

MÉMOIRES DE LA S. M. F.

GILLES ROBERT

Unités elliptiques et formules pour le nombre de classes des extensions abéliennes d'un corps quadratique imaginaire

Mémoires de la S. M. F., tome 36 (1973)

http://www.numdam.org/item?id=MSMF_1973__36__5_0

© Mémoires de la S. M. F., 1973, tous droits réservés.

L'accès aux archives de la revue « Mémoires de la S. M. F. » (<http://smf.emath.fr/Publications/Memoires/Presentation.html>) 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/>

UNITES ELLIPTIQUES ET FORMULES
POUR LE NOMBRE DE CLASSES DES EXTENSIONS ABELIENNES
D'UN CORPS QUADRATIQUE IMAGINAIRE

par Gilles ROBERT

	pages
INTRODUCTION.....	6
§ 1. FONCTIONS THETA REDUITES DE DIVISEUR (0) RELATIVES A UN TORE \mathbb{C}/Γ	7
§ 2. LES INVARIANTS $\varphi_f(c)$ ASSOCIES AUX CLASSES DE RAYON c MODULO f .	
2.1. Notations.....	13
2.2. Construction des invariants $\varphi_f(c)$	14
2.3. Propriétés des invariants $\varphi_f(c)$	17
2.4. Expression de la valeur des fonctions $L(s, \chi)$ au point $s=1$ à l'aide des invariants $\varphi_f(c)$	21
§ 3. FORMULES POUR LE NOMBRE DE CLASSES DES EXTENSIONS ABELIENNES NON RAMIFIEES.	
3.1. Les invariants $\delta(c)$	24
3.2. Formules pour le nombre de classes.....	26
§ 4. UNITES DANS LES EXTENSIONS ABELIENNES RAMIFIEES.	
4.1. Racines de l'unité.....	31
4.2. Valeurs singulières de certaines fonctions thêta réduites.....	32
4.3. Notations.....	36
4.4. Racines (e_f) -ièmes des invariants $\varphi_f(c)$	36
4.5. Racines (e_f) -ièmes des invariants $\varphi_H(c)$	41
4.6. Rangs des groupes d'unités V_H , Φ_H et Ω_H	44
§ 5. LE GROUPE DES UNITES ELLIPTIQUES.....	47
§ 6. FORMULES POUR LE NOMBRE DE CLASSES DES EXTENSIONS ABELIENNES DE CONDUCTEUR PUISSANCE D'UN IDEAL PREMIER.	
6.1. Les invariants $\psi(c)$ et $\phi(c)$	50
6.2. Le groupe d'unités Ψ	52
6.3. Les groupes d'unités V , Λ et Λ^*	56
6.4. Intersections des groupes V , Ψ , Λ et Λ^* avec $E_{\text{HOH}}(1)$	58
6.5. Formules pour le nombre de classes.....	63
APPENDICE : Une illustration numérique.....	67
BIBLIOGRAPHIE.....	77

INTRODUCTION

Nous nous proposons de décrire, pour toute extension abélienne H d'un corps quadratique imaginaire K , un groupe d'unités \mathfrak{E}_H construit à l'aide des valeurs singulières de certaines fonctions modulaires. Les éléments des groupes \mathfrak{E}_H sont analogues aux unités circulaires de la théorie des extensions cyclotomiques du corps des rationnels, nous les appelons unités elliptiques. Lorsque le conducteur de l'extension H/K est puissance d'un idéal premier \mathfrak{p} de K , nous montrons (th. 16 § 6.5) - à l'aide de la formule de décomposition de la fonction zéta du corps H en produit de séries L - que l'indice du groupe \mathfrak{E}_H dans le groupe E_H est donné par la formule

$$(E_H : \mathfrak{E}_H) = \lambda h_H / [HH_{(1)} : H],$$

où h_H est le nombre de classes du corps H , où $H_{(1)}$ est le corps de classes absolu de K , et où $\lambda = 2^\alpha 3^\beta$, $\alpha \geq 0$, $\beta \geq 0$ (plus précisément, on a $\lambda = 12^{[H:K]-1} / \mu$, où μ est un certain entier qui divise 6). On observera que le quotient $h_H / [HH_{(1)} : H]$ est nécessairement un nombre entier, puisque l'extension $HH_{(1)}/H$ est abélienne et non ramifiée.

Soit p le plus petit entier > 0 qui appartient à \mathfrak{p} . Des formules, exprimant l'indice de certains sous-groupes de \mathfrak{E}_H dans le groupe E_H comme produit de $h_H / [HH_{(1)} : H]$ par un entier λ , ont déjà été construites par FUETER [F], SIEGEL [S], RAMACHANDRA [R] et NOVIKOV [N_1]; l'entier λ était alors le produit de puissances de p , de puissances de h et d'un autre facteur entier. Ici λ ne contient que des puissances de 2 et de 3; en particulier, si $p \neq 2, 3$, la formule peut être utilisée pour démontrer des critères de divisibilité de $h_H / [HH_{(1)} : H]$ par p analogues à ceux de NOVIKOV [N_2]; nous ne le ferons pas ici.

Je tiens à exprimer ici ma dette à l'égard de MM. les professeurs A. NERON, dont les remarques m'ont fourni le point de départ de mes recherches concernant les formules pour le nombre de classes, J.P. SERRE, qui a lu avec attention plusieurs versions du manuscrit et m'a fait avec pertinence un grand nombre d'observations et de suggestions, et G. POITOU qui a su diriger avec tact et persévérance l'élaboration de ce travail. Je remercie enfin Mme BONNARDEL qui s'est chargée avec autant de gentillesse que d'efficacité de la dactylographie de mon manuscrit.

§ 1. FONCTIONS THETA REDUITES DE DIVISEUR (0) RELATIVES A UN TORE \mathbb{C}/Γ .

Ce paragraphe contient les résultats préliminaires à la construction des invariants $\varphi_f(C)$ du § 2. Ces résultats seront également utilisés dans les §§ 4.2 et 4.4, lorsque nous rechercherons les racines f -ièmes des invariants $\varphi_f(C)$. Notre terminologie est celle de WEIL [W ℓ] chap. VI.

Soient $t \in \mathbb{C}$ et $w \in \mathbb{C}$ avec $\text{Im}(w) > 0$. On définit

$$\eta(w) = q^{1/24} \prod_{n=1}^{\infty} (1-q^n),$$

$$\theta_1(t, w) = 2q^{1/8} \sin(\pi t) \prod_{n=1}^{\infty} (1-q^n)(1-2q^n \cos(2\pi t) + q^{2n}),$$

avec $q = \exp(2\pi iw)$, $q^{1/8} = \exp(\pi iw/4)$ et $q^{1/24} = \exp(\pi iw/12)$; les deux produits infinis convergent absolument. La fonction $\Delta(w) = (2\pi)^{12} \eta^{24}(w)$ est une forme modulaire de poids 12. La fonction $t \mapsto \theta_1(t, w)$ est identique à la fonction $t \mapsto \theta_{11}(t, w)$ de WEBER [Wb] § 24 p. 85; elle est donc entière, elle vérifie les identités

$$(1) \quad \begin{cases} \theta_1(t+1, w) = -\theta_1(t, w) \\ \theta_1(t+w, w) = -\exp(-\pi i(2t+w)) \theta_1(t, w), \end{cases}$$

cf. [Wb] § 20 p. 69; ses zéros sont les points du réseau de base 1, w , chacun d'ordre un, cf. [Wb] § 21 p. 73; sa dérivée au point $t = 0$ est égale à $2\pi \eta^3(w)$.

Soient Γ un réseau complexe et w_1, w_2 une base de Γ telle que $\text{Im}(w_2/w_1) > 0$; les invariants $a(\Gamma) = (w_2 \bar{w}_1 - w_1 \bar{w}_2)/2i$ (l'aire de \mathbb{C}/Γ) et $\Delta(\Gamma) = w_1^{-12} \Delta(w_2/w_1)$ sont indépendants du choix de la base w_1, w_2 . Posons

$$\theta(t; w_1, w_2) = \eta^{-1}(w_2/w_1) \exp(\pi t^2 \bar{w}_1/2w_1 a(\Gamma)) \theta_1(t/w_1, w_2/w_1).$$

La fonction $t \mapsto \theta(t; w_1, w_2)$ est entière; ses zéros sont les points de Γ , chacun d'ordre 1; sa dérivée au point $t=0$ est égale à $2\pi w_1^{-1} \eta^2(w_2/w_1)$. Pour $i=1$ ou 2, on déduit de (1) l'identité

$$(2) \quad \theta(t+w_1; w_1, w_2) = -\exp(\mathfrak{H}(w_1, t) + \mathfrak{H}(w_1, w_1)/2) \theta(t; w_1, w_2),$$

avec $\mathfrak{H}(t, t') = \pi \bar{t} t' / a(\Gamma)$. Il en résulte que la fonction $t \mapsto \theta(t; w_1, w_2)$ est l'unique fonction thêta réduite de diviseur (0) relative au tore \mathbb{C}/Γ , dont la dérivée au point $t=0$ est égale à $2\pi w_1^{-1} \eta^2(w_2/w_1)$; cf. [WL] chap. VI pp. 113 et suivantes. La fonction $t \mapsto \theta^{12}(t; w_1, w_2)$ est donc l'unique fonction thêta réduite de diviseur $12(0)$ relative au tore \mathbb{C}/Γ telle que

$$\lim_{t \rightarrow 0} \theta^{12}(t; w_1, w_2) / t^{12} = (2\pi)^{12} w_1^{-12} \eta^{24}(w_2/w_1) = \Delta(\Gamma);$$

elle ne dépend pas du choix de la base w_1, w_2 de Γ , et on pose

$$\theta^{(12)}(t; \Gamma) = \theta^{12}(t; w_1, w_2).$$

Soit
$$\varphi(t; w_1, w_2) = \theta(t; w_1, w_2) \exp(-\mathfrak{H}(t, t)/2);$$

la fonction $t \mapsto \varphi^{12}(t; w_1, w_2)$ ne dépend pas du choix de w_1, w_2 et on pose

$$\varphi^{(12)}(t; \Gamma) = \theta^{(12)}(t; \Gamma) \exp(-6\mathfrak{H}(t, t)) = \varphi^{12}(t; w_1, w_2);$$

on déduit de (2) l'identité

$$(3) \quad \varphi(t+\gamma; w_1, w_2) = -\exp(\mathfrak{Y}(\gamma, t)/2) \varphi(t; w_1, w_2), \quad \gamma \in \Gamma,$$

avec $\mathfrak{Y}(\gamma, t) = \mathfrak{H}(\gamma, t) - \mathfrak{H}(t, \gamma)$.

Le résultat suivant est immédiat :

Lemme 1. Pour tout nombre complexe $a \neq 0$, on a $\theta(at; aw_1, aw_2) = \theta(t; w_1, w_2)$ et $\varphi(at; aw_1, aw_2) = \varphi(t; w_1, w_2)$; par conséquent $\theta^{(12)}(at; a\Gamma) = \theta^{(12)}(t; \Gamma)$ et $\varphi^{(12)}(at; a\Gamma) = \varphi^{(12)}(t; \Gamma)$.

Soient γ et γ' deux éléments de Γ , le nombre

$$\mathfrak{Y}(\gamma, \gamma') / 2\pi i = (\mathfrak{H}(\gamma, \gamma') - \mathfrak{H}(\gamma', \gamma)) / 2\pi i = (\gamma' \bar{\gamma} - \gamma \bar{\gamma}') / (w_2 \bar{w}_1 - w_1 \bar{w}_2)$$

est un entier et par conséquent $\exp(\mathfrak{Y}(\gamma, \gamma')) = 1$. On déduit alors de (3) le résultat suivant :

Lemme 2. Soit f un entier > 0 . Lorsque $t \in \mathbb{C}$ est tel que $ft \in \Gamma$, les nombre $\varphi^{2f}(t; w_1, w_2)$ et $\varphi^{(12)f}(t; \Gamma) = \varphi^{12f}(t; w_1, w_2)$ ne dépendent que de la

classe de t modulo Γ .

Soient maintenant Γ et Γ' deux réseaux tels que $\Gamma' \supset \Gamma$; le groupe Γ'/Γ est fini, on note $n = (\Gamma':\Gamma)$ son ordre et n_1 le plus petit entier > 0 tel que $n_1 \Gamma' \subset \Gamma$. Démontrons le résultat suivant, qui généralise les formules (88) à (91), p. 128 de [R] § 6.

Proposition 1. Soit $\{t_1 = 0, t_2, \dots, t_n\}$ un système complet de représentants de Γ'/Γ ; soient f un entier > 0 et $t \in \mathbb{C}$, tels que $ft \in \Gamma$; on a

$$(\Delta(\Gamma')/\Delta(\Gamma))^{n_1} = \prod_{i=2}^n \varphi^{(12)n_1}(t_i; \Gamma),$$

et

$$\varphi^{(12)m}(t; \Gamma') = \prod_{i=1}^n \varphi^{(12)m}(t+t_i; \Gamma)$$

où m est le p.p.c.m de f et de n_1 .

Démonstration : soient w_1, w_2 une base de Γ et w'_1, w'_2 une base de Γ' telles que $\text{Im}(w_2/w_1) > 0$ et $\text{Im}(w'_2/w'_1) > 0$. La fonction $t \mapsto \theta(t; w'_1, w'_2)$ est une fonction thêta réduite de diviseur (0) relative au tore \mathbb{C}/Γ' ; c'est aussi une fonction thêta réduite de diviseur $\sum_{j=1}^n (t_j)$ relative au tore \mathbb{C}/Γ . Soit θ la fonction définie par

$$t \mapsto \theta(t) = \prod_{j=1}^n \exp(-\frac{1}{2}(t_j, t)) \theta(t+t_j; w_1, w_2);$$

d'après [Wl] chap. VI p. 111, le j -ième facteur de θ est une fonction thêta réduite de diviseur (t_j) relative au tore \mathbb{C}/Γ ; par conséquent θ est une fonction thêta réduite de diviseur $\sum_{j=1}^n (t_j)$ relative au tore \mathbb{C}/Γ . Les fonctions $t \mapsto \theta(t)$ et $t \mapsto \theta(t; w'_1, w'_2)$ sont donc proportionnelles : il existe $K_1 \in \mathbb{C}$, tel que

$$(4) \quad \theta(t) = K_1 \theta(t; w'_1, w'_2).$$

Dérivons l'identité (4) au point $t=0$, il vient

$$(5) \quad \prod_{j=2}^n \theta(t_j; w_1, w_2) = K_1 \eta_2(w'_1, w'_2) \eta_2^{-1}(w_1, w_2),$$

où $\eta_2(w_1, w_2) = w_1^{-1} \eta^2(w_2/w_1)$ et $\eta_2(w'_1, w'_2) = w'_1{}^{-1} \eta^2(w'_2/w'_1)$. Posons

$K_2 = K_1 \exp(-\sum_{j=1}^n \mathfrak{H}(t_j, t_j)/2)$ et $\tau = \sum_{j=1}^n t_j$, on déduit des identités (4) et (5) :

$$(6) \quad \exp(\mathfrak{H}(t, \tau)/2) \prod_{j=1}^n \varphi(t+t_j; w_1, w_2) = K_2 \varphi(t; w'_1, w'_2)$$

$$(7) \quad \prod_{j=2}^n \varphi(t_j; w_1, w_2) = K_2 \eta_2(w'_1, w'_2) \eta_2^{-1}(w_1, w_2).$$

Comme, d'après le lemme 2, les nombres $\varphi^{2n_1}(t_j; w_1, w_2)$ ne dépendent que de la classe de t_j modulo Γ , il résulte de (7) que la constante K , définie par $K = K(w_1, w_2; w'_1, w'_2) = K_2^{2n_1}$, ne dépend pas du choix du système de représentants $\{t_1 = 0, t_2, \dots, t_n\}$ de Γ'/Γ .

Notons m_1 le p.p.c.m de $4f$ et de $2n_1$. Comme 2τ et ft appartiennent à Γ , le nombre $\mathfrak{H}(ft, 2\tau)/2\pi i$ est un entier et on a $\exp(\mathfrak{H}(t, \tau)/2)^{4f} = \exp(\mathfrak{H}(ft, 2\tau)) = 1$; par conséquent, si l'on élève les identités (6) et (7) respectivement à la puissance m_1 et à la puissance $2n_1$, il vient

$$(8) \quad \begin{cases} \prod_{j=1}^n \varphi^{m_1}(t+t_j; w_1, w_2) = K^{m_1/2n_1} \varphi^{m_1}(t; w'_1, w'_2) \\ \prod_{j=2}^n \varphi^{2n_1}(t_j; w_1, w_2) = K \eta_2^{2n_1}(w'_1, w'_2) \eta_2^{-2n_1}(w_1, w_2). \end{cases}$$

La proposition 1 résultera des identités (8) si nous démontrons que $K(w_1, w_2; w'_1, w'_2)$ est une racine 6-ième de l'unité.

Considérons d'abord les réseaux Γ et $\Gamma/2$, et observons que $K(w_1, w_2; w_1/2, w_2/2) = 1$ pour toute base w_1, w_2 de Γ ; il résulte en effet de la définition de $\varphi(t; w_1, w_2)$ que

$$\begin{aligned} & \varphi^4(w_1/2; w_1, w_2) \varphi^4(w_2/2; w_1, w_2) \varphi^4(w_1/2+w_2/2; w_1, w_2) = \\ & \eta^{-12}(w) \exp(2\pi i w) \theta_1^4(1/2, w) \theta_1^4(w/2, w) \theta_1^4((1+w)/2, w), \end{aligned}$$

où $w = w_2/w_1$; de plus on sait d'après [wb] § 21 p. 73 et § 34 p. 112 que

$$\exp(2\pi i w) \theta_1^4(1/2, w) \theta_1^4(w/2, w) \theta_1^4((1+w)/2, w) = \theta_{00}^4 \theta_{10}^4 \theta_{01}^4,$$

et que $\theta_{00} \theta_{10} \theta_{01} = 2\eta^3(w)$; d'où

$$\varphi^4(w_1/2; w_1, w_2) \varphi^4(w_2/2; w_1, w_2) \varphi^4((w_1+w_2)/2; w_1, w_2) = 2^4,$$

et $K(w_1, w_2; w_1/2, w_2/2) = 1$ d'après (8) puisque $\eta_2(w_1/2, w_2/2)/\eta_2(w_1, w_2) = 2$.

Revenons au cas général. Soient respectivement $\{s_1 = 0, s_2, s_3, s_4\}$, $\{s'_1 = 0, s'_2, s'_3, s'_4\}$ et $\{t_1 = 0, t_2, \dots, t_n\}$, $\{t'_1 = 0, t'_2, \dots, t'_n\}$ des systèmes complets de représentants des quotients $(\Gamma/2)/\Gamma$, $(\Gamma'/2)/\Gamma'$ et $(\Gamma'/2)/(\Gamma/2)$, Γ'/Γ .

Appliquons les identités (8) aux couples $\Gamma/2$, $\Gamma'/2$ et Γ , Γ' , il vient

$$(9) \quad \prod_{j=2}^n \varphi^{4n_1}(t_j; w_1/2, w_2/2) = K^2(w_1/2, w_2/2; w'_1/2, w'_2/2) \eta_2^{4n_1}(w'_1/2, w'_2/2) \eta_2^{-4n_1}(w_1/2, w_2/2),$$

et

$$(10) \quad \prod_{j=2}^n \varphi^{4n_1}(t'_j; w_1, w_2) \prod_{i=2}^4 \prod_{j=1}^n \varphi^{4n_1}(t'_j + s'_i; w_1, w_2) \\ = K^8(w_1, w_2; w'_1, w'_2) \eta_2^{4n_1}(w'_1, w'_2) \eta_2^{-4n_1}(w_1, w_2) \prod_{i=2}^4 \varphi^{4n_1}(s'_i; w'_1, w'_2).$$

Posons
$$A = \prod_{\substack{(i,j) \in (1, \dots, 4) \\ (i,j) \neq (1,1)}} (1, \dots, n) \varphi^{4n_1}(s_i + t_j; w_1, w_2)$$

et
$$A' = \prod_{\substack{(i,j) \in (1, \dots, 4) \\ (i,j) \neq (1,1)}} (1, \dots, n) \varphi^{4n_1}(s'_i + t'_j; w_1, w_2).$$

Puisque $K(w_1, w_2; w_1/2, w_2/2) = K(w'_1, w'_2; w'_1/2, w'_2/2) = 1$, nous avons d'après (8),

$$\prod_{i=1}^4 \varphi^{4n_1}(s_i + t_j; w_1, w_2) = \varphi^{4n_1}(t_j; w_1/2, w_2/2), \quad 2 \leq j \leq n,$$

et
$$\prod_{i=2}^4 \varphi^4(s_i; w_1, w_2) = \prod_{i=2}^4 \varphi^4(s'_i; w'_1, w'_2) = 2^4.$$

Substituons ces identités dans (9) et (10), il vient

$$A = 2^{4n_1} K^2(w_1/2, w_2/2; w'_1/2, w'_2/2) \eta_2^{4n_1}(w'_1, w'_2) \eta_2^{-4n_1}(w_1, w_2)$$

et
$$A' = 2^{4n_1} K^8(w_1, w_2; w'_1, w'_2) \eta_2^{4n_1}(w'_1, w'_2) \eta_2^{-4n_1}(w_1, w_2).$$

Les nombres $\{r_{i,j} = s_i + t_j \mid i \in (1, \dots, 4) \text{ et } j \in (1, 2, \dots, n)\}$ et $\{r'_{i,j} = s'_i + t'_j \mid i \in (1, \dots, 4) \text{ et } j \in (1, 2, \dots, n)\}$ forment chacun un système complet de représentants de $(\Gamma'/2)/\Gamma$, et d'après le lemme 2, le nombre $\varphi^{4n}(r_{i,j}; w_1, w_2)$ ne dépend que de la classe de $r_{i,j}$ modulo Γ ; il en résulte que $A = A'$, d'où

$$K^8(w_1, w_2; w'_1, w'_2) = K^2(w_1/2, w_2/2; w'_1/2, w'_2/2).$$

D'autre part, d'après le lemme 1, nous avons

$$K(w_1, w_2; w'_1, w'_2) = K(w_1/2, w_2/2; w'_1/2, w'_2/2),$$

par conséquent $K(w_1, w_2; w'_1, w'_2)$ est bien une racine 6-ième de l'unité; la proposition 1 est démontrée.

§ 2. LES INVARIANTS $\varphi_f(C)$ ASSOCIES AUX CLASSES DE RAYONS C MODULO f .

Nous rappelons dans le § 2.1 quelques notions de théorie du corps de classes et précisons nos notations. Dans le § 2.2 nous définissons les invariants $\varphi_f(C)$ et nous montrons qu'ils coïncident avec les conjugués complexes des invariants $\Phi_{f,(1)}(C)$ introduits dans [R] § 3. Le théorème 1 § 2.3 est un rappel des propriétés algébriques des invariants $\varphi_f(C)$ démontrées dans [R] §§ 5.6, théorème 5 et théorème 7 ; le théorème 2 § 2.3 décrit certaines relations algébriques vérifiées par les invariants $\varphi_f(C)$, relations qui résultent de la proposition 1 § 1. Nous empruntons le théorème 3 § 2.4 à MEYER [M] et SIEGEL [S] ; ce théorème exprime le produit $h_H R_H$ du nombre de classes et du régulateur d'une extension abélienne H d'un corps quadratique imaginaire, à l'aide des logarithmes des valeurs absolues des invariants $\varphi_f(C)$. Nous observons enfin (corollaire du théorème 3) comment le théorème 2 § 3 de [R] peut se déduire du théorème 2 et du théorème 3, (i).

2.1. Notations.

Soient K un corps quadratique imaginaire et σ l'anneau des entiers de K . Les symboles Tr et N désigneront respectivement la trace et la norme d'un élément de K relativement au corps des nombres rationnels. On note $\alpha, \beta, \gamma, \dots$ des idéaux de K . L'idéal \mathfrak{d} est la différentielle et l'entier négatif $-d$ le discriminant de K . On note e le nombre de racines de l'unité qui appartiennent à K et h le nombre de classes de K . Pour tout entier $n > 0$, on désigne par μ_n le groupe des racines n -ièmes de l'unité.

Pour toute extension abélienne H de K , on note e_H le nombre de racines de l'unité qui appartiennent au corps H , et on note E_H le groupe des unités, h_H le nombre de classes et R_H le régulateur de H .

Pour tout idéal entier f de K , on désigne par e_f le nombre de racines de l'unité de K congrues à 1 modulo f . On note $\text{Cl}(f)$ le groupe de classes de rayon modulo f de K , c'est-à-dire le quotient du groupe des idéaux premiers avec f par le "rayon modulo f " formé des idéaux principaux (λ) tel que $\lambda \equiv 1 \pmod{f}$, cf. Note. Pour tout caractère χ du groupe $\text{Cl}(f)$ et pour tout idéal en-

tier α de K , nous posons $\chi(\alpha) = 0$ si $(\alpha, \mathfrak{f}) \neq (1)$ et $\chi(\alpha) = \chi(C_\alpha)$ si $(\alpha, \mathfrak{f}) = (1)$, où $C_\alpha \in \text{Cl}(\mathfrak{f})$ est la classe à laquelle appartient α .

