B. Oriat
Nagoya Math. J.
Vol. 81 (1981), 45-56

# ANNULATION DE GROUPES DE CLASSES REELLES

BERNARD ORIAT

## Introduction

Il est bien connu que le groupe des classes relatives d'une extension abélienne du corps des rationnels est annulé par tout élément entier de l'idéal de Stickelberger. Soit $\ell$ un nombre premier impair. Nous montrons dans les pages qui suivent qu'un certain groupe de $\ell$-classes réelles $\mathscr{H}(\chi)$, associé à un caractère $\chi$ d'ordre $g$ et considéré comme $\boldsymbol{Z}_\ell^{(g)}$-module est annulé par la valeur en 1 de la fonction $L$ $\ell$-adique: $L_\ell(1, \chi)$, ou bien par un multiple bien défini de cette valeur. Pour l'essentiel, la méthode employée consiste à transposer par "Spiegelungssatz" le théorème d'annulation de Stickelberger. Cette méthode a été introduite par Georges Gras dans [3]. La démonstration donnée ici semble un peu plus simple et le résultat obtenu plus général: on ne fait plus ici l'hypothèse "$\ell$ premier à $g$".

## 1. Notations et définitions

On désigne par $\ell$ un nombre premier impair. Soit $\chi$ un caractère résiduel d'ordre $g$ et de conducteur $f$, réel, différent du caractère unité. On note $K/\boldsymbol{Q}$ l'extension cyclique, de corps de base le corps des rationnels $\boldsymbol{Q}$, correspondant à $\chi$. Nous voulons dire par là,que si l'on considère $\chi$ comme un homomorphisme de Gal $(\boldsymbol{Q}^{(f)}/\boldsymbol{Q}) = (\boldsymbol{Z}/f\boldsymbol{Z})^*$ dans le groupe des racines $g^{\text{ème}}$ de l'unité, alors le noyau de $\chi$ est le groupe de Galois Gal $(\boldsymbol{Q}^{(f)}/K)$. On désigne par $G$ le groupe de Galois de $K/\boldsymbol{Q}$. Le caractère $\chi$ peut aussi être considéré comme un homomorphisme de $G$ dans $\boldsymbol{Q}_\ell^{(g)*}$, groupe multiplicatif du corps $\boldsymbol{Q}_\ell^{(g)}$; ce corps est le corps obtenu en ajoutant au corps $\ell$-adique $\boldsymbol{Q}_\ell$, les racines $g^{\text{ème}}$ de l'unité. On désigne par $\chi_1$ le prolongement $\boldsymbol{Z}_\ell$-linéaire de $\chi$ à $\boldsymbol{Z}_\ell[G]$. Le noyau de $\chi_1$ est un idéal de $\boldsymbol{Z}_\ell[G]$ qui peut être défini à l'aide d'un idempotent de l'algèbre $\boldsymbol{Q}_\ell[G]$ de la façon suivante: Soit $\psi$ le caractère $\ell$-adique issu de $\chi$, c'est-à-dire la trace de $\chi$ dans l'extension

Received April 26, 1979.

$\boldsymbol{Q}_\ell^{(g)}/\boldsymbol{Q}_\ell$. Soit $1_\psi = (1/|G|)\sum_{\tau\in G}\psi(\tau^{-1})\tau$ l'idempotent de $\boldsymbol{Q}_\ell[G]$ associé à $\psi$. Alors $\operatorname{Ker}\chi_1$ est l'ensemble des $x$ de $\boldsymbol{Z}_\ell[G]$ tels que $x1_\psi = 0$. Une autre façon de définir $\operatorname{Ker}\chi_1$ est utilisée dans la suite: désignons par $\sigma$ un générateur de $G$ et par $P(Y)$ le polynôme $\prod(Y-\chi(\sigma)^u)$, $u$ parcourant le groupe $\operatorname{Gal}(\boldsymbol{Q}_\ell^{(g)}/\boldsymbol{Q}_\ell)$. Il s'agit du polynôme cyclotomique $\ell$-adique ayant $\chi(\sigma)$ comme racine. L'idéal $\operatorname{Ker}\chi_1$ est l'idéal de $\boldsymbol{Z}_\ell[G]$ engendré par $P(\sigma)$. Remarquons aussi que $\chi_1$ a pour image $\boldsymbol{Z}_\ell^{(g)}$, anneau des entiers de $\boldsymbol{Q}_\ell^{(g)}$. On a donc un isomorphisme d'anneaux entre $\boldsymbol{Z}_\ell[G]/\operatorname{Ker}\chi_1$ et $\boldsymbol{Z}_\ell^{(g)}$. Cet isomorphisme fait correspondre à la classe de $\sum_{\tau\in G} a_\tau\tau$ modulo $\operatorname{Ker}\chi_1$, l'élément $\sum_{\tau\in G} a_\tau\chi(\tau)$ de $\boldsymbol{Z}_\ell^{(g)}$. Ainsi tout $\boldsymbol{Z}_\ell[G]$-module annulé par $\operatorname{Ker}\chi_1$ peut être considéré comme un $\boldsymbol{Z}_\ell^{(g)}$-module.

D'une façon générale, dans toute la suite, si $A/B$ est une extension galoisienne et si $C$ est un corps intermédiaire tel que $A/C$ soit abélienne, et $C/B$ galoisienne, on entend par opération de $\operatorname{Gal}(C/B)$ sur $\operatorname{Gal}(A/C)$, l'opération conjugaison ainsi notée: Si $u$ appartient à $\operatorname{Gal}(A/C)$ et si $\tau$ appartient à $\operatorname{Gal}(C/B)$, alors $u^\tau$ est égal à $t^{-1}$ ut, où $t$ est un prolongement de $\tau$ à $A$. Précisons de plus que si $a$ appartient à $A$, on désigne par $a^u$ l'image de $a$ par $u$ et, en conséquence, la composition des automorphismes $u$ et $v$ de $A$ est notée suivant la convention $a^{(uv)} = (a^u)^v$.

