Astérisque

R. GILLARD

Extensions abéliennes et répartition modulo 1

Astérisque, tome 61 (1979), p. 83-93

<http://www.numdam.org/item?id=AST_1979__61__83_0>

Société Mathématique de France
Astérisque 61 (1979) p. 83-93

EXTENSIONS ABÉLIENNES ET RÉPARTITION MODULO 1

par R. GILLARD

Je me propose d'exposer les importants résultats de B. Ferrero et L. Washington, cf. [2] et [13]. Pour les détails et les démonstrations complètes, je renvoie à leurs articles. Par ailleurs, ceux-ci rappellent les preuves de la plupart des préliminaires utilisés. La différence principale avec la conférence donnée à Luminy est l'unification des démonstrations à l'aide d'un résultat de [13].

§ 1. - RÉSULTATS.

Soient p (resp. ℓ) un nombre premier et k un corps de nombres de degré fini sur $\mathbb{Q}$. Désignons par k_∞/k une $\mathbb{Z}_p$-extension, i.e. une extension galoisienne avec $\mathrm{Gal}(k_\infty/k) \simeq \mathbb{Z}_p$. Ainsi on peut écrire

$$k_\infty = \bigcup_{n\in\mathbb{N}} k_n \quad \text{avec} \quad \mathrm{Gal}(k_n/k) \simeq \mathbb{Z}/p^n\mathbb{Z} .$$

Notons h_n le nombre de classes de k_n et $e_n^{(\ell)}$ l'exposant de ℓ dans h_n ; si $\ell = p$, K. Iwasawa a démontré :

THÉORÈME 1, [4]. - *Il existe des entiers* λ, μ, ν *avec* $\lambda \geq 0$, $\mu \geq 0$ *tels que* $e_n^{(p)} = \mu p^n + \lambda n + \nu$ *pour tout* n *assez grand*.

Exemple fondamental : $k = \mathbb{Q}(\zeta_p)$, $k_n = \mathbb{Q}\left(\zeta_{p^{n+1}}\right)$, $k_\infty = \bigcup_{n\in\mathbb{N}} k_n$, avec $p \neq 2$, où pour $m \in \mathbb{N}$, ζ_m désigne une racine primitive $m^{\text{ième}}$ de l'unité. On savait que μ est nul dans les cas suivants :

- $e_o^{(p)} = 0$, i.e. p est régulier.
- $p \leq 4\,000$, cf. [5].
- $p \leq 8\,000$, cf. [7].
- $p \leq 30\,000$, cf. [8].
- $p \leq 125\,000$, cf. [11].

Remarque : Iwasawa a construit des $\mathbb{Z}_p$-extensions dont l'invariant μ est > 0 , cf. [6].

Désignons par $\mathbb{Q}_\infty$ l'unique $\mathbb{Z}_p$-extension de $\mathbb{Q}$. Dans la suite, nous supposons que k est une extension abélienne de $\mathbb{Q}$ et que k_∞ est l'extension composée $k.\mathbb{Q}_\infty$. Notons $\mu(k)$ l'invariant μ pour cette $\mathbb{Z}_p$-extension de k .

THÉORÈME 2, [1]. -
1) Si $e_o^{(p)} = 0$ et k contient ζ_p , alors $\mu(k) = 0$.
2) Si $p = 2$ ou 3 , alors $\mu(k) = 0$.

La partie 2) résulte du fait qu'on a à considérer (cf. plus loin) des sommes sur un 1/2 système de racines de l'unité dans $\mathbb{Z}_p$. Ainsi, pour $p = 2$ ou 3 ces sommes se réduisent à un seul terme et cette simplification permet de conclure.

THÉORÈME 3, [2]. - Pour tout k , on a $\mu(k) = 0$.

La démonstration de ce théorème, comme celle de la partie 1) du théorème 2, utilise des arguments de répartition modulo 1 ; ceux employés dans [2] sont plus forts et plus naturels que ceux de [1].

Soient S un ensemble d'idéaux premiers de k contenant les diviseurs premiers de p et k_S la p-extension de k non ramifiée en dehors de S maximale : k_S contient k_∞ et en est une extension galoisienne.

COROLLAIRE. - Si k contient ζ_p (ζ_4 si $p = 2$) , $\mathrm{Gal}(k_S/k_\infty)$ est un pro-p-groupe libre.

En effet, on sait, [10], que ceci est une conséquence de $\mu(k) = 0$.

