SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

MARIE-JOSÉ FERTON

Sur les idéaux d'une extension cyclique de degré premier d'un corps local

Séminaire de théorie des nombres de Grenoble, tome 2 (1972-1973), exp. n° 2, p. 1-9
<http://www.numdam.org/item?id=STNG_1972-1973__2__A2_0>

Marie-José FERTON

24 mai 1973

SUR LES IDEAUX D'UNE EXTENSION CYCLIQUE DE DEGRE PREMIER D'UN CORPS LOCAL

On se propose, pour une extension cyclique K de degré premier d'un corps local k, de caractériser parmi les idéaux de l'anneau des entiers de K ceux qui sont libres sur leurs ordres associés dans l'algèbre $k[G]$ du groupe $G = Gal(K/k)$ sur le corps k.

On retrouvera en particulier le théorème de [1], cf. remarque 2.

1. PRELIMINAIRES SUR LES ORDRES ASSOCIES AUX IDEAUX D'UNE EXTENSION CYCLIQUE DE DEGRE p.

Soit k un corps local de caractéristique 0, de caractéristique résiduelle le nombre premier p et d'indice de ramification absolu e. K est une extension cyclique de degré p de k, G est le groupe de Galois de cette extension et σ est un générateur de G. On désigne par A l'anneau des entiers de k et par B_o la clôture intégrale de A dans K. On note respectivement ϖ et π des uniformisantes de A et de B_o.

On définit pour tout entier rationnel r :

$B_r = \{\alpha \in K , v_K(\alpha) \geq r\}$ où v_K est la valuation normalisée dans K.

La famille des B_r est celle des idéaux de B_o.

$\mathfrak{O}_r$ désigne l'ordre associé à B_r dans $k[G]$ c'est-à-dire :

$$\mathfrak{O}_r = \{\lambda \in k[G] , \lambda B_r \subset B_r\} .$$

Proposition 1.

Soient r et r' des entiers rationnels vérifiant $r \equiv r' \pmod{p}$

a) on a $\mathfrak{O}_r = \mathfrak{O}_{r'}$,

b) l'application ψ de $B_{r'}$ dans B_r définie par $\psi(x) = \varpi^{\frac{r-r'}{p}} x$ est un isomorphisme de $\mathfrak{O}_r$ modules.

Démonstration de la proposition 1 : Supposons que $r = r'+kp$ avec $k \geq 0$.

a) Nous avons : $B_r = \varpi^k B_{r'}$ et par suite :

$$\mathfrak{O}_r = \{\lambda \in k[G] \ , \ \lambda \varpi^k B_{r'} \subset \varpi^k B_{r'}\} = \mathfrak{O}_{r'} \ .$$

b) Si $B_r = \mathfrak{O}_r \cdot \alpha$, $\alpha \in B_r$ on aura $B_{r'} = \mathfrak{O}_{r'} \cdot \varpi^k \alpha$.

La proposition 1 permet de limiter l'étude aux idéaux B_h , avec $0 \leq h \leq p-1$.

2. ETUDE DES IDEAUX B_h AVEC $0 \leq h \leq p-1$.

■ 2.1. Soit t le nombre de ramification de l'extension K/k . On note a le plus petit entier positif ou nul congru à t modulo p et on pose : $t = a_o p+a$; on note aussi $\frac{t}{p} = [a_o, a_1, \ldots, a_n]$ avec $a_n > 1$, le développement en fraction continue de $\frac{t}{p}$, c'est-à-dire $\frac{t}{p} = a_o + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ldots}}}$. On suppose dans toute la suite que $t \geq 1$ (cf. remarque 3 à la fin).

Rappels.

- Si $a = 0$, on sait que k contient les racines p-ièmes de l'unité et qu'on peut choisir ϖ et π telles que $\varpi = \pi^p$, les éléments θ_h définis pour $0 \leq h \leq p-1$ par : $\theta_h = \pi^h + \pi^{h+1} + \ldots + \pi^{p-1} + \varpi + \varpi\pi + \ldots + \varpi\pi^{h-1}$, engendrent alors tous une base normale de K/k . (1)

- Si $a \neq 0$, l'élément π^a de B_o (respectivement $\varpi\pi^a$) engendre une base normale de K/k (1) .

Définition.

