J. Math. Soc. Japan
Vol. 32, No. 4, 1980

Unités elliptiques et unités de Minkowski

Par Roland GILLARD

(Reçu le 18 janv., 1979)

1. Présentation des résultats.

Soient k un corps quadratique imaginaire, p un nombre premier impair et K/k une extension cyclique de degré p. Soit $G=Gal(K/k)$. 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 $\boldsymbol{C}$ 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 $\boldsymbol{Z}[\zeta_p]$.* b) *Pour que E_K/μ_K soit $\boldsymbol{Z}[G]$-monogène, il suffit* (*resp. il faut*) *que tout* (*resp. au moins un*) *idéal de $\boldsymbol{Z}[\zeta_p]$, 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 $k=\boldsymbol{Q}$; 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.

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

Enonçons tout de suite le lemme:

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

DEMONSTRATION. Si un nombre premier l divise w_K/w_k, on a $\boldsymbol{Q}(\zeta_l)\subseteq K$, d'où $l=3$ 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 $\boldsymbol{Z}[G]$ et par J l'annulateur du $\boldsymbol{Z}[G]$-module μ_K. Posons

* Ceci répond à une question de J. J. Payan posée lors de la soutenance de thèse de N. Moser.

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

où $\varphi_{\mathfrak{f}}(C)$ est défini comme dans [6, § 2.2]; le produit est pris sur le noyau de l'application de réciprocité $Cl(\mathfrak{f}) \to G$, 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 $u \in \boldsymbol{Z}[G]$. 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 $\boldsymbol{Q}[G] \to \boldsymbol{Q}[\zeta_p]$ définie en envoyant un générateur g de G sur ζ_p; elle définit des isomorphismes

$$I \xrightarrow{\sim} (\zeta_p - 1) \cdot \boldsymbol{Z}[\zeta_p], \quad I \cap J \xrightarrow{\sim} (\zeta_p - 1) \cdot \mathfrak{L},$$

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

$$\mu_K \Omega_K / \mu_K \xrightarrow{\sim} (\zeta_p - 1) \cdot \mathfrak{L}$$

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

$$\phi_K : E_K / \mu_K \xrightarrow{\sim} \mathfrak{A}_K,$$

avec $\mathfrak{A}_K$ idéal fractionnaire de $\boldsymbol{Z}[\zeta_p]$. Posons $\mathfrak{B}_K = (\zeta_p - 1) \cdot \mathfrak{A}_K^{-1}$; la norme de $\mathfrak{L} \cdot \mathfrak{B}_K$ 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 $\boldsymbol{Z}[G]$-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 $\boldsymbol{Z}[G]$ et par J l'idéal $\{\sum n(s) \cdot s \in \boldsymbol{Z}[G] \mid \prod s^{n(s)} = 1\}$. 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 $\boldsymbol{Z}[G]$. Pour $u \in I \cap J$, $\delta_K(u)$ est une puissance d'ordre $h_k \cdot w_k$ dans E_K; posons

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

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 $\boldsymbol{Q}[G]$ dans $\boldsymbol{Q}(\zeta_p)$ qui envoie g sur ζ_p. Elle définit des isomorphismes

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

On a donc aussi un isomorphisme

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

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

$$\phi_K : E_K/\mu_K \to \mathfrak{A}_K\,,$$

avec $\mathfrak{A}_K$ idéal fractionnaire de $\boldsymbol{Z}(\zeta_p)$. 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 $\boldsymbol{Z}[G]$-monogène, d'où le théorème 1 dans le cas non ramifié.

4. Cas diédral.

Supposons de plus que K soit une extension diédrale de $\boldsymbol{Q}$. 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 $C\in Cl(\mathfrak{f})$; 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 ϕ_K des §2 et 3 sont compatibles avec l'action de t sur E_K et $\boldsymbol{Q}(\zeta_p)$. Ainsi $\mathfrak{A}_K$ est un idéal de $\boldsymbol{Q}(\zeta_p)$ invariant par t. En identifiant la multiplication par un générateur fixé g de G à celle par ζ_p, on munit $\boldsymbol{Q}(\zeta_p)$ et ses idéaux fractionnaires d'une action de $\boldsymbol{Z}(Gal(K/\boldsymbol{Q}))$.

