Werk

Titel: Structure galoisienne des anneaux d'entiers.

Autor: CASSOU-NOGUÈS, Philippe

PURL: https://resolver.sub.uni-goettingen.de/purl?320141322_0006|log20

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

Séminaire de Théorie des Nombres
Année 1976-1977 - exposé n° 27

STRUCTURE GALOISIENNE DES ANNEAUX D'ENTIERS

par

Philippe CASSOU-NOGUÈS

-:-:-:-

1. - Introduction

On note O_L l'anneau des entiers de toute sous-extension L de la clôture algébrique $\bar{\mathbb{Q}}$ de $\mathbb{Q}$ dans $\mathbb{C}$.

Soit N une extension galoisienne finie d'un corps de nombres K. Le groupe de Galois Γ de N sur K opère sur O_N et nous appelons structure galoisienne de O_N la structure de O_N en tant que module sur l'algèbre de groupe $\mathbb{Z}[\Gamma]$. Dans cette étude N est une extension modérément ramifiée de K, O_N est donc un $\mathbb{Z}[\Gamma]$-module localement libre et nous notons $U_{N|K}$ l'élément qu'il définit dans le groupe des classes $C(\mathbb{Z}[\Gamma])$.

Problème 1.- Lorsque N est une extension abélienne de $\mathbb{Q}$, Hilbert et Speiser [9], ont montré que le $\mathbb{Z}[\Gamma]$-module O_N est libre, c'est-à-dire qu'il existe un entier a de N tel que $\{a^\gamma, \gamma \in \Gamma\}$ soit une base sur $\mathbb{Z}$ de O_N ; on dit que N possède une base normale d'entiers. Par contre, Martinet [10], a construit une extension modérément ramifiée de $\mathbb{Q}$ dont l'anneau d'entiers n'est pas

stablement libre sur $\mathbb{Z}[\Gamma]$. Ceci démontre qu'il n'existe pas toujours de base normale d'entiers et plus généralement que l'ordre de $U_{N|K}$ dans $C(\mathbb{Z}[\Gamma])$ n'est pas toujours égal à 1 . Nous appelons problème 1 le problème de l'ordre de $U_{N|K}$ dans le groupe $C(\mathbb{Z}[\Gamma])$.

Problème 2.- Soit θ un caractère de Γ . Nous désignons par $\Lambda(\ ,\theta, N|K)$ le prolongement à tout le plan complexe de la série L-d'Artin généralisée associée à θ . C'est une fonction méromorphe qui satisfait l'équation fonctionnelle :

$$\Lambda(s,\theta,N|K) = W(\theta,N|K)\,\Lambda(1-s,\bar{\theta},N|K)\ , \quad s\in\mathbb{C}$$

où $\bar{\theta}$ désigne le caractère complexe conjugué de θ . On définit ainsi un nombre complexe $W(\theta,N|K)$ de module 1 qu'on appelle constante de l'équation fonctionnelle. Si le caractère θ est à valeurs réelles, on a :

$$W(\theta,N|K) = \pm 1\ .$$

Fröhlich et Queyrut [8], ont démontré que $W(\theta,N|K)=1$ lorsque θ est orthogonal mais on sait que $W(\theta,N|K)$ peut être égal à -1 lorsque θ est symplectique. Le problème 2 est le problème des valeurs $W(\theta,N|K)$ pour les caractères symplectiques θ de Γ .

Lorsque Γ est le groupe quaternionien H_8 l'ordre de $C(\mathbb{Z}[\Gamma])$ est égal à 2 . On identifie ce groupe au groupe multiplicatif $\{\pm 1\}$.
L'unique caractère non abélien de H_8 est symplectique et nous notons $W_{N|\mathbb{Q}}$ la valeur de la constante associée. Fröhlich, [6], a démontré l'égalité :

$$U_{N|\mathbb{Q}} = W_{N|\mathbb{Q}}\ .$$

Ce résultat surprenant, obtenu dans ce cas particulier, a conduit Fröhlich à développer récemment une théorie qui montre l'existence d'un lien général entre les problèmes 1 et 2. Il fait la conjecture suivante :

Conjecture de Fröhlich.- On a : $U^2_{N|K}=1$ et même $U_{N|K}=1$ lorsque les constantes $W(\theta,N|K)$ associées aux caractères symplectiques θ de Γ sont égales à 1 .

Fröhlich a démontré que $U_{N|K}$ appartient au noyau $D(\mathbb{Z}[\Gamma])$ de l'homomorphisme induit par l'extension des scalaires de $C(\mathbb{Z}[\Gamma])$ sur le groupe des classes $C(\mathfrak{M})$ d'un ordre maximal $\mathfrak{M}$ de $\mathbb{Q}[\Gamma]$ contenant $\mathbb{Z}[\Gamma]$. Dans cet exposé nous définissons un sous-groupe en général strict de $D(\mathbb{Z}[\Gamma])$, qu'on note $H(\mathbb{Z}[\Gamma])$, et nous obtenons le résultat suivant :

THÉORÈME. - Si N est une extension galoisienne, finie et modérément ramifiée d'un corps de nombres K alors $U_{N|K}$ se décompose en un produit de deux éléments $t(W_{N|K})$ et $V_{N|K}$ tels que :

(i) $t(W_{N|K})$ est un élément défini à partir des constantes d'équation fonctionnelle, son ordre est égal à 1 ou 2 ; il est égal à 1 lorsque les constantes associées aux caractères symplectiques de Γ sont égales à 1.

(ii) $V_{N|K}$ est un élément de $H(\mathbb{Z}[\Gamma])$, son ordre divise $[N:K]'$ où $[N:K]'$ désigne le quotient de $[N:K]$ par le produit de ses diviseurs premiers.

Ce résultat amélioré permet de démontrer la conjecture de Fröhlich, c'est-à-dire que $V_{N|K} = 1$, dans de nouveaux cas particuliers.

Cet exposé est un résumé rapide de résultats et de méthodes développés dans [2] et [3]. Il se termine par deux appendices. Dans le premier nous montrons sur un exemple que les résultats de Fröhlich [5], sont insuffisants pour démontrer le théorème précédent. La démonstration de ce théorème conduit à définir une nouvelle application, notée y, du groupe additif R_Γ des caractères virtuels de Γ à valeurs dans le groupe des racines de l'unité satisfaisant certaines propriétés de congruence.

Dans le deuxième appendice nous comparons les valeurs de y et celles des constantes de l'équation fonctionnelle lorsque Γ est le groupe quaternionien H_{4m} où m est un entier impair.

