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-

Bull. Soc. math. France
135 (2), 2007, p. 299–

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`

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

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

© Société Mathématique de France

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. $\mathrm{Cl}(F)_p$) 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 χ de $\mathrm{Gal}(F/k)$, les χ-composantes de $(\mathcal{O}_F^\times/\mathcal{C}_F)_p$ et $\mathrm{Cl}(F)_p$ 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 Ω_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_∞ 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_∞ 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_∞} l'ensemble des idéaux premiers de k ramifiés dans F mais pas dans F_∞/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_∞/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 μ_∞ est le μ-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 $\mathrm{Gal}(F_n/k)$ 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_∞ 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_∞/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 μ_∞ 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 $\mathfrak{f}$ (resp. $\mathfrak{f}_n$) 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 $\mathfrak{f} \neq (1)$ on notera $\mathfrak{p}_1, \ldots, \mathfrak{p}_e$ les idéaux premiers de k qui divisent $\mathfrak{f}$. 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 $\mathfrak{f}_n$ 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.

2. Les groupes $\mathcal{C}_F$ et Ω_F

Commençons par rappeler la définition du groupe $\mathcal{C}_F$. Pour cela nous utiliserons la famille de fonctions elliptiques $\Psi(\,.\,; L, L') : z \mapsto \Psi(z; L, L')$ 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

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

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

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

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

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

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

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

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

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

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

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

De plus on a

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

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

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