SÉMINAIRE N. BOURBAKI

JOSEPH OESTERLÉ

Travaux de Ferrero et Washington sur le nombre de classes d'idéaux des corps cyclotomiques

Séminaire N. Bourbaki, 1978-1979, exp. n° 535, p. 170-182

<http://www.numdam.org/item?id=SB_1978-1979__21__170_0>

© Association des collaborateurs de Nicolas Bourbaki, 1978-1979, tous droits réservés.

L'accès aux archives du séminaire Bourbaki (http://www.bourbaki.ens.fr/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/legal.php). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI 535-01
31e année, 1978/79, n° 535 Février 1979

TRAVAUX DE FERRERO ET WASHINGTON

SUR LE NOMBRE DE CLASSES D'IDÉAUX DES CORPS CYCLOTOMIQUES

par Joseph OESTERLÉ

Le présent exposé se propose de rendre compte des récents travaux de Ferrero et Washington ([3], [4], [20], [21]) concernant l'étude de la partie première à p des nombres de classes d'idéaux dans une $\mathbb{Z}_p$-extension abélienne sur $\mathbb{Q}$, et la démonstration de la nullité de l'invariant μ associé par Iwasawa à une telle extension.

§ 1. Historique du problème

Soient p un nombre premier et k un corps. Une extension galoisienne K de k est appelée $\mathbb{Z}_p$-extension de k si le groupe de Galois $\Gamma = \mathrm{Gal}(K/k)$ est un groupe profini isomorphe au groupe additif $\mathbb{Z}_p$ des entiers p-adiques. On a alors $K = \bigcup_{n \geq 0} k_n$, avec $[k_n : k] = p^n$.

Soit K une $\mathbb{Z}_p$-extension d'un corps de nombres k (par un corps de nombres, nous entendons une extension finie de $\mathbb{Q}$). Notons $h_n(K/k)$ le nombre de classes d'idéaux de k_n, et, pour tout nombre premier ℓ, notons $e_n^{(\ell)}(K/k)$ l'exposant de ℓ dans h_n. Lorsqu'il n'y aura pas d'ambiguïté, nous écrirons simplement h_n et $e_n^{(\ell)}$.

Problème fondamental. Comment varie $e_n^{(\ell)}$ en fonction de n ?

Si $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont deux suites d'entiers, écrivons $a_n \sim b_n$ si la suite $(a_n - b_n)_{n\in\mathbb{N}}$ est constante pour n assez grand. La première réponse au problème fondamental, lorsque $\ell = p$, a été obtenue par Iwasawa qui étudiait la structure de Γ-module de $\mathrm{Gal}(L/K)$, où L est la p-extension abélienne non ramifiée maximale de K (cf. [9], ou [18] pour une démonstration simplifiée due à Serre) :

THÉORÈME 1.- *Soit K une $\mathbb{Z}_p$-extension d'un corps de nombres k. Il existe des entiers naturels $\mu(K/k)$ et $\nu(K/k)$ tels que :*

$$e_n^{(p)}(K/k) \sim \mu(K/k)p^n + \nu(K/k)n .$$

Après avoir conjecturé en 1970 que $\mu(K/k)$ est nul pour toute $\mathbb{Z}_p$-extension K/k ([11]), Iwasawa exhibe en 1973 un contre-exemple à sa conjecture ([13]), mais prouve néanmoins les résultats suivants :

THÉORÈME 2.- Soient k un corps de nombres, k' une extension finie de k et K une $\mathbb{Z}_p$-extension de k. Le corps Kk' est alors une $\mathbb{Z}_p$-extension de k'. De plus :

(i) $\mu(Kk'/k') = 0 \implies \mu(K/k) = 0$.

(ii) Supposons que $[k' : k]$ soit une puissance de p et qu'aucun idéal premier de k ramifié dans k' ne soit totalement décomposé dans K. Si $p = 2$, supposons en outre k totalement imaginaire. Alors on a :

$$\mu(K/k) = 0 \implies \mu(Kk'/k') = 0 .$$

Si $m \in \mathbb{N}^*$, notons $\mathbb{Q}(\zeta_m)$ le corps des racines m-ièmes de l'unité. Posons $\mathbb{Q}(\zeta_{p^\infty}) = \bigcup_{n \geq 0} \mathbb{Q}(\zeta_{p^n})$. C'est une extension galoisienne de $\mathbb{Q}$, dont le groupe de Galois G est canoniquement isomorphe au groupe $\mathbb{Z}_p^*$ des éléments inversibles de l'anneau $\mathbb{Z}_p$. Le sous-groupe de torsion T de G est fini, d'ordre $p-1$ si $p \neq 2$, d'ordre 2 si $p = 2$; soit B_p le corps fixé par T. La théorie du corps de classe montre que B_p est l'unique $\mathbb{Z}_p$-extension de $\mathbb{Q}$. Si k est un corps de nombres, on appelle $\mathbb{Z}_p$-extension cyclotomique de k la $\mathbb{Z}_p$-extension kB_p de k.

