ACTA ARITHMETICA
109.3 (2003)

Sur les modules d'Iwasawa des $\mathbb{Z}_p^*/\{\pm 1\}$-extensions

par

Marc Perret (Toulouse) et Nicolas Saby (Montpellier)

Soit $X_\infty \to \ldots \to X_{n+1} \to X_n \to \ldots \to X_1 \to X_0$ une *tour* au sens de Mazur–Wiles (voir [12]), c'est-à-dire une $\mathbb{Z}_p^*/\{\pm 1\}$-extension d'une courbe algébrique projective et lisse X_0 définie sur le corps fini $\mathbb{F}_q$ à q éléments de caractéristique p, *où chaque point ramifié de* X_0 *l'est totalement*. Cela signifie que X_n est un revêtement galoisien totalement ramifié de X_0, de groupe de Galois isomorphe à $(\mathbb{Z}/p^n\mathbb{Z})^*/\{\pm 1\}$. La limite $X_\infty = \varprojlim X_n$ est alors un revêtement (ramifié) infini de X_0, de groupe de Galois isomorphe à $\mathbb{Z}_p^*/\{\pm 1\}$.

Nous nous proposons de donner quelques estimations sur les composantes isotypiques du module d'Iwasawa de $X_\infty \to X_0$, défini de la façon suivante. Notons $A_n = J_n(\mathbb{F}_q)[p]$ le p-Sylow du groupe des points rationnels sur $\mathbb{F}_q$ de la jacobienne J_n de X_n, et $A = \varprojlim A_n$ le *module d'Iwasawa* de la $\mathbb{Z}_p^*/\{\pm 1\}$-extension. Puisque le revêtement total est galoisien, le groupe quotient $\mathrm{Gal}(X_1/X_0) \simeq \mathbb{F}_p^*/\{\pm 1\}$ agit sur A. On peut donc décomposer A en somme directe de *composantes isotypiques*

$$A = \sum_\chi A^\chi,$$

la somme portant sur les caractères de $\mathbb{F}_p^*/\{\pm 1\}$, c'est-à-dire sur les caractères pairs (i.e. vérifiant $\chi(-1) = 1$) de $\mathbb{F}_p^*$. Puisque le groupe du revêtement total est abélien, le groupe de Galois intermédiaire $\mathrm{Gal}(X_\infty/X_1) \simeq \mathbb{Z}_p$ agit sur chaque composante A^χ, qui se trouve donc être un Λ-module, où Λ désigne *l'anneau d'Iwasawa* $\varprojlim \mathbb{Z}_p[\mathbb{Z}/p^n\mathbb{Z}] \simeq \mathbb{Z}_p[[T]]$. Le corollaire de la proposition 3 de [12, p. 513] affirme que le dual de Pontryagin $M(\chi)$ de A^χ est de type fini et de torsion comme Λ-module. On peut donc lui appliquer le théorème de structure pour les Λ-modules de type-fini (voir par exemple [14]) :

2000 *Mathematics Subject Classification*: Primary 11R23; Secondary 14G15.

THÉORÈME (Iwasawa). *Si M est un Λ-module de type-fini, alors il existe un homomorphisme de Λ-modules*

$$M \to \bigoplus_{i=1}^{r} \Lambda/(p^{m_i}) \times \bigoplus_{j=1}^{s} \Lambda/(f_j(T)^{n_j}) \times \Lambda^t$$

de noyau et conoyau finis, où $r, s, t, m_1, \ldots, m_r, n_1, \ldots, n_s$ sont des entiers positifs, et $f_1, \ldots, f_s$ sont des polynômes non constants d'un certain type de Λ. De plus, ces entiers et ces polynômes sont uniquement déterminés par M.

Les groupes $A_n^\chi = J_n(\mathbb{F}_q)[p]^\chi$ peuvent être calculés à partir de A^χ :

PROPOSITION (Iwasawa). *Si les places ramifiées de X_∞ sur X_0 le sont totalement, alors*

$$A_n^\chi \simeq A^\chi/((1+T)^{p^n} - 1).A^\chi.$$

Un calcul élémentaire montre alors que la croissance du p-rang de $A_n^\chi = J_n(\mathbb{F}_q)[p]^\chi$ est de la forme

$$d_p(J_n(\mathbb{F}_q)[p]^\chi) = r_\chi p^{n-1} + c_\chi$$

pour une constante $c_\chi \geq 0$, où $d_p(G)$ désigne le p-rang d'un groupe fini G et r_χ est le nombre de facteurs de la forme Λ/p^m dans la décomposition d'Iwasawa du dual de Pontryagin $M(\chi)$. Une des questions importantes en théorie d'Iwasawa est l'étude des *invariants d'Iwasawa* μ_χ et λ_χ, où $\mu_\chi = \sum_{i=1}^{r_\chi} m_i \geq r_\chi$ et $\lambda_\chi = \sum_{j=1}^{s_\chi} n_j \deg f_j$. En particulier, la nullité de μ_χ (où, ce qui revient au même, de r_χ) est d'un grand intérêt. L'objet essentiel de cet article est de prouver le théorème suivant :

