

Astérisque

JEAN COUGNARD

Sur l'anneau des entiers des p -extensions

Astérisque, tome 24-25 (1975), p. 15-20

<http://www.numdam.org/item?id=AST_1975__24-25__15_0>

© Société mathématique de France, 1975, 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/>

SUR L'ANNEAU DES ENTIERS DES p -EXTENSIONS

par

Jean COUGNARD

-:-:-:-

Soit $N/\mathbb{Q}$ une extension galoisienne et G son groupe de Galois. On note $\mathbb{O}_N$ la clôture intégrale de $\mathbb{Z}$ dans N , c'est un $\mathbb{Z}[G]$ module. Soit B un ordre maximal de $\mathbb{Q}[G]$ contenant $\mathbb{Z}[G]$. Le B -module $\mathcal{M} = B \otimes_{\mathbb{O}_N}$ est B -projectif. On conjecture que $\mathcal{M}$ est B stablement libre.

Lorsque $N/\mathbb{Q}$ est modérément ramifiée la conjecture est démontrée [3].

Nous allons regarder le cas où G est un p -groupe fini sans hypothèse sur la ramification.

L'algèbre $\mathbb{Q}[G]$ est semi-simple et se décompose en un produit d'algèbres simples $L_i = e_i \mathbb{Q}[G]$, les e_i étant des idempotents du centre. On a alors $B = \prod B_i$ (resp. $\mathcal{M} = \prod \mathcal{M}_i$) avec $B_i = e_i B$ (resp. $\mathcal{M}_i = e_i \mathcal{M}$) et on pose $\Lambda_i = e_i \mathbb{Z}[G]$.

Le B -module $\mathcal{M}$ est B -stablement libre si et seulement si pour chaque i , $\mathcal{M}_i$ est B_i -stablement libre.

Etant donné ψ , un caractère absolument irréductible de G , il se prolonge par linéarité à $\mathbb{Q}[G]$ et il existe un unique facteur simple de $\mathbb{Q}[G]$ sur lequel ψ ne s'annule pas [2]. Désignons par L_ψ ce facteur. Rappelons le résultat suivant sur les caractères des p -groupes [2]:

PROPOSITION. - Soit ψ un caractère absolument irréductible d'un p -groupe fini G . Il existe un sous-groupe H et un caractère η de H tels que :

- a) ψ est le caractère induit par η
- b) $Q(\psi) = Q(\eta)$
- c) si p est impair $H/\text{Ker } \eta$ est un groupe cyclique d'ordre p^n ,
si $p = 2$, $H/\text{Ker } \eta$ est soit un groupe cyclique d'ordre 2^n , soit un
groupe diédral d'ordre 2^{n+1} ($n \geq 2$), soit un groupe de type M_n ("faux diédral")
d'ordre 2^{n+1} ($n \geq 3$).

Dans chacun des cas il existe un sous-groupe H' de H et un caractère χ , de degré 1, de H' tels que η soit induit par χ et que $H'/\text{Ker } \chi$ soit un groupe cyclique d'ordre p^n . Dans le cas p impair on constate aisément que $H' = H$. On notera K le sous-corps de N invariant par H' . Si p^r est l'exposant du groupe G , on notera $\mathbb{Q}''$ le corps obtenu en adjoignant à $\mathbb{Q}$ les racines p^r -ièmes de l'unité. Pour tout corps C on désignera par C' le corps obtenu en adjoignant à C les racines p^n -ièmes de l'unité.

On pose $t = [G : H]$. Si on appelle ρ la représentation induite par le caractère χ on constate, dans le cas p impair, que l'on peut identifier au moyen de ρ le facteur simple L_ψ avec $M_t(\mathbb{Q}')$. On remarque alors que l'image de $\mathbb{Z}[G]$ est incluse dans l'ordre maximal $M_t(\mathbb{Z}[\zeta])$ où ζ désigne une racine primitive p^n -ième de l'unité. On peut alors démontrer :

THÉORÈME. - Soit $N/\mathbb{Q}$ une p -extension galoisienne finie de groupe de Galois G , linéairement disjointe de $\mathbb{Q}'$ sur $\mathbb{Q}$ alors $B^{\mathbb{Q}_N}$ est B -stablement libre.

