SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

FRANÇOISE BERTRANDIAS

Décomposition du Galois-module des entiers d'une p-extension cyclique d'un corps local

Séminaire de théorie des nombres de Grenoble, tome 6 (1977-1978), exp. n° 4, p. 1-29

<http://www.numdam.org/item?id=STNG_1977-1978__6__A4_0>

Séminaire de Théorie des Nombres
24 novembre 1977
Grenoble

DECOMPOSITION DU GALOIS-MODULE DES ENTIERS D'UNE p-EXTENSION CYCLIQUE D'UN CORPS LOCAL

par

Françoise BERTRANDIAS

Soit K un corps local de caractéristique 0 et de caractéristique résiduelle p ; soit L une extension galoisienne de K, dont le groupe de Galois G est cyclique d'ordre p^n. On désigne par A l'anneau de valuation de K ; la clôture intégrale B de A dans L est un $A[G]$-module de rang 1. On sait [4] que B est somme directe, d'une manière unique, d'une famille fixée de sous-$A[G]$-modules indécomposables.

On se propose de déterminer cette décomposition lorsque l'extension L/K est totalement ramifiée.

Dans le § 1, on étudie la décomposition des $A[G]$-modules de rang 1 vérifiant une condition restrictive (H).

Dans le § 2, on montre que le $A[G]$-module B est décomposable dans le seul cas de ramification presque maximale (en supposant que (H) est vérifiée).

Dans le § 3, on détermine l'ordre associé à B dans $K[G]$, dans le cas de ramification presque maximale (l'indice e de ramification de K étant supposé non divisible par p).

Dans le § 4, on en déduit, sous les mêmes hypothèses, la décomposition de B en somme directe de sous-$A[G]$-modules indécomposables.

Cette étude généralise au cas cyclique de degré p^n des résultats précédemment démontrés dans le cas cyclique de degré p . ([2] , [3] , [4]).

1. DECOMPOSITION D'UN A[G]-MODULE DE RANG 1 .

On rappelle que G est un groupe cyclique d'ordre p^n (avec $n \geq 1$) , et A l'anneau de valuation du corps local K .

1.1. - Les caractères irréductibles de G sur K .

Soit, pour tout entier $i \geq 1$, $\Phi_{p^i}(X)$ le polynôme cyclotomique d'indice p^i . On a l'isomorphisme de $K[G]$-modules :

$$K[G] \simeq K[X]/X-1 \times K[X]/\Phi_p(X) \times \ldots \times K[X]/\Phi_{p^n}(X)$$

(où un générateur σ de G opère sur $K[X]$ par multiplication par X).

On notera : χ_0 le caractère de la représentation triviale de G sur K , χ_i le caractère de la représentation $K[X]/\Phi_{p^i}(X)$, pour $1 \leq i \leq n$.

Les représentations irréductibles de G sur K sont les composants irréductibles des modules $K[X]/\Phi_{p^i}(X)$, $1 \leq i \leq n$. Notons :

$$\Phi_{p^i}(X) = P_{i,1}(X)\, P_{i,2}(X) \ldots P_{i,r_i}(X)$$

la décomposition de $\Phi_{p^i}(X)$ en produit de polynômes irréductibles de $K[X]$. Le module $K[X]/\Phi_{p^i}(X)$ est somme directe des r_i $K[G]$-modules irréductibles $K[X]/P_{i,j}(X)$, $1 \leq j \leq r_i$.

Le groupe G possède donc $1 + \sum_{i=1}^{n} r_i$ représentations (resp. caractères) irréductibles sur K. On notera I_K l'ensemble des caractères irréductibles de G sur K.

Notons : $\mathbb{Q}_p$ le corps des nombres p-adiques, $\mathbb{Q}_p^{(p^i)}$ (resp. $K^{(p^i)}$) le corps obtenu en adjoignant à $\mathbb{Q}_p$ (resp. K) les racines p^i-ème de 1,