On pose :

pour $a \neq 0$: $\theta_h = \pi^a$ si $0 \leq h \leq a$, $\theta_h = \varpi\pi^a$ si $a < h \leq p-1$

pour $a = 0$: $\theta_h = \pi^h + \pi^{h+1} + \ldots + \pi^{p-1} + \varpi + \varpi\pi + \ldots + \varpi\pi^{h-1}$

et dans tous les cas $\mathfrak{A}_h = \{\lambda \in k[G] , \lambda\theta_h \in B_h\}$.

Proposition 2 (cf(1), proposition 1).

a) Pour tout $0 \leq h \leq p-1$, on a l'inclusion $\mathfrak{O}_h \subset \mathfrak{A}_h$ et $\mathfrak{A}_h$ est un idéal à gauche de $\mathfrak{O}_h$.

b) On a $B_h = \mathfrak{A}_h \cdot \theta_h$.

c) Si $\mathfrak{A}_h$ est un anneau, alors B_h est un $\mathfrak{O}_h$-module libre et on a $\mathfrak{O}_h = \mathfrak{A}_h$.

d) B_h est un $\mathfrak{O}_h$-module libre si et seulement si $\mathfrak{A}_h$ est idéal à gauche principal de $\mathfrak{O}_h$.

■ 2.2. Etude de l'idéal $\mathfrak{A}_h$ de $\mathfrak{O}_h$.

Si σ est un générateur de G on pose $f = \sigma - 1$. On note $[x]$, la partie entière d'un nombre réel x .

Proposition 3.

a) Si $a = 0$, $\mathfrak{A}_h$ coïncide avec l'ordre maximal de $k[G]$.

b) Si $a \neq 0$, $\mathfrak{A}_h$ est le sous-A-module de $k[G]$ engendré par la famille $\left(\frac{f^i}{\varpi^{\nu_i^{(h)}}}\right)_{0 \leq i \leq p-1}$ où pour tout i , $0 \leq i \leq p-1$ on a :

- si $0 \leq h \leq a$, $\nu_i^{(h)} = \left[\frac{it+a-h}{p}\right] = ia_o + \left[\frac{(i+1)a-h}{p}\right]$

- si $a < h \leq p-1$, $\nu_i^{(h)} = \left[\frac{it+a+p-h}{p}\right] = ia_o + \left[\frac{(i+1)a+p-h}{p}\right]$.

Démonstration de la proposition 3 :

a) Si $a = 0$, d'après [2] ch.II §2.1 proposition 1.b), l'ordre maximal de $k[G]$ est le sous-A-module de $k[G]$ engendré par les idempotents,

$0 \le i \le p-1$: ${}_1\chi_i = \frac{1}{p}\sum_{j=0}^{p-1} \zeta^{-ji}\sigma^j$, ζ étant une racine primitive p-ème de l'unité. D'autre part, on a : ${}_1\chi_i\,\theta_h = \begin{cases} \pi^i \text{ si } h \le i \le p-1 \\ \varpi\pi^i \text{ si } 0 \le i < h \end{cases}$; les ${}_1\chi_i\,\theta_h$, $0 \le i \le p-1$, forment donc une A-base de B_h et $\mathfrak{A}_h$ coïncide avec l'ordre maximal.

b) Si $0 \le h \le a$, $a \ne 0$, π^a engendre une base normale de K/k et $\pi^a \in B_h$. On a $v_K(f^i\pi^a) = it+a$ (où v_K est la valuation normalisée dans K) cf. [2] ch.II §2.1 lemme 1 . Les p éléments, $f^i\pi^a$, $0 \le i \le p-1$, sont de valuations toutes différentes modulo p , on en déduit que la famille $\left(\frac{f^i}{\varpi^{\nu_i^{(h)}}}\right)_{0\le i\le p-1}$ avec $\nu_i^{(h)} = \left[\frac{it+a-h}{p}\right]$ est une A-base de B_h , d'où le résultat.

Si $a < h \le p-1$, $\varpi\pi^a$ engendre une base normale de K/k et $\varpi\pi^a \in B_h$, de plus, $v_K(f^i\varpi\pi^a) = it+a+p$. Pour la même raison la famille $\left(\frac{f^i}{\varpi^{\nu_i^{(h)}}}\right)_{0\le i\le p-1}$ avec $\nu_i^{(h)} = \left[\frac{it+a+p-h}{p}\right]$ est une A-base de B_h .

