Séminaire de Théorie des Nombres.

- Besançon -

Année 1974-1975

CALCUL DU NOMBRE DE CLASSES ET DES UNITES DES EXTENSIONS ABELIENNES REELLES DE $\mathbb{Q}$.

Georges GRAS - Marie-Nicole GRAS
Faculté des Sciences. Mathématiques .
25030 BESANCON CEDEX

Table des matières

CALCUL DU NOMBRE DE CLASSES ET DES UNITES DES EXTENSIONS ABELIENNES REELLES DE $\mathbb{Q}$.

par Georges GRAS et Marie-Nicole GRAS .

Introduction

Soient K un corps de nombres et A_K l'anneau des entiers de K ([14], chap. I, § 2) . Soient $\mathfrak{J}$ le groupe des idéaux fractionnaires de A_K et $\mathfrak{J}_o$ le sous-groupe de $\mathfrak{J}$ formé par les idéaux fractionnaires principaux au sens habituel ([14], chap. I, § 6) .

L'invariant le plus important concernant l'arithmétique dans A_K est le groupe des classes $\mathfrak{H}(K) = \mathfrak{J}/\mathfrak{J}_o$ qui est un groupe abélien fini ([25], p. 69) ; son ordre h_K (appelé le nombre de classes au sens ordinaire de K) est très difficile à calculer même dans des cas particuliers (voir cependant dans [4] et [28] le cas des extensions quadratiques qui est complètement résolu et permet d'élaborer des tables numériques ([22])) . L'importance du nombre de classes provient déjà du fait que lorsqu'il est égal à 1 , l'arithmétique dans A_K est relativement analogue à celle dans $\mathbb{Z}$ (notamment il y a unicité de la décomposition des éléments de A_K en facteurs irréductibles car ce dernier est principal) ; lorsque le nombre de classes est différent de 1 , certains problèmes sont aisément solubles à condition que ce nombre ne soit pas divisible par certains nombres premiers particuliers dépendant du problème considéré (par exemple : soit ℓ un nombre premier impair et soit ξ une racine primitive $\ell^{\text{è}}$ de l'unité ; si le nombre de classes du corps $\mathbb{Q}(\xi)$ n'est pas divisible par ℓ , alors le théorème de Fermat est vrai pour l'exposant ℓ ([2], chap. V, § 7, 1)) .

Un second invariant, tout aussi important pour l'arithmétique dans A_K , est constitué par le groupe des unités de A_K. Sa structure de $\mathbb{Z}$-module est connue grâce au théorème de Dirichlet ([25], chap. IV, §4), cependant, comme pour le nombre de classes, il n'existe pas d'algorithme valable pour tous les corps de nombres, permettant un calcul numérique des unités ; on connait quelques procédés applicables dans des cas particuliers , notamment pour le cas des corps quadratiques ([4])

et des extensions cycliques de degré 3 et 4 (Hasse) ; signalons qu'il existe un très grand nombre de travaux concernant le cas des corps quadratiques et le cas des corps cubiques (galoisiens ou non) que nous ne pouvons mentionner ici (le lecteur intéressé par les problèmes numériques en théorie des nombres lira [30] avec profit) .

Il y a trois grandes directions selon lesquelles on peut rechercher un algorithme pour le calcul du nombre de classes :

(i) Méthodes géométriques. On sait que toute classe de $\mathcal{S}(K)$ contient un idéal entier de norme majorée par la constante de Minkowski M ([14], chap. V, § 4) . Les idéaux entiers de norme inférieure à M sont en nombre fini ; le nombre de classes est donc obtenu après avoir trouvé toutes les relations de dépendance (modulo $\mathfrak{Z}_o$) qui existent entre ces idéaux (sinon on obtient un multiple de h_K (comme dans [11])) ; toute la difficulté est donc de prouver la principalité (ou la non principalité) d'un certain nombre d'idéaux ; mais dire que l'idéal entier $\mathfrak{a}$ est principal c'est dire qu'il existe $\alpha \in A_K$ tel que $\mathfrak{a} = (\alpha)A_K$, donc que l'équation diophantienne $N_{K/\mathbb{Q}}(\alpha) = \pm a$ (où $a \in \mathbb{N}^*$ désigne la norme absolue de l'idéal $\mathfrak{a}$ ([25], p. 62)) a une solution ; or on ne connait pas de critère général permettant de savoir si une telle équation est soluble ou non ; on ne peut même pas entreprendre une recherche systématique car les solutions éventuelles ne sont pas toujours bornées . Pour surmonter la difficulté, on est conduit à élaborer des algorithmes , de nature géométrique, dont la programmation est fort complexe (par exemple [29]) .

Cette méthode aboutit, par exemple, lorsque le nombre de classes est égal à 1 et que l'on a eu la chance de prouver que tous les idéaux considérés étaient principaux , c'est-à-dire de trouver une solution pour chacune des équations dont nous venons de parler (voir à ce sujet l'exemple instructif de [14], p. 121) .

(ii) Méthodes arithmétiques . Certaines méthodes à la fois algébriques et arithmétiques ne donnent que des diviseurs du nombre de classes (par exemple [6] , [7] , [8]) et sont plutôt intéressantes sur le plan théorique ; il y aurait dans cette direction un nombre considérable de publications à citer .

(iii) Méthodes analytiques . L'étude de la fonction $\zeta_K(s)$ du corps de nombres K conduit à la formule analytique du nombre de classes ([2], chap. V , § 1 , th. 2) qui est le point de départ de nombreuses méthodes . Malheureusement, les expressions de h_K qui s'en déduisent

sent font intervenir les unités fondamentales de K sous la forme du régulateur du corps ([2], chap. II, § 4) et ne sont pas de ce fait directement utilisables, à moins de calculer les unités fondamentales de K par une méthode géométrique indépendante .

Hasse montre dans [12] (§ I,5) que, lorsque $K/\mathbb{Q}$ est abélienne et imaginaire, h_K se décompose sous la forme $h_K = h^* h_o$, h^* (appelé le nombre de classes relatives) étant un entier calculable au moyen d'une formule ne faisant intervenir que des constantes arithmétiques élémentaires du corps considéré et h_o étant le nombre de classes du sous-corps réel maximal K_o de K .
Hasse ([12], § III, 20) montre aussi que le groupe des unités de K est connu dès que celui de K_o l'est . Ceci explique que l'on peut, dans le cas abélien, se limiter à l'étude du nombre de classes et des unités des corps abéliens réels .

Principe de la méthode proposée . Cet article illustre, dans le cas abélien réel, la méthode analytique que nous venons de rappeler . Son point de départ est un travail de Leopoldt ([15]) qui établit une interprétation arithmétique de la formule analytique du nombre de classes. Comme nous le rappelons dans la partie I , l'expression du nombre de classes d'un corps abélien réel trouvée par Leopoldt est de la forme

$h_K = \frac{Q_K}{Q_G} \prod_{\varkappa} h_\varkappa$, où les nombres Q_K , Q_G , $h_\varkappa$ sont des entiers rationnels et $\varkappa$ désigne un caractère de K (cf. partie I, § 1) ; Q_G est une constante ne dépendant que du groupe de Galois de $K/\mathbb{Q}$; Q_K est un " terme correctif " dépendant du groupe des unités de K , mais qui est relativement facile à déterminer car ses diviseurs premiers , possibles à priori , sont connus ; en outre, dans les cas les plus simples (notamment le cas où $K/\mathbb{Q}$ est cyclique de degré premier) , on a $Q_K/Q_G = 1$.
Pour chaque caractère $\varkappa$, le nombre $h_\varkappa$ est égal à l'indice dans un sous-groupe $E_\varkappa$ d'unités de K bien défini (mais que l'on ne connait pas numériquement) d'un sous-groupe d'unités $F_\varkappa$ qui lui est parfaitement connu numériquement, lorsque K est donné (unités cyclotomiques) . Ainsi le calcul de h_K repose-t-il essentiellement sur celui des $h_\varkappa = (E_\varkappa : F_\varkappa)$.

Notre méthode consiste en une exploitation convenable de la remarque très simple suivante : supposons que l'on ait trouvé une unité η de $F_\varkappa$ de la forme ϵ^p , $p > 1$, ϵ étant une unité de $F_\varkappa$ n'appartenant pas à $F_\varkappa$, alors le sous-groupe $F'_\varkappa$ de $E_\varkappa$ engendré par $E_\varkappa$ et ϵ vérifie $F_\varkappa \subset F'_\varkappa \subset E_\varkappa$ et l'indice $(E_\varkappa : F'_\varkappa)$ est strictement inférieur à $(E_\varkappa : F_\varkappa)$;

il suffit alors de recommencer l'opération à partir de $F'_\varkappa$; on obtient ainsi une suite de groupes $F_\varkappa$, $F'_\varkappa$, ... , $F_\varkappa^{(n)}$ et on aura $F_\varkappa^{(n)} = E_\varkappa$ à partir du moment où il sera impossible de trouver $\eta \in F_\varkappa^{(n)}$ puissance non triviale d'une unité ε n'appartenant pas à $F_\varkappa^{(n)}$. On obtient alors simultanément $E_\varkappa$ et l'indice cherché $h_\varkappa = (E_\varkappa : F_\varkappa)$.

Il est clair que le procédé, tout en étant fini, n'est pas borné à priori, ce qui explique qu'il soit nécessaire de majorer $h_\varkappa = (E_\varkappa : F_\varkappa)$ par une borne effectivement calculable . Ce premier problème est résolu dans la partie II et le majorant trouvé est fonction des données suivantes, où $K_\varkappa$ est un sous-corps de K dépendant de $\varkappa$: degré $[K_\varkappa : \mathbb{Q}]$, conducteur de $K_\varkappa$ et groupe $F_\varkappa$ des unités cyclotomiques . Le deuxième problème à résoudre est celui de savoir reconnaître, pour p donné, s'il existe une unité η de $F_\varkappa^{(i)}$, telle que $\eta = \varepsilon^p$, $\varepsilon \notin F_\varkappa^{(i)}$. Ce problème , plus simple que le précédent , est résolu dans la partie IV .

Bien que la majoration de $h_\varkappa$ utilise un résultat de géométrie des nombres (le théorème de Minkowski sur les réseaux ([25], p. 67)), l'obtention d'un majorant de $h_\varkappa$ repose essentiellement sur les propriétés arithmétiques des corps $K_\varkappa$. De par sa nature, cette méthode est propre au cas abélien et son inconvénient est de ne pas donner la structure du groupe des classes $\mathfrak{H}(K)$ (cependant de nombreux résultats purement arithmétiques du genre de ceux de [6] et de [7] doivent permettre de conclure dans beaucoup de cas). Par contre son intérêt réside dans le fait qu'elle donne simultanément le groupe des unités et le nombre de classes de K et que sa programmation sur ordinateur soit relativement aisée et performante (pour s'en convaincre, se reporter aux tables numériques de [9] où l'un des auteurs a traité par cette méthode le cas des extensions cubiques cycliques) .

Perspectives sur la méthode . Cette méthode doit pouvoir, à priori , traiter les extensions abéliennes réelles de degré quelconque. Bien entendu, le temps de calcul sur ordinateur ainsi que les ordres de grandeur des nombres manipulés sont des fonctions rapidement croissantes du degré et du conducteur, et les limites sont dues à des problèmes de programmation .

Cette méthode nous semble être la seule à pouvoir fournir un contre-exemple (s'il en existe) à l'existence d'une " unité de Minkowski" (voir à ce sujet le problème précisé par Brumer [3] et Payan [24]).

Enfin, après l'étude des résultats numériques fournis par les tables de [9], nous avons formulé une conjecture (partie V) qui établirait un lien non trivial entre la structure du groupe des classes et celle des groupes finis $E_\varkappa / F_\varkappa$.

I Préliminaires

1) Caractères des extensions abéliennes de $\mathbb{Q}$.

a) Conducteur de K . Soit K une extension abélienne de $\mathbb{Q}$, de degré g et de groupe de Galois G . On rappelle que, d'après le théorème de Kronecker-Weber ([14], p. 210) , K est contenue dans un corps cyclotomique $\mathbb{Q}^{(f)}$ ($\mathbb{Q}^{(f)}$ désignant l'extension engendrée sur $\mathbb{Q}$ par les racines $f^{\text{èmes}}$ de l'unité) ; le plus petit entier f tel que $K \subset \mathbb{Q}^{(f)}$ s'appelle le conducteur de K . On rappelle que le groupe de Galois de $\mathbb{Q}^{(f)}/\mathbb{Q}$ est canoniquement isomorphe au groupe multiplicatif $(\mathbb{Z}/f\mathbb{Z})^*$ ([25], p. 108). Soit H le sous-groupe de $(\mathbb{Z}/f\mathbb{Z})^*$ image de $\mathrm{Gal}(\mathbb{Q}^{(f)}/K)$ par cet isomorphisme . Alors G est isomorphe à $(\mathbb{Z}/f\mathbb{Z})^*/H$ et il est clair que K est entièrement déterminé par le couple (f, H) .

b) Caractères complexes de K . Soit $\mathfrak{X}'_{\mathbb{Q}^{(f)}}$ le groupe des caractères de degré 1 de $(\mathbb{Z}/f\mathbb{Z})^*$ à valeurs dans $\mathbb{C}^*$ (i.e. le groupe des homomorphismes de $(\mathbb{Z}/f\mathbb{Z})^*$ dans $\mathbb{C}^*$) . On appelle groupe des caractères complexes de K le sous-groupe $\mathfrak{X}'_K$ de $\mathfrak{X}'_{\mathbb{Q}^{(f)}}$ formé des éléments triviaux sur H : $\mathfrak{X}'_K = \{\varkappa' \in \mathfrak{X}'_{\mathbb{Q}^{(f)}} , \varkappa'(\bar{a}) = 1 , \text{ pour tout } \bar{a} \in H\}$. Les applications $\varkappa'$ sont en fait définies sur $(\mathbb{Z}/f\mathbb{Z})^*$ mais pour éviter un surcroit de notations, nous faisons les conventions d'écriture suivantes : soit $\bar{a} \in (\mathbb{Z}/f\mathbb{Z})^*$, $a \in \mathbb{Z}$; soit $\sigma \in \mathrm{Gal}(\mathbb{Q}^{(f)}/\mathbb{Q})$ correspondant à $\bar{a}$ par l'isomorphisme canonique $(\mathbb{Z}/f\mathbb{Z})^* \longrightarrow \mathrm{Gal}(\mathbb{Q}^{(f)}/\mathbb{Q})$ et soit $\bar{\sigma} \in G$ la classe de σ modulo H : on notera indifféremment par $\varkappa'(a)$, $\varkappa'(\sigma)$ ou $\varkappa'(\bar{\sigma})$ le nombre $\varkappa'(\bar{a})$. Pour tout élément $\varkappa'$ de $\mathfrak{X}'_K$, on notera $g_{\varkappa'}$ son ordre ; alors le groupe $\varkappa'(G)$ coïncide avec le groupe cyclique des racines $g_{\varkappa'}$-èmes de l'unité et son ordre , noté $\|\varkappa'(G)\|$, est égal à $g_{\varkappa'}$ (en effet, tout sous-groupe fini de $\mathbb{C}^*$ est cyclique ([25], p. 28)) .

c) Caractères rationnels de K . On définit sur $\mathfrak{X}'_K$ la relation d'équivalence suivante : soient $\varkappa'$ et ψ' deux éléments de $\mathfrak{X}'_K$; on dit que $\varkappa'$ et ψ' sont $\Gamma_{\mathbb{Q}}$-conjugués (cf. [27] p. 41) si $\psi' = \varkappa'^k$, avec k entier premier à l'ordre de $\varkappa'$. Il revient au même de dire que ψ' et $\varkappa'$ engendrent le même sous-groupe de $\mathfrak{X}'_K$; on vérifie que cette propriété est aussi équivalente à $\ker \varkappa' = \ker \psi'$.

Pour tout $\chi' \in \mathfrak{X}'_K$, on notera $\tilde{\chi}$ la $\Gamma_{\mathbb{Q}}$-classe de conjugaison de χ' ; on a $\tilde{\chi} = \{\chi'^k, (k, g_{\chi'}) = 1\}$; il en résulte que $\tilde{\chi}$ possède $\varphi(g_{\chi'})$ éléments (φ désignant la fonction d'Euler) et que les nombres

$\sum_{\psi' \in \tilde{\chi}} \psi'(\bar{a}) = \sum_{(k, g_{\chi'})=1} \chi'^k(\bar{a}) = \mathrm{Tr}_{\mathbb{Q}(g_{\chi'})/\mathbb{Q}}(\chi'(\bar{a}))$ sont des entiers rationnels pour tout $\bar{a} \in (\mathbb{Z}/f\mathbb{Z})^*$. On définit les applications χ :

$$\chi : (\mathbb{Z}/f\mathbb{Z})^* \longrightarrow \mathbb{Z} \quad \text{par} \quad \chi(\bar{a}) = \sum_{\psi' \in \tilde{\chi}} \psi'(\bar{a}) \ .$$

Ces applications sont appelées les <u>caractères rationnels irréductibles de</u> K (ou plus brièvement : les <u>caractères de</u> K) .
On notera par $\mathfrak{X}_K$ l'ensemble de ces caractères et on adoptera pour $\chi \in \mathfrak{X}_K$ les mêmes conventions d'écriture que celles introduites pour $\chi' \in \mathfrak{X}'_K$. L'élément neutre de $\mathfrak{X}'_K$ coïncide avec le caractère rationnel associé ; ces deux caractères seront notés 1 .

d) <u>Définition des corps</u> K_χ . Pour tout $\chi' \in \mathfrak{X}'_K$, on considère le sous-corps K_χ, de K fixe par $\mathrm{Ker}\,\chi'$; on a

$\mathrm{Gal}(K_\chi/\mathbb{Q}) \simeq (\mathbb{Z}/f\mathbb{Z})^*/\mathrm{Ker}\,\chi' \simeq \chi'((\mathbb{Z}/f\mathbb{Z})^*) \simeq \chi'(G)$ qui est un sous-groupe cyclique de $\mathbb{C}^*$; donc K_χ, est une extension <u>cyclique</u> de $\mathbb{Q}$; son degré est égal à $\|\chi'(G)\| = g_{\chi'}$; comme $\mathrm{Ker}\,\chi'$, K_χ, et $g_{\chi'}$ ne dépendent pas du choix de $\chi' \in \tilde{\chi}$, on peut les noter respectivement $\mathrm{Ker}\,\chi$, K_χ et g_χ ; on notera G_χ le groupe de Galois de $K_\chi/\mathbb{Q}$ et f_χ le conducteur de K_χ (on dit aussi que f_χ est le conducteur de χ et, par abus de langage , que $\mathrm{Ker}\,\chi$ est le noyau de χ et g_χ l'ordre de χ) .

Réciproquement, si k est un sous-corps cyclique contenu dans K et si τ engendre $\mathrm{Gal}(k/\mathbb{Q})$, on peut, en posant $\psi'(\tau) = \zeta$, ζ racine primitive de l'unité d'ordre $[k:\mathbb{Q}]$, définir un caractère ψ' de K dont le noyau est $\mathrm{Gal}(\mathbb{Q}^{(f)}/k)$, d'où $k = K_\psi$.

