数理解析研究所講究録
第 603 巻 1987 年 60-71

Nombres de classes

dans certaines extensions infinies.

par R. Gillard (Grenoble)

Le but de cette conférence † est de discuter comment le théorème de **Washington**,prolongé par **Friedman**, (*cf.* [W1] et [F]) peut se transposer dans le cadre des extensions abéliennes d'un corps quadratique imaginaire. Pour plus de détails, je renvoie à mon article [Gi3].

Rappelons brièvement la situation cyclotomique. Pour l un nombre premier, notons $\mathbf{Q}_{l^\infty}$ l'unique $\mathbf{Z}_l$–extension de $\mathbf{Q}$; elle est contenue dans la réunion des corps cyclotomiques $\mathbf{Q}(\zeta_{l^n})$, pour n dans N, ζ_{l^n} racine de 1 d'ordre l^n. Soient pour s entier $l_1,\ldots,l_s$ des nombres premiers distincts fixés; posons $\Lambda := \prod l_i$ et $\Lambda^{\mathbf{n}} := \prod {l_i}^{n_i}$, si $\mathbf{n} := (n_1,\ldots,n_s)$. On note $\mathbf{Q}_{\Lambda^\infty}$ l'extension composée des $\mathbf{Q}_{l_i^\infty}$. Pour $F/\mathbf{Q}$ une extension abélienne, notons F_{Λ^∞} l'extension composée $F.\mathbf{Q}_{\Lambda^\infty}$ et $F_{\Lambda^{\mathbf{n}}}$, $\mathbf{n}$ comme ci-dessus, la sous-extension de F_{Λ^∞}/F de degré $\Lambda^{\mathbf{n}}$. Fixons un nombre premier p et notons $e(\mathbf{n})$ l'exposant de p dans le nombre de classes de $F_{\Lambda^{\mathbf{n}}}$. D'après [F],on a:

0.1. THEORÈME. — *Avec les notations précédentes, fixons Λ et F: si p ne divise pas Λ, l'exposant $e(\mathbf{n})$ est borné lorsque $\mathbf{n}$ parcourt $\mathbf{N}^s$.*

Ce théorème redonne celui de [W1] lorsque $s = 1$. En utilisant le théorème de Ferrero–Washington, [FW] ($\mu = 0$; c'est le cas $s = 1$ dans 0.2), Friedman en déduit:

0.2. THÉORÈME. — *Avec les notations précédentes, si p est égal à l_1, il existe des entiers $\lambda \geq 0, \nu \in \mathbf{Z}, m_1,\ldots,m_s \in \mathbf{N}$ tels que pour tout $\mathbf{n} = (n_1,\ldots,n_s)$ vérifiant $n_1 \geq m_1,\ldots,n_s \geq m_s$, on ait:*

(0.2.1) $$e(\mathbf{n}) = \lambda.n_1 + \nu\ .$$

De plus la limite projective naturelle des groupes de classes des extensions $F_{\Lambda^{\mathbf{n}}}$ pour $\mathbf{n} \in \mathbf{N}^s$ est isomorphe à $(\mathbf{Z}_p)^\lambda$.

† Je remercie sincèrement la fondation **Taniguchi** qui l'a permise

1. Résultats.

1.0. — Plaçons nous maintenant dans la situation "elliptique" en choisissant un corps quadratique imaginaire K d'anneau des entiers R. Pour chaque idéal premier $\underline{l}$ de R soit $R_{\underline{l}}$ le complété de R en $\underline{l}$ et $K_{\underline{l}^\infty}$ l'unique $R_{\underline{l}}$-extension de K non ramifiée en dehors de $\underline{l}$; si $\underline{l}$ diffère de son conjugué $\underline{l}'$, notre $K_{\underline{l}^\infty}$ est la $\mathbf{Z}_l$-extension de K non ramifiée en dehors de $\underline{l}$; si $\underline{l} = \underline{l}'$, c'est la $\mathbf{Z}_l \times \mathbf{Z}_l$ extension de K. Soient, pour s entier, des idéaux premiers distincts $\underline{l}_1, \ldots, \underline{l}_s$ de R de F et Λ leur produit. Pour $\mathbf{n} := (n_1, \ldots, n_s)$, posons $\Lambda^{\mathbf{n}} := \prod \underline{l}_i^{n_i}$. Soit R_Λ le complété Λ-adique de R: il s'identifie au produit des $R_{\underline{l}_i}$; notons K_{Λ^∞} la composée des extensions $K_{\underline{l}_i^\infty}$; on a $\mathrm{Gal}(K_{\Lambda^\infty}/K) \simeq R_\Lambda$.