2.- Notations et rappels ([4], [5])

Le groupe multiplicatif des éléments inversibles d'un anneau A est noté A^*. Un corps de nombres K est une extension finie de $\mathbb{Q}$ contenue dans $\bar{\mathbb{Q}}$. On note $U(K)$ le groupe des idèles unités de K et on définit $U(\bar{\mathbb{Q}})$ comme limite inductive des groupes $U(K)$ lorsque K parcourt l'ensemble des corps de nombres. Si Γ est un groupe fini on note $|\Gamma|$ son ordre. On entend par caractère irréductible (resp. de degré 1) de Γ un caractère absolument irréductible (resp. irréductible de degré 1). Le groupe de Galois de $\bar{\mathbb{Q}}$ sur $\mathbb{Q}$, qu'on note $\Omega_{\mathbb{Q}}$, opère sur les groupes R_Γ (groupe des caractères de Γ), $O_{\bar{\mathbb{Q}}}^*$, $U(\bar{\mathbb{Q}})$ et μ (groupe des racines de l'unité de $\bar{\mathbb{Q}}$) et l'on définit le groupe $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_\Gamma, U(\bar{\mathbb{Q}}))$ (resp. $\mathrm{Hom}^+_{\Omega_{\mathbb{Q}}}(R_\Gamma, U(\bar{\mathbb{Q}}))$ des $\Omega_{\mathbb{Q}}$-homomorphismes (resp. $\Omega_{\mathbb{Q}}$-homomorphismes f dont la composante $f(\theta)_u$ est réelle et positive pour toute place infinie u de $\bar{\mathbb{Q}}$ et tout caractère symplectique θ de Γ) de R_Γ dans $U(\bar{\mathbb{Q}})$ et son sous-groupe $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_\Gamma, O_{\bar{\mathbb{Q}}}^*)$ (resp. $\mathrm{Hom}^+_{\Omega_{\mathbb{Q}}}(R_\Gamma, O_{\bar{\mathbb{Q}}}^*)$). On définit un homomorphisme noté det. du groupe des idèles unités $U(\mathbb{Z}[\Gamma])$ de $\mathbb{Z}[\Gamma]$ dans $\mathrm{Hom}^+_{\Omega_{\mathbb{Q}}}(R_\Gamma, U(\bar{\mathbb{Q}}))$ en prolongeant par linéarité à R_Γ l'application qui à α associe $\det(\alpha)$ défini pour le caractère θ de la représentation T par $\det_\theta(\alpha) = \det(T(\alpha))$ où $\det(T(\alpha))$ désigne le déterminant usuel. Fröhlich [5], construit un isomorphisme naturel de $D(\mathbb{Z}[\Gamma])$ sur :

$$\mathrm{Hom}^+_{\Omega_{\mathbb{Q}}}(R_\Gamma, U(\bar{\mathbb{Q}})) \Big/ \mathrm{Hom}^+_{\Omega_{\mathbb{Q}}}(R_\Gamma, O_{\bar{\mathbb{Q}}}^*).\det(U(\mathbb{Z}[\Gamma]))$$

à l'aide duquel nous identifions $D(\mathbb{Z}[\Gamma])$ à ce dernier groupe.

Si Γ est le groupe de Galois d'une extension modérément ramifiée N de K, $U_{N|K}$ admet un représentant v dans $\mathrm{Hom}^+_{\Omega_{\mathbb{Q}}}(R_\Gamma, U(\bar{\mathbb{Q}}))$ qui vérifie pour tout nombre premier ℓ qui divise $|\Gamma|$:

$$(1) \qquad v(\theta)_\ell = (\eta_{K|\mathbb{Q}}(a|\theta)\ \tau(\theta)^{-1}\ W'_{N|K}(\theta))_\ell \quad \text{pour tout } \theta \in R_\Gamma .$$

Dans cette formule $\eta_{K|\mathbb{Q}}(a|\theta)$ désigne la norme au sens de [5] de la résolvante $(a|\theta)$ associée à un élément a de N qui engendre une base normale de N sur K et une base normale d'entiers localement pour toute place infinie et toute place finie de K au-dessus d'un diviseur premier de $|\Gamma|$, $\tau(\theta)$ est la somme de Gauss galoisienne associée au caractère θ, $W'_{N|K}(\theta)$ est défini sur les caractères irréductibles de Γ par : $W'_{N|K}(\theta) = W_{N|K}(\theta)$, constante de l'équation fonctionnelle de la série L associée à θ (resp. 1) si θ est symplectique (resp. non symplectique) et se prolonge par linéarité à R_Γ, $v(\theta)_\ell$ désigne la ℓ-composante de

$v(\theta)$ dans $U(\bar{\Omega})$. Désignons par $R_\Gamma^{(s)}$ (resp. $T(R_\Gamma)$) le sous-groupe de R_Γ des caractères symplectiques (resp. l'image de l'application T définie par $T(\theta)=\theta+\bar{\theta}$ où $\bar{\theta}$ désigne le caractère complexe conjugué de θ). L'application : $\theta \longrightarrow W_{N|K}(\theta)$, définie sur R_Γ, induit un $\Omega_\mathbb{Q}$-homomorphisme, noté $W_{N|K}$, de $R_\Gamma^{(s)}/T(R_\Gamma)$ muni de sa structure naturelle de $\Omega_\mathbb{Q}$-module dans le groupe multiplicatif à deux éléments $\{\pm 1\}$ muni de sa structure de $\Omega_\mathbb{Q}$-module trivial. Le $\Omega_\mathbb{Q}$-homomorphisme de R_Γ sur $R_\Gamma^{(s)}/T(R_\Gamma)$ qui à tout caractère irréductible et non symplectique (resp. symplectique) de Γ associe 0 (resp. sa classe modulo $T(R_\Gamma)$) et un plongement canonique de -1 dans $U(\bar{\Omega})$ permettent de relever tout élément f de $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_\Gamma^{(s)}/T(R_\Gamma), \pm 1)$ en un élément $t(f)$ de $\overset{+}{\mathrm{Hom}}_{\Omega_\mathbb{Q}}(R_\Gamma, U(\bar{\Omega}))$.

Si ℓ est un nombre premier on désigne par $\mathfrak{L}$ le radical de l'idéal $\ell O_{\bar{\Omega}}$ et par $\mathrm{Ker}\, d_{\ell,\Gamma}$ le sous-groupe de R_Γ des caractères θ tels que $\theta(\gamma)=0$ pour tout élément γ ℓ-régulier. On note V_ℓ le groupe $(O_{\bar{\Omega}}/\mathfrak{L})^*$ et μ_ℓ (resp. μ'_ℓ) le groupe des racines de l'unité dont l'ordre est une puissance de ℓ (resp. est premier avec ℓ). Tout élément u de μ s'écrit de manière unique comme un produit $u'u''$ où u'' (resp. u') est un élément de μ_ℓ (resp. μ'_ℓ) et on note ε_ℓ le $\Omega_\mathbb{Q}$-homomorphisme : $(u \to u'')$ de μ sur μ_ℓ. On définit un homomorphisme $r_\ell(\Gamma)$ de $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_\Gamma, U(\bar{\Omega}))$ sur $\mathrm{Hom}_{\Omega_\mathbb{Q}}(\mathrm{Ker}\, d_{\ell,\Gamma}, V_\ell)$ en posant

$$r_\ell(\Gamma)(f)(\theta) = (\pi_\ell \circ f \circ i_\ell)(\theta) \quad , \quad \theta \in \mathrm{Ker}\, d_{\ell,\Gamma}$$

où π_ℓ (resp. i_ℓ) est la surjection (resp. injection) canonique de $U(\bar{\Omega})$ sur V_ℓ (resp. $\mathrm{Ker}\, d_{\ell,\Gamma}$ dans R_Γ). L'image par $r_\ell(\Gamma)$ de $\det(U(\mathbb{Z}[\Gamma]))$ est réduite à l'élément neutre.

