Astérisque

JEAN COUGNARD

Résultats et problèmes sur la structure galoisienne des anneaux d'entiers

Astérisque, tome 94 (1982), p. 17-30

<http://www.numdam.org/item?id=AST_1982__94__17_0>

RÉSULTATS ET PROBLÈMES SUR LA STRUCTURE GALOISIENNE DES ANNEAUX D'ENTIERS

par

Jean COUGNARD

-:-:-:-

Introduction

a) Généralités

Avant de présenter les problèmes, donnons quelques notations. Toute extension algébrique L de degré fini sur $\mathbb{Q}$ est supposée contenue dans une clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ fixée une fois pour toutes ; notons $\Omega_L = \mathrm{Gal}(\overline{\mathbb{Q}}/L)$. Soient K une extension algébrique de degré fini sur $\mathbb{Q}$ et N une extension galoisienne de degré fini de K, de groupe de Galois $G \simeq \Omega_K/\Omega_N$. Pour toute extension L de $\mathbb{Q}$ (resp. de $\mathbb{Q}_\ell$, complété ℓ-adique de $\mathbb{Q}$ pour la place ℓ), on note $\mathfrak{O}_L$ la clôture intégrale de $\mathbb{Z}$ (resp. $\mathbb{Z}_\ell$) dans L. L'anneau $\mathfrak{O}_N$ est un $\mathfrak{O}_K[G]$-module de rang 1 et, par restriction, un $\mathbb{Z}[G]$-module de rang $[K : \mathbb{Q}]$.

C'est Hilbert qui, le premier semble-t-il, s'est intéressé à la structure de $\mathfrak{O}_N$ comme $\mathfrak{O}_K[G]$-module. En particulier, quand $\mathfrak{O}_N$ est-il $\mathfrak{O}_K[G]$-libre ? $\mathbb{Z}[G]$-libre ? On peut aisément donner une condition nécessaire : soient $\mathfrak{P}$ un idéal premier de $\mathfrak{O}_K$, $p\mathbb{Z} = \mathfrak{P} \cap \mathbb{Z}$ et $\mathfrak{P}\mathfrak{O}_N = \left(\prod_{i=1}^{g} \mathfrak{P}_i\right)^e$ la décomposition de $\mathfrak{P}\mathfrak{O}_N$ en produit d'idéaux premiers de $\mathfrak{O}_N$. On dit que N/K est modérément ramifiée en $\mathfrak{P}$ si $p \nmid e$; on dit que N/K est modérément ramifiée si elle est modérément ramifiée pour tout $\mathfrak{P}$. On a :

PROPOSITION 1. - Pour que $\mathfrak{O}_N$ soit $\mathfrak{O}_K[G]$-projectif, il faut et il suffit que N/K soit modérément ramifiée.

On a en fait le résultat plus précis suivant : si $\mathfrak{P}$ est un idéal premier de $\mathfrak{O}_K$ modérément ramifié dans N/K et $\mathfrak{O}_{K_\mathfrak{P}}$ le complété de $\mathfrak{O}_K$ en $\mathfrak{P}$, alors il existe un élément a de $\mathfrak{O}_N$ tel que $\mathfrak{O}_{K_\mathfrak{P}} \otimes_{\mathfrak{O}_K} \mathfrak{O}_N$ soit isomorphe à $\mathfrak{O}_{K_\mathfrak{P}}[G]a$. On dit que $\mathfrak{O}_N$ est localement libre en $\mathfrak{P}$ sur $\mathfrak{O}_K[G]$ ([No], [S 1]).

Dans les deux premières parties, nous supposons N/K modérément ramifiée. La première partie est consacrée aux liens entre la structure de $\mathfrak{O}_N$ comme $\mathbb{Z}[G]$-module et les constantes de l'équation fonctionnelle des fonctions L d'Artin. Dans la seconde partie, nous indiquons des résultats récents sur la structure de $\mathfrak{O}_K[G]$-module de $\mathfrak{O}_N$ lorsque $K \neq \mathbb{Q}$. Dans la troisième partie, nous donnons un aperçu des travaux effectués lorsque l'on ne dispose plus de l'hypothèse de ramification modérée. Mais avant même d'aborder la première partie, il convient de modifier le problème et, dans la question $\mathfrak{O}_N$ est-il $\mathfrak{O}_K[G]$ (ou $\mathbb{Z}[G]$)-libre, de remplacer libre par stablement libre :

Soient $\mathcal{C}_{\ell\ell}(\mathfrak{O}_K[G])$ la catégorie des $\mathfrak{O}_K[G]$-modules localement libres et $K_o(\mathfrak{O}_K[G])$ le groupe de Grothendieck de cette catégorie. Le rang d'un module localement libre permet de définir un homomorphisme de groupe de $K_o(\mathfrak{O}_K[G])$ sur $\mathbb{Z}$. Le noyau de cet homomorphisme est le groupe des classes projectives de $\mathfrak{O}_K[G]$, on le note $Cl(\mathfrak{O}_K[G])$.

