Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Marie-Josée Ferton

Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 14, n° 1 (1972-1973), exp. n° 2, p. 1-6

<http://www.numdam.org/item?id=SDPP_1972-1973__14_1_A2_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
14e année, 1972/73, n° 2, 6 p.

16 octobre 1972

SUR L'ANNEAU DES ENTIERS D'UNE EXTENSION CYCLIQUE DE DEGRÉ PREMIER D'UN CORPS LOCAL

par Marie-Josée FERTON

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

1.1. A désigne un anneau de Dedekind de corps des quotients k, et K est une extension galoisienne de k de groupe de Galois G. On appelle B la clôture intégrale de A dans K. Pour que B soit un $A[G]$-module libre, il est nécessaire que l'extension K/k soit modérément ramifiée ; cette condition n'est pas suffisante en général, mais si A est un anneau local elle l'est, d'après E. NOETHER [12].

Pour étudier la structure de B sans faire d'hypothèses sur la ramification dans K/k, on introduit, un sous-anneau de $k[G]$, $\mathfrak{O}$, $\mathfrak{O} = \{\lambda \in k[G],\ \lambda B \subset B\}$. On montre que $\mathfrak{O}$ est un ordre de A dans $k[G]$, on appelle $\mathfrak{O}$ l'ordre associé à B dans $k[G]$. B est donc muni d'une structure de $\mathfrak{O}$-module, et l'on peut se poser la question suivante : pour quelles extensions K/k, B est-il un $\mathfrak{O}$-module libre ?

On connaît de nombreux cas d'extensions pour lesquelles B est libre sur $\mathfrak{O}$:

(a) si $k = \mathbb{Q}$, corps des rationnels et si G est abélien [8],

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

On se propose ici de caractériser les extensions cycliques de degré premier p, d'un corps local, pour lesquelles B est libre sur $\mathfrak{O}$.

1.2. Pour étudier B en tant que $\mathfrak{O}$-module, on introduit un idéal à gauche de $\mathfrak{O}$ dans $k[G]$ qui soit isomorphe à B comme $\mathfrak{O}$-module. A étant un anneau de Dedekind, on sait qu'il existe toujours un élément θ de B qui engendre une base normale de K/k. Pour un tel θ, soit :

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

D'après les définitions de $\mathfrak{O}$ et de $\mathfrak{A}_\theta$ et les résultats de [5], on voit que $B = \mathfrak{A}_\theta.\theta$, que $\mathfrak{O} \subset \mathfrak{A}_\theta$, que $\mathfrak{A}_\theta$ est un idéal à gauche de $\mathfrak{O}$, et on obtient le résultat suivant :

PROPOSITION 1. - Les quatre assertions suivantes sont équivalentes :

(i) B est un $\mathfrak{O}$-module libre,

(ii) il existe un θ tel que $\mathfrak{A}_\theta = \mathfrak{O}$,

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

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

2. Cas d'une extension cyclique de corps locaux.

Dans ce paragraphe, k désigne un corps local de caractéristique 0, et dont la caractéristique résiduelle est le nombre premier p ; K est une extension cyclique de degré p de k.

On note σ un générateur du groupe G, et $f = \sigma - 1$ dans $k[G]$. e est l'indice de ramification absolu de k, et t le nombre de ramification de l'extension K/k.

2.1. Rappels.

Si $t = -1$, l'extension K/k est modérément ramifiée, et on a $\mathfrak{O} = A[G]$, et B est libre sur $A[G]$ [10].

On a l'inégalité $t \leqslant pe/(p-1)$, et réciproquement, étant donnés le corps k et un entier t premier à p tel que $1 \leqslant t \leqslant pe/(p-1)$, il existe des extensions cycliques de degré p de k, K, ayant t pour nombre de ramification [13].

Si le nombre de ramification t est divisible par p, k contient les racines p-ième de l'unité, et il existe une uniformisante ϖ de k telle que

$$K = k(\varpi^{1/p}) .$$

De plus, $t = pe/(p-1)$ ([9], théorème 3).

