JEAN COUGNARD

Les travaux de A. Fröhlich, Ph. Cassou-Noguès et M. J. Taylor sur les bases normales

Astérisque, tome 105-106 (1983), Séminaire Bourbaki, exp. nº 598, p. 25-38

<http://www.numdam.org/item?id=SB_1982-1983__25__25_0>

Séminaire BOURBAKI
35e année, 1982/83, n° 598 Novembre 1982

LES TRAVAUX DE A. FRÖHLICH, PH. CASSOU-NOGUÈS ET M. J. TAYLOR SUR LES BASES NORMALES

par
Jean COUGNARD(*)

1 - INTRODUCTION :

Cet exposé fait suite à celui de Jacques Martinet [23] en juin 1974 : "Bases normales et constante de l'équation fonctionnelle des fonctions L d'Artin".

Rappelons les problèmes tels qu'ils ont alors été posés. On fixe une clôture algébrique $\bar{\mathbb{Q}}$ de $\mathbb{Q}$ et, pour toute extension algébrique L de $\mathbb{Q}$ de degré fini, on note Ω_L le groupe de Galois de $\bar{\mathbb{Q}}/L$ et O_L l'anneau des entiers de L. On se donne une extension K/k, galoisienne de degré fini de corps de nombres, de groupe de Galois G. On peut alors :

1 - donner à O_K une structure de $O_k[G]$-module et, par restriction une structure de $\mathbb{Z}[G]$-module,

2 - associer à chaque caractère virtuel χ de G une fonction $\Lambda(s,\chi,K/k)$ méromorphe sur $\mathbb{C}$: la fonction L d'Artin étendue. Cette fonction vérifie l'équation fonctionnelle :

$$\Lambda(1-s,\chi,K/k) = W(\chi,K/k)\Lambda(s,\bar{\chi},K/k)$$

où le symbole $^-$ désigne la conjugaison complexe et $W(\chi) = W(\chi,K/k)$ est un nombre complexe de module 1. On a la formule :

$$W(\chi) = \frac{\tau(\bar{\chi})}{\sqrt{N(f(\chi))}} \quad W_\infty(\chi)$$

. $\tau(\chi)$ est la somme de Gauss galoisienne associée au caractère χ et à l'extension K/k. Elle admet une décomposition en produit de

(*) E.R.A. au CNRS n°070654

facteurs locaux (le produit étant pris sur l'ensemble des places finies).

- $\sqrt{N(f(\chi))}$ désigne la racine carrée positive du générateur positif de la norme absolue du conducteur d'Artin du caractère χ. Ce nombre possède également une décomposition en produit (sur les places finies) de facteurs locaux.
- $W_\infty(\chi)$ est la "partie infinie" de $W(\chi)$.
- Le nombre $W(\chi)$ possède une décomposition en produit (sur toutes les places) de facteurs locaux. Pour plus de détails on peut consulter les exposés de Martinet et de Tate [24], [27].

On pose les questions suivantes :

Question 1 : Existe-t-il une base normale de O_K sur O_k ? C'est-à-dire un entier θ formant avec ses conjugués une base du O_k-module O_K. Autrement dit est-ce que O_K est un $O_k[G]$-module libre ?

Dans de nombreux cas on peut apporter une réponse négative, soit en remarquant que O_K n'est pas O_k libre soit en se basant sur des propriétés de plongement [5] ; mais il n'y a pas de critère qui permette de répondre en général. Il n'en va pas de même pour la question suivante :

Question 2 : Le $\mathbb{Z}[G]$-module O_K est-il libre ?

Dans son rapport, J. Martinet expose les liens entre cette question et les valeurs de $W(\chi)$. Ces liens étaient évidents dans l'article de A. Fröhlich [8] faisant suite à celui de J. Martinet [22]. Ils avaient conduit A. Fröhlich à formuler des conjectures qui ont été démontrées l'une par M. J. Taylor l'autre par Ph. Cassou-Noguès et M. J. Taylor.

Dans beaucoup de formules intervient le groupe des caractères virtuels de G ; on le note R_G et on peut le considérer comme le groupe de Grothendieck de la catégorie des $\bar{\mathbb{Q}}[G]$-modules de type fini. Le groupe $\Omega_{\mathbb{Q}}$ opère sur R_G par : $\forall \chi \in R_G, \forall g \in G, \forall \omega \in \Omega_{\mathbb{Q}} \left(\chi^{\omega}\right)(g) = \left(\chi(g)\right)^{\omega}$.