On dit que deux $\mathfrak{O}_K[G]$-modules localement libres M_1 et M_2 sont stablement isomorphes s'ils ont même rang et même image dans $Cl(\mathfrak{O}_K[G])$. Il revient au même de dire que $M_1 \oplus \mathfrak{O}_K[G]$ et $M_2 \oplus \mathfrak{O}_K[G]$ sont isomorphes. Deux modules isomorphes sont stablement isomorphes mais la réciproque est fausse ([S 2]). La distinction entre isomorphe et stablement isomorphe n'existe que si $K[G]$ ne vérifie pas la condition d'Eichler ([S 2], [V]). Enfin, lorsque les modules sont de rang strictement supérieur à 1, les deux notions coïncident ([F 2]).

On peut développer ces notions avec tout autre ordre de $K[G]$.

Dans le cas des extensions modérément ramifiées, on doit donc comparer la classe de $\mathfrak{O}_N$ et celle de $\mathfrak{O}_K[G]$ (resp. $(\mathbb{Z}[G])^{[K:\mathbb{Q}]}$) dans $Cl(\mathfrak{O}_K[G])$ (resp. $Cl(\mathbb{Z}[G])$).

b) Description du groupe des classes ([F 3])

A. Fröhlich a donné une description de $Cl(\mathfrak{O}_K[G])$ particulièrement adaptée aux problèmes de structures galoisiennes des anneaux d'entiers. Soit R_G le groupe des caractères virtuels de G. Pour $\mathbb{Q} \subset L \subset \bar{\mathbb{Q}}$ et $[L:\mathbb{Q}] < \infty$, on note $J(L)$ le groupe des idèles de L et $J(\bar{\mathbb{Q}}) = \varinjlim J(L)$.

Considérons χ le caractère d'une représentation T de G ; on obtient, en prolongeant par linéarité un homomorphisme d'anneaux de $\mathfrak{O}_K[G]$ dans $M_m(\bar{\mathbb{Q}})$. Pour chaque $x \in \mathfrak{O}_K[G]^*$, le déterminant de $T(x)$: $\det(T(x))$ appartient à $\mathbb{Q}^*$; si T_1 et T_2 sont deux représentations de G correspondant au même caractère χ, on a $\det(T_1(x)) = \det(T_2(x))$. On note $\det_\chi(x)$ cet élément. L'application, qui à χ associe $\det_\chi(x)$ se prolonge en une application de R_G dans $\bar{\mathbb{Q}}^*$, commutant à l'action de Ω_K. On en déduit un homomorphisme de $\mathfrak{O}_K[G]^*$ dans $\mathrm{Hom}_{\Omega_K}(R_G, \bar{\mathbb{Q}}^*)$, on note $\mathrm{Det}((\mathfrak{O}_K[G])^*)$ son image. De façon analogue, en notant $U(\mathfrak{O}_K[G]) = \overline{\prod_p} (\mathfrak{O}_{K_p}[G]^*)$, on construit un sous-groupe $\mathrm{Det}(U(\mathfrak{O}_K[G]))$ de $\mathrm{Hom}_{\Omega_K}(R_G, \overline{\prod_p} J(\bar{\mathbb{Q}}))$. On a l'isomorphisme :

$$(1) \qquad Cl(\mathfrak{O}_K[G]) \simeq \mathrm{Hom}_{\Omega_K}(R_G, J(\bar{\mathbb{Q}}))/\mathrm{Hom}_{\Omega_K}(R_G, \bar{\mathbb{Q}}^*) \cdot \mathrm{Det}(U(\mathfrak{O}_K[G])).$$

1. - Structure de $\mathbb{Z}[G]$-module lorsque N/K est modérément ramifiée

La classe $(\mathfrak{O}_N)$ de $\mathfrak{O}_N$ se trouve dans un sous-groupe de $Cl(\mathbb{Z}[G])$: Soit $\mathfrak{M}$ un ordre maximal de $\mathbb{Q}[G]$ contenant $\mathbb{Z}[G]$ à $\mathfrak{M}$ définit un homomorphisme de $Cl(\mathbb{Z}[G])$ dans $Cl(\mathfrak{M})$ et $(\mathfrak{O}_N)$ se trouve dans le noyau $D(\mathbb{Z}[G])$ de cet homomorphisme. On peut donner une autre description de ce sous-groupe.

Soit S l'ensemble des diviseurs premiers de G, pour $p \in S$, on note $U_p = \varinjlim (\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathfrak{O}_L)^*$ et $U_S = \overline{\prod_{p \in S}} U_p$, on pose également $\bar{\mathfrak{O}}^* = \varinjlim \mathfrak{O}_L^*$ (les limites inductives étant, comme précédemment, prises sur les extensions L de degré fini de $\mathbb{Q}$) on a alors :

$$(2) \qquad D(\mathbb{Z}[G]) \simeq \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, U_S)/\mathrm{Hom}^+_{\Omega_{\mathbb{Q}}}(R_G, \bar{\mathfrak{O}}^*)\,\mathrm{Det}(\overline{\prod_{p \in S}}(\mathbb{Z}_p[G]^*)) .$$

Le signe + signifiant que l'on ne considère que les fonctions prenant des valeurs totalement positives pour les caractères symplectiques ([F 3] théorème 11 et appendice).

