

# Bulletin

de la SOCIÉTÉ MATHÉMATIQUE DE FRANCE

## INDICE DES UNITÉS ELLIPTIQUES DANS LES $\mathbb{Z}_p$ -EXTENSIONS

Hassan Oukhaba

**Tome 135**  
**Fascicule 2**

**2007**

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Publié avec le concours du Centre national de la recherche scientifique

pages 1-

## INDICE DES UNITÉS ELLIPTIQUES DANS LES $\mathbb{Z}_p$ -EXTENSIONS

PAR HASSAN OUKHABA

---

RÉSUMÉ. — Nous comparons le comportement dans les  $\mathbb{Z}_p$ -extensions du nombre de classes d'idéaux avec le comportement de l'indice du groupe des unités elliptiques de Rubin.

ABSTRACT (*Index of elliptic units in  $\mathbb{Z}_p$ -extensions*). — We compare the behavior in  $\mathbb{Z}_p$ -extensions of the ideal class number with the behavior of the index of Rubin's group of elliptic units.

### 1. Introduction

Soient  $k \subset \mathbb{C}$  un corps quadratique imaginaire et  $H \subset \mathbb{C}$  son corps de classes de Hilbert. Soit  $F \subset \mathbb{C}$  une extension abélienne finie de  $k$  telle que  $H \subset F$ . Soient  $\mathcal{O}_F$  l'anneau des entiers de  $F$  et  $\mathcal{O}_F^\times$  son groupe des unités. On s'intéresse au groupe des unités elliptiques de  $F$  défini par K. Rubin [10, § 1]. Ce groupe, que nous noterons  $\mathcal{C}_F$ , possède au moins deux propriétés importantes. En effet, ses éléments interviennent directement dans la construction de systèmes d'Euler, principal ingrédient dans la démonstration de Rubin de la conjecture principale de la théorie d'Iwasawa pour les corps quadratiques imaginaires. Ces mêmes systèmes d'Euler apparaissent dans le récent travail

---

*Texte reçu le 3 octobre 2006, révisé le 2 février 2007*

HASSAN OUKHABA, Laboratoire de Mathématique, Université de Franche-Comté, 25030 Besançon Cedex (France) • E-mail : [hassan.oukhaba@univ-fcomte.fr](mailto:hassan.oukhaba@univ-fcomte.fr)

Classification mathématique par sujets (2000). — 11G16, 11R23.

Mots clefs. — Unités elliptiques, indice,  $\mathbb{Z}_p$ -extensions.

de W. Bley [1] qui étend en particulier les résultats de Rubin au cas presque général afin de les appliquer à la conjecture sur les nombres de Tamagawa. La deuxième propriété que nous souhaitons évoquer est le fait que le groupe  $\mathcal{C}_F$  est d'indice fini dans  $\mathcal{O}_F^\times$ . De plus, si  $h_F$  est le nombre de classes d'idéaux de  $F$ , alors on peut déduire des travaux de Gillard [2] que si  $p > 3$  est un nombre premier tel que  $p \nmid [F : k]$  alors  $[\mathcal{O}_F^\times : \mathcal{C}_F]_p = (h_F)_p$ , où pour tout entier naturel non nul  $A$  nous désignons par  $A_p$  la  $p$ -partie de  $A$ , c'est-à-dire la plus grande puissance de  $p$  qui divise  $A$ . Notons  $(\mathcal{O}_F^\times/\mathcal{C}_F)_p$  (resp.  $\text{Cl}(F)_p$ ) le  $p$ -Sylow de  $\mathcal{O}_F^\times/\mathcal{C}_F$  (resp. du groupe de classes d'idéaux de  $F$ ). Alors, la technique des systèmes d'Euler permet d'affiner l'égalité entre  $p$ -parties citée ci-dessus, en montrant que pour tout caractère  $p$ -adique irréductible  $\chi$  de  $\text{Gal}(F/k)$ , les  $\chi$ -composantes de  $(\mathcal{O}_F^\times/\mathcal{C}_F)_p$  et  $\text{Cl}(F)_p$  ont même ordre, cf. [10, Thm. 3.3].

Dans le cas général, il n'existe pas de formule reliant l'indice  $[\mathcal{O}_F^\times : \mathcal{C}_F]$  à  $h_F$ . À la fin du paragraphe 2, nous en proposons une qui exprime  $c_F = [\mathcal{O}_F^\times : \mathcal{C}_F]/h_F$  à l'aide de quantités liées à la ramification dans  $F$  et d'autres liées à la structure galoisienne des unités elliptiques. Pour cela nous utilisons le théorème A de [5] qui donne une formule pour l'indice  $[\mathcal{O}_F^\times : \Omega_F]$ , où  $\Omega_F$  est le groupe de Kubert-Lang engendré par les invariants de Kersey introduits dans [4, p. 307].

Nous montrons ensuite que la formule d'indice (2.10) peut être efficacement exploitée pour étudier le comportement de  $c_F$  dans les  $\mathbb{Z}_p$ -extensions de  $F$  qui sont abéliennes sur  $k$ . En effet, soient  $p$  un nombre premier et  $F_\infty$  une  $\mathbb{Z}_p$ -extension de  $F$  abélienne sur  $k$ . Pour tout entier  $n$ , on notera  $F_n$  l'unique extension de  $F$  contenue dans  $F_\infty$  et de degré  $p^n$  sur  $F$ .

**THÉORÈME.** — *Il existe deux entiers  $\mu_\infty \in \mathbb{N}$  et  $\nu_\infty \in \mathbb{Z}$  tels que*

$$[\mathcal{O}_{F_n}^\times : \mathcal{C}_{F_n}]_p = p^{\mu_\infty p^n + \nu_\infty} (h_{F_n})_p,$$

*pour tout entier  $n$  assez grand. Notons  $S_{F, F_\infty}$  l'ensemble des idéaux premiers de  $k$  ramifiés dans  $F$  mais pas dans  $F_\infty/F$ . Pour tout  $\mathfrak{q} \in S_{F, F_\infty}$ , notons  $D_{\mathfrak{q}}(F_\infty)$  le groupe de décomposition de  $\mathfrak{q}$  dans  $F_\infty/k$ . Supposons que les groupes  $D_{\mathfrak{q}}(F_\infty)$  sont tous infinis. Alors on a  $\mu_\infty = 0$ , de plus il existe  $c_{F_\infty} \in \mathbb{Q}^\times$  tel que*

$$[\mathcal{O}_{F_n}^\times : \mathcal{C}_{F_n}] = c_{F_\infty} h_{F_n},$$

*pour tout entier  $n$  assez grand.*

Signalons que  $\mu_\infty$  est le  $\mu$ -invariant d'un certain module d'Iwasawa qui apparaît lors de l'étude de la suite d'indices  $(R^{(n)} : U^{(n)})$  (voir § 3). Bien que nous n'en donnons pas la démonstration ici, nous attirons l'attention du lecteur que dans le cas semi-simple, c'est-à-dire le cas où  $p \nmid [F : k]$ , on a  $\mu_\infty = 0$ . En effet, le  $p$ -Sylow de  $\text{Gal}(F_n/k)$  est cyclique et cela permet de montrer que  $p \nmid (R^{(n)} : U^{(n)})$ . Il est aussi possible de montrer que l'on a  $\mu_\infty = 0$  si au plus

deux idéaux premiers  $\mathfrak{q} \in S_{F, F_\infty}$  sont tels que  $D_{\mathfrak{q}}(F_\infty)$  est fini. Comme expliqué aux §§ 2 et 3, les techniques pour étudier la suite d'indices  $(R^{(n)} : U^{(n)})$  sont empruntées à Sinnott [11]. Nous dirons que  $F_\infty$  vérifie l'hypothèse de décomposition si les groupes  $D_{\mathfrak{q}}(F_\infty)$ ,  $\mathfrak{q} \in S_{F, F_\infty}$ , sont tous infinis. Il est évident que la  $\mathbb{Z}_p$ -extension cyclotomique de  $F$  vérifie l'hypothèse de décomposition. Il en est de même si  $p$  est totalement décomposé dans  $k/\mathbb{Q}$  et si  $F_\infty/F$  est la  $\mathbb{Z}_p$ -extension non ramifiée en dehors d'un idéal premier  $\mathfrak{p}$  de  $k$  au-dessus de  $p$ . Cependant il existe bien des cas où cette hypothèse n'est pas satisfaite. En effet, soit  $M$  la  $\mathbb{Z}_p^2$ -extension de  $F$  abélienne sur  $k$  et soit  $\mathfrak{q}$  un idéal premier de  $k$  qui ne divise pas  $p$ . Alors le groupe de décomposition de  $\mathfrak{q}$  dans  $M/F$ , qu'on notera  $D_{\mathfrak{q}}$ , est isomorphe à  $\mathbb{Z}_p$ . Son corps fixe  $F(D_{\mathfrak{q}})$  est donc une  $\mathbb{Z}_p$ -extension de  $F$  abélienne sur  $k$  et  $\mathfrak{q}$  se décompose totalement dans  $F(D_{\mathfrak{q}})/F$ . Remarquons que si  $\mathfrak{q}$  n'est pas décomposé dans  $k/\mathbb{Q}$  alors  $F(D_{\mathfrak{q}})$  est la  $\mathbb{Z}_p$ -extension anticyclotomique de  $F$ . Dans un article en cours de rédaction nous donnerons justement des exemples où le  $\mu_\infty$  est non nul pour la  $\mathbb{Z}_p$ -extension anticyclotomique. Enfin, notons que l'hypothèse  $H \subset F$  n'est pas nécessaire. Elle sert avant tout à rendre ce travail moins technique.

Avant de passer au paragraphe suivant, voici quelques notations qui serviront tout au long de cet article. On notera  $f$  (resp.  $f_n$ ) le conducteur de  $F/k$  (resp.  $F_n/k$ ),  $\mu(F)$  le groupe des racines de l'unité de  $F$  et  $w_F$  l'ordre de  $\mu(F)$ . Lorsque  $f \neq (1)$  on notera  $\mathfrak{p}_1, \dots, \mathfrak{p}_e$  les idéaux premiers de  $k$  qui divisent  $f$ . Si  $\mathfrak{a}$  est un idéal fractionnaire de  $k$  premier au conducteur de  $F/k$  alors on notera  $(\mathfrak{a}, F/k)$  l'automorphisme de  $F/k$  associé à  $\mathfrak{a}$  par l'application de réciprocité d'Artin. Lorsque  $\mathfrak{a} \subset \mathcal{O}_k$  on notera  $N(\mathfrak{a})$  le cardinal de l'anneau fini  $\mathcal{O}_k/\mathfrak{a}$  et  $\widehat{\mathfrak{a}}$  le produit des idéaux premiers de  $k$  qui divisent  $\mathfrak{a}$ . Si  $\mathfrak{a} = (1)$  on pose  $\widehat{\mathfrak{a}} := (1)$ . Enfin, on sait qu'on peut décomposer  $f_n$  de manière unique  $f_n = \mathfrak{h} \mathfrak{g}_n$ , où  $\mathfrak{h}$  est premier à  $\mathfrak{g}_n$  et ne dépend pas de  $n$  et  $\mathfrak{g}_n$  est divisible uniquement par les idéaux premiers de  $k$  qui se ramifient dans  $F_\infty/F$ .

## 2. Les groupes $\mathcal{C}_F$ et $\Omega_F$

Commençons par rappeler la définition du groupe  $\mathcal{C}_F$ . Pour cela nous utilisons la famille de fonctions elliptiques  $\Psi(\cdot; L, L') : z \mapsto \Psi(z; L, L')$  introduites par G. Robert dans [9] et [7], paramétrées par les couples de réseaux  $(L, L')$  de  $\mathbb{C}$  tels que  $L \subset L'$  et  $[L' : L]$  est premier à 6. L'intérêt de ces fonctions s'explique en partie par les résultats suivants, cf. [9] et [8].

Soit  $\mathfrak{m} \neq (1)$  un idéal de  $\mathcal{O}_k$  et soit  $k_{\mathfrak{m}}$  le corps de classes de  $k$  de rayon modulo  $\mathfrak{m}$ . Soit  $\mathfrak{a}$  un idéal de  $\mathcal{O}_k$  premier avec  $6\mathfrak{m}$ ; alors  $\Psi(1; \mathfrak{m}, \mathfrak{a}^{-1}\mathfrak{m}) \in k_{\mathfrak{m}}$ . De plus si  $\varphi_{\mathfrak{m}}(1)$  est l'invariant de Robert-Ramachandra, comme défini

dans [12, p. 96] par exemple, alors on a

$$(2.1) \quad \Psi(1; \mathfrak{m}, \mathfrak{a}^{-1}\mathfrak{m})^{12e_{\mathfrak{m}}} = \varphi_{\mathfrak{m}}(1)^{N(\mathfrak{a}) - (\mathfrak{a}, k_{\mathfrak{m}}/k)},$$

où  $e_{\mathfrak{m}}$  est le générateur positif de  $\mathfrak{m} \cap \mathbb{Z}$ . Rappelons que  $\varphi_{\mathfrak{m}}(1)$  est une unité de  $k_{\mathfrak{m}}$  si  $\mathfrak{m}$  est divisible par au-moins deux idéaux premiers. Dans le cas où  $\mathfrak{m} = \mathfrak{q}^e$ ,  $\mathfrak{q}$  un idéal premier de  $k$ , alors

$$(2.2) \quad \varphi_{\mathfrak{m}}(1)\mathcal{O}_{k_{\mathfrak{m}}} = \mathfrak{q}_{\mathfrak{m}}^u,$$

où  $\mathfrak{q}_{\mathfrak{m}}$  est le produit des idéaux premiers de  $k_{\mathfrak{m}}$  qui divisent  $\mathfrak{q}$  et

$$u := \frac{12}{w_k} r_{\mathfrak{m}} e_{\mathfrak{m}}.$$

Par définition,  $r_{\mathfrak{m}}$  est le nombre de racines de l'unité de  $k$  congrus à 1 modulo l'idéal  $\mathfrak{m}$ , soit

$$r_{\mathfrak{m}} := \#\{\zeta \in \mu(k), \zeta \equiv 1 \text{ modulo } \mathfrak{m}\}.$$

