

ROLAND GILLARD

Unités elliptiques et unités de Minkowski

Séminaire de théorie des nombres de Grenoble, tome 7 (1978-1979), exp. n° 3, p. 1-7

http://www.numdam.org/item?id=STNG_1978-1979__7__A3_0

© Institut Fourier – Université de Grenoble, 1978-1979, tous droits réservés.

L'accès aux archives du séminaire de théorie des nombres de Grenoble implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

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

Grenoble

UNITES ELLIPTIQUES ET UNITES DE MINKOWSKI

par
Roland GILLARD

1. - PRESENTATION DES RESULTATS.

Soient k un corps quadratique imaginaire, p un nombre premier impair et K/k une extension cyclique de degré p . Soit $G = \text{Gal}(K/k)$. On note h_K (resp. h_k) le nombre de classes, E_K (resp. E_k) le groupe des unités de K (resp. de k), μ_K (resp. μ_k) son sous-groupe de torsion et w_K (resp. w_k) l'ordre de μ_K (resp. de μ_k). On plonge tous les corps considérés dans \mathbb{C} et pour tout entier m , on pose $\zeta_m = \exp(2\pi i/m)$.

THEOREME 1 (*). -

- a) h_K/h_k est norme d'un idéal de $\mathbb{Z}[\zeta_p]$.
- b) Pour que E_K/μ_K soit $\mathbb{Z}[G]$ -monogène, il suffit (resp. il faut) que tout (resp. au moins un) idéal de $\mathbb{Z}[\zeta_p]$, de norme $(h_K \cdot w_k)/(h_k \cdot w_K)$ soit principal.

Un théorème analogue a été établi par A. BRUMER [1], pour $k = \mathbb{Q}$; la méthode suivie ici s'inspire d'ailleurs de celle de [1]. Le résultat a) peut être établi directement et est connu dans un cadre général.

(*) Ceci répond à une question de J.J. PAYAN posée lors de la soutenance de thèse de N. MOSER.

La démonstration du théorème 1 est faite aux §2 et 3 . Au §4, on retrouve des résultats de N. MOSER, dans le cas où K/\mathbb{Q} est diédrale. Au §5, on étudie le cas où l'extension K est abélienne sur \mathbb{Q} . Si F est son sous-corps réel maximal, on compare la théorie pour K/k à celle pour F/\mathbb{Q} au moyen de [2] .

Enonçons tout de suite le lemme :

LEMME. - On a $w_K = w_k$, sauf si l'extension K/k est $\mathbb{Q}(\zeta_9)/\mathbb{Q}(\zeta_3)$ (on a alors $w_K = 3w_k$) ou $\mathbb{Q}(\zeta_\ell)/\mathbb{Q}(\sqrt{-\ell})$ (on a alors $w_K = \ell w_k$) avec $\ell = 2p+1$ et ℓ premier.

Démonstration. Si un nombre premier ℓ divise w_K/w_k , on a $\mathbb{Q}(\zeta_\ell) \subseteq K$, d'où $\ell = 3$ ou $2p+1$; le lemme en résulte aussitôt.

2. - CAS RAMIFIÉ.

Soient \mathfrak{f} le conducteur de K/k , f le plus petit entier rationnel > 0 contenu dans \mathfrak{f} et $e(\mathfrak{f})$ le nombre d'éléments de μ_k congrus à 1 modulo \mathfrak{f} . Désignons par I l'idéal d'augmentation de $\mathbb{Z}[G]$ et J l'annulateur du $\mathbb{Z}[G]$ -module μ_K . Posons

$$\varphi_K = \prod \varphi_{\mathfrak{f}}(C) ,$$

où $\varphi_{\mathfrak{f}}(C)$ est défini comme dans [6, §2.2] ; le produit est pris sur le noyau de l'application de réciprocity $Cl(\mathfrak{f}) \rightarrow G$, avec $Cl(\mathfrak{f})$ groupe des classes de rayon \mathfrak{f} de k . En étendant par multiplicativité l'action de G sur E_K , on définit φ_K^u pour $u \in \mathbb{Z}[G]$. Si u est dans $I \cap J$, φ_K^u est une puissance d'ordre $12fe(\mathfrak{f})$ dans E_K ; posons

$$\Omega_K = \{x \in E_K \mid x^{12fe(\mathfrak{f})} \in \varphi_K^{I \cap J}\} .$$

