambda(\Gamma_1(N))_{\mathbb{Q}}$, s'écrit comme un produit d'anneaux :*

$$\mathbb{T}_{\mathbb{Q}} = R_{f_1} \times R_{f_2} \times \cdots \times R_{f_k},$$

où chacun de ces R_{f_i} correspond à l'orbite sous Galois d'une newform f_i en niveau M_i divisant N, et caractère ε.

Plus précisément, le facteur R_{f_i} est la restriction de $\mathbb{T}_{\mathbb{Q}}$ au sous-espace $\mathcal{E}_{f_i}$ de $S_\lambda(\Gamma_1(N))_{\mathbb{Q}}$, qui est engendré sur $\mathbb{Q}$ par les orbites sous Galois des $B_d(f_i)$, d parcourant les diviseurs de N/M_i.

Si K_{f_i} désigne le corps de nombres engendré par les coefficients a_n du développement de Fourier de f_i à l'infini, l'idéal R_{f_i} est de forme un produit tensoriel d'anneaux des quatre types suivants :

- $K_{f_i}[X]/(X^n)$;
- $K_{f_i} \times K_{f_i}[X]/(X^n)$;
- $K_{f_i}[X]/(X^2 - a_q X + \varepsilon(q)q^{\lambda-1}) \times K_{f_i}[Y]/(Y^n)$;

ou encore :

- $K_{f_i}[X]/(X^2) \times K_{f_i}[Y]/(Y^n)$.

Notons un corollaire partiel de ce théorème qui nous servira dans la suite :

Corollaire 3.6 *Soit A une algèbre de dimension finie sur un corps K, et qui a un unique idéal minimal non trivial ; alors A est de Gorenstein, i.e. son dual en tant que K-espace vectoriel, $A^\vee$, est un A-module libre de rang 1. En particulier, l'algèbre de Hecke sur $\mathbb{Q}$ (pour Γ_1, en niveau et poids quelconques) $\mathbb{T}_\mathbb{Q}$, est de Gorenstein.*

Preuve. Soit A une algèbre comme dans l'énoncé. Son idéal minimal est par définition principal, engendré par n'importe lequel de ses éléments non nuls. Soit g l'un de ceux-là. Il existe un élément L de $A^\vee$ qui ne s'annule pas en g. On en déduit donc que le noyau de l'application linéaire :

$$\left\{ \begin{array}{ccc} A & \to & A^\vee \\ a & \mapsto & (x \mapsto L(a.x)) \end{array} \right.$$

est un idéal trivial de A, puisqu'il ne contient pas l'idéal minimal. Donc cette application est injective, et en fait bijective puisque les deux espaces A et $A^\vee$ ont même dimension.

Pour ce qui est de $\mathbb{T}_\mathbb{Q}$, le théorème précédent dit qu'elle se décompose en produits d'anneaux de la forme $K[X_1, X_2, \ldots, X_n]/(X_1^{m_1} X_2^{m_2} \ldots X_n^{m_n})$, où K est un corps de nombres (en effet, chaque A_{f_i} se décompose encore ainsi). Puisque $K[X_1, X_2, \ldots, X_n]/(X_1^{m_1} X_2^{m_2} \ldots X_n^{m_n})$ possède un seul idéal minimal, et puisque la propriété d'être de Gorenstein est clairement stable par somme directe finie, on peut appliquer la première partie de la proposition. □

Montrons aussi un réultat dont on se sert dans la sous-section suivante (et qui sera redémontré en partie en 4.7 grâce à 3.6) :

Proposition 3.7 *Pour tous niveau N et poids λ, $S_\lambda(\Gamma_1(N))_\mathbb{Q}$ est un $\mathbb{T}_\mathbb{Q}$-module libre de rang 1.*

Preuve. On a un accouplement parfait $[\ ,\ ]$, $\mathbb{C}$-bilinéaire, entre $\mathbb{T}_\mathbb{C}$ et $S_\lambda(\Gamma_1(N))_\mathbb{C}$:

$$\left\{ \begin{array}{ccc} S_\lambda(\Gamma_1(N))_\mathbb{C} \times \mathbb{T}_\mathbb{C} & \to & \mathbb{C} \\ (f = \sum_{n\geq 1} a_n q^n, T) & \mapsto & a_1(Tf)\ , \end{array} \right.$$

qui est défini sur $\mathbb{Q}$, pour lequel tout opérateur de l'algèbre de Hecke est auto-adjoint. Maintenant, notons $\langle\ ,\ \rangle_\mathrm{P}$ le produit scalaire de Petersson. Appelons

σ l'involution sur $S_\lambda(\Gamma_1(N))_\mathbb{C}$ définie par l'opération de conjugaison complexe des coefficients de Fourier en l'infini d'une forme parabolique. Rappelons aussi l'opérateur (classique) W_N, dont l'opération sur $S_\lambda(\Gamma_1(N))_\mathbb{C}$ est définie par $W_N(f(z)) = N^{-\lambda/2} z^{-\lambda} f(-1/Nz)$; il vérifie $W_N^2 = (-1)^\lambda$, et l'adjoint pour le produit scalaire de Petersson de tout opérateur de Hecke T_n est $W_N T_n W_N^{-1}$ (de même, l'adjoint de l'opérateur diamant $\langle n \rangle$ pour n premier à N est $W_N \langle n \rangle W_N^{-1}$) (voir par exemple [4], I.4). Considérons alors l'altération suivante : $(f,g) \to \{f,g\} = \langle f, \sigma \circ W_N(g) \rangle_\mathrm{P}$ du produit scalaire de Petersson, c'est-à-dire :

$$\left\{ \begin{array}{rcl} S_\lambda(\Gamma_1(N))_\mathbb{C} \times S_\lambda(\Gamma_1(N))_\mathbb{C} & \to & \mathbb{C} \\ (f,g) & \mapsto & \int_\Delta (\sum_{n\geq 1} a_n q^n)\, W_N(\sum_{n\geq 1} b_n \overline{q}^n)\, y^\lambda \frac{dx\,dy}{y^2} \ , \end{array} \right.$$

où $(\sum_{n\geq 1} a_n q^n)$ et $(\sum_{n\geq 1} b_n q^n)$ sont les développements de Fourier de f et g respectivement en l'infini, et Δ est un domaine fondamental du quotient du demi-plan de Poincaré par $\Gamma_1(N)$. Par construction, ce produit est $\mathbb{C}$-bilinéaire, et pour lui également l'algèbre de Hecke est auto-adjointe. Les deux accouplements $[\ ,\ ]$ et $\{\ ,\ \}$ présentent donc respectivement $\mathbb{T}_\mathbb{C}$ et $S_\lambda(\Gamma_1(N))_\mathbb{C}$ comme les duaux comme $\mathbb{C}$-espaces de $S_\lambda(\Gamma_1(N))_\mathbb{C}$, ce qui donne un isomorphisme de $\mathbb{C}$-espaces vectoriels entre eux. Mais l'auto-adjonction de $\mathbb{T}_\mathbb{C}$ pour les deux montre que cette application est aussi un morphisme de $\mathbb{T}_\mathbb{C}$-module, donc que $S_\lambda(\Gamma_1(N))_\mathbb{C}$ est un $\mathbb{T}_\mathbb{C}$-module libre de rang 1. Enfin, que ceci soit vrai sur $\mathbb{Q}$ est une conséquence du résultat de géométrie algébrique élémentaire suivant : si k est un corps infini dont K est une extension, si R est une k-algèbre et M un R-module qui est un k-espace vectoriel de dimension finie, et tel que $M \otimes_k K$ soit un $R \otimes_k K$-module libre de rang 1, alors M est soi-même un R-module libre de rang 1. Ce résultat se montre comme suit. Choisisons des éléments r_i de R, $1 \leq i \leq \dim_k M$, tel que les $r_i.y$ forment une K-base de $M \otimes_k K$ pour un y de $M \otimes_k K$. La fonction f qui à tout élément x de M associe le déterminant de $(r_i.x)$ est polynômiale en les coordonnées de x dans une k-base de M, et n'est pas nulle sur $M \otimes_k K$. Ce qui veut dire que le polynôme correspondant est non nul, et comme k est infini, on a bijection entre polynômes et fonctions polynômiales sur M : donc f ne peut être uniformément nulle sur M, et M est un R-module de rang 1. Qu'enfin M soit R-libre provient de sa $R \otimes_k K$-fidélité après extension des scalaires à K. □

3.8 Finitude du quotient d'enroulement.

On la démontre en niveau quelconque, avec les résultats qui précèdent appliqués au cas de poids λ égal à 2, le caractère ε étant trivial. Soit N un entier ; on considère la courbe modulaire $X_0(N)_\mathbb{Q}$ et sa jacobienne $J_0(N)_\mathbb{Q}$ sur $\mathbb{Q}$. On rappelle les notations de l'introduction, dans ce cadre plus général : e désigne l'élément d'enroulement, c'est-à-dire l'élément de $H_1(X_0(N)\,;\mathbb{Q})$ défini par l'intégration entre zéro et l'infini sur notre courbe modulaire ; $\mathcal{A}_e$ désigne l'idéal d'enroulement, c'est-à-dire l'idéal annulateur dans $\mathbb{T}_\mathbb{Z}$ de e. Notons aussi

$\mathcal{A}_{e,\mathbb{Q}} = \mathcal{A}_e \otimes_{\mathbb{Z}} \mathbb{Q}$. Le quotient d'enroulement J_0^e est la variété abélienne quotient $J_0(N)/\mathcal{A}_e J_0(N)$.

Théorème 3.9 *$J_0^e(\mathbb{Q})$ est fini.*

Preuve. Notons d'abord $S_2(N)_{\mathbb{Q}}$ le $\mathbb{Q}$-espace des formes paraboliques de poids deux pour $\Gamma_0(N)$ à coefficients dans $\mathbb{Q}$, et $\mathrm{Cot}_0(J_0(N)_{\mathbb{Q}})$ l'espace cotangent à $J_0(N)_{\mathbb{Q}}$ en zéro ; on a les identifications suivantes :

$$S_2(N)_{\mathbb{Q}} \simeq H^0(X_0(N)_{\mathbb{Q}}, \Omega^1) \simeq H^0(J_0(N)_{\mathbb{Q}}, \Omega^1) \simeq \mathrm{Cot}_0(J_0(N)_{\mathbb{Q}}),$$

et $S_2(N)_{\mathbb{Q}}$ est un $\mathbb{T}\otimes_{\mathbb{Z}}\mathbb{Q}$-module libre de rang 1 (voir la proposition 3.7 ou 4.7).