Pour toute famille $\{\ell_i, 1 \le i \le q\}$ de diviseurs premiers de $|\Gamma|$ on note $r_{\ell_1 \cdots \ell_q}(\Gamma)$ l'homomorphisme $(\prod_{1 \le i \le q} r_{\ell_i}(\Gamma))$ de $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_\Gamma, U(\bar{\Omega}))$ sur $(\prod_{1 \le i \le q} \mathrm{Hom}_{\Omega_\mathbb{Q}}(\mathrm{Ker}\, d_{\ell_i,\Gamma}, V_{\ell_i}))$ et $h_{\ell_1 \cdots \ell_q}(\Gamma)$ l'homomorphisme induit par $r_{\ell_1 \cdots \ell_q}(\Gamma)$ de $D(\mathbb{Z}[\Gamma])$ sur le groupe $E_{\ell_1 \cdots \ell_q}(\Gamma)$ défini par l'égalité :

$$E_{\ell_1 \cdots \ell_q}(\Gamma) = (\prod_{1 \le i \le q} \mathrm{Hom}_{\Omega_\mathbb{Q}}(\mathrm{Ker}\, d_{\ell_i,\Gamma}, V_{\ell_i}))/r_{\ell_1 \cdots \ell_q}(\Gamma)(\overset{+}{\mathrm{Hom}}_{\Omega_\mathbb{Q}}(R_\Gamma, O^*_{\bar{\Omega}}))$$

En composant avec $r_{\ell_1 \cdots \ell_q}(\Gamma)$ l'homomorphisme t on obtient par passage au quotient un homomorphisme $k_{\ell_1 \cdots \ell_q}(\Gamma)$ de $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_\Gamma^{(s)}/T(R_\Gamma), \pm 1)$ dans $E_{\ell_1 \cdots \ell_q}(\Gamma)$. Lorsque $\{\ell_i, 1 \leq i \leq q\}$ désigne l'ensemble des diviseurs premiers de $|\Gamma|$ on note $r(\Gamma)$, $h(\Gamma)$, $k(\Gamma)$ (resp. $E(\Gamma)$) les homomorphismes (resp. le groupe) $r_{\ell_1 \cdots \ell_q}(\Gamma)$, $h_{\ell_1 \cdots \ell_q}(\Gamma)$, $k_{\ell_1 \cdots \ell_q}(\Gamma)$ (resp. $E_{\ell_1 \cdots \ell_q}(\Gamma)$).

Si a est un élément de N vérifiant les propriétés rappelées après la formule (1), on a les congruences :

$$\eta_{K|\mathbb{Q}}(a|\theta) \equiv 1 \pmod{\mathfrak{L}} \text{ pour tout } \theta \in \mathrm{Ker}\, d_{\ell,\Gamma}$$

En outre on a le théorème suivant :

THÉORÈME 2.1 (Fröhlich, [5]). - Si P est un idéal premier de K modérément ramifié dans N il existe un unique élément $y_{P,\ell}$ de $\mathrm{Hom}^{+}_{\Omega_{\mathbb{Q}}}(\mathrm{Ker}\, d_{\ell,\Gamma}, \mu'_\ell)$ tel que l'on ait :

$$y_{P,\ell}(\theta) \equiv \tau_P(\theta) \pmod{\mathfrak{L}} \text{ pour tout } \theta \text{ de } \mathrm{Ker}\, d_{\ell,\Gamma} \ ;$$

où l'on désigne par $\tau_P(\theta)$ la somme de Gauss galoisienne locale en P associée à θ ([11]).

En utilisant la formule (2), le théorème 2.1 et le représentant v de $U_{N|K}$ donné par (1), on obtient :

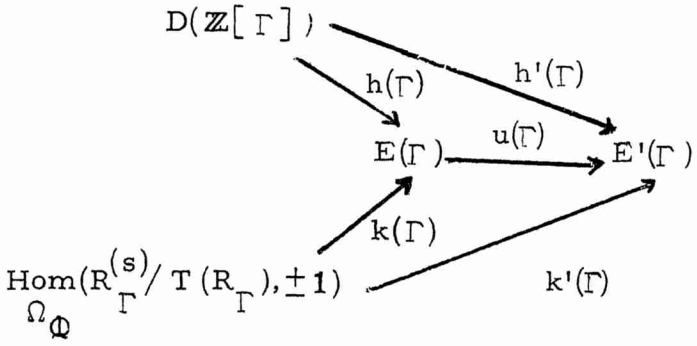
THÉORÈME 2.2 (Fröhlich, [5]). - Si N est une extension galoisienne modérément ramifiée du corps de nombres K, de groupe de Galois Γ, pour tout nombre premier ℓ on a :

$$h_\ell(\Gamma)(U_{N|K}) = k_\ell(\Gamma)(W_{N|K})$$

Le théorème 2.2 est un théorème local "en ℓ" en se pose naturellement le problème de l'analogue global de ce théorème, c'est-à-dire de l'égalité $h(\Gamma)(U_{N|K}) = k(\Gamma)(W_{N|K})$ dans le groupe $E(\Gamma)$. Nous donnons une rapide idée

de la démonstration de ce résultat dans le paragraphe suivant .

Remarque. - On peut définir un groupe $E'(\Gamma)$ par l'égalité : $E'(\Gamma) = \prod_{1 \le i \le q} E_{\ell_i}(\Gamma)$ où $\{\ell_i, 1 \le i \le q\}$ désigne l'ensemble des diviseurs premiers de $|\Gamma|$ et un homomorphisme $h'(\Gamma)$ (resp. $k'(\Gamma)$) par $h'(\Gamma) = \prod_{1 \le i \le q} h_{\ell_i}(\Gamma)$ (resp. $k'(\Gamma) = \prod_{1 \le i \le q} k_{\ell_i}(\Gamma)$). Il existe un homomorphisme $u(\Gamma)$ de $E(\Gamma)$ sur $E'(\Gamma)$ tel que le diagramme suivant soit commutatif :



Le théorème 2.2 implique l'égalité $h'(\Gamma)(U_{N|K}) = k'(\Gamma)(W_{N|K})$. En donnant,(Appendice I) , un exemple de groupe Γ où $u(\Gamma)$ n'est pas un isomorphisme de groupe nous montrons que cette égalité n'implique pas en général l'égalité : $h(\Gamma)(U_{N|K}) = k(\Gamma)(W_{N|K})$.