THÉORÈME 1. *Soit $X_\infty \to X_0$ une $\mathbb{Z}_p^*/\{\pm 1\}$-extension d'une courbe algébrique projective irréductible lisse X_0 de genre $g(X_0)$ définie sur le corps fini $\mathbb{F}_q$. On note ϱ (respectivement $\overline{\varrho}$) le nombre de points fermés (resp. géométriques) de X_0, ramifiés dans X_∞. On suppose que $\varrho > 0$, et que chacun de ces points est totalement ramifié dans X_∞. Soit χ un caractère pair de $\mathbb{F}_p^*$. Alors :*

(i) *L'invariant r_χ est majoré par*

$$2g(X_0) + (\varrho + \overline{\varrho}) - 1.$$

(ii) *L'invariant global $\lambda = \sum_\chi \lambda_\chi$ est minoré par ϱ.*

On peut aussi obtenir une majoration des r_χ à l'aide de la cohomologie étale p-adique en modifiant la technique de Crew dans [3]. Nous en esquisserons les étapes dans la remarque 2 ci-dessous. L'intérêt de la preuve que nous proposons ici est quadruple. Elle donne une majoration meilleure, elle est parfaitement élémentaire, elle donne des résultats pour les corps de nombres (voir la remarque 3), et enfin elle donne un bien meilleur résultat pour

le caractère trivial et les tours d'Igusa (qui sont les prototypes des *tours*) comme l'affirme le théorème 2 suivant. Commençons par rappeler ce que sont les tours d'Igusa.

Lorsque N est un entier premier à p, la *courbe d'Igusa* $\mathrm{Ig}(Np^n)$ de niveau Np^n est le modèle projectif lisse sur le corps premier $\mathbb{F}_p$ à p éléments de la courbe affine représentant (relativement si $N=1$) le problème de module (voir [11], [12] ou [13])

$$S(\text{schéma de caractéristique } p) \to \begin{cases} \text{Classes d'isomorphismes} \\ \text{de courbes elliptiques } E/S, \\ \text{avec un point } P \text{ d'ordre } N \\ \text{et un générateur } Q \text{ de} \\ \text{l'itéré du Verschiebung } V^n. \end{cases}$$

Il s'agit d'un revêtement galoisien de $X_1(N)$ de groupe $(\mathbb{Z}/p^n\mathbb{Z})^*/\{\pm 1\}$ si $N \leq 4$, et $(\mathbb{Z}/p^n\mathbb{Z})^*$ sinon, totalement ramifié en les points supersinguliers de $X_1(N)$, et non ramifiés ailleurs. La limite projective est donc une tour, appellée *tour d'Igusa* au-dessus de la courbe modulaire $X_1(N)$.

Soit $M(p,\chi)$ la limite projective des duaux de Pontryagin des modules $J_{\mathrm{Ig}(p^n)}(\mathbb{F}_p)[p]^\chi$ pour un nombre premier p et un caractère pair χ de $\mathbb{F}_p^*$ donnés. Mazur et Wiles appellent ([12, p. 515]) *Igusa-régulier* un tel couple (p,χ), pour lequel $M(p,\chi)=0$. Ils prouvent alors qu'un couple (p,χ) Igusa-régulier est régulier au sens ordinaire. Réciproquement, ils posent la question ([12, p. 518]) de savoir s'il arrive souvent qu'un couple (p,χ) soit Igusa-irrégulier, bien que classiquement régulier. Le résultat suivant, qui est une conséquence directe du théorème 1(ii) pour $N=1$, apporte une réponse très partielle à cette question. Il affirme par exemple que même si p est régulier au sens ordinaire, il existe au moins un caractère χ pour lequel (p,χ) soit Igusa-irrégulier.