Par ailleurs, on peut associer à tout caractères virtuel χ de G une fonction d'Artin $\Lambda(s,\chi)$ méromorphe sur $\mathbb{C}$, vérifiant une équation fonctionnelle

$$\Lambda(s,\chi) = W(\chi)\ \Lambda(1-s,\bar{\chi}).$$

On définit ensuite :

$W'(\chi) = W(\chi)$ si χ est symplectique

$W'(\chi) = 1$ sinon.

L'extension N/K étant modérément ramifiée, W' appartient à $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, U_S)$ ([F 3]).

Le théorème suivant, démontré par M. J. Taylor résout une conjecture de Fröhlich.

THÉORÈME 1 ([T 2]). - L'image (W') de W' dans $Cl(\mathbb{Z}[G])$ est égale à $(\mathfrak{O}_N)$.

Les premières conséquences sont immédiates : les valeurs de W' étant ± 1, on a $\mathfrak{O}_N \oplus \mathfrak{O}_N \simeq (\mathbb{Z}[G])^{2[K:\mathbb{Q}]}$ et, par ailleurs, si l'ordre de G n'est pas divisible par 4, $\mathfrak{O}_N \simeq \mathbb{Z}[G]^{[K:\mathbb{Q}]}$.

Une conséquence plus inattendue est la suivante :

COROLLAIRE ([F 6]). - Si l'ordre de G est m et si K contient les racines m-ièmes de l'unité, alors $\mathfrak{O}_N$ est $\mathbb{Z}[G]$-libre.

Ceci tient au fait qu'alors $(W') = 1$ et $[K:\mathbb{Q}] \geq 2$. Avant de démontrer le théorème, il faut construire une fonction de R_G dans U_S, commutant avec l'action de $\Omega_{\mathbb{Q}}$ et représentant $(\mathfrak{O}_N)$. A chaque caractère virtuel χ de G, on associe la somme de Gauss galoisienne $\tau_{N/K}(\chi)$ ([M], [F 3]). Par ailleurs, la proposition 1 associée au théorème d'approximation faible montre l'existence d'un élément a de $\mathfrak{O}_N$ tel que, pour p de S :

$$(\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathfrak{O}_K[G])\, a \simeq \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathfrak{O}_N .$$

Soient alors $\{\sigma\}$ un système de représentants des classes de $\Omega_{\mathbb{Q}}/\Omega_K$ et $A = \overline{\prod_{\sigma} \left(\sum_{g \in G} g\sigma(a).g^{-1} \right)} \in M[G]$ (M clôture galoisienne de N sur $\mathbb{Q}$). L'élément A définit une application Det(A) de R_G dans $\bar{\mathbb{Q}}^*$. Fröhlich démontre ([F 3] théorème 4) que $\mathrm{Det}(A)\,\tau_{N/K}^{-1}$ est un élément de $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, U_S)$ et que $(\mathfrak{O}_N)$ est représenté par $u = \mathrm{Det}(A)\,\tau_{N/K}^{-1} W'$.

Indications sur la méthode suivie par M. J. Taylor ([T 1], [T 2])

Il suffit de prouver que $\mathrm{Det}(A)\,\tau_{N/K}^{-1}$ appartient à $\mathrm{Hom}^{+}_{\Omega_{\mathbb{Q}}}(R_G, \bar{\mathfrak{O}}^*)\ \mathrm{Det}(\overline{\prod_{p\in S} \mathbb{Z}_p[G]^*})$. Comme les sommes de Gauss se décomposent en produits de facteurs locaux $\tau_{N/K,\mathfrak{P}}$, on se ramène à un problème local. Pour chaque place $\mathfrak{P}$ de K, on utilise la fonction $y_{\mathfrak{P}}$ définie par Deligne ([D]) appartenant à $\mathrm{Hom}^{+}_{\Omega_{\mathbb{Q}}}(R_G, U_S)$ ([F-T]) et qui satisfait certaines congruences ([F 3] théorème 13). Taylor démontre qu'il existe une extension E de K, galoisienne sur $\mathbb{Q}$ telle que

$$(3) \qquad * \quad \mathrm{Det}(A)\overline{\prod_{\mathfrak{P}\mid \ell}} \tau_{N/K,\mathfrak{P}}^{-1}\, y_{\mathfrak{P}}^{-1} \in \mathrm{Det}\Big(\overline{\prod_{\mathfrak{L}\mid \ell}} \mathfrak{O}_{E_{\mathfrak{L}}}[G]^*\Big)$$

$$(3') \qquad * \quad \tau_{N/K,\mathfrak{P}}\, y_{\mathfrak{P}} \in \mathrm{Det}\Big(\overline{\prod_{\mathfrak{p}\mid \ell}} (\mathfrak{O}_{K_{\mathfrak{p}}}[G]^*)\Big) \quad \text{si } \mathfrak{P}\not| \ell\,.$$

(On a en particulier $\tau_{N/K,\mathfrak{P}} = y_{\mathfrak{P}} = 1$ si $\mathfrak{P}$ n'est pas ramifié dans $M/\mathbb{Q}$.)

On en déduit que la ℓ-composante de uW' appartient à $\Big(\overline{\prod_{\mathfrak{L}\mid \ell}} \mathrm{Det}(\mathfrak{O}_{E_{\mathfrak{L}}}[G]^*)\Big)^{\mathrm{Gal}(E/\mathbb{Q})}$.