Remarque 1. - Nous donnerons l'esquisse de la démonstration pour p -impair.

Remarque 2. - L'hypothèse de disjonction linéaire n'est pas essentielle mais permet de simplifier les démonstrations.

Remarque 3. - Le résultat est indépendant du choix de B , on peut donc supposer dans le cas p -impair que $B_{\Psi} = M_t(\mathbb{Z}[\zeta])$.

DÉFINITION. - Soit θ un élément de N , on appelle résolvante de Lagrange de θ et de χ l'élément de N' :

$$\langle \theta, \chi \rangle = \sum_{h \in H} h(\theta) \chi(h^{-1})$$

Notations. - On choisit γ_i ($i = 1, \dots, t$) un système de représentants des classes à droite de G modulo H .

On considère θ_0 un élément de N qui engendre une base normale de $N/\mathbb{Q}$ et de N/K .

Le choix de θ_0 définit un $\mathbb{Q}[G]$ -isomorphisme g entre $\mathbb{Q}[G]$ et N . Dans cet isomorphisme l'image réciproque de $\mathbb{Q}_N$ est un idéal fractionnaire de $\mathbb{Z}[G]$; il existe donc un idéal fractionnaire $\mathfrak{J}$ de B tel que $g(\mathfrak{J}) = B^{\mathbb{Q}_N}$ et on a $\mathfrak{J} = \prod \mathfrak{J}_i$ avec $\mathfrak{J}_i = e_i \mathfrak{J}$.

On démontre aisément la proposition :

PROPOSITION. - L'application φ de N dans K' définie par $\varphi(\theta) = \frac{\langle \theta, \chi \rangle}{\langle \theta_0, \chi \rangle}$ est un homomorphisme surjectif de $\mathbb{Q}$ -espaces vectoriels.

On en déduit immédiatement que les $\varphi(v_j^{-1} \theta_0)$ forment une $\mathbb{Q}'$ base de K' .

DÉFINITION. - Soit V le $\mathbb{Q}'$ espace vectoriel défini par $V = \bigoplus_{i=1}^t V_i$ où chacun des V_i est une copie de K' et soit f l'application de N dans V définie par :

$$f(\theta) = (\varphi(v_1^{-1} \theta), \dots, \varphi(v_i^{-1} \theta), \dots, \varphi(v_t^{-1} \theta)).$$

On constate que le noyau de f est invariant par G et donc qu'il est possible, par transport de structure, de considérer $f(N)$ comme un $\mathbb{Q}[G]$ -module, de sorte que f soit un homomorphisme de $\mathbb{Q}[G]$ -modules.

On veut obtenir des renseignements complémentaires concernant $f(N)$. On regarde pour cela V . On a : $\dim_{\mathbb{Q}'}(V) = t^2 \dim_{\mathbb{Q}}(M_t(\mathbb{Q}'))$. Grâce à cette remarque, on va faire opérer $M_t(\mathbb{Q}')$ sur V . Choisissons v_{ij} la $\mathbb{Q}'$ base de V où v_{ij} est l'élément dont toutes les composantes sont nulles sauf la i -ème égale à $\varphi(v_j^{-1} \theta_0)$. Si $e_{k,\ell}$ est la matrice carrée d'ordre t dont tous les coefficients sont nuls, sauf celui de la k -ième ligne et de la ℓ -ième colonne qui vaut 1, on pose : $e_{k,\ell} * v_{ij} = \delta_{\ell,i} v_{k,j}$. On remarque que $e_{11} * V = V_1$ et que $f(g \theta_0) = \rho(g) * f(\theta_0)$. La seconde remarque permet de démontrer que $f(N) = V$ et que $f \circ g$ induit un L_Ψ isomorphisme entre L_Ψ et V .