2 - LES GROUPES DES CLASSES DE G-MODULES :

On dit qu'une extension M/L de corps de nombres est modérément ramifiée si pour tout idéal premier $\mathfrak{p}$ non nul de O_L et tout idéal premier $\mathfrak{p}'$ de O_M au-dessus de $\mathfrak{p}$, l'indice de ramification $e(\mathfrak{p}'/\mathfrak{p})$ n'èst pas divisible par la caractéristique du corps résiduel $O_L/\mathfrak{p}$. On a le résultat élémentaire suivant :

(2. 1) Proposition : Le $O_k[G]$-module O_K est projectif si et seulement si l'extension K/k est modérément ramifiée.

On en déduit immédiatement que seules les extensions modérément ramifiées peuvent fournir une réponse positive aux questions 1 et 2.

Nous supposons désormais que l'extension K/k est modérément ramifiée ; de plus les $O_k[G]$-modules sont de type fini.

Les $O_k[G]$-modules projectifs possèdent une propriété intéressante : ils sont localement libres, autrement dit, pour chaque idéal premier $\mathfrak{p}$ de O_k, le localisé en $\mathfrak{p}$ d'un tel module est libre sur $O_{k_\mathfrak{p}}[G]$. On peut définir le rang d'un tel module. La première étape consiste, pour un corps de nombres L, à faire une classification des $O_L[G]$-modules projectifs. On Considère $\mathcal{K}_o\left(O_L[G]\right)$ le groupe de Grothendieck de la catégorie des $O_L[G]$-modules projectifs de type fini. Pour tout $O_L[G]$-module projectif E, on note $[E]$ son image dans $\mathcal{K}_o\left(O_L[G]\right)$. Deux modules E_1 et E_2 sont tels que $[E_1]=[E_2]$ si et seulement si $E_1 \oplus O_L[G] \simeq E_2 \oplus O_L[G]$; on dit que E_1 et E_2 sont stablement isomorphes et l'on connait des conditions suffisantes pour que cela implique l'isomorphisme de E_1 et de E_2 [20]. A l'heure actuelle le théorème de Taylor [32] permet de dire quand on a l'égalité $[O_K]=[k:\mathbb{Q}]\,[\mathbb{Z}[G]]$. Le rang d'un module permet de construire un homomorphisme surjectif r de $\mathcal{K}_o\left(O_L[G]\right)$ sur $\mathbb{Z}$; son noyau $C\ell\left(O_L[G]\right)$ est le groupe des classes projectives des $O_L[G]$-modules. Pour tout module E, on note (E) l'élément $[E]-r(E)[O_L[G]]$ de $C\ell\left(O_L[G]\right)$. On s'intéresse donc à l'élément $\left(O_K\right)$ de $C\ell\,(\mathbb{Z}[G])$.

Notations : Pour tout corps M on note $Ad(M)$ l'anneau des adèles de M, $J(M)$ le groupe des idèles et $J(\bar{\mathbb{Q}}) = \varinjlim J(M)$. La description de $C\ell\left(O_L[G]\right)$ pour un corps L repose sur celle d'un sous-groupe de $\mathrm{Hom}_{\Omega_L}\left(R_G, J(\bar{\mathbb{Q}})\right)$:

Une représentation T de G de degré m est un homomorphisme de G dans $GL_m(\bar{\mathbb{Q}})$. Il se prolonge en un homomorphisme d'algèbre de $Ad(L)\otimes_L L[G]$ dans $M_m\left(Ad(L)\otimes_L \bar{\mathbb{Q}}\right)$. En restreignant à $\prod_\mathfrak{p}\left(O_{L_\mathfrak{p}}[G]\right)^*$ (produit pris sur toutes les places de L) et en composant avec le déterminant on obtient un homomorphisme de $U\left(O_L[G]\right)=\prod_\mathfrak{p}\left(O_{L_\mathfrak{p}}[G]\right)^*$ dans $J(\bar{\mathbb{Q}})$ ne dépendant que du caractère χ. On le note $\det_\chi$. La relation $\det_{\chi+\chi'}=\det_\chi\cdot\det_{\chi'}$ permet pour $x\in U\left(O_L[G]\right)$ de définir un Ω_L homomorphisme $\mathrm{Det}(x)$ de R_G dans $J(\bar{\mathbb{Q}})$ et, lorsque x décrit $U\left(O_L[G]\right)$ un sous-groupe $\mathrm{Det}\left(U(O_L[G]\right)$ de $\mathrm{Hom}_{\Omega_L}\left(R_G, J(\bar{\mathbb{Q}})\right)$. On a la formule[13] :

$$C\ell\left(O_L[G]\right) \simeq \frac{\mathrm{Hom}_{\Omega_L}\left(R_G, J(\bar{\mathbb{Q}})\right)}{\mathrm{Hom}_{\Omega_L}\left(R_G, \bar{\mathbb{Q}}^*\right)\mathrm{Det}\left(U(O_L[G])\right)}$$

Cette présentation offre l'intérêt de donner des formules explicites pour les changements de groupe, de corps de base. Il existe des formules analogues pour les autres ordres de $L[G]$. On peut alors interpréter aisément l'extension des scalaires d'un ordre de $L[G]$ à un autre le contenant. Pour plus de détails on peut consulter [13], [19], [25]. Ces propriétés permettent fréquemment d'utiliser un théorème de Brauer et de remplacer G par un groupe "p-élémentaire".

