Séminaire Delange-Pisot-Poitou. Théorie des nombres

Philippe Cassou-Noguès

# Structure galoisienne des anneaux d'entiers

*Séminaire Delange-Pisot-Poitou. Théorie des nombres*, tome 19, n° 1 (1977-1978), exp. n° 17, p. 1-11

<http://www.numdam.org/item?id=SDPP_1977-1978__19_1_A14_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
19e année, 1977/78, n° 17, 11 p.



19 décembre 1977

# STRUCTURE GALOISIENNE DES ANNEAUX D'ENTIERS

par Philippe CASSOU-NOGUÈS

Résumé. - Dans cet exposé, on donne une méthode nouvelle pour étudier l'ordre de l'élément défini dans le groupe des classes projectives $Cl(\mathbb{Z}[\Gamma])$ par l'anneau d'entiers d'une extension galoisienne finie et modérément ramifiée d'un corps de nombres, de groupe de Galois $\Gamma$ sur ce corps.

## 1. Introduction.

Pour tout ordre $\Lambda$ de $\mathbb{Z}$ dans l'algèbre $\mathbb{Q}[\Gamma]$ d'un groupe fini $\Gamma$, on désigne par $Cl(\Lambda)$ le groupe des classes projectives de $\Lambda$.

Soient $N$ une extension finie, galoisienne d'un corps de nombres $K$, $\Gamma$ le groupe de Galois de $N$ sur $K$, et $O_N$ l'anneau des entiers de $N$. Lorsque $N$ est une extension modérément ramifiée de $K$, ce qu'on suppose désormais réalisé, $O_N$ est un $\mathbb{Z}[\Gamma]$-module projectif. Lorsque $\Gamma$ est abélien, on sait, grâce à un résultat ancien de HILBERT et SPSEISER [11], récemment généralisé par M. TAYLOR [15], que $O_N$ est un $\mathbb{Z}[\Gamma]$-module libre. Par contre, on peut construire [13] des extensions $N$ de $K$ telles que $O_N$ ne soit pas un $\mathbb{Z}[\Gamma]$-module stablement libre. Ceci montre que l'élément défini par $O_N$ dans $Cl(\mathbb{Z}[\Gamma])$ n'est pas toujours l'élément neutre, et pose le problème de l'ordre de cet élément, qu'on note $U_{N|K}$, dans le groupe $Cl(\mathbb{Z}[\Gamma])$. Certains résultats obtenus, lorsque $\Gamma$ est quaternionien ([7], [8]), ont conduit FRÖHLICH à conjecturer que l'ordre de $U_{N|K}$ est égal à 1 ou 2, et qu'il est égal à 1, lorque les constantes de l'équation fonctionnelle des séries L d'Artin, associées aux caractères symplectiques de $\Gamma$, sont égales à 1. On sait que $U_{N|K}$ appartient au noyau noté $D(\mathbb{Z}[\Gamma])$ de l'homomorphisme induit par l'extension des scalaires de $Cl(\mathbb{Z}[\Gamma])$ sur $Cl(\mathfrak{M})$, où $\mathfrak{M}$ est un ordre maximal de $\mathbb{Q}[\Gamma]$ contenant $\mathbb{Z}[\Gamma]$ ; ce résultat avait été conjecturé lorque $K = \mathbb{Q}$ par J. MARTINET. La conjecture de Fröhlich a été jusqu'à présent démontrée pour certaines extensions non abéliennes pour lesquelles le groupe $D(\mathbb{Z}[\Gamma])$ est connu ([9], [6]).

Cet exposé est un résumé d'une méthode nouvelle qui permet d'obtenir une majoration non triviale, générale, de l'ordre de $U_{N|K}$, et de démontrer la conjecture de Fröhlich dans de nouveaux cas particuliers, notamment pour de nombreuses extensions dont le groupe de Galois est métacyclique et pour les extensions dièdrales de degré $2m$ et quaternioniennes de degré $4m$, où $m$ est un nombre entier impair. Les démonstrations de ces résultats sont donnés dans [1], [2] et [3].

Pour tout nombre premier $\ell$, FRÖHLICH définit un quotient $E_\ell(\Gamma)$ du groupe $D(\mathbb{Z}[\Gamma])$, une projection $h_\ell(\Gamma)$ de $D(\mathbb{Z}[\Gamma])$ sur ce groupe, et il démontre que l'image de $U_{N|K}$ par $h_\ell(\Gamma)$ est d'ordre 1 ou 2, et d'ordre 1 lorsque les constantes symplectiques sont égales à 1 ([5], theorème 15). On peut définir un quotient $E(\Gamma)$ de $D(\mathbb{Z}[\Gamma])$ et une projection $h(\Gamma)$ de $D(\mathbb{Z}[\Gamma])$ sur $E(\Gamma)$ qui fasse intervenir simultanément tous les nombres premiers. Nous obtenons un analogue