Il faut maintenant utiliser le "logarithme entier" pour montrer que ce groupe est inclus dans $\mathrm{Det}(\mathbb{Z}_\ell[G]^*)$, puis procéder de même pour chacune des places $\ell \in S$.

Mais, pour arriver aux propriétés (3) et (3'), on constate qu'il suffit de montrer que les fonctions $\tau_{N/K,\mathfrak{P}}\, y_{\mathfrak{P}}$ appartiennent à un groupe $\mathrm{Det}(\ )$. C'est ici que le formalisme introduit par Fröhlich pour décrire $\mathrm{Cl}(\mathbb{Z}[G])$ et $D(\mathbb{Z}[G])$ prend tout son intérêt. En travaillant avec R_G, et non avec un facteur simple de $\mathbb{Q}[G]$, il met en évidence des propriétés fonctorielles liées aux changements de groupes ([F 3], appendice). Or on a des propriétés semblables pour les sommes de Gauss. Ceci permet à Taylor d'utiliser un théorème de Brauer sur la représentation des groupes et de se ramener d'abord au cas où G est un groupe élémentaire puis au cas où G est un p-groupe. Là, à nouveau, il peut utiliser son "logarithme entier" pour vérifier des congruences sur les sommes de Gauss et conclure.

La fonction W' permet de connaître la structure de $\mathfrak{O}_N$ comme $\mathbb{Z}[\mathrm{Gal}(N/K)]$-module. Le problème inverse de la détermination de W' à partir de propriétés algébriques de $\mathfrak{O}_N$ vient d'être résolu ([C.N-T]). La seule

structure de $\mathbb{Z}[G]$-module de $\mathfrak{O}_N$ n'étant pas suffisante ([F 4]), il convient de lui ajouter une structure hermitienne ([F 4]).

2. - Structure de $\mathfrak{O}_K[G]$-module lorsque N/K est modérément ramifiée ($K \neq \mathbb{Q}$)

On a peu de résultats précis dans le cas "relatif". Il semble qu'aucune conjecture ne soit envisagée à l'heure actuelle.

Pour un certain nombre d'extensions abéliennes, L. Mc Culloh sait déterminer quels sont les éléments de $Cl(\mathfrak{O}_K[G])$ qui sont de la forme $(\mathfrak{O}_N)$ [Mc C 1], [Mc C 2].

Récemment, une nouvelle approche a été tentée par I. Brinkhuis ([Br]) liant ce problème aux problèmes de plongement des extensions, ce qui impose certaines contraintes :

Soient K/k une extension galoisienne de groupe de Galois $Gal(K/k)$, une suite exacte d'homomorphismes de groupes :

$$(E) \qquad 1 \longrightarrow \Delta \longrightarrow \Gamma \longrightarrow \Sigma \longrightarrow 1$$

et un isomorphisme entre Σ et $Gal(K/k)$. On fait opérer Γ sur $K[\Delta]$ par :

$$\forall v \in K, \ \forall \delta \in \Delta, \ \forall \gamma \in \Gamma \qquad \gamma(v\,\delta) = \gamma(v)\ \gamma\,\delta\,\gamma^{-1}$$

où l'action de Γ sur K se fait via Σ.

Considérons A un sous-anneau de $K[\Delta]$ stable par l'action de Γ et cherchons une extension N de K galoisienne sur k avec des isomorphismes entre $Gal(N/K)$ (resp. $Gal(N/k)$) et Δ (resp. Γ) de sorte que le diagramme suivant soit commutatif.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Delta & \longrightarrow & \Gamma & \longrightarrow & \Sigma & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & Gal(N/K) & \longrightarrow & Gal(N/k) & \longrightarrow & Gal(K/k) & \longrightarrow & 1 \end{array}$$

et qu'en plus $A\mathfrak{O}_N$ soit A isomorphe à A.

Lorsque $A = K[\Delta]$, on obtient le problème de plongement usuel, pour $A = \mathfrak{O}_K[\Delta]$, on obtient le problème de plongement avec base normale. On a la condition nécessaire :

PROPOSITION 2. - Supposons que ce problème de plongement ait une solution, alors l'application $\rho_\Delta : \Delta \longrightarrow A^*$ définie par $\rho_\Delta(\delta) = \delta^{-1}$ se prolonge en un 1-cocycle ρ_A de Γ dans A^* .

Si, maintenant, on suppose que Δ est abélien, on peut avoir une meilleure interprétation. Considérons la suite exacte de Hochschild-Serre ([Mc L]) :

$$1 \longrightarrow H^1(\Sigma, A^*) \xrightarrow{\inf} H^1(\Gamma, A^*) \xrightarrow{\text{res}} H^1(\Delta, A^*)^\Sigma \xrightarrow{\tau} H^2(\Sigma, A^*)$$
$$\uparrow$$
$$H^2(\Sigma, \Delta)$$

où l'homomorphisme de $H^2(\Sigma, \Delta)$ dans $H^2(\Sigma, A^*)$ se déduit de l'injection de Δ dans A^* .

La suite exacte (E) définit un élément C_E de $H^2(\Sigma, \Delta)$; si le problème du plongement possède une solution, l'image de C_E dans $H^2(\Sigma, A^*)$ est égale à celle de $[\rho_A]$ par la transgression τ .