Corollaire. *Pour tout nombre premier p impair, il existe au moins un caractère pair χ de $\mathbb{F}_p^*$, pour lequel le couple (p,χ) soit Igusa irrégulier.*

D'autre part, on peut donner une majoration de la composante triviale du rang $r_{N,1}$ pour ces tours d'Igusa :

Théorème 2. *Pour le caractère trivial 1 de $\mathbb{F}_p^*$, et pour la tour d'Igusa au-dessus de $X_1(N)$, on a la majoration*

$$r_{N,1} \leq s_N$$

où s_N est le nombre de points supersinguliers de $X_1(N)$.

Preuve du théorème 1(i). D'après le théorème de structure des Λ-modules de type fini déjà évoqué, pour n assez grand, le p-rang a_n de $J_n(\mathbb{F}_q)[p]^\chi$ vérifie $a_n = r_\chi p^{n-1} + c_\chi$. Il existe par la théorie du corps de classes un revêtement non ramifié Y_n de X_n, de groupe de Galois isomorphe à $(\mathbb{Z}/p\mathbb{Z})^{a_n}$,

et tel que $\mathrm{Gal}(X_n/X_0)$ agisse sur $\mathrm{Gal}(Y_n/X_n)$ par $\sigma x \sigma^{-1} = x^{\chi(\sigma)}$. Soit P l'un des points fermés ramifiés de X_n. Puisqu'il est non ramifié dans Y_n, son groupe de décomposition est un sous-groupe cyclique de $\mathrm{Gal}(Y_n/X_n) \simeq (\mathbb{Z}/p\mathbb{Z})^{a_n}$. Il est donc trivial ou cyclique d'ordre p. Le revêtement abélien maximal intermédiaire Z_n non ramifié de X_n, de groupe de Galois de la forme $(\mathbb{Z}/p\mathbb{Z})^{b_n}$, où $\mathrm{Gal}(X_n/X_0)$ agisse selon χ, et où de plus les ϱ points ramifiés de X_n sont totalement décomposés, vérifie donc $b_n \geq r_\chi p^{n-1} + c_\chi - \varrho$.

Pour fixer les idées, et par analogie avec le cas des tours d'Igusa, on appelera *supersingulier* les points de X_n (totalement) ramifiés dans la tour.

$$\begin{array}{rcl} & Z_n & \\ \text{non ramifié, supersinguliers totalement decomposés} & \left\{ \begin{array}{c} \\ \downarrow \\ \\ \end{array} \right. & (\mathbb{Z}/p\mathbb{Z})^{b_n} \\ & X_n & \\ \text{supersinguliers totalement ramifiés, non ramifié ailleurs} & \left\{ \begin{array}{c} \\ \downarrow \\ \\ \end{array} \right. & (\mathbb{Z}/p^n\mathbb{Z})^*/\{\pm 1\} \\ & X_0 & \end{array}$$

L'action du groupe cyclique $\mathrm{Gal}(X_n/X_0)$ sur $(\mathbb{Z}/p\mathbb{Z})^{b_n}$ par conjugaison est déterminée par la matrice M image dans $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})^{b_n} = \mathrm{GL}_{b_n}(\mathbb{Z}/p\mathbb{Z})$ d'un de ses générateurs. Puisque $M^{\frac{p-1}{2}p^{n-1}} = I$, par réduction de Jordan, M s'écrit dans une base convenable comme une matrice diagonale par blocs $M = \mathrm{diag}(A_1, \ldots, A_{c_n})$, où chaque A_i est un bloc élémentaire de la forme

$$A_i = \begin{pmatrix} \zeta & 1 & 0 & \ldots & 0 \\ 0 & \zeta & 1 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \ldots & 0 & \zeta & 1 \\ 0 & \ldots & \ldots & 0 & \zeta \end{pmatrix},$$

pour une certaine racine $(p-1)/2$-ième de l'unité ζ dans $\mathbb{F}_p$ commune aux A_i, précisément puisque l'on ne considère qu'une composante isotypique.

Nous affirmons que A_i est de taille $\leq p^{n-1}$. Supposons en effet le contraire. Le coefficient sur la première ligne et la $(p^{n-1}+1)$-ième colonne de

$$I = A_i^{\frac{p-1}{2}p^{n-1}} = (\zeta I + J)^{\frac{p-1}{2}p^{n-1}}$$

(où J est la matrice avec des zéros partout, sauf sur la seconde diagonale où il y a des 1) serait alors égal au coefficient binômial $C^{p^{n-1}}_{\frac{p-1}{2}p^{n-1}}$, qui n'est pas nul modulo p, ce qui est une contradiction ! Par la minoration ci-dessus de b_n, on a donc $c_n p^{n-1} \geq b_n \geq r_\chi p^{n-1} + c_\chi - \varrho$, c'est-à-dire (pourvu que n soit assez grand)