THÉORÈME 4, [13]. - Pour k et ℓ fixés, avec $\ell \neq p$, la suite $e_n^{(\ell)}$ est stationnaire.

Remarquons que pour $p = 2$ ou 3 , ce résultat est déjà dans [12] qui utilise la même simplification que pour la partie 2) du théorème 2.

Signalons enfin que les démonstrations des résultats précédents peuvent être rendues effectives (cf. [2] § 4) et peuvent donner pour k , ℓ , p fixés des bornes pour l'invariant λ du théorème 1 et pour le plus petit indice n_o tel que $e_{n_o}^{(\ell)} = e_{n_o+1}^{(\ell)}$.

Notations. - Désignons par Ω_p (resp. Ω_ℓ) une clôture algébrique de $\mathbb{Q}_p$ (resp. $\mathbb{Q}_\ell$) et par $\mathfrak{P}$ (resp. $\mathfrak{L}$) son idéal maximal. Désignons par R un système de représentants des racines de l'unité de $\mathbb{Z}_p$ modulo ± 1 . On suppose dans la suite $p \neq 2$. Si $\alpha \in \mathbb{Z}_p$, on note $t_m(\alpha)$ le $m^{\text{ième}}$ coefficient de son développement p-adique et $s_n(\alpha)$ la $n^{\text{ième}}$ somme partielle :

$$\alpha = \sum_0^\infty t_m(\alpha) p^m \quad \text{avec} \quad 0 \leq t_m(\alpha) < p \ ,$$

$$s_n(\alpha) = \sum_0^n t_m(\alpha) p^m \quad \text{d'où} \quad 0 \leq s_n(\alpha) < p^{n+1} \quad \text{et} \quad s_n(\alpha) \equiv \alpha \bmod p^{n+1} \ .$$

§ 2. - RÉPARTITION MODULO 1 DES $p^{-n-1} s_n(\alpha\eta)$, $\alpha \in \mathbb{Z}_p^*$, $\eta \in R$.

2.1. Introduisons le concept clef de [2] :

DÉFINITION. - *Des entiers p-adiques $\gamma_1, \ldots, \gamma_r$ sont dits conjointement normaux si et seulement si la suite $(p^{-n-1} s_n(\gamma_1), \ldots, p^{-n-1} s_n(\gamma_r))_{n \geq 0}$ est uniformément répartie dans $([0,1[)^r$.*

Cette définition transpose aux nombres p-adiques une définition classique ([9] chap. I, § 8, notes) en répartition modulo 1 pour les nombres réels ; il faut remplacer $1/p$ par p dans les développements p-adiques.

Pour $k \in \mathbb{N}^*$, soit $\mathfrak{M}_k$ l'ensemble des matrices c à r lignes et k colonnes dont les coefficients c_{ij} sont des entiers vérifiant $0 \leq c_{ij} < p$. Pour toute matrice c dans $\mathfrak{M}_k$, désignons par $S(c)$ l'ensemble des entiers $n \geq 1$ vérifiant

$$t_{n+j}(\gamma_i) = c_{ij} \quad \text{pour tout} \quad i = 1, \ldots, r \quad \text{et} \quad j = 1, \ldots, k \ .$$

En traduisant sur les chiffres du développement p-adique la condition

$$p^{-n-1}s_n(\gamma_i) \in [p^{-N}a_i\ ,\ p^{-N}(a_i+1)[\quad ,\ \text{pour}\quad N \in \mathbb{N}^*\ ,$$

on trouve :

PROPOSITION 1. - Les entiers p-adiques $\gamma_1,\ldots,\gamma_r$ sont conjointement normaux si et seulement si pour tout $k \in \mathbb{N}^*$ et tout $c \in \mathfrak{M}_k$, $S(c)$ admet une densité égale à p^{-rk}.

En s'inspirant d'une démonstration classique (cf. [9], théorème 4.1), Ferrero et Washington démontrent :

PROPOSITION 2. - 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), les nombres $\alpha\gamma_1,\ldots,\alpha\gamma_r$ sont conjointement normaux.