L'invariant  $\varphi_{\mathfrak{m}}(1)$  et ses conjugués interviennent dans la seconde formule limite de Kronecker. En effet, si  $\chi$  est un caractère complexe de  $G_{\mathfrak{m}} := \text{Gal}(k_{\mathfrak{m}}/k)$  alors on a

$$L'(0, \chi) = -\frac{1}{12r_{\mathfrak{m}}e_{\mathfrak{m}}} \sum_{\sigma \in G_{\mathfrak{m}}} \chi(\sigma) \log(|\varphi_{\mathfrak{m}}(1)^{\sigma}|^2),$$

où  $s \mapsto L(s, \chi)$  est la fonction  $L$  associée à  $\chi$ , définie pour les nombres complexes tels que  $\text{Re}(s) > 1$  par le produit Eulérien

$$L(s, \chi) = \prod_{\mathfrak{l} \nmid \mathfrak{m}} (1 - \chi(\mathfrak{l})N(\mathfrak{l})^{-s})^{-1},$$

où  $\mathfrak{l}$  désigne tous les idéaux premiers de  $\mathcal{O}_k$  qui ne divisent pas  $\mathfrak{m}$ , cf. [3]. Soit  $\mathfrak{q}$  un idéal premier de  $\mathcal{O}_k$  et soit  $\mathfrak{a}$  un idéal de  $\mathcal{O}_k$  premier à  $6\mathfrak{m}\mathfrak{q}$ . Alors on a les formules de normes suivantes

$$N_{k_{\mathfrak{m}\mathfrak{q}}/k_{\mathfrak{m}}}(\Psi(1; \mathfrak{m}\mathfrak{q}, \mathfrak{a}^{-1}\mathfrak{m}\mathfrak{q}))^{r_{\mathfrak{m}}/r_{\mathfrak{m}\mathfrak{q}}} = \begin{cases} \Psi(1; \mathfrak{m}, \mathfrak{a}^{-1}\mathfrak{m}) & \text{si } \mathfrak{q} \mid \mathfrak{m}, \\ \Psi(1; \mathfrak{m}, \mathfrak{a}^{-1}\mathfrak{m})^{1-(\mathfrak{q}, k_{\mathfrak{m}}/k)^{-1}} & \text{si } \mathfrak{q} \nmid \mathfrak{m}. \end{cases}$$

De plus on a

$$(2.3) \quad N_{k_{\mathfrak{q}}/H}(\Psi(1; \mathfrak{q}, \mathfrak{a}^{-1}\mathfrak{q}))^{12w_k/r_{\mathfrak{q}}} = \left( \frac{\Delta(\mathcal{O}_k)}{\Delta(\mathfrak{q})} \right)^{N(\mathfrak{a}) - (\mathfrak{a}, H/k)},$$

où, pour tout réseau  $L$  de  $\mathbb{C}$ ,  $\Delta(L) = g_2(L)^3 - 27g_3(L)^2$  est le discriminant de l'équation

$$\wp'(z, L)^2 = 4\wp(z, L)^3 - g_2(L)\wp(z, L) - g_3(L),$$

satisfaite par la fonction  $\wp(z, L)$  de Weierstrass et sa dérivée  $\wp'(z, L)$ . Rappelons aussi la relation

$$(2.4) \quad \Psi(1; \mathfrak{m}, \mathfrak{a}^{-1}\mathfrak{m})^{N(\mathfrak{b}) - (\mathfrak{b}, k_{\mathfrak{m}}/k)} = \Psi(1; \mathfrak{m}, \mathfrak{b}^{-1}\mathfrak{m})^{N(\mathfrak{a}) - (\mathfrak{a}, k_{\mathfrak{m}}/k)}.$$

Nous disposons maintenant du matériel nécessaire à la définition de  $\mathcal{C}_F$ . Pour tout idéal  $\mathfrak{m} \neq (1)$  de  $\mathcal{O}_k$ , notons  $\mathcal{C}_{F,\mathfrak{m}}$  le sous-groupe de  $\mathcal{O}_F^\times$  engendré par  $\mu(F)$  et par les normes

$$N_{k_{\mathfrak{m}}/k_{\mathfrak{m}} \cap F}(\Psi(1; \mathfrak{m}, \mathfrak{a}^{-1}\mathfrak{m}))^{\sigma^{-1}},$$

où  $\sigma \in \text{Gal}(F/k)$  et  $\mathfrak{a}$  parcourt l'ensemble des idéaux entiers de  $k$  premiers avec  $6\mathfrak{m}$ . Alors on pose

**DÉFINITION 2.1.** — Le groupe  $\mathcal{C}_F$  est le sous-groupe de  $\mathcal{O}_F^\times$  engendré par tous les  $\mathcal{C}_{F,\mathfrak{m}}$ ,  $\mathfrak{m} \neq (1)$ . On posera

$$V_F := \mu(F)\mathcal{C}_F^{12w_k e_{\mathfrak{f}}}.$$

Nous allons maintenant rappeler la définition de  $\Omega_F$ . Soit  $Q$  le sous-groupe de  $H^\times$  engendré par les quotients

$$\left( \frac{\Delta(\mathcal{O}_k)}{\Delta(\mathfrak{q})} \right)^\tau,$$

où  $\mathfrak{q}$  parcourt les idéaux premiers de  $k$  et  $\tau \in \text{Gal}(H/k)$ . On sait que  $\Delta(\mathcal{O}_k)/\Delta(\mathfrak{q})$  engendre dans  $H$  l'idéal fractionnaire  $\mathfrak{q}^{12}\mathcal{O}_H$ . De plus on a

$$\left( \frac{\Delta(\mathcal{O}_k)}{\Delta(\mathfrak{q})} \right)^{(\mathfrak{b}, H/k)^{-1}} = \frac{\Delta(\mathfrak{b})}{\Delta(\mathfrak{q}\mathfrak{b})}.$$

Soit  $\mathfrak{g}$  un idéal propre de  $\mathcal{O}_k$  tel que  $\mathfrak{g} \mid \mathfrak{f}$ . Alors on pose

$$(2.5) \quad \varphi_{F,\mathfrak{g}} := N_{k_{\mathfrak{g}}/k_{\mathfrak{g}} \cap F}(\varphi_{\mathfrak{g}}(1))^{e(\mathfrak{f},\mathfrak{g})}, \quad e(\mathfrak{f},\mathfrak{g}) := \frac{w_k e_{\mathfrak{f}}}{r_{\mathfrak{g}} e_{\mathfrak{g}}}.$$

Soit  $h$  le nombre de classes d'idéaux de  $k$ . Les entiers algébriques  $(\varphi_{F,\mathfrak{g}})^h$  ont été introduits pour la première fois dans le livre [4, p. 307] de D. Kubert et S. Lang et sont appelées invariants de Kersey. Ce sont en quelque sorte des normalisations des invariants de Robert-Ramachandra. Rappelons que ces derniers satisfont des relations de norme mis en évidence par G. Robert [6, th. 2]. Elles ont comme conséquence immédiate les formules suivantes : pour toute paire d'idéaux  $\mathfrak{g}$  et  $\mathfrak{q}$  tels que  $\mathfrak{q}$  est premier et  $\mathfrak{g}\mathfrak{q} \mid \mathfrak{f}$ , on a

$$(2.6) \quad N_{k_{\mathfrak{g}\mathfrak{q}\mathfrak{q}}/k_{\mathfrak{g}\mathfrak{q}} \cap F}(\varphi_{F,\mathfrak{g}\mathfrak{q}}) = \begin{cases} \varphi_{F,\mathfrak{g}} & \text{si } \mathfrak{q} \mid \mathfrak{g}, \\ [\varphi_{F,\mathfrak{g}}]^{1-(\mathfrak{q}, k_{\mathfrak{g}} \cap F/k)^{-1}} & \text{si } \mathfrak{q} \nmid \mathfrak{g} \text{ et } \mathfrak{g} \neq (1), \\ (\Delta(\mathcal{O}_k)/\Delta(\mathfrak{q}))^{e_{\mathfrak{f}}} & \text{si } \mathfrak{g} = (1). \end{cases}$$

La relation (2.1) et les différentes formules de norme rappelées ci-dessus permettent d'exprimer les éléments du groupe  $\mathcal{C}_{F,\mathfrak{m}}^{12w_k e_{\mathfrak{f}}}$  en fonction de  $\varphi_{F,\mathfrak{g}}$ , où  $\mathfrak{g} = \mathfrak{m} + \mathfrak{f}$  est le plus grand commun diviseur de  $\mathfrak{m}$  et  $\mathfrak{f}$ . En effet, soit  $I_F$  l'idéal d'augmentation de  $\mathbb{Z}[\text{Gal}(F/k)]$  et soit  $J_F$  le noyau de l'homomorphisme  $j_F : \mathbb{Z}[\text{Gal}(F/k)] \rightarrow \text{Hom}(\mu(F), \mu(F))$  prolongeant l'action naturelle de  $\text{Gal}(F/k)$

sur  $\mu(F)$ . Il est bien connu que si on fixe  $S$  un ensemble fini d'idéaux premiers de  $\mathcal{O}_k$  contenant au moins ceux qui divisent  $w_F \mathfrak{f}$ , alors  $J_F$  est engendré sur  $\mathbb{Z}$  par les éléments  $N(\mathfrak{a}) - (\mathfrak{a}, F/k)$ , où  $\mathfrak{a}$  parcourt l'ensemble des idéaux de  $\mathcal{O}_k$  premiers à  $S$ , cf. [12], chap. IV-1. Pour tout  $\mathfrak{n} \mid \mathfrak{m}$  posons

$$\theta(\mathfrak{m}, \mathfrak{n}) = \prod_{\substack{\mathfrak{p} \mid \mathfrak{m} \\ \mathfrak{p} \nmid \mathfrak{n}\mathfrak{g}}} (1 - (\mathfrak{p}, F \cap k_{\mathfrak{g}}/k)^{-1}),$$

le produit étant pris sur tous les idéaux premiers qui divisent  $\mathfrak{m}$  mais ne divisent pas  $\mathfrak{n}\mathfrak{g}$ . Alors on a

$$(2.7) \quad \mathcal{C}_{F, \mathfrak{m}}^{12w_k e_{\mathfrak{f}}} = \begin{cases} (\varphi_{F, \mathfrak{g}})^{\theta(\mathfrak{m}, (1))r_{\mathfrak{m}} I_F J_F} & \text{si } \mathfrak{g} \neq (1), \\ (\Delta(\mathcal{O}_k)/\Delta(\mathfrak{q}))^{\theta(\mathfrak{m}, \mathfrak{q})r_{\mathfrak{m}} e_{\mathfrak{f}} I_F J_F} & \text{si } \mathfrak{g} = (1), \end{cases}$$

où  $\mathfrak{q}$  désigne un diviseur premier quelconque de  $\mathfrak{m}$ .

DÉFINITION 2.2. — Le sous-module galoisien de  $F^\times$  engendré par  $\mu(F)$ ,  $Q^{e_{\mathfrak{f}}}$  et par tous les  $\varphi_{F, \mathfrak{g}}$  ( $\mathfrak{g} \mid \mathfrak{f}$  et  $\mathfrak{g} \neq (1)$ ) sera noté  $\mathcal{P}_F$ . De plus on posera

$$\Omega_F := \mathcal{P}_F \cap \mathcal{O}_F^\times.$$

On voit grâce à (2.7) que  $V_F \subset \Omega_F$ .

Dans cette dernière partie du paragraphe 2, nous supprimons, sauf mention expresse du contraire, l'hypothèse  $H \subset F$ .

Posons  $R := \mathbb{Z}[\text{Gal}(F/k)]$ . Nous allons introduire un certain sous- $R$ -module  $U$  de  $\mathbb{Q}[\text{Gal}(F/k)]$ . Celui-ci apparaît dans les formules d'indice 2.9 et 2.10 ci-dessous. Mais fixons d'abord quelques notations. Si  $D$  est un sous-groupe de  $\text{Gal}(F/k)$ , alors on pose

$$s(D) := \sum_{\sigma \in D} \sigma \in R.$$

L'ordre de  $D$  sera noté indifféremment  $|D|$  ou  $\#D$ . Soit  $\mathfrak{p}$  un idéal premier de  $k$ . Le groupe d'inertie de  $\mathfrak{p}$  dans  $F/k$  sera noté  $T_{\mathfrak{p}}$ . De plus on posera

$$e_{\mathfrak{p}} := \frac{s(T_{\mathfrak{p}})}{|T_{\mathfrak{p}}|} \quad \text{et} \quad (\mathfrak{p}, F) := \lambda_{\mathfrak{p}}^{-1} e_{\mathfrak{p}},$$

où  $\lambda_{\mathfrak{p}}$  est un automorphisme de Frobenius associé à  $\mathfrak{p}$  dans  $F/k$ . On pose  $T_{(1)} := \{1\}$  et pour tout diviseur  $\mathfrak{r} \neq (1)$  de  $\widehat{\mathfrak{f}}$  on note  $T_{\mathfrak{r}}$  le sous-groupe de  $\text{Gal}(F/k)$  engendré par les groupes d'inertie  $T_{\mathfrak{p}}$ ,  $\mathfrak{p} \mid \mathfrak{r}$ .

DÉFINITION 2.3. — Soit  $\mathfrak{s}$  un diviseur de  $\widehat{\mathfrak{f}}$ . Si  $\mathfrak{s} \neq (1)$  alors on note  $U_{\mathfrak{s}}$  ou  $U_{\mathfrak{s}, F}$  le sous- $R$ -module de  $\mathbb{Q}[\text{Gal}(F/k)]$  engendré par les éléments

$$\alpha(\mathfrak{r}, \mathfrak{s}, F) = s(T_{\mathfrak{r}}) \prod_{\mathfrak{p} \mid \mathfrak{s}/\mathfrak{r}} (1 - (\mathfrak{p}, F)), \quad \mathfrak{r} \mid \mathfrak{s}.$$

De plus on pose  $U_{(1)} = U_{(1),F} := R$  et  $U = U_F := U_{\widehat{\mathfrak{f}},F}$ .