L'algèbre de Hecke à coefficients dans $\mathbb{Q}$ s'écrit donc comme on l'a explicité plus haut, *i.e.* comme un produit d'anneaux (ou comme une somme directe d'idéaux) R_f, correspondants aux restrictions de $\mathbb{T}_{\mathbb{Q}}$ aux orbites sous l'action du groupe de Galois des newforms f de niveau M divisant N.

D'après le théorème d'Atkin-Lehner (théorème 3.2), si on note $S_2(M)_{\mathbb{C}}^{\mathrm{new}}$ le sous-$\mathbb{C}$-espace de $S_2(M)_{\mathbb{C}}$ engendré par les *newforms* de niveau M, on a en faisant la somme directe des opérateurs B_d convenables un isomorphisme de $\mathbb{C}$-espaces vectoriels :

$$\oplus_{M|N}\oplus_{d|(N/M)} S_2(M)_{\mathbb{C}}^{\mathrm{new}} \xrightarrow{\sim} S_2(N)_{\mathbb{C}}.$$

Grâce à l'interprétation en termes d'espaces cotangents des espaces de formes paraboliques, on déduit des opérateurs B_d des isogénies $J_0(M)_{\mathbb{Q}} \xrightarrow{B_d^*} J_0(N)_{\mathbb{Q}}$ (les opérateurs B_d sont définis sur $\mathbb{Q}$), et pour tout M on définit $J_0(M)_{\mathrm{new}} := J_0(M)/(\sum_{d|M} \mathrm{Im}(B_d^*))$. On déduit alors de l'isomorphisme précédent (entre espaces de formes paraboliques) l'isogénie :

$$J_0(N)_{\mathbb{Q}} \to \oplus_{M|N}\oplus_{d|(N/M)} J_0(M)_{\mathbb{Q},\mathrm{new}}.$$

On a, encore et toujours selon la décomposition d'Atkin-Lehner, des isogénies $J_0(M)_{\mathbb{Q},\mathrm{new}} \to \oplus_{G_{\mathbb{Q}}f} J_f$, où la somme est prise sur les orbites sous Galois $G_{\mathbb{Q}}f$ des newforms f en niveau M, et J_f est la variété abélienne "découpée" dans $J_0(M)_{\mathbb{Q}}$ avec la forme f : avec les notations de 3.5, l'annulateur $\mathrm{Ann}_{\mathbb{T}_{\mathbb{Q}}} f$ de f dans $\mathbb{T}_{\mathbb{Q}}$ est $R^f := \oplus_{g\neq f} R_g$, donc J_f est isogène à $J_0(M)_{\mathbb{Q}}/R^f J_0(M)_{\mathbb{Q}}$. On a donc pour finir l'isogénie :

$$J_0(N)_{\mathbb{Q}} \to \oplus_{G_{\mathbb{Q}}.f} (J_f)^{\sigma_0(N/M)},$$

où la somme est prise sur les orbites sous l'action de Galois de toutes les newforms en niveaux M divisant N.

L'accouplement bilinéaire :

$$\begin{cases} H_1(X_0(N)\,;\,\mathbb{Q}) \times S_2(N)_{\mathbb{C}} & \to & \mathbb{C} \\ (c, f) & \mapsto & \langle c, f\rangle = \int_c f(z)dz \end{cases}$$

est non dégénéré, et pour lui les opérateurs de Hecke sont auto-adjoints.

On va d'abord prouver :

Lemme 3.10 *Soit f une newform en niveau M divisant N tel que $\langle e, f\rangle \neq 0$. Alors $\mathcal{A}_e \cap R_f = \{0\}$.*

Preuve du lemme. Calculons l'effet de B_D (D entier quelconque) sur l'accouplement :

$$\langle e, B_D(f)\rangle = \int_e f(D.z)dz = i\int_0^\infty f(iDz)dz = \frac{i}{D}\int_0^\infty f(iz)dz = \frac{1}{D}\langle e, f\rangle.$$

Avant de faire des calculs explicites, expliquons l'idée de la preuve. On a vu que $S_2(N)_{\mathbb{Q}}$ était un $\mathbb{T}_{\mathbb{Q}}$-module libre de rang 1 : comme tel, selon le théorème 3.5, il est isomorphe à un produit de $\mathbb{Q}$-espaces vectoriels de type $K[X_1, \ldots, X_n]/(X_1^{m_1} \ldots X_n^{m_n})$, sur lesquels la restriction de $\mathbb{T}_{\mathbb{Q}}$ a la même forme, et agit par simple multiplication. Si donc on prend un élément $t = \sum_j \lambda_j X_1^{m_1^j} X_2^{m_2^j} \ldots X_m^{m_n^j}$ de la "partie" $K[X_1, \ldots, X_n]/(X_1^{m_1} \ldots X_n^{m_n})$ de $\mathbb{T}_{\mathbb{Q}} \cap \mathcal{A}_e$, en le multipliant par des monômes judicieux de $K[X_1, \ldots, X_n]/(X_1^{m_1} \ldots X_n^{m_n})$ (vu cette fois comme le sous-espace des formes modulaires sur lequel t agit), on aura que l'accouplement de e avec des monômes de type $\lambda_j X_1^{\alpha_1} \ldots X_n^{\alpha_n}$ sera nul, pour tous les λ_j. Mais de tels monômes correspondront à des "décalages" par des opérateurs B_d de notre newform originelle f, décalages qui, comme le montre l'intégration par parties ci-dessus, ne font que multiplier le produit $\langle e, f\rangle$ par des constantes non nulles. On déduira donc de la non nullité de ce produit $\langle e, f\rangle$ que tous les coefficients λ_j sont nuls, et donc t.

Écrivons-le maintenant précisément. Soit t élément de R_f. On a les équivalences suivantes :

$$(t.e = 0) \Leftrightarrow (\forall g \in S_2(N)_{\mathbb{C}}, \langle t.e, g\rangle = 0) \Leftrightarrow (\forall g \in \mathcal{B}_f, \langle e, t.g\rangle = 0).$$

Supposons de plus t dans $\mathcal{A}_e$. On décompose E_f comme somme directe des intersections des sous-espaces caractéristiques des opérateurs U_q pour q divisant N. Considérons la restriction $\tilde{t}$ de t à l'un de ces sous-espaces, $\tilde{E}_f$. On écrit $\tilde{t}$ comme un polynôme en les U_q, pour q divisant N, à coefficients dans $\mathbb{Q}[T_l, ...]$ (l ne divisant pas N), c'est-à-dire à coefficients dans (un corps isomorphe à) K_f. On peut ne considérer que les U_q qui n'agissent pas diagonalement sur $\tilde{E}_f$. Si on note α_q la valeur propre de U_q sur $\tilde{E}_f$, alors $u_q := (U_q - \alpha_q \mathrm{Id}|_{\tilde{E}_f})$ est nilpotent.

On écrit donc $\tilde{t}$ sous forme d'un polynôme :

$$\tilde{t} = \sum_{j \geq 0} \lambda_j \, u_{q_1}^{\alpha_1^j} u_{q_2}^{\alpha_2^j} \ldots u_{q_m}^{\alpha_m^j},$$

où les multi-indices α_k^j sont ordonnés par exemple de façon lexicographique ($j < j'$ si $\alpha_s^j < \alpha_s^{j'}$, où $s := \inf\{r \text{ tel que } \alpha_r^j \neq \alpha_r^{j'}\}$).

D'après la réduction de Jordan de la partie précédente, il existe des polynômes en B_{q_j} : $P_j(B_{q_j})$, et un élément :

$$g_1 := [P_1(B_{q_1}) \otimes P_2(B_{q_2}) \otimes \cdots P_m(B_{q_m})](f) \in S_2(N)_{\mathbb{C}} \ ,$$

tel que $u_{q_j}^{\alpha_j^1}(P_j(B_{q_j})(f)) =: \mathcal{P}_j(B_{q_j}(f)) \neq 0$ et $u_{q_j}^{\alpha_j^1+1}(P_j(B_{q_j})(f)) = 0$. Pour être plus explicite, $\mathcal{P}_j(B_{q_j}(f))$ a l'une des quatre formes suivantes :

1. (f) si on est sur l'espace caractéristique associé à 0 et $q_j^2|M$;
2. $(B_{q_j}(f) - a_{q_j} f)$ si on est sur l'espace caractéristique associé à 0 et $q_j||M$;
3. $(B_{q_j}^2(f) - (a_{q_j}/q_j)B_{q_j}(f) + (1/q_j)f)$ si on est sur l'espace caractéristique associé à 0 et q_j ne divise pas M ;
4. $(-q_j B_{q_j}(f) + \alpha_{q_j} f)$ si q_j ne divise pas M et on est sur le sous-espace $\mathrm{Ker}(U_{q_j}^2 - a_{q_j}U_{q_j} + q_j) = \mathrm{Ker}(U_{q_j} - \alpha_{q_j}\mathrm{Id})^2$.

Alors

$$0 = \langle e, t.g_1\rangle = \lambda_1 \int_0^{i\infty} \prod_{j=1}^{m} \mathcal{P}_j(B_{q_j}(f))\, dz = \lambda_1 \prod_{j=1}^{m} \mathcal{P}_j(\frac{1}{q_j}) \int_0^{i\infty} f\, dz$$

$$= \lambda_1 \prod_{j=1}^{m} \mathcal{P}_j(\frac{1}{q_j})\langle e, f\rangle \ ;$$

or aucun des facteurs $\mathcal{P}_j(\frac{1}{q_j})$ n'est nul, puisque respectivement de forme :

1. 1,
2. $(1/q_j - a_{q_j}) = (1/q_j \ \pm 1)$,
3. $(1/q_j^2 - a_{q_j}/q_j^2 \ + 1/q_j) = (1/q_j^2)(q_j \ + 1 \ - a_{q_j})$, ou encore :
4. $(\alpha_{q_j} - 1) = (\pm\sqrt{q_j} - 1)$.