Soient F une extension abélienne de K et F_{Λ^∞} l'extension composée $F.K_{\Lambda^\infty}$. Choisissons maintenant un nombre premier p et un diviseur premier de $\overline{p}$ dans R; on suppose que

HYPOTHÈSE. — *p est $\neq 2$ ou 3 et est non ramifié dans $K/\mathbf{Q}$.*

Pour chaque extension L/K notons $M(L)/L$ la plus grande p-extension abélienne non ramifiée en dehors de $\underline{p}$. Soit $X(L)_\tau$ la partie de torsion de $X(L) := \mathrm{Gal}(M(L)/L)$ et $x(L)$ l'exposant de p dans son ordre. On peut se demander:

QUESTION. — *Quelles sont les conditions sur F et Λ qui assurent que*

(1.0.1) le nombre $x(L)$ reste borné lorsque F parcourt l'ensemble des sous-extensions de F_{Λ^∞}/F.

Le résultat suivant incite à la prudence:

1.1. THÉORÈME. — *Soit $l \neq p$ un nombre premier; prenons $\Lambda = (l)$. Considérons $H^{(p)}$ la plus grande p-extension non ramifiée de K: elle possède une infinité d'extensions cycliques $F/H^{(p)}$ de degré p, abéliennes sur K, et ne vérifiant pas (1.0.1).*

Démonstration. — (esquisse: *cf.* aussi [I1]) On considère les extensions

$F/H^{(p)}$ comme ci-dessus qui sont ramifiées en suffisamment d'idéaux premiers au dessus de nombres premiers inertes dans K: on constate que ces idéaux se décomposent totalement dans une $\mathbf{Z}_l$-sous-extension de K_{Λ^∞}. On applique alors une formule des classes invariantes (similaire à celle de [Gr]) pour les extensions $L/L \cap H^{(p)}_{\Lambda^\infty}$. On a remplacé K par $H^{(p)}$ pour assurer l'existence de tels F. □

Notre résultat essentiel donne une condition suffisante pour avoir (1.0.1):

1.2. THÉORÈME. — *On suppose que p ne divise pas Λ. Avec les notations de 1.0, et l'hypothèse sur p, si l'extension F_{Λ^∞}/F est pro-cyclique,alors (1.0.1) est vraie.*

Imposer que F_{Λ^∞}/F soit pro-cyclique revient à demander que l'idéal Λ soit premier à son conjugué: les idéaux $\underline{l}_i$ sont alors de degré 1 et ne sont pas conjugués deux à deux.

Démonstration. — On déduit 1.2 du théorème 3.2.4 ci dessous et de critères de Kummer (*cf.* [Gi2] et [R2] ou pour plus de détails [Gi3]).□

En suivant la méthode de Friedman et en s'appuyant sur le résultat $\mu = 0$ de [Gi2], on déduit assez facilement de 1.2 l'analogue de 0.2:

1.3 THÉORÈME. — *On suppose l'extension F_{Λ^∞}/F pro-cyclique et on note $F_{\Lambda^{\mathbf{n}}}$ la sous-extension de degré $N(\Lambda^{\mathbf{n}})$. Alors si $\underline{p} = \underline{l}_1$ et si p vérifie l'hypothèse de (1.0), la limite projective naturelle des $X(F_{\Lambda^{\mathbf{n}}})$ est un $\mathbf{Z}_p$-module libre de rang fini. En notant λ son rang, on trouve qu'il existe des entiers $\nu \in \mathbf{Z}$ et $m_1, \ldots, m_s \in \mathbf{Z}$ tels que*

$$x(F_{\Lambda^{\mathbf{n}}}) = \lambda . n_1 + \nu \ ,$$

pour $\mathbf{n}$ dans $\mathbf{N}^s$ vérifiant $n_1 \geq m_1, \ldots, n_s \geq m_s$.

Démonstration. — Si L/K est une extension infinie, posons

$$M(L) := \bigcup M(L'),\ X_\tau(L) := \varprojlim X(L')_\tau = \mathrm{Gal}(M(L)/L_{\underline{p}^\infty}) \ ,$$

où dans la réunion et la limite projective L' parcourt l'ensemble des sous-extensions finies de L. Notons Λ_0 le produit de $\underline{l}_i$ pour $i \geq 2$ et F_n (resp. F'_n) la sous

extension de degré p^n de $F_{\underline{p}^\infty}/F$ (resp. $F_{\Lambda^\infty}/F_{\Lambda_0^\infty}$). On remarque tout d'abord que le théorème 1.2 implique la finitude de $X_\tau(F'_n)$, et on en déduit que $X_\tau(F_{\Lambda^\infty})$ est un $\mathbf{Z}_p[[T]]$-module de torsion (on a identifié $T-1$ à un générateur fixé de $\mathrm{Gal}(F_{\Lambda^\infty}/F_{\Lambda_0^\infty})$. Comme dans [F], on ramène facilement son étude à celle de $X_\tau(L)$ pour un L compris entre $F_{\underline{p}^\infty}$ et F_{Λ^∞} et $[L : F_{\underline{p}^\infty}]$ fini. On vérifie que $L = F''_{\underline{p}^\infty}$ pour une extension F'' convenable.La formule du début se déduit de la théorie d'Iwasawa appliquée à F'' (*cf.* [W2] 13.5), compte tenu du théorème 3.4 ($\mu = 0$) de [Gi2].□

1.4. — Les énoncés précédents sont encore valides en remplaçant $X(L)$ par le p-groupe des classes de L, cela en est une conséquence facile si p est décomposé; pour p inerte c'est un peu plus délicat.

