MÉMOIRES DE LA S. M. F.

MARIE-JOSE FERTON

Sur l’anneau des entiers d’extensions cycliques d’un corps local

Mémoires de la S. M. F., tome 37 (1974), p. 69-74
<http://www.numdam.org/item?id=MSMF_1974__37__69_0>

Journées arithmétiques [1973, Grenoble]
Bull. Soc. math. France,
Mémoire 37, 1974, p. 69-74

SUR L'ANNEAU DES ENTIERS D'EXTENSIONS CYCLIQUES D'UN CORPS LOCAL

par

Marie-José FERTON

-:-:-:-

(Les résultats exposés ont été obtenus avec la collaboration de Madame F. Bertrandias).

1. Préliminaires sur l'anneau des entiers d'une extension galoisienne.

1.1. Si k est le corps des quotients d'un anneau de Dedekind A , et si K/k est une extension galoisienne de groupe de Galois G , alors la clôture intégrale de A dans K , B , est un $A[G]$-module. B est un $A[G]$-module projectif si et seulement si K/k est une extension modérément ramifiée. Pour que B soit un $A[G]$-module libre il est donc nécessaire que l'extension K/k soit modérément ramifiée ; cette condition n'est pas suffisante en général, elle l'est cependant dans le cas où k est un corps local [8] .

Pour étudier la structure de B sans faire d'hypothèses sur la ramification dans K/k , on introduit le sous-anneau $\mathfrak{B}$ de $k[G]$ défini par :

$$\mathfrak{B} = \{\lambda \in k[G], \lambda . B \subset B\} . \quad [7]$$

On montre que $\mathfrak{B}$ est un ordre de A dans $k[G]$, on l'appelle l'ordre associé à B dans $k[G]$. B est donc un $\mathfrak{B}$-module, on est alors amené à chercher pour quelles extensions, K/k , B est un $\mathfrak{B}$-module libre.

On sait par exemple, que B est libre sur son ordre associé dans les cas suivants :

a) $k = \mathbb{Q}$, corps des rationnels, et G est abélien [6] .

b) $k = \mathbb{Q}$ et G est un groupe diédral d'ordre $2p$ [1] .

On s'intéresse ici aux extensions K/k d'un corps local k .

1.2. Pour étudier B comme $\mathfrak{B}$-module, on introduit un idéal à gauche de $\mathfrak{B}$ dans $k[G]$ qui soit isomorphe à B en tant que $\mathfrak{B}$-module.

A étant un anneau de Dedekind, il existe un élément θ de B qui engendre une base normale de K/k .

Pour un tel θ , on définit :

$$\mathfrak{A}_\theta = \{\lambda \in k[G], \lambda.\theta \in B\} .$$

On voit que $B = \mathfrak{A}_\theta.\theta$, que $\mathcal{B} \subset \mathfrak{A}_\theta$ et que $\mathfrak{A}_\theta$ est un idéal à gauche de $\mathcal{B}$ [3] . D'autre part, on démontre que :

PROPOSITION 1. - Les quatre assertions suivantes sont équivalentes :

(i) B est un $\mathcal{B}$-module libre.

(ii) Il existe θ tel que $\mathfrak{A}_\theta = \mathcal{B}$.

(iii) Il existe θ tel que $\mathfrak{A}_\theta$ soit un anneau.

(iv) Quel que soit θ , $\mathfrak{A}_\theta$ est un idéal principal de $\mathcal{B}$.

2. Cas d'une extension cyclique de degré premier d'un corps local.

2.1. Dans ce paragraphe, k est un corps local de caractéristique 0 et de caractéristique résiduelle p , p nombre premier. K est une extension cyclique de degré p de k . On note σ un générateur du groupe de Galois G et $f = \sigma - 1$ dans $k[G]$. e est l'indice de ramification absolu de k et t le nombre de ramification de K/k ; on sait que $-1 \leq t \leq \frac{pe}{p-1}$ [9] . On supposera dans la suite que $t \geq 1$.

Posons $t = a_o p + a$, a_o étant la partie entière de $\frac{t}{p}$, $a_o = [\frac{t}{p}]$; on vérifie que a peut prendre toutes les valeurs de 0 à $p-1$ [9] .

Pour $a = 0$, on a $t = \frac{pe}{p-1}$ et B est libre sur $\mathcal{B}$ qui coïncide dans ce cas avec l'ordre maximal dans $k[G]$.

