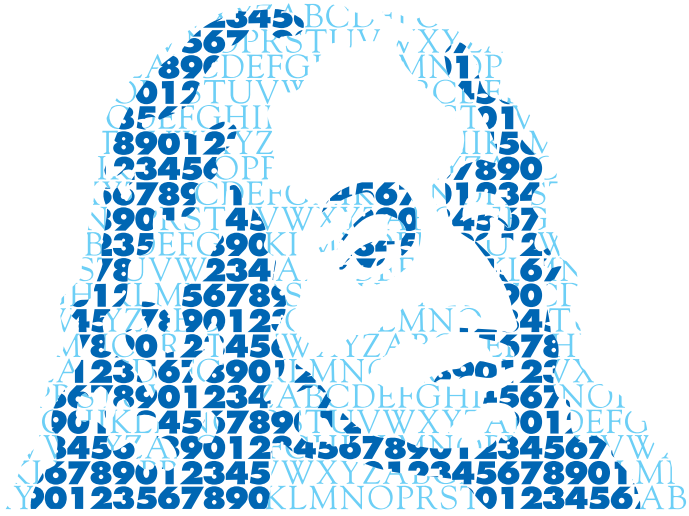
ANNALES MATHÉMATIQUES



BLAISE PASCAL

Hassan Oukhaba

Unités elliptiques, indice et $\mathbf{Z}_p$-extensions

Volume 16, n° 1 (2009), p. 165-188.

<http://ambp.cedram.org/item?id=AMBP_2009__16_1_165_0>

Publication éditée par le laboratoire de mathématiques de l'université Blaise-Pascal, UMR 6620 du CNRS Clermont-Ferrand — France

cedram

Article mis en ligne dans le cadre du Centre de diffusion des revues académiques de mathématiques
http://www.cedram.org/

Annales mathématiques Blaise Pascal **16**, 165-188 (2009)

Unités elliptiques, indice et $\mathbf{Z}_p$-extensions

Hassan Oukhaba

Résumé

Cet article rend compte de résultats sur les unités elliptiques prouvés récemment par l'auteur concernant l'indice des groupes engendrés par ces unités et son comportement dans les $\mathbf{Z}_p$-extensions.

1. Introduction

Cet article est consacré aux unités elliptiques. Lesquelles, rappelons le, interviennent de manière critique dans l'arithmétique des courbes elliptiques à multiplication complexe. Nous présentons ci-dessous deux résultats importants, à savoir le Théorème 2.8 et le Théorème 3.16. Le Théorème 2.8 donne l'indice du groupe de Kubert-Lang défini au paragraphe 2. Signalons que dans le cas des corps de rayon on peut prouver des résultats nettement plus précis. Voir [4], [5] et [6]. Dans le Théorème 3.16 on rend compte du comportement dans les $\mathbf{Z}_p$-extensions du quotient de la p-partie de l'indice des unités elliptiques de Rubin, cf. Définition 3.1, par la p-partie du nombre de classes d'idéaux. On exhibe ainsi un certain μ_∞-invariant qui contrôle ce comportement. On donne une condition suffisante, portant sur les groupes de décomposition, pour que cet invariant μ_∞ s'annule.

Notation 1.1. Tous nos corps sont supposés plongés dans le corps des nombres complexes $\mathbf{C}$. On fixera k, un corps quadratique imaginaire et on notera H son corps de classe de Hilbert. Le degré $[H : k]$ sera noté h. Soit F une extension abélienne finie de k. Alors on notera $\mathcal{O}_F$ (resp. $\mathcal{O}_F^\times$) l'anneau des entiers (resp. le groupe des unités) de F. Le groupe des racines de l'unité de F sera noté μ_F, son ordre w_F. Soit $\mathfrak{a}$ un idéal fractionnaire de k. Alors on notera $\bar{\mathfrak{a}}$ l'image de $\mathfrak{a}$ par la conjugaison complexe. Si $\mathfrak{a}$ est entier alors on notera $\hat{\mathfrak{a}}$ le produit des idéaux premiers de $\mathcal{O}_k$ qui

Mots-clés : Unités elliptiques, indice, $\mathbf{Z}_p$-extensions.
Classification math. : 11G16, 11R23.

divisent $\mathfrak{a}$. Si $\mathfrak{a}$ est 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 d'Artin. Souvent on aura recours à la notation G_F pour désigner le groupe $\mathrm{Gal}(F/k)$. Le groupe d'inertie dans F/k d'un idéal premier $\mathfrak{p}$ de $\mathcal{O}_k$ sera noté $T_{\mathfrak{p}}(F)$. Soit $\mathfrak{m}$ un idéal de $\mathcal{O}_k$. Alors nous noterons $k_{\mathfrak{m}}$ le corps de rayon de k modulo $\mathfrak{m}$. On notera $N(\mathfrak{m})$ (resp. $e_{\mathfrak{m}}$) le cardinal de l'idéal $\mathcal{O}_k/\mathfrak{m}$ (resp. $\mathbf{Z}/\mathbf{Z}\cap\mathfrak{m}$). Le nombre de racines de l'unité de k qui sont équivalents à 1 modulo $\mathfrak{m}$ sera noté $r_{\mathfrak{m}}$. Si X est un ensemble fini alors nous noterons aussi bien $\#X$ ou $|X|$ son cardinal.

2. Le groupe des unités elliptiques de Kubert-Lang

Dans ce qui suit nous allons introduire et étudier un groupe d'unités elliptiques de F que nous noterons Ω_F. Bien que légèrement distinct du groupe introduit par D. Kubert et S. Lang dans [3], page 314 nous l'appelons groupe de Kubert-Lang puisque c'est cette référence qui nous a inspiré pour définir Ω_F.

2.1. Le groupe Ω_F

Comme ingrédient important nous utiliserons les quotients de discriminants. Rappelons que le discriminant d'un réseau L de $\mathbf{C}$ est

$$\Delta(L) = g_2(L)^3 - 27g_3(L)^2,$$

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 $\wp'(z,L)$. Il est facile de vérifier que pour tout $\lambda \in \mathbf{C}^\times$ on a $\Delta(\lambda L) = \lambda^{-12}\Delta(L)$. La théorie de la multiplication complexe permet de montrer que pour tout idéal fractionnaire $\mathfrak{a}$ de k le quotient

$$\frac{\Delta(\mathcal{O}_k)}{\Delta(\mathfrak{a})} \in H, \tag{2.1}$$

et engendre l'idéal $\mathfrak{a}^{12}\mathcal{O}_H$. De plus, si $\tau \in \mathrm{Gal}(H/k)$ alors on a

$$\Big(\frac{\Delta(\mathcal{O}_k)}{\Delta(\mathfrak{a})}\Big)^{\tau} = \frac{\Delta(\mathfrak{b})}{\Delta(\mathfrak{a}\mathfrak{b})},$$

où $\mathfrak{b}$ est un idéal fractionnaire quelconque de k satisfaisant $(\mathfrak{b}, H/k) = \tau^{-1}$. Remarquons qu'étant donnés $\sigma \in \mathrm{Gal}(H/k)$, $\mathfrak{a}$ idéal fractionnaire de k et $x \in k$ tels que $(\mathfrak{a}, H/k) = \sigma^{-1}$ et $\mathfrak{a}^h = x\mathcal{O}_k$, alors le nombre

$$\varphi_{(1)}(\sigma) = x^{12}\Delta(\mathfrak{a})^h,$$

ne dépend que de σ. Ces invariants nous serviront plus loin. Quant aux invariants de Ramachandra, leur construction nécessite l'introduction, pour tout réseau L de $\mathbf{C}$, de la fonction $\sigma(z, L)$ de Weierstrass ainsi que la fonction $\mathfrak{f}(z, L)$ de Klein. Par définition

$$\sigma(z, L) = z \prod_{\omega \in L} (1 - \frac{z}{\omega}) e^{\frac{z}{\omega} + \frac{1}{2}(\frac{z}{\omega})^2}.$$

