

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 ℓ^n ème de l'unité " . Le résultat obtenu (théorème III) a la forme suivante :

Soit ϕ un caractère de $G = \text{Gal}(L/k)$, irréductible sur \mathbb{Q}_ℓ et soit $\bar{\phi}$ 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}° des ℓ -unités primaires de L .

Nous obtenons les inégalités :

$$\dim_m \mathcal{H}^{\bar{\phi}} - \dim_m \mathcal{H}^\phi \leq \dim_\ell \mathcal{E}^{\circ\phi} ,$$

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 supposons 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 $m^{\text{ème}}$ 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 $\text{Gal}(M/L)$. Si u appartient à $\text{Gal}(M/L)$ la quantité $t^{-1}ut$ appartient à $\text{Gal}(M/L)$ et elle est indépendante du choix de t . En posant $u^\tau = t^{-1}ut$ on définit sur $\text{Gal}(M/L)$ une structure de G -module.

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

Considérons le groupe W/L^* . Si w appartient à W et si u appartient à $\text{Gal}(M/L)$, w^{u-1} est une racine $m^{\text{ème}}$ 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 $\text{Gal}(M/L)^\wedge$ ainsi défini : Si wL^* appartient à W/L^* , l'homomorphisme $\alpha(wL^*)$ de $\text{Gal}(M/L)$ dans L^* correspondant à wL^* est défini par : $\alpha(wL^*)(u) = w^{u-1}$, pour tout u de $\text{Gal}(M/L)$.

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

$m^{\text{ème}}$ de l'unité : \mathfrak{S} . 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 $\text{Gal}(M/L)^\wedge$ sont liées par la relation : $(\alpha(wL^*))^\tau = \alpha((wL^*)^{\chi^*(\tau)\tau^{-1}})$, pour tout w de W et tout τ de $\text{Gal}(M/L)$.

Leopoldt appelle cette relation : "Spiegelungsrelation".

Démonstration. Soit u un élément de $\text{Gal}(M/L)$. Les notations τ et t ont toujours le même sens. Nous avons, d'après 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 $m^{\text{ème}}$ de 1. Son image par τ est donc égale à sa puissance $\chi^*(\tau)^{\text{ème}}$ 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 hypothèse assure la semi-simplicité de l'algèbre $F_\ell[G]$.

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}_ℓ . (C'est la trace d'une représentation linéaire irréductible de G sur \mathbb{Q}_ℓ). Ce caractère ϕ est une application de G dans \mathbb{Z}_ℓ et comme ℓ ne divise pas l'ordre de G , son résidu modulo ℓ est

un caractère irréductible de G sur \mathbb{F}_ℓ . De plus, on obtient par ce moyen une bijection entre l'ensemble des caractères irréductibles de G sur \mathbb{Q}_ℓ et l'ensemble des caractères irréductibles de G sur \mathbb{F}_ℓ . ([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 :

$$1_\phi = (\chi(1) / |G|) \sum_{\sigma \in G} \phi(\sigma^{-1}) \sigma. \text{ Il s'agit donc d'un élément de } \mathbb{Z}_\ell[G].$$

Si H est un $\mathbb{Z}_\ell[G]$ -module noté multiplicativement, nous appellerons 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}_ℓ .

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 :

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

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_ℓ , \dim_m , \dim_ϕ , $\dim_{\phi m}$. 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}_ℓ -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 :

$$\dim_{\phi m} H = \dim_\phi H^{m/\ell} / H^m. \text{ On déduit du lemme ci-dessus la relation:}$$

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

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

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}_{ℓ} . 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'appellerons 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}_{ℓ} dont le noyau contient U et l'ensemble des caractères irréductibles de G/U sur \mathbb{Q}_{ℓ} . 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 $U = \text{Gal}(L/K)$. Si ϕ_1 est un caractère de G/U irréductible sur \mathbb{Q}_{ℓ} 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 $\text{Ker } j$. Il existe donc \mathfrak{a} dans L tel que : $\mathfrak{a}A_L = \mathfrak{a}A_L$, d'où :
 $\mathfrak{a}^{[L:K]} = N_{L/K}(\mathfrak{a})A_K$ et $\mathfrak{a}^{[L:K]}$ est principal. Or $\text{Cl}_K(\mathfrak{a})$ est