2. Un résultat d' indépendance algébrique.

Comme dans [Gi2],[S1] et [S2], la démonstration repose sur un résultat d'indépendance algébrique . On prend R et Λ comme en 1.0.

2.1. — Soit E une courbe elliptique à multiplications complexes par R définie sur un corps k de caractéristique première à Λ. Notons $E[\Lambda^\infty]$ les points de E à valeurs dans une clotûre algébrique $\overline{k}$ de k et annulés par une puissance (variable) de Λ.

2.2. PROPOSITION. — *Soit W une partie infinie de $E[\Lambda^\infty]$ et $\beta_1, \ldots, \beta_s$ des éléments de R_Λ linéairement indépendants sur R; alors les points $P(w)$ de composantes $\beta_i.w$, pour w dans W, dans le produit E^s de s copies de E, forment un ensemble dense pour la topologie de Zariski.*

Démonstration. — La fermeture de l'ensemble des $P(w)$ est une sous-variété abélienne de E^s. Si ce n'était pas E^s lui-même, les $P(w)$ seraient dans le noyau d'un morphisme surjectif de variétés abéliennes $E^s \to E$, ce qui fournirait une relation de dépendance entre les β_i.□

2.3. COROLLAIRE. — *Soient W une partie infinie de $E(\Lambda^\infty)$ et des δ_j, pour $j = 1,\dots,m$ dans R_Λ^*, ainsi que des fonctions rationnelles f_j sur E. Si les δ_j représentent des classes distinctes dans le quotient $R_\Lambda^*/R_\Lambda^* \cap R$ et si la somme $\sum f_j \circ \delta_j$ est nulle sur W, alors les fonctions f_j sont constantes.*

Démonstration. — Il suffit de reprendre celle de [S1].□

3. Etude d'une famille infinie de nombres de Bernoulli-Hurwitz.

3.1. Notations complémentaires. — Soient $K = \mathbf{Q}(\sqrt{d})$ notre corps quadratique imaginaire ($d < 0$ est le discriminant), et $\underline{p}$ comme en 1.0; on identifie les nombres algébriques dans $\mathbf{C}$ et $\mathbf{C}_p$ (complété d'une clotûre algébrique $\overline{\mathbf{Q}}_p$ de $\mathbf{Q}_p$) à l'aide d'inclusions $\overline{\mathbf{Q}} \subset \mathbf{C}$ et $\overline{\mathbf{Q}} \subset \mathbf{C}_p$ fixées: ceci définit un prolongement v à $\overline{\mathbf{Q}}$ de la valuation $\underline{p}$-adique de K compatible avec la valuation de $\mathbf{C}_p$ que l'on note aussi v et que l'on normalise par $v(p) = 1$. Pour toute extension L de $\mathbf{Q}$ ou $\mathbf{Q}_p$, on note $R(L)$ son anneau d'entiers. On note $\overline{\underline{p}}$ l'idéal maximal de $R(\mathbf{C}_p)$. On pose $R := R(K)$.

Soit E une courbe elliptique admettant R comme anneau d'endomorphismes. Pour $a \in R$, on note $[a]$ l'endomorphisme correspondant. On suppose que E est définie sur H, le corps de Hilbert de K, et a bonne réduction en les diviseurs premiers de $\underline{p}$.

Pour $\mathcal{L} := R.\Omega$, un réseau convenable, on a le paramétrage de Weierstrass

$$z \to (X,Y) := (\wp(z,\mathcal{L}), \wp'(z,\mathcal{L}))\ . \tag{3.1.1}$$

Pour λ un point de torsion de E, on note $z(\lambda) \in \mathbf{C}$ un nombre complexe le représentant par (3.1.1). Comme toujours, on utilise une fonction θ, $\theta(z,\mathcal{L})$ que l'on tord avec une combinaison linéaire d'idéaux de R, $\alpha = \sum \alpha(\mathbf{a})\ \mathbf{a}$ telle que

$$\alpha(\mathbf{a}) \in \mathbf{Z}\ , \sum \alpha(\mathbf{a}) = \sum \alpha(\mathbf{a}).N(\mathbf{a}) = 0\ , \tag{3.1.2}$$

où $N(\mathbf{a})$ est la norme de $\mathbf{a}$, pour obtenir une fonction elliptique F_α, rationnelle sur H : on définit F_α sur $\mathbf{C}$ par sa composée $\Theta(z,\alpha)$ avec (3.1.1):

$$\Theta(z,\alpha) := \prod_{\mathbf{a}} \prod_{\lambda} \left(\wp(z,\mathcal{L}) - \wp(z(\lambda),\mathcal{L})\right)^{12.\alpha(\mathbf{a})}\ , \tag{3.1.3}$$

où dans le produit interne λ parcourt un système de représentants $\neq 0$ de la a-torsion de E modulo l'action de ± 1. On a

$$F_\alpha \circ [a] = F_{\alpha(a)} \,. \tag{3.1.4}$$

Soit D la dérivation invariante $\frac{d}{dz}$ sur E: elle est rationnelle sur H car elle s'écrit encore $D = Y\,dX$; ainsi $D \log \Theta(z, \alpha)$ est la fonction rationnelle sur E:

$$D \log F_\alpha = \sum_{\mathbf{a}} \sum_{\lambda} 12.\alpha(\mathbf{a}) \frac{Y}{X - X(\lambda)} \,. \tag{3.1.5}$$

