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

$h_K = \dfrac{Q_K}{Q_G} \prod_{\chi} h_\chi$, où les nombres Q_K , Q_G , h_χ sont des entiers rationnels et χ 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 χ , le nombre h_χ est égal à l'indice dans un sous-groupe E_χ d'unités de K bien défini (mais que l'on ne connait pas numériquement) d'un sous-groupe d'unités F_χ 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 $h_\chi = (E_\chi : F_\chi)$.

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

il suffit alors de recommencer l'opération à partir de $F'_\varkappa$; on obtient ainsi une suite de groupes $F_\varkappa$, $F'_\varkappa$, ... , $F^{(n)}_\varkappa$ et on aura $F^{(n)}_\varkappa = E_\varkappa$ à partir du moment où il sera impossible de trouver $\eta \in F^{(n)}_\varkappa$ puissance non triviale d'une unité ε n'appartenant pas à $F^{(n)}_\varkappa$. 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 $F^{(i)}_\varkappa$, telle que $\eta = \varepsilon^p$, $\varepsilon \notin F^{(i)}_\varkappa$. 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_χ / F_χ .

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 : $\mathfrak{X}'_K = \{\chi' \in \mathfrak{X}'_{\mathbb{Q}^{(f)}} , \chi'(\bar{a}) = 1 , \text{ pour tout } \bar{a} \in H\}$. Les applications χ' 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 $\chi'(a)$, $\chi'(\sigma)$ ou $\chi'(\bar{\sigma})$ le nombre $\chi'(\bar{a})$. Pour tout élément χ' de $\mathfrak{X}'_K$, on notera $g_{\chi'}$ son ordre ; alors le groupe $\chi'(G)$ coïncide avec le groupe cyclique des racines $g_{\chi'}$-èmes de l'unité et son ordre , noté $\|\chi'(G)\|$, est égal à $g_{\chi'}$ (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 χ' et ψ' deux éléments de $\mathfrak{X}'_K$; on dit que χ' et ψ' sont $\Gamma_{\mathbb{Q}}$-conjugués (cf. [27] p. 41) si $\psi' = \chi'^k$, avec k entier premier à l'ordre de χ' . Il revient au même de dire que ψ' et χ' engendrent le même sous-groupe de $\mathfrak{X}'_K$; on vérifie que cette propriété est aussi équivalente à $\ker \chi' = \ker \psi'$.

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 K</u> (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 $K_{\chi'}$ 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 $K_{\chi'}$ est une extension <u>cyclique</u> de $\mathbb{Q}$; son degré est égal à $\|\chi'(G)\| = g_{\chi'}$; comme $\mathrm{Ker}\,\chi'$, $K_{\chi'}$ 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 $\Phi_\varkappa(\sigma_\varkappa)e_\varkappa = \left(\prod_{(k, g_\varkappa)=1} (\sigma_\varkappa - \zeta_\varkappa^k) \right) e_\varkappa$. 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 $\left(\sum_{\sigma \in G} \varkappa'(\sigma^{-1})_\sigma \right)(\sigma_\varkappa - \zeta_\varkappa^\lambda) = 0$ 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_χ est génératrice , tout $\tau \in G$ s'écrit de façon unique $\tau = \sigma_\chi^k \tau'$, k défini modulo g_χ et $\tau' \in \mathrm{Ker}\,\chi$; on a alors $\tau' e_\chi = e_\chi$ soit $\tau e_\chi = \sigma_\chi^k e_\chi$ image de X^k par l'homomorphisme considéré; d'où la surjectivité .

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

Pour simplifier les notations , nous noterons Q_χ le corps $Q^{(g_\chi)}$ et Z_χ l'anneau des entiers de Q_χ . Puisque $Z_\chi = Z[\zeta_\chi]$, Z_χ est isomorphe à $Z[G]e_\chi$ 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 χ-relatives . Soit χ un caractère de K . Soit K_χ le sous-corps cyclique de K correspondant à χ (cf. § 1, d) . On dit qu'une unité ε de K_χ est χ-relative (" eigentliche $\tilde{\chi}$- Relativeinheit " au sens de Leopoldt ([15],§4)) si $N_{K_\chi/k}(\varepsilon) = \pm 1$ pour tout sous-corps strict k de K_χ . On note E_χ (noté E_χ^+ dans Leopoldt) le sous-groupe des unités χ-relatives de K_χ (pour $\chi = 1$, on posera $E_1 = \{\pm 1\}$; on remarque que +1 et -1 sont χ-relatives quel que soit χ) .