global du théorème précédent, qui implique le résultat de Fröhlich, pour tout nombre premier $\ell$ . De façon plus précise, on décompose $U_{N|K}$ en produit de 2 éléments $t(W_{N|K})$ , $V_{N|K}$ de $D(\underset{\sim}{Z}[\Gamma])$ , où $t(W_{N|K})$ est un élément d'ordre 1 ou 2 défini à partir des constantes d'équation fonctionnelle des séries L , égal à 1 lorsque les constantes symplectiques sont égales à 1 , et nous démontrons que $h(\Gamma)(V_{N|K})$ est égal à l'élément neutre (théorème 5.1). Nous utilisons les descriptions du groupe $Cl(\underset{\sim}{Z}[\Gamma])$ et de l'élément $U_{N|K}$ données par FRÖHLICH [5], et la démonstration du théorème 5.1 nécessite la construction de nouveaux homomorphismes du groupe des caractères virtuels de $\Gamma$ dans le groupe des racines de l'unité, satisfaisant des propriétés de congruence avec les sommes de Gauss galoisiennes. Les propriétés de ces homomorphismes et leur lien avec les constantes globales ou locales de Langlands et Deligne sont étudiées dans [1]. Le théorème 5.1 montre l'intérêt arithmétique du noyau de $h(\Gamma)$ , qu'on note $H(\underset{\sim}{Z}[\Gamma])$ . Pour tout groupe fini $\Gamma$, nous donnons une description du sous-groupe $H(\underset{\sim}{Z}[\Gamma])$ de $D(\underset{\sim}{Z}[\Gamma])$ , et nous obtenons une majoration de l'exposant de $H(\underset{\sim}{Z}[\Gamma])$ et du noyau de l'homomorphisme naturel qu'on peut définir de $H(\underset{\sim}{Z}[\Gamma])$ sur $H(\underset{\sim}{Z}[G])$ , où G est un quotient de $\Gamma$ , qui généralise les résultats de [2]. On en déduit une majoration de l'ordre de $V_{N|K}$ lorsque $\Gamma$ est le groupe de Galois de N sur K , et la démonstration de la conjecture dans certains cas particuliers.

Lorsque $\Gamma$ est un $\ell$-groupe, les groupes $H(\underset{\sim}{Z}[\Gamma])$ et $D(\underset{\sim}{Z}[\Gamma])$ sont égaux, et la méthode précédente ne permet pas de démontrer la conjecture de Fröhlich. Dans ce cas, M. TAYLOR [16] a défini, pour tout entier n , des groupes $A_n(\Gamma)$ et des homomorphismes $a_n(\Gamma)$ de $D(\underset{\sim}{Z}[\Gamma])$ sur $A_n(\Gamma)$ tels que $a_n(\Gamma)(U_{N|K})$ soit égal à l'élément neutre. Il en déduit la conjecture de Fröhlich, pour tout groupe d'ordre $\ell^3$ .

## 2. Notations ([4] et [5]).

On note $A^*$ le groupe multiplicatif des éléments inversibles d'un anneau A . Si G est un groupe fini, et x un élément de G , on note $|G|$ (resp. $|x|$ ) l'ordre de G (resp. x ). Si $\ell$ est un nombre premier, et n un nombre entier de la forme $\ell^n \ell'$ , où $\ell$ ne divise pas $\ell'$ , on note $n_\ell$ l'entier $\ell^n$ . On désigne par $\bar{\underset{\sim}{Q}}$ la clôture algébrique du corps $\underset{\sim}{Q}$ des rationnels dans le corps $\underset{\sim}{C}$ des nombres complexes. Si L est un corps de nombres, c'est-à-dire une extension finie de $\underset{\sim}{Q}$ contenue dans $\bar{\underset{\sim}{Q}}$ , on note $\Omega_L$ le groupe de Galois de $\bar{\underset{\sim}{Q}}$ sur L , $O_L$ son anneau d'entiers, Ad(L) son anneau d'adèles, J(L) son groupe d'idèles, et U(L) son groupe d'idèles unités. Pour toute place P de L , on note $L_P$ le complété de L pour la valuation P-adique. Si P est fini, on note $v_{L_P}$ la valuation de $L_P$ normalisée par $v_{L_P}(M_P) = 1$ , pour toute uniformisante $M_P$ de $L_P$ , $O_{L_P}$ l'anneau de valuation de $L_P$ et $U_P^1(L)$ le sous-groupe des éléments x de $O_{L_P}^*$ tels que $v_{L_P}(x - 1) > 0$ . Soit E une extension finie de L , k une extension de $\underset{\sim}{Q}$

contenue dans $L$, et $P$ une place de $k$. On note $E_P$ (resp. $O_{E_P}$) le produit tensoriel $k_P \otimes_k E$ (resp. $O_{k_P} \otimes_{O_k} O_E$) qu'on identifie au produit direct $\prod_{\mathfrak{P}|P} E_{\mathfrak{P}}$ (resp. $\prod_{\mathfrak{P}|P} O_{E_{\mathfrak{P}}}$), où $\mathfrak{P}$ parcourt les places de $E$ qui relèvent $P$ ; on désigne par $U_P(E)$ (resp. $U_P^1(E)$) le produit direct $\prod_{\mathfrak{P}|P} O_{E_{\mathfrak{P}}}^*$ (resp. $\prod_{\mathfrak{P}|P} U_{\mathfrak{P}}^1(E)$). Il est clair que $U_P(E)$ et $U_P^1(E)$ se plongent canoniquement dans $U(E)$.

Soient $K$ un corps de nombres, $\Gamma$ un groupe fini, $R_\Gamma$ le groupe additif des caractères virtuels de $\Gamma$, et $F$ une extension finie de $K$ qui contient les extensions $N$ de $K$ qu'on considère dans la suite de cet exposé et sur laquelle les représentations de $\Gamma$ sont réalisables. Le groupe $\Omega_K$ opère sur $R_\Gamma$ et $J(F)$ et, pour tout sous $\Omega_K$-module $G$ de $J(F)$, on note $\mathrm{Hom}_{\Omega_K}(R_\Gamma, G)$ le groupe des homomorphismes de $\Omega_K$-modules de $R_\Gamma$ dans $G$. Notons $M_n(A)$ (resp. $GL_n(A)$) l'algèbre des matrices (resp. le groupe linéaire) $n \times n$ à coefficients dans $A$. Soit $T$ une représentation de $\Gamma$ dans $GL_n(F)$, et $B$ une $K$-algèbre commutative ; $T$ induit un homomorphisme d'algèbre de $B[\Gamma]$ dans $M_n(B \otimes_K F)$. Pour tout $\alpha$ de $B[\Gamma]^*$, le déterminant de $T(\alpha)$ est un élément de $(B \otimes_K F)^*$ qui ne dépend que du caractère $\theta$ de $T$, qu'on note $\mathrm{Det}_\theta(\alpha)$. On définit par linéarité $\mathrm{Det}_\theta(\alpha)$, pour tout $\theta$ de $R_\Gamma$. Si $B$ est égal à $Ad(K)$, on note $J(K[\Gamma])$ le groupe $B[\Gamma]^*$ pour tout $\alpha$ de $J(K[\Gamma])$, l'application $(\theta \longrightarrow \mathrm{Det}_\theta(\alpha))$ définit un élément de $\mathrm{Hom}_{\Omega_K}(R_\Gamma, J(F))$ qu'on note $\mathrm{Det}(\alpha)$.