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

Soit \mathfrak{a} un idéal de L , dont la classe est invariante par U . On aura alors $N_{L/K}(\mathfrak{a}) A_L = \mathfrak{a}^{[L:K]}$. En utilisant une relation de Bezout entre $[L:K]$ et l'ordre de $\text{Cl}_L(\mathfrak{a})$, on obtient :

$\text{Cl}_L(\mathfrak{a}) = \text{Cl}_L(N_{L/K}(\mathfrak{a})^u A_L)$ et cela montre que $\text{Cl}_L(\mathfrak{a})$ appartient à $j(\mathcal{H}_K)$. Comme $\prod(1_\phi) = 1_{\phi_1}$, nous avons $\mathcal{H}_K^{1_{\phi_1}} = \mathcal{H}_K^{1_\phi}$ et $j(\mathcal{H}_K^{1_{\phi_1}}) = j(\mathcal{H}_K)^\phi \subset \mathcal{H}_L^\phi$. Réciproquement, si τ appartient à U , τ appartient à $\text{Ker } \phi$ et vérifie : $\tau 1_\phi = 1_\phi$. On en déduit que tout élément de \mathcal{H}_L^ϕ est invariant par U , ce qui démontre l'inclusion :

$$\mathcal{H}_L^\phi \subset j(\mathcal{H}_K^{1_{\phi_1}}).$$

Conséquence. Convenons d'identifier l'ensemble des caractères de G/U irréductibles sur \mathbb{Q}_ℓ à l'ensemble des caractères de G , irréductibles sur \mathbb{Q}_ℓ 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}_ℓ de $G/U = \text{Gal}(K/k)$.

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 : $\text{Gal}(L/K)$. Soit E_K le groupe des unités de K . Posons :

$$\mathcal{E}_K = E_K / E_K^\ell. \text{ Nous appellerons } \mathcal{E}_K \text{ le groupe des } \ell\text{-unités de } K.$$

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 $U = \text{Gal}(L/K)$. Si ϕ_1 est un caractère de G/U irréductible sur

\mathbb{Q}_ℓ 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 appellerons ce caractère 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}_ℓ dont il est le résidu modulo ℓ . En ce sens, χ^* est l'homomorphisme de G dans le groupe multiplicatif de \mathbb{Z}_ℓ 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_0 . Désignons par σ_∞ la conjugaison complexe de \mathbb{C} . Soient π_1, \dots, π_s les plongements réels de L dans \mathbb{C} et $\pi_{1+s}, \dots, \pi_{t+s}$, $\bar{\pi}_{1+s}, \dots, \bar{\pi}_{t+s}$ les plongements complexes de L dans \mathbb{C} . Convenons que $\bar{\pi}$ est le conjugué de π , c'est-à-dire que $\bar{\pi} = \pi \sigma_\infty$. Nous définissons ψ_0 de la façon suivante : si τ appartient à G et diffère de 1, alors $\psi_0(\tau)$ est le demi nombre de plongements complexes π de L dans \mathbb{C} tels que $\bar{\pi} = \tau \pi$. D'autre part, on posera $\psi_0(1) = s+t$.

Cas particulier. Supposons un instant L/\mathbb{Q} galoisienne. Supposons L plongé dans \mathbb{C} et soit $L_0 = L \cap \mathbb{R}$ et $H_0 = \text{Gal}(L/L_0)$. Le groupe H_0

possède donc 1 ou 2 éléments. On peut alors vérifier que l'application ψ_0 définie ci-dessus est la restriction à G du caractère de $\text{Gal}(L/\mathbb{Q})$ induit par le caractère principal de H_0 .

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 $\ell^{\text{ème}}$ de l'unité, alors le caractère du $\mathbb{F}_\ell[G]$ -module \mathcal{E}_L est $\Psi_L = \chi^* \psi_0 - 1$. Si L ne contient pas de racine primitive $\ell^{\text{ème}}$ de l'unité, le caractère de \mathcal{E}_L est $\Psi_L = \psi_0 - 1$.

Corollaire. Soit ϕ un caractère de G , irréductible sur \mathbb{Q}_ℓ . 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 $\mathcal{L} : E_L \longrightarrow \mathbb{R}^{s+t}$
 $\varepsilon \longrightarrow (\text{Log} |\varepsilon^{\prod_i}|)_{1 \leq i \leq s+t}$

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

$\tau \prod_1 = \prod_{j_\tau(i)} \text{ ou } \overline{\prod}_{j_\tau(i)}$. 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 :

$(x_i)_{1 \leq i \leq s+t} \cdot \tau = (x_{j_\tau(i)})_{1 \leq i \leq s+t}$. Le plongement \mathcal{L} devient alors un

homomorphisme de G -modules.