Soit $\mathbf{g}$ un idéal de R et choisissons un générateur sur R, $\rho_\mathbf{g}$ de la $\mathbf{g}$-torsion $E(\mathbf{g})$ de E. Si $\mathbf{g}$ est premier à Λ, on prend $\rho_{\mathbf{g}\Lambda^n} = \rho_\mathbf{g} + \rho_{\Lambda^n}$.

On note $Cl(\mathbf{g})$ (resp. $H_\mathbf{g}$) le groupe (resp. le corps) de classes de rayon $\mathbf{g}$, $\mu(\mathbf{g})$ le groupe des racines de 1 dans K congrues à 1 modulo $\mathbf{g}$ et $e(\mathbf{g})$ son ordre. Le nombre $\Theta(\rho_\mathbf{g}, \alpha)$ est une unité elliptique; son image par l'automorphisme d'Artin $[\mathbf{b}, H_\mathbf{g}/K]$ est donné,*cf.* [R1] §4.2 prop. 9 cor., par:

$$[\mathbf{b}, H_\mathbf{g}/K]\, \Theta(\rho_\mathbf{g}, \alpha) = \Theta(\rho_\mathbf{g}, \alpha\,\mathbf{b}) \,. \tag{3.1.6}$$

Soit ν un caractère de Dirichlet de K de conducteur $\mathbf{g}$: par la loi de réciprocité, on l'identifiera à un caractère de $\mathrm{Gal}(H_\mathbf{g}/K)$ ou même de $\mathrm{Gal}((H_\mathbf{g})_{\Lambda^\infty}/K)$. Si ν est modérément ramifié en $\underline{p}$, son conducteur est de la forme $\mathbf{g}$ ou $\mathbf{g}\,\underline{p}$ pour $\mathbf{g}$ premier à $\underline{p}$. On voit facilement qu'il existe un entier $n = n(\nu) \in [1, N(\underline{p}) - 1]$ tel que pour a dans R congru à 1 modulo $\mathbf{g}$, on ait:

$$\nu((a)) \equiv a^n \bmod \overline{\underline{p}} \,. \tag{3.1.7}$$

D'après (3.1.7), n est divisible par $e(\mathbf{g})$.

Pour $k \in \mathbf{N}$, et $k \geq 0$, on note $LF_\alpha^{(k)}$ la fonction rationnelle de E/H définie par la fonction complexe $\frac{D^k}{(k-1)!} \log F_\alpha$. De (3.1.4), on déduit

$$LF_{\alpha(b)}^{(k)} = b^k\, LF_\alpha^{(k)} \circ [b] \,. \tag{3.1.8}$$

Remarquons l'intégralité de $LF_\alpha^{(k)}$ en $\underline{p}$ pour $k \in [1, N(\underline{p}) - 1]$, *cf.* [K] si p est inerte dans K. Si le conducteur de ν est $\mathbf{g}$ ou $\mathbf{g}\,\underline{p}$, on déduit de (3.1.7) que pour $n = n(\nu)$,

$$\nu^{-1}(\mathbf{b})\, LF_{\alpha\mathbf{b}}^{(n)}(\rho_\mathbf{g}) \equiv LF_\alpha^{(n)}(\rho_\mathbf{g}) \bmod \overline{\underline{p}} \,, \tag{3.1.9}$$

si $\mathbf{b}$ est de la forme (b) avec $b \equiv 1 \bmod \mathbf{g}$. On peut par ailleurs exprimer ces nombres au moyen des valeurs spéciales de séries d'Eisenstein ajustées (*cf.* [Gi2] 2.4.4)

$$LF_{\alpha}^{(n)}(\rho_{\mathbf{g}}) = 12\,(-1)^{n-1} \sum_{\mathbf{a}} \alpha(\mathbf{a})\, E_n^*(\rho_{\mathbf{g}}, \mathbf{a}^{-1}\mathcal{L})\,. \tag{3.1.10}$$

3.2. Nombres de Bernoulli-Hurwitz. — Soit ν un caractère de Dirichlet modérément ramifié en $\underline{p}$: on peut écrire la somme:

$$B_{\alpha}(\nu) := \sum \nu^{-1}(\mathbf{b})\; LF_{\alpha\mathbf{b}}^{(n)}(\rho_{\mathbf{g}})\,. \tag{3.2.1}$$

où $\mathbf{b}$ parcourt un système de représentants de $Cl(\mathbf{g})$ premiers à $\underline{p}$ et $n = n(\nu)$; $B_{\alpha}(\nu) \bmod \overline{\underline{p}}$ est indépendant du système choisi, *cf.* (3.1.9). Dans le cas où $n = N(\underline{p}) - 1$ (cas non ramifié en $\underline{p}$), on utilise aussi les nombres

$$b_{\alpha}(\nu) := \sum \nu^{-1}(\mathbf{b})\, \log_p F_{\alpha\mathbf{b}}(\rho_{\mathbf{g}})\,, \tag{3.2.2}$$

où $\log_p$ est le logarithme calculé dans $\overline{\mathbf{Q}}_p$, relié à $B_{\alpha}(\nu)$ par une congruence.