(La seule non-nullité qui ne soit pas triviale est la troisième : c'est la borne de Weil ($|a_{q_j}| \leq 2\sqrt{q_j}$) qui la montre.) Donc λ_1 est nul, et en recommençant la même opération, par récurrence tous les λ_j sont nuls - donc $\tilde{t}$ l'est aussi. Ceci étant vrai pour toutes les restrictions $\tilde{t}$ de t aux intersections de sous-espaces caractéristiques, t est lui-même nul. □

Fin de la preuve du théorème. On a montré que si $\langle e, f\rangle \neq 0$, $\mathcal{A}_{e,\mathbb{Q}} \cap R_f = 0$, et réciproquement il est évident que si $\langle e, f\rangle = 0$ alors $\mathcal{A}_{e,\mathbb{Q}} \cap R_f = R_f$. Comme $L(f, 1) = 2\pi\langle e, f\rangle$, on peut donc écrire :

$$\mathcal{A}_{e,\mathbb{Q}} = \bigoplus_{G_\mathbb{Q} f / L(f,1)=0} R_f \ ,$$

et on a des isogénies :

$$J_0^e(\mathbb{Q}) = (J_0(N)/\mathcal{A}_e J_0(N))(\mathbb{Q}) \to \prod_{R_f \not\subset \mathcal{A}_{e,\mathbb{Q}}} (J_0(N)/(\mathbb{T}_\mathbb{Q}/R_f)J_0(N))(\mathbb{Q}) \to$$

$$\to \prod_{G_{\mathbb{Q}} f / L(f,1) \neq 0} J_f(\mathbb{Q}).$$

Selon le théorème de Kolyvagin-Logachev, les $J_f(\mathbb{Q})$ ci-dessus sont finies (à cause justement de la non-nullité en 1 de la fonction $L(f,s)$, voir le théorème 0.3 de [12], complété par des résultats de [21] ou [2]). Et donc le quotient d'enroulement est bien de rang nul. □

4 Espaces tangents et cotangents.

4.1 Espace tangent à $J_0(N)_{/\mathbb{Z}[1/N]}$ en zéro.

Soit N un entier, fixé pour toute cette partie. On montre dans cette sous-section :

Théorème 4.2 *L'espace tangent à $J_0(N)_{/\mathbb{Z}[1/N]}$ en zéro, $\mathrm{Tan}_0(J_0(N)_{/\mathbb{Z}[1/N]})$, est un $\mathbb{T}_{\mathbb{Z}} \otimes \mathbb{Z}[1/N]$-module libre de rang 1, de base $\frac{d}{dq}|_0$.*

On va donner quatre lemmes préliminaires, desquels le théorème découlera naturellement. Dans ce qui suit, pour alléger les notations, on notera M le module $\mathrm{Tan}_0(J_0(N)_{/\mathbb{Z}[1/N]})$, et R l'anneau $\mathbb{T}_{\mathbb{Z}} \otimes \mathbb{Z}[1/N]$, qui est un $\mathbb{Z}[1/N]$-module libre de type fini ($\mathbb{T}_{\mathbb{Z}}$ l'est sur $\mathbb{Z}$, puisqu'on peut le voir comme un sous-module des endomorphismes de $J_0(N)_{/\mathbb{Z}}$).

Lemme 4.3 *Le R-module M est fidèle.*

Preuve. Comme ni R ni M n'ont de $\mathbb{Z}[1/N]$-torsion, on peut voir le lemme en étendant les scalaires à $\mathbb{Q}$, et en remarquant qu'alors, le dual de $M \otimes \mathbb{Q}$ (comme $\mathbb{Q}$-espace vectoriel), qui est $\mathrm{Cot}_0(J_0(N)_{\mathbb{Q}})$, est bien $\mathbb{T} \otimes \mathbb{Q}$-fidèle, comme on le voit dans la partie précédente. □

Lemme 4.4 *Pour tout idéal maximal $\mathcal{M}$ de R, on a $M/\mathcal{M}M \neq 0$.*

Preuve. Supposons qu'il existe un idéal maximal $\mathcal{M}$ tel que $M/\mathcal{M}M = 0$. Puisque M est un R-module fini, le faisceau associé $\tilde{M}$ sur le schéma affine noethérien $X :=\mathrm{Spec}(R)$ est cohérent ; notons x le point correspondant à $\mathcal{M}$. On a :

$$M/\mathcal{M}M = M \otimes_R R/\mathcal{M} = M \otimes_R R_{\mathcal{M}}/\mathcal{M}R_{\mathcal{M}} = M_{\mathcal{M}}/\mathcal{M}M_{\mathcal{M}},$$

donc le lemme de Nakayama dit que $M_{\mathcal{M}} = 0$. Si g est un point générique de X (correspondant à l'idéal $\mathcal{P}$ de R) qui se spécialise en x, on a $\tilde{M}_g = 0$ (comme localisation de $\tilde{M}_x$). Puisque R est sans $\mathbb{Z}$-torsion, g est au-dessus du point générique de $\mathbb{Z}[1/N]$; et puisque c'est un $\mathbb{Z}[1/N]$-module de type fini, $\mathrm{Spec}(R \otimes_{\mathbb{Z}[1/2N]} \mathbb{Q})$ est de dimension nulle. On a donc $R \otimes \mathbb{Q} \simeq \prod_{\mathcal{Q}} R_{\mathcal{Q}}$, où le produit (fini) est pris sur les idéaux minimaux $\mathcal{Q}$ de R : ce qui veut dire que $R_{\mathcal{P}}$ est isomorphe à un facteur de $R \otimes_{\mathbb{Z}[1/N]} \mathbb{Q}$. Mais alors la fidélité de M comme R-module contredit le fait que $\tilde{M}_g = 0$. □

Lemme 4.5 *Pour tout idéal maximal $\mathcal{M}$ de R, l'élement $\frac{d}{dq}|_0$ de M est d'image non nulle dans le quotient $M/\mathcal{M}M$.*

Preuve. Soit $\mathcal{M}$ un idéal maximal de R. De la finitude comme $\mathbb{Z}$-module de $\mathbb{T}_{\mathbb{Z}}$ on déduit d'abord que le sous corps premier de $F := R/\mathcal{M}$ est nécéssairement fini, $\mathbb{F}_l$, et que F en est une extension finie. Posons $\overline{R} := R \otimes_{\mathbb{Z}} \overline{\mathbb{F}}_l$, et $\overline{M} := M \otimes_{\mathbb{Z}} \overline{\mathbb{F}}_l$. On a la suite exacte : $\mathcal{M} \otimes_{\mathbb{Z}} \overline{\mathbb{F}}_l \to \overline{R} \to F \otimes_{\mathbb{Z}} \overline{\mathbb{F}}_l \to 0$. Choisissons un plongement $i : F \hookrightarrow \overline{\mathbb{F}}_l$, et déduisons-en un morphisme de $\overline{\mathbb{F}}_l$-algèbre :

$$i \otimes 1 : F \otimes_{\mathbb{F}_l} \overline{\mathbb{F}}_l \to \overline{\mathbb{F}}_l.$$

Notons $\overline{\mathcal{M}}$ son noyau : on a la suite exacte $0 \to \overline{\mathcal{M}} \to \overline{R} \to \overline{\mathbb{F}}_l \to 0$. On vérifie alors qu'on a :

$$\left.\frac{d}{dq}\right|_0 \mapsto (M/\mathcal{M}M) \hookrightarrow (M/\mathcal{M}M) \otimes_F \overline{\mathbb{F}}_l \simeq \overline{M}/\overline{\mathcal{M}}\,\overline{M}.$$

Si E est un $\overline{\mathbb{F}}_l$-espace vectoriel, notons $E^\vee$ son dual, et désignons par $\overline{M}^\vee[\overline{\mathcal{M}}]$ le sous-$\overline{R}$-module de $\overline{M}^\vee$ tué par $\overline{\mathcal{M}}$. Avec ces notations,

$$(\overline{M}/\overline{\mathcal{M}}\,\overline{M})^\vee \simeq \overline{M}^\vee[\overline{\mathcal{M}}]$$

en tant que $\overline{R}$-modules. (En effet, les formes $\overline{\mathbb{F}}_l$-linéaires sur l'espace vectoriel quotient $(\overline{M}/\overline{\mathcal{M}}\,\overline{M})$ s'identifient avec celles sur $\overline{M}$ dont le noyau contient $\overline{\mathcal{M}}\,\overline{M}$, et l'action de $\overline{R}$-module que l'on considère est : $(t.f)(\ ) = f(t.\ )$, ($t \in \overline{R}$, $f \in \overline{M}^\vee$).) On a donc enfin :

$$\overline{M}^\vee[\overline{\mathcal{M}}] = H^0(X_0(N)_{\overline{\mathbb{F}}_l}, \Omega^1)[\overline{\mathcal{M}}] \simeq S_2(N)_{\overline{\mathbb{F}}_l}[\overline{\mathcal{M}}].$$

On a montré dans le lemme précédent que $M/\mathcal{M}M$ était non nul : soit donc f une forme parabolique non nulle appartenant à $S_2(N)_{\overline{\mathbb{F}}_l}[\overline{\mathcal{M}}]$. Le corollaire III, 12.9 de [7] assure que $H^0(X_0(N)_{\overline{\mathbb{F}}_l}, \Omega^1) = H^0(X_0(N)_{/\mathbb{Z}[1/N]}, \Omega^1) \otimes \overline{\mathbb{F}}_l$, ce qui implique que, quitte à prendre un relèvement de f, on peut supposer qu'on est en caractéristique nulle, et même dans $S_2(N)_{\mathbb{C}}$: pour voir que les coefficients de f vérifient la relation :

$$a_1(T_n.f) = a_n(f)$$

même si f n'est pas une newform (cela résulte par exemple de la formule (3.5.12) de [27]). On en déduit que pour tout entier n, $\frac{d}{dq}|_0(T_n.f) = a_n(f)$. Mais puisque $X_0(N)_{\overline{\mathbb{F}}_l}$ est intègre et lisse, ses formes différentielles sont définies par leur développement de Fourier en l'infini : donc $\frac{d}{dq}|_0$ ne peut être d'image nulle. □

Lemme 4.6 *Pour tout idéal maximal $\mathcal{M}$ de R, $M/\mathcal{M}M$ est un $R/\mathcal{M}$-module libre de rang* 1, *de base l'image de $\frac{d}{dq}|_0$.*

Preuve. Les résultats précédents montrent qu'il suffit maintenant de prouver que $\dim_{R/\mathcal{M}}(M/\mathcal{M}M) \leq 1$. Si (l) est l'idéal premier de $\mathbb{Z}$ au-dessus duquel $\mathcal{M}$ se trouve, choisissons comme dans la preuve du précédent lemme un plongement de $F = R/\mathcal{M}$ dans $\overline{\mathbb{F}}_l$. Toujours selon la preuve précédente et avec les mêmes notations, les propriétés suivantes sont équivalentes :

1. $(M/\mathcal{M}M)$ est un F-espace vectoriel de dimension 1 ;
2. $(M/\mathcal{M}M) \otimes_F \overline{\mathbb{F}}_l$ est un $\overline{\mathbb{F}}_l$-espace vectoriel de dimension 1 ;
3. $(\overline{M}/\overline{\mathcal{M}}\,\overline{M})$ est un $\overline{\mathbb{F}}_l$-espace vectoriel de dimension 1 ;
4. $\overline{M}^{\vee}[\overline{\mathcal{M}}]$ est un $\overline{\mathbb{F}}_l$-espace vectoriel de dimension 1.