2.2. On peut renforcer l'énoncé précédent :

PROPOSITION 3, [13]. - Soient $\beta_1,\ldots,\beta_r$ des entiers p-adiques $\mathbb{Q}$-linéairement indépendants. Donnons-nous un nombre réel $\varepsilon > 0$, des entiers $m,d,g_1,\ldots,g_r$ vérifiant $m > 0$, $d > 0$, d premier à p, et des nombres réels $x_1,\ldots,x_r$ appartenant à $[0,1]$. Alors pour tout n entier assez grand, il existe un entier p-adique α vérifiant :

(1) $\alpha \equiv 1 \mod p^m$

(2) $s_n(\alpha\beta_j) \equiv g_j \mod d$, pour tout $j = 1,\ldots,r$

(3) $|p^{-n-1}s_n(\alpha\beta_j) - x_j| < \varepsilon$ pour tout $j = 1,\ldots,r$

Pour démontrer la proposition 3, Washington utilise la proposition 2 pour trouver un élément β de $\mathbb{Z}_p$ congru à 1 modulo p^m, tels que les nombres $\gamma_j = \beta\beta_j$ soient conjointement normaux ; si $c \in \mathfrak{M}_k$ pour k assez grand, choisissons $n_o \in S(c)$. Avec les données de la proposition 3, soit n entier supérieur ou égal à $n_o + k + m$. Washington construit une

matrice c telle que pour un entier convenable q , $n_o < q \leq n_o + k$, l'entier p-adique $\alpha = \beta(1+p^{n-q})$ vérifie les conditions (1), (2) et (3).

2.3. Nous utiliserons les résultats de 2.1 et 2.2 sous la forme suivante (cf. [13]) dont l'énoncé suppose R convenablement choisi :

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

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

(5) $s_{n+m}(\alpha_2\eta) = s_n(\alpha_2\eta) \equiv 0 \mod d$ pour tout $\eta \in R - \{\eta_o\}$

(6) $s_{n+m}(\alpha_2\eta_o) = s_n(\alpha_2\eta_o) + p^{n+1} \equiv 0 \mod d$.

Démonstration : Soient $\eta_1,\ldots,\eta_{(p-1)/2}$ les éléments de R ordonnés de façon à ce que $\eta_1,\ldots,\eta_r$ soient $\mathbb{Q}$-linéairement indépendants ($r=\varphi(p-1)$, φ fonction d'Euler). Pour $j = 1,\ldots,(p-1)/2$, on a

$$\eta_j = \sum_{i=1}^{r} a_{ji}\eta_i \quad \text{pour des } a_{ji} \text{ entiers.}$$

Soient $c_1 > \ldots > c_r$ des éléments de $]0,1]$ et posons

$$c_j = \sum_{i=1}^{r} a_{ji}c_i \quad \text{pour } j = r+1,\ldots,(p-1)/2 .$$

On peut choisir, cf. [2] ou [13], c_2 puis c_3 puis ... puis c_r suffisamment petits pour qu'il existe j_o tel que

$$0 < c_j < c_{j_o} \quad \text{pour tout } j \neq j_o ,$$

si R a été convenablement choisi. Choisissons x_{j_o} dans $]p^{-m},2p^{-m}[$ et posons $x_j = c_j x_{j_o}/c_{j_o}$. Supposons x_{j_o} suffisamment proche de p^{-m} pour avoir $x_j \in]0,p^{-m}[$ si $j \neq j_o$. Posons $g_j = 0$ et prenons ϵ suffisamment petit pour la suite. Soit α_2 un entier p-adique vérifiant les conditions de la proposition 3 avec $\beta_j = \eta_j$ si $j = 1,\ldots,r$ où n est remplacé par $n+m$: la condition (3) implique alors

$$0 < \sum_{i=1}^{r} a_{ji} s_{n+m}(\alpha_2 \eta_i) < p^{n+1} \quad \text{si} \quad j = 1,\ldots,(p-1)/2 \quad \text{et} \quad j \neq j_o$$

$$p^{n+1} < \sum_{i=1}^{r} a_{j_o i} s_{n+m}(\alpha_2 \eta_i) < 2p^{n+1} .$$

On en déduit les égalités

$$s_{n+m}(\alpha_2 \eta_j) = \sum_{i=1}^{r} a_{ji} s_{n+m}(\alpha_2 \eta_i) = s_n(\alpha_2 \eta_j) \quad \text{si} \quad j \neq j_o$$

$$s_{n+m}\left(\alpha_2 \eta_{j_o}\right) = \sum_{i=1}^{r} a_{j_o i} s_{n+m}(\alpha_2 \eta_i) = s_n\left(\alpha_2 \eta_{j_o}\right) + p^{n+1} .$$

Ainsi α_2 vérifie (5) et (6) avec $\eta_o = \eta_{j_o}$. Pour α_1 on procède de même, mais en choisissant x_{j_o} dans $]0, p^{-m}[$. Dans la proposition 4, on peut donc choisir η_o indépendant de n.