Soit D le sous-ensemble de \mathbb{R}^{s+t} ainsi défini :

$D = \{(\lambda, \dots, \lambda) ; \lambda \in \mathbb{Z}\}$. 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

$(x_i)_{1 \leq i \leq s+t}$, $(x_i) \cdot \tau_{1 \leq i \leq s+t}$. L'application qui associe à τ , la trace de

A_τ est le caractère du $\mathbb{Q}[G]$ -module $(\mathcal{L}(E_L) \oplus D) \cdot \mathbb{Q}$, 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 $\text{Tr}(A_\tau)$, il suffit de chercher comment A_τ transforme la base canonique de \mathbb{R}^{s+t} . On obtiendra : $\text{Tr}(A_1) = s+t$, Si τ diffère 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: $\tau \rightarrow \text{Tr}(A_\tau)$, est donc égale à Ψ_0 .

Comme G agit trivialement sur D , on en déduit que $\Psi_0 - 1$ est le caractère de $\mathcal{L}(E_L) \cdot \mathbb{Q}$, c'est-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}_ℓ défini par $\zeta^\sigma = \zeta^{\chi^*(\sigma)}$ pour tout σ de G . Si ϕ est un caractère irréductible de G sur \mathbb{Q}_ℓ , 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}_ℓ . Ce caractère $\bar{\phi}$ est aussi irréductible sur \mathbb{Q}_ℓ . On l'appellera le "reflet" de ϕ . (Spiegelbild). L'application $\phi \rightarrow \bar{\phi}$ est une involution de l'ensemble des caractères irréductibles de G sur \mathbb{Q}_ℓ ; 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_{ϕ_m} et \dim_ϕ 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 ℓ^n 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}_ℓ , 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 :

$$\dim_{\bar{\phi}_m} \mathcal{H} - \dim_{\phi_m} \mathcal{H} \leq \dim_\phi \mathcal{E}^\circ .$$

Remarque . Comme \mathcal{E}° 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}_ℓ , 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}_ℓ 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}_ℓ , 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^n , 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 :

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

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

$\text{Gal}(M/L)$ sont isomorphes (en tant que G -modules) par l'isomorphisme de réciprocity du corps des classes. Les groupes $\text{Gal}(M/M_m)$ et $\text{Gal}(M/M_{m/\ell})$ 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 : $\text{Gal}(M_m/M_{m/\ell})$ et $\mathcal{H}^{m/\ell}/\mathcal{H}^m$. D'où l'égalité :

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

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 $\alpha_m : W_m/L^* \cong \text{Gal}(M_m/L)^\wedge$ a pour restriction à $W_{m/\ell}/L^*$ l'isomorphisme $\alpha_{m/\ell} : W_{m/\ell}/L^* \cong \text{Gal}(M_{m/\ell}/L)^\wedge$.

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

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

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 :

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

En passant au quotient, on obtient :

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

Dans l'isomorphisme β_m , $\text{Gal}(M_m/M_{m/\ell})^\wedge{}^{1\bar{\phi}}$ correspond donc à $(W_m/W_{m/\ell})^\phi$. D'après le lemme IV, $\text{Gal}(M_m/M_{m/\ell})^\wedge{}^{1\bar{\phi}}$ est un groupe isomorphe à $\text{Gal}(M_m/M_{m/\ell})^{\bar{\phi}\wedge}$. Nous aurons donc :

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

Proposition IV a . Les quantités : $\dim_{\bar{\phi}_m} \mathcal{H}$ 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 $m^{\text{ème}}$ 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 $m^{\text{ème}}$ appartient à L et engendre un idéal qui est une puissance $m^{\text{ème}}$ d'un idéal α de L . On a donc : $w^m A_L = \alpha^m$. La classe de l'idéal α (notée $\text{Cl}(\alpha)$) est un élément de $\mathcal{H}^{(m)}$. En associant à $wW_{m/\ell}$ la classe de $\text{Cl}(\alpha)$ 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 $w^m A_L = \alpha^m$, il existe donc un élément a de L tel que $\alpha^{m/\ell} = aA_L$. D'où $w^m A_L = a^{\ell} A_L$ et il existe une unité ε de L telle que $w^m = a^{\ell} \varepsilon$. 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

