Astérisque

PHILIPPE CASSOU-NOGUES

Quelques théorèmes de base normale

Astérisque, tome 41-42 (1977), p. 183-189

<http://www.numdam.org/item?id=AST_1977__41-42__183_0>

© Société mathématique de France, 1977, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Société Mathématique de France
Astérisque 41-42 (1977) p.183-189

QUELQUES THÉORÈMES DE BASE NORMALE

par

Philippe CASSOU-NOGUÈS

-:-:-:-

Soit une extension galoisienne N du corps $\mathbb{Q}$ des nombres rationnels, de degré fini, dont le groupe de Galois (resp. l'anneau d'entiers) sur $\mathbb{Q}$, est noté Γ (resp. O_N). On s'intéresse à la structure de O_N en tant que module sur l'algèbre de groupe $\mathbb{Z}[\Gamma]$ et plus particulièrement à la recherche des cas où O_N est un $\mathbb{Z}[\Gamma]$-module libre, c'est-à-dire où il existe une base normale d'entiers. On sait que O_N est un $\mathbb{Z}[\Gamma]$-module localement libre si et seulement si N est une extension modérément ramifiée de $\mathbb{Q}$; on suppose cette hypothèse réalisée dans la suite de cet exposé et on note $[O_N]$ la classe de O_N dans le groupe projectif $C(\mathbb{Z}[\Gamma])$ associé à $\mathbb{Z}[\Gamma]$. On sait qu'il existe une base normale d'entiers lorsque Γ est un groupe abélien (Hilbert et Speiser, [6]), ou un 2-groupe diédral ou quaternionien d'ordre supérieur à 8 (Fröhlich-Keating-Wilson, [5]) ou un groupe métacyclique d'ordre ℓq où ℓ est un nombre premier, q un diviseur de $(\ell-1)$ (Fröhlich, [4]). Par contre Martinet ([7]) a donné un exemple d'extension modérément ramifiée de $\mathbb{Q}$, de groupe de Galois quaternionien d'ordre 8, où il n'existe pas de base normale d'entiers. L'étude de cet exemple et du cas où le groupe Γ est quaternionien généralisé d'ordre $4\ell^n$, avec ℓ nombre premier impair, a montré qu'il existait un lien entre le problème de la structure de module galoisien de O_N et le signe de la constante $W(\chi)$ de l'équation fonctionnelle des séries L-d'Artin associées aux caractères irréductibles symplectiques χ du groupe Γ. Fröhlich ([2]) a montré que $[O_N]$ appartient à $D(\Gamma)$, noyau de l'homomor-

phisme de $C(\mathbb{Z}[\Gamma])$ sur le groupe analogue $C(\mathcal{M})$ associé à un ordre maximal de $\mathbb{Z}$ dans $\mathbb{Q}[\Gamma]$ contenant $\mathbb{Z}[\Gamma]$, induit par l'extension des scalaires. On déduit du théorème de Hilbert-Speiser que $[O_N]$ appartient au groupe $D_o(\Gamma)$ noyau de l'homomorphisme naturel de $D(\Gamma)$ sur le groupe $D(\Gamma^{(ab)})$, associé au groupe Γ rendu abélien. Fröhlich conjecture en outre que $[O_N]^2 = 1$ et même que $[O_N] = 1$ si le groupe Γ ne possède pas de représentations symplectiques irréductibles. Dans les exemples déjà cités la conjecture est vérifiée mais on peut remarquer qu'elle est une conséquence de la forme particulièrement simple dans ces cas du groupe $D_o(\Gamma)$, explicitement calculable ; or on ne sait pas en général déterminer le groupe $D_o(\Gamma)$, ([1]).

