Séminaire de Théorie des Nombres .

- Besançon -

Année 1975 - 1976

SPIEGELUNGSSATZ .

Bernard ORIAT

Faculté des Sciences . Mathématiques

25030 BESANCON CEDEX

SPIEGELUNGSSATZ .

Par Bernard ORIAT .

Nous exposons ci-après un " Spiegelungssatz " un peu plus général que celui de Leopoldt ;[6] . L'extension $L/\mathbb{Q}$ considérée par ce dernier est remplacée par une extension L/k . Soit ℓ un nombre premier . Les hypothèses :" ℓ ne divise pas $[L:\mathbb{Q}]$ et L contient une racine primitive $\ell^{\text{ème}}$ de l'unité " sont remplacées par " ℓ ne divise pas $[L:k]$ et L contient une racine primitive $\ell^{n\text{ ème}}$ de l'unité " . Le résultat obtenu (théorème III) a la forme suivante :

Soit ϕ un caractère de $G = \mathrm{Gal}(L/k)$, irréductible sur $\mathbb{Q}_\ell$ et soit $\overline{\phi}$ son reflet . Notons $\dim_m \mathcal{H}^\phi$ le m-rang de la ϕ-composante du ℓ-groupe des classes d'idéaux $\mathcal{H}$ de L, et $\dim_\ell \mathcal{E}^{\circ\phi}$ le ℓ-rang de la ϕ -composante du groupe $\mathcal{E}^\circ$ des ℓ-unités primaires de L .
Nous obtenons les inégalités :

$$\dim_m \mathcal{H}^{\overline{\phi}} - \dim_m \mathcal{H}^\phi \leqslant \dim_\ell \mathcal{E}^{\circ\phi} ,$$

pour toute puissance de ℓ , notée m et inférieure à ℓ^n .

Dans son principe , la démonstration reste semblable à celle de Leopoldt .

I

Relation du miroir.

Notations . Nous désignerons par :

L/k une extension finie galoisienne de corps de nombres ,

G son groupe de Galois ,

m un entier ,

ζ une racine primitive $m^{\text{ème}}$ de l'unité .

Nous supposerons que L contient ζ . D'autre part , soit M un corps de nombres contenant L ,tel que M/k soit galoisienne et M/L abélienne d'exposant divisant **m** . Comme L contient les racines $m^{ème}$ de 1 , l'extension M /L est une extension de Kummer d'exposant divisant m . Nous désignerons par W son radical , c'est-à-dire :

$$W = \{ w ; w \in M^*, w^m \in L \} .$$

Définitions de trois structures de G-modules . Soit τ un élément de G et t un prolongement de τ à M .

Considérons le groupe de Galois de M /L , noté Gal (M /L) Si u appartient à Gal (M /L) la quantité $t^{-1}ut$ appartient à Gal (M /L) et elle est indépendante du choix de t . En posant $u^\tau = t^{-1}ut$ on définit sur Gal (M /L) une stucture de G-module .

On note Gal (M/L)^ le groupe des homomorphismes de Gal (M/L) dans le groupe multiplicatif de L ,noté L^* . Comme M /L est d'exposant divisant m , et que L contient les racines $m^{ème}$ de 1 , ce groupe est le groupe des caractères de degré 1 de Gal (M /L). Si γ appartient à Gal (M/L)^ , nous définissons γ^τ en posant : $\gamma^\tau(u) = \gamma(u^\tau)$, pour tout u de Gal (M /L) . On obtient ainsi une structure de G-module pour Gal (M/L)^ .(En toute rigueur , Gal (M /L) étant un G-module à droite , il faudrait noter Gal (M /L)^ comme un G-module à gauche).

Considérons le groupe W/L^*. Si w appartient à W et si u appartient à Gal(M/ L) , w^{u-1} est une racine $m^{ème}$ de 1 et appartient donc à L . Il s'en suit que $w^t L^*$ est indépendant du choix de t. En posant : $(wL^*)^\tau = w^t L^*$, on définit sur W/L^* une structure de G-module .

Rappelons que la théorie de Kummer donne un isomorphisme canonique α entre les deux groupes W/L^* et Gal(M/L)^ ainsi défini: Si wL^* appartient à W/L^* , l'homomorphisme $\alpha(wL^*)$ de Gal(M/L) dans L^* correspondant à wL^* est défini par : $\alpha(wL^*)(u) = w^{u-1}$, pour tout u de Gal(M/L) .

Première définition de χ^*. Pour tout τ de G , nous désignerons par $\chi^*(\tau)$,la classe résiduelle modulo m définie par : $\zeta^\tau = \zeta^{\chi^*(\tau)}$.
Il est clair que $\chi^*(\tau)$ ne dépend pas du choix de la racine primitive

$m^{ème}$ de l'unité : ζ . De plus , $\chi^*(\tau)$ étant première à m , on peut considérer χ^* comme une application de G dans $(\mathbb{Z}/m\mathbb{Z})^*$. C'est un homomorphisme .

Théorème I. Les structures de G-module de W/L^* et $Gal(M/L)\hat{}$ sont liées par la relation : $(\alpha(wL^*))^\tau = \alpha((wL^*)^{\chi^*(\tau)\tau^{-1}})$, pour tout w de W et tout τ de Gal(M/L) .

Leopoldt appelle cette relation : "Spiegelungsrelation ".

Démonstration . Soit u un élément de Gal (M/L) . Les notations τ et t ont toujours le même sens . Nous avons , d'aprés la définition de $\alpha(wL^*)$: $\alpha(wL^*)(u^\tau)\, w = w^{u^\tau}$. D'autre part : $w^{t^{-1}u} = \alpha(wL^{*\tau^{-1}})(u)\, w^{t^{-1}}$, d'où l'on déduit que w^{u^τ} peut aussi s'écrire sous la forme : $w^{u^\tau} = w^{t^{-1}ut} = (\alpha(wL^{*\tau^{-1}})(u)\, w^{t^{-1}})^t = (\alpha(wL^{*\tau^{-1}})(u))^\tau\, w$. Or $\alpha(wL^{*\tau^{-1}})(u)$ est une racine $m^{ème}$ de 1 . Son image par τ est donc égale à sa puissance $\chi^*(\tau)^{ème}$ et nous avons : $w^{u^\tau} = \alpha((wL^*)^{\chi^*(\tau)\tau^{-1}})(u)\, w$. D'où la relation annoncée .

II

Décomposition du ℓ-groupe des classes d'idéaux et du groupe des ℓ-unités d'une extension de degré premier à ℓ. Caractère du groupe des ℓ-unités .

Nous désignerons toujours par L/k une extension finie galoisienne de corps de nombres et par G son groupe de Galois . Soit ℓ un nombre premier ne divisant pas le degré [L:k]. Cette hypothése assure la semi-simplicité de l'algébre $\mathbb{F}_\ell[G]$.

Rappels concernant les caractères ℓ-adiques de G . On trouvera dans [7]un exposé élémentaire sur les caractères ℓ-adiques d'un groupe abélien . Pour le cas général , nous renvoyons à [3] et [9] .

Soit ϕ un caractère irréductible de G sur le corps ℓ-adique : $\mathbb{Q}_\ell$. (C'est la trace d'une représentation linéaire irréductible de G sur $\mathbb{Q}_\ell$). Ce caractère ϕ est une application de G dans $\mathbb{Z}_\ell$ et comme ℓ ne divise pas l'ordre de G , son résidu modulo ℓ est

un caractére irréductible de G sur $\mathbb{F}_\ell$. De plus , on obtient par ce moyen une bijection entre l'ensemble des caractères irréductibles de G sur $\mathbb{Q}_\ell$ et l'ensemble des caractères irréductibles de G sur $\mathbb{F}_\ell$. ([3] §76). C'est la raison pour laquelle nous noterons de la même façon ϕ et son résidu modulo ℓ .