Ainsi , à toute extension abélienne K de $\mathbb{Q}$, on a associé la famille des sous-corps cycliques K_χ de K , et l'application $x \in \mathfrak{X}_K \longrightarrow K_\chi$ est une bijection de $\mathfrak{X}_K$ sur l'ensemble des sous-corps cycliques de K .

e) <u>Remarques</u> .

(i) L'intérêt de la notion de caractère de K réside dans le fait que l'étude des propriétés arithmétiques de K se ramène, pour l'essentiel, à l'étude des propriétés arithmétiques des corps K_χ , étude plus facile puisque les extensions $K_\chi/\mathbb{Q}$ sont cycliques .

(ii) Les définitions précédentes sont valables pour une extension abélienne réelle ou imaginaire . Par la suite, le corps K consi-

déré sera réel (cf. Introduction) ; du point de vue des caractères complexes, les corps réels sont caractérisés par le fait que pour tout $\varkappa' \in \mathfrak{X}'_K$, $\varkappa'(-1) = 1$.

2) L'algèbre $\mathbb{Q}[G]$. On appelle $\mathbb{Q}[G]$ la $\mathbb{Q}$-algèbre dont une $\mathbb{Q}$-base est constituée par la famille $(\sigma)_{\sigma \in G}$, le produit dans $\mathbb{Q}[G]$ étant défini à partir de celui dans G (cf. [13], p. 106) . Pour tout $\varkappa \in \mathfrak{X}_K$, soit $e_\varkappa = \frac{1}{g} \sum_{\sigma \in G} \varkappa(\sigma^{-1})_\sigma$; on vérifie que les $e_\varkappa$ forment un système d'idempotents orthogonaux de $\mathbb{Q}[G]$, c'est-à-dire que les $e_\varkappa$ vérifient :

$$e_\varkappa^2 = e_\varkappa \quad \text{pour tout } \varkappa ,$$
$$e_\varkappa e_\psi = 0 \quad \text{si } \psi \neq \varkappa ,$$
$$\sum_{\varkappa \in \mathfrak{X}_K} e_\varkappa = 1 ;$$

on a donc la décomposition $\mathbb{Q}[G] = \bigoplus_{\varkappa \in \mathfrak{X}_K} \mathbb{Q}[G] e_\varkappa$. Montrons que $\mathbb{Q}[G]e_\varkappa$ (considéré comme anneau d'unité $e_\varkappa$) est isomorphe au corps cyclotomique $\mathbb{Q}^{(g_\varkappa)}$ et que dans cet isomorphisme l'anneau des entiers $\mathbb{Z}^{(g_\varkappa)}$ de $\mathbb{Q}^{(g_\varkappa)}$ correspond à $\mathbb{Z}[G]e_\varkappa$ (cf. [23], 1ère partie) .

Soit $\sigma_\varkappa$ un élément de G dont l'image dans le groupe cyclique $G_\varkappa = \mathrm{Gal}(K_\varkappa/\mathbb{Q})$ soit génératrice . On considère l'homomorphisme d'anneaux $\mathbb{Q}[X] \longrightarrow \mathbb{Q}[G]e_\varkappa$.
$P \qquad\qquad P(\sigma_\varkappa)e_\varkappa$

Soit $\Phi_\varkappa$ le $g_\varkappa$ ème polynome cyclotomique ; on a $\Phi_\varkappa(X) = \prod_{(k, g_\varkappa)=1} (X - \zeta_\varkappa^k)$,

$\zeta_\varkappa$ désignant une racine primitive $g_\varkappa$ - ème de l'unité ; donc $\Phi_\varkappa(\sigma_\varkappa)e_\varkappa = \Big(\prod_{(k, g_\varkappa)=1} (\sigma_\varkappa - \zeta_\varkappa^k) \Big) e_\varkappa$. On remarque que

$e_\varkappa = \sum_{\varkappa' \in \tilde{\varkappa}} \frac{1}{g} \sum_{\sigma \in G} \varkappa'(\sigma^{-1})_\sigma$ et que $\sigma_\varkappa \sum_{\sigma \in G} \varkappa'(\sigma^{-1})_\sigma = \varkappa'(\sigma_\varkappa) \sum_{\sigma \in G} \varkappa'(\sigma^{-1})_\sigma$;

par choix de $\sigma_\varkappa$, $\varkappa'(\sigma_\varkappa)$ est une racine primitive $g_\varkappa$ - ème de l'unité ; donc $\varkappa'(\sigma_\varkappa) = \zeta_\varkappa^\lambda$, $(\lambda, g_\varkappa) = 1$, donc $\Big(\sum_{\sigma \in G} \varkappa'(\sigma^{-1})_\sigma \Big)(\sigma_\varkappa - \zeta_\varkappa^\lambda) = 0$ et $\Phi_\varkappa(\sigma_\varkappa)e_\varkappa = 0$, d'où un homomorphisme d'anneaux unitaires de $\mathbb{Q}[X]/(\Phi_\varkappa) \simeq \mathbb{Q}^{(g_\varkappa)}$ dans $\mathbb{Q}[G]e_\varkappa$; cet homomorphisme est injectif car $\mathbb{Q}^{(g_\varkappa)}$ est un corps . La surjectivité résulte de la remarque suivante : comme $\sigma_\varkappa$ est

un élément de G dont l'image dans $G_\varkappa$ est génératrice , tout $\tau \in G$ s'écrit de façon unique $\tau = \sigma_\varkappa^k \tau'$, k défini modulo $g_\varkappa$ et $\tau' \in \mathrm{Ker}\ \varkappa$; on a alors $\tau' e_\varkappa = e_\varkappa$ soit $\tau e_\varkappa = \sigma_\varkappa^k e_\varkappa$ image de X^k par l'homomorphisme considéré; d'où la surjectivité .

Cet isomorphisme sera aussi utilisé de la manière suivante: à $\tau \in G$, $\tau = \sigma_\varkappa^k \tau'$, on associe $\zeta_\varkappa^k$.

Pour simplifier les notations , nous noterons $Q_\varkappa$ le corps $Q^{(g_\varkappa)}$ et $Z_\varkappa$ l'anneau des entiers de $Q_\varkappa$. Puisque $Z_\varkappa = Z[\zeta_\varkappa]$, $Z_\varkappa$ est isomorphe à $Z[G]e_\varkappa$ dans l'isomorphisme décrit ci-dessus .

3) Etude du groupe des unités de K (d'après Leopoldt [15]).

On suppose désormais que K est réel . Soit E_K le groupe des unités de K ; comme les seules racines de l'unité contenues dans K sont ± 1 , nous identifions $E_K/\{\pm 1\}$ au groupe des valeurs absolues de E_K : $|E_K|$; comme G opère trivialement sur $\{\pm 1\}$, $|E_K|$ et $E_K/\{\pm 1\}$ seront des G-modules isomorphes si l'on pose $|\varepsilon|^\sigma = |\varepsilon\sigma|$ pour tout $\varepsilon \in E_K$ et tout $\sigma \in G$. On rappelle que $|E_K|$ est un Z-module libre de dimension g-1 ([25], p. 72) .

a) Unités $\varkappa$-relatives . Soit $\varkappa$ un caractère de K . Soit $K_\varkappa$ le sous-corps cyclique de K correspondant à $\varkappa$ (cf. § 1, d) . On dit qu'une unité ε de $K_\varkappa$ est $\varkappa$-relative (" eigentliche $\tilde{\varkappa}$- Relativeinheit " au sens de Leopoldt ([15],§4)) si $N_{K_\varkappa/k}(\varepsilon) = \pm 1$ pour tout sous-corps strict k de $K_\varkappa$. On note $E_\varkappa$ (noté $E_\varkappa^+$ dans Leopoldt) le sous-groupe des unités $\varkappa$-relatives de $K_\varkappa$ (pour $\varkappa = 1$, on posera $E_1 = \{\pm 1\}$; on remarque que +1 et -1 sont $\varkappa$-relatives quel que soit $\varkappa$) .

D'après Leopoldt ([15], § 5, 2 et 3), on a les propriétés suivantes :

(i) $|E_\varkappa|$, pour $\varkappa \neq 1$, est un Z-module libre de dimension $\varphi(g_\varkappa)$.

(ii) Une condition nécessaire et suffisante pour qu'une unité ε de $K_\varkappa$ soit $\varkappa$-relative est que $|\varepsilon|^{e_\varkappa} = |\varepsilon|$, $e_\varkappa = \frac{1}{g} \sum_{\sigma \in G} \varkappa(\sigma^{-1})\sigma$ étant l'idempotent de $Q[G]$ associé à $\varkappa$ et défini au § 2 , avec la signification suivante : Comme $|E_\varkappa|$ est un Z-module libre , il s'injecte canoniquement dans l'espace vectoriel $Q \otimes_Z |E_\varkappa|$ sur lequel on étend la loi de G -

module par linéarité ; il en résulte que l'écriture $|\varepsilon|^{\frac{1}{g}\sum_\sigma \varkappa(\sigma^{-1})\sigma} = |\varepsilon|$ doit être considérée comme une relation dans $\mathbb{Q}\otimes_{\mathbb{Z}} |E_\varkappa|$ équivalente par définition à la relation $|\varepsilon|^{\sum_\sigma \varkappa(\sigma^{-1})\sigma} = |\varepsilon|^g$ dans $|E_\varkappa|$.

Soit E^K le sous-G-module de E_K engendré par les $E_\varkappa$ pour $\varkappa \in \mathfrak{X}_K$; alors d'après [15], § 5, 4 , on a $|E^K| = \bigoplus_{\substack{\varkappa \in \mathfrak{X}_K \\ \varkappa \neq 1}} |E_\varkappa|$. Comme $\dim_{\mathbb{Z}} |E_\varkappa| = \varphi(g_\varkappa)$, pour $\varkappa \neq 1$, on aura $\dim_{\mathbb{Z}} |E^K| = \sum_{\varkappa \neq 1} \varphi(g_\varkappa) = g-1$; donc E^K est un sous-$\mathbb{Z}$-module de E_K d'indice fini dans E_K .

b) Structures de $\mathbb{Z}_\varkappa$-modules des groupes $|E_\varkappa|$. Les éléments de $|E_\varkappa|$ ont la propriété d'être invariants par $e_\varkappa$, ce qui fait que $|E_\varkappa|$ est un $\mathbb{Z}[G]e_\varkappa$-module , donc un $\mathbb{Z}_\varkappa$-module . Compte-tenu de la description de l'isomorphisme entre $\mathbb{Z}[G]e_\varkappa$ et $\mathbb{Z}_\varkappa$ donnée au § 2 , si $\omega = \sum_i a_i \zeta_\varkappa^i \in \mathbb{Z}_\varkappa$, l'action de ω sur $|\varepsilon| \in |E_\varkappa|$ s'écrit $|\varepsilon|^\omega = \prod_i |\varepsilon^{\sigma_\varkappa^i}|^{a_i}$. Montrons que $|E_\varkappa|$ est sans $\mathbb{Z}_\varkappa$-torsion ; en effet, soit $\varepsilon \in E_\varkappa$, $|\varepsilon| \neq 1$ et soit $\omega \in \mathbb{Z}_\varkappa$ tel que $|\varepsilon|^\omega = 1$; soit $a = N_{\mathbb{Q}_\varkappa/\mathbb{Q}}(\omega)$; alors $|\varepsilon|^a = 1$; mais $|E_\varkappa|$ est sans $\mathbb{Z}$-torsion , donc $a = 0$ et $\omega = 0$.
Il en résulte que, comme $\mathbb{Z}_\varkappa$-module , $|E_\varkappa|$ est isomorphe à un idéal de $\mathbb{Z}_\varkappa$; en effet, d'après [1] (Prop. 24) tout module de type fini sans torsion sur un anneau de Dedekind est isomorphe à une somme directe de r idéaux de cet anneau ; or, d'une part un idéal de $\mathbb{Z}_\varkappa$ est un $\mathbb{Z}$-module libre de dimension $[\mathbb{Q}_\varkappa : \mathbb{Q}] = \varphi(g_\varkappa)$ ([25], § 3,5) et, d'autre part, $|E_\varkappa|$ est de dimension $\varphi(g_\varkappa)$ sur $\mathbb{Z}$, d'où $r = 1$.

Il faut remarquer que $|E_\varkappa|$ n'est pas $\mathbb{Z}_\varkappa$-libre en général ; en effet, $|E_\varkappa|$ est isomorphe à un idéal de $\mathbb{Z}_\varkappa$ et est libre sur $\mathbb{Z}_\varkappa$ si et seulement si cet idéal est principal ([1], Prop. 24) . On ne connait pas d'exemple où $|E_\varkappa|$ ne soit pas libre (la plus petite valeur de $g_\varkappa$ pour laquelle $\mathbb{Z}_\varkappa$ n'est pas principal étant 23 , on peut espérer trouver un tel exemple en considérant les extensions cycliques $K/\mathbb{Q}$ de degré 23) .

4) Formule analytique du nombre de classes . Leopoldt obtient dans [15] une interprétation arithmétique du nombre de classes h_K (au sens ordinaire) de K : Pour tout caractère $\varkappa \in \mathfrak{X}_K$, $\varkappa \neq 1$, le corps $K_\varkappa$ de conducteur $f_\varkappa$, est contenu dans $\mathbb{Q}^{(f_\varkappa)}$, et le groupe de Galois de $\mathbb{Q}^{(f_\varkappa)}/\mathbb{Q}$ est canoniquement isomorphe à $(\mathbb{Z}/f_\varkappa\mathbb{Z})^*$; soit $H_\varkappa$ le sous - groupe de $(\mathbb{Z}/f_\varkappa\mathbb{Z})^*$ image de $\mathrm{Gal}(\mathbb{Q}^{(f_\varkappa)}/K_\varkappa)$ par cet isomorphisme et soit $a_\varkappa$ un

système exact de représentants de $H_\chi/\{-1,+1\}$; soit $\mathbb{Q}_0^{(f_\chi)}$ le sous-corps réel maximal de $\mathbb{Q}^{(f_\chi)}$; alors a_χ correspond à $\mathrm{Gal}(\mathbb{Q}_0^{(f_\chi)}/K_\chi)$. Soit $\xi'_\chi = \exp(i\pi/f_\chi)$ et soit $\Theta_\chi = \prod_{a \in a_\chi} (\xi'^{a}_\chi - \xi'^{-a}_\chi)$. On pose

$$\Lambda_\chi = \frac{1}{\|H_\chi\|} \Big(\sum_{\tau \in H_\chi} \tau \Big) \prod_{\substack{\ell \mid g_\chi \\ \ell \text{ premier}}} \Big(1 - \sigma_\chi^{g_\chi/\ell} \Big) \quad .$$

On considère $\eta_\chi = \Theta_\chi^{\Lambda_\chi}$ (pour $\chi = 1$, on pose $\eta_\chi = -1$) . On vérifie que η_χ est une unité de K_χ qui est χ-relative et qui engendre un sous-module F_χ d'indice fini dans E_χ ([15], § 8) ; on appelle η_χ l'unité cyclotomique χ-relative génératrice .
Le groupe $|F_\chi|$ est un sous-$\mathbb{Z}_\chi$-module de $|E_\chi|$, libre de dimension 1 (une base est déterminée par $|\eta_\chi|$) .

Soit $h_\chi = (|E_\chi| : |F_\chi|)$; alors le nombre de classes h_K est donné par la formule ([15], § 9,2) :

$$h_K = \frac{Q_K}{Q_G} \prod_{\chi \in \mathfrak{X}_K} h_\chi \quad ,$$

où $Q_K = (|E_K| : |E^K|)$ et $Q_G = \Big(g^{g-2} / \prod_{\chi \in \mathfrak{X}_K} d_\chi \Big)^{\frac{1}{2}}$, où d_χ est le discriminant du corps $\mathbb{Q}_\chi$ ([15], § 1,3) .

Remarque I 1. Les h_χ ne sont pas nécessairement les nombres de classes des corps K_χ ; ils ne s'interprêtent pas comme des nombres de classes en général (voir cependant dans la partie V, § 2) .

Remarque I 2. Il est important de constater que les invariants E_χ , F_χ et h_χ ne dépendent que de l'extension cyclique $K_\chi/\mathbb{Q}$ et non du sur-corps K donné (cela se vérifie aisément sur les définitions) .
On est donc conduit à ne plus faire référence à un corps K et à donner une définition plus intrinsèque de la notion de caractère. Nous allons préciser cela dans le paragraphe suivant .

5) Définition des ensembles $\mathfrak{X}'$, $\mathfrak{X}$, $\mathfrak{X}'_\chi$ et $\mathfrak{X}_\chi$. Soit f un entier qui soit le conducteur d'une extension abélienne de $\mathbb{Q}$ et soit χ' un caractère complexe de $\mathbb{Q}^{(f)}$ de conducteur f . On appelle $\mathfrak{X}'$ l'ensemble des caractères χ' ainsi obtenus (il revient au même de dire que $\mathfrak{X}' = \bigcup_f \mathfrak{X}''_{\mathbb{Q}}(f)$ où $\mathfrak{X}''_{\mathbb{Q}}(f) = \{\chi' \in \mathfrak{X}'_{\mathbb{Q}}(f) \ , \ f_{\chi'} = f\}$) . On définit de la même manière $\mathfrak{X}$ comme la réunion des caractères rationnels de conducteur f des corps $\mathbb{Q}^{(f)}$ (les éléments de $\mathfrak{X}$ sont appelés : caractères) .

Il est alors facile de vérifier que $\mathfrak{X}$ est en correspondance bijective et canonique avec la famille des extensions cycliques de $\mathbb{Q}$ et pour rappeler ce fait nous noterons encore K_χ l'unique extension cyclique de $\mathbb{Q}$ associée à $\chi \in \mathfrak{X}$ par le même procédé qu'au § 1,d) .

Soit maintenant $\chi \in \mathfrak{X}$ (il est équivalent de dire qu'il existe f tel que χ soit un caractère de $\mathbb{Q}^{(f)}$ de conducteur f , donc que le corps K_χ correspondant est de conducteur f) ; alors $\mathfrak{X}'_{K_\chi}$ s'identifie canoniquement à l'ensemble des caractères $\psi' \in \mathfrak{X}'$ tels que $K_\psi \subset K_{\chi^{(f)}}$: soit $\hat{\psi}' \in \mathfrak{X}'_{K_\chi}$, c'est donc un caractère complexe de $\mathbb{Q}^{\chi}$ dont le noyau laisse fixe un sous-corps de K_χ de la forme K_ψ ; si f_ψ est le conducteur de ψ , alors f_ψ divise f_χ et par factorisation :

$$\begin{array}{ccc} (\mathbb{Z}/f_\chi\mathbb{Z})^* & \xrightarrow{\hat{\psi}'} & \mathbb{C}^* \\ \downarrow & \nearrow_{\psi'} & \\ (\mathbb{Z}/f_\psi\mathbb{Z})^* & & \end{array}$$

on en déduit ψ' élément de $\mathfrak{X}'$ tel que $K_\psi \subset K_\chi$. Réciproquement, à ψ' on associe $\hat{\psi}'$ par composition avec la projection canonique $(\mathbb{Z}/f_\chi\mathbb{Z})^* \longrightarrow (\mathbb{Z}/f_\psi\mathbb{Z})^*$.