Le but de cet exposé est de donner de nouveaux exemples d'existence de base normale d'entiers et d'interprétation de $[O_N]$ à l'aide des constantes $W(\chi)$, en particulier pour des extensions modérément ramifiées de $\mathbb{Q}$ ayant pour groupe de Galois le groupe quaternionien d'ordre $4\ell_1 \ldots \ell_q$, avec (ℓ_i), $1 \leq i \leq q$, nombres premiers impairs et distincts ou $4\ell^n$ où ℓ est un nombre premier impair, régulier et tel que 2 soit d'ordre pair modulo ℓ si $n > 1$. On sait maintenant que certaines extensions modérément ramifiées de $\mathbb{Q}$ dont le groupe de Galois est métacyclique d'ordre ℓ^3, où ℓ est un nombre premier possède, une base normale d'entiers (Taylor, [9]).

1. - Description du groupe $E(\Gamma)$ et des homomorphismes h et k .

On utilise les notations de Fröhlich, ([2]). Soient R_Γ le groupe additif des caractères virtuels du groupe Γ, E un corps de nombres qui contient les valeurs prises par les caractères de Γ, O_E^* (resp. $U(E)$) le groupe des unités (resp. le groupe des idèles unités). Le groupe $\Omega_{\mathbb{Q}}$ des $\mathbb{Q}$-automorphismes d'une clôture algébrique de $\mathbb{Q}$ opère sur les groupes R_Γ, O_E^*, $U(E)$ et on définit alors le groupe additif des $\Omega_{\mathbb{Q}}$-homomorphismes (resp. $\Omega_{\mathbb{Q}}$-homomorphismes, totalement positifs au sens de [2] pour les caractères symplectiques) de R_Γ dans $U(E)$ qu'on note : $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_\Gamma, U(E))$ (resp. $\mathrm{Hom}^+_{\Omega_{\mathbb{Q}}}(R_\Gamma, U(E))$ et son sous-groupe : $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_\Gamma, O_E^*)$ (resp. $\mathrm{Hom}^+_{\Omega_{\mathbb{Q}}}(R_\Gamma, O_E^*)$). On définit un homomorphisme du groupe des idèles unités $U(\mathbb{Z}[\Gamma])$ de $\mathbb{Z}[\Gamma]$ dans $\mathrm{Hom}^+_{\Omega_{\mathbb{Q}}}(R_\Gamma, U(E))$ noté Det. en prolongeant par linéarité à R_Γ l'application définie pour tout caractère χ d'une représentation T de Γ par : $\mathrm{Det}_\chi(\alpha) = \mathrm{Det}(T(\alpha))$ où $\mathrm{Det}(T(\alpha))$ désigne le

déterminant usuel. On a alors un isomorphisme :

$$D(\Gamma) \longrightarrow \mathrm{Hom}^{+}_{\Omega_{\mathbb{Q}}}(R_\Gamma, U(E)) \;/\; \mathrm{Hom}^{+}_{\Omega_{\mathbb{Q}}}(R_\Gamma, O_E^*).\ \mathrm{Det}(U(\mathbb{Z}[\Gamma])) .$$

A tout diviseur premier ℓ de l'ordre du groupe Γ on associe le sous-groupe $\mathrm{Ker}\, d_\ell$ de R_Γ, noyau de l'homomorphisme de décomposition d_ℓ, l'idéal $\mathfrak{L}$ de O_E produit des idéaux premiers au-dessus de ℓ dans E, W_ℓ le groupe des éléments inversibles de l'anneau $(O_E/\mathfrak{L})$. L'homomorphisme de restriction de R_Γ à $\mathrm{Ker}\, d_\ell$ et la surjection naturelle de $U(E)$ sur W_ℓ permettent de définir un homomorphisme R_ℓ de $\mathrm{Hom}^{+}_{\Omega_{\mathbb{Q}}}(R_\Gamma, U(E))$ sur le groupe $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(\mathrm{Ker}\, d_\ell, W_\ell)$ et par passage au quotient h_ℓ de $D(\Gamma)$ sur le groupe :

$$E_\ell(\Gamma) = \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(\mathrm{Ker}\, d_\ell, W_\ell) \;/\; R_\ell(\mathrm{Hom}^{+}_{\Omega_{\mathbb{Q}}}(R_\Gamma, O_E^*)) .$$