Supposons, pour la suite de ce paragraphe que $A = \mathfrak{O}_K[\Delta]$ et que Δ est abélien. La suite exacte de Hochschild-Serre se révèle plus efficace si on la rapproche d'une suite exacte due à Fröhlich et C. T. C. Wall ([F-W]). On a :

$$\begin{array}{ccccccc}
1 \longrightarrow & H^1(\Sigma, \Delta) & \longrightarrow & H^1(\Omega_k, \Delta) & \longrightarrow & H^1(\Omega_K, \Delta)^\Sigma & \xrightarrow{\tau} H^2(\Sigma, \Delta) \\
& \downarrow & & \vdots\, g_k & & \vdots\, g & \downarrow \\
1 \longrightarrow & H^1(\Sigma, \mathfrak{O}_K[\Delta]^*) & \longrightarrow & \mathrm{Pic}(\mathfrak{O}_K[\Delta], \Sigma) & \longrightarrow & \mathrm{Pic}(\mathfrak{O}_K[\Delta])^\Sigma & \longrightarrow H^2(\Sigma, \mathfrak{O}_K[\Delta]^*).
\end{array}$$

On a des homomorphismes naturels entre les groupes qui se trouvent aux extrémités de chaque ligne. On constate que $H^1(\Omega_K, \Delta)^\Sigma = \mathrm{Hom}_\Sigma(\Omega_K, \Delta)$; à un homomorphisme surjectif de Ω_K sur Δ correspond une extension galoisienne N de K , également galoisienne sur k . Brinkhius construit des applications "faiblement multiplicatives" g (resp. g_k) de $H_1(\Omega_K, \Delta)^\Sigma$ (resp. $H^1(\Omega_K, \Delta)$) dans $\mathrm{Pic}(\mathfrak{O}_K[\Delta])^\Sigma$ (resp. $\mathrm{Pic}(\mathfrak{O}_K[\Delta], \Sigma)$) : en particulier si f_1 et f_2 sont deux éléments surjectifs de $\mathrm{Hom}_\Sigma(\Omega_K, \Delta)$ correspondant à des extensions de discriminants (relativement à K) premiers entre eux alors $g(f_1 f_2) = g(f_1)\, g(f_2)$.

Soit alors N une extension de K , modérément ramifiée sur K , galoisienne sur K correspondant à un élément f de $H^1(\Omega_K, \Delta)^\Sigma$ l'image $\tau(f)$ est la classe de

l'extension de groupe :

$$1 \longrightarrow \mathrm{Gal}(N/K) \longrightarrow \mathrm{Gal}(N/k) \longrightarrow \mathrm{Gal}(K/k) \longrightarrow 1$$

et son image par g est la classe de $\mathfrak{O}_N$ dans $\mathrm{Pic}(\mathfrak{O}_K, \Delta)$.

On peut donc, étant données une classe dans $H^2(\Sigma, \Delta)$ et une autre dans $\mathrm{Pic}(\mathfrak{O}_K[\Delta])^{\Sigma}$, se poser la question de savoir s'il existe un élément surjectif f de $\mathrm{Hom}_{\Sigma}(\Omega_k, \Delta)$ dont elles soient les images. Bien entendu, il est nécessaire que ces deux classes aient même image dans $H^2(\Sigma, \mathfrak{O}_K[\Delta]^*)$. C'est l'étude de cette condition qui conduit au résultat suivant :

THÉORÈME 2 ([Br]) : Soit N/K une extension abélienne de groupe de Galois Δ, abélien d'exposant; n ; soit μ_n une racine primitive n-ième de l'unité. On suppose que $K/\mathbb{Q}$ est abélienne, modérée, et qu'il existe un sous-corps k de K vérifiant les hypothèses :

- $K \cap k(\mu_n) = k$
- $1 \longrightarrow \mathrm{Gal}(N/K) \longrightarrow \mathrm{Gal}(N/k) \longrightarrow \mathrm{Gal}(K/k) \longrightarrow 1$ est une extension centrale non scindée dont la classe de cohomologie est d'ordre impair.

Dans ces conditions $\mathfrak{O}_N$ ne possède pas de $\mathfrak{O}_K$-base normale.

Exemple 1. - Soient ℓ un nombre premier impair, $N/\mathbb{Q}$ une extension cyclique de degré ℓ^2 et K le sous-corps de degré ℓ. L'extension N/K ne possède pas de $\mathfrak{O}_K$-base normale.

Exemple 2. - Soient ℓ un nombre premier impair, p un nombre premier congru à 1 modulo ℓ^2, $N = \mathbb{Q}^{(p)}$ et K l'unique sous-corps de degré $p-1/\ell$. L'extension N/K ne possède pas de base normale.

L'étude du même carré commutatif conduit pour $\ell = 2$ également à des résultats originaux ([Br]) :

Soient $K = \mathbb{Q}(\sqrt{d})$ une extension quadratique réelle ($d \equiv 1(4)$), ε l'unité fondamentale ; on suppose que $N_{K/\mathbb{Q}}(\varepsilon) = -1$. Les $\mathfrak{O}_K[\mathbb{Z}/2\mathbb{Z}]$ modules de rang 1 réalisables comme anneaux d'entiers forment un sous-groupe de $\mathrm{Pic}(\mathfrak{O}_K[\mathbb{Z}/2\mathbb{Z}])$ isomorphe au sous-groupe des éléments d'ordre 2 du groupe des classes de K Considérons les extensions quadratiques N de K, cycliques sur

$\mathbb{Q}$ et n'ayant pas de ramification en dehors de celle de $K/\mathbb{Q}$: toutes les classes réalisables sont réalisées une fois et une seule par un corps N de ce type.

