

Séminaire de Théorie des Nombres .

- Besançon -

Année 1974-1975

SUR L'ARTICLE DE H. W. LEOPOLDT INTITULÉ

|| Über Einheitengruppe und Klassenzahl
|| reeller abelscher Zahlkörper [2] .

Bernard ORIAT
Faculté des Sciences. Mathématiques .
25030 BESANCON CEDEX

SUR L'ARTICLE DE H.W. LEOPOLDT INTITULE

|| Uber Einheitengruppe und Klassenzahl
|| reeller abelscher Zahlkörper [2] .

par Bernard ORIAT

Introduction

Le présent article n'a aucune prétention à quelque originalité que ce soit . Nous nous proposons d'énoncer et de démontrer les résultats de [2] qui nous ont paru les plus importants . Les autres seront cités sans démonstration ou plus simplement omis .

Nous supposerons connus les paragraphes I, III et IV de [3] . Nous conserverons d'ailleurs les notations de cet exposé et ne ferons à ce sujet aucun rappel .

Fixons quelques notations . Dans la suite , sauf mention contraire , K/\mathbb{Q} sera une extension abélienne finie réelle , G sera son groupe de Galois et \mathfrak{X} son groupe de caractères . On désignera par \mathfrak{X}' l'ensemble des caractères de G irréductibles sur \mathbb{Q} . On notera E_K le groupe des unités de K , R_K le régulateur de K , h_K le nombre de classes d'idéaux de K .

Si M est un $\mathbb{Q}[G]$ -module (noté multiplicativement) , il se décompose en produit direct $M = \prod_{\kappa' \in \mathfrak{X}'} M^{e_{\kappa'}}$, où $e_{\kappa'}$ est l'idempotent de $\mathbb{Q}[G]$ associé à κ' . Le fil conducteur de l'article que nous nous proposons d'étudier est le suivant :

Essayer d'obtenir des décompositions du même type (c'est-à-dire sous forme de produits de quantités indicées par les éléments de \mathfrak{X}') pour les paramètres suivants : le régulateur de K et le nombre de classes d'idéaux de K .

Soit κ un caractère de K . Dans les paragraphes I et II, on introduira les groupes E_κ et E_κ^+ . Il s'agit de groupes d'unités abéliennes réelles ne dépendant que du caractère rationnel κ' . (Nous noterons indifféremment E_κ ou $E_{\kappa'}$, E_κ^+ ou $E_{\kappa'}^+$.) Les éléments de E_κ seront appelés des κ -unités. En général ce ne sont pas des unités de K . Quant à E_κ^+ , il est défini comme l'intersection de E_κ avec le sous-corps K_κ de K . La proposition Ib donnera une majoration de $[E_\kappa : E_\kappa^+]$ et la proposition IIb montrera que $|E_\kappa|$ et $|E_\kappa^+|$ (groupes des valeurs absolues de E_κ et E_κ^+) sont des $\mathbb{Z}[G]$ -modules isomorphes, simples de caractère κ' .

On introduira également deux sous-groupes de E_K : E^K et E^{K+} . Le premier est tel que $|E^K|$ soit le noyau de $|E_K|$, c'est-à-dire le plus grand sous-module complet de $|E_K|$. (Les notions de modules simples et complets ont été introduites dans [3] § III). L'autre vérifie $E^{K+} \subset E^K$ et $|E^{K+}|$ est aussi complet. On a les décompositions en produit direct :

$$|E^{K+}| = \prod_{\kappa' \in \mathfrak{X}'} |E^{K+}|_{e_{\kappa'}}, \quad \text{avec } |E^{K+}|_{e_{\kappa'}} = |E_{\kappa'}^+|;$$

$$|E^K| = \prod_{\kappa' \in \mathfrak{X}'} |E^K|_{e_{\kappa'}}, \quad \text{avec } |E^K|_{e_{\kappa'}} = |E_{\kappa'} \cap K|.$$

Le groupe E^{K+} et les groupes $E_{\kappa'}^+$ seront plus utilisés que E^K et $E_{\kappa'}$. Les groupes de κ -unités E_κ n'interviennent d'ailleurs que par l'intermédiaire de E^K . Ils ne servent qu'à obtenir les majorations de $Q_K^+ = [E_K : E^{K+}]$ données par les propositions IIc, IId et IIe.

Le paragraphe III traite des régulateurs. Soit H un sous-groupe de E_K , complet en tant que $\mathbb{Z}[G]$ -module. On introduit des quantités $R_{\kappa'}^K(H)$, appelées κ' -régulateurs de H dans K . Le résultat essentiel de ce paragraphe est la proposition IIIf qui montre que le régulateur de H est le produit de $\prod_{\kappa' \in \mathfrak{X}'} R_{\kappa'}^K(H)$ par un coefficient ne dépendant que du groupe de Galois G .

Dans le paragraphe IV, on s'intéresse à la décomposition de h_K . On introduit des quantités $h_{\kappa'}$, qu'on appelle κ' -nombres de classes et qui ne dépendent que du caractère κ' . La proposition IVc montre que

le nombre de classes de K , h_K , est le produit de $\prod_{\chi \in \mathfrak{X}} h_\chi$, par deux coefficients : l'un ne dépend que du groupe de Galois G et l'autre est égal à $Q_K^+ = [E_K : E^+]$. La démonstration de ce résultat utilise la décomposition de R_K obtenue dans le paragraphe précédent et la formule analytique donnant le nombre de classes (réelles) de K . On est conduit à définir des « unités cyclotomiques » de K et on obtient, à la proposition IV b une formule qui montre que l'indice du groupe des unités cyclotomiques de K dans le groupe des unités de K est le produit de h_K par un coefficient ne dépendant que du groupe de Galois G . Ce résultat est à rapprocher de ceux obtenus par Hasse et contenus dans [1], mais n'en est pas, semble-t-il, conséquence ; non plus qu'inversement. Les unités cyclotomiques de Leopoldt ne sont d'ailleurs pas les mêmes que celles de Hasse.

I

Première définition des κ - unités .

1) Préliminaires . Soient κ un caractère résiduel et K_κ/\mathbb{Q} l'extension cyclique correspondante ([3] § IV) . Soit \mathfrak{X} le groupe des caractères engendré par κ , c'est-à-dire le groupe des caractères de K_κ . Soit a un élément de K_κ non carré dans K_κ . Considérons l'extension quadratique $K_\kappa(\sqrt{a})/K_\kappa$.

Lemme I a . Supposons que κ soit pair et $K_\kappa(\sqrt{a})/\mathbb{Q}$ réelle et abélienne. Supposons que l'idéal de K_κ engendré par a soit le carré d'un idéal de K_κ . Alors le corps $K_\kappa(\sqrt{a})$ est composé de K_κ et d'un corps quadratique réel ; en d'autres termes, il existe un caractère quadratique ψ de conducteur f_ψ tel que $K_\kappa(\sqrt{a}) = K_\kappa(\sqrt{f_\psi})$.

démonstration

Montrons tout d'abord que l'extension $K_\kappa(\sqrt{a})/\mathbb{Q}$ n'est pas cyclique . En effet, si il en était ainsi, désignons par τ un générateur de son groupe de Galois et par 2^n son degré . Nous aurions alors

$$(\sqrt{a})^{\tau^n} = -\sqrt{a} \text{ d'où :}$$

$$((\sqrt{a})^{1+\tau+\dots+\tau^{n-1}})^\tau = -\sqrt{a}^{1+\tau+\dots+\tau^{n-1}} \text{ et } N_{K_\kappa/\mathbb{Q}}(a) \text{ n'appartien -}$$

drat pas à \mathbb{Q}^2 . Or cette quantité doit engendrer le carré d'un idéal de \mathbb{Z} et elle doit être positive puisque $K_\kappa(\sqrt{a})$ est réel.

L'extension $K_\kappa(\sqrt{a})/\mathbb{Q}$ doit donc être composée de K_κ et d'un corps quadratique réel. Désignons par ψ son caractère. Comme le conducteur d'un corps quadratique réel coïncide avec son discriminant, nous aurons donc $K_\kappa(\sqrt{a}) = K_\kappa(\sqrt{f_\psi})$.

Définition. Toute extension $K_\kappa(\sqrt{a})/K_\kappa$ vérifiant les hypothèses du lemme précédent sera appelée une ψ -extension.

Lemme 1b. Soient $K_\kappa(\sqrt{f_\psi})/K_\kappa$ une ψ -extension et L le plus grand sous-corps de K_κ tel que $[L:\mathbb{Q}]$ soit une puissance de 2.

Les deux conditions suivantes sont équivalentes :

- Il existe une unité α de K_κ telle que $K_\kappa(\sqrt{f_\psi}) = K_\kappa(\sqrt{\alpha})$.
- Il existe une unité η de L telle que $L(\sqrt{f_\psi}) = L(\sqrt{\eta})$.

démonstration

Posons $[K_\kappa:\mathbb{Q}] = 2^n u$, avec u impair. Si la première condition est vérifiée, on aura $f_\psi = b^2 \epsilon$, avec b dans K_κ . D'où :
 $f_\psi^u = N_{K_\kappa/L}(b)^2 N_{K_\kappa/L}(\epsilon)$ et $L(\sqrt{f_\psi}) = L(\sqrt{N_{K_\kappa/L}(\epsilon)})$.

La réciproque est évidente.