Pour répondre à la question 2 il faut maintenant trouver un représentant de $\left(O_K\right)$ et montrer qu'il est égal à un élément accessible par le calcul.

3 - LA CONSTANTE DE L'ÉQUATION FONCTIONNELLE :

Par construction des fonctions $\Lambda(s,\chi,K/k)$ on constate que $W(\bar{\chi}) = \overline{W(\chi)}$; en particulier si χ est à valeurs réelles $W(\chi)$ ne peut prendre que les valeurs $+1$ ou -1. On sait que les caractères à valeurs réelles sont des combinaisons linéaires à coefficients entiers de caractères des trois types suivants : [26]

1 - les caractères des représentations absolument irréductibles de G par des matrices à coefficients réels,

2 - les caractères somme de deux caractères absolument irréductibles conjugués Φ et $\bar{\Phi}$ où Φ prend au moins une valeur non réelle,

3 - les caractères absolument irréductibles et symplectiques.

Les caractères du type 3 et les caractères $\Phi + \bar{\Phi}$ $\left(\Phi \in R_G\right)$ engendrent le sous-groupe R_G^S des caractères symplectiques de G. Pour que le caractère χ d'une représentation ρ de G dans $GL(V)$ appartienne à R_G^S, il faut et il suffit qu'existe sur V une forme bilinéaire alternée non dégénérée invariante par G.

Pour ce qui est des valeurs de $W(\chi)$, s'il est évident que $W(\chi) = +1$ si χ est du type 2, il n'en va pas de même s'il est d'un autre type :

(3. 1) Théorème [21] : Si χ est le caractère d'une représentation de G par des matrices à coefficients réels alors $W(\chi) = +1$.

Les caractères du type 3 peuvent prendre les valeurs +1 ou −1 [9],[1]. Le théorème suivant, dû à Fröhlich, est particulièrement important pour la suite.

(3. 2) Théorème [9] : Sous les hypothèses de ramification modérée, on a pour tout χ de R_G et tout $\omega \in \Omega_{\mathbb{Q}}$: $W\left(\chi^{\omega}\right) = W(\chi)^{\omega}$.

En conséquence, l'homomorphisme W_S de R_G dans $J(\bar{\mathbb{Q}})$ défini sur les caractères absolument irréductibles par :

$$W_S(\chi) = W(\chi) \text{ si } \chi \in R_G^s \quad ; \quad W_S(\chi) = 1 \quad \text{sinon}$$

est un élément de $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}\left(R_G, J(\bar{\mathbb{Q}})\right)$.

4 - LE THÉORÈME DE TAYLOR :

En 1971, Jacques Martinet montrait [22] que l'anneau des entiers d'une extension quaternionienne de $\mathbb{Q}$ de degré 8 peut ne pas avoir de base normale. Dans une lettre qu'il lui adressait J.P. Serre faisait remarquer que ces exemples dépourvus de base normale sont tels que $W(\chi) = -1$ pour l'unique caractère symplectique irréductible du groupe de Galois. Il suggérait que ce n'était peut-être pas un hasard. A la même époque, Armitage [1] mettait au point une méthode pour construire des extensions quaternioniennes de $\mathbb{Q}$ de degré 8 telles que $W(\chi) = -1$. Utilisant les caractérisations de Martinet il constatait que leurs anneaux d'entiers n'admettent pas de base normale. C'est à la suite de ces travaux que Fröhlich démontre :

(3. 3) Théorème [8] : Si $k/\mathbb{Q}$ est une extension quaternionienne de degré 8 l'anneau des entiers O_K possède une base normale si et seulement si $W(\chi)$ est égal à +1 pour l'unique caractère irréductible symplectique du groupe de Galois.

Il conjecture que la fonction W_S détermine (O_N). Plus précisément, en suivant Ph. Cassou-Noguès on définit un $\Omega_{\mathbb{Q}}$-homomorphisme $t(W)$ de la façon suivante : si $W_S(\chi) = -1$, on pose $t(W)(\chi) = (x_v)$ où (x_v) est l'idèle dont les composantes valent 1 pour les places à l'infini et −1 ailleurs sinon $t(W)(\chi) = 1$. En 1981, Taylor démontre :

(3. 4) Théorème [31], [32] : L'image de $t(W)$ dans $C\ell(\mathbb{Z}[G])$ est égale à $\left(O_K\right)$.