De même nous identifierons canoniquement $\mathfrak{X}_{K_\chi}$ et $\{\psi \in \mathfrak{X} , K_\psi \subset K_\chi\}$. Pour simplifier les notations, nous poserons : $\mathfrak{X}'_\chi = \mathfrak{X}'_{K_\chi} = \{\psi' \in \mathfrak{X}', K_\psi \subset K_\chi\}$, $\mathfrak{X}_\chi = \mathfrak{X}_{K_\chi} = \{\psi \in \mathfrak{X} , K_\psi \subset K_\chi\}$, $\mathfrak{X}'^*_\chi = \mathfrak{X}'_\chi \setminus \{1\}$ et $\mathfrak{X}^*_\chi = \mathfrak{X}_\chi \setminus \{1\}$, 1 désignant l'élément commun à $\mathfrak{X}'$ et $\mathfrak{X}$ associé au corps $\mathbb{Q}$. Nous noterons enfin $\mathfrak{X}^+$ le sous-ensemble de $\mathfrak{X}$ formé par les caractères pairs (on rappelle que $\chi \in \mathfrak{X}^+$ si et seulement si, pour n'importe quel $\chi' \in \tilde{\chi}$, on a $\chi'(-1) = 1$) . On remarque que si $\chi \in \mathfrak{X}^+$ alors $\mathfrak{X}_\chi \subset \mathfrak{X}^+$.

6) Conclusion. La remarque I 2 rappelle que pour étudier E_χ , F_χ et h_χ , il suffit de considérer uniquement l'extension $K_\chi/\mathbb{Q}$; il en résulte en particulier, que la famille $(h_\chi)_{\chi \in \mathfrak{X}^+}$ constitue une famille de nombres " universelle" pour le calcul du nombre de classes des corps abéliens réels quelconques .

II

Majoration des indices $h_\varkappa = (|E_\varkappa| : |F_\varkappa|)$.

Soit $\varkappa \in \mathfrak{X}^+$, $\varkappa \neq 1$, fixé . On rappelle que $G_\varkappa$ est le groupe de Galois de $K_\varkappa/\mathbb{Q}$ et est d'ordre $g_\varkappa$. Soit F un sous-$G_\varkappa$-module de $E_\varkappa$ de même rang ; nous noterons $r(F)$ l'indice $(|E_\varkappa| : |F|)$. Nous allons, dans cette partie, établir une majoration générale de $r(F)$ indépendante de $E_\varkappa$.

1) Plongement logarithmique du groupe des unités de $K_\varkappa$. Considé - rons, dans $\mathbb{R}^{g_\varkappa}$, le plongement logarithmique du groupe des unités de $K_\varkappa$, $E_{K_\varkappa}$: si $|\varepsilon| \in |E_{K_\varkappa}|$, on pose $L_\varkappa(\varepsilon) = (\ldots, \mathrm{Log}|\varepsilon^\sigma|, \ldots)_{\sigma \in G_\varkappa}$. L'image de $|E_\varkappa|$ par $L_\varkappa$ est un réseau relatif de dimension $\varphi(g_\varkappa)$ ([25], § 5,3) contenu dans l'hyperplan $\Pi_\varkappa = \left\{ x = (x_\sigma)_{\sigma \in G_\varkappa} , \sum_{\sigma \in G_\varkappa} x_\sigma = 0 \right\}$; c'est aussi un $G_\varkappa$-module avec la loi $\tau(L_\varkappa(\varepsilon)) = L_\varkappa(\varepsilon^\tau)$ et $L_\varkappa$ est un homomorphisme de $G_\varkappa$-modules .

Soient $\mathfrak{D}_\varkappa = \left\{ x = (x_\sigma)_{\sigma \in G_\varkappa} , |x_\sigma| \leq 1 , \text{ pour tout } \sigma \neq 1 \right\}$ et $D_\varkappa = \mathfrak{D}_\varkappa \cap V_\varkappa$, où $V_\varkappa$ désigne le sous-espace de $\mathbb{R}^{g_\varkappa}$ engendré sur $\mathbb{R}$ par $L_\varkappa(E_\varkappa)$.

Lemme II 1. Le domaine $D_\varkappa$ de $V_\varkappa$ est un compact convexe symétrique par rapport à O de mesure $m_\varkappa$ finie non nulle (i.e. une jauge compacte).

On vérifie facilement que $D_\varkappa$ est convexe localement compact comme intersection de convexes localement compacts et qu'il est symé - trique par rapport à O .

Pour montrer que $D_\varkappa$ est borné, il suffit de vérifier que $\mathfrak{D}_\varkappa \cap \Pi_\varkappa$ est borné, ce qui est immédiat puisque $|x_\sigma| \leq 1$ pour tout $\sigma \neq 1$ et que $|x_1| = \left| - \sum_{\sigma \neq 1} x_\sigma \right| \leq g_\varkappa - 1$.

Enfin, $D_\varkappa$ est de mesure non nulle. En effet, soit $S_\varkappa$ la boule unité euclidienne de $\mathbb{R}^{g_\varkappa}$ centrée en O ; on a $S_\varkappa \subset \mathfrak{D}_\varkappa$ et par consé - quent $S_\varkappa \cap V_\varkappa \subset D_\varkappa$.

2) Résultat préliminaire . Le sous-groupe $L_\nu(F)$ de $L_\nu(E_\nu)$ est un sous-réseau qui engendre aussi V_ν . Nous noterons $\mathfrak{M}_\nu(F)$ la mesure du domaine fondamental du réseau $L_\nu(F)$; on a alors

$r(F) = (|E_\nu| : |F|) = \dfrac{\mathfrak{M}_\nu(F)}{\mathfrak{M}_\nu(E_\nu)}$ (dans le cas particulier où $F = F_\nu$, on a $r(F_\nu) = h_\nu$) . Par abus de langage nous dirons que $\mathfrak{M}_\nu(F)$ est la mesure de F relativement au plongement logarithmique L_ν .

Proposition II 1. Il existe dans E_ν une unité ε_o , $|\varepsilon_o| \neq 1$, telle que :

$$\operatorname*{Max}_{\sigma \in G_\nu} (\operatorname{Log} |\varepsilon_o^\sigma|) \leq 2\left(\frac{\mathfrak{M}_\nu(F)}{m_\nu\, r(F)}\right)^{\frac{1}{\varpi(g_\nu)}} .$$

démonstration

Soit c un réel positif . D'après le théorème de Minkowski , ([25], p. 67) , appliqué au réseau relatif $\frac{1}{c} L_\nu(E_\nu)$ de $\mathbb{Z}$-rang $\varpi(g_\nu)$ et de mesure $\left(\frac{1}{c}\right)^{\varpi(g_\nu)} \mathfrak{M}_\nu(E_\nu)$, la jauge D_ν contient un point de $\frac{1}{c} L_\nu(E_\nu)$ autre que l'origine dès que $m_\nu \geq \left(\frac{2}{c}\right)^{\varpi(g_\nu)} \mathfrak{M}_\nu(E_\nu)$; comme $r(F) = \dfrac{\mathfrak{M}_\nu(F)}{\mathfrak{M}_\nu(E_\nu)}$, il revient au même d'écrire $m_\nu \geq \left(\frac{2}{c}\right)^{\varpi(g_\nu)} \dfrac{\mathfrak{M}_\nu(F)}{r(F)}$. La plus grande valeur de c pour laquelle cette condition soit encore vérifiée est donc $c_o = 2\left(\dfrac{\mathfrak{M}_\nu(F)}{m_\nu\, r(F)}\right)^{\frac{1}{\varpi(g_\nu)}}$. Soit $\frac{1}{c_o} L_\nu(\varepsilon_o')$ le point autre que 0 du réseau $\frac{1}{c_o} L_\nu(E_\nu)$ ainsi contenu dans D_ν ; on a aussi $-\frac{1}{c_o} L_\nu(\varepsilon_o') \in D_\nu$; soit ε_o l'unité égale à ε_o' ou $\varepsilon_o'^{-1}$ et telle que $\operatorname{Log} |\varepsilon_o| \leq 0$: alors , pour tout $\sigma \in G_\nu$, $\operatorname{Log} |\varepsilon_o^\sigma| \leq c_o$.

3) Résultat fondamental : majoration de $r(F)$.

Soit Φ une fonction polynome homogène à coefficients réels de degré $d_\Phi \geq 1$ des variables réelles x_σ , $\sigma \in G_\nu$. Nous utiliserons es-

sentiellement les types de polynomes Φ suivants :

(i) le polynome " discriminant " (cf. [25], p. 49) :

$$\Delta_n(x) = \prod_{\substack{\sigma,\tau \in G_n \\ \sigma \neq \tau}} (x_\sigma - x_\tau)$$

(ii) les polynomes " norme de résolvantes de Lagrange " :

$$N_\psi^n(x) = \prod_{\psi' \in \tilde{\psi}} \sum_{\sigma \in G_n} \psi'(\sigma^{-1}) x_\sigma \quad , \text{ pour tout } \psi \in \mathfrak{X}_n \ .$$

Lemme II 2. Soit Φ une telle fonction. Alors $\operatorname{Sup}_{\substack{x \in \mathbb{R}^{g_n} \\ x \neq 0}} \left(\dfrac{|\Phi(x)|}{\operatorname{Max}_{\sigma \in G_n} (|x_\sigma|^{d_\Phi})} \right)$ existe et est égal au nombre strictement positif $\mu_\Phi = \operatorname{Sup}_{x \in C_n} |\Phi(x)|$, où C_n est la sphère unité (centrée en O) pour la distance du maximum dans $\mathbb{R}^{g_n}$ $\left(C_n = \left\{ (x_\sigma)_{\sigma \in G_n} \ , \ \operatorname{Max}_\sigma (|x_\sigma|) = 1 \right\} \right)$.

En effet , soit $\overline{\Phi}(x) = \dfrac{|\Phi(x)|}{\operatorname{Max}_{\sigma \in G_n} (|x_\sigma|^{d_\Phi})}$ pour $x \neq 0$; $\overline{\Phi}$ est une fonction homogène de degré 0 (pour tout $\lambda \in \mathbb{R}^*$ et tout $x \neq 0$, $\overline{\Phi}(\lambda x) = \overline{\Phi}(x)$) ; donc on aura en particulier $\operatorname{Sup}_{x \in \mathbb{R}^{g_n}} (\overline{\Phi}(x)) = \operatorname{Sup}_{x \in C_n} (\overline{\Phi}(x))$ puisque pour tout $y \neq 0$ de $\mathbb{R}^{g_n}$ il existe $x \in C_n$ et $\lambda \in \mathbb{R}^*$ tels que $x = \lambda y$. Si $x \in C_n$ alors $\operatorname{Max}_{\sigma \in G_n} (|x_\sigma|) = 1$, donc $\operatorname{Max}_{\sigma \in G_n} (|x_\sigma|^{d_\Phi}) = 1$, d'où $\operatorname{Sup}_{x \in \mathbb{R}^{g_n}} (\overline{\Phi}(x)) = \operatorname{Sup}_{x \in C_n} |\Phi(x)|$. Comme $|\Phi|$ est continue et que C_n est compact , Φ atteint son maximum sur C_n .

Théorème II 1. Soit $\chi \in \mathfrak{X}^+$, $\chi \neq 1$. Soit F un sous-G_χ-module de E_χ de même rang et soit $r(F) = (|E_\chi| : |F|) = \dfrac{\mathfrak{m}_\chi(F)}{\mathfrak{m}_\chi(E_\chi)}$. Soit Φ une fonction polynome homogène réelle de degré $d_\Phi \geq 1$ des variables réelles x_σ , $\sigma \in G_\chi$; on suppose qu'il existe une constante M_Φ ne dépendant que de Φ vérifiant $M_\Phi > u_\Phi$ et telle que pour tout $\varepsilon \in E_\chi$, $|\varepsilon| \neq 1$, on ait $|\Phi(\ldots, \varepsilon^\sigma, \ldots)| \geq M_\Phi$. Alors on a :

$$r(F) \leq \frac{\mathfrak{m}_\chi(F)}{m_\chi} \left(\frac{1}{2 d_\Phi} \operatorname{Log} \frac{M_\Phi}{u_\Phi} \right)^{-w(g_\chi)} .$$

En particulier on a $h_\chi \leq \dfrac{\mathfrak{m}_\chi(F_\chi)}{m_\chi} \left(\dfrac{1}{2 d_\Phi} \operatorname{Log} \dfrac{M_\Phi}{u_\Phi} \right)^{-w(g_\chi)}$

sous les hypothèses précédentes .

démonstration

Soit $\varepsilon_o \in E_\chi$, $|\varepsilon_o| \neq 1$; d'après le lemme II 2 , on a $|\Phi(\ldots, \varepsilon_o^\sigma, \ldots)| \leq u_\Phi \underset{\sigma \in G_\chi}{\operatorname{Max}} (|\varepsilon_o^\sigma|^{d_\Phi})$; on a donc $\underset{\sigma \in G_\chi}{\operatorname{Max}} (|\varepsilon_o^\sigma|^{d_\Phi}) \geq \dfrac{M_\Phi}{u_\Phi} > 1$ et , comme Log est une fonction croissante , on a $\underset{\sigma \in G_\chi}{\operatorname{Max}} (\operatorname{Log} |\varepsilon_o^\sigma|) \geq \dfrac{1}{d_\Phi} \operatorname{Log} \dfrac{M_\Phi}{u_\Phi} > 0$. Supposons maintenant que ε_o soit une unité dont la proposition II 1 affirme l'existence ; on a alors

$$\frac{1}{d_\Phi} \operatorname{Log} \frac{M_\Phi}{u_\Phi} \leq \underset{\sigma \in G_\chi}{\operatorname{Max}} (\operatorname{Log} |\varepsilon_o^\sigma|) \leq 2 \left(\frac{\mathfrak{m}_\chi(F)}{m_\chi \, r(F)} \right)^{\frac{1}{w(g_\chi)}} , \text{ soit,}$$

en considérant les deux membres extrêmes (qui sont positifs) :

$$\left(\frac{1}{d_\Phi} \operatorname{Log} \frac{M_\Phi}{u_\Phi} \right)^{w(g_\chi)} \leq 2^{w(g_\chi)} \frac{\mathfrak{m}_\chi(F)}{m_\chi \, r(F)} \quad \text{soit}$$

$$r(F) \leq \frac{\mathfrak{m}_\chi(F)}{m_\chi} \left(\frac{1}{2 d_\Phi} \operatorname{Log} \frac{M_\Phi}{u_\Phi} \right)^{-w(g_\chi)} .$$

Remarques sur l'utilisation pratique du théorème II 1 . La majoration effective de $r(F)$ repose uniquement sur la possibilité de trouver une fonction arithmétique Φ telle que $\Phi(\varepsilon) \geq M_\Phi > \mu_\Phi$, pour tout $\varepsilon \in E_\varkappa$, $|\varepsilon| \neq 1$. On montrera que, quel que soit le corps $K_\varkappa$ considéré, la fonction $\Phi = \Delta_\varkappa$ vérifie les conditions du théorème : pour cela on prouvera (Prop. III 1) que les unités $\varkappa$-relatives ε , $|\varepsilon| \neq 1$, sont des éléments primitifs dans l'extension $K_\varkappa/\mathbb{Q}$, donc que leur discriminant est non nul ([25], p. 41) ; comme il est un multiple du discriminant du corps , M_Φ pourra être prise égale au discriminant de $K_\varkappa$. On vérifiera ensuite , en calculant μ_Φ (Prop. III 3) , que M_Φ/μ_Φ est toujours plus grand que 1 (Corol. III 1) .

La majoration de $r(F)$ est donc fonction :

(i) de la constante géométrique $m_\varkappa$ qui ne dépend que du groupe de Galois $G_\varkappa$,

(ii) de deux constantes associées à la fonction Φ : d_Φ et μ_Φ ,

(iii) de la constante arithmétique M_Φ dépendant à la fois de Φ et du conducteur du corps $K_\varkappa$,

(iv) de F par l'intermédiaire de $\mathfrak{M}_\varkappa(F)$.

Il est clair que toute fonction Φ vérifiant les hypothèses du théorème II 1 conduit à une majoration de $r(F)$ et qu'il convient de choisir celle qui donne la majoration la plus fine . Nous verrons que la fonction $\Phi = N_\varkappa^\varkappa$ est meilleure , en général , que la fonction discriminant $\Delta_\varkappa$ mais les hypothèses nécessaires à son utilisation ne sont pas toujours satisfaites .

4) Calcul effectif de $\mathfrak{M}_\varkappa(F)$ et $m_\varkappa$.

a) Résolution d'un système linéaire particulier . Soit $(a_\varkappa)_{\varkappa \in \mathfrak{X}^+}$ une famille de nombres indexée par $\mathfrak{X}^+$; on suppose que pour tout $\varkappa \in \mathfrak{X}^+$, on a les relations suivantes :

$$\prod_{\psi \in \mathfrak{X}_\varkappa} a_\psi = 1 \quad ;$$

alors nécessairement $a_\varkappa = 1$ pour tout $\varkappa \in \mathfrak{X}^+$.

Démontrons ce résultat :

Fixons $\varkappa \in \mathfrak{X}^+$; on a vu que $\mathfrak{X}_\varkappa$ s'identifie canoniquement à l'ensemble des caractères de $K_\varkappa$, donc correspond bijectivement à la famille des sous-corps de $K_\varkappa$, car $K_\varkappa/\mathbb{Q}$ est cyclique ; il en résulte

aussi que la famille des sous-corps de $K_\varkappa$ correspond bijectivement à l'ensemble des diviseurs de $g_\varkappa$ (à d , diviseur de $g_\varkappa$, on associe le sous-corps de $K_\varkappa$ fixe par l'unique sous-groupe cyclique d'ordre d de $G_\varkappa$) ; avec un changement évident de notations , les relations précédentes conduisent , pour un $\varkappa$ fixé , à des relations de la forme $\prod_{\delta \mid d} a'_\delta = 1$, pour tout diviseur d de $g_\varkappa$; la formule d'inversion de Möbius donne immédiatement le résultat .

b) Constante $\gamma_\varkappa$ et calcul de $\mathfrak{m}_\varkappa(F)$. On rappelle que $|E^{K_\varkappa}| = \bigoplus_{\psi \in \mathfrak{X}^*_\varkappa} |E_\psi|$ (partie I, § 3,a) . Pour tout $\psi \in \mathfrak{X}$ soit $|F_\psi|$ le groupe des valeurs absolues d'un sous-G_ψ-module de $|E_\psi|$ (de même rang) et soit $|F^{K_\varkappa}| = \bigoplus_{\psi \in \mathfrak{X}^*_\varkappa} |F_\psi|$ (par exemple , les F_ψ seront les groupes d'unités cyclotomiques définis dans la partie I , § 4) . Soit $L_\varkappa$ le plongement logarithmique défini au § 1 ; pour tout $\psi \in \mathfrak{X}^*_\varkappa$, $L_\varkappa(F_\psi)$ est un réseau relatif de $\mathbb{R}^{g_\varkappa}$ dont la mesure est $\mathfrak{m}_\varkappa(F_\psi)$. Lorsqu'on réalise le plongement logarithmique L_ψ , la mesure $\mathfrak{m}_\psi(F_\psi)$ de $L_\psi(F_\psi)$ est distincte en général de $\mathfrak{m}_\varkappa(F_\psi)$. Dans $\mathbb{R}^{g_\varkappa}$, désignons par $V^\varkappa_\psi$ le sous-espace engendré sur $\mathbb{R}$ par $L_\varkappa(E_\psi)$; on remarque que $\Pi_\varkappa = \bigoplus_{\psi \in \mathfrak{X}^*_\varkappa} V^\varkappa_\psi$. Nous avons donc $V^\varkappa_\varkappa = V_\varkappa$ ($V_\varkappa$ ayant été défini dans la partie II , § 1). On a alors le résultat suivant :

Lemme II 3 . On a $\mathfrak{m}_\varkappa(F_\psi) = (g_\varkappa/g_\psi)^{\varpi(g_\psi)/2}\, \mathfrak{m}_\psi(F_\psi)$.