Nous utiliserons également le résultat suivant concernant les déterminants de groupes :

Lemme 1c. Soit G un groupe abélien fini. Soit (u_σ) une suite d'indéterminées sur \mathbb{Q} indexée par G . Posons $u = \sum_{\sigma \in G} u_\sigma \sigma$; c'est un élément

de l'algèbre $\mathbb{Q}(u_\sigma)[G]$. Soit \mathfrak{X}' l'ensemble des caractères de G irréductibles sur \mathbb{Q} . Soit \hat{u} l'application de $\mathbb{Q}(u_\sigma)[G]$ dans lui-même, définie par $\hat{u}(z) = uz$ et soit $\hat{u}_{\kappa'}$, sa restriction à l'idéal $\mathbb{Q}(u_\sigma)[G]_{e_{\kappa'}}$. Les déterminants de \hat{u} et $\hat{u}_{\kappa'}$, sont donnés par :

$$\text{Det } \hat{u}_{\kappa'} = \prod_{\psi \in \kappa'} \sum_{\sigma \in G} \psi(\sigma) u_\sigma .$$

$$\text{Det } \hat{u} = \prod_{\kappa' \in \mathfrak{X}'} \text{Det } \hat{u}_{\kappa'} .$$

démonstration

Nous avons $\mathbb{Q}(u_\sigma)[G] = \bigoplus_{\kappa' \in \mathfrak{X}'} \mathbb{Q}(u_\sigma)[G] e_{\kappa'}$. Le déterminant de $\overset{\circ}{u}$ est donc le produit des déterminants des restrictions $\overset{\circ}{u}_{\kappa'}$, de $\overset{\circ}{u}$ à chacun des idéaux $\mathbb{Q}(u_\sigma)[G] e_{\kappa'}$. Etendons $\overset{\circ}{u}_{\kappa'}$ à $\mathbb{C}(u_\sigma)[G] e_{\kappa'}$ = $\bigoplus_{\psi \in \kappa'} \mathbb{C}(u_\sigma)[G] e_\psi$. L'ensemble $\{e_\psi\}_{\psi \in \kappa'}$ est une base de ce \mathbb{C} -espace vectoriel et comme $\sigma e_\psi = \psi(\sigma) e_\psi$, nous aurons $\overset{\circ}{u}_{\kappa'}(e_\psi) = u e_\psi = \left(\sum_{\sigma \in G} u_\sigma \psi(\sigma) \right) e_\psi$. D'où l'égalité :

$$\text{Det } \overset{\circ}{u}_{\kappa'} = \prod_{\psi \in \kappa'} \left(\sum_{\sigma \in G} \psi(\sigma) u_\sigma \right).$$

2) Définition des κ -unités. On dira que ε est une unité réelle et abélienne si ε est une unité contenue dans une extension réelle et abélienne de \mathbb{Q} . Soit κ un caractère résiduel pair et K_κ le corps cyclique (réel) correspondant. On dira que ε est une κ -unité si ε vérifie les 3 conditions :

- a : ε est une unité réelle et abélienne.
- b : ε^2 appartient à K_κ .
- c : $N_{K_\kappa/L}(\varepsilon^2) = 1$ pour tout sous-corps strict L de K_κ .

Une κ -unité sera dite propre si elle appartient à K_κ et impropre dans le cas contraire. On désignera par E_κ (resp. E_κ^+) le groupe des κ -unités (resp. κ -unités propres).

Remarque. Les groupes d'unités définis ci-dessus ne dépendent en fait, que du caractère rationnel κ' . Nous emploierons indifféremment l'une ou l'autre des notations E_κ ou $E_{\kappa'}$, E_κ^+ ou $E_{\kappa'}^+$.

On prendra la même liberté avec d'autres quantités indexées par \mathfrak{X}' .

L'application $\varepsilon \rightarrow \varepsilon^2$ est une application de E_κ dans E_κ^+ et cela prouve que l'indice $[E_\kappa^+ : E_\kappa]$, s'il est fini, est une puissance de 2.

Définissons q_κ en posant $[E_\kappa^+ : E_\kappa] = 2^{q_\kappa}$. L'objet du paragraphe suivant est de montrer que q_κ vaut 0 ou 1.

3) Majoration de q_κ .

Proposition Ia . Soit κ un caractère pair , dont l'ordre g_κ est divisible par un nombre premier impair . On a alors $q_\kappa = 0$. C'est-à-dire qu'il n'existe pas de κ -unité impropre .

démonstration

Soit ε une κ -unité . L'extension $K_\kappa(\varepsilon)/K_\kappa$ est une ψ -extension . Reprenons les notations du lemme Ib . Il existe une unité η de L telle que $\varepsilon^2 = b^2 \eta$.

Comme L est différent de K_κ nous avons :

$$1 = N_{K_\kappa/L}(\varepsilon^2) = N_{K_\kappa/L}(b^2) \eta^u \quad \text{et} \quad K_\kappa(\varepsilon) = K_\kappa(\sqrt{\eta}) = K_\kappa .$$

Cela prouve que ε appartient à K_κ .

Lemme Id . Soit κ un caractère pair dont l'ordre g_κ est une puissance de 2 , c'est-à-dire $g_\kappa = 2^n$. Soit σ un générateur de $\text{Gal}(K_\kappa/\mathbb{Q})$. Si une unité α de K_κ vérifie les quatre conditions :

a' : α est totalement positive .

b' : $\alpha^{1+\sigma^{2^{n-1}}}$ = 1 .

c' : $\alpha^{1-\sigma}$ appartient à K_κ^2 .

d' : α n'appartient pas à K_κ ,

alors $\sqrt{\alpha}$ est une κ -unité impropre . Réciproquement si η est une κ -unité impropre , alors $\alpha = \eta^2$ vérifie les quatre conditions ci-dessus .

démonstration

Soit α remplissant les conditions ci-dessus .

On déduit de a' et d' que $K_\kappa(\sqrt{\alpha})/K_\kappa$ est réelle de degré 2 .

On déduit de c' que $K_\kappa(\sqrt{\varepsilon})/\mathbb{Q}$ est galoisienne . Soit G son groupe de Galois . Il possède un sous-groupe H d'ordre 2 distingué . Ce sous-groupe H est donc inclus dans le centre de G et comme G/H est cyclique, on en déduit que G est abélien . Enfin , la condition c se déduit de la condition b' . La réciproque n'est pas plus difficile .

Proposition 1b . Pour tout caractère κ pair , la quantité \downarrow_{κ} vaut 0 ou 1 .

démonstration

Compte-tenu de la proposition précédente , nous allons sup - poser que l'ordre g_{κ} de κ est égal à 2^n . Considérons $|E_{\kappa}^+|$, ensemble des valeurs absolues des éléments de E_{κ}^+ (ou si l'on préfère : $|E_{\kappa}^+| = E_{\kappa}^+ / \{\pm 1\}$) . Soit G_{κ} le groupe de Galois de K_{κ}/\mathbb{Q} et σ un gé - nérateur . Nous avons donc , pour tout ϵ de E_{κ}^+ , $\epsilon^{1+\sigma^{2^{n-1}}} = 1$.

Le groupe $|E_{\kappa}^+|$ est un $\mathbb{Z}[G]$ - module , libre de type fini en tant que \mathbb{Z} - module . Etendons l'anneau des scalaires $\mathbb{Z}[G]$ à $\mathbb{Q}[G]$. Nous obtenons alors $|E_{\kappa}^+|^{\mathbb{Q}} = \mathcal{E}_{\kappa}^+$. Si ψ' est un caractère rationnel de G_{κ} dif - férent de κ' , nous aurons $\sigma^{2^{n-1}} e_{\psi} = e_{\psi}$, d'où $\sigma^{2^{n-1}} e_{\psi'} = e_{\psi'}$, et $e_{\psi'} = \frac{1}{2} (1 + \sigma^{2^{n-1}}) e_{\psi'}$. D'où $|\epsilon|^{e_{\psi'}} = 1$ pour toute κ - unité ϵ . Ceci montre que les composantes simples de \mathcal{E}_{κ}^+ ont toutes pour caractère κ' . D'autre part , considérons le groupe des unités de K_{κ} noté $E_{K_{\kappa}}$.

Nous savons que $\mathcal{E}_{K_{\kappa}} = |E_{K_{\kappa}}|^{\mathbb{Q}}$ a pour caractère la somme des carac - tères rationnels de G_{κ} différents de 1 ([3] Proposition III a) . On en déduit que $|E_{\kappa}|$ est un $\mathbb{Z}[G_{\kappa}]$ - module simple de caractère κ' . (Ce ré - sultat est d'ailleurs toujours vrai , quel que soit la valeur de g_{κ} . Ceci sera démontré dans le paragraphe suivant) .

Introduisons maintenant l'ensemble :

$E_{\kappa}^{++} = \{ \epsilon , \epsilon \in E_{\kappa}^+ ; \epsilon^{1-\sigma} \in K_{\kappa}^2 \}$. Nous avons les inclusions : $E_{\kappa}^+ \supset E_{\kappa}^{++} \supset E_{\kappa}^{+2} \supset E_{\kappa}^{++(1-\sigma)}$ et $|E_{\kappa}^{++}|$ est un $\mathbb{Z}[G_{\kappa}]$ - module simple de caractère κ' . Considérons l'application de $|E_{\kappa}^{++}|$ dans $|E_{\kappa}^{++}|$ qui asso - cie $|\epsilon|^{1-\sigma}$ à $|\epsilon|$. En appliquant le lemme 1c avec $G = G_{\kappa}$ et $u = 1 - \sigma$, nous constatons que :

$$[|E_{\kappa}^{++}| : |E_{\kappa}^{++}|^{1-\sigma}] = \det \overset{\circ}{u}_{\kappa} = N_{\mathbb{Q}(g_{\kappa})/\mathbb{Q}}(1 - \kappa(\sigma)) = 2 .$$

Nous en déduisons que $[E_{\kappa}^{++} : E_{\kappa}^{+2}] = 1$ ou 2 . Enfin, considérons l'ap - plication de E_{κ} dans E_{κ}^{++} qui associe ϵ^2 à ϵ . Elle induit un isomorphisme de E/E_{κ}^+ dans $E_{\kappa}^{++}/E_{\kappa}^{+2}$. En effet , si η

appartient à E_{κ}^{++} , η vérifie les conditions a', b', c' et appartient à K_{κ} .
Donc η ne vérifie pas d'.

Remarque Ia. On trouvera dans [2] le résultat suivant, qui donne aussi une majoration de q_{κ} : Si κ est un caractère pair de conducteur une puissance d'un nombre premier, alors $q_{\kappa} = 0$.

4) Existence de κ -unités impropres.

Proposition Ic. Soit κ un caractère quadratique pair. Si l'extension correspondante $\mathbb{Q}(\sqrt{f_{\kappa}})/\mathbb{Q}$ possède une unité fondamentale de norme 1, alors il existe une κ -unité impropre. C'est-à-dire $q_{\kappa} = 1$.

En effet, l'unité fondamentale de $\mathbb{Q}(\sqrt{f_{\kappa}})$ vérifie les conditions du lemme Id.

Remarque Ib. Leopoldt montre dans [2] un résultat plus fort. Pour tout n , il existe une infinité de caractères κ d'ordre 2^n tels que $q_{\kappa} = 1$.