3. - Les extensions sauvagement ramifiées

La condition de la proposition 1 n'est plus vérifiée. Le module $\mathfrak{O}_N$ n'est plus $\mathfrak{O}_K[G]$-projectif et donc n'est plus $\mathbb{Z}[G]$-projectif. Il n'est plus question de chercher son image dans $Cl(\mathbb{Z}[G])$. Face à cette situation, plusieurs directions de recherches donnant lieu à des exemples, des contre-exemples et quelques résultats synthétiques ont été explorées : soit en essayant d'étudier $\mathfrak{O}_N$ sur un autre ordre que $\mathbb{Z}[G]$, soit en introduisant une autre catégorie de $\mathbb{Z}[G]$-modules.

1°) L'ordre associé

Soit $\Lambda = \{\lambda \in K[G],\ \lambda \mathfrak{O}_N \subset \mathfrak{O}_N\}$ l'ordre associé à $\mathfrak{O}_N$ dans $K[G]$. Lorsque $K = \mathbb{Q}$, on peut, pour un certain nombre de groupes, montrer que $\mathfrak{O}_N$ est Λ-localement libre et parfois Λ-libre ([L], [B 1], [J]) ; malheureusement A.-M. Bergé ([B 2]) a construit des exemples où $\mathfrak{O}_N$ n'est pas Λ-projectif, et mis en évidence des phénomènes qui expliquent ces propriétés ([B 3]).

2°) L'ordre maximal

On sait ([R]) que tout module de type fini, sans torsion, sur un ordre maximal est localement libre. Pour un ordre maximal $\mathfrak{M}$ de $\mathbb{Q}[G]$ on construit le $\mathfrak{M}$-module $\mathfrak{M}\,\mathfrak{O}_N$. Là encore le comportement est agréable pour certaines familles de groupes ([C 1], [F 5]) mais devient vite décevant ([C 2], [W]), la $\mathfrak{M}$-structure de $\mathfrak{M}\,\mathfrak{O}_N$ pouvant dépendre étroitement de l'ordre $\mathfrak{M}$ choisi. A moins qu'il n'existe un ordre maximal privilégié. Cette question est en fait liée à des résultats de M. J. Taylor ([T 3], [T 4]) qui envisage le rôle de l'ordre maximal sous un autre aspect, dans un certain nombre de cas particuliers : Soit $\mathfrak{M}$ un ordre maximal de $\mathbb{Q}[G]$ contenant $\mathbb{Z}[G]$ au lieu de considérer $\mathfrak{M}\,\mathfrak{O}_N$, il étudie $\mathfrak{O}_N^{(\mathfrak{M})}$ le plus grand $\mathfrak{M}$-module inclus dans $\mathfrak{O}_N$. Il suppose en outre :

- tous les caractères absolument irréductibles de G sont de la forme $\chi_* = \mathrm{Ind}_{H_{\chi_*}}^{G}(\chi)$ où χ est un caractère de degré 1 d'un sous-groupe H_{χ_*} de G

et de plus, $\mathbb{Q}(\chi) = \mathbb{Q}(\chi_*)$

- si n est l'exposant du groupe G, K contient les racines n-ièmes de l'unité. On peut écrire $\mathbb{Q}[G] \simeq \bigoplus_{\chi_*} M_{[G:H_{\chi_*}]}(\mathbb{Q}(\chi_*))$ et donc

$$K[G] \simeq \bigoplus_{\chi_*} M_{[G:H_{\chi_*}]}(K \otimes_{\mathbb{Q}} \mathbb{Q}(\chi_*)) .$$

L'ordre $R(\chi_*) = M_{[G/H_{\chi_*}]}(\mathbb{Z}[\chi_*])$ (resp. $R_K(\chi_*) = M_{[G:H_{\chi_*}]}(\mathfrak{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}[\chi])$) est un ordre maximal de $M_{[G:H_{\chi_*}]}(\mathbb{Q}(\chi_*))$ (resp. $M_{[G:H_{\chi_*}]}(K \otimes_{\mathbb{Q}} \mathbb{Q}(\chi_*))$). On a alors :

THÉORÈME 3. - Le plus grand $R_K(\chi_*)$-module inclus dans $\mathfrak{O}_N$ est isomorphe à $R_K(\chi_*)$ comme $R(\chi_*)$-module.

En fait l'intérêt pour $\mathfrak{O}_N^{(m)}$ remonte, au moins, à un article de Fröhlich ([F 1]), article qui est à l'origine d'un travail d'A. Nelson en partie publié ([N1], [N2]). Comme le travail précédent de Taylor, celui de Nelson met l'accent sur les représentations monomiales.