Il nous faut encore rappeler la définition de l'indice généralisé de Sinnott. Soit  $\ell$  un nombre premier et notons  $v_\ell$  la valuation normalisée associée à  $\ell$  ( $v_\ell(\ell) = 1$ ). Soit  $\mathbb{F}$  un des deux corps  $\mathbb{Q}$  ou  $\mathbb{Q}_\ell$ . Soit  $\mathfrak{o}$  le complété de  $\mathbb{Z}$  dans  $\mathbb{F}$ . Étant donné  $E$  un  $\mathbb{F}$ -espace vectoriel de dimension finie  $d$  et  $M$  et  $N$  deux réseaux de  $E$ , c'est-à-dire deux sous- $\mathfrak{o}$ -modules libres de  $E$ , de rang  $d$ , on définit l'indice

$$(M : N) = \begin{cases} |\det(\gamma)| & \text{si } \mathbb{F} = \mathbb{Q}, \\ \ell^{v_\ell(\det(\gamma))} & \text{si } \mathbb{F} = \mathbb{Q}_\ell, \end{cases}$$

où  $\gamma$  est un endomorphisme du  $\mathbb{F}$ -espace vectoriel  $E$  tel que  $\gamma(M) = N$ . Nous renvoyons le lecteur à [11] où sont démontrées les propriétés les plus remarquables de cet indice généralisé. Ici on est concerné par les  $R$ -modules  $U_{\mathfrak{s},F}$ . On peut montrer, exactement comme dans [11, lemme 5.1], que  $U_{\mathfrak{s},F}$  est un réseau de  $\mathbb{Q}[\text{Gal}(F/k)]$ . De plus, si  $\mathfrak{q}$  est un idéal premier de  $\mathcal{O}_k$  qui divise  $\mathfrak{f}$  mais ne divise pas  $\mathfrak{s}$ , alors l'indice  $(U_{\mathfrak{s},F} : U_{\mathfrak{s}\mathfrak{q},F})$ , qui est donc bien défini, est un entier dont l'ensemble des diviseurs premiers est inclus dans celui de  $\#T_{\mathfrak{q}}$ . Ainsi, si on note  $\mathfrak{s}_0, \dots, \mathfrak{s}_e$  les idéaux définis par les relations  $\mathfrak{s}_0 := (1)$  et  $\mathfrak{s}_{i+1} := \mathfrak{s}_i \mathfrak{p}_{i+1}$ , alors la décomposition

$$(R : U) = \prod_{i=0}^{e-1} (U_{\mathfrak{s}_i} : U_{\mathfrak{s}_{i+1}})$$

de  $(R : U)$  comme produit des indices  $(U_{\mathfrak{s}_i} : U_{\mathfrak{s}_{i+1}})$  montre que  $(R : U) \in \mathbb{N}$ . De plus, si  $\ell$  est un nombre premier tel que  $\ell \mid (R : U)$  alors  $\ell$  divise  $\#\text{Gal}(F/F \cap H)$ . D'ailleurs le théorème 5.2 de [11] a bien un analogue dans la situation présente. Cet analogue nous servira au paragraphe suivant. Il s'agit de la proposition 2.1 ci-dessous où nous noterons  $D$  (resp.  $\Delta$ ) le  $\ell$ -Sylow (resp. le sous-groupe des éléments d'ordre premier à  $\ell$ ) de  $\text{Gal}(F/k)$ , de sorte qu'on a la décomposition  $\text{Gal}(F/k) = \Delta \times D$ . Tout caractère multiplicatif de  $\Delta$  peut être vu comme un caractère de  $\text{Gal}(F/k)$  trivial sur  $D$ . Soit  $F_\chi$  le corps fixe de  $\ker(\chi)$  et soit  $\mathfrak{m}(\chi)$  son conducteur. Alors  $\chi$  se factorise en un caractère de  $\text{Gal}(F_\chi/k)$  que nous noterons encore  $\chi$ . Pour tout idéal  $\mathfrak{a}$  de  $\mathcal{O}_k$  premier à  $\mathfrak{m}(\chi)$ , on pose  $\chi(\mathfrak{a}) = \chi(\mathfrak{a}, F_\chi/k)$ , sinon on pose  $\chi(\mathfrak{a}) = 0$ .

**PROPOSITION 2.1.** — *Soient  $F'$  le corps fixe de  $\Delta$  et  $\chi$  un caractère de  $\Delta$ . On peut voir  $\chi$  comme caractère de  $\text{Gal}(F/k)$  trivial sur  $D$ . Notons alors  $\mathfrak{f}_\chi$  le produit des idéaux premiers  $\mathfrak{q}$  de  $k$  qui se ramifient dans  $F'$  et tels que  $\chi(\mathfrak{q}) = 1$ . Alors la puissance exacte de  $\ell$  qui divise  $(R : U)$  est le produit*

$$(2.8) \quad \prod_{\chi} (\mathbb{Z}[\text{Gal}(F'/k)] : U_{\mathfrak{f}_\chi, F'})$$

où  $\chi$  parcourt tous les caractères multiplicatifs de  $\Delta$ .



*Démonstration.* — Nous allons suivre de près la démonstration du théorème 5.2. de [11]. Posons  $R_\ell := \mathbb{Z}_\ell[\text{Gal}(F/k)]$  et pour tout diviseur  $\mathfrak{r}$  de  $\widehat{\mathfrak{f}}$ , notons  $U_{\mathfrak{r},\ell}$  le sous- $R_\ell$ -module de  $\mathbb{Q}_\ell[\text{Gal}(F/k)]$  engendré par  $U_{\mathfrak{r}}$ . On obtient ainsi des réseaux de  $\mathbb{Q}_\ell[\text{Gal}(F/k)]$ . De plus, si  $\mathfrak{q}$  est un idéal premier de  $k$  tel que  $\mathfrak{q} \mid \widehat{\mathfrak{f}}$  mais  $\mathfrak{q} \nmid \mathfrak{r}$  alors

$$v_\ell((U_{\mathfrak{r}} : U_{\mathfrak{r}\mathfrak{q}})) = v_\ell((U_{\mathfrak{r},\ell} : U_{\mathfrak{r}\mathfrak{q},\ell})).$$

Si  $\mathfrak{q}$  n'est pas ramifié dans  $F'$ , alors le groupe d'inertie en  $\mathfrak{q}$  est inclus dans  $\Delta$ ,  $T_{\mathfrak{q}} \subset \Delta$ . En particulier  $\ell$  ne divise pas  $\#T_{\mathfrak{q}}$  et  $(U_{\mathfrak{r},\ell} : U_{\mathfrak{r}\mathfrak{q},\ell}) = 1$  (voir les commentaires donnés juste avant la proposition). D'autre part on peut décomposer  $U_{\mathfrak{r},\ell}$  et  $U_{\mathfrak{r}\mathfrak{q},\ell}$  en somme directe de sous- $R_\ell$ -modules

$$U_{\mathfrak{r},\ell} = \bigoplus_{\tilde{\chi}} e_{\tilde{\chi}} U_{\mathfrak{r},\ell} \quad \text{et} \quad U_{\mathfrak{r}\mathfrak{q},\ell} = \bigoplus_{\tilde{\chi}} e_{\tilde{\chi}} U_{\mathfrak{r}\mathfrak{q},\ell},$$

où  $\tilde{\chi}$  décrit l'ensemble des caractères  $\mathbb{Q}_\ell$ -irréductibles de  $\delta$  et pour chaque  $\tilde{\chi}$  on a posé

$$e_{\tilde{\chi}} = \frac{1}{|\Delta|} \sum_{\tau \in \delta} \tilde{\chi}(\tau) \tau^{-1} \in \mathbb{Z}_\ell[\Delta],$$

qui est l'idempotent classiquement associé à  $\tilde{\chi}$ . Soit  $\overline{\mathbb{Q}}_\ell$  une clôture algébrique de  $\mathbb{Q}_\ell$ . Fixons alors un caractère multiplicatif  $\chi$  de  $\Delta$ , à valeurs dans  $\overline{\mathbb{Q}}_\ell$  et dont la trace à  $\mathbb{Q}_\ell$  est égale à  $\tilde{\chi}$ . Si  $\chi(\mathfrak{q}) = 0$ , ce qui revient à dire que  $e_{\tilde{\chi}} s(T_{\mathfrak{q}}) = 0$ , alors on a  $e_{\tilde{\chi}} U_{\mathfrak{r},\ell} = e_{\tilde{\chi}} U_{\mathfrak{r}\mathfrak{q},\ell}$  par définition même de ces modules. Si  $\chi(\mathfrak{q}) \neq 0$  et  $\chi(\mathfrak{q}) \neq 1$ , alors  $\chi(\mathfrak{q})$  est une racine de l'unité d'ordre premier à  $\ell$ . Par conséquent  $1 - \chi(\mathfrak{q})^{-1}$  est inversible dans l'anneau de valuation discrète engendré sur  $\mathbb{Z}_\ell$  par les valeurs de  $\chi$  et que nous noterons  $\mathbb{Z}_\ell(\chi)$ . Soit  $A = \sum a_g(g) \in \mathbb{Z}_\ell[\Delta]$  tel que  $(1 - \chi(\mathfrak{q})^{-1})(\sum a_g \chi(g)) = 1$ . Alors on a

$$e_{\tilde{\chi}} = (e_{\tilde{\chi}} A)(e_{\tilde{\chi}}(1 - (\mathfrak{q}, F))),$$

ce qui permet de déduire encore un fois l'égalité  $e_{\tilde{\chi}} U_{\mathfrak{r},\ell} = e_{\tilde{\chi}} U_{\mathfrak{r}\mathfrak{q},\ell}$ . De ce qui précède on déduit

$$(e_{\tilde{\chi}} R_\ell : e_{\tilde{\chi}} U_{\widehat{\mathfrak{f}},\ell}) = (e_{\tilde{\chi}} R_\ell : e_{\tilde{\chi}} U_{f_\chi,\ell}).$$

Considérons maintenant l'isomorphisme d'anneaux

$$\rho_\chi : e_{\tilde{\chi}} \mathbb{Q}_\ell[\text{Gal}(F/k)] \longrightarrow \mathbb{Q}_\ell(\chi)[D]$$

qui à  $e_{\tilde{\chi}} \sigma_1 \sigma_2$  associe  $\chi(\sigma_1) \sigma_2$ , pour tout  $(\sigma_1, \sigma_2) \in \Delta \times D$ . Par définition  $\mathbb{Q}_\ell(\chi)$  est l'extension de  $\mathbb{Q}_\ell$  engendrée par les valeurs de  $\chi$ . On a évidemment  $\rho_\chi(e_{\tilde{\chi}} R_\ell) = \mathbb{Z}_\ell(\chi)[D]$ . Mais il est aussi facile de vérifier la relation

$$\rho_\chi(e_{\tilde{\chi}} \alpha(\mathfrak{r}, f_\chi, F)) = \#(T_{\mathfrak{r}} \cap \Delta) \alpha(\mathfrak{r}, f_\chi, F'), \quad \mathfrak{r} \mid f_\chi,$$

d'où l'on déduit

$$(\rho_\chi(e_{\tilde{\chi}} R_\ell) : \rho_\chi(e_{\tilde{\chi}} U_{f_\chi,\ell})) = (\mathbb{Z}_\ell(\chi) \cdot R'_\ell : \mathbb{Z}_\ell(\chi) \cdot U'_{f_\chi,\ell}) = (R'_\ell : U'_{f_\chi,\ell})^{d_\chi},$$

où  $R'_\ell = \mathbb{Z}_\ell[\text{Gal}(F'/k)]$ ,  $d_\chi = [\mathbb{Q}_\ell(\chi) : \mathbb{Q}_\ell]$  et  $U'_{f_\chi, \ell}$  est le sous- $R'_\ell$ -module de  $\mathbb{Q}_\ell[\text{Gal}(F'/k)]$  engendré par  $U_{f_\chi, F'}$ . On voit en particulier que si  $\tilde{\psi} = \tilde{\chi}$ , alors  $(R'_\ell : U'_{f_\psi, \ell}) = (R'_\ell : U'_{f_\chi, \ell})$ . On peut maintenant conclure puisqu'on a

$$(e_{\tilde{\chi}} R_\ell : e_{\tilde{\chi}} U_{\hat{f}_\ell}) = \prod_{\psi \sim \chi} (\mathbb{Z}[\text{Gal}(F'/k)] : U_{f_\psi, F'}),$$

le produit étant pris sur tous les caractères  $\psi$  de  $\Delta$  conjugués à  $\chi$  sur  $\mathbb{Q}_\ell$ .  $\square$

Pour tout idéal maximal  $\mathfrak{p}$  de  $\mathcal{O}_k$  posons  $F_{\mathfrak{p}^\infty} := F \cap (\bigcup_n k_{\mathfrak{p}^n})$ . Alors nous avons démontré dans [5, th. A] la formule d'indice suivante, valable dans le cas où  $H \subset F$ ,

$$(2.9) \quad [\mathcal{O}_F^\times : \Omega_F] = h_F \frac{(12w_k e_f)^{[F:k]-1}}{w_F/w_k} \frac{\prod_{\mathfrak{p}} [F_{\mathfrak{p}^\infty} : H]}{[F : H]} (R : U),$$

d'où l'on déduit

$$(2.10) \quad [\mathcal{O}_F^\times : \mathcal{C}_F] = h_F \frac{\prod_{\mathfrak{p}} [F_{\mathfrak{p}^\infty} : H]}{[F : H]} (R : U) \frac{[\Omega_F : V_F]}{w_F/w_k}.$$

### 3. L'indice $(R : U)$ dans les $\mathbb{Z}_p$ -extensions

Posons  $R^{(n)} := \mathbb{Z}[\text{Gal}(F_n/k)]$  et  $U^{(n)} := U_{F_n}$ . Nous étudions la suite d'indices  $(R^{(n)} : U^{(n)})$ . À cette fin, pour tout nombre premier  $\ell$  nous noterons  $R_\ell^{(n)}$  la  $\mathbb{Z}_\ell$ -algèbre  $\mathbb{Z}_\ell[\text{Gal}(F_n/k)]$  et  $U_\ell^{(n)}$  le sous- $R_\ell^{(n)}$ -module de  $\mathbb{Q}_\ell[\text{Gal}(F_n/k)]$  engendré par  $U^{(n)}$ .