Soit $\Lambda$ un ordre de $K[\Gamma]$ contenant $O_K[\Gamma]$. On note $U(\Lambda)$ le produit direct $\prod_P \Lambda_P^*$, où $P$ parcourt l'ensemble des places de $K$, et où $\Lambda_P$ désigne $O_{K_P} \otimes_{O_K} \Lambda$ (resp. $K_P[\Gamma]$), lorsque $P$ est une place finie (resp. infinie). Il est clair que $U(\Lambda)$ est un sous-groupe de $J(K[\Gamma])$, et on note $\mathrm{Det}\, U(\Lambda)$ l'image de $U(\Lambda)$ par l'application déterminant dans $\mathrm{Hom}_{\Omega_K}(R_\Gamma, J(F))$. FRÖHLICH [5] a démontré que $Cl(\Lambda)$ est isomorphe au groupe quotient :

$$\mathrm{Hom}_{\Omega_K}(R_\Gamma, J(F))/\mathrm{Hom}_{\Omega_K}(R_\Gamma, F^*)\ \mathrm{Det}\, U(\Lambda)\ .$$

Lorsque $\Lambda$ est un ordre maximal, le groupe $\mathrm{Det}\, U(\Lambda)$ est égal au groupe $\mathrm{Hom}^+_{\Omega_K}(R_\Gamma, U(F))$ des éléments $f$ de $\mathrm{Hom}_{\Omega_K}(R_\Gamma, U(F))$ tels que $f(\theta)_P$ soit positif, pour toute place infinie $P$ de $F$ et tout caractère symplectique $\theta$ de $\Gamma$. On en déduit que le noyau $D(\mathbb{Z}[\Gamma])$ de l'homomorphisme induit par l'extension des scalaires de $Cl(\mathbb{Z}[\Gamma])$ sur $Cl(\mathfrak{M})$, où $\mathfrak{M}$ est un ordre maximal, est isomorphe au groupe suivant :

$$\mathrm{Hom}^+_{\Omega_{\mathbb{Q}}}(R_\Gamma, U(F))/\mathrm{Hom}^+_{\Omega_{\mathbb{Q}}}(R_\Gamma, O_F^*)\ \mathrm{Det}\, U(\mathbb{Z}[\Gamma])\ .$$

Soit $k$ une extension de $\mathbb{Q}$ contenue dans $K$, et $\{\sigma\}$ un système de représentants des classes à droite de $\Omega_k$ modulo $\Omega_K$. A tout $f$ de $\mathrm{Hom}_{\Omega_K}(R_\Gamma, J(F))$, on associe un élément noté $\pi_{K|k}(f)$ de $\mathrm{Hom}_{\Omega_K}(R_\Gamma, J(F))$, défini par

$$\pi_{K|k}(f)(\theta) = \prod_\sigma f(\theta^{\sigma^{-1}})^\sigma \text{ , pour tout } \theta \text{ de } R_\Gamma .$$

Soit N une extension galoisienne, finie et modérément ramifée de K , de groupe de Galois $\Gamma$ sur K . On peut trouver un élément a de $O_N$ qui engendre une base normale de N sur K et une base normale d'entiers localement, c'est-à-dire une base de $O_{N_P}$ en tant que $O_{K_P}[\Gamma]$-module libre, pour toute place finie P de K au-dessus d'un diviseur premier de $|\Gamma|$ et toute place infinie. On associe à a l'élément $b = \prod_{\gamma\in\Gamma} a^\gamma \gamma^{-1}$ de $O_N[\Gamma]$ , et on définit l'élément résolvant $(a|\theta)$ par

$$(a|\theta) = \mathrm{Det}_\theta(b) \text{ , pour tout } \theta \text{ de } R_\Gamma .$$

On note $W(\theta)$ (resp. $\tau(\theta)$ ) la constante de l'équation fonctionnelle de la série L d'Artin (resp. la somme de Gauss galoisienne) associée au caractère $\theta$ de $\Gamma$. Pour tout caractère $\theta$ symplectique (resp. non symplectique) et irréductible, on pose $W'(\theta) = W(\theta)$ (resp. 1 ), et on définit $W'(\theta)$ par linéarité, pour tout $\theta$ de $R_\Gamma$ . FRÖHLICH [5] a démontré que l'élément $U_{N|K}$ défini par $O_N$ dans $Cl(\mathbb{Z}[\Gamma])$ est représenté par l'élément $u_{N|K}$ de $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_\Gamma , U_S(F))$ défini par

$$u_{N|K}(\theta)_\ell = (\pi_{K|\mathbb{Q}}(a|\theta)\ \tau(\theta)^{-1}\ W'(\theta))_\ell ,$$

pour tout $\theta$ de $R_\Gamma$ et, pour tout $\ell$ de l'ensemble S des diviseurs premiers de $|\Gamma|$ . On a noté $U_S(F)$ le produit $\prod_{\ell\in S} U_\ell(F)$ .

On remarque qu'on obtient un élément de $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_\Gamma , U_S(F))$ , noté $W_{N|K}$ , en posant :

$$W_{N|K}(\mathbb{C})_\ell = W'(\theta)_\ell \text{ , pour tout } \ell \text{ de S et tout } \theta \text{ de } R_\Gamma .$$

On note $t(W_{N|K})$ l'élément de $D(\mathbb{Z}[\Gamma])$ défini par $W_{N|K}$ , et $V_{N|K}$ l'élément $U_{N|K}\cdot t(W_{N|K})^{-1}$ .