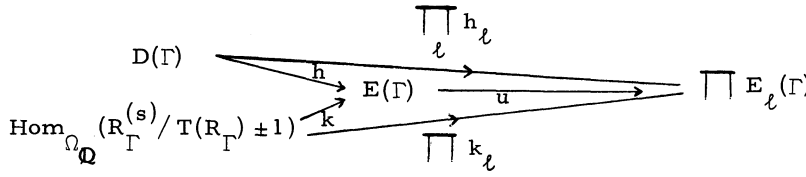
Soit $\{\ell_i,\ 1 \le i \le q\}$ une famille (resp. l'ensemble) des diviseurs premiers de l'ordre de Γ ; on désigne par $E_{\ell_1 \dots \ell_q}(\Gamma)$ (resp. $E(\Gamma)$) le groupe quotient :

$$\Big(\prod_{i=1}^{q} R_{\ell_i}\Big)\big(\mathrm{Hom}^{+}_{\Omega_{\mathbb{Q}}}(R_\Gamma, U(E))\big) \;/\; \Big(\prod_{i=1}^{q} R_{\ell_i}\Big)\big(\mathrm{Hom}^{+}_{\Omega_{\mathbb{Q}}}(R_\Gamma, O_E^*)\big)$$

et par $h_{\ell_1 \dots \ell_q}$ (resp. h) l'homomorphisme de $D(\Gamma)$ sur le groupe $E_{\ell_1 \dots \ell_q}(\Gamma)$ (resp. $E(\Gamma)$).

Soit $R_\Gamma^{(s)}$ (resp. $T(R_\Gamma)$) le sous-groupe de R_Γ des caractères symplectiques (resp. l'image de R_Γ par l'homomorphisme $T : \chi \to \chi + \bar{\chi}$). Le groupe $\Omega_{\mathbb{Q}}$ opère (resp. opère trivialement) sur le groupe $R_\Gamma^{(s)}/T(R_\Gamma)$ (resp. le groupe à 2 éléments ± 1). Les constantes d'équations fonctionnelles permettent de définir une application $(\chi \to W(\chi))$ de R_Γ dans $\{\pm 1\}$ et par passage au quotient un élément noté $W_{N|\mathbb{Q}}$ du groupe $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_\Gamma^{(s)}/T(R_\Gamma), \pm 1)$. Il existe un homomorphisme naturel de R_Γ sur $R_\Gamma^{(s)}/T(R_\Gamma)$ et un plongement canonique de -1 dans $U(E)$ qui permettent de définir un homomorphisme t^+ de $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_\Gamma^{(s)}/T(R_\Gamma), \pm 1)$ dans $\mathrm{Hom}^{+}_{\Omega_{\mathbb{Q}}}(R_\Gamma, U(E))$ et en composant avec R_ℓ (resp. $\prod_{i=1}^{q} R_{\ell_i}$) un homomorphisme de ce groupe dans $E_\ell(\Gamma)$ (resp. $E_{\ell_1 \dots \ell_q}(\Gamma)$ ou $E(\Gamma)$) qu'on note k_ℓ (resp. $k_{\ell_1 \dots \ell_q}$ ou k). Fröhlich ([2]) a montré l'égalité : $h_\ell([O_N]) = k_\ell(W_{N|\mathbb{Q}})$. Pour vérifier la conjecture de Fröhlich cette égalité est intéressante lorsque $\prod_{\ell} h_\ell$, où ℓ divise l'ordre de Γ,

est injectif, or ceci est généralement faux. Considérons en effet le diagramme commutatif suivant :



On montre que pour un groupe diédral $D_{5\ell}$, où ℓ est un nombre premier, le noyau de l'homomorphisme u est un 2-groupe, non trivial lorsque $\ell \equiv 1$ (mod. 4). Le groupe $E(\Gamma)$ donne donc une meilleure approche de $D(\Gamma)$ que le produit $\prod_\ell E_\ell(\Gamma)$. Nous allons montrer l'égalité $h([O_N]) = k(W_{N|\mathbb{Q}})$ pour certains groupes et donner des exemples où h est injective.