**PROPOSITION 3.1.** — *Supposons que  $F_\infty$  vérifie l'hypothèse de décomposition. Alors pour tout  $\ell \neq p$  la suite  $(R_\ell^{(n)} : U_\ell^{(n)})$  ne dépend pas de  $n$  pour tout entier  $n$  assez grand.*

*Démonstration.* — Ici aussi il suffit de reprendre la première partie de la démonstration de Sinnott de son théorème 6.1 dans [11]. En effet, la plus grande extension de  $k$  de degré une puissance de  $\ell$ , contenue dans  $F_n$  ne dépend pas de  $n$ . Notons-la  $F'$ . D'après la proposition 2.1, on doit considérer les indices  $(\mathbb{Z}[\text{Gal}(F'/k)] : U_{f_\chi, F'})$ , où  $\chi$  parcourt les caractères de  $\text{Gal}(F_n/F')$ . Par hypothèse il existe  $n_0$  tel que  $\text{Gal}(F_n/F_{n_0})$ , pour  $n \geq n_0$ , est contenu dans tous les groupes de décomposition des idéaux premiers de  $k$  qui se ramifient dans  $F_n/k$ . En particulier, si  $f_\chi \neq (1)$  alors  $\chi$  est nécessairement trivial sur  $\text{Gal}(F_n/F_{n_0})$ . D'où la formule

$$(R_\ell^{(n)} : U_\ell^{(n)}) = \prod_{\chi} (\mathbb{Z}[\text{Gal}(F'/k)] : U_{f_\chi, F'}), \quad n \geq n_0,$$

où  $\chi$  parcourt tous les caractères de  $\text{Gal}(F_{n_0}/k)$ .  $\square$

Soit  $\mathfrak{s}$  un diviseur de  $\hat{f}_n$  (qui est par définition le produit des idéaux premiers de  $\mathcal{O}_k$  qui divisent  $f_n$ ). Alors on pose  $U_{\mathfrak{s}}^{(n)} := U_{\mathfrak{s}, F_n}^{(n)}$  et on note  $U_{\mathfrak{s}, p}^{(n)}$  le sous- $R_p^{(n)}$ -module de  $\mathbb{Q}_p[\text{Gal}(F_n/k)]$  engendré par  $U_{\mathfrak{s}}^{(n)}$ . Rappelons que  $U_{\mathfrak{s}, p}^{(n)}$  est un réseau de  $\mathbb{Q}_p[\text{Gal}(F_n/k)]$ . Si  $\mathfrak{q}$  est un idéal premier de  $\mathcal{O}_k$  qui divise  $f_n$  mais ne divise pas  $\mathfrak{s}$ , alors on a

$$v_p((U_{\mathfrak{s}}^{(n)} : U_{\mathfrak{s}\mathfrak{q}}^{(n)})) = v_p((U_{\mathfrak{s}, p}^{(n)} : U_{\mathfrak{s}\mathfrak{q}, p}^{(n)})).$$

PROPOSITION 3.2. — Soient  $\mathfrak{s}$  et  $\mathfrak{s}'$  deux diviseurs de  $\hat{h}$  tels que  $\mathfrak{s}\mathfrak{s}' = \hat{h}$ . Soit  $\mathfrak{q}$  un idéal premier de  $\mathcal{O}_k$  qui divise  $\mathfrak{s}'$ . Alors il existe  $\mu \in \mathbb{N}$  et  $\nu \in \mathbb{Z}$  tel que l'indice

$$(U_{\mathfrak{s}, p}^{(n)} : U_{\mathfrak{s}\mathfrak{q}, p}^{(n)}) = p^{\mu p^n + \nu}$$

pour tout entier  $n$  assez grand. De plus, si le groupe de décomposition de  $\mathfrak{q}$  dans  $F_{\infty}/k$  est infini alors on a  $\mu = 0$ .

Démonstration. — Les arguments que nous utilisons ici sont empruntés à [11], lemme 3.2 et proposition 6.1. La démonstration que nous en donnons reprend largement les arguments de Sinnott. Posons

$$\Lambda := \varprojlim \mathbb{Z}_p[\text{Gal}(F_n/F)], \quad R^{\infty} := \varprojlim R_p^{(n)} \quad \text{et} \quad E := \varprojlim \mathbb{Q}_p[\text{Gal}(F_n/k)].$$

Notons  $P_n$  la projection canonique  $E \rightarrow \mathbb{Q}_p[\text{Gal}(F_n/k)]$  et pour tout sous- $\Lambda$ -module  $A$  de  $E$  posons  $A^{(n)} = P_n(A)$  et  $A_n = A \cap \ker(P_n)$ . On peut remarquer que  $R^{\infty}$  est une sous- $\Lambda$ -algèbre de  $E$ , libre de rang fini. Comme base on peut prendre une partie quelconque de  $\text{Gal}(F_{\infty}/k)$  en bijection avec  $\text{Gal}(F/k)$  par restriction des automorphismes. On en déduit l'identité  $R_n^{\infty} = \omega_n R^{\infty}$ , où on a posé  $\omega_n = \gamma^{p^n} - 1$ ,  $\gamma$  étant un générateur topologique de  $\text{Gal}(F_{\infty}/F)$ . D'autre part, la limite inverse

$$U_{\mathfrak{s}}^{\infty} := \varprojlim U_{\mathfrak{s}, p}^{(n)}$$

n'est autre que le sous- $R^{\infty}$ -module de  $E$  engendré par les éléments de la forme

$$s(\tilde{T}_{\mathfrak{r}}) \prod_{\mathfrak{p} | \mathfrak{s}/\mathfrak{r}} (1 - (\mathfrak{p}, F_{\infty})), \quad \mathfrak{r} | \mathfrak{s},$$

où  $\tilde{T}_{\mathfrak{r}}$  est le sous-groupe (fini) de  $\text{Gal}(F_{\infty}/k)$  engendré par les groupes d'inertie  $\tilde{T}_{\mathfrak{p}}$  dans  $F_{\infty}/k$  des idéaux premiers qui divisent  $\mathfrak{r}$ . Le symbole  $(\mathfrak{p}, F_{\infty})$  est défini comme suit

$$(\mathfrak{p}, F_{\infty}) := \lambda_{\mathfrak{p}}^{-1} \frac{s(\tilde{T}_{\mathfrak{p}})}{|\tilde{T}_{\mathfrak{p}}|},$$

où  $\lambda_{\mathfrak{p}}$  est un Frobenius en  $\mathfrak{p}$  dans  $F_{\infty}/k$ . En particulier  $U_{\mathfrak{s}}^{\infty}$  est un  $\Lambda$ -module de type fini. De plus on a  $P_n(U_{\mathfrak{s}}^{\infty}) = U_{\mathfrak{s}, p}^{(n)}$ , si bien que

$$(3.1) \quad (U_{\mathfrak{s}, p}^{(n)} : U_{\mathfrak{s}\mathfrak{q}, p}^{(n)}) = \frac{[U_{\mathfrak{s}, p}^{(n)} + U_{\mathfrak{s}\mathfrak{q}, p}^{(n)} : U_{\mathfrak{s}\mathfrak{q}, p}^{(n)}]}{[U_{\mathfrak{s}, p}^{(n)} + U_{\mathfrak{s}\mathfrak{q}, p}^{(n)} : U_{\mathfrak{s}, p}^{(n)}]} = \frac{[A^{(n)} : C^{(n)}]}{[A^{(n)} : B^{(n)}]},$$

où  $A = U_s^\infty + U_{sq}^\infty$ ,  $B = U_s^\infty$  et  $C = U_{sq}^\infty$ .

Nous dirons qu'un sous- $\Lambda$ -module  $X$  de  $E$  est admissible s'il existe  $u, v \in \mathbb{N}$  tels que  $p^u(R^\infty) \subset X$  et  $p^v(X) \subset R^\infty$ . Ceci entraîne en particulier que  $X^{(n)}$  est un réseau de  $\mathbb{Q}_p[\text{Gal}(F_n/k)]$ . Si  $Y \subset X$  sont deux sous- $\Lambda$ -modules admissibles de  $E$ , alors on peut exprimer l'ordre du groupe fini  $X^{(n)}/Y^{(n)}$  au moyen de l'invariant  $\mu$  de  $X/Y$ . En effet, d'après la théorie des  $\Lambda$ -modules, il existe  $X'$  un  $\Lambda$ -module libre et un homomorphisme injectif  $f : X \rightarrow X'$  tel que  $X'/f(X)$  est fini. Comme on a  $p^{u+v}(X_n) \subset \omega_n X$  le groupe  $(f(X_n) + \omega_n X')/\omega_n X'$  est fini puisqu'il est annulé à la fois par  $\omega_n$  et par  $p^{u+v}$ . L'injection canonique

$$(f(X_n) + \omega_n X')/\omega_n X' \longrightarrow X'/\omega_n X'$$

et le fait que  $X'/\omega_n X'$  est un  $\mathbb{Z}_p$ -module libre permettent de conclure à l'inclusion  $f(X_n) \subset \omega_n X'$ . Le quotient  $\omega_n X'/f(X_n)$  est fini car, d'une part la multiplication par  $\omega_n$  donne une application surjective

$$X'/f(X) \longrightarrow \omega_n X'/f(X_n).$$

et d'autre part  $X'/f(X)$  est fini. D'ailleurs cette dernière propriété a pour autre conséquence l'inclusion  $\omega_n X' \subset f(X)$ , pour tout  $n$  assez grand. Ainsi, pour tout  $n$  assez grand  $\omega_n X'/f(X_n) \subset f(X)/f(X_n)$ . Mais  $f(X)/f(X_n) \simeq X/X_n \simeq X^{(n)}$  est un  $\mathbb{Z}_p$ -module libre. Il vient  $f(X_n) = \omega_n X'$ , pour tout  $n$  assez grand. Par la théorie d'Iwasawa on a

$$[(X'/f(Y)) : \omega_n(X'/f(Y))] = p^{\mu' p^n + \nu'}, \quad \text{pour tout } n \text{ assez grand,}$$

où  $\nu' \in \mathbb{Z}$  et  $\mu' = \mu(X'/f(Y))$  est l'invariant du  $\Lambda$ -module  $X'/f(Y)$ . Pour déduire l'ordre de  $X^{(n)}/Y^{(n)}$ , il suffit de constater les isomorphismes

$$\begin{aligned} X^{(n)}/Y^{(n)} &\simeq X/(X_n + Y) \simeq f(X)/(f(X_n) + f(Y)), \\ X'/(\omega_n X' + f(Y)) &\simeq (X'/f(Y))/\omega_n(X'/f(Y)), \end{aligned}$$

et comme  $f$  induit un quasi isomorphisme de  $X/Y$  dans  $X'/f(Y)$ , il vient

$$(3.2) \quad \#X^{(n)}/Y^{(n)} = p^{\mu_1 p^n + \nu_1}, \quad \text{pour tout } n \text{ assez grand,}$$

où  $\nu_1 \in \mathbb{Z}$  et  $\mu_1 = \mu(X/Y)$ . Ainsi pour obtenir la formule pour  $(U_{s,p}^{(n)} : U_{sq,p}^{(n)})$ , il suffit d'appliquer (3.2) aux couples de modules  $(A, B)$  et  $(A, C)$ , les modules  $A, B, C$  étant ceux introduits ci-dessus. Ils sont évidemment admissibles. Il suffit ensuite d'utiliser (3.1). On obtient alors  $\mu = \mu(A/C) - \mu(A/B)$ . Il nous reste à montrer l'identité  $\mu(A/C) = \mu(A/B)$  dans le cas où le groupe de décomposition de  $\mathfrak{q}$  dans  $F_\infty/k$  est infini. Pour cela nous allons construire un quasi-isomorphisme de  $A/C$  dans  $A/B$ . Mais il est d'abord utile de remarquer la relation

$$U_{sq}^\infty = U_s^\infty(\widetilde{T}_{\mathfrak{q}}) + (1 - (\mathfrak{q}, F_\infty))U_s^\infty,$$

où  $U_{\mathfrak{s}}^{\infty}(\widetilde{T}_{\mathfrak{q}})$  est le sous- $R^{\infty}$ -module de  $E$  engendré par les éléments de la forme

$$s(\widetilde{T}_{\mathfrak{r}\mathfrak{q}}) \prod_{\mathfrak{p} \mid \frac{\mathfrak{s}}{\mathfrak{r}}} (1 - (\mathfrak{p}, F_{\infty})), \quad \mathfrak{r} \mid \mathfrak{s}.$$

De plus l'idempotent  $e = s(\widetilde{T}_{\mathfrak{q}})/|\widetilde{T}_{\mathfrak{q}}|$  est tel que  $(1 - e)U_{\mathfrak{s}\mathfrak{q}}^{\infty} = (1 - e)U_{\mathfrak{s}}^{\infty}$ . Or le noyau de la multiplication par  $1 - e$  dans tout  $R^{\infty}$ -module  $M$  est égal à son sous-module  $M^{\widetilde{T}_{\mathfrak{q}}}$ , qui est par définition l'ensemble des éléments de  $M$  invariants sous l'action de  $\widetilde{T}_{\mathfrak{q}}$ . Par conséquent les injections naturelles

$$A^{\widetilde{T}_{\mathfrak{q}}}/C^{\widetilde{T}_{\mathfrak{q}}} \longrightarrow A/C \quad \text{et} \quad A^{\widetilde{T}_{\mathfrak{q}}}/B^{\widetilde{T}_{\mathfrak{q}}} \longrightarrow A/B$$

sont des isomorphismes. Comme  $C^{\widetilde{T}_{\mathfrak{q}}} = U_{\mathfrak{s}}^{\infty}(\widetilde{T}_{\mathfrak{q}}) + (1 - \lambda_{\mathfrak{q}}^{-1})B^{\widetilde{T}_{\mathfrak{q}}} \subset B^{\widetilde{T}_{\mathfrak{q}}}$ , on a un homomorphisme naturel  $A^{\widetilde{T}_{\mathfrak{q}}}/C^{\widetilde{T}_{\mathfrak{q}}} \rightarrow A^{\widetilde{T}_{\mathfrak{q}}}/B^{\widetilde{T}_{\mathfrak{q}}}$ , qui est surjectif et dont le noyau est  $W = B^{\widetilde{T}_{\mathfrak{q}}}/C^{\widetilde{T}_{\mathfrak{q}}}$ . On sait déjà que ce groupe est annulé par une puissance de  $p$ . En effet, on a

$$|\widetilde{T}_{\mathfrak{q}}|B^{\widetilde{T}_{\mathfrak{q}}} \subset s(\widetilde{T}_{\mathfrak{q}})B \subset U_{\mathfrak{s}}^{\infty}(\widetilde{T}_{\mathfrak{q}}).$$