Pour tout entier n, soit a_n l'image dans $\overline{R}/\overline{\mathcal{M}} \simeq \overline{\mathbb{F}}_l$ de l'opérateur de Hecke T_n. Soit f un élément non nul de $H^0(X_0(N)_{\overline{\mathbb{F}}_l}, \Omega^1)[\overline{\mathcal{M}}]$; f est une forme propre pour les opérateurs de Hecke : pour tout n, $T_n(f) = a_n f$. À une constante multiplicative non nulle près, le développement de Fourier de f en l'infini est donc : $q + a_2 q^2 + a_3 q^3 + \cdots$. De même que plus haut, on déduit du fait que $X_0(N)_{\overline{\mathbb{F}}_l}$ soit intègre et lisse que toute forme différentielle sur $X_0(N)_{\overline{\mathbb{F}}_l}$ est définie par son q-développement en l'infini ; donc f engendre l'espace vectoriel $S_2(N)_{\overline{\mathbb{F}}_l}$. □

Preuve du théorème. Montrons que le module $M' := M/(R.(\frac{d}{dq})|_0)$ est nul. D'après le lemme précédent, pour tout idéal maximal $\mathcal{M}$ de R,

$$M'/\mathcal{M}M' = M' \otimes_R R_{\mathcal{M}}/\mathcal{M}R_{\mathcal{M}} = 0 \ ;$$

donc par le lemme de Nakayama, $M'_{\mathcal{M}}$ est nul. On peut alors appliquer le raisonnement de la preuve du lemme 4.4, et en conclure que le faisceau $\tilde{M'}$ sur $\mathrm{Spec}(R)$ est de fibre nulle en chaque point, donc nul. Enfin, M est un R-module libre puisque fidèle. □

Notons au passage un corollaire de ce dernier théorème (voir aussi 3.7) :

Proposition 4.7 *L'espace des formes paraboliques $S_2(N)_{\mathbb{Q}}$ est un $\mathbb{T}_{\mathbb{Q}}$ - module libre de rang 1.*

Preuve. Une application du corollaire 3.6 du chapitre précédent donne que la $\mathbb{Q}$-algèbre de Hecke $\mathbb{T}_{\mathbb{Q}}$ (pour $\Gamma_0(N)$, en poids 2) est de Gorenstein. De plus, on vient de montrer que $\mathrm{Tan}_0(J_0(N)_{\mathbb{Q}})$ était comme $\mathbb{T}_{\mathbb{Q}}$-module isomorphe à $\mathbb{T}_{\mathbb{Q}}$ lui-même ; et comme $\mathrm{Cot}_0(J_0(N)_{\mathbb{Q}}) = \mathrm{Tan}_0(J_0(N)_{\mathbb{Q}})^{\vee}$, $\mathrm{Cot}_0(J_0(N)_{\mathbb{Q}})$ est isomorphe à $\mathbb{T}_{\mathbb{Q}}$ soi-même comme $\mathbb{T}_{\mathbb{Q}}$-module. □

4.8 Espace tangent au quotient de la jacobienne.

Soit I un idéal de $\mathbb{T}_{\mathbb{Z}}$, saturé (*i.e.* tel que $\mathbb{T}/I$ soit sans $\mathbb{Z}$-torsion). On déduit de la jacobienne $J_0(N)$ sur $\mathbb{Z}[1/2N]$ les schémas abéliens $J^I := I.J_0(N)$ et $J_I := J_0(N)/I.J_0(N)$. Le but de cette section est de démontrer le théorème suivant, voisin et corollaire de la celui de la section précédente :

Théorème 4.9 *L'espace tangent à $J_{I,\mathbb{Z}[1/2N]}$ en zéro, $\mathrm{Tan}_0(J_{I,\mathbb{Z}[1/2N]})$, est un $\mathbb{T}/I \otimes \mathbb{Z}[1/2N]$-module libre de rang 1, de base l'image de $\frac{d}{dq}|_0$.*

On commence par travailler sur $\mathbb{Q}$:

Proposition 4.10 *On a $\mathrm{Tan}_0(J^I_{\mathbb{Q}}) = I.\mathrm{Tan}_0(J_0(N)_{\mathbb{Q}})$.*

Preuve de la proposition. Soit $(i_1, i_2, \ldots, i_n)$ un système de générateurs de I ($\mathbb{T}$ est noethérien puisque $\mathbb{Z}$-module de type fini) ; $J^I_{\mathbb{Q}}$ est donc l'image du morphisme :

$$\oplus_{1\leq j\leq n} J_0(N)_{\mathbb{Q}} \stackrel{\phi}{\to} J_0(N)_{\mathbb{Q}}$$

défini par la multiplication par ce système. On en déduit sur les espaces tangents :

$$\oplus_{1\leq j\leq n} \mathrm{Tan}_0(J_0(N)_{\mathbb{Q}}) \stackrel{\tilde{\phi}}{\to} \mathrm{Tan}_0(J_0(N)_{\mathbb{Q}}).$$

La proposition découle alors du lemme :

Lemme 4.11 *Pour tout morphisme $A \stackrel{\psi}{\to} B$ de variétés abéliennes sur $\mathbb{Q}$, on a $\mathrm{Tan}_0(\psi(A)) = \tilde{\psi}(\mathrm{Tan}_0(A))$.*

Preuve du lemme. Le foncteur $A \mapsto \mathrm{Tan}_0(A)$ de la catégorie des groupes algébriques commutatifs sur $\mathbb{Q}$ dans celle des $\mathbb{Q}$-espaces vectoriels, est exact à gauche. Mais il est aussi exact à droite : de la suite exacte $0 \to A \to B \to C \to 0$ se déduit celle sur les tangents : $0 \to \mathrm{Tan}_0(A) \to \mathrm{Tan}_0(B) \to \mathrm{Tan}_0(C)$; si les dimensions des variétés sont a, b et c respectivement, on a $a + c = b$, et comme les dimensions des espaces tangents associés sont les mêmes (lissité des groupes algébriques sur $\mathbb{Q}$), la dernière flèche de la dernière suite est surjective.

Si donc on a un morphisme ψ :

$$0 \to \ker(\psi) \to A \stackrel{\psi}{\to} \psi(A) \to 0,$$

on a bien

$$\mathrm{Tan}_0(\psi(A)) = \mathrm{Tan}_0(A)/\mathrm{Tan}_0(\ker(\psi)) = \tilde{\psi}(\mathrm{Tan}_0(A)). \ \square$$

Considérons maintenant le problème sur $\mathbb{Z}[1/2N]$.

Preuve du théorème. De la suite exacte de variétés abéliennes sur $\mathbb{Q}$:

$$0 \to J^I_{\mathbb{Q}} \to J_0(N)_{\mathbb{Q}} \to J_{I,\mathbb{Q}} \to 0,$$

on déduit par propriété universelle des modèles de Néron un complexe de schémas abéliens :

$$0 \to J^I_{\mathbb{Z}[1/2N]} \to J_0(N)_{\mathbb{Z}[1/2N]} \to J_{I,\mathbb{Z}[1/2N]} \to 0,$$

qui est en réalité une *suite exacte*, d'après un résultat de Raynaud (voir section 1, proposition 1.2 de [16]). Ce résultat assure encore que la suite :

$$0 \to \mathrm{Tan}_0(J^I_{\mathbb{Z}[1/2N]}) \to \mathrm{Tan}_0(J_0(N)_{\mathbb{Z}[1/2N]}) \to \mathrm{Tan}_0(J_{I,\mathbb{Z}[1/2N]}) \to 0$$

est exacte elle aussi (même référence, corollaire 1.1). Or on voit par la section précédente que $\mathrm{Tan}_0(J_0(N)_{\mathbb{Z}[1/2N]})$ est un $\mathbb{T}\otimes\mathbb{Z}[1/2N]$-module libre de rang 1, de base $\frac{d}{dq}|_0$; il existe donc un idéal I' de $\mathbb{T}[1/2N]$ tel que la suite précédente de $\mathbb{T}[1/2N]$-modules soit isomorphe à :

$$0 \to I' \to \mathbb{T}\otimes\mathbb{Z}[1/2N] \to \mathbb{T}\otimes\mathbb{Z}[1/2N]/I' \to 0.$$

Mais puisque sur $\mathbb{Q}$ on a $I_{\mathbb{Q}} = I'_{\mathbb{Q}}$, que I est par hypothèse saturé, et que I' l'est aussi (puisque $\mathrm{Tan}_0(J_{I,\mathbb{Z}[1/2N]}) \simeq \mathbb{T}[1/2N]/I'$ est sans torsion), on a bien $I' = I_{\mathbb{Z}[1/2N]}$. Donc

$$\mathrm{Tan}_0(J_{I,\mathbb{Z}[1/2N]}) \simeq (\mathbb{T}/I)_{\mathbb{Z}[1/2N]}. \ \square$$

4.12 Preuve de la proposition "critère de Kamienny".

On rappelle la situation dans laquelle on s'est mis avec notre problème initial de borne pour la torsion de courbes elliptiques (voir la section 1, dont on reprend les hypothèses et notations). Rappelons le morphisme naturel $f_d : X_0(p^n)^{(d)}_{\mathrm{lisse}} \to J^e_0$, normalisé par $\infty^{(d)} \mapsto 0$. On a défini en (1.3) un point $j'^{(d)}$, à valeurs dans $\mathbb{Z}$, de $X_0(p^n)^{(d)}_{\mathrm{lisse}}$, qui croise $\infty^{(d)}$ sur la fibre en l. On va d'abord montrer que ceci implique que f_d n'est pas une immersion formelle au point $\infty^{(d)}_{\mathbb{F}_l}$, en suivant l'exposé de [22].