On désigne par $H_{\mathfrak{f}}$ le "corps de classes du rayon modulo \mathfrak{f} de K ", le corps $H_{\mathfrak{f}}$ est l'extension abélienne maximale de K dont le conducteur divise \mathfrak{f} . On note $g(C)$ l'automorphisme de $H_{\mathfrak{f}}/K$ associé à une classe $C \in \text{Cl}(\mathfrak{f})$ par la loi de réciprocité d'Artin ; l'application $C \mapsto g(C)$ définit un isomorphisme du groupe $\text{Cl}(\mathfrak{f})$ sur le groupe de Galois de $H_{\mathfrak{f}}/K$. Soit H/K une sous-extension de $H_{\mathfrak{f}}/K$; nous attachons à l'extension H/K le groupe de classes d'idéaux $\text{Cl}(H/K)$, quotient du groupe $\text{Cl}(\mathfrak{f})$ par le groupe $\text{Cl}(H_{\mathfrak{f}}/H)$ formé des classes de rayon $C \in \text{Cl}(\mathfrak{f})$ telles que $g(C)$ définisse un automorphisme de $H_{\mathfrak{f}}/H$; les groupes $\text{Cl}(H_{\mathfrak{f}}/H)$ et $\text{Cl}(H/K)$ sont respectivement isomorphes au groupe de Galois de $H_{\mathfrak{f}}/H$ et H/K , et les caractères du groupe $\text{Cl}(H/K)$ s'identifient aux caractères χ du groupe $\text{Cl}(\mathfrak{f})$, tels que $\chi(C) = 1$ pour toutes les classes $C \in \text{Cl}(H_{\mathfrak{f}}/H)$.

2.2. Construction des invariants $\varphi_{\mathfrak{f}}(C)$.

Soient \mathfrak{f} un idéal entier de K et f le plus petit entier > 0 qui appartient à \mathfrak{f} . On considère l'ensemble $A(\mathfrak{f})$ des couples (t, \mathfrak{b}) , où $t \in \mathbb{C}$ et \mathfrak{b} est un idéal de K , tels que $\mathfrak{f} = \{\alpha \in \sigma \mid \alpha t \in \mathfrak{b}\} = \sigma \cap t^{-1}\mathfrak{b}$. On dit que deux couples $\{t, \mathfrak{b}\}$ et $\{t', \mathfrak{b}'\}$ sont équivalents s'il existe $\theta \in K^*$ tel que l'idéal $(t'/\theta t)$ appartienne au rayon modulo \mathfrak{f} et $\mathfrak{b}' = \theta \mathfrak{b}$; il existe alors une unité u de K telle que $t' \equiv u \theta t \pmod{\mathfrak{b}'}$ et nous avons le résultat suivant :

Lemme 3. Soient (t, \mathfrak{b}) et $(t', \mathfrak{b}') \in A(\mathfrak{f})$ deux couples équivalents ; alors

$$\varphi^{(12)f}(t; \mathfrak{b}) = \varphi^{(12)f}(t'; \mathfrak{b}').$$

Démonstration : d'après les lemmes 1 et 2 § 1, nous avons

$$\varphi^{(12)f}(t; \mathfrak{b}) = \varphi^{(12)f}(t; \mathfrak{b}'\theta^{-1}) = \varphi^{(12)f}(u\theta t; u\mathfrak{b}') = \varphi^{(12)f}(t'; \mathfrak{b}'); \text{ C.Q.F.D.}$$

Note. La congruence $\lambda \equiv 1 \pmod{\mathfrak{f}}$ signifie qu'il existe des entiers α et $\beta \in \sigma$ premiers avec \mathfrak{f} tels que $\lambda = \alpha/\beta$ et $\alpha \equiv \beta \pmod{\mathfrak{f}}$.

Pour tout couple $(t, \mathfrak{f}) \in A(\mathfrak{f})$, l'idéal $t\mathfrak{f}\mathfrak{f}^{-1}$ est entier et premier avec \mathfrak{f} ; soit $C_{(t, \mathfrak{f})} \in Cl(\mathfrak{f})$ la classe de $t\mathfrak{f}\mathfrak{f}^{-1}$, nous avons le résultat suivant :

Lemme 4. Désignons par \sim l'équivalence dans $A(\mathfrak{f})$. L'application
 $(t, \mathfrak{f}) \mapsto C_{(t, \mathfrak{f})}$ définit un isomorphisme des groupes $A(\mathfrak{f})/\sim$ et $Cl(\mathfrak{f})$ (*) .

Démonstration : soient (t, \mathfrak{f}) et (t', \mathfrak{f}') $\in A(\mathfrak{f})$ deux couples équivalents ; la classe $C_{(t', \mathfrak{f}')}/C_{(t, \mathfrak{f})}$ est celle de l'idéal $t'\mathfrak{f}'\mathfrak{f}'^{-1}/t\mathfrak{f}\mathfrak{f}^{-1} = (t'/\theta t)$; comme $(t'/\theta t)$ appartient au rayon modulo \mathfrak{f} nous avons $C_{(t', \mathfrak{f}')} = C_{(t, \mathfrak{f})}$. Par conséquent l'application $(t, \mathfrak{f}) \mapsto C_{(t, \mathfrak{f})}$ définit, par passage au quotient, un homomorphisme du groupe $A(\mathfrak{f})/\sim$ dans le groupe $Cl(\mathfrak{f})$.

Réciproquement, soient α et α' des idéaux entiers de K , premiers avec \mathfrak{f} , et soient (t, \mathfrak{f}) et (t', \mathfrak{f}') des couples tels que $\alpha\mathfrak{f}\mathfrak{f}^{-1} = (t)$ et $\alpha'\mathfrak{f}'\mathfrak{f}'^{-1} = (t')$. Nous avons (t, \mathfrak{f}) et $(t', \mathfrak{f}') \in A(\mathfrak{f})$; en effet pour tout entier $\alpha \in \sigma$, une condition nécessaire et suffisante pour que $\alpha t \in \mathfrak{f}$ est que l'idéal $\alpha t \mathfrak{f}^{-1} = \alpha \alpha \mathfrak{f}^{-1}$ soit entier ; comme l'idéal α est entier et premier avec \mathfrak{f} cette condition équivaut à $\alpha \in \mathfrak{f}$. D'autre part, supposons que les classes dans $Cl(\mathfrak{f})$ de α et de α' soient égales. Les idéaux \mathfrak{f} et \mathfrak{f}' appartiennent alors à la même classe absolue de K , il existe donc $\theta \in K^*$ tel que $\mathfrak{f}' = \theta \mathfrak{f}$ et $(t'/\theta t) = \alpha' \mathfrak{f}' / \theta \alpha \mathfrak{f} = \alpha' / \alpha$, et le quotient α' / α appartient au rayon modulo \mathfrak{f} . Par conséquent les couples (t, \mathfrak{f}) et (t', \mathfrak{f}') sont équivalents et nous avons construit l'application réciproque de l'homomorphisme $(t, \mathfrak{f}) \mapsto C_{(t, \mathfrak{f})}$ de $A(\mathfrak{f})/\sim$ dans $Cl(\mathfrak{f})$. Le lemme 4 est démontré.

Définition. Pour tout idéal entier $\mathfrak{f} \neq (1)$ de K et pour toute classe
 $C \in Cl(\mathfrak{f})$, on pose

$$\varphi_{\mathfrak{f}}(C) = \varphi^{(12)\mathfrak{f}}(t; \mathfrak{f}),$$

où $(t, \mathfrak{f}) \in A(\mathfrak{f})$ est tel que $C_{(t, \mathfrak{f})} = C$. Lorsque $\mathfrak{f} = (1)$, on a $t \in \mathfrak{f}$ d'où

(*) Cette construction nous a été suggérée par Jean-Pierre SERRE.

$\varphi^{(12)}(t; \mathfrak{t}) = 0$; pour toute classe $c \in Cl(1)$, on pose alors

$$\varphi_{(1)}(c) = |(2\pi)^{-12} N(\mathfrak{t})^6 \Delta(\mathfrak{t})| ,$$

où l'idéal \mathfrak{t} appartient à c^{-1} . D'après le lemme 3, les invariants $\varphi_{\mathfrak{f}}(c)$ ne dépendent que de l'idéal \mathfrak{f} et de la classe $C \in Cl(\mathfrak{f})$.

Les invariants $\varphi_{\mathfrak{f}}(c)$ sont les conjugués complexes des invariants définis dans [R] § 3 ; plus précisément, nous avons :

Proposition 2. Soit \mathfrak{f} un idéal entier de K , et soit $C \in Cl(\mathfrak{f})$ une classe de rayon modulo \mathfrak{f} ; on a $\varphi_{\mathfrak{f}}(c) = \overline{\Phi_{\mathfrak{f},(1)}(c)}$, où l'invariant $\Phi_{\mathfrak{f},(1)}(c)$ est défini comme dans [R] § 3 pp. 108-110.

Démonstration : soit γ un élément de K tel que l'idéal $\gamma \mathfrak{f}$ soit entier et premier avec \mathfrak{f} ; soient \mathfrak{t} un idéal entier de K premier avec \mathfrak{f} tel que $\gamma \mathfrak{f} \mathfrak{t} \in C$, et b_1, b_2 une base de \mathfrak{t} telle que $\text{Im}(b_2/b_1) > 0$. Lorsque $\mathfrak{f} = (1)$, nous avons $\varphi_{\mathfrak{f}}(c) = \Phi_{\mathfrak{f},(1)}(c) = \overline{\Phi_{\mathfrak{f},(1)}(c)}$. Lorsque $\mathfrak{f} \neq (1)$, l'invariant $\Phi_{\mathfrak{f},(1)}(c)$ est défini par

$$\Phi_{\mathfrak{f},(1)}(c) = \varphi^{(12)f}(\text{Tr}(\gamma b_2)_{b_1} - \text{Tr}(\gamma b_1)_{b_2}; \mathfrak{t}) ;$$

comme $\text{Tr}(\gamma b_2)_{b_1} - \text{Tr}(\gamma b_1)_{b_2} = -i\sqrt{d} \bar{\gamma} N(\mathfrak{t})$, il résulte du lemme 1 § 1 que

$$\Phi_{\mathfrak{f},(1)}(c) = \varphi^{(12)f}(-i\sqrt{d} \bar{\gamma} N(\mathfrak{t}); \mathfrak{t}) = \varphi^{(12)f}(-i\sqrt{d} \bar{\gamma}; \mathfrak{t}^{-1}) ,$$

d'où $\overline{\Phi_{\mathfrak{f},(1)}(c)} = \varphi^{(12)f}(i\sqrt{d} \gamma; \mathfrak{t}^{-1})$; l'identité $\overline{\Phi_{\mathfrak{f},(1)}(c)} = \varphi_{\mathfrak{f}}(c)$ s'en déduit immédiatement, puisque pour l'idéal entier $\gamma \mathfrak{f} \mathfrak{t}$ de C l'on a $(\gamma \mathfrak{f} \mathfrak{t}) \mathfrak{t}^{-1} \mathfrak{f}^{-1} = (i\sqrt{d} \gamma)$, d'où $c_{(i\sqrt{d} \gamma, \mathfrak{t}^{-1})} = c$.

2.3. Propriétés des invariants $\varphi_{\mathfrak{f}}(C)$.

Vu la proposition 2, on déduit de [R] §§ 5 et 6, théorème 5 et théorème 7 les propriétés suivantes des invariants $\varphi_{\mathfrak{f}}(C)$.

Théorème 1. Pour tout idéal entier $\mathfrak{f} \neq (1)$ du corps K et pour toutes classes C et $C' \in \text{Cl}(\mathfrak{f})$,

- (i) L'invariant $\varphi_{\mathfrak{f}}(C)$ est un élément entier du corps de classes $H_{\mathfrak{f}}$;
- (ii) Le quotient $\varphi_{\mathfrak{f}}(C)/\varphi_{\mathfrak{f}}(C')$ est une unité de $H_{\mathfrak{f}}$;
- (iii) On a $\varphi_{\mathfrak{f}}(C)^{g(C')} = \varphi_{\mathfrak{f}}(CC')$.

Démontrons maintenant, à l'aide de la proposition 1 § 1, les relations suivantes.

Théorème 2. Soient \mathfrak{f} un idéal entier et \mathfrak{p} un idéal premier de K . Soient respectivement f, p et f' les plus petits entiers > 0 qui appartiennent aux idéaux $\mathfrak{f}, \mathfrak{p}$ et \mathfrak{fp} . On pose $\varepsilon = e_{\mathfrak{f}}/e_{\mathfrak{fp}}$ ($\varepsilon = 1, 2, 3, 4$ ou 6); et, lorsque $(\mathfrak{f}, \mathfrak{p}) = (1)$, on note $C_{\mathfrak{p}} \in \text{Cl}(\mathfrak{f})$ la classe à laquelle \mathfrak{p} appartient. Pour toute classe $C \in \text{Cl}(\mathfrak{f})$, on a :

- (i) Lorsque $\mathfrak{p} \nmid \mathfrak{f}$, l'entier f'/f est égal à p si $f \notin \mathfrak{fp}$ et à 1 si $f \in \mathfrak{fp}$, et

$$\varphi_{\mathfrak{f}}(C)^{f'/f} = \prod_{C' \subset C} \varphi_{\mathfrak{fp}}(C')^{\varepsilon};$$

- (ii) Lorsque $(\mathfrak{p}, \mathfrak{f}) = (1)$ et $\mathfrak{f} \neq (1)$, l'entier f'/f est égal à p , et

$$\varphi_{\mathfrak{f}}(C)^{f'/f} \varphi_{\mathfrak{f}}(CC_{\mathfrak{p}}^{-1})^{-f'/f} = \prod_{C' \subset C} \varphi_{\mathfrak{fp}}(C')^{\varepsilon};$$

- (iii) Lorsque $\mathfrak{f} = (1)$, on a

$$\Delta^p(\mathfrak{b})\Delta^{-p}(\mathfrak{b}\mathfrak{p}) = \prod_{C' \subset C} \varphi_{\mathfrak{p}}(C')^{\varepsilon}$$

pour tout idéal $\mathfrak{b} \in C^{-1}$;

où les trois produits sont pris sur toutes les classes $C' \in \text{Cl}(\mathfrak{fp})$ contenues dans la classe $C \in \text{Cl}(\mathfrak{f})$.

Démonstration :

Soit $(t, \ell) \in A(\mathcal{f})$ un couple tel que $C_{(t, \ell)} = C$. Soit $\{u_i \mid u_i \in \sigma, i \in (1, 2, \dots, N(\mathfrak{p}))\}$ un système complet de résidus de σ modulo $\mathfrak{f}\mathfrak{p}$ congrus à 1 modulo \mathfrak{f} . Lorsque $\mathfrak{p} \nmid \mathfrak{f}$, les nombres $u_i, i \in (1, 2, \dots, N(\mathfrak{p}))$, sont premiers avec \mathfrak{p} et on a

$$(11) \quad \prod_{C' \subset C} \varphi_{\mathfrak{f}\mathfrak{p}}(C')^\varepsilon = \prod_{i=1}^{N(\mathfrak{p})} \varphi^{(12)f'}(tu_i; \ell\mathfrak{p}).$$

Lorsque $(\mathfrak{p}, \mathfrak{f}) = (1)$, supposons que $u_1 \in \mathfrak{p}$; alors, les nombres $u_i, i \in (2, 3, \dots, N(\mathfrak{p}))$, sont premiers avec \mathfrak{p} ; on a

$$(12) \quad \varphi_{\mathfrak{f}}(C C_{\mathfrak{p}}^{-1}) = \varphi^{(12)f'}(tu_1; \ell\mathfrak{p}), \text{ et}$$

$$(13) \quad \prod_{C' \subset C} \varphi_{\mathfrak{f}\mathfrak{p}}(C')^\varepsilon = \prod_{i=2}^{N(\mathfrak{p})} \varphi^{(12)f'}(tu_i; \ell\mathfrak{p}).$$

Comme $(t, \ell) \in A(\mathcal{f})$, on a $\mathcal{f} = \{\alpha \in \sigma \mid \alpha t \in \ell\}$; par conséquent

$\{u_i t - t \mid i \in (1, 2, \dots, N(\mathfrak{p}))\}$ est un système complet de résidus de ℓ modulo $\ell\mathfrak{p}$; lorsque $\mathfrak{f} = (1)$, on a $t \in \ell$ et $u_1 t \in \ell\mathfrak{p}$, et $\{u_i t \mid i \in (2, 3, \dots, N(\mathfrak{p}))\}$ est un système complet de résidus non nuls de ℓ modulo $\ell\mathfrak{p}$. Nous déduisons alors de la proposition 1 § 1 les identités suivantes; lorsque $\mathfrak{f} \neq (1)$, on a

$$(14) \quad \prod_{i=1}^{N(\mathfrak{p})} \varphi^{(12)f'}(tu_i; \ell\mathfrak{p}) = \varphi^{(12)f'}(t; \ell) = \varphi_{\mathfrak{f}}(C)^{f'/f};$$

et, lorsque $\mathfrak{f} = (1)$, on a

$$(15) \quad \prod_{i=2}^{N(\mathfrak{p})} \varphi^{(12)f'}(tu_i; \ell\mathfrak{p}) = \Delta^P(\ell) \Delta^{-P}(\ell\mathfrak{p}).$$

Remarquons enfin que $f'/f = p$ ou 1 selon que $\mathfrak{f} \nmid \mathfrak{p}$ ou $\mathfrak{f} \in \mathfrak{p}$, en particulier $f'/f = p$ lorsque $(\mathfrak{f}, \mathfrak{p}) = (1)$. Le théorème 2, (i) résulte alors des identités (11) et (14), le théorème 2, (ii) des identités (12), (13) et (14), et le théorème 2, (iii) des identités (13) et (15).

Remarque. D'après le théorème 1 l'idéal de $H_{\mathfrak{f}}$ engendré par $\varphi_{\mathfrak{f}}(C)$ est indépendant de C et invariant par Galois. D'après le théorème 2, (ii) cet idéal est (1) si \mathfrak{f} est divisible par deux idéaux premiers distincts. D'autre part, soit

\mathfrak{p} un idéal premier de K et supposons que $\mathfrak{f} = \mathfrak{p}^n$, $n > 0$; l'idéal \mathfrak{p} se décompose dans $H_{\mathfrak{p}^n}$ en un produit $\prod_{i=1}^k \mathfrak{p}_i^n$ $[H_{\mathfrak{p}^n} : H_{(1)}]$, où les idéaux \mathfrak{p}_i , $i \in (1, 2, \dots, k)$, sont premiers dans $H_{\mathfrak{p}^n}$ et tous distincts; d'après [D] § 22 pp. 42-43, pour tout idéal \mathfrak{b} , le quotient $\Delta(\mathfrak{b})/\Delta(\mathfrak{b}\mathfrak{p})$ engendre l'idéal \mathfrak{p}^{12} ; si l'on note p^m , $0 < m \leq n$, le plus petit entier > 0 qui appartient à \mathfrak{p}^n , on déduit alors du théorème 2, (i) et (iii) que $(\varphi_{\mathfrak{p}^n}(c)) = \prod_{i=1}^k \mathfrak{p}_i^{12} p^m / \varepsilon$ avec $\varepsilon = e/e_{\mathfrak{p}^n}$.

Pour tout caractère χ du groupe $\text{Cl}(\mathfrak{f})$, notons $S(\chi)$ la somme $\sum_{C \in \text{Cl}(\mathfrak{f})} \bar{\chi}(C) \log |\varphi_{\mathfrak{f}}(C)|$. Nous déduisons du théorème 2 les propriétés suivantes des sommes $S(\chi)$.

Corollaire 1. Pour tout caractère $\chi \neq 1$ du groupe $\text{Cl}(\mathfrak{f})$, notons $\tilde{\chi}$ le caractère du groupe $\text{Cl}(\mathfrak{f}\mathfrak{p})$ qui, à toute classe $\tilde{C} \in \text{Cl}(\mathfrak{f}\mathfrak{p})$, fait correspondre le nombre $\chi(C)$, où $C \in \text{Cl}(\mathfrak{f})$ est l'unique classe qui contient \tilde{C} . Nous avons

$$f \cdot e_{\mathfrak{f}} \cdot S(\tilde{\chi}) = e_{\mathfrak{f}\mathfrak{p}} \cdot f' \cdot (1 - \bar{\chi}(\mathfrak{p})) S(\chi).$$

Corollaire 2. Pour tout caractère $\chi \neq 1$ du groupe $\text{Cl}(\mathfrak{f})$, notons f_{χ} le plus petit entier > 0 qui appartient au conducteur \mathfrak{f}_{χ} de χ , et χ' le caractère primitif du groupe $\text{Cl}(\mathfrak{f}_{\chi})$ associé à χ . Nous avons

$$e_{\mathfrak{f}_{\chi}} \cdot f_{\chi} \cdot S(\chi) = e_{\mathfrak{f}_{\chi}} \cdot f_{\chi} \cdot \prod_{\mathfrak{p}|\mathfrak{f}_{\chi}} (1 - \bar{\chi}'(\mathfrak{p})) \cdot S(\chi'),$$

où le produit est pris sur tous les idéaux premiers \mathfrak{p} qui divisent \mathfrak{f} .

Démonstration : on obtient l'identité du corollaire 1, en prenant le logarithme des valeurs absolues des deux membres des égalités du théorème 2, puis en sommant sur toutes les classes $C \in \text{Cl}(\mathfrak{f})$, et enfin en tenant compte :

- (i) Lorsque $\mathfrak{p} \nmid \mathfrak{f}$, de ce que $\chi(\mathfrak{p}) = 0$;
- (ii) Lorsque $(\mathfrak{p}, \mathfrak{f}) = (1)$ et $\mathfrak{f} \neq (1)$, de ce que

$$\sum_{C \in \text{Cl}(\mathfrak{f})} \bar{\chi}(C) \log |\varphi_{\mathfrak{f}}(CC_{\mathfrak{p}}^{-1})| = \sum_{C \in \text{Cl}(\mathfrak{f})} \bar{\chi}(CC_{\mathfrak{p}}) \log |\varphi_{\mathfrak{f}}(C)|,$$

d'où
$$\sum_{c \in \text{Cl}(\mathfrak{f})} \bar{\chi}(c) \log |\varphi_{\mathfrak{f}}(c)/\varphi_{\mathfrak{f}}(cc^{-1})| = (1 - \bar{\chi}(\mathfrak{p})) S(\chi) ;$$

(iii) Lorsque $\mathfrak{f} = (1)$, de ce que

$$|\Delta(\mathfrak{b})/\Delta(\mathfrak{b}\mathfrak{p})| = N(\mathfrak{p})^6 \varphi_{(1)}(c)/\varphi_{(1)}(cc^{-1})$$

pour tout $\mathfrak{b} \in \mathcal{C}^{-1}$, d'où

$$\sum_{c \in \text{Cl}(1)} \bar{\chi}(c) \log |\Delta(\mathfrak{b})/\Delta(\mathfrak{b}\mathfrak{p})| = (1 - \bar{\chi}(\mathfrak{p})) S(\chi) .$$

Le corollaire 2 se déduit du corollaire 1 par récurrence sur le nombre de facteurs premiers de l'idéal $\mathfrak{f}/\mathfrak{f}_{\chi}$.

Démontrons une dernière conséquence du théorème 2.

Corollaire 3. Soit H une extension abélienne non ramifiée de K . Posons $\ell = [H_{(1)}:H]$ et soit $\{\mathfrak{b}_1, \mathfrak{b}_2, \dots, \mathfrak{b}_{\ell}\}$ un système complet de représentants du groupe de classes $\text{Cl}(H_{(1)})/H$. Alors, pour tous idéaux \mathfrak{b} et \mathfrak{b}' de K , le produit

$$\rho = \prod_{j=1}^{\ell} \Delta(\mathfrak{b}\mathfrak{b}_j)/\Delta(\mathfrak{b}'\mathfrak{b}_j)$$

est une puissance e -ième dans H ; en particulier $\Delta(\mathfrak{b})/\Delta(\mathfrak{b}')$ est une puissance e -ième dans $H_{(1)}$.

Démonstration : notons $c_1, c_2, \dots, c_{\ell}$ et $c, c' \in \text{Cl}(1)$ les classes respectives des idéaux $\mathfrak{b}_1^{-1}, \mathfrak{b}_2^{-1}, \dots, \mathfrak{b}_{\ell}^{-1}$ et $\mathfrak{b}^{-1}, \mathfrak{b}'^{-1}$. Choisissons dans la classe cc^{-1} des idéaux premiers \mathfrak{p}_1 et \mathfrak{p}_2 , tels que $(N(\mathfrak{p}_1), N(\mathfrak{p}_2)) = 1$ et qui ne divisent pas 6; notons p_1 et p_2 les plus petits entiers > 0 qui appartiennent à \mathfrak{p}_1 et à \mathfrak{p}_2 . Pour $i = 1$ ou 2 , posons

$$\rho_i = \prod_{j=1}^{\ell} \prod_{\substack{c \in \text{Cl}(\mathfrak{p}_i) \\ c \subset c_j c_i}} \varphi_{\mathfrak{p}_i}(c) .$$

D'après le théorème 1, (i) le produit ρ_i appartient au corps $H_{\mathfrak{p}_i}$, et l'on déduit du théorème (1), (iii), pour tout automorphisme σ de l'extension $H_{\mathfrak{p}_i}/H$, l'identité $\rho_i^{\sigma} = \rho_i$; par conséquent $\rho_i \in H$. D'autre part, d'après le théorème 2,

(iii), nous avons

$$(16) \quad \prod_{j=1}^l \Delta^{p_i}(\mathfrak{t}_j) / \Delta^{p_i}(\mathfrak{t}_j \rho_i) = \rho_i^e ;$$

soient λ_1 et λ_2 des éléments de K tels que $\mathfrak{t}' = \lambda_i \rho_i \mathfrak{t}$, $i = 1$ ou 2 , et soient s_1 et s_2 des entiers tels que $s_1 p_1 + s_2 p_2 = 1$; on déduit de (16) l'identité

$$\rho = \lambda_1^{12 \ell p_1 s_1} \lambda_2^{12 \ell p_2 s_2} \rho_1^{e s_1} \rho_2^{e s_2} .$$

Par conséquent le produit ρ est une puissance e -ième dans H .