$$E_i = K \cap \mathbb{Q}_p^{(p^i)} .$$

On remarque que les degrés $[\mathbb{Q}_p^{(p^i)} : E_i]$ et $[K^{(p^i)} : K]$ sont égaux (en effet l'extension $\mathbb{Q}_p^{(p^i)}/E_i$ est galoisienne). Par suite, les polynômes $P_{i,j}(X)$ appartiennent à $E_i[X]$ et donc la représentation irréductible de G de module $K[X]/P_{i,j}(X)$ provient par extension des scalaires de la représentation irréductible de G sur E_i de module $E_i[X]/P_{i,j}(X)$. On a l'égalité : $[E_i : \mathbb{Q}_p] = r_i$; en effet, notant $m_i = [K^{(p^i)} : K]$, on a : $d^\circ \Phi_{p^i}(X) = r_i m_i$, et $[\mathbb{Q}_p^{(p^i)} : \mathbb{Q}_p] = [E_i : \mathbb{Q}_p]\, m_i$.

Le groupe de Galois de l'extension $E_i/\mathbb{Q}_p$ permute transitivement les polynômes $P_{i,j}(X)$ $(1 \le j \le r_i)$, et donc aussi les représentations $E_i/P_{i,j}(X)$ et leurs caractères.

La suite des corps E_i est croissante (au sens large) ; notons $E = E_n$. Le groupe $\mathrm{Gal}(E/\mathbb{Q}_p)$ opère transitivement sur l'ensemble des caractères irréductibles χ des représentations $K[X]/P_{i,j}(X)$, $1 \le j \le r_i$ (caractères dont la somme est χ_i, et qu'on appellera les composants irréductibles de χ_i). Le groupe $\mathrm{Gal}(E/\mathbb{Q}_p)$ opère donc sur l'ensemble I_K des caractères irréductibles de G sur K ; il y a $n+1$ trajectoires : $\{\chi_0\}$, et, pour $1 \le i \le n$, $\{\chi \,;\, \chi$ composant irréductible de $\chi_i\}$.

Remarque 1. - $I_K = I_E$, c'est-à-dire : le groupe G a mêmes caractères irréductibles sur K et sur E. En effet, $E \cap \mathbb{Q}_p^{(p^i)} = E_i$, d'où il résulte comme ci-dessus que les représentations irréductibles de G sur E sont les représentations $E[X]/P_{i,j}(X)$ et la représentation triviale.

Remarque 2. - Les entiers $r_i = [E_i : \Phi_p]$ sont donnés par : $r_i = \begin{cases} rp^{i-1} & , \text{ si } i \leq \alpha \\ rp^{\alpha-1} & , \text{ si } i \geq \alpha \end{cases}$, où α est le plus grand entier tel que $K^{(p)}$ contienne les racines p^α-èmes de 1 (ceci se déduit de l'évaluation $[\Phi_p^{(p^i)} : \Phi_p]$, en remarquant que $[\Phi_p^{(p^i)} : \Phi_p^{(p^\alpha)}] = [K^{(p^i)} : K^{(p)}]$, si $i \geq \alpha$).

1.2. - Décomposition d'un A[G]-module de rang 1 .

Soit M un A[G]-module de rang 1, c'est-à-dire un A[G]-module sans torsion sur A, tel que $K \otimes_A M$ soit un K[G]-module libre à 1 générateur.

On appelle ordre associé à M dans K[G] l'ordre $\mathcal{O}(M)$ de A dans K[G] défini par : $\mathcal{O}(M) = \{\lambda \in K[G] \ ; \ \lambda M \subset M\}$ (cf. [7]). On montre [4] :

> Soit S l'ensemble des idempotents primitifs de $\mathcal{O}(M)$; le A[G]-module M admet la décomposition : $M = \bigoplus_{e \in S} eM$; les modules eM sont indécomposables. Cette décomposition est l'unique décomposition de M en somme directe de sous A[G]-modules indécomposables.

Trouver la décomposition de M revient donc à trouver l'ensemble S des idempotents primitifs de $\mathcal{O}(M)$; on sait [4] que ces idempotents sont 2 à 2 orthogonaux et ont pour somme 1 .

D'autre part, pour tout caractère χ de G sur K, on note : $e_\chi = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1})g$. On montre que e_χ est un idempotent de K[G] et que $\{e_\chi ; \chi \in I_K\}$ est l'ensemble des idempotents primitifs de K[G] ; de plus, tout idempotent de K[G] s'écrit comme une somme finie d'idempotents e_χ (cf [4]). En particulier, pour tout i : $1 \leq i \leq n$, e_{χ_i} est la somme des e_χ, χ parcourant l'ensemble des composants irréductibles de χ_i .