D'après [3] , on sait que $[E_K : \mu_K \Omega_K] = h_K/h_k$ et on voit que $[I : I \cap J] = w_K/w_k$. Considérons l'application $\mathbb{Q}[G] \rightarrow \mathbb{Q}[\zeta_p]$ définie en envoyant un générateur g de G sur ζ_p ; elle définit des isomorphismes

$$I \xrightarrow{\cong} (\zeta_p - 1)\mathbb{Z}[\zeta_p] \quad , \quad I \cap J \xrightarrow{\cong} (\zeta_p - 1) \cdot \mathfrak{g} \quad ,$$

avec \mathfrak{g} idéal entier de $\mathbb{Z}[\zeta_p]$, de norme w_K/w_k . On a donc aussi un isomorphisme

$$\mu_K \Omega_K / \mu_K \xrightarrow{\cong} (\zeta_p - 1) \cdot \mathfrak{g}$$

envoyant la classe de φ_K^{g-1} sur $12fe(\mathfrak{f}) \cdot (\zeta_p - 1)$. Cet isomorphisme se prolonge de façon unique en un isomorphisme

$$\tilde{\delta}_K : E_K / \mu_K \xrightarrow{\cong} \mathfrak{A}_K \quad ,$$

avec \mathfrak{A}_K idéal fractionnaire de $\mathbb{Z}[\zeta_p]$. Posons $\mathfrak{B}_K = (\zeta_p - 1) \cdot \mathfrak{A}_K^{-1}$; la norme de $\mathfrak{g} \cdot \mathfrak{B}_K$ est h_K/h_k , d'où la partie a) du théorème 1. La partie b) résulte de ce que E_K/μ_K est $\mathbb{Z}[G]$ -monogène si et seulement si \mathfrak{B}_K est principal et de ce que la norme de \mathfrak{B}_K est $(h_K w_k)/(h_k w_K)$.

3. - CAS NON RAMIFIÉ.

Désignons par I l'idéal d'augmentation de $\mathbb{Z}[G]$ et par J l'idéal $\{\sum n(s) \cdot s \in \mathbb{Z}[G] \mid \prod s^{n(s)} = 1\}$. Pour $s \in G$, posons

$$\delta_K(s) = \prod \delta(C)$$

où $\delta(C)$ est défini comme dans [6, §3.1]; le produit est pris sur toutes les classes absolues d'idéaux de k dont l'image par l'application de réciprocité est s . Prolongeons δ_K par multiplicativité à $\mathbb{Z}[G]$. Pour $u \in I \cap J$, $\delta_K(u)$ est une puissance d'ordre $h_k \cdot w_k$ dans E_K ; posons

$$\Omega_K = \{x \in E_K \mid x^{h_k \cdot w_k} \in \delta_K(I \cap J)\} \quad .$$

D'après [6, §3], on sait que $[E_K : \mu_K \Omega_K] = 12^{p-1} \cdot p \cdot (h_K/h_k) \cdot (w_k/w_K)$ et que $[I : I \cap J] = p$. D'après le lemme du §1, on a ici $w_k = w_K$. Pour g générateur de G , considérons l'application de $\mathbb{Q}[G]$ dans $\mathbb{Q}(\zeta_p)$ qui envoie g sur ζ_p . Elle définit des isomorphismes

$$I \rightarrow (\zeta_p - 1) \cdot \mathbb{Z}[\zeta_p] \quad , \quad I \cap J \rightarrow (\zeta_p - 1)^2 \cdot \mathbb{Z}[\zeta_p] \quad .$$

On a donc aussi un isomorphisme

$$\mu_K \Omega_K / \mu_K \rightarrow (\zeta_p - 1)^2 \mathbb{Z}[\zeta_p] ,$$

envoyant la classe de $\delta_K(g^2 - 2g + 1)$ sur $h_k \cdot w_k \cdot (\zeta_p - 1)^2$. Cet isomorphisme se prolonge de façon unique en un isomorphisme