De plus, comme le groupe de décomposition  $D_{\mathfrak{q}}(F_{\infty})$  de l'idéal  $\mathfrak{q}$  dans  $F_{\infty}/k$  est topologiquement engendré par  $\widetilde{T}_{\mathfrak{q}}$  et par  $\lambda_{\mathfrak{q}}$ , les relations  $(1 - \lambda_{\mathfrak{q}}^{-1})W = 0$  et  $(1 - \sigma)W = 0$ , pour tout  $\sigma \in \widetilde{T}_{\mathfrak{q}}$  entraînent  $(1 - \sigma)W = 0$ , pour tout  $\sigma \in D_{\mathfrak{q}}(F_{\infty})$ . Or  $D_{\mathfrak{q}}(F_{\infty})$  est infini par hypothèse. Il existe donc  $n$  un entier naturel tel que  $\gamma^{p^n} \in D_{\mathfrak{q}}(F_{\infty})$ . Par conséquence  $\omega_n W = 0$ . Le groupe  $W$  est donc fini. Ce qu'il fallait démontrer.  $\square$

**COROLLAIRE 3.1.** — *Soit  $\mathfrak{s}$  un diviseur de  $\widehat{\mathfrak{h}}$ . Alors il existe  $\mu_{\mathfrak{s}} \in \mathbb{N}$  et  $\nu_{\mathfrak{s}} \in \mathbb{Z}$  tel que*

$$(R_p^{(n)} : U_{\mathfrak{s},p}^{(n)}) = p^{\mu_{\mathfrak{s}}p^n + \nu_{\mathfrak{s}}}$$

*pour tout entier  $n$  assez grand. De plus, si les groupes de décomposition des idéaux premiers de  $k$  qui divisent  $\mathfrak{s}$  sont infinis, alors on a  $\mu_{\mathfrak{s}} = 0$ .*

*Démonstration.* — Soient  $\mathfrak{q}_1, \dots, \mathfrak{q}_d$  les idéaux premiers de  $\mathcal{O}_k$  qui divisent  $\mathfrak{s}$ . Alors on a

$$(R_p^{(n)} : U_{\mathfrak{s},p}^{(n)}) = \prod_{i=0}^{d-1} (U_{\mathfrak{s}_i,p}^{(n)} : U_{\mathfrak{s}_{i+1},p}^{(n)}),$$

où  $\mathfrak{s}_0 = (1)$  et  $\mathfrak{s}_i = \mathfrak{q}_1 \cdots \mathfrak{q}_i$  si  $i \geq 1$ . La proposition 3.2 permet de conclure.  $\square$

Si  $M \subset L$  sont des extensions abéliennes finies de  $k$  alors on note

$$\text{cor}_{L/M} : \mathbb{Z}_p[\text{Gal}(M/k)] \longrightarrow \mathbb{Z}_p[\text{Gal}(L/k)]$$

l'homomorphisme de  $\mathbb{Z}_p$ -modules défini pour  $\sigma \in \text{Gal}(M/k)$  par

$$\text{cor}_{L/M}(\sigma) := s(\text{Gal}(L/M))\tilde{\sigma},$$

où  $\tilde{\sigma}$  est un prolongement quelconque de  $\sigma$  à  $L$ . L'homomorphisme  $\text{cor}_{L/M}$  est injectif. En effet, notons  $\text{res}_{L/M} : \mathbb{Z}_p[\text{Gal}(L/k)] \rightarrow \mathbb{Z}_p[\text{Gal}(M/k)]$  l'homomorphisme de  $\mathbb{Z}_p$ -modules qui à  $\tau \in \text{Gal}(L/k)$  associe sa restriction au corps  $M$ , alors on a  $\text{res}_{L/M} \circ \text{cor}_{L/M}(x) = [L : M]x$ .

PROPOSITION 3.3. — Posons  $\mathfrak{a} = \widehat{\mathfrak{h}}$  et, pour tous  $m \geq n$ , notons  $G(m, n)$  le groupe de Galois de  $F_m/F_n$ . Alors pour tout  $n_0$  assez grand l'application  $\text{cor}_{F_m/F_n}$ ,  $m \geq n$ , induit un isomorphisme

$$(3.3) \quad \text{cor}_{F_m/F_n} : (U_{\mathfrak{a}, p}^{(n)})^{G(n, n_0)} \xrightarrow{\simeq} (U_{\mathfrak{a}, p}^{(m)})^{G(m, n_0)},$$

pour tous  $m \geq n \geq 2n_0$ .

Démonstration. — Posons  $A = U_{\mathfrak{a}, p}^\infty$ . Il existe  $X$  un  $\Lambda$ -module libre et un homomorphisme injectif  $f : A \rightarrow X$  tel que  $X/f(A)$  est fini. Comme nous l'avons montré au cours de la preuve de la proposition 3.2, il existe  $n_0 \in \mathbb{N}$  tel que  $f(A_n) = \omega_n X$ , pour tout  $n \geq n_0$ . Rappelons que  $A_n$  est le noyau de la projection  $A \rightarrow \mathbb{Q}_p[\text{Gal}(F_n/k)]$ . En particulier on a

$$(U_{\mathfrak{a}, p}^{(n)})^{G(n, n_0)} \simeq (A/A_n)^{\Gamma_{n_0}} \simeq (f(A)/\omega_n X)^{\Gamma_{n_0}},$$

où on a posé  $\Gamma_{n_0} := \text{Gal}(F_\infty/F_{n_0})$ . Comme  $X/f(A)$  est fini on peut choisir  $n_0$  assez grand de sorte que

$$(f(A)/\omega_n X)^{\Gamma_{n_0}} = (X/\omega_n X)^{\Gamma_{n_0}}, \quad n \geq 2n_0.$$

En effet, il suffit que  $p^{n_0}$  et  $\omega_{n_0}$  annulent  $X/f(A)$ . Alors dans ce cas l'application corestriction (3.3) correspond à l'injection

$$i : (X/\omega_n X)^{\Gamma_{n_0}} \longrightarrow (X/\omega_m X)^{\Gamma_{n_0}}, \quad x \longmapsto (\omega_m/\omega_n)x$$

qui est nécessairement surjective puisque  $X$  est  $\Lambda$ -libre. D'où la proposition.  $\square$

Notons  $\mathfrak{b}$  le produit des idéaux premiers de  $k$  qui se ramifient dans  $F_\infty/F$ . Si  $\mathfrak{q} \mid \mathfrak{b}$  alors on note  $T_{\mathfrak{q}}^{(n)}$  le groupe d'inertie de  $\mathfrak{q}$  dans  $F_n/k$ .

COROLLAIRE 3.2. — Pour tout  $n_0$  assez grand et tout diviseur  $\mathfrak{s}$  de  $\mathfrak{b}$ , l'application  $\text{cor}_{F_m/F_n}$ ,  $m \geq n$ , induit un isomorphisme

$$\text{cor}_{F_m/F_n} : (U_{\mathfrak{as}, p}^{(n)})^{G(n, n_0)} \xrightarrow{\simeq} (U_{\mathfrak{as}, p}^{(m)})^{G(m, n_0)},$$

pour tout entier  $n \geq 2n_0$ .

Démonstration. — Nous allons montrer par récurrence sur  $\mathfrak{s}$  qu'il suffit de prendre  $n_0$  assez grand à la fois pour vérifier l'hypothèse de la proposition 3.3 et pour que  $G(n, n_0) \subset T_{\mathfrak{q}}^{(n)}$  pour tout  $\mathfrak{q} \mid \mathfrak{b}$  et tout  $n \geq n_0$ . Le cas  $\mathfrak{s} = (1)$

est la proposition 3.3. Considérons donc  $\mathfrak{q}$  un idéal premier de  $k$  tel que  $\mathfrak{q} \mid \mathfrak{b}$  mais  $\mathfrak{q} \nmid \mathfrak{s}$ . Alors on a

$$U_{\mathfrak{asq},p}^{(n)} = U_{\mathfrak{as},p}^{(n)}(T_{\mathfrak{q}}^{(n)}) + (1 - (\mathfrak{q}, F_n))U_{\mathfrak{as},p}^{(n)}.$$

D'autre part, comme  $G(n, n_0) \subset T_{\mathfrak{q}}^{(n)}$  pour  $n \geq n_0$ , on peut vérifier les identités

$$\begin{aligned} (U_{\mathfrak{asq},p}^{(n)})^{G(n, n_0)} &= U_{\mathfrak{as},p}^{(n)}(T_{\mathfrak{q}}^{(n)}) + (1 - (\mathfrak{q}, F_n))(U_{\mathfrak{as},p}^{(n)})^{G(n, n_0)}, \\ \text{cor}_{F_m/F_n}(U_{\mathfrak{as},p}^{(n)}(T_{\mathfrak{q}}^{(n)})) &= U_{\mathfrak{as},p}^{(m)}(T_{\mathfrak{q}}^{(m)}). \end{aligned}$$

Ainsi notre hypothèse de récurrence implique que l'image

$$\text{cor}_{F_m/F_n}(U_{\mathfrak{asq},p}^{(n)})^{G(n, n_0)} = (U_{\mathfrak{asq},p}^{(m)})^{G(m, n_0)},$$

pourvu que  $m \geq n \geq 2n_0$ . Comme la corestriction est injective la démonstration du corollaire est complète.  $\square$

**COROLLAIRE 3.3.** — *Soit  $\mathfrak{s}$  un diviseur de  $\mathfrak{b}$  et soit  $\mathfrak{q}$  un idéal premier de  $k$  divisant  $\mathfrak{b}$  mais tel que  $\mathfrak{q} \nmid \mathfrak{s}$ . Alors l'application*

$$\text{cor}_{F_m/F_n} : (U_{\mathfrak{as},p}^{(n)})^{T_{\mathfrak{q}}^{(n)}} \xrightarrow{\simeq} (U_{\mathfrak{as},p}^{(m)})^{T_{\mathfrak{q}}^{(m)}}, \quad m \geq n,$$

*est un isomorphisme pour tout entier  $n$  assez grand.*

*Démonstration.* — Ce résultat est la conséquence immédiate du corollaire 3.2 ci-dessus.  $\square$

**COROLLAIRE 3.4.** — *Soient  $\mathfrak{s}$  et  $\mathfrak{q}$  comme dans le corollaire 3.3 ci-dessus. Alors l'indice  $(U_{\mathfrak{as},p}^{(n)} : U_{\mathfrak{asq},p}^{(n)})$  ne dépend pas de  $n$  pour tout  $n$  assez grand.*

*Démonstration.* — On a d'une part

$$(U_{\mathfrak{as},p}^{(n)} : U_{\mathfrak{asq},p}^{(n)}) = [(U_{\mathfrak{as},p}^{(n)})^{T_{\mathfrak{q}}^{(n)}} : U_{\mathfrak{as},p}^{(n)}(T_{\mathfrak{q}}^{(n)}) + (1 - \lambda_{\mathfrak{q}}^{(n)})(U_{\mathfrak{as},p}^{(n)})^{T_{\mathfrak{q}}^{(n)}}],$$

où  $\lambda_{\mathfrak{q}}^{(n)}$  est un automorphisme de Frobenius en  $\mathfrak{q}$  dans  $F_n/k$ . Mais on sait d'autre part, grâce au corollaire 3.3, que si  $n$  est assez grand alors  $\varphi := \text{cor}_{F_m/F_n}$  est un isomorphisme de  $(U_{\mathfrak{as},p}^{(n)})^{T_{\mathfrak{q}}^{(n)}}$  sur  $(U_{\mathfrak{as},p}^{(m)})^{T_{\mathfrak{q}}^{(m)}}$ . On a aussi la relation

$$\varphi[(U_{\mathfrak{as},p}^{(n)}(T_{\mathfrak{q}}^{(n)}) + (1 - \lambda_{\mathfrak{q}}^{(n)})(U_{\mathfrak{as},p}^{(n)})^{T_{\mathfrak{q}}^{(n)}})] = U_{\mathfrak{as},p}^{(m)}(T_{\mathfrak{q}}^{(m)}) + (1 - \lambda_{\mathfrak{q}}^{(m)})(U_{\mathfrak{as},p}^{(m)})^{T_{\mathfrak{q}}^{(m)}}.$$

Le corollaire en découle.  $\square$

**THÉORÈME 3.1.** — *Il existe  $\mu_{\infty} \in \mathbb{N}$  et  $\nu \in \mathbb{Z}$  tels que*

$$(R_p^{(n)} : U_p^{(n)}) = p^{\mu_{\infty} p^n + \nu},$$

*pour tout  $n$  assez grand. De plus, si  $F_{\infty}$  vérifie l'hypothèse de décomposition alors on  $\mu_{\infty} = 0$ .*

*Démonstration.* — On peut décomposer  $(R_p^{(n)} : U_p^{(n)})$  sous la forme

$$(R_p^{(n)} : U_p^{(n)}) = (R_p^{(n)} : U_{\mathfrak{a},p}^{(n)})(U_{\mathfrak{a},p}^{(n)} : U_{\mathfrak{ab},p}^{(n)}).$$