On obtient ainsi une fonction holomorphe sur $\mathbf{C}$, avec des zéros simples aux points du réseau L. De plus, pour tout $\lambda \in \mathbf{C}^\times$ on a $\sigma(\lambda z, \lambda L) = \lambda\sigma(z, L)$. Sa dérivée logarithmique $\zeta(z, L)$ est appelée fonction zeta de Weierstrass. Elle est égale à la somme infinie

$$\zeta(z, L) = \frac{d\log(\sigma(z, L))}{dz} = \frac{1}{z} + \sum_{\omega \in L} (\frac{1}{z - \omega} + \frac{1}{\omega} + \frac{z}{\omega^2})$$

qui converge absolument et uniformément sur tout compact de $\mathbf{C} - L$, définissant ainsi une fonction méromorphe sur $\mathbf{C}$. Ses pôles forment l'ensemble L et sont tous simples. On a aussi la relation

$$\frac{d\zeta(z, L)}{dz} = -\wp(z, L).$$

Comme $\wp(z, L)$ est elliptique de réseau L, il exist un homomorphisme de groupes $\eta(., L) : L \longrightarrow \mathbf{C}$, tel que on a

$$\eta(\omega, L) = \zeta(z + \omega, L) - \zeta(z, L),$$

pour tout $\omega \in L$ et tout $z \in \mathbf{C} - L$. D'où l'on peut déduire l'identité

$$\sigma(z + \omega, L) = \psi(\omega) e^{\eta(\omega, L)(z + \frac{1}{2}\omega)} \sigma(z, L),$$

où $\psi(\omega) = 1$ si $\omega \in 2L$ et $\psi(\omega) = -1$ sinon. Prolongeons $\eta(., L)$ au corps $\mathbf{C}$ de manière à obtenir une application $\mathbf{R}$-linéaire de $\mathbf{C}$ dans lui-même, et considérons ensuite la fonction

$$\mathfrak{f}(z, L) = e^{-\eta(z, L)z/2} \sigma(z, L). \tag{2.2}$$

De ce qui précède on peut déduire la loi de transformation de la fonction de Klein, c'est à dire, pour tout $\omega \in L$ et tout $z \in \mathbf{C} - L$ on a

$$\mathfrak{f}(z+\omega, L) = \psi(\omega) e(Im(z\bar{\omega}/2M(L)))\mathfrak{f}(z, L),$$

où $e(x) = e^{2\pi i x}$ et $M(L)$ est la mesure du tore $\mathbf{C}/L$. Si (ω_1, ω_2) est une base de L alors $M(L) = |Im(\omega_1\bar{\omega_2})|$. Enfin, considérons la fonction $\varphi(z, L)$ définie de la façon suivante

$$\varphi(z, L) = \mathfrak{f}(z, L)^{12}\Delta(L). \tag{2.3}$$

Vue ce qui précède on a la propriété d'homogénéité $\varphi(\lambda z, \lambda L) = \varphi(z, L)$. Soit $\mathfrak{m} \neq (1)$ un idéal propre de $\mathcal{O}_k$. Soient $\sigma \in \mathrm{Gal}(k_\mathfrak{m}/k)$ et $\mathfrak{a}$ un idéal de $\mathcal{O}_k$ premier à $\mathfrak{m}$, tels que $\sigma = (\mathfrak{a}, k_\mathfrak{m}/k)$ alors le nombre

$$\varphi_\mathfrak{m}(\sigma) = \varphi(1, \mathfrak{a}^{-1}\mathfrak{m})^{e_\mathfrak{m}}$$

est non nul et ne dépend que de σ. On l'appelle l'invariant de Ramachandra. Grâce à la théorie de la multiplication complexe on peut montrer que

$$\varphi_\mathfrak{m}(\sigma) \in \mathcal{O}_{k_\mathfrak{m}} \quad \text{et} \quad \varphi_\mathfrak{m}(\sigma)^{\sigma'} = \varphi_\mathfrak{m}(\sigma\sigma'),$$

pour tous $\sigma, \sigma' \in \mathrm{Gal}(k_\mathfrak{m}/k)$. Dans [9], G. Robert montre que les fonctions $\varphi(z, L)$ vérifient des relations de distribution très remarquables puis en déduit, grâce notamment aux propriétés énumérées ci-dessus, les formules de norme suivantes. Soit $\mathfrak{q}$ un idéal premier de $\mathcal{O}_k$. Alors on a

$$N_{k_{\mathfrak{m}\mathfrak{q}}/k_\mathfrak{m}}(\varphi_{\mathfrak{m}\mathfrak{q}}(1))^{\frac{r_\mathfrak{m}}{r_{\mathfrak{m}\mathfrak{q}}}} = \begin{cases} \varphi_\mathfrak{m}(1)^{\frac{e_{\mathfrak{m}\mathfrak{q}}}{e_\mathfrak{m}}}, & \text{si } \mathfrak{q}|\mathfrak{m} \\ [\varphi_\mathfrak{m}(1)]^{\frac{e_{\mathfrak{m}\mathfrak{q}}}{e_\mathfrak{m}}(1-(\mathfrak{q}, k_\mathfrak{m}/k)^{-1})}, & \text{si } \mathfrak{q} \nmid \mathfrak{m} \text{ et } \mathfrak{m} \neq (1) \\ \Big(\dfrac{\Delta(\mathcal{O}_k)}{\Delta(\mathfrak{q})}\Big)^{e_\mathfrak{q}}, & \text{si } \mathfrak{m} = (1). \end{cases} \tag{2.4}$$

Vu que les invariants de Ramachandra sont des entiers algébriques les formules de normes ci-dessus permettent de déduire 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 $\mathcal{O}_k$, alors

$$\varphi_\mathfrak{m}(1)\mathcal{O}_{k_\mathfrak{m}} = \mathfrak{q}_\mathfrak{m}^u, \tag{2.5}$$

où $\mathfrak{q}_\mathfrak{m}$ est le produit des idéaux premiers de $k_\mathfrak{m}$ qui divisent $\mathfrak{q}$ et $u := \frac{12}{w_k} r_\mathfrak{m} e_\mathfrak{m}$.