1.3. - Action du groupe de Galois de l'extension $E/\mathbb{Q}_p$ sur l'algèbre $E[G]$.

Posons, pour tout $\varphi \in Gal(E/\mathbb{Q}_p)$ et tout $\lambda = \sum_{g\in G} a_g g \in K[G]$:

$$\varphi\Big(\sum_{g\in G} a_g g\Big) = \sum_{g\in G} \varphi(a_g) g \ .$$

On montre facilement qu'on définit ainsi une action de $Gal(E/\mathbb{Q}_p)$ sur $E[G]$; à tout φ de $Gal(E/\mathbb{Q}_p)$ est associé un $\mathbb{Q}_p$ - automorphisme d'algèbre de $E[G]$, qu'on note encore φ .

Comme les caractères irréductibles de G sur K sont à valeurs dans E , (§1.1), les idempotents e_χ (où $\chi \in I_K$) appartiennent à $E[G]$. On voit facilement que : $\varphi(e_\chi) = e_{\varphi(\chi)}$, et on en déduit :

PROPOSITION 1. - Le groupe $Gal(E/\mathbb{Q}_p)$ opère sur l'ensemble des idempotents e_χ , où χ décrit l'ensemble des caractères irréductibles de G sur K ; il y a $n+1$ trajectoires : $\{e_{\chi_0}\}$ et, pour $1 \le i \le n$, $\{e_\chi \ ; \ \chi$ composant irréductible de $\chi_i\}$.

Soit M un $A[G]$-module de rang 1 et soit $\mathcal{O}(M)$ son ordre associé. On considère $\mathcal{O}(M) \cap E[G]$, qui est un ordre de A dans $E[G]$. On supposera, dans le paragraphe suivant, que le module M vérifie la condition suivante :

Hypothèse d'invariance (H) : L'ordre $\mathcal{O}(M) \cap E[G]$ est globalement invariant par tout élément φ de $Gal(E/\mathbb{Q}_p)$.

1.4. - Modules M décomposables.

PROPOSITION 2. - Soit M un $A[G]$-module de rang 1 décomposable, et vérifiant l'hypothèse d'invariance (H) . Il existe un idempotent e de $\mathcal{O}(M)$ de la forme : $e = \sum_{0\le i\le n} \delta_i e_{\chi_i}$, avec $\delta_i = 0$ ou 1 .

Démonstration : Soit ε un idempotent primitif de $\mathcal{O}(M)$ et soit F le plus petit corps intermédiaire entre $\mathbb{Q}_p$ et E tel que ε appartienne à $F[G]$. Si $F = \mathbb{Q}_p$, on a nécessairement : $\varepsilon = e_{\chi_0}$. Supposons $F \neq \mathbb{Q}_p$. On a :

$$\varepsilon = \sum_{\theta \in I_F} \delta_\theta e_\theta \text{ , où } \delta_\theta \text{ vaut 0 ou 1 .}$$

Quel que soit $\varphi \in \mathrm{Gal}(F/\mathbb{Q}_p)$, φ non identité , $\varphi(\varepsilon)$ est différent de ε ; or $\varphi(\varepsilon)$ est un idempotent primitif de $\mathcal{O}(M)$; par suite : $\varepsilon\varphi(\varepsilon) = 0$. On en déduit : $\delta_\theta \delta_{\varphi^{-1}(\theta)} = 0$, pour tout $\varphi \in \mathrm{Gal}(F/\mathbb{Q}_p)$, φ non identité

Ceci signifie que les idempotents e_θ figurant dans la décomposition de e avec un coefficient 1 appartiennent à des trajectoires différentes, et de longueur maximum $[F:\mathbb{Q}_p]$. Pour un tel idempotent e_θ , la somme $\sum_{\varphi \in \mathrm{Gal}(F/\mathbb{Q}_p)} \varphi(e_\theta)$ est égale à la somme $\sum e_{\theta'}$, où θ' parcourt la trajectoire de θ sous l'action de $G(F/\mathbb{Q}_p)$; cette somme est donc égale à l'un des e_{χ_i} (cf. § 1.2). Par suite, l'idempotent $e = \sum_{\varphi \in G(F/\mathbb{Q}_p)} \varphi(\varepsilon)$ a la forme indiquée dans l'énoncé.