2. - Groupes presque élémentaires

DÉFINITION. - Nous dirons qu'un groupe Γ est presque élémentaire s'il vérifie les deux conditions :

(i) Γ est produit semi-direct d'un sous-groupe abélien F par un sous-groupe abélien distingué H ,

(ii) tout sous-groupe de H est distingué dans Γ .

Notons m (resp. s) l'ordre de H (resp. F), m_o le P. P. C. M. des ordres des éléments de H , $(\mathbb{Z}/m_o\mathbb{Z})^*$ le groupe des éléments inversibles de l'anneau quotient $(\mathbb{Z}/m_o\mathbb{Z})$. La condition (ii) est équivalente à la condition suivante : Pour tout $y \in F$, il existe $r_y \in (\mathbb{Z}/m_o\mathbb{Z})^*$, tel que $yxy^{-1} = x^{r_y}$ pour tout x de H . On peut noter que les groupes Γ_K-élémentaires, ([8]), et les groupes métacycliques sont presque élémentaires.

Le groupe F opère sur le groupe multiplicatif des caractères de degré 1 de H ; on note $\hat{\chi}$ l'orbite du caractère χ de H , $g_{\hat{\chi}}$ l'ordre de χ qui ne dépend que de $\hat{\chi}$ et $F_{\hat{\chi}}$ le groupe d'isotropie de χ dans F . Soient y_i , $1 \leq i \leq q$, des éléments de F dont les classes modulo $F_{\hat{\chi}}$ engendrent le groupe $F/F_{\hat{\chi}}$;

notons $h_{\hat{\chi}}$ (resp. $d_{\hat{\chi}}$) l'ordre de $F_{\hat{\chi}}$ (resp. le P. G. C. D. $(g_{\hat{\chi}}, r_{y_i}-1)$, $1 \leq i \leq q$). On dit que Γ vérifie la condition (C) si on a pour toute classe $\hat{\chi}$ de caractères de H, $(g_{\hat{\chi}}, h_{\hat{\chi}}) = 1$ et $(g_{\hat{\chi}}/d_{\hat{\chi}}, d_{\hat{\chi}}) = 1$.

THÉORÈME 1. - L'anneau O_N des entiers d'une extension N galoisienne modérément ramifiée de $\mathbb{Q}$ dont le groupe de Galois est presque élémentaire et vérifie la condition (C) satisfait l'égalité : $h([O_N]) = k(W_{N|\mathbb{Q}})$.

Pour démontrer le théorème il suffit de construire un élément y de $\mathrm{Hom}^{+}_{\Omega_{\mathbb{Q}}}(R_\Gamma, O_E^*)$ à valeurs dans le groupe des racines $2s$-èmes de l'unité et qui vérifie les congruences : $y(\chi) \equiv \tau(\chi)^{-1} \pmod{\mathfrak{L}}$ pour tout caractère χ de $\mathrm{Ker}\, d_\ell$ et tout diviseur premier ℓ de l'ordre de Γ où $\tau(\chi)$ désigne la somme de Gauss galoisienne associée à χ.

Remarque 1. - Tout groupe Γ_K-élémentaire qui vérifie la 2-ème condition de (C) et tout groupe dont les sous-groupes de Sylow sont cycliques est du type précédent.

Remarque 2. - Soit χ un caractère irréductible orthogonal de Γ, il est induit par un caractère de degré 1 d'un sous-groupe U de Γ ; notons E le corps des invariants de U, 1^* le caractère $\mathrm{Ind}_U^\Gamma 1$ et $n(\chi)$ le nombre de diviseurs premiers inertes dans E du conducteur du caractère $\chi - 1^*$. On peut alors remarquer que la restriction de y aux caractères de Γ à valeurs réelles est triviale sur les caractères symplectiques et vérifie $y(\chi - 1^*) = (-1)^{n(\chi)}$ pour les caractères orthogonaux irréductibles.