Remarque Ic. Soit ϵ une κ -unité impropre. L'extension $K_{\kappa}(\epsilon)/K_{\kappa}$ peut être ramifiée ou non ramifiée.

II

Deuxième définition des κ -unités. Propriétés de structure.

1) Définition du symbole $|\epsilon|_{\kappa}$. Soit K/\mathbb{Q} une extension abélienne finie réelle, G son groupe de Galois, g son degré, E_K le groupe des unités de K . On désigne par $|E_K|$ le groupe des valeurs absolues des éléments de E_K . Il s'agit d'un $\mathbb{Z}[G]$ -module, le groupe G opérant par $|\alpha|^{\sigma} = |\alpha^{\sigma}|$. On désignera par \mathcal{E}_K le $\mathbb{Q}[G]$ -module déduit de $|E_K|$ par extension de l'anneau des scalaires à \mathbb{Q} . (Ce que l'on avait noté dans [3] § III : $|E_K|^{\mathbb{Q}}$).

Si L est un sous-corps de K , alors \mathcal{E}_L peut être considéré comme une partie de \mathcal{E}_K . Il s'agit alors d'un sous- $\mathbb{Q}[G]$ -module de \mathcal{E}_K et c'est l'ensemble des éléments de \mathcal{E}_K invariants par $\text{Gal}(K/L)$.

Soit κ un caractère de K , c'est-à-dire un caractère complexe de G . Soit e_{κ} , l'idempotent de $\mathbb{Q}[G]$ correspondant au caractère rationnel κ' de G . On a donc $e_{\kappa} = \frac{1}{g} \sum_{\sigma \in G} \kappa'(\sigma^{-1})\sigma$. Si α est un élément de

\mathcal{E}_K , $\alpha^{e_{\kappa}}$ est aussi un élément de \mathcal{E}_K . Soit K_1/\mathbb{Q} une extension abélienne réelle telle que K_1 contienne K . Introduisons comme précédemment $G_1, g_1, \mathcal{E}_{K_1}$. L'élément α appartient aussi à \mathcal{E}_{K_1} . Soit $\Pi : G_1 \rightarrow G$

l'homomorphisme de restriction. Il s'étend en un homomorphisme de $\mathbb{Q}[G_1]$ sur $\mathbb{Q}[G]$ au moyen duquel \mathcal{E}_K devient un $\mathbb{Q}[G_1]$ -module. Le caractère κ' peut aussi être considéré comme un caractère rationnel de G_1 (en le confondant avec $\kappa' \circ \Pi$). Il lui correspond alors un idempotent $e_{\kappa'}^1 = \frac{1}{g_1} \sum_{\sigma \in G_1} \kappa'(\sigma^{-1})\sigma$. Nous avons : $\Pi(e_{\kappa'}^1) = e_{\kappa}$, et $\alpha^{e_{\kappa'}} = \alpha^{e_{\kappa}^1}$.

Nous avons donc montré, que bien qu'il existe une ambiguïté dans la notation e_{κ} , qui ne fait pas apparaître le groupe G sur lequel a lieu la « décomposition » $e_{\kappa} = \frac{1}{g} \sum_{\sigma \in G} \kappa'(\sigma^{-1})\sigma$, par contre il n'y en a plus

pour $\alpha^{e_{\kappa}}$ qui ne dépend plus que de κ' . Nous poserons $\alpha_{\kappa} = \alpha^{e_{\kappa}}$ et nous appellerons cette quantité : κ' -composante de α .

Soit ε une unité abélienne réelle et soit κ un caractère résiduel pair. Il existe une extension abélienne réelle K/\mathbb{Q} telle que κ soit un caractère de K et telle que ε appartienne à K . La quantité $|\varepsilon|_{\kappa}$, que l'on appellera κ' -composante de ε , ne dépend donc pas du choix de K . Ce n'est pas, en général, une unité réelle abélienne. Comme elle est invariante par $\text{Gal}(K/K_{\kappa})$ c'est un élément de $\mathcal{E}_{K_{\kappa}}$.

2) Deuxième définition des κ' -unités. Soit κ un caractère résiduel pair et ε une unité réelle et abélienne.

Proposition II a. L'unité ε est une κ' -unité si et seulement si

$$|\varepsilon|_{\kappa} = |\varepsilon|.$$

démonstration

Soit donc K/\mathbb{Q} une extension abélienne réelle telle que κ soit un caractère de K et ε une unité de K . Soit G son groupe de Galois, g son degré. Soit g_κ l'ordre de κ . Nous désignerons par σ un élément de G tel que $\kappa(\sigma)$ engendre $\kappa(G)$. Soit enfin $e_{\kappa'}$ l'idempotent
$$e_{\kappa'} = \frac{1}{g} \sum_{\tau \in G} \kappa'(\tau^{-1}) \tau.$$
 Nous allons commencer par mettre $e_{\kappa'}$ sous

une autre forme. Si $\tau\tau'^{-1}$ appartient à $\text{Ker } \kappa$, nous avons $\kappa(\tau) = \kappa(\tau')$ et $\kappa'(\tau) = \kappa'(\tau')$. D'où :

$$e_{\kappa'} = \frac{1}{g} \left(\sum_{\tau \in \text{Ker } \kappa} \tau \right) \left(\sum_{0 < k \leq g_\kappa} \kappa'(\sigma^{-k}) \sigma^k \right).$$

Si $(k', g_\kappa) = k$, on a $\kappa'(\sigma^{-k'}) = \kappa'(\sigma^{-k})$, d'où :

$$e_{\kappa'} = \frac{1}{g} \left(\sum_{\tau \in \text{Ker } \kappa} \tau \right) \left(\sum_{k|g_\kappa} \kappa'(\sigma^{-k}) \sum_{\substack{(k', g_\kappa) = k \\ 0 < k' \leq g_\kappa}} \sigma^{k'} \right).$$

Posons pour tout k divisant g_κ :

$$A(\sigma^k) = \sum_{\substack{(k', g_\kappa) = k \\ 0 < k' \leq g_\kappa}} \sigma^{k'} \quad \text{et} \quad B(\sigma^k) = \sum_{\substack{k|u \\ 0 < u \leq g_\kappa}} \sigma^u.$$

On vérifie élémentairement que $B(\sigma^k) = \sum_{k|d|g_\kappa} A(\sigma^d)$.

En inversant à l'aide de la fonction de Möbius, on obtient :

$$A(\sigma^k) = \sum_{k|d|g_\kappa} \mu\left(\frac{d}{k}\right) B(\sigma^d).$$

$$\text{D'où } e_{\kappa'} = \frac{1}{g} \left(\sum_{\tau \in \text{Ker } \kappa} \tau \right) \left(\sum_{k|g_\kappa} \kappa'(\sigma^{-k}) \sum_{k|d|g_\kappa} \mu\left(\frac{d}{k}\right) B(\sigma^d) \right)$$

$$= \frac{1}{g} \left(\sum_{\tau \in \text{Ker } \kappa} \tau \right) \left(\sum_{d|g_\kappa} \left(\sum_{k|d} \kappa'(\sigma^{-k}) \mu\left(\frac{d}{k}\right) \right) B(\sigma^d) \right).$$

En posant $C(d) = \frac{1}{g_\kappa} \sum_{k|d} \kappa'(\sigma^{-k}) \mu\left(\frac{d}{k}\right)$, nous obtenons :

$$e_{\kappa'} = \frac{g_\kappa}{g} \left(\sum_{\tau \in \text{Ker } \kappa} \tau \right) \left(\sum_{d|g_\kappa} C(d) B(\sigma^d) \right).$$

Montrons maintenant que $C(g_\kappa) = 1$. Soit ζ une racine primitive g_κ -ème de 1. Nous avons :

$$\begin{aligned} \sum_{k \in \mathbb{Z}/g_\kappa} (\sigma^{-k}) \mu\left(\frac{g_\kappa}{k}\right) &= \sum_{k \mid g_\kappa} \text{Tr}_{\mathbb{Q}(g_\kappa)/\mathbb{Q}} (\zeta^k) \mu\left(\frac{g_\kappa}{k}\right) \\ &= \sum_{d \mid g_\kappa} \frac{\varphi(g_\kappa)}{\varphi(d)} \text{Tr}_{\mathbb{Q}(d)/\mathbb{Q}} (\zeta^{g_\kappa/d}) \mu(d) \\ &= \sum_{d \mid g_\kappa} \varphi(g_\kappa)/\varphi(d) = g_\kappa \end{aligned}$$

car $\text{Tr}_{\mathbb{Q}(d)/\mathbb{Q}} (\zeta^{g_\kappa/d}) = \mu(d)$ et $\mu(d)^2 = 1$.

Supposons que ϵ soit une κ -unité. D'après la condition b, ϵ^2 doit appartenir à K_κ . On aura donc : $\epsilon^{2\tau} = \epsilon^2$ pour tout τ appartenant à $\text{Ker } \kappa$, d'où :

$$\epsilon^{2 \sum_{\tau \in \text{Ker } \kappa} \tau} = \epsilon^{2(g/g_\kappa)}$$

On en déduit les égalités :

$$\begin{aligned} \epsilon^{2e_\kappa} &= \epsilon^{2(g_\kappa/g) \left(\sum_{\tau \in \text{Ker } \kappa} \tau \right) \sum_{d \mid g_\kappa} C(d) B(\sigma^d)} \\ &= \epsilon^{2 \sum_{d \mid g_\kappa} C(d) B(\sigma^d)} = \prod_{d \mid g_\kappa} (\epsilon^{2B(\sigma^d)})^{C(d)}. \end{aligned}$$

Or $\epsilon^{2B(\sigma^d)} = N_{K_\kappa/L_d}(\epsilon^2)$; en désignant par L_d le sous-corps de K_κ

de degré d sur \mathbb{Q} . Cette quantité est égale à 1 pour tout d différent de g_κ , en vertu de la condition c.

Il reste donc $\epsilon^{2e_\kappa} = \epsilon^{2C(g_\kappa)} = \epsilon^2$ d'où $|\epsilon|^{e_\kappa} = |\epsilon|$.

Réciproquement, supposons que $|\epsilon|_{\kappa'} = |\epsilon|$. Nous avons $\tau e_\kappa = e_\kappa$, pour tout τ de $\text{Ker } \kappa$. Cela montre que ϵ^2 est invariant par tout élément de $\text{Ker } \kappa$, donc appartient à K_κ (condition b).