Pour tout nombre premier $\ell$ de S , on note $\mathrm{Ker}\ d_{\ell,\Gamma}$ le noyau de la réduction modulo $\ell$ de $R_\Gamma$ , c'est-à-dire le sous-groupe de $R_\Gamma$ des caractères virtuels $\theta$ de $\Gamma$ tels que $\theta(\gamma) = 0$ , pour tout élément $\gamma$ , $\ell$-régulier de $\Gamma$ . Si $\mathfrak{L}$ désigne le produit des relèvements premiers de $\ell$ dans $O_F$ et $V_\ell$ le groupe $(O_F/\mathfrak{L})^*$ , on définit un homorphisme naturel $r_{\ell,\Gamma}$ de $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_\Gamma , U(F))$ dans $\mathrm{Hom}_{\Omega_\mathbb{Q}}(\mathrm{Ker}\ d_{\ell,\Gamma} , V_\ell)$ en posant :

$$r_{\ell,\Gamma}(f)(\theta) = (\pi_\ell \circ f \circ i_\ell)(\theta) ,$$

pour tout f de $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_\Gamma , U(F))$ , où $\pi_\ell$ (resp. $i_\ell$ ) désigne la surjection (resp. injection) canonique de $U(F)$ sur $V_\ell$ (resp. $\mathrm{Ker}\ d_{\ell,\Gamma}$ dans $R_\Gamma$ ). On sait que, pour tout nombre premier $\ell$ , le groupe $r_{\ell,\Gamma}(\mathrm{Det}\ U_\ell(\mathbb{Z}[\Gamma]))$ est réduit à l'élément neutre. On en déduit un homomorphisme $h_\ell(\Gamma)$ de $D(\mathbb{Z}[\Gamma])$ sur le groupe quotient $E_\ell(\Gamma)$ , défini par l'égalité

$$E_\ell(\Gamma) = (\mathrm{Hom}_{\Omega_\mathbb{Q}}(\mathrm{Ker}\ d_{\ell,\Gamma}, V_\ell)/r_{\ell,\Gamma}(\mathrm{Hom}^+_{\Omega_\mathbb{Q}}(R_\Gamma , O_F^*)) ,$$

et un homorphisme $h(\Gamma)$ de $D(\underset{\sim}{Z}[\Gamma])$ sur le groupe quotient $E(\Gamma)$, défini par l'égalité

$$E(\Gamma) = (\prod_{\ell\in S} \mathrm{Hom}_{\underset{\sim}{\Omega_Q}}(\mathrm{Ker}\ d_{\ell,\Gamma}, V_\ell))/(\prod_{\ell\in S} r_{\ell,\Gamma})(\mathrm{Hom}^+_{\underset{\sim}{\Omega_Q}}(R_\Gamma, O_F^*)) .$$

On note $r_\Gamma$ l'homomorphisme $(\prod_{\ell\in S} r_{\ell,\Gamma})$.

## 3. Le groupe $H(\underset{\sim}{Z}[\Gamma])$.

Nous avons défini le groupe $H(\underset{\sim}{Z}[\Gamma])$ comme le noyau de l'homomorphisme $h(\Gamma)$ de $D(\underset{\sim}{Z}[\Gamma])$ sur $E(\Gamma)$. Compte tenu des descriptions que nous avons données de ces groupes dans le § 2, on peut identifier $H(\underset{\sim}{Z}[\Gamma])$ et le groupe quotient :

$$\mathrm{Ker}\ r_\Gamma/\mathrm{Det}\ U(\underset{\sim}{Z}[\Gamma])(\mathrm{Hom}^+_{\underset{\sim}{\Omega_Q}}(R_\Gamma, O_F^*)) \cap \mathrm{Ker}\ r_\Gamma) .$$

Pour tout nombre premier $\ell$, on désigne par $G_\ell(\underset{\sim}{Z}[\Gamma])$ le groupe quotient suivant :

$$\mathrm{Hom}_{\underset{\sim}{\Omega_Q}}(R_\Gamma, U_\ell(F)) \cap r^{-1}_{\ell,\Gamma}(\mathrm{Hom}_{\underset{\sim}{\Omega_Q}}(\mathrm{Ker}\ d_{\ell,\Gamma}, V_\ell))/\mathrm{Det}(U_\ell(\underset{\sim}{Z}[\Gamma])) .$$

On a un homomorphisme naturel $\eta_{\ell,\Gamma}$ de $G_\ell(\underset{\sim}{Z}[\Gamma])$ dans $H(\underset{\sim}{Z}[\Gamma])$, et nous désignons par $H_\ell(\underset{\sim}{Z}[\Gamma])$ l'image de $G_\ell(\underset{\sim}{Z}[\Gamma])$.

THÉORÈME 3.1.

(i) *On a l'égalité de groupes*

$$H(\underset{\sim}{Z}[\Gamma]) = \prod^* H_\ell(\underset{\sim}{Z}[\Gamma]) ,$$

*où* $\prod^*$ *désigne le produit sur les diviseurs premiers* $\ell$ *de* $|\Gamma|$.

(ii) *Si* $|\Gamma|$ *est égal à* $\ell^n \ell'$, *où* $\ell$ *est un nombre premier, et* $\ell'$ *un entier non divisible par* $\ell$, *alors l'exposant de* $H_\ell(\underset{\sim}{Z}[\Gamma])$ *divise* $\ell^{n-1}$.

On a le corollaire immédiat suivant.

COROLLAIRE 3.1. - *Si* $\Gamma$ *est un groupe fini dont l'ordre est égal à* $\ell_1^{n_1} \dots \ell_q^{n_q}$, où $\ell_i$, $1 \leqslant i \leqslant q$, *sont des nombres premiers distincts, alors l'exposant du groupe* $H(\underset{\sim}{Z}[\Gamma])$ *divise* $\ell_1^{n_1-1} \dots \ell_q^{n_q-1}$.