On peut citer les corollaires suivants :

(3.5) Corollaire : Le $\mathbb{Z}[G]$-module $O_K \oplus O_K$ est isomorphe à $\mathbb{Z}[G]^{2[k:\mathbb{Q}]}$. De plus, si l'ordre de G n'est pas divisible par 4, O_K est isomorphe à $\mathbb{Z}[G]^{[k:\mathbb{Q}]}$.

Le corollaire suivant est moins attendu :

(3.6) Corollaire [18] : Si m est l'ordre de G et si k contient les racines m-ièmes de l'unité alors O_K est $\mathbb{Z}[G]$-libre.

On peut citer les principales étapes qui ont conduit à la démonstration de la conjecture. Dans l'article [13], qui est resté la référence de base pour la question, A. Fröhlich montre :

(3.7) Théorème : Si $\mathfrak{M}$ est un ordre maximal de $\mathbb{Q}[G]$, contenant $\mathbb{Z}[G]$, le $\mathfrak{M}$-module $\mathfrak{M} O_K$ est stablement libre.

L'élément (O_K) se trouve dans le noyau $D(\mathbb{Z}[G])$ de l'homomorphisme de $C\ell(\mathbb{Z}[G])$ dans $C\ell(\mathfrak{M})$ qui se déduit de l'extension des scalaires de $\mathbb{Z}[G]$ à $\mathfrak{M}$; ce sous-groupe est isomorphe à

$$\mathrm{Hom}^+_{\Omega_{\mathbb{Q}}}\left(R_G, U(\bar{\mathbb{Q}})\right) / \mathrm{Hom}^+_{\Omega_{\mathbb{Q}}}\left(R_G, O^*_{\bar{\mathbb{Q}}}\right) \mathrm{Det}(U(\mathbb{Z}[G])).$$

Dans cette formule, $U(\bar{\mathbb{Q}})$ désigne les idèles qui sont des unités en toute place, $O^*_{\bar{\mathbb{Q}}}$ les unités de $\varinjlim O_L$ et le signe + signifie que les homomorphismes prennent des valeurs réelles positives aux places à l'infini pour $\chi \in R^s_G$.

A. Fröhlich montre alors que l'on peut procéder de la façon suivante pour obtenir un représentant de (O_K) : soit $a \in O_K$ tel que $k[G]a = K$ et tel que pour toute place $\mathfrak{p}$ de k divisant l'ordre de G $O_{k_\mathfrak{p}}[G]a = O_{K_\mathfrak{p}}$; pour toute représentation T de G de caractère χ, on forme la quantité $\langle a, \chi\rangle = \det\left(\sum_{g \in G} g(a)T(g^{-1})\right)$ qui généralise les résolvantes de Lagrange.

L'application $\chi \longmapsto \langle a, \chi\rangle$ se prolonge en une application de R_G dans $J(\bar{\mathbb{Q}})$ et le module O_K est représenté par le $\Omega_{\mathbb{Q}}$-homomorphisme dont les $\mathfrak{p}$ composantes pour $\mathfrak{p} \mid |G|$ sont :

$$f : \chi \longmapsto \tau(\chi)^{-1} W_S(\chi) \prod_{\sigma \in \mathfrak{S}} \langle a, \chi^{\sigma^{-1}}\rangle^{\sigma}$$

où $\mathfrak{S}$ est un système de représentants de $\Omega_{\mathbb{Q}}/\Omega_k$.

Au cours de la démonstration de ce théorème, Fröhlich retrouve le théorème de Dwork prouvant que les sommes de Gauss galoisiennes sont des entiers algébriques.

La démonstration du théorème (3.4) revient à prouver que la fonction f modifiée par un élément de $\mathrm{Hom}^{+}_{\Omega_{\mathbb{Q}}}\left(R_G, O^{*}_{\bar{\mathbb{Q}}}\right)$ appartient à $\mathrm{Det}(U(\mathbb{Z}[G]))$.

Pendant les années suivantes, la méthode de Fröhlich a été perfectionnée par Cassou-Noguès et a donné lieu à des démonstrations de la conjecture dans des cas particuliers ([2], [3], [4]). Dans d'autres cas particuliers elle a été vérifiée par A. Fröhlich ([12], [16]).