3.2.3. Conditions sur α. — On suppose que les idéaux $\mathbf{a}$ tels que $\alpha(\mathbf{a}) \neq 0$ sont premiers à $6\underline{p}\mathbf{g}\Lambda$. On suppose aussi que α n'a pas tous ses coefficients $\alpha(\mathbf{a})$ divisibles par p.

Notons $\mathrm{Gal}(K_{\Lambda^\infty}/K)^*$ le groupe des caractères de $\mathrm{Gal}(K_{\Lambda^\infty}/K)$. Notre résultat principal est le suivant:

3.2.4. THÉORÈME. — *Si Λ et Λ' sont premiers entre eux et premiers à p et si χ est un caractère de Dirichlet modérément ramifié en $\underline{p}$, l'ensemble*

$$M(\chi) := \{\varphi \in \mathrm{Gal}(K_{\Lambda^\infty}/K)^* \mid B_{\alpha}(\varphi\chi) \equiv 0 \bmod \overline{\underline{p}}\}$$

est fini.

La proposition suivante joue un rôle capital:

3.2.5. PROPOSITION. — *Un automorphisme $\sigma \in Gal(\overline{\mathbf{Q}}/H)$ agit sur le nombre algébrique $B_{\alpha}(\nu)$ en vérifiant la congruence:*

$$\sigma B_{\alpha}(\nu) = c(\sigma)\, B_{\alpha}(\sigma\nu) \bmod \overline{\underline{p}}\,,$$

où $\sigma\nu$ est le caractère déduit de ν par action sur ses valeurs, et $c(\sigma)$ est une unité dans $\overline{\mathbf{Q}}_p$.□

3.3. Trace du caractère $\nu = \varphi\chi$. — Choisissons deux entiers N et M ayant les mêmes facteurs premiers que Λ, avec $N \geq M$ et assez grands pour que

$$\text{(3.3.1)} \qquad \mathrm{Gal}(H(\mu_N)/H(\mu_M)) \simeq \mathrm{Gal}(\mathbf{Q}(\mu_N)/\mathbf{Q}(\mu_M)) \ ,$$

et notons $Tr_{N/M}$ l'opérateur $\sum\sigma$ où σ parcourt $\mathrm{Gal}(H(\mu_N)/H(\mu_M))$.

3.3.2. LEMME. — *Si ν est un caractère d'ordre M, on a:*

$$Tr_{N/M}(\nu(\mathfrak{b})) = \begin{cases} [\mathbf{Q}(\mu_N) : \mathbf{Q}(\mu_M)]\ \nu(\mathfrak{b}) & \text{si } \nu(\mathfrak{b})^M = 1, \\ 0 & \text{sinon.} \end{cases}$$

Ce lemme évident est important car suivant l'astuce de [W1], il permet de réduire des caractères de Dirichlet à des fonctions caractéristiques pour des sous-ensembles de $Cl(\mathfrak{g}\Lambda^{\mathfrak{n}})$.

Voici un premier exemple d'utilisation. Notons $B'_\alpha(\nu)$ le nombre défini comme $B_\alpha(\nu)$ mais en restreignant la sommation aux idéaux $\mathfrak{b}$ tels que

$$\text{(3.3.3)} \qquad [\mathfrak{b}, H \cap K_{\Lambda^\infty}/K] = 1 \ ;$$

comme en (3.2.5), on a:

$$\text{(3.3.4)} \qquad \sigma B'_\alpha(\nu) \equiv c(\sigma)\, B'_\alpha(\sigma\nu) \bmod \underline{\overline{p}} \ .$$

3.3.5. PROPOSITION. — *Pour que $\mathcal{M}(\chi)$ soit fini, il suffit qu'il en soit de même pour*

$$\mathcal{M}'(\chi) := \{\varphi \in \mathrm{Gal}(K_{\Lambda^\infty}/K)^* \mid B'_\alpha(\varphi\chi) \equiv 0 \bmod \underline{\overline{p}}\}$$