En effet , si $\eta \in F_\psi$, on a

$$L_\varkappa(\eta) = (\mathrm{Log}|\eta^\sigma|)_{\sigma \in G_\varkappa} = (\ldots ; \mathrm{Log}|\eta^\tau|, \mathrm{Log}|\eta^\tau|, \ldots, \mathrm{Log}|\eta^\tau| ; \ldots)_{\tau \in G_\psi}$$

élément de $\mathbb{R}^{g_\varkappa/g_\psi} \times \ldots \times \mathbb{R}^{g_\varkappa/g_\psi}$ (g_ψ groupements de $g_\varkappa/g_\psi$ composantes égales) . Pour calculer la mesure du réseau relatif $L_\psi(F_\psi) \subset \mathbb{R}^{g_\psi}$, on choisit une base orthonormale de $V^\psi_\psi = V_\psi$, $(b_1, \ldots, b_{\varpi(g_\psi)})$, et la mesure du réseau est le déterminant , dans cette base , des composantes des vecteurs d'une $\mathbb{Z}$-base de $L_\psi(F_\psi)$; pour calculer la mesure

du réseau relatif $L_\nu(F_\psi)$ de $\mathbb{R}^{g_\nu}$, on peut prendre , comme base orthonormale du sous-espace V_ψ^ν engendré sur $\mathbb{R}$ par le réseau $L_\nu(F_\psi)$, la base $(B_i)_i = \left(\frac{1}{\sqrt{g_\nu/g_\psi}}(b_i, b_i, \dots, b_i)\right)_i \in \mathbb{R}^{g_\nu/g_\psi} \times \dots \times \mathbb{R}^{g_\nu/g_\psi}$, $i = 1, \dots, \varpi(g_\psi)$, qui est encore orthonormale ; on a alors , de façon évidente , $\mathfrak{M}_\nu(F_\psi) = (\sqrt{g_\nu/g_\psi})^{\varpi(g_\psi)}\, \mathfrak{M}_\psi(F_\psi)$.

Dans la pratique c'est le ψ-régulateur $R_\psi(F_\psi)$ qui se calcule aisément ([15], § 7) ; on va s'y ramener en remarquant que $\mathfrak{M}_\psi(F_\psi)$ lui est proportionnel (cf. [15], § 7, 4) ; la constante de proportionnalité , étant de nature géométrique , ne dépend que de ψ . On pose :

$$R_\psi(F_\psi) = \gamma_\psi\, \mathfrak{M}_\psi(F_\psi)$$

(le ψ-régulateur $R_\psi(F_\psi)$ est égal à $\prod_{\psi' \in \tilde{\psi}} \left(\sum_{\sigma \in G_\psi} \psi'(\sigma^{-1}) \operatorname{Log} |\eta^\sigma| \right)$ lorsque $|F_\psi|$ est $\mathbb{Z}_\psi$-libre de base $|\eta|$; pour le cas général cf. [15] § 7, 2) . On a donc

$$\mathfrak{M}_\nu(F_\psi) = \frac{(\sqrt{g_\nu/g_\psi})^{\varpi(g_\psi)}}{\gamma_\psi}\, R_\psi(F_\psi) \quad .$$

Lemme II 4 . On a $\gamma_\psi = \sqrt{g_\psi^{\varpi(g_\psi)}/d_\psi}$ où d_ψ est le discriminant de $\mathbb{Q}_\psi$.

D'après Leopoldt ([15], § 7 , Satz 17 et Satz 14) on a la relation suivante : $g_\nu\, Q_{G_\nu}\, \mathfrak{R}(F^{K^\nu}) = \prod_{\psi \in \mathfrak{X}_\nu^*} ((g_\nu/g_\psi)^{\varpi(g_\nu)}\, R_\psi(F_\psi))$ où $\mathfrak{R}(F^{K^\nu})$ est le régulateur du réseau $L_\nu(F^{K^\nu})$ (définition habituelle , puisque $L_\nu(F^{K^\nu})$ engendre sur $\mathbb{R}$ le plan Π_ν de codimension 1 dans $\mathbb{R}^{g_\nu}$). On sait que la mesure $\mathfrak{M}_\nu(F^{K^\nu})$ du réseau $L_\nu(F^{K^\nu})$ est égale à $\sqrt{g_\nu}\, \mathfrak{R}(F^{K^\nu})$; on aura donc , en vertu de ce qui précède :

$$\sqrt{g_\nu}\, Q_{G_\nu}\, \mathfrak{M}_\nu(F^{K^\nu}) = \prod_{\psi \in \mathfrak{X}_\nu^*} \left((g_\nu/g_\psi)^{\varpi(g_\psi)/2}\, \gamma_\psi\, \mathfrak{M}_\nu(F_\psi) \right) =$$

$$= g_\nu^{\frac{g_\nu - 1}{2}} \prod_{\psi \in \mathfrak{X}_\nu^*} \mathfrak{M}_\nu(F_\psi) \prod_{\psi \in \mathfrak{X}_\nu^*} \frac{\gamma_\psi}{g_\psi^{\varpi(g_\psi)/2}}$$

soit , compte-tenu de l'expression de $Q_{G_\varkappa}$ $\left(Q_{G_\varkappa} = (g_\varkappa^{g_\varkappa - 2} / \prod_\psi d_\psi)^{\frac{1}{2}}\right)$:

$$\mathfrak{M}_\varkappa(F^{K_\varkappa}) = \prod_{\psi \in \mathfrak{X}_\varkappa^*} \mathfrak{M}_\varkappa(F_\psi) \prod_{\psi \in \mathfrak{X}_\varkappa} \frac{\gamma_\psi \sqrt{d_\psi}}{g_\psi^{\varphi(g_\psi)/2}} \quad \text{(en convenant que } \gamma_1 = 1\text{)} \ ;$$

or on vérifie que dans $\mathbb{R}^{g_\varkappa}$, les sous-espaces $V_\psi^\varkappa$ sont deux à deux orthogonaux ([15], § 7, 4) ; donc, puisque $|F^{K_\varkappa}| = \bigoplus_{\psi \in \mathfrak{X}_\varkappa^*} |F_\psi|$, on a $\mathfrak{M}_\varkappa(F^{K_\varkappa}) = \prod_{\psi \in \mathfrak{X}_\varkappa^*} \mathfrak{M}_\varkappa(F_\psi)$; d'où $\prod_{\psi \in \mathfrak{X}_\varkappa} \frac{\gamma_\psi \sqrt{d_\psi}}{g_\psi^{\varphi(g_\psi)/2}} = 1$, qui conduit, en

vertu des résultats du § 4, a) à

$$\gamma_\psi = \frac{g_\psi^{\varphi(g_\psi)/2}}{\sqrt{d_\psi}} \quad .$$

Corollaire. On a pour tout $\varkappa \neq 1$, $\mathfrak{M}_\varkappa(F_\varkappa) = \sqrt{d_\varkappa / g_\varkappa^{\varphi(g_\varkappa)}}\, R_\varkappa(F_\varkappa)$.

c) Procédé de calcul de $\mathfrak{m}_\varkappa$. Posons pour simplifier $x_i = x_{\sigma_\varkappa^i}$, $\sigma_\varkappa$ générateur de $G_\varkappa$, $i = 1, \ldots, g_\varkappa$. On rappelle que

$V_\varkappa = \left\{ x \in \mathbb{R}^{g_\varkappa} , \sum_{j=1}^{g_\varkappa/d} x_{i+jd} = 0 \ , \ d \mid g_\varkappa \ , \ i = 1, \ldots, d \right\}$; on déduit de ces relations que l'on peut exprimer les x_i , $i = 1, \ldots, g_\varkappa$ comme combinaisons linéaires $f_i(\ldots, x_k, \ldots)$, $(k, g_\varkappa) = 1$. On est alors amené à calculer le volume d'un polyèdre convexe symétrique de $V_\varkappa$ défini par les inégalités $|f_i(\ldots, x_k, \ldots)| \leq 1$, $i = 1, \ldots, g_\varkappa - 1$, $(k, g_\varkappa) = 1$. On vérifie ensuite que l'élément de volume dans $V_\varkappa$ défini à partir du paramétrage précédent est égal à $\gamma_\varkappa \, dx_1 \ldots dx_k \ldots dx_{g_\varkappa - 1}$, $(k, g_\varkappa) = 1$,

et donc que $\mathfrak{m}_\varkappa = \gamma_\varkappa \int_{V_\varkappa} dx_1 \ldots dx_k \ldots dx_{g_\varkappa - 1}$, intégrale sur le domaine $V_\varkappa$ de $\mathbb{R}^{\varphi(g_\varkappa)}$ défini par les inégalités $|f_i(\ldots, x_k, \ldots)| \leq 1$, $i = 1, \ldots, g_\varkappa - 1$, $(k, g_\varkappa) = 1$.

Corollaire . On aura $\mathfrak{m}_\varkappa(F_\varkappa)/m_\varkappa = \frac{1}{\gamma_\varkappa^2} \frac{R_\varkappa(F_\varkappa)}{\int_{\gamma_\varkappa} dx_1 \dots dx_k \dots dx_{g_\varkappa - 1}}$ et si $g_\varkappa$ est égal à un nombre premier ℓ , alors $\mathfrak{m}_\varkappa(F_\varkappa)/m_\varkappa = \frac{1}{\ell} \frac{R_\varkappa(F_\varkappa)}{2^{\ell-1}}$.

III

Calculs explicites des constantes M_Φ et μ_Φ .

Dans cette partie, nous allons expliciter les fonctions Φ introduites précédemment, calculer les différentes constantes qui interviennent dans la majoration du théorème III 1 et vérifier que les hypothèses nécessaires à l'application de ce théorème peuvent toujours être satisfaites .

1) Etude de la fonction discriminant $\Delta_\varkappa$.

a) Détermination de la constante $M_{\Delta_\varkappa}$. Soit $\varkappa$ un caractère pair , $\varkappa \neq 1$, et soit $\Delta_\varkappa$ le polynome homogène de degré $g_\varkappa(g_\varkappa - 1)$ défini par $\Delta_\varkappa(x) = \pm \prod_{\substack{\sigma,\tau \in G_\varkappa \\ \sigma \neq \tau}} (x_\sigma - x_\tau)$ (le signe, qui ne dépend que de $g_\varkappa$, étant choisi de telle façon que $\Delta_\varkappa(x)$ soit un carré parfait) ; si $x_\sigma = \theta^\sigma$, avec θ entier de $K_\varkappa$, alors $\Delta_\varkappa(x)$ est le discriminant de la famille $(1, \theta, \theta^2, \dots, \theta^{g_\varkappa - 1})$ (i.e. le discriminant du polynome irréductible de θ) donc un entier rationnel (non nul si θ est primitif ([25], p. 41)) multiple du discriminant $\Delta(K_\varkappa)$ du corps $K_\varkappa$ ([14], chap. III, § 3) .

Proposition III 1. Soit ε une unité $\varkappa$-relative autre que ± 1 ; alors $\Delta_\varkappa(\dots, \varepsilon^\sigma, \dots) \geq \Delta(K_\varkappa)$ (i.e. la constante $M_{\Delta_\varkappa}$ du théorème II 1 peut être prise égale à $\Delta(K_\varkappa)$) .

démonstration

Montrons que ε est primitive : si on avait $\varepsilon^{\sigma_\varkappa^i} = \varepsilon$, on aurait, en vertu de la loi de $\mathbb{Z}_\varkappa$-module sans torsion sur $|E_\varkappa|$, $e_\varkappa(\sigma_\varkappa^i - 1) = 0$, soit $\sigma_\varkappa^i = 1$, soit $i \equiv 0 \bmod g_\varkappa$; donc ε possède bien $g_\varkappa$ conjugués distincts.

Dans la pratique, $\Delta(K_\nu)$ sera calculé au moyen de la "Führerdiskriminantenproduktformel" $\Delta(K_\nu) = \prod_{\psi' \in \mathfrak{X}'_\nu} f_{\psi'}$ ([26], p. 112) .

b) Calcul de la constante μ_{Δ_ν} . On rappelle que $\mu_{\Delta_\nu} = \operatorname{Sup}_{x \in C_\nu} (\Delta_\nu(x))$ (lemme II 2) ; soit $x^\circ = (x^\circ_\sigma)_{\sigma \in G_\nu}$ un point de C_ν où Δ_ν atteint son maximum .

Lemme III 1 . Les nombres x°_σ (compris entre -1 et +1) sont tous distincts et les valeurs -1 et +1 sont nécessairement prises .

Comme $x^\circ \in C_\nu$, il est clair que l'une de ses composantes vaut ± 1 ; comme $\Delta_\nu(x^\circ) = \Delta_\nu(-x^\circ)$, on peut supposer que c'est +1 qui est atteint . Soit $t \in G_\nu$ défini par $x^\circ_t = \operatorname{Min}_{\sigma \in G_\nu} (x^\circ_\sigma)$; on peut écrire $\Delta_\nu(x^\circ) =$

$$\left| \prod_{\sigma \neq t} \prod_{\tau \neq \sigma, t} (x^\circ_\sigma - x^\circ_\tau) \right| \prod_{\tau \neq t} (x^\circ_\tau - x^\circ_t)^2 \quad ;$$

si $x^\circ_t > -1$ alors on a $(x^\circ_\tau - x^\circ_t)^2 < (x^\circ_\tau + 1)^2$ pour tout $\tau \neq t$ et $\Delta_\nu(x^\circ)$ ne serait pas maximum , d'où le lemme . On est donc ramené au problème suivant : soit $n \geq 2$; trouver un système de $n-2$ points distincts $x^\circ_1, \ldots, x^\circ_{n-2}$ de l'intervalle $]-1, +1[$ tels que

$$\operatorname{Sup}_{|x_i| < 1} \Delta_\nu(-1, x_1, \ldots, x_{n-2}, 1) = \Delta_\nu(-1, x^\circ_1, \ldots, x^\circ_{n-2}, 1) \quad .$$

Considérons un tel système et soit P_n le polynome unitaire de degré n admettant pour racines les nombres $-1, x^\circ_1, \ldots, x^\circ_{n-2}, 1$. On a alors le résultat suivant :

Proposition III 2 . Le polynome P_n est unique et est solution de l'équation différentielle $(u^2 - 1) P''_n(u) = n(n-1) P_n(u)$.

démonstration

On considère $\Delta_\nu(x) = \Delta_\nu(-1, x_1, \ldots, x_{n-2}, 1)$ comme fonction de $n-2$ variables dans le domaine $C'_\nu = \{x = (x_1, \ldots, x_{n-2}), |x_i| \leq 1\}$; comme le maximum est atteint en un point intérieur x° de C'_ν , les $n-2$ dérivées partielles de Δ_ν en ce point seront nulles . On a

$$\Delta_n(x) = \prod_{i=1}^{n-2}(1-x_i^2)^2 \left| \prod_{\substack{i=1\\ i\neq k}}^{n-2} \prod_{\substack{j=1\\ j\neq k,i}}^{n-2} (x_i - x_j) \right| \prod_{\substack{i=1\\ i\neq k}}^{n-2} (x_i - x_k)^2 \quad \text{d'où}$$

$$\frac{\partial \Delta_n}{\partial x_k} = \Delta_n(x)\left(\frac{-4x_k}{1-x_k^2} - \sum_{\substack{i=1\\ i\neq k}}^{n-2} \frac{2}{x_i - x_k}\right) \quad , \text{ mais}$$

$$-\frac{1}{1-x_k} - \frac{1}{-1-x_k} = \frac{-2x_k}{1-x_k^2} \quad \text{d'où} \quad \frac{\partial \Delta_n}{\partial x_k} = -2\,\Delta_n(x) \sum_{\substack{i=0\\ i\neq k}}^{n-1} \frac{1}{x_i - x_k} \quad , \text{ où}$$

l'on a posé $x_o = -1$ et $x_{n-1} = 1$. Au maximum x^o on aura donc

$$\sum_{\substack{i=0\\ i\neq k}}^{n-1} \frac{1}{x_i^o - x_k^o} = 0 \quad , \quad \text{pour } k = 1, 2, \ldots, n-2 \ .$$

On a $P_n(u) = \prod_{i=0}^{n-1}(u - x_i^o)$, $P_n'(u) = P_n(u) \sum_{i=0}^{n-1} \frac{1}{u - x_i^o}$ et

$$P_n''(u) = -P_n(u) \sum_{i=0}^{n-1} \frac{1}{(u-x_i^o)^2} + P_n'(u) \sum_{i=0}^{n-1} \frac{1}{u - x_i^o} =$$

$$= -P_n(u) \sum_{i=0}^{n-1} \frac{1}{(u-x_i^o)^2} + P_n(u)\left(\sum_{i=0}^{n-1} \frac{1}{u - x_i^o}\right)^2 =$$

$$= \sum_{i=0}^{n-1} \frac{P_n(u)}{u - x_i^o} \sum_{\substack{j=0\\ j\neq i}}^{n-1} \frac{1}{u - x_j^o} \quad ;$$

on a alors $P_n''(x_k) = \prod_{\substack{j=0\\ j\neq k}}^{n-1} (x_k^o - x_j^o) \sum_{\substack{i=0\\ i\neq k}}^{n-1} \frac{1}{x_k^o - x_i^o} = 0$ pour $k = 1, \ldots, n-2$.

Le polynome P_n'' de degré n-2 admet pour racines les nombres $x_1^o, \ldots, x_{n-2}^o$; on a donc $(u^2-1)P_n''(u) = \lambda P_n(u)$, $\lambda \in \mathbb{R}$; le calcul de λ résulte par identification de ce que P_n est de degré n .

L'unicité de P_n provient du fait que l'équation différentielle n'admet qu'un seul polynome unitaire de degré n comme solution ; ainsi le système $\{x_1^o, \ldots, x_{n-2}^o\}$ est unique (la vérification de l'unicité se fai -

sant en posant $P_n(u) = \sum_{i=0}^{n} a_{n-i}\, u^{n-i}$, $a_n = 1$, et en identifiant les coefficients obtenus à partir de la relation $(u^2-1)P_n''(u) = n(n-1)P_n(u)$.