La technique adoptée par Taylor semble indépendante des perfectionnements précédents et s'apparente à une descente : il s'agit de montrer que le représentant modifié appartient à $\mathrm{Det}\left(U\left(O_L[G]\right)\right)$ pour une extension L galoisienne sur $\mathbb{Q}$ convenablement choisie puis que :

$$\mathrm{Det}\left(U\left(O_L[G]\right)\right)^{\mathrm{Gal}(L/\mathbb{Q})} = \mathrm{Det}\left(U(\mathbb{Z}[G])\right).$$

Cette démarche basée sur l'utilisation puis une généralisation du logarithme p-adique apparait dans les articles [28], [29], [30].

4 - LE PROBLÈME RÉCIPROQUE ET LES MODULES HERMITIENS :

Dès que la conjecture de Fröhlich s'est avérée plausible la question suivante est apparue logique :

Question 3 : Est-ce que la connaissance de la structure de $\mathbb{Z}[G]$-module de O_K permet de retrouver les valeurs de W_S ?

Du point de vue local on constate immédiatement qu'il n'en est rien ; en effet, les localisés de O_K sont toujours libres sur le localisé de $O_k[G]$ même si les constantes locales valent -1. Il est logique de se demander s'il n'en va pas de même dans le cas global. En fait la question se précise lors de l'article [10] de Fröhlich consacré aux extensions quaternioniennes de $\mathbb{Q}$ de degré $4\ell^r$ (on peut aussi consulter les indications données par Martinet dans [23] § 2). En fait, c'est en 1980 que l'on a une réponse négative à la question 3, en comparant les résultats de [9] et [16] : dans [9], Fröhlich avait montré qu'il est possible de construire des extensions quaternioniennes de $\mathbb{Q}$ de degré 2^n $(n \geq 3)$ avec des valeurs de $W_S(\chi)$ imposées, et dans [16] il montre que pour $n > 3$ l'image de W_S et l'élément (O_K) sont égaux à l'élément neutre de

$C\ell(\mathbb{Z}[G])$. La connaissance de (O_K) n'implique donc pas en général celle de W_S.

En fait, dès 1974, convaincu de la réponse négative à cette question, il envisage pour retrouver les valeurs de W_S de munir O_K d'une structure de $\mathbb{Z}[G]$-module hermitien [11], [14], [15].

Le problème étant à la fois un problème local et un problème global on unifie les notations pour traiter simultanément les deux aspects. On se donne un corps de base F qui est une extension algébrique de degré fini de $\mathbb{Q}$ ou d'un de ses complétés $\mathbb{Q}_p$ (on n'envisage ici que le cas des places finies) et un groupe fini G. L'algèbre $F[G]$ est munie d'une involution : $\widetilde{\sum_{g\in G} a_g g} = \sum_{g\in G} a_g g^{-1}$. Cette involution se prolonge aux algèbres de matrices $M_n(F[G])$ par $\widetilde{(\alpha_{i,j})} = {}^t(\widetilde{\alpha_{i,j}})$.

(4.1) Définition : On appelle $O_F[G]$-module hermitien un $O_F[G]$-module localement libre (libre dans le cas local) muni d'une application $h : (F\otimes_{O_F} M) \times (F\otimes_{O_F} M) \longrightarrow F[G]$ vérifiant :

- h est $F[G]$ linéaire à gauche,
- $h(u_1, u_2) = \widetilde{h(u_2, u_1)}$ quels que soient u_1 et u_2 dans M.

(4.2) Exemples :

- Si k est une extension algébrique de degré fini de F et K/k une extension galoisienne de degré fini et de groupe de Galois G, on munit K de la forme : $T(m,n) = \sum_{g\in G} Tr_{K/F}(g(m)n)g^{-1}$; le couple (O_K, T) est un module hermitien.
- Si k est une extension algébrique de degré fini de F, on considère $\xi : k[G] \times k[G] \longrightarrow F[G]$ où $\xi(x,y) = Tr_{k/F}(x\tilde{y})$ où $Tr_{k/F}$ est la trace prolongée par linéarité à $k[G]$. Le couple $(O_k[G], \xi)$ est un module hermitien.

Les travaux qui ont conduit à la démonstration du théorème (3.4) ont été dominés par la volonté de comparer O_K à $\mathbb{Z}[G]^{[k:\mathbb{Q}]}$ ce qui peut se justifier (outre les explications données) par le fait qu'en étendant les scalaires de $\mathbb{Z}$ à $\mathbb{Q}$ on obtient un isomorphisme de $\mathbb{Q}[G]$-modules entre K et $\mathbb{Q}[G]^{[k:\mathbb{Q}]}$.