Soit $U/K$ la $\ell$-extension abélienne maximale de $K$, non ramifiée en dehors de $\ell$. Le groupe de Galois $\operatorname{Gal}(U/K)$ est un $\boldsymbol{Z}_\ell[G]$-module. Soit $K_\infty$ la $\boldsymbol{Z}_\ell$-extension maximale de $K$ (Comme $K$ est réel, il s'agit donc de la $\boldsymbol{Z}_\ell$-extension cyclotomique de $K$). On sait que $\operatorname{Gal}(U/K_\infty)$ est le sous-module de torsion de $\operatorname{Gal}(U/K)$ et qu'il est fini. Nous désignons par $\mathscr{H}(\chi)$ le $\boldsymbol{Z}_\ell[G]$-module quotient $\operatorname{Gal}(U/K_\infty)/\operatorname{Gal}(U/K_\infty)^{P(\sigma)}$. Il s'agit donc d'un $\boldsymbol{Z}_\ell^{(g)}$-module.

## 2. Enoncé des résultats obtenus

Rappelons que $\chi$ est un caractère réel, différent du caractère unité et que $g$ est son ordre.

THÉORÈME A. *Si $g$ n'est pas une puissance de $\ell$, alors $\mathscr{H}(\chi)$ est annulé en tant que $\boldsymbol{Z}_\ell^{(g)}$-module par $L_\ell(1,\chi)$, valeur en 1 de la fonction $L$ $\ell$-adique relative à $\chi$.*

THÉORÈME B. *Si $g$ est une puissance de $\ell$ et si $\zeta_g$ est une racine primitive $g^{\text{ème}}$ de 1, alors $\mathscr{H}(\chi)$ est annulé par $(1-\zeta_g)L_\ell(1,\chi)$.*

https://doi.org/10.1017/S0027763000019140 Published online by Cambridge University Press

## 3. Démonstration des théorèmes

Soit $N$ le corps intermédiaire entre $U$ et $K$ tel que $\mathrm{Gal}(U/N) = \mathrm{Gal}(U/K)^{P(\sigma)}$. Ainsi $N/K$ est la $\ell$-extension abélienne, non ramifiée sauf en $\ell$, maximale telle que $N/\boldsymbol{Q}$ soit galoisienne et $\mathrm{Gal}(N/K)$ soit annulé par $P(\sigma)$. Soit, pour tout entier $n$, $\boldsymbol{Q}_n$ le sous-corps de $\boldsymbol{Q}^{(\ell n)}$ défini par $[\boldsymbol{Q}^{(\ell n)} : \boldsymbol{Q}_n] = \ell - 1$. Pour tout corps $A$, on pose $A_i = A\boldsymbol{Q}_i$. On désigne par $\boldsymbol{Q}_\infty = \bigcup_{i \geq 1} \boldsymbol{Q}_i$ et $K_\infty = \bigcup_{i \geq 1} K_i = K\boldsymbol{Q}_\infty$ les $\boldsymbol{Z}_\ell$-extensions cyclotomiques de $\boldsymbol{Q}$ et $K$. Soit $n_0$ l'entier non nul défini par $\boldsymbol{Q}_{n_0} = \boldsymbol{Q}_\infty \cap K$. On a donc $K_{n_0} = K \neq K_{n_0+1}$.

PROPOSITION 3.1. *Si $g$ n'est pas une puissance de $\ell$, l'intersection $N \cap K_\infty$ est égale à $K$. Si $g$ est une puissance de $\ell$ alors $N \cap K_\infty$ est égal à $K_{n_0+1}$. Dans tous les cas, $\mathscr{H}(\chi)$ est isomorphe, en tant que $\boldsymbol{Z}_\ell^{(g)}$-module, à* $\mathrm{Gal}(N/N \cap K_\infty)$.

*Démonstration.* Comme l'extension $N \cap K_\infty/\boldsymbol{Q}$ est abélienne, le $\boldsymbol{Z}_\ell[G]$-module $\mathrm{Gal}(N \cap K_\infty/K)$ est annulé par $\sigma - 1$ et $P(\sigma)$. Donc il est annulé par $P(1)$. Si $g$ n'est pas une puissance de $\ell$, alors $P(1)$ est une unité de $\boldsymbol{Z}_\ell$ et $N \cap K_\infty = K$. Si par contre, $g$ est une puissance de $\ell$, alors $P(1) = \ell$ et le degré $[N \cap K_\infty : K]$ ne peut excéder $\ell$. Nous avons donc $N \cap K_\infty \subset K_{n_0+1}$. D'autre part, l'extension $K_{n_0+1}/\boldsymbol{Q}$ est abélienne et $\mathrm{Gal}(K_{n_0+1}/K)$ est annulé par $\sigma - 1$ et $\ell = P(1)$, donc par $P(\sigma)$. Ainsi, on a $K_{n_0+1} = N \cap K_\infty$.

Démontrons maintenant l'égalité $\mathrm{Gal}(U/K)^{P(\sigma)} \cap \mathrm{Gal}(U/K_\infty) = \mathrm{Gal}(U/K_\infty)^{P(\sigma)}$. Soit $h$ un élément de $\mathrm{Gal}(U/K)$ et supposons que $h^{P(\sigma)}$ appartienne à $\mathrm{Gal}(U/K_\infty)$. Comme $\mathrm{Gal}(U/K_\infty)$ est le sous-module de torsion de $\mathrm{Gal}(U/K)$, il existe un entier $k$ tel que $h^{\ell^k P(\sigma)} = 1$. Mais $K_\infty/\boldsymbol{Q}$ est abélienne et $h^{\ell^k P(1)}$ appartient à $\mathrm{Gal}(U/K_\infty)$. Donc $h$ appartient lui-même à $\mathrm{Gal}(U/K_\infty)$. Nous en déduisons les égalités et isomorphismes: $\mathscr{H}(\chi) = \mathrm{Gal}(U/K_\infty)/\mathrm{Gal}(U/K_\infty)^{P(\sigma)} = \mathrm{Gal}(U/K_\infty)/(\mathrm{Gal}(U/K)^{P(\sigma)} \cap \mathrm{Gal}(U/K_\infty)) \simeq (\mathrm{Gal}(U/K)^{P(\sigma)}\, \mathrm{Gal}(U/K_\infty))/\mathrm{Gal}(U/K)^{P(\sigma)} = \mathrm{Gal}(U/N \cap K_\infty)/\mathrm{Gal}(U/N) \simeq \mathrm{Gal}(N/N \cap K_\infty)$. Ce qui termine la démonstration de la proposition 3.1.