Cas particulier : posons $q = p$ si $p \neq 2$ et $q = 4$ si $p = 2$. Alors la $\mathbb{Z}_p$-extension cyclotomique de $\mathbb{Q}(\zeta_q)$ est $\mathbb{Q}(\zeta_{p^\infty})$.

Nous noterons $\mu_p(k)$ et $\lambda_p(k)$ les invariants associés par Iwasawa à la $\mathbb{Z}_p$-extension cyclotomique du corps de nombres k. Iwasawa conjecture que $\mu_p(k) = 0$ pour tout corps de nombres k en se fondant sur les résultats suivants :

- Si $k = \mathbb{Q}(\zeta_q)$ avec p régulier (i.e. : p ne divise pas le nombre de classes d'idéaux de $\mathbb{Q}(\zeta_q)$), ou si $k = \mathbb{Q}$, on a $\mu_p(k) = 0$. De fait, on a même $e_n^{(p)}(kB_p/k) = 0$ pour tout $n \geq 0$ ([7]).

- Si $[k : \mathbb{Q}]$ est une puissance de p, on a $\mu_p(k) = 0$. Cela résulte du théorème 2 ([13]).

- Iwasawa et Sims montrent en 1966, par calcul sur ordinateur, qu'on a $\mu_p(\mathbb{Q}(\zeta_p)) = 0$ pour $p < 4001$ ([14]).

L'évidence numérique n'a fait que se renforcer depuis :

Johnson, 1973, ([15]) : on a $\mu_p(\mathbb{Q}(\zeta_p)) = 0$ pour $p < 8000$.

Johnson, 1975, ([16]) : on a $\mu_p(\mathbb{Q}(\zeta_p)) = 0$ pour $p < 30\,000$.

Wagstaff, 1978, ([19]) : on a $\mu_p(\mathbb{Q}(\zeta_p)) = 0$ pour $p < 125\,000$.

Ernvall et Metsänkylä, 1978, ([2]) : on a $\mu_p(\mathbb{Q}(\zeta_{4p})) = 0$ pour $p < 10\,000$.

§ 2. Les résultats de Ferrero et Washington

THÉORÈME 3.- *Soit* k *une extension abélienne finie de* $\mathbb{Q}$. *On a* $\mu_p(k) = 0$.

Le cas où $p = 2$ ou 3 a été traité par Ferrero ([3]), et une généralisation convenable des méthodes employées a permis à Ferrero et Washington de démontrer le cas général ([4]). Les démonstrations sont effectives, en ce sens qu'elles permettent d'obtenir des majorations de $\lambda_p(k)$, mais celles-ci sont très éloignées de celles que suggérerait le calcul numérique des $\lambda_p(k)$.

Washington utilise les techniques introduites dans la démonstration du théorème 3 pour aborder le problème fondamental du § 1 lorsque $\ell \neq p$. Il obtient le résultat suivant ([21]) :

THÉORÈME 4.- *Soient* k *une extension abélienne finie de* $\mathbb{Q}$ *et* K *sa* $\mathbb{Z}_p$*-extension cyclotomique. On a*

$$e_n^{(\ell)}(K/k) \sim 0 .$$

Washington s'aperçoit aussi que les méthodes d'Iwasawa décrites au § 1 permettent d'exhiber une $\mathbb{Z}_p$-extension K/k (non cyclotomique) telle que la suite $e_n^{(\ell)}(K/k)$ soit non bornée pour un nombre premier $\ell \neq p$, et de démontrer l'analogue suivant du théorème 2 :

Soient k'/k une extension finie de corps de nombres et K une $\mathbb{Z}_p$-extension de k . Soit ℓ un nombre premier distinct de p . On a

$$e_n^{(\ell)}(Kk'/k') \sim 0 \implies e_n^{(\ell)}(K/k) \sim 0 .$$

La réciproque est vraie si $[k' : k]$ est une puissance de ℓ , si aucun idéal premier de k ramifié dans k' n'est totalement décomposé dans K , et si, lorsque $p = 2$, k est totalement imaginaire.

§ 3. Questions en suspens

a) Les théorèmes 3 et 4 restent-ils vrais pour toute $\mathbb{Z}_p$-extension cyclotomique ? Plus généralement, restent-ils vrais pour toute $\mathbb{Z}_p$-extension K/k telle qu'aucun idéal premier de k ne soit totalement décomposé dans K ?

b) Les calculs de Wagstaff montrent que pour tout nombre premier p impair inférieur à 125 000, on a, pour tout $n \geq 0$, $e_n^{(p)}(\mathbb{Q}(\zeta_{p^\infty}) / \mathbb{Q}(\zeta_p)) = \lambda_p n + \lambda_p$, où λ_p est le nombre d'entiers i , $1 \leq i \leq \frac{p-3}{2}$, pour lesquels p divise le nombre de Bernoulli B_{2i} .