3. -Théorème principal

a) Endomorphismes de R_Γ

Soit ℓ un nombre premier. Tout élément γ de Γ s'écrit d'une manière unique sous la forme $\gamma = \gamma' \gamma''$ avec $\gamma'\gamma'' = \gamma''\gamma'$ où γ' (resp. γ'') est un élément de Γ dont l'ordre est premier avec ℓ (resp. est égal à une puissance de ℓ) . Pour tout caractère θ de Γ on définit l'application $\delta_\ell(\theta)$ de Γ dans $\mathbb{C}$ par :

$$\delta_\ell(\theta)(\gamma) = \theta(\gamma').$$

PROPOSITION 3-1. - Pour tout nombre premier ℓ, δ_ℓ est un $\Omega_{\mathbb{Q}}$-endomorphisme idempotent de R_Γ

On montre de façon immédiate que δ_ℓ est un opérateur d'Adams de R_Γ. Si ℓ et ℓ' sont 2 nombres premiers les endomorphismes $\delta_\ell \circ \delta_{\ell'}$ et $\delta_{\ell'} \circ \delta_\ell$ de R_Γ sont égaux et on note $\delta_{\ell\ell'}$ cet endomorphisme. Plus généralement pour toute famille $\{\ell_i,\ 1 \leq i \leq q\}$ de nombres premiers on définit $\delta_{\ell_1 \ldots \ell_q}$ (resp. $\Delta_{\ell_1 \ldots \ell_q}$) par $\delta_{\ell_1 \ldots \ell_q} = \delta_{\ell_1} \circ \ldots \circ \delta_{\ell_q}$ (resp. $I - \delta_{\ell_1 \ldots \ell_q}$ où I désigne l'identité de R_Γ) et on note δ'_ℓ (resp. Δ'_ℓ) l'endomorphisme $\delta_{\ell_1 \ldots \ell_q}$ (resp. $\Delta_{\ell_1 \ldots \ell_q}$) lorsque $\{\ell_i,\ 1 \leq i \leq q\}$ est l'ensemble des diviseurs premiers de $|\Gamma|$ qui sont différents de ℓ.

Nous avons étudié dans [2] les propriétés de ces endomorphismes. Nous utiliserons dans cet exposé les propriétés suivantes :

Soit $\{\ell_i,\ 1 \leq i \leq q\}$ un ensemble fini de nombres premiers alors :

(i) La restriction de $\delta_{\ell_1 \ldots \ell_q}$ à $\operatorname{Ker} d_{\ell_i,\Gamma}$ est nulle et la restriction de $\Delta_{\ell_1 \ldots \ell_q}$ à $\operatorname{Ker} d_{\ell_i,\Gamma}$ est l'identité quelque soit i, $1 \leq i \leq q$.

(ii) L'image de $\Delta_{\ell_1 \ldots \ell_q}$ est le sous-groupe $\sum_{i=1}^{q} \operatorname{Ker} d_{\ell_i,\Gamma}$ de R_Γ.

On en déduit que pour tout nombre premier ℓ, $\operatorname{Ker} d_{\ell,\Gamma}$ est stable par $\delta_{\ell_1 \ldots \ell_q}$ et $\Delta_{\ell_1 \ldots \ell_q}$ et on obtient la décomposition canonique suivante de $\operatorname{Ker} d_{\ell,\Gamma}$ en somme directe de sous-modules :

$$\operatorname{Ker} d_{\ell,\Gamma} = \delta'_\ell (\operatorname{Ker} d_{\ell,\Gamma}) \oplus \Delta'_\ell (\operatorname{Ker} d_{\ell,\Gamma})$$

on note $\operatorname{Ker} d'_{\ell,\Gamma}$ le sous-module $\delta'_\ell (\operatorname{Ker} d_{\ell,\Gamma})$.

On a les propriétés suivantes :

$$\delta'_\ell (\operatorname{Ker} d_{\ell,\Gamma}) \cap \Big(\sum_{\ell' \neq \ell} \operatorname{Ker} d_{\ell',\Gamma}\Big) = \{0\}$$

$$\Delta'_\ell (\operatorname{Ker} d_{\ell,\Gamma}) = \operatorname{Ker} d_{\ell,\Gamma} \cap \Big(\sum_{\ell' \neq \ell} \operatorname{Ker} d_{\ell',\Gamma}\Big)$$

b) Fonctions y_P et y

Soit K un corps de nombres et P un idéal premier. Les extensions L de K sont galoisiennes et finies. On note $G(L|K)$ le groupe de Galois de L sur K, $R_{L|K}$, $\mathrm{Ker}\, d_{\ell, L|K}$, $\mathrm{Ker}\, d'_{\ell, L|K}$, les groupes $R_{G(L|K)}$, $\mathrm{Ker}\, d_{\ell, G(L|K)}$, $\mathrm{Ker}\, d'_{\ell, G(L|K)}$ et $\varepsilon_{L|K}$ le caractère trivial de $G(L|K)$. On désigne par $R_m(K)$ (resp. $R_{m,P}(K)$) les couples $(\theta, L|K)$ où L est une extension modérément ramifiée (resp. modérément ramifiée en P) de K et où θ appartient à $R_{L|K}$. Si $(\theta, L|K)$ appartient à $R_{m,P}(K)$ on note $\tau_P(\theta, L|K)$ la somme de Gauss galoisienne locale en P.

THÉORÈME 3.1 ([2]). - Pour tout idéal premier P de K il existe une unique application y_P de $R_{m,P}(K)$ dans μ qui vérifie les propriétés suivantes :

(i) Pour toute extension L de K modérément ramifiée en P on a $y_P(\varepsilon_{L|K}, L|K) = 1$ et l'application : $\theta \to y_P(\theta, L|K)$ appartient à $\underset{\Omega_{\mathbb{Q}}}{\mathrm{Hom}^{+}}(R_{L|K}, \mu)$.

(ii) Pour tout nombre premier ℓ et tout élément $(\theta, L|K)$ de $R_{m,P}(K)$ alors $y_P(\theta, L|K)$ appartient à μ'_ℓ si θ appartient à $\mathrm{Ker}\, d'_{\ell, L|K}$. En outre on a la congruence :

$$y_P(\theta, L|K) \equiv \tau_P(\theta, L|K) \pmod{\mathfrak{L}}$$

si θ appartient à $\mathrm{Ker}\, d_{\ell, L|K}$.

On montre que pour toute extension L de K modérément ramifiée en P $\theta \to y_P(\theta, L|K)$ est triviale pour presque tout P. On définit alors une fonction y de $R_m(K)$ à valeurs dans μ par l'égalité : $y(\theta, L|K) = \prod_P y_P(\theta, L|K)$ où P parcourt les idéaux premiers de K. Elle satisfait des propriétés analogues aux propriétés (i) et (ii) du théorème.

Pour tout nombre premier ℓ et tout élément $(\theta, L|K)$ de $R_{m,P}(K)$ (resp. $R_m(K)$) où θ appartient à $\mathrm{Ker}\, d_{\ell, L|K}$ le théorème 2-1 nous permet

de définir un élément $y_{P,\ell}(\theta, L|K)$ (resp. $y_\ell(\theta, L|K) = \prod_P y_{P,\ell}(\theta, L|K)$ où P parcourt les idéaux premiers de K) de μ'_ℓ .