Ce corollaire généralise les théorèmes 3.1 et 3.2 de [2].

Nous donnons un résumé de la démonstration du théorème. Il est clair que les groupes $H_\ell(\underset{\sim}{Z}[\Gamma])$ engendrent le groupe $H(\underset{\sim}{Z}[\Gamma])$. En outre, si $\ell$ ne divise pas $|\Gamma|$, les groupes $\mathrm{Det}\ U_\ell(\underset{\sim}{Z}[\Gamma])$ et $\mathrm{Hom}_{\underset{\sim}{\Omega_Q}}(R_\Gamma, U_\ell(F))$ sont égaux, ce qui implique que le groupe $G_\ell(\underset{\sim}{Z}[\Gamma])$ est réduit à l'élément neutre. Ceci démontre (i). La démonstration de (ii) nécessite la démonstration de 2 lemmes que nous énonçons.

LEMME 3.1 ([2]). - *On a l'égalité de groupes suivante* :

$$\mathrm{Hom}_{\underset{\sim}{\Omega_Q}}(R_\Gamma, U_\ell(F)) \cap r^{-1}_{\ell,\Gamma}(\mathrm{Hom}_{\underset{\sim}{\Omega_Q}}(\mathrm{Ker}\ d_{\ell,\Gamma}, V_\ell)) = \mathrm{Hom}_{\underset{\sim}{\Omega_Q}}(R_\Gamma, U^1_\ell(F))\ \mathrm{Det}(U_\ell(\underset{\sim}{Z}[\Gamma])) .$$

On déduit de ce lemme l'isomorphisme de groupe suivant :

$$G_\ell(\underset{\sim}{Z}[\Gamma]) \simeq \mathrm{Hom}_{\underset{\sim}{\Omega_Q}}(R_\Gamma , U^1_\ell(F))/\mathrm{Det}\ U^1_\ell(\underset{\sim}{Z}[\Gamma]) ,$$

où $\mathrm{Det}\ U^1_\ell(\underset{\sim}{Z}[\Gamma])$ désigne le groupe

$$\mathrm{Hom}_{\underset{\sim}{\Omega_Q}}(R_\Gamma , U^1_\ell(F)) \cap \mathrm{Det}\ U_\ell(\underset{\sim}{Z}[\Gamma]) .$$

Désignons par $\{\theta_i\}$ , $1 \leqslant i \leqslant m$ , une famille de représentants des orbites des caractères irréductibles de $\Gamma$ sur lesquels opère le groupe de Galois sur $\underset{\sim}{Q}_\ell$ d'une clôture algébrique de $\underset{\sim}{Q}_\ell$ . A tout entier $i$ , $1 \leqslant i \leqslant m$ , on associe un facteur simple $A_i$ de $\underset{\sim}{Q}_\ell[\Gamma]$ . C'est une algèbre de matrices $M_{n_i}(D_i)$ sur un corps gauche $D_i$ , de centre $K_i$ , et on désigne par $L_i$ une extension non ramifiée de $K_i$ , sous-corps commutatif maximal de $D_i$ . Soit $\Lambda$ un ordre maximal de $\underset{\sim}{Q}_\ell[\Gamma]$ , contenant $\underset{\sim}{Z}_\ell[\Gamma]$ , qui se décompose en un produit direct $\prod_{i=1}^m \Lambda_i$ , où $\Lambda_i$ est un ordre maximal de $A_i$ contenant $O_{L_i}$ .

Pour tout élément $f$ de $\mathrm{Hom}_{\underset{\sim}{\Omega_Q}}(R_\Gamma , U^1_\ell(F))$ , on montre facilement qu'il existe un élément $a_f = (a_i)$ de $\prod_{i=1}^m U^1(L_i)$ tel qu'on ait :

$$f(\theta_i) = N_{L_i|K_i}(a_i) , \quad 1 \leqslant i \leqslant m ,$$

où $N_{L_i|K_i}$ désigne la norme usuelle de corps de $L_i$ sur $K_i$ .

Soit $\mathfrak{F}$ le conducteur central de $\Lambda$ dans $\underset{\sim}{Z}_\ell[\Gamma]$ , c'est-à-dire le plus grand idéal du centre de $\underset{\sim}{Q}_\ell[\Gamma]$ , tel qu'on ait,

$$\mathfrak{F}\,\Lambda \subset \underset{\sim}{Z}_\ell[\Gamma] .$$

Cet idéal se décompose en un produit direct $\prod_{i=1}^m \mathfrak{F}_i$ , où $\mathfrak{F}_i$ est l'idéal de $K_i$ , défini par l'égalité [10],

$$\mathfrak{F}_i = \ell^n/\theta_i(1) \cdot d(K_i)^{-1} ,$$

où $\theta_i(1)$ désigne le degré du caractère $\theta_i$ et $d(K_i)$ la différente de $K_i$ . Désignons par $v_{L_i}$ la valuation $P_i$-adique de $L_i$ , où $P_i$ est l'unique idéal maximal de $L_i$ . On a le lemme suivant.