Pour démontrer que $\mathcal{M}_\Psi$ est B_Ψ -stablement libre, il faut et il suffit que l'on démontre que $N_{\text{red}} I_\Psi$ est un idéal principal. On note $\chi(R_1, R_2)$ l'invariant relatif de deux $\mathbb{Z}[\zeta]$ réseaux de même rang [4]. On a :

$$N_{\text{red}}^t(I_\Psi) = N(I_\Psi) = \chi(I_\Psi, B_\Psi) = \chi(f \circ g(I_\Psi), f \circ g(B_\Psi)) = \chi(f(B \otimes_N), f(B \otimes_O))$$

mais puisque l'on a choisi $B_\Psi = M_t(\mathbb{Z}[\zeta])$

$$\chi(f(B \otimes_N), f(B \otimes_O)) = \chi^t(e_{11} * f(B \otimes_N), e_{11} * f(B \otimes_O)).$$

Le calcul de l'invariant relatif de deux réseaux se fait localement. Soit donc $\mathfrak{L}$ un idéal premier de $\mathbb{Q}[\zeta]$. Supposons $\mathfrak{L}$ premier à p , on a alors

$\Lambda_{\psi, \mathfrak{L}} = B_{\psi, \mathfrak{L}}$, d'où :

$$\begin{aligned} v_{\mathfrak{L}}[\chi(e_{11} * f(B \otimes_N), e_{11} * f(B \otimes_0))] &= v_{\mathfrak{L}}[\chi(e_{11} * B_{\psi, \mathfrak{L}}^{f(\otimes_N)}, e_{11} * B_{\psi, \mathfrak{L}}^{f(\otimes_0)})] \\ &= v_{\mathfrak{L}}[\chi(e_{11} * \Lambda_{\psi, \mathfrak{L}}^{f(\otimes_N)}, e_{11} * \Lambda_{\psi, \mathfrak{L}}^{f(\otimes_0)})] \\ &= v_{\mathfrak{L}}[\chi(e_{11} * \mathbb{Z}[\zeta]_{\mathfrak{L}} \otimes_{\mathbb{Z}[\zeta]} f(\otimes_N), e_{11} * \mathbb{Z}[\zeta]_{\mathfrak{L}} \otimes_{\mathbb{Z}[\zeta]} f(\mathbb{Z}[G] \otimes_0)) \\ &= v_{\mathfrak{L}}(\chi(\varphi(\otimes_N), \varphi(\mathbb{Z}[G] \otimes_0))). \end{aligned}$$

De ces égalités il découle que $N_{\text{red}}^{(I_{\psi})}$ coïncide avec $\chi(\varphi(\otimes_N), \varphi(\mathbb{Z}[G] \otimes_0))$ sauf pour la place de $\mathbb{Z}[\zeta]$ au-dessus de (p) . Donc il faut et il suffit que $\chi(\varphi(\otimes_N), \varphi(\mathbb{Z}[G] \otimes_0))$ soit principal. Ce résultat se déduit de la décomposition de $\langle \otimes_0, \chi \rangle^{p^n}$ en idéaux et des propriétés de Stickelberger [1].

Remarque. - Dans le cas $p = 2$, $H/\text{Ker } \eta$ non cyclique, on aboutit à $N_{\text{red}}^2(\mathfrak{I})$ et $\chi(\varphi(\otimes_B), \varphi(\mathbb{Z}[G] \otimes_0))$ coïncident sauf éventuellement au dessus de 2. Le résultat découle alors du fait que le nombre de classes (resp. le nombre de classes au sens restreint) d'un sous-corps de $\mathbb{Q}(\zeta)$ (resp. du sous-corps réel maximal de $\mathbb{Q}[\zeta]$) est impair.

-:-:-:-

BIBLIOGRAPHIE

- [1] CHATELET A. - Idéaux principaux dans les corps circulaires. Colloque du C. N. R. S. Algèbre et Théorie des Nombres, Paris (1949) p. 103-106.

J. COUGNARD

- [2] FONTAINE J. M. - Sur la décomposition des algèbres de groupes. Annales de l'E. N. S. , 4ème série, T. 4. (1971) p. 121 à 180.
- [3] FRÖHLICH A. - Galois module structure. Journées Arithmétiques de Bordeaux, 1974.
- [4] SERRE J. -P. - Corps locaux. Paris, Hermann.

-:-:-:-

Jean COUGNARD
E.R.A. au C.N.R.S. n° 362
U. E. R. de Mathématiques
et d'Informatique
Université de Bordeaux I
351, cours de la Libération
33405 TALENCE