§ 3. - DÉMONSTRATION DU THÉORÈME 3 ($\ell = p$).

3.1. Supposons $k = \mathbb{Q}(\zeta_p)$. Rappelons le résultat de [3] §3 :

PROPOSITION 5. - $\mu(k)$ est non nul si et seulement s'il existe $a \in \mathbb{N}$, a impair, tel que pour tout $\alpha \in \mathbb{Z}_p^*$ et $n \in \mathbb{N}$, on ait

(7) $$\sum_{\eta \in \pm R} t_{n+1}(\alpha\eta).\eta^a \equiv 0 \mod \mathfrak{P} .$$

La démonstration d'Iwasawa utilise le théorème de Stickelberger sur l'annulation du groupe des classes. On peut aussi (cf. [2]) utiliser la formule analytique du nombre de classes en interprétant les nombres de Bernoulli avec les séries d'Iwasawa.

En regroupant les termes correspondants à η et $-\eta$, (7) s'écrit :

$$2 \sum_{\eta \in R} t_{n+1}(\alpha\eta).\eta^a - (p-1) \sum_{\eta \in R} \eta^a \equiv 0 \mod \mathfrak{P} .$$

Ainsi si $\mu(k)$ est $\neq 0$, il existe a impair tel que

(8) $$\sum_{\eta \in R} t_{n+1}(\alpha_1\eta)\eta^a \equiv \sum_{\eta \in R} t_{n+1}(\alpha_2\eta)\eta^a \mod \mathfrak{P}$$

pour tout $n \in \mathbb{N}$ et tout α_1, tout $\alpha_2 \in \mathbb{Z}_p^*$. Mais en choisissant α_1 et α_2 comme dans la proposition 4, on trouve

$t_{n+1}(\alpha_1\eta) = 0$ pour tout $\eta \in R$

$t_{n+1}(\alpha_2\eta) = 0$ pour tout $\eta \in R - \{\eta_o\}$, $t_{n+1}(\alpha_2\eta_o) = 1$.

En reportant dans (8), on obtient la contradiction

$$0 \equiv \eta_o^a \mod \mathfrak{P} ,$$

d'où le théorème 3 pour $k = \mathbb{Q}(\zeta_p)$.

3.2. Rappelons le résultat de [1] § 1.8 et 2.4 :

PROPOSITION 6. - Si $\mu(\mathbb{Q}(\zeta_p)) = 0$, alors il existe une extension abélienne finie k de $\mathbb{Q}$ avec $\mu(k) \neq 0$ si et seulement si on peut trouver un caractère de Dirichlet (*) χ , impair, tel que

(9) le conducteur f de χ est égal à d ou $d.p$ avec un entier $d \geq 2$, d premier à p .

(10) Pour tout $\alpha \in \mathbb{Z}_p^*$ et $n \in \mathbb{N}$ on a :
$$\sum_{\eta \in R} \sum_{i=0}^{d-1} i\chi(s_n(\alpha\eta) + p^{n+1}i) \equiv 0 \mod \mathfrak{P} .$$

La démonstration de Ferrero consiste à :

1) remarquer (cf. [12] lemme 1), que sans changer k_n pour n assez grand on peut supposer que p^2 ne divise pas le conducteur de k d'où la condition (9) ci-dessus (sachant que k n'est pas inclus dans $\mathbb{Q}(\zeta_p)$).

2) Montrer (cf. [1] § 1.7), en utilisant l'inégalité "du miroir" (Spiegelungsatz de H. Leopoldt) qu'on peut se limiter aux classes "relatives" i.e. aux caractères de Dirichlet impairs.

3) Utiliser la formule analytique du nombre de classes, en interprétant les nombres de Bernoulli en termes de série d'Iwasawa.

(*) à valeurs dans Ω_p .

Démonstration du théorème 3 : Soit χ un caractère de Dirichlet impair vérifiant (9) et (10). Choisissons n assez grand et vérifiant $p^n \equiv 1 \mod d$. Considérons alors la congruence (10) pour α_1 et α_2 comme dans la proposition 4 : seuls les termes relatifs à $\eta = \eta_o$ diffèrent ; en comparant on obtient :

$$(11) \qquad \sum_{i=0}^{d-1} i\chi(a+ip) \equiv \sum_{i=0}^{d-1} i\chi(a-p+ip) \mod \mathfrak{P} ,$$