Pour $a \neq 0$, on détermine un $\mathfrak{A}_\theta$ et l'ordre associe $\mathcal{B}$. π et ϖ désignant respectivement des uniformisantes de B et de A , on a :

2.2. PROPOSITION 2. - Si $t \geq 1$ et $t \not\equiv 0 \pmod p$, $\theta = \pi^a$ engendre une base normale de K/k et $\mathfrak{A}_\theta$ est le sous A-module de $k[G]$ engendré par la famille $\left(\frac{f^i}{\varpi^{\nu_i}}\right)_{0 \leq i \leq p-1}$ où $\nu_i = [\frac{it+a}{p}] = ia_o + [\frac{(i+1)a}{p}]$.

PROPOSITION 3. - L'ordre associé $\mathfrak{D}$ est le sous A-module de $k[G]$ engendré par la famille $\left(\frac{f^i}{\varpi^{n_i}}\right)_{0\le i\le p-1}$ où $n_i = \min_{0\le j\le p-1-i} (\nu_{i+j}-\nu_j)$.

Remarque 1 : L'idempotent $\frac{1}{p}\sum_{i=0}^{p-1}\sigma^i$ de $k[G]$ appartient à $\mathfrak{D}$ si et seulement si :

$$\frac{pe}{p-1} - 1 \le t \le \frac{pe}{p-1} .$$

Dans ces conditions, on dira que l'indice t est "presque maximal" [5].

2.3. Cas où l'indice de ramification t , n'est pas "presque maximal".

On démontre que pour $a \neq 0$:

PROPOSITION 4. -

a) Si $\theta = \pi^a$, $\mathfrak{A}_\theta = \mathfrak{D}$ si et seulement si a divise $p-1$.

b) Si $t < \frac{pe}{p-1}-1$ et si a ne divise pas $p-1$, $\mathfrak{A}_\theta$ n'est pas un idéal principal de $\mathfrak{D}$.

Ces résultats se résument dans le théorème :

THEOREME 1. -

a) Si $t \equiv 0 \pmod p$, B est libre sur $\mathfrak{D}$.

b) Si $t \not\equiv 0 \pmod p$ et si $t < \frac{pe}{p-1}-1$, pour que B soit libre sur $\mathfrak{D}$, il faut et il suffit que a divise $p-1$.

Remarque 2 : Si l'on introduit le développement en fraction continue de $\frac{t}{p}$,

$$\frac{t}{p} = a_o + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}} = [a_o, a_1, \dots, a_n] \text{ avec } a_n > 1 ,$$

on remarque que l'on a $a = 0$ où a divise $p-1$ si et seulement si $n \le 2$.

COROLLAIRE (d'après une remarque de J. MARTINET). - Si t vérifie les conditions : $t \not\equiv 0 \pmod p$, $t < \frac{pe}{p-1} - 1$ et si a ne divise pas $p-1$, B n'est pas un $\mathfrak{D}$-module projectif.

Ceci donne une réponse à la question posée dans [7] .

2.4. Cas où l'indice de ramification est "presque maximal", c'est-à-dire où

$$\frac{pe}{p-1} - 1 \leq t \leq \frac{pe}{p-1} .$$

Le résultat est le suivant [2 bis] :

THEOREME 2. - <u>Si</u> t <u>est</u> "<u>presque maximal</u>", <u>pour que</u> B <u>soit libre sur son ordre associé</u> $\mathfrak{A}$, <u>il faut et il suffit que</u>, <u>dans le développement en fraction continue de</u> $\frac{t}{p}$, n <u>soit inférieur ou égal à</u> 4 (<u>voir remarque</u> 2, <u>pour la définition de</u> n).

Exemples : Si $p = 7$, $t = 5$, $e = 5$, t est "presque maximal" et $n = 3$, B est donc une $\mathfrak{A}$-module libre.

Si $p = 13$, $t = 8$, $e = 8$, t est "presque maximal" et $n = 5$, B n'est donc pas libre sur son ordre associé.

Le problème est donc entièrement résolu pour les extensions cycliques de degré premier d'un corps local ; la rédaction détaillée des démonstrations se trouve dans [4] .

3. <u>Cas d'une extension cyclique de degré</u> p^2 <u>d'un corps local</u>.