Proposition III 3 . Soit δ_n le discriminant du polynome P_n , $n \geq 2$, alors δ_n est défini à partir de la relation de récurrence

$$\delta_{n+1} = \frac{(n+1)^{n+1}(n-1)^{n-1}}{(2n-1)^{2n-1}}\,\delta_n \ , \quad \delta_2 = 4 \ . \ \text{On a } \mu_{\Delta_\chi} = \delta_n \text{ avec } n = g_\chi \ .$$

démonstration

Elle s'effectue en plusieurs étapes .

Lemme III 2 . Pour tout $n \geq 2$, P_n est de la parité de n et vérifie les deux relations suivantes :

$$\text{(i)} \qquad u\frac{P_n'}{n} - P_n = \frac{P_{n-1}'}{2n-3} \ ,$$

$$\text{(ii)} \qquad u\frac{P_n'}{n} - \frac{P_{n+1}'}{n+1} = \frac{n-1}{(2n-1)(2n-3)}\,P_{n-1}' \ .$$

Posons $P_n(u) = \sum_{i=0}^{n} a_{n-i}\, u^{n-i}$ (avec $a_n = 1$) , alors la relation $(u^2-1)P_n''(u) = n(n-1)P_n(u)$ conduit aux relations :

$$(n-1)(n-2)\,a_{n-1} = n(n-1)\,a_{n-1} \quad \text{et}$$

$$(n-1-2k)(n-2-2k)a_{n-1-2k} - (n+1-2k)(n-2k)a_{n+1-2k} = n(n-1)a_{n-1-2k} \ ,$$

$1 \leq k \leq \frac{n-1}{2}$, soit $a_{n-1} = 0$ et

$$2(2k+1)(k+1-n)a_{n-1-2k} = (n+1-2k)(n-2k)a_{n+1-2k} \ , \quad 1 \leq k \leq \frac{n-1}{2} \ ,$$

d'où la nullité des coefficients a_{n-1-2k} pour $0 \leq k \leq \frac{n-1}{2}$.

(i) Posons $T = u\frac{P_n'}{n} - P_n$; alors $T' = u\frac{P_n''}{n} + \frac{P_n'}{n} - P_n' = u\frac{P_n''}{n} - \frac{n-1}{n}P_n'$ et $T'' = u\frac{P_n'''}{n} + \frac{P_n''}{n} - \frac{n-1}{n}P_n'' = u\frac{P_n'''}{n} - \frac{n-2}{n}P_n''$ et on obtient la relation

$(u^2-1)\,T'' + 2u\,T' = u(u^2-1)\dfrac{P'''_n}{n} - \dfrac{n-2}{n}(u^2-1)\,P''_n + 2u^2\dfrac{P''_n}{n} - 2\dfrac{n-1}{n}u\,P'$;

en tenant compte de la relation $(u^2-1)\,P''_n = n(n-1)\,P_n$ et de celle qui s'en déduit par dérivation , on obtient

$(u^2-1)T'' + 2uT' = (n-1)(n-2)\left(u\dfrac{P'_n}{n} - P_n\right) = (n-1)(n-2)\,T$ par conséquent il existe une primitive $\overline{T}$ de T telle que $(u^2-1)\overline{T}'' = (n-1)(n-2)\overline{T}$;

or $T = u\dfrac{P'_n}{n} - P_n$ a pour terme de plus haut degré

$\left(\dfrac{n-2}{n}\,a_{n-2} - a_{n-2}\right)u^{n-2} = \dfrac{n-1}{2n-3}\,u^{n-2}$ après avoir calculé a_{n-2} à l'aide de la relation $(u^2-1)\,P''_n = n(n-1)\,P_n$; $\overline{T}$, de degré n-1 , sera déterminé de manière unique, et, compte-tenu de son terme de plus haut degré $\left(\dfrac{u^{n-1}}{2n-3}\right)$, on aura $\overline{T} = \dfrac{P_{n-1}}{2n-3}$, d'où $T = \dfrac{P'_{n-1}}{2n-3}$.

(ii) Si on considère la relation (i) précédente au rang n+1 , on a $u\dfrac{P'_{n+1}}{n+1} - P_{n+1} = \dfrac{n}{2n-1}\dfrac{P'_n}{n}$ qui donne en dérivant

$u\dfrac{P''_{n+1}}{n+1} + \dfrac{P'_{n+1}}{n+1} - P'_{n+1} = \dfrac{P''_n}{2n-1}$ soit (avec $(u^2-1)P''_{n+1} = n(n+1)P_{n+1}$)

$u\,P_{n+1} - (u^2-1)\dfrac{P'_{n+1}}{n+1} = \dfrac{n-1}{2n-1}\,P_n$; or $P_n = u\dfrac{P'_n}{n} - \dfrac{P'_{n-1}}{2n-3}$ et

$P_{n+1} = u\dfrac{P'_{n+1}}{n+1} - \dfrac{P'_n}{2n-1}$ d'où

$u\left(u\dfrac{P'_{n+1}}{n+1} - \dfrac{1}{2n-1}P'_n\right) - (u^2-1)\dfrac{P'_{n+1}}{n+1} = \dfrac{n-1}{2n-1}\left(u\dfrac{P'_n}{n} - \dfrac{P'_{n-1}}{2n-3}\right)$ soit

$u\dfrac{P'_n}{n} - \dfrac{P'_{n+1}}{n+1} = \dfrac{n-1}{(2n-1)(2n-3)}\,P'_{n-1}$.

Pour calculer δ_{n+1} et δ_n , on introduit le résultant de P_n et P'_n (cf. [12]) : le résultant de deux polynomes P et Q sera noté $\mathcal{R}(P,Q)$; on sait que $\delta_n = \mathcal{R}(P_n , P'_n)$ car P_n est unitaire .

Lemme III 3 . Soient Q_n et Q_{n-1} deux polynomes unitaires de degrés respectifs $n \geq 1$ et $n-1$ ayant la parité de leurs degrés .

Alors $\mathfrak{R}(Q_n , Q_{n-1}) = (-1)^{n-1} \mathfrak{R}(Q_n - u Q_{n-1} , Q_{n-1})$.

Posons $Q_n = u^n + a_2 u^{n-2} + a_4 u^{n-4} + \dots$ et $Q_{n-1} = u^{n-1} + b_2 u^{n-3} + b_4 u^{n-5} + \dots$; alors $\mathfrak{R}(Q_n , Q_{n-1}) =$

$$\left|\begin{matrix} 1 & 0 & a_2 & 0 & a_4 & \dots \\ 0 & 1 & 0 & a_2 & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \\ 1 & 0 & b_2 & 0 & b_4 & \dots \\ 0 & 1 & 0 & b_2 & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \end{matrix}\right| \begin{matrix} \\ \\ \} n-1 \\ \\ \} n \end{matrix} = \left|\begin{matrix} 0 & 0 & a_2-b_2 & 0 & a_4-b_4 & \dots \\ 0 & 0 & 0 & a_2-b_2 & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \\ 1 & 0 & b_2 & 0 & b_4 & \dots \\ 0 & 1 & 0 & b_2 & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \end{matrix}\right| \begin{matrix} \\ \\ \} n-1 \\ \\ \} n \end{matrix}$$

(en retranchant à la $i^{\text{è}}$ ligne , la ligne $i+n-1$, pour $i = 1, 2, \dots, n-1$) ; d'où

$$\mathfrak{R}(Q_n , Q_{n-1}) = (-1)^{n-1} \left|\begin{matrix} a_2-b_2 & 0 & a_4-b_4 & 0 & \dots \\ 0 & a_2-b_2 & 0 & a_4-b_4 & \dots \\ \vdots & \vdots & \vdots & \vdots & \\ 1 & 0 & b_2 & 0 & \dots \\ 0 & 1 & 0 & b_2 & \dots \\ \vdots & \vdots & \vdots & \vdots & \end{matrix}\right| \begin{matrix} \\ \} n-1 \\ \\ \} n-2 \end{matrix} =$$

$(-1)^{n-1} \mathfrak{R}(Q_n - u Q_{n-1} , Q_{n-1})$

(après un développement partiel du déterminant par rapport aux deux premières colonnes) .

Fin de la démonstration de la proposition .

On a $\delta_n = \mathfrak{R}(P_n , P'_n) = n^n \mathfrak{R}\left(P_n , \frac{P'_n}{n}\right) = (-1)^{n+1} n^n \mathfrak{R}\left(P_n - u \frac{P'_n}{n} , \frac{P'_n}{n}\right)$

$= (-1)^{n-1} n^n \mathfrak{R}\left(-\frac{n-1}{2n-3} \frac{P'_{n-1}}{n-1} , \frac{P'_n}{n}\right)$ (Lemme III 3 et

lemme III 2 , (i)) , d'où $\delta_n = n^n \left(\frac{n-1}{2n-3}\right)^{n-1} \mathfrak{R}\left(\frac{P'_{n-1}}{n-1} , \frac{P'_n}{n}\right)$.

De même on aura $\delta_{n+1} = (n+1)^{n+1} \left(\frac{n}{2n-1}\right)^n \mathfrak{R}\left(\frac{P'_n}{n} , \frac{P'_{n+1}}{n+1}\right)$;

on applique à nouveau le lemme III 3 : on a

$$\mathfrak{R}\Big(\frac{P'_n}{n}, \frac{P'_{n+1}}{n+1}\Big) = \mathfrak{R}\Big(\frac{P'_{n+1}}{n+1}, \frac{P'_n}{n}\Big) = (-1)^{n-1}\,\mathfrak{R}\Big(\frac{P'_{n+1}}{n+1} - u\frac{P'_n}{n}, \frac{P'_n}{n}\Big) =$$

$$= \mathfrak{R}\Big(-\frac{(n-1)^2}{(2n-1)(2n-3)}\,\frac{P'_{n-1}}{n-1}, \frac{P'_n}{n}\Big) \text{ (lemme III 2, (ii)),}$$

soit $\delta_{n+1} = (n+1)^{n+1}\Big(\frac{n}{2n-1}\Big)^n\Big(\frac{(n-1)^2}{(2n-1)(2n-3)}\Big)^{n-1}\mathfrak{R}\Big(\frac{P'_{n-1}}{n-1}, \frac{P'_n}{n}\Big)$;

les expressions ainsi obtenues pour δ_n et δ_{n+1} conduisent au résultat .

Remarque III 1 . Les premières valeurs de δ_n sont : $\delta_2 = 4$, $\delta_3 = 4$, $\delta_4 = 2^{12}/5^5$, $\delta_5 = 2^{12}3^3/7^7$, $\delta_6 = 2^{26}/3^9 7^7$, ... ; on vérifie qu'on a $\frac{\delta_{n+1}}{\delta_n} \sim \frac{2ne}{4^n}$ et que pour tout $n \geq 2$ on a $\frac{\delta_{n+1}}{\delta_n} \leq \frac{2n}{4^n} e^{1+\frac{1}{n}}$.

Corollaire III 1 . La condition $\frac{M_\Phi}{\mu_\Phi} > 1$ du théorème II 1 est toujours vérifiée lorsque $\Phi = \Delta_\varkappa$ et $M_\Phi = \Delta(K_\varkappa)$ (Proposition III 1) .

En effet, on a $M_\Phi \geq 5$ (discriminant de $\mathbb{Q}(\sqrt{5})$) et $M_\Phi < 1$ sauf dans les cas $g_\varkappa = 2$, $g_\varkappa = 3$ et $g_\varkappa = 4$; dans ces trois cas , on vérifie que $\mu_\Phi \leq 4$.

2) Etude des fonctions " résolvantes de Lagrange " $N_\psi^\varkappa$.

a) Définition et propriétés des résolvantes . Soit $\varkappa$ un caractère pair . Soit $\psi' \in \mathfrak{X}'_\varkappa$ et soit $\psi \in \mathfrak{X}$ le caractère associé ; soit $\langle \varkappa, \psi' \rangle = \sum_{\sigma \in G_\varkappa} \psi'(\sigma^{-1})\, x_\sigma$ où les x_σ sont $g_\varkappa$ variables réelles ; comme ψ' prend ses valeurs dans Z_ψ , on peut considérer que $\Gamma_\psi = \mathrm{Gal}(\mathbb{Q}_\psi/\mathbb{Q})$ opère sur la $\Gamma_\mathbb{Q}$- classe $\tilde{\psi}$ de ψ . Pour $s \in \Gamma_\psi$, on posera $\psi'^s = \psi'^{a_s}$ où a_s est l'entier modulo g_ψ défini par $\zeta_\psi^s = \zeta_\psi^{a_s}$; lorsque s parcourt Γ_ψ , ψ'^s parcourt $\tilde{\psi}$ (d'après la partie I, § 1, c) , donc le produit

$N_{\psi}^{\varkappa}(x) = \prod_{s \in \Gamma_{\psi}} \langle x, \psi'^{s} \rangle = \prod_{\psi' \in \tilde{\psi}} \langle \varkappa, \psi' \rangle$ ne dépend que de la $\Gamma_{\mathbb{Q}}$-classe $\tilde{\psi}$ de ψ' (c'est une fonction polynomiale homogène réelle de degré $d_{N_{\psi}^{\varkappa}} = \varphi(g_{\psi})$) .

Lemme III 4 . Soit θ un entier du corps $K_{\varkappa}$; alors pour x défini par $x_{\sigma} = \theta^{\sigma}$, $\langle x, \psi' \rangle$, notée $\langle \theta, \psi' \rangle$, est un élément du corps $K_{\varkappa} \mathbb{Q}_{\psi}$ qui vérifie les relations suivantes :

(i) Soit $\bar{\tau} \in \mathrm{Gal}(K_{\varkappa} \mathbb{Q}_{\psi} / \mathbb{Q}_{\psi})$ considéré comme prolongement d'un élément τ de $G_{\varkappa}$, alors $\langle \theta, \psi' \rangle^{\bar{\tau}} = \psi'(\tau) \langle \theta, \psi' \rangle$.

(ii) $\langle \theta, \psi' \rangle^{g_{\psi}}$ est un élément de $\mathbb{Q}_{\psi}$.

(iii) $\sum_{\psi' \in \mathfrak{X}'_{\varkappa}} \langle \theta, \psi' \rangle = g_{\varkappa} \theta$.

Ces assertions sont immédiates .

b) Représentation des éléments de $K_{\varkappa}$ (d'après Leopoldt [16]) .

Soit $\psi' \in \mathfrak{X}'_{\varkappa}$; on considère la somme de Gauss $\tau(\psi') = \sum_{t \in (\mathbb{Z}/f_{\psi}\mathbb{Z})^*} \psi'(t) \xi_{\psi}^{t}$, où $\xi_{\psi} = \exp(2i\pi/f_{\psi})$; $\tau(\psi')$ est un élément de $\mathbb{Q}_{\psi} \mathbb{Q}^{(f_{\psi})}$ et $\tau(\psi')^{g_{\psi}} \in \mathbb{Q}_{\psi}$. Soit $\theta \in K_{\varkappa}$, d'après [16] (§1, 1 et 3) , on peut écrire $\theta = \frac{1}{g_{\varkappa}} \sum_{\psi' \in \mathfrak{X}'_{\varkappa}} y(\psi', \theta) \tau(\psi')$, les composantes $y(\psi', \theta)$ étant des éléments de $\mathbb{Q}_{\psi}$ déterminés de façon unique . Si θ est entier alors les $y(\psi', \theta)$ sont des entiers . On a alors ([16], § 1,2) : $(\det(\theta^{\sigma\tau}))^2 = \prod_{\psi'} y(\psi', \theta)^2 \Delta(K_{\varkappa})$ où $\Delta(K_{\varkappa})$ est le discriminant de $K_{\varkappa}$.

Lemme III 5 . On a $\langle \theta, \psi' \rangle = y(\psi', \theta) \tau(\psi')$.

On a $\langle \theta, \psi' \rangle = \sum_{\sigma \in G_{\varkappa}} \psi'(\sigma^{-1}) \theta^{\sigma} =$

$$= \frac{1}{g_{\varkappa}} \sum_{\sigma \in G_{\varkappa}} \psi'(\sigma^{-1}) \Big(\sum_{\varphi' \in \mathfrak{X}'_{\varkappa}} y(\varphi', \theta) \tau(\varphi') \Big)^{\sigma} \quad ;$$

d'après [16] (§ 1,1) , on aura

$$\langle \theta, \psi' \rangle = \frac{1}{g_\varkappa} \sum_{\sigma \in G_\varkappa} \psi'(\sigma^{-1}) \sum_{\varphi' \in \mathfrak{X}'_\varkappa} \varphi'(\sigma)\, y(\varphi', \theta)\, \tau(\varphi') =$$

$$= \frac{1}{g_\varkappa} \sum_{\varphi' \in \mathfrak{X}'_\varkappa} y(\varphi', \theta)\, \tau(\varphi') \sum_{\sigma \in G_\varkappa} \varphi'(\sigma)\, \psi'(\sigma^{-1}) \quad ;$$

or $\sum_{\sigma \in G_\varkappa} \varphi'(\sigma)\, \psi'(\sigma^{-1}) = \sum_{\sigma \in G_\varkappa} (\varphi'\, \psi'^{-1})(\sigma) = 0$ sauf si $\psi' = \varphi'$ auquel cas

la somme vaut $g_\varkappa$; d'où le résultat .

Lemme III 6 . Soit $\theta \in K_\varkappa$ un élément primitif . Pour tout sous-corps strict k de $K_\varkappa$, il existe un caractère $\psi' \in \mathfrak{X}'_\varkappa$ non trivial sur $\mathrm{Gal}(K_\varkappa/k)$ tel que $\langle \theta, \psi'^s \rangle \neq 0$ pour tout $s \in \Gamma_\psi$.

D'après le lemme III 4 , (iii) , on a $g_\varkappa \theta = \sum_{\psi'} \langle \theta, \psi' \rangle$;

on peut écrire $g_\varkappa \theta = \sum_{\psi'_1} \langle \theta, \psi'_1 \rangle + \sum_{\psi'_2} \langle \theta, \psi'_2 \rangle$ où ψ'_1 parcourt l'ensemble des caractères non triviaux sur $\mathrm{Gal}(K_\varkappa/k)$; en regroupant les sommations par $\Gamma_{\mathbb{Q}}$-classes on obtient $g_\varkappa \theta = \sum_{\psi_1} \langle \theta, \psi_1 \rangle + \sum_{\psi_2} \langle \theta, \psi_2 \rangle$, où l'on a posé $\langle \theta, \psi \rangle = \sum_{\psi' \in \tilde{\psi}} \langle \theta, \psi' \rangle$; soit $\tau \in \mathrm{Gal}(K_\varkappa/k)$, comme ψ'_1 est trivial sur $\mathrm{Gal}(K_\varkappa/k)$, on a $\sum_{\psi_1} \langle \theta, \psi_1 \rangle = \sum_{\psi'_1 \in \tilde{\psi}_1} \sum_{\sigma \in G_\varkappa} \psi'_1(\sigma^{-1})\, \theta^\sigma =$

$= \sum_{\psi'_1 \in \tilde{\psi}_1} \sum_{\sigma \in \mathrm{Gal}(k/\mathbb{Q})} \psi'_1(\sigma^{-1}) \left(\mathrm{Tr}_{K_\varkappa/k}\, \theta \right)^\sigma$ qui est un élément de k ;

ainsi $\sum_{\psi_2} \langle \theta, \psi_2 \rangle$ n'est pas nulle car sinon on aurait $\theta \in k$, ce qui est absurde ; ceci entraîne bien l'existence d'un caractère ψ' non trivial sur $\mathrm{Gal}(K_\varkappa/k)$ et tel que $\langle \theta, \psi' \rangle \neq 0$; en vertu du lemme III 4 , (ii) , on aura $\langle \theta, \psi'^s \rangle \neq 0$ pour tout $s \in H_\psi$.