PROPOSITION 3. - Soit M un $A[G]$-module de rang 1 vérifiant l'hypothèse d'invariance (H) . On suppose que l'ordre $\mathcal{O}(M)$ contient un idempotent e_{χ_i} , pour un entier i compris entre 0 et n . Alors, il existe un corps $F_i : \mathbb{Q}_p \subset F_i \subset E_i$, tel que les ordres $\mathcal{O}(M)e_{\chi_i}$ et $F_i[G]\, e_{\chi_i}$ aient les mêmes idempotents.

Démonstration : Soit F_i le plus petit corps intermédiaire entre $\mathbb{Q}_p$ et E_i tel que $F_i[G]$ contienne tous les idempotents de $\mathcal{O}(M)e_{\chi_i}$. Il existe un idempotent primitif e de $\mathcal{O}(M)e_{\chi_i}$ tel que les éléments $\varphi(e)$, φ parcourant $G(F_i/\mathbb{Q}_p)$, soient tous distincts. Les éléments $\varphi(e)$ sont primitifs dans $\mathcal{O}(M)e_{\chi_i}$, 2 à 2 orthogonaux, et ils sont au nombre de $[F_i : \mathbb{Q}_p]$. D'autre part, le nombre d'idempotents primitifs e_θ de $F_i[G]\, e_{\chi_i}$ est égal au nombre de caractères θ de G sur F composants irréductibles de χ_i , soit, puisque $F_i \subset E_i \subset \mathbb{Q}_p^{(p^i)}$, à $[F_i:\mathbb{Q}_p]$

(cf. § 1.1). Les ordres $\mathcal{O}(M)e_{\chi_i}$ et $F_i[G]\,e_{\chi_i}$ ont donc le même ensemble d'idempotents primitifs.

COROLLAIRE. - Le corps F_i de la proposition 3 est le plus grand sous-corps de E_i tel que $\mathcal{O}(M)e_{\chi_i}$ contienne l'ordre maximal de l'algèbre $F_i[G]\,e_{\chi_i}$.

En effet, pour tout corps F contenu dans $\mathbb{Q}_p^{(p^n)}$, l'ordre maximal de l'algèbre $F[G]$ est le $A_F[G]$-module engendré par les idempotents e_θ, lorsque θ décrit l'ensemble I_F des caractères irréductibles de G sur F (A_F désignant l'anneau de valuation de F) ; la démonstration de ce résultat est analogue à celle de [4], § 3.4, lemme 2.

2. MODULES D'ENTIERS DECOMPOSABLES.

On désigne par L une extension galoisienne du corps local K de groupe de Galois G, et par B l'anneau de valuation de L. On sait ("théorème de la base normale") que B est un $A[G]$-module de rang 1. On suppose l'extension L/K totalement ramifiée.

2.1. - Modules d'entiers vérifiant l'hypothèse d'invariance (H).

Dans le cas $n = 1$, tout module d'entiers B vérifie (H) (cf. [2], [3], [4]). Si $n \geq 2$, on ignore si (H) est vérifiée pour une extension L/K quelconque.

PROPOSITION 4. - Si l'extension $L/\mathbb{Q}_p$ est abélienne, le module B vérifie l'hypothèse d'invariance (H).

Démonstration : Soit φ un $\mathbb{Q}_p$-automorphisme de E ; φ se prolonge en un $\mathbb{Q}_p$-automorphisme $\tilde{\varphi}$ de L, et on note encore $\tilde{\varphi}$ le $\mathbb{Q}_p$-automorphisme d'algèbre de $L[G]$ défini par : $\tilde{\varphi}\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} \tilde{\varphi}(a_g)g$, où $a_g \in L$. Soit λ un élément de $\mathcal{O}(B)$; $\lambda \in K[G]$, et pour tout x de

B , $\lambda x \in B$. On en déduit : $\tilde{\varphi}(\lambda x) \in B$; or $\tilde{\varphi}(\lambda x) = \tilde{\varphi}(\lambda)\tilde{\varphi}(x)$; comme $\tilde{\varphi}(x)$ décrit B quand x décrit B , il en résulte : $\tilde{\varphi}(\lambda) \in \mathcal{O}(B)$. $\mathcal{O}(B)$ est donc globalement invariant par tout Φ_p - automorphisme $\tilde{\varphi}$ de $K[G]$; par suite l'hypothèse (H) est vérifiée.