Soit S un schéma quelconque. Si $\phi : X \to Y$ est un morphisme de S-schémas noethériens, on dit que c'est une *immersion formelle* en un point x de X si l'application $\hat{\mathcal{O}}_{Y,\phi(x)} \to \hat{\mathcal{O}}_{X,x}$ déduite de ϕ entre complétés d'anneaux locaux est surjective. Si s est l'image dans S de x (et y), on montre que ceci équivaut à ce que la restriction de ϕ aux fibres en s soit une immersion formelle en x. On démontre ensuite dans [22] (lemme 5.1) :

Lemme 4.13 *Supposons que X soit séparé, que $\phi : X \to Y$ soit une immersion formelle en x. Supposons qu'il existe un schéma intègre noethérien T et deux points p_1 et p_2 de X à valeur dans T, tel qu'en un point t de T on ait $x = p_1(t) = p_2(t)$. Si de plus on a $\phi \circ p_1 = \phi \circ p_2$, alors $p_1 = p_2$.*

On va aussi utiliser le lemme de spécialisation suivant, (avec une preuve qui m'a été signalée par Bas Edixhoven) :

Lemme 4.14 *Soit R un anneau de valuation discrète, de caractéristique 0 et caractéristique résiduelle $l > 0$. Notons K le corps de fractions de R, k son corps résiduel, et v la valuation de R ; supposons $v(l) < l - 1$. Soit G un schéma en groupes sur R. Alors, si P est un point d'ordre fini n de $G(R)$, la spécialisation P_k de P est également d'ordre n.*

Preuve. Supposons que l'ordre m de P_k divise strictement n. Quitte à remplacer P par un de ses multiples, on peut suposer $m = 1$, et que n est premier. Soit e l'élément neutre de $G(R)$. Fixons $\mathrm{Spec}(A)$ un voisinage affine ouvert (dans G) de l'image de $e_k = P_k$; il contient tous les multiples de P. Le morphisme P_K induit un morphisme de schémas de $\mathrm{Spec}(K)$ dans $\mathrm{Spec}(A)$, qui ne peut être égal à e_K, car $\mathrm{Spec}(A)$ est séparé sur $\mathrm{Spec}(R)$ (puisqu'affine), et P n'est pas trivial ; P_K est donc d'ordre n. Le point P permet de définir un morphisme de schémas en groupes de $(\mathbb{Z}/n\mathbb{Z})_R$ dans G, qui se factorise (en tant que morphisme de schémas) par $\mathrm{Spec}(A)$, et qui induit une immersion fermée de $(\mathbb{Z}/n\mathbb{Z})_K$ dans G_K, se factorisant par $\mathrm{Spec}(A_K)$. Soit F_K l'image schématique de cette immersion, F' sa fermeture schématique dans $\mathrm{Spec}(A)$, et F leur fermeture schématique dans G. Soit I_K l'idéal de définition de F_K ; alors $F' = \mathrm{Spec}(A/I)$, où I la pré-image de I_K dans A. Les compositions de morphismes de schémas : $(\mathbb{Z}/n\mathbb{Z})_K \to (\mathbb{Z}/n\mathbb{Z})_R \to F$ et $(\mathbb{Z}/n\mathbb{Z})_K \simeq F_K \to F$ sont égales, d'où on déduit que les compositions des morphismes de R-modules : $A/I \to R^n \to K^n$ et $A/I \to A_K/I_K \simeq K^n$ le sont aussi. Mais par définition des objets, $A/I \to K^n$ est une injection, donc $A/I \to R^n$ en est une également ; on déduit de tout cela que A/I est un R-module libre de rang n.

Montrons maintenant que F, puis F' sont des schémas en groupes sur $\mathrm{Spec}(R)$. Considérons la catégories dont les objets sont les immersions fermées dans la fibre générique des R-schémas, et les flèches sont les diagrammes commutatifs évidents. L'opération de prendre l'adhérence schématique de chaque sous-schéma de la fibre générique dans le schéma auquel il appartient définit un foncteur de cette catégorie dans celle des R-schémas. De plus, cette opération commute au produit fibré sur R (au sens où "l'adhérence d'un produit est le produit des adhérences") (on vérifie tout cela facilement sur des voisinages affines). Il en résulte clairement que F est un schéma en groupes. Pour F', il suffit de montrer que le morphisme de multiplication de F induit par restriction un morphisme de $F' \times_R F' \to F'$. (Dans notre cas l'inversion est la multiplication par $n - 1$.) Mais F' est un sous-schéma ouvert de F, donc il suffit de montrer que topologiquement, la multiplication restreinte à $F' \times_R F'$ a son image dans F', ce qui est évident par sa définition. Donc F' est un R-schéma en groupes.

Alors, si T est un schéma sur $\mathrm{Spec}(R)$, l'action de $F(T)$ sur lui-même par translation à droite induit un automorphisme de schéma de F_T. D'où un morphisme injectif de R-foncteurs en groupes de F dans $\mathrm{GL}_{n,R}$. L'image de P dans $\mathrm{GL}_n(R)$ est de forme $1+a$ pour un a non nul tel que $\mathrm{val}(a) \geq 1$ (où pour M une matrice à coefficients dans R, $\mathrm{val}(M)$ est la plus petite des valuations des coefficients de M). Comme $1 = (1+a)^n$, on a $a^n + n.a = n.a^2.b$, ce qui n'est possible

que si d'une part $v(n) > 0$ (*i.e.* $n = l$), et d'autre part $\mathrm{val}(a^l) = \mathrm{val}(l.a)$, donc $v(l) + \mathrm{val}(a) = \mathrm{val}(a^l) \geq l.\mathrm{val}(a)$. Ce qui contredit les hypothèses de l'énoncé. □

Les deux lemmes précédents permettent de montrer :

Théorème 4.15 *Le morphisme f_d n'est pas une immersion formelle en $\infty^{(d)}_{\mathbb{F}_l}$.*

Preuve. Puisque $j'^{(d)}$ croise $\infty^{(d)}$ sur la fibre en l, le point $f_d(j'^{(d)})$ de $J_0^e(\mathbb{Z}_{(l)})$ se réduit en 0 au-dessus de l. Ce point est de torsion, car $J_0^e(\mathbb{Q})$ l'est, et comme $l > 2$ le lemme 4.14 assure que $f_d(j'^{(d)})$ est nul dans tout $J_0^e(\mathbb{Z}_{(l)})$. Mais alors, on peut appliquer le lemme 4.13 et en conclure que si f_d était une immersion formelle en $\infty^{(d)}_{\mathbb{F}_l}$, on aurait $j'^{(d)} = \infty^{(d)}$ - ce qui contredit évidemment l'interprétation modulaire de ces points. □

La courbe $X_0(N)$ a en l'infini la coordonnée formelle q ; donc $X_0(N)^d$ a les coordonnées formelles $q_1, \ldots, q_d$ au point $(\infty, \ldots, \infty)$, et les fonctions symétriques élémentaires $\sigma_1 = q_1 + \cdots + q_d$, $\ldots$, $\sigma_d = q_1 \cdots q_d$ sont des coordonnées formelles au point $\infty^{(d)}$ de $X_0(N)^{(d)}$, donc $d\sigma_1, \ldots, d\sigma_d$ forment une base de $\mathrm{Cot}_{\infty^{(d)}}(X_0(N)^{(d)})$. On a alors le lemme :

Lemme 4.16 (Kamienny.) *Soit ω un élément de $\mathrm{Cot}_0(J^e_{0/\mathbb{Z}[1/N]})$. Alors $f_1^*(\omega)$ est une forme différentielle sur $X_0(N)_{/\mathbb{Z}[1/N]}$. Notons $(\sum_{n\geq 1} a_n q^n)(dq/q)$ son développement de Fourier à l'infini. On a :*

$$f_d^*(\omega) = a_1 d\sigma_1 - a_2 d\sigma_2 + \cdots + (-1)^{d-1} a_d d\sigma_d \ \in \mathrm{Cot}_{\infty^{(d)}}(X_0(N)^{(d)}_{/\mathbb{Z}[1/N]}).$$

Preuve. Notons $s_n = \sum_{i=1}^d q_i^n$ pour tout entier n. Soit ϕ le morphisme naturel : $X_0(N)^d \to X_0(N)^{(d)}$; alors $\phi^* f_d^*(\omega) = \sum_{n\geq 1} a_n\, n^{-1}.ds_n$. Or on a pour $1 \leq n \leq d$ les relations de Newton : $\sum_{i=0}^n (-1)^i s_i.\sigma_{n-i} = 0$, où on pose $s_0 = 0 = \sigma_0$. D'où l'évaluation en l'infini de la différenciation : $n^{-1}.ds_n = (-1)^{n-1} d\sigma_n$, qui donne la formule de l'énoncé. □

On en déduit :

Corollaire 4.17 *L'application tangente à f_d en $\infty^{(d)}$ envoie $\frac{d}{d\sigma_1}, \ldots, \frac{d}{d\sigma_d}$ sur $T_1(\frac{d}{dq}|_0), -T_2(\frac{d}{dq}|_0), \ldots, (-1)^{d-1} T_d(\frac{d}{dq}|_0)$ respectivement.*

Preuve. La relation $a_1(T_n f) = a_n(f)$ pour toute forme modulaire (voir la preuve du lemme 4.5) et le lemme précédent suffisent à conclure. □

Et on arrive au théorème qu'on veut finalement montrer :

Théorème 4.18 *On a équivalence entre :*

1. *f_d est une immersion formelle en $\infty^{(d)}_{\mathbb{F}_l}$, et*
2. *$T_1 e, ..., T_d e$ sont $\mathbb{F}_l$-linéairement indépendants dans $\mathbb{T}e/l\mathbb{T}e$.*

De plus, ces deux conditions sont satisfaites si l'est :

3. *$T_1\{0,\infty\}, ..., T_{d.s}\{0,\infty\}$ sont $\mathbb{F}_l$-linéairement indépendants dans l'espace vectoriel $H_1(X_0(p^n)$, pointes$\,;\mathbb{Z})\otimes\mathbb{F}_l$ (où s désigne le plus petit nombre premier différent de p).*

Preuve. D'abord l'équivalence des deux premiers points. La propriété pour un morphisme d'être une immersion formelle en un point est, formulation duale de celle sur les espaces cotangents, que l'application induite par ce morphisme sur les tangents correspondants est une injection. Le corollaire 4.17 dit donc que f_d est une immersion formelle en $\infty^{(d)}_{\mathbb{F}_l}$ si et seulement si les vecteurs $T_i(\frac{d}{dq}|_0)$, $1\leq i\leq d$ sont linéairement indépendants dans $\mathrm{Tan}_0(J_0^e(\overline{\mathbb{F}}_l))$. Mais le théorème 4.9 assure que cet espace tangent est un $\mathbb{T}/\mathcal{A}_e\otimes_{\mathbb{Z}}\overline{\mathbb{F}}_l$-module libre de rang 1 de base $\frac{d}{dq}|_0$, d'où l'équivalence des propriétés *1.* et *2.* du théorème.