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

l'application de $\text{Ker } \theta_m$ dans $E^\circ/E^\ell = E^\circ$ 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 $\text{Ker } \theta_m$ dans E° . On en déduit les inégalités :

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

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}_ℓ -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 $\text{Gal}(\tilde{k}/k)$, l'image de H_L par N correspond à $\text{Gal}(\tilde{k}/L\tilde{k})$. Dans l'isomorphisme de réciprocité liant H_L et $\text{Gal}(\tilde{L}/L)$ le noyau de N correspond à $\text{Gal}(\tilde{L}/L\tilde{k})$.

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 $\text{Gal}(\tilde{k} / \tilde{k} \cap L)$. Réciproquement, soit σ un élément de $\text{Gal}(\tilde{k} / \tilde{k} \cap L)$. 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 $L_0 = L \cap \mathbb{R}$. On appelle groupe des classes réelles de L , le groupe des classes de L_0 et on appelle groupe des classes relatives de L , le noyau de l'application N de H_L dans H_{L_0} déduite de la norme relative à L/L_0 . (Ces notions dépendent donc du plongement de L dans \mathbb{C} choisi. Si L/\mathbb{Q} est abélienne, L_0 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}_0 de L_0 , l'intersection $\tilde{L}_0 \cap L$ sera égale à L_0 . Il s'en suit que $N(H_L) = H_{L_0}$. 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 $[L:L_0] = 2$.

Désignons encore par L un corps de nombres plongé dans \mathbb{C} et par L_0 l'intersection : $L_0 = L \cap \mathbb{R}$. L'extension L/L_0 est galoisienne si et seulement si $[L:L_0] \leq 2$. En effet, si L/L_0 est galoisienne, de degré différent de 1, la restriction σ_∞ de la conjugaison de \mathbb{C} à L appartient au groupe de Galois de L/L_0 . Le corps fixe de σ_∞ sera donc L_0 et $[L:L_0] = 2$.

Supposons désormais, que L (et son plongement dans \mathbb{C}) vérifie cette condition. Soit ℓ un nombre premier impair et soit \mathcal{H} (resp. $\mathcal{H}_0, \mathcal{H}^*$) 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 : $\mathcal{H}_0 \cong \mathcal{H} / \mathcal{H}^*$. Mais nous pouvons énoncer un résultat plus précis : \mathcal{H} est produit direct de \mathcal{H}_0 et \mathcal{H}^* .

En effet, supposons $[L:L_0] = 2$. (Sinon, c'est clair).

Posons : $L_0 = k$, $G = \text{Gal}(L/k) = \{1, \sigma_\infty\}$. Le groupe G possède deux caractères irréductibles sur \mathbb{Q}_ℓ : 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 $K = k = L_0$) le groupe \mathcal{H}^1 est isomorphe par l'injection j de \mathcal{H}_0 dans \mathcal{H} , au ℓ -groupe des classes réelles \mathcal{H}_0 de L . On vérifie aussi, que \mathcal{H}^ϕ coïncide 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}^ϕ .

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 $L_0 = L \cap \mathbb{R}$. On suppose que $[L:L_0] = 2$. Si ℓ est un nombre premier impair, soit n le plus grand entier tel que L contienne une racine ℓ^n 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}_0 et \mathcal{H}^* de L , vérifient les inégalités :

$$\begin{aligned} \dim_m \mathcal{H}^* - \dim_m \mathcal{H}_0 &\leq \dim_{\mathbb{Z}} E_L, \\ \dim_m \mathcal{H}_0 - \dim_m \mathcal{H}^* &\leq \dim_{\mathbb{Z}} E_L - \dim_{\mathbb{Z}} E_{L_0} + 1. \end{aligned}$$

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

$$\dim_m \mathcal{H}_0 - \dim_m \mathcal{H}^* \leq \dim_{\mathbb{Z}} E_L - \dim_{\mathbb{Z}} E_{L_0}.$$

Les quantités $\dim_{\mathbb{Z}} E_L$ et $\dim_{\mathbb{Z}} E_{L_0}$ sont les dimensions des \mathbb{Z} -modules libres, quotients des groupes des unités E_L et E_{L_0} de L et L_0 par leurs sous-groupes de torsion.