2.2. Nous allons déterminer un élément θ de B, engendrant une base normale de K/k, l'idéal $\mathfrak{A}_\theta$ associé et l'ordre $\mathfrak{O}$.

ϖ et π désignent respectivement des uniformisantes de k et K, et on pose a le plus petit entier positif ou nul tel que $t = a_0 p + a$, c'est-à-dire $a_0 = [t/p]$, où $[x]$ désigne la partie entière d'un nombre réel x.

PROPOSITION 2.

(a) *si* $t \geqslant 1$ *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* $\left(\frac{f^i}{\varpi^{\nu_i}}\right)$, $0 \leqslant i \leqslant p-1$, *où*

$$\nu_i = \left[\frac{it + a}{p}\right] = ia_0 + \left[(i+1)\frac{a}{p}\right] .$$

(b) *si* $t \equiv 0 \pmod p$, *et si* ϖ *et* π *sont des uniformisantes respectives de* k *et de* K *telles que* $\pi^p = \varpi$, $\theta = 1 + \pi + \pi^2 + \ldots + \pi^{p-1}$ *engendre une base normale de* K/k, *et* $\mathfrak{A}_\theta$ *coïncide avec l'ordre maximal de* $k[G]$.

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

Pour démontrer cette proposition, on utilise le fait que

$$\mathfrak{O} = \{\lambda \in k[G] , \ \lambda.\mathfrak{U}_\theta \subset \mathfrak{U}_\theta\} .$$

Remarque. - L'idempotent $\frac{1}{p}\sum_{i=0}^{p-1} \sigma^i$ de $k[G]$ appartient à $\mathfrak{O}$ si, et seulement si, $e \leqslant n_{p-1}$, ce qui équivaut à :

$$(1) \qquad \frac{pe}{p-1} - 1 \leqslant t \leqslant \frac{pe}{p-1} .$$

Dans ces conditions, on dira que l'indice de ramification est "presque maximal" [7].

2.3. Cas où l'indice de ramification n'est pas "presque maximal".

LEMME. - $\mathfrak{U}_\theta$ est un anneau si, et seulement si, quel que soit le couple d'entiers (i , j) compris entre 0 et $p - 1$, on a :

(α) si $i + j \leqslant p - 1$, $\nu_i + \nu_j \leqslant \nu_{i+j}$.

(β) si $i + j \geqslant p$, $\nu_i + \nu_j \leqslant e + \nu_{i+j+1-p}$.

Ce lemme se démontre facilement si l'on remarque que $(1 + f)^p = 1$, c'est-à-dire que :

$$f^p = - pf^{p-1} - \binom{p}{2} f^{p-2} - \ldots - \binom{p}{k} f^{p-k} - \ldots - pf .$$

PROPOSITION 4. -

(a) θ étant l'élément défini dans la proposition 2, on a $\mathfrak{U}_\theta = \mathfrak{O}$ si, et seulement si, $a = 0$ ou a divise $p - 1$.

(b) si $t < \frac{pe}{p-1} - 1$, si $a \neq 0$ et si a ne divise pas $p - 1$, $\mathfrak{U}_\theta$ n'est pas un idéal principal de $\mathfrak{O}$.

Démonstration du (a).

$a = 0$, $\mathfrak{U}_\theta$ est égal à l'ordre maximal, et B est donc libre sur $\mathfrak{U}_\theta = \mathfrak{O}$.

$a \neq 0$, les conditions du lemme s'écrivent :

(α') si $i + j \leqslant p - 1$: $[(i + 1)\frac{a}{p}] + [(j + 1)\frac{a}{p}] \leqslant [(i + j + 1)\frac{a}{p}]$

(β') si $i + j \geqslant p$: $[(i + 1)\frac{a}{p}] + [(j + 1)\frac{a}{p}] \leqslant e - (p - 1)\, a_0 + [(i+j+2-p)\frac{a}{p}]$.