Soit χ un caractère de G absolument irréductible , au dessus de ϕ . Soit $\mathbb{Q}_\ell(\chi)$ son corps des valeurs . Comme l'algèbre $\mathbb{Q}_\ell[G]$ est décomposée , ϕ sera la trace de χ dans l'extension $\mathbb{Q}_\ell(\chi)/\mathbb{Q}_\ell$. Soit 1_ϕ l'idempotent associé à ϕ . Il est donné par : $1_\phi = (\chi(1)/|G|) \sum_{\sigma \in G} \phi(\sigma^{-1})\sigma$. Il s'agit donc d'un élément de $\mathbb{Z}_\ell[G]$.

Si H est un $\mathbb{Z}_\ell[G]$-module noté multiplicativement , nous appelerons ϕ-composante de H , le sous-module :

$$H^{1_\phi} = \{ h^{1_\phi} ; h \in H \} .$$

Nous le noterons simplement H^ϕ . On déduit des relations d'orthogonalité entre caractères , que H est le produit direct : $H = \prod H^\phi$, ϕ parcourant l'ensemble des caractères irréductibles de G sur $\mathbb{Q}_\ell$.

Lemme II. Si H est un $\mathbb{Z}_\ell[G]$-module et si J est un sous $\mathbb{Z}_\ell[G]$-module de H , la ϕ-composante de H/J est canoniquement isomorphe au quotient des ϕ-composantes de H et J . C'est-à-dire :

$$H^\phi/J^\phi \simeq (H/J)^\phi$$

En effet : considérons l'application de H^ϕ dans $(H/J)^\phi$, qui associe à h appartenant à H^ϕ , sa classe modulo J . C'est un homomorphisme surjectif qui a pour noyau J^ϕ.

Définitions des symboles : $\dim_\ell$, $\dim_m$, $\dim_\phi$, $\dim_{\phi m}$. Soit H un $\mathbb{Z}_\ell[G]$-module tel que $H^\ell = 1$. Il s'agit donc d'un $\mathbb{F}_\ell[G]$-module . Nous noterons $\dim_\phi H$ le nombre de $\mathbb{F}_\ell[G]$-modules simples de caractère ϕ qui interviennent dans une décomposition de H en produit direct de $\mathbb{F}_\ell[G]$-modules simples . Cette quantité est liée à la dimension de H^ϕ en tant que $\mathbb{F}_\ell$-espace vectoriel par : $\dim_\ell H^\phi = \phi(1)\dim_\phi H$.

Soit maintenant H un $\mathbb{Z}_\ell[G]$-module quelconque et soit m une puissance de ℓ . On désignera par $\dim_m H$ le m-rang de H , c'est-à-dire : $\dim_m H = \dim_\ell H^{m/\ell}/H^m$. On posera également : $\dim_{\phi m} H = \dim_\phi H^{m/\ell} / H^m$. On déduit du lemme ci-dessus la relation:

$\phi(1) \dim_{\phi m} H = \dim_m H^\phi$. En effet:
$\phi(1) \dim_\phi H^{m/\ell} / H^m = \dim_\ell (H^{m/\ell} / H^m)^\phi = \dim_\ell (H^\phi)^{m/\ell} / (H^\phi)^m = \dim_m H^\phi$.

Groupe des ℓ-classes d'idéaux. Soit K un corps intermédiaire entre k et L, tel que K/k soit galoisien. Soit U le groupe de Galois de L/K. Désignons par $\mathcal{H}_K$ (resp. $\mathcal{H}_L$) le ℓ-groupe des classes d'idéaux de K (resp. L). Notons j l'application de $\mathcal{H}_K$ dans $\mathcal{H}_L$ déduite de l'injection canonique du groupe des idéaux de K dans le groupe des idéaux de L.

Soit ϕ un caractère irréductible de G sur $\mathbb{Q}_\ell$. Rappelons que l'ensemble des éléments τ de G, tels que $\phi(\tau) = \phi(1)$ est le noyau de la représentation linéaire de G de caractère ϕ. Nous l'appelerons simplement le noyau de ϕ. Si ϕ_1 est un caractère de G/U, en composant ϕ_1 avec la surjection canonique π de G sur G/U, on obtient un caractère ϕ de G dont le noyau contient U. Si ϕ_1 est irréductible, alors ϕ est irréductible. On obtient ainsi une bijection canonique entre l'ensemble des caractères irréductibles de G sur $\mathbb{Q}_\ell$ dont le noyau contient U et l'ensemble des caractères irréductibles de G/U sur $\mathbb{Q}_\ell$. Désignons encore par π l'application de $\mathbb{Q}_\ell[G]$ sur $\mathbb{Q}_\ell[G/U]$ déduite de π par linéarité. Si $\phi = \phi_1 \circ \pi$, les idempotents associés à ϕ et ϕ_1 vérifient : $\pi(1_\phi) = 1_{\phi_1}$.

Proposition II a. L'application j est un homomorphisme injectif. Son image $j(\mathcal{H}_K)$ est l'ensemble des éléments de $\mathcal{H}_L$ invariants par U = Gal(L/K). Si ϕ_1 est un caractère de G/U irréductible sur $\mathbb{Q}_\ell$ et si $\phi = \phi_1 \circ \pi$, on a alors : $j(\mathcal{H}_K^{\phi_1}) = \mathcal{H}_L^\phi$.

Démonstration. Désignons par A_K, A_L les anneaux d'entiers de K et L. Soit $\mathfrak{a}$ un idéal de K dont la classe appartient à Ker j. Il existe donc a dans L tel que : $\mathfrak{a}A_L = aA_L$, d'où :
$\mathfrak{a}^{[L:K]} = N_{L/K}(a) A_K$ et $\mathfrak{a}^{[L:K]}$ est principal. Or $Cl_K(\mathfrak{a})$ est

d'ordre une puissance de ℓ et ℓ ne divise pas $[L:K]$. L'idéal a est donc principal et j est injectif .

Soit a un idéal de L , dont la classe est invariante par U. On aura alors $N_{L/K}(a)\, A_L = a^{[L:K]}$. En utilisant une relation de Bezout entre $[L:K]$ et l'ordre de $Cl_L(a)$, on obtient : $Cl_L(a) = Cl_L(N_{L/K}(a)^u A_L)$ et cela montre que $Cl_L(a)$ appartient à $j(\mathcal{H}_K)$. Comme $\Pi(1_\phi) = 1_{\phi_1}$, nous avons $\mathcal{H}_K^{1\phi_1} = \mathcal{H}_K^{1\phi}$ et $j(\mathcal{H}_K^{\phi_1}) = j(\mathcal{H}_K)^\phi \subset \mathcal{H}_L^\phi$. Réciproquement , si τ appartient à U , τ appartient à $\mathrm{Ker}\ \phi$ et vérifie : $\tau 1_\phi = 1_\phi$. On en déduit que tout élément de $\mathcal{H}_L^\phi$ est invariant par U , ce qui démontre l'inclusion : $\mathcal{H}_L^\phi \subset j(\mathcal{H}_K^{\phi_1})$.