Soit $n$ un entier non nul. Définissons $N^n$ comme le corps intermédiaire entre $N$ et $N \cap K_\infty$ maximal tel que $\mathrm{Gal}(N^n/N \cap K_\infty)$ soit d'exposant divisant $\ell^n$. Alors $\mathscr{H}(\chi)/\mathscr{H}(\chi)^{\ell^n}$ est isomorphe en tant que $\boldsymbol{Z}_\ell[G]$-module à $\mathrm{Gal}(N^n/N \cap K_\infty)$. Introduisons $L$, corps obtenu en ajoutant à $K$ les racines $\ell^{\text{ème}}$ de 1, c'est-à-dire $L = K\boldsymbol{Q}^{(\ell)}$, et $M^n = N^n L = N^n \boldsymbol{Q}^{(\ell)}$. Nous avons alors

https://doi.org/10.1017/S0027763000019140 Published online by Cambridge University Press

$M_n^n = M^n Q_n = N^n L_n = N^n Q^{(\ell^n)}$. Soit $G_n$ le groupe de Galois $\mathrm{Gal}(L_n/Q)$. Il est clair que tous les $G$-modules introduits précédemment peuvent également être considérés comme des $G_n$-modules.

PROPOSITION 3.2. *On suppose que $n$ est un entier non nul. Si $g$ est une puissance de $\ell$, on suppose de plus $n$ supérieur à $n_o + 1$. Alors $\mathscr{H}(\chi)/\mathscr{H}(\chi)^{\ell^n}$ est isomorphe en tant que $G_n$-module à $\mathrm{Gal}(M_n^n/L_n)$.*

*Démonstration.* Nous avons $M_n^n = N^n L_n$. D'autre part, on vérifie l'égalité $N^n \cap L_n = N \cap K_\infty$. On en déduit l'isomorphisme $\mathrm{Gal}(M_n^n/L_n) \simeq \mathrm{Gal}(N^n/N \cap K_\infty)$; d'où le résultat en utilisant la proposition 3.1.

L'extension $M_n^n/L_n$ est une extension de Kummer d'exposant divisant $\ell^n$. Nous notons $W_n$ son radical, c'est-à-dire: $W_n = \{w; w \in L_n; \sqrt[\ell^n]{w} \in M_n^n\}$. Le groupe $W_n/(L_n^*)^{\ell^n}$ est évidemment un $G_n$-module et en tant que groupe il est isomorphe à $\mathrm{Gal}(M_n^n/L_n)$. Les structures de $G_n$-modules de ces deux groupes sont liées par l'involution du miroir que nous allons rappeler:

Soit $A_n = Z/\ell^n Z$ l'anneau des classes résiduelles d'entiers modulo $\ell^n$ et $A_n^*$ son groupe multiplicatif. Si $\xi_n$ est une racine primitive $(\ell^n)^{\text{ème}}$ de 1, alors on note $\chi^*$ l'homomorphisme de $G_n$ dans $A_n^*$ défini par $\xi_n^\tau = \xi_n^{\chi^*(\tau)}$. Si $x = \sum_{\tau \in G} a_\tau \tau$ est un élément de $A_n[G_n]$, on pose $\bar{x} = \sum_{\tau \in G} a_\tau \chi^*(\tau)\tau^{-1}$. L'application de l'algèbre $A_n[G_n]$ dans elle-même qui à $x$ fait correspondre $\bar{x}$ est un automorphisme involutif de $A_n[G_n]$ que l'on appelle: "involution du miroir". Les groupes $\mathrm{Gal}(M_n^n/L_n)$ et $W_n/(L_n^*)^{\ell^n}$ sont des $A_n[G_n]$-modules et leurs structures sont liées par la proposition suivante:

PROPOSITION 3.3. *Les annulateurs, dans $A_n[G_n]$, de $W_n/(L_n^*)^{\ell^n}$ et $\mathrm{Gal}(M_n^n/L_n)$ sont images l'un de l'autre par l'involution du miroir.*

Nous ne réécrivons pas ici la démonstration de la "Spiegelungsrelation" d'où provient ce résultat. On peut consulter [4] ou [5].

Introduisons $n_1$ et $f_0$ définis par l'égalité $f = \ell^{n_1} f_0$, $f_0$ étant premier à $\ell$ et $f$ désignant le conducteur de $\chi$ (On a donc $n_1 \geq n_0$ sauf si $n_1 = 0$ et $n_0 = 1$). Posons $f_n = \ell^n f_0$ et supposons désormais $n$ supérieur à $n_1$. Alors $f_n$ est le conducteur de $L_n$. On désigne par $(L_n/a)$ le symbole d'Artin attaché à l'extension $L_n/Q$, $a$ étant un entier premier à $f_n$. On considère l'élément de $Q_\ell[G_n]$ défini par $s_n = (1/f_n) \sum_a a(L_n/a)^{-1}$, la somme étant étendue aux entiers $a$ de 1 à $f_n$ et premiers à $f_n$. Rappelons le théorème de Stickelberger: l'idéal $s_n Z_\ell[G_n] \cap Z_\ell[G_n]$ de $Z_\ell[G_n]$ annule le groupe des $\ell$-classes d'idéaux (au sens ordinaire) de $L_n$. D'autre part nous utilisons également un élément $s'_n$ défini par: $s'_n = s_n - 1/2 \sum_a (L_n/a)$, cette somme étant étendue aux entiers $a$ de 1 à $f_n$ et premiers à $f_n$. Si $b$ est un entier premier à $f_n$, nous posons $y_n = (1 - b(L_n/b)^{-1})s_n$ et $y'_n = (1 - b(L_n/b)^{-1})s'_n$. La première quantité appartient à $\boldsymbol{Z}[G_n]$ et en imposant à $b$ d'être impair, $y'_n$ est aussi dans $\boldsymbol{Z}[G_n]$; ce que nous supposerons dans la suite.