Démonstration. — En appliquant 3.3.2,on déduit de la congruence d'un $B_\alpha(\varphi\chi)$ des congruences analogues portant sur des sommes analogues où $\mathfrak{b}$ parcourt un système des représentants de $Cl(\mathfrak{g}\Lambda^{\mathfrak{n}})$ (où $\mathfrak{g}\Lambda^{\mathfrak{n}}$ est la partie première à $\underline{p}$ du conducteur de $\varphi\chi$) tels que $\mathfrak{b}$ induise l'identité sur $K_{(M)}$ (on désigne par $K_{(M)}$ la sous-extension de degré M de K_{Λ^∞}/K et on choisit l'ordre N de $\varphi\chi$

et M assez grands). On termine en sommant sur un système de représentants de $\mathrm{Gal}(K_{(M)}/K_{\Lambda^\infty} \cap H)$.□

3.4. Comment $B'_\alpha(\varphi\chi)$ dépend de φ. — Le passage de $B_\alpha(\varphi\chi)$ à $B'_\alpha(\varphi\chi)$ va nous permettre d'isoler φ dans les sommations.Posons

$$\Lambda^{(\mathbf{n})} = \mathrm{pgcd}\,(\Lambda, 2)\,\Lambda^{\mathbf{n}}\,\Lambda\,.$$

On suppose maintenant que φ est de conducteur exactement $\Lambda^{(\mathbf{n})}$ et que le conducteur de χ divise $\mathbf{g}\underline{p}\Lambda^{(0)}$: ceci est possible par une translation éventuelle sur $\mathcal{M}'(\chi)$. On peut prendre comme système de représentants de $Cl(\mathbf{g}\Lambda^{(\mathbf{n})})$ le système des

$$\mathbf{b} = \mathbf{c}.i(x)\,, \tag{3.4.1}$$

où $\mathbf{c}$ parcourt un système de représentants de $Cl(\mathbf{g}\Lambda^{(0)})$; si x appartient à $1+\Lambda^{(0)}$, on définit $i(x)$ comme étant un idéal (x') avec $x' \equiv 1 \bmod \mathbf{g}\Lambda^{(0)}$ et $x' \equiv x \bmod \Lambda^{(\mathbf{n})}$: sa classe dans $Cl(\mathbf{g}\Lambda^{(\mathbf{n})}$ est bien définie. On écrit simplement $\varphi(x)$ pour $\varphi(i(x))$. On observe que $n(\varphi\chi) = n(\chi)$ donc est indépendant de φ. Pour $\mathbf{b}$ vérifiant (3.3.3), il existe un β unique dans $1 + \Lambda^{(0)}$ tel que pour tout φ dans $\mathrm{Gal}(K_{\Lambda^\infty}/K)^*$, on ait:

$$\varphi(\mathbf{b}) = \varphi(\beta)\,. \tag{3.4.2}$$

Bien sur si $\mathbf{b} = \mathbf{c}.i(x)$, on doit prendre $\beta = \gamma.x$ avec $\gamma = \gamma(\mathbf{c})$ défini par la condition analogue à 3.4.2.

Après quelques calculs, on obtient:

$$B'_\alpha(\varphi\chi) = \sum_z \varphi^{-1}(z) \sum_{\mathbf{c}} \chi^{-1}(\mathbf{c})\; LF^{(n)}_{\alpha\mathbf{c}}(\rho_{\mathbf{g}} + z\,\gamma^{-1}\,\rho_{\Lambda^{(\mathbf{n})}})\,, \tag{3.4.1}$$

où z parcourt $1 + \Lambda^{(0)}/1 + \Lambda^{(\mathbf{n})}$ et $\mathbf{c}$ un ensemble $\mathcal{R}$ d'idéaux en bijection par $\mathbf{c} \to [\mathbf{c}, H_{\mathbf{g}\Lambda^{(0)}}/K]$ avec $\mathrm{Gal}(H_{\mathbf{g}\Lambda^{(0)}}/H \cap K_\infty)$.

3.5. Transformation de Fourier. — Pour ρ un point de torsion annulé par $\Lambda^{(\mathbf{n})}$, on introduit le caractère *additif* sur R:

$$\lambda_\rho(a) := \exp 2\pi i \mathrm{Tr}(a\frac{z(\rho)}{\Omega\sqrt{d}})\,. \tag{3.5.1}$$

Si ρ est primitif, on a ainsi une dualité sur $R/\Lambda^{(\mathbf{n})}$ définie par $(x,y) \to \lambda_\rho(x.y)$. Pour f fonction sur $R/\Lambda^{(\mathbf{n})}$, on peut introduire sa transformée de Fourier

$$\mathcal{F}_\rho(f)(y) := \sum_x \lambda_\rho(x.y)\, f(x)\ , \tag{3.5.2}$$

somme sur $R/\Lambda^{(\mathbf{n})}$.