Ceci reste-t-il vrai pour tout p ? (cf. aussi les exposés de Coates ([1]) et Iwasawa ([10]) pour des descriptions conjecturales des groupes de classes

d'idéaux dans les $\mathbb{Z}$-extensions cyclotomiques).

c) Washington conjecture que, pour toute $\mathbb{Z}_p$-extension K/k, on a $e_n^{(\ell)}(K/k) \sim \beta p^n$, β étant un nombre rationnel. Cela me semble un peu optimiste ; peut-être pourrait-on prouver qu'il existe $M > 0$ tel que $e_n^{(\ell)}(K/k)$ soit majoré par Mp^n pour tout $n \geq 0$. Il revient au même de prouver que le groupe de Galois $\mathrm{Gal}(L/K)$, où L est la ℓ-extension abélienne non ramifiée maximale de K est un module de type fini sur l'anneau $\varprojlim \mathbb{Z}_\ell[\mathrm{Gal}(k_n/k)]$, annulé par une puissance de ℓ.

§ 4. Des critères analytiques

Notations : p et ℓ sont des nombres premiers (non nécessairement distincts). On pose $q = p$ si $p \neq 2$ et $q = 4$ si $p = 2$. Soit α un entier p-adique ; pour tout $m \geq 0$, notons $s_m(\alpha)$ l'unique entier vérifiant

$$0 \leq s_m(\alpha) < qp^m \quad \text{et} \quad \alpha \equiv s_m(\alpha) \mod. qp^m .$$

Si p est différent de 2 et si $\sum_{r=0}^{\infty} t_r(\alpha)p^r$ est l'unique développement de α tel que $t_r(\alpha) \in \{0, 1, \ldots, p-1\}$, on a $s_m(\alpha) = \sum_{r=0}^{m} t_r(\alpha)p^r$. Notons R un système de représentants du groupe H des racines de l'unité de $\mathbb{Z}_p$ modulo $\{1,-1\}$ (H est d'ordre $p-1$ si $p \neq 2$ et d'ordre 2 si $p = 2$).

Soient $K = \bigcup_{n \geq 0} k_n$ la $\mathbb{Z}_p$-extension cyclotomique d'un corps de nombres k abélien sur $\mathbb{Q}$ et k' le plus grand sous-corps de k dont le conducteur n'est pas divisible par qp. Il existe un entier $e \geq 0$ tel que $k_n = k'_{n+e}$ pour tout $n \geq 0$ ([19]). Par suite, quitte à remplacer k par $k'(\zeta_{2\ell})$, on peut, d'après le théorème 2 (i), et l'énoncé analogue cité au § 2, supposer pour la démonstration des théorèmes 3 et 4 la condition suivante satisfaite :

k est un corps de nombres abélien sur $\mathbb{Q}$, contenant les racines 2ℓ-ièmes de l'unité, et dont le conducteur n'est pas divisible par qp.

Le corps k est alors totalement imaginaire. Notons k^+, k_n^+, K^+ les sous-corps totalement réels maximaux de k, k_n, K respectivement. La $\mathbb{Z}_p$-extension cyclotomique de k^+ est $K^+ = \bigcup_{n \geq 0} k_n^+$. Pour tout $n \geq 0$, on a $h_n = h_n^+ h_n^-$, où h_n^- est un entier appelé "premier facteur du nombre de classes de k_n".

Notons $e_n^{+(\ell)}$ (resp. $e_n^{-(\ell)}$) l'exposant de ℓ dans h_n^+ (resp. h_n^-). Il existe des entiers naturels μ^+, μ^-, λ^+ et λ^- tels que

$$e_n^{+(p)} \sim \mu^+ p^n + \lambda^+ n$$
$$e_n^{-(p)} \sim \mu^- p^n + \lambda^- n .$$

Comme k contient les racines 2ℓ-ièmes de l'unité, l'inégalité du miroir (Spiegelungsatz de Leopoldt) entraîne les résultats suivants ([3] et [20]) :

$$\mu^- = 0 \quad \Longrightarrow \quad \mu = 0$$

$$e_n^{-(\ell)} \sim 0 \quad \Longrightarrow \quad e_n^{(\ell)} \sim 0 \qquad \text{si} \quad \ell \neq p \ .$$

Ceci permet de se limiter à étudier h_n^-, pour lequel on dispose de la formule explicite suivante ([6]) :

$$(1) \qquad h_n^- = Q_n \, w_n \prod_{\chi} \left(-\frac{1}{2} B_{1,\chi} \right) \ ,$$

où :

- Q_n est un entier égal à 1 ou 2 ;
- w_n est le nombre de racines de l'unité contenues dans k_n ; on a $w_n = w_o \, p^n$ si $\mathbb{Q}(\zeta_q) \subset k$ et $w_n = w_o$ sinon ;
- χ décrit l'ensemble des caractères de Dirichlet impairs attachés à l'extension k_n de $\mathbb{Q}$. Ce sont les caractères de la forme $\lambda\psi$, où λ décrit l'ensemble des caractères de Dirichlet impairs attachés à l'extension k de $\mathbb{Q}$, et où ψ décrit le groupe cyclique D_n des caractères de Dirichlet attachés à l'unique extension cyclique de degré p^n de $\mathbb{Q}$ contenue dans B_p ;
- pour tout caractère de Dirichlet impair χ, de conducteur f_χ, on a :

$$B_{1,\chi} = \frac{1}{f_\chi} \sum_{a=0}^{f_\chi - 1} a \, \chi(a) \ .$$

A) Le cas où $\ell = p$.

a) Cas où $k = \mathbb{Q}(\zeta_p)$ et $p \neq 2$.