$$c_n \geq r_\chi.$$

Considérons alors la courbe T_n correspondant au quotient maximal $(\mathbb{Z}/p\mathbb{Z})^{c_n}$ de $\mathrm{Gal}(Z_n/X_n)$, sur lequel $\mathrm{Gal}(X_n/X_0)$ agisse par homothéties. On est en présence d'une extension

$$1 \to \mathrm{Gal}(T_n/X_n) = (\mathbb{Z}/p\mathbb{Z})^{c_n} \to \mathrm{Gal}(T_n/X_0) \to \mathbb{Z}\Big/\frac{p-1}{2}p^{n-1}\mathbb{Z} \to 1,$$

où le quotient $\mathbb{Z}/\frac{p-1}{2}p^{n-1}\mathbb{Z}$ agit par $\overline{k} \mapsto \zeta^k \,\mathrm{Id}$ sur le noyau abélien $(\mathbb{Z}/p\mathbb{Z})^{c_n}$. Soit σ un élément de $\mathrm{Gal}(T_n/X_0)$, dont la restriction $\overline{\sigma}$ à X_n engendre le quotient $\mathrm{Gal}(X_n/X_0) \simeq \mathbb{Z}/\frac{p-1}{2}p^{n-1}\mathbb{Z}$.

$$\sigma \in \mathrm{Gal}(T_N/X_0) \quad \left(A \left(\begin{array}{c} T_n \\ \downarrow \\ X_n \\ \downarrow \\ X_1 \\ \downarrow \\ X_0 \end{array} \right) \right. \begin{array}{ll} \\ \\ \\ \\ \\ \\ \end{array} \begin{array}{l} \\ E \simeq (\mathbb{Z}/p\mathbb{Z})^{c_n} \\ \\ \langle \overline{\sigma}^{(p-1)/2} \rangle \simeq \mathbb{Z}/p^{n-1}\mathbb{Z} \\ \\ \langle \sigma_{|_{X_1}} \rangle \simeq (\mathbb{Z}/p\mathbb{Z})^*/\{\pm 1\} \end{array}$$

Notons E le groupe de Galois $\mathrm{Gal}(T_n/X_n)$. Puisque σ agit sur E par $\zeta \,\mathrm{Id}_E$, $\sigma^{(p-1)/2}$ y agit trivialement. Cela signifie que le groupe $\mathrm{Gal}(T_n/X_1)$ est un p-groupe *abélien* A. On considère alors l'un des ϱ points fermés supersinguliers de X_1. Puisqu'il est totalement ramifié dans l'extension cyclique intermédiaire X_n, puis totalement décomposé dans T_n, il a un groupe de décomposition cyclique d'ordre p^{n-1} dans $\mathrm{Gal}(T_n/X_1)$. Les groupes de décompositions des points supersinguliers de X_1 engendrent donc un sous-groupe, que l'on notera D, de $A = \mathrm{Gal}(T_n/X_1)$, engendré par ϱ éléments. La courbe U_n fixée par D est donc un revêtement p-élémentaire de X_1 *non ramifié* (puisque T_n n'est ramifiée sur X_0 qu'en les supersinguliers), de groupe de Galois isomorphe à $(\mathbb{Z}/p\mathbb{Z})^{d_n}$ avec

$$d_n \geq c_n - \varrho \geq r_\chi - \varrho.$$

On en déduit que U_n est un revêtement *modérément ramifié* de X_0, ramifié seulement en les supersinguliers, et où au moins un point fermé est totalement décomposé. Par le théorème de Grothendieck (voir [5, chapitre XIII, cor. 2.12]), le groupe de Galois $\mathrm{Gal}(U_n/X_0)$ peut donc être engendré par $2g(X_0) + \overline{\varrho} - 1$ éléments.

Mais ce groupe est par le théorème de Burnside le produit semi-direct de $\mathrm{Gal}(U_n/X_1)$ par $\mathrm{Gal}(X_1/X_0)$. Un élément de $\mathrm{Gal}(U_n/X_0)$ peut donc être représenté par un couple $(x, \sigma^k_{|_{X_1}}) \in (\mathbb{Z}/p\mathbb{Z})^{d_n} \times \mathrm{Gal}(X_1/X_0)$, la loi de groupe étant

$$(x, \sigma^k_{|_{X_1}}) \times (y, \sigma^l_{|_{X_1}}) = (x + \zeta^k y, \sigma^{k+l}_{|_{X_1}}).$$

On observe que le projeté sur le premier facteur d'un produit est dans l'espace vectoriel engendré par les projetés des deux termes. En particulier,

toute partie génératrice de $\mathrm{Gal}(U_n/X_0)$ a au moins d_n éléments. Il en résulte que

$$r_\chi - \varrho \leq d_n \leq 2g(X_0) + \overline{\varrho} - 1,$$

ce qui n'est autre que l'assertion (i).