Conséquence . Convenons d'identifier l'ensemble des caractères de G/U irréductibles sur $\mathbb{Q}_\ell$ à l'ensemble des caractères de G , irréductibles sur $\mathbb{Q}_\ell$ et dont le noyau contient U . Convenons également de considérer $\mathcal{H}_K$ comme un sous-groupe de $\mathcal{H}_L$. Nous constatons alors que la décomposition du ℓ-groupe des classes de tout corps intermédiaire K galoisien sur k , pourra s'écrire : $\mathcal{H}_K = \prod_\phi \mathcal{H}_L^\phi$, ce produit étant direct et étendu aux caractères irréductibles sur $\mathbb{Q}_\ell$ de $G/U = \mathrm{Gal}(K/k)$.

Groupe des ℓ-unités . On désigne encore par K un corps intermédiaire entre L et k , galoisien sur k et par U le groupe de Galois : $\mathrm{Gal}(L/K)$. Soit E_K le groupe des unités de K . Posons : $\mathcal{E}_K = E_K / E_K^\ell$. Nous appelerons $\mathcal{E}_K$ le groupe des ℓ-unités de K . Nous désignerons par i l'application de $\mathcal{E}_K$ dans $\mathcal{E}_L$ déduite de l'injection canonique de E_K dans E_L .

Proposition II b . L'application i est un homomorphisme injectif . Son image $i(\mathcal{E}_K)$ est l'ensemble des éléments de $\mathcal{E}_L$ invariants par $U = \mathrm{Gal}(L/K)$. Si ϕ_1 est un caractère de G/U irréductible sur

$\mathbb{Q}_\ell$ et si $\phi = \phi_1 \circ \Pi$, alors $i(\mathcal{E}_K^{\phi_1}) = \mathcal{E}_L^{\phi}$.

La démonstration de cette proposition est semblable à celle de la proposition précédente .

Deuxième définition de χ^*. Soit T le sous-groupe de torsion de E_L. Considérons le quotient T/T^ℓ . C'est un $\mathbb{F}_\ell[G]$-module . Il n'est pas réduit à 1 si et seulement si L contient une racine primitive $\ell^{\text{ème}}$ de 1 . Supposons que cette condition soit vérifiée et appelons ζ une racine de 1 appartenant à L , d'ordre une puissance de ℓ la plus grande possible : ℓ^n . La classe de ζ modulo T^ℓ engendre donc T/T^ℓ . Introduisons l'application χ^* définie au paragraphe précédent comme un homomorphisme de G dans $(\mathbb{Z}/\ell^n\mathbb{Z})^*$ tel que : $\zeta^\sigma = \zeta^{\chi^*(\sigma)}$. Considérons le résidu modulo ℓ de χ^*, c'est-à-dire l'application de G dans $(\mathbb{Z}/\ell\mathbb{Z})^*$ qui associe à σ la classe de $\chi^*(\sigma)$ modulo ℓ. Il s'agit du caractère du $\mathbb{F}_\ell[G]$-module T/T^ℓ . Nous appelerons ce caractére le miroir de L/k et nous le noterons encore χ^*. Par la suite , comme nous l'avons dit au début de ce paragraphe , nous désignerons aussi par χ^* le caractère de G sur $\mathbb{Q}_\ell$ dont il est le résidu modulo ℓ . En ce sens , χ^* est l'homomorphisme de G dans le groupe multiplicatif de $\mathbb{Z}_\ell$ tel que $\zeta^\sigma = \zeta^{\chi^*(\sigma)}$ pour tout σ de G .

Nous allons essayer maintenant d'exprimer le caractère du $\mathbb{F}_\ell[G]$-module $\mathcal{E}_L$.

Définition de ψ_o. Désignons par σ_∞ la conjugaison complexe de $\mathbb{C}$. Soient $\Pi_1, \ldots \Pi_s$ les plongements réels de L dans $\mathbb{C}$ et $\Pi_{1+s}, \ldots \Pi_{t+s}$, $\overline{\Pi}_{1+s}, \ldots \overline{\Pi}_{t+s}$ les plongements complexes de L dans $\mathbb{C}$. Convenons que $\overline{\Pi}$ est le conjugué de Π , c'est-à-dire que $\overline{\Pi} = \Pi\sigma_\infty$. Nous définissons ψ_o de la façon suivante : si τ appartient à G et différe de 1 , alors $\psi_o(\tau)$ est le demi nombre de plongements complexes Π de L dans $\mathbb{C}$ tels que $\overline{\Pi} = \tau\Pi$. D'autre part , on posera $\psi_o(1) = s+t$.

Cas particulier . Supposons un instant $L/\mathbb{Q}$ galoisienne . Supposons L plongé dans $\mathbb{C}$ et soit $L_o = L \cap \mathbb{R}$ et $H_o = \mathrm{Gal}(L/L_o)$. Le groupe H_o

possède donc 1 ou 2 éléments . On peut alors vérifier que l'application ψ_o définie ci-dessus est la restriction à G du caractère de $Gal(L/\mathbb{Q})$ induit par le caractère principal de H_o .

Théorème II . Soit L/k une extension finie galoisienne , de groupe de Galois G . Soit ℓ un nombre premier ne divisant pas $[L:k]$. Soit $\mathcal{E}_L$ le groupe des ℓ-unités de L , c'est-à-dire : $\mathcal{E}_L = E_L / E_L^{\ell}$. Notons 1 le caractère unité de G . Si L contient une racine primitive $\ell^{ème}$ de l'unité , alors le caractère du $\mathbb{F}_\ell[G]$-module $\mathcal{E}_L$ est $\psi_L = \chi^* + \psi_o - 1$. Si L ne contient pas de racine primitive $\ell^{ème}$ de l'unité , le caractère de $\mathcal{E}_L$ est $\psi_L = \psi_o - 1$.

Corollaire . Soit ϕ un caractère de G , irréductible sur $\mathbb{Q}_\ell$. Soit χ le caractère absolument irréductible dont ϕ est issu . Le nombre de modules simples de caractères ϕ dont $\mathcal{E}_L$ est produit direct est : $\dim_\phi \mathcal{E}_L = (1/|G|) \sum_{\sigma \in G} \chi(\sigma^{-1}) \psi_L(\sigma)$.

Démonstration . Soit $\mathcal{L} : E_L \longrightarrow \mathbb{R}^{t+s}$
$\varepsilon \longrightarrow (\mathrm{Log}|\varepsilon^{\pi_i}|)_{1 \leq i \leq s+t}$

le plongement canonique de E_L dans $\mathbb{R}^{s+t}$. Rappelons que $\mathcal{L}(E_L)$ est un sous-groupe discret de l'hyperplan de $\mathbb{R}^{s+t}$ d'équation : $\sum_{1 \leq i \leq s} x_i + 2 \sum_{1 \leq i \leq t} x_{s+i} = 0$. Définissons sur $\mathbb{R}^{s+t}$ une structure de G-module de la façon suivante : Si τ appartient à G , soit j_τ l'application de l'ensemble des s+t premiers nombres entiers dans lui-même , définie par $\tau\pi_i = \pi_{j_\tau(i)}$ ou $\overline{\pi}_{j_\tau(i)}$. Soit $(x_i)_{1 \leq i \leq s+t}$ un élément de $\mathbb{R}^{s+t}$. Faisons opérer (à droite) G sur $\mathbb{R}^{s+t}$ en posant : $(x_i).\tau_{1 \leq i \leq s+t} = (x_{j_\tau(i)})_{1 \leq i \leq s+t}$. Le plongement $\mathcal{L}$ devient alors un homomorphisme de G-modules.