Soit un sous-corps de K_κ . Il est de la forme K_ψ avec ψ caractère de G tel que $\text{Ker } \psi \supset \text{Ker } \kappa$. Comme ϵ^2 est invariante par tout élément de $\text{Ker } \kappa$ et comme $\text{Gal}(K_\kappa/K_\psi)$ est isomorphe à $\text{Ker } \psi / \text{Ker } \kappa$, nous avons donc :

$$N_{K_\kappa/K_\psi}(\epsilon^2) = \epsilon \sum_{\tau \in \text{Ker } \psi} \tau^{2(1/|\text{Ker } \kappa|)} .$$

Considérons la quantité $(1/|\text{Ker } \kappa|) \sum_{\tau \in \text{Ker } \psi} \tau$. Il s'agit d'un idempotent de $\mathbb{Q}[G]$ et il est facile de voir que c'est la somme des idempotents e_{ψ_1} , pour tous les caractères ψ_1 rationnels irréductibles de G tels

que $\text{Ker } \psi_1 \supset \text{Ker } \psi$. Si donc $K_\kappa \neq K_\psi$, e_κ n'apparaît donc pas dans cette somme et l'on aura :

$$e_\kappa \sum_{\tau \in \text{Ker } \psi} \tau = 0 . \text{ Ceci prouve que } N_{K_\kappa/K_\psi}(\epsilon^2) = 1$$

(condition c) .

Remarque II . On trouvera dans [2] une troisième définition des κ -unités qui s'énonce ainsi : Soit κ un caractère résiduel pair , g_κ son ordre , ϕ_κ le $g_\kappa^{\text{ème}}$ polynôme cyclotomique et σ un générateur de $\text{Gal}(K_\kappa/\mathbb{Q})$. Une unité ϵ est une κ -unité si et seulement si elle vérifie les trois conditions :

- ϵ est une unité réelle et abélienne
- ϵ^2 appartient à K_κ
- $\epsilon^{2\phi_\kappa(\sigma)} = 1$.

3) Structure des groupes de κ -unités . Soient κ un caractère résiduel pair différent de 1 , g_κ son ordre , K_κ/\mathbb{Q} l'extension cyclique réelle correspondante , G_κ son groupe de Galois . Les groupes des valeurs absolues des κ -unités $|E_\kappa|$ et $|E_\kappa^+|$ sont des $\mathbb{Z}[G_\kappa]$ -modules .

La proposition suivante précise la structure de ces modules (la notion de module « simple » a été définie en [3] § III) .

Proposition IIb . Les $\mathbb{Z}[G_\kappa]$ -modules $|E_\kappa|$ et $|E_\kappa^+|$ sont isomorphes . Ce sont des $\mathbb{Z}[G_\kappa]$ -modules simples de caractères κ' . En tant que \mathbb{Z} -modules , ils sont libres de rang $\varphi(g_\kappa)$.

démonstration

Si $q_\kappa = 0$, les deux groupes E_κ et E_κ^+ coïncident. Supposons donc que $q_\kappa = 1$. Reprenons les notations introduites dans la proposition Ib et sa démonstration. L'application $|\epsilon| \rightarrow \epsilon^2$ est un isomorphisme de $|E_\kappa|$ sur $|E_\kappa^{++}|$. D'autre part, puisque $[E_\kappa^{++} : E_\kappa^{+2}] = 2$, on aura alors $E_\kappa^{+2} = E_\kappa^{++}(1-\sigma)$. L'application $|\epsilon| \rightarrow \epsilon^2$ est un isomorphisme de $|E_\kappa^+|$ sur $|E_\kappa^+|^2$. En résumé, on a les G_κ -isomorphismes suivants :

$$|E_\kappa| \cong |E_\kappa^{++}| \cong |E_\kappa^{++}|^{1-\sigma} = |E_\kappa^+|^2 \cong |E_\kappa^+|.$$

Soit E_{K_κ} le groupe des unités du corps K_κ . Soient \mathfrak{e}_κ^+ et \mathfrak{e}_{K_κ} les $\mathbb{Q}[G_\kappa]$ -modules déduits de $|E_\kappa^+|$ et $|E_{K_\kappa}|$ par extension de l'anneau des scalaires de \mathbb{Z} à \mathbb{Q} . Le module \mathfrak{e}_κ^+ est un sous-module de \mathfrak{e}_{K_κ} . Le caractère de ce $\mathbb{Z}[G_\kappa]$ -module est la somme des caractères de G_κ irréductibles sur \mathbb{Q} , différents de 1 ([3] Proposition III a). On déduit de la proposition II a que le caractère de \mathfrak{e}_κ^+ est κ' . Ce $\mathbb{Q}[G_\kappa]$ -module est donc isomorphe à l'idéal $\mathbb{Q}[G]e_\kappa$, de $\mathbb{Q}[G]$. Celui-ci est isomorphe à $\mathbb{Q}(g_\kappa)$ ([3] Proposition I a). Le rang de $|E_\kappa^+|$, en tant que \mathbb{Z} -module, est donc $\varphi(g_\kappa)$.

4) Groupe des unités d'un corps abélien réel. Soit K/\mathbb{Q} une extension abélienne finie réelle. Les notations $G, g, \mathfrak{X}, \mathfrak{X}', E_K, |E_K|$ ont toujours la même signification.

Définition de E^K et Q_K . Pour tout κ de \mathfrak{X} , on pose $E_\kappa^K = E_K \cap E_\kappa$. On désignera par E^K le produit $\prod_{\kappa' \in \mathfrak{X}'} E_{\kappa'}^K$, et par Q_K l'indice : $Q_K = [E_K : E^K]$ (Les notions de « noyau » et module « complet » employées ci-dessous ont été définies en [3] § III).

Proposition II c. Le groupe $|E^K|$ est égal au produit direct $\prod_{\kappa' \in \mathfrak{X}'} |E_{\kappa'}^K|$.

Le $\mathbb{Z}[G]$ -module $|E^K|$ est le noyau de $|E_K|$, c'est-à-dire le plus grand sous- $\mathbb{Z}[G]$ -module de $|E_K|$ complet. L'indice Q_K est fini et divise g^{g-1} .

démonstration

Si ε appartient à $E_{\kappa'}^K$, nous aurons alors $|\varepsilon|^{e_{\kappa'}} = |\varepsilon|$ et $|\varepsilon|^{e_{\psi'}} = 1$ si $\psi' \neq \kappa'$ (Proposition II a) .

Ceci montre que le produit $\prod_{\kappa' \in \mathfrak{X}'} |E_{\kappa'}^K|$ est direct . Soit maintenant H un sous-module de $|E_K|$ complet . Nous aurons $H^{e_{\kappa'}} \subset H \subset |E_K|$ et en vertu de la proposition IIa , $H^{e_{\kappa'}} \subset |E_{\kappa}|$, d'où $H^{e_{\kappa'}} \subset |E_{\kappa'}^K|$. En faisant le produit sur les κ' de \mathfrak{X}' , nous obtiendrons $H \subset |E^K|$. Ceci montre que tout sous- $\mathbb{Z}[G]$ -module complet de $|E_K|$ est contenu dans $|E^K|$. Montrons maintenant que $|E^K|$ est complet . On déduit de la proposition Ib que E_{κ}^K est égal à E_{κ} ou E_{κ}^+ . Ceci montre , d'après la proposition IIb , que $|E_{\kappa}^K|$ est un $\mathbb{Z}[G_{\kappa}]$ -module simple , donc complet ([3] Proposition III c) . Il conserve ces propriétés en tant que $\mathbb{Z}[G]$ -module . Finalement , $|E^K|$ sera donc un $\mathbb{Z}[G]$ -module complet et c'est donc le noyau de $|E^K|$. Sa dimension sur \mathbb{Z} est $g-1$ et nous avons vu dans la démonstration de la proposition III b de [3] que $|E_K|^g$ est inclus dans le noyau de $|E_K|$, c'est-à-dire dans $|E^K|$. On en déduit que Q_K divise g^{g-1} . Cette majoration sera améliorée par la proposition suivante .

Définition de l'ordre limite \mathfrak{B} de $\mathbb{Q}[G]$. Nous appellerons ainsi la somme $\mathfrak{B} = \mathbb{Z}[G] + e_1 \mathbb{Z}[G]$, où e_1 désigne l'idempotent de $\mathbb{Q}[G]$ associé au caractère unité de G , c'est-à-dire $e_1 = \frac{1}{g} \sum_{\sigma \in G} \sigma$. C'est un ordre de $\mathbb{Q}[G]$ qui vérifie $\mathbb{Z}[G] \subset \mathfrak{B} \subset \mathcal{O}$. Son discriminant est g^{g-2} . On appellera indice limite et on notera Q_G l'indice $[\mathcal{O} : \mathfrak{B}]$.

Compte-tenu de la valeur du discriminant de \mathcal{O} ([3] , § III) , on a

$$Q_G = \left(g^{g-2} / \prod_{\kappa' \in \mathfrak{X}'} d_{\kappa'} \right)^{1/2} ,$$

où d_{κ} est le discriminant du corps cyclotomique $\mathbb{Q}^{(g_{\kappa})}$.

Pour toute unité ε de K , on a $|\varepsilon|^{e_1} = 1$. On en déduit que $|E_K|$ est un \mathfrak{B} -module .

Leopoldt affirme , dans [2] :

Proposition II d . L'indice Q_K divise l'indice limite Q_G .

Définition de E^{K+} et Q_K^+ . Nous poserons $E^{K+} = \prod_{\kappa' \in \mathfrak{X}'} E_{\kappa'}^+$.

On a $E^{K+} \subset E^K$. On désigne par Q_K^+ l'indice $Q_K^+ = [E_K : E^{K+}]$.

Proposition II e . Le groupe $|E^{K+}|$ est égal au produit direct $\prod_{\kappa' \in \mathfrak{X}'} |E_{\kappa'}^+|$. Le $\mathbb{Z}[G]$ -module $|E^{K+}|$ est complet et contenu dans le noyau $|E^K|$ de $|E_K|$. L'indice Q_K^+ est de la forme $Q_K^+ = 2^{q_K} Q_K$ avec $q_K \leq \sum_{\kappa' \in \mathfrak{X}'} q_{\kappa'}$.

La démonstration ne fait pas intervenir d'autres arguments que ceux employés dans la démonstration de II c .