Les deux formules limites de Kronecker peuvent s'énoncer comme suit. Posons $h_{\mathfrak{m}} = h$ si $\mathfrak{m} = (1)$ et $h_{\mathfrak{m}} = 1$ sinon. Soit χ un caractère complexe non trivial de $\mathrm{Gal}(k_{\mathfrak{m}}/k)$. Alors on a

$$L'(0,\chi) = -\frac{1}{12 r_{\mathfrak{m}} e_{\mathfrak{m}} h_{\mathfrak{m}}} \sum_{\sigma \in G_{\mathfrak{m}}} \chi(\sigma) \log(|\varphi_{\mathfrak{m}}(\sigma)|^2), \tag{2.6}$$

où $G_{\mathfrak{m}} = \mathrm{Gal}(k_{\mathfrak{m}}/k)$ et $s \longmapsto L(s,\chi)$ est la fonction L associée à χ, définie pour les nombres complexes s tels que $Re(s) > 1$, par le produit Eulérien

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

où $\mathfrak{l}$ désigne tous les idéaux premiers de $\mathcal{O}_k$ qui ne divisent pas $\mathfrak{m}$. cf. [2].

Soit $\mathfrak{f}$ le conducteur de l'extension F/k. Si $\mathfrak{f} \neq (1)$ alors pour tout idéal $\mathfrak{g} \neq (1)$ de $\mathcal{O}_k$ qui divise $\mathfrak{f}$ on pose

$$\varphi_{F,\mathfrak{g}} = N_{k_{\mathfrak{g}}/k_{\mathfrak{g}} \cap F}(\varphi_{\mathfrak{g}}(1))^{e(\mathfrak{f},\mathfrak{g})}, \quad e(\mathfrak{f},\mathfrak{g}) = \frac{w_k e_{\mathfrak{f}}}{r_{\mathfrak{g}} e_{\mathfrak{g}}}. \tag{2.7}$$

Définition 2.1. Nous noterons Q le sous-groupe de $H^\times$ engendré par tous les quotients

$$\frac{\Delta(\mathfrak{a})}{\Delta(\mathfrak{b})},$$

où $\mathfrak{a}$ et $\mathfrak{b}$ désignent deux idéaux fractionnaires quelconques de k.

Définition 2.2. Posons $Q_F = N_{H/H\cap F}(Q)^{e_{\mathfrak{f}}}$. Alors, le sous-module galoisien de $F^\times$ engendré par μ_F, Q_F et par tous les $\varphi_{F,\mathfrak{g}}$ ($\mathfrak{g}|\mathfrak{f}$ et $\mathfrak{g} \neq (1)$) sera noté $\mathcal{P}_F$. De plus on posera

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

2.2. **L'indice** $[\mathcal{O}_F^\times : \Omega_F]$

Afin d'aller plus loin nous devons décrire l'image de $\mathcal{P}_F$ par l'application logarithme $l_F : F^\times \longrightarrow \mathbf{R}[G_F]$, où $\mathbf{R}[G_F]$ est l'anneau de groupe de G_F sur le corps des nombres réels, définie pour $x \in F^\times$ par

$$l_F(x) = -\sum_{\sigma \in G_F} \log(|x^\sigma|^2)\sigma^{-1}.$$

L'application l_F est un G_F-homomorphisme vérifiant $\ker l_F \cap \mathcal{O}_F^\times = \mu_F$.

Associons à tout caractère complexe χ de G_F l'idempotent

$$e_\chi = \frac{1}{|G_F|} \sum_{\sigma \in G_F} \chi(\sigma)\sigma^{-1} \in \mathbf{C}[G_F].$$

Soient $\mathfrak{f}_\chi$ le conducteur de χ, et $\chi_{\rm pr}$ le caractère primitif de $\mathrm{Gal}(k_{\mathfrak{f}_\chi}/k)$ déterminé par χ. Si χ est non trivial alors la fonction $L(s, \chi_{\rm pr})$ admet un prolongement analytique à tout le plan complexe, avec 0 comme zéro simple, cf. [16] Proposition 3.4, page 24. On posera

$$\omega_F = 12 w_k e_{\mathfrak{f}} \sum_{\chi \neq \chi_0} L'(0, \bar{\chi}_{\rm pr}) e_\chi \in \mathbf{R}[G_F] \quad \text{et} \quad l_F^* = (1 - e_{\chi_0}) l_F,$$

où χ_0 est le caractère trivial de G_F. Posons $R_F = \mathbf{Z}[G_F]$. Nous allons introduire maintenant un certain R_F-sous-module U_F de $\mathbf{Q}[G_F]$. Celui-ci est intimement lié au groupe $\mathcal{P}_F$. Son étude est un point clef de toutes nos investigations sur les unités elliptiques. Mais fixons d'abord quelques notations. Si D est un sous-groupe de G_F alors on pose

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

Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_k$. Alors on pose

$$(\mathfrak{p}, F) = F_{\mathfrak{p}}^{-1} \frac{s(T_{\mathfrak{p}}(F))}{\# T_{\mathfrak{p}}(F)},$$

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

Définition 2.3. Soit $\mathfrak{s}$ un diviseur de $\hat{\mathfrak{f}}$. Si $\mathfrak{s} \neq (1)$ alors on note $U_{\mathfrak{s}}$ ou $U_{\mathfrak{s},F}$ le R_F-sous-module de $\mathbf{Q}[G_F]$ engendré par les éléments

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

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

Le lien entre les différents objets que nous venons d'introduire est donné par la proposition suivante où pour tout R_F-module M on a noté M_0 le noyau dans M de la multiplication par $s(G_F)$

Proposition 2.4. *On a* $l_F^*(\mathcal{P}_F) = \omega_F U_0$.

Démonstration. Il est possible de montrer un résultat plus précis. En effet, soient $\mathfrak{u}$ et $\mathfrak{v}$ deux diviseurs de $\mathfrak{f}$ premiers entre eux et tels que $\mathfrak{uv} = \mathfrak{f}$. Si $\mathfrak{u} \neq (1)$ alors on a

$$l_F^*(\varphi_{F,\mathfrak{u}}) = \omega_F \alpha(\hat{\mathfrak{v}}, \hat{\mathfrak{f}}).$$

En effet, cela revient à vérifier l'identité

$$l_F^*(\varphi_{F,\mathfrak{u}}) e_\chi = \omega_F \alpha(\hat{\mathfrak{v}}, \hat{\mathfrak{f}}) e_\chi, \tag{2.8}$$

pour tout caractère complexe de G_F. Ceci est évident pour le caractère trivial χ_0. Supposons $\chi \neq \chi_0$. Si χ n'est pas trivial sur $T_{\mathfrak{v}}(F) = \mathrm{Gal}(F/F \cap k_{\mathfrak{u}})$ alors on a nécessairement $l_F^*(\varphi_{F,\mathfrak{u}}) e_\chi = \omega_F \alpha(\hat{\mathfrak{v}}, \hat{\mathfrak{f}}) e_\chi = 0$. Si χ est trivial sur ce groupe alors on peut voir χ comme caractère de $\mathrm{Gal}(k_{\mathfrak{u}}/k)$. D'après (2.6) on a

$$l_F^*(\varphi_{F,\mathfrak{u}}) e_\chi = 12 w_k e_{\mathfrak{f}} L'(0, \bar{\chi})[F : F \cap k_{\mathfrak{u}}] e_\chi.$$