Prouvons la dernière implication. Le problème ici est que c'est avec les symboles modulaires, vivant dans l'homologie relative aux pointes, qu'on sait travailler ; mais c'est dans l'homologie absolue qu'il nous faut une indépendance $\mathbb{F}_l$-linéaire. Pour s'y ramener, on fait agir l'opérateur $I_s := T_s - \sigma_1(s)$ sur $\{0,\infty\}$. En effet, puisque s est premier au niveau, l'opérateur T_s envoie les pointes 0 et ∞ sur $(s+1)$-fois elles-mêmes, donc I_s pousse bien $\{0,\infty\}$ dans $H_1(X_0(p^n)\,;\mathbb{Z})$ vu comme sous-module de $H_1(X_0(p^n)$, pointes$\,;\mathbb{Z})$. Considérons aussi $H_1(X_0(p^n)\,;\mathbb{Z})$ comme un sous-module de $H_1(X_0(p^n)\,;\mathbb{Q})$.

Supposons que la propriété *2.* du théorème ne soit pas vérifiée. Il existe donc une relation de dépendance :

$$\overline{\lambda_1}T_1e+\cdots+\overline{\lambda_k}T_ke=0\in\mathbb{T}e/l\mathbb{T}e,$$

pour un $k\leq d$ tel que $\overline{\lambda_k}$ soit non nul. On la relève en

$$\lambda_1T_1e+\cdots+\lambda_kT_ke=l\,x\in l\mathbb{T}e\subseteq H_1(X_0(p^n)\,;\mathbb{Q}),$$

on la multiplie par I_s pour obtenir

$$I_s(\sum_{i=1}^{k}\lambda_iT_ie)=\sum_{i=1}^{k}\lambda_iT_i(I_se)=\lambda_kT_{sk}\,e+\sum_{i=1}^{sk-1}\mu_iT_ie=l\,I_sx\in l\mathbb{T}e.$$

(En effet, la définition des opérateurs de Hecke (par exemple avec la série formelle) donne que $T_s.T_n = T_{s.n}+$ (combinaison linéaire de termes d'indice plus petit).) Les formes linéaires que définissent $I_s\{0,\infty\}$ et I_se par l'intégration sont les mêmes, et puisqu'on peut voir ces deux éléments comme appartenants à $H_1(X_0(p^n)\,;\mathbb{R})$, ils sont en fait égaux. On en déduit une relation de dépendance linéaire :

$$\lambda_kT_{sk}\,\{0,\infty\}+(\sum_{i=1}^{sk-1}\mu_iT_i\{0,\infty\})=l\,I_sx\in lH_1(X_0(p^n)\text{, pointes}\,;\mathbb{Z}),$$

et en considérant son image dans $H_1(X_0(p^n)$, pointes$\,;\mathbb{Z})\otimes\mathbb{F}_l$, une contradiction avec la propriété *3.* du théorème. □

5 Lemme combinatoire.

Le but de cette partie est de prouver la proposition-clé de la démonstration générale :

Proposition 1.9 *Soit p un nombre premier. Posons $C_p = \sqrt{65}$ si p est différent de 2, et $C_2 = \sqrt{129}$. Supposons $d > 2$, et notons s_p le plus petit nombre premier différent de p. Si $p^n > C^2.(sd)^6$, alors les $T_i\{0,\infty\}$, $1 \leq i \leq sd$ sont $\mathbb{F}$-linéairement indépendants dans le $\mathbb{F}$-espace vectoriel $H_1(X_0(p^n),$ pointes$\,;\mathbb{Z})\otimes\mathbb{F}$ pour tout corps $\mathbb{F}$.*

5.1 Notations et rappels.

On identifie $\Gamma_0(p^n)\backslash SL_2(\mathbb{Z})$ à $\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$ avec :

$$\Gamma_0(p^n)\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (\overline{c},\overline{d}) = (c \bmod(p^n), d \bmod(p^n)).$$

L'application de $\Gamma_0(p^n)\backslash SL_2(\mathbb{Z})$ vers $H_1(X_0(p^n),$ pointes$;\mathbb{Z})$: $g \mapsto \{g\cdot 0, g\cdot\infty\}$ s'identifie alors à une application de $\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$ vers la même chose, qu'on note ξ :

$$\xi(\overline{w},\overline{t}) = \left\{\overline{\begin{pmatrix} a & b \\ w & t \end{pmatrix}}\cdot 0, \overline{\begin{pmatrix} a & b \\ w & t \end{pmatrix}}\cdot\infty\right\} = \left\{\frac{b}{t},\frac{a}{w}\right\},$$

avec w,t, relèvements dans $\mathbb{Z}$ de $\overline{w}$ et $\overline{t}\in\mathbb{Z}/p^n\mathbb{Z}$ et $a,b\in\mathbb{Z}$ tels que $\begin{pmatrix} a & b \\ w & t \end{pmatrix}$ soit dans $SL_2(\mathbb{Z})$.

On sait de plus qu'on a :

$$T_r\{0,\infty\} = \sum_{\substack{0\leq w<t \\ 0\leq v<u \\ ut-vw=r}} \xi(\overline{w},\overline{t}) \ ,$$

où on pose $\xi(\overline{w},\overline{t}) = 0$ si $\mathrm{pgcd}(w,t,p) > 1$ (voir [18], théorème 2 et proposition 20, ou la démonstration du lemme 2 de [19]).

Soit $\sigma = \overline{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}}$ et $\tau = \overline{\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}}$. On choisit pour représentants de $\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$: $\{(R_1,1),\ R_1$ un système de représentants de $\mathbb{Z}/p^n\mathbb{Z}\}\cup\{(1,p.R_2),\ R_2$ un système de représentants de $\mathbb{Z}/p^{n-1}\mathbb{Z}\}$. On note w/t au lieu de $(\overline{w},\overline{t})$, souvent. On fait agir $SL_2(\mathbb{Z})$ sur $\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$ à droite, comme d'habitude. En particulier :

$$(\overline{w},\overline{t})\cdot\sigma = (\overline{w},\overline{t})\overline{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}} = (\overline{-t},\overline{w}),$$

et de même $(w/t)\cdot\tau = -t/(w+t)$.

On note encore $\Sigma_r = \{(\overline{w},\overline{t}),\ 0 \leq w < t,\ (w,t) \neq (1,r)$ et il existe $(v,u),\ 0 \leq v < u\ ,\ 0 \leq (ut - vw) \leq r\}$, et $\mathbb{Z}[\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})]^\sigma$ (respectivement, $\mathbb{Z}[\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})]^\tau$) désigne l'ensemble des éléments de $\mathbb{Z}[\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})]$ stables par l'opération de σ (respectivement, τ). Le symbole $\sum_\sigma$ désignera une somme à valeurs dans $\mathbb{Z}[\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})]^\sigma$, et de même avec τ.

On a la présentation de Manin de $H_1(X_0(p^n)$, pointes ; $\mathbb{Z})$, *i.e.* la suite exacte (voir par exemple [17]) :

$$\mathbb{Z}[\mathbb{P}^1\,(\mathbb{Z}/p^n\mathbb{Z})\,]^\sigma \times \mathbb{Z}[\mathbb{P}^1\,(\mathbb{Z}/p^n\mathbb{Z})\,]^\tau \xrightarrow{\phi_1} \mathbb{Z}[\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})] \xrightarrow{\phi_2} H_1(X_0(p^n),\ \text{pointes}\,;\,\mathbb{Z}) \to 0,$$

avec $\phi_1 : (\Sigma\alpha_x x, \Sigma\beta_x x) \mapsto (\Sigma\alpha_x x + \Sigma\beta_x x)$, et $\phi_2 : \Sigma\lambda_x x \mapsto \Sigma\lambda_x.\xi(x)$.

Dans la suite, on considèrera le graphe $\mathcal{G}$, dont les sommets seront les éléments de $\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$, et les arêtes uniront les éléments des paires de type $\{x, x\cdot\sigma\}$, $\{x, x\cdot\tau\}$ et $\{x, x\cdot\tau^2\}$, pour tout x dans $\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$.

Enfin, de même que dans [19] on prouve avec l'aide de Fouvry le :

Lemme 5.2 *Soit A et B deux intervalles de $\{1, 2, ..., p^n - 1\}$ tel que*

$$|A|.|B| \geq C'_p.p^{3n/2},$$

où $C'_p = 8$ si p est impair, et $C'_2 = 8\sqrt{2}$. Alors il existe $y \in A$ et $z \in B$ tel que $y.z = -1\ mod\ (p^n)$.

(On a prouvé une version moins bonne de ce lemme, utilisant une constante $C'_p = (512\pi^2)/(2\sqrt{2}-1)$, dans [24], lemme 7 ; la forme ici utilisée de ce lemme est obtenue en optimisant les calculs par Oesterlé dans [23].)

5.3 Preuve de la proposition 1.9.

On va donner d'abord deux propositions préliminaires. (Dans toute cette sous-section, $\mathbb{F}$ désigne un corps quelconque.)