2.4. Expression des valeurs des fonctions $L(s, \chi)$ au point $s = 1$ à l'aide des invariants $\varphi_f(C)$.

Pour tout idéal entier \mathfrak{f} de K , et pour tout caractère χ de $\text{Cl}(\mathfrak{f})$, on définit la série L attachée à χ par

$$L(s, \chi) = \sum_{\mathfrak{a}} \chi(\mathfrak{a}) / N(\mathfrak{a})^s, \quad \text{Re}(s) > 1,$$

où la sommation porte sur tous les idéaux entiers \mathfrak{a} de K . Soit γ un élément de K tel que l'idéal $\gamma \mathfrak{f}$ soit entier et premier avec \mathfrak{f} , nous définissons une somme de Gauss $\tau(\chi)$ par

$$\tau(\chi) = \sum_{\lambda \bmod \mathfrak{f}} \overline{\chi}(\lambda \gamma \mathfrak{f}) \exp(2\pi i \text{Tr}(\lambda \gamma)),$$

où la sommation porte sur un système complet de résidus λ modulo \mathfrak{f} ; la somme $\tau(\chi)$ ne dépend que du caractère χ , et, lorsque χ est primitif, le module du quotient $\rho(\chi) = \tau(\chi) / N(\mathfrak{f})^{\frac{1}{2}}$ est 1; cf. [3] chap. II, § 4, pp. 139-140.

On trouvera la démonstration du résultat suivant dans [M] formules (4.35) p. 31, (5.41) p. 44, (15.8) et (15.9) p. 129, ou bien dans [S] formule (74) chap. II, § 2, p. 102, et th. 9 et 10 chap. II, § 4, pp. 144 et 149.

Théorème 3. Soient $\chi \neq 1$ un caractère de $\text{Cl}(\mathfrak{f})$, et $\chi' \neq 1$ le caractère primitif de $\text{Cl}(\mathfrak{f}_\chi)$ associé à χ .

$$(i) \quad \text{On a } (\sqrt{d}/2\pi) L(1, \chi') \tau(\chi') = -s(\chi') / 6f_\chi e_{\mathfrak{f}_\chi} .$$

(ii) Pour toute extension abélienne H de K, dont le conducteur est f , le produit $h_{H,H}^R$ du nombre de classes et du régulateur de H est donné par la formule :

$$h_{H,H}^R = h(e_H/e) \times \prod_{\chi \neq 1} [-S(\chi')/6f \cdot e_{\chi} \cdot \rho(\chi')],$$

où le produit est pris sur tous les caractères $\chi \neq 1$ de $Cl(H/K)$.

On déduit immédiatement du théorème 3, (i) et du corollaire 2 du théorème 2 le résultat suivant, dont le contenu est identique à celui de l'identité (64) du théorème 2, § 4, p. 117 de [R].

Corollaire. Pour tout caractère $\chi \neq 1$ de $Cl(f)$, on a

$$(-2\pi/6f\sqrt{d}) S(\chi) = e_{\chi} \tau(\chi') L(1, \chi') \prod_{p|f} (1 - \bar{\chi}'(p)).$$

§ 3. FORMULES POUR LE NOMBRE DE CLASSES DES EXTENSIONS ABELIENNES NON RAMIFIEES.

Pour toute extension abélienne non ramifiée H de K , nous construisons - à l'aide des valeurs singulières de la forme modulaire $\Delta(w)$ - des invariants $\delta_H(c)$ associés aux classes $c \in \text{Cl}(H/K)$. Lorsque c et c' parcourent le groupe $\text{Cl}(H/K)$, les quotients $\delta_H(c)/\delta_H(c')$ engendrent un sous-groupe Δ_H du groupe E_H des unités de H ; nous montrons (th. 4 § 3.2) que l'indice de Δ_H dans E_H est donné par la formule

$$(E_H : \Delta_H) = 12^{k-1} h_H^{k-2} e_{h_H}^k,$$

où $k = [H:K]$ et où h_H est le nombre de classes de H ; notre démonstration reprend celle de la formule (76) de [S] chap. II § 2 p. 105.

Soit c_0 la classe unité de $\text{Cl}(H/K)$. Les produits $\prod_{c \in \text{Cl}(H/K)} \delta_H(c)^{n(c)}$, où les entiers rationnels $n(c)$, $c \in \text{Cl}(H/K)$, sont tels que

$$\sum_{c \in \text{Cl}(H/K)} n(c) = 0 \quad \text{et} \quad \prod_{c \in \text{Cl}(H/K)} c^{n(c)} = c_0,$$

forment un sous-groupe V_H d'indice k du groupe Δ_H ; cf. proposition 5 § 3.2.

Nous montrons (th. 5 § 3.2) que les éléments de V_H sont des puissances (eh) -ièmes dans H . Par conséquent il existe un plus grand sous-groupe Ω_H de E_H , tel que $\Omega_H^{eh} = V_H$. Nous avons les inclusions

$$V_H \subset \Delta_H \subset \Omega_H \subset E_H,$$

cf. proposition 6, (i) § 3.2, et nous montrons (th. 6 § 3.2) que l'indice du groupe $\mu_{e_H} \Omega_H$ dans E_H est donné par la formule

$$(E_H : \mu_{e_H} \Omega_H) = \lambda h_H / [H_{(1)} : H],$$

où $\lambda = 12^{[H:K]-1} e_{e_H}$. On observera que le quotient $h_H / [H_{(1)} : H]$ est entier, puisque l'extension $H_{(1)}/H$ est abélienne et non ramifiée.

3.1. Les invariants $\delta(c)$ et $\delta_H(c)$.

Définition. Soit $c \in \text{Cl}(1)$ une classe absolue de K , et soient \mathfrak{f} un idéal de c^{-1} et β un élément de K tels que $\mathfrak{f}^h = (\beta)$. Comme dans [S] chap. II § 2, on pose

$$\delta(c) = (2\pi)^{-12h} \beta^{12} \Delta^h(\mathfrak{f});$$

le nombre complexe $\delta(c)$ ne dépend que de c .

Les invariants $\delta(c)$ possèdent les propriétés suivantes :

Proposition 3. Pour toutes classes c, c' et $c'' \in \text{Cl}(1)$, et pour tous idéaux $\mathfrak{f}, \mathfrak{f}'$ et \mathfrak{f}'' appartenant à c^{-1}, c'^{-1} et c''^{-1} :

(i) Le quotient $\Delta(\mathfrak{f})/\Delta(\mathfrak{f}')$ appartient à $H(1)$ et $\delta(c)/\delta(c')$ est une unité de $H(1)$;

(ii) On a $(\Delta(\mathfrak{f})/\Delta(\mathfrak{f}'))^{g(c'')} = \Delta(\mathfrak{f}\mathfrak{f}'')/\Delta(\mathfrak{f}'\mathfrak{f}'')$, et $(\delta(c)/\delta(c'))^{g(c'')} = \delta(cc'')/\delta(c'\mathfrak{f}'')$.

Démonstration (d'après [S] chap. II § 2 pp. 103-104) : choisissons dans la classe cc'^{-1} des idéaux premiers \mathfrak{p}_1 et \mathfrak{p}_2 , tels que $(N(\mathfrak{p}_1), N(\mathfrak{p}_2)) = 1$ et qui ne divisent pas 6 ; soient p_1 et p_2 les plus petits entiers > 0 qui appartiennent à \mathfrak{p}_1 et \mathfrak{p}_2 , et $\lambda_1, \lambda_2, \mu_1, \mu_2$ des éléments de K tels que $\mathfrak{p}_i^h = (\lambda_i)$ et $\mathfrak{f}\mathfrak{p}_i = \mu_i \mathfrak{f}'$ avec $i = 1$ ou 2 . D'après DEURING [D] § 22 pp. 42-43, les nombres complexes $(\alpha_i) = N(\mathfrak{p}_i)^{12} \Delta(\mathfrak{f}\mathfrak{p}_i)/\Delta(\mathfrak{f})$ appartiennent à $H(1)$ et $(\alpha_i) = \bar{\mu}_i^{12}$; par conséquent le quotient $\Delta(\mathfrak{f})/\Delta(\mathfrak{f}') = \Delta(\mathfrak{f})/\mu_1^{12} \Delta(\mathfrak{f}\mathfrak{p}_1)$ appartient à $H(1)$ et $\delta(c)/\delta(c') = \Delta^h(\mathfrak{f})/\lambda_1^{12} \Delta^h(\mathfrak{f}\mathfrak{p}_1)$ est une unité de $H(1)$.

Pour $i = 1$ ou 2 , posons

$$\rho_i(c) = \prod_{\substack{c \in \text{Cl}(\mathfrak{p}_i) \\ c \subset c}} \varphi_{\mathfrak{p}_i}(c)^e = \Delta^{p_i}(\mathfrak{f})/\Delta^{p_i}(\mathfrak{f}\mathfrak{p}_i);$$

cf. th. 2, (iii) § 2.3. Les produits $\rho_i(c)$ appartiennent à $H(1)$, et l'on déduit du th. 1, (iii) § 2.3, l'identité

$$(17) \quad \rho_i(c)^{g(c'')} = \rho_i(cc'') \quad \text{avec } c'' \in \text{Cl}(1).$$

Soient s_1 et s_2 des entiers rationnels tels que $s_1 p_1 + s_2 p_2 = 1$; on a

$$(18) \quad \begin{cases} \Delta(\mathfrak{f})/\Delta(\mathfrak{f}') = \rho_1(c)^{s_1} \rho_2(c)^{s_2} / \mu_1^{12p_1 s_1} \mu_2^{12p_2 s_2}, \text{ et} \\ \delta(c)/\delta(c') = \rho_1(c)^{hs_1} \rho_2(c)^{hs_2} / \lambda_1^{12p_1 s_1} \lambda_2^{12p_2 s_2} \end{cases}$$

Il résulte de (17) et (18), que $(\Delta(\mathfrak{f})/\Delta(\mathfrak{f}'))^{\mathfrak{g}(c'')} = \Delta(\mathfrak{f}'')/\Delta(\mathfrak{f}''')$, et

$$(\delta(c)/\delta(c'))^{\mathfrak{g}(c'')} = \delta(cc'')/\delta(c'c''). \text{ La proposition 3 est démontrée.}$$

Soit maintenant H une extension abélienne non ramifiée de K . Pour toute classe $c \in \text{Cl}(H/K)$, posons

$$\delta_H(c) = \prod_{\substack{\tilde{c} \in \text{Cl}(1) \\ \tilde{c} \subset c}} \delta(\tilde{c}),$$

où le produit est pris sur toutes les classes absolues $\tilde{c} \in \text{Cl}(1)$ contenues dans c . Les invariants $\delta_H(c)$ possèdent les propriétés suivantes.

Proposition 4. Pour toutes classes c , c' et $c'' \in \text{Cl}(H/K)$, et pour toutes classes \tilde{c} et $\tilde{c}' \in \text{Cl}(1)$, telles que $\tilde{c} \subset c$ et $\tilde{c}' \subset c'$:

- (i) On a $N_{H(1)/H}(\delta(\tilde{c}')/\delta(\tilde{c})) = \delta_H(c')/\delta_H(c)$;
- (ii) Le quotient $\delta_H(c')/\delta_H(c)$ est une unité de H ;
- (iii) On a $(\delta_H(c')/\delta_H(c))^{\mathfrak{g}(c'')} = \delta_H(c'c'')/\delta_H(cc'')$.

Démonstration : notons c_0 la classe unité de $\text{Cl}(H/K)$. D'après la proposition 3, (ii) et le th. 1, (iii) § 2.3, on a

$$N_{H(1)/H}(\delta(\tilde{c}')/\delta(\tilde{c})) = \prod_{\substack{\tilde{c}'' \in \text{Cl}(1) \\ \tilde{c}'' \subset c_0}} (\delta(\tilde{c}')/\delta(\tilde{c}))^{\mathfrak{g}(\tilde{c}'')} = \prod_{\substack{\tilde{c}'' \in \text{Cl}(1) \\ \tilde{c}'' \subset c_0}} (\delta(\tilde{c}'\tilde{c}'')/\delta(\tilde{c}\tilde{c}'')) ;$$

d'où $N_{H(1)/H}(\delta(\tilde{c}')/\delta(\tilde{c})) = \delta_H(c')/\delta_H(c)$, ce qui prouve (i). Les assertions (ii) et (iii) sont des conséquences immédiates de (i) et des assertions (i) et (ii) de la proposition 3.

3.2. Formules pour le nombre de classes.

Soit H une extension abélienne non ramifiée de K . On pose $k = [H:K]$ et $h = [H_{(1)}:H]$; on note $c_0 \in \text{Cl}(H/K)$ et $\tilde{c}_0 \in \text{Cl}(1)$ les classes unités des groupes $\text{Cl}(H/K)$ et $\text{Cl}(1)$; on note $c_1, c_2, \dots, c_{k-1} \in \text{Cl}(H/K)$ les éléments de $\text{Cl}(H/K)$ différents de c_0 , et $\tilde{c}_1, \tilde{c}_2, \dots, \tilde{c}_{h-1} \in \text{Cl}(1)$ les éléments de $\text{Cl}(H_{(1)}/H)$ différents de \tilde{c}_0 .

Définition. D'après la proposition 4, (ii), les quotients

$\delta_{H,i} = \delta_H(c_i)/\delta_H(c_0)$, $i \in (1, 2, \dots, k-1)$, engendrent un sous-groupe Δ_H de E_H .

Démonstrons le résultat suivant (cf. [S] chap. II § 2 p. 105 Formule (76)).

Théorème 4. Les unités $\delta_{H,i}$, $i \in (1, 2, \dots, k-1)$, forment un système maximal d'unités indépendantes de H . Le groupe Δ_H est donc un sous-groupe d'indice fini de E_H ; cet indice est donné par la formule

$$(E_H : \Delta_H) = 12^{k-1} h^{k-2} e^k h_H.$$

Démonstration : soit W le déterminant de la matrice carrée d'ordre $k-1$ et de terme général

$$\log |\delta_{H,i}^{g(c_j)}| = \log |\delta_H(c_i c_j)| - \log |\delta_H(c_j)|,$$

où $i \in (1, 2, \dots, k-1)$ et $j \in (1, 2, \dots, k-1)$. Le déterminant W a la forme d'un déterminant de groupe et par conséquent (cf. [S] chap. II § 2 p. 102) on a

$$|W| = \left| \prod_{\chi \neq 1} \sum_{i=0}^{k-1} \bar{\chi}(c_i) \log |\delta_H(c_i)| \right|,$$

où le produit est pris sur tous les caractères $\chi \neq 1$ de $\text{Cl}(H/K)$. Comme

$$\delta(c) = \prod_{\substack{\tilde{c} \in \text{Cl}(1) \\ \tilde{c} \subset c}} \delta(\tilde{c}),$$

nous avons

$$(19) \quad \sum_{i=0}^{k-1} \bar{\chi}(c_i) \log |\delta_H(c_i)| = \sum_{\tilde{c} \in \text{Cl}(1)} \bar{\chi}(\tilde{c}) \log |\delta(\tilde{c})|.$$

Vu que $|\delta(\tilde{c})| = \varphi_{(1)}^h(\tilde{c})$, on déduit de (19) l'identité

$$(20) \quad \sum_{i=0}^{k-1} \bar{\chi}(c_i) \log |\delta_H(c_i)| = h S(\chi).$$

Substituons l'identité (20) dans la formule du th.3, (ii) § 2.4, il vient

$$h_{H/R_H} = (e_H/e) \prod_{\chi \neq 1} \sum_{i=0}^{k-1} \bar{\chi}(c_i) \log |\delta_H(c_i)| / (6e)^{k-1} h^{k-2}.$$

Par conséquent le déterminant W est $\neq 0$; les unités $\delta_{H,i}$, $i \in (1, 2, \dots, k-1)$ forment un système maximal d'unités indépendantes de H ; et le quotient

$e_H 2^{k-1} |W|/R_H$, qui n'est autre que l'indice de Δ_H dans E_H , est égal à $12^{k-1} h^{k-2} e^k h_H$. Le th. 4 est démontré.

Définition. Soit V_H le sous-groupe de Δ_H , formé des produits $\prod_{i=1}^{k-1} \delta_{H,i}^{n_i}$,

où les entiers rationnels n_i , $i \in (1, 2, \dots, k-1)$, sont tels que $\prod_{i=1}^{k-1} c_i^{n_i} = c_0$.

Proposition 5. L'indice de V_H dans Δ_H est égal à k .

Démonstration : d'après le th. 4 les unités $\delta_{H,i}$, $i \in (1, 2, \dots, k-1)$, sont multiplicativement indépendantes; par conséquent l'application

$$\prod_{i=1}^{k-1} \delta_{H,i}^{n_i} \mapsto \prod_{i=1}^{k-1} c_i^{n_i}$$

définit un homomorphisme de Δ_H dans $Cl(H/K)$. Cet homomorphisme est surjectif, son noyau V_H est un sous-groupe d'indice $k = \text{card}(Cl(H/K))$ de Δ_H ; C.Q.F.D.

Démontrons maintenant le résultat suivant :

Théorème 5. Tout élément de V_H est une puissance (eh) -ième dans H .

Démonstration : soit δ un élément de V_H , et soient n_i , $i \in (1, 2, \dots, k-1)$, des entiers rationnels tels que $\prod_{i=1}^{k-1} c_i^{n_i} = c_0$ et $\delta = \prod_{i=1}^{k-1} \delta_{H,i}^{n_i}$. Pour tout $i \in (1, 2, \dots, k-1)$ soit α_i un idéal qui appartient à c_i^{-1} ; le produit $\prod_{i=1}^{k-1} \alpha_i^{n_i}$ appartient à c_0 , et, par conséquent, on peut trouver un élément α de K tel que $\prod_{i=1}^{k-1} \alpha_i^{n_i} = (\alpha)$. Soient $\mathfrak{t}_0, \mathfrak{t}_1, \dots, \mathfrak{t}_{\ell-1}$ des idéaux qui appartiennent aux classes

$\tilde{c}_0, \tilde{c}_1, \dots, \tilde{c}_{\ell-1}$; nous avons

$$\delta = \alpha^{12h} \prod_{i=1}^{k-1} \prod_{j=0}^{\ell-1} \Delta_i^{n_i} (\alpha_i \mathfrak{t}_j) / \Delta_i^{n_i} (\mathfrak{t}_j);$$

il résulte alors du corollaire 3 du th. 2, (iii) § 2.3 que le nombre $\delta \in V_H$ est une puissance (eh)-ième dans H . Le th. 5 est démontré.

Définition. On déduit du th. 5 l'existence d'un plus grand sous-groupe Ω_H de E_H tel que $\Omega_H^{eh} = V_H$.

Démontrons les propriétés suivantes des groupes V_H , Δ_H et Ω_H .

Proposition 6.

(i) Les groupes V_H , Δ_H et Ω_H sont des sous-groupes d'indices finis de E_H ;

(ii) Pour tout automorphisme σ de H/K , on a $V_H^\sigma = V_H$, $\Delta_H^\sigma = \Delta_H$ et $\Omega_H^\sigma = \Omega_H$;

(iii) On a $V_H = \Omega_H^{eh} \subset \Delta_H \subset \Omega_H \subset E_H$.

Démonstration : l'assertion (i) résulte immédiatement du th. 4 et de la proposition 5. L'assertion (ii) est essentiellement triviale. Pour toute classe $c \in \text{Cl}(H/K)$, on a $c^h = c_0$, par conséquent $\delta_H(c)^h / \delta_H(c_0)^h$ est un élément de V_H ; d'où $\Delta_H^h \subset \Omega_H^{eh} \subset \Omega_H^h$, et par conséquent $\Delta_H \subset \Omega_H$; les autres inclusions de l'assertion (iii) sont triviales.

Enfin, déterminons l'indice $(E_H : \mu_e \Omega_H)$.

Théorème 6. L'indice du groupe $\mu_e \Omega_H$ dans E_H est donné par la formule

$$(E_H : \mu_e \Omega_H) = \lambda h_H / [H(\zeta) : H],$$

avec $\lambda = 12^{[H:K]-1} e/e_H$.

Démonstration : d'après le th. 4, le groupe Δ_H est engendré par $k-1$ unités indépendantes ; par conséquent V_H , sous-groupe d'indice fini de Δ_H , est également engendré par $k-1$ unités indépendantes. Il en résulte que nous pouvons trouver un sous-groupe A de Ω_H , tel que $A^{eh} = V_H$, $A \cap \mu_e = \{1\}$ et $\Omega_H = \mu_e A$ où g est le nombre de racines de l'unité qui appartiennent à Ω_H . Nous avons alors

$$(\mu_{e_H} \Omega_H : V_H) = e_H(A : V_H) = e_H(A : A^{eh}) = e_H(eh)^{k-1} ;$$

et la formule du th. 6 résulte de la détermination des indices $(E_H : \Delta_H)$ et $(\Delta_H : V_H)$ effectuée dans le th. 4 et la proposition 5.

§ 4. UNITES DANS LES EXTENSIONS ABELIENNES RAMIFIEES.

Nous nous intéressons maintenant aux extensions abéliennes H de K , dont le conducteur est un idéal entier $\mathfrak{f} \neq (1)$; nous avons $e_H \mid 12f$, où e_H est l'ordre du groupe des racines de l'unité de H et où f est le plus petit entier > 0 qui appartient à \mathfrak{f} ; cf. lemme 7 § 4.1.

Pour toute classe $C \in \text{Cl}(H/K)$, posons

$$\varphi_H(C) = \prod_{\substack{\tilde{C} \in \text{Cl}(\mathfrak{f}) \\ \tilde{C} \subset C}} \varphi_{\mathfrak{f}}(\tilde{C}).$$

Lorsque C et C' parcourent $\text{Cl}(H/K)$, les quotients $\varphi_H(C)/\varphi_H(C')$ engendrent un sous-groupe Φ_H de E_H . Pour toute classe $C \in \text{Cl}(H/K)$, soit $\mathfrak{a}(C)$ un idéal entier, premier avec $12f$, qui appartient à C ; le résidu de $N(\mathfrak{a}(C))$ modulo e_H ne dépend que de C , cf. lemme 5 § 4.1; nous notons V_H le sous-groupe de Φ_H formé des produits

$$\prod_{C \in \text{Cl}(H/K)} \varphi_H(C)^{n(C)},$$

où les entiers rationnels $n(C)$, $C \in \text{Cl}(H/K)$, sont tels que

$$\sum_{C \in \text{Cl}(H/K)} n(C) = 0 \quad \text{et} \quad \sum_{C \in \text{Cl}(H/K)} n(C)N(\mathfrak{a}(C)) \equiv 0 \pmod{e_H}.$$

Nous démontrons (th. 7 § 4.3 et th. 8 § 4.4) que les éléments de V_H sont des puissances d'ordre $e_{\mathfrak{f}}f$ dans H . Par conséquent, il existe un plus grand sous-groupe Ω_H de E_H , tel que $\Omega_H^{e_{\mathfrak{f}}f} = V_H$. Nous avons les inclusions

$$V_H \subset \Phi_H \quad \text{et} \quad \Phi_H^{12/e} \subset \Omega_H \subset E_H,$$

cf. proposition 13 § 4.4 et proposition 16, (ii) § 4.5.

Le groupe Ω_H n'est pas, en général, un sous-groupe d'indice fini de E_H . Toutefois, lorsque \mathfrak{f} est puissance d'un idéal premier \mathfrak{p} de K , notons $D(\mathfrak{p})$ le corps de décomposition de \mathfrak{p} dans $H_{(1)}$; nous démontrons (corollaire 2 du th. 10 § 4.6) que Ω_H est un sous-groupe d'indice fini du groupe $E_H/D(\mathfrak{p})\Omega_H$ formé des unités de H dont la norme, relativement à l'extension $H/D(\mathfrak{p})\Omega_H$, est une racine de l'unité.

4.1. Racines de l'unité.

Soient m un entier > 0 et n un multiple de m . L'automorphisme d'Artin de $K(\mu_m)/K$ associé à un idéal entier α , premier avec n , est défini par $z \mapsto z^{N(\alpha)}$, où $z \in \mu_m$. Ceci nous permet, à l'aide des résultats généraux de théorie du corps de classes, de caractériser l'inclusion $\mu_m \subset H$, lorsque H est une extension abélienne de K ; énonçons ce critère sous les deux formes suivantes :

Lemme 5. Pour que $\mu_m \subset H$, il faut et il suffit que tout idéal entier α , premier avec n , qui appartient à la classe unité de $Cl(H/K)$, vérifie $N(\alpha) \equiv 1 \pmod{m}$.

Lemme 6. Lorsque μ_m est l'ensemble des racines de l'unité qui appartiennent à H , l'idéal (m) est engendré par les nombres $N(\alpha) - 1$, lorsque α parcourt l'ensemble des idéaux entiers, premiers avec n , qui appartiennent à la classe unité de $Cl(H/K)$.

Une conséquence du lemme 5 est le résultat suivant :

Lemme 7. Soient f le conducteur de H/K , et f le plus petit entier > 0 qui appartient à f ; alors $e_H \mid 12f$.