Il suffit maintenant d'appliquer les corollaires 3.1 et 3.4.  $\square$

#### 4. La suite des indices $[\Omega_{F_n} : V_{F_n}]$

Nous étudions dans ce paragraphe la suite  $[\Omega_{F_n} : V_{F_n}]$ . Pour cela nous avons besoin de quelques notations supplémentaires. Nous poserons  $L_n := F_n \cap k_{\mathfrak{g}_n}$  et  $L_\infty = \bigcup L_n$ . On a  $F_\infty = FL_\infty$ ,  $F_n = FL_n$  et  $L_\infty$  est une  $\mathbb{Z}_p$ -extension de  $L_0$  abélienne sur  $k$ . En particulier on a  $\text{Gal}(F_\infty/L_\infty) \simeq \text{Gal}(F_n/L_n)$ . De plus, l'égalité  $F_n = FL_n$  montre bien que pour  $n$  assez grand, disons  $n \geq n_0$ , le conducteur de  $L_n/k$  est égal à  $\mathfrak{g}_n$ . Nous allons commencer par étudier la suite des indices  $[\Omega_{L_n} : V_{L_n}]$ . En cela nous utiliserons le groupe

$$\mathcal{P}'_{L_n} = \mathcal{P}_{L_n} / \mu(L_n)(k^\times)^{12e_{\mathfrak{g}_n}}$$

qu'il est possible de représenter par générateurs et relations. Rappelons l'égalité  $x^{12} = \Delta(\mathcal{O}_k)/\Delta(x\mathcal{O}_k)$ , pour tout  $x \in k^\times$ , qui prouve que l'on a bien  $(k^\times)^{12e_{\mathfrak{g}_n}} \subset \mathcal{P}_{L_n}$ . Il n'est pas difficile de vérifier que

$$\mathcal{P}_{L_n} / \Omega_{L_n}(k^\times)^{12e_{\mathfrak{g}_n}}$$

est un groupe fini. On en déduit que  $\mathcal{P}'_{L_n}$  est de type fini comme groupe abélien, de même rang que  $\Omega_{L_n}$ , c'est à dire  $[L_n : k] - 1$ . On est dans un cas favorable puisque, comme on va le voir ci-dessous, les seules relations reliant les éléments de  $\mathcal{P}'_{L_n}$  sont celles issues des formules de norme (2.6). De manière formelle, les choses se présentent comme suit. Soit  $\mathcal{A}$  le groupe abélien libre de base la réunion disjointe

$$\bigsqcup_{\mathfrak{g} \in \Sigma_n} \text{Gal}(L_n \cap k_{\mathfrak{g}}/k),$$

où  $\Sigma_n = \{(1), \mathfrak{g}_n\}$  si  $\mathfrak{g}_n$  est divisible par un seul idéal premier et

$$\Sigma_n = \{(1), \mathfrak{g}_n, \mathfrak{p}^{i_n}, \bar{\mathfrak{p}}^{j_n}\}$$

si  $\mathfrak{g}_n = \mathfrak{p}^{i_n} \bar{\mathfrak{p}}^{j_n}$ . Le groupe  $\mathcal{A}$  est naturellement un module galoisien. De plus nous disposons d'un homomorphisme surjectif  $\mathcal{F} : \mathcal{A} \rightarrow \mathcal{P}'_{L_n}$ , défini pour  $\sigma$  dans  $\text{Gal}(L_n \cap k_{\mathfrak{g}}/k)$  où  $\mathfrak{g} \in \Sigma_n$  par

$$\mathcal{F}(\sigma) = \begin{cases} \text{la classe de } (\varphi_{L_n, \mathfrak{g}})^\sigma & \text{si } \mathfrak{g} \neq (1), \\ \text{la classe de } (\Delta(\mathfrak{a}^{-1})/\Delta(\mathcal{O}_k))^{e_{\mathfrak{g}_n}} & \text{si } \mathfrak{g} = (1) \text{ et } \sigma = (\mathfrak{a}, H/k). \end{cases}$$

Le noyau de  $\mathcal{F}$  contient le  $\mathbb{Z}$ -module  $\mathcal{R}$  engendré par les sommes

$$S_{\mathfrak{g}, \mathfrak{g}'}(\sigma) = \sum_{\tau \rightarrow \sigma} \tau - \sigma \left( \prod_{\mathfrak{q} | \mathfrak{g}'} (1 - (\mathfrak{q}, L_n \cap k_{\mathfrak{g}}/k)^{-1}) \right),$$



où  $\mathfrak{g}, \mathfrak{g}' \in \Sigma_n$  sont premiers entre eux et tels que  $\mathfrak{g}' \neq (1)$ . De plus  $\sigma$  appartient à  $\text{Gal}(L_n \cap k_{\mathfrak{g}}/k)$  et  $\sum_{\tau \rightarrow \sigma} \tau$  désigne la somme des éléments de  $\text{Gal}(L_n \cap k_{\mathfrak{g}\mathfrak{g}'}/k)$  dont la restriction à  $L_n \cap k_{\mathfrak{g}}$  est égal à  $\sigma$ . Le produit

$$\prod_{\mathfrak{q}|\mathfrak{g}'} (1 - (\mathfrak{q}, L_n \cap k_{\mathfrak{g}}/k)^{-1})$$

est pris sur les idéaux premiers qui divisent  $\mathfrak{g}'$ . Ces sommes  $S_{\mathfrak{g}, \mathfrak{g}'}(\sigma)$  sont en fait la formalisation des relations de norme citées ci-dessus.

On peut exhiber une  $\mathbb{Z}$ -base de  $\mathcal{A}$  qui nous permettra en même temps d'en déduire directement une base de  $\mathcal{A}/\mathcal{R}$ . En effet, pour tout  $(1) \neq \mathfrak{g} \in \Sigma_n$  divisible par un seul idéal premier, on fixe  $X_{\mathfrak{g}} \subset \text{Gal}(L_n \cap k_{\mathfrak{g}}/k)$  tel que la restriction des automorphismes est une bijection de  $X_{\mathfrak{g}}$  sur  $\text{Gal}(H/k)$ . De plus, si  $\mathfrak{g}_n = \mathfrak{p}^{i_n} \bar{\mathfrak{p}}^{j_n}$  alors pour tous  $\sigma_1 \in \text{Gal}(L_n \cap k_{\mathfrak{p}^{i_n}}/k)$  et tout  $\sigma_2 \in \text{Gal}(L_n \cap k_{\bar{\mathfrak{p}}^{j_n}}/k)$  tels que  $\sigma_1$  et  $\sigma_2$  coïncident sur  $H$ , on fixe  $\gamma(\sigma_1, \sigma_2) \in \text{Gal}(L_n/k)$  un automorphisme qui prolonge à la fois  $\sigma_1$  et  $\sigma_2$ . Posons alors

$$X_{\mathfrak{g}_n} = \{\gamma(\sigma_1, \sigma_2), \text{ tel que } \sigma_1 \in X_{\mathfrak{p}^{i_n}} \text{ ou } \sigma_2 \in X_{\bar{\mathfrak{p}}^{j_n}}\}.$$

Posons aussi  $X_{(1)} = \emptyset$  et pour tout  $\mathfrak{g} \in \Sigma_n$ , introduisons l'ensemble

$$\Upsilon_{\mathfrak{g}} = \{S_{\mathfrak{g}, \mathfrak{g}'}(\sigma), \text{ tel que } \mathfrak{g}' \in \Sigma_n \text{ est premier à } \mathfrak{g} \text{ et } \sigma \in \text{Gal}(L_n \cap k_{\mathfrak{g}}/k) - X_{\mathfrak{g}}\},$$

où  $S_{\mathfrak{g}, (1)}(\sigma) = \sigma$ . Maintenant on peut montrer

**PROPOSITION 4.1.** — *L'ensemble  $\Upsilon = \bigsqcup_{\mathfrak{g} \in \Sigma_n} \Upsilon_{\mathfrak{g}}$  est une  $\mathbb{Z}$ -base de  $\mathcal{A}$ . On en déduit que l'ensemble  $\bigsqcup_{\mathfrak{g} \in \Sigma_n} \text{Gal}(L_n \cap k_{\mathfrak{g}}/k) - X_{\mathfrak{g}}$  est une base de  $\mathcal{A}/\mathcal{R}$ .*

*Démonstration.* — Il suffit de montrer la première assertion de la proposition. De plus, comme le cardinal de  $\Upsilon$  est égal au rang de  $\mathcal{A}$ , il suffit en fait de vérifier que  $\Upsilon$  engendre  $\mathcal{A}$ . Si  $B$  est une partie de  $\mathcal{A}$ , alors nous noterons  $\langle B \rangle$  le sous- $\mathbb{Z}$ -module de  $\mathcal{A}$  engendré par  $B$ . Soit donc  $\mathfrak{g} \in \Sigma_n$ , divisible par un seul idéal premier. Soit  $\sigma \in \text{Gal}(L_n \cap k_{\mathfrak{g}}/k)$  et soit  $\gamma$  sa restriction à  $H$ . Par définition même de  $X_{\mathfrak{g}}$ , la somme  $\sum_{\tau \rightarrow \gamma} \tau$  contient un seul  $\tau \in X_{\mathfrak{g}}$ . En particulier si  $\sigma \in X_{\mathfrak{g}}$ , alors

$$\sigma - S_{(1), \mathfrak{g}}(\gamma) \in \langle \Upsilon_{\mathfrak{g}} \bigsqcup \Upsilon_{(1)} \rangle.$$

D'où l'on déduit que  $\sigma \in \langle \Upsilon \rangle$ . Supposons maintenant que  $\mathfrak{g}_n = \mathfrak{p}^{i_n} \bar{\mathfrak{p}}^{j_n}$ . Posons  $\mathfrak{g} = \mathfrak{p}^{i_n}$  et  $\mathfrak{g}' = \bar{\mathfrak{p}}^{j_n}$ . Soit  $\sigma \in X_{\mathfrak{g}_n}$ , c'est-à-dire  $\sigma = \gamma(\sigma_1, \sigma_2)$ , avec  $\sigma_1 \in X_{\mathfrak{g}}$  ou  $\sigma_2 \in X_{\mathfrak{g}'}$ . Si  $\sigma_2 \notin X_{\mathfrak{g}'}$ , alors en raisonnant comme ci-dessus on voit que

$$\sigma - S_{\mathfrak{g}', \mathfrak{g}}(\sigma_2) \in \left\langle \Upsilon_{\mathfrak{g}_n} \bigsqcup \text{Gal}(L_n \cap k_{\mathfrak{g}'}/k) \right\rangle \subset \langle \Upsilon \rangle.$$

Comme  $S_{\mathfrak{g}', \mathfrak{g}}(\sigma_2) \in \langle \Upsilon_{\mathfrak{g}'} \rangle$  on peut conclure que  $\sigma \in \langle \Upsilon \rangle$ . Si  $\sigma_1 \in X_{\mathfrak{g}}$  et  $\sigma_2 \in X_{\mathfrak{g}'}$ , il suffit d'utiliser  $\sigma - S_{(1), \mathfrak{g}_n}(\gamma)$  pour se ramener aux cas précédents, où  $\gamma$  est la restriction de  $\sigma$  à  $H$ . La proposition est maintenant entièrement démontrée.  $\square$

Notons  $\mathcal{A}' \subset \mathcal{A}$  le noyau de l'homomorphisme  $\deg : \mathcal{A} \rightarrow \mathbb{Z}$  défini par  $\deg(\sigma) = 0$  si  $\sigma \in \text{Gal}(L_n \cap k_{\mathfrak{g}}/k)$  avec  $(1) \neq \mathfrak{g} \in \Sigma_n$  et  $\deg(\sigma) = 1$  si  $\sigma \in \text{Gal}(H/k)$ . On constate que  $\mathcal{R} \subset \mathcal{A}'$ . De plus la restriction de  $\mathcal{F}$  à  $\mathcal{A}'$ , qu'on notera  $\mathcal{F}'$ , est surjective. Or le rang de  $\mathcal{A}'/\mathcal{R}$  est égal à  $[L_n : k] - 1$ . Ainsi on obtient, par factorisation de  $\mathcal{F}'$ , un isomorphisme

$$(4.1) \quad \mathcal{A}'/\mathcal{R} \simeq \mathcal{P}'_{L_n}.$$

LEMME 4.1. — *Il existe un entier  $\kappa$  tel que pour tout  $n$  le groupe  $\Omega_{L_n}/V_{L_n}$  a au plus  $\kappa$  générateurs.*

*Démonstration.* — Notons  $A_n$  le sous-module galoisien de  $\mathcal{P}_{L_n}$  engendré par  $Q^{e_{\mathfrak{g}_n}}$  et par tous les  $\varphi_{L_n, \mathfrak{g}}$ ,  $\mathfrak{g} \in \Sigma_n - \{(1), \mathfrak{g}_n\}$  si cet ensemble est non vide. Notons aussi  $B_n$  le sous-module galoisien de  $\mathcal{P}_{L_n}$  engendré par  $\varphi_{L_n, \mathfrak{g}_n}$ . Il est clair que  $\Omega_{L_n}/V_{L_n}$  est engendré par les classes des éléments des groupes  $A_n \cap \mathcal{O}_{L_n}^\times$  et  $B_n \cap \mathcal{O}_{L_n}^\times$ . Si  $\mathfrak{g}_n$  est divisible par un seul idéal premier alors  $A_n \cap \mathcal{O}_{L_n}^\times \subset \mathcal{O}_H^\times$ . Si  $\mathfrak{g}_n = \mathfrak{p}^{i_n} \bar{\mathfrak{p}}^{j_n}$  alors  $L_n \cap k_{\mathfrak{p}^{i_n}}$  et  $L_n \cap k_{\bar{\mathfrak{p}}^{j_n}}$  ne dépendent pas de  $n$  pour  $n$  assez grand. Si  $K$  est le compositum de tous ces corps. C'est un corps de nombres, et on a  $A_n \cap \mathcal{O}_{L_n}^\times \subset \mathcal{O}_K^\times$ . Il nous reste donc à étudier  $B_n \cap \mathcal{O}_{L_n}^\times$ . Posons alors  $d = [L_0 : k]$  et soient  $\mathfrak{a}_1, \dots, \mathfrak{a}_d$  des idéaux de  $\mathcal{O}_k$  tels que  $(\mathfrak{a}_1, L_n/k)$  engendre le groupe cyclique  $\text{Gal}(L_n/L_0)$  et  $\text{Gal}(L_0/k) - \{1\} = \{(\mathfrak{a}_2, L_0/k), \dots, (\mathfrak{a}_d, L_0/k)\}$ . On peut facilement montrer que  $J_{L_n}/I_{L_n}J_{L_n}$  est engendré sur  $\mathbb{Z}$  par les classes de  $w_{L_n}$  et par tous les  $\nu_i = N(\mathfrak{a}_i) - (\mathfrak{a}_i, L_n/k)$ . Comme on peut écrire  $\sigma = (\sigma - N(\mathfrak{a}_\sigma)) + N(\mathfrak{a}_\sigma)$ , pour tout  $\sigma \in \text{Gal}(L_n/k)$  et tout idéal  $\mathfrak{a}_\sigma$  de  $\mathcal{O}_k$  tel que  $\sigma = (\mathfrak{a}_\sigma, L_n/k)$  on voit que  $B_n/B_n \cap V_{L_n}$  a au plus  $d + 1$  générateurs. D'où le lemme.  $\square$

DÉFINITION 4.1. — Pour toute extension abélienne finie  $K$  de  $k$  contenant  $H$ , on pose

$$\mathfrak{X}_K := \frac{\prod_{\mathfrak{p}} [K_{\mathfrak{p}^\infty} : H]}{[K : H]}$$

où le produit est pris sur tous les idéaux premiers de  $\mathcal{O}_k$ .