PROPOSITION 3.4. *On suppose toujours que $n$ est un entier non nul, supérieur à $n_1$. Si $g$ est une puissance de $\ell$, supposons de plus $n$ supérieur à $n_0 + 1$. Alors $W_n/(L_n^*)^{\ell^n}$ est annulé par $y'_n$.*

*Démonstration.* Soit $w$ un élément de $W_n$. Comme l'extension $L_n(\sqrt[\ell^n]{w})/L_n$ est non ramifiée, sauf en $\ell$, l'idéal de $L_n$ engendré par $w$ est de la forme $\mathfrak{a}^{\ell^n}\mathfrak{b}$, où $\mathfrak{a}$ est un idéal de $L_n$ premier *à* $\ell$ et $\mathfrak{b}$ un idéal de $L_n$ dont la décomposition en idéaux premiers ne contient que des idéaux au-dessus de $\ell$. Notons $\mathcal{T}(\ell)$ le groupe des idéaux engendré par les idéaux premiers de $L_n$ au-dessus de $\ell$, et $D$ le groupe de décomposition de $\ell$ dans $L_n/\boldsymbol{Q}$. Le groupe $\mathcal{T}(\ell)$ est un $\boldsymbol{Z}[G_n]$-module et plus précisément un $\boldsymbol{Z}[G_n/D]$-module. Considérons l'élément $s'_n$ de $\boldsymbol{Q}[G_n]$. Sa restriction à $\boldsymbol{Q}[G_n/D]$ est nulle d'après le théorème II 3 de [2]. Il en sera de même de la restriction de $y'_n$ à $\boldsymbol{Z}[G_n/D]$ et $y'_n$ annule le groupe $\mathcal{T}(\ell)$. Nous avons donc $\mathfrak{b}^{y'_n} = 1$.

D'autre part, on déduit du théorème de Stickelberger que $\mathfrak{a}^{y'_n}$ est principal. Il existe donc un élément $u$ dans $L_n$ et une unité $\varepsilon$ de $L_n$ tels que $w^{y'_n} = u^{\ell^n}\varepsilon$.

Introduisons maintenant la conjugaison complexe $\sigma_\infty$ de $G_n$. Puisque $K$ est réel, $\sigma_\infty$ appartient à Gal$(L_n/K)$ et $\sigma_\infty - 1$ annule Gal$(M_n^n/L_n)$. Mais $\chi^*(\sigma_\infty) = -1$ et l'image de $\sigma_\infty - 1$ par l'involution du miroir est $-(\sigma_\infty + 1)$. On déduit de la proposition 3.2 que $\sigma_\infty + 1$ annule $W_n/(L_n^*)^{\ell^n}$. Cela implique que $\varepsilon^{\sigma_\infty + 1}$ est une puissance $(\ell^n)^{\text{ème}}$ d'un élément de $L_n$, donc finalement d'une unité de $L_n$. Considérons le groupe des unités $E$ de $L_n$ et le quotient $\mathcal{E} = E/E^{\ell^n}$. Ce groupe se décompose en produit direct sous la forme: $\mathcal{E} = \mathcal{E}^{(1+\sigma_\infty)/2}\mathcal{E}^{(1-\sigma_\infty)/2}$. Le premier facteur s'identifie par injection canonique à $E_0/E_0^{\ell^n}$, où $E_0$ est le groupe des unités du sous-corps réel maximal de $L_n$. Le deuxième est cyclique, engendré par la classe d'une racine de l'unité. Ainsi, si $\varepsilon^{\sigma_\infty+1}$ appartient à $E^{\ell^n}$, alors $\varepsilon$ est, modulo $E^{\ell^n}$, une racine de l'unité. Nous aurons donc $w^{y'_n} = v^{\ell^n}\zeta$, avec $v$ dans $L_n$ et $\zeta$ racine de l'unité appartenant à $L_n$. Comme $n \geq n_1$, nous avons $L_n \neq L_{n+1}$ et $\zeta^{\ell^n} = 1$. Ceci montre que les racines $(\ell^n)^{\text{ème}}$ de $w^{y'_n}$ appartiennent à $M_n^n \cap L_{2n}$.

https://doi.org/10.1017/S0027763000019140 Published online by Cambridge University Press

Il reste à calculer cette intersection: Nous avons $M_n^n \cap L_{2n} = (L_n N^n) \cap L_{2n} = L_n(N^n \cap L_{2n})$. Si $g$ n'est pas une puissance de $\ell$, on a $N^n \cap L_{2n} = K$. Si $g$ est une puissance de $\ell$, alors $N^n \cap L_{2n} = K_{n_0+1}$. D'où l'on déduit $M_n^n \cap L_{2n} = L_n K$ ou $L_n K_{n_0+1}$ suivant les cas. Mais si $g$ est une puissance de $\ell$, on a supposé $n \geq n_0 + 1$. Nous avons donc dans tous les cas $M_n^n \cap L_{2n} = L_n$. Ainsi $w^{y'_n}$ appartient à $(L_n^*)^{\ell^n}$; ce qui démontre la proposition 3.4.

Introduisons maintenant les éléments de $\boldsymbol{Q}_\ell[G_n]$:

$$x_n = \left((1 - b^{\varphi(\ell^n)}\left(\frac{L_n}{b}\right)\right)(1/f_n\varphi(\ell^n)) \sum_a a^{\varphi(\ell^n)}\left(\frac{L^n}{a}\right),$$

$$x'_n = x_n - \frac{1}{2}(1 - b) \sum_a a\left(\frac{L_n}{a}\right)^{-1}.$$

L'entier $b$ est le même que précédemment. Il est seulement pour l'instant supposé premier à $f_n$ et impair. L'indicateur d'Euler est noté $\varphi$ et $\sum_a$ désigne la somme sur les entiers $a$, de 1 à $f_n$, premiers à $f_n$.