Démonstration : il nous suffit de prouver le lemme lorsque $H = H(f)$. Soit p un nombre premier, et soient respectivement a et b les plus grands entiers ≥ 0 tels que $\mu_{p^a} \subset H(f)$ et $p^b \mid f$. D'après le lemme 5, on a $\mu_{p^a} \subset H_{(p^a)}$; et comme

$$H_{(p^a)} \cap H_{(f)} = H_{(p^{\inf(a,b)})} \subset H_{(p^b)},$$

on en déduit $\mu_{p^a} \subset H_{(p^b)}$. Par conséquent, d'après le lemme 5, pour tout entier rationnel α , premier avec p , tel que $\alpha \equiv 1 \pmod{p^b}$, nous avons $\alpha^2 \equiv 1 \pmod{p^a}$.

Il en résulte :

- (i) Si $p \neq 2$ et $p \neq 3$, on a $a \leq b$; d'où $p^a \mid f$.
- (ii) Si $p = 3$, dans le cas où $b > 0$ on a $a \leq b$, et dans le cas où $b = 0$ on a $a = 0$ ou 1 ; d'où $p^a \mid 3f$.
- (iii) Si $p = 2$, dans le cas où $b > 1$ on a $a \leq b+1$, et dans le cas où

$b \in \{0, 1\}$ on a $a = 1$ ou 2 ; d'où $p^a | 4f$.

Finalement, pour tout nombre premier p , l'entier p^a divise $12f$; ce qui prouve que $e_{H(f)} | 12f$ et démontre le lemme 7.

4.2. Valeurs singulières de certaines fonctions thêta réduites.

Pour tout idéal \mathfrak{t} de K , posons

$$g_2(\mathfrak{t}) = 60 \sum_{\substack{\beta \in \mathfrak{t} \\ \beta \neq 0}} \beta^{-4} \quad \text{et} \quad g_3(\mathfrak{t}) = 140 \sum_{\substack{\beta \in \mathfrak{t} \\ \beta \neq 0}} \beta^{-6} ;$$

le nombre $\Delta(\mathfrak{t}) = g_2^3(\mathfrak{t}) - 27g_3^2(\mathfrak{t})$ est $\neq 0$, et l'on pose $j(\mathfrak{t}) = 1728 g_2^3(\mathfrak{t}) / \Delta(\mathfrak{t})$.

Suivant que $e = 2, 4$ ou 6 notons $\tau(t, \mathfrak{t})$ l'expression $g_2(\mathfrak{t})g_3(\mathfrak{t})\mathcal{P}(t, \mathfrak{t}) / \Delta(\mathfrak{t})$, $\mathcal{P}^2(t, \mathfrak{t}) / g_2(\mathfrak{t})$ ou $\mathcal{P}^3(t, \mathfrak{t}) / g_3(\mathfrak{t})$, avec

$$\mathcal{P}(t, \mathfrak{t}) = t^{-2} + \sum_{\substack{\beta \in \mathfrak{t} \\ \beta \neq 0}} ((t+\beta)^{-2} - \beta^{-2}) , \quad t \in \mathbb{C} - \mathfrak{t} .$$

Les fonctions $t \mapsto \mathcal{P}(t, \mathfrak{t})$ et $t \mapsto \tau(t, \mathfrak{t})$ sont elliptiques sur le tore \mathbb{C}/\mathfrak{t} ; cf. HASSE [H1]I.

Définitions. Pour toute classe $C \in \text{Cl}(\mathfrak{t})$, on pose $j(C) = j(\mathfrak{t})$ où $\mathfrak{t} \in C^{-1}$. Pour toute classe $C \in \text{Cl}(\mathfrak{q})$ avec $\mathfrak{q} \neq (1)$, on pose $\tau(C) = \tau(t, \mathfrak{t})$, où $(t, \mathfrak{t}) \in A(\mathfrak{q})$ est tel que $C_{(t, \mathfrak{t})} = C$; cf. § 2.2. D'après [H1]I, les invariants $j(C)$ et $\tau(C)$ ne dépendent que de $C \in \text{Cl}(\mathfrak{q})$.

Rappelons les résultats fondamentaux suivants, cf. [H1]I.

Proposition 7.

(i) Pour toutes classes C et $C' \in \text{Cl}(1)$, on a $H_{(1)} = K(j(C))$ et $j(C)^{g(C')} = j(CC')$.

(ii) Pour toutes classes C et $C' \in \text{Cl}(\mathfrak{q})$ avec $\mathfrak{q} \neq (1)$, on a $H_{\mathfrak{q}} = H_{(1)}(\tau(C))$ et $\tau(C)^{g(C')} = \tau(CC')$.

Soit \mathfrak{a} un idéal entier de K . Nous posons

$$\theta^{(12)}(t, \mathfrak{t}; \mathfrak{a}) = \theta^{(12)}(t; \mathfrak{t}\mathfrak{a}^{-1}) / \theta^{(12)}(t; \mathfrak{t})^{N(\mathfrak{a})} ;$$

démonstrons les résultats suivants :

Lemme 8.

- (i) Pour tout $\lambda \in K^*$, on a $\theta^{(12)}(\lambda t, \lambda t; \alpha) = \theta^{(12)}(t, t; \alpha)$;
- (ii) La fonction $t \mapsto \theta^{(12)}(t, t; \alpha)$ est elliptique sur le tore \mathcal{C}/\mathfrak{t} ;
- (iii) Pour tous couples équivalents (t, t) et $(t', t') \in A(\mathfrak{f})$ avec $\mathfrak{f} \neq (1)$,

on a

$$\theta^{(12)}(t, t; \alpha) = \theta^{(12)}(t', t'; \alpha) .$$

Démonstration : l'assertion (i) résulte du lemme 1 § 1. Posons

$\mathfrak{W}(t, t') = 24\pi i \bar{t}t'/a(\mathfrak{t})$, où $a(\mathfrak{t})$ est l'aire de \mathcal{C}/\mathfrak{t} , cf. § 1. Il résulte de la formule (2) § 1 que, pour tout $\beta \in \mathfrak{t}$, on a

$$\theta^{(12)}(t+\beta; \mathfrak{t}) = \exp(\mathfrak{W}(\beta, t) + \mathfrak{W}(\beta, \beta)/2) \theta^{(12)}(t; \mathfrak{t}) ,$$

et

$$\theta^{(12)}(t+\beta; \mathfrak{t}\alpha^{-1}) = \exp(N(\alpha)(\mathfrak{W}(\beta, t) + \mathfrak{W}(\beta, \beta)/2)) \theta^{(12)}(t; \mathfrak{t}\alpha^{-1}) ;$$

d'où $\theta^{(12)}(t+\beta, \mathfrak{t}; \alpha) = \theta^{(12)}(t, \mathfrak{t}; \alpha)$, ce qui est l'assertion (ii). On déduit l'assertion (iii) de (i) et (ii), comme on a déduit le lemme 3 § 2.2 des lemmes 1 et 2 § 1.

Définitions. Pour toute classe $C \in Cl(\mathfrak{f})$ avec $\mathfrak{f} \neq (1)$, posons

$$\theta(C; \alpha) = \theta^{(12)}(t, \mathfrak{t}; \alpha) ,$$

où $(t, \mathfrak{t}) \in A(\mathfrak{f})$ est tel que $C_{(t, \mathfrak{t})} = C$. D'après le lemme 8, (iii), pour α fixé, l'invariant $\theta(C; \alpha)$ ne dépend que de $C \in Cl(\mathfrak{f})$.

Pour tout idéal entier \mathfrak{g} de K , soit $T(X, \mathfrak{t}; \mathfrak{g})$ le polynôme ainsi défini :

(i) On pose $T(X, \mathfrak{t}; (1)) = 1$

(ii) Si $\mathfrak{g} \neq (1)$, on pose $T(X, \mathfrak{t}; \mathfrak{g}) = \prod (X - \tau(C))$, où le produit est pris sur toutes les classes $C \in Cl(\mathfrak{g})$ contenues dans la classe absolue de $\mathfrak{g}\mathfrak{t}^{-1}$.

D'après [H1]II, Satz 16 p. 83, nous avons le résultat suivant :

Proposition 8. La fonction $T(X, \mathfrak{t}; \mathfrak{g})$ est un polynôme en X et $j(\mathfrak{t})$, dont les coefficients appartiennent à K et ne dépendent pas de \mathfrak{t} .

Définition. Pour toute classe $C \in \text{Cl}(\mathfrak{f})$ avec $\mathfrak{f} \neq (1)$, posons

$$T(C; \mathfrak{q}) = T(\tau(t, \mathfrak{t}), \mathfrak{t}; \mathfrak{q}),$$

où $(t, \mathfrak{t}) \in A(\mathfrak{f})$ est tel que $C_{(t, \mathfrak{t})} = C$. D'après les propositions 7 et 8, pour \mathfrak{q} fixé, l'invariant $T(C; \mathfrak{q})$ ne dépend que de $C \in \text{Cl}(\mathfrak{f})$, et l'on a le résultat suivant :

Corollaire. Pour toutes classes C et $C' \in \text{Cl}(\mathfrak{f})$ avec $\mathfrak{f} \neq (1)$, l'invariant $T(C; \mathfrak{q})$ appartient à $H_{\mathfrak{f}}$ et l'on a $T(C; \mathfrak{q})^{\mathfrak{g}(C')} = T(CC'; \mathfrak{q})$.

Définition. Posons $L(\mathfrak{t}; \alpha) = \Delta(\mathfrak{t}\alpha^{-1})/\Delta(\mathfrak{t})M(\mathfrak{t})^{1-N(\alpha)}$, avec $M(\mathfrak{t}) = 2^{30}3^{24}/j^2(\mathfrak{t})(j(\mathfrak{t}) - 1728)^3$ si $e = 2$, et $M(\mathfrak{t}) = 1$ ou $-(27)^{-1}$ suivant que $e = 4$ ou 6 .

Remarque. D'après les propositions 3 § 3.1 et 7, l'invariant $L(\mathfrak{t}; \alpha)$ appartient à $H_{(1)}$; il ne dépend que de la classe absolue de \mathfrak{t} , et l'on a $L(\mathfrak{t}; \alpha)^{\mathfrak{g}(c')} = L(\mathfrak{t}\mathfrak{t}'; \alpha)$ pour toute classe $c' \in \text{Cl}(1)$ et tout idéal \mathfrak{t}' de \mathfrak{e}'^{-1} .

Démontrons le résultat suivant :

Proposition 9. Lorsque $(\alpha, 6) = (1)$, on a l'identité

$$\theta^{(12)}(t, \mathfrak{t}; \alpha) = L(\mathfrak{t}; \alpha) \prod_{\mathfrak{q}|\alpha} T(\tau(t, \mathfrak{t}), \mathfrak{t}; \mathfrak{q})^{12},$$

où le produit est pris sur tous les diviseurs entiers \mathfrak{q} de α .

Démonstration : la fonction $t \mapsto F(t, \mathfrak{t}; \mathfrak{q}) = T(\tau(t, \mathfrak{t}), \mathfrak{t}; \mathfrak{q})$ est elliptique sur le tore $\mathfrak{C}/\mathfrak{q}$, et on vérifie qu'elle admet pour zéros les points proprement de \mathfrak{q} -division de $\mathfrak{C}/\mathfrak{t}$ (c'est-à-dire les points $t \in \mathfrak{C}$, tels que $\mathfrak{q} = \{\alpha \in \sigma \mid \alpha t \in \mathfrak{t}\}$) chacun d'ordre $e_{\mathfrak{q}}$, et pour pôles les points de \mathfrak{t} chacun d'ordre $e_{\mathfrak{q}}\mu(\mathfrak{q})$ (où $\mu(\mathfrak{q})$ désigne le nombre d'éléments inversibles de l'anneau σ/\mathfrak{q}). Supposons que $(\alpha, 6) = 1$, pour tous les diviseurs entiers \mathfrak{q} de α on a alors $e_{\mathfrak{q}} = 1$; par conséquent la fonction

$$t \mapsto G(t, \mathfrak{t}; \alpha) = \prod_{\mathfrak{q}|\alpha} F(t, \mathfrak{t}; \mathfrak{q})$$

admet pour zéros les points de $\mathfrak{t}\alpha^{-1}$ qui n'appartient pas à \mathfrak{t} , chacun d'ordre 1,

et pour pôles les points de \mathfrak{t} , chacun d'ordre $N(\alpha) - 1 = \sum_{\sigma_j | \alpha} \mu(\sigma_j)$; il en résulte que les fonctions elliptiques $t \mapsto \theta^{(12)}(t, \mathfrak{t}; \alpha)$ et $t \mapsto G^{12}(t, \mathfrak{t}; \alpha)$ admettent mêmes zéros et mêmes pôles, elles sont donc proportionnelles. On vérifie, en comparant leurs comportements lorsque $t \rightarrow 0$, que $\theta^{(12)}(t, \mathfrak{t}; \alpha) / G^{12}(t, \mathfrak{t}; \alpha) = L(\mathfrak{t}; \alpha)$; C.Q.F.D.

A l'aide du corollaire de la proposition 8 et de la remarque faite plus haut, on déduit de la proposition 9 le résultat suivant :

Corollaire. Pour toutes classes C et $C' \in Cl(\mathfrak{f})$ avec $\mathfrak{f} \neq (1)$, l'invariant $\theta(C; \alpha)$ appartient à $H_{\mathfrak{f}}$ et l'on a $\theta(C; \alpha)^{g(C')} = \theta(CC'; \alpha)$.

Les invariants $\theta(C; \alpha)$ sont des racines f -ièmes des invariants $\varphi_{\mathfrak{f}}(C)$; plus précisément :

Proposition 10. Lorsque $(\alpha, 6\mathfrak{f}) = (1)$, pour toute classe $C \in Cl(\mathfrak{f})$ avec $\mathfrak{f} \neq (1)$, nous avons

$$\varphi_{\mathfrak{f}}(CC_{\alpha}) / \varphi_{\mathfrak{f}}(C)^{N(\alpha)} = \theta(C; \alpha)^f,$$

où $C_{\alpha} \in Cl(\mathfrak{f})$ est la classe de α .

Démonstration : soit $(t, \mathfrak{t}) \in A(\mathfrak{f})$ un couple tel que $C_{(t, \mathfrak{t})} = C$. Nous avons

$$\varphi^{(12)}(t; \mathfrak{t}\alpha^{-1}) = \exp(-N(\alpha)\mathfrak{H}(t, t)/2) \theta^{(12)}(t; \mathfrak{t}\alpha^{-1}),$$

et

$$\varphi^{(12)}(t; \mathfrak{t}) = \exp(-\mathfrak{H}(t, t)/2) \theta^{(12)}(t; \mathfrak{t}).$$

D'où $\theta^f(t, \mathfrak{t}; \alpha) = \varphi^{(12)f}(t; \mathfrak{t}\alpha^{-1}) / \varphi^{(12)fN(\alpha)}(t; \mathfrak{t}) = \varphi_{\mathfrak{f}}(CC_{\alpha}) / \varphi_{\mathfrak{f}}(C)^{N(\alpha)}$; C.Q.F.D.

4.3. Notations.

Introduisons les notations suivantes que nous utiliserons dans les §§ 4.4 à 4.6.

Soient \mathfrak{f} et \mathfrak{f}' deux idéaux entiers de K tels que $\mathfrak{f} \mid \mathfrak{f}'$ et $\mathfrak{f} \neq (1)$; soient H et H' deux extensions abéliennes de K , telles que $H \subset H_{\mathfrak{f}}$ et $H \subset H' \subset H_{\mathfrak{f}'}$. Nous appelons f et f' les plus petits entiers > 0 qui appartiennent à \mathfrak{f} et \mathfrak{f}' ; nous posons $k = \deg(H/K)$ et $k' = \deg(H'/K)$.

Nous notons g le plus grand diviseur de $e_{\mathfrak{f}} f$ tel que $\exp(2\pi i/g) \in H$; d'après le lemme 7, nous avons $g \mid e_H \mid 2f$.

Pour toute classe $C \in \text{Cl}(H/K)$ (resp. $C' \in \text{Cl}(H'/K)$), soit $\alpha(C)$ (resp. $\alpha(C')$) un idéal entier, premier avec $2f$ (resp. $2f'$), qui appartient à C (resp. C'); d'après le lemme 5, le résidu de $N(\alpha(C))$ modulo e_H (resp. $N(\alpha(C'))$ modulo $e_{H'}$) ne dépend que de C (resp. C'); en particulier, pour toutes classes $C \in \text{Cl}(H/K)$ et $C' \in \text{Cl}(H'/K)$ telles que $C' \subset C$, nous avons $N(\alpha(C)) \equiv N(\alpha(C')) \pmod{e_H}$. Pour tout idéal entier α de K , premier avec $2f$, nous notons $C'_{\alpha} \in \text{Cl}(H'/K)$ la classe de α .

Nous notons respectivement $C_0 \in \text{Cl}(H/K)$ et $C'_0 \in \text{Cl}(H'/K)$ les classes unités des groupes $\text{Cl}(H/K)$ et $\text{Cl}(H'/K)$; nous notons $C_1, C_2, \dots, C_{k-1} \in \text{Cl}(H/K)$ les éléments de $\text{Cl}(H/K)$ différents de C_0 , et $C'_1, C'_2, \dots, C'_{k'-1} \in \text{Cl}(H'/K)$ les éléments de $\text{Cl}(H'/K)$ différents de C'_0 .

4.4. Racines $(e_{\mathfrak{f}} f)$ -ièmes des invariants $\varphi_{\mathfrak{f}}(C)$.

Lemme 9. Pour toutes classes $C \in \text{Cl}(H/K)$ et $\tilde{C} \in \text{Cl}(\mathfrak{f})$ telles que $\tilde{C} \subset C$, nous avons

$$N_{H_{\mathfrak{f}}/H}(\varphi_{\mathfrak{f}}(\tilde{C})) = \prod_{\substack{C' \in \text{Cl}(\mathfrak{f}) \\ C' \subset C}} \varphi_{\mathfrak{f}}(C').$$

Démonstration : nous savons que

$$N_{H_f/H}(\varphi_f(\tilde{C})) = \prod_{\substack{C' \in \text{Cl}(f) \\ C' \subset C_0}} \varphi_f(\tilde{C})^{\varepsilon(C')};$$

d'où, d'après le th. 1, (iii) § 2.3 :

$$N_{H_f/H}(\varphi_f(\tilde{C})) = \prod_{\substack{C' \in \text{Cl}(f) \\ C' \subset C_0}} \varphi_f(\tilde{C}C') = \prod_{\substack{C'' \in \text{Cl}(f) \\ C'' \subset C}} \varphi_f(C''); \quad \text{C.Q.F.D.}$$

Nous supposons dorénavant que $H = H_f$ et $H' = H_{f'}$.

Définitions. D'après le th. 1, (ii) § 2.3, les quotients

$$\varphi_{f,i} = \varphi_f(C_i) / \varphi_f(C_0), \quad i \in (1, 2, \dots, k-1),$$

engendrent un sous-groupe Φ_f de E_{H_f} .

Soit V_f le sous-groupe de Φ_f formé des produits $\prod_{i=1}^{k-1} \varphi_{f,i}^{n_i}$, où les entiers rationnels n_i , $i \in (1, 2, \dots, k-1)$, sont tels que

$$\sum_{i=1}^{k-1} n_i [N(\alpha(C_i)) - 1] \equiv 0 \pmod{e_{H_f}}.$$

Déduisons du th. 2, (i) § 2.3 le résultat suivant :

Proposition 11. S'il existe un diviseur premier ρ de f tel que $f'/f = \rho^n$,

$n \geq 0$, on a :

$$\begin{aligned} \text{(i)} \quad & N_{H_{f'}/H_f}(\Phi_{f'}^\varepsilon) = \Phi_f^{f'/f}, \\ \text{(ii)} \quad & N_{H_{f'}/H_f}(V_{f'}^\varepsilon) = V_f^{f'/f}, \end{aligned}$$

avec $\varepsilon = e_f/e_{f'}$, ($\varepsilon = 1, 2, 3$ ou 4).

Démonstration : nous pouvons nous borner au cas $n = 1$, le cas général s'en déduisant par récurrence sur n .

D'après le lemme 9, pour toutes classes $C \in \text{Cl}(f)$ et $C' \in \text{Cl}(f\rho)$ telles que $C' \subset C$, on a

$$N_{H_{f\rho}/H_f}(\varphi_{f\rho}(C')) = \prod_{\substack{C \in \text{Cl}(f\rho) \\ C \subset C}} \varphi_{f\rho}(\tilde{C}).$$

On déduit alors du th. 2, (i) § 2.3 l'identité

$$(21) \quad N_{H_{f^p}/H_f}(\varphi_{f^p}(C')/\varphi_{f^p}(C'_0))^E = (\varphi_f(C)/\varphi_f(C_0))^{f'/f}.$$

L'identité (i) en résulte immédiatement.

Soit w un élément de V_{f^p} , et soient n_i , $i \in (1, 2, \dots, k'-1)$, des entiers rationnels tels que

$$(22) \quad \sum_{i=1}^{k'-1} n_i [N(\alpha(C'_i)) - 1] \equiv 0 \pmod{e_{H_{f^p}}},$$

et

$$w = \prod_{i=1}^{k'-1} \varphi_{f^p, i}^{n_i}.$$

Posons $m_j = \sum_{\{i | C'_i \subset C_j\}} n_i$, $j \in (1, 2, \dots, k-1)$; on déduit de (22) la congruence

$$\sum_{j=1}^{k-1} m_j [N(\alpha(C_j)) - 1] \equiv 0 \pmod{e_{H_f}},$$

et, d'après (21), nous avons

$$N_{H_{f^p}/H_f}(w^E) = \prod_{j=1}^{k-1} \varphi_{f, j}^{m_j f'/f}.$$

Par conséquent $N_{H_{f^p}/H_f}(w^E)$ appartient à $V_f^{f'/f}$, d'où $N_{H_{f^p}/H_f}(V_{f^p}^E) \subset V_f^{f'/f}$.

Réciproquement, soit w un élément de V_f , et soient n_i , $i \in (1, 2, \dots, k-1)$, des entiers rationnels tels que

$$\sum_{i=1}^{k-1} n_i [N(\alpha(C_i)) - 1] \equiv 0 \pmod{e_{H_f}} \quad \text{et} \quad w = \prod_{i=1}^{k-1} \varphi_{f, i}^{n_i}.$$

D'après le lemme 6, l'idéal (e_{H_f}) est engendré par les entiers $N(\alpha) - 1$, lorsque α parcourt l'ensemble des idéaux entiers, premiers avec $12f'$, qui appartiennent à C_0 . Nous pouvons donc trouver des idéaux entiers $\alpha_1, \alpha_2, \dots, \alpha_r \in C_0$, premiers avec $12f'$, et des entiers rationnels m_1, m_2, \dots, m_r , tels que

$$(23) \quad \sum_{j=1}^r m_j (N(\alpha_j) - 1) + \sum_{i=1}^{k-1} n_i [N(\alpha(C_i)) - 1] = 0.$$

Posons

$$w' = \prod_{j=1}^r (\varphi_{f^p}(C'_j)/\varphi_{f^p}(C'_0))^{m_j} \prod_{i=1}^{k-1} (\varphi_{f^p}(C'_i)/\varphi_{f^p}(C'_0))^{n_i};$$

on déduit de (23) que w' appartient à V_{f^p} , et d'après (21) nous avons

$$N_{H_{\ell^2}/H_{\ell}}(w, \varepsilon) = \prod_{i=1}^{k-1} \varphi_{\ell, i}^{n_i f'/f} = w^{f'/f}.$$

Par conséquent $w^{f'/f}$ appartient à $N_{H_{\ell^2}/H_{\ell}}(V_{\ell}^{\varepsilon})$, d'où $V_{\ell}^{f'/f} \subset N_{H_{\ell^2}/H_{\ell}}(V_{\ell}^{\varepsilon})$. Ce qui complète la démonstration de l'identité (ii).

Théorème 7. Tout élément de V_{ℓ} est une puissance $(e_{\ell} f)$ -ième dans H_{ℓ} .

Démonstration : soit w un élément de V_{ℓ} , et soient n_i , $i \in (1, 2, \dots, k-1)$,

des entiers rationnels tels que

$$\sum_{i=1}^{k-1} n_i [N(\alpha(C_i)) - 1] \equiv 0 \pmod{e_{H_{\ell}} f} \quad \text{et} \quad w = \prod_{i=1}^{k-1} \varphi_{\ell, i}^{n_i}.$$

D'après la proposition 10, nous avons

$$w = \prod_{i=1}^{k-1} \varphi_{\ell}(C_0)^{n_i [N(\alpha(C_i)) - 1]} \theta(C_0; \alpha(C_i))^{n_i f};$$

comme dans la démonstration de la proposition 11, nous pouvons trouver des idéaux

entiers $\alpha_1, \alpha_2, \dots, \alpha_r \in C_0$, premiers avec $12f$, et des entiers rationnels

m_1, m_2, \dots, m_r , tels que

$$(23) \quad \sum_{j=1}^r m_j (N(\alpha_j) - 1) + \sum_{i=1}^{k-1} n_i [N(\alpha(C_i)) - 1] = 0.$$

Nous avons alors, d'après la proposition 10,

$$(24) \quad w = \prod_{j=1}^r \theta(C_0; \alpha_j)^{m_j f} \prod_{i=1}^{k-1} \theta(C_0; \alpha(C_i))^{n_i f}.$$

D'après le corollaire de la proposition 9, le membre de droite de (24) est une

puissance f -ième dans H_{ℓ} . Ce qui démontre le th. 7 lorsque $e_{\ell} = 1$.