Soit D le sous-ensemble de $\mathbb{R}^{s+t}$ ainsi défini : $D = \{(\lambda, \ldots, \lambda) ; \lambda \in \mathbb{Z}\}$. La somme directe $\mathcal{L}(E_L) \oplus D$ est un sous-

groupe discret de $\mathbb{R}^{s+t}$. Il s'en suit , qu'une $\mathbb{Z}$-base de $\mathcal{L}(E_L) \oplus D$ sera une $\mathbb{R}$-base de $\mathbb{R}^{s+t}$. Si τ appartient à G , soit A_τ la matrice de l'application de $\mathcal{L}(E_L) \oplus D$ dans lui-même qui associe à $(x_i)_{1 \leq i \leq s+t}$, $(x_i).\tau_{1 \leq i \leq s+t}$. L'application qui associe à τ , la trace de A_τ est le caractère du $\mathbb{Q}[G]$-module $(\mathcal{L}(E_L) \oplus D).\mathbb{Q}$, c'est-à-dire du $\mathbb{Q}[G]$-module déduit de $\mathcal{L}(E_L) \oplus D$ par extension de l'anneau des scalaires à $\mathbb{Q}[G]$. Le résidu modulo ℓ de cette application sera le caractère du $\mathbb{F}_\ell[G]$-module $\mathcal{L}(E_L) \oplus D \,/\, \ell(\mathcal{L}(E_L) \oplus D)$.

Pour calculer $Tr(A_\tau)$, il suffit de chercher comment A_τ transforme la base canonique de $\mathbb{R}^{s+t}$. On obtiendra : $Tr(A_1) = s+t$, Si τ différe de 1 , la trace de A_τ est le nombre des entiers i compris entre s+1 et s+t tels que $j(i) = i$. L'application : $\tau \longrightarrow Tr(A_\tau)$, est donc égale à ψ_0.

Comme G agit trivialement sur D , on en déduit que $\psi_0 - 1$ est le caractère de $\mathcal{L}(E_L).\mathbb{Q}$, c'et-à-dire du $\mathbb{Q}[G]$-module déduit de $\mathcal{L}(E_L)$ par extension de l'anneau des scalaires à $\mathbb{Q}[G]$. Le résidu modulo ℓ de $\psi_0 - 1$ sera le caractère du $\mathbb{F}_\ell[G]$-module $\mathcal{L}(E_L) / \ell\mathcal{L}(E_L)$. De plus , le noyau de $\mathcal{L}$ est le sous-groupe de torsion T de E_L et $\mathcal{L}(E_L) / \ell\mathcal{L}(E_L)$ est quotient de $E_L / E_L^\ell = \mathcal{C}_L$ par T / T^ℓ . Il s'en suit , que le caractère de $\mathcal{C}_L$, ψ_L , est obtenu en ajoutant à $\psi_0 - 1$, le caractère de T / T^ℓ. Si ce groupe est réduit à 1 , c'est-à-dire si L ne contient pas de racine primitive $\ell^{\text{ème}}$ de 1 , son caractère est nul ; sinon , il s'agit du miroir : χ^*.

Le corollaire s'en déduit . En effet le produit scalaire de χ et ψ_L : $(1/|G|) \sum_{\sigma \in G} \chi(\sigma^{-1})\psi_L(\sigma)$ mesure le nombre de modules simples de caractères ϕ dont $\mathcal{C}_L$ est produit direct .

III

Enoncé du Spiegelungssatz .

Nous désignerons toujours par L/k une extension finie galoisienne de corps de nombres , par G son groupe de Galois , par ℓ un nombre premier .

Hypothèses . On suppose que L contient une racine primitive ζ d'ordre ℓ^n de 1 et que $[L:k]$ est premier à ℓ.

Définitions . Rappelons d'abord que χ^*, appelé le miroir de L/k , est le caractère de G sur $\mathbb{Q}_\ell$ défini par $\zeta^\sigma = \zeta^{\chi^*(\sigma)}$ pour tout σ de G . Si ϕ est un caractère irréductible de G sur $\mathbb{Q}_\ell$, nous poserons : $\bar{\phi}(\tau) = \phi(\tau^{-1})\,\chi^*(\tau)$, pour tout τ de G . En introduisant la représentation dont ϕ est le caractère , on vérifie que $\bar{\phi}$ est le caractère d'une représentation linéaire de G sur $\mathbb{Q}_\ell$. Ce caractère $\bar{\phi}$ est aussi irréductible sur $\mathbb{Q}_\ell$. On l'appelera le " reflet " de ϕ. (Spiegelbild) . L'application $\phi \to \bar{\phi}$ est une involution de l'ensemble des caractères irréductibles de G sur $\mathbb{Q}_\ell$; c'est-à-dire : $\bar{\bar{\phi}} = \phi$.

Soit E (resp. E°) le groupe des unités de L (resp. des unités ℓ-primaires de L) . On pose $\mathcal{E} = E/E^\ell$ et $\mathcal{E}^\circ = E^\circ/E^\ell$. On appelle ces groupes : groupes des ℓ-unités de L et groupes des ℓ-unités primaires de L .

Les symboles $\dim_{\phi^m}$ et $\dim_\phi$ ont été définis au paragraphe précédent .

Théorème III Soient L/k une extension finie galoisienne de corps de nombres et G son groupe de Galois . Soit ℓ un nombre premier . On suppose que L contient une racine $\ell^{n\text{ ème}}$ de 1 et que ℓ ne divise pas le degré $[L:k]$. Pour toute puissance de ℓ, notée m , et inférieure à ℓ^n , et pour tout caractère ϕ de G irréductible sur $\mathbb{Q}_\ell$, les ϕ et $\bar{\phi}$-composantes du ℓ-groupe des classes $\mathcal{H}$ de L et la ϕ-composante du groupe des ℓ-unités primaires de L vérifient :

$$\dim_{\bar{\phi}^m} \mathcal{H} - \dim_{\phi^m} \mathcal{H} \leqslant \dim_\phi \mathcal{E}^\circ .$$

Remarque . Comme $\mathcal{E}^\circ$ s'injecte dans $\mathcal{E}$, nous avons aussi : $\dim_\phi \mathcal{E}^\circ \leq \dim_\phi \mathcal{E}$. Cette dernière valeur est donnée par le théorème II.

IV

Démonstration du théorème III .

Lemme IV . Soit H un $\mathbb{Z}_\ell[G]$-module et $H^\wedge$ son dual , c'est-à-dire le groupe des homomorphismes de H dans $\mathbb{C}^*$. Munissons $H^\wedge$ de la structure de $\mathbb{Z}_\ell[G]$-module ainsi définie : $\gamma^\tau(x) = \gamma(x^\tau)$, pour tout τ de G et tout x de H . Pour tout caractère ϕ de G irréductible sur $\mathbb{Q}_\ell$, les modules $(H^\phi)^\wedge$ et $(H^\wedge)^\phi$ sont canoniquement isomorphes .