PROPOSITION 1.- *Supposons $p \neq 2$. Si $\mu_p(\mathbb{Q}(\zeta_p)) > 0$, il existe un entier impair d tel que la classe résiduelle de la somme $\sum_{\eta \in R} t_n(\alpha\eta)\eta^d$ modulo p soit indépendante de l'entier $n \geq 0$ et de l'élément α de $\mathbb{Z}_p^*$.*

Cette proposition n'est qu'une reformulation d'un critère démontré par Iwasawa dès 1958 ([8]) en utilisant les renseignements sur le groupe des classes d'idéaux de k_n fournis par la condition $\mu^- > 0$ et le théorème de Stickelberger.

b) Cas général.

Soient Ω une clôture algébrique de $\mathbb{Q}_p$, w une valuation de Ω prolongeant la valuation normalisée de $\mathbb{Q}_p$, $\mathcal{O}$ et $\mathfrak{p}$ l'anneau et l'idéal de la valuation w. Soit Λ l'ensemble des séries formelles $f \in \mathcal{O}[[T]]$ dont les coefficients engendrent une extension finie de $\mathbb{Q}_p$, de sorte que $f(\alpha) \in \mathcal{O}$ soit défini pour tout $\alpha \in \mathfrak{p}$. Si $f = \sum_{n=0}^{\infty} a_n T^n$ appartient à Λ, on pose

$$\mu(f) = \inf_{n \geq 0} w(a_n) .$$

Notons A (resp. A') l'ensemble des caractères de Dirichlet impairs attachés à $k/\mathbb{Q}$ (resp. à $\mathbb{Q}(\zeta_q)/\mathbb{Q}$). La construction des séries L p-adiques par Iwasawa ([12]) montre qu'il existe, pour tout $\lambda \in A - A'$, une série formelle $f_\lambda \in \Lambda$ vérifiant la condition suivante :

Pour tout $n > 0$, il existe une bijection $\psi \longmapsto \zeta_\psi$ de $D_n - \{1\}$ sur l'ensemble des racines p^n-ièmes de l'unité dans Ω , distinctes de 1 , telle que :

$$\forall\ \psi \in D_n - \{1\} , \qquad f_\lambda(\zeta_\psi - 1) = -\frac{1}{2} B_{1,\lambda\psi} .$$

Il résulte alors facilement de la formule (1), appliquée successivement pour k et pour $\mathbb{Q}(\zeta_q)$, qu'on a :

$$\mu_p^-(k) - \mu_p^-(\mathbb{Q}(\zeta_q)) = \sum_{\lambda \in A - A'} \mu(f_\lambda) . \tag{2}$$

PROPOSITION 2.- S'il existe un corps de nombres k abélien sur $\mathbb{Q}$ tel que $\mu_p(k) > 0$, l'une des conditions suivantes est réalisée :

a) On a $\mu_p(\mathbb{Q}(\zeta_q)) > 0$.

b) Il existe un caractère de Dirichlet impair λ de conducteur d ou dq , avec $d \neq 1$ et $(d,p) = 1$, tel que, pour tout $n \geq 0$, et tout $\alpha \in \mathbb{Z}_p$, on ait :

$$\sum_{\eta \in R} \sum_{i=0}^{d-1} i\, \lambda(s_n(\alpha\eta) + iqp^n) \equiv 0 \mod \mathfrak{P} . \tag{3}$$

En vertu de (2), il suffit de montrer que pour un caractère de Dirichlet impair λ , de conducteur d ou dq , avec $d \neq 1$ et $(d,p) = 1$, et tel que $\mu(f_\lambda)$ soit non nul, on a les congruences (3) pour tout $n \geq 0$ et tout $\alpha \in \mathbb{Z}_p$. Mais ceci résulte des congruences mêmes utilisées par Iwasawa pour définir les séries formelles f_λ , ainsi que le remarque Ferrero ([3]).

B) Cas où $\ell \neq p$.

Il est facile de voir que la suite $e_n^{-(\ell)}$ est croissante ; par suite elle est bornée si et seulement si on a $e_n^{-(\ell)} \sim 0$.

Soient v une valuation de $\overline{\mathbb{Q}}$ prolongeant la valuation normalisée de $\mathbb{Q}$ et $\mathfrak{P}$ son idéal. Notons D'_n l'ensemble $D_n - D_{n-1}$ si $n \geq 1$; lorsque $p \neq 2$, D'_n est l'ensemble des caractères de Dirichlet impairs d'ordre p^n et de conducteur p^{n+1} .

D'après la formule (1), si la suite $e_n^{-(\ell)}$ n'est pas bornée, il existe $\lambda \in A$ tel que pour une infinité d'entiers $m \geq 1$ on ait $v(\frac{1}{2} B_{1,\lambda\psi}) > 0$ pour au moins un caractère ψ appartenant à D'_m . Le conducteur de λ est égal à d ou

dq , avec $(d,p) = 1$.