Soit $(\theta, L|K)$ un élément de $R_m(K)$. Le caractère $\theta - \theta(1)\varepsilon_{L|K}$ admet une décomposition $\sum_\ell \theta_\ell$ sur le groupe $\sum_\ell \operatorname{Ker} d_{\ell, L|K}$. Notons $\Delta'_\ell(L|K)$ l'endomorphisme $\Delta'_{\ell, G(L|K)}$ de $R_{L|K}$. Pour tout ℓ le caractère $\Delta'_\ell(\theta_\ell, L|K)$ admet une décomposition $\sum_{\ell' \neq \ell} \theta_{\ell'}$ sur le groupe $\sum_{\ell' \neq \ell} \operatorname{Ker} d_{\ell', L|K}$. On démontre que la racine de l'unité $\varepsilon_\ell\left(\prod_{\ell' \neq \ell} y_{\ell'}(\theta_{\ell'}, L|K)\right)$ ne dépend pas de la décomposition de $\Delta'_\ell(\theta_\ell, L|K)$; on note $\varepsilon_\ell(\Delta'_\ell(\theta_\ell, L|K))$ cette unité. En outre on démontre que le produit :

$$\prod_\ell \varepsilon_\ell(\Delta'_\ell(\theta_\ell, L|K))\, y_\ell(\theta_\ell, L|K)$$

ne dépend pas de la décomposition de $\theta - \theta(1)\varepsilon_{L|K}$. L'application y est définie par l'égalité :

$$y(\theta, L|K) = \prod_\ell \varepsilon_\ell(\Delta'_\ell(\theta_\ell, L|K))\, y_\ell(\theta_\ell, L|K) .$$

On détermine les valeurs de cette fonction pour un cas particulier dans l'appendice II.

c) Enoncé du théorème principal

En utilisant le représentant v de $U_{N|K}$ et le théorème 3.1 on démontre :

THÉORÈME 3.2 ([2]). - *Pour toute extension* N *modérément ramifiée d'un corps de nombres* K *on a l'égalité* :

$$h(\Gamma)(U_{N|K}) = k(\Gamma)(W_{N|K})$$

COROLLAIRE 1 . - *On a les égalités suivantes* :

(i) $h(\Gamma)(U_{N|K})^2 = 1$

(ii) *Si pour tout caractère symplectique* θ *du groupe de Galois* Γ *de* N *sur* K *on a* : $W(\theta, N|K) = 1$, *alors* $h(\Gamma)(U_{N|K}) = 1$.

Si x est un élément de $D(\mathbb{Z}[\Gamma])$ représenté par g de $\overset{+}{\underset{\Omega_{\mathbb{Q}}}{\mathrm{Hom}}}(R_\Gamma, U(\overline{\mathbb{Q}}))$ notons $\bar{x}$ l'élément représenté par $\bar{g}$ avec $\bar{g}(\theta) = \overline{g(\theta)}$.

COROLLAIRE 2.- Pour toute extension modérément ramifiée N d'un corps de nombres K on a : $h(\Gamma)(U_{N|K} \cdot \overline{U}_{N|K}) = 1$

4.- Ordre de $U_{N|K}$ ([3])

Désignons par $H(\mathbb{Z}[\Gamma])$ le noyau de $h(\Gamma)$. C'est un sous-groupe en général strict, (cf appendice I), du sous-groupe $\bigcap_\ell \mathrm{Ker}\, h_\ell(\Gamma)$ de $D(\mathbb{Z}[\Gamma])$; on note $H(\Gamma)$ son exposant. On note $D_o(\mathbb{Z}[\Gamma])$ le noyau de l'homomorphisme naturel défini de $D(\mathbb{Z}[\Gamma])$ sur $D(\mathbb{Z}[\Gamma^{(ab)}])$ où $\Gamma^{(ab)}$ désigne le groupe Γ rendu abélien et $H_o(\mathbb{Z}[\Gamma])$ (resp. $H_o(\Gamma)$) le groupe $H(\mathbb{Z}[\Gamma]) \cap D_o(\mathbb{Z}[\Gamma])$ (resp. son exposant).

Lorsque Γ est le groupe de Galois d'une extension modérément ramifiée N d'un corps de nombres K le théorème 3.2 montre qu'on peut écrire $U_{N|K}$ sous forme d'un produit $t(W_{N|K})\, V_{N|K}$ où $V_{N|K}$ appartient à $H(\mathbb{Z}[\Gamma])$. En outre si l'anneau des entiers du corps des invariants de N par le groupe des commutateurs de Γ est libre sur $\mathbb{Z}[\Gamma^{(ab)}]$, ce qui est toujours le cas lorsque $K = \mathbb{Q}$, alors $V_{N|K}$ appartient à $H_o(\mathbb{Z}[\Gamma])$.

Soient $\{\theta_i,\ 1 \leq i \leq q\}$ les caractères irréductibles de degré >1 du groupe Γ, on note $|\Gamma|_o$ l'entier $|\Gamma|/(\theta_1(1), \ldots, \theta_q(1))$ où $(\theta_1(1), \ldots, \theta_q(1))$ désigne le P.G.C.D de $\{(\theta_1(1), \ldots, \theta_q(1)\}$. Lorsque Γ est le groupe de Galois de N sur K on note $[N:K]_o$ l'entier $|\Gamma|_o$. Pour tout entier n on note n' le quotient de n par le produit de ses diviseurs premiers.

THÉORÈME 4.1.- Soit Γ un groupe fini alors :

(i) $H(\Gamma)$ divise l'entier $|\Gamma|'$

(ii) $H_o(\Gamma)$ divise l'entier $|\Gamma|_o'$.

COROLLAIRE 1.- Si N est une extension galoisienne finie et modérément ramifiée d'un corps de nombres K alors on a l'égalité suivante dans $D(\mathbb{Z}[\Gamma])$:

$$U_{N|K} = t(W_{N|K})\, V_{N|K}$$

où l'ordre de $V_{N|K}$ divise $[N : K]'$. En outre si $K = \mathbb{Q}$ ou si $D(\mathbb{Z}[\Gamma^{(ab)}])$ est réduit à l'élément neutre l'ordre de $V_{N|K}$ divise $[N : K]'_o$.

COROLLAIRE 2.- L'anneau des entiers d'une extension N galoisienne et modérément ramifiée d'un corps de nombres K dont le degré sur K est sans facteur carré est un $\mathbb{Z}[\Gamma]$-module libre.

En effet puisque 4 ne divise pas $[N : K]$ alors $G(N|K)$ ne possède pas de caractère symplectique irréductible ; en outre $[N : K]' = 1$.

On note x_2 la 2-composante d'un élément x d'un groupe abélien.

COROLLAIRE 3.- Si N est une extension galoisienne modérément ramifiée d'un corps de nombres K dont le groupe de Galois est isomorphe au groupe quaternionien H_{4m} où m est un nombre entier impair, alors on a les égalités :

(i) $U_{N|K,2} = t(W_{N|K})$

(ii) Si m est sans facteur carré ou égal à la puissance d'un nombre premier régulier : $U_{N|K} = t(W_{N|K})$.