Soit $\varphi \in \mathrm{Gal}(K_{\Lambda^\infty}/K)^*$, un caractère de conducteur $\Lambda^{(\mathbf{n})}$. Choisissons deux éléments $\mathbf{n}$ et $\mathbf{m}$ de $\mathbf{N}^s$ assez gros (*i.e.* toutes leurs composantes sont assez grosses): les entiers $N := N(\Lambda^{(\mathbf{n})})$ et $M := N(\Lambda^{(\mathbf{m})})$ vérifient la condition (3.3.1). On a le résultat suivant qui nous débarrassera de φ:

3.5.3. PROPOSITION. — *Supposons que $M'(\chi)$ contienne un caractère φ de conducteur $\Lambda^{(\mathbf{n})}$, alors le point de torsion $\rho_{\Lambda^{(\mathbf{n})}}$ vérifie*

$$\sum_\varepsilon \lambda_\varepsilon(1) \sum_{\mathbf{c}} \chi^{-1}(\mathbf{c})\ LF^{(n)}_{\alpha\mathbf{c}}(\gamma^{-1}\rho_{\Lambda^{(\mathbf{n})}} + \gamma^{-1}\varepsilon + \rho_{\mathbf{g}}) \equiv 0 \bmod \underline{\mathfrak{p}}\,,$$

où dans la somme ε parcourt $E[\Lambda^{(\mathbf{m})}]$.

Enonçons quelques lemmes utiles pour la démonstration de 3.5.3.

3.5.4. LEMME. — *Si $\varphi \in Gal(K_{\Lambda^\infty}/K)^*$ est un caractère de conducteur $\Lambda^{(\mathbf{n})}$, il existe un point ω de $\Lambda^{(\mathbf{n})}$-torsion, primitif,tel que*

$$\varphi(1+T) = \lambda_\omega(T)\ ;$$

pour tout T dans $\Lambda^{(\mathbf{n}-\mathbf{m})}$.□

En fait quitte à remplacer φ par un conjugué, on peut même prendre $\omega = -\rho_{\Lambda^{(\mathbf{n})}}$ dans 3.5.4. C'est dans le résultat suivant que l'hypothèse que Λ et Λ' sont premiers entre eux s'avère indispensable car elle permet d'exprimer le noyau de $\varphi^{\mathbf{m}}$ dans R_Λ^* et d'appliquer 3.3.2.

3.5.5. LEMME. — *Si $x_0 \in 1+\Lambda^{\mathbf{m}}$ et si x dans $x_0\,\eta\,(1+\Lambda^{(\mathbf{n}-\mathbf{m})})$, avec $\eta \in \mu(R_\Lambda)$ le groupe des racines de 1 dans R_Λ, on a*

$$Tr_{N/M}\ \varphi(x/x_0) = [\mathbf{Q}(\mu_N) : \mathbf{Q}(\mu_M)]\ \ \lambda_\omega(\frac{x}{\eta} - x_0)\ .$$

C'est 0 si x est dans R_Λ mais pas dans $x_0\,\mu(R_\Lambda)\,(1+\Lambda^{(\mathbf{n}-\mathbf{m})})$.□

3.6. Démonstration de 3.5.3.(esquisse). — Posons

$$G(z) := \sum_{\mathbf{c}} \chi^{-1}(\mathbf{c})\ LF^{(n)}_{\alpha\mathbf{c}}(z\gamma^{-1}\rho_{\Lambda(\mathfrak{n})} + \rho_{\mathbf{g}})\ . \tag{3.6.1}$$

Partant de (3.4.5), en utilisant (3.3.5),on obtient

$$\sum_{z} \sigma\varphi^{-1}(z)\ G(z) \equiv 0 \bmod \underline{p}\ . \tag{3.6.2}$$

pour σ dans $\mathrm{Gal}(H(\mu_N)/H(\mu_M))$. Multipliant le membre de gauche de (3.6.2) par $\sum_x \lambda_\rho(x)\ \sigma\varphi(x)$ (somme sur un système de représentants de $R/\Lambda^{(\mathfrak{n})}$; on a posé $\rho = \rho_{\Lambda(\mathfrak{n})}$) et remplaçons x par xz dans la sommation: nous faisons apparaitre $\mathcal{F}_\rho(\sigma\varphi)$. La proposition s'obtient en faisant une combinaison linéaire astucieuse g des fonctions $\sigma\varphi$ pour avoir une fonction $\mathcal{F}_\rho(g)$ très simple, en utilisant 3.5.5. □

3.7. Démonstration de 3.2.4. — Nous allons utiliser le résultat du §2, mais auparavant il nous (encore!) transformer la congruence de 3.5.3. Posons $\mathbf{c} = \mathbf{b}.(x)$ où b parcourt un ensemble $\mathcal{R}_1$ d'idéaux de R premiers à $\Lambda^{(0)}$, ensemble en bijection par $\mathbf{b} \to [\mathbf{b}, H_{\Lambda(0)}/H_{\Lambda(0)} \cap K_{\Lambda^\infty}]$ avec $\mathrm{Gal}(H_{\Lambda(0)}/H_{\Lambda(0)} \cap K_{\Lambda^\infty})$ † et où x parcourt un système de représentants $\mathcal{R}_2$ tous congrus à 1 mod $\Lambda^{(0)}$ de $(R/\mathbf{g})^*$. Ainsi les nombres β et γ associés à $\mathbf{b}$ et à $\mathbf{c}$ par (3.4.4) vérifient $\gamma = \beta.x$. En utilisant 3.1.8, la congruence de 3.5.3 s'écrit donc