PROPOSITION 3.5. *Les éléments $x_n$ et $y_n$ appartiennent à $\boldsymbol{Z}_\ell[G_n]$. Leurs résidus modulo $\ell^n$ sont des éléments de $A_n[G_n]$, images l'un de l'autre par l'involution du miroir.*

*Démonstration.* Le symbole $\sum_a$ désigne la somme sur les entiers $a$, de 1 à $f_n$, premiers à $f_n$. On peut écrire:

$$x_n = (1/f_n\varphi(\ell^n))\left(\sum_a a^{\varphi(\ell^n)}\left(\frac{L_n}{a}\right) - \sum_a a^{\varphi(\ell^n)} b^{\varphi(\ell^n)}\left(\frac{L_n}{b}\right)\left(\frac{L_n}{a}\right)\right).$$

Définissons $a'$ par $\begin{cases} ba' \equiv a \mod (f_n) \\ 1 \leq a' \leq f_n \end{cases}$. Il est clair que $a \to a'$ réalise une permutation de l'ensemble des entiers premiers à $f_n$ et compris entre 1 et $f_n$. Nous aurons donc:

$$x_n = (1/f_n\varphi(\ell^n))\left(\sum_a a^{\varphi(\ell^n)}\left(\frac{L_n}{a}\right) - \sum_a a'^{\varphi(\ell^n)} b^{\varphi(\ell^n)}\left(\frac{L_n}{b}\right)\left(\frac{L_n}{a'}\right)\right)$$

d'où

$$x_n = (1/f_n\varphi(\ell^n)) \sum_a [a^{\varphi(\ell^n)} - a'^{\varphi(\ell^n)} b^{\varphi(\ell^n)}] \left(\frac{L_n}{a}\right).$$

Il apparaît clairement dans cette écriture que $x_n$ appartient à $\boldsymbol{Z}_\ell[G_n]$. Mais $\chi^*(L_n/a)$ est le résidu modulo $\ell^n$ de $a$. Donc l'image du résidu modulo $\ell^n$

https://doi.org/10.1017/S0027763000019140 Published online by Cambridge University Press

de $x_n$ par l'involution du miroir est le résidu modulo $\ell^n$ de $\bar{x}_n$ défini par:

$$\bar{x}_n = (1/f_n\varphi(\ell^n)) \sum_a a[a^{\varphi(\ell^n)} - a'^{\varphi(\ell^n)}b^{\varphi(\ell^n)}]\left(\frac{L_n}{a}\right)^{-1}.$$

Calculons maintenant la quantité entre crochets: Nous pouvons écrire:

$$a^{\varphi(\ell^n)} - a'^{\varphi(\ell^n)}b^{\varphi(\ell^n)} = (a - a'b)\ A$$

avec

$$A = a^{\varphi(\ell^n)-1} + a'ba^{\varphi(\ell^n)-2} + \cdots + (a'b)^{\varphi(\ell^n)-1}.$$

Mais si $a'b = a + \lambda\ell^n$, nous avons alors

$$(a'b)^i = a^i + ia^{i-1}\lambda\ell^n + \cdots \equiv a^i + ia^{i-1}\lambda\ell^n \qquad \bmod (\ell^{2n}).$$

Remplaçons dans $A$: nous obtenons alors

$$A \equiv \varphi(\ell^n)a^{\varphi(\ell^n)-1} + a^{\varphi(\ell^n)-2}(1 + 2 + \cdots + (\varphi(\ell^n) - 1))\lambda\ell^n \qquad \bmod (\ell^{2n}).$$

D'où

$$A \equiv \varphi(\ell^n)a^{\varphi(\ell^n)-1} \qquad \bmod (\ell^{2n-1})$$

et

$$A/\varphi(\ell^n) \equiv a^{\varphi(\ell^n)-1} \qquad \bmod (\ell^n)$$

et enfin

$$aA/\varphi(\ell^n) \equiv a^{\varphi(\ell^n)} \equiv 1 \qquad \bmod (\ell^n).$$

Nous obtenons donc: $\bar{x}_n \equiv (1/f_n) \sum_a (a - a'b)(L_n/a)^{-1} \bmod (\ell^n)$.
Il reste à constater que cette dernière quantité n'est autre que $y_n$. En effet, on $a$: $y_n = (1 - b(L_n/b)^{-1})(1/f_n) \sum_a a(L_n/a)^{-1} = (1/f_n)(\sum_a a(L_n/a)^{-1} - \sum_a ab(L_n/a)^{-1}(L_n/b)^{-1})$. Nous raisonnons alors de la même façon qu'au début de la démonstration: on peut remplacer dans la dernière somme $a$ par $a'$ et on obtiendra:

$$\begin{aligned} y_n &= (1/f_n)\left(\sum_a a\left(\frac{L_n}{a}\right)^{-1} - \sum_a a'b\left(\frac{L_n}{a'}\right)^{-1}\left(\frac{L_n}{b}\right)^{-1}\right) \\ &= (1/f_n) \sum_a (a - a'b)\left(\frac{L_n}{a}\right)^{-1}. \end{aligned}$$

PROPOSITION 3.6. *On suppose toujours que $n$ est un entier non nul, supérieur à $n_1$. Si $g$ est une puissance de $\ell$, on suppose de plus que $n$ est*

https://doi.org/10.1017/S0027763000019140 Published online by Cambridge University Press

*supérieur à* $n_0+1$. *Alors le groupe de Galois* Gal $(M_n^n/L_n)$, *considéré comme* $Z_\ell[G_n]$*-module, est annulé par* $x'_n$.

*Démonstration.* Les résidus modulo $\ell^n$ de $\sum_a (L_n/a)$ et $\sum_a a(L_n/a)^{-1}$ se correspondent par l'involution du miroir. On déduit donc de la proposition précédente (3.5) que les résidus de $x'_n$ et $y'_n$ se correspondent par l'involution du miroir. On déduit alors des propositions 3.3 et 3.4 que $x'_n$ annule Gal $(M_n^n/L_n)$.

*Remarque.* On peut constater que $\sum_a a(L_n/a)^{-1}$ annule Gal $(M_n^n/L_n)$ et en déduire que $x_n$ annule Gal $(M_n^n/L_n)$. D'où finalement, on constate que $y_n$ annule $W_n/(L_n^*)^{\ell^n}$. Pourquoi avoir introduit $s'_n$, $x'_n$, $y'_n$? Uniquement à cause de l'annulation de l'idéal $\mathfrak{b}$ au cours de la démonstration de la proposition 3.3. En effet, nous avons vu à ce niveau que $\mathfrak{b}^{y'_n}=1$. Il ne nous a pas semblé très simple de montrer directement que $\mathfrak{b}^{y_n}$ est la puissance $(\ell^n)^{\text{ème}}$ d'un idéal principal.

Introduisons la notation suivante: $S_n$ est l'élément de $Q_\ell^{(g)}$ défini par $S_n=(1/f_n\varphi(\ell^n))\sum_a a^{\varphi(\ell^n)}\chi(a)$. La somme est étendue aux entiers $a$, compris entre 1 et $f_n$ et premiers à $f_n$. D'autre part, on considère dans la suite $\chi$ comme un caractère de $G_n$ ou de Gal $(Q^{(f_n)}/Q)$. La valeur $\chi(a)$ est par définition égale à $\chi(L_n/a)$; cela provient de l'identification de Gal $(Q^{(f_n)}/Q)$ et de $(Z/f_nZ)^*$.