Proposition 5.4 *Soient x et S un élément et un sous-ensemble respectivement de $\mathbb{P}^1\,(\mathbb{Z}/p^n\mathbb{Z})$, x non élément de S. Supposons que $x.\sigma$ et $x.\tau$ (ou bien $x.\tau^2$) soient dans la même composante connexe de $\mathcal{G} - (S \cup \{x\})$. Alors l'intersection des sous-groupes de $H_1(X_0(p^n)$, pointes ; $\mathbb{F})$ engendrés l'un par $\xi(x)$ et l'autre par $\xi(S)$, est nulle.*

Preuve. Soit a un élément de l'intersection des deux sous-groupes de l'énoncé : $a = \lambda_x.\xi(x) = \sum_{y\in S} \lambda_y.\xi(y)$, pour des λ dans $\mathbb{F}$; on va montrer sa nullité. La présentation de Manin de $H_1(X_0(p^n)$, pointes ; $\mathbb{F})$ (suite exacte de la sous-section précédente) permet d'écrire la relation :

$$\lambda_x.x - \sum_{y\in S} \lambda_y.y = \sum_\sigma \alpha_z.z - \sum_\tau \beta_z.z \text{ dans } \mathbb{F}[\mathbb{P}^1\,(\mathbb{Z}/\mathrm{p^n}\mathbb{Z})],$$

où on rappelle que les deux sommes à droite sont stables par σ et τ respectivement. Soit $\mathcal{C}$ une composante connexe de $\mathcal{G} - (S \cup \{x\})$. Le coefficient λ_z de tout élément z de $\mathcal{C}$ dans l'égalité précédente est nul, donc $\alpha_z = \beta_z$. De plus, si on considère une arête $\{z, z\sigma\}$ (respectivement, $\{z, z.\tau\}$ ou $\{z, z\tau^2\}$) de $\mathcal{C}$, on voit que $\beta_z = \alpha_z = \alpha_{z.\sigma} = \beta_{z.\sigma}$ (respectivement, $\alpha_z = \beta_z = \beta_{z.\tau} = \alpha_{z.\tau}$ ou $\alpha_z = \beta_z = \beta_{z.\tau^2} = \alpha_{z.\tau^2}$). Donc α_z et β_z sont constants et égaux sur $\mathcal{C}$. En appliquant ceci à la composante connexe de $\mathcal{G} - (S \cup \{x\})$ qui contient $x.\sigma$ et $x.\tau$ (respectivement $x.\tau^2$), on obtient que $\alpha_{x.\sigma}$ est égal à $\beta_{x.\tau}$ (respectivement $\beta_{x.\tau^2}$). Mais alors :

$$\lambda_x = \alpha_x - \beta_x = \alpha_{x.\sigma} - \beta_{x.\tau} = \alpha_{x.\sigma} - \beta_{x.\tau^2} = 0,$$

et $a = 0$. □

Proposition 5.5 *Soit r un entier, $1 < r \leq s_p.d$. Si $p^n > C_p^2.(s_p.d)^6$, alors $\xi(\overline{1/r})$ n'appartient pas au sous-groupe de $H_1(X_0(p^n)$, pointes$; \mathbb{F})$ engendré par $\xi(\Sigma_r)$.*

Preuve. Il suffit de montrer que, si $p^n > C_p^2.(s_p.d)^6$, d'une part $(\overline{1/r})$ n'appartient pas à Σ_r, et d'autre part $(\overline{1/r}).\sigma$ et $(\overline{1/r}).\tau^2$ sont dans une même composante connexe de $\mathcal{G} - (\Sigma_r \cup \{x\})$: une application de la proposition précédente donnera en effet que $(\overline{1/r})$ ne peut appartenir au sous-groupe engendré par $\xi(\Sigma_r)$ que si $\xi(\overline{1/r}) = 0$; ce qui n'est pas, comme le montre la preuve de la même proposition avec pour S l'ensemble vide.

Montrons d'abord que $(\overline{1/r})$ n'appartient pas à Σ_r. Si on a $(\overline{1}, \overline{r}) = (\overline{w}, \overline{t}) \in \Sigma_r$, on peut écrire $(rw - t) = 0 \bmod(p^n)$, ou $t = rw + \lambda.p^n$, avec t, w, λ dans $\mathbb{Z}$ vérifiant $\{0 \leq w < t, (w,t) \neq (1,r)$ et il existe (v,u), $0 \leq v < u$, $1 \leq (ut - vw) \leq r\}$. Remarquons que ces conditions impliquent : $r \geq ut - vw \geq ut - (u-1)(t-1)$ donc $0 \leq w < t \leq r - u + 1 \leq r \leq s_p.d$. Ce qui veut dire que $w \leq 1$ (sinon $\lambda < 0$; mais alors par hypothèse de la proposition $t \leq wr - p^n < r^2 - p^n < 0$). Cela implique $w = 1$ et $t = r$, ce qui est impossible par définition de Σ_r.

Montrons maintenant que $(\overline{1/r}).\sigma$ et $(\overline{1/r}).\tau^2$ sont dans la même composante connexe de $\mathcal{G} - (\Sigma_r \cup \{x\})$. Posons $D = s_p d$. Remarquons que $(\tau\sigma) = \overline{\begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}}$, donc $(\overline{w}, \overline{t}) \cdot \tau\sigma = (\overline{w}, \overline{t}) + \overline{1}$ (et de même $(\overline{w}, \overline{t}) \cdot \sigma\tau^2 = (\overline{w}, \overline{t}) - \overline{1}$). On va construire deux chemins $\mathcal{A}$ et $\mathcal{B}$ sur le graphe, localement de la forme :

$$\begin{array}{ccccc} \ldots \to (\overline{a}, \overline{1}) & \xrightarrow{\tau} & (\overline{-1}, \overline{a+1}) & \xrightarrow{\sigma} & (\overline{a+1}, \overline{1}) \to \ldots , \\ & \longrightarrow & +\overline{1} = \tau\sigma & \longrightarrow & \end{array}$$

dont on va montrer qu'ils vérifient les propriétés suivantes :

- ils contiennent $(\overline{1}, \overline{r}) \cdot \tau^2$ et $(\overline{1}, \overline{r}) \cdot \sigma$ respectivement,

- ils ne rencontrent pas d'éléments de $\Sigma_r \cup \{x\}$,

- et ils contiennent des intervalles (c'est-à-dire des sous-ensembles de forme $\{...(x,1),\ (x+1,1),\ (x+2,1),\ ...\}$) de cardinal supérieur à $(p^n/D) - D - 2$ et $(p^n/D^2) - 2$ respectivement.

Alors par le lemme de théorie analytique des nombres, pour

$$((p^n/D) - D - 2).((p^n/D^2) - 2) \geq C'_p.p^{3n/2},\ i.e.$$

$$p^n \geq C_p^2.D^6,$$

on aura dans $\mathcal{A}$ et dans $\mathcal{B}$ respectivement des éléments y et z tel que $y \cdot \sigma = \frac{-1}{y} = z$ (on explicite ces calculs, et notament le passage de C'_p à C_p, à la fin de la section). De plus $y \cdot \sigma$ sera un élément de $\mathcal{A}$, puisque par construction ce chemin est stable par σ. Les deux chemins s'intersectent donc, ce qu'on voulait démontrer.

Montrons qu'on peut construire ces chemins. (Dans tous les calculs qui suivent, on confond l'écriture d'un entier w et de sa réduction $\overline{w}$, pour alléger les notations.)

Premier chemin : $\mathcal{A}$ partant de $\frac{1}{r}\ \tau^2 = -r - 1$.
1) Si $\frac{w}{t} - (-r-1) = \overline{a}$, avec a choisi dans $\{-p^n + 1, ..., -1, 0\}$, et $\overline{a}$: classe de a mod p^n ($\iff w + t(r+1) = at + b.p^n$, $b \in \mathbb{Z}$).
Si $b = 0$: $t(r+1) - at = -w$: incompatibilité de signes.
Si $b \neq 0$: $|a| = \frac{1}{t}|b.p^n - t(r+1) - w| \geq \frac{(p^n - D(D+1) - D)}{D} \geq \frac{p^n}{D} - D - 2$ (Rappelons qu'on a en effet $r \geq ut - vw \geq ut - (u-1)(t-1)$ et $u + t - 1 \leq r,\ t \leq r - u + 1 \leq r \leq D$).
2) Si $(\frac{w}{t})\sigma - (-r-1) = \frac{-t}{w} + r + 1 = \overline{a},\ a \in \{-p^n + 1, ..., -1, 0\}$; $-t + w(r+1) = aw + bp^n$;
Si $b = 0$: $w(r + 1 - a) = t$; mais $(r + 1 - a) \geq r + 1$, et $0 \leq w < t \leq r$: contradiction.
Si $b \neq 0$, $|a| \geq (\frac{p^n - D(D+1) + D}{D}) \geq \frac{p^n}{D} - D$.
On peut donc "reculer" $(... \ \alpha \xrightarrow{\sigma} . \xrightarrow{\tau^2} \alpha - 1 \xrightarrow{\sigma} . \xrightarrow{\tau^2} \alpha - 2\ ...)$ à partir de $(-r-1)$, et décrire ainsi un chemin contenant un intervalle de cardinal supérieur à $p^n/D\ - D - 2$.
Second chemin. On doit là distinguer deux cas, selon que p divise ou non r (voir **Figure 1**).
a) Si p ne divise pas r, chemin $\mathcal{B}$: on part de $(\frac{1}{r})$ lui même, on recule de même :
1) $\frac{w}{t} - \frac{1}{r} = \overline{a},\ -p^n < a \leq 0 \iff wr - t = art + b.p^n$;
$b = 0$: $t = r(w - at) \Rightarrow a = 0,\ w = 1,\ t = r$: c'est $\frac{1}{r}$ lui-même.
$b \neq 0$: $|a| \geq \frac{p^n - D^2}{D^2}$ de même que plus haut.

2) $-\frac{t}{w}-\frac{1}{r}=\overline{a}$: $-rt-w=awr+b.p^n$;
$\underline{b=0} \Rightarrow r|w$, impossible (car $w \leq r-1$, et : $w=0 \Rightarrow t=0$).
$\underline{b \neq 0} \Rightarrow |a| \geq \frac{p^n}{D^2}-2$.