III

Régulateurs

1) Définitions des κ -régulateurs d'unités . Soient, comme précédemment, K/\mathbb{Q} une extension abélienne finie réelle, G son groupe de Galois, E_K le groupe de ses unités . On désigne toujours par \mathcal{E}_K le $\mathbb{Q}[G]$ -module déduit de $|E_K|$ par extension de l'anneau des scalaires de \mathbb{Z} à \mathbb{Q} . Soit α un élément de \mathcal{E}_K et soit κ un caractère de K différent de 1 . Nous po-

serons $R_{\kappa}^K(\alpha) = \prod_{\psi \in \kappa'} \left(\sum_{\sigma \in G} \psi(\sigma^{-1}) \text{Log} |\alpha^{\sigma}| \right)$ et nous appelle-

rons cette quantité le κ -régulateur de α dans K . Comme il ne dépend que de κ' et non de κ , on le notera aussi $R_{\kappa'}^K(\alpha)$.

Dans le cas particulier où K serait égal à K_{κ} nous parlerons seulement de κ -régulateur et nous le noterons alors $R_{\kappa}(\alpha)$. La proposition suivante relie ces deux notions :

Proposition III a . Le κ -régulateur de α dans K dépend uniquement du κ -régulateur de α_{κ} , et du degré $[K:K_{\kappa}]$. Plus précisément on a la for-

mule $R_{\kappa}^K(\alpha) = [K:K_{\kappa}]^{\varphi(g_{\kappa})} R_{\kappa}(\alpha_{\kappa})$.

démonstration

On désigne toujours par \mathfrak{X}' l'ensemble des caractères de G irréductibles sur \mathbb{Q} . Nous avons $\alpha = \prod_{\kappa' \in \mathfrak{X}'} \alpha_{\kappa'}$, et on en déduit :

$$\begin{aligned} \sum_{\sigma \in G} \psi(\sigma^{-1}) \operatorname{Log} |\alpha^\sigma| &= \sum_{\kappa' \in \mathfrak{X}'} \left(\sum_{\sigma \in G} \psi(\sigma^{-1}) \operatorname{Log} |\alpha_{\kappa'}^\sigma| \right) \\ &= \sum_{\kappa' \in \mathfrak{X}'} \left(\sum_{\tau \in \operatorname{Ker} \kappa} \left(\sum_{\sigma \bmod \operatorname{Ker} \kappa} \psi(\sigma^{-1} \tau^{-1}) \operatorname{Log} |\alpha_{\kappa'}^{\sigma \tau}| \right) \right). \end{aligned}$$

La dernière somme est effectuée suivant un système de représentants de G modulo $\operatorname{Ker} \kappa$. Puisque τ appartient à $\operatorname{Ker} \kappa$ nous avons $\tau e_{\kappa'} = e_{\kappa'}$, et

$\alpha_{\kappa'}^{\sigma \tau} = \alpha_{\kappa'}^\sigma$, d'où l'égalité :

$$\begin{aligned} \sum_{\sigma \in G} \psi(\sigma^{-1}) \operatorname{Log} |\alpha^\sigma| &= \\ &= \sum_{\kappa' \in \mathfrak{X}'} \left(\sum_{\tau \in \operatorname{Ker} \kappa} \psi(\tau^{-1}) \right) \left(\sum_{\sigma \bmod \operatorname{Ker} \kappa} \psi(\sigma^{-1}) \operatorname{Log} |\alpha_{\kappa'}^\sigma| \right). \end{aligned}$$

La quantité $\sum_{\tau \in \operatorname{Ker} \kappa} \psi(\tau^{-1})$ est égale à 0 si $\operatorname{Ker} \kappa$ n'est pas inclus dans

$\operatorname{Ker} \psi$. Supposons donc que $\operatorname{Ker} \kappa$ soit inclus dans $\operatorname{Ker} \psi$; la somme contenue dans la dernière parenthèse peut se décomposer de la façon suivante :

$$\begin{aligned} \sum_{\tau \bmod \operatorname{Ker} \psi} \left(\sum_{\sigma \equiv \tau (\operatorname{Ker} \kappa)} \psi(\sigma^{-1}) \operatorname{Log} |\alpha_{\kappa'}^\sigma| \right) &= \\ &= \sum_{\tau \bmod \operatorname{Ker} \psi} \psi(\tau^{-1}) \sum_{\sigma \equiv \tau (\operatorname{Ker} \kappa)} \operatorname{Log} |\alpha_{\kappa'}^\sigma|. \end{aligned}$$

La dernière somme peut s'écrire comme le logarithme du produit

$\prod_{\sigma \equiv \tau (\operatorname{Ker} \kappa)} \alpha_{\kappa'}^\sigma$. Mais $\alpha_{\kappa'}$ appartient à $\mathcal{E}_{K_{\kappa'}}$ et ce produit est égal à

$\prod \alpha_{\kappa'}^\sigma$, σ parcourant $\operatorname{Gal}(K_{\kappa'}/k_\psi)$. Si $\kappa' \neq \psi'$, alors $\operatorname{Ker} \kappa \neq \operatorname{Ker} \psi$ et $K_{\kappa'} \neq K_\psi$. Par un calcul analogue à celui qui est développé dans la réciproque de la proposition II a, on montrerait que ce produit vaut 1.

Il reste donc :

$$\begin{aligned} \sum_{\sigma \in G} \psi(\sigma^{-1}) \text{Log} |\alpha^\sigma| &= [K:K_\psi] \sum_{\sigma \text{ mod Ker } \psi} \psi(\sigma^{-1}) \text{Log} |\alpha_\psi^\sigma| \\ &= [K:K_\psi] \sum_{\sigma \in G_\psi} \psi(\sigma^{-1}) \text{Log} |\alpha_\psi^\sigma| , \end{aligned}$$

en désignant par G_ψ le groupe de Galois de K_ψ/\mathbb{Q} . En effectuant le produit sur les caractères Γ -conjugués de ψ , on obtient le résultat annoncé.

Remarque III a. Il est montré également dans [2], que $R_\kappa(\alpha_{\kappa'})$ est nul si et seulement si $\alpha_{\kappa'} = 1$.

2) κ -régulateur d'un groupe d'unités. Soient κ un caractère résiduel pair, différent de 1 et ϵ un élément de \mathcal{E}_κ .

Soit $\langle \epsilon \rangle$ le groupe engendré par ϵ et ses conjugués. Si G_κ désigne le groupe de Galois de K_κ/\mathbb{Q} , $\langle \epsilon \rangle$ est donc le $\mathbb{Z}[G_\kappa]$ -module engendré par ϵ .

Remarque III b. Si ϵ est différent de 1, alors $\langle \epsilon \rangle$ est un $\mathbb{Z}[G_\kappa]$ -module simple de caractère κ' . En tant que \mathbb{Z} -module, il est libre de rang $\varphi(g_\kappa)$. En particulier, si ϵ est une κ -unité différente de ± 1 , l'indice $[E_\kappa : \langle \epsilon \rangle]$ est fini.

En effet, $\langle \epsilon \rangle$ est $\sqrt[\text{un}]{\mathbb{Z}}$ -module sans torsion et de type fini, donc libre. Si l'on étend l'anneau des scalaires à \mathbb{Q} , nous obtenons $\langle \epsilon \rangle^{\mathbb{Q}}$ qui est inclus dans \mathcal{E}_κ . Or ce $\mathbb{Q}[G_\kappa]$ -module est simple (Proposition II b). Nous aurons donc $\langle \epsilon \rangle^{\mathbb{Q}} = \mathcal{E}_\kappa$.

Soit maintenant ϵ_1 un élément de $\langle \epsilon \rangle$. (Il est entendu que ϵ et ϵ_1 sont différents de 1). Il existe u dans $\mathbb{Z}[G_\kappa]$ tel que $\epsilon_1 = \epsilon^u$. Rappelons que dans la démonstration de la proposition Ia de [3], nous avons étendu κ à $\mathbb{Q}[G]$. L'homomorphisme obtenu, que l'on note encore κ , a pour noyau $\bigoplus_{\psi' \neq \kappa'} \mathbb{Q}[G_\kappa] e_{\psi'}$, et réalise un isomorphisme entre

$\mathbb{Q}[G_\kappa] e_\kappa$, et $\mathbb{Q} \binom{g_\kappa}{(g_\kappa)}$. Le symbole $\kappa(u)$ représente donc un élément de

$\mathbb{Q} \binom{g_\kappa}{(g_\kappa)}$. De plus, $\mathbb{Z}[G_\kappa] e_\kappa$, correspond dans l'isomorphisme ci-dessus

à l'anneau des entiers de $\mathbb{Q} \binom{g_\kappa}{(g_\kappa)}$. Ceci montre que $\kappa(u)$ est un entier de

$\mathbb{Q} \binom{g_\kappa}{(g_\kappa)}$. Nous poserons :

$N_{\kappa}(u) = N_{\mathbb{Q}(\mathfrak{g}_{\kappa})/\mathbb{Q}}(\kappa(u))$. (Si l'on remplace κ par un caractère Γ -

conjugué , $\kappa(u)$ est remplacé par un conjugué et $N_{\kappa}(u)$ n'a pas changé. Cette quantité ne dépend donc que de κ' et peut donc être notée $N_{\kappa'}(u)$. Nous avons :

$$\sum_{\sigma \in G_{\kappa}} \kappa(\sigma^{-1}) \text{Log} |\epsilon^{u\sigma}| = \kappa(u) \sum_{\sigma \in G_{\kappa}} \kappa(\sigma^{-1}) \text{Log} |\epsilon^{\sigma}|$$

d'où l'on déduit $R_{\kappa}(\epsilon^u) = N_{\kappa}(u) R_{\kappa}(\epsilon)$.