Proposition 4.

$\frac{t}{p} = [a_o, a_1, \ldots, a_n]$, $a_n > 1$ étant le développement en fraction continue de $\frac{t}{p}$ on a :

a) si $a = 0$, $\mathfrak{A}_h$ coïncide avec $\mathfrak{D}_h$ pour tout h , $0 \le h \le p-1$.

b) si $a = 1$, $\mathfrak{A}_h$ coïncide avec $\mathfrak{D}_h$ si et seulement si $h = 0$, $h = 1$, ou encore $h > \frac{p+1}{2}$ avec $t < \frac{pe}{p-1} - 1$.

c) si $a \ne 0$ et $a \ne 1$, $\mathfrak{A}_h$ coïncide avec $\mathfrak{D}_h$ si et seulement si h vérifie la condition (C) suivante :

pour n pair : $h = a$ ou $h = a - a_n$

pour n impair : $a - \frac{1}{2}a_n \le h \le a$.

Démonstration de la proposition 4 :

■ Le résultat du a) est évident d'après la proposition 2 a) et la proposition 3 a) .

■ Si $a \neq 0$, $\mathfrak{A}_h$ coïncide avec $\mathfrak{O}_h$ si et seulement si $\mathfrak{A}_h$ est un anneau. Pour que $\mathfrak{A}_h$ soit un anneau, il faut et il suffit que pour tout couple (i,j) d'entiers compris entre 0 et p-1 les relations suivantes soient vérifiées.

(1) si $i+j \leq p-1$, $\nu_i^{(h)} + \nu_j^{(h)} \leq \nu_{i+j}^{(h)}$

(2) si $i+j > p$, $\nu_i^{(h)} + \nu_j^{(h)} \leq e + \nu_{i+j+1-p}^{(h)}$, cf. [2], chapitre II, §2.2, lemme 2 .

Démontrons que si $a \neq 0$, $a \neq 1$ et n pair, alors dans le cas $0 \leq h \leq a$, $\mathfrak{A}_h$ ne coïncide avec $\mathfrak{O}_h$ que si $h = a$ où $h = a-a_n$.

On vérifie aisément que, dans le cas $h \leq a$, les conditions (2) sont toujours satisfaites en effet, l'inégalité : $t \leq \frac{pe}{p-1}$ implique que : $a \leq e-(p-1)a_o$. Les conditions (1) s'écrivent :

$$(1) \qquad i+j \leq p-1 \quad , \quad \left[\frac{(i+1)a-h}{p}\right] + \left[\frac{(j+1)a-h}{p}\right] \leq \left[\frac{(i+j+1)a-h}{p}\right] \quad .$$

Elles sont satisfaites de manière évidente si $h = a$, dans la suite nous supposerons donc $h \neq a$ et nous démontrerons premièrement que si $h \neq a-a_n$, il existe un couple (i,j) ne vérifiant pas (1) , ensuite que si $h = a-a_n$ les inégalités (1) sont vérifiées.

Si $\underset{\vee}{x}$ désigne la partie fractionnaire d'un nombre réel x , les conditions (1) s'écrivent aussi :

$$(1') \quad \text{si} \quad i+j \leq p-1 \quad , \quad \underbrace{\frac{(i+1)a-h}{p}} + \underbrace{\frac{(j+1)a-h}{p}} \geq \frac{a-h}{p} + \underbrace{\frac{(i+j+1)a-h}{p}} \quad .$$

Soient q_i les dénominateurs des réduites successives de $\frac{t}{p}$, $q_o = 1$, $q_1 = a_1, \ldots, q_i = a_i q_{i-1} + q_{i-2}, \ldots, q_n = p$. On sait que si n est pair : $\underbrace{q_{n-1}\frac{a}{p}} = \frac{p-1}{p}$. Posons q l'entier compris entre 0 et p-1 tel que $\underbrace{(q+1)\frac{a}{h}} = \frac{h}{p}$.

On voit que $h = a-a_n$ si et seulement si $q_{n-2} = p-q$; en effet $\underbrace{(p-q)\frac{a}{p}} = \frac{a-h}{p}$ et $q_{n-2} = p-a_n q_{n-1}$ et par suite $\underbrace{q_{n-2}\,\frac{a}{p}} = \frac{a_n}{p}$.