PROPOSITION 3.7. *Supposons que $g$ n'est pas une puissance de $\ell$. Soit $n$ un entier non nul, supérieur à $n_1$. Alors $S_n$ appartient à $Z_\ell^{(g)}$ et annule le $Z_\ell^{(g)}$-module $\mathscr{H}(\chi)/\mathscr{H}(\chi)^{\ell^n}$.*

*Démonstration.* Imposons de plus à l'entier $b$ la condition suivante: $\chi(b)$ est une racine de 1 d'ordre non puissance de $\ell$. Nous avons $\chi_1(x_n)=(1-b^{\varphi(\ell^n)}\chi(b))S_n$ et $1-\chi(b)$ est une unité de $Z_\ell^{(g)}$. Mais nous avons $1-b^{\varphi(\ell^n)}\chi(b)\equiv 1-\chi(b) \mod (\ell^n)$ et $1-b^{\varphi(\ell^n)}\chi(b)$ est une unité de $Z_\ell^{(g)}$. Comme $x_n$ appartient à $Z_\ell[G_n]$, $\chi_1(x_n)$ appartient à $Z_\ell^{(g)}$ et $S_n$ également.

D'autre part, on déduit des propositions 3.2 et 3.6 que $x'_n$ annule $\mathscr{H}(\chi)/\mathscr{H}(\chi)^{\ell^n}$. En termes de $Z_\ell^{(g)}$-modules, cela veut dire que $\chi_1(x'_n)$ annule $\mathscr{H}(\chi)/\mathscr{H}(\chi)^{\ell^n}$.

Il reste donc à vérifier que $\chi_1(x_n)=\chi_1(x'_n)$. En effet, $\chi_1(x_n-x'_n)=1/2(1-b)\sum_a a\chi(a)^{-1}$. Comme $\chi$ est un caractère réel, on a $\chi(a)=\chi(f_n-a)$ et on en déduit $\chi_1(x'_n-x_n)=0$. Nous avons démontré la proposition.

Nous pouvons maintenant justifier le théorème A: en effet, le groupe $\mathscr{H}(\chi)$ est fini. Donc si $n$ est assez grand, $\mathscr{H}(\chi)^{\ell^n}$ est égal à 1 et $\mathscr{H}(\chi)$ est annulé par $S_n$. Il reste alors à utiliser l'approximation $\ell$-adique de $L_\ell(1, \chi)$ telle qu'elle est donnée par Fresnel dans [1]. On a $-L_\ell(1, \chi) = \lim_{n\to\infty} S_n$. Donc $L_\ell(1, \chi)$ annule $\mathscr{H}(\chi)$.

Proposition 3.8. *Supposons que $g$ est une puissance de $\ell$. Soit $n$ un entier supérieur à $n_1$ et $n_0 + 1$. Soit $\zeta_g$ une racine primitive $g^{\text{ème}}$ de 1. Alors $(1 - \zeta_g)S_n$ appartient à $Z_\ell^{(g)}$ et annule le $Z_\ell^{(g)}$-module $\mathscr{H}(\chi)/\mathscr{H}(\chi)^{\ell^n}$.*

*Démonstration.* Nous imposons maintenant à $b$ de vérifier la condition suivante: $\chi(b)$ est une racine primitive de 1, d'ordre $g$. Alors, les idéaux de $Z_\ell^{(g)}$ engendrés par $1 - \chi(b)$ et $1 - \zeta_g$ sont les mêmes: à savoir l'idéal maximal de $Z_\ell^{(g)}$. On déduit de la congruence $1 - b^{\varphi(\ell^n)}\chi(b) \equiv 1 - \chi(b)$ mod $(\ell^n)$, que $(1 - b^{\varphi(\ell^n)}\chi(b))/(1 - \zeta_g)$ est une unité de $Z_\ell^{(g)}$. Comme $x_n$ appartient à $Z_\ell[G_n]$, $\chi_1(x_n)$ appartient à $Z_\ell^{(g)}$ et $(1 - \zeta_g)S_n$ également. Ces deux éléments engendrent dans $Z_\ell^{(g)}$ le même idéal. D'autre part, on déduit des propositions 3.2 et 3.6 que $x'_n$ annule $\mathscr{H}(\chi)/\mathscr{H}(\chi)^{\ell^n}$. Ceci implique que $\chi_1(x'_n)$ annule $\mathscr{H}(\chi)/\mathscr{H}(\chi)^{\ell^n}$. On a aussi, comme précédemment, $\chi_1(x_n) = \chi_1(x'_n)$. Ceci démontre la proposition 3.8. Le théorème B s'en déduit de la même façon que le théorème A se déduisait de la proposition 3.7.

*Remarque.* Nous avons vu au cours de la démonstration de la proposition 3.7, que si $g$ n'est pas une puissance de $\ell$, alors $S_n$ appartient à $Z_\ell^{(g)}$. On peut constater d'autre part, que si $f$ n'est pas une puissance de $\ell$, alors $S_n$ appartient à $Z_\ell^{(g)}$.

*Démonstration.* Pour tout entier $a$, premier à $f_n$, il existe des entiers $a'$ et $a''$ uniques tels que: $a \equiv a'a''$ mod $(f_n)$; $a' \equiv 1$ mod $(f_0)$; $a'' \equiv 1$ mod $(\ell^n)$; $1 \leq a' < f_n$ et $1 \leq a'' < f_n$. Nous aurons donc $a^{\varphi(\ell^n)} \equiv a'^{\varphi(\ell^n)}a''^{\varphi(\ell^n)}$ mod $(\ell^{2n-1})$ et on en déduit

$$\sum_a a^{\varphi(\ell^n)}\,\chi(a) \equiv \Big(\sum_{a'} a'^{\varphi(\ell^n)}\chi(a')\Big)\Big(\sum_{a''} a''^{\varphi(\ell^n)}\chi(a'')\Big) \mod (\ell^{2n-1})\,.$$