D'autre part l'indice $[\langle \epsilon \rangle : \langle \epsilon_1 \rangle]$ est le déterminant de l'application $x \rightarrow x^u$ de \mathcal{E}_{κ} dans \mathcal{E}_{κ} . Comme \mathcal{E}_{κ} est isomorphe à $\mathbb{Q}[G_{\kappa}]e_{\kappa}$, en tant que $\mathbb{Q}[G_{\kappa}]$ -module , l'indice considéré est égal au déterminant de l'endomorphisme : $y \rightarrow yu$ de $\mathbb{Q}[G_{\kappa}]e_{\kappa}$. La matrice de cette application se diagonalise dans \mathbb{C} . Elle est semblable à la matrice diagonale :

$$\begin{pmatrix} \psi(u) \\ \vdots \\ \psi(u) \end{pmatrix} ,$$

où ψ parcourt la Γ -classe de κ . Le déterminant de cet endomorphisme est donc $N_{\kappa}(u)$. Nous avons démontré :

Proposition III b . Soit κ un caractère pair . Soient ϵ un élément de \mathcal{E}_{κ} et $\langle \epsilon \rangle$ le sous-groupe de \mathcal{E}_{κ} engendré par les conjugués de ϵ . Soit u un élément de $\mathbb{Z}[G_{\kappa}]$; la quantité ϵ^u est donc un élément de $\langle \epsilon \rangle$. Si ϵ et ϵ^u diffèrent de 1 , les groupes $\langle \epsilon \rangle$ et $\langle \epsilon^u \rangle$ sont des \mathbb{Z} -modules libres de rang $\varphi(\mathfrak{g}_{\kappa})$ et nous avons les égalités :

$$[\langle \epsilon \rangle : \langle \epsilon^u \rangle] = R_{\kappa}(\epsilon^u) / R_{\kappa}(\epsilon) = N_{\mathbb{Q}(\mathfrak{g}_{\kappa})/\mathbb{Q}}(\kappa(u)) ,$$

où $N_{\mathbb{Q}(\mathfrak{g}_{\kappa})/\mathbb{Q}}(\kappa(u))$ désigne la norme dans $\mathbb{Q}(\mathfrak{g}_{\kappa})/\mathbb{Q}$ de $\kappa(u)$.

Désignons par H un $\mathbb{Z}[G_{\kappa}]$ -module , de type fini en tant que \mathbb{Z} -module et contenu dans \mathcal{E}_{κ} . Nous pouvons faire au sujet de H la même remarque que celle qui fut faite pour $\langle \epsilon \rangle$: Si H n'est pas réduit à 1 , H est un $\mathbb{Z}[G_{\kappa}]$ -module simple . En tant que \mathbb{Z} -module il est donc libre de rang $\varphi(\mathfrak{g}_{\kappa})$. Il est entendu que désormais H est supposé différent de 1 .

Si ϵ appartient à H et diffère de 1 , désignons par \mathfrak{h} l'idéal de $\mathbb{Q}[G_{\kappa}]e_{\kappa}$, dont l'inverse est défini par

$$\mathfrak{h}^{-1} = \{v ; v \in \mathbb{Q}[G_{\kappa}]e_{\kappa}, \epsilon^v \in H\} .$$

Désignons également par $N_{\kappa}(\mathfrak{h})$ la quantité $N_{\mathbb{Q}[G_{\kappa}]/\mathbb{Q}}(\kappa(\mathfrak{h}))$.

Proposition III c. L'idéal \mathfrak{h} ainsi défini est entier. Sa classe ne dépend pas du choix de ϵ dans H . Elle est égale à la classe principale si et seulement si H est engendré par les conjugués d'un de ses éléments (autrement dit si H est un $\mathbb{Z}[G_{\kappa}]$ -module monogène). La quantité $R_{\kappa}(\epsilon)/N_{\kappa}(\mathfrak{h})$ est indépendante du choix de ϵ dans H .

démonstration

$\mathbb{Z}[G_{\kappa}]e_{\kappa}$, est l'anneau des entiers de $\mathbb{Q}[G_{\kappa}]e_{\kappa}$. Puisque ϵ appartient à H , $\mathbb{Z}[G_{\kappa}]e_{\kappa}$ est donc inclus dans \mathfrak{h}^{-1} ; ceci montre que \mathfrak{h} est entier. Soit ϵ_1 un autre élément de H , différent de 1. Puisque \mathcal{E}_{κ} est un $\mathbb{Q}[G_{\kappa}]$ -module simple (Proposition II b) il existe v dans $\mathbb{Q}[G_{\kappa}]$ tel que $\epsilon_1 = \epsilon^v$. On peut supposer que v appartient à $\mathbb{Z}[G_{\kappa}]$. (Si cela n'est pas, on peut toujours s'y ramener puisqu'il existe $\epsilon_2 = \epsilon^u = \epsilon_1^{u_1}$ avec u et u_1 dans $\mathbb{Z}[G_{\kappa}]$). Soit \mathfrak{h}_1 l'idéal défini comme \mathfrak{h} à partir de ϵ_1 . Nous avons $\mathfrak{h}_1 = u\mathfrak{h} = u e_{\kappa} \mathfrak{h}$. On en déduit que \mathfrak{h} et \mathfrak{h}_1 sont dans la même classe. D'autre part on déduit de la proposition III b l'égalité :

$$R_{\kappa}(\epsilon) / N_{\kappa}(\mathfrak{h}) = R_{\kappa}(\epsilon_1) / N_{\kappa}(\mathfrak{h}_1)$$

Supposons que H soit engendré par les conjugués de ϵ . On a donc $H = \langle \epsilon \rangle$. Remarquons que, puisque \mathcal{E}_{κ} est un $\mathbb{Q}[G_{\kappa}]e_{\kappa}$ -espace vectoriel, la condition $\epsilon^v = \epsilon^w$ avec v et w dans $\mathbb{Q}[G_{\kappa}]e_{\kappa}$, implique $v = w$. Si donc v appartient à $\mathbb{Q}[G_{\kappa}]e_{\kappa}$, et si ϵ^v appartient à $\langle \epsilon \rangle$, alors on aura $\epsilon^v = \epsilon^{we_{\kappa}}$ avec w dans $\mathbb{Z}[G_{\kappa}]e_{\kappa}$. L'idéal \mathfrak{h} sera donc égal à $\mathbb{Z}[G_{\kappa}]e_{\kappa}$. Réciproquement, supposons que \mathfrak{h} soit engendré par un élément de la forme ue_{κ} , avec u dans $\mathbb{Z}[G_{\kappa}]$, on peut alors vérifier que H est engendré par les conjugués de $\epsilon^{(ue_{\kappa})^{-1}}$.

Définition du κ -régulateur de H . On posera $R_{\kappa}(H) = R_{\kappa}(\epsilon)/N_{\kappa}(\mathfrak{h})$ et on appellera cette quantité le κ -régulateur de H . Pour un sous-groupe de \mathcal{E}_{κ} réduit à 1 on posera $R_{\kappa}(1) = 0$.

Remarque III c . Si H est engendré par les conjugués de ε , on a alors $R_{\kappa}(H) = R_{\kappa}(\varepsilon)$.

En effet , nous avons vu au cours de la démonstration précédente , que , dans ce cas , l'idéal \mathfrak{h} était égal à $Z[G_{\kappa}]e_{\kappa}$.

Proposition III d . Si H_1 est un sous- $Z[G_{\kappa}]$ -module de H , on a alors :

$$[H:H_1] = R_{\kappa}(H_1) / R_{\kappa}(H) .$$

démonstration

Soit ε un élément de H_1 différent de 1 . Soient \mathfrak{h} et \mathfrak{h}_1 les idéaux de $\mathbb{Q}[G_{\kappa}]e_{\kappa}$, définis par :

$$\mathfrak{h}^{-1} = \{u ; \varepsilon^u \in H\} \quad \text{et} \quad \mathfrak{h}_1^{-1} = \{u ; \varepsilon^u \in H_1\} .$$

Considérons l'application $u \rightarrow \varepsilon^u$ de \mathfrak{h}^{-1} dans H . Comme H est un $Z[G_{\kappa}]$ -module simple , cet homomorphisme est surjectif . Il applique \mathfrak{h}_1^{-1} sur H_1 .

En factorisant nous obtenons $[H:H_1] = [\mathfrak{h}^{-1} : \mathfrak{h}_1^{-1}] = [\mathfrak{h}_1 : \mathfrak{h}]$.

D'autre part , les idéaux \mathfrak{h} et \mathfrak{h}_1 sont entiers . Nous avons donc

$$[\mathfrak{h}_1 : \mathfrak{h}] = N_{\kappa}(\mathfrak{h}) / N_{\kappa}(\mathfrak{h}_1) = R_{\kappa}(H_1) / R_{\kappa}(H) .$$

Soit maintenant K/\mathbb{Q} une extension abélienne finie réelle . Les notations $G, \mathfrak{K}, \mathfrak{K}'$ ont toujours la même signification . Soit κ un caractère de K . Soit H un sous-groupe de \mathcal{E}_K , de type fini en tant que Z -module .

Définition du κ -régulateur de H dans K . Posons $H_{\kappa} = H^{e_{\kappa}}$; il est donc inclus dans \mathcal{E}_{κ} . Supposons que $H_{\kappa} \neq 1$ et soit ε un élément de H tel que $\varepsilon_{\kappa} \neq 1$. Désignons par \mathfrak{h} l'idéal de $\mathbb{Q}[G]e_{\kappa}$, ainsi défini :

$$\mathfrak{h}^{-1} = \{u ; u \in \mathbb{Q}[G]e_{\kappa} ; \varepsilon_{\kappa}^u \in H_{\kappa}\} .$$

De même qu'à la proposition III c , le rapport $R_{\kappa}^K(\varepsilon) / N_{\kappa}(\mathfrak{h})$ est indépendant de ε ; nous l'appellerons le κ -régulateur de H dans K et le noterons $R_{\kappa}^K(H)$. Si $H_{\kappa} = 1$, on posera $R_{\kappa}^K(H) = 0$.

Proposition III e . Le κ -régulateur de H dans K est lié au κ -régulateur de H_{κ} , par la formule :

$$R_{\kappa}^K(H) = [K:K_{\kappa}]^{\varphi(g_{\kappa})} R_{\kappa}(H_{\kappa}) .$$

C'est une conséquence immédiate de la proposition III a .

3) Décomposition du régulateur . Désignons toujours par K/\mathbb{Q} une extension abélienne finie réelle , G son groupe de Galois , g son degré . Notons les éléments de G de la façon suivante : $G = \{\sigma_1, \sigma_2, \dots, \sigma_g\}$. Soient d'autre part $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{g-1}$ des unités de K et H le sous-groupe engendré par celles-ci .