Démontrons ce lemme . Considérons l'application de $(H^\wedge)^\phi$ dans $(H^\phi)^\wedge$ qui associe à γ , appartenant à $(H^\wedge)^\phi$, sa restriction à H^ϕ. C'est un homomorphisme . Montrons qu'il est injectif . Supposons que la restriction de γ à H^ϕ soit égale à 1 . Pour tout x de H et pour tout caractère ψ de G irréductible sur $\mathbb{Q}_\ell$ et différent de ϕ, nous avons : $\gamma(x^{1_\psi}) = \gamma(x^{1_\phi 1_\psi}) = \gamma(1) = 1$. D'où l'on déduit que : $\gamma(x^{1_\psi}) = 1$ pour tout caractère ψ ; d'où finalement : $\gamma = 1$. Pour montrer que cet homomorphisme est surjectif , considérons un élément δ de $(H^\phi)^\wedge$. Comme H est égal au produit direct : $H = \prod H^\psi$, ψ parcourant l'ensemble des caractères irréductibles de G sur $\mathbb{Q}_\ell$, il est possible d'obtenir un prolongement γ de δ à H tel que la restriction de γ à H^ψ , pour tout ψ différent de ϕ, soit égale à 1 .

Venons en à la démonstration proprement dite du théorème III. Désignons par M/L la ℓ-extension abélienne non ramifiée maximale de L . Pour tout m, puissance de ℓ inférieure à ℓ^m , désignons par M_m le corps intermédiaire entre M et L maximal tel que M_m/L soit d'exposant divisant m . L'extension M_m/L est une extension de Kummer et l'on désigne par W_m son radical; c'est à-dire :

$W_m = \{ w \; ; \; w \in M_m \; ; \; w^m \in L^* \}$. (On a donc : $M_1 = L$ et $W_1 = L^*$).

Munissons W_m/L^* , $\mathrm{Gal}(M_m/L)$ et $\mathrm{Gal}(M_m/L)^\wedge$ des structures de G-modules définies au paragraphe I . Rappelons que $\mathcal{H}$ et

$Gal(M/L)$ sont isomorphes (en tant que G-modules) par l'isomorphisme de réciprocité du corps des classes . Les groupes $Gal(M/M_m)$ et $Gal(M/M_{m/\ell})$ correspondent dans cet isomorphisme à $\mathcal{H}^m$ et $\mathcal{H}^{m/\ell}$. Par restriction et passage au quotient , on en déduit l'existence d'un isomorphisme de G-modules entre : $Gal(M_m/M_{m/\ell})$ et $\mathcal{H}^{m/\ell}/\mathcal{H}^m$. D'où l'égalité :

$$\dim_{\overline{\phi}_m} \mathcal{H} = \dim_{\overline{\phi}} \mathcal{H}^{m/\ell}/\mathcal{H}^m = \dim_{\overline{\phi}} Gal(M_m/M_{m/\ell}) .$$

D'autre part , $W_{m/\ell}/L^*$ est un sous-G-module de W_m/L^* et nous confondrons le quotient $(W_m/L^*)/(W_{m/\ell}/L^*)$ avec $W_m/W_{m/\ell}$ qui lui est canoniquement isomorphe . L'isomorphisme de la théorie de Kummer α_m : $W_m/L^* \cong Gal(M_m/L)\hat{}$ a pour restriction à $W_{m/\ell}/L^*$ l'isomorphisme $\alpha_{m/\ell}$: $W_{m/\ell}/L^* \cong Gal(M_{m/\ell}/L)\hat{}$.

En effectuant le quotient , on obtient un isomorphisme de groupes :

$$\beta_m : W_m/W_{m/\ell} \cong Gal(M_m/M_{m/\ell})\hat{} .$$

Nous avons vu (Théorème I) que la relation du miroir était :

$$(\alpha_m(wL^*))^{\tau} = \alpha_m((wL^*)^{\chi^*(\tau)\tau^{-1}}) .$$

Maintenant , ℓ ne divise pas l'ordre de G et on en déduit :

$$(\alpha_m(wL^*))^{1\phi} = \alpha_m((wL^*)^{1\overline{\phi}}) .$$

En passant au quotient , on obtient :

$$(\beta_m(wW_{m/\ell}))^{1\phi} = \beta_m((wW_{m/\ell})^{1\overline{\phi}}) , \text{ pour tout } w \text{ de } W_m .$$

Dans l'isomorphisme β_m , $Gal(M_m/M_{m/\ell})\hat{}^{\overline{\phi}}$ correspond donc à $(W_m/W_{m/\ell})^{\phi}$. D'après le lemme IV , $Gal(M_m/M_{m/\ell})\hat{}^{\overline{\phi}}$ est un groupe isomorphe à $Gal(M_m/M_{m/\ell})^{\overline{\phi}\wedge}$. Nous aurons donc :

$\dim_{\ell} Gal(M_m/M_{m/\ell})^{\overline{\phi}} = \dim_{\ell}(W_m/W_{m/\ell})^{\phi}$. Comme $\phi(1) = \overline{\phi}(1)$, nous en déduisons : $\dim_{\overline{\phi}} Gal(M_m/M_{m/\ell}) = \dim_{\phi} W_m/W_{m/\ell}$. Nous avons démontré :

Proposition IV a . Les quantités : $\dim_{\overline{\phi}_m} \mathcal{H}$ et $\dim_{\phi} W_m/W_{m/\ell}$ sont égales .

Définitions des applications θ_m et ψ_m. Notons $\mathcal{H}^{(m)}$ l'ensemble des éléments de $\mathcal{H}$ dont la puissance $m^{ème}$ est égale à 1. C'est-à-dire : $\mathcal{H}^{(m)} = \{h ; h \in \mathcal{H} ; h^m = 1\}$. Notons A_L l'anneau des entiers de L. Si w appartient à W_m, sa puissance $m^{ème}$ appartient à L et engendre un idéal qui est une puissance $m^{ème}$ d'un idéal $\mathfrak{a}$ de L. On a donc : $w^m A_L = \mathfrak{a}^m$. La classe de l'idéal $\mathfrak{a}$ (notée $Cl(\mathfrak{a})$) est un élément de $\mathcal{H}^{(m)}$. En associant à $wW_{m/\ell}$ la classe de $Cl(\mathfrak{a})$ modulo $\mathcal{H}^{(m/\ell)}$, on définit une application :

$$\theta_m : W_m/W_{m/\ell} \longrightarrow \mathcal{H}^{(m)} / \mathcal{H}^{(m/\ell)} .$$

Il s'agit d'un homomorphisme de G-modules.

Soit $wW_{m/\ell}$ un élément du noyau de θ_m. Si $w^m A_L = \mathfrak{a}^m$, il existe donc un élément $\mathfrak{a}$ de L tel que $\mathfrak{a}^{m/\ell} = \mathfrak{a} A_L$. D'où $w^m A_L = \mathfrak{a}^\ell A_L$ et il existe une unité ε de L telle que $w^m = \mathfrak{a}^\ell \varepsilon$. L'extension $L(\sqrt[\ell]{\varepsilon})/L$ est une sous-extension de M_m/L et elle est donc non ramifiée. L'unité ε est donc ℓ-primaire et appartient à E°. Soit

$$\psi_m : \operatorname{Ker} \theta_m \longrightarrow \mathcal{E}^\circ$$

l'application de $\operatorname{Ker} \theta_m$ dans $E^\circ/E^\ell = \mathcal{E}^\circ$ qui associe à $w^m W_{m/\ell}$ la classe de ε modulo E^ℓ. On vérifie que ψ_m est un homomorphisme de G-modules. De plus ψ_m est injectif. En effet si ε appartient à E^ℓ, w^m appartient à L^ℓ et $w^{m/\ell}$ appartient à L. D'où w appartient à $W_{m/\ell}$. Nous avons démontré :