$$\sum_{\mathbf{b}\in\mathcal{R}_1} \chi^{-1}(\mathbf{b})\ G_{\mathbf{b}}(\beta^{-1}.\rho_{\Lambda(\mathfrak{n})}) \equiv 0 \bmod \underline{p}\ . \tag{3.7.1}$$

où $G_{\mathbf{b}}$ est la fonction rationnelle sur E:

$$G_{\mathbf{b}}(P) := \sum_{x\in\mathcal{R}_2} \sum_{\varepsilon\in E[\Lambda^{\mathbf{m}}]} \lambda_\varepsilon(1)\ \chi^{-1}((x))\ x^n\ LF^{(n)}_{\alpha\mathbf{b}}(x\rho_{\mathbf{g}} + \beta^{-1}\varepsilon + P)\ . \tag{3.7.2}$$

Nous allons utiliser le lemme facile:

3.7.3. LEMME. — *Deux éléments* $\mathbf{b}$ *et* $\mathbf{b}'$ *de* $\mathcal{R}_1$ *donnent des nombres* β *et* β' *de* $1 + \Lambda^{(0)}$ *dont les classes dans* $R^*_\Lambda/R^*_\Lambda \cap R$ *sont distinctes.*□

Supposons que $M'(\chi)$ soit infini : d'après 3.5.3, l'ensemble W des points de Λ^∞-torsion w tels que

$$\sum \chi^{-1}(\mathbf{b})\ G_{\mathbf{b}}(\beta^{-1}w) \equiv 0 \bmod \underline{p}$$

† on notera que $K_{\Lambda^\infty} \cap H_{\mathbf{g}\Lambda(0)} = K_{\Lambda^\infty} \cap H_{\Lambda(0)} = K_{\Lambda^\infty} \cap H$.

est infini. D'après 2.3, et 3.7.3, toutes les fonctions $G_{\mathfrak{b}}$ se réduisent modulo $\overline{p}$ en des constantes. Or ceci est absurde, comme on le constate en calculant explicitement le diviseur polaire de $G_{\mathfrak{b}}$.□

Bibliographie

[F] FRIEDMAN E. — *Ideal class group in basic $\mathbf{Z}_{p_1} \times \ldots \times \mathbf{Z}_{p_s}$-extensions of abelian number fields*, Invent. Math., **65** (1982), 425-440.

[FW] FERRERO B. ET WASHINGTON L. — *The Iwasawa invariant vanishes for abelian number fields*, Ann. of Math., **109** (1979), 377-395.

[Gi1] GILLARD R. — *Séries d'Eisenstein et critère de Kummer*, Sém. Th. nombres, Paris,1981-1982,p. 59-72, Birkhaüser: Boston–Basel–Stuttgart, 1983.

[Gi2] GILLARD R. — *Fonctions L p-adiques des corps quadratiques...*, J. reine angew. Math., **328** (1985), 76-91.

[Gi3] GILLARD R. — Croissance du nombre de classes dans des $\mathbf{Z}_l$ extensions liées aux corps quadratiques imaginaires. A paraître probablement aux Math. Annalen,1987.

[GR] GILLARD R. ET ROBERT G. — *Groupes d'unités elliptiques*, Bull. Soc. Math. France, **107** (1979), 305-317.

[Gr] GRAS G. — *Groupe de Galois de la p-extension abélienne p-ramifiée maximale d'un corps de nombres*, J. reine angew. math., **333** (1982), 86-132.

[I1] IWASAWA K. — *On the μ invariant of $\mathbf{Z}_l$-extensions in Number Theory, algebraic geometry and commutative algebra,p.1-11*, Kinokuniya,Tokyo, 1973.

[I2] IWASAWA K. — *On Z_l-extensions of algebraic number fields*, ann. of Math., **98** (1973), 246-326.

[K] KATZ N. — *Divisibilities,congruences and Cartier duality*, J. Fac Soc. Univ. Tokyo, **28** (1982), 667-678.

[R1] ROBERT G. — *Unités elliptiques*, Bull. Soc. Math. France mém., **36** (1973), 77 p.

[R2] ROBERT G. — *Nombres de Hurwitz et unités elliptiques*, Ann. Sc. Ec. Norm. Sup., **11** (1978), 297–389.

[S1] SINNOTT W. — *On the μ-invariant of the Γ-tansform of a rational function*, Invent. Math., **75** (1984), 273-282.

[S2] SINNOTT W. — On a theorem of L. Washington. Exposé aux journées arithmétiques de Besançon,1985.

[W1] WASHINGTON L. — *The non p-part of the class number in a cyclotomic $\mathbf{Z}_p$-extension*, Invent. Math., **49** (1978), 87-97.

[W2] WASHINGTON L. — *Introduction to Cyclotomic fields*, Graduate text in Math., Springer Verlag, New-York, 1982.

Université de Grenoble I

Institut Fourier
Laboratoire de Mathématiques
associé au CNRS
BP 74
38402 Saint Martin d'Hères
France