Le régulateur de H est la valeur absolue de l'un quelconque des mineurs d'ordre $g-1$ de la matrice $\left(\text{Log} |\varepsilon_i^{\sigma_j}| \right)_{\substack{1 \leq i \leq g-1 \\ 1 \leq j \leq g}}$. On le notera $R_K(H)$.

Rappelons que : $R_K(H)$ est différent de 0 si et seulement si $|\varepsilon_1|, \dots, |\varepsilon_{g-1}|$ sont linéairement indépendantes . Si H_1 est un sous-groupe de H et si tous deux sont engendrés par $g-1$ unités linéairement indépendantes, alors on a l'égalité :

$$[H : H_1] = R_K(H_1) / R_K(H) .$$

Supposons désormais que H est un sous- $\mathbb{Z}[G]$ -module de $|E_K|$, complet . Posons $H_{\kappa'} = H^{\varepsilon_{\kappa'}}$ pour tout κ' de \mathfrak{X}' . Puisque la norme d'une unité de K est ± 1 , la composante H_1 de H relative au caractère unité est réduite à 1 . Nous aurons donc

$$H = \prod_{\kappa' \in \mathfrak{X}', \kappa' \neq 1} H_{\kappa'} .$$

Proposition III f . Si H est un sous- $\mathbb{Z}[G]$ -module de $|E_K|$ complet, son régulateur se décompose de la façon suivante :

$$g \cdot Q_G R_K(H) = \prod R_{\kappa'}^K(H) ;$$

ce produit étant étendu aux caractères irréductibles rationnels κ' de G , différents du caractère unité .

démonstration

Si l'une des composantes $H_{\kappa'}$, pour $\kappa' \neq 1$ est réduite à 1, alors H ne peut avoir pour rang $g-1$. Les deux membres de l'égalité à démontrer sont donc nuls . Nous supposons désormais que $H_{\kappa'}$ est différent de 1 pour tout $\kappa' \neq 1$.

Démontrons l'égalité d'abord dans le cas où il existe une unité ε de H telle que pour tout $\kappa' \neq 1$, $H_{\kappa'}$ soit engendré par les conjugués de $\varepsilon_{\kappa'}$; c'est-à-dire $H_{\kappa'} = \langle \varepsilon_{\kappa'} \rangle$. Utilisons le lemme Ic .

On peut remplacer la première ligne de la matrice de $\overset{\circ}{u}$ par la somme de toutes les lignes . Chaque terme de cette première ligne sera alors égal à $\prod_{\sigma \in G} u_{\sigma} = \text{Det } \overset{\circ}{u}_1$. En simplifiant par cette quantité nous obtenons

$$\text{Det } M = \prod_{\kappa' \in \mathfrak{X}', \kappa' \neq 1} \prod_{\psi \in \kappa'} \sum_{\sigma \in G} \psi(u_{\sigma}) u_{\sigma}$$

où M désigne la matrice obtenue à partir de la matrice de $\overset{\circ}{u}$ en remplaçant chaque terme de la première ligne par 1 . Posons maintenant $u_{\sigma} = \text{Log} |\epsilon^{\sigma}|$ et développons M par rapport à la première ligne . On a alors :

$\text{det } M = g R_K(H_0)$, où H_0 désigne le sous-groupe de H engendré par les conjugués de ϵ . D'autre part on reconnaît dans $\prod_{\psi \in \kappa'} \sum_{\sigma \in G} \psi(\sigma) u_{\sigma}$ le κ' -régulateur de ϵ dans K , c'est-à-dire le κ' -régulateur de H dans K (Remarque III c) . Nous avons donc

$$g R_K(H_0) = \prod_{\kappa' \in \mathfrak{X}', \kappa' \neq 1} R_{\kappa'}^K(H) .$$

Considérons maintenant l'application de \mathcal{O} dans H qui associe ϵ^u à u (\mathcal{O} est défini en [3] § III) .

Comme H est complet et que $H_{\kappa'}$ est simple , il s'agit d'une application surjective . Elle a pour noyau $\mathbb{Z} e_1$; e_1 désignant l'idempotent de $\mathbb{Q}[G]$ associé au caractère unité . Sa restriction à l'ordre limite \mathfrak{L} (introduit en II 4) a pour image H_0 . Nous avons donc :

$$R_K(H_0) / R_K(H) = [H:H_0] = [\mathcal{O}:\mathfrak{L}] = Q_G .$$

On en déduit l'égalité cherchée :

$$g Q_G R_K(H) = \prod R_{\kappa'}^K(H) .$$

Il reste maintenant à supposer que H est un sous- $\mathbb{Z}[G]$ -module complet quelconque de $|E_K|$. Soit ϵ un élément de H et soit I le sous-groupe de H engendré par les conjugués des $\epsilon_{\kappa'}$, κ' parcourant \mathfrak{X}' . Le $\mathbb{Z}[G]$ -module I est complet et vérifie de plus l'hypothèse supplémentaire faite tout à l'heure sur H . Nous avons donc :

$$g Q_G R_K(I) = \prod R_{\kappa'}^K(I) .$$

D'autre part nous avons :

$$R_K(I) / R_K(H) = [H:I] = \prod [H_{\kappa'} / I_{\kappa'}] .$$

Il reste alors à utiliser la proposition III d pour voir que :

$$g Q_G R_K(H) = \prod R_{\kappa'}^K(H) .$$

4) Système d'équations associé à un groupe abélien . Soient G un groupe abélien , \mathfrak{X} le groupe de ses caractères complexes et \mathfrak{X}' l'ensemble de ses caractères irréductibles sur \mathbb{Q} .

Pour tout sous-groupe S de \mathfrak{X} et tout caractère κ' de \mathfrak{X}' posons :

$$\begin{aligned} \delta_{S\kappa'} &= 0 \quad \text{si } \kappa' \notin S \\ &= 1 \quad \text{si } \kappa' \in S . \end{aligned}$$

Nous appellerons système d'équations associé au groupe G le système

$$\text{d'équations : } \sum_S \delta_{S\kappa'} x_S = 0 , \quad \kappa' \text{ parcourant } \mathfrak{X}' .$$

Les sommes ci-dessus sont prises sur l'ensemble des sous-groupes S de \mathfrak{X} . Les inconnues x_S sont indexées par les sous-groupes de \mathfrak{X} et il y a $\text{Card}(\mathfrak{X}')$ équations .

Proposition III g . Les équations du système associé au groupe G sont indépendantes . La dimension de l'espace des solutions est égale au nombre de sous-groupes non cycliques de G . En particulier , le système associé au groupe G admet la solution triviale comme unique solution si et seulement si le groupe G est cyclique .

démonstration

Ecrivons le système associé à G sous la forme

$$\sum_S \delta_{S\kappa'} x_S = \sum_{S'} -\delta_{S\kappa'} x_{S'} ,$$

où la somme de gauche est étendue aux sous-groupes cycliques de \mathfrak{X} et où celle de droite est étendue aux sous-groupes non cycliques de \mathfrak{X} . Ordonnons les sous-groupes cycliques de \mathfrak{X} par une relation d'ordre total α telle que si $S \alpha S'$, alors $\text{Card}(S) \leq \text{Card}(S')$. Il y a une bijection triviale entre \mathfrak{X}' et l'ensemble de ces sous-groupes cycliques . Ordonnons \mathfrak{X}' à l'aide de la relation déduite de α par cette bijection , et écri -

vons la matrice $(\delta_{S\kappa'})_{\kappa' \in \mathfrak{X}'}$ et S cyclique, en respectant cet ordre sur les deux ensembles d'indices. On constate alors que cette matrice est triangulaire avec des termes diagonaux égaux à 1. Le système écrit sous la forme ci-dessus est donc un système de Krammer, d'inconnues principales x_S , S parcourant l'ensemble des sous-groupes cycliques de \mathfrak{X} . D'où le résultat annoncé.

Remarque III d. On trouvera dans [2] un calcul explicite des solutions.

5) Relations entre les régulateurs des sous-corps d'un corps abélien réel. On désigne toujours par K/\mathbb{Q} une extension abélienne finie réelle. Les notations $G, g, \mathfrak{X}, \mathfrak{X}'$ ont la même signification. Soient, de plus, L un sous-corps de K , G_L le groupe de Galois de l'extension L/\mathbb{Q} , g_L son degré, \mathfrak{X}_L son groupe de caractères, \mathfrak{X}'_L l'ensemble des caractères de G_L irréductibles sur \mathbb{Q} .

Appliquons la proposition III f, au corps L et au $\mathbb{Z}[G_L]$ -module complet E^{L+} (défini au § II 4). Nous aurons donc :

$$g_L Q_{G_L} R_L(E^{L+}) = \prod_{\kappa' \in \mathfrak{X}'_L, \kappa' \neq 1} R_{\kappa'}^L(E^{L+}) .$$

Posons $R_{\kappa'} = R_{\kappa'}(E_{\kappa'}^+)$ et utilisons la proposition III e :

$$R_{\kappa'}^L(E^{L+}) = (g_L/g_{\kappa'})^{\varphi(g_{\kappa'})} R_{\kappa'} .$$

Posons encore : $Q'_{G_L} = g_L Q_{G_L} / \prod_{\kappa' \in \mathfrak{X}'_L, \kappa' \neq 1} (g_L/g_{\kappa'})^{\varphi(g_{\kappa'})}$.

Nous en déduisons :

$$Q'_{G_L} R_L(E^{L+}) = \prod_{\kappa' \in \mathfrak{X}'_L, \kappa' \neq 1} R_{\kappa'} .$$

Désignons par R_L le régulateur de L , c'est-à-dire : $R_L = R_L(E_L)$.

Nous pouvons remplacer $R_L(E^{L+})$ par $Q'^+_L R_L$. D'autre part introduisons les $\delta_{S\kappa'}$ définis en III 4. L'égalité précédente peut alors s'écrire

$$Q'_{G_L} Q_L^+ R_L = \prod_{\kappa' \in \mathfrak{X}'_L} R_{\kappa'}^{\delta_{\mathfrak{X}'_L \kappa'}}$$

(en posant $R_1 = 1$) .