Nous sommes maintenant prêt à donner un premier résultat sur la suite

$$\Lambda(L_n) = \frac{[\Omega_{L_n} : V_{L_n}] \mathfrak{X}_{L_n}}{w_{L_n}} = \prod_{\ell} \ell^{r(L_n, \ell)},$$

où  $\ell$  parcourt tous les nombres premiers.

PROPOSITION 4.2. — *Soit  $\ell$  un nombre premier. Alors la suite  $(r(L_n, \ell))_n$  est bornée. De plus si  $\ell \nmid w_H$  alors les termes de cette suite ne dépendent pas de  $n$  pour tout  $n$  assez grand.*

*Démonstration.* — Notons  $\delta_n$  le plus grand diviseur commun de  $[L_n : L_n \cap k_{\mathfrak{p}^{i_n}}]$  et  $[L_n : L_n \cap k_{\bar{\mathfrak{p}}^{j_n}}]$  si  $\mathfrak{g}_n = \mathfrak{p}^{i_n} \bar{\mathfrak{p}}^{j_n}$ . Si  $\mathfrak{g}_n$  est divisible par un seul idéal premier nous poserons simplement  $\delta_n = 1$ . Considérons l'application  $\mathbb{Z}$ -linéaire  $\Psi : \mathcal{A} \rightarrow \mathbb{Z} \times \text{Hom}(\mu(L_n), \mu(L_n))$  définie pour un  $\sigma \in \text{Gal}(L_n \cap k_{\mathfrak{g}}/k)$  par

$$\Psi(\sigma) = \begin{cases} 0 & \text{si } \mathfrak{g} \neq \mathfrak{g}_n, \\ (1, w_H j_{L_n}(\sigma)) & \text{si } \mathfrak{g} = \mathfrak{g}_n. \end{cases}$$

Il est facile de vérifier que si  $\mathfrak{g}_n$  est divisible par un seul idéal premier, alors on a  $\Psi(\mathcal{R}) \subset \{0\} \times \{0\}$ . De plus, lorsque  $\mathfrak{g}_n = \mathfrak{p}^{i_n} \bar{\mathfrak{p}}^{j_n}$  le nombre de racines de l'unité de  $L_n \cap k_{\mathfrak{p}^{i_n}}$  et de  $L_n \cap k_{\bar{\mathfrak{p}}^{j_n}}$  est égal à  $w_H$ . Ceci permet de voir que dans ce cas on a  $\Psi(\mathcal{R}) \subset \delta_n \mathbb{Z} \times \{0\}$ . Ainsi grâce à l'isomorphisme (4.1), l'application  $\Psi$  induit de manière naturelle un homomorphisme de groupes abéliens

$$\rho_n : \Omega_{L_n} \longrightarrow \mathbb{Z}/\delta_n \mathbb{Z} \times \text{Hom}(\mu(L_n), \mu(L_n)).$$

On a

$$\text{Im}(\rho_n) = \begin{cases} \{0\} \times j_{L_n}(w_k w_H) & \text{si } \mathfrak{g}_n = \mathfrak{p}^{i_n}, \\ \mathbb{Z}/\delta_n \mathbb{Z} \times j_{L_n}(w_H) & \text{sinon.} \end{cases}$$

D'où l'on déduit

$$[\Omega_{L_n} : \ker(\rho_n)] = \begin{cases} w_{L_n} / \gcd(w_k w_H, w_{L_n}) & \text{si } \mathfrak{g}_n = \mathfrak{p}^{i_n}, \\ \delta_n w_{L_n} / w_H & \text{sinon,} \end{cases}$$

où  $\gcd(w_k w_H, w_{L_n})$  est le plus grand diviseur commun de  $w_k w_H$  et  $w_{L_n}$ . Par ailleurs, il est immédiat que  $V_{L_n} \subset \ker(\rho_n)$ . De plus, les relations de normes (2.6) permettent de voir que le groupe  $\ker(\rho_n)/V_{L_n}$  est tué par  $(N(\mathfrak{c}) - 1)w_H$ , pour tout idéal  $\mathfrak{c}$  de  $\mathcal{O}_k$  premier à  $\mathfrak{g}_n$ . Or  $w_k$  est le plus grand diviseur commun de ces entiers  $N(\mathfrak{c}) - 1$ . Il en découle que  $\ker(\rho_n)/V_{L_n}$  est tué par  $w_k w_H$ . Ainsi, on déduit grâce au lemme 4.1 que l'indice  $[\ker(\rho_n) : V_{L_n}]$  divise  $(w_k w_H)^\kappa$ . Comme  $\delta_n \mathfrak{X}_{L_n}$  est constant pour  $n$  assez grand, la proposition suit.  $\square$

Nous avons besoin de relier les deux groupes  $\Omega_{L_n}/V_{L_n}$  et  $\Omega_{F_n}/V_{F_n}$  pour pouvoir compléter notre étude. On part de l'inclusion

$$(\mathcal{P}_{L_n})^{e_{f_n}/e_{\mathfrak{g}_n}} \subset \mathcal{P}_{F_n}, \quad n \geq n_0,$$

qui permet de définir un homomorphisme de modules galoisiens

$$\Phi_n : \mathcal{P}_{L_n} \longrightarrow \mathcal{P}_{F_n}, \quad \Phi_n(x) = x^{v_n},$$

où  $v_n = e_{f_n}/e_{\mathfrak{g}_n}$ . D'autre part, comme on a aussi  $(V_{L_n})^{v_n} \subset V_{F_n}$  l'application  $\Phi_n$  induit un homomorphisme

$$\Phi'_n : \Omega_{L_n}/V_{L_n} \longrightarrow \Omega_{F_n}/V_{F_n}, \quad n \geq n_0,$$

L'étude de  $\text{Im}(\Phi'_n)$  et  $\text{coker}(\Phi'_n)$  nous permettra de conclure. Nous utiliserons les deux familles d'homomorphismes

$$\Psi_{n,m} : \Omega_{F_n}/V_{F_n} \longrightarrow \Omega_{F_m}/V_{F_m} \quad \text{et} \quad N_{m,n} : \Omega_{F_m}/V_{F_m} \longrightarrow \Omega_{F_n}/V_{F_n},$$

définis pour tous  $m \geq n$  de la façon suivante. On pose  $\Psi_{n,m}(x) = x^{e(n,m)}$ , où  $e(n,m) := e_{f_m}/e_{f_n}$ , alors que  $N_{m,n}$  associe à la classe de  $z \in \Omega_{F_m}$  la classe d'une racine  $e(n,m)$ -ième de  $N_{F_m/F_n}(z)$ . Il n'est pas difficile de vérifier que  $\Psi_{n,m}$  et  $N_{m,n}$  sont bien définis et sont effectivement des homomorphismes de groupes. D'après la preuve du lemme 4.1,  $\text{Im}(\Phi'_n)$  est engendré par les images dans  $\Omega_{F_n}/V_{F_n}$  des groupes

$$\Phi_n(A_n) \cap \mathcal{O}_{F_n}^\times = \Phi_n(A_n \cap \mathcal{O}_{L_n}^\times) \quad \text{et} \quad \Phi_n(B_n) \cap \mathcal{O}_{F_n}^\times = \Phi_n(B_n \cap \mathcal{O}_{L_n}^\times),$$

qu'on notera respectivement  $A_n^F$  et  $B_n^F$ . Précisons qu'en définitive  $\Phi_n(A_n)$  est le sous-module galoisien de  $\mathcal{P}_{F_n}$  engendré par  $Q^{e_{f_n}}$  et par tous les  $\varphi_{F_n, \mathfrak{g}}$ ,  $\mathfrak{g} \in \Sigma_n - \{(1), \mathfrak{g}_n\}$  si cet ensemble est non vide. De même  $\Phi_n(B_n)$  est le sous-module galoisien de  $\mathcal{P}_{F_n}$  engendré par  $\varphi_{F_n, \mathfrak{g}_n}$ . La relation

$$N_{F_m/F_n}(\varphi_{F_m, \mathfrak{g}_m}) = (\varphi_{F_n, \mathfrak{g}_n})^{e(n,m)},$$

donne

$$(4.2) \quad N_{m,n}(B_m^F) = B_n^F.$$

Comme on l'a déjà remarqué, lorsque  $\mathfrak{g}_n = \mathfrak{p}^{i_n} \bar{\mathfrak{p}}^{j_n}$  les corps  $F_n \cap k_{\mathfrak{p}^{i_n}}$  et  $F_n \cap k_{\bar{\mathfrak{p}}^{j_n}}$  ne dépendent pas de  $n$  pour tout  $n$  assez grand. On en déduit les deux égalités

$$\varphi_{F_m, \mathfrak{p}^{i_m}} = (\varphi_{F_n, \mathfrak{p}^{i_n}})^{e(n,m)} \quad \text{et} \quad \varphi_{F_m, \bar{\mathfrak{p}}^{j_m}} = (\varphi_{F_n, \bar{\mathfrak{p}}^{j_n}})^{e(n,m)},$$

pour tous  $m \geq n$  assez grands. Ce qui permet de conclure que dans tous les cas on a

$$(4.3) \quad \Psi_{n,m}(A_m^F) = A_m^F,$$

pour tous  $m \geq n$  assez grands.

**DÉFINITION 4.2.** — Pour tout nombre premier  $\ell$ , on note  $\ell^{\pi_n(\ell)}$  l'ordre du  $\ell$ -sous-groupe de Sylow de  $\text{Im}(\Phi'_n)$ .

**PROPOSITION 4.3.** — *Pour tout  $\ell$  il existe  $N$  un entier (qu'on peut prendre indépendant de  $\ell$ ) tel que la suite  $(\pi_n(\ell))_{n \geq N}$  est croissante. De plus, si la suite  $(w_{F_n})_n$  est bornée et  $\mathfrak{g}_n$  est divisible par un seul idéal premier, alors  $\pi_n(\ell)$  ne dépend pas de  $n$  pour tout  $n$  assez grand.*

*Démonstration.* — La formule (4.3) montre que les groupes  $A_n^F$  sont isomorphes pour  $n$  assez grand. Comme on a

$$\Psi_{n,m}(A_n^F \cap B_n^F) \subset A_m^F \cap B_m^F,$$

les groupes  $A_n^F \cap B_n^F$  sont aussi isomorphes pour  $n$  assez grands. De plus, d'après (4.2), la restriction de  $N_{m,n} : B_m^F \rightarrow B_n^F$  est surjective. L'isomorphisme

$$\mathrm{Im}(\Phi'_n)/A_n^F \simeq B_n^F/A_n^F \cap B_n^F,$$

le fait que  $B_n^F$  est tué par  $w_k w_{L_n} \delta_n$  et le lemme 4.1 permettent de conclure.  $\square$

**PROPOSITION 4.4.** — *Supposons que la suite  $(w_{F_n})_n$  est bornée et  $\mathfrak{g}_n$  est divisible par deux idéaux premiers. Alors on a  $\pi_{n+1}(p) \geq \pi_n(p) + 1$ , pour tout  $n$  assez grand.*

*Démonstration.* — On sait grâce à la preuve de la proposition 4.3 qu'il suffit de vérifier que le  $p$ -Sylow de  $\ker(N_{n+1,n}) \cap B_{n+1}^F$  est non trivial pour tout  $n$  assez grand. Notons alors  $w_{F_\infty}$  le nombre de racines de l'unité de  $F_\infty$ , qui est fini par hypothèse. Soit  $p^a$  la puissance exacte de  $p$  qui divise  $w_k w_{F_\infty} [F_\infty : L_\infty]$ . Choisissons  $n$  assez grand de sorte que  $p^{a+1}$  divise  $\delta_n$  et  $\delta_m = \delta_n [L_m : L_n]$  pour tout  $m \geq n$ . Posons  $x_m = w_k w_{F_\infty} \delta_m / p^{a+1}$ . Alors l'élément  $\varphi_{F_m, \mathfrak{g}_m}$  de  $\mathrm{Im}(\Phi'_m)$  est tel que

$$(\varphi_{F_m, \mathfrak{g}_m})^{x_m} \notin V_{F_m}, \quad \text{pour tout } m \geq n.$$

Car le contraire entraînerait, en prenant la norme de  $F_m$  à  $L_m$ , que l'unité  $(\varphi_{L_m, \mathfrak{g}_m})^{x_m [F_\infty : L_\infty]} \in V_{L_m} \subset \ker(\rho_m)$ . Ce qui est faux. En revanche on a évidemment

$$(\varphi_{F_m, \mathfrak{g}_m})^{x_m p^{a+1}} \in V_{F_m}, \quad \text{pour tout } m \geq n.$$

On en déduit que l'ensemble des entiers  $c \in \mathbb{N}$  satisfaisant  $(\varphi_{F_m, \mathfrak{g}_m})^{x'_m} \in V_{F_m}$ , pour tout  $m \geq n$  assez grand, où  $x'_m = x_m p^{a+1-c}$ , est non vide et majoré par  $a$ . Soit  $b$  le plus grand élément de cet ensemble. Posons

$$\Gamma_m = \text{la classe de } (\varphi_{F_m, \mathfrak{g}_m})^{x_m p^{a-b}} \text{ dans } \Omega_{F_m}/V_{F_m}, \quad \text{pour tout } m \geq n.$$

Par définition de  $\Gamma_m$  on a  $N_{m+1,m}(\Gamma_{m+1}) = 1$  et  $\Gamma_{m+1}^p = 1$ , pour tout  $m \geq n$  assez grand. D'autre part, comme on a  $\Psi_{m,m+1}(\Gamma_m) = \Gamma_{m+1}$ , on voit que  $\Gamma_{m+1} \neq 1$ , pour tout  $m \geq n$  assez grand.  $\square$

**PROPOSITION 4.5.** — *Supposons que la suite  $(w_{F_n})_n$  n'est pas bornée et  $\mathfrak{g}_n$  est divisible par un seul idéal premier. Alors on a  $\pi_{n+1}(p) \geq \pi_n(p) + 1$ , pour tout  $n$  assez grand.*