b) Si p divise r, on a alors que le chemin $\mathcal{B}$ précédent : $\frac{1}{r} \xrightarrow{\sigma\tau^2} \frac{1-r}{r} \xrightarrow{\sigma\tau^2}$ ... est bien de longueur supérieure à $(\frac{p^n}{D^2})$; mais il ne contient pas cette fois d'intervalle, puisque r n'est pas inversible modulo p^n, donc l'action de $\sigma\tau^2$ ne correspond plus à l'addition de (-1) (les k/pl ne sont plus relevables en éléments de $\mathbb{Z}/p^n\mathbb{Z}$). Cependant, le calcul précédent montre que $\frac{r}{r-1}=\frac{1}{r}\cdot\sigma\tau^2\sigma$; et $(r-1)$ est, cette fois, inversible modulo p^n, donc en "avançant" à partir de cet élément et à l'aide de $(\tau\sigma)$, on aura bien un intervalle ; on note $\mathcal{B}'$ ce chemin. On minore encore une fois sa longueur :
1) $\frac{w}{t}-\frac{r}{r-1}=\overline{a} \iff w(r-1)-rt=at(r-1)+b.p^n$ (on écrit cette fois cela avec $0 \leq a \leq p^n-1$).
$\underline{\text{Si } b=0}$: $t\,(r+a(r-1))=w(r-1)$; mais $w<t$, et $a(r-1)+r>r-1$, contradiction.
$\underline{\text{Si } b \neq 0}$: $|a| \geq \frac{p^n}{D^2}-1$.
2) $\frac{w}{t}\cdot\sigma-\frac{r}{r-1}=-\frac{t}{w}-\frac{r}{r-1}=\overline{a} \iff -t(r-1)-rw=aw(r-1)+b.p^n$.
$\underline{b=0}$: $t(r-1)=-w\,(a(r-1)+r)$, contradiction de signes.
$\underline{b \neq 0}$: $|a| \geq \frac{p^n}{D^2}-2$.
Dans chaque cas, on obtient bien que ce second chemin contient un intervalle de cardinal supérieur ou égal à $(p^n/D^2)-2$. Montrons pour finir comment on passe des nombres C'_p du lemme 5.2 aux C_p de la proposition 5.5. On a vu qu'on pouvait prendre $|A| \geq (p^n/D^2)-2$ et $|B| \geq (p^n/D)-D-2$. On a $p^n \geq (C_p^2).D^6$, et $C_p^2 \geq 65$, $s_p \geq 2$, donc $D \geq 6$. Minorons la taille de A : $p^n/D^2 \geq 65.D^4 \geq 84240 = 42120.(2)$, donc $|A| \geq (42119/42120).(p^n/D^2)$. Pour B, on a : $D+2 \leq (4/3).D$, et $p^n/D \geq 65.D^5.D \geq 379080.(D+2)$; donc $|B| \geq (379079/379080).(p^n/D)$. Si on pose $\lambda := (42119/42120).(379079/379080)$, on a donc :

$$|A|.|B| \geq \lambda.p^{2n}/D^3.$$

Pour que les conditions du lemme soient vérifiées, il suffit qu'on ait $\lambda.p^{2n}/D^3 \geq C'_p.p^{3n/2}$, *i.e.* $p^n \geq (C'^2_p/\lambda^2).D^6$, et évidemment C_p a été choisie pour que ça marche. □

Preuve de la proposition 1.9. On peut enfin donner cette preuve : supposons que pour un $r \leq s_p.d$, il existe une relation de liaison : $\sum_{i=1}^{r}\lambda_i T_i\{0,\infty\}=0$ dans $H_1(X_0(p^n)$, pointes ; $\mathbb{F})$, avec $\lambda_r \neq 0$. Alors les formules sur les opérateurs de Hecke de la sous-section précédente permettent de récrire l'égalité ci-dessus :

$$\lambda_r.\xi(\overline{1/r}) = \sum_{y \in \Sigma_r} \mu_y.\xi(y)\,,$$

pour des μ_y éléments de $\mathbb{F}$. Il suffit alors d'appliquer la proposition précédente. □

Remerciements. Je remercie ici Loïc Merel qui m'a suggéré l'idée essentielle

de ce papier, et Bas Edixhoven qui encadre tout ce travail. Merci aussi à Joseph Oesterlé pour l'idée du lemme 1.5.

References

[1] *A.O.L. Atkin, J. Lehner*, Hecke Operators on $\Gamma_0(m)$, Math. Ann. **185** (1970), 134-160.

[2] *D. Bump, S. Friedberg, J. Hoffstein*, Nonvanishing theorems for L-functions of modular forms and their derivatives, Inventiones Mathematicæ **102** (1990), 543-618.

[3] *Robert F. Coleman, Bas Edixhoven*, On the semi-simplicity of the U_p-operator on modular forms, Math. Ann., à paraître.

[4] *Fred Diamond, John Im*, Modular forms and modular curves, Canadian Mathematical Society Conference Proceedings, à paraître.

[5] *B. Edixhoven*, Rational torsion points on elliptic curves over number fields, Séminaire Bourbaki **782** (1993), Astérisque **227** (1995), 209-227.

[6] *A. Grothendieck*, Éléments de géométrie algébrique IV, (Étude locale des morphismes de schémas), Publications mathématiques de l'I.H.E.S. **28** (1965).

[7] *R. Hartshorne*, Algebraic Geometry, GTM **52**, Springer-Verlag.

[8] *S. Kamienny*, Torsion points on elliptic curves and q-coefficients of modular forms, Inventiones Mathematicæ **109** (1992), 221-229.

[9] *S. Kamienny*, Torsion points on elliptic curves over fields of higher degree, International Mathematics Research Notices **6** (1992).

[10] *S. Kamienny, B. Mazur*, Rational torsion of prime order in elliptic curves over number fields, Astérisque (à paraître).

[11] *N. Katz and B. Mazur*, Arithmetic Moduli of Elliptic Curves, Annals of Mathematics Studies **108**, Princeton University Press (1985).

[12] *V.A. Kolyvagin, D.Yu. Logachev*, Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties, Leningrad Math. J., Vol. **1**, number **5** (1990).

[13] *Manin*, A Uniform Bound for p-torsion of Elliptic Curves, Izv. Akad. Nau. CCCP **33** (1969).

[14] *Y. Manin*, Parabolic points and zeta function of modular curves, Math. USSR Izvestija **6** (1972), 19-64.

[15] *B. Mazur*, Modular curves and the Eisenstein ideal, Publications mathématiques de l'I.H.E.S. **47** (1977), 33-186.

[16] *B. Mazur*, Rational Isogenies of Prime Degree, Inventiones Mathematicæ **44** (1978), 129-162.

[17] *Loïc Merel*, Sur quelques aspects géométriques et arithmétiques de la théorie des symboles modulaires, Thèse de doctorat de l'université de Paris VII (1993).

[18] *Loïc Merel*, Universal Fourier expansions of modular forms, *in* On Artin's conjecture for odd 2-dimensional representations, Lecture Notes in Mathematics **1585** (1994), 59-94, Springer-Verlag.

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

[20] *David Mumford*, Abelian Varieties, Oxford University Press (1970).

[21] *M. R. Murty, V. K. Murty*, Mean values of derivatives of modular L-series, Ann. Math. **133** (1991), pages 447-475.

[22] *Joseph Oesterlé*, Torsion des courbes elliptiques sur les corps de nombres, article à paraître.

[23] *J. Oesterlé*, Un lemme de théorie analytique des nombres, à paraître.

[24] *P. Parent*, Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres, prépublication de l'IRMAR (université de Rennes) **95-33**, (1995).

[25] *Grothendieck et al.*, Séminaire de géométrie algébrique du Bois-Marie 7-I (Groupes de monodromie en géométrie algébrique), Lecture Notes in Mathematics **288** (1972), Springer-Verlag.

[26] *Jean-Pierre Serre*, Groupes algébriques et corps de classes, Hermann (1959).

[27] *Goro Shimura*, Introduction to the Arithmetic Theory of Automorphic Functions, Princeton University Press (1971).

Pierre Parent

IRMAR

Université de Rennes I

35 042 RENNES Cédex France

E-mail : parent@campagnarde.univ-rennes1.fr

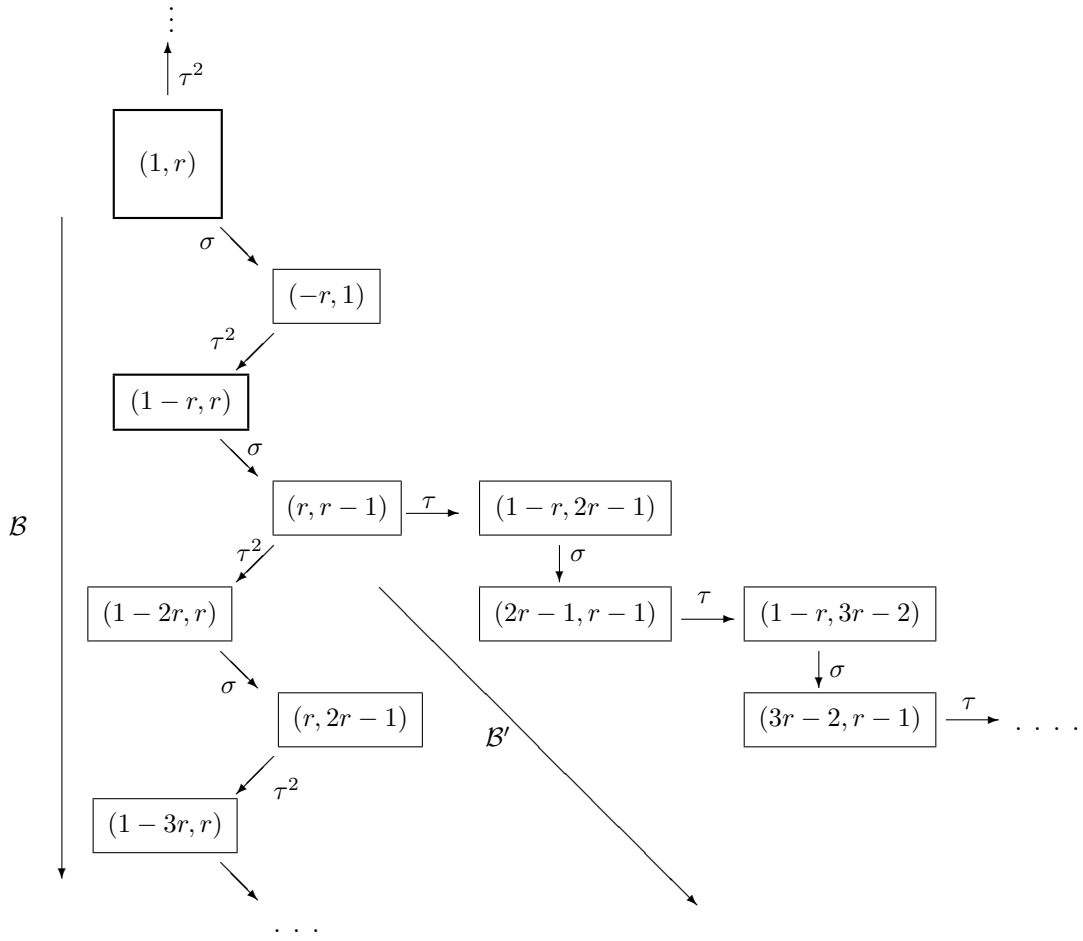
τ^2
$(1,r)$
σ
$(-r,1)$
τ^2
$(1-r,r)$
σ
$(r,r-1)$
τ
$(1-r,2r-1)$
$\mathcal{B}$
τ^2
σ
$(1-2r,r)$
$(2r-1,r-1)$
τ
$(1-r,3r-2)$
σ
σ
$(r,2r-1)$
$\mathcal{B}'$
$(3r-2,r-1)$
τ
. . . .
τ^2
$(1-3r,r)$
. . .

Figure 1