Or par définition on a

$$\omega_F \alpha(\hat{\mathfrak{v}}, \hat{\mathfrak{f}}) e_\chi = 12 w_k e_{\mathfrak{f}} L'(0, \bar{\chi}_{\mathrm{pr}})[F : F \cap k_{\mathfrak{u}}] \prod_{\mathfrak{p}|\mathfrak{u}} (1 - \bar{\chi}_{\mathrm{pr}}(\mathfrak{p})) e_\chi.$$

L'égalité (2.8) découle maintenant de la relation

$$L'(0, \bar{\chi}) = \prod_{\mathfrak{p}|\mathfrak{u}} (1 - \bar{\chi}_{\mathrm{pr}}(\mathfrak{p})) L'(0, \bar{\chi}_{\mathrm{pr}}).$$

De même on vérifie l'identité

$$l_F^*(N_{H/F\cap H}(\frac{\Delta(\mathfrak{a})}{\Delta(\mathcal{O}_k)}))^{e_{\mathfrak{f}}} = \omega_F \alpha(\hat{\mathfrak{f}}, \hat{\mathfrak{f}})(\tau_{\mathfrak{a}} - 1) = \omega_F s(\mathrm{Gal}(F/F \cap H))(\tau_{\mathfrak{a}} - 1), \tag{2.9}$$

où $\mathfrak{a}$ est un idéal fractionnaire de k et $\tau_{\mathfrak{a}}$ est un prolongement quelconque de $(\mathfrak{a}, H/k)$ à F. Et ceci complète la preuve de la proposition. □

Notre formule d'indice pour le groupe Ω_F fait intervenir la notion d'indice généralisé de Sinnott que nous allons rappeler ci-dessous. Soit ℓ un nombre premier et soit v_ℓ la valuation normalisée associée à ℓ ($v_\ell(\ell) = 1$). Soit $\mathbf{F}$ un corps choisi parmi $\mathbf{Q}$, $\mathbf{Q}_\ell$ ou $\mathbf{R}$. Posons $\mathfrak{o} = \mathbf{Z}$ si $\mathbf{F}$ est égal à $\mathbf{Q}$ ou $\mathbf{R}$ et $\mathfrak{o} = \mathbf{Z}_\ell$ si $\mathbf{F} = \mathbf{Q}_\ell$. Soit E un $\mathbf{F}$-espace vectoriel de dimension finie d. Rappelons qu'un réseau Λ de E est un sous-$\mathfrak{o}$-module libre de E, de rang d et tel que le $\mathbf{F}$-espace vectoriel engendré par Λ est égal à E. Étant donné deux réseaux M et N de E, on définit l'indice

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

où γ est un endomorphisme du $\mathbf{F}$-espace vectoriel E tel que $\gamma(M) = N$. Nous renvoyons le lecteur à [14] où sont démontrées les propriétés les plus remarquables de cette notion. Ici on est concerné par les R_F-modules $U_{\mathfrak{s},F}$. On peut montrer, exactement comme dans [14] Lemma 5.1, que $U_{\mathfrak{s},F}$ est un réseau de $\mathbf{Q}[G_F]$. 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 $(U_{\mathfrak{s},F} : U_{\mathfrak{sq},F})$, qui est donc bien défini, est un entier dont l'ensemble des diviseurs premiers est inclus dans celui de $\#T_{\mathfrak{q}}(F)$. Ainsi, si on note $\mathfrak{s}_0, \ldots, \mathfrak{s}_t$ les idéaux définis par les relations $\mathfrak{s}_0 = (1)$ et $\mathfrak{s}_{i+1} = \mathfrak{s}_i\mathfrak{p}_{i+1}$, où $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ sont les idéaux premiers qui divisent $\mathfrak{f}$, alors la décomposition

$$(R_F : U_F) = \prod_{i=0}^{t-1} (U_{\mathfrak{s}_i,F} : U_{\mathfrak{s}_{i+1},F})$$

de $(R_F : U_F)$ comme produit des indices $(U_{\mathfrak{s}_i,F} : U_{\mathfrak{s}_{i+1},F})$ montre que $(R_F : U_F) \in \mathbf{N}$. De plus, si ℓ est un nombre premier tel que $\ell | (R_F : U_F)$ alors ℓ divise $\#\mathrm{Gal}(F/F \cap H)$. Nous reviendrons plus loin sur l'indice $(R_F : U_F)$ pour étudier son comportement dans des $\mathbf{Z}_p$-extensions.

Proposition 2.5. *U_0 et $\omega_F U_0$ sont des réseaux de $\mathbf{R}[G_F]_0$. De plus, on a*

$$(U_0 : \omega_F U_0) = (12 w_K e_{\mathfrak{f}})^{[F:k]-1} \frac{w_k}{w_F} \frac{\mathrm{Reg}(F) h_F}{h}, \tag{2.10}$$

où h_F (resp. $\mathrm{Reg}(F)$*) est le nombre de classes d'idéaux (resp. le régulateur) de F.*

Démonstration. Il est clair que la multiplication par ω_F est un isomorphisme de $\mathbf{R}[G_F]_0$. Aussi suffit-il de prouver que U_0 est un réseau de $\mathbf{R}[G_F]_0$. En fait, il suffit de montrer que U_0 est un réseau de $\mathbf{Q}[G_F]_0$, ou encore, que son $\mathbf{Z}$-rang est égal à $[F : k] - 1$. Or U_0 est un R_F-module dont il est facile de vérifier que pour tout caractère complexe non trivial de G_F on a $U_0 e_\chi \neq 0$. Ce qui prouve que U_0 a le rang qu'il faut. De plus, on a

$$(U_0 : \omega_F U_0) = |\det \omega_F| = \prod_{\chi \neq \chi_0} \omega_F e_\chi.$$

Il suffit maintenant de revenir à la définition de ω_F et d'utiliser la formule analytique pour le nombre de classes, c'est à dire

$$\frac{h_F \mathrm{Reg}(F)}{w_F} = \frac{h}{w_K} \prod_{\chi \neq 1} L'(0, \chi_{\mathrm{pr}}).$$

□

Définition 2.6. Nous posons $d(F) = [\mathcal{P}_F^{w_F} \cap k : Q_F^{w_F} \cap k]$, et pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_k$ nous noterons $k_{\mathfrak{p}^\infty}$ l'extension abélienne maximale de k non ramifiée en dehors de $\mathfrak{p}$.