Proposition IV b. Il existe un homomorphisme de G-modules θ_m de $W_m/W_{m/\ell}$ dans $\mathcal{H}^{(m)}/\mathcal{H}^{(m/\ell)}$. Il existe un homomorphisme de G-modules, injectif ψ_m de $\operatorname{Ker} \theta_m$ dans $\mathcal{E}^\circ$. On en déduit les inégalités :

$$\dim_\phi W_m/W_{m/\ell} - \dim_\phi \mathcal{H}^{(m)}/\mathcal{H}^{(m/\ell)} \leq \dim_\phi \operatorname{Ker} \theta_m \leq \dim_\phi \mathcal{E}^\circ .$$

Pour déduire le théorème III de ces deux propositions, il reste à voir que $\dim_\phi \mathcal{H}^{(m)}/\mathcal{H}^{(m/\ell)} = \dim_{\phi^m} \mathcal{H}$. Or nous avons d'après le lemme II : $(\mathcal{H}^{m/\ell}/\mathcal{H}^m)^\phi \cong \mathcal{H}^{\phi m/\ell}/\mathcal{H}^{\phi m}$. Ce groupe est isomorphe en tant que $\mathbb{F}_\ell$-module à $\mathcal{H}^{\phi(m)}/\mathcal{H}^{\phi(m/\ell)}$ et celui-ci est isomorphe ,

d'après le lemme II à : $(\mathcal{H}^{(m)} / \mathcal{H}^{(m/\ell)})^{\phi}$. Nous avons donc : $\dim_{\ell} (\mathcal{H}^{m/\ell} / \mathcal{H}^{m})^{\phi} = \dim_{\ell} (\mathcal{H}^{(m)} / \mathcal{H}^{(m/\ell)})^{\phi}$. En multipliant par $\phi(1)$, nous obtenons : $\dim_{\phi} \mathcal{H}^{m/\ell} / \mathcal{H}^{m} = \dim_{\phi} \mathcal{H}^{(m)} / \mathcal{H}^{(m/\ell)}$.

V

Exemples .

1. Rappels concernant les classes réelles et les classes relatives .

Soit L/k une extension finie de corps de nombres ; soient $\tilde{L}$ et $\tilde{k}$ les corps des classes de Hilbert de L et k , et soient H_k et H_L les groupes des classes d'idéaux de k et L . Désignons par N l'application de H_L dans H_k déduite de la norme dans l'extension L/k .

Proposition V a . Dans l'isomorphisme de réciprocité liant H_k et $\mathrm{Gal}(\tilde{k}/k)$, l'image de H_L par N correspond à $\mathrm{Gal}(\tilde{k}/L\cap\tilde{k})$. Dans l'isomorphisme de réciprocité liant H_L et $\mathrm{Gal}(\tilde{L}/L)$ le noyau de N correspond à $\mathrm{Gal}(\tilde{L}/L\tilde{k})$.

Démonstration. Si $\mathfrak{b}$ est un idéal de L , le symbole d'Artin : $(N_{L/k}(\mathfrak{b}), \tilde{k}/k)$ est la restriction à $\tilde{k}$ de $(\mathfrak{b}, L\tilde{k}/L)$ et il laisse invariant $\tilde{k}\cap L$. Donc il appartient à $\mathrm{Gal}(\tilde{k}/\tilde{k}\cap L)$. Réciproquement , soit σ un élément de $\mathrm{Gal}(\tilde{k}/\tilde{k}\cap L)$. Cet automorphisme est la restriction à $\tilde{k}$ d'un automorphisme τ de $L\tilde{k}/L$ et il existe un idéal $\mathfrak{b}$ de L tel que $\tau = (\mathfrak{b}, L\tilde{k}/L)$; d'où : $\sigma = (N_{L/k}(\mathfrak{b}), \tilde{k}/k)$. La deuxième assertion se démontre de la même façon .

Définitions . Soit L un corps de nombres plongé dans $\mathbb{C}$. Posons $L_o = L\cap\mathbb{R}$. On appelle groupe des classes réelles de L , le groupe des classes de L_o et on appelle groupe des classes relatives de L , le noyau de l'application N de H_L dans H_{L_o} déduite de la norme relative à L/L_o . (Ces notions dépendent donc du plongement de L dans $\mathbb{C}$ choisi . Si $L/\mathbb{Q}$ est abélienne , L_o ne dépend plus de ce plongement)

On déduit de la proposition ci-dessus que l'application N est surjective . En effet , puisqu'aucune place de L ne peut se ramifier dans le corps des classes de Hilbert $\tilde{L}_o$ de L_o , l'intersection $\tilde{L}_o \cap L$ sera égale à L_o . Il s'en suit que $N(H_L) = H_{L_o}$. Nous avons démontré :

Corollaire . Le groupe des classes réelles de L est isomorphe au quotient du groupe des classes de L par le groupe des classes relatives de L .

2. Comparaison du ℓ-groupe des classes relatives et du ℓ-groupe des classes réelles de L, lorsque L contient une racine $\ell^{\text{ème}}$ de 1 et lorsque $[L:L_o] = 2$.

Désignons encore par L un corps de nombres plongé dans $\mathbb{C}$ et par L_o l'intersection : $L_o = L \cap \mathbb{R}$. L'extension L/L_o est galoisienne si et seulement si $[L:L_o] \leqslant 2$. En effet , si L/L_o est galoisienne , de degré différent de 1 , la restriction σ_∞ de la conjugaison de $\mathbb{C}$ à L appartient au goupe de Galois de L/L_o . Le corps fixe de σ_∞ sera donc L_o et $[L:L_o] = 2$.

Supposons désormais , que L (et son plongement dans $\mathbb{C}$) vérifie cette condition . Soit ℓ un nombre premier impair et soit $\mathcal{H}$ (resp. $\mathcal{H}_o$, $\mathcal{H}^*$) le ℓ-Sylow du groupe des classes de L (resp. du groupe des classes réelles de L , du groupe des classes relatives de L) . D'après le corollaire énoncé ci-dessus , nous avons : $\mathcal{H}_o \cong \mathcal{H} / \mathcal{H}^*$. Mais nous pouvons énoncer un résultat plus précis: $\mathcal{H}$ est produit direct de $\mathcal{H}_o$ et $\mathcal{H}^*$.

En effet , supposons $[L:L_o] = 2$.(Sinon , c'est clair) . Posons : $L_o = k$, $G = \mathrm{Gal}(L/k) = \{1 , \sigma_\infty\}$. Le groupe G possède deux caractères irréductibles sur $\mathbb{Q}_\ell$: 1 et ϕ donnés par le tableau:

	1	σ_∞
1	1	1
ϕ	1	-1

Les idempotents correspondants sont : $1_1 = \frac{1}{2}(1+\sigma_\infty)$ et $1_\phi = \frac{1}{2}(1-\sigma_\infty)$.

D'après la proposition II a (appliquée avec $K = k = L_o$) le groupe $\mathcal{H}^1$ est isomorphe par l'injection j de $\mathcal{H}_o$ dans $\mathcal{H}$, au ℓ-groupe des classes réelles $\mathcal{H}_o$ de L . On vérifie aussi , que $\mathcal{H}^\phi$ coincide avec le ℓ-groupe $\mathcal{H}^*$ des classes relatives de L . Enfin , il est clair que $\mathcal{H}$ est produit direct de $\mathcal{H}^1$ et $\mathcal{H}^\phi$.