En effet $[N : K]'_o$ est impair.

Soit $G_{\ell^n q}$ le groupe métacyclique engendré par ω et σ qui vérifient les égalités : $\omega^{\ell^n} = 1 = \sigma^q, \sigma\omega\sigma^{-1} = \omega^r$ où r est une racine primitive q-ème de 1 modulo ℓ, ℓ un nombre premier, régulier et impair et q un diviseur de $(\ell-1)$.

COROLLAIRE 4.- Si N est une extension galoisienne et modérément ramifiée de $\mathbb{Q}$ dont le groupe de Galois est isomorphe à $G_{\ell^n q}$ on a l'égalité :

$$U_{N|\mathbb{Q}} = t(W_{N|\mathbb{Q}}) .$$

Les corollaires 2, 3, 4 donnent de nouveaux exemples où la conjecture de Fröhlich est démontrée.

Appendice I

Soient ℓ_1 et ℓ_2 deux nombres premiers impairs distincts et soit $D_{2\ell_1\ell_2}$ le groupe diédral d'ordre $2\ell_1\ell_2$. On adopte dans ce paragraphe les notations suivantes : η_d est une racine primitive d-ème de l'unité et $K^{(d)}$ (resp. $R^{(d)}$) désigne la sous-extension réelle maximale (resp. l'anneau d'entiers de $K^{(d)}$) du corps $\mathbb{Q}^{(d)} = \mathbb{Q}(\eta_d)$. Pour $i = 1$ ou 2 on note I_{ℓ_i} l'idéal $(1-\eta_{\ell_i}) \cap R^{(\ell_1\ell_2)}$ de $R^{(\ell_1\ell_2)}$ et π_{ℓ_i} (resp. $\pi_{\ell_1\ell_2}$) la surjection canonique de $R^{(\ell_1\ell_2)}$ sur $(R^{(\ell_1\ell_2)}/I_{\ell_i})$ (resp. sur $(R^{(\ell_1\ell_2)}/I_{\ell_1}) \times (R^{(\ell_1\ell_2)}/I_{\ell_2})$). Nous étudions dans ce cas particulier les groupes $E(D_{2\ell_1\ell_2})$, $E_{\ell_i}(D_{2\ell_1\ell_2})$, pour $i = 1$ ou 2, et l'homomorphisme u. On peut trouver dans [1] une étude numérique plus complète du groupe $D(\mathbb{Z}[\Gamma])$ pour un groupe Γ diédral.

PROPOSITION. - Il existe des isomorphismes de groupe φ et ψ qui rendent commutatif le diagramme suivant :

$$\begin{array}{ccc} E(D_{2\ell_1\ell_2}) & \xrightarrow{\varphi} & (R^{(\ell_1\ell_2)}/I_{\ell_1} \cap I_{\ell_2})^* / \pi_{\ell_1\ell_2}(R^{(\ell_1\ell_2)*}) \\ \downarrow u & & \downarrow v \\ E_{\ell_1}(D_{2\ell_1\ell_2}) \times E_{\ell_2}(D_{2\ell_1\ell_2}) & \xrightarrow{\psi} & (R^{(\ell_1\ell_2)}/I_{\ell_1})^* / \pi_{\ell_1}(R^{(\ell_1\ell_2)*}) \times (R^{(\ell_1\ell_2)}/I_{\ell_2})^* / \pi_{\ell_2}(R^{(\ell_1\ell_2)*}) \end{array}$$

où v désigne l'homomorphisme induit par l'identité de $(R^{(\ell_1\ell_2)}/I_{\ell_1} \cap I_{\ell_2})^*$ par passage au quotient

La démonstration est élémentaire ; nous nous bornons à indiquer la construction de ψ. On désigne par θ_{ℓ_1} (resp. θ_{ℓ_2}), θ_o, $\theta_{\ell_1\ell_2}$, un caractère de degré 1 et d'ordre ℓ_1 (resp. ℓ_2), le caractère trivial, le caractère $\theta_{\ell_1} \cdot \theta_{\ell_2}$ du sous-groupe cyclique d'ordre $\ell_1\ell_2$ de $D_{2\ell_1\ell_2}$. Notons θ^* le caractère de $D_{2\ell_1\ell_2}$

induit par le caractère θ de ce sous-groupe et désignons par i et j deux entiers distincts tels que : $\{i,j\} = \{1,2\}$. Le groupe $\mathrm{Ker}\, d_{\ell_i}$ est engendré par les caractères : $(\theta_{\ell_i} - \theta_o)^*, (\theta_{\ell_1\ell_2} - \theta_j)^*$ et leurs conjugués par $\Omega_{\mathbb{Q}}$. Notons $R_{\ell_i}^{(\ell_i)}$ (resp. $R_{\ell_i}^{(\ell_1\ell_2)}$) l'anneau $R^{(\ell_i)} \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_{\ell_i}$ (resp. $R^{(\ell_1\ell_2)} \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_{\ell_i}$) où $\mathbb{Z}_{\ell_i}$ désigne l'anneau des entiers ℓ_i-adiques ; l'homomorphisme : $f \to (f((\theta_{\ell_i} - \theta_o)^*), f((\theta_{\ell_1\ell_2} - \theta_j)^*))$ de $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(\mathrm{Ker}\, d_{\ell_i}, U(\mathbb{Q})_{\ell_i})$ sur $R_{\ell_i}^{(\ell_i)*} \times R_{\ell_i}^{(\ell_1\ell_2)*}$ est un isomorphisme qui induit un nouvel isomorphisme de : $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(\mathrm{Ker}\, d_{\ell_i}, V_{\ell_i})$ sur $(R^{(\ell_i)}/I_{\ell_i} \cap R^{(\ell_i)})^* \times (R^{(\ell_1\ell_2)}/I_{\ell_i})^*$.

L'image de $r_{\ell_i}(\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_{D_{2\ell_1\ell_2}}, O_{\bar{\mathbb{Q}}}^*))$ par cet isomorphisme est égale à : $\pi_{\ell_i}(R^{(\ell_i)*}) \times \pi_{\ell_i}(R^{(\ell_1\ell_2)*})$. En outre on sait que tout élément de $(R^{(\ell_i)}/I_{\ell_i} \cap R^{(\ell_i)})^*$ a pour représentant l'image par π_{ℓ_i} d'une unité cyclotomique de $R^{(\ell_i)}$. On obtient ainsi pour i = 1 ou 2 un isomorphisme de groupe :

$$E_{\ell_i}(D_{2\ell_1\ell_2}) \simeq (R^{(\ell_1\ell_2)}/I_{\ell_i})^* \Big/ \pi_{\ell_i}(R^{(\ell_1\ell_2)*})$$

ceci nous permet de définir ψ.