Remarque III 2 . Lorsque $G_\varkappa$ est d'ordre ℓ^n , ℓ premier , alors pour tout élément primitif $\theta \in K_\varkappa$, on a $\langle \theta, \varkappa \rangle \neq 0$. En effet , il suffit d'appliquer le lemme précédent au sous-corps k cyclique de degré ℓ^{n-1} sur $\mathbb{Q}$,

les seuls caractères de $K_\varkappa$ non triviaux sur $Gal(K_\varkappa/k)$ étant les éléments de $\tilde{\varkappa}$.

Proposition III 4 . Soit θ un élément primitif de $K_\varkappa$; on suppose θ entier . Soit $\psi' \in \mathfrak{X}'^{*}_{\varkappa}$ tel que $\langle \theta, \psi' \rangle \neq 0$.

Alors $\quad |N^{\varkappa}_{\psi}(\ldots, \theta^{\sigma}, \ldots)| \geq f_{\psi}^{\varphi(g_\psi)/2}$.

démonstration

Soit ψ' un caractère de $G_\varkappa$ non trivial tel que $\langle \theta, \psi' \rangle$ soit non nul (cf. Lemme III 6) . On sait (lemme III 4 , (ii)) que $\langle \theta, \psi' \rangle^{g_\psi} \in \mathbf{Q}_\psi$, or $\langle \theta, \psi' \rangle^{g_\psi} = y(\psi', \theta)^{g_\psi} \tau(\psi')^{g_\psi}$ et $y(\psi', \theta)$ est un élément de $\mathbf{Z}_\psi$ par conséquent $N_{\mathbf{Q}_\psi/\mathbf{Q}} \langle \theta, \psi' \rangle^{g_\psi}$ sera un rationnel multiple entier de $N_{\mathbf{Q}_\psi/\mathbf{Q}}(\tau(\psi')^{g_\psi})$.

On a $N_{\mathbf{Q}_\psi/\mathbf{Q}}(\tau(\psi')^{g_\psi}) = \prod_{s \in \Gamma_\psi} (\tau(\psi'))^{g_\psi s}$ et on distingue deux cas :

(i) $\mathbf{Q}_\psi$ est imaginaire (i.e. $g_\psi > 2$) . Alors en appelant Γ^{o}_{ψ} le groupe de Galois du sous-corps réel maximal de $\mathbf{Q}_\psi$, on aura

$N_{\mathbf{Q}_\psi/\mathbf{Q}}(\tau(\psi')^{g_\psi}) = \prod_{s \in \Gamma^{o}_{\psi}} (\tau(\psi')^{g_\psi} \overline{\tau(\psi')}^{g_\psi})^{s}$ où $\overline{\tau(\psi')}$ est le conjugué complexe de $\tau(\psi')$. Or on sait que $\tau(\psi')\overline{\tau(\psi')} = f_\psi$ ([14] , p. 82) par conséquent on obtient $N_{\mathbf{Q}_\psi/\mathbf{Q}}(\tau(\psi')^{g_\psi}) = f_{\psi}^{g_\psi \varphi(g_\psi)/2}$; or

$N^{\varkappa}_{\psi}(\ldots, \theta^{\sigma}, \ldots)^{g_\psi} = \prod_{s \in \Gamma_\psi} \langle \theta, \psi'^{s} \rangle^{g_\psi} = N_{\mathbf{Q}_\psi/\mathbf{Q}}(\langle \theta, \psi' \rangle^{g_\psi})$ (lemme III 4, (ii)) soit $N^{\varkappa}_{\psi}(\ldots, \theta^{\sigma}, \ldots)^{g_\psi} \geq f_{\psi}^{g_\psi \varphi(g_\psi)/2}$, d'où le résultat .

(ii) Si $g_\psi = 2$, alors ψ' est un caractère quadratique (non trivial) ; $N^{\varkappa}_{\psi}(\ldots, \theta^{\sigma}, \ldots)^2$ sera un multiple entier de $\tau(\psi')^2 \in \mathbf{Z}$; on a $\tau(\psi')\overline{\tau(\psi')} = f_\psi$ et $\tau(\psi')^2 \in \mathbf{Z}$ d'où $(\tau(\psi'))^2 = \pm f_\psi$ soit $|N^{\varkappa}_{\psi}(\ldots, \theta^{\sigma}, \ldots)| \geq \sqrt{f_\psi}$.

Remarque III 3 . La constante M_Φ du théorème II 1 relative à $\Phi = N_\psi^\varkappa$ est donc de la forme $f_\psi^{\varphi(g_\psi)/2}$ sous réserve que le caractère ψ considéré soit tel que $\langle \varepsilon, \psi' \rangle \neq 0$ pour tout $\varepsilon \in E_\varkappa^*$, $|\varepsilon| \neq 1$. Par exemple , lorsque $g_\varkappa = \ell^n$, ℓ premier , on a $M_\Phi = f_\varkappa^{\varphi(g_\varkappa)/2}$ où $\Phi = N_\varkappa^\varkappa$ (cf. Remarque III 2) . Plus généralement , lorsqu'on n'a pas d'information sur la non nullité des résolvantes $\langle \varepsilon, \psi' \rangle$, $\varepsilon \in E_\varkappa$, on devra prendre comme fonction Φ (de type résolvante) la fonction $\Phi = N_\psi^\varkappa$ telle que $\frac{1}{2d_\Phi} \operatorname{Log} \frac{M_\Phi}{\mu_\Phi}$ soit minimum (autrement dit le théorème II 1 conduit , dans ce cas , à une inégalité de la forme $r(F) \leq \frac{\mathfrak{M}_\varkappa(F)}{\mathfrak{m}_\varkappa(F)} \left(\operatorname{Min}_\psi \frac{1}{2\varphi(g_\psi)} \operatorname{Log} \frac{f_\psi^{\varphi(g_\psi)/2}}{\mu_{N_\psi^\varkappa}} \right)^{-\varphi(g_\varkappa)}$, sous réserve que l'on ait $f_\psi^{\varphi(g_\psi)/2} > \mu_{N_\psi^\varkappa}$ pour tout ψ) .

On remarque que la condition $\frac{M_\Phi}{\mu_\Phi} > 1$ n'est pas toujours vérifiée (elle l'est dès que le conducteur est plus grand qu'une certaine valeur critique) . On est donc obligé dans ce cas d'utiliser la fonction discriminant .

c) Première réduction pour le calcul de la constante μ_Φ pour $\Phi = N_\psi^\varkappa$.

On a $\mu_\Phi = \operatorname{Sup}_{x \in C_\varkappa} |N_\psi^\varkappa(x)|$ où $C_\varkappa$ est , dans $\mathbb{R}^{g_\varkappa}$, la sphère unité pour la distance du maximum . Pour certaines valeurs particulières de $g_\varkappa$ on peut trouver la valeur exacte de μ_Φ ; dans le cas général on établira des majorations .

Lemme III 7 . Soit $\psi' \in \mathfrak{X}'_\varkappa$, soit K_ψ le sous-corps de $K_\varkappa$ correspondant à ψ . Alors on a la relation $\mu_{N_\psi^\varkappa} = \mu_{N_\psi^\psi} \left(\frac{g_\varkappa}{g_\psi} \right)^{\varphi(g_\psi)}$.

On a en effet $N_\psi^\varkappa(x) = \prod_{\psi' \in \tilde{\psi}} \langle x, \psi' \rangle$ et

$$\langle x, \psi' \rangle = \sum_{\sigma \in G_\varkappa} \psi'(\sigma^{-1}) x_\sigma = \sum_{\tau \in G_\psi} \psi'(\tau^{-1}) \sum_{\sigma \in \Gamma} x_{\sigma\tau} = \langle \sum_{\sigma \in \Gamma} x_\sigma , \psi' \rangle ,$$

où $\Gamma = \mathrm{Gal}(K_\varkappa / K_\psi)$, cette résolvante étant relative au groupe G_ψ ; on a donc $N_\psi^\varkappa(x) = \prod_{\psi' \in \tilde{\psi}} \langle y, \psi' \rangle = N_\psi^\psi(y)$, où $y_\tau = \sum_{\sigma \in \Gamma} x_{\sigma\tau}$, or

$$\mu_{N_\psi^\varkappa} = \sup_{x \in C_\varkappa} |N_\psi^\varkappa(x)| = \sup_{x \in C'_\varkappa} |N_\psi^\varkappa(x)| \quad \text{où}$$

$C'_\varkappa = \left\{ x \in \mathbb{R}^{g_\varkappa} , |x_\sigma| \leq 1 , \text{ pour tout } \sigma \in G_\varkappa \right\}$. Lorsque les x_σ varient dans $[-1,+1]$, $y = (y_\tau)_{\tau \in G_\psi}$, parcourt le domaine $C''_\varkappa = \left\{ y \in \mathbb{R}^{g_\psi} , |y_\tau| \leq \frac{g_\varkappa}{g_\psi} , \text{ pour tout } \tau \in G_\psi \right\}$; comme N_ψ^ψ est homogène de degré $\varphi(g_\psi)$ on aura

$$\sup_{x \in C'_\varkappa} |N_\psi^\varkappa(x)| = \sup_{y \in C''_\varkappa} |N_\psi^\psi(y)| = \left(\frac{g_\varkappa}{g_\psi}\right)^{\varphi(g_\psi)} \sup_{z \in C'_\psi} |N_\psi^\psi(z)| =$$

$$= \left(\frac{g_\varkappa}{g_\psi}\right)^{\varphi(g_\psi)} \mu_{N_\psi^\psi} .$$

On est ainsi ramené au calcul des constantes $\mu_{N_\psi^\psi}$ pour tout caractère ψ.

d) Majoration de μ_Φ pour $\Phi = N_\varkappa^\varkappa$.

On a $N_\varkappa^\varkappa(x) = \prod_{\varkappa' \in \tilde{\varkappa}} \langle x, \varkappa' \rangle = \prod_{s \in \Gamma_\varkappa} \langle x, \varkappa'^s \rangle$ où $\varkappa'$ est un élément quelconque de $\tilde{\varkappa}$.

Dans le cas $g_\varkappa = 2$, on a $N_\varkappa^\varkappa(x) = x_1 - x_\sigma$ et on a $\mu_\Phi = 2$.

Dans le cas $g_\varkappa > 2$, on peut écrire

$N_\varkappa^\varkappa(x) = \prod_{s \in \Gamma_\varkappa^o} \langle x, \varkappa'^s \rangle \overline{\langle x, \varkappa'^s \rangle}$ où $\Gamma_\varkappa^o = \mathrm{Gal}(\mathbb{Q}(\zeta_\varkappa + \zeta_\varkappa^{-1}) / \mathbb{Q})$: soit

$A_s = \langle x, \varkappa'^s \rangle \overline{\langle x, \varkappa'^s \rangle}$, pour $s \in \Gamma_\varkappa^o$, alors on a

$$A_s = \sum_{\sigma \in G_\varkappa} \varkappa'^{a_s(\sigma^{-1})} x_\sigma \overline{\sum_{\tau \in G_\varkappa} \varkappa'^{a_s(\tau^{-1})} x_\tau} =$$

$$= \sum_{\sigma,\tau \in G_\varkappa} \varkappa'^{a_s(\sigma^{-1}) - a_s(\tau^{-1})} x_\sigma x_\tau = \sum_{\sigma,\tau \in G_\varkappa} \varkappa'^{a_s(\sigma^{-1}\tau)} x_\sigma x_\tau =$$

$$= \sum_{\sigma,\tau \in G_\varkappa} \varkappa'^{a_s(\tau)} x_\sigma x_{\sigma\tau} \quad .$$

D'après l'inégalité de la moyenne arithmétique et de la moyenne géométrique , on a

$$(N_\varkappa^\varkappa(x))^{2/\varphi(g_\varkappa)} = \Big(\prod_{s \in \Gamma_\varkappa^o} A_s \Big)^{2/\varphi(g_\varkappa)} \le \frac{2}{\varphi(g_\varkappa)} \sum_{s \in \Gamma_\varkappa^o} A_s =$$

$$= \frac{2}{\varphi(g_\varkappa)} \sum_{s \in \Gamma_\varkappa^o} \sum_{\sigma,\tau \in G_\varkappa} \varkappa'^{a_s(\tau)} x_\sigma x_{\sigma\tau} =$$

$$= \frac{1}{\varphi(g_\varkappa)} \sum_{s \in \Gamma_\varkappa} \sum_{\sigma,\tau \in G_\varkappa} \varkappa'^{a_s(\tau)} x_\sigma x_{\sigma\tau}$$

puisque la somme est réelle ; on obtient donc

$$(N_\varkappa^\varkappa(x))^{2/\varphi(g_\varkappa)} \le \frac{1}{\varphi(g_\varkappa)} \sum_{\sigma,\tau \in G_\varkappa} x_\sigma x_{\sigma\tau} \sum_{s \in \Gamma_\varkappa} \varkappa'^{a_s(\tau)} \quad ;$$

or $\sum_{s \in H_\varkappa} \varkappa'^{a_s(\tau)} = \varkappa(\tau)$ par définition du caractère rationnel $\varkappa$;

$$\text{d'où } (N_\varkappa^\varkappa(x))^{2/\varphi(g_\varkappa)} \le \frac{1}{\varphi(g_\varkappa)} \sum_{\sigma,\tau \in G_\varkappa} \varkappa(\tau) x_\sigma x_{\sigma\tau} =$$

$$= \frac{1}{\varphi(g_\varkappa)} \sum_{\sigma,\tau \in G_\varkappa} \varkappa(\sigma^{-1}\tau) x_\sigma x_\tau \quad .$$

Appelons $q_\varkappa$ la forme quadratique $\sum_{\sigma,\tau \in G_\varkappa} \varkappa(\sigma^{-1}\tau) x_\sigma x_\tau$ dont la matrice associée est $(\varkappa(\sigma^{-1}\tau))_{\sigma,\tau \in G_\varkappa}$. Pour $g_\varkappa = 2$ définissons $q_\varkappa = (x_1 - x_\sigma)^2$. Dans tous les cas on aura

$\mu_\Phi = \sup_{x \in C_\varkappa} N_\varkappa^\varkappa(x) \leq \left(\frac{1}{\varphi(g_\varkappa)} \sup_{x \in C_\varkappa} q_\varkappa(x) \right)^{\varphi(g_\varkappa)/2}$; on a le résultat suivant :

Lemme III 8 . Soit $\hat{C}_\varkappa = \left\{ x = (x_\sigma)_{\sigma \in G_\varkappa} , x_\sigma \in \{-1,+1\} \right\}$ (ensemble des $2^{g_\varkappa}$ sommets de l'hypercube unité) ; alors $\sup_{x \in C_\varkappa} q_\varkappa(x) = \sup_{x \in \hat{C}_\varkappa} q_\varkappa(x)$.

Soit x° un point de $C_\varkappa$ où $q_\varkappa$ atteint son maximum ; supposons que l'une des composantes de x° soit différente de ± 1 ; on peut supposer que c'est x_1° car $q_\varkappa$ est invariante par permutation circulaire des variables . Fixons les variables x_σ aux valeurs x_σ° pour $\sigma \neq 1$ et considérons la fonction $\gamma(x_1) = q_\varkappa(x_1, \ldots, x_\sigma^\circ, \ldots)$ d'une variable . On a $\gamma'(x_1^\circ) = 0$ puisque x_1° est un maximum local ; or on a $\gamma''(x_1) = 2\varkappa(1) = 2\varphi(g_\varkappa) > 0$, par conséquent x_1° ne peut représenter qu'un minimum de la fonction γ , donc on aura $\max_{-1 \leq x_1 \leq +1} \gamma(x_1) = \gamma(-1)$ ou $\gamma(1)$.

Corollaire 1 . On peut trouver un majorant de μ_Φ après un nombre fini d'essais . On a

$$\mu_\Phi \leq \left(\frac{1}{\varphi(g_\varkappa)} \sup_{x, x_\sigma \in \{\pm 1\}} q_\varkappa(x) \right)^{\varphi(g_\varkappa)/2} .$$

Cependant , pour un degré élevé , le nombre d'essais devient prohibitif .

Corollaire 2 . Lorsque $g_\varkappa$ est égal à un nombre premier $\ell > 2$, on a l'inégalité $\mu_\Phi \leq (\ell+1)^{(\ell-1)/2}$. Pour $g_\varkappa = 2$ on a $\mu_\Phi = 2$.

Dans ce cas on aura $\varkappa(1) = \ell - 1$ et , pour tout $\sigma \in G_\varkappa$, $\sigma \neq 1$, $\varkappa(\sigma) = -1$; d'où $q_\varkappa(x) = (\ell-1) \sum_{\sigma \in G_\varkappa} x_\sigma^2 - \sum_{\substack{\sigma, \tau \in G_\varkappa \\ \sigma \neq \tau}} x_\sigma x_\tau$.

Soit a le nombre de variables égales à +1 au maximum (les ℓ-a autres valent -1) ; on a immédiatement
$q_\varkappa(x) = (\ell-1)\ell - a(a-1) - (\ell-a)(\ell-a-1) + 2a(\ell-a) = -4a^2 + 4a\ell$ dont

la valeur maximum est atteinte pour $a = \frac{\ell-1}{2}$ (et $a = \frac{\ell+1}{2}$) et sa valeur est $\ell^2 - 1$, d'où le résultat .

Remarque III 4 . On vérifie que , pour les nombres $g_\varkappa$ premiers , la double majoration ci-dessus peut être atteinte : par exemple, pour $\ell = 7$ on a $N_{\mathbb{Q}(7)/\mathbb{Q}}(1 + \zeta - \zeta^2 + \zeta^3 - \zeta^4 - \zeta^5 - \zeta^6) = 8^3$; pour $\ell = 11$ on a $N_{\mathbb{Q}(11)/\mathbb{Q}}(1 + \zeta - \zeta^2 + \zeta^3 - \zeta^4 - \zeta^5 + \zeta^6 - \zeta^7 - \zeta^8 - \zeta^9 + \zeta^{10}) = 12^5$;

par contre, pour $\ell = 5$ elle n'est pas atteinte car dans ce cas la cons - tante μ est égale à 25 .