LEMME 3.2. ([2]). - <u>Pour tout nombre entier</u> $m$ <u>et tout élément</u> $x$ <u>de</u> $U^1(L_i)$ , on a l'inégalité :

$$v_{L_i}(x^{\ell^{m-1}} - 1) \geqslant v_{L_i}(\ell^m\, d(K_i)^{-1}) .$$

Démontrons maintenant le théorème 3.1 (ii). Pour cela, nous démontrons que l'exposant de $G_\ell(\underset{\sim}{Z}[\Gamma])$ divise $\ell^{n-1}$ . Soit $x$ un élément de $G_\ell(\underset{\sim}{Z}[\Gamma])$ ; il possède (lemme 3.1) un représentant $f$ dans $\mathrm{Hom}_{\underset{\sim}{\Omega_Q}}(R_\Gamma , U^1_\ell(F))$ auquel on associe un élément $a_f$ de $\prod_{i=1}^m U^1(L_i)$ . Le lemme 3.2 implique que $a_f^{\ell^{n-1}}$ appartient à $\underset{\sim}{Z}_\ell[\Gamma]^*$ . On en déduit l'existence d'un élément $b_f$ de $\underset{\sim}{Z}_\ell[\Gamma]^*$ , tel qu'on ait

$$f^{\ell^{n-1}}(\theta_i) = \mathrm{Det}_{\theta_i}(b_f) = N_{L_i|K_i}(a_i^{\ell^{n-1}}) \ , \quad 1 \leq i \leq m \ .$$

Ceci démontre que $f^{\ell^{n-1}}$ appartient au groupe $\mathrm{Det}\, U^1_\ell(\mathbb{Z}[\Gamma])$ , et que $x^{\ell^{n-1}} = 1$ , ce qui achève la démonstration.

Soit $G$ un quotient du groupe $\Gamma$ . On a des homomorphismes naturels de $D(\mathbb{Z}[\Gamma])$ dans $D(\mathbb{Z}[G])$ , et $E(\Gamma)$ dans $E(G)$ . On en déduit des homomorphismes de $H(\mathbb{Z}[\Gamma])$ dans $H(\mathbb{Z}[G])$ et, pour tout nombre premier $\ell$ , de $H_\ell(\mathbb{Z}[\Gamma])$ dans $H_\ell(\mathbb{Z}[G])$ . On désigne par $|\Gamma_G|$ l'entier $|\Gamma|/(\mathrm{pgcd}\ (\theta_j(1))$ , où $\theta_j$ parcourt les caractères irréductibles de $\Gamma$ qui ne relèvent pas un caractère de $G$ . Le théorème 3.1 admet la généralisation suivante.

THÉORÈME 3.2. - *Soient $\Gamma$ un groupe fini, et $G$ un quotient de $\Gamma$ tel que tout caractère irréductible de $G$ se relève en un caractère irréductible de $\Gamma$ alors, si $|\Gamma_G|$ est égal à $\ell^m \ell'$ , où $\ell$ est un nombre premier et $\ell'$ un entier non divisible par $\ell$ , l'exposant du noyau de l'homomorphisme naturel de $H_\ell(\mathbb{Z}[\Gamma])$ dans $H_\ell(\mathbb{Z}[G])$ divise $\ell^{m-1}$ .*

COROLLAIRE 3.2. - *Sous les hypothèses du théorème 3.2, si*

$$|\Gamma_G| = \ell_1^{m_1} \dots \ell_q^{m_q} \ ,$$

*où $\ell_i$ , $1 \leq i \leq q$ , sont des nombres premiers distincts, alors l'exposant du noyau de l'homomorphisme naturel de $H(\mathbb{Z}[\Gamma])$ dans $H(\mathbb{Z}[G])$ divise $\ell_1^{m_1-1} \dots \ell_q^{m_q-1}$ .*

La démonstration du théorème 3.2 est donnée dans [3].

*Remarque.* - Si $G$ designe le groupe $\Gamma$ rendu abélien, les hypothèses du théorème 3.2 sont toujours réalisées.

## 4. Fonctions $y_P$ et $y$ .

Dans ce paragraphe, $P$ désigne un idéal maximal du corps $K$ . Les extensions $L$ de $K$ sont galoisiennes et de degré fini sur $K$ . On note $R_{L|K}$ le groupe $R_{G(L|K)}$ et, pour tout nombre premier $\ell$ , $\mathrm{Ker}\, d_{\ell,L|K}$ le sous-groupe

$$\mathrm{Ker}\, d_{\ell,G(L|K)} \ ,$$

où $G(L|K)$ désigne le groupe de Galois de $L$ sur $K$ . On désigne par $R_m(K)$ (resp. $R_{m,P}(K)$ ) l'ensemble des couples $(\theta\ ,\ L|K)$ , où $L$ est une extension modérément ramifiée (resp. modérément ramifiée en $P$ ) de $K$ et $\theta$ un caractère de $G(L|K)$ . On note $\mu$ le groupe des racines de l'unité.

THÉORÈME 4.1 [1]. - *Pour tout idéal premier $P$ de $K$ , il existe une application $y_P$ de $R_{m,P}(K)$ dans $\mu$ qui vérifie les propriétés suivantes :*

*(i) Pour toute extension modérément ramifiée en $P$ , $L$ de $K$ l'application $\theta \longrightarrow y_P(\theta\ ,\ L|K)$ appartient à $\mathrm{Hom}^+_{\Omega_Q}(R_{L|K}\ ,\ \mu)$ .*

(ii) Pour tout nombre premier $\ell$ et tout élément $(\theta , L|K)$ de $R_{m,P}(K)$, où $\theta$ appartient à $\operatorname{Ker} d_{\ell,L|K}$, on a la congruence

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

où $\tau_P$ désigne la somme de Gauss galoisienne locale en $P$.

Remarque. - Les sommes de Gauss galoisiennes locales sont définies et étudiées dans [14].

FRÖHLICH a défini [5], pour tout nombre premier $\ell$, des fonctions $y_{P,\ell}$ satisfaisant les congruences de (ii). Pour démontrer le théorème 4.1, nous avons construit, à partir des fonctions $y_{P,\ell}$ et de certains endomorphismes idempotents de $R_{L|K}$ liés aux opérateurs d'Adams, des fonctions $y_P$ qui conviennent, pour tout nombre premier $\ell$.

Si $L$ est une extension modérément ramifiée de $K$, la fonction

$$\theta \longrightarrow y_P(\theta , L|K)$$

est triviale, pour presque tout idéal $P$ de $K$. On définit alors une application $y$ de $R_m(K)$ dans $\mu$ par

$$y(\theta , L|K) = \prod_P y_P(\theta , L|K) ,$$

où $P$ parcourt les idéaux maximaux de $K$.