Théorème 2.7. *On a l'identité*

$$d(F)[l_F^*(\mathcal{P}_F) : l_F(\Omega_F)] = [F \cap H : k] \prod_{\mathfrak{p}} [F \cap k_{\mathfrak{p}^\infty} : F \cap H], \qquad (2.11)$$

où $\mathfrak{p}$ décrit l'ensemble des idéaux premiers de $\mathcal{O}_k$. De plus, si $H \subset F$ ou $F \subset H$ alors $d(F) = 1$

Démonstration. Posons $P' = \mathcal{P}_F^{w_F}$ et $\Omega' = \Omega_F^{w_F}$. Alors on a l'égalié des indices $[l_F^*(\mathcal{P}_F) : l_F^*(\Omega_F)] = [l_F^*(P') : l_F^*(\Omega')]$. Posons aussi $Q' = Q_F^{w_F}$ et $\Delta' = Q' \cap \mathcal{O}_F^\times$. On a

$$Q' \cap \ker l_F^* = Q' \cap k \quad \text{et} \quad P' \cap \ker l_F^* = P' \cap k.$$

En conséquence on obtient le diagramme commutatif suivant

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & Q' \cap k & \longrightarrow & Q'/\Delta' & \xrightarrow{l_F^*} & l_F^*(Q')/l_F^*(\Delta') & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & P' \cap k & \longrightarrow & P'/\Omega' & \xrightarrow{l_F^*} & l_F^*(P')/l_F^*(\Omega') & \longrightarrow & 1
\end{array}$$

dont les lignes et les colonnes sont exactes. Les colonnes correspondent à l'inclusion. Le lemme du serpent nous donne alors

$$\frac{[l_F^*(P') : l_F^*(\Omega')]}{[l_F^*(Q') : l_F^*(\Delta')]} = \frac{[P'/\Omega' : Q'/\Delta']}{[P' \cap k : Q' \cap k]}.$$

Posons $s(F/F \cap H) = s(\mathrm{Gal}(F/F \cap H))$. D'après (2.9) on a

$$l_F^*(Q') = \omega_F s(F/F \cap H)(R_F)_0 \quad \text{et} \quad l_F^*(\Delta') = \omega_F s(F/F \cap H)(R_F)_0^2],$$

d'où l'on déduit

$$[l_F^*(Q') : l_F^*(\Delta')] = [F \cap H : k]$$

Calculons $[P'/\Omega' : Q'/\Delta']$. Nous pouvons supposer $\mathfrak{f} \neq (1)$. Soient alors $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ les idéaux premiers de $\mathcal{O}_k$ qui divisent $\mathfrak{f}$, et fixons $\mathfrak{p}_1', \ldots, \mathfrak{p}_t'$ des idéaux premiers de $\mathcal{O}_F$ choisis de sorte que $\mathfrak{p}_i \subset \mathfrak{p}_i'$. Alors, on obtient

un homomorphisme de groupes abéliens $v_F : F^\times \longrightarrow \mathbf{Z}^t$, qui à x associe $v_F(x) = (v_1(x), \ldots, v_t(x))$, où v_i est la valuation normalisée associée à $\mathfrak{p}'_i$. D'après (2.5) on a

$$v_F(P') = 12e_\mathfrak{f} w_F[H : F \cap H](e(F/F \cap k_{\mathfrak{p}_1^{e_1}})\mathbf{Z}, \ldots, e(F/F \cap k_{\mathfrak{p}_t^{e_t}})\mathbf{Z}),$$

où $\mathfrak{p}_i^{e_i}$ est l'exacte puissance de $\mathfrak{p}_i$ qui divise $\mathfrak{f}$ et $e(F/F \cap k_{\mathfrak{p}_i^{e_i}})$ est l'indice de ramification en $\mathfrak{p}_i$ dans $F/F \cap k_{\mathfrak{p}_i^{e_i}}$. De même on a

$$v_F(Q') = 12e_\mathfrak{f} w_F[H : F \cap H](\#T_{\mathfrak{p}_1}(F)\mathbf{Z}, \ldots, \#T_{\mathfrak{p}_t}(F)\mathbf{Z}).$$

De plus, comme on a $P' \cap v_F^{-1}(Q') = \Omega' Q'$ on obtient

$$[P'/\Omega' : Q'/\Delta'] = \prod_{i=1}^{t} [F \cap k_{\mathfrak{p}_i^{e_i}} : F \cap H].$$

Ce qui complète la preuve de la première partie du Théorème. D'autre part si $F \subset H$ alors $P' = Q'$ et dans ce cas on a bien sûr $d(F) = 1$. Supposons que $H \subset F$. Soit $x \in \mathcal{P}_F$. On peut montrer (cette vérification est laissée au lecteur) qu'il existe une extension abélienne finie M de k, $y \in M$ et $\alpha \in k$ tels que

$$x = \alpha^{12e_\mathfrak{f}} y^{12w_k e_\mathfrak{f}}.$$

Si de plus on a $x^{w_F} \in k$ alors on sait d'après Lemma 6 de [15] que

$$y^{12w_k w_F e_\mathfrak{f}} = \zeta z^{12w_F e_\mathfrak{f}}, \quad \text{avec} \quad \zeta \in \mu_k \quad \text{et} \quad z \in k.$$

Remarquons que $\zeta \in \mu_k \cap F^{w_F} = \{1\}$. D'où $x^{w_F} \in (k^\times)^{12w_F e_\mathfrak{f}} \subset Q'$. Le théorème est maintenant entièrement démontré. □

Nous arrivons maintenant au résultat principal de ce paragraphe

Théorème 2.8. *On a*

$$[\mathcal{O}_F^\times : \Omega_F] = \frac{(12w_k e_\mathfrak{f})^{[F:k]-1}}{\frac{w_F}{w_k}} \frac{h_F}{[H : H \cap F]} \frac{\prod_\mathfrak{p}[F \cap k_{\mathfrak{p}^\infty} : F \cap H]}{[F : F \cap H]} \frac{(R_F : U_F)}{d(F)}.$$

De plus, si $H \subset F$ ou $F \subset H$ alors $d(F) = 1$.

Démonstration. Comme $\ker l_F \cap \mathcal{O}_F^\times = \mu_F$ on a $[\mathcal{O}_F^\times : \Omega_F] = [l_F(\mathcal{O}_F^\times) : l_F(\Omega_F)]$. Posons $R = R_F$ et $U = U_F$. On a

$$[l_F(\mathcal{O}_F^\times) : l_F(\Omega_F)] = \frac{(R_0 : U_0)}{(R_0 : l_F^*(\mathcal{O}_F^\times))}(U_0 : l_F^*(P_F))(l_F^*(P_F) : l_F(\Omega_F)).$$

Il n'est pas difficile de vérifier l'identité $(R_0 : l_F(\mathcal{O}_F^\times)) = \mathrm{Reg}(F)$. De plus, les indices $(U_0 : l_F^*(P_F))$ et $(l_F^*(P_F) : l_F(\Omega_F))$ sont donnés par les formules (2.10) et (2.11). La formule d'indice pour $[\mathcal{O}_F^\times : \Omega_F]$ découle maintenant de l'égalité $(R : U) = [F : F \cap H](R_0 : U_0)$. Pour la deuxième partie du Théorème se reporter au Théorème 2.7. □

3. **Indice et $\mathbf{Z}_p$-extensions**

Dans ce paragraphe on suppose que $H \subset F$ et on s'intéresse au groupe des unités elliptiques de F défini par K. Rubin dans [13] § 1. Les éléments de ce groupe que nous noterons $\mathcal{C}_F$ 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 apparaîssent dans le récent travail de W. Bley où il étend en particulier les résultats de Rubin au cas presque général afin de les appliquer à la conjecture équivariante sur les nombres de Tamagawa, cf. [1].

Dans ce qui suit nous allons utiliser le Théorème 2.8 pour étudier le comportement du quotient $[\mathcal{O}_F^\times : \mathcal{C}_F]/h_F$ de $[\mathcal{O}_F^\times : \mathcal{C}_F]$ par h_F, dans les $\mathbf{Z}_p$-extensions. Mais nous devons d'abord rappeler la définition de $\mathcal{C}_F$.