Supposons que $e_{\ell} \geq 2$, d'où $\ell \mid 6$. Soit p un diviseur premier de ℓ , nous avons $\ell p^2 \nmid 6$ d'où $e_{\ell p^2} = 1$. Posons $\ell' = \ell p^2$, d'après la proposition 11, (ii) nous avons

$$V_{\ell'}^{f'/f} = N_{H_{\ell'}/H_{\ell'}}(V_{\ell'}^{\varepsilon});$$

or, les éléments de $V_{\ell'}$ sont des puissances f' -ièmes dans $H_{\ell'}$ (d'après la partie déjà démontrée du th. 7), par conséquent les éléments de $V_{\ell'}^{f'/f}$ sont des puissances $(e_{\ell'} f')$ -ièmes dans $H_{\ell'}$; C.Q.F.D.

Définition. On déduit du th. 7 l'existence d'un plus grand sous-groupe Ω_f de E_{H_f} tel que $\Omega_f^{e_f f} = V_f$.

Le résultat suivant est essentiellement trivial.

Proposition 12. Pour tout automorphisme σ de H_f/K nous avons $V_f^\sigma = V_f$, $\Phi_f^\sigma = \Phi_f$ et $\Omega_f^\sigma = \Omega_f$.

Nous pouvons décrire Ω_f de la manière suivante

Théorème 8. Soit (t, ℓ) un élément de $A(f)$. Le groupe Ω_f est engendré par les racines g -ièmes de l'unité et par les racines e_f -ièmes des produits

$$\prod_{i=1}^s \theta^{(12)m_i}_i(t; \ell \alpha_i^{-1}),$$

où les α_i sont des idéaux entiers de K , premiers avec $12f$, et où les entiers rationnels m_i , $i \in (1, 2, \dots, s)$, sont tels que $\sum_{i=1}^s m_i = 0$ et $\sum_{i=1}^s m_i N(\alpha_i) = 0$.

Démonstration : posons $C = C_{(t, \ell)} \in Cl(f)$; comme $\theta(C; \alpha) = \theta^{(12)}(t; \ell \alpha^{-1}) / \theta^{(12)}(t; \ell)^{N(\alpha)}$, il nous suffit de démontrer que V_f est l'ensemble des puissances f -ièmes des produits $w = \prod_{i=1}^s \theta(C; \alpha_i)^{m_i}$, où les entiers rationnels m_i , $i \in (1, 2, \dots, s)$, sont tels que $\sum_{i=1}^s m_i [N(\alpha_i) - 1] = 0$. D'après la proposition 12 et le corollaire de la proposition 9, nous pouvons supposer que $C = C_0$; les identités (23) et (24) nous montrent que tout élément de V_f est la puissance f -ième d'un tel produit w ; réciproquement, on déduit de la proposition 10 que w^f appartient bien à V_f ; C.Q.F.D.

Proposition 13. Nous avons $V_f \subset \Phi_f$ et $\Phi_f^{12/e} \subset \Omega_f \subset E_{H_f}$.

Démonstration : d'après le lemme 7 nous savons que $e_{H_f} \mid 12f$, et pour tout idéal entier α de K , premier avec e , nous avons $N(\alpha) - 1 \equiv 0 \pmod{e}$. Il en résulte que $\varphi_{f,i}^{12f/e}$ appartient à V_f pour tout $i \in (1, 2, \dots, k-1)$; par conséquent nous avons

$$\Phi_f^{12f/e} \subset \Omega_f^{e_f f} \subset \Omega_f^f, \text{ d'où } \Phi_f^{12/e} \subset \Omega_f.$$

Les autres inclusions de la proposition 13 sont triviales.

Enfin, on déduit immédiatement de la proposition 11, (ii) le résultat suivant :

Proposition 14. S'il existe un diviseur premier \mathfrak{p} de f tel que $f'/f = \mathfrak{p}^n$,

$n > 0$, on a

$$\mu_{\mathfrak{p}}^{N_{H_{\mathfrak{p}'}/H_{\mathfrak{p}}}}(\Omega_{\mathfrak{p}'}) = \Omega_{\mathfrak{p}}.$$

4.5. Racines (e, f) -ièmes des invariants $\varphi_H(C)$.

Soit H une extension abélienne de K de conducteur $\mathfrak{f} \neq (1)$. Pour toute classe $C \in \text{Cl}(H/K)$, posons

$$\varphi_H(C) = \prod_{\tilde{C} \subset C} \varphi_{\mathfrak{f}}(\tilde{C}),$$

où le produit est pris sur toutes les classes $\tilde{C} \in \text{Cl}(\mathfrak{f})$ contenues dans C .

Proposition 15. Pour toutes classes C et $C' \in \text{Cl}(H/K)$ et pour toute classe $\tilde{C} \in \text{Cl}(\mathfrak{f})$ contenue dans C ,

- (i) On a $\varphi_H(C) = N_{H_{\mathfrak{f}'}/H_{\mathfrak{f}}}(\varphi_{\mathfrak{f}}(\tilde{C}))$;
- (ii) L'invariant $\varphi_H(C)$ est un élément entier de H ;
- (iii) Le quotient $\varphi_H(C)/\varphi_H(C')$ est une unité de H ;
- (iv) On a $\varphi_H(C)^{\mathfrak{e}(C')} = \varphi_H(CC')$.

Démonstration : l'assertion (i) est un cas particulier du lemme 9 ; les assertions (ii), (iii) et (iv) sont des conséquences immédiates de (i) et des assertions (i), (ii) et (iii) du th. 1 § 2.3.

Supposons pour l'instant que $\mathfrak{f}' = \mathfrak{f}$ et $H' = H_{\mathfrak{f}}$.

Définitions. D'après la proposition 15, (iii), les quotients

$$\varphi_{H,i} = \varphi_H(C_i)/\varphi_H(C_0), \quad i \in (1, 2, \dots, k-1),$$

engendrent un sous-groupe Φ_H de E_H . On déduit de la proposition 15, (i) l'égalité $\Phi_H = N_{H_{\mathfrak{f}'}/H_{\mathfrak{f}}}(\Phi_{\mathfrak{f}})$.

Soit V_H le sous-groupe de Φ_H formé des produits $\prod_{i=1}^{k-1} \varphi_{H,i}^{n_i}$, où les entiers rationnels n_i , $i \in (1, 2, \dots, k-1)$, sont tels que

$$\sum_{i=1}^{k-1} n_i [N(\alpha(C_i)) - 1] \equiv 0 \pmod{e_H}.$$

Théorème 9. Nous avons $V_H = N_{H_f/H}(V_f)$, et tout élément de V_H est une puissance $(e_f f)$ -ième dans H .

Démonstration : soit w un élément de V , et soient n_i , $i \in (1, 2, \dots, k-1)$, des entiers rationnels tels que

$$(25) \quad \sum_{i=1}^{k-1} n_i [N(\alpha(C_i)) - 1] \equiv 0 \pmod{e_{H_f}}$$

et

$$w = \prod_{i=1}^{k-1} \varphi_{f,i}^{n_i}.$$

Posons $m_j = \sum_{\{i | C_i' \subset C_j\}} n_i$, $j \in (1, 2, \dots, k-1)$; nous avons

$$N_{H_f/H}(w) = \prod_{j=1}^{k-1} \varphi_{H,j}^{m_j},$$

et l'on déduit de (25) la congruence

$$\sum_{j=1}^{k-1} m_j [N(\alpha(C_j)) - 1] \equiv 0 \pmod{e_H}.$$

Par conséquent $N_{H_f/H}(w)$ appartient à V_H , d'où $N_{H_f/H}(V_f) \subset V_H$.

Réciproquement, soit w un élément de V_H et soient n_i , $i \in (1, 2, \dots, k-1)$, des entiers rationnels tels que

$$\sum_{i=1}^{k-1} n_i [N(\alpha(C_i)) - 1] \equiv 0 \pmod{e_H} \quad \text{et} \quad w = \prod_{i=1}^{k-1} \varphi_{H,i}^{n_i}.$$

Comme dans la démonstration de la proposition 11, nous pouvons trouver des idéaux entiers $\alpha_1, \alpha_2, \dots, \alpha_r \in C_0$, premiers avec $12f$, et des entiers rationnels m_1, m_2, \dots, m_r , tels que

$$(23) \quad \sum_{j=1}^r m_j (N(\alpha_j) - 1) + \sum_{i=1}^{k-1} n_i [N(\alpha(C_i)) - 1] = 0.$$

Posons

$$w' = \prod_{j=1}^r (\varphi_f(C_j') / \varphi_f(C_0'))^{m_j} \prod_{i=1}^{k-1} (\varphi_f(C_i') / \varphi_f(C_0'))^{n_i};$$

nous avons $w = N_{H_f/H}(w')$, et il résulte de (23) que le produit w' appartient à

V_f ; d'où $V_H \subset N_{H_f/H}(V_f)$.

Nous avons donc $V_H = N_{H_f/H}(V_f)$, et il résulte du th. 7 que tout élément de V_H est une puissance $(e_f f)$ -ième dans H ; C.Q.F.D.

Définition. On déduit du th. 9 que le groupe

$$\Omega_H = \mu_{\mathcal{E}} N_{H_f/H}(\Omega_f)$$

est le plus grand sous-groupe de E_H tel que $\Omega_H^{e_f f} = V_H$.

On déduit des propositions 12 et 13 les résultats suivants.

Proposition 16.

- (i) Pour tout automorphisme σ de H/K , nous avons $V_H^\sigma = V_H$, $\Phi_H^\sigma = \Phi_H$ et $\Omega_H^\sigma = \Omega_H$;
- (ii) Nous avons $V_H \subset \Phi_H$ et $\Phi_H^{12/e} \subset \Omega_H \subset E_H$.

Supposons maintenant que f' est un multiple de f , et H' une extension abélienne de K de conducteur f' telle que $H \subset H'$. Nous déduisons des propositions 11 et 14 le résultat suivant :

Proposition 17. S'il existe un diviseur premier \mathfrak{p} de f tel que $f'/f = \mathfrak{p}^n$,

$n \geq 0$, on a

- (i) $N_{H'/H}(\Phi_{H'}^\varepsilon) = \Phi_H^{f'/f}$,
- (ii) $N_{H'/H}(V_{H'}^\varepsilon) = V_H^{f'/f}$,
- (iii) $\mu_{\mathcal{E}} N_{H'/H}(\Omega_{H'}) = \Omega_H$,

avec $\varepsilon = e_f/e_{f'}$.

On déduit immédiatement de la proposition 16, (i) la conséquence suivante de la proposition 17 :

Corollaire. On a $\Phi_H^{f'/f} \subset \Phi_H^\varepsilon$, $V_H^{f'/f} \subset V_H^\varepsilon$ et $\Omega_H \subset \Omega_{H'}$.

4.6. Le rang des groupes d'unités V_H , Φ_H et Ω_H .

Soit H une extension abélienne de K de conducteur $\mathfrak{f} \neq (1)$; nous supposons que $\mathfrak{f}' = \mathfrak{f}$ et $H' = H$, cf. § 4.3.

Pour tout entier $i \in (0, 1, \dots, k-1)$ et toute unité u de H , posons

$$\rho_i(u) = \log \left| u^{g(c_i)} \right|^2.$$

L'homomorphisme

$$u \in E_H \mapsto \rho(u) = (\rho_0(u), \rho_1(u), \dots, \rho_{k-1}(u)) \in \mathbb{C}^k$$

définit une représentation de E_H dans \mathbb{C}^k ; nous avons

$$\rho(E_H) \otimes \mathbb{C} = \left\{ (\rho_0, \rho_1, \dots, \rho_{k-1}) \in \mathbb{C}^k \mid \sum_{i=0}^{k-1} \rho_i = 0 \right\}.$$

Pour tout caractère $\chi \neq 1$ de $\text{Cl}(H/K)$, notons \mathfrak{f}_χ le conducteur de χ et χ' le caractère primitif de $\text{Cl}(H \cap H_{\mathfrak{f}_\chi}/K)$ associé à χ . Posons

$$\varphi(\chi) = \sum_{i=0}^{k-1} \bar{\chi}(c_i) \rho(\varphi_{H,i});$$

nous déduisons du th. 3 § 2.4 et de son corollaire le résultat suivant :

Théorème 10. Nous avons

$$\rho(\Phi_H) \otimes \mathbb{C} = \bigoplus_{\substack{\chi \in \text{Cl}(H/K) \\ \chi \neq 1}} \mathbb{C} \cdot \varphi(\chi);$$

et pour que $\varphi(\chi) = 0$, il faut et il suffit que, lorsque \mathfrak{p} parcourt l'ensemble des diviseurs premiers de \mathfrak{f} , le produit $\prod_{\mathfrak{p}|\mathfrak{f}} (1 - \bar{\chi}'(\mathfrak{p}))$ soit nul.

Démonstration : soit M la matrice carrée d'ordre $k-1$ et de terme général $\bar{\chi}(c)$, où χ parcourt l'ensemble des caractères $\neq 1$ de $\text{Cl}(H/K)$ et où c parcourt l'ensemble des éléments $\neq c_0$ de $\text{Cl}(H/K)$. L'identité

$$\rho(\Phi_H) \otimes \mathbb{C} = \bigoplus_{\substack{\chi \in \text{Cl}(H/K) \\ \chi \neq 1}} \mathbb{C} \cdot \varphi(\chi)$$

résulte de ce que M est inversible et les vecteurs $\rho(\varphi_{H,i})$, $i \in (1, 2, \dots, k-1)$, engendrent $\rho(\Phi_H)$.

Pour tout caractère $\chi \neq 1$ de $\text{Cl}(H/K)$, posons

$\varphi(\chi) = (\varphi_0(\chi), \varphi_1(\chi), \dots, \varphi_{k-1}(\chi))$; pour tout entier $j \in (0, 1, \dots, k-1)$, nous avons

$$\begin{aligned} \varphi_j(\chi) &= \sum_{i=0}^{k-1} \bar{\chi}(c_i) \rho_j(\varphi_H(c_i)) \\ &= \sum_{i=0}^{k-1} \bar{\chi}(c_i) \log |\varphi_H(c_i c_j)|^2 \\ &= 2 \chi(c_j) \sum_{i=0}^{k-1} \bar{\chi}(c_i) \log |\varphi_H(c_i)|. \end{aligned}$$

Comme $\sum_{i=0}^{k-1} \bar{\chi}(c_i) \log |\varphi_H(c_i)| = \sum_{j=0}^{k-1} \bar{\chi}(c_j) \log |\varphi_H(c_j)| = S(\chi)$,

pour que $\varphi(\chi) = 0$ il faut et il suffit que $S(\chi) = 0$. Comme $L(1, \chi')$ est $\neq 0$ lorsque χ est $\neq 1$, il résulte du th. 3, (i) § 2.4 et de son corollaire que la somme $S(\chi)$ est nulle si et seulement si $\prod_{\mathfrak{p}|\mathfrak{f}} (1 - \bar{\chi}'(\mathfrak{p})) = 0$. Le th. 10 est démontré.

D'après la proposition 16, (ii) § 4.5, nous avons

$$V_H = \Omega_H^{e_{\mathfrak{f}} f} \subset \Phi_H \text{ et } \Phi_H^{12/e} \subset \Omega_H;$$

les groupes V_H , Φ_H et Ω_H ont donc même rang. Comme le rang de Φ_H est égal à la \mathfrak{O} -dimension de $\rho(\Phi_H) \otimes \mathfrak{O}$, nous déduisons du th. 10 le résultat suivant :

Corollaire 1. Soit m le nombre de caractères χ de $\text{Cl}(H/K)$ tels que

$\prod_{\mathfrak{p}|\mathfrak{f}} (1 - \bar{\chi}'(\mathfrak{p})) = 0$. Le rang des groupes V_H , Φ_H et Ω_H est égal à $k-m$.

Supposons maintenant que $\mathfrak{f} = \mathfrak{p}^n$, $n > 0$, pour un idéal premier \mathfrak{p} de K .

Notons $D(\mathfrak{p})$ le corps de décomposition dans $H(1)$ de l'idéal \mathfrak{p} ; les caractères du groupe $\text{Cl}(H \cap D(\mathfrak{p})/K)$ sont les caractères χ de $\text{Cl}(H \cap H(1)/K)$ tels que $\chi(\mathfrak{p}) = 1$. Soit $E_{H/H \cap D(\mathfrak{p})}$ le groupe formé des unités u de H telles que $N_{H/H \cap D(\mathfrak{p})}(u^{12}) = 1$. On déduit du th. 10 le résultat suivant :

Corollaire 2. Lorsque $\mathfrak{f} = \mathfrak{p}^n$, $n > 0$, les groupes V_H , Φ_H et Ω_H sont des sous-groupes d'indices finis de $E_{H/H \cap D(\mathfrak{p})}$.

Démonstration : les éléments de $E_{H/H\cap D(\mathfrak{p})}$ sont les unités u de H telles que, pour tout caractère χ de $Cl(H\cap D(\mathfrak{p})/K)$, la somme $\sum_{i=0}^{k-1} \bar{\chi}(C_i) \rho(u^{g(C_i)})$ soit nulle. Or, pour toute classe $C \in Cl(H/K)$, on a :

$$\sum_{i=0}^{k-1} \bar{\chi}(C_i) \rho((\varphi_H(C)/\varphi_H(C_0))^{g(C_i)}) = \sum_{i=0}^{k-1} \bar{\chi}(C_i) \rho(\varphi_H(CC_i)/\varphi_H(C_i)) = (\chi(C) - 1)\varphi(\chi) ;$$

comme $\varphi(\chi) = 0$ pour tout caractère χ de $Cl(H\cap D(\mathfrak{p})/K)$, le quotient $\varphi_H(C)/\varphi_H(C_0)$ appartient à $E_{H/H\cap D(\mathfrak{p})}$. Par conséquent Φ_H est un sous-groupe de $E_{H/H\cap D(\mathfrak{p})}$; de plus, d'après le corollaire 1, les rangs de Φ_H et $E_{H/H\cap D(\mathfrak{p})}$ sont égaux à $k-m$; il en résulte que Φ_H est un sous-groupe d'indice fini de $E_{H/H\cap D(\mathfrak{p})}$. Comme $E_{H/H\cap D(\mathfrak{p})}$ ne possède pas d'extension non triviale dans E_H qui ait le rang $k-m$, les groupes V_H et Ω_H sont également des sous-groupes d'indices finis de $E_{H/H\cap D(\mathfrak{p})}$; C.Q.F.D.

§ 5. LE GROUPE DES UNITÉS ELLIPTIQUES D'UNE EXTENSION ABÉLIENNE.

Pour toute extension abélienne H de K de conducteur f , nous appelons groupe des unités elliptiques de H le groupe

$$\mathfrak{E}_H = \mu_{e_H} \prod_{\mathfrak{q}|f} \Omega_{H\cap H}^{\mathfrak{q}},$$

où le produit est pris sur tous les diviseurs entiers \mathfrak{q} de f ; cf. définitions §§ 3.2 et 4.5.

Soit $f = \prod_{i=1}^{\ell} p_i^{n_i}$ une décomposition de f en produit de facteurs premiers distincts p_i , $i \in (1, 2, \dots, \ell)$. Pour tout ℓ -uplet $\varepsilon = (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_\ell)$ d'entiers ε_i égaux à 0 ou 1, posons $f_\varepsilon = \prod_{i=1}^{\ell} p_i^{\varepsilon_i n_i}$ et notons f_ε le plus petit entier > 0 qui appartient à f_ε . Il résulte du corollaire de la proposition 17 que

$$\mathfrak{E}_H = \mu_{e_H} \prod_{\varepsilon=(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_\ell)} \Omega_{H\cap H}^{\mathfrak{q}_{f_\varepsilon}},$$

où le produit est pris sur tous les ℓ -uplets ε formés de 0 et de 1.

Dans [R] K. RAMACHANDRA décrit certains systèmes maximaux d'unités indépendantes de H , dont les éléments appartiennent au produit

$$U_H = \Delta_{H\cap H}^f(1) \prod_{\substack{\varepsilon=(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_\ell) \\ \varepsilon \neq (0, 0, \dots, 0)}} \Phi_{H\cap H}^{hf/f_\varepsilon} f_\varepsilon;$$

cf. th. 4 p. 119, formule (95) p. 113 et th. 12 § 7 p. 134 de [R].

Comme $\Delta_{H\cap H}(1) \subset \Omega_{H\cap H}(1)$ et $\Phi_{H\cap H}^{12/e} \subset \Omega_{H\cap H} f_\varepsilon$

(cf. proposition 6, (iii) § 3.2 et proposition 16, (ii) § 4.5), nous avons

$U_H^{12/e} \subset \mathfrak{E}_H$; d'où le résultat suivant :

Théorème 11. L'indice de \mathfrak{E}_H dans E_H est fini.

Remarque. Nous ne possédons pas de formule générale permettant de déterminer l'indice $(E_H : \mathfrak{E}_H)$. Rappelons à ce propos que l'on ne connaît pas non plus de formule générale permettant de déterminer l'indice du groupe des unités circulaires d'une extension cyclotomique dans le groupe de toutes ses unités; cf. HASSE [Ha 2].

La suite de notre travail sera consacrée à la détermination de l'indice $(E_H : \mathfrak{E}_H)$ dans le cas où le conducteur de H/K est puissance d'un idéal premier. Rappelons que, dans le cas d'une extension cyclotomique H dont le conducteur est puissance d'un nombre premier, l'indice du groupe des unités circulaires de H dans le groupe des valeurs absolues de toutes les unités de H est égal au nombre de classes de H .

§ 6. FORMULES POUR LE NOMBRE DE CLASSES DES EXTENSIONS ABELIENNES
DE CONDUCTEUR PUISSANCE D'UN IDEAL PREMIER.

Soit H une extension abélienne de K , dont le conducteur est puissance d'un idéal premier. Nous nous proposons de démontrer (th. 16 § 6.5) que l'indice de \mathfrak{E}_H dans E_H est donné par la formule

$$(E_H : \mathfrak{E}_H) = \lambda h_H / [HH_{(1)} : H],$$

où h_H est le nombre de classes de H , où $H_{(1)}$ est le corps de classes absolu de K et où $\lambda = 12^{[H:K]-1} / \mu$, l'entier μ étant un certain diviseur du quotient $e_{H \cap H_{(1)}} / e$. Lorsque H/K est non ramifiée, nous avons $\mu = e_H / e$ et la formule est celle du th. 6 § 3.2.

Supposons H/K ramifié et traçons les grandes lignes de notre démonstration. Il existe un idéal premier \mathfrak{p} de K et un entier $n > 0$, tels que \mathfrak{p}^n soit le conducteur de H/K ; nous notons p et p^m , $0 < m < n$, les plus petits entiers > 0 qui appartiennent à \mathfrak{p} et \mathfrak{p}^n ; nous posons $r = e_{\mathfrak{p}^n} p^m$. Nous construisons des groupes

$$\Psi \subset \Delta_{H \cap H_{(1)}}^r \Phi_H,$$

$$V \subset \Delta_{H \cap H_{(1)}}^r V_H \quad \text{tel que} \quad V \subset \Psi$$

et $\Lambda \subset \Delta_{H \cap H_{(1)}}^r \Omega_H \quad \text{tel que} \quad \Lambda^r = V,$

et nous posons $\Lambda^* = \mu_e \Lambda;$

les groupes Ψ , V , Λ et Λ^* sont des sous-groupes d'indices finis de E_H ; cf. proposition 21, (i) § 6.3. Les résultats du § 2 nous permettent de calculer les indices

$$(E_H : \Psi) \quad \text{et} \quad (E_{H \cap H_{(1)}} : \Psi \cap E_{H \cap H_{(1)}}),$$

selon la technique déjà développée dans [R]; nous en déduisons la valeur des indices

$$(E_H : \Lambda^*) \quad \text{et} \quad (E_{H \cap H_{(1)}} : \Lambda^* \cap E_{H \cap H_{(1)}});$$

cf. th. 12 et 13 § 6.2 et th. 15 § 6.4.

L'identité $\xi_{H \cap H(1)} \Lambda^* = \xi_H$ de la proposition 25 § 6.5 nous permet d'utiliser Λ^* comme intermédiaire pour déterminer l'indice $(E_H : \xi_H)$; plus précisément, nous avons

$$(E_H : \xi_H) = (E_{H \cap H(1)} : \xi_{H \cap H(1)}) (E_H : \Lambda^*) / (E_{H \cap H(1)} : \Lambda^* \cap E_{H \cap H(1)});$$

notre calcul se termine en observant que la valeur de l'indice $(E_{H \cap H(1)} : \xi_{H \cap H(1)})$ nous est donnée par le th. 6 § 3.2.

6.1. Les invariants $\psi(C)$.

Soient \mathfrak{p} un idéal premier de K , et H une extension abélienne de K de conducteur \mathfrak{p}^n , $n > 0$. Nous notons p et p^m , $0 < m \leq n$, les plus petits entiers > 0 qui appartiennent à \mathfrak{p} et \mathfrak{p}^n ; nous posons $r = e_{\mathfrak{p}}^{n/p^m}$. Nous pouvons préciser la valeur de l'entier m :

- (i) Lorsque l'idéal (p) est inerte ou bien décomposé dans K , nous avons $m = n$;
- (ii) Lorsque l'idéal (p) est ramifié dans K , nous avons $m = n/2$ ou $m = (n+1)/2$ suivant que n est pair ou impair.