Proposition III 5 . On a pour $\Phi = N_\varkappa^\varkappa$, $\mu_\Phi \leq \left(\frac{g_\varkappa^2}{\varphi(g_\varkappa)}\left(1 - \frac{1}{\ell^2}\right)\right)^{\varphi(g_\varkappa)/2}$,

où ℓ est le plus petit diviseur premier impair de $g_\varkappa$ (si $g_\varkappa$ est une puissance de 2 on a seulement $\mu_\Phi \leq \left(\frac{g_\varkappa^2}{\varphi(g_\varkappa)}\right)^{\varphi(g_\varkappa)/2}$) .

démonstration

Pour simplifier les notations posons $g_\varkappa = n$, remplaçons les variables x_σ , $\sigma \in G_\varkappa$ par les variables x_i , $i = 1, 2, \ldots, n$, i défini modulo n , et posons $\zeta_d = \exp(2i\pi/d)$. Pour tout diviseur d de n , soit

$$q_d^{(n)} = \sum_{(j,d)=1}^{n} \sum_{i=1}^{n} \zeta_n^{ijn/d} \sum_{k=1}^{n} x_k x_{k+i} \quad ; \text{ on a pour } n \geq 2$$

$$q_n^{(n)} = \sum_{(j,n)=1}^{n} \sum_{i=1}^{n} \sum_{k=1}^{n} \zeta^{ij} x_k x_{k+i} = q_\varkappa \text{ et la définition de } q_d^{(n)} ,$$

$d|n$, est cohérente .

Soit d un diviseur de n ; on a

$$\sum_{\delta|d} q_\delta^{(n)} = \sum_{\delta|d} \sum_{(j,\delta)=1} \sum_{i,k=1}^{n} \zeta_n^{ijn/\delta} x_k x_{k+i} =$$

$$= \sum_{i=1}^{n} \left(\sum_{\delta|d} \sum_{(j,\delta)=1} \zeta_n^{ijn/\delta} \right) \sum_{k=1}^{n} x_k x_{k+i} =$$

$$= \sum_{i=1}^{n} \left(\sum_{\lambda=1}^{d} \zeta_d^{i\lambda} \right) \sum_{k=1}^{n} x_k x_{k+i} = \sum_{\ell=1}^{n/d} d \sum_{k=1}^{n} x_k x_{k+\ell d} =$$

.../...

$$= d \sum_{i=1}^{d} \sum_{\ell,\lambda=1}^{n/d} x_{i+(\lambda+\ell)d}\, x_{i+\lambda d} =$$

$$= d \sum_{i=1}^{d} \sum_{\lambda,\ell=1}^{n/d} x_{i+\ell d}\, x_{i+\lambda d} = d \sum_{i=1}^{d} \Big(\sum_{\lambda=1}^{n/d} x_{i+\lambda d} \Big)^2 .$$

Si l'on pose $\rho_d^{(n)} = d \sum_{i=1}^{d} \Big(\sum_{\lambda=1}^{n/d} x_{i+\lambda d} \Big)^2$, $d|n$, on a $\sum_{\delta|d} q_\delta^{(n)} = \rho_d^{(n)}$ pour tout diviseur d de n ; il en résulte alors la formule $q_d^{(n)} = \sum_{\delta|d} \mu\Big(\frac{d}{\delta}\Big) \rho_d^{(n)}$, $d|n$, où μ est la fonction de Möbius .

On remarque alors que $\rho_d^{(n)} = \rho_d^{(d)} \Big(\dots, \sum_{\lambda=1}^{n/d} x_{i+\lambda d}, \dots \Big)$ et

$q_d^{(n)} = q_d^{(d)} \Big(\dots, \sum_{\lambda=1}^{n/d} x_{i+\lambda d}, \dots \Big)$.

Soit maintenant p un diviseur premier de n ; posons $n = p^\alpha n' = pn''$, $\alpha \geq 1$, $(p,n') = 1$. Alors

$$q_n = q_n^{(n)} = \sum_{\substack{d|n \\ p|d}} \mu\Big(\frac{n}{d}\Big) \rho_d^{(n)} + \sum_{\substack{d|n \\ p\nmid d}} \mu\Big(\frac{n}{d}\Big) \rho_d^{(n)} =$$

$$= \sum_{d|n''} \mu\Big(\frac{n''}{d}\Big) \rho_{pd}^{(n)} + \sum_{d|n'} \mu\Big(p^\alpha \frac{n'}{d}\Big) \rho_d^{(n)} =$$

$$= p \sum_{d|n''} \mu\Big(\frac{n''}{d}\Big) d \sum_{i=1}^{pd} \Big(\sum_{\lambda=1}^{n''/d} x_{i+\lambda pd} \Big)^2 + \mu(p^\alpha) \sum_{d|n'} \mu\Big(\frac{n'}{d}\Big) \rho_d^{(n)} =$$

$$= p \sum_{d|n''} \mu\Big(\frac{n''}{d}\Big) d \sum_{j=1}^{p} \sum_{\ell=1}^{d} \Big(\sum_{\lambda=1}^{n''/d} x_{j+p(\ell+\lambda d)} \Big)^2 + \mu(p^\alpha) q_{n'}^{(n)} =$$

$$= p \sum_{j=1}^{p} \Big(\sum_{d|n''} \mu\Big(\frac{n''}{d}\Big) d \sum_{\ell=1}^{d} \Big(\sum_{\lambda=1}^{n''/d} x_{j+p(\ell+\lambda d)} \Big)^2 \Big) + \mu(p^\alpha) q_{n'}^{(n)} =$$

$$= p \sum_{j=1}^{p} q_{n''}^{(n'')} \big(x_{p+j}, x_{2p+j}, \dots, x_{n''p+j} \big) + \mu(p^\alpha)\, q_{n'}^{(n)} .$$

Posons $s_d = \text{Sup}\, q_d^{(d)}(x)$, la borne supérieure étant prise sur l'hypercube unité de $\mathbb{R}^d$. On a $\omega(p^\alpha) \in \{0,-1\}$ et on vérifie que $q_{n'}^{(n)} \geq 0$, d'où $s_n \leq p^2 s_{n''}$ (en effet . les p systèmes de variables $(x_{p+j}, \ldots, x_{n''p+j})$ pour $j = 1, \ldots, p$, sont indépendants) . Si $g_\varkappa = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t}$, alors $s_{g_\varkappa} \leq p_1^{2(\alpha_1-1)} p_2^{2\alpha_2} \ldots p_t^{2\alpha_t} s_{p_1}$ avec $s_{p_1} \leq p_1^2 - 1$ si $p_1 \neq 2$ (corollaire 2) .

On aura donc $\dfrac{s_{g_\varkappa}}{\varphi(g_\varkappa)} \leq \dfrac{g_\varkappa^2}{\varphi(g_\varkappa)} \dfrac{p_1^2-1}{p_1^2} = \dfrac{g_\varkappa^2}{\varphi(g_\varkappa)}\left(1-\dfrac{1}{p_1^2}\right)$; la majoration est meilleure si l'on prend pour p_1 le plus petit diviseur premier impair de $g_\varkappa$. D'où le résultat (dans le cas où $g_\varkappa$ est une puissance de 2 , on a $s_2 = 4$ d'où l'inégalité dans ce cas) .

Remarque III 5 . On montre par une étude directe que , lorsque $g_\varkappa$ est de la forme $p^\alpha q^\beta$, p, q premiers , $2 < p \leq q$, $\alpha\beta \geq 0$, alors $s_{g_\varkappa} = g_\varkappa^2\left(1-\dfrac{1}{p^2}\right)$.

3) Cas particulier . Dans le cas où $[K:\mathbb{Q}]$ est un nombre premier impair ℓ , l'expression du majorant de h_K relatif à la fonction résolvante (théorème II 1) est particulièrement simple . Soit f le conducteur de K et soit $\mathcal{R}(\eta)$ le régulateur de l'unité cyclotomique génératrice au sens habituel ([12]) ; on a le résultat suivant :

Proposition III 6 . Si Φ est la fonction résolvante associée au caractère non trivial de $\text{Gal}(K/\mathbb{Q})$, alors le nombre de classes de K vérifie l'inégalité

$$h_K \leq \frac{\mathcal{R}(\eta)}{\left(\text{Log}\sqrt{\dfrac{f}{\ell+1}}\right)^{\ell-1}} \quad .$$

démonstration

Dans le cas où $[K:\mathbb{Q}]$ est premier impair , la formule du nombre de classes devient $h_K = h_\varkappa$ où $\varkappa$ est l'unique caractère rationnel irréductible non trivial de K , d'où

$$h_K \leq \frac{\mathfrak{M}_\varkappa(F_\varkappa)}{m_\varkappa}\left(\frac{1}{2d_\Phi}\,\mathrm{Log}\,\frac{M_\Phi}{\mu_\Phi}\right)^{1-\ell} \quad \text{avec } \mathfrak{M}_\varkappa(F_\varkappa) = \sqrt{\ell}\,\mathfrak{R}(\eta)\,,\ m_\varkappa = 2^{\ell-1}$$

(partie II, § 4, b) , $d_\Phi = \ell-1$, $M_\Phi = f^{\frac{\ell-1}{2}}$ (cf. Remarques III 2 et III 3) et $\mu_\Phi \leq (\ell+1)^{(\ell-1)/2}$ (corollaire 2 précédent) . Enfin , comme le plus petit conducteur possible est au moins égal à $2\ell+1$, l'hypothèse M_Φ / μ_Φ est toujours vérifiée et le théorème II 1 est toujours valable .

Dans la pratique on ne calcule pas $\mathfrak{R}(\eta)$ mais le $\varkappa$-régula - teur $R_\varkappa(F_\varkappa)$ qui est un produit de formes linéaires en Log $|\eta^\sigma|$; on utilise alors la relation $\mathfrak{R}(\eta) = \frac{1}{\ell} R_\varkappa(F_\varkappa)$.

Corollaire . Si $K/\mathbb{Q}$ est une extension cubique cyclique , alors

$$h_K \leq 4\,\frac{\mathfrak{R}(\eta)}{\left(\mathrm{Log}\,\frac{f}{4}\right)^2} \quad .$$

Remarques III 6 .

(i) Cette majoration améliore légèrement celle trouvée dans [9], par une autre méthode . En fait , la méthode utilisée dans [9] conduit aussi à la même majoration (cf.[10]) à condition d'utiliser les meil - leures constantes possibles .

(ii) En considérant la fonction discriminant ($\ell = 3$) on trouve l'inégalité $h_K \leq 9\,\frac{\mathfrak{R}(\eta)}{\left(\mathrm{Log}\,\frac{f}{2}\right)^2}$ qui est moins bonne que la précédente pour $f > 19$.

IV

Algorithmes généraux .

Dévissage des unités cyclotomiques . Soit $\varkappa \neq 1$ un caractère pair fixé. Nous allons d'abord donner un moyen de reconnaître si un nombre algébrique est puissance $q^{\text{ème}}$ dans $K_\varkappa$:

Lemme IV 1 . Soit θ un entier primitif de $K_\varkappa$ et soit $q \in \mathbb{Z}$, $q > 1$. On suppose que lorsque q est pair , tous les conjugués de θ sont positifs . Pour tout $\sigma \in G_\varkappa$ on pose $t_\sigma = (\theta^\sigma)^{1/q}$ (pour q pair, $t_\sigma = \sqrt[q]{\theta^\sigma} > 0$; pour q impair, t_σ est la racine $q^{\text{ème}}$ réelle de θ^σ) :

(i) Dans le cas q impair , une condition nécessaire et suffisante pour que les nombres t_σ appartiennent à $K_\varkappa$ est que le polynome $P = \prod_{\sigma \in G_\varkappa} (X - t_\sigma)$ soit à coefficients entiers rationnels . Lorsque cette condition est réalisée alors $t_\sigma = t_1^\sigma$ pour tout $\sigma \in G_\varkappa$.

(ii) Dans le cas q pair , une condition nécessaire et suffisante pour que les nombres t_σ appartiennent à $K_\varkappa$ est qu'il existe des nombres $\delta_\sigma \in \{-1,+1\}$ tels que le polynome $P = \prod_{\sigma \in G_\varkappa} (X - \delta_\sigma t_\sigma)$ soit à coefficients entiers rationnels . Lorsque cette condition est réalisée , on a $t_\sigma = \delta_1 \delta_\sigma t_1^\sigma$.

démonstration

Ces conditions sont trivialement nécessaires car on vérifie alors que les t_σ sont les conjugués d'un élément de $K_\varkappa$.

(i) Supposons que P soit à coefficients dans $\mathbb{Z}$; soit $\sigma \in G_\varkappa$ et soit $k_\sigma = \mathbb{Q}(t_\sigma)$; on a par hypothèse $K_\varkappa = \mathbb{Q}(t_\sigma^q)$, d'où l'inclusion $K_\varkappa \subset k_\sigma$ qui prouve que $[k_\sigma : \mathbb{Q}] \geq g_\varkappa$; or $[k_\sigma : \mathbb{Q}]$ est égal au degré du polynome irréductible de t_σ sur $\mathbb{Q}$; comme t_σ est racine de $P \in \mathbb{Z}[X]$ de degré $g_\varkappa$, on aura $[k_\sigma : \mathbb{Q}] \leq g_\varkappa$ d'où $k_\sigma = K_\varkappa$ (et ceci pour tout $\sigma \in G_\varkappa$). On a par exemple $\mathbb{Q}(t_1) = K_\varkappa$, et t_1^σ vérifie $(t_1^\sigma)^q = \theta^\sigma = t_\sigma^q$, d'où $t_1^\sigma = t_\sigma$ puisque q est impair .

(ii) On démontre de la même façon que précédemment que $\mathbb{Q}(\delta_\sigma t_\sigma) = \mathbb{Q}(t_\sigma) = K_\kappa$, pour tout $\sigma \in G_\kappa$. Le polynome $P \in \mathbb{Z}[X]$ est donc irréductible et son groupe de Galois est cyclique d'ordre g_κ; toutes ses racines sont conjuguées de $\delta_1 t_1$ par exemple , donc $\delta_\sigma t_\sigma = (\delta_1 t_1)^{\varphi_\sigma}$ où $\varphi_\sigma \in G_\kappa$; ceci entraîne $t_\sigma^q = t_1^{q\varphi_\sigma}$ soit $\theta^\sigma = \theta^{\varphi_\sigma}$; comme θ est primitif , on a $\varphi_\sigma = \sigma$, d'où $\delta_\sigma t_\sigma = (\delta_1 t_1)^\sigma = \delta_1 t_1^\sigma$ et $t_1^\sigma = \delta_1 \delta_\sigma t_\sigma$.

Soit F un sous-G_κ-module de E_κ de même rang ; on rappelle que l'on a posé $r(F) = (|E_\kappa| : |F|)$; on note $H(F)$ la constante du théorème II 1 qui majore $r(F)$

$\left(r(F) \le H(F) = \frac{\mathfrak{M}_\kappa(F)}{m_\kappa} \left(\frac{1}{2 d_\Phi} \operatorname{Log} \frac{M_\Phi}{\mu_\Phi} \right)^{-\varphi(g_\kappa)} \right)$ relativement à une

fonction Φ pour laquelle les conditions d'application du théorème II 1 sont satisfaites .

Lemme IV 2 . Soit $|F|$ un sous-$\mathbb{Z}_\kappa$-module de $|E_\kappa|$ de rang 1 . Le quotient $|E_\kappa| / |F|$ est isomorphe à $\mathbb{Z}_\kappa / \mathfrak{A}_\kappa$ où $\mathfrak{A}_\kappa = \left\{ \omega \in \mathbb{Z}_\kappa , |E_\kappa|^\omega \subset |F| \right\}$. Le nombre $r(F) = (|E_\kappa| : |F|)$ est égal à la norme absolue de $\mathfrak{A}_\kappa$.

On sait que $|E_\kappa|$ est isomorphe à un idéal de $\mathbb{Z}_\kappa$ et qu'un idéal d'un anneau de Dedekind peut être engendré par deux éléments non nuls dont l'un est choisi arbitrairement ; soit $\eta \in F$, $|\eta| \neq 1$, il existe $\varepsilon_o \in E_\kappa$ telle que $|E_\kappa|$ soit engendré par $|\varepsilon_o|$ et $|\eta|$. On a alors , en désignant par q l'homomorphisme canonique $|E_\kappa| \to |E_\kappa| / |F_\kappa|$, la suite exacte : $1 \to \left\{ \omega \in \mathbb{Z}_\kappa , q(|\varepsilon_o|^\omega) = 1 \right\} \to \mathbb{Z}_\kappa \to |E_\kappa| / |F_\kappa| \to 1$

$\omega \to q(|\varepsilon_o|^\omega)$

et on vérifie que $\left\{ \omega \in \mathbb{Z}_\kappa , q(|\varepsilon_o|^\omega) = 1 \right\} = \mathfrak{A}_\kappa$. La deuxième assertion est évidente .

a) Cas où $\mathbb{Z}_\kappa$ est principal . Dans ce cas , on peut trouver une $\mathbb{Z}_\kappa$-base de F notée η ($\mathbb{Z}_\kappa$ n'est principal que dans un nombre fini de cas (29 cas) donnés récemment par Masley ([21]) .

Soit p un nombre premier , soit n_p son degré résiduel dans $Z_\varkappa$ et soit $\Gamma_\varkappa = \mathrm{Gal}(Q_\varkappa/Q)$; comme $Z_\varkappa$ est supposé principal , on peut trouver un entier $\omega \in Z_\varkappa$ de norme $\pm p^{n_p}$.

Proposition IV 1 . Les conditions suivantes sont équivalentes :

(i) p divise $r(F)$,

(ii) p^{n_p} divise $r(F)$,

(iii) il existe un élément $\omega \in Z_\varkappa$ de norme $\pm p^{n_p}$ et une unité $\varepsilon \in E_\varkappa$ tels que $\eta^\Omega = \varepsilon^{p^{n_p}}$ où $\Omega = \prod_{\substack{s \in \Gamma \\ s \neq 1^\varkappa}} \omega^s$.

démonstration

D'après le lemme IV 2 , (deuxième assertion) , on a (i) $\Leftrightarrow$ (ii) . Posons $q = p^{n_p}$ et supposons que q divise $r(F)$; soit ε_o une $Z_\varkappa$ - base de $E_\varkappa$, alors , d'après le lemme IV 2 (première assertion) et le fait que $Z_\varkappa$ soit supposé principal , il existe $\omega' \in Z_\varkappa$ tel que $\eta = \varepsilon_o^{\omega'}$ avec $N\omega' = \pm r(F)$; si q divise $r(F)$, l'idéal $\omega' Z_\varkappa$ sera divisible par un idéal premier au-dessus de p , (ω) , de norme q ; on a donc $\omega' = \omega\omega_1$, $\omega_1 \in Z_\varkappa$; il suffit alors de poser $\varepsilon = \varepsilon_o^{\omega_1}$, on aura $\eta^\Omega = \varepsilon_o^{\Omega\omega'} = \varepsilon_o^{\Omega\omega\omega_1} = \varepsilon^{p^{n_p}}$. La réciproque est alors triviale .

Lemme IV 3 . Soit $\eta \in E_\varkappa$. On suppose que $\eta = \varepsilon^q$, $q \in Z$, $q > 1$, $\varepsilon \in K_\varkappa^*$. Alors ε est un élément de $E_\varkappa$.

En effet , utilisons la propriété caractéristique des éléments de $E_\varkappa$ donnée dans I, 3 ; on a $N_{K_\varkappa/k} \varepsilon^q = N_{K_\varkappa/k} \eta = \pm 1$ pour tout sous-corps strict k de $K_\varkappa$; comme $K_\varkappa$ ne contient que ± 1 comme racines de l'unité , on aura $N_{K_\varkappa/k} \varepsilon = \pm 1$.