Dans ce paragraphe K/k est une extension cyclique de degré p^2 d'un corps local k de caractéristique résiduelle p et d'indice de ramification absolu e . σ est un générateur du groupe de Galois G . t_1 et t_2 désignant les deux nombres inférieurs de ramification de l'extension, on sait que :

$$t_1 \leq \frac{pe}{p-1} \quad , \quad t_2 \leq \frac{p^2 e}{p-1} \quad \text{et} \quad t_1 \equiv t_2 \pmod p .$$

On note a l'entier compris entre 0 et $p-1$ tel que $t_1 \equiv a \pmod p$. On montre que les idempotents $\frac{T}{p^2} = \frac{1}{p^2} \sum_{i=0}^{p^2-1} \sigma^i$ et $\frac{T_1}{p} = \frac{1}{p} \sum_{i=0}^{p-1} \sigma^{ip}$ appartiennent à l'ordre associé à B dans $k[G]$, $\mathfrak{A}$, si et seulement si : $\frac{pe}{p-1} - 1 \leq t_1 \leq \frac{pe}{p-1}$; dans ce cas on dira que la fonction indice est "presque maximale" [5] .

En utilisant une méthode analogue à celle employée dans le cas cyclique de degré premier, on obtient les résultats suivants, qui ne sont que partiels :

PROPOSITION 5. - <u>On suppose que les conditions suivantes sont vérifiées</u> :

$$\frac{1}{2}\frac{pe}{p-1} < t_1 < \frac{pe}{p-1} - 1 \ , \ t_1 \not\equiv t_2 \ (\mathrm{mod}\ p^2) \quad \text{et} \quad t_2 \equiv a(1+p) \ (\mathrm{mod}\ p^2) \ ;$$

<u>alors</u>, <u>quel que soit</u> a, B <u>n'est pas un $\mathfrak{D}$-module libre</u>.

PROPOSITION 6. - <u>On suppose la fonction indice</u> "<u>presque maximale</u>" <u>et</u> $t_1 \not\equiv t_2 \ (\mathrm{mod}\ p^2)$; <u>alors si</u> $a = 0$ <u>ou si</u> a <u>divise</u> p-1 , B <u>est un $\mathfrak{D}$-module libre</u>.

Pour les corps locaux, k , d'indice de ramification absolu $e = 1$, on a pour toute extension cyclique de degré p^2 , K/k , $t_1 = 1$ et $t_2 = 1+p$; la fonction indice est donc "presque maximale" et par suite B est toujours libre sur son ordre associé.

-:-:-:-

BIBLIOGRAPHIE

[1] A.M. BERGE. - Sur l'arithmétique d'une extension diédrale. Séminaire Delange-Pisot - Poitou : Théorie des nombres, 12e année, 1970/71, n° 14.

[2] F. BERTRANDIAS et M.J. FERTON. - C.R. Acad. Sc. Paris, t. 274, 1972, Sér.A, p. 1330-1333.

[2bis] F. BERTRANDIAS, J.P. BERTRANDIAS et M.J. FERTON. - C.R. Acad. Sc. Paris, t. 274, 1972, Sér.A, p.1388-1391.

[3] M. DEURING. - Algebren. Berlin, Springer Verlag, 1935.

[4] M.J. FERTON. - Sur l'anneau des entiers d'extensions cycliques de degré p et d'extensions diédrales de degré 2p d'un corps local. (Thèse 3e cycle, Math. Univ. Grenoble).

[5] H. JACOBINSKI. - J. reine angew. Math., t.213, 1964, p.151-164.

[6] H.W. LEOPOLDT. - J. reine angew. Math., t.201, 1959, p.119-149.

[7] J. MARTINET. - Anneau des entiers d'une extension galoisienne considéré comme module sur l'algèbre du groupes de Galois. Colloque de Théorie des Nombres [1969-Bordeaux], Bull. Soc. Math. France, Mémoire 25, 1971, p.123-126.

[8] E. NOETHER. - J. reine angew. Math., t.267, 1932, p. 147-152.

[9] J.P. SERRE. - Corps locaux. Hermann, Paris, 1962.

-:-:-:-

Université scientifique et médicale de Grenoble
Institut de Mathématiques Pures
Associé au C.N.R.S. n° 188
BP 116

38402 ST MARTIN D'HERES