Une idée analogue sert de fil directeur dans le cas des modules hermitiens : soit $\overline{F}$ une clôture algébrique de F ; si $k = F$ on peut démontrer que l'application φ de $K' = \overline{F} \otimes_F K$ sur $\overline{F}[G]$ définie par

$\varphi(\alpha \otimes n) = \alpha \sum_{g \in G} g(n) g^{-1}$ est une isométrie de (K', T) sur $(\overline{F}[G], \xi)$ où T et ξ sont prolongés par linéarité.

Pour comparer les modules hermitiens $(O_k[G], \xi)$ et (O_K, T) on définit un groupe permettant d'en faire une classification.

5 - LE GROUPE DES CLASSES HERMITIENNES - LE DISCRIMINANT :

On pense bien entendu au groupe de Grothendieck $\mathcal{K}_0 H(O_F[G])$ des classes d'isométrie des $O_F[G]$-modules hermitiens, relativement aux sommes orthogonales. Il semble malheureusement que la littérature soit avare de renseignement sur la description de ce groupe ; c'est ce qui a amené A. Fröhlich à définir un groupe des classes hermitiennes $HC\ell(O_F[G])$ et un homomorphisme d, qu'il appelle discriminant, de $\mathcal{K}_0 H(O_F[G])$ dans $HC\ell(O_F[G])$ (on peut voir sur des exemples la justification de cette terminologie [17]). La définition de $HC\ell(O_F[G])$ diffère suivant qu'il s'agit du cas local ou du cas global.

(5.1) Cas local : $HC\ell(O_F[G]) = \mathrm{Hom}_{\Omega_F}(R_G^s, \overline{F}^*)/\mathrm{Det}^S(O_F[G]^*)$ où $\mathrm{Det}^S(O_F[G]^*)$ est le sous-groupe de $\mathrm{Hom}_{\Omega_F}(R_G^s, \overline{F}^*)$ formé des homomorphismes $\chi \longmapsto \det_\chi(b)$ avec b dans $O_F[G]^*$ et χ parcourant R_G^s.

Cas global : On considère l'homomorphisme Δ de $\mathrm{Hom}_{\Omega_F}(R_G, \bar{\mathbb{Q}}^*)$ dans $\left(\mathrm{Hom}_{\Omega_F}(R_G, J(\bar{\mathbb{Q}}))/\mathrm{Det}(U(O_F[G]))\right) \times \mathrm{Hom}_{\Omega_F}(R_G^s, \bar{\mathbb{Q}}^*)$ défini par $\Delta(f) = ($classe de $1/f$, restriction de f à $R_G^s)$. On pose alors :

(5.2) $$HC\ell(O_F[G]) = \mathrm{Coker}(\Delta).$$

La définition du discriminant est basée sur la notion de pfaffien ; nous la donnons dans le cas local et renvoyons le lecteur à [17] ou à [19] pour le cas global. Jusqu'à la fin de ce paragraphe les corps, à part $\overline{F}$, sont tous des extensions algébriques de degré fini d'un corps $\mathbb{Q}_p$. Soit E un $O_F[G]$-module libre muni d'une structure hermitienne définie par une forme h et $(x_1, x_2, \ldots, x_n)$ une base de M. On construit la matrice $(h(x_i, x_j))$ de $GL_n(O_F[G])$. Toute représentation T de G dans

dans $GL_m(\bar{F})$ de caractère χ, se prolonge en un homorphisme (toujours noté T) de $GL_n\left(O_F[G]\right)$ dans $GL_{mn}(\bar{F})$. Si on compose avec le déterminant on construit un élément noté $\det_\chi\left(h\left(x_i, x_j\right)\right)$. On constate aisément que la matrice $h\left(x_i, x_j\right)$ est symétrique pour le prolongement de l'involution $\sim$. Ceci a une grande importance lorsque χ est un caractère symplectique. On sait en effet que T est une représentation symplectique de G dans $GL_m(\bar{F})$ si et seulement si il existe une forme bilinéaire alternée sur $\bar{F}^m$ invariante par G. Soit j l'involution adjointe à cette forme alternée, elle se prolonge à $M_{mn}(\bar{F})$ et on a pour tout y de $GL_n\left(O_F[G]\right)$:

$$T(\tilde{y}) = T(a)^j$$

en particulier si y est symétrique $T(a) = T(a)^j$. Or :

(5.3) Lemme : Si la matrice S de $GL_{mn}(\bar{F})$ est telle que $S = S^j$ alors il existe une matrice P telle que $S = PP^j$.

On constate donc que $\det_\chi\left(h\left(x_i, x_j\right)\right)$ pour χ parcourant R_G^s est un carré et qu'il y a une manière non ambigüe d'extraire la racine carrée. Avec les notations du lemme 5.3, on appelle pfaffien de S le nombre det (P).