*Démonstration.* — Là aussi il suffit de vérifier que le  $p$ -Sylow de  $\ker(N_{n+1,n}^F) \cap B_{n+1}^F$  est non trivial pour tout  $n$  assez grand. Soit  $\mathfrak{c}$  un idéal propre de  $\mathcal{O}_k$  premier à  $6\mathfrak{f}_m$ , pour tout  $m$ . Soit  $p^a$  la puissance exacte de  $p$  qui divise  $w_k w_H(N(\mathfrak{c}) - 1)[F_\infty : L_\infty]$ . Choisissons  $n$  assez grand de sorte que  $p^{a+1}$  divise  $w_{L_n}$  et  $w_{L_m} = [L_m : L_n] w_{L_n}$  pour tout  $m \geq n$ . Posons  $\sigma_m = (\mathfrak{c}, F_m/k)$  et  $z_m = w_k(\sigma_m - 1)w_{L_m}/p^{a+1}$ . On constate alors que

$$(\varphi_{F_m, \mathfrak{g}_m})^{z_m} \notin V_{F_m}, \quad \text{pour tout } m \geq n.$$

Car le contraire entraînerait, en prenant la norme de  $F_m$  à  $L_m$ , que  $(\varphi_{L_m, \mathfrak{g}_m})^{z_m[F_\infty:L_\infty]}$  est dans  $V_{L_m} \subset \ker(\rho_m)$ . Ce qui est faux. En revanche on a

$$(\varphi_{F_m, \mathfrak{g}_m})^{z_m p^{a+1}} \in V_{F_m}, \quad \text{pour tout } m \geq n.$$

On en déduit que l'ensemble des entiers  $c \in \mathbb{N}$  satisfaisant  $(\varphi_{F_m, \mathfrak{g}_m})^{z'_m} \in V_{F_m}$ , pour tout  $m \geq n$  assez grand, où  $z'_m = z_m p^{a+1-c}$ , est non vide et majoré par  $a$ . Soit  $b$  le plus grand élément de cet ensemble. Posons

$$\Lambda_m = \text{la classe de } (\varphi_{F_m, \mathfrak{g}_m})^{z_m p^{a-b}} \text{ dans } \Omega_{F_m}/V_{F_m}, \quad \text{pour tout } m \geq n.$$

Par définition de  $\Lambda_m$  on a  $N_{m+1, m}(\Lambda_{m+1}) = 1$  et  $\Lambda_{m+1}^p = 1$ , pour tout  $m \geq n$  assez grand. D'autre part, comme on a  $\Psi_{m, m+1}(\Lambda_m) = \Lambda_{m+1}$  on voit que  $\Lambda_{m+1} \neq 1$ , pour tout  $m \geq n$  assez grand.  $\square$

PROPOSITION 4.6. — *Si la suite  $(w_{F_n})_n$  n'est pas bornée et  $\mathfrak{g}_n$  est divisible par deux idéaux premiers alors on a  $\pi_{n+1}(p) \geq \pi_n(p) + 2$ , pour tout  $n$  assez grand.*

*Démonstration.* — Soit  $\mathfrak{c}$  un idéal propre de  $\mathcal{O}_k$  premier à  $6f_m$ , pour tout  $m$ . Choisissons aussi  $n$  assez grand de sorte que  $w_{L_m} = [L_m : L_n]w_{L_n}$  et  $\delta_m = \delta_n[L_m : L_n]$  pour tout  $m \geq n$ . Posons  $\sigma_m = (\mathfrak{c}, F_m/k)$ . Comme prouvé précédemment, il existe bien  $b \in \mathbb{N}$  tel que si on pose  $b_m = w_k(\sigma_m - 1)w_{L_m}/p^{b+1}$ , alors la classe  $\Xi_m$  de  $(\varphi_{F_m, \mathfrak{g}_m})^{b_m}$  dans  $\Omega_{F_m}/V_{F_m}$  est telle que

$$N_{m+1, m}(\Xi_{m+1}) = 1, \quad \Xi_{m+1}^p = 1 \quad \text{et} \quad \Xi_{m+1} \neq 1,$$

pour tout  $m \geq n$  assez grand. Notons  $E$  l'ensemble des entiers  $u \in \mathbb{N}$  tel qu'il existe un couple  $(v, v') \in \mathbb{N} \times \mathbb{N}$  satisfaisant

$$(\varphi_{F_m, \mathfrak{g}_m})^{(y_m/p^u) - \eta_m(v, v', u)} \in V_{F_m},$$

pour tout  $m \geq n$  assez grand, où on a posé

$$y_m = w_k(\sigma_m - N(\mathfrak{c}))\delta_m \quad \text{et} \quad \eta_m(v, v', u) = w_k v'(\sigma_m - 1)w_{L_m}/p^u.$$

L'ensemble  $E$  contient 0 et est majoré. Soit  $c$  son plus grand élément et soit  $\Theta_m$  la classe dans  $\Omega_{F_m}/V_{F_m}$  de

$$(\varphi_{F_m, \mathfrak{g}_m})^{(y_m/p^{c+1}) - (\eta_m(v, v', c)/p)}.$$

Alors le sous-groupe  $\langle \Xi_m, \Theta_m \rangle$  de  $\Omega_{F_m}/V_{F_m}$  engendré par  $\Xi_m$  et  $\Theta_m$  est isomorphe à  $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ , pour tout  $m \geq n$  assez grand. De plus on a

$$\langle \Xi_{m+1}, \Theta_{m+1} \rangle \subset \ker(N_{n+1, n}) \cap B_{n+1}^F.$$

D'où la proposition.  $\square$

Il nous reste maintenant une dernière étape qui est l'étude de l'ordre de coker  $(\Phi'_n)$ . Mais d'ores et déjà on peut énoncer :

PROPOSITION 4.7. — *Il existe  $N \in \mathbb{N}$  tel que la suite  $(\#\text{coker}(\Phi'_n))_{n \geq N}$  est croissante.*

*Démonstration.* — Notons  $C_n$  le sous-module galoisien de  $\mathcal{P}_{F_n}$  engendré par l'ensemble

$$X_n := \{\varphi_{F_n, \mathfrak{g}} \text{ tel que } (1) \neq \mathfrak{g} \mid \mathfrak{h}\} \cup X'_n$$

où  $X'_n := \emptyset$  si  $\mathfrak{g}_n$  est divisible par un seul idéal premier de  $\mathcal{O}_k$ . Si  $\mathfrak{g}_n = \mathfrak{p}^{i_n} \bar{\mathfrak{p}}^{j_n}$  alors

$$X'_n := \{\varphi_{F_n, \mathfrak{g}} \text{ tels que } \mathfrak{g} = \mathfrak{u}\mathfrak{v} \text{ avec } (1) \neq \mathfrak{u} \mid \mathfrak{h} \text{ et } \mathfrak{v} = \mathfrak{p}^{i_n} \text{ ou } \bar{\mathfrak{p}}^{j_n}\}.$$

Notons aussi  $D_n$  le sous-module galoisien de  $\mathcal{P}_{F_n}$  engendré par les  $\varphi_{F_n, \mathfrak{g}}$  tels que  $\mathfrak{g} = \mathfrak{u}\mathfrak{g}_n$  avec  $(1) \neq \mathfrak{u} \mid \mathfrak{h}$ . Soit  $\beta_n$  la projection canonique  $\beta_n : \Omega_{F_n} \rightarrow \text{coker}(\Phi'_n)$ . Alors  $\text{coker}(\Phi'_n)$  est engendré par

$$C_{n,F} := \beta_n(C_n \cap \mathcal{O}_{F_n}^\times) \quad \text{et} \quad D_{n,F} := \beta_n(D_n \cap \mathcal{O}_{F_n}^\times).$$

Notons  $\bar{\Psi}_{n,m} : \text{coker}(\Phi'_n) \rightarrow \text{coker}(\Phi'_m)$  et  $\bar{N}_{m,n} : \text{coker}(\Phi'_m) \rightarrow \text{coker}(\Phi'_n)$  les familles d'homomorphismes respectivement induites par  $\Psi_{n,m}$  et  $N_{m,n}$  pour tous  $m \geq n$ . Comme on a

$$C_n^{e(n,m)} = C_m \quad \text{et} \quad N_{F_m/F_n}(D_m) = D_n^{e(n,m)},$$

pour tous  $m \geq n$  assez grands, il vient  $\bar{\Psi}_{n,m}(C_{n,F}) = C_{m,F}$  et  $\bar{N}_{m,n}(D_{m,F}) = D_{n,F}$ , pour tous  $m \geq n$  assez grands. On peut maintenant conclure puisque on a aussi la propriété  $\bar{\Psi}_{n,m}(C_{n,F} \cap D_{n,F}) \subset C_{m,F} \cap D_{m,F}$ , pour tous  $m \geq n$  assez grands.  $\square$

PROPOSITION 4.8. — *L'ordre du groupe  $\text{coker}(\Phi'_n)$  ne dépend pas de  $n$  pour tout  $n$  assez grand.*

*Démonstration.* — D'après la proposition 4.7, il suffit de montrer que l'ordre de  $\text{coker}(\Phi'_n)$  est borné indépendamment de  $n$ . Il suffit même de vérifier cela pour les groupes  $D_{n,F}$ . Or les formules de norme (2.6) entraînent en particulier l'inclusion  $N_{F_n/L_n}(D_n) \subset B_n^{v_n} = \Phi_n(B_n)$ . De plus on a

$$w_k \left( [F_n : L_n] - \sum_{\tau \in \text{Gal}(F_n/L_n)} \tau \right) (w_{F_n}/w_{L_n}) \in I_{F_n} J_{F_n}.$$

On en déduit que l'ordre d'un élément quelconque de  $D_{n,F}$  divise l'entier  $w_k[F_n : L_n](w_{F_n}/w_{L_n})$ . D'autre part, comme pour la démonstration du lemme 4.1, on peut montrer que le groupe  $D_{n,F}/D_{n,F} \cap V_{F_n}$  est engendré par tous les

$$\varphi_{F_n, \mathfrak{u}\mathfrak{g}_n} \quad \text{et} \quad \varphi_{F_n, \mathfrak{u}\mathfrak{g}_n}^{N(\mathfrak{b}_i) - (\mathfrak{b}_i, F_n/k)},$$

où  $(1) \neq \mathfrak{u} \mid \mathfrak{h}$  et  $\mathfrak{b}_1, \dots, \mathfrak{b}_t$  sont des idéaux de  $\mathcal{O}_k$  tels que  $(\mathfrak{b}_1, F_n/k)$  engendre le groupe cyclique  $\text{Gal}(F_n/F)$  et  $\text{Gal}(F/k) - \{1\} = \{(\mathfrak{b}_2, F/k), \dots, (\mathfrak{b}_t, F/k)\}$ . Ce qui permet de conclure.  $\square$

THÉORÈME 4.1. — *La suite*

$$\Lambda(F_n) := \frac{[\Omega_{F_n} : V_{F_n}] \mathfrak{X}_{K_n}}{w_{F_n}}$$

*ne dépend pas de  $n$  pour tout  $n$  assez grand.*

*Démonstration.* — Décomposons  $\Lambda(F_n) = \prod_{\ell} \ell^{r(F_n, \ell)}$  en produit de puissances de nombres premiers. Alors l'égalité

$$\Lambda(F_n) = \#\mathrm{Im}(\Phi'_n) \cdot \#\mathrm{coker}(\Phi'_n) \cdot \frac{\mathfrak{X}_{K_n}}{w_{F_n}}$$

et les propositions 4.3, 4.4, 4.5, 4.6 et 4.8 montrent que pour tout nombre premier  $\ell$  la suite d'entiers rationnels  $(r(F_n, \ell))_{n \geq N}$  est croissante à partir d'un certain rang  $N$ . Or on a aussi

$$\Lambda(F_n) = \Lambda(L_n) \frac{\mathfrak{X}_{F_n}}{\mathfrak{X}_{L_n}} \frac{w_{L_n}}{w_{F_n}} \frac{1}{\#\ker(\Phi'_n)}.$$

Ce qui permet de voir, grâce à la proposition 4.2, que la suite  $(r(F_n, \ell))_n$  est majorée. D'où le théorème.  $\square$

## 5. Conclusion

Nous arrivons maintenant à la preuve du théorème de l'introduction. La première assertion de celui-ci découle de la formule (2.10), le théorème 3.1 ainsi que le théorème 4.1. Pour obtenir la deuxième partie du théorème il faut aussi utiliser la proposition 3.1.

**Remerciements.** — Une partie de ce travail a été effectuée lors du séjour de l'auteur à l'Université de Tsinghua à Pékin. Je voudrais ici exprimer toute ma gratitude à Linsheng Yin et à tout le département de Mathématiques de cette université, pour l'accueil chaleureux qu'ils m'ont réservé.

## BIBLIOGRAPHIE

- [1] W. BLEY — « Equivariant Tamagawa number conjecture for abelian extensions of a quadratic imaginary field », *Doc. Math.* **11** (2006), p. 73–118.
- [2] R. GILLARD — « Remarques sur les unités cyclotomiques et les unités elliptiques », *J. Number Theory* **11** (1979), p. 21–48.
- [3] B. H. GROSS & M. ROSEN — « Fourier series and the special values of  $L$ -functions », *Adv. in Math.* **69** (1988), p. 1–31.
- [4] D. S. KUBERT & S. LANG — *Modular units*, Grundlehren der Mathematischen Wissenschaften, vol. 244, Springer, 1981.



- [5] H. OUKHABA – « Index formulas for ramified elliptic units », *Compositio Math.* **137** (2003), p. 1–22.
- [6] G. ROBERT – *Unités elliptiques*, Société Mathématique de France, 1973, Bull. Soc. Math. France, Mém. n° 36, t. 101.
- [7] ———, « Concernant la relation de distribution satisfaite par la fonction  $\phi$  associée à un réseau complexe », *Invent. Math.* **100** (1990), p. 231–257.
- [8] ———, « Unités de Stark et racine 12-ième canonique », Prépublication de l’institut Fourier n° 181, 1991.
- [9] ———, « La racine 12-ième canonique de  $\Delta(L)^{[L:L]}/\Delta(\underline{L})$  », in *Séminaire de Théorie des Nombres, Paris, 1989–90*, Progr. Math., vol. 102, Birkhäuser Boston, 1992, p. 209–232.
- [10] K. RUBIN – « The “main conjectures” of Iwasawa theory for imaginary quadratic fields », *Invent. Math.* **103** (1991), p. 25–68.
- [11] W. SINNOTT – « On the Stickelberger ideal and the circular units of an abelian field », *Invent. Math.* **62** (1980/81), p. 181–234.
- [12] J. TATE – *Les conjectures de Stark sur les fonctions  $L$  d’Artin en  $s = 0$* , Progress in Mathematics, vol. 47, Birkhäuser Boston Inc., 1984, Lecture notes édité par Dominique Bernardi et Norbert Schappacher.