L'extension $H \cap H(1)/K$ est la sous extension abélienne non ramifiée maximale de H/K ; nous posons $k_1 = [H \cap H(1) : K]$ et $k = [H : K]$. Nous notons c_0 et C_0 les classes unités des groupes $\text{Cl}(H \cap H(1)/K)$ et $\text{Cl}(H/K)$; nous notons $c_1, c_2, \dots, c_{k_1-1}$ les éléments de $\text{Cl}(H \cap H(1)/K)$ différents de c_0 , et C_1, C_2, \dots, C_{k-1} les éléments de $\text{Cl}(H/K)$ différents de C_0 . Pour toute classe $C \in \text{Cl}(H/K)$, nous notons $c(C) \in \text{Cl}(H \cap H(1)/K)$ la classe qui contient C . Nous avons

$$\xi_{H \cap H(1)} = \mu_{e_{H \cap H(1)}} \Omega_{H \cap H(1)} \quad \text{et} \quad \xi_H = \mu_e \Omega_{H \cap H(1)} \Omega_H.$$

Définition. Pour toute classe $C \in \text{Cl}(H/K)$, nous posons

$$\psi(C) = \delta_{H \cap H(1)} (c(C))^r \varphi_H(C).$$

Nous déduisons des propositions 4 § 3.1 et 15 § 4.5 les propriétés suivantes des invariants $\psi(C)$.

Proposition 18. Pour toutes classes C, C' et $C'' \in \text{Cl}(H/K)$,

- (i) Le quotient $\psi(C)/\psi(C')$ est une unité de H ;
- (ii) On a $(\psi(C)/\psi(C'))^{\mathfrak{g}(C'')} = \psi(CC'')/\psi(C'C'')$.

Définition. Pour toute classe $c \in \text{Cl}(H \cap H_{(1)})/K$, nous posons

$$\psi(c) = \prod_{\substack{C \in \text{Cl}(H/K) \\ C \subset c}} \psi(C).$$

Proposition 19. Pour toutes classes c, c' et $c'' \in \text{Cl}(H \cap H_{(1)})/K$ et pour toutes classes C et $C' \in \text{Cl}(H/K)$ telles que $C \subset c$ et $C' \subset c'$,

- (i) On a $N_{H/H \cap H_{(1)}}(\psi(C)/\psi(C')) = \psi(c)/\psi(c')$;
- (ii) Le quotient $\psi(c)/\psi(c')$ est une unité de $H \cap H_{(1)}$;
- (iii) On a $(\psi(c)/\psi(c'))^{\mathfrak{g}(c'')} = \psi(cc'')/\psi(c'c'')$.

Démonstration : d'après le lemme 9 § 4.4, on a

$$N_{H/H \cap H_{(1)}}(\varphi_H(c)) = \prod_{\substack{\tilde{C} \in \text{Cl}(H/K) \\ \tilde{C} \subset c}} \varphi_H(\tilde{C}).$$

Il en résulte que

$$\psi(c)/\psi(c') = (\delta_{H \cap H_{(1)}}(c)/\delta_{H \cap H_{(1)}}(c'))^{\text{rk}/k} N_{H/H \cap H_{(1)}}(\varphi_H(c)/\varphi_H(c'));$$

d'où l'assertion (i). Les assertions (ii) et (iii) résultent immédiatement de (i) et des assertions (i) et (ii) de la proposition 18.

6.2. Le groupe d'unités Ψ .

Définition. D'après la proposition 18, (ii) les quotients $\phi_i = \phi(C_i)/\phi(C_0)$, $i \in (1, 2, \dots, k-1)$, engendrent un sous-groupe Ψ de E_H .

Démontrons le résultat suivant :

Théorème 12. Les unités ϕ_i , $i \in (1, 2, \dots, k-1)$, forment un système maximal d'unités indépendantes de H . Par conséquent Ψ est un sous-groupe d'indice fini de E_H ; cet indice est donné par la formule

$$(E_H : \Psi) = B(H \cap H_{(1)}) (12r)^{k-1} e_{h_H/h},$$

où $B(H \cap H_{(1)})$ est l'entier > 0 ainsi défini :

(i) L'entier $B(K)$ est 1 ;

(ii) Lorsque $H \cap H_{(1)} \neq K$, l'entier $B(H \cap H_{(1)})$ est le produit

$\prod_{\chi \neq 1} (1 - \bar{\chi}(\rho) + ehk/k_1)$, où χ parcourt l'ensemble des caractères $\neq 1$ de

$Cl(H \cap H_{(1)})/K$.

Démonstration : soit W le déterminant de la matrice carrée d'ordre $k-1$ et de terme général

$$\log |\phi_i^{g(C_j)}| = \log |\phi(C_i C_j)| - \log |\phi(C_j)|,$$

où $i \in (1, 2, \dots, k-1)$ et $j \in (1, 2, \dots, k-1)$. Le déterminant W a la forme d'un déterminant de groupe et par conséquent (cf. démonstration du th. 4 § 3.2 et [S] chap. II § 2 p. 102) on a

$$|W| = \left| \prod_{\chi \neq 1} \sum_{i=0}^{k-1} \bar{\chi}(C_i) \log |\phi(C_i)| \right|,$$

où le produit est pris sur tous les caractères $\chi \neq 1$ de $Cl(H/K)$. Comme

$\phi(C) = \delta_{H \cap H_{(1)}}(c(C))^r \varphi_H(C)$, nous avons

$$(26) \quad \sum_{i=0}^{k-1} \bar{\chi}(C_i) \log |\phi(C_i)| = A + rB,$$

avec $A = \sum_{i=0}^{k-1} \bar{\chi}(C_i) \log |\varphi_H(C_i)|$ et $B = \sum_{i=0}^{k-1} \bar{\chi}(C_i) \log |\delta_{H \cap H_{(1)}}(c(C_i))|$.

Puisque

$$\varphi_H(C) = \prod_{\substack{\tilde{c} \in \text{Cl}(\mathfrak{p}^n) \\ \tilde{c} \subset C}} \varphi_{\mathfrak{p}^n}(\tilde{c}), \text{ nous avons}$$

$$(27) \quad A = \sum_{\tilde{c} \in \text{Cl}(\mathfrak{p}^n)} \bar{\chi}(\tilde{c}) \log |\varphi_{\mathfrak{p}^n}(\tilde{c})| = S(\chi).$$

Notons f_χ le conducteur de χ et χ' le caractère primitif de $\text{Cl}(f_\chi)$ associé à χ .

(i) Si $f_\chi = \mathfrak{p}^s$ avec $s > 0$, nous avons

$$B = \sum_{j=0}^{k_1-1} \log |\delta_{\text{H}\cap\text{H}(1)}(c_j)| \left[\sum_{\substack{C \in \text{Cl}(\text{H}/K) \\ C \subset c_j}} \bar{\chi}(C) \right] = 0;$$

nous déduisons alors de (26) et (27) l'identité

$$(28) \quad \sum_{i=0}^{k-1} \bar{\chi}(C_i) \log |\psi(C_i)| = S(\chi).$$

Notons p^t le plus petit entier > 0 qui appartient à \mathfrak{p}^s ; nous déduisons de (28)

et du corollaire 2 du th. 2 § 2.3 l'identité

$$(29) \quad \sum_{i=0}^{k-1} \bar{\chi}(C_i) \log |\psi(C_i)| = p^{m-t} \left(\frac{e}{\mathfrak{p}^n} / \frac{e}{\mathfrak{p}^s} \right) S(\chi').$$

(ii) Si $f_\chi = (1)$, on a

$$B = (k/k_1) \sum_{i=0}^{k_1-1} \bar{\chi}'(c_j) \log |\delta_{\text{H}\cap\text{H}(1)}(c_j)|;$$

en utilisant l'identité (20) § 3.2, il vient $B = (hk/k_1) S(\chi')$. Nous déduisons

alors de (26) et (27) l'identité

$$(30) \quad \sum_{i=0}^{k-1} \bar{\chi}(C_i) \log |\psi(C_i)| = S(\chi) + (rhk/k_1) S(\chi').$$

Nous déduisons de (30) et du corollaire 2 du th. 2 § 2.3 l'identité

$$(31) \quad \sum_{i=0}^{k-1} \bar{\chi}(C_i) \log |\psi(C_i)| = (r/e) (1 - \bar{\chi}'(\mathfrak{p}) + ehk/k_1) S(\chi').$$

Substituons les identités (29) et (31) dans la formule du th. 3, (ii) § 2.4, il

vient

$$h_{\text{H}\cap\text{H}}^{\text{R}} = h(e_{\text{H}}/e) \prod_{\chi \neq 1} \left| \sum_{i=0}^{k-1} \bar{\chi}(C_i) \log |\psi(C_i)| \right| / (B(\text{H}\cap\text{H}(1)) (6r)^{k-1}).$$

Par conséquent le déterminant w est $\neq 0$; les unités ψ_i , $i \in (1, 2, \dots, k-1)$, forment un système maximal d'unités indépendantes de H , et le quotient $e_H^{2^{k-1}} |w| / R_H$, qui n'est autre que l'indice de Ψ dans E_H , est égal à

$$B(H \cap H_{(1)}) (12r)^{k-1} e_{H/H} / h ; \text{ C.Q.F.D.}$$

Démontrons maintenant le résultat suivant :

Théorème 13. Nous avons $N_{H/H \cap H_{(1)}}(\Psi) = \Psi \cap E_{H \cap H_{(1)}}$. Les unités $\psi(c_j) / \psi(c_0)$, $j \in (1, 2, \dots, k_1-1)$, engendrent $\Psi \cap E_{H \cap H_{(1)}}$ et forment un système maximal d'unités indépendantes de $H \cap H_{(1)}$. Par conséquent $\Psi \cap E_{H \cap H_{(1)}}$ est un sous-groupe d'indice fini de $E_{H \cap H_{(1)}}$; cet indice est donné par la formule

$$(E_{H \cap H_{(1)}} : \Psi \cap E_{H \cap H_{(1)}}) = B(H \cap H_{(1)}) (12r)^{k_1-1} e_{H \cap H_{(1)}} / h ,$$

où $B(H \cap H_{(1)})$ est le même nombre que dans le th. 12.

Démonstration : le groupe Ψ est l'ensemble des produits

$\phi = \prod_{C \in \text{Cl}(H/K)} \psi(C)^{n(C)}$, où les entiers rationnels $n(C)$, $C \in \text{Cl}(H/K)$, sont tels que $\sum_{C \in \text{Cl}(H/K)} n(C) = 0$. Pour toute classe $C' \in \text{Cl}(H/K)$, on déduit de la proposition (18), (ii) l'identité

$$\psi^{g(C')} = \prod_{C \in \text{Cl}(H/K)} \psi(CC')^{n(C)} .$$

Pour que le produit ϕ appartienne à $H \cap H_{(1)}$, il faut et il suffit que, pour toute classe $C' \in \text{Cl}(H/K)$ contenue dans c_0 , on ait $\psi^{g(C')} = \psi$; c'est-à-dire que

$$(32) \quad \prod_{C \in \text{Cl}(H/K)} \psi(C)^{n(C)} = \prod_{C \in \text{Cl}(H/K)} \psi(CC')^{n(C)} .$$

D'après le th. 12 les unités $\psi(C) / \psi(c_0)$, $C \in \text{Cl}(H/K)$ et $C \neq c_0$, sont multiplicativement indépendantes ; comme $\sum_{C \in \text{Cl}(H/K)} n(C) = 0$, on déduit de (32) qu'une condition nécessaire et suffisante pour que $\phi \in E_{H \cap H_{(1)}}$ est que, pour toute classe $C \in \text{Cl}(H/K)$ et pour toute classe $C' \in \text{Cl}(H/K)$ contenue dans c_0 , on ait

$n(c) = n(CC')$. Il en résulte que $\Psi \cap E_{H \cap H(1)}$ est l'ensemble des produits

$$\psi = \prod_{c \in \text{Cl}(H \cap H(1)/K)} \psi(c)^{m(c)},$$

où les entiers rationnels $m(c)$, $c \in \text{Cl}(H \cap H(1)/K)$, sont tels que

$$\sum_{c \in \text{Cl}(H \cap H(1)/K)} m(c) = 0;$$

nous avons alors $\psi = \prod_{c \in \text{Cl}(H \cap H(1)/K)} (\psi(c)/\psi(c_0))^{m(c)}$,

et les unités $\psi(c)/\psi(c_0)$, $c \in \text{Cl}(H \cap H(1)/K)$, engendrent $\Psi \cap E_{H \cap H(1)}$. On déduit alors immédiatement de la proposition (19), (i), l'identité

$$\Psi \cap E_{H \cap H(1)} = N_{H/H \cap H(1)}(\Psi).$$

Considérons maintenant le déterminant W_1 de la matrice carrée d'ordre $k_1 - 1$ et de terme général :

$$\log |(\psi(c_i)/\psi(c_0))^{g(c_j)}| = \log |\psi(c_i c_j)| - \log |\psi(c_j)|,$$

où $i \in (1, 2, \dots, k_1 - 1)$ et $j \in (1, 2, \dots, k_1 - 1)$. Le déterminant W_1 a la forme d'un déterminant de groupe et par conséquent, comme dans la démonstration du th. 12, on a

$$|W_1| = \left| \prod_{\chi \neq 1} \sum_{i=0}^{k_1-1} \bar{\chi}(c_i) \log |\psi(c_i)| \right|,$$

où le produit est pris sur tous les caractères $\chi \neq 1$ de $\text{Cl}(H \cap H(1)/K)$. Nous avons

$$\sum_{i=0}^{k_1-1} \bar{\chi}(c_i) \log |\psi(c_i)| = \sum_{i=0}^{k_1-1} \bar{\chi}(c_i) \log \left| \prod_{\substack{c \in \text{Cl}(H/K) \\ C \subset c_i}} \psi(c) \right| = \sum_{j=0}^{k-1} \bar{\chi}(c(c_j)) \log |\psi(c_j)|.$$

Nous déduisons alors de (31) l'identité

$$(33) \quad \sum_{i=0}^{k_1-1} \bar{\chi}(c_i) \log |\psi(c_i)| = (r/e)(1 - \bar{\chi}(\rho) + ehk/k_1)S(\chi).$$

Appliquons le th. 3, (ii) § 2.4 à $H \cap H(1)/K$, et substituons l'identité (33) dans la formule pour le produit $h_{H \cap H(1)} R_{H \cap H(1)}$; il vient

$$h_{\mathbb{H}\mathbb{H}(1)} R_{\mathbb{H}\mathbb{H}(1)} = h(e_{\mathbb{H}\mathbb{H}(1)}/e) \prod_{\chi \neq 1} \left| \sum_{i=0}^{k-1} \bar{\chi}(c_i) \log |\psi(c_i)| \right| / B(\mathbb{H}\mathbb{H}(1)) (6r)^{k-1} ;$$

Par conséquent le déterminant W_1 est $\neq 0$; les unités $\psi(c_i)/\psi(c_0)$, $i \in \{1, 2, \dots, k-1\}$, forment un système maximal d'unités indépendantes de $\mathbb{H}\mathbb{H}(1)$, et le quotient

$$e_{\mathbb{H}\mathbb{H}(1)}^{2^{k-1}} |W_1| / R_{\mathbb{H}\mathbb{H}(1)},$$

qui n'est autre que l'indice de $\Psi \cap E_{\mathbb{H}\mathbb{H}(1)}$ dans $E_{\mathbb{H}\mathbb{H}(1)}$, est égal à

$$B(\mathbb{H}\mathbb{H}(1)) (12r)^{k-1} e_{\mathbb{H}\mathbb{H}(1)} / h ; \text{ C.Q.F.D.}$$

6.3. Les groupes d'unités V , Λ et Λ^* .

Pour toute classe $C \in \text{Cl}(\mathbb{H}/K)$ (resp. $c \in \text{Cl}(\mathbb{H}\mathbb{H}(1)/K)$) désignons par $\alpha(C)$ (resp. $\alpha(c)$) un idéal entier, premier avec $12p$, qui appartient à C (resp. c). D'après le lemme 5 § 4.1, le résidu de $N(\alpha(C))$ (resp. $N(\alpha(c))$) modulo e_H (resp. $e_{\mathbb{H}\mathbb{H}(1)}$) ne dépend que de C (resp. c) ; en particulier, pour toutes classes $c \in \text{Cl}(\mathbb{H}\mathbb{H}(1)/K)$ et $C \in \text{Cl}(\mathbb{H}/K)$ telles que $C \subset c$, on a $N(\alpha(C)) \equiv N(\alpha(c)) \pmod{e_{\mathbb{H}\mathbb{H}(1)}}$. Pour tout idéal entier α de K , premier avec $12p$, nous noterons $C_\alpha \in \text{Cl}(\mathbb{H}/K)$ la classe de α .

Définition. Soit V le sous-groupe de Ψ formé des produits $\prod_{i=1}^{k-1} \psi_i^{n_i}$, où les entiers rationnels n_i , $i \in \{1, 2, \dots, k-1\}$, sont tels que

$$\sum_{i=1}^{k-1} n_i [N(\alpha(C_i)) - 1] \equiv 0 \pmod{e_H}.$$

Proposition 20. L'indice de V dans Ψ est égal à e_H/e .

Démonstration : d'après le th. 12, les unités ψ_i , $i \in \{1, 2, \dots, k-1\}$, sont multiplicativement indépendantes ; par conséquent l'application ρ , qui à un produit

$$\prod_{i=1}^{k-1} \psi_i$$

fait correspondre le résidu modulo e_H de la somme

$$\sum_{i=1}^{k-1} n_i [N(\alpha(C_i)) - 1],$$

définit un homomorphisme de Ψ dans le groupe des résidus modulo e_H dont le noyau est V . D'après le lemme 6 § 4.1, l'image de ρ est le groupe des résidus modulo e_H congrus à 0 modulo e ; par conséquent l'indice de V dans Ψ est égal à e_H/e ; C.Q.F.D.

Théorème 14. On a $V \subset \Delta_{H\Omega H(1)}^r V_H$ et $V_H \subset \Delta_{H\Omega H(1)}^r V$. Tout élément de V est une puissance r-ième dans H .

Démonstration : soient n_i , $i \in (1, 2, \dots, k-1)$, des entiers rationnels tels que

$$\sum_{i=1}^{k-1} n_i [N(\alpha(C_i)) - 1] \equiv 0 \pmod{e_H};$$

posons $\phi = \prod_{i=1}^{k-1} \phi_i^{n_i}$, $\varphi = \prod_{i=1}^{k-1} \varphi_{H,i}^{n_i}$ et $\delta = \prod_{i=1}^{k-1} (\delta_{H\Omega H(1)}(c(C_i)) / \delta_{H\Omega H(1)}(c_0))^{n_i}$.

Les produits ϕ , φ et δ appartiennent respectivement à V , V_H et $\Delta_{H\Omega H(1)}$, et on a $\phi = \delta^r \varphi$ et $\varphi = \delta^{-r} \phi$; d'où

$$V \subset \Delta_{H\Omega H(1)}^r V_H \text{ et } V_H \subset \Delta_{H\Omega H(1)}^r V.$$

D'après le th. 9 § 4.5, tout élément de V_H est une puissance r-ième dans H ; par conséquent tout élément de $V \subset \Delta_{H\Omega H(1)}^r V_H$ est également une puissance r-ième dans H ; C.Q.F.D.

Définitions. On déduit du th. 14 l'existence d'un plus grand sous-groupe Λ de E_H tel que $\Lambda^r = V$. On pose $\Lambda^* = \mu_e \Lambda$.

Proposition 21.

(i) Les groupes V , Ψ , Λ et Λ^* sont des sous-groupes d'indices finis de

E_H ;

(ii) Pour tout automorphisme σ de H/K , on a $V^\sigma = V$, $\Psi^\sigma = \Psi$, $\Lambda^\sigma = \Lambda$ et $\Lambda^{*\sigma} = \Lambda^*$;

(iii) On a $\Psi^{12/e} \subset \Lambda \subset \Lambda^* \subset \mathbb{C}_H \subset \mathbb{F}_H$ et $V \subset \Psi$.

Démonstration : l'assertion (i) résulte immédiatement du th. 12 et de la proposition 20. L'assertion (ii) est essentiellement triviale. On déduit du th. 14

l'inclusion $V \subset \Delta_{H\Omega H(1)}^r \Omega_H^r$, d'où $\Lambda \subset \Delta_{H\Omega H(1)} \Omega_H$ et par conséquent $\Lambda^* = \mu_e \Lambda \subset \mu_e \Delta_{H\Omega H(1)} \Omega_H \subset \mathbb{C}_H$. D'autre part, d'après le lemme 7, nous savons que $e_H | 12p^m$, et pour tout idéal entier α de K , premier avec e , nous avons $N(\alpha) - 1 \equiv 0 \pmod{e}$. Il en résulte que $\phi_i^{12p^m/e}$ appartient à V pour tout $i \in \{1, 2, \dots, k-1\}$; par conséquent nous avons

$$\Psi^{12p^m/e} \subset \Lambda^r \subset \Lambda^p, \text{ d'où } \Psi^{12/e} \subset \Lambda.$$

Les autres inclusions de l'assertion (iii) sont triviales.

6.4. Intersections des groupes d'unités V, Ψ, Λ et Λ^* avec $\mathbb{F}_{H\Omega H(1)}$.

Démontrons d'abord le résultat suivant :

Proposition 22. On a $N_{H/H\Omega H(1)}(\Phi_H) \subset \Omega_{H\Omega H(1)}^r$.

Démonstration : d'après le th. 2, (i) et (iii) § 2.3, pour tout

$i \in \{1, 2, \dots, k-1\}$, on a

$$N_{H/H\Omega H(1)}(\phi_{H,i}^e) = N_{H(1)/H\Omega H(1)}(\Delta(\mathfrak{t}_i)\Delta(\mathfrak{p})/\Delta(\mathfrak{t}_i\mathfrak{p})\Delta(\sigma))^r,$$

où \mathfrak{t}_i est un idéal qui appartient à $c(C_i)^{-1}$. Il résulte des considérations du § 3.2, que toutes les racines e -ièmes de

$$N_{H(1)/H\Omega H(1)}(\Delta(\mathfrak{t}_i)\Delta(\mathfrak{p})/\Delta(\mathfrak{t}_i\mathfrak{p})\Delta(\sigma))$$

appartiennent à $\Omega_{H\Omega H(1)}$; par conséquent on a $N_{H/H\Omega H(1)}(\Phi_H) \subset \Omega_{H\Omega H(1)}^r$; C.Q.F.D.

La proposition 22 a les conséquences suivantes :

Corollaire 1. On a $\Psi \cap \mathbb{F}_{H\Omega H(1)} \subset \Omega_{H\Omega H(1)}^r$.

Démonstration : d'après le th. 13, on a $\Psi \cap E_{H\Omega H(1)} = N_H/H\Omega H(1) \cdot (\Psi)$; comme $\Psi \subset \Delta_{H\Omega H(1)}^r \cdot \Phi_H$, on déduit de la proposition 22 que $N_H/H\Omega H(1) \cdot (\Psi) \subset (\Delta_{H\Omega H(1)} \cdot \Omega_{H\Omega H(1)}^r)^r$. Il en résulte que $\Psi \cap E_{H\Omega H(1)} \subset \Omega_{H\Omega H(1)}^r$, puisque $\Delta_{H\Omega H(1)} \subset \Omega_{H\Omega H(1)}^r$ d'après la proposition 6, (iii) § 3.2.

Corollaire 2. Le groupe $\Lambda \cap E_{H\Omega H(1)}$ est le plus grand sous-groupe de $E_{H\Omega H(1)}$ tel que $(\Lambda \cap E_{H\Omega H(1)})^r = V \cap E_{H\Omega H(1)}$.

Démonstration : nous avons $V \subset \Psi$, d'où $V \cap E_{H\Omega H(1)} \subset \Omega_{H\Omega H(1)}^r$ d'après le corollaire 1. Par définition, le groupe $\Lambda \cap E_{H\Omega H(1)}$ est l'ensemble des racines r -ièmes d'éléments de V qui appartiennent à $E_{H\Omega H(1)}$; comme $V \cap E_{H\Omega H(1)} \subset \Omega_{H\Omega H(1)}^r$, tout élément de $V \cap E_{H\Omega H(1)}$ possède une telle racine dans $E_{H\Omega H(1)}$; ce qui démontre le corollaire 2.

Corollaire 3. On a $\Lambda^* \cap E_{H\Omega H(1)} = \mu_{e_{H\Omega H(1)}} (\Lambda \cap E_{H\Omega H(1)})$.

Démonstration : il résulte du corollaire 2, que tout élément de $\Lambda^* \cap E_{H\Omega H(1)}$ est le produit d'un élément de $\Lambda \cap E_{H\Omega H(1)}$ et d'une racine de l'unité, d'où le corollaire 3.

Corollaire 4. On a $\Lambda^* \cap E_{H\Omega H(1)} \subset \mathfrak{E}_{H\Omega H(1)}$.