3°) Les représentations monomiales

Soit l'ensemble des couples (H, φ) où H est un sous-groupe de G et φ un caractère de degré un de H. Par conjugaison intérieure, le groupe G opère sur ces couples. Considérons $M_{G, \mathbb{C}^*}$ le groupe abélien libre engendré par les classes de conjugaison (en fait, on peut définir une structure d'anneau sur cet ensemble : [Dr], [D]). L'induction des caractères permet de définir un homomorphisme d'anneaux de $M_{G, \mathbb{C}^*}$ dans R_G.

On peut également construire un anneau A_G en définissant une multiplication sur le groupe abélien libre engendré par les classes de conjugaison des couples (Δ, Σ) où $\Sigma \subset \Delta \subset G$, Σ distingué dans Δ et Δ/Σ abélien ([N1]. On construit un homomorphisme de groupes η_G de A_G dans $M_{G, \mathbb{C}^*}$ par :

$$\eta_G((\Delta, \Sigma)) = \sum_{\varphi|\Sigma = 1} (\Delta, \varphi) .$$

Ces anneaux et les applications définies ont de "bonnes" propriétés relativement aux opérations liées aux changements de groupes ([N1]).

Soient maintenant L un corps de nombres, Γ un groupe abélien et $\mathfrak{M}$ l'ordre maximal de $L[G]$ relativement à $\mathfrak{O}_L$ (Γ étant abélien il est unique). Pour tout $\mathfrak{O}_L[\Gamma]$-module M engendrant un $L[\Gamma]$-module libre de rang n, on désigne par $M^{(\mathfrak{M})}$ le plus grand $\mathfrak{M}$-module inclus dans M et on définit :

$$b(M, \mathfrak{O}_L[\Gamma]) = [\mathfrak{M} : \mathfrak{O}_L[\Gamma]]^{2n} / [M : M^{(\mathfrak{M})}]^2$$

(idéal fractionnaire de $\mathfrak{O}_L$, introduit par Fröhlich, à l'aide d'invariants relatifs de réseaux dans [F1]).

Revenons à notre situation initiale où K est un corps de nombres, G un groupe fini et M un $\mathfrak{O}_K[G]$-module engendrant un $K[G]$-module libre. On définit un homomorphisme de groupes b_M de A_G dans le groupe I_K des idéaux fractionnaires de K en posant, pour un générateur (Δ, Σ) :

$$b_M((\Delta, \Sigma)) = b(M^{\Sigma}, \mathfrak{O}_K[\Delta/\Sigma]).$$

On dit que le module M est "monomialement factorisable" si b_M se factorise par $M_{G, \mathbb{C}^*}$ via η_G. On peut aisément trouver des modules qui ne vérifient pas cette propriété ([N1]), en revanche :

THÉORÈME 4 ([N1], [N2]). - <u>L'anneau des entiers $\mathfrak{O}_N$ est monomialement factorisable</u>.

<u>Remarque</u>. - L'application qui factorise $b_{\mathfrak{O}_N}$ se décrit en termes d'invariants arithmétiques.

4°) <u>Changement de catégorie</u>

Il s'agit essentiellement des idées de J. Queyrut ([Q1], [Q2], [C.N-Q]. Soit S l'ensemble des diviseurs premiers p de l'ordre de G pour lesquels il existe un idéal premier $\mathfrak{P}$ de N, au-dessus de p, sauvagement ramifié dans N/K.

On définit le groupe $G_{\oplus}^{S}(\mathbb{Z}[\Gamma])$ de la façon suivante : c'est le quotient du groupe abélien libre engendré par les classes d'isomorphismes de $\mathbb{Z}[G]$-modules de type fini, sans torsion, par le sous-groupe engendré par les éléments $(M) - (M') - (M'')$ où

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

est une suite exacte localement scindée pour les places n'appartenant pas à S . On peut énoncer :

THÉORÈME 5 [Q 2]. - Dans $G_{\oplus}^{S}(\mathbb{Z}[G])$ on a l'égalité

$$[\mathfrak{D}_N] - [K : \mathbb{Q}]\,[\mathbb{Z}[G]] = 0 .$$

On peut penser que ce résultat n'est pas le meilleur possible car pour $S = \emptyset$, on obtient un résultat plus faible que le théorème 1.

Il semble qu'il faille considérer $\mathcal{C}_{\mathcal{U}}^{S}(\mathbb{Z}[G])$ la catégorie des $\mathbb{Z}[G]$-modules de type fini, localement libres pour les places n'appartenant pas à S et $K_o^S(\mathbb{Z}[G])$ son groupe de Grothendieck. Tous les groupes définis dans ce quatrième point admettent une description analogue à celles des formules (1) et (2) ([Q 1]). La conjecture suivante est rendue plausible par le nombre de cas où elle est vérifiée ([C.N-Q]) :

CONJECTURE. - L'élément $[\mathfrak{D}_N] - [K : \mathbb{Q}]\,[\mathbb{Z}[G]]$ est d'odre 2 dans $K_o^S(\mathbb{Z}[G])$, il est trivial si les constantes de l'équation fonctionnelle des fonctions L d'Artin valent +1 pour les caractères symplectiques de G .

-:-:-:-

BIBLIOGRAPHIE

[Br] I. BRINKHUIS, Embedding problems and Galois modules, Thèse Leyde 1981.

[C 1] J. COUGNARD, Propriétés galoisiennes des anneaux d'entiers des p-extensions, Compositio Math. 33 (1976), pp. 303-336.