■ Si $h \neq a-a_n$ montrons qu'il existe un couple (i,j) ne vérifiant pas (1') .

si $q+q_{n-1} < p$, le couple $i = q$, $j = q_{n-1}$ ne vérifie pas (1')
si $q+q_{n-1} \geq p$, le couple $i = q-q_{n-1}$, $j = q_{n-1}-q_{n-2}$ ne vérifie pas (1') car :

$$\underbrace{\frac{(q-q_{n-1}+1)a-h}{p}} = \frac{1}{p}$$

et puisque $\underbrace{q_{n-2}\frac{a}{p}} < \frac{a-h}{p} : \underbrace{\frac{(q_{n-1}-q_{n-2}+1)a-h}{p}} < \frac{a-h}{p}$.

■ Si $h = a-a_n$, on a : $q = a_n q_{n-1}$ et seuls les couples (i,j) tels que : $\underbrace{\frac{(i+1)a-h}{p}} + \underbrace{\frac{(j+1)a-h}{p}} = \frac{a-h}{p} + \underbrace{\frac{(i+j+1)a-h}{p}} - 1$ peuvent ne pas vérifier (1') ; c'est-à-dire les couples (i,j) où $\underbrace{\frac{(i+1)a-h}{p}} < \frac{a-h}{p}$ et $\underbrace{\frac{(j+1)a-h}{p}} < \frac{a-h}{p}$. Si $\underbrace{\frac{(i+1)a-h}{p}} < \frac{a-h}{p}$, c'est que $i = xq_{n-1}$ avec $0 \leq x \leq a_n$. Soit donc un couple (i,j) avec $i = xq_{n-1}$, $j = yq_{n-1}$; comme $i+j < p$ on a $x+y \leq a_n$, en effet $p < (a_n+1)q_{n-1}$. Par suite $\underbrace{\frac{(i+j+1)a-h}{p}} < \frac{a-h}{p}$. Comme $p-q = q_{n-2}$ on a $a-h \leq \frac{p-1}{2}$ et par suite

$$\underbrace{\frac{(i+1)a-h}{p}} + \underbrace{\frac{(j+1)a-h}{p}} = \underbrace{\frac{a-h}{p}} + \underbrace{\frac{(i+j+1)a-h}{p}} \quad .$$

Tout couple (i,j) , $i+j \leq p-1$ vérifie donc la condition (1') .

D'après le (c) de la proposition 2, pour les valeurs de h telles que $\mathfrak{A}_h$ coïncide avec $\mathfrak{O}_h$, valeurs données par la proposition 4, B_h est un $\mathfrak{O}_h$-module libre. En particulier, on peut déduire de la proposition 4 un corollaire qui répond à la question suivante de H. Jacobinski : "Existe-t-il toujours pour une extension cyclique de degré premier d'un corps local un idéal qui soit libre sur son ordre associé ? ".

Corollaire.

K/k étant une extension cyclique de degré premier p d'un corps local, si t est le nombre de ramification de K/k , alors tout idéal B_r , où r est un entier rationnel congru à t modulo p , est libre sur son ordre associé dans l'algèbre $k[G]$ du groupe $G = Gal(K/k)$ sur le corps k .

■ 2.3. Détermination de l'ordre associé $\mathfrak{O}_h$. (cf.(1) proposition 4).

Proposition 5.

Si $t < \frac{pe}{p-1} - 1$, c'est-à-dire si l'indice de ramification n'est pas presque maximal (cf.1 §2, Remarque), l'ordre $\mathfrak{O}_h$ est le sous-A-module de $k[G]$ engendré par la famille $\left(\frac{f^i}{\varpi^{n_i^{(h)}}}\right)_{0\le i\le p-1}$ où $n_i^{(h)} = \mathrm{Min}_{0\le j\le p-1-i}(\nu_{i+j}^{(h)} - \nu_j^{(h)})$.

Remarque 1.

Lorsque l'indice de ramification est presque maximal, c'est-à-dire $t \ge \frac{pe}{p-1} - 1$, on obtient un résultat analogue pour l'ordre associé $\mathfrak{O}_h$ mais pour les entiers h tels que $h > a$, dans les formules donnant les entiers $n_i^{(h)}$ interviennent les indices j tels que $i+j \ge p$.