La proposition suivante a été obtenue par L. Bouvier dans [2] sous des hypothèses un peu plus restrictives :

Proposition V b . Soit L un corps de nombres plongé dans $\mathbb{C}$ et soit $L_o = L \cap \mathbb{R}$. On suppose que $[L : L_o] = 2$. Si ℓ est un nombre premier impair , soit n le plus grand entier tel que L contienne une racine $\ell^{n\text{ ème}}$ de 1 , notée ζ. Supposons $n \neq 0$. (C'est -à-dire : supposons que L contienne une racine primitive $\ell^{\text{ème}}$ de 1) Pour toute puissance de ℓ , notée m et inférieure à ℓ^n , les m-rangs des ℓ-groupes des classes réelles et relatives : $\mathcal{H}_o$ et $\mathcal{H}^*$ de L , vérifient les inégalités :

$$\dim_m \mathcal{H}^* - \dim_m \mathcal{H}_o \leqslant \dim_{\mathbb{Z}} E_L ,$$

$$\dim_m \mathcal{H}_o - \dim_m \mathcal{H}^* \leqslant \dim_{\mathbb{Z}} E_L - \dim_{\mathbb{Z}} E_{L_o} + 1 .$$

Si de plus , ζ n'est pas une unité ℓ-primaire de L , on a alors plus précisément :

$$\dim_m \mathcal{H}_o - \dim_m \mathcal{H}^* \leqslant \dim_{\mathbb{Z}} E_L - \dim_{\mathbb{Z}} E_{L_o} .$$

Les quantités $\dim_{\mathbb{Z}} E_L$ et $\dim_{\mathbb{Z}} E_{L_o}$ sont les dimensions des $\mathbb{Z}$-modules libres , quotients des groupes des unités E_L et E_{L_o} de L et L_o par leurs sous-groupes de torsion.

Démonstration . Appliquons le théorème III à L et $k = L_o$. Comme $\zeta^{\sigma_\infty} = \zeta^{-1}$, le caractère miroir de L/k est ϕ . De plus 1 et ϕ sont reflets l'un de l'autre . Nous avons donc :

$$\dim_{1m} \mathcal{B} - \dim_{\phi m} \mathcal{B} \leqslant \dim_\phi \mathcal{E}^\circ \leqslant \dim_\phi \mathcal{E} ,$$

$$\dim_{\phi m} \mathcal{B} - \dim_{1m} \mathcal{B} \leqslant \dim_1 \mathcal{E}^\circ \leqslant \dim_1 \mathcal{E} .$$

Pour calculer $\dim_1 \mathcal{E}$ et $\dim_\phi \mathcal{E}$, on peut appliquer le théorème II . Mais dans ce cas particulier, il suffit d'utiliser la proposition IIb. On a un isomorphisme : $\mathcal{E}^1 \simeq \mathcal{E}_{L_o}$ et $\mathcal{E}$ est produit direct : $\mathcal{E} = \mathcal{E}^1 \mathcal{E}^\phi$. Nous

aurons donc: $\dim_1 \mathcal{E} = \dim_\ell \mathcal{E}^1 = \dim_\ell \mathcal{E}_{L_o} = \dim_{\mathbb{Z}} E_{L_o}$, puisque L_o ne peut contenir de racine $\ell^{\text{ème}}$ de 1 . D'autre part, puisque L contient une racine $\ell^{\text{ème}}$ de 1 : $\dim_\ell \mathcal{E} = \dim_{\mathbb{Z}} E_L + 1$. D'où:

$\dim_\phi \mathcal{E} = \dim_\ell \mathcal{E} - \dim_\ell \mathcal{E}^1 = \dim_{\mathbb{Z}} E_L - \dim_{\mathbb{Z}} E_{L_o} + 1$.

Supposons maintenant que ζ ne soit pas une unité ℓ-primaire de L , c'est-à-dire que $L(\sqrt[\ell]{\zeta})/L$ soit ramifiée . Considérons le $\mathbb{F}_\ell[G]$-module $\mathcal{E}/\mathcal{E}^\circ$, isomorphe à E/E° . Le sous-module de E/E° engendré par la classe de ζ modulo E° n'est pas réduit à 1 et a pour caractère : $\chi^* = \phi$. Il s'en suit que $\mathcal{E}/\mathcal{E}^\circ$ contient un $\mathbb{F}_\ell[G]$-module simple de caractère $\chi^* = \phi$. Comme le caractère de $\mathcal{E}$ est $\psi_L = \chi^* + \psi_o - 1$, le caractère de $\mathcal{E}^\circ$ est " au plus " $\psi_o - 1$ et on a : $\dim_\phi \mathcal{E}^\circ \leqslant \dim_\phi \mathcal{E} - 1$.

Remarques . La dernière hypothèse : " ζ n'est pas une unité ℓ-primaire de L " est vérifiée en particulier dans le cas où L est le $\ell^{n\ \text{ème}}$ corps cyclotomique . Par exemple , pour n = 1 , nous obtenons :
Si $\mathcal{X}_o$ et $\mathcal{H}^*$ sont les ℓ-groupes des classes réelles et relatives de $\mathbb{Q}^{(\ell)}$, la différence des ℓ-rangs de ces groupes est bornée par :

$$0 \leqslant \dim_\ell \mathcal{H}^* - \dim_\ell \mathcal{H}_o \leqslant (\ell - 3)/2 .$$

Ces inégalités ont été obtenues par Hecke ; [5] .

Kummer avait déjà montré que si ℓ divise le nombre de classes réelles de $\mathbb{Q}^{(\ell)}$, alors ℓ divise également le nombre de classes relatives de $\mathbb{Q}^{(\ell)}$. Ce résultat lui permettait de caractériser les nombres premiers ℓ divisant le nombre de classes de $\mathbb{Q}^{(\ell)}$ (nombres premiers irréguliers) au moyen des nombres de Bernouilli . Il l'obtenait à l'aide des formules analytiques ; ([1] Ch 5 § 6) .

Signalons encore l'existence d'une autre " propriété de Kummer " : ℓ étant toujours un nombre premier impair et n un entier quelconque , si le nombre de classes réelles du $\ell^{n\ \text{ème}}$ corps cyclotomique est pair , alors le nombre de classes relatives de ce même corps est également pair . Ceci peut se démontrer facilement à l'aide de la formule des classes ambiges appliquée à l'extension : $\mathbb{Q}^{(\ell^n)} / \mathbb{Q}_o^{(\ell^n)}$. Toutefois , pour étudier ce type de question , les méthodes utilisant les formules analytiques paraissent plus précises . On peut voir par exemple : [4] § 37 et 38 .

3. Comparaison des 3-groupes des classes de $k(\sqrt{d})$ et $k(\sqrt{-3d})$.

Proposition V c. Soit k un corps de nombres ne contenant pas $\sqrt{-3}$. Soit d un élément de k tel que ni $\sqrt{d}$, ni $\sqrt{-3d}$ n'appartiennent à k. Posons $K = k(\sqrt{d})$, $\overline{K} = k(\sqrt{-3d})$ et $k' = k(\sqrt{-3})$. Soient $\mathcal{H}_K$, $\mathcal{H}_{\overline{K}}$, $\mathcal{H}_{k'}$, $\mathcal{H}_k$ les 3-groupes des classes d'idéaux de K, $\overline{K}$, k' et k. Soient j, $\bar{j}$, j' les injections canoniques de $\mathcal{H}_k$ dans $\mathcal{H}_K$, $\mathcal{H}_{\overline{K}}$, $\mathcal{H}_{k'}$. Pour toute puissance de 3, notée m et telle que le sous-corps réel maximal du $m^{\text{ème}}$ corps cyclotomique soit contenu dans k, on a les inégalités :

(1) $\dim_m \mathcal{H}_{\overline{K}}/\bar{j}(\mathcal{H}_k) - \dim_m \mathcal{H}_K/j(\mathcal{H}_k) \leqslant \dim_{\mathbb{Z}} E_K - \dim_{\mathbb{Z}} E_k$,

(2) $\dim_m \mathcal{H}_k - \dim_m \mathcal{H}_{k'}/j'(\mathcal{H}_k) \leqslant \dim_{\mathbb{Z}} E_{k'} - \dim_{\mathbb{Z}} E_k + 1$,

(3) $\dim_m \mathcal{H}_{k'}/j'(\mathcal{H}_k) - \dim_m \mathcal{H}_k \leqslant \dim_{\mathbb{Z}} E_k$.