où a désigne un entier multiple de d et congru à η_o modulo p. Or,

$$(12) \qquad \sum_{i=0}^{d-1} \chi(a+ip) = 0 .$$

Ceci est clair si tous les termes de la somme sont nuls ou si le conducteur de χ est égal à d. Sinon on se ramène à montrer que

$$\sum_{i=0}^{d-1} \chi(1+ip) = 0 \quad ;$$

la somme porte en fait sur le noyau de l'homomorphisme $(\mathbb{Z}/f\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$: sur ce groupe χ est $\neq 1$ car son conducteur est $\neq p$. En utilisant (12), on peut réécrire (11) sous la forme

$$\sum_{i=0}^{d-1} (i+1)\chi(a+ip) \equiv \sum_{i=0}^{d-1} i\chi(a+(i-1)p) \mod \mathfrak{P} .$$

Après simplification, il ne reste que le terme correspondant à $i = d-1$ dans la somme de gauche, i.e. :

$$(13) \qquad d\chi(a-p) \equiv 0 \mod \mathfrak{P} .$$

Comme $a-p$ est congru à $-p$ modulo d et à η_o modulo p, ce nombre est premier à $f = d$ ou dp ; $\chi(a-p)$, non nul, est donc une racine de l'unité : (13) est donc absurde.

§ 4. - DÉMONSTRATION DU THÉORÈME 4 ($\ell \neq p$) .

4.1. Pour $m \in \mathbb{N}$, soit D_m l'ensemble des caractères de Dirichlet à valeurs dans Ω_ℓ^* dont le conducteur et l'ordre valent respectivement p^m et p^{m+1}. Les éléments de D_m peuvent être prolongés en des fonctions continues de $\mathbb{Z}_p$ dans Ω_ℓ. Si ψ appartient à D_{n+m} et α à $\mathbb{Z}_p$, le nombre $\psi_m(\alpha) = \psi(1+\alpha^{-1}p^{n+1})$ est une racine de 1 d'ordre divisant p^m et ne dépendant de α que modulo p^m.

PROPOSITION 7, [12]. - Supposons qu'il existe une extension abélienne finie k de $\mathbb{Q}$ avec $\lim_{n\to\infty} e_n^{(\ell)} = +\infty$; alors on peut trouver un caractère de Dirichlet (*) χ, impair, tel que

(14) le conducteur de χ est égal à d ou $d.p$ avec $d \in \mathbb{N}$, d premier à p,

(15) pour tout m entier assez grand, il existe une infinité de $n \in \mathbb{N}$ tels que pour au moins un élément ψ de D_{n+m}, on ait :

$$\forall \alpha \in \mathbb{Z}_p^* \quad \sum_{\eta \in R} \sum_{i=0}^{d-1} \psi(\alpha^{-1} s_n(\alpha\eta))\chi(s_n(\alpha\eta) + ip^{n+1}) \frac{\psi_m(\alpha\eta)^i}{\psi_m(\alpha\eta)^d - 1} \equiv 0 \mod \mathfrak{L} .$$

En effet, avec l'hypothèse de la proposition 7, avec la formule analytique du nombre de classes, on peut montrer, [12], qu'il existe un caractère de Dirichlet impair χ vérifiant (14) tel que pour une infinité de n dans $\mathbb{N}$, on ait

$$\frac{1}{2} B_{1,\chi\psi} \equiv 0 \mod \mathfrak{L} \tag{16}$$

pour un élément ψ au moins de D_{n+m} ; ici $B_{1,\chi\psi}$ désigne le nombre de Bernoulli

$$\frac{1}{p^{n+m+1}d} \sum_{a=1}^{dp^{n+m+1}} a(\chi\psi)(a) .$$

Désignons par F_n le corps engendré sur $\mathbb{Q}_\ell$ par l'image de χ et ζ_{p^n}. On suppose dans la suite m assez grand pour avoir $F_m \neq F_{m+1}$. Si (16) est vérifié, on obtient (15) pour $\alpha \in \mathbb{Z}_p^*$ et $n \geq m$ en calculant la trace entre F_{n+m} et F_m de $\psi(\alpha^{-1})B_{1,\chi\psi}/2$.