Construisons maintenant l'homomorphisme discriminant d. Pour un $O_F[G]$-module hermitien (E, h) on choisit une base $\left(e_1, e_2, \ldots, e_p\right)$. A chaque représentation symplectique T de G on associe $Pf\left(T\left(h(e_i, e_j)\right)\right)$ qui ne dépend que du caractère χ de T. Ceci permet de construire une application de R_G^s dans $\bar{F}^*$: $\chi \longmapsto Pf_\chi\left(h(e_i, e_j)\right)$. L'homomorphisme de $K_oH\left(O_F[G]\right)$ dans $HC\ell\left(O_F[G]\right)$ induit par ce procédé est d.

Les propriétés du pfaffien montrent que la définition de d ne dépend pas de la base choisie. Enfin, la notion de pfaffien est liée à celle de résolvante, citons par exemple :

(5.4) Proposition [17] : Si k est égal à F et si la forme h sur K est définie par la trace (cf 4.2 exemple 1), pour tout élément a engendrant une base normale de K sur F et tout caractère symplectique χ de G, on a :

$$Pf_\chi(h(a, a)) = \langle a, \chi\rangle.$$

On peut trouver dans [19] toutes les propriétés du discrimiant et du groupe des classes hermitiennes liées aux changements de groupe, changements de corps de base ...

6 - LES THÉORÈMES DE Ph. CASSOU-NOGUÈS ET M. J. TAYLOR ([6], [7]) :

Dans ce paragraphe le corps F est égal à $\mathbb{Q}$ dans le cas global (à $\mathbb{Q}_p$ dans le cas local). Pour comparer les $O_F[G]$-modules hermitiens (O_K, T) et $(O_k[G], \xi)$ Cassou-Noguès et Taylor étudient l'image par d de la différence $X_{N/k}$ des classes de (O_K, T) et $(O_k[G], \xi)$ dans $\mathcal{K}_o H(O_F[G])$. Ils obtiennent les résultats suivants :

a) Cas global :

(6. 1) Proposition : Le groupe $T(\mathbb{Z}[G]) = \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G^s, \mathbb{Q}^*) \times \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G^s, \pm 1)$ est isomorphe à un sous-groupe de $HC\ell(\mathbb{Z}[G])$ avec lequel nous l'identifions. L'élément $d(X_{N/k})$ appartient à $T(\mathbb{Z}[G])$.

De plus :

(6. 2) Théorème : La projection η de $T(\mathbb{Z}[G])$ sur $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G^s, \mathbb{Q}^*)$ est telle que pour tout caractère χ de R_G^s :

$$\eta\left(d\left(X_{K/k}\right)\right)(\chi) = N\left(f_{K/k}(\chi)\right)^{1/2} \quad W_\infty(\chi)$$

avec les notations données dans l'introduction. La projection θ de $T(\mathbb{Z}[G])$ sur $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G^s, \pm 1)$ est telle que $\theta\left(d\left(X_{K/k}\right)\right) = W_S$.

b) Cas local :

Le même groupe $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G^s, \mathbb{Q}^*) \times \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G^s, \pm 1)$ intervient mais cette fois-ci ce n'est plus un sous-groupe de $HC\ell(\mathbb{Z}_p[G])$, il faut considérer $\bar{\mathbb{Q}}_p$ plongé dans $J(\bar{\mathbb{Q}})$ ce qui donne un homomorphisme i de $HC\ell(\mathbb{Z}_p[G])$ dans le groupe $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G^s, J(\bar{\mathbb{Q}}))/\mathrm{Det}^S(U(\mathbb{Z}[G]))$ que l'on note $AHC\ell(\mathbb{Z}[G])$. On peut alors identifier $T(\mathbb{Z}[G])$ à un sous-groupe de $AHC\ell(\mathbb{Z}[G])$. L'élément $i \circ d(X_{K/k})$ appartient à $T(\mathbb{Z}[G])$; les projections η et θ donnent respectivement la racine carrée positive de la norme absolue du conducteur d'Artin et les constantes locales $W_S(\chi)$.

L'existence du groupe $T(\mathbb{Z}[G])$ repose tant dans le cas local que dans le cas global sur la formule $\mathrm{Hom}(R_G^s, \pm 1) \cap \mathrm{Det}^S(U_+(O[G])) = \{1\}$. (formule 5. 1 de [6]). Curieusement, les propriétés des fonctions θ et η ne nécessitent pas d'autres résultats arithmétiques que ceux démontrés dans [32] et conduisant au théorème 3.4.