■ 2.4. Proposition 6 (cf.(1) proposition 6).

a) si $1 \le t < \frac{pe}{p-1} - 1$, si $0 \le h \le a$ et si $\mathfrak{A}_h$ ne coïncide pas avec $\mathfrak{O}_h$ alors $\mathfrak{A}_h$ n'est pas un idéal principal de $\mathfrak{O}_h$.

b) si $1 \le t < \frac{pe}{p-1} - 2$, si $a < h \le p-1$ et si $\mathfrak{A}_h$ ne coïncide pas avec $\mathfrak{O}_h$ alors $\mathfrak{A}_h$ n'est pas un idéal principal de $\mathfrak{O}_h$.

3. On peut déduire des résultats obtenus le théorème :

Théorème.

a) si $t \equiv 0 \pmod p$, B_h est un $\mathfrak{O}_h$-module libre quel que soit h , $0 \le h \le p-1$.

b) si $t \equiv 1 \pmod p$ et si $1 \le t < \frac{pe}{p-1} - 2$, B_h est libre sur $\mathfrak{O}_h$ si et seulement si $h = 0$, $h = 1$ ou $h > \frac{p+1}{2}$.

c) si $t \not\equiv 0$ et $t \not\equiv 1 \pmod p$ alors :

- si $1 \le t < \frac{pe}{p-1} - 1$ pour des h tels que $0 \le h \le a$, B_h n'est libre sur $\mathfrak{O}_h$ que si h vérifie la condition (c) de la proposition 4.
- si $1 \le t < \frac{pe}{p-1} - 2$ pour des h tels que $a < h \le p-1$, B_h n'est pas libre sur $\mathfrak{O}_h$.

Remarque 2.

Si $h = 0$, le théorème précédent permet de retrouver le résultat de (1) , à savoir si $t < \frac{pe}{p-1} - 1$, B_o est libre sur $\mathfrak{O}_o$ si et seulement si $a = 0$ ou a divise $p-1$.

Remarque 3.

Si $t = -1$, l'extension K/k est modérément ramifiée, on sait que B_o est libre sur $A[G]$, son ordre associé, et on peut facilement voir que tous les idéaux de B_o sont libres aussi sur $A[G]$.

Remarque 4.

B_h est libre sur $A[G]$ si et seulement si B_h est libre sur $\mathfrak{O}_h$ et $\mathfrak{O}_h = A[G]$.

Si l'indice n'est pas presque maximal, on démontre que ces conditions ne sont réalisées que dans deux cas :

1°) $t = -1$; voir remarque 3.

2°) $t = 1$ alors B_1 est libre $A[G]$.

On retrouve ainsi, dans un cas particulier, les résultats de S. Ullom [3] , c'est-à-dire : B_h n'est libre sur $A[G]$ que si $\mathrm{Trace}_{K/k} B_h = B_{h \cap k}$.

Exemples :

Si $p = 7$, $t = a = 1$, $e = 3$, $B_{o+\lambda_p}$, $B_{1+\lambda_p}$, $B_{5+\lambda_p}$, $B_{6+\lambda_p}$ pour $\lambda \in \mathbb{Z}$, sont les seuls idéaux libres sur leurs ordres associés.

Si $p = 13$, $t = a = 5$, $e = 6$, $B_{3+\lambda_p}$, $B_{5+\lambda_p}$ pour $\lambda \in Z$ sont les seuls idéaux libres sur leurs ordres associés car $\frac{5}{13} = [0,2,1,1,2]$.

Si $p = 13$, $t = a = 7$, $e = 8$, les idéaux libres sur leurs ordres associés sont $B_{4+\lambda_p}$, $B_{5+\lambda_p}$, $B_{6+\lambda_p}$ et $B_{7+\lambda_p}$ pour $\lambda \in Z$, en effet $\frac{7}{13} = [0,1,1,6]$.

-:-:-:-:-

BIBLIOGRAPHIE

[1] - F. BERTRANDIAS et M.J. FERTON : "Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local". C.R.Acad.Sc. Paris, t.274, pp.1330-1333 (3 Mai 1972).

[2] - 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 de Doctorat du 3e cycle présentée à l'Université Scientifique et Médicale de Grenoble (31 Mai 1972).

[3] - S. ULLOM : "Integral normal Bases in Galois Extensions of Local fields". Nagoya Math. J. Vol.39 (1970), pp. 141-148.

-:-:-:-