Preuve du théorème 2. Supposons que cette majoration soit fausse, et reprenons mot pour mot la preuve précédente jusqu'à l'introduction de la courbe T_n. Dans le cas qui nous occupe, $X_0 = X_1(N)$ est la réduite modulo p de la courbe modulaire pour le sous-groupe de congruence $\Gamma_1(N)$, X_1 est la courbe d'Igusa $\mathrm{Ig}(Np)$ de niveau Np et ϱ est le nombre de points supersinguliers de $X_1(N)$, traditionnellement noté $\varrho = s_N$. Puisqu'on considère le caractère trivial, $\mathrm{Gal}(T_n/X_0)$ est alors extension d'un groupe abélien par un groupe cyclique *avec action triviale*. Il est donc lui même abélien, ce qui implique qu'il ne peut être engendré par moins de c_n éléments (avec toujours $c_n \geq r_{N,1}$). D'autre part, les s_N points supersinguliers de $X_0 = X_1(N)$ ont un groupe de décomposition cyclique dans $\mathrm{Gal}(T_n/X_0)$, puisqu'ils sont totalement ramifiés dans l'extension cyclique X_n/X_0, puis totalement décomposés dans T_n/X_n. Le sous-groupe D_1 de $\mathrm{Gal}(T_n/X_0)$ engendré par les supersinguliers de $X_1(N)$ est donc strictement contenu dans $\mathrm{Gal}(T_n/X_0)$, puisqu'on a supposé que la majoration était fausse. La courbe fixée par D_1 est donc un revêtement *non ramifié* de $X_1(N)$, *non-trivial*, où les supersinguliers de $X_1(N)$ sont *totalement décomposés*. Soit $X(N)$ la réduite modulo p de la courbe modulaire pour le sous-groupe de congruence $\Gamma(N)$. Par produit fibré avec $X(N)$ au-dessus de $X_1(N)$, cela fournit un revêtement de $X(N)$ du même type, toujours non trivial puisque $X(N)$ est de degré N premier à p sur $X_1(N)$. Cela est en contradiction avec le théorème suivant :

Théorème (Ihara, [8]). *Soit N un entier premier à p. Alors $X(N)$ ne possède pas de revêtement galoisien non ramifié et non trivial, où les points supersinguliers soient totalement décomposés.*

Preuve du théorème 1(ii). Soit $n \geq 1$. On note pour simplifier G_n le groupe de Galois de X_n sur X_0 et $P(X_n)$ le groupe des diviseurs principaux sur X_n. La suite exacte

$$1 \to P(X_n) \to \mathrm{Div}^0(X_n) \to J_n(\mathbb{F}_q) \to 1$$

donne

$$1 \to P(X_n)^{G_n} \to \mathrm{Div}^0(X_n)^{G_n} \to J_n(\mathbb{F}_q)^{G_n},$$

d'où une composée de deux injections

$$\mathrm{Div}^0(X_n)^{G_n}/P(X_n)^{G_n} \to J_n(\mathbb{F}_q)^{G_n} \to J_n(\mathbb{F}_q). \tag{1}$$

D'autre part, il y a deux suites exactes

$$1 \to P(X_n)^{G_n}/P(X_0) \to \mathrm{Div}^0(X_n)^{G_n}/P(X_0) \to \mathrm{Div}^0(X_n)^{G_n}/P(X_n)^{G_n} \to 1 \tag{2}$$

et

$$\mathrm{Div}^0(X_n)^{G_n}/P(X_0) \to \mathrm{Div}^0(X_n)^{G_n}/\mathrm{Div}^0(X_0) \to 1. \tag{3}$$

Mais :

1) Puisque $\mathrm{Div}^0(X_n)^{G_n}/\mathrm{Div}^0(X_0) \simeq \prod_{P\in X_0 \text{ ram dans } X_n} \mathbb{Z}/e_P\mathbb{Z}$, et puisque $X_n \to X_0$ est totalement ramifié en ϱ points avec indice de ramification $e = \frac{p-1}{2}p^{n-1}$, on obtient, par (3), que

$$\left(\mathbb{Z}\Big/\frac{p-1}{2}p^{n-1}\mathbb{Z}\right)^{\varrho} \text{ est un quotient de } \mathrm{Div}^0(X_n)^{G_n}/P(X_0). \tag{4}$$