La première somme est étendue aux entiers $a$, de 1 à $f_n$, premiers à $f_n$; la deuxième aux entiers $a'$, de 1 à $f_n$, premiers à $f_n$, congrus à 1 modulo $f_0$ et la troisième aux entiers $a''$, de 1 à $f_n$, premiers à $f_n$, congrus à 1 modulo $\ell^n$. Considérons la dernière somme: Nous avons

$$a''^{\varphi(\ell^n)} \equiv 1 \mod (\ell^{2n-1}). \quad \text{Donc } \sum_{a''} a''^{\varphi(\ell^n)}\chi(a'') \equiv \sum_{a''} \chi(a'') \mod (\ell^{2n-1})\,.$$

https://doi.org/10.1017/S0027763000019140 Published online by Cambridge University Press

Mais si $f_0$ est différent de 1, cette dernière somme est nulle. On a donc $\sum_a a^{\varphi(\ell^n)}\chi(a) \equiv 0 \bmod (\ell^{2n-1})$ et ceci montre que $S_n$ appartient à $\boldsymbol{Z}_\ell^{(g)}$.

## 4. Dernières remarques

Examinons les approximations de $L_\ell(1, \chi)$ fournies par les quantités $S_n$.

PROPOSITION 4.1. *L'entier n est toujours supposé non nul et supérieur à $n_1$. Si g n'est pas une puissance de $\ell$, alors on a la congruence $S_{n+1} \equiv S_n \bmod (\ell^n)$. Si g est une puissance de $\ell$ et si f n'est pas une puissance de $\ell$, alors on a $(1-\zeta_g)S_{n+1} \equiv (1-\zeta_g)S_n \bmod (\ell^n)$. Si f et g sont des puissances de $\ell$, on a seulement $(1-\zeta_g)^2 S_n \equiv (1-\zeta_g)^2 S_{n+1} \bmod (\ell^n)$.*

*Démonstration.* On choisit l'entier $b$ comme il est indiqué dans les démonstrations des propositions 3.7 et 3.8. Ce choix fait pour $n$, convient aussi pour $n+1$. Considérons la restriction de $\boldsymbol{Z}[G_{n+1}]$ à $\boldsymbol{Z}[G_n]$. Un calcul élémentaire montre que l'image de $y'_{n+1}$ par cette restriction est $y'_n$; (Théorème II 3 [2]). D'autre part, si l'on considère la restriction de $A_{n+1}[G_{n+1}]$ à $A_n[G_n]$ et les involutions du miroir relatives à $L_{n+1}/\boldsymbol{Q}$ et $L_n/\boldsymbol{Q}$, on constate que ces opérations permutent. Il découle de la proposition 3.5 que le résidu modulo $\ell^n$ de $x'_n$ coïncide avec le résidu modulo $\ell^n$ de la restriction de $x'_{n+1}$ à $\boldsymbol{Z}_\ell[G_n]$. Notant de la même façon: $\chi$, le caractère $\chi$ de $G$, son prolongement à $G_n$ et son prolongement à $G_{n+1}$ et notant de la même façon: $\chi_1$ les prolongements $\boldsymbol{Z}_\ell$-linéaires de $\chi$ à $\boldsymbol{Z}_\ell[G_{n+1}]$ et $\boldsymbol{Z}_\ell[G_n]$, nous avons donc $\chi_1(x'_n) \equiv \chi_1(x'_{n+1}) \bmod (\ell^n)$. C'est-à-dire: $(1-b^{\varphi(\ell^n)}\chi(b))S_n \equiv (1-b^{\varphi(\ell^{n+1})}\chi(b))S_{n+1} \bmod (\ell^n)$. Mais nous avons $1-b^{\varphi(\ell^n)}\chi(b) \equiv 1-\chi(b) \bmod (\ell^n)$ et $1-b^{\varphi(\ell^{n+1})}\chi(b) \equiv 1-\chi(b) \bmod (\ell^{n+1})$. Lorsque $f$ ou $g$ n'est pas une puissance de $\ell$, on en déduit à l'aide de la remarque placée à la fin du paragraphe 3, la congruence $(1-\chi(b))S_n \equiv (1-\chi(b))S_{n+1} \bmod (\ell^n)$. Si $g$ n'est pas une puissance de $\ell$, alors $1-\chi(b)$ est une unité de $\boldsymbol{Z}_\ell^{(g)}$; d'où $S_n \equiv S_{n+1} \bmod (\ell^n)$. Si $g$ est une puissance de $\ell$ et si $f$ n'est pas une telle puissance, alors $(1-\chi(b))/1-\zeta_g$ est une unité de $\boldsymbol{Z}_\ell^{(g)}$; d'où $(1-\zeta_g)S_n \equiv (1-\zeta_g)S_{n+1} \bmod (\ell^n)$. Si, enfin, $f$ et $g$ sont des puissances de $\ell$, alors $(1-\zeta_g)S_n$ appartient à $\boldsymbol{Z}_\ell^{(g)}$ et on obtient alors le résultat annoncé en utilisant les mêmes arguments.

CONSEQUENCE. On déduit de la proposition 4.1 la convergence de la suite $S_n$. De plus, le résidu modulo $\ell^n$ de $L_\ell(1, \chi)$ (ou $(1-\zeta_g)L_\ell(1, \chi)$, ou $(1-\zeta_g)^2 L_\ell(1, \chi)$ suivant les cas) est l'opposé du résidu de $S_n$ (ou $(1-\zeta_g)S_n$

ou $(1-\zeta_g)^2 S_n)$. Pour obtenir celui-ci, on peut utiliser le calcul effectué dans la proposition 3.5. En effet, on a, en reprenant les notations adoptées lors de la démonstration de cette proposition:

$$S_n = (1/f_n\varphi(\ell^n)) \sum_a a^{\varphi(\ell^n)}\chi(a)$$

et

$$(1 - b^{\varphi(\ell^n)}\chi(b))S_n = (1/f_n\varphi(\ell^n)) \sum_a (a^{\varphi(\ell^n)} - a'^{\varphi(\ell^n)}b^{\varphi(\ell^n)})\chi(a) .$$

Mais d'après la proposition 3.5, on a aussi:
$(1 - b^{\varphi(\ell^n)}\chi(b))S_n \equiv (1/f_n) \sum_a a^{-1}(a - a'b)\chi(a) \bmod (\ell^n)$; en désignant par $a^{-1}$ un entier, inverse de $a$ modulo $\ell^n$. Cette formule permet de calculer plus facilement le résidu modulo $\ell^n$ de $L_\ell(1, \chi)$. (G. Gras a dernièrement généralisé ces considérations et obtenu de façon analogue le résidu modulo $\ell^n$ de $L_\ell(s, \chi)$: " Sur la construction des fonctions $L$ $p$-adiques abéliennes "; à paraître au Séminaire D.P.P.).