Les résultats ci-dessus conduisent à l'algorithme suivant (lorsque $Z_\varkappa$ est principal) :

Algorithme . On part de l'unité $\eta_1 = \eta_\varkappa$ qui engendre $F_1 = F_\varkappa$; pour les nombres premiers p_1 (considérés par ordre croissant) tels que $p_1^{n_{p_1}} \leq H(F_1)$ on teste la divisibilité de $r(F_1)$ par $p_1^{n_{p_1}}$ au moyen du lemme IV 1 et de la proposition IV 1 . Si le test est toujours négatif , alors $r(F_1) = h_\varkappa = 1$. Dans le cas contraire , on a trouvé p_1 minimum tel que $p_1^{n_{p_1}}$ divise $r(F_1)$. Soit η_2 l'unité (de $E_\varkappa$ nécessairement , en vertu du lemme IV 3) telle que $\eta_1^{\Omega_1} = \eta_2^{p_1^{n_{p_1}}}$ (notations de la proposition IV 1) et soit F_2 le $G_\varkappa$-module engendré par η_2 (on a $(|F_2| : |F_1|) = p_1^{n_{p_1}}$ et $(|E_\varkappa| : |F_2|) = r(F_2)$ est égal à $h_\varkappa / p_1^{n_{p_1}}$) . On est alors ramené intégralement à un problème identique à partir de F_2 au lieu de F_1 : on calcule $H(F_2)$ qui , en vertu de l'expression donnée par le théorème II 1 , est égal à $H(F_1) / p_1^{n_{p_1}}$ et on effectue les tests de divisibilités relatifs aux nombres premiers $p_2 \geq p_1$ tels que $p_2^{n_{p_2}} \leq H(F_2)$. Lorsque $H(F_n)$ devient inférieur strictement à $p_n^{n_{p_n}}$ pour la dernière valeur p_n considérée , on est sûr que $r(F_n) = 1$, autrement dit que $F_n = E_\varkappa$. On a ainsi un générateur de $E_\varkappa$ (c'est η_n) et la valeur de $h_\varkappa$: $h_\varkappa = \prod_{j=1}^{n} p_j^{n_{p_j}}$; l'idéal $\mathfrak{A}_\varkappa$ (lemme IV 2) de norme absolue $h_\varkappa$ est égal à l'idéal engendré par $\prod_{j=1}^{n} \omega_j$, où ω_j est l'entier de norme $p_j^{n_{p_j}}$ trouvé au $j^{\text{ème}}$ dévissage .

Remarque IV 1 . Dans l'algorithme précédent on est amené à choisir des entiers ω de norme p^{n_p} ; ce choix est donc effectué modulo le groupe des unités de $\mathbb{Z}_\varkappa$, ce qui fait que la suite des générateurs η_1 , η_2 , ... , η_n n'est pas unique . Dans la pratique on pourra choisir les η_i de telle façon que leurs conjugués soient le plus petit possible , par exemple .

b) Cas où $\mathbb{Z}_\varkappa$ n'est pas principal . L'algorithme dans ce cas est plus compliqué mais il est intéressant d'entreprendre le calcul de $h_\varkappa$ dans ce cas car c'est , semble-t-il , le seul moyen pour trouver des contre-exemples à l'existence d'une " unité de Minkowski " dans le cas des exten-

sions cycliques de degré premier de $\mathbb{Q}$ (ou plus généralement des contre-exemples au fait que les $Z_\varkappa$-modules $|E_\varkappa|$ sont $Z_\varkappa$-libres dans tous les exemples connus) (cf. [3], [24]) . Un algorithme peut être construit à partir du test de divisibilité suivant de $r(F)$: soit p un nombre premier tel que $p^{n_p} \leq H(F)$:

Proposition IV 2 . Les conditions suivantes sont équivalentes :

(i) p divise $r(F)$,

(ii) p^{n_p} divise $r(F)$,

(iii) il existe un idéal entier α de $Z_\varkappa$ premier à p , un idéal premier $\mathfrak{p}$ au-dessus de p dans $Z_\varkappa$ tels que $\alpha \prod_{\substack{s \in \Gamma \\ s \neq 1^\varkappa}} \mathfrak{p}^s$ soit principal ($= \Omega Z_\varkappa$) et il existe une unité $\varepsilon \in E_\varkappa$ tels que l'on ait $\eta^\Omega = \varepsilon^{p^{n_p}}$.

démonstration

Analogue à celle de la proposition IV 1 .

Il s'introduit alors dans le " dévissage " de l'indice $r(F_\varkappa)$ des facteurs parasites de la forme $N\alpha$ mais ils sont connus numériquement à chaque étape , ce qui permet le calcul effectif de $h_\varkappa$.

c) Calcul de h_K et de E_K . Revenons provisoirement au cas d'une extension $K/\mathbb{Q}$ abélienne réelle quelconque : la formule donnant le nombre de classes de K est $h_K = \dfrac{Q_K}{Q_G} \prod_{\varkappa \in \mathfrak{X}_K} h_\varkappa$ (cf. partie I, § 4) . Ayant déterminé le produit des $h_\varkappa$, il reste à trouver h_K , donc à calculer Q_K/Q_G . D'après Leopoldt ([15], § 5,4) , il existe un entier q^K (compris entre 0 et le nombre de $\varkappa \in \mathfrak{X}_K$, $\varkappa \neq 1$) tel que $Q_K = 2^{q^K} Q_K^*$; alors Q_K^* est un entier qui divise Q_G ; or les diviseurs premiers de Q_G sont à prendre parmi ceux de $g = [K:\mathbb{Q}]$, ce qui fait que pour tout p premier ne divisant pas g , la p-participation à h_K est égale à celle trouvée dans $\prod_{\varkappa \in \mathfrak{X}_K} h_\varkappa$.

On peut donc procéder de l'une des deux façons suivantes :

(i) On calcule $\prod_{\varkappa \in \mathfrak{X}_K} h_\varkappa$ et on en extrait le plus grand diviseur

premier à g . On calcule ensuite , pour chaque diviseur premier p divisant g et pour le nombre p = 2 , la p-participation de h_K par la méthode développée dans [6] . Le nombre h_K en résulte alors immédiatement. Il faut ensuite si l'on veut un système d'unités fondamentales de K , partir du groupe $|E^K| = \bigoplus_{\mathfrak{p} \in \mathfrak{X}_K} |E_{\mathfrak{p}}|$ dont on connait l'indice dans le groupe E_K.

(ii) On peut aussi , à partir de $|E^K| = \bigoplus_{\mathfrak{p} \in \mathfrak{X}_K} |E_{\mathfrak{p}}|$, déterminer E_K (ce qui nécessite un nombre fini d'essais car on connait une base de E^K et , au sujet de l'indice $(E_K : E^K)$, on connait les diviseurs possibles et un majorant de cet indice) . On utilise ensuite la relation $Q_K = (E_K : E^K)$. Bien entendu , dans certains cas , on sait à priori que $Q_K = Q_G$ (c'est le cas des extensions cycliques de degré premier impair, cf. [12], [15]) .

Par exemple , soit K le sous-corps de degré 9 de $\mathbb{Q}_o^{(63)}$; il est non cyclique et contient les quatre sous-corps cubiques suivants : $\mathbb{Q}_o^{(9)}$, $\mathbb{Q}_o^{(7)}$ et les deux corps cubiques de conducteur 63 . Ces deux derniers ont pour nombre de classes 3 ([9]) tandis que les deux premiers sont principaux ; donc ici $\prod_{\mathfrak{p} \in \mathfrak{X}_K} h_{\mathfrak{p}} = 9$ et $h_K = 9 \dfrac{Q_K}{Q_G}$ avec $Q_G = 3^5$. Si on applique la formule de Chevalley ([6], Th. 4.1) dans l'extension $K/\mathbb{Q}_o^{(9)}$ (dans laquelle , seul l'idéal premier au-dessus de 7 est ramifié) on trouve que le 3-groupe des classes de K est trivial , d'où $h_K = 1$, d'où $Q_K = 3^3$.

V Conjecture

1) Invariants associés à un module de torsion sur un anneau de Dedekind.

On sait ([20], p.6 et [1] Prop. 23) que tout module de torsion M sur un anneau de Dedekind A est isomorphe à $A/\mathfrak{A}_1 \times \ldots \times A/\mathfrak{A}_r$, $\mathfrak{A}_i$ idéal entier de A , $\mathfrak{A}_i \neq (0)$, $\mathfrak{A}_i$ divisant $\mathfrak{A}_{i-1}$ pour $2 \leq i \leq r$ et cette écriture est unique . Ceci permet de définir l'invariant $\chi_A(M) = \mathfrak{A}_1 \ldots \mathfrak{A}_r$, idéal entier de A , et les invariants suivants qui s'en déduisent : $\chi_{A,\ell}(M)$, le plus grand diviseur de $\chi_A(M)$ ne contenant que des idéaux premiers au-dessus de ℓ (ℓ premier)

$\left(\text{on a donc } \chi_A(M) = \prod_{\ell} \chi_{A,\ell}(M) \right)$.

2) Interprétation des h_κ . Soit K une extension abélienne réelle . Soit ℓ un nombre premier ne divisant pas $g = [K:\mathbb{Q}]$; soit $\mathfrak{H}_\ell(K)$ le ℓ-groupe des classes de K ; comme g est inversible modulo ℓ , il en résulte que $\mathfrak{H}_\ell(K)$ est un $\mathbb{Z}_{(\ell)}[G]$-module . Posons $\mathfrak{H}_{\ell,\kappa}(K) = \mathfrak{H}_\ell(K)^{e_\kappa}$ pour tout $\kappa \in \mathfrak{X}_K$ (les e_κ sont les idempotents de $\mathbb{Z}_{(\ell)}[G]$); on a donc $\mathfrak{H}_\ell(K) = \bigoplus_{\kappa \in \mathfrak{X}_K} \mathfrak{H}_{\ell,\kappa}(K)$ et pour chaque $\kappa \in \mathfrak{X}_K$, $\mathfrak{H}_{\ell,\kappa}(K)$ est un module de torsion sur $\mathbb{Z}_\kappa$.

D'un autre côté , soient $\mathfrak{e}_\kappa(K)$ les groupes $|E_\kappa| / |F_\kappa|$ et soient $\mathfrak{e}_{\ell,\kappa}(K)$ les ℓ-sous-groupes de Sylow des $\mathfrak{e}_\kappa(K)$. On peut aussi considérer $\mathfrak{e}_{\ell,\kappa}(K)$ comme un $\mathbb{Z}_\kappa$-module de torsion de la forme $\mathbb{Z}_\kappa/\mathfrak{A}_\kappa$.

On démontre facilement ([15], § 9, 4) que pour ℓ ne divisant pas g , $\|\mathfrak{e}_{\ell,\kappa}(K)\| = \|\mathfrak{H}_{\ell,\kappa}(K)\|$ (ce qui donne une interprétation des ℓ-participations des nombres h_κ) .

3) Structures de $\mathbb{Z}_\kappa$-modules cohérentes . On a vu que $\mathfrak{H}_{\ell,\kappa}(K)$ et $\mathfrak{e}_{\ell,\kappa}(K)$ sont des $\mathbb{Z}_{(\ell)}[G]e_\kappa$-modules , ce qui fait qu'on peut les considérer comme des $\mathbb{Z}_\kappa$-modules (cf. partie I, § 3, b) après le double choix d'un générateur σ_κ de G_κ et d'une racine primitive g_κ-ème de l'unité ζ_κ . Il y a donc , sur un $\mathbb{Z}_{(\ell)}[G]e_\kappa$- module , $\varphi(g_\kappa)$ lois de $\mathbb{Z}_\kappa$-modules

possibles qui se déduisent de la loi de $\mathbb{Z}_{(\ell)}[G]$-modules . On dira ici que les deux lois de $\mathbb{Z}_\pi$-modules considérées sur $\mathfrak{H}_{\ell,\pi}(K)$ et $\mathcal{E}_{\ell,\pi}(K)$ sont cohérentes si le choix (σ_π , ζ_π) est le même pour les deux modules (autrement dit, si l'on pose $h^{\zeta_\pi} = h^{\sigma_\pi}$ et $q(\varepsilon)^{\zeta_\pi} = q(\varepsilon^{\sigma_\pi})$ pour tout $h \in \mathfrak{H}_{\ell,\pi}(K)$ et tout $q(\varepsilon) \in \mathcal{E}_{\ell,\pi}(K)$) .

On peut se convaincre sur des exemples que $\mathcal{E}_{\ell,\pi}(K)$ et $\mathfrak{H}_{\ell,\pi}(K)$ ne sont pas isomorphes en général (malgré l'égalité de leurs ordres) . Cependant nous conjecturons que leurs structures de $\mathbb{Z}_\pi$-modules sont liées par le résultat suivant :

Conjecture . Pour tout nombre premier ℓ ne divisant pas g , pour tout $\pi \in \mathfrak{T}_K$, on a $\chi_{\mathbb{Z}_{\pi,\ell}}(\mathcal{E}_{\ell,\pi}(K)) = \chi_{\mathbb{Z}_{\pi,\ell}}(\mathfrak{H}_{\ell,\pi}(K))$ lorsque les deux structures de $\mathbb{Z}_\pi$-modules sont cohérentes .

Remarque V 1 . Cette conjecture a été vérifiée sur un assez grand nombre d'exemples numériques , pour $g = 3$ et $\ell \equiv 1 \bmod 3$ (le cas $\ell \equiv 2 \bmod 3$ étant sans intérêt car l'idéal (ℓ) est inerte dans $\mathbb{Z}^{(3)}$ et la fonction χ_ℓ est déterminée par l'ordre du $\mathbb{Z}^{(3)}$-module considéré) . Tous les corps cubiques testés , de nombre de classes divisible par ℓ , ont vérifié la conjecture (la plupart des $\ell < 100$ ont été rencontrés) . Un certain nombre de vérifications ont été faites en collaboration avec Smadja ; certains exemples ont été traités indépendamment par Smadja et nous-mêmes par des méthodes différentes et ont donné le même résultat .

L'énoncé de cette conjecture est sans doute trop général , compte-tenu des exemples traités . En tout cas aucune démonstration pour le cas le plus simple (à savoir $g = 3$, $\ell = 7$) n'existe , à notre connaissance . Le problème , reliant par un énoncé algébrique l'aspect " corps de classes " (opération de G sur le groupe des classes) à l'aspect "analytique " (unités cyclotomiques) , nous semble difficile . Cependant une récente étude que nous avons entreprise et qui est basée sur la comparaison des résultats du " Spiegelungssatz " de Leopoldt avec ceux fournis par les méthodes analytiques (via les nombres de Bernoulli généralisés) nous a amené à démontrer très partiellement la conjecture (classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés , par Georges GRAS, Sém. de théorie des Nombres de Besançon, Avril 1975).

Bibliographie

[1] BOURBAKI N. :
Algèbre commutative, Ch. VII , Paris (1965) .

[2] BOREVICH Z.I. - SHAFAREVICH I.R. :
Number Theory , Acad. Press, New-York-London (1966) .

[3] BRUMER A. :
On the group of units of an absolutely cyclic number field of prime degree, J. Math. Soc. of Japan, 21, 3, (1969) .

[4] CHATELET A. :
L'arithmétique des corps quadratiques,
Ens. Math., 9, Genève (1962) .

[5] FRESNEL J. :
Nombres de Bernoulli et fonctions L p-adiques,
Ann. Inst. Fourier, Grenoble, 17, 2, 281-333 (1967) .

[6] GRAS G. :
Sur les ℓ-classes d'idéaux dans les extensions cycliques relatives de degré premier ℓ (Thèse), Ann. Inst. Fourier , XXIII, 3, 1-48 et XXIII, 4, 1-43 (1973) .

[7] GRAS G. :
Signature des unités cyclotomiques et parité du nombre de classes des extensions abéliennes de $\mathbb{Q}$ de degré impair (à paraître) .

[8] GRAS G. - GRAS M.N. :
Signature des unités cyclotomiques et parité du nombre de classes des extensions cycliques de $\mathbb{Q}$ de degré premier impair (à paraître aux Ann. Inst. Fourier) .

[9] GRAS M.N. :
Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de $\mathbb{Q}$ (à paraître au J. de Crelle) .

[10] GRAS M.N. :
Nombre de classes et unités des corps cubiques cycliques .
Séminaire de théorie des Nombres de Besançon (1974).

[11] GRAS M.N. - MOSER N. - PAYAN J.J. :
Approximation algorithmique du groupe des classes de certains corps cubiques cycliques, Acta Arithmetica, XXIII , 295-300 (1973) .

[12] HASSE H. :
Über die Klassenzahl abelscher Zahlkörper, Akademie-Verlag, Berlin (1952) .

[13] LANG S. :
Algebra, Addison-Wesley Pub. C. (1967) .

[14] LANG S. :
Algebraic Number Theory, Addison-Wesley Pub. C. (1970).

[15] LEOPOLDT H.W. :
Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper, Abh. Deutsche Akad. Wiss. Berlin, Math., 2 (1954) .

[16] LEOPOLDT H.W. :
Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, J. reine angew. Math., 201, 119-149 (1959) .

[17] LEOPOLDT H.W. :
Eine Verallgemeinerung der Bernoullischen Zahlen , Abh. Hambourg, 22 , 131-140 (1957) .

[18] LEOPOLDT H.W. :
Zur Struktur der ℓ-Klassengruppe galoisscher Zahlkörper , J. für reine angew. Math., 199, 165-174 (1958) .

[19] LEOPOLDT H.W. :
Über Fermatquotienten von Kreiseinheiten und Klassenzahlformeln modulo p , Rend. Cric. Math. di Palermo II , IX , 1, 39-50 (1960) .

[20] MARTINET J. :
Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre 2p (chap. II) , Ann. Inst. Fourier, 19 , 1, 1-80 (1969) .

[21] MASLEY J. :
Solution of class Number one problem for cyclotomic fields (à paraître) .

[22] ORIAT B. :
Structure du groupe des classes des corps quadratiques réels et imaginaires $\mathbb{Q}(\sqrt{\pm d})$, $d < 10000$, Inst. Math. de Besançon (tables) (1974) .

[23] ORIAT B. :
Exposé sur " Über Einheintengruppe und Klassenzahl reeller abelscher Zahlkörper " de Leopoldt , Séminaire de théorie des Nombres de Besançon (1974) .

[24] PAYAN J.J. :
Modules sur certains anneaux de Dedekind , Séminaire de théorie des Nombres de Grenoble (1972) .

[25] SAMUEL P. :
Théorie algébrique des Nombres , Hermann, Paris (1967).

[26] SERRE J.P. :
Corps locaux, Hermann, Paris (1962) .

[27] SERRE J.P. :
Représentations linéaires des groupes finis, Hermann , Paris (1967) .

[28] SHANKS D. :
Class number , a theory of factorization , and genera. Proc. Sympos. Pure Math., Vol. XX, 415-440 . Amer. Math. Soc., Providence (1970) .

[29] SMADJA R. :
Sur le groupe des classes des corps de nombres , C.R.A.S., A , 276 , 1639-1641 (1973) .

[30] ZIMMER H.G. :
Computational Problems , Methods , and Results in Algebraic Number Theory , Lecture Notes in Math., 262 , Springer-Verlag (1972) .