$\mathfrak{F}_K : E_K / \mu_K \rightarrow \mathfrak{A}_K$, avec \mathfrak{A}_K idéal fractionnaire de $\mathbb{Z}(\zeta_p)$. Posons $\mathfrak{B}_K = (\zeta_p - 1) \cdot (12\mathfrak{A}_K)^{-1}$. Ainsi, h_K / h_k est la norme de \mathfrak{B}_K ; de plus \mathfrak{B}_K est principal si et seulement si E_K / μ_K est $\mathbb{Z}[G]$ -monogène, d'où le théorème 1 dans le cas non ramifié.

4. - CAS DIÉDRAL.

Supposons de plus que K soit une extension diédrale de \mathbb{Q} . Notons t la conjugaison complexe. Si K/k est ramifiée, avec les notations du §2, on a $t \cdot f = f$ et $t \cdot \varphi_{\mathfrak{f}}(C) = \varphi_{\mathfrak{f}}(t \cdot C)$ si $C \in \text{Cl}(\mathfrak{f})$; on voit alors que $t \cdot \varphi_K = \varphi_K$, d'où

$$t \cdot \varphi_K^s = (ts) \cdot \varphi_K = (s^{-1} \cdot t) \cdot \varphi_K = \varphi_K^{s^{-1}} .$$

De même dans le cas non ramifié, on a $t \cdot \delta(C) = \delta(t \cdot C)$ pour C classe absolue d'idéaux d'où pour $s \in G$

$$t(\delta_K(s)) = \delta_K(s^{-1}) .$$

Ceci prouve que les isomorphismes \mathfrak{F}_K des §2 et 3 sont compatibles avec l'action de t sur E_K et $\mathbb{Q}(\zeta_p)$. Ainsi \mathfrak{A}_K est un idéal de $\mathbb{Q}(\zeta_p)$ invariant par t . En identifiant la multiplication par un générateur fixé g de G à celle par ζ_p , on munit $\mathbb{Q}(\zeta_p)$ et ses idéaux fractionnaires d'une action de $\mathbb{Z}(\text{Gal}(K/\mathbb{Q}))$.

THEOREME 2. - Si K/\mathbb{Q} est une extension diédrale, E_K / μ_K est $\mathbb{Z}(\text{Gal } K/\mathbb{Q})$ -isomorphe à $(1 - \zeta_p)^\epsilon \cdot \mathfrak{A}_K^+ \cdot \mathbb{Z}[\zeta_p]$ où \mathfrak{A}_K^+ désigne un idéal du sous-corps réel maximum de $\mathbb{Q}(\zeta_p)$ et où ϵ vaut 0 ou 1. De plus ϵ vaut 0 si et seulement si la puissance de p dans $(h_k \cdot w_k) / (h_K \cdot w_K)$ est impaire.

Démonstration. La structure de E_K / μ_K provient immédiatement des considérations précédentes et la valeur de ϵ s'obtient en considé-

rant la norme de \mathfrak{A}_K .

Ce théorème redonne des résultats de [5].

5. - CAS ABELIEN.

Supposons maintenant K abélien sur \mathbb{Q} , on a alors $E_K/\mu_K = E_F/\{\pm 1\}$, cf. [4] Satz 24, où E_F désigne le groupe des unités du sous-corps réel maximum F de K ; de plus l'extension K/k est ramifiée. Il est donc équivalent de dire que E_K/μ_K est $\mathbb{Z}[G]$ -monogène ou que $E_F/\{\pm 1\}$ l'est. La condition " \mathfrak{B}_K est principal" est donc équivalente à la condition analogue de [1]. Rappelons celle-ci. Soit f_0 le conducteur de F et posons

$$\theta_F = [N_{\mathbb{Q}(\zeta_{f_0})/F} (1 - \zeta_{f_0})]^{1/2}.$$

Le groupe des unités cyclotomiques de F , cf. [4], est θ_F^I et on a un isomorphisme

$$\theta_F^I \simeq (\zeta_p - 1) \cdot \mathbb{Z}[\zeta_p],$$

qui se prolonge à $E_F/\{\pm 1\} = E_K/\mu_K$ de façon unique en un isomorphisme

$$\mathfrak{I}_F : E_K/\mu_K \simeq \mathfrak{A}_F,$$

avec \mathfrak{A}_F idéal fractionnaire de $\mathbb{Q}(\zeta_p)$. Posons $\mathfrak{B}_F = (\zeta_p - 1) \mathfrak{A}_F^{-1}$: sa norme est égale au nombre h_F de classes de F et E_K/μ_K est monogène si et seulement si \mathfrak{B}_F est principal.