2) D'autre part, la suite exacte

$$1 \to \mathbb{F}_q^* \to \mathbb{F}_q(X_n)^* \to P(X_n) \to 1$$

donne

$$1 \to \mathbb{F}_q^* \to \mathbb{F}_q(X_0)^* \to P(X_n)^{G_n} \to H^1(G_n, \mathbb{F}_q^*) \to H^1(G_n, \mathbb{F}_q(X_n)^*) = 1,$$

c'est-à-dire

$$1 \to P(X_0) \to P(X_n)^{G_n} \to H^1(G_n, \mathbb{F}_q^*) \to 1.$$

Le H^1 en jeu est calculé pour l'action triviale de G_n sur $\mathbb{F}_q^*$, donc

$$H^1(G_n, \mathbb{F}_q^*) = \mathrm{Hom}(G_n, \mathbb{F}_q^*).$$

Puisque $G_n = \mathbb{Z}/\frac{p-1}{2}p^{n-1}\mathbb{Z}$,

$$P(X_n)^{G_n}/P(X_0) = H^1(G_n, \mathbb{F}_q^*) \simeq \mathrm{End}\left(\mathbb{Z}\Big/\frac{p-1}{2}\mathbb{Z}\right) \text{ ne dépend pas de } n. \tag{5}$$

Lorsque l'on injecte ces deux points (4) et (5) dans la suite exacte (2), on obtient que, à un groupe borné près, $\mathrm{Div}^0(X_n)^{G_n}/P(X_n)^{G_n}$, et donc aussi $J_n(\mathbb{F}_q)$, est au moins aussi gros que $\left(\mathbb{Z}/\frac{p-1}{2}p^{n-1}\mathbb{Z}\right)^{\varrho}$. Mais il est aisé de s'assurer, à l'aide de la proposition d'Iwasawa rappelée dans l'introduction, que l'invariant global λ n'est autre que le nombre de facteurs cycliques du p-Sylow de $J_n(\mathbb{F}_q)$ dont les ordres tendent vers l'infini avec n. Il en résulte bien que λ est minoré par ϱ.

Remarque 1 (Tours de Shimura et de Mazur–Wiles). Le théorème 2 ne se généralise pas au cas général des tours faute d'un théorème à la Ihara. Cependant, toujours d'après Ihara, un tel théorème existe pour les courbes

de Shimura (voir [9]) : étant donné une courbe de Shimura S sur $\mathbb{F}_p$, il existe un groupe fini G_S tel que tout revêtement galoisien X de S non ramifié, où les points supersinguliers sont totalement décomposés, ait pour groupe de Galois un quotient de G_S. Par exemple, le théorème de Ihara énoncé lors de la preuve du théorème 2 affirme que pour la courbe modulaire $X(N)$ de niveau N premier à p réduite modulo p, on a $G_{X(N)} = 1$. On peut fabriquer une tour au sens de Mazur–Wiles d'Igusa–Shimura à partir des composantes d'Igusa des courbes de Shimura (cf. [1] ou [2]). On pourrait donc donner une majoration de l'invariant r d'une tour d'Igusa–Shimura pour le caractère trivial en fonction du p-rang de G_S. Malheureusement, la preuve de l'existence de G_S est totalement ineffective, ce qui ôte tout intérêt à une telle majoration.

Remarque 2 (Majoration de r_χ à l'aide de la cohomologie p-adique). On ne reprend que partiellement les notations de [3, pp. 34 et 35] : soit S/k un schéma séparé de type fini sur un corps algébriquement clos k de caractéristique p et G un p-groupe fini agissant librement sur S, de quotient S/G. On suppose qu'un groupe Δ fini d'ordre premier à p agit aussi sur S. Il agit donc sur la suite spectrale de Hochschild–Serre. Si les actions de G et de Δ commutent, il y a alors pour chaque caractère χ de Δ une suite spectrale pour les composantes isotypique $H^i_c(S, \mathbb{Q}_p)^\chi$, qui montre que

$$H^i_c(S/G, \mathbb{Q}_p)^\chi = (H^i_c(S, \mathbb{Q}_p)^\chi)^G.$$

Supposons maintenant que Y soit revêtement ramifié d'une courbe algébrique projective est lisse X sur k, galoisien de groupe de Galois un p-groupe G, et que Δ agisse sur X en commutant à G. Si C est l'une de ces deux courbes, la χ-partie du p-rang de C est définie par $p^\chi_C := \dim_{\mathbb{Q}_p} H^i_c(C, \mathbb{Q}_p)^\chi$. La suite exacte d'excision jointe au théorème 1.5 de Crew et à la remarque précédente montre alors, de la même façon que l'on montre le corollaire 1.8 de [3] :