On a le corollaire suivant.

COROLLAIRE 4.1. - Il existe une application $y$ de $R_m(K)$ dans $\mu$ qui vérifie les propriétés suivantes :

(i) Pour toute extension modérément ramifiée $L$ de $K$, l'application

$$\theta \longrightarrow y(\theta , L|K)$$

appartient à $\operatorname{Hom}^+_{\Omega_{\mathbb{Q}}}(R_{L|K} , \mu)$.

(ii) Pour tout nombre premier $\ell$ et tout élément $(\theta , L|K)$ de $R_m(K)$, où $\theta$ appartient à $\operatorname{Ker} d_{\ell,L|K}$, on a la congruence

$$y(\theta , L|K) \equiv \tau(\theta , L|K) \pmod{\mathfrak{L}} ,$$

où $\tau$ désigne la somme de Gauss galoisienne.

## 5. Application à la structure des anneaux d'entiers.

THEOREME 5.1. - Si $N$ est une extension galoisienne, finie et modérément ramifiée d'un corps de nombres $K$, de groupe de Galois $\Gamma$ sur $K$, alors dans le groupe $D(\mathbb{Z}[\Gamma])$ on a l'égalité $U_{N|K} = t(W_{N|K})\, V_{N|K}$, où $t(W_{N|K})$ est un élément d'ordre 1 ou 2, égal à 1 si les constantes associées aux caractères symplectiques de $\Gamma$ sont égales à 1, et où $V_{N|K}$ appartient à $H(\mathbb{Z}[\Gamma])$.

Démontrons ce théorème, c'est-à-dire que $V_{N|K}$ appartient à $H(\underset{\sim}{Z}[\Gamma])$ . Nous avons vu, § 2 , que $V_{N|K}$ admet pour représentant dans $\mathrm{Hom}^{+}_{\underset{\sim}{\Omega}_Q}(R_\Gamma , U(F))$ l'élément $f_{N|K}$ , défini par

$$(f_{N|K}(\theta))_P = (\mathfrak{N}_{K|Q}(a|\theta)\ \tau(\theta)^{-1})_P \quad \text{(resp. 1 )},$$

pour tout caractère $\theta$ de $\Gamma$ et toute place $P$ de $K$ au-dessus (resp. qui n'est pas au-dessus) d'un diviseur premier $\ell$ de $|\Gamma|$ . Désignons par $y_{N|K}$ un élément de $\mathrm{Hom}^{+}_{\underset{\sim}{\Omega}_Q}(R_\Gamma , O_F^*)$ satisfaisant les propriétés (i) et (ii) du corollaire 4.1. Il est clair que l'élément $f_{N|K}\, y_{N|K}$ de $\mathrm{Hom}^{+}_{\underset{\sim}{\Omega}_Q}(R_\Gamma , U(F))$ est un représentant de $V_{N|K}$ qui appartient au noyau de $r_\Gamma$ . Ceci démontre le théorème.

Remarque. - Le théorème 5.1 et le corollaire 3.1 impliquent que l'ordre de $V_{N|K}$ divise strictement le degré $[N : K]$ . En outre, $O_N$ est un $\underset{\sim}{Z}[\Gamma]$-module libre, lorsque $|\Gamma|$ est sans facteur carré.

Le théorème 3.2 permet d'améliorer la majoration de $|V_{N|K}|$ que donne le théorème 3.1.

Soient $\Delta$ un sous-groupe distingué de $\Gamma$ , $G$ le groupe quotient $\Gamma/\Delta$ , $L$ le corps des invariants de $N$ par $\Delta$ , et $\varphi_G$ l'homomorphisme naturel de $H(\underset{\sim}{Z}[\Gamma])$ dans $H(\underset{\sim}{Z}[G])$ . On note $H_G(\Gamma)$ (resp. $H_0(\Gamma)$ ) l'exposant du noyau de $\varphi_G$ (resp. $\varphi_{\Gamma^{(ab)}}$ , où $\Gamma^{(ab)}$ désigne le groupe $\Gamma$ rendu abélien).

COROLLAIRE 5.1.

(i) $|V_{L|K}|$ *divise* $|V_{N|K}|$ *et* $|V_{N|K}|/|V_{L|K}|$ *divise* $H_G(\Gamma)$ .

(ii) $|V_{N|K}|$ *divise* $(H_0(\Gamma) , A(\Gamma))$ , *où* $A(\Gamma)$ *désigne l'exposant d'Artin de* $\Gamma$ . *On note* $(m , n)$ *le pgcd des entiers* $m$ *et* $n$ .

On sait que la conjecture de Fröhlich est démontrée pour toute extension abélienne de corps de nombres [15]. On peut en déduire que $|V_{N|K}|$ divise $A(\Gamma)$ . En outre, (i) implique que $|V_{N|K}|$ divise $H_0(\Gamma)$ , donc il suffit de démontrer (i) pour démontrer (ii). On peut démontrer le lemme suivant qui implique (i).

LEMME 5.1 [3]. - *On a l'égalité*

$$\varphi_G(V_{N|K}) = V_{L|K} .$$

Remarque. - En utilisant les résultats de LAM [12], on peut montrer que, lorsque les $\ell$-sous-groupes de Sylow de $\Gamma$ ne sont pas cycliques, $H_0(\Gamma)_\ell$ divise $A(\Gamma)_\ell$ . Par contre, si $\Gamma$ possède un $\ell$-sous-groupe de Sylow cyclique et distingué, $A(\Gamma)_\ell$ est égal à 1 .