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

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

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

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

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

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

Il faut remarquer que $|E_\chi|$ n'est pas $\mathbb{Z}_\chi$-libre en général ; en effet, $|E_\chi|$ est isomorphe à un idéal de $\mathbb{Z}_\chi$ et est libre sur $\mathbb{Z}_\chi$ si et seulement si cet idéal est principal ([1], Prop. 24) . On ne connait pas d'exemple où $|E_\chi|$ ne soit pas libre (la plus petite valeur de g_χ pour laquelle $\mathbb{Z}_\chi$ 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 $\chi \in \mathfrak{X}_K$, $\chi \neq 1$, le corps K_χ , de conducteur f_χ , est contenu dans $\mathbb{Q}^{(f_\chi)}$, et le groupe de Galois de $\mathbb{Q}^{(f_\chi)}/\mathbb{Q}$ est canoniquement isomorphe à $(\mathbb{Z}/f_\chi\mathbb{Z})^*$; soit H_χ le sous - groupe de $(\mathbb{Z}/f_\chi\mathbb{Z})^*$ image de $\mathrm{Gal}(\mathbb{Q}^{(f_\chi)}/K_\chi)$ par cet isomorphisme et soit a_χ un

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

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

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

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

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

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

Remarque I 1. Les $h_\varkappa$ ne sont pas nécessairement les nombres de classes des corps $K_\varkappa$;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 $E_\varkappa$, $F_\varkappa$ et $h_\varkappa$ ne dépendent que de l'extension cyclique $K_\varkappa/\mathbb{Q}$ 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 $\mathfrak{X}'$, $\mathfrak{X}$, $\mathfrak{X}'_\varkappa$ et $\mathfrak{X}_\varkappa$. Soit f un entier qui soit le conducteur d'une extension abélienne de $\mathbb{Q}$ et soit $\varkappa'$ un caractère complexe de $\mathbb{Q}^{(f)}$ de conducteur f . On appelle $\mathfrak{X}'$ l'ensemble des caractères $\varkappa'$ ainsi obtenus (il revient au même de dire que $\mathfrak{X}' = \bigcup_f \mathfrak{X}''_{\mathbb{Q}(f)}$ où $\mathfrak{X}''_{\mathbb{Q}(f)} = \{\varkappa' \in \mathfrak{X}'_{\mathbb{Q}(f)} , f_{\varkappa'} = f\}$) . 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 $K_\psi \subset K_\chi$:

soit $\hat{\psi}' \in \mathfrak{X}'_{K_\chi}$, c'est donc un caractère complexe de $\mathbb{Q}^{(f)}$ 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 $(h_\chi)_{\chi \in \tilde{\mathfrak{X}}^+}$ 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 $K_\varkappa$. Considérons, 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 symétrique 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 conséquent $S_\varkappa \cap V_\varkappa \subset D_\varkappa$.

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

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

En particulier on a $h_\nu \leq \frac{\mathfrak{m}_\nu(F_\nu)}{m_\nu} \left(\frac{1}{2 d_\Phi} \operatorname{Log} \frac{M_\Phi}{\mu_\Phi} \right)^{-\varphi(g_\nu)}$

sous les hypothèses précédentes .

démonstration

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

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

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

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

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

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 $\mathfrak{m}_\varkappa(F_\psi) = (g_\varkappa/g_\psi)^{\varphi(g_\psi)/2}\, \mathfrak{m}_\psi(F_\psi)$.

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 $V^\psi_\psi = V_\psi$, $(b_1, \ldots, b_{\varphi(g_\psi)})$, 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 $L_\mathfrak{p}(F_\psi)$ de $\mathbb{R}^{g_\mathfrak{p}}$, on peut prendre , comme base orthonormale du sous-espace $V_\psi^\mathfrak{p}$ engendré sur $\mathbb{R}$ par le réseau $L_\mathfrak{p}(F_\psi)$, la base $(B_i)_i = \left(\frac{1}{\sqrt{g_\mathfrak{p}/g_\psi}}(b_i, b_i, \dots, b_i)\right)_i \in \mathbb{R}^{g_\mathfrak{p}/g_\psi} \times \dots \times \mathbb{R}^{g_\mathfrak{p}/g_\psi}$,

$i = 1, \dots, \varpi(g_\psi)$, qui est encore orthonormale ; on a alors , de façon évidente , $\mathfrak{m}_\mathfrak{p}(F_\psi) = (\sqrt{g_\mathfrak{p}/g_\psi})^{\varpi(g_\psi)}\, \mathfrak{m}_\psi(F_\psi)$.