Proposition 1. *Dans la situation précédente* :

(i) *Si χ n'est pas le caractère trivial, alors*

$$p^\chi_X = (\sharp G) p^\chi_Y.$$

(ii) *Pour le caractère trivial* 1, *on a*

$$p^1_X - 1 = (\sharp G)(p^1_Y - 1) + \sum_{x \in X^{\mathrm{ram}}} (e_x - 1).$$

On rappelle que si C est de genre g_C, on a $p^\chi_C \leq p_C \leq g_C$. Revenons alors à notre situation des tours $X_\infty \to X_0$ sur le corps premier $\mathbb{F}_p$, et considérons un caractère non trivial χ de $\Delta = \mathrm{Gal}(X_1/X_0) = \mathbb{F}_p^*/\{\pm 1\}$. La proposition 1 appliquée au revêtement ramifié X_n de X_1, puis la formule de

Riemann–Hurwitz appliquée au revêtement *modérément ramifié* X_1 de X_0 donnent, en supposant pour simplifier que p est impair,

$$r_\chi p^{n-1} + c_\chi \leq p^\chi_{X_n} = p^{n-1} p^\chi_{X_1} \leq p^{n-1} g(X_1)$$

avec

$$2g(X_1) - 2 = \frac{p-1}{2}\,(2g(X_0) - 2) + \overline{\varrho}\left(\frac{p-1}{2} - 1\right).$$

On obtient donc la majoration

$$r_\chi \leq \frac{p-1}{2}\, g(X_0) + \frac{p-3}{4}\,(\overline{\varrho} - 2),$$

qui est moins bonne que celle du théorème 1 dès que $p > 5$.

Remarque 3 (Le cas des corps de nombres). La technique de la preuve du théorème 2 fonctionne très bien dans le cas des corps de nombres. En revanche, la preuve de (ii) ne s'adapte pas du tout à ce cas. Pour ce qui concerne la preuve de (i), il manque malheureusement un analogue du théorème de Grothendieck. Cet analogue a cependant été conjecturé par Harbater (dans [6] dans le cas où $K = \mathbb{Q}$, et dans [7] dans le cas général) : pour un corps de nombres K et un idéal entier I de K, notons $\pi^t_A(K, I)$ le *groupe fondamental algébrique modéré* de $\operatorname{Spec} \mathcal{O}_K[I^{-1}]$, c'est-à-dire l'ensemble des groupes finis apparaissant comme groupe de Galois d'une extension modérément ramifiée de $\mathbb{Q}$ et non ramifiée hors de I.

Conjecture (Harbater). *Il existe une constante absolue C telle que pour tout corps de nombres K de genre $g(K)$ (au sens de Weil), ayant $r(K)$ plongements réels, et pour tout idéal entier I de K, tout élément de $\pi^t_A(K, I)$ peut être engendré par $2g(K) + r(K) - 1 + C + \log N_{K/\mathbb{Q}}(I)$ éléments.*

Nous rappelons que le groupe de Galois de $\bigcup_n K(\exp(2\imath\pi/p^n))/K$ est de la forme $\mathbb{F}_p^*/G \times \mathbb{Z}_p$ pour un sous-groupe G de $\mathbb{F}_p^*$ convenable.

Théorème 3. *Soit p un nombre premier impair, K un corps de nombres, G un sous-groupe fini de $\mathbb{F}_p^*$ et $K = K_0 \subset K_1 \subset \ldots \subset K_\infty$ une $\mathbb{F}_p^*/G \times \mathbb{Z}_p$-extension de K. On suppose que les ϱ idéaux premiers $\mathcal{P}_1, \ldots, \mathcal{P}_\varrho$ de K au-dessus de p sont totalement ramifiés dans K_∞. Soit χ un caractère de $\mathbb{F}_p^*/G$. Alors*

(i) *Sous la conjecture d'Harbater, les invariants $r_{p,\chi}$ sont majorés par*

$$2g(K) + (\varrho + [K : \mathbb{Q}] \log p) - 1 + (r(K) + C).$$

(ii) *Pour le caractère trivial $\chi = 1$, l'invariant $r_{p,1}$ est majoré par*

$$\varrho + d_p(\mathcal{C}l(K)/\langle \overline{\mathcal{P}}_1, \ldots, \overline{\mathcal{P}}_\varrho \rangle).$$