Démonstration : d'après le corollaire 2, on a

$$(\Lambda \cap E_{H\Omega H(1)})^r = V \cap E_{H\Omega H(1)} \subset \Omega_{H\Omega H(1)}^r,$$

d'où

$$\Lambda \cap E_{H\Omega H(1)} \subset \mu_{e_{H\Omega H(1)}} \Omega_{H\Omega H(1)}^r.$$

Par conséquent

$$\Lambda^* \cap E_{H\Omega H(1)} = \mu_{e_{H\Omega H(1)}} (\Lambda \cap E_{H\Omega H(1)})$$

est contenu dans

$$\mathfrak{E}_{H\Omega H(1)} = \mu_{e_{H\Omega H(1)}} \Omega_{H\Omega H(1)}^r ; \text{ C.Q.F.D.}$$

Démontrons maintenant les résultats suivants :

Proposition 23. Le groupe $N_{H/H\Omega H(1)}(v)$ est l'ensemble des produits

$\prod_{i=1}^{k_1-1} (\psi(c_i)/\psi(c_0))^{n_i}$, où les entiers rationnels n_i , $i \in (1, 2, \dots, k_1-1)$, sont tels que

$$\sum_{i=1}^{k_1-1} n_i [N(\alpha(c_i)) - 1] \equiv 0 \pmod{e_{H\Omega H(1)}}.$$

Démonstration : soit w un élément de v , et soient n_i , $i \in (1, 2, \dots, k_1-1)$, des entiers rationnels tels que

$$(34) \quad \sum_{i=1}^{k_1-1} n_i [N(\alpha(c_i)) - 1] \equiv 0 \pmod{e_H}$$

et
$$w = \prod_{i=1}^{k_1-1} \psi_i^{n_i}.$$

Posons
$$m_j = \sum_{\{i | c_i \subset c_j\}} n_i, \quad j \in (1, 2, \dots, k_1-1);$$

nous déduisons de (34) la congruence

$$\sum_{j=1}^{k_1-1} m_j [N(\alpha(c_j)) - 1] \equiv 0 \pmod{e_{H\Omega H(1)}},$$

et, d'après la proposition 19, (i), on a

$$N_{H/H\Omega H(1)}(w) = \prod_{j=1}^{k_1-1} (\psi(c_j)/\psi(c_0))^{m_j}.$$

Réciproquement, soient n_i , $i \in (1, 2, \dots, k_1-1)$, des entiers rationnels tels que

$$\sum_{i=1}^{k_1-1} n_i [N(\alpha(c_i)) - 1] \equiv 0 \pmod{e_{H\Omega H(1)}}$$

posons $w = \prod_{i=1}^{k_1-1} (\psi(c_i)/\psi(c_0))^{n_i}$. Comme dans la démonstration de la proposition 11 § 4.4, nous pouvons trouver des idéaux entiers $\alpha_1, \alpha_2, \dots, \alpha_s \in c_0$, premiers avec $12p$, et des entiers rationnels m_1, m_2, \dots, m_s , tels que

$$(23) \quad \sum_{j=1}^s m_j (N(\alpha_j) - 1) + \sum_{i=1}^{k_1-1} n_i [N(\alpha(c_i)) - 1] = 0.$$

Posons
$$w' = \prod_{j=1}^s (\psi(c_{\alpha_j})/\psi(c_0))^{m_j} \times \prod_{i=1}^{k_1-1} (\psi(c_{\alpha(c_i)})/\psi(c_0))^{n_i};$$

on déduit de la proposition 19, (i) que $w = N_{H/H\Omega H(1)}(w')$, et il résulte de (23) que w' est un élément de V . La proposition 23 est démontrée.

Corollaire. L'indice de $N_{H/H\Omega H(1)}(V)$ dans $\Psi \cap E_{H\Omega H(1)}$ est égal à $e_{H\Omega H(1)}/e$.

Démonstration : d'après le th. 13, les unités $\phi(c_i)/\phi(c_0)$, $i \in \{1, 2, \dots, k-1\}$, sont multiplicativement indépendantes ; par conséquent l'application ρ , qui à un produit

$$\prod_{i=1}^{k-1} (\phi(c_j)/\phi(c_0))^{n_i}$$

fait correspondre le résidu modulo $e_{H\Omega H(1)}$ de la somme

$$\sum_{i=1}^{k-1} n_i [N(\alpha(c_i)) - 1],$$

définit un homomorphisme du groupe $\Psi \cap E_{H\Omega H(1)}$ dans le groupe des résidus modulo $e_{H\Omega H(1)}$. D'après la proposition 23, le noyau de ρ est $N_{H/H\Omega H(1)}(V)$; et d'après le lemme 6 § 4.1, l'image de ρ est le groupe des résidus modulo $e_{H\Omega H(1)}$ congrus à zéro modulo e . Par conséquent l'indice de $N_{H/H\Omega H(1)}(V)$ dans $\Psi \cap E_{H\Omega H(1)}$ est égal à $e_{H\Omega H(1)}/e$; C.Q.F.D.

Proposition 24. On a $N_{H/H\Omega H(1)}(V) \subset (\Lambda \cap E_{H\Omega H(1)})^x \subset \Psi \cap E_{H\Omega H(1)}$.

Démonstration : on a

$$N_{H/H\Omega H(1)}(V) = N_{H/H\Omega H(1)}(\Lambda^x) \subset (\Lambda \cap E_{H\Omega H(1)})^x$$

et $(\Lambda \cap E_{H\Omega H(1)})^x \subset \Lambda^x \cap E_{H\Omega H(1)} = V \cap E_{H\Omega H(1)}$;

la proposition 24 résulte alors de ce que $V \cap E_{H\Omega H(1)} \subset \Psi \cap E_{H\Omega H(1)}$, puisque $V \subset \Psi$.

Définition. On pose $\mu = (\Psi \cap E_{H\Omega H(1)} : (\Lambda \cap E_{H\Omega H(1)})^x)$. D'après le corollaire de la proposition 23, l'entier μ divise $e_{H\Omega H(1)}/e$; comme $e_{H\Omega H(1)}$ divise 12, on en déduit que μ divise 6.

Nous sommes maintenant en mesure de démontrer le résultat suivant :

Théorème 15. Soit $B(H \cap H(1))$ l'entier défini dans le th. 12.

(i) L'indice de Λ^* dans E_H est donné par la formule

$$(E_H : \Lambda^*) = B(H \cap H(1))_1 2^{k-1} h_H / h ;$$

(ii) L'indice de $\Lambda^* \cap E_{H \cap H(1)}$ dans $E_{H \cap H(1)}$ est donné par la formule

$$(E_{H \cap H(1)} : \Lambda^* \cap E_{H \cap H(1)}) = B(H \cap H(1))_1 2^{k-1} (\mu_{e_{H \cap H(1)}})^{h_{H \cap H(1)}} / h .$$

Démonstration : d'après le th. 12, le groupe Ψ est engendré par $k-1$ unités indépendantes ; par conséquent V , qui est un sous-groupe d'indice fini de Ψ , est également engendré par $k-1$ unités indépendantes. Il en résulte que nous pouvons trouver un sous-groupe A de Λ , tel que $A^r = V$, $A \cap \mu_{e_H} = \{1\}$ et $\Lambda^* = \mu_{e_H} A$. Nous avons :

$$(\Lambda^* : V) = e_H(A : V) = e_H(A : A^r) = e_H r^{k-1} .$$

La formule du th. 15, (i) résulte alors de la détermination des indices $(E_H : \Psi)$ et $(\Psi : V)$ effectuée dans le th. 12 et la proposition 20.

De même, d'après le th. 13, le groupe $\Psi \cap E_{H \cap H(1)}$ est engendré par k_1-1 unités indépendantes ; par conséquent $(\Lambda \cap E_{H \cap H(1)})^r$, qui est un sous-groupe d'indice fini de $\Psi \cap E_{H \cap H(1)}$ est également engendré par k_1-1 unités indépendantes. Il en résulte que nous pouvons trouver un sous-groupe B de $\Lambda \cap E_{H \cap H(1)}$ tel que

$$B^r = (\Lambda \cap E_{H \cap H(1)})^r \text{ et } B \cap \mu_{e_{H \cap H(1)}} = \{1\} ;$$

nous déduisons du corollaire 3 de la proposition 22 que $\mu_{e_{H \cap H(1)}} B = \Lambda^* \cap E_{H \cap H(1)}$.

Nous avons

$$(\Lambda^* \cap E_{H \cap H(1)} : (\Lambda \cap E_{H \cap H(1)})^r) = (\Lambda^* \cap E_{H \cap H(1)} : B^r) = e_{H \cap H(1)} (B : B^r) = e_{H \cap H(1)}^r r^{k_1-1} .$$

La formule du th. 15, (ii) résulte alors de la définition de μ et de la détermination de l'indice $(E_{H \cap H(1)} : \Psi \cap E_{H \cap H(1)})$ effectuée dans le th. 13.

6.5. Formules pour le nombre de classes.

La possibilité d'utiliser le groupe Λ^* comme intermédiaire pour déterminer l'indice $(E_H : \mathfrak{E}_E)$ repose sur le résultat suivant :

Proposition 25. On a $\mathfrak{E}_{H\Omega H(1)} \Lambda^* = \mathfrak{E}_H$.

Démonstration : d'après le th. 14, on a

$$V \subset \Delta_{H\Omega H(1)}^r V_H = \Delta_{H\Omega H(1)}^r \Omega_H^r,$$

d'où $\Lambda \subset \Delta_{H\Omega H(1)} \Omega_H$. Il en résulte que

$$\Lambda^* \subset \mu_{e_H} \Delta_{H\Omega H(1)} \Omega_H \subset \mathfrak{E}_H, \text{ d'où } \mathfrak{E}_{H\Omega H(1)} \Lambda^* \subset \mathfrak{E}_H.$$

Réciproquement, d'après le th. 14, on a

$$V_H \subset \Delta_{H\Omega H(1)}^r V = \Delta_{H\Omega H(1)}^r \Lambda^r,$$

d'où $\Omega_H \subset \Delta_{H\Omega H(1)} \Lambda$ et par conséquent $\mu_{e_H} \Omega_H \subset \Delta_{H\Omega H(1)} \Lambda^*$. Finalement,

il en résulte que $\mathfrak{E}_H = \mu_{e_H} \Omega_{H\Omega H(1)} \Omega_H \subset \Lambda^* \mathfrak{E}_{H\Omega H(1)}$.

La proposition 25 est démontrée.

Déduisons de la proposition 25 le résultat suivant :

Proposition 26. On a $\mathfrak{E}_H \cap E_{H\Omega H(1)} = \mathfrak{E}_{H\Omega H(1)}$.

Démonstration : d'après la proposition 25, on a

$$\mathfrak{E}_H \cap E_{H\Omega H(1)} = (\mathfrak{E}_{H\Omega H(1)} \Lambda^*) \cap E_{H\Omega H(1)} = \mathfrak{E}_{H\Omega H(1)} (\Lambda^* \cap E_{H\Omega H(1)}).$$

Or, d'après le corollaire 4 de la proposition 22, on a $\Lambda^* \cap E_{H\Omega H(1)} \subset \mathfrak{E}_{H\Omega H(1)}$;

il en résulte que $\mathfrak{E}_H \cap E_{H\Omega H(1)} = \mathfrak{E}_{H\Omega H(1)}$; C.Q.F.D.

Nous pouvons maintenant déterminer l'indice $(E_H : \mathfrak{E}_H)$.

Théorème 16. Soit H une extension abélienne de K , de conducteur puissance d'un idéal premier. L'indice de \mathfrak{E}_H dans E_H est donné par la formule

$$(E_H : \mathfrak{E}_H) = \lambda h_H / [HH(1) : H],$$

où $\lambda = 12^{[H:K]-1} e/e_H$ lorsque H/K est non ramifiée, et $\lambda = 12^{[H:K]-1} / \mu$ lorsque

H/K est ramifiée (l'entier μ étant le diviseur de $e_{H \cap H(1)}$) /e défini à la suite de la proposition 24 § 6.4).

Démonstration : lorsque H/K est non ramifiée l'énoncé du th. 16 reprend la formule du th. 6 § 3.2.

Supposons H/K ramifiée. D'après la proposition 25, on a

$$E_H / \mathfrak{E}_H = E_H / \mathfrak{E}_{H \cap H(1)} \Lambda^* \approx (E_H / \Lambda^*) / (\mathfrak{E}_{H \cap H(1)} \Lambda^* / \Lambda^*) .$$

D'après le corollaire 4 de la proposition 22, on a $\Lambda^* \cap E_{H \cap H(1)} \subset \mathfrak{E}_{H \cap H(1)}$; et, d'après le th. 15, l'indice de $\Lambda^* \cap E_{H \cap H(1)}$ dans $\mathfrak{E}_{H \cap H(1)}$ est fini. Par conséquent le groupe

$$\mathfrak{E}_{H \cap H(1)} \Lambda^* / \Lambda^* \approx \mathfrak{E}_{H \cap H(1)} / \Lambda^* \cap E_{H \cap H(1)}$$

est fini, et on a

$$(E_H : \mathfrak{E}_H) = (E_H : \Lambda^*) / (\mathfrak{E}_{H \cap H(1)} : \Lambda^* \cap E_{H \cap H(1)}) , \text{ d'où}$$

$$(35) \quad (E_H : \mathfrak{E}_H) = (E_{H \cap H(1)} : \mathfrak{E}_{H \cap H(1)}) (E_H : \Lambda^*) / (E_{H \cap H(1)} : \Lambda^* \cap E_{H \cap H(1)}) .$$

En utilisant la formule pour $(E_{H \cap H(1)} : \mathfrak{E}_{H \cap H(1)})$ donnée par le th. 6 § 3.2 et les formules du th. 15, nous en déduisons l'égalité

$$(E_H : \mathfrak{E}_H) = 12^{[H:K]-1} n_H / \mu [H(1) : H \cap H(1)] ;$$

ce qui est la formule du th. 16 puisque

$$[HH(1) : H] = [H(1) : H \cap H(1)] .$$

Remarque. Esquissons une alternative pour la démonstration du th. 16.

Soit a un entier > 0 . Pour toute classe $c \in Cl(H/K)$, posons

$$\psi_a(c) = \delta_{H \cap H(1)}(c(c))^{ar} \varphi_H(c) ;$$

et soit $B(a, H \cap H(1))$ l'entier > 0 défini par

$$B(a, H \cap H(1)) = \prod_{\substack{\chi \neq 1 \\ \chi \in Cl(H \cap H(1))/K}} (1 - \bar{\chi}(a) + a\epsilon h/k_1)$$

lorsque $H \cap H_{(1)} \neq K$, et par $B(a, K) = 1$. Comme dans le th. 12, le groupe Ψ_a engendré par les quotients $\psi_a(C)/\psi_a(C_0)$, $C \in \text{Cl}(H/K)$, est un sous-groupe d'indice fini de E_H , cet indice est donné par la formule :

$$(36) \quad (E_H : \Psi_a) = B(a, H \cap H_{(1)})(12r)^{k-1} e_{H/H} / h ;$$

et comme dans le th. 13, le groupe $\Psi_a \cap E_{H \cap H_{(1)}}$ est de son côté un sous-groupe d'indice fini de $E_{H \cap H_{(1)}}$, cet indice est donné par la formule

$$(37) \quad (E_{H \cap H_{(1)}} : \Psi_a \cap E_{H \cap H_{(1)}}) = B(a, H \cap H_{(1)})(12r)^{k_1-1} e_{H \cap H_{(1)}/h} .$$

Soit V_a le sous-groupe de Ψ_a formé des produits $\prod_{C \in \text{Cl}(H/K)} \psi_a(C)^{n(C)}$, où les entiers rationnels $n(C)$, $C \in \text{Cl}(H/K)$, sont tels que

$$\sum_{C \in \text{Cl}(H/K)} n(C) = 0 \quad \text{et} \quad \sum_{C \in \text{Cl}(H/K)} n(C) N(\alpha(C)) \equiv 0 \pmod{e_H} .$$

Comme dans le th. 14, nous avons

$$V_a \subset \Delta_{H \cap H_{(1)}}^r V_H \quad \text{et} \quad V_H \subset \Delta_{H \cap H_{(1)}}^r V_a ,$$

et tout élément de V_a est une puissance r -ième dans H . Par conséquent il existe un plus grand sous-groupe Λ_a de E_H tel que $\Lambda_a^r = V_a$; nous posons $\Lambda_a^* = \mu_e \Lambda_a$. On déduit alors de (36) que l'indice de Λ_a^* dans E_H est donné par la formule

$$(38) \quad (E_H : \Lambda_a^*) = B(a, H \cap H_{(1)}) 12^{k-1} h_H / h ;$$

et l'on déduit de (37) que l'indice de $\Lambda_a^* \cap E_{H \cap H_{(1)}}$ dans $E_{H \cap H_{(1)}}$ donné par la formule

$$(39) \quad (E_{H \cap H_{(1)}} : \Lambda_a^* \cap E_{H \cap H_{(1)}}) = B(a, H \cap H_{(1)}) 12^{k_1-1} (\mu_e / e_{H \cap H_{(1)}})_{h_{H \cap H_{(1)}}} / h ,$$

avec $\mu = (\Psi \cap E_{H \cap H_{(1)}} : (\Lambda \cap E_{H \cap H_{(1)}})^r) = (\Psi_a \cap E_{H \cap H_{(1)}} : (\Lambda_a \cap E_{H \cap H_{(1)}})^r)$.

Comme dans la proposition 25 nous démontrons que $\mathfrak{E}_{H \cap H_{(1)}}^* \Lambda_a^* = \mathfrak{E}_H^*$; nous avons alors la formule

$$(40) \quad (E_H : \mathfrak{E}_H^*) = (E_{H \cap H_{(1)}} : \mathfrak{E}_{H \cap H_{(1)}}^*) (E_H : \Lambda_a^*) / (E_{H \cap H_{(1)}} : \Lambda_a^* \cap E_{H \cap H_{(1)}}) ,$$

analogue à la formule (35).

En utilisant, comme précédemment, la formule pour $(E_{H \cap H(1)} : \mathfrak{E}_{H \cap H(1)})$ donnée par le th. 6 § 3.2, nous déduisons des formules (38), (39) et (40) la formule du th. 16.

Démontrons la conséquence suivante du th. 16.

Corollaire. L'indice de $E_{H \cap H(1)} \mathfrak{E}_H$ dans E_H est donné par la formule

$$(E_H : E_{H \cap H(1)} \mathfrak{E}_H) = \lambda' n_H / h_{H \cap H(1)},$$

où $\lambda' = 12 \frac{[H:K] - [H \cap H(1):K]}{e_{H \cap H(1)} / \mu^e}$.

Démonstration : on a l'isomorphisme

$$E_H / E_{H \cap H(1)} \mathfrak{E}_H \approx (E_H / \mathfrak{E}_H) / (E_{H \cap H(1)} \mathfrak{E}_H / \mathfrak{E}_H);$$

or, d'après la proposition 26, on a

$$E_{H \cap H(1)} \mathfrak{E}_H / \mathfrak{E}_H \approx E_{H \cap H(1)} / \mathfrak{E}_H \cap E_{H \cap H(1)} = E_{H \cap H(1)} / \mathfrak{E}_{H \cap H(1)}.$$

Par conséquent, l'indice $(E_H : E_{H \cap H(1)} \mathfrak{E}_H)$ est le quotient des indices $(E_H : \mathfrak{E}_H)$ et $(E_{H \cap H(1)} : \mathfrak{E}_{H \cap H(1)})$, dont les valeurs nous sont données par le th. 16 ; la formule du corollaire s'en déduit immédiatement.

Remarque. On observera que le quotient $n_H / h_{H \cap H(1)}$ est nécessairement un nombre entier, puisque l'extension $H / H \cap H(1)$ est composée d'extensions totalement ramifiées, cf. CHEVALLEY [C].

APPENDICE

UNE ILLUSTRATION NUMERIQUE

Soit $K = \mathbb{Q}(\sqrt{-d})$, $d > 0$, un corps quadratique imaginaire de nombre de classes un. Il résulte de la remarque (9) de [H2] chap. III § 26 p. 75 que toutes les unités du corps $K(\sqrt{5}) = \mathbb{Q}(\sqrt{5}, \sqrt{-d})$ sont réelles. On déduit alors de la formule de Dirichlet pour le nombre de classes des corps biquadratiques imaginaires (cf. HASSE [H2] chap. III § 26 p. 74, formule (6)) que le nombre de classes de $K(\sqrt{5})$ est égal à la moitié du nombre de classes de $\mathbb{Q}(\sqrt{-5d})$. Or, suivant que $d = 1, 2, 3, 7, 11, 19, 43, 67$ ou 163 le nombre de classes de $\mathbb{Q}(\sqrt{-5d})$ est égal à $2, 2, 2, 2, 4, 8, 14, 18$ ou 30 . Par conséquent, le corps $K = \mathbb{Q}(\sqrt{-163})$ est le seul corps quadratique imaginaire de nombre de classes un, tel que $K(\sqrt{5})$ possède des classes d'idéaux d'ordre 5. Posons $\zeta = \exp(2\pi i/5)$; comme l'idéal (5) est inerte dans $K = \mathbb{Q}(\sqrt{-163})$, les extensions $H = K(\zeta)$ et $H' = K(\sqrt{5})$ de K ont l'idéal (5) pour conducteur; nous nous proposons de déterminer leurs groupes d'unités elliptiques respectifs.

§1. Désignons par \mathbb{Z} l'anneau des entiers rationnels et par \mathbb{F} le corps des résidus de \mathbb{Z} modulo 5. Notons respectivement G et G' les groupes de Galois de H/K et H'/K . Soit $C_{\sqrt{-163}} \in \text{Cl}(H/K)$ la classe de l'idéal $(\sqrt{-163})$; notons $\sigma = g(C_{\sqrt{-163}})$ l'automorphisme d'Artin de H/K associé à $C_{\sqrt{-163}}$. Nous avons les résultats suivants :

Lemme 9.

(i) Nous avons $\zeta_5^\sigma = \zeta_5^3$, et G est le groupe cyclique d'ordre 4 engendré par σ tandis que G' s'identifie au quotient $G/\{1, \sigma^2\}$.

(ii) Pour toute classe $C \in \text{Cl}(H/K)$, l'invariant $\varphi_H(C)$ est un nombre réel.

Démonstration :

L'assertion (i) résulte de ce que $N(\sqrt{-163}) \equiv 3 \pmod{5}$, et l'assertion (ii) de ce que $C_{\sqrt{-163}}$ - qui engendre $\text{Cl}(H/K)$ - est invariante par l'action de la conjugaison complexe.

Soit Υ le caractère de G à valeur dans \mathbb{F} , qui à tout automorphisme $\tau = g(C)$, $C \in \text{Cl}(H/K)$, associe le résidu de $N(\alpha(C))$ modulo 5, où $\alpha(C)$ est un idéal entier, premier avec 10, qui appartient à C ; cf. lemme 5 § 4.1. On a $\Upsilon(1) = 1$, $\Upsilon(\sigma) = 3$, $\Upsilon(\sigma^2) = 4$ et $\Upsilon(\sigma^3) = 2$. Le groupe des caractères de G est le groupe $\{1, \Upsilon, \Upsilon^2, \Upsilon^3\}$, et le groupe des caractères de G' est le groupe $\{1, \Upsilon^2\}$. Pour tout automorphisme $\tau = g(C)$, $C \in \text{Cl}(H/K)$, nous posons $\varphi_H(\tau) = \varphi_H(C)$. Nous avons les résultats suivants :

Lemme 10.

(i) Le groupe Φ_H est l'ensemble des produits

$$w = \prod_{i=1}^3 (\varphi_H(\sigma^i)/\varphi_H(1))^{n_i} \text{ avec } n_i \in \mathbb{Z} \text{ pour } i \in \{1,2,3\}.$$

(ii) Pour que le produit w appartienne à V_H il faut et il suffit que

$$\sum_{i=1}^3 n_i (\varphi(\sigma^i) - 1) \equiv 0 \pmod{5}.$$

Démonstration : le groupe Φ_H est l'ensemble des produits

$$w = \prod_{C \in \text{Cl}(H/K)} (\varphi_H(C)/\varphi_H(C_0))^{n(C)} \text{ avec } n(C) \in \mathbb{Z} \text{ pour } C \in \text{Cl}(H/K);$$

l'assertion (i) en résulte immédiatement.

Pour que le produit w appartienne à V_H il faut et il suffit que

$$\sum_{C \in \text{Cl}(H/K)} n(C) [N(\alpha(C)) - 1] \equiv 0 \pmod{e_H}; \text{ cf. } \S 4.4.$$

Or, pour tout idéal entier α de K , premier avec e , on a $N(\alpha) - 1 \equiv 0 \pmod{e}$; par conséquent, lorsque $(e_H/e, e) = 1$, une condition nécessaire et suffisante pour que w appartienne à V_H est que

$$\sum_{C \in \text{Cl}(H/K)} n(C) [N(\alpha(C)) - 1] \equiv 0 \pmod{e_H/e}.$$

Dans le cas présent, on a $e = 2$, $e_H = 10$ et $e_H/e = 5$; l'assertion (ii) résulte alors de ce qui précède, puisque pour tout automorphisme $\tau = g(C)$, $C \in \text{Cl}(H/K)$, on a $\varphi(\tau) \equiv N(\alpha(C)) \pmod{5}$.

L'action de G munit les groupes E_H et \mathfrak{E}_H ainsi que $E_{H'}$ et $\mathfrak{E}_{H'}$ de structures de $Z[G]$ -modules; par passage au quotient, on en déduit que l'action de G munit les groupes

$$E = E_H/E_H^5 \text{ et } \mathfrak{E} = \mathfrak{E}_H/\mathfrak{E}_H^5 \text{ ainsi que } E' = E_{H'}/E_{H'}^5 \text{ et } \mathfrak{E}' = \mathfrak{E}_{H'}/\mathfrak{E}_{H'}^5,$$

de structures de $F[G]$ -modules. A chaque caractère χ de G associons l'élément

$$1_\chi = \sum_{\tau \in G} \chi(\tau^{-1}) \tau \text{ de } F[G];$$

pour tout $i \in \{0,1,2,3\}$, posons

$$E_i = 1_{\varphi^i} \cdot E \text{ et } \mathfrak{E}_i = 1_{\varphi^i} \cdot \mathfrak{E};$$

nous avons

$$E = \bigoplus_{i=0}^3 E_i \text{ et } \mathfrak{E} = \bigoplus_{i=0}^3 \mathfrak{E}_i.$$

On démontre aisément le résultat suivant

Lemme 11. On a $E_0 = \mathfrak{E}_0 = \{1\}$ ainsi que $E' = E_2$ et $\mathfrak{E}' = \mathfrak{E}_2$.