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

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

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 : $g_\mathfrak{p}\, Q_{G_\mathfrak{p}}\, \mathfrak{R}(F^{K_\mathfrak{p}}) = \prod_{\psi \in \mathfrak{X}_\mathfrak{p}^*} ((g_\mathfrak{p}/g_\psi)^{\varpi(g_\mathfrak{p})}\, R_\psi(F_\psi))$ où $\mathfrak{R}(F^{K_\mathfrak{p}})$ est le régulateur du réseau $L_\mathfrak{p}(F^{K_\mathfrak{p}})$ (définition habituelle , puisque $L_\mathfrak{p}(F^{K_\mathfrak{p}})$ engendre sur $\mathbb{R}$ le plan $\Pi_\mathfrak{p}$ de codimension 1 dans $\mathbb{R}^{g_\mathfrak{p}}$). On sait que la mesure $\mathfrak{m}_\mathfrak{p}(F^{K_\mathfrak{p}})$ du réseau $L_\mathfrak{p}(F^{K_\mathfrak{p}})$ est égale à $\sqrt{g_\mathfrak{p}}\, \mathfrak{R}(F^{K_\mathfrak{p}})$; on aura donc , en vertu de ce qui précède :

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

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

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

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

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 $m_\varkappa$. 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 $m_\varkappa = \gamma_\varkappa \int_{V_\varkappa} dx_1 \ldots dx_k \ldots dx_{g_\varkappa - 1}$, 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 $\mathfrak{m}_\varkappa(F_\varkappa)/m_\varkappa = \frac{1}{g_\varkappa^{g_\varkappa}} \frac{R_\varkappa(F_\varkappa)}{\int_{\mathfrak{m}_\varkappa} dx_1 \dots dx_k \dots dx_{g_\varkappa - 1}}$ 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, $\Delta(K_\varkappa)$ sera calculé au moyen de la "Führerdiskriminantenproduktformel" $\Delta(K_\varkappa) = \prod_{\psi' \in \mathfrak{X}'_\varkappa} f_{\psi}$, ([26], p. 112) .

b) Calcul de la constante $\mu_{\Delta_\varkappa}$. On rappelle que $\mu_{\Delta_\varkappa} = \operatorname{Sup}_{x \in C_\varkappa} (\Delta_\varkappa(x))$ (lemme II 2) ; soit $x^\circ = (x^\circ_\sigma)_{\sigma \in G_\varkappa}$ un point de $C_\varkappa$ où $\Delta_\varkappa$ 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 $x^\circ \in C_\varkappa$, il est clair que l'une de ses composantes vaut ± 1 ; comme $\Delta_\varkappa(x^\circ) = \Delta_\varkappa(-x^\circ)$, on peut supposer que c'est +1 qui est atteint . Soit $t \in G_\varkappa$ défini par $x^\circ_t = \operatorname{Min}_{\sigma \in G_\varkappa} (x^\circ_\sigma)$; on peut écrire $\Delta_\varkappa(x^\circ) =$

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

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 $\Delta_\varkappa(x^\circ)$ 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

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

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

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

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

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

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

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

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

$(u^2-1)T'' + 2uT' = u(u^2-1)\frac{P'''_n}{n} - \frac{n-2}{n}(u^2-1)P''_n + 2u^2\frac{P''_n}{n} - 2\frac{n-1}{n}uP'$;

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

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

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

$\left(\frac{n-2}{n}a_{n-2} - a_{n-2}\right)u^{n-2} = \frac{n-1}{2n-3}u^{n-2}$ 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 $\left(\frac{u^{n-1}}{2n-3}\right)$, on aura $\overline{T} = \frac{P_{n-1}}{2n-3}$, d'où $T = \frac{P'_{n-1}}{2n-3}$.

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

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

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

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

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

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

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 .