Soit $\Gamma$ un groupe $(\underset{\sim}{\Gamma}_Q\ \ell)$-élémentaire, produit semi-direct d'un sous-groupe cyclique et distingué $C$ d'ordre $m$ par un $\ell$-groupe $U$ . Pour tout diviseur premier $p$ de $m$ , on note $C_p$ le $p$-sous-groupe de Sylow de $C$ . On dira que $\Gamma$ vérifie la condition (*), si, pour tout diviseur premier $p$ de $m$ , le noyau de

l'homomorphisme $s_p$ de $U$ dans $Aut(C_p)$ , défini par

$$s_p(u)(x) = uxu^{-1} \text{ , pour tout } u \text{ de } U \text{ et } x \text{ de } C_p \text{ ,}$$

est d'ordre 1 ou $\ell$ . Si $\Gamma$ est le groupe de Galois de $N$ sur $K$ , on note $L$ le corps des invariants de $C$ .

THÉORÈME 5.2. - L'élément $V_{N|K}$ est égal à l'élément neutre dans les cas particuliers suivants :

(i) $[N : K]$ est sans facteur carré.

(ii) Le groupe de Galois de $N$ sur $K$ est $\Gamma_{\underline{Q}}$-élémentaire, vérifie la condition (*) et $V_{L|K} = 1$ .

(iii) Le groupe de Galois de $N$ sur $K$ est diédral d'ordre $2m$ ou quaternionien d'ordre $4m$ , où $m$ est un nombre entier impair.

Nous avons déjà démontré (i), en outre (iii) est un cas particulier de (ii) ; il suffit donc de démontrer (ii). On sait, par le corollaire 5.1 (i), que $|V_{N|K}|$ divise $H_{\Gamma/C}(\Gamma)$ , et le théorème 3.2 implique que $\ell$ ne divise pas cet entier. Or $|V_{N|K}|$ divise $A(\Gamma)$ qui, dans ce cas, est égal à une puissance de $\ell$ ; on en déduit que $V_{N|K} = 1$ .

Remarques.

1° Lorsque $\Gamma$ est un groupe $(\Gamma_{\underline{Q}}\ \ell)$-élémentaire métacyclique ou plus généralement métabélien, la condition $V_{L|K} = 1$ de (ii) est toujours réalisée. En particulier, la conjecture est démontrée pour toute extension $N$ de $K$ dont le groupe de Galois est $(\Gamma_{\underline{Q}}\ \ell)$-élémentaire d'ordre $m\ell$ ou $m\ell^2$, avec $(\ell , m) = 1$ .

2° Si $N$ est une extension quaternionienne ou diédrale de $K$ , on a $U^2_{N|K} = 1$ ; en effet, la constante d'Artin $A(\Gamma)$ est égal à 2 .

3° L'étude de la structure de $H(\underline{Z}[\Gamma])$ , comme module sur l'anneau des $\underline{Q}$-caractères virtuels de $\Gamma$ , permet de ramener la démonstration de la conjecture au cas particulier où $\Gamma$ est $\Gamma_{\underline{Q}}$-élémentaire, et d'améliorer le théorème 5.2 [3].

## BIBLIOGRAPHIE


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

[2] CASSOU-NOGUÈS (Ph.). - Quelques théorèmes de base normale d'entiers, Annales Inst. Fourier, Grenoble, 3e série, t. 28, 1978.

[3] CASSOU-NOGUÈS (Ph.). - Modules de Frobenius et structure des anneaux d'entiers (à paraître).

[4] FRÖHLICH (A.). - Galois module structure, "Algebraic number fields ( L-functions and Galois properties) [1975, Durham], Symposium organised by the London mathematical Society", p. 133-191. - London, Academic Press, 1977.

[5] FRÖHLICH (A.). - Arithmetic and Galois module structure for tame extensions, J. für die reine und angew. Math. t. 286-287, 1976, p. 380-440.

[6] FRÖHLICH (A.). - A normal integral basis theorem, J. of Algebra, t. 39, 1976, p. 131-137.

[7] FRÖHLICH (A.). - Module invariants and root numbers for quaternion fields of degree $4\ell^r$, Proc. Cambridge phil. Soc., t. 76, 1974, p. 393-399.

[8] FRÖHLICH (A.). - Artin-root numbers and normal integral bases for quaternion fields, Invent. Math., Berlin, t. 17, 1972, p. 143-166.

[9] FRÖHLICH (A.) KEATING (E.) and WILSON (S. M. J.). - The class-group of quaternion and dihedral 2-groups, Mathematika, London, t. 21, 1974, p. 64-71.

[10] JACOBINSKI (H.). - On extensions of lattices, Michigan math. J., t. 13, 1966, p. 471-475.

[11] HILBERT (D.). - Die theorie des algebraischen Zahlkörper, Jahresbericht deutschen Math. Verein., t. 4, 1897, p. 175-525.

[12] LAM (T. Y.). - Artin exponent of finite groups, J. of Algebra, t. 9, 1968, p. 94-119.

[13] MARTINET (J.). - Modules sur l'algèbre du groupe quaternionien, Annales scient. Ec. Norm. Sup., 4e série, t. 4, 1971, p. 399-408.

[14] MARTINET (J.). - Character theory and Artin L-functions, "Algebraic number fields ( L-functions and Galois properties) [1975, Durham], Symposium organised by the London mathematical Society", p. 1-87. - London, Academic Press, 1977.

[15] TAYLOR (M.). - Galois module structure of integers of relative abelian extensions, J. für die reine und angew. Math. (à paraître).

[16] TAYLOR (M.). - Adams operations, local root numbers and the galois module stru structure of rings of integers (à paraître).

[17] ULLOM (S.). - The exponent of class groups, J. of Algebra, t. 29, 1974, p. 124-132.

(Texte reçu le 17 juin 1978)

Philippe CASSOU-NOGUÈS
U. E. R. de Mathématiques et d'Informatique
Laboratoire associé au C. N. R. S. n° 226
Université de Bordeaux-I
351 cours de la libération
33405 TALENCE CEDEX