Application numérique

Nous cherchons un couple de nombres premiers impairs distincts $\{\ell_1, \ell_2\}$ tel que le noyau de l'homomorphisme v défini précédemment ne soit pas réduit à l'élément neutre ; la proposition 2.1. implique qu'alors u n'est pas injectif. Nous choisissons $\ell_1 = 5$; dans ce cas $K^{(5)}$ est une extension quadratique réelle de $\mathbb{Q}$ dont nous choisissons une unité fondamentale : $x_o = \eta_5 + \eta_5^{-1} + 1$. Choisissons $\ell = \ell_2 \equiv 2$ ou 3 (modulo 5) le groupe $(R^{(5\ell)}/I_\ell)^*$ est un groupe cyclique dont l'ordre est égal à $(\ell^2 - 1)$. Notons $U_5(R^{(5\ell)})$ (resp. $U_5(R^{(5)})$) le groupe des unités de $R^{(5\ell)}$ (resp. $R^{(5)}$) congrues à 1 mod. $(1 - \eta_5)$. On a les égalités numériques suivantes :

$$|\pi_{5\ell}(R^{(5\ell)*})| = |\pi_5(R^{(5\ell)*})|\,|\pi_\ell(U_5(R^{(5\ell)}))|$$

et donc :

$$|\mathrm{Ker}\, u| = |\mathrm{Ker}\, v| = |\pi_\ell(R^{(5\ell)*})| \,/\, |\pi_\ell(U_5(R^{(5\ell)}))|.$$

Si m est un nombre entier on note m_2 l'entier 2^α si 2^α divise m et $2^{\alpha+1}$ ne divise pas m.

LEMME. - (i) $|\pi_\ell(x_o)|_2 = 2(\ell+1)_2$.

(ii) Si $\ell \equiv 1 \pmod 4$, $|\pi_\ell(U_5(R^{(5\ell)}))|_2$ divise $(\ell-1)_2$.

En utilisant le polynôme minimal de x_o sur $\mathbb{Q}$ on vérifie la congruence : $\pi_\ell(x_o)^{\ell+1} \equiv -1 \pmod{I_\ell}$ ce qui démontre (i).

La norme usuelle de $K^{(5\ell)}$ sur $K^{(5)}$ induit un homomorphisme de $U_5(R^{(5\ell)})$ dans $U_5(R^{(5)})$; elle induit en outre l'homomorphisme : $x \to x^{(\ell-1)}$ sur le groupe $(R^{(5\ell)}/I_\ell)^*$ donc $[\pi_\ell(U_5(R^{(5\ell)})) : \pi_\ell(U_5(R^{(5)}))]$ divise $(\ell-1)$. Le groupe $\pi_\ell(U_5(R^{(5)}))$ est engendré par $-\pi_\ell(x_o)^2$; donc en utilisant (i), lorsque $\ell \equiv 1 \pmod 4$, $|\pi_\ell(U_5(R^{(5)}))|$ divise $(\ell+1)/2$ ce qui implique que $|\pi_\ell(U_5(R^{(5)}))|_2 = 1$ et donc on obtient (ii).

Il nous suffit, pour donner l'exemple d'un groupe diédral pour lequel u n'est pas un isomorphisme, de trouver un nombre premier impair ℓ vérifiant les congruences : $\ell \equiv 2$ ou $3 \pmod 5$, $\ell \equiv 1 \pmod 4$ tel que $|\pi_\ell(R^{(5\ell)*})|_2 = 2(\ell-1)_2$. Prenons $\ell = 13$ et $x_1 = (\eta_{65} + \eta_{65}^{-1} - 2)$. Cette unité de $R^{(65)*}$ vérifie l'égalité : $\pi_{13}(x_1)^6 = \pi_{13}(x_o)$ et donc $|\pi_{13}(x_1)|_2 = 8$. Donc le groupe $\operatorname{Ker} u_{D_{130}}$ contient un 2-groupe non trivial.

Appendice II (Exemple de Calcul y)

On désigne par y la solution particulière considérée au paragraphe précédent. Lorsque $(N|K)$ est une extension modérément ramifiée de corps de nombres, l'application $y(\ ,N|K)$ est déterminée dès qu'on connaît $y(\theta, N|K)$ pour les caractères irréductibles θ de $G(N|K)$. Nous allons donner ces valeurs lorsque le groupe $G(N|K)$ est le groupe quaternionien H_{4m} où m désigne un nombre entier impair.

On adopte les notations suivantes : E est l'unique extension quadratique de K contenue dans N, M (resp. L) est l'unique extension de degré m (resp. quadratique) de E contenue dans N. Les quatre caractères de degré 1 de $G(N|K)$ proviennent des caractères de degré 1 de $G(L|K)$; on note θ l'unique

caractère quadratique de $G(N|K)$ non trivial ; il provient du caractère non trivial de $G(E|K)$. Si on note φ^* le caractère de $G(N|K)$ induit par un caractère φ de $G(N|E)$ on a deux familles de caractères de degré 2 irréductibles de $G(N|K)$: la famille A des caractères irréductibles orthogonaux, qui sont les caractères $(\chi u_o)^*$ où χ provient du caractère χ non trivial de degré 1 de $G(M|E)$ et u_o est le caractère trivial de $G(L|E)$ et la famille $\tilde{A}$ des caractères irréductibles symplectiques qui sont les caractères $(\chi u)^*$ où u provient du caractère quadratique non trivial de $G(L|E)$. Si ψ est l'élément $(\chi u_o)^*$ de A on note $\tilde{\psi}$ l'élément $(\chi u)^*$ de $\tilde{A}$. On note ψ_o (resp. $\tilde{\psi}_o$) le caractère réductible orthogonal (resp. symplectique) u_o^* (resp. u^*).

LEMME . - *Si ψ appartient à A alors l'idéal $f(\psi-\psi_o)$ est un carré dans K.*

Le caractère $(\psi-\psi_o)$ est à valeurs réelles, l'extension N de K est modérément ramifiée et $\det(\psi-\psi_o)$ est trivial. Ce résultat est démontré dans [11].

PROPOSITION *Si N est une extension modérément ramifiée de K dont le groupe de Galois est le groupe quaternionien H_{4m} où m est un entier impair $y(\ ,N|K)$ est définie sur les caractères irréductibles par les égalités suivantes :*

(i) *si* $\psi(1)=1$, $y(\psi,N|K)=1$

(ii) *si* ψ *appartient à* A, $y(\psi,N|K)=\theta[f(\psi-\psi_o)^{\frac{1}{2}}]$

(iii) *si* $\tilde{\psi}$ *appartient à* $\tilde{A}$, $y(\tilde{\psi},N|K)=1$.