3. - Théorèmes de base normale

Nous donnons maintenant des exemples de groupe Γ pour lesquels $D_o(\Gamma)$ est isomorphe à un groupe $E_{\ell_1 \cdots \ell_q}(\Gamma)$. Nous nous restreignons à des groupes métacycliques, c'est-à-dire à des groupes tels que H et F soient cycliques. Soit y un générateur de F ; on note r (resp. u) l'entier r_y (resp. l'ordre de r dans $(\mathbb{Z}/m\mathbb{Z})^*$).

THÉORÈME 2. - Soit Γ un groupe métacyclique. Si l'une des deux conditions suivantes est vérifiée :

(i) $ms/\chi(1)$ est sans facteur carré pour tout caractère irréductible χ de Γ tel que $\chi(1)>1$,

(ii) m est de la forme ℓ^n où ℓ est un nombre premier impair, régulier si $n>1$, u est égal à s ou $s/2$ et l'ordre de 2 dans $(\mathbb{Z}/\ell\,\mathbb{Z})^*$ est pair si $n>1$ et $u=s/2$.

Alors il existe des diviseurs premiers ℓ_i , $1\leq i\leq q$, de l'ordre de Γ tels que les groupes $D_o(\Gamma)$ et $E_{\ell_1\cdots\ell_q}(\Gamma)$ soient isomorphes.

COROLLAIRE 1. - Toute extension galoisienne et modérément ramifiée de $\mathbb{Q}$ dont le degré est sans facteur carré possède une base normale d'entiers.

COROLLAIRE 2. - Soit N une extension galoisienne modérément ramifiée de $\mathbb{Q}$ dont le groupe de Galois Γ est isomorphe au groupe quaternionien généralisé H_{4m} d'ordre 4m , m impair. Si l'une des deux conditions suivantes est vérifiée :

(i) m est sans facteur carré,

(ii) m est de la forme ℓ^n où ℓ est un nombre premier régulier et l'ordre de 2 dans $(\mathbb{Z}/\ell\,\mathbb{Z})^*$ est pair.

Alors $[O_N]$ est la classe dans $D(\Gamma)$ de $t^+(W_{N|\mathbb{Q}})$.

Remarque. - Le résultat (ii) du corollaire 2 complète un résultat de Fröhlich ([3]). Si $(-)$ désigne le symbole de Legendre, on remarque que $(\frac{2}{\ell})=-1$ implique (resp. équivaut à, si $\ell\not\equiv 1 \bmod 4$) : l'ordre de 2 dans $(\mathbb{Z}/\ell\,\mathbb{Z})^*$ est pair. On en déduit que si ℓ est un nombre premier régulier, $\ell\equiv 1 \bmod 4$, $\ell\not\equiv 1 \bmod 8$, il existe une base normale d'entiers et que si $\ell\equiv -1 \bmod 4$, $\ell\not\equiv -1 \bmod 8$, une telle base existe si et seulement si $W_{N|\mathbb{Q}}(\chi)=1$ pour tous les caractères χ symplectiques et irréductibles de Γ .

-:-:-:-

BIBLIOGRAPHIE

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

[2] A. FRÖHLICH, Galois module structure, Durham symposium in algebraic number theory, Academic press, à paraître.

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

[4] A. FRÖHLICH, A normal integral basis theorem, J. of Algebra, vol. 39 (1976), n° 1.

[5] A. FRÖHLICH, E. KEATING and S. M. J. WILSON, The class group of quaternion and dihedral 2-groups, Mathematika, vol. 21 (1974), n° 41.

[6] D. HILBERT, Die theorie der algebraishen Zahlkörper, Jahresbericht D. Math. ver., (1897).

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

[8] J.-P. SERRE, Représentation linéaire des groupes finis, (deuxième édition), Paris, Hermann, 1971.

[9] M. TAYLOR, Journées arithmétiques de Caen, (1976), à paraître.

-:-:-:-

Philippe CASSOU-NOGUÈS
Laboratoire de Mathématiques
et d'Informatique dépendant
de l'Université de Bordeaux I
associé au C. N. R. S.
351, cours de la Libération
33405 TALENCE