3.1. **Le groupe $\mathcal{C}_F$**

La définition la plus élégante du groupe $\mathcal{C}_F$ utilise la famille de fonctions elliptiques $\Psi(\,.\,; L, L') : z \longmapsto \Psi(z; L, L')$ introduites par G.Robert dans [12] et [10], paramétrées par les couples de réseaux (L, L') de $\mathbf{C}$ 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. [12] et [11].

Soit $\mathfrak{m} \neq (1)$ un idéal de $\mathcal{O}_k$. 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, on a

$$\Psi(1; \mathfrak{m}, \mathfrak{a}^{-1}\mathfrak{m})^{12e_\mathfrak{m}} = \varphi_\mathfrak{m}(1)^{N(\mathfrak{a})-(\mathfrak{a}, k_\mathfrak{m}/k)}. \tag{3.1}$$

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

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

De plus on a

$$N_{k_\mathfrak{q}/H}(\Psi(1;\mathfrak{q},\mathfrak{a}^{-1}\mathfrak{q}))^{12\frac{w_k}{r_\mathfrak{q}}} = \Big(\frac{\Delta(\mathcal{O}_k)}{\Delta(\mathfrak{q})}\Big)^{N(\mathfrak{a})-(\mathfrak{a},H/k)}. \tag{3.2}$$

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

Définition 3.1. On note $\mathcal{C}_F$ le sous-groupe de $\mathcal{O}_F^\times$ engendré par tous les $\mathcal{C}_{F,\mathfrak{m}}$, $\mathfrak{m} \neq (1)$. On posera $V_F = \mu_F \mathcal{C}_F^{12w_k e_\mathfrak{f}}$, où $\mathfrak{f}$ est le conducteur de F.

Le théorème 2.8 du chapitre 2 peut être reformulé comme suit.

$$[\mathcal{O}_F^\times : \mathcal{C}_F] = h_F \frac{\prod_\mathfrak{p}[F\cap k_{\mathfrak{p}^\infty} : F\cap H]}{[F : F\cap H]} \frac{(R_F : U_F)}{d(F)} \frac{[\Omega_F : V_F]}{\frac{w_F}{w_k}}, \tag{3.3}$$

puisque $H \subset F$ et donc $d(F) = 1$. C'est cette formule d'indice que nous exploiterons pour étudier le comportement du quotient $[\mathcal{O}_F^\times : \mathcal{C}_F]/h_F$ dans les $\mathbf{Z}_p$-extensions. Pour la convenance du lecteur nous allons tout d'abord énoncer un résultat analogue au Theorem 5.2 de [14]. Il s'agit de la proposition 3.2 ci-dessous où nous noterons D (resp. Δ) le ℓ-Sylow (resp. le sous-groupe des éléments d'ordre premier à ℓ) de $\mathrm{Gal}(F/k)$, de sorte qu'on a la décomposition $\mathrm{Gal}(F/k) = \Delta \times D$.

Proposition 3.2. *Soient F' le corps fixe de Δ et χ un caractère de Δ. On peut voir χ comme caractère de $\mathrm{Gal}(F/k)$ trivial sur D. Notons alors $m(\chi)$ le produit des idéaux premiers $\mathfrak{q}$ de k qui se ramifient dans F' et tels que $\chi_{\mathrm{pr}}(\mathfrak{q}) = 1$. Alors la puissance exacte de ℓ qui divise $(R_F : U_F)$ est le produit*

$$\prod_\chi (\mathbf{Z}[\mathrm{Gal}(F'/k)] : U_{m(\chi),F'}) \tag{3.4}$$

où χ parcourt tous les caractères multiplicatifs de Δ.

Démonstration. Voir [7] Proposition 2.1. □

Dans toute la suite de ce paragraphe on fixera p un nombre premier et F_∞ une $\mathbf{Z}_p$-extension de F abélienne sur k. Si n est un entier naturel on notera F_n l'unique extension de F contenue dans F_∞ et de degré p^n sur F.

On notera aussi $\mathfrak{f}_n$ le conducteur de F_n. On sait qu'on peut décomposer $\mathfrak{f}_n$ de manière unique $\mathfrak{f}_n = \mathfrak{h}\mathfrak{g}_n$, 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_∞/F. Pour tous idéal premier $\mathfrak{p}$ et tout entien n on notera $T_\mathfrak{p}^{(n)}$ au lieu de $T_\mathfrak{p}(F_n)$ le groupe d'inertie en $\mathfrak{p}$ dans F_n/k. Notons S_{F,F_∞} l'ensemble des idéaux premiers de k qui divisent $\mathfrak{h}$, et pour tout $\mathfrak{q} \in S_{F,F_\infty}$ notons $D_\mathfrak{q}(F_\infty)$ le groupe de décomposition de $\mathfrak{q}$ dans F_∞/k. Nous dirons que F_∞ vérifie l'hypothèse de décomposition si les groupes $D_\mathfrak{q}(F_\infty)$, $\mathfrak{q} \in S_{F,F_\infty}$, sont tous infinis.

3.2. **La suite** $(R_{F_n} : U_{F_n})$

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

Proposition 3.3. *Supposons que F_∞ 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. La plus grande extension de k de degré une puissance de ℓ, contenue dans F_n ne dépend pas de n. Notons la F'. D'après la proposition 3.2 on doit considérer les indices $(\mathbf{Z}[\mathrm{Gal}(F'/k)] : U_{m(\chi),F'})$, où χ parcourt les caractères de $\mathrm{Gal}(F_n/F')$. Par hypothèse il existe n_0 tel que $\mathrm{Gal}(F_n/F_{n_0})$, 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 $m(\chi) \neq (1)$ alors χ est nécessairement trivial sur $\mathrm{Gal}(F_n/F_{n_0})$. D'où la formule

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

où χ parcourt tous les caractères de $\mathrm{Gal}(F_{n_0}/k)$. □

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

qui divise $\mathfrak{f}_n$ mais ne divise pas $\mathfrak{s}$ alors on a

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

Proposition 3.4. *Soient $\mathfrak{s}$ et $\mathfrak{s}'$ deux diviseurs de $\hat{\mathfrak{h}}$ tels que $\mathfrak{ss}' = \hat{\mathfrak{h}}$. Soit $\mathfrak{q}$ un idéal premier de $\mathcal{O}_k$ qui divise $\mathfrak{s}'$. Alors il existe $\mu \in \mathbf{N}$ et $\nu \in \mathbf{Z}$ tel que l'indice*