Si $m \geq 1$, le corps $F_m = \mathbb{Q}(\lambda , \psi_m)$ des valeurs prises par λ et ψ_m est indépendant du choix de ψ_m dans D'_m . Soit m suffisamment grand pour que F_{m+1} soit distinct de F_m et que l'idéal premier défini par v dans F_m soit inerte dans F_{n+m} , pour tout $n \geq 0$. Alors, pour tout $\psi \in D_{n+m}$ et tout $\alpha \in \mathbb{Z}_p^*$, on a

$$(4) \quad v(\tfrac{1}{2} B_{1,\lambda\psi}) > 0 \implies v(\mathrm{Tr}_{F_{m+n}/F_m}(\tfrac{1}{2} \psi(\alpha)^{-1} B_{1,\lambda\psi})) > 0 ,$$

ψ étant étendu par continuité à $\mathbb{Z}_p$, et un calcul immédiat ([20]) montre que l'on a :

$$\mathrm{Tr}_{F_{m+n}/F_m}(\tfrac{1}{2} \psi(\alpha)^{-1} B_{1,\lambda\psi}) = \frac{p^{n-m}}{d} \psi(\alpha)^{-1} \sum_{\eta \in R} \sum_{i=0}^{dp^m - 1} i \, \lambda\psi(s_n(\alpha\eta) + iqp^n) .$$

Nous avons ainsi obtenu la proposition suivante.

PROPOSITION 3.- *Soit ℓ un nombre premier distinct de p . S'il existe un corps de nombres k abélien sur $\mathbb{Q}$ pour lequel on n'ait pas $e_n^{(\ell)} \sim 0$, il existe un caractère de Dirichlet impair λ de conducteur d ou dq , avec $(d,p) = 1$, vérifiant la condition suivante :*

Il existe un entier $m \geq 1$ et une infinité d'entiers $n \geq 0$, tels que, pour un élément ψ de D'_{n+m} au moins, on ait :

$$(5) \quad \forall \alpha \in \mathbb{Z}_p^* , \quad \frac{\psi(\alpha)^{-1}}{d} \sum_{\eta \in R} \sum_{i=0}^{dp^m - 1} i \, \lambda\psi(s_n(\alpha\eta) + iqp^n) \equiv 0 \mod \mathfrak{L} .$$

§ 5. Démonstration des théorèmes 3 et 4

Pour un choix convenable de R , on a :

PROPOSITION 4.- *Soient m et d deux entiers > 0 , d étant premier à p . Pour tout n assez grand, il existe deux entiers p-adiques α_1 et α_2 , congrus à 1 modulo p^m et un élément η_o de R tels que :*

$$s_{n+m}(\alpha_1\eta) = s_n(\alpha_1\eta) \equiv 0 \mod d \text{ pour tout } \eta \in R ;$$

$$s_{n+m}(\alpha_2\eta) = s_n(\alpha_2\eta) \equiv 0 \mod d \text{ pour tout } \eta \in R , \eta \neq \eta_o ;$$

$$s_{n+m}(\alpha_2\eta_o) = s_n(\alpha_2\eta) + qp^n \equiv 0 \mod d .$$

Cinq propositions analogues ont été utilisées par Ferrero et Washington pour prouver les théorèmes 3 et 4, et Roland Gillard a remarqué que dans tous les cas, on peut leur substituer la proposition 4 précédente ([5]). Nous repoussons la démonstration de cette proposition au § 6.

A) Démonstration du théorème 3.

a) Cas où $k = \mathbb{Q}(\zeta_q)$.

Comme 2 est régulier, on peut supposer $p \neq 2$. Appliquons alors la proposition 4 avec $m = 1$ et $d = 1$. Il existe un entier $n \geq 0$, deux entiers p-adiques α_1 et α_2 et un élément η_o de R tels que

$$t_{n+1}(\alpha_1\eta) = t_{n+1}(\alpha_2\eta) = 0 \quad \text{pour tout } \eta \in R,\ \eta \neq \eta_o ;$$

$$t_{n+1}(\alpha_1\eta_o) = 0$$

$$t_{n+1}(\alpha_2\eta_o) = 1 .$$

La conclusion résulte donc de la proposition 1.

b) Cas général.

Supposons $\mu_p(k) > 0$. D'après a), la condition b) de la proposition 2 est satisfaite pour un certain caractère λ de conducteur d ou dq , avec $(d,p) = 1$ et $d \neq 1$. Appliquons la proposition 4 avec $m = 2$. Il existe un entier $n \geq 0$, deux entiers p-adiques α_1 et α_2 congrus à 1 modulo q et un élément η_o de R satisfaisant aux conditions de la proposition 4. En particulier, si η est différent de η_o , on a :

$$s_n(\alpha_1\eta) \equiv \eta \equiv s_n(\alpha_2\eta) \mod q$$

$$s_n(\alpha_1\eta) \equiv 0 \equiv s_n(\alpha_2\eta) \mod d$$

et par suite $\lambda(s_n(\alpha_1\eta) + iqp^n) = \lambda(s_n(\alpha_2\eta) + iqp^n)$ pour tout $i < d$. On démontre de même la congruence

$$s_n(\alpha_2\eta_o) \equiv s_n(\alpha_1\eta_o) - qp^n \mod dq .$$

Posons $a = s_n(\alpha_1\eta_o)$. La condition b) de la proposition 2 entraîne :

$$\sum_{i=0}^{d-1} i\,\lambda(a + iqp^n) \equiv \sum_{i=0}^{d-1} i\,\lambda(a + (i-1)qp^n) \mod \mathfrak{P} .$$