THEOREME 2. *Si $K/\boldsymbol{Q}$ est une extension diédrale, E_K/μ_K est $\boldsymbol{Z}(Gal\ (K/\boldsymbol{Q}))$-isomorphe à $(1-\zeta_p)^{\varepsilon}\cdot\mathfrak{A}_K^+\cdot\boldsymbol{Z}[\zeta_p]$ où $\mathfrak{A}_K^+$ désigne un idéal du sous corps réel maximum de $\boldsymbol{Q}(\zeta_p)$ 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.*

DEMONSTRATION. La structure de E_K/μ_K provient immédiatement des considérations précédentes et la valeur de ε s'obtient en considérant la norme de $\mathfrak{A}_K$.

Ce théorème redonne des résultats de [5].

5. Cas abélien.

Supposons maintenant K abélien sur $\boldsymbol{Q}$, on a alors $E_K/\mu_K=E_F/\{\pm1\}$, 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 $\boldsymbol{Z}[G]$-monogène ou que $E_F/\{\pm1\}$ 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

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

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

$$\theta_F^I \xrightarrow{\sim} (\zeta_p-1)\cdot\boldsymbol{Z}[\zeta_p],$$

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

$$\phi_F: E_K/\mu_K \xrightarrow{\sim} \mathfrak{A}_F,$$

avec $\mathfrak{A}_F$ idéal fractionnaire de $\boldsymbol{Q}(\zeta_p)$. Posons $\mathfrak{B}_F=(\zeta_p-1)\cdot\mathfrak{A}_F^{-1}$: 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 $k/\boldsymbol{Q}$ et f_1 le conducteur de $K/\boldsymbol{Q}$. D'après [2] corollaire du théorème 2, on a

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

on a posé $\alpha(s)=\sum B_1\left(\frac{a}{f_1}\right)$ où $B_1(X)=X-(1/2)$ 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 $\zeta_{f_1}\to\zeta_{f_1}^a$ soit précisément s. On vérifie immédiatement que $(I\cap J)\alpha$ est inclus dans I; avec les notations du § 2, l'image de $\mu_K\cdot\Omega_K/\mu_K$ par ϕ_F est $x\cdot(\zeta_p-1)\cdot\mathfrak{L}$ avec

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

Ainsi ϕ_F est égal à x fois le plongement ϕ_K de E_K/μ_K dans $\boldsymbol{Q}(\zeta_p)$ 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:

$$\begin{aligned} N(x)&=\prod_{\chi\neq 1}\Big(\sum_{s\in G}\chi(s)\cdot\alpha(s)\Big)\\ &=\prod\Big(\frac{1}{2}\sum_{\substack{a=1\\(a,f_1)=1}}^{f_1}\chi_1(a)\cdot B_1\Big(\frac{a}{f_1}\Big)\Big)\\ &=\pm(h_K\cdot w_k)/(h_F\cdot h_k\cdot w_K).\end{aligned}$$

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 $K/\boldsymbol{Q}$; La dernière égalité provient de la formule analytique du nombre de classes, cf. [4], appliquée à K et k.

Bibliographie

[1] A. Brumer, On the group of units of an absolutely cyclic number field of prime degree, J. Math. Soc. Japan, 21 (1969), 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, **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 $\boldsymbol{Q}$, Abh. Math. Sem. Univ. Hamburg, à paraître.
[6] G. Robert, Unités elliptiques, Bull. Soc. Math. France, mémoire **36**, 1973.

R. GILLARD
Institut Fourier
Laboratoire associé au C.N.R.S. n° 188
Université de Grenoble I
B.P. 116
38402 Saint-Martin d'Hères
France