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

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

Démonstration. Posons

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

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

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

n'est autre que le sous R^∞-module de E engendré par les éléments de la forme

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

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

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

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

$$(U_{\mathfrak{s},p}^{(n)} : U_{\mathfrak{sq},p}^{(n)}) = \frac{[U_{\mathfrak{s},p}^{(n)} + U_{\mathfrak{sq},p}^{(n)} : U_{\mathfrak{sq},p}^{(n)}]}{[U_{\mathfrak{s},p}^{(n)} + U_{\mathfrak{sq},p}^{(n)} : U_{\mathfrak{s},p}^{(n)}]} = \frac{[A^{(n)} : C^{(n)}]}{[A^{(n)} : B^{(n)}]}, \tag{3.5}$$

où $A = U_{\mathfrak{s}}^{\infty} + U_{\mathfrak{sq}}^{\infty}$, $B = U_{\mathfrak{s}}^{\infty}$ et $C = U_{\mathfrak{sq}}^{\infty}$.
Nous dirons qu'un sous-Λ-module X de E est admissible s'il existe $u, v \in \mathbf{N}$ 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 $\mathbf{Q}_p[\mathrm{Gal}(F_n/k)]$. Si $Y \subset X$ sont deux sous- Λ-modules admissibles de E alors il est facile de voir que l'invariant λ de X/Y est nul. De plus il est possible d'exprimer l'ordre du groupe fini $X^{(n)}/Y^{(n)}$ au moyen de l'invariant μ de X/Y. En effet, d'après la théorie des Λ-modules il existe X' un Λ-module libre et un homomorphisme injectif $f : X \longrightarrow X'$ 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 puiqu'il est annulé à la fois par ω_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 $\mathbf{Z}_p$-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 ω_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 comme $f(X)/f(X_n) \simeq X/X_n \simeq X^{(n)}$ est un $\mathbf{Z}_p$-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 $\nu' \in \mathbf{Z}$ et $\mu' = \mu(X'/f(Y))$ est l'invariant du Λ-module $X'/f(Y)$. Pour déduire l'ordre de $X^{(n)}/Y^{(n)}$ il suffit de constater les isomorphismes

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

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

$$\#X^{(n)}/Y^{(n)} = p^{\mu_1 p^n + \nu_1}, \quad \text{pour tout } n \text{ assez grand,} \tag{3.6}$$

où $\nu_1 \in \mathbf{Z}$ et $\mu_1 = \mu(X/Y)$. Ainsi pour obtenir la formule pour $(U_{\mathfrak{s},p}^{(n)} : U_{\mathfrak{sq},p}^{(n)})$ il suffit d'appliquer (3.6) aux couples de modules (A, B) et (A, C). Les modules A, B et C étant ceux introduits ci-dessus. Ils sont évidemment admissibles. Il suffit ensuite d'utiliser (3.5). 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_∞/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

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

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

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

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^∞-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 $A^{\widetilde{T}_{\mathfrak{q}}}/C^{\widetilde{T}_{\mathfrak{q}}} \longrightarrow A^{\widetilde{T}_{\mathfrak{q}}}/B^{\widetilde{T}_{\mathfrak{q}}}$, 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_∞/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. □

Corollaire 3.5. *Soit $\mathfrak{s}$ un diviseur de $\hat{\mathfrak{h}}$. Alors il existe $\mu_{\mathfrak{s}} \in \mathbf{N}$ et $\nu_{\mathfrak{s}} \in \mathbf{Z}$ 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 $\mathfrak{q}_1, \ldots, \mathfrak{q}_d$ 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 3.4 permet de conclure. □

Proposition 3.6. *Posons $\mathfrak{a} = \hat{\mathfrak{h}}$ et soit $\mathfrak{b}$ le produit des idéaux premiers de k qui se ramifient dans F_∞/F. Soient $\mathfrak{s}$ un diviseur de $\mathfrak{b}$ et $\mathfrak{q}$ un idéal premier de k divisant $\mathfrak{b}$ mais tel que $\mathfrak{q} \nmid \mathfrak{s}$. Alors l'indice $(U_{\mathfrak{as},p}^{(n)} : U_{\mathfrak{asq},p}^{(n)})$ ne dépend pas de n pour tout n assez grand.*

Démonstration. Voir [7] Corollaire 3.4. □

Théorème 3.7. *Il existe $\mu_\infty \in \mathbf{N}$ et $\nu \in \mathbf{Z}$ tels que*

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

pour tout n assez grand. De plus si F_∞ 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 le corollaire 3.5 et la proposition 3.6. □

3.3. **La suite des indices** $[\Omega_{F_n} : V_{F_n}]$

Dans ce § nous étudions la suite $[\Omega_{F_n} : V_{F_n}]$. Par commodité nous supposerons que $H \subset F$. Posons $L_n = F_n \cap k_{\mathfrak{g}_n}$ et $L_\infty = \bigcup L_n$. On a $F_\infty = FL_\infty$, $F_n = FL_n$ et L_∞ est une $\mathbf{Z}_p$-extension de L_0 abélienne sur k. En particulier on a $\mathrm{Gal}(F_\infty/L_\infty) \simeq \mathrm{Gal}(F_n/L_n)$. 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 Ω_{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 reliants les éléments de $\mathcal{P}'_{L_n}$ sont celles issues des formules de norme (2.4). De manière formelle les choses se présentent comme suit. Soit $\mathcal{A}$ le groupe abélien libre de base la réunion disjointe

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

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

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

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

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

où $\mathfrak{g}, \mathfrak{g}' \in \Sigma_n$ sont premiers entre eux et tels que $\mathfrak{g}' \neq (1)$. De plus σ appartient à $\mathrm{Gal}(L_n \cap k_{\mathfrak{g}}/k)$ et $\sum_{\tau\longrightarrow\sigma} \tau$ désigne la somme des éléments de $\mathrm{Gal}(L_n \cap k_{\mathfrak{g}\mathfrak{g}'}/k)$ dont la restriction à $L_n \cap k_{\mathfrak{g}}$ est égal à σ. 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 $\mathbf{Z}$-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 $X_{\mathfrak{g}} \subset \mathrm{Gal}(L_n \cap k_{\mathfrak{g}}/k)$ tel que la restriction des automorphismes est une bijection de $X_{\mathfrak{g}}$ sur $\mathrm{Gal}(H/k)$. De plus, si $\mathfrak{g}_n = \mathfrak{p}^{i_n}\bar{\mathfrak{p}}^{j_n}$ alors pour tous $\sigma_1 \in \mathrm{Gal}(L_n \cap k_{\mathfrak{p}^{i_n}}/k)$ et tout $\sigma_2 \in \mathrm{Gal}(L_n \cap k_{\bar{\mathfrak{p}}^{j_n}}/k)$ tels que σ_1 et σ_2 coincident sur H on fixe $\gamma(\sigma_1, \sigma_2) \in \mathrm{Gal}(L_n/k)$ un automorphisme qui prolonge à la fois σ_1 et σ_2.

Posons alors

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

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

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

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

Proposition 3.8. *L'ensemble* $\Upsilon = \bigsqcup_{\mathfrak{g}\in\Sigma_n} \Upsilon_{\mathfrak{g}}$ *est une* $\mathbf{Z}$*-base de* $\mathcal{A}$*. En conséquence l'ensemble*

$$\bigsqcup_{\mathfrak{g}\in\Sigma_n} \mathrm{Gal}(L_n \cap k_{\mathfrak{g}}/k) - X_{\mathfrak{g}}$$

est une base de $\mathcal{A}/\mathcal{R}$*.*

Démonstration. Voir [7] Proposition 4.1. □

Notons $\mathcal{A}' \subset \mathcal{A}$ le noyau de l'homomorphisme $\deg : \mathcal{A} \longrightarrow \mathbf{Z}$ défini par $\deg(\sigma) = 0$ si $\sigma \in \mathrm{Gal}(L_n \cap k_{\mathfrak{g}}/k)$ avec $(1) \neq \mathfrak{g} \in \Sigma_n$ et $\deg(\sigma) = 1$ si $\sigma \in \mathrm{Gal}(H/k)$. 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 factoristation de $\mathcal{F}'$, un isomorphisme

$$\mathcal{A}'/\mathcal{R} \simeq \mathcal{P}'_{L_n}. \tag{3.7}$$

Lemme 3.9. *Il existe un entier* κ *tel que pour tout* n *le groupe* Ω_{L_n}/V_{L_n} *a au plus* κ *générateurs.*

Démonstration. Voir [7] Lemme 4.1 □ □

Définition 3.10. Pour toute extension abélienne finie K de k contenenant 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 ℓ parcourt tous les nombres premiers.