Examinons le cas particulier où $f$ et $g$ sont des puissances de $\ell$:

PROPOSITION 4.2. *Supposons que $f$ et $g$ soient tous deux des puissances de $\ell$. On a alors $K = \boldsymbol{Q}_{n_0} = \boldsymbol{Q}_{n_1}$. Le corps $N$ est égal à $\boldsymbol{Q}_{n_0+1}$ et $\mathscr{H}(\chi)$ est réduit à 1. D'autre part $(1-\zeta_g)L_\ell(1, \chi)$ est une unité de $\boldsymbol{Z}_\ell^{(g)}$.*

*Démonstration.* La première assertion de cet énoncé est évidente. Posons pour simplifier $n = n_0 = n_1$. Le degré de $\chi$ est donc $g = \ell^{n-1}$ et son conducteur $f = \ell^n$. Nous voulons montrer maintenant que $(1-\zeta_g)L_\ell(1, \chi)$ est une unité de $\boldsymbol{Z}_\ell^{(g)}$. Choisissons d'abord un entier $b$. Pour que $\chi(b)$ soit une racine primitive $g^{\text{ème}}$ de 1, il est suffisant de prendre $b = 1 + \ell$, ou bien tout entier congru à 1 modulo $\ell$ et non congru à 1 modulo $\ell^2$. Utilisons la suite exacte:

$$0 \longrightarrow (1-\zeta_g)\boldsymbol{Z}_\ell^{(g)} \longrightarrow \boldsymbol{Z}_\ell^{(g)} \xrightarrow{\alpha} \boldsymbol{Z}_\ell/\ell\boldsymbol{Z}_\ell \longrightarrow 0 ,$$

où l'homomorphisme $\alpha$ est défini par $\alpha(\sum_i c_i\zeta_g^i) = \sum_i c_i + \ell\boldsymbol{Z}_\ell$ (les $c_i$ sont dans $\boldsymbol{Z}_\ell$). Considérons l'élément de $\boldsymbol{Z}_\ell^{(g)}$: $(1 - b^{\varphi(\ell^n)}\chi(b))S_n$ et calculons son image par $\alpha$. Pour cela il est nécessaire d'écrire cet élément comme combinaison linéaire à coefficients dans $\boldsymbol{Z}_\ell$ de $1, \zeta_g, \zeta_g^2, \cdots$ etc. Comme au début de la démonstration de la proposition 3.5, nous écrivons ($\sum_a$ a le même sens) $(1 - b^{\varphi(\ell^n)}\chi(b)) \sum_a a^{\varphi(\ell^n)}\chi(a) = \sum_a (a^{\varphi(\ell^n)} - a'^{\varphi(\ell^n)}b^{\varphi(\ell^n)})\chi(a)$ et $a^{\varphi(\ell^n)} - a'^{\varphi(\ell^n)}b^{\varphi(\ell^n)} \equiv 0 \bmod (\ell^{2n-1})$. L'image par $\alpha$ cherchée est donc la classe modulo $\ell$ de $(\sum_a a^{\varphi(\ell^n)} - a'^{\varphi(\ell^n)} b^{\varphi(\ell^n)})/f_n\varphi(\ell^n)$. Le même calcul montre que cette expression est la classe modulo $\ell$ de $(1 - b^{\varphi(\ell^n)})(1/f_n\varphi(\ell^n)) \sum_a a^{\varphi(\ell^n)}$. Or il est facile de vérifier que cet élément de $\boldsymbol{Z}_\ell$ est premier à $\ell$: en effet, puisque $b \not\equiv 1 \bmod (\ell^2)$, on a $b^{\varphi(\ell^n)} \not\equiv 1 \bmod (\ell^{n+1})$ et $(1 - b^{\varphi(\ell^n)})/f_n$ est une unité de $\boldsymbol{Z}_\ell$. De même, $a^{\varphi(\ell^n)} \equiv 1 \bmod (\ell^n)$ et $\sum_a a^{\varphi(\ell^n)} \equiv \varphi(\ell^n) \bmod (\ell^n)$, montre que $(\sum_a a^{\varphi(\ell^n)})/\varphi(\ell^n)$ est aussi une unité de $\boldsymbol{Z}_\ell$. On déduit donc de la suite exacte écrite plus haut que $(1 - b^{\varphi(\ell^n)}\chi(b))S_n$ est une unité de $\boldsymbol{Z}_\ell^{(g)}$. Il en sera de même de $(1 - \zeta_g)S_n$. D'après la proposition 4.1, $(1 - \zeta_g)L_\ell(1, \chi)$ est aussi une unité de $\boldsymbol{Z}_\ell^{(g)}$.

Il découle alors du théorème B que le groupe $\mathscr{H}(\chi)$ est réduit à 1 et que le corps $N$ est égal à $\boldsymbol{Q}_{n+1}$.

## Bibliographie


[1] Fresnel, J., Nombres de Bernoulli et fonctions L $p$-adiques, Ann. Inst. Fourier, **17**, **2** (1967), 281–333.

[2] Grass, G., Application de la notion de $\varphi$-objet à l'étude du groupe des classes d'idéaux des extensions abéliennes, Publications mathématiques de la Faculté des Sciences de Besançon, 1975–1976.

[3] Gras, G., Annulation du groupe des $\ell$-classes généralisées d'une extension abélienne réelle de degré premier à $\ell$, Ann. Inst. Fourier, **29**, 1 (1979).

[4] Leopoldt, H. W., Zur Struktur der $\ell$-Klassengruppe galoischer Zahlkörper, Journ. für die reine und ang. Math., **199** (1958).

[5] Oriat, B. et Satgé, P., Un essai de généralisation du "Spiegelungssatz", Journ. für die reine und ang. Math., **307** (1979).



*Mathématiques E.R.A. n° 070654*
*Faculté des Sciences*
*25030 BESANCON Cedex*