Or on a $\sum_{i=0}^{d-1} \lambda(a + iqp^n) = 0$, car le conducteur de λ ne divise pas qp^n . Il en résulte :

$$\sum_{i=0}^{d-1} (i+1)\,\lambda(a + iqp^n) \equiv \sum_{i=0}^{d-1} i\,\lambda(a + (i-1)qp^n) \mod \mathfrak{P} ,$$

d'où

$$d\lambda(a + (d-1)qp^n) \equiv 0 \mod \mathfrak{P} .$$

Ceci est absurde car $a + (d-1)qp^n$ est premier à dq : en effet

$$a + (d-1)qp^n \equiv a \equiv \eta_o \mod q$$

$$a + (d-1)qp^n \equiv a - qp^n \equiv -qp^n \mod d .$$

B) Démonstration du théorème 4.

Supposons que l'on n'ait pas $e_n^{(\ell)} \sim 0$. Il existe d'après la proposition 3 un caractère λ de conducteur d ou dq , avec $(d,p) = 1$, un entier $m \geq 1$ et une infinité d'entiers $n \geq 0$ tels que pour un élément ψ de D'_{n+m} au moins on ait les congruences (5). Choisissons n assez grand pour que les conditions de la proposition 4 soient satisfaites par des entiers p-adiques α_1 et α_2 et par un élément η_o de R . On a en particulier, pour $\alpha = \alpha_1$ et $\alpha = \alpha_2$ et pour $\eta \in R$:

$$\alpha^{-1}(s_{n+m}(\alpha\eta) + iqp^n) \equiv \eta + iqp^n \quad \text{modulo} \quad p^{n+m} .$$

On montre alors, comme en A) b), que l'on a :

$$\frac{1}{d}\sum_{i=0}^{dp^m-1} i\ \lambda(a + iqp^n)\psi(\eta_o + iqp^n) \equiv \frac{1}{d}\sum_{i=0}^{dp^m-1} i\lambda(a + (i-1)qp^n)\psi(\eta_o + (i-1)qp^n) \quad \text{mod. } \mathfrak{L} ,$$

en posant $a = s_n(\alpha_1\eta_o)$, et que ceci entraîne la congruence :

$$\frac{1}{d}\, dp^m\, \lambda(a + (dp^n - 1)qp^n)\psi(\eta_o + (dp^m - 1)qp^n) \equiv 0 \quad \text{mod. } \mathfrak{L} ,$$

ce qui est absurde car $a + (dp^m - 1)qp^n$ est premier à dp et $\eta_o + (dp^m - 1)qp^n$ est premier à p . D'où le résultat.

§ 6. Démonstration de la proposition 4

Rappelons ([17]) qu'une suite a_n d'éléments de $[0,1[^r$ est dite équirépartie dans $[0,1[^r$ si pour tout pavé Δ contenu dans $[0,1[^r$, l'ensemble des entiers n tels que $a_n \in \Delta$ a pour densité $\mu(\Delta)$, μ étant la mesure de Lebesgue sur $\mathbb{R}^r$ telle que $\mu([0,1[^r) = 1$. Le critère de Weyl ([17]) affirme qu'une condition nécessaire et suffisante pour que la suite $n \longmapsto (a_{n,1}, \ldots, a_{n,r})$ soit équirépartie est que, pour tout élément non nul $(t_1,\ldots,t_r)$ de $\mathbb{Z}^r$, on ait :

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N} \exp(2\pi i \sum_{j=1}^{r} t_j\, a_{n,j}) = 0 .$$

PROPOSITION 5.- *Soient $\gamma_1,\ldots,\gamma_r$ des entiers p-adiques $\mathbb{Q}$-linéairement indépendants. Alors pour presque tout $\alpha \in \mathbb{Z}_p$ (au sens de la mesure de Haar), la suite $n \longmapsto a_n = (a_{n,1}, \ldots, a_{n,r})$, où $a_{n,j} = p^{-n}q^{-1}s_n(\alpha\gamma_j)$ est équirépartie*

Soit $t = (t_1,\ldots,t_r) \in \mathbb{Z}^r - \{0\}$. On a $\exp(2\pi i \sum_{j=1}^{r} t_j a_{n,j}) = \exp(2\pi i p^{-n-1} s_n(\alpha\beta_t))$ où $\beta_t = \sum_{j=1}^{r} t_j\gamma_j$ est un entier p-adique non nul. Il est immédiat que la suite

$p^{-n}q^{-1}s_n(\alpha\beta_\ell)$ est équirépartie dans $[0,1[$ pour presque tout α, et la proposition en résulte, puisque $\mathbb{Z}^r$ est dénombrable.