4.2. Soit χ un caractère de Dirichlet impair vérifiant (14) et (15). Pour n assez grand, choisissons α_1 et α_2 comme dans la proposition 4. Comparons la congruence de (15) pour $\alpha = \alpha_1$ et $\alpha = \alpha_2$: seuls les termes relatifs à $\eta = \eta_o$ diffèrent ; en simplifiant, on obtient :

(*) à valeurs dans Ω_ℓ.

$$\sum_{i=0}^{d-1} \psi(\alpha_1^{-1} s_n(\alpha_1\eta_o))\chi(s_n(\alpha_1\eta_o) + ip^{n+1}) \frac{\psi_m(\alpha_1\eta_o)^i}{\psi_m(\alpha_1\eta_o)^d - 1}$$

$$\equiv \sum_{i=0}^{d-1} \psi(\alpha_2^{-1} s_n(\alpha_2\eta_o))\chi(s_n(\alpha_2\eta_o) + ip^{n+1}) \frac{\psi_m(\alpha_2\eta_o)^i}{\psi_m(\alpha_2\eta_o)^d - 1} \mod \mathfrak{L} .$$

Comme $\alpha_1 \equiv \alpha_2 \equiv 1 \mod p^m$, on a $\psi_m(\alpha_1\eta_o) = \psi_m(\alpha_2\eta_o) = \psi_m(\eta_o)$. Soit a un entier multiple de d et congru à η_o modulo p. En remarquant que

$$\psi(\alpha_1^{-1} s_n(\alpha_1\eta_o)) = \psi(\alpha_1^{-1} s_{n+m}(\alpha_1\eta_o)) = \psi(\eta_o) = 1$$

et $$\psi(\alpha_2^{-1} s_n(\alpha_2\eta_o)) = \psi(\alpha_2^{-1} s_{n+m}(\alpha_2\eta_o) - \alpha_2^{-1} p^{n+1}) = \psi(\eta_o - \alpha_2^{-1} p^{n+1})$$

$$= \psi(\eta_o)\psi(1 - \eta_o^{-1}\alpha_2^{-1} p^{n+1}) = \psi_m(\eta_o)^{-1} ,$$

on déduit

$$\sum_{i=0}^{d-1} \chi(a + ip^{n+1})\psi_m(\eta_o)^i \equiv \sum_{i=0}^{d-1} \chi(a + (i-1)p^{n+1})\psi_m(\eta_o)^{i-1} .$$

Après simplification, il ne reste que le terme correspondant à $i = 0$ (resp. $i = d-1$) dans le terme de droite (resp. de gauche) c'est-à-dire

$$\chi(a + p^{n+1}(d-1))\psi_m(\eta_o)^{d-1} \equiv \chi(a - p^{n+1})\psi_m(\eta_o)^{-1} \mod \mathfrak{L}$$

ou encore

$$(\psi_m(\eta_o)^d - 1)\chi(a - p^{n+1}) \equiv 0 \mod \mathfrak{L} .$$

Comme $a - p^{n+1}$ est congru à $-p^{n+1}$ modulo d et à η_o modulo p, $a - p^{n+1}$ est premier à dp donc $\chi(a - p^{n+1})$ est $\neq 0$ donc est une racine de 1. La contradiction provient du fait que $\psi_m(\eta_o)^d - 1 \not\equiv 0 \mod \mathfrak{L}$, puisque $\psi_m(\eta_o)^d$ est une racine de 1 d'ordre p^m. Le théorème 4 résulte alors du fait que la suite $e_n^{(\ell)}$ est croissante.

BIBLIOGRAPHIE.

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

[2] B. FERRERO et L. WASHINGTON.- The Iwasawa invariant μ_p vanishes for abelian number fields, à paraître aux Ann. of Math.

[3] K. IWASAWA.- On some invariants of cyclotomic fields, Amer. J. Math., 80 (1958).

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

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

[6] K. IWASAWA. - On the μ invariants of $\mathbb{Z}_\ell$-extensions, in : Number theory, Algebraic Geometry and Commutative Algebra, in honor of Y. Akizuki, Kinokuniya, Tokyo, 1-11, 1973.

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

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

[9] L. KUIPERS et H. NIEDERREITER. - Uniform distribution of sequences, Wiley, 1974.

[10] L. KUZMIN. - Cohomological dimension of some Galois groups, Math. USSR IZV., 9 (1975) = Izv. Akad. Nauk SSSR Ser. Mat., 39 (1975).

[11] S. WAGSTAFF. - The irregular primes to 125 000, Math. Comp., 32, (1978).

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

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

-:-:-:-

Roland GILLARD
UNIVERSITE SCIENTIFIQUE ET
MÉDICALE DE GRENOBLE I
Laboratoire de Mathématiques Pures
associé au C.N.R.S. n° 188
B.P. 116
38402 SAINT MARTIN D'HERES

(décembre 1978)