On sait que (iii) est vérifié par définition même. Si ψ est un caractère de degré 1 son ordre est une puissance de 2 et donc $\psi-\epsilon_{N|K}$ appartient à $\operatorname{Ker} d_{2,N|K}$, on a donc par définition :

$$y(\psi,N|K)=\varepsilon_2(\Delta'_2(\psi-\epsilon_{N|K}))\,y_2(\psi-\epsilon_{N|K},N|K).$$

On a $\delta'_2(\psi)=\psi$ et donc $\psi-\epsilon_{N|K}=\delta'_2(\psi-\epsilon_{N|K})$ ce qui implique que le caractère $\Delta'_2(\psi-\epsilon_{N|K})$ est le caractère nul et donc $\varepsilon_2(\Delta'_2(\psi-\epsilon_{N|K}))=1$. Le lemme 7.1. de [2] implique que $y_2(\psi-\epsilon_{N|K},N|K)$ est égal à 1 ; on a démontré (i). Démontrons (ii). Le caractère ψ_o est un caractère réductible de degré 2, somme de deux caractères de degré 1 ; le point (i) implique que $y(\psi_o,N|K)$ est égal à 1 ; donc pour tout élément ψ de A on a l'égalité :

$$y(\psi,N|K)=y(\psi-\psi_o,N|K).$$

On note $\{\ell_1, \dots, \ell_t\}$ l'ensemble des nombres premiers qui divisent l'ordre du caractère χ si ψ est égal à $(\chi u_o)^*$. Le caractère $(\psi-\psi_o)$ s'écrit sous la forme : $(\psi-\psi_o) = \sum_{i=1}^{t} \theta_{\ell_i}$ où θ_{ℓ_i} désigne l'élément de $\operatorname{Ker} d_{\ell_i, N|K}$ défini par l'égalité :

$$\theta_{\ell_i} = (\delta_{\ell_1 \dots \ell_{i-1}}(\chi)\, u_o - \delta_{\ell_1 \dots \ell_i}(\chi) u_o)^* .$$

On a l'égalité :

$$y(\psi-\psi_o, N|K) = \prod_{i=1}^{t} \varepsilon_{\ell_i}(\Delta'_{\ell_i}(\theta_{\ell_i}))\, y_{\ell_i}(\theta_{\ell_i}, N|K) .$$

Puisque $(\psi-\psi_o)_t$ est un caractère à valeurs réelles, on a : $y(\psi-\psi_o, N|K) = \pm 1$; on en déduit que $\prod_{i=1}^{t} \varepsilon_{\ell_i}(\Delta'_{\ell_i}(\theta_{\ell_i})) = 1$ et le lemme 7.1. de [2] nous donne l'égalité :

$$y_{\ell_i}(\theta_{\ell_i}, N|K) = (-\delta_{\ell_1 \dots \ell_i}(\chi) u_o)(f(\delta_{\ell_1 \dots \ell_{i-1}}(\chi) u_o - \delta_{\ell_1 \dots \ell_i}(\chi) u_o))^{-1}$$

donc :

$$y_{\ell_i}(\theta_{\ell_i}, N|K) = (-1)^{n(\delta_{\ell_1 \dots \ell_{i-1}}(\chi) u_o - \delta_{\ell_1 \dots \ell_i}(\chi) u_o)}$$

où $n(\delta_{\ell_1 \dots \ell_{i-1}}(\chi) u_o - \delta_{\ell_1 \dots \ell_i}(\chi) u_o)$ désigne le nombre d'idéaux premiers de E qui divisent $f(\delta_{\ell_1 \dots \ell_{i-1}}(\chi) u_o)$ et ne divisent pas $f(\delta_{\ell_1 \dots \ell_i}(\chi) u_o)$; en effet, puisque θ_{ℓ_i} est à valeurs réelles, on a : $y_{\ell_i}(\theta_{\ell_i}, N|K) = \varepsilon_2(y_{\ell_i}(\theta_{\ell_i}, N|K))$. On en déduit l'égalité : $y(\psi-\psi_o, N|K) = (-1)^{n(\chi u_o - u_o)} = (-1)^{n(\chi)}$. On a les égalités :

$$f(\psi) = N_{E|K} f(\chi) . \Delta(E|K)$$
$$f(\psi_o) = \Delta(E|K)$$

où $\Delta(E|K)$ désigne le discriminant de E sur K. Le lemme implique que $N_{E|K} f(\chi)$ est un carré ; le nombre d'idéaux premiers qui divisent $f(\chi)$ est donc congru modulo 2 au nombre d'idéaux premiers de K inertes dans E qui divisent $f(\psi-\psi_o)^{\frac{1}{2}}$; on en déduit donc l'égalité (ii). On remarque l'analogie de ces résultats avec les formules données par Fröhlich ([7]) ou Queyrut ([12]) pour les constantes W. Si ψ appartient à A, on a : $W(\psi, N|K) = 1$, si $\tilde{\psi}$ appartient à $\tilde{A}$, l'idéal $f(\tilde{\psi}-\tilde{\psi}_o)$ est un carré dans K et on a : $W(\tilde{\psi}, N|K) = \theta[f(\tilde{\psi}-\tilde{\psi}_o)^{\frac{1}{2}}]$.

-:-:-:-

BIBLIOGRAPHIE

[1] Ph. CASSOU-NOGUÈS, Groupe des classes de l'algèbre d'un groupe métacyclique, J. of Algebra, vol. 41 (1976), n° 1.

[2] Ph. CASSOU-NOGUÈS, Structure galoisienne des anneaux d'entiers, Proc. London Math. Soc., (à paraître).

[3] Ph. CASSOU-NOGUÈS, Quelques théorèmes de base normale d'entiers, Ann. Inst. Fourier, vol. 28 (1978), fasc. 3 (à paraître).

[4] A. FRÖHLICH, Galois module structure, Proc. Durham Symposium, Algebraic Number Fields, A. Fröhlich éd., Academic Press (1977), p. 133-191.

[5] A. FRÖHLICH, Arithmetic and Galois module structure for tame extensions, J. reine Angew. Math. 286-287 (1976), p. 380-439.

[6] A. FRÖHLICH, Artin root numbers and normal integral bases for quaternion fields, Invent. Math. 17 (1972).

[7] A. FRÖHLICH, Artin root numbers, conductors and representations for generalised quaternion groups, Proc. London Math. Soc. 28 (1974).

[8] A. FRÖHLICH and J. QUEYRUT, On the functional equation of the Artin L-function for characters of real representations, Invent. Math. 20 (1973), p. 125-138.

[9] D. HILBERT, Die theorie der Algebraishen Zahlkörper, Jahresbericht D. Math. Ver., (1897).

[10] J. MARTINET, Modules sur l'algèbre du groupe quaternionien, Ann. Sc. de l'E.N.S., 4ème série, 4 (1971), p. 299-308.

[11] J. MARTINET, Character theory and Artin L-functions, Proc. Durham Symposium, Algebraic Number Fields, A. Fröhlich éd., Academic Press, (1977), p. 1-87.

[12] J. QUEYRUT, Extensions quaternioniennes généralisées et constante de l'équation fonctionnelle des séries L-d'Artin, Publ. Math. Bordeaux 4 (1972-1973), p. 91-119.

-:-:-:-

Philippe CASSOU-NOGUÈS
U.E.R. de Mathématiques
et d'Informatique de
l'Université de Bordeaux I
351, cours de la Libération
33405 TALENCE CEDEX