PROPOSITION 6.- *Soient $\gamma_1,\dots,\gamma_r$ des entiers p-adiques $\mathbb{Q}$-linéairement indépendants, $\varepsilon > 0$ un nombre réel, $m > 0$ un entier, $A \in \mathbb{Z}_p$ un entier p-adique, $d > 0$ un entier premier à p, et $(x_1,\dots,x_r)$ un élément de $]0,1[^r$. Pour tout entier n assez grand, il existe $\alpha \in \mathbb{Z}_p$ vérifiant :*

(i) $\alpha \equiv A \mod p^m$;

(ii) $\left|p^{-n}q^{-1}s_n(\alpha\gamma_j) - x_j\right| \le \varepsilon$ *pour tout* $j \le r$;

(iii) $s_n(\alpha\gamma_j) \equiv 0 \mod d$ *pour tout* $j < r$.

Posons $A' = \frac{A}{d}$, $x = (x_1,\dots,x_r)$, $\gamma = (\gamma_1,\dots,\gamma_r)$, $x' = \frac{x}{d}$ et $\varepsilon' = \frac{\varepsilon}{2d}$. Supposons en outre ε suffisamment petit pour que $[x_j - \varepsilon, x_j + \varepsilon]$ soit inclus dans $]0,1[$ pour tout $j \le r$.

Si $\beta = (\beta_1,\dots,\beta_r) \in \mathbb{Z}_p^r$, notons $a_n(\beta)$ l'élément de $[0,1[^r$ dont la j-ième coordonnée est $p^{-n}q^{-1}s_n(\beta_j)$. Si $y \in \mathbb{R}^r$ et $z \in \mathbb{R}^r$, posons

$$\|y - z\| = \inf_{u \in z + \mathbb{Z}^r} |y - u| .$$

Par passage au quotient, $(y,z) \mapsto \|y - z\|$ définit une distance sur $\mathbb{R}^r/\mathbb{Z}^r$. Comme $\mathbb{R}^r/\mathbb{Z}^r$ est compact, il existe une suite finie $y_1,\dots,y_D$ d'éléments de $\mathbb{R}^r$ telle que :

$$\forall\, z \in \mathbb{R}^r, \ \exists\, i \le D, \quad \|z - y_i\| \le \varepsilon' .$$

Appliquant la proposition 5, on trouve, pour tout $i \le D$ un entier $n_i \ge 0$ et un entier p-adique α_i tels que

$$\|a_{n_i}(\alpha_i\gamma) - y_i\| \le \varepsilon' .$$

Posons $n_o = m + \sup_{i \le R} n_i$. Soit $n \ge n_o$.

Par définition des y_i, il existe $i \le D$ tel que l'on ait :

$$\|x' - a_n(A'\gamma) - y_i\| \le \varepsilon' .$$

Posons $\alpha' = A' + p^{n-n_i}\alpha_i$. On a $\alpha' \equiv A' \mod p^m$ et

$$\|a_n(A'\gamma) + a_{n_i}(\alpha_i\gamma) - a_n(\alpha'\gamma)\| = 0 ,$$

d'où $\|x' - a_n(\alpha'\gamma)\| \le 2\varepsilon' = \frac{\varepsilon}{d}$ par l'inégalité triangulaire, et donc

$$p^{-n}q^{-1}s_n(\alpha'\gamma_j) \in \left[\frac{x_j - \varepsilon}{d}, \frac{x_j + \varepsilon}{d}\right] \quad \text{pour tout } j \le r .$$

Si on pose $\alpha = d\alpha'$, on a $s_n(\alpha\gamma_j) = ds_n(\alpha'\gamma_j)$ et α satisfait aux conditions requises.

Démontrons maintenant la proposition 4. Elle résulte immédiatement de la proposition 6 lorsque les éléments de R sont $\mathbb{Q}$-linéairement indépendants ; nous pouvons donc supposer p impair et s strictement supérieur à r, en posant

$$s = \frac{p-1}{2} \quad \text{et} \quad r = \varphi(p-1) .$$

Quitte à changer les éléments de R de signe, on peut s'arranger pour que R soit égal à $\{\eta_1,\dots,\eta_s\}$, les propriétés suivantes étant satisfaites [4] :

(i) Les η_j, pour $j \leq r$, sont $\mathbb{Q}$-linéairement indépendants.

(ii) Si $r < i \leq s$, on a $\eta_i = \sum_{j=1}^{r} a_{ij}\eta_j$, avec $a_{ij} \in \mathbb{Z}$.

(iii) Si $r < i \leq s$ et si j est le plus petit indice tel que $a_{ij} \neq 0$, on a $a_{ij} > 0$.

(iv) Si $r < i < s$ et si j est le plus petit indice tel que $a_{ij} \neq a_{sj}$, on a $a_{ij} < a_{sj}$; on a en outre $a_{s1} > 0$ et $a_{sj} \geq 0$ pour tout $j \leq r$.

Si $1 \leq i \leq r$, posons $x'_i = \rho^i$; si $r < i \leq s$, posons $x_i = \sum_{j=1}^{r} a_{ij} x_j$.