Comme E_H et \mathfrak{E}_H sont chacun engendrés par $-\zeta$ et par 3 unités indépendantes, les 5-rangs des quotients E et \mathfrak{E} sont égaux à 4 ; on peut donc énoncer :

Lemme 12. Les 5-rangs de E et \mathfrak{E} sont égaux à 4.

Soient maintenant φ_1 , φ_2 et $\varphi_3 \in \Phi_H$ les unités réelles (cf. Lemme 9, (ii)) de H définies par :

$$\begin{aligned}\varphi_1 &= \varphi_H(1)\varphi_H(\sigma)^2/\varphi_H(\sigma^2)\varphi_H(\sigma^3)^2, \\ \varphi_2 &= \varphi_H(1)\varphi_H(\sigma^2)/\varphi_H(\sigma)\varphi_H(\sigma^3) \text{ et} \\ \varphi_3 &= \varphi_H(1)\varphi_H(\sigma^3)^2/\varphi_H(\sigma^2)\varphi_H(\sigma)^2.\end{aligned}$$

Pour tout $j \in \{1, 2, 3\}$, on a

$$(41) \quad \varphi_j \equiv \prod_{i=1}^3 (\varphi_H(\sigma^i)/\varphi_H(1)) \Psi^j(\sigma^{-i}) \text{ modulo } \Phi_H^5.$$

Comme la somme

$$\sum_{i=1}^3 \Psi^j(\sigma^{-i})(\Psi(\sigma) - 1)$$

est congrue à 0 ou 4 suivant que $j \in \{2, 3\}$ ou $j = 1$, on déduit du lemme 10, (ii)

que les nombres φ_1^5 , φ_2 et φ_3 appartiennent à V_H et que φ_1 n'y appartient pas ; puisque $\zeta \in \Omega_H$, les identités $w_2^5 = \varphi_2$ et $w_3^5 = \varphi_3$ définissent deux nombres réels w_2 et $w_3 \in \Omega_H$.

On démontre sans difficulté le résultat suivant.

Proposition 27.

(i) On a $w_2^\sigma = w_2^{-1}$ et $\mathfrak{E}_{H^1} = \{\pm w_2^n \mid n \in \mathbb{Z}\}$.

(ii) Les unités w_2 , w_3 et w_3^σ sont indépendantes, on a $\varphi_1 = w_3^{4\sigma}/w_3^3$ et \mathfrak{E}_H

est l'extension de degré deux du groupe

$$A = \{(-\zeta)^a w_2^b w_3^c w_3^{d\sigma} \mid a, b, c, d \in \mathbb{Z}\}$$

obtenu par l'adjonction des racines carrées de

$$(\varphi_H(\sigma)/\varphi_H(1))^2 = 1/w_2^5 w_3^3 w_3^\sigma.$$

Posons $w'_3 = w_2^2 w_3^\sigma$, on a $w_3^\sigma = w_3^{2\sigma} / w_3 = (w'_3)^2 / w_3^5$, d'où

$$w_3^\sigma \equiv w_3^4 \Psi^3(\sigma) \pmod{\mathfrak{L}_H^5}.$$

D'autre part, on déduit de (41) la relation

$$\varphi_1^\sigma \equiv \varphi_1^4 \Psi(\sigma) \pmod{\mathfrak{L}_H^5}.$$

Le groupe A est l'extension de degré 11 du groupe

$$B = \{(-\zeta_5)^a \varphi_1^b w_2^c w_3^d \mid a, b, c, d \in \mathbb{Z}\}$$

obtenue par adjonction de la racine 11-ième réelle de

$$w_3^{11} = (w'_3)^4 / \varphi_1.$$

On démontre alors sans difficultés le résultat suivant.

Proposition 28. On a les congruences

$$\zeta^\sigma \equiv \zeta^4 \Psi(\sigma) \pmod{\mathfrak{L}_H^5}, \quad \varphi_1^\sigma \equiv \varphi_1^4 \Psi(\sigma) \pmod{\mathfrak{L}_H^5};$$

$$w_2^\sigma \equiv w_2^4 \Psi^2(\sigma) \pmod{\mathfrak{L}_H^5} \text{ et } w_3^\sigma \equiv w_3^4 \Psi^3(\sigma) \pmod{\mathfrak{L}_H^5}.$$

Les classes de ζ et φ_1 modulo \mathfrak{L}_H^5 engendrent \mathfrak{L}_1 ; les classes de w_2 et w_3 modulo \mathfrak{L}_H^5 engendrent respectivement \mathfrak{L}_2 et \mathfrak{L}_3 .

§2. L'anneau des entiers σ de $K = \mathbb{Q}(\sqrt{-163})$ a pour base le couple $(1, (1 + \sqrt{-163})/2)$; nous posons $d = 163$ et $\alpha = (1 + \sqrt{-d})/2$. Il résulte des définitions §§2.2 et 4.5 que les invariants

$$\varphi_H(1), \varphi_H(\sigma), \varphi_H(\sigma^2) \text{ et } \varphi_H(\sigma^3)$$

sont donnés par les formules suivantes :

$$\varphi_H(1) = \varphi^{(12)5}(1/5; \sigma) \varphi^{(12)5}(\alpha/5; \sigma) \varphi^{(12)5}((\alpha-1)/5; \sigma),$$

$$\varphi_H(\sigma) = \varphi^{(12)5}((2\alpha-1)/5; \sigma) \varphi^{(12)5}((\alpha-2)/5; \sigma) \varphi^{(12)5}((1+\alpha)/5; \sigma),$$

$$\varphi_H(\sigma^2) = \varphi^{(12)5}(2/5; \sigma) \varphi^{(12)5}(2\alpha/5; \sigma) \varphi^{(12)5}((2\alpha-2)/5; \sigma) \text{ et}$$

$$\varphi_H(\sigma^3) = \varphi^{(12)5}((2+\alpha)/5; \sigma) \varphi^{(12)5}((1+2\alpha)/5; \sigma) \varphi^{(12)5}((2+2\alpha)/5; \sigma).$$

Ces formules permettent le calcul numérique des quotients

$$\varphi_H(\sigma)/\varphi_H(1), \varphi_H(\sigma^2)/\varphi_H(1) \text{ et } \varphi_H(\sigma^3)/\varphi_H(1).$$

Nous aurons besoin des résultats suivants.

Lemme 13. Soit $w \in \Omega_H$ une unité elliptique de H . La valeur absolue de w est une puissance 6-ième dans le plus grand sous-corps réel H_0 de H ; il existe un entier rationnel a tel que $w = \zeta^a |w|$.

Démonstration : soit α un idéal entier de K , premier avec 30 ; démontrons tout d'abord que le nombre $\theta^{(12)}(1/5, \sigma; \alpha)$ est une puissance 12-ième dans $H_{(5)}$. D'après les propositions 7 et 9 § 4.2, il suffit de vérifier que $L(\sigma; \alpha)$ est une puissance 12-ième dans $H_{(5)}$. Or, nous avons

$$L(\sigma; \alpha) = a^{12} M(\sigma)^{N(\alpha)-1},$$

où $a \in \sigma$ est un générateur de l'idéal α ; et l'invariant $M(\sigma)$ est donné par la formule :

$$M(\sigma) = 2^{30} 3^{24} / j^2(\sigma) (j(\sigma) - 1728)^3.$$

D'après [wb] § 125 p. 462 et § 134 p. 504, nous avons

$$j(\sigma) = -(64.3.5.23.29)^3 \text{ et } j(\sigma) - 1728 = -163(8.27.7.11.19.127)^2;$$

par conséquent $M(\sigma)$ est une puissance 6-ième dans $K = \mathbb{Q}(\sqrt{-163})$, et comme $N(\alpha) - 1 \equiv 0 \pmod{2}$ l'invariant $L(\sigma; \alpha)$ est une puissance 12-ième dans K . Le nombre $\theta^{(12)}(1/5, \sigma; \alpha)$ est donc une puissance 12-ième dans $H_{(5)}$.

D'autre part, d'après le th. 8 § 4.4 et les définitions 4.5, le groupe Ω_H est engendré par ζ et par les normes, relatives à $H_{(5)}/H$, des produits

$$\prod_{i=1}^m \theta^{(12)n_i}(1/5, \sigma; \alpha_i),$$

où les α_i sont des idéaux entiers de K , premiers avec 30 , et où les entiers rationnels n_i sont tels que

$$\sum_{i=1}^m n_i (N(\alpha_i) - 1) = 0.$$

Il résulte de ce qui précède que les unités $w \in \Omega_H$ sont des puissances 12-ièmes dans H .

Soit $u \in E_H$ une unité telle que $w = u^{12}$; comme H est une extension abélienne du corps des nombres rationnels nous pouvons appliquer la Satz 14 § 20 p. 54 de [H2] à l'extension H/H_0 ; nous en déduisons l'existence d'une unité réelle v et d'un nombre rationnel a , tels que $u^2 = (-\zeta)^a v$. D'où $w = \zeta^a v^6$, et par conséquent la valeur absolue $|w| = v^6$ est une puissance 6-ième dans H_0 ; C.Q.F.D.

Lemme 14. Pour tous entiers $u \in \{-2, -1, 0, 1, 2\}$ et $v \in \{0, 1, 2\}$, nous avons

$$|\varphi((u+v\alpha)/5; 1, \alpha)|^2 / M^2 A(u, v) B(u, v) C(u, v) = 1 + \varepsilon(u, v) ;$$

où $|\varepsilon(u, v)| < 5 \cdot 10^{-18}$, et où $M = 2 \exp(-\pi\sqrt{d}/12)$, $A(u, v) = \exp(-\pi v^2 \sqrt{d}/25)$,

$$B(u, v) = 2 \operatorname{ch}(\pi v \sqrt{d}/5) - 2 \cos(\pi(2u+v)/5)$$

et $C(u, v) = 1 + 2 \cos(\pi(2u+v)/5) \exp(-\pi(5-v)\sqrt{d}/5)$.

Démonstration : d'après le §1, pour tout $t \in \mathbb{C}$, nous avons

$$\varphi(t; 1, \alpha) = -M \sin(\pi t) \exp[\pi i t(t-\bar{t})/(\alpha-\bar{\alpha})] \prod_{n=1}^{\infty} (1 - 2q^n \cos(2\pi t) + q^{2n}).$$

Lorsque $t = (u+v\alpha)/5$, nous avons

$$|\exp(\pi i t(t-\bar{t})/(\alpha-\bar{\alpha}))|^2 = A(u, v) \quad \text{et} \quad |\sin(\pi t)|^2 = B(u, v).$$

De plus, on vérifie que

$$| [C(u, v) / \prod_{n=1}^{\infty} (1 - 2q^n \cos(2\pi t) + q^{2n})]^2 - 1 | < \exp(-\pi\sqrt{d}) ;$$

l'assertion du lemme résulte de l'estimation

$$0 < \exp(-\pi\sqrt{d}) < 5 \cdot 10^{-18}.$$

Lemme 15. Posons $\rho = \exp(-\pi\sqrt{d}/5)$; nous avons

$$\rho^{8/5} |\varphi_H(1)|^{1/30} / M^6 \mu(1) = 1 + \varepsilon_1,$$

$$\rho^{14/5} |\varphi_H(\sigma)|^{1/30} / M^6 \mu(\sigma) = 1 + \varepsilon_2,$$

$$\rho^{12/5} |\varphi_H(\sigma^2)|^{1/30} / M^6 \mu(\sigma^2) = 1 + \varepsilon_3 \quad \text{et}$$

$$\rho^{16/5} |\varphi_H(\sigma^3)|^{1/30} / M^6 \mu(\sigma^3) = 1 + \varepsilon_4 ;$$

où, pour tout $i \in \{1, 2, 3, 4\}$, on a $|\varepsilon_i| < 10^{-13}$, et où

$$\mu(1) = (2 - 2 \cos(2\pi/5))(1 - 2\rho \cos(\pi/5) + \rho^2)^2 ,$$

$$\mu(\sigma) = (1 - 2\rho^2)(1 - 2\rho \cos(3\pi/5) + \rho^2)^2(1 + 2\rho^3) ,$$

$$\mu(\sigma^2) = (2 - 2 \cos(4\pi/5))(1 - 2\rho^2 \cos(2\pi/5))^2(1 + 2\rho^3 \cos(2\pi/5))^2$$

et
$$\mu(\sigma^3) = (1 + 2\rho + \rho^2)(1 - 2\rho^2 \cos(4\pi/5))^2(1 + 2\rho^3 \cos(4\pi/5))^2 .$$

Démonstration : ce lemme résulte du lemme 14 et des formules pour les invariants

$$\varphi_H(1) , \varphi_H(\sigma) , \varphi_H(\sigma^2) \text{ et } \varphi_H(\sigma^3)$$

données au début de ce paragraphe, compte tenu de l'estimation

$$0 < 8 \exp(-4\pi\sqrt{d}/5) < 10^{-13} .$$

§3. Nous sommes maintenant en mesure de déterminer les nombres w_2 et w_3 .

a) Calcul de w_2 .

Posons $A = |w_2|^{1/6} + |w_2|^{-1/6}$, d'après le lemme 15, nous avons

$$\mu(\sigma)\mu(\sigma^3)|w_2|^{1/6}/\rho^2\mu(1)\mu(\sigma^2) = 1 + \varepsilon_5 \text{ avec } |\varepsilon_5| < 4.10^{-13} ;$$

par conséquent

$$A = (1 + \varepsilon_6) \exp(2\pi\sqrt{d}/5)\mu(\sigma)\mu(\sigma^3)/\mu(1)\mu(\sigma^2) \text{ avec } |\varepsilon_6| < 5.10^{-13} .$$

D'autre part, d'après le lemme 12, le nombre A est un entier rationnel ; comme $|w_2|^{1/6} < |w_2|^{-1/6}$, le nombre w_2 est donc la puissance 6-ième de la plus petite racine du polynôme $X^2 - AX + 1$.

Ayant fait le calcul à l'aide d'une calculatrice fournissant 10 chiffres significatifs, nous avons trouvé $A = 1\ 860\ 498,000$; la plus petite racine du polynôme $X^2 - 1\ 860\ 498 X + 1$ est $((\sqrt{5}-1)/2)^{30}$ d'où $w_2 = ((\sqrt{5}-1)/2)^{180}$.

Comme, d'après la proposition 27, on a

$$\mathfrak{E}_H = \{ \pm w_2^n \mid n \in \mathbf{Z} \} ,$$

et d'autre part

$$\mathbb{E}_H = \{ \pm ((\sqrt{5}-1)/2)^n \mid n \in \mathbf{Z} \} ,$$

il vient $(\mathbb{E}_H : \mathfrak{E}_H) = 180$. Comme $H_{(1)} = K$, l'entier μ défini § 6.4 est nécessairement 1 ; la formule du th. 16 § 6.5 nous donne alors

$$h_{H^1} = (E_{H^1} : \mathfrak{G}_{H^1})/12 = 15 ,$$

ce qui est la valeur déjà connue par la formule de Dirichlet.

β) Calcul de w_3 .

Posons

$$B = |w_3|^{1/6} + |w_3|^{-1/6} \quad \text{et} \quad C = |w_3^\sigma|^{1/6} + |w_3^\sigma|^{-1/6} .$$

D'après le lemme 15, nous avons

$$\mu(\sigma)^2 \mu(\sigma^2) |w_3|^{1/6} / \mu(\sigma^3)^2 \mu(1) = 1 + \varepsilon_7 \quad \text{avec} \quad |\varepsilon_7| < 6 \cdot 10^{-13}$$

$$\text{et} \quad \mu(\sigma^2)^2 \mu(\sigma^3) |w_3^\sigma|^{1/6} / \rho^2 \mu(1)^2 \mu(\sigma) = 1 + \varepsilon_8 \quad \text{avec} \quad |\varepsilon_8| < 6 \cdot 10^{-13} ;$$

par conséquent

$$B = (1 + \varepsilon_9) [(\mu(\sigma)^2 \mu(\sigma^2) / \mu(\sigma^3)^2 \mu(1)) + (\mu(\sigma^3)^2 \mu(1) / \mu(\sigma)^2 \mu(\sigma^2))] \quad \text{avec} \quad |\varepsilon_9| < 12 \cdot 10^{-13},$$

$$\text{et} \quad C = (1 + \varepsilon_{10}) \exp(2\pi\sqrt{5}/5) \mu(\sigma^2)^2 \mu(\sigma^3) / \mu(1)^2 \mu(\sigma) \quad \text{avec} \quad |\varepsilon_{10}| < 7 \cdot 10^{-13} .$$

D'autre part, d'après le lemme 12, les nombres $B+C$ et BC sont des entiers rationnels ; par conséquent B est la plus petite racine du polynôme $X^2 - (B+C)X + BC$.

Nous avons obtenu les valeurs suivantes pour $S = B+C$ et $P = BC$:
 $S = 63\,776\,191,00$ et $P = 191\,408\,459,0$. On vérifie que $S^2 - 4P = 5D^2$ avec
 $D = 28\,521\,577$; d'où $B = (S - D\sqrt{5})/2$ et $C = (S + D\sqrt{5})/2$.

Comme $|w_3|^{1/6} < |w_3|^{-1/6}$, nous en déduisons que w_3 est la puissance 6-ième de la plus petite racine du polynôme $X^2 - ((S - D\sqrt{5})/2)X + 1$. Il vient finalement

$$w_3 = (1/2)^6 [(S - D\sqrt{5})/2 - (\alpha - \beta\sqrt{5})\sqrt{163(5 - \sqrt{5})/2}]^6 ,$$

avec $\alpha = 1\,313\,302$ et $\beta = 587\,237$.

§4. Rappelons la définition des logarithmes de Kummer en l'adaptant à notre situation ; cf. HERBRAND [He] §3 pp. 421 à 423. Pour tout élément α de H , entier et premier avec 5, choisissons une fonction rationnelle $f(x)$, à coefficients 5-entiers dans K , telle que $f(\zeta) = \alpha$; pour $i \in \{1, 2, 3\}$, les classes modulo 5 des nombres

$$\ell^{(i)}(\alpha) = (d^i \log f(e^u)/du^i)(0)$$

ne dépendent que de α . Notons \mathfrak{l} l'idéal $(1-\zeta)$ de H ; on démontre sans peine les résultats suivants.

Lemme 16. Pour tous éléments μ et ν de H , entiers et premiers avec 5, et pour tout automorphisme τ de H/K :

(i) On a $\ell^{(i)}(\mu\nu) \equiv \ell^{(i)}(\mu) + \ell^{(i)}(\nu) \pmod{5}$, en particulier
 $\ell^{(i)}(\mu^5) \equiv 0 \pmod{5}$;

(ii) On a $\ell^{(i)}(\mu^\tau) \equiv \tau^i(\ell^{(i)}(\mu)) \pmod{5}$;

(iii) Si $\mu \equiv \nu \pmod{\mathfrak{l}^{i+1}}$, alors $\ell^{(i)}(\mu) \equiv \ell^{(i)}(\nu) \pmod{5}$.

Comme dans [He] §3 pp. 422-423, on démontre le résultat suivant.

Lemme 17. Pour qu'un élément μ de H , entier et premier avec 5, soit congru à une puissance 5-ième de H modulo \mathfrak{l}^5 , il faut et il suffit que

$$\ell^{(i)}(\mu) \equiv 0 \pmod{5} \quad \text{pour} \quad i \in \{1, 2, 3\}.$$

Posons $e_2 = ((\sqrt{5}-1)/2)^{36}$, de telle sorte que $w_2 = e_2^5$. La connaissance effective de w_3 , la proposition 28 et le lemme 16, nous permettent de dresser le tableau suivant, qui donne les valeurs de $\ell^{(i)}$, avec $i \in \{1, 2, 3\}$, pour les nombres

$$\zeta, \varphi_1 = w_3^{4\sigma}/w_3^3, e_2 \quad \text{et} \quad w'_3 = w_3^2 w_3^\sigma.$$

	$\ell^{(1)}$	$\ell^{(2)}$	$\ell^{(3)}$
ζ	1	0	0
φ_1	$-i\sqrt{5}$	0	0
e_2	0	1	0
w'_3	0	0	0

On déduit alors du lemme 17 le résultat suivant.

Proposition 29. Pour qu'un produit $\zeta^a \varphi_1^b e_2^c w_3^d$, avec $a, b, c, d \in \mathbb{Z}$, soit congru à une puissance 5-ième de H modulo \mathfrak{l}^5 , il faut et il suffit que
 $a \equiv b \equiv c \equiv 0 \pmod{5}$.

D'autre part, l'injection $\mathfrak{C}_H \hookrightarrow E_H$ définit un $F[G]$ -morphisme j de \mathfrak{C} dans E ; et nous avons $j(\mathfrak{C}_i) \subset E_i$ pour tout $i \in \{1, 2, 3\}$. Comme w_2 est une puissance

5-ième dans E_H nous avons $j(\xi_2) = 0$; d'autre part, d'après la proposition 29, pour que le produit $\zeta^a \varphi_1^b$ soit une puissance 5-ième dans H il faut et il suffit que $a \equiv b \equiv 0 \pmod{5}$, par conséquent j est une injection de ξ_1 dans E_1 ; le calcul nous a permis de vérifier que $w'_3 = w_3^2 w_3^\sigma$ n'était pas une puissance 5-ième dans H_0 , il en résulte que w'_3 n'est pas une puissance 5-ième dans H et j est une injection de ξ_3 dans E_3 . Enfin, comme e_2 n'est pas une puissance 5-ième dans H , la classe de e_2 modulo E_H^5 est un élément non trivial de E_2 ; vu que le 5-rang de $E = E_H/E_H^5$ est 4 d'après le lemme 12, nous en déduisons le résultat suivant.

Proposition 30. Les classes de ζ et φ_1 modulo E_H^5 engendrent E_1 ; les classes de e_2 et w'_3 modulo E_H engendrent respectivement E_2 et E_3 .

Nous déduisons immédiatement des propositions 28 et 30 le résultat suivant.

Corollaire 1. L'indice $(E_H : \xi_H)$ est divisible par 5 et n'est pas divisible par 5^2 .

Il résulte du th. 16 § 6.5 et du corollaire précédent que le corps H possède une unique extension abélienne non ramifiée de degré 5, que nous notons L ; nous avons le résultat suivant :

Corollaire 2. On a $L = H(\sqrt[5]{w'_3})$.

Démonstration : d'après le corollaire 1, il suffit de vérifier que $H(\sqrt[5]{w'_3})$ est bien une extension non ramifiée de H . Cela résulte du fait que w'_3 , congru à une puissance 5-ième de H modulo ℓ^5 d'après la proposition 29, est une unité primaire cf. th. N° XI p. 47 § 9 de HASSE [H3].

BIBLIOGRAPHIE

- [C] Claude CHEVALLEY.- Relation entre le nombre de classes d'un sous-corps et celui d'un sur-corps, C. R. Paris N° 191 pp. 257-258 (1931).
- [D] Max DEURING.- Die Klassenkörper der komplexen Multiplication, Enzycl. der Math. Wiss., Band I, 2, 23, Teubner (1958).
- [F] R. FUETER.- Die verallgemeinerte kroneckersche Grenzformel und ihre Anwendung auf die Berechnung der Klassenzahl, Rendiconti di Palermo, Tomo 29 pp. 380-395 (1910).
- [H1] Helmut HASSE.- Neue Begründung der komplexen Multiplication I, J. r. ang. Math. 157 pp. 115-139 (1927) ; II, ibid. 165 pp. 64-88 (1932).
- [H2] Helmut HASSE.- Über die Klassenzahl Abelscher Zahlkörper, Berlin (1952).
- [H3] Helmut HASSE.- Bericht über neuere Untersuchungen und Probleme der algebraischen Zahlkörper II, 2. Auflage Physica Verlag Würzburg-Wien (1965).
- [He] Jacques HERBRAND.- Sur les classes des corps circulaires, Journ. Math. Pures et Appliquées, 9ème Série N° 11 pp. 417-441 (1932).
- [M] Curt MEYER. Die Berechnung der Klassenzahl Abelscher Körper über quadratischen Zahlkörpern, Berlin (1957).
- [N1] A.P. NOVIKOV.- Sur le nombre de classes des extensions abéliennes d'un corps quadratique imaginaire (en russe). Isv. Akad. Nauk SSSR, N° 31 pp. 717-726 (1967).
- [N2] A.P. NOVIKOV.- Sur la régularité des idéaux premiers de degré un d'un corps quadratique imaginaire (en russe), Isv. Akad. Nauk SSSR, N° 33 pp. 1059-1079 (1969).
- [R] K. RAMACHANDRA.- Some applications of Kronecker's limit formulas, Ann. of Math. N° 80 pp. 104-148 (1964).
- [S] Carl Ludwig SIEGEL.- Lectures notes on advanced analytic number theory, Tata Inst. of Fund. Research, Bombay (1961).
- [Wb] Heinrich WEBER.- Lehrbuch der Algebra, 3-ième ed. Tome III, Strassburg (1909).
- [Wl] André WEIL.- Introduction à l'étude des variétés kählériennes, Hermann (1957).

Gilles ROBERT
14 rue Lacretelle
75015 PARIS