Soit θ le caractère de Dirichlet défini par k/\mathbb{Q} et f_1 le conducteur de K/\mathbb{Q} . D'après [2] corollaire du théorème 2, on a

$$\mu_K \cdot \Omega_K = \mu_K \cdot \theta_F^{(I \cap J)} \cdot \alpha \quad \text{avec} \quad \alpha = \sum_{s \in G} \alpha(s) \cdot s^{-1};$$

on a posé $\alpha(s) = \sum B_1\left(\frac{a}{f_1}\right)$ où $B_1(X) = X - \frac{1}{2}$ et où dans la somme, a parcourt l'ensemble des entiers de 1 à f_1 , premiers à f_1 et tels que la restriction à K de l'automorphisme $\zeta_{f_1} \rightarrow \zeta_{f_1}^a$ soit précisément s . On vérifie immédiatement que $(I \cap J)\alpha$ est inclus dans I ; avec les

III.6

notations du § 2, l'image de $\mu_K \cdot \Omega_K / \mu_K$ par \mathfrak{F}_F est $x \cdot (\zeta_p - 1) \cdot \mathfrak{g}$ avec

$$x = \sum_{i=0}^{p-1} \alpha(g^i) \cdot \zeta_p^{-i}$$

Ainsi \mathfrak{F}_F est égal à x fois le plongement \mathfrak{F}_K de E_K / μ_K dans $\mathbb{Q}(\zeta_p)$ utilisé au § 2. On a donc $\mathfrak{B}_K = x \cdot \mathfrak{B}_F$, ce qui fait le lien entre la condition du § 2 et celle de [1]. On peut retrouver par un calcul direct la valeur de la norme de x :

$$\begin{aligned} N(x) &= \prod_{\chi \neq 1} \left(\sum_{s \in G} \chi(s) \cdot \alpha(s) \right) = \prod_{\substack{f_1 \\ (a, f_1) = 1}} \left(\sum_{a=1}^{f_1} \chi_1(a) \cdot B_1\left(\frac{a}{f_1}\right) \right) \\ &= \pm (h_K \cdot w_k) / (h_F \cdot h_K \cdot w_K) \quad . \end{aligned}$$

Dans la première égalité χ décrit l'ensemble des caractères non triviaux de G et dans la deuxième χ_1 décrit l'ensemble des caractères de Dirichlet impairs $\neq \theta$ définis par K/\mathbb{Q} ; la dernière égalité provient de la formule analytique du nombre de classes, cf. [4], appliquée à K et k .

Remarque.

$$\mu_K \theta_F^I / \mu_K \Omega_K \simeq \mathbb{Z}[\zeta_p] / (x \cdot \quad) \quad .$$

BIBLIOGRAPHIE

- [1] A. BRUMER, On the group of units of an absolutely cyclic number field of prime degree, J. Math. Soc. Japan, vol.21, n°3 (1969), pp. 357-358.
- [2] R. GILLARD, Unités cyclotomiques et unités elliptiques, à paraître.
- [3] R. GILLARD et G. ROBERT, Groupes d'unités elliptiques, Bull. Soc. Math. France, t. 107 (1979).
- [4] H. HASSE, Über die Klassenzahl abelschen Zahlkörper, Akademie Verlag, Berlin (1952).
- [5] N. MOSER, Unités et nombres de classes d'une extension galoisienne diédrale de \mathbb{Q} , Abh. Math. Sem. Hamburg, à paraître.
- [6] G. ROBERT, Unités elliptiques, Bull. Soc. Math. France, mémoire 36 (1973).