Lorsque $\rho > 0$ est suffisamment petit, les conditions suivantes sont réalisées :

(i') Pour tout i tel que $1 \leq i \leq s$, on a $x'_i > 0$ (d'après (iii)).

(ii') Pour tout i tel que $1 \leq i < s$, on a $x'_i < x'_s$ (d'après (iv)).

Par suite, pour un choix convenable de la constante c, on a, en posant $x_i = cx'_i$:

$$0 < x_i < p^{-m} \quad \text{si} \quad 1 \leq i < s ,$$

$$p^{-m} < x_s < 2p^{-m} .$$

Choisissons ε suffisamment petit pour que, quel que soit $n \geq 0$, les inégalités $|p^{-n-1}s_n(\alpha\eta_j) - x_j| \leq \varepsilon$ pour $j \leq r$ impliquent :

$$\begin{cases} s_n(\alpha\eta_i) = \sum_{j=1}^{r} a_{ij}\, s_n(\alpha\eta_j) & \text{si} \quad r < i \leq s, \\ 0 < p^{-n-1}s_n(\alpha\eta_i) < p^{-m} & \text{si} \quad 1 \leq i < s , \\ p^{-m} < p^{-n-1}s_n(\alpha\eta_s) < 2p^{-m} . \end{cases}$$

La proposition 6 montre qu'il existe, pour tout n assez grand, un entier p-adique α_2 vérifiant les conditions suivantes :

$$\alpha_2 \equiv 1 \mod. p^m$$

$$s_{n+m}(\alpha_2\eta_j) \equiv 0 \mod. d \quad \text{si} \quad 1 \leq j \leq r$$

$$|p^{-n-m-1}s_{n+m}(\alpha\eta_j) - x_j| \leq \varepsilon \quad \text{si} \quad 1 \leq j \leq r .$$

L'entier α_2 satisfait aux conditions de la proposition 4 (en posant $\eta_o = \eta_s$).

On démontre de même l'existence de α_1, en choisissant cette fois-ci la constante c de telle sorte que l'on ait $0 < x_i < p^{-m}$ pour tout $i \leq s$.

BIBLIOGRAPHIE

[1] J. COATES - p-adic L-functions and Iwasawa's theory, Algebraic Number Fields, Academic Press, London, 1977, 269-353.

[2] R. ERNVALL and T. METSÄNKYLÄ - Cyclotomic invariants and E-irregular primes, Math. of Comp., 32(1978).

[3] B. FERRERO - Iwasawa invariants of abelian number fields, Math. Ann., 234 (1978), 9-24.

[4] B. FERRERO and L. WASHINGTON - The Iwasawa invariant μ_p vanishes for abelian number fields, Annals of Math., à paraître.

[5] R. GILLARD - Extensions abéliennes et répartition modulo 1 , dans "Journées arithmétiques de Marseille", Astérisque, vol. 61 , 1979, à paraître.

[6] H. HASSE - Über die Klassenzahl abelscher Zahlkörper, Akademie-Verlag Berlin, 1952.

[7] K. IWASAWA - A note on class numbers of algebraic number fields, Abh. Math. Sem. Hamb., 20 (1956), 257-258.

[8] K. IWASAWA - On some invariants of cyclotomic fields, Amer. J. Math., 80(1958), 773-783 ; erratum 81(1959), 280.

[9] K. IWASAWA - On Γ-extensions of algebraic number fields, Bull. Amer. Math. Soc., 65(1959), 183-226.

[10] K. IWASAWA - On p-adic L-functions, Ann. of Math., 89(1969), 198-205.

[11] K. IWASAWA - On some infinite abelian extensions of algebraic number fields, Actes , Congrès Intern.Math., 1970, tome 1, 391-394.

[12] K. IWASAWA - Lectures on p-adic L-functions, Princeton University Press, 1972.

[13] K. IWASAWA - On the μ-invariants of $\mathbb{Z}_p$-extensions, Number Theory, Algebraic Geometry and Commutative Algebra, in honour of Y. Akizuki, Kinokuniya, Tokyo, 1973, 1-11.

[14] K. IWASAWA and C. SIMS - Computations of invariants in the theory of cyclotomic fields, J. Math. Soc. Japan, 18(1966), 86-96.

[15] W. JOHNSON - On the vanishing of the Iwasawa invariant μ_p for $p < 8000$, Math. Comp., 27(1973), 387-396.

[16] W. JOHNSON - Irregular primes and cyclotomic invariants, Math. Comp., 29(1975), 653-657.

[17] L. KUIPERS and H. NIEDERREITER - Uniform distribution of sequences, Wiley-Interscience, 1974.

[18] J.-P. SERRE - Classes des corps cyclotomiques, Séminaire Bourbaki, Exposé 174, Décembre 1958, W. Benjamin/Addison-Wesley, N.Y.

[19] S. WAGSTAFF, Jr. - The irregular primes to 125 000 , Math. of Comp., 32 (1978), 583-591.

[20] L. WASHINGTON - Class numbers and $\mathbb{Z}_p$-extensions, Math. Ann., 214(1975), 177-193.

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