Comparons ce théorème 3 aux théorèmes 1 et 2. Dans l'assertion (i) du théorème 3, la quantité $[K : \mathbb{Q}] \log p = \log N_{[K:\mathbb{Q}]}(p\mathcal{O}_K)$ est l'analogue pour les corps de nombres du degré du diviseur réduit de ramification

$\overline{\varrho} = \deg(\sum_{i=1}^{\varrho} P_i) = \sum_{i=1}^{\varrho} \deg P_i$ de la situation géométrique. Dans cette même assertion, le terme supplémentaire $r(K)+C$ provient de la conjecture d'Harbater. Quant à l'assertion (ii), le terme correctif $d_p(\mathcal{C}l(K)/\langle\overline{\mathcal{P}}_1,\ldots,\overline{\mathcal{P}}_\varrho\rangle)$ est l'analogue du p-rang du groupe G_S dont il a été question dans la remarque 1 pour les courbes de Shimura.

Notons que pour $p=2$, un énoncé analogue vaut en adjoignant la racine quatrième de l'unité $\imath$ à K. Par exemple, l'assertion (ii) montre que les invariants r_p de la $\mathbb{Z}_p$-extension cyclotomique de $\mathbb{Q}[\sqrt[3]{2}]$ sont inférieurs à 3 pour tout p. Rappelons que, d'après Ferrero et Washington (voir [4]), les invariants μ_p (où, ce qui revient au même, les invariants r_p) des $\mathbb{Z}_p$-extensions cyclotomiques des extensions abéliennes de $\mathbb{Q}$ sont nuls. Cette nullité a d'ailleurs été conjecturée par Iwasawa pour tous les corps de nombres. D'autre part, il existe d'après Iwasawa (voir [10]) des $\mathbb{Z}_p$-extensions (non cyclotomiques !) de corps de nombres, dont les invariants μ (et donc aussi r) sont non nuls.

Remerciements. Nous tenons à remercier le rapporteur pour ses remarques très utiles.

Références

[1] K. Buzzard, *Integral models of certain Shimura curves*, Duke Math. J. 87 (1997), 591–612.

[2] H. Carayol, *Sur la mauvaise réduction des courbes de Shimura*, Compositio Math. 59 (1986), 151–230.

[3] R. Crew, *Etale p-covers in characteristic p*, ibid. 52 (1984), 31–45.

[4] B. Ferrero and L. Washington, *The Iwasawa invariants μ_p vanishes for abelian number fields*, Ann. of Math. 109 (1979), 377–395.

[5] A. Grothendieck, *Revêtements étales et groupe fondamental*, *SGA I*, Lecture Notes in Math. 224, Springer, 1971.

[6] D. Harbater, *Galois groups with prescribed ramification*, dans : Arithmetic Geometry, N. Childress and W. Jones (eds.), Contemp. Math. 174, Amer. Math. Soc., Providence, RI, 1994, 35–60.

[7] —, communication privée.

[8] Y. Ihara, *On modular curves over finite fields*, dans : Discrete Subgroups of Lie Groups and Applications to Moduli, Oxford, 1975, 161–202.

[9] —, *Congruence relations and fundamental groups*, J. Algebra 75 (1982), 445–451.

[10] K. Iwasawa, *On the μ-invariants of Z_l-extensions*, dans : Number Theory, Algebraic Geometry and Commutative Algebra in honor to Y. Akizuki, Kinokuniya, Tokyo, 1973, 1–11.

[11] N. Katz and B. Mazur, *Arithmetic Moduli of Elliptic Curves*, Ann. of Math. Stud. 108, Princeton Univ. Press, 1985.

[12] B. Mazur and A. Wiles, *Analogies between function fields and number fields*, Amer. J. Math. 105 (1983), 507–521.

[13] N. Saby, *Théorie d'Iwasawa géométrique : un théorème de comparaison*, J. Number Theory 59 (1996), 225–247.

[14] L. Washington, *Introduction to Cyclotomic Fields*, Grad. Texts in Math. 83, Springer, New York, 1982.

GRIMM
Université de Toulouse II le Mirail
5 Allées Antonio Machado
31 058 Toulouse Cedex, France
E-mail: perret@univ-tlse2.fr

Département de Mathématiques
Université de Montpellier II
case 051
Place Eugène Bataillon
34 095 Montpellier Cedex 5, France
E-mail: saby@math.univ-montp2.fr

Reçu le 17.9.2001
et révisé le 11.7.2002 (4106)