Proposition 3.11. *Soit ℓ 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 δ_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 $\mathbf{Z}$-linéaire $\Psi : \mathcal{A} \longrightarrow \mathbf{Z} \times Hom(\mu(L_n), \mu(L_n))$ définie pour un $\sigma \in \mathrm{Gal}(L_n \cap k_{\mathfrak{g}}/k)$ 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 $\Psi(\mathcal{R}) \subset \delta_n\mathbf{Z} \times \{0\}$. Ainsi grâce à l'isomorphisme (3.7) l' application Ψ induit de manière naturelle un homomorphisme de groupes abéliens

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

On a

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

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, on constate que le groupe $\ker(\rho_n)/V_{L_n}$ est annulé 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 3.9 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. □

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

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

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 $v_n = e_{\mathfrak{f}_n}/e_{\mathfrak{g}_n}$. D'autre part, comme on a aussi $(V_{L_n})^{v_n} \subset V_{F_n}$ l'application Φ_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 $\mathrm{Im}(\Phi'_n)$ et $\mathrm{coker}(\Phi'_n)$ nous permettra de conclure.

Définition 3.12. Pour tout nombre premier ℓ on note $\ell^{\pi_n(\ell)}$ l'ordre du ℓ-sous-groupe de Sylow de $\mathrm{Im}(\Phi'_n)$.

Proposition 3.13. *Soit ℓ un nombre premier. Il existe N un entier tel que la suite $(\pi_n(\ell))_{n\geq N}$ est croissante. 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. Supposons $\ell = p$, alors*

i) Si la suite $(w_{F_n})_n$ est bornée et $\mathfrak{g}_n$ est divisible par deux idéaux premiers, ou si $(w_{F_n})_n$ 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.

ii) Si $(w_{F_n})_n$ 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. Voir [7] Propositions 4.3, 4.4, 4.5 et 4.6. □

Proposition 3.14. *L'ordre du groupe* $\mathrm{coker}(\Phi'_n)$ *ne dépend pas de n pour tout n assez grand.*

Démonstration. voir [7] Proposition 4.8. □

Théorème 3.15. *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

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

et les propositions 3.13 et 3.14 montrent que pour tout nombre premier ℓ 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 3.11, que la suite $(r(F_n,\ell))_n$ est majorée. D'où le théorème. □

Nous arrivons maintenant à la conclusion de ce paragraphe 3.

Théorème 3.16. *Supposons $H \subset F$. Alors, il existe deux entiers $\mu_\infty \in \mathbf{N}$ et $\nu_\infty \in \mathbf{Z}$ 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. Supposons que F_∞ vérifie l'hypothèse de décomposition. Alors on a $\mu_\infty = 0$, de plus il existe $c_{F_\infty} \in \mathbf{Q}^\times$ tel que

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

pour tout entier n assez grand.

Démonstration. La première assertion découle de la formule (3.3), le Théorème 3.7 et le Théorème 3.15. Pour obtenir la deuxième partie du Théorème il faut aussi utiliser la Proposition 3.3. □

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, car alors le p-Sylow de $\mathrm{Gal}(F_n/k)$ est cyclic et cela permet de montrer que $p \nmid (R^{(n)} : U^{(n)})$. Il est aussi possible de montrer que $\mu_\infty = 0$ si au plus deux idéaux premiers $\mathfrak{q} \in S_{F,F_\infty}$ sont tels que $D_\mathfrak{q}(F_\infty)$ est fini. Dans un article à paraître, cf. [8], nous donnons, en revanche, des exemples où le μ_∞ est non nul pour la $\mathbf{Z}_p$-extension anticyclotomique.

Références

[1] W. Bley – « Equivariant Tamagawa number conjecture for abelian extensions of a quadratic imaginary field », *Doc. Math.* **11** (2006), p. 73–118(electronic).

[2] B. Gross et M. Rosen – « Fourier series and the special values of L-functions », *Adv. in Math.* **69** (1988), no. 1, p. 1–31.

[3] D. Kubert et S. Lang – *Modular units*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Science], vol. 244, Springer-Verlag, New York, 1981.

[4] H. Oukhaba – « Index formulas for ramified elliptic units », *Compositio Math.* **137** (2003), no. 1, p. 1–22.

[5] H. Oukhaba – « Sign functions of imaginary quadratic fields and applications », *Annales de l'Institut Fourier* **55** (2005), no. 3, p. 753–772.

[6] H. Oukhaba – « Sign functions and elliptic units », *Math. Annalen* **336** (2006), no. 3, p. 639–657.

[7] ———, « L'indice des unités elliptiques dans les $\mathbb{Z}_p$-extensions », *Bull. Soc. Math. France* **135** (2007), no. 1, p. 135–167.

[8] ———, « The index of elliptic units in $\mathbb{Z}_p$-extensions, II », à paraître dans Tohoku Math. Journal, 2008.

[9] G. Robert – *Unités elliptiques*, Société Mathématique de France, Paris, 1973, Bull. Soc. Math. France, Mém. No. 36, Tome 101.

[10] ———, « Concernant la relation de distribution satisfaite par la fonction φ associée à un réseau complexe », *Invent. Math.* **100** (1990), p. 231–257.

[11] ———, « Unités de stark et racine 12-ième canonique », Prépublication de l'institut Fourier n° 181, 1991.

[12] ———, « La racine 12-ième canonique $\Delta(L)^{[\underline{L}:\,L]}/\Delta(\underline{L})$ », Séminaire de Théorie des Nombres, Paris, 1989–90, Birkhäuser Boston, 1992, p. 209–232.

[13] K. Rubin – « The main conjectures of Iwasawa theory for imaginary quadratic fields », *Invent. Math.* **103** (1991), p. 25–68.

[14] W. Sinnott – « On the Stickelberger ideal and the circular units of an abelian field », *Invent. Math.* **62** (1980/81), no. 2, p. 181–234.

[15] H. M. Stark – « L-functions at $s = 1$. IV. First derivatives at $s = 0$ », *Adv. in Math.* **35** (1980), no. 3, p. 197–235.

[16] J. Tate – *Les conjectures de Stark sur les fonctions L d'Artin en s = 0*, Birkhäuser Boston Inc, 1984, Lecture notes edited by Dominique Bernardi and Norbert Schappacher.

Hassan Oukhaba
Laboratoire de Mathématique
Université de Franche-Comté
25030 Besançon cedex
France.
hassan.oukhaba@univ-fcomte.fr