Les conditions (β') sont toujours vérifiées.

si a divise $p - 1$, c'est-à-dire $a = (p - 1)/d$, d entier, les conditions (α') s'écrivent : $[i/d] + [j/d] \leqslant [(i + j)/d]$, elles sont donc vérifiées.

si a ne divise pas $p - 1$, montrons qu'il existe un couple (i , j), $i + j \leqslant p - 1$, tel que :

$$[(i + 1)\frac{a}{p}] + [(j + 1)\frac{a}{p}] > [(i + j + 1)\frac{a}{p}] .$$

Ceci s'écrit, si l'on note $\hat{x}$ la partie fractionnaire d'un nombre réel x :

$$\widehat{(i+1)\frac{a}{p}} + \widehat{(j+1)\frac{a}{p}} < \frac{a}{p} + \widehat{(i+j+1)\frac{a}{p}} .$$

Faisons intervenir le développement en fraction continue de t/p ,

$$\frac{t}{p} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}} = [a_0 , a_1 , a_2 , \ldots , a_n] \quad \text{avec} \quad a_n > 1 .$$

Si l'on note q_i les dénominateurs des réduites successives, $q_0 = 1$, $q_1 = a_1$, $q_2 = a_1 q_1 + q_0$, $\cdots$ $q_i = a_i q_{i-1} + q_{i-2}$, $\cdots$ $q_n = p$, on rappelle que : $\widehat{q_m(a/p)} < \frac{a}{p}$ si m est un entier pair strictement positif, et

$$\widehat{q_{n-1}\frac{a}{p}} = \begin{cases} \dfrac{1}{p} & \text{si } n-1 \text{ est pair.} \\ \dfrac{p-1}{p} & \text{si } n-1 \text{ est impair.} \end{cases}$$

Il existe donc k , $1 < k \leqslant p-2$, tel que $\widehat{(k+1)\frac{a}{p}} = (p-1)/p$, prenons en effet

$$k+1 = \begin{cases} q_{n-1} & \text{si } n \text{ est pair} \\ p - q_{n-1} & \text{si } n \text{ est impair.} \end{cases}$$

Il existe i , $1 \leqslant i < k$, tel que $\widehat{(i+1)\frac{a}{p}} < \frac{a}{p}$, prenons

$$i+1 = \begin{cases} q_{n-2} & \text{si } n \text{ est pair} \\ q_{n-1} & \text{si } n \text{ est impair.} \end{cases}$$

En posant $j = k - i$, on a $i + j = k < p - 1$, et

$$\widehat{(i+j)\frac{a}{p}} + \widehat{(j+1)\frac{a}{p}} < \frac{a}{p} + \frac{p-1}{p} = \frac{a}{p} + \widehat{(i+j+1)\frac{a}{p}} .$$

Pour démontrer le (b) de la proposition 4, on montre, par des méthodes d'algèbre linéaire, que si $t < (pe/(p-1)) - 1$, si $a \neq 0$, et si a ne divise pas $p-1$, alors pour tout α dans $\mathfrak{A}_\theta$, l'application, qui à un élément λ de $\mathfrak{O}$ fait correspondre l'élément $\lambda\alpha$ de $\mathfrak{A}_\theta$, n'est pas surjective.

On peut résumer les résultats précédents par le théorème suivant.

THÉORÈME 1.

(a) Si $t \equiv 0 \pmod p$, B est un $\mathfrak{O}$-module libre.

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

COROLLAIRE 1. - Si t vérifie les conditions, $t \not\equiv 0 \pmod p$, $t < (pe/(p-1)) - 1$ et si a ne divise pas $p-1$, B n'est pas un $\mathfrak{O}$-module projectif.

Le corollaire se déduit du théorème en remarquant que $\mathfrak{O}$ est un anneau semi-local et donc que tout $\mathfrak{O}$-module projectif de rang défini est libre [4].

Cette remarque est due à Jacques MARTINET, et le corollaire 1 donne une réponse à la question posée dans [11].

Exemple. - Soit $k = \mathbb{Q}_5(5^{1/4})$, et soit K le corps de décomposition sur k du polynôme $x^5 - x - 5^{-3/4}$, l'extension K/k est cyclique de degré 5 , son nombre de ramification est $t = a = 3$ ([13], chapitre IV, paragraphe 2, exercice 5).