[C 2] J. COUGNARD, Contre-exemple à une conjecture de Martinet, Algebraic Number Fields (éd. A. Fröhlich) Academic Press (London) 1977.

[C.N-T] Ph. CASSOU-NOGUÈS and M. J. TAYLOR, Local root numbers and Hermitian-Galois-module Structure of rings of integers, à paraître.

[C.N-Q] Ph. CASSOU-NOGUÈS et J. QUEYRUT, Structure galoisienne des anneaux d'entiers d'extensions sauvagement ramifiées, II, Ann. Inst. Fourier, Grenoble, vol. 32, fasc. 1, (1982), 7-27.

[D] P. DELIGNE, Les constantes des équations fonctionnelles des fonctions L. Modular forms in one variable, Lecture Notes in Mathematics 349 (1973), pp. 501-597.

[Dr] A. DRESS, The ring of monomial representations I , Structure theory, J. Algebra 18 (1971), pp. 137-157

[F 1] A. FRÖHLICH, Invariants for modules over commutative separable orders, Quart. J. Math. Oxford (2), 16 (1965), pp. 193-232.

[F 2] A. FRÖHLICH, Locally free modules over arithmetic orders, Jour. reine angew. Math. 274/75 (1975), pp. 112-138.

[F 3] A. FRÖHLICH, Arithmetic and Galois module structure for tame extensions, Jour. reine angew. Math. 286/87 (1976), pp. 380-440.

[F 4] A. FRÖHLICH, Galois-module Structure and Artin L-functions, Astérisque 24/25 (1975), pp. 9-13.

[F 5] A. FRÖHLICH, Some problems of Galois-module-structure for wild extensions, Proc. London Math. Soc. (3) 28 (1974), pp. 402-438.

[F 6] A. FRÖHLICH, Value Distributions of Symplectic Rootnumbers, à paraître.

[F-T] A. FRÖHLICH and M. J. TAYLOR, The arithmetic theory of local Galois Gauss sums for tame characters, Philosophical Transactions of the royal society, 298 (1980), pp. 141-181.

[F - W] A. FRÖHLICH and C. T. C. WALL, Equivariant Brauer groups in Algebraic number theory, Bull. Soc. Math. France, mémoire 25 (1971), pp. 91-96.

[J] J.-F. JAULENT, Thèse de troisième cycle, Besançon 1979.

[L] H. W. LEOPOLDT, Über die Hauptordnung der ganzen Elementen eines abelschen Zahlkörpers, Jour. reine angew. Math. 201 (1959), pp. 11 pp. 119-149.

[M] J. MARTINET, Character theory and Artin L-functions, Algebraic number Fields (éd. A. Fröhlich) Academic Press (London), 1977.

[Mc C 1] L. Mac CULLOH, Galois module structure for Kummer extensions, Algebraic Number Fields (éd. A. Fröhlich) Academic Press (London), 1977.

[Mc C 2] L. Mac CULLOH, Class number formula for elementary abelian group rings, Compte rendus des journées arithmétiques d'Exeter, 1980.

[Mc L] S. Mac LANE, Homology, Springer Verlag (1967).

[N 1] A. NELSON, Modules over group rings and abelian subquotients, à paraître.

[N 2] A. NELSON, Modules Resolvents, Notes manuscrites.

[No] E. NOETHER, Normal basis bei Körpern ohne höhere Verzweigung, Jour. reine angew. Math. 167 (1932), pp. 147-152.

[Q 1] J. QUEYRUT, S-groupe des classes d'un ordre arithmétique, à paraître dans J. Algebra.

[Q 2] J. QUEYRUT, Structure galoisienne des anneaux d'entiers d'extensions sauvagement ramifiées, I, Ann. Inst. Fourier, Grenoble 31, fasc. 3 (1981), 1-35.

[R] I. REINER, Maximal orders, Academic Press, 1975.

[S 1] R. G. SWAN, Induced representations and projective modules, Ann. of Math. 71 (1960), pp. 552-578.

[S 2] R. G. SWAN, Projective modules over group rings and maximal orders, Ann. of Math. 76 (1962), pp 55-61.

[T 1] M. J. TAYLOR, A logarithmic approach to classgroup of integral group rings, J. Algebra 66 (1980), pp. 321-353.

[T 2] M. J. TAYLOR, On Fröhlich's conjecture for rings of integers of tame extensions, Invent. Math. 63 (1981), pp. 41-79.

[T 3] M. J. TAYLOR, Galois module structure of rings of integers in Kummer extensions, Bull. London Math. Soc. 12 (1980), pp. 96-98.

[T 4] M. J. TAYLOR, Monomial representations and ring of integers, Jour. reine angew. Math. 324 (1981), 127-135.

[V] M.-F. VIGNÉRAS, Quaternion et applications, Astérisque 24/25 (1975), pp. 47-55.

[W] S. M. J. WILSON, Some counter-examples in the Theory of the Galois module structure of wild extensions, Ann. Inst. Fourier, Grenoble 30, fasc. 3 (1980), pp. 1-8.

-:-:-:-

Jean COUGNARD
E.R.A. C.N.R.S. 070654
Faculté des Sciences de Besançon
La Bouloie - Route de Gray
F 25030 BESANÇON CEDEX