Les quantités $\dim_{\mathbb{Z}} E_K$, $\dim_{\mathbb{Z}} E_{k'}$, $\dim_{\mathbb{Z}} E_k$ sont les dimensions des $\mathbb{Z}$-modules libres, quotients des groupes des unités : E_K, $E_{k'}$, E_k de K, k' et k par leurs sous-groupes de torsion.

Démonstration. Posons $L = k(\sqrt{d}, \sqrt{-3d})$ et $G = \mathrm{Gal}(L/k)$. Ce groupe est un groupe de Klein. Notons ses éléments de la façon suivante : $G = \{1, \sigma, \bar{\sigma}, \sigma\bar{\sigma}\}$ et supposons que σ invarie K et $\bar{\sigma}$ invarie $\overline{K}$. Soient $1, \phi, \bar{\phi}, \chi^*$ les caractères irréductibles de G sur $\mathbb{Q}_3$ définis par le tableau suivant :

	1	σ	$\bar{\sigma}$	$\sigma\bar{\sigma}$
1	1	1	1	1
χ^*	1	-1	-1	1
ϕ	1	1	-1	-1
$\bar{\phi}$	1	-1	1	-1

Soit n le plus grand entier tel que le sous-corps réel maximal $\mathbb{Q}_o^{(3^n)}$ du $3^{n\ \text{ème}}$ corps cyclotomique soit inclus dans k. Soit ζ une racine primitive $3^{n\ \text{ème}}$ de 1. Elle appartient à L. Le caractère miroir de L/k est χ^* et 1, χ^* d'une part, ϕ et $\bar{\phi}$ d'autre part, sont reflets l'un

de l'autre . Appliquons le théorème III à L/k , avec $\ell = 3$. On obtient les inégalités : ($\mathcal{H}$ et $\mathcal{E}$ désignentle groupe des ℓ-classes et le groupe des ℓ-unités de L)

$$\dim_{\bar{\phi}\,m} \mathcal{H} - \dim_{\phi m} \mathcal{H} \leqslant \dim_{\phi} \mathcal{E} ,$$
$$\dim_{1m} \mathcal{H} - \dim_{\chi^* m} \mathcal{H} \leqslant \dim_{\chi^*} \mathcal{E},$$
$$\dim_{\chi^* m} \mathcal{H} - \dim_{1m} \mathcal{H} \leqslant \dim_{1} \mathcal{E} ,$$

pour toute puissance de 3 notée m et inférieure à 3^n .

D'après la proposition II a nous avons $\mathcal{H}_K = \mathcal{H}^1 \mathcal{H}^{\phi}$,(en considérant $\mathcal{H}_K$ comme un sous-groupe de $\mathcal{H}$) et $\mathcal{H}^1 = j(\mathcal{H}_k)$ d'où : $\mathcal{H}^{\phi} \cong \mathcal{H}_K / j(\mathcal{H}_k)$ et $\dim_{\phi m} \mathcal{H} = \dim_m \mathcal{H}_K / j(\mathcal{H}_k)$. On interpréte de la même façon les quantités : $\dim_{\bar{\phi}\,m} \mathcal{H}$, $\dim_{1m} \mathcal{H}$, $\dim_{\chi^* m} \mathcal{H}$.

Soit i l'injection canonique de $\mathcal{E}_k$ dans $\mathcal{E}_K$. Considérons $\mathcal{E}_K$ comme un sous-groupe de $\mathcal{E}$, nous aurons $\mathcal{E}_K = \mathcal{E}^{\phi} \mathcal{E}^1$ et $\mathcal{E}^1 = i(\mathcal{E}_k)$ (proposition II b). Nous en déduisons $\mathcal{E}^{\phi} \cong \mathcal{E}_K / i(\mathcal{E}_k)$ et $\dim_{\phi} \mathcal{E} = \dim_3 \mathcal{E}^{\phi} = \dim_3 \mathcal{E}_K - \dim_3 \mathcal{E}_k$. Remarquons enfin que ni K , ni k ne contiennent de racine cubique de 1 . Il s'en suit que : $\dim_3 \mathcal{E}_K = \dim_{\mathbb{Z}} E_K$ et $\dim_3 \mathcal{E}_k = \dim_{\mathbb{Z}} E_k$. On a donc : $\dim_{\phi} \mathcal{E} = \dim_{\mathbb{Z}} E_K - \dim_{\mathbb{Z}} E_k$.

La quantité $\dim_{\chi^*} \mathcal{E}$ s'interpréte de la même façon . La seule différence est que k' contient les racines cubiques de 1 et : $\dim_3 \mathcal{E}_{k'} = \dim_{\mathbb{Z}} E_{k'} + 1$.

Remarques . De même qu'à la proposition précédente , on peut ajouter que si ζ n'est pas une unité 3-primaire de k' , alors le chiffre 1 apparaissant dans l'égalité (2) peut être remplacé par 0 .

Dans le cas particulier où $k = \mathbb{Q}$, les inégalités (2) et(3) deviennent triviales . Il reste , si $K = \mathbb{Q}(\sqrt{d})$ et $\bar{K} = \mathbb{Q}(\sqrt{-3d})$, avec d rationnel positif , les inégalités :

$$0 \leqslant \dim_3 \mathcal{H}_{\bar{K}} - \dim_3 \mathcal{H}_K \leqslant 1 .$$

Ce résultat est du à Scholtz ([8]) .

Bibliographie.

[1] Borevitch (Z.I.) et Chafarevitch (I.R.), Théorie des nombres , Gauthier-Villars , Paris , (1967).

[2] Bouvier (L.) , Généralisation d'une inégalité de Hecke sur les nombres de classes , Séminaire de Théorie des Nombres de Grenoble . (1969) .

[3] Curtis (C.W.) and Reiner (I.) , Representation theory of finite groups and associative algebras , Interscience Publishers, (1962).

[4] Hasse (H.) , Uber die Klassenzahl abelscher Zahlkörpern , Berlin , (1952) .

[5] Hecke (E.) , Uber nicht-reguläre Primzahlen und den Fermatschen Satz , Gött. Nachr. Math. Phys. Kl. (1910) 420-424 .

[6] Leopoldt (H.W.) Zur Struktur der ℓ-Klassengruppe galoisscher Zahlkörper , Journ. für die reine und ang. Math. 199 ,(1958).

[7] Oriat (B.) , Quelques caractères utiles à l'arithmétique , Publications Mathématiques de la Faculté de Besançon , (1974).

[8] Scholtz (A.) Uber die Beziehung der Klassenzahlen quadratischer Körper zueinander , Journ. für die reine und ang. Math. 166 , (1931) 201-203 .

[9] Serre (J.P.) , Représentations linéaires des groupes finis , Hermann , (1971) .