La connaissance de la structure hermitienne de O_K permet de retrouver les normes absolues des conducteurs d'Artin locaux et globaux, les constantes locales et globales de l'équation fonctionnelle et donc les sommes de Gauss galoisiennes locales et globales pour les caractères symplectiques.

BIBLIOGRAPHIE

[1] J.V. ARMITAGE, Zeta functions with a zero at $s = 1/2$. Invent. Math. 15, (1972), 199-207.

[2] Ph. CASSOU-NOGUÈS, Quelques théorèmes de base normale. Astérisque 41-42, (1977), 183-189.

[3] Ph. CASSOU-NOGUÈS, Modules de Frobenius et structure galoisienne des anneaux d'entiers. J. of Algebra 71, (1981), 268-289.

[4] Ph. CASSOU-NOGUÈS, Sur une conjecture de Fröhlich pour les extensions quaternioniennes de corps de nombres. Séminaire Bordeaux I, 1981-1982.

[5] J. BRINKHUIS, Embedding problems and Galois modules. Thèse, Université de Leyde, (1981).

[6] Ph. CASSOU-NOGUÈS, M.J. TAYLOR, Local root numbers of hermition galois module structure of rings of integers. A paraitre dans Math. Annal.

[7] Ph. CASSOU-NOGUÈS, M.J. TAYLOR, Constante de l'équation fonctionnelle de la fonction L d'Artin d'une représentation symplectique modérée. A paraitre dans Ann. Inst. Fourier.

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

[9] A. FRÖHLICH, Artin root numbers, conductors and representations for generalized quaternion groups. Proc. London Math. Soc. (3), 28, (1974), 402-438.

[10] A. FRÖHLICH, Module invariants and root numbers for quaternion fields of degree $4p^r$. Proc. Camb. Phil. Soc. 76, (1974), 393-399.

[11] A. FRÖHLICH, Galois module structure and Artin L functions. Proc. Int. Cong. Math. Vancouvert, (1974), 351-356.

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

[13] A. FRÖHLICH, Arithmetic and Galois module structure for tame extensions. J. reine angew. Math. 286/287, (1976), 380-440.

[14] A. FRÖHLICH, Symplectic local constants and hermitian Galois module structure. Internat. Symp. Kyoto (ed. S. Iyanaga) Japan Soc. for the promotion of Science Tokyo, (1977), 25-42.

[15] A. FRÖHLICH, Local hermitian group modules, quadratic form conference. Queen's papers on pure and app. Math., 46, Kingston Ontario, (1977).

[16] A. FRÖHLICH, Galois structure and root numbers for quaternion extensions of degree 2^n. J. of number theory 12, (1980), 499-518.

[17] A. FRÖHLICH, The hermitian class group. Integral representations and applications. Lecture Notes in Math. 882, 191-206, Springer Verlag 1981.

[18] A. FRÖHLICH, Value distributions of symplectic root numbers. A paraitre.

[19] A. FRÖHLICH, Class groups, in particular hermitian class groups. A paraitre.

[20] A. FRÖHLICH, Locally free modules over arithmetic orders. J. reine angew. Math. 274/275, (1975), 112-138.

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

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

[23] J. MARTINET, Bases normales et constante de l'équation fonctionnelle des fonctions L d'Artin. Séminaire Bourbaki exp. 450, (1974).

[24] J. MARTINET, Character theory and Artin L functions. Algebraic Number fields, 1-87, édité par A. Fröhlich, Academic Press, (1977).

[25] J. QUEYRUT, S-groupe des classes d'un ordre arithmétique. J. of Algebra, 76, (1982), 234-260.

[26] J.-P. SERRE, Représentations linéaires des groupes finis. 2ème édition, Hermann, Paris, (1977).

[27] J.-T. TATE, Local constants. Algebraic Number fields, 89-131, édité par A. Fröhlich, Academic Press, (1977).

[28] M.-J. TAYLOR, Locally free classgroups of prime power order. J. of Algebra, 50, (1978), 463-487.

[29] M.-J. TAYLOR, Galois module structure of integers of relative abelian extensions. J. reine angew. Math. 303/304, (1978), 97-101.

[30] M.-J. TAYLOR, Galois module structure of rings of integers. Ann. Inst. Fourier Grenoble 30-3, (1980), 11-48.

[31] M.-J. TAYLOR, A logarithmic approach to classgroups of integral group-rings. J. of Algebra, 66, (1980), 321-353.

[32] M.-J. TAYLOR, On Fröhlich's conjecture for rings of integers of tame extensions. Invent. Math. 63, (1981), 41-79.

J. COUGNARD
Laboratoire de Mathématiques
Faculté des Sciences de Besançon
25030 BESANCON CEDEX