Rappelons que l'application $L \rightarrow \mathfrak{X}_L$ réalise une bijection entre les sous-corps L de K et les sous-groupes de \mathfrak{X} ([3] Proposition IV a) . Nous pouvons donc indexer les composantes d'une solution X du système d'équations associé à G par les sous-corps de K . Soit $X = (x_L)$ une telle solution . Nous avons donc :

$$\prod_{L \subset K} (Q'_{G_L} Q_L^+ R_L)^{x_L} = 1 ,$$

ce produit étant étendu à tous les sous-corps de K .

$$\text{Posons } \gamma(G, X) = \prod_{L \subset K} Q'_{G_L}^{x_L} .$$

Pour calculer cette constante , nous utiliserons la valeur de l'indicelimité Q'_{G_L} donnée en II 4 . On a :

$$Q'_{G_L} = g_L^{(g_L+2)/2} / \prod_{\kappa' \in \mathfrak{X}'_L} (g_L/g_{\kappa'})^{\varphi(g_{\kappa'})} d_{\kappa'}^{1/2} .$$

Lorsqu'on effectue le produit sur les sous-corps L de K , les produits $\prod_{\kappa' \in \mathfrak{X}'_L}$ écrits ci-dessus vont disparaître . Il reste :

$$\gamma(G, X) = \prod_{L \subset K} g_L^{\frac{g_L+2}{2} x_L} .$$

Nous avons démontré :

Proposition III h . Soient K/\mathbb{Q} une extension abélienne réelle , G son groupe de Galois . Soit $X = (x_L)$ une solution du système d'équations associé à G (indexée par les sous-corps L de K) . Il existe entre les régulateurs R_L des sous-corps L de K la relation :

$$\prod_{L \subset K} R_L^{x_L} = \gamma(G, X)^{-1} \prod_{L \subset K} (Q_L^+)^{-x_L} .$$

La constante $\gamma(G, X)$ ne dépend que de G et de la solution X . Les produits sont étendus à l'ensemble des sous-corps L de K .

IV

Nombres de classes et unités cyclotomiques .

1) κ -unités cyclotomiques . On désigne par κ un caractère résiduel pair différent de 1 et par f_κ son conducteur . Le caractère κ peut donc être considéré comme un homomorphisme de $(\mathbb{Z}/f_\kappa\mathbb{Z})^*$ dans \mathbb{C}^* . Nous noterons a_κ un demi-système de représentants modulo f_κ de $\text{Ker } \kappa$, c'est-à-dire que a_κ est un ensemble de nombres entiers tels que :

- $\text{Ker } \kappa$ est l'ensemble des classes modulo f_κ de $a_\kappa \cup (-a_\kappa)$.
- l'intersection $a_\kappa \cap (-a_\kappa)$ est vide .

Nous désignerons par a_κ le cardinal de a_κ . Nous avons donc $a_\kappa = \varphi(f_\kappa)/2g_\kappa$. Si m est un entier nous désignerons par ζ_m la racine primitive $m^{\text{ème}}$ de 1 : $e^{2i\pi/m}$.

$$\text{Posons } \theta_\kappa = \prod_{n \in a_\kappa} (\zeta_{2f_\kappa}^n - \zeta_{2f_\kappa}^{-n}) .$$

Il est clair que θ_κ ne dépend pas , au signe près , de a_κ .

De plus les notions introduites ci-dessus ne dépendent en fait que de κ' .

Lemme IV a . La quantité θ_κ^2 appartient à $\text{Ker } \kappa$. Si le conducteur f_κ de κ est une puissance d'un nombre premier , alors θ_κ^2 engendre l'unique idéal premier ramifié de K_κ . Sinon θ_κ^2 est une unité de K_κ . Si θ'_κ est un conjugué de θ_κ , alors $\theta_\kappa/\theta'_\kappa$ est une unité de K_κ .

démonstration

C'est un exercice de trigonométrie élémentaire que de vérifier l'égalité :

$$-(1 - \zeta_{f_\kappa}^n)(1 - \zeta_{f_\kappa}^{-n}) = (\zeta_{2f_\kappa}^n - \zeta_{2f_\kappa}^{-n})^2 . \text{ On en déduit :}$$

$$\theta_\kappa^2 = (-1)^{a_\kappa} N_{\mathbb{Q}(f_\kappa)/K_\kappa} (1 - \zeta_{f_\kappa}) . \text{ Désignons par } \phi_n \text{ le } n^{\text{ème}} \text{ polynôme}$$

cyclotomique . Si p est premier , on a $\phi_n(1) = p$ et si n n'est pas pre-

mier , on a $\phi_n(1) = 1$. On en déduit que $1 - \zeta_{f_\kappa}$ est un générateur de

l'unique idéal premier ramifié de $\mathbb{Q}(f_\kappa)$ ou une unité de $\mathbb{Q}(f_\kappa)$ selon que f_κ soit une puissance d'un nombre premier ou non . La norme de $1 - \zeta_{f_\kappa}$

vérifiera donc une propriété analogue dans K_κ . Dans les deux cas, $\theta_\kappa/\theta'_\kappa$ sera une unité. De plus, $K(\theta_\kappa)/\mathbb{Q}$ est abélienne. On a donc $K_\kappa(\theta_\kappa) = K_\kappa(\theta'_\kappa)$ et on en déduit que $\theta_\kappa/\theta'_\kappa$ appartient à K_κ .

Remarque IV a. Leopoldt montre aussi les résultats suivants :

Si il existe deux caractères κ_1 et κ_2 , pairs, différents de 1, de conducteurs premiers entre eux et tels que $\kappa = \kappa_1 \kappa_2$, alors θ_κ appartient à K_κ . Si par contre le conducteur de κ est une puissance d'un nombre premier, alors θ_κ n'appartient pas à K_κ . Si enfin, κ ne vérifie ni l'une, ni l'autre des conditions énoncées ci-dessus, alors les deux éventualités peuvent se produire.

Remarque IV b. De plus, θ_κ^2 engendre K_κ . La justification de cette propriété sera donnée plus loin (Remarque IV d).

Soit g_κ l'ordre de κ et G_κ le groupe de Galois de K_κ/\mathbb{Q} . Désignons par σ_κ un générateur de G_κ et $\bar{\sigma}_\kappa$ un prolongement de σ_κ à $K_\kappa(\theta_\kappa)$. Nous poserons :

$$D_\kappa = \prod_{\ell | g_\kappa} (1 - \sigma_\kappa^{g_\kappa/\ell}) \quad \text{et} \quad \bar{D}_\kappa = \prod_{\ell | g_\kappa} (1 - \bar{\sigma}_\kappa^{g_\kappa/\ell}),$$

ces produits étant étendus aux nombres premiers divisant g_κ .

Proposition IV a. La quantité $\gamma_\kappa = \theta_\kappa^{\bar{D}_\kappa}$ est une κ -unité propre.

démonstration

En vertu du lemme précédent, γ_κ est une unité de K_κ . D'autre part θ_κ^2 appartient à K_κ .

Nous avons donc $\gamma_\kappa^2 = \theta_\kappa^{2\bar{D}_\kappa} = \theta_\kappa^{2D_\kappa}$. Pour appliquer la proposition II a, il suffit donc de vérifier que $D_\kappa e_{\kappa'} = D_\kappa$. Désignons par \mathfrak{X}' l'ensemble des caractères irréductibles sur \mathbb{Q} de G_κ . Nous avons

$1 = \sum_{\kappa' \in \mathfrak{X}'} e_{\kappa'}$, et il suffit de vérifier que $D_\kappa e_\psi = 0$ pour tout caractère

ψ de G_κ tel que $\psi' \neq \kappa'$. Considérons κ et ψ comme des homomorphismes de G_κ dans \mathbb{C}^* . Le premier est injectif et la condition $\psi' \neq \kappa'$ équivaut donc à $\text{Ker } \psi \neq 1$. Si cette condition est vérifiée, il existera un nom-

bre premier ℓ divisant $|\text{Ker } \psi|$ et $\sigma_\kappa^{g_\kappa/\ell}$ appartiendra à $\text{Ker } \psi$; d'où

$$\sigma_{\kappa}^{g_{\kappa}/\ell} e_{\psi} = e_{\psi} \text{ et } D_{\kappa} e_{\psi} = 0 .$$

Définition . Nous désignerons par H_{κ} le sous-groupe de E_{κ}^{+} engendré par -1 et les conjugués de γ_{κ} . Nous appellerons ses éléments des κ -unités cyclotomiques .

Remarque IV c . Posons $\tau = \sigma_{\kappa}^{g_{\kappa}/\ell}$. En utilisant l'identité $(1 - \tau)(1 + \tau + \dots + \tau^{n-1}) = 1 - \tau^n$, on vérifie que H_{κ} ne dépend pas du choix de σ_{κ} . D'autre part , H_{κ} ne dépend que de la Γ -classe de κ . Nous écrirons indifféremment H_{κ} ou $H_{\kappa'}$.

2) Unités cyclotomiques de K et interprétation du nombre de classes de K . On conserve les notations habituelles : $G, g, \mathfrak{X}, \mathfrak{X}'$.

Posons $H_K = \prod_{\kappa' \in \mathfrak{X}', \kappa' \neq 1} H_{\kappa'}$. Nous appellerons unités cyclotomiques de K les éléments de H_K . Nous avons $|H_K| = \prod_{\kappa' \in \mathfrak{X}', \kappa' \neq 1} |H_{\kappa'}|$

et ce produit est direct . Comme $|E_{\kappa}^{+}|$ est un $\mathbb{Z}[G]$ -module simple (Proposition II b) , $|H_{\kappa}|$ sera lui aussi simple ou réduit à 1 . (En fait , il n'est pas réduit à 1 . Remarque IV d) . Il s'en suit , ([3] Proposition III c) que $|H_K|$ est un $\mathbb{Z}[G]$ -module complet . La κ' -composante de H_K est $H_{\kappa'}$, c'est-à-dire : $H_{\kappa'} = H_K^{e_{\kappa'}}$.

Proposition IV b . L'indice du groupe des unités cyclotomiques dans le groupe des unités de K est égal au produit du nombre de classes d'idéaux de K par l'indice limite de G .

C'est-à-dire : $h_K Q_G = [E_K : H_K]$.

démonstration

Nous utiliserons la formule analytique donnant le nombre de classes de K ([1] § II 16) .

$$h_K = \left(\prod_{\kappa \in \mathfrak{X}, \kappa \neq 1} \sum_{\sigma \text{ mod Ker } \kappa} \kappa(\sigma^{-1}) \text{Log} |\theta_{\kappa}^{\sigma}| \right) / R_K$$

la somme est étendue à un système de représentants de $G \text{ mod. Ker } \kappa$.