On en déduit que B n'est pas un $\mathfrak{O}$-module projectif.

2.4. Cas où l'indice de ramification est "presque maximal" [3]. - Dans ce paragraphe, le nombre de ramification t est supérieur ou égal à 1 , et vérifie

$$(1) \qquad \frac{pe}{p-1} - 1 \leqslant t \leqslant \frac{pe}{p-1} .$$

Les méthodes employées dans ce cas sont analogues à celles de la démonstration de la proposition 4 ; les démonstrations sont toutefois plus difficiles.

On obtient le théorème suivant.

THÉORÈME 2. - Si t est "presque maximal", pour que B soit un $\mathfrak{O}$-module libre, il faut et il suffit que, dans le développement de t/p en fraction continue, n soit inférieur ou égal à 4 .(Définition de n dans la proposition 4).

Exemples. -

Si $p = 7$, $t = 5$, $e = 5$, t vérifie (1) et $n = 3$: B est libre sur $\mathfrak{O}$.

Si $p = 13$, $t = 8$, $e = 8$, t vérifie (1) et $n = 5$: B n'est pas projectif sur $\mathfrak{O}$.

(On sait qu'il existe des extensions K/k avec p , t , e comme ci-dessus, cf. paragraphe 2.1).

Le problème posé au début de cet exposé est donc résolu ; on a caractérisé par les théorèmes 1 et 2, toutes les extensions K/k , cycliques, de degré p , d'un corps local pour lesquelles B est libre sur son ordre associé dans $k[G]$.

Ces résultats, obtenus en collaboration avec Françoise BERTRANDIAS et Jean-Paul BERTRANDIAS, font l'objet de deux notes aux comptes rendus de l'Académie des Sciences [2] et [3]. Le détail des démonstrations se trouve dans [6].

BIBLIOGRAPHIE

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

[2] BERTRANDIAS (F.) et FERTON (M.-J.). - Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local, C. R. Acad. Sc. Paris, t. 274, 1972, Série A, p. 1330-1333.

[3] BERTRANDIAS (F.) BERTRANDIAS (J.-P.) et FERTON (M.-J.). - Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local, C. R. Acad. Sc. Paris, t. 274, 1972, Série A, p. 1388-1391.

[4] BOURBAKI (N.). - Algèbre commutative, chapitres 2 et 4. - Paris, Hermann, 1961 (Act. scient. et ind., 1290 et 1293 ; Bourbaki, 27 et 28).

[5] DEURING (M.). - Algebren. - Berlin, Springer-Verlag 1935 (Ergebnisse der Mathematik..., 4).

[6] FERTON (M.-J.). - 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,).

[7] JACOBINSKI (H.). - Über die Hauptordnung eines Körpers als Gruppenmodul, J. reine und angew. Math., t. 213, 1964, p. 151-164.

[8] LEOPOLDT (H. W.). - Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, J. reine und angew.Math., t. 201, 1959, p. 119-149.

[9] MACKENZIE (R. E.) et WHAPLES (G.). - Artin-Schreier equations in characteristic zero, Amer. J. Math., t. 78, 1956, p. 473-485.

[10] MARTINET (J.). - Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre 2p , Ann. Inst. Fourier, Grenoble, t. 19, 1969, fascicule 1, p. 1-180.

[11] MARTINET (J.). - Anneau des entiers d'une extension galoisienne considéré comme module sur l'algèbre du groupe de Galois, Colloque de Théorie des nombres [1969. Bordeaux], Bull. Soc. math. France, Mémoire 25, 1971, p. 123-126.

[12] NOETHER (E.). - Normal basis bei Körpern ohne höhere Verzweigung, J. reine und angew. Math., t. 167, 1932, p. 147-152.

[13] SERRE (J.-P.). - Corps locaux. - Paris, Hermann, 1962 (Act. scient. et ind., 1296 ; Publ. Inst. Math. Univ. Nancago, 8).

(Texte reçu le 16 avril 1973)

Marie-Josée FERTON
Institut de Mathématiques pures
Université scientifique et médicale de Grenoble
Boîte postale 116
38402 SAINT MARTIN D'HÈRES