Démonstration. Appliquons le théorème III à L et $k = L_0$. Comme $\zeta^{\ell_0} = \zeta^{-1}$, le caractère miroir de L/k est ϕ . De plus 1 et ϕ sont reflète l'un de l'autre. Nous avons donc :

$$\begin{aligned} \dim_{1m} \mathcal{H} - \dim_{\phi m} \mathcal{H} &\leq \dim_{\phi} \mathcal{E}^{\circ} \leq \dim_{\phi} \mathcal{E}, \\ \dim_{\phi m} \mathcal{H} - \dim_{1m} \mathcal{H} &\leq \dim_1 \mathcal{E}^{\circ} \leq \dim_1 \mathcal{E}. \end{aligned}$$

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 : $\mathcal{E}^1 \cong \mathcal{E}_{L_0}$ et \mathcal{E} est produit direct : $\mathcal{E} = \mathcal{E}^1 \mathcal{E}^{\phi}$. Nous

aurons donc: $\dim_1 \mathcal{E} = \dim_{\ell} \mathcal{E}^1 = \dim_{\ell} \mathcal{E}_{L_0} = \dim_{\mathbb{Z}} E_{L_0}$, puisque L_0 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:

$$\dim_{\phi} \mathcal{E} = \dim_{\ell} \mathcal{E} - \dim_{\ell} \mathcal{E}^1 = \dim_{\mathbb{Z}} E_L - \dim_{\mathbb{Z}} E_{L_0} + 1.$$

Supposons maintenant que \mathcal{S} ne soit pas une unité ℓ -primaire de L , c'est-à-dire que $L(\sqrt[\ell]{\mathcal{S}})/L$ 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 \mathcal{S} modulq 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 $\psi_L = \chi^* + \psi_0 - 1$, le caractère de \mathcal{E}° est "au plus" $\psi_0 - 1$ et on a: $\dim_{\phi} \mathcal{E}^{\circ} \leq \dim_{\phi} \mathcal{E} - 1$.

Remarques. La dernière hypothèse: " \mathcal{S} n'est pas une unité ℓ -primaire de L " est vérifiée en particulier dans le cas où L est le ℓ^n ème corps cyclotomique. Par exemple, pour $n = 1$, nous obtenons:

Si \mathcal{H}_0 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:

$$0 \leq \dim_{\ell} \mathcal{H}^* - \dim_{\ell} \mathcal{H}_0 \leq (\ell - 3)/2.$$

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 Bernoulli. 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 ℓ^n 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: $\mathbb{Q}^{(\ell^n)}/\mathbb{Q}_0^{(\ell^n)}$. 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 $K = k(\sqrt{d})$, $\bar{K} = k(\sqrt{-3d})$ et $k' = k(\sqrt{-3})$. Soient \mathcal{H}_K , $\mathcal{H}_{\bar{K}}$, $\mathcal{H}_{k'}$, \mathcal{H}_k les 3-groupes des classes d'idéaux de K , \bar{K} , k' et k .

Soient j , \bar{j} , j' les injections canoniques de \mathcal{H}_k dans \mathcal{H}_K , $\mathcal{H}_{\bar{K}}$, $\mathcal{H}_{k'}$.

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 :

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

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

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

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 $G = \text{Gal}(L/k)$. 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 \bar{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 $\mathbb{Q}_3^{(3^n)}$ du 3^n ème corps cyclotomique soit inclus dans k . Soit ζ une racine primitive 3^n 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 reflètes l'un

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

$$\begin{aligned} \dim_{\bar{\phi}_m} \mathcal{H} - \dim_{\phi_m} \mathcal{H} &\leq \dim_{\phi} \mathcal{E} , \\ \dim_{1m} \mathcal{H} - \dim_{\chi^*_m} \mathcal{H} &\leq \dim_{\chi^*} \mathcal{E} , \\ \dim_{\chi^*_m} \mathcal{H} - \dim_{1m} \mathcal{H} &\leq \dim_1 \mathcal{E} , \end{aligned}$$

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 interprète 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'interprète 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 \mathcal{S} 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 :

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

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.) , Über die Klassenzahl abelscher Zahlkörpern , Berlin , (1952) .
- [5] Hecke (E.) , Über 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.) Über 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) .