2.2. - Notations.

On notera :

L_h le corps des invariants du sous-groupe G^{p^h} ,

B_h l'anneau de valuation de L_h ,

π_h (resp. ϖ) une uniformisante de L_h (resp. K) ,

v_L (resp. v_K) la valuation normalisée de L (resp. K) ,

$e = v_K(p)$ l'indice absolu de ramification de K ,

σ un générateur de G .

On pose, pour tout entier h , $0 \leq h \leq n-1$:

$$e_h = \frac{1}{p^{n-h}} \sum_{g \in G^{p^h}} g \ ,$$

on voit facilement que e_h est un idempotent de $\Phi_p[G]$, lié à la trace de L/L_h par : $p^{n-h}e_h = \mathrm{Tr}\, L/L_h$. Les idempotents e_h sont liés aux idempotents e_{χ_h} dans $K[G]$ par les relations :

$$(1) \qquad \begin{cases} e_{\chi_0} = e_0 \\ e_{\chi_1} = e_1 - e_0 \\ \cdots\cdots\cdots \\ e_{\chi_h} = e_h - e_{h-1} \\ \cdots\cdots\cdots \\ e_{\chi_n} = 1 - e_{n-1} \ . \end{cases}$$

Ces relations se déduisent facilement des valeurs prises par les caractères χ_i , valeurs données par :

$$\chi_i(\sigma^h) = \begin{cases} 0 & , \text{ si } p^{i-1} \nmid h \ , \\ -p^{i-1} & , \text{ si } p^{i-1} \mid h \text{ et } p^i \nmid h \ , \\ p^i - p^{i-1} & , \text{ si } p^i \mid h \ . \end{cases}$$

On note $t_1, t_2, \ldots, t_n$ les nombres inférieurs de ramification de l'extension L/K . Pour tout entier h compris entre 1 et n , on a [8] :

$t_h \leq \frac{p^h e}{p-1}$, et : $t_h \equiv t_1 \mod p$.

On désignera par a , $0 \leq a \leq p-1$, le reste de la division de t_1 par p.

2.3. - Ramification presque maximale.

PROPOSITION 5. - Les conditions suivantes sont équivalentes :

(i) Pour $h = 1,2,\ldots,n$, $e_h \in \mathcal{O}(B)$

(ii) Pour $h = 1,2,\ldots,n$, $t_h \geq \frac{p^h e}{p-1} - 1$

(iii) Il existe h , $1 \leq h \leq n$: $t_h \geq \frac{p^h e}{p-1} - 1$

(iv) Il existe h , $1 \leq h \leq n$: $e_h \in \mathcal{O}(B)$.

Démonstration : La valuation de la différente de l'extension L/K_h est donnée par (cf. [8]) :

$$(2) \qquad v_L(\mathfrak{d}_{L/K_h}) = (p-1)(t_n + pt_{n-1} + \ldots + p^{n-h-1}t_{h+1}) + p^{n-h} - 1 .$$

Soit $\mu_h = [\frac{v_L(\mathfrak{d}_{L/K_h})}{p^{n-h}}]$; on sait ([8]) que μ_h est le plus grand entier tel que $\mathrm{Tr}_{L/K_h}(B) \subset \pi_h^{\mu_h} B$. Par suite, l'idempotent e_h appartient à $\mathcal{O}(B)$ si, et seulement si $\mu_h \geq (n-h)p^h e$.

La condition (i) est donc vérifiée si et seulement si, pour tout h compris entre 1 et n , on a :

$$(p-1)(t_n + pt_{n-1} + \ldots + p^{n-h-1}t_{h+1}) + p^{n-h} - 1 \geq (n-h)p^n e ;$$

cette inégalité s'écrit aussi :

$$(3) \qquad (t_n + 1 - \frac{p^n e}{p-1}) + p(t_{n-1} + 1 - \frac{p^{n-1} e}{p-1}) + \ldots + p^{n-h-1}(t_{h+1} + 1 - \frac{p^{h+1} e}{p-1}) \geq 0 .$$

Si, pour tout h , $t_k \geq \frac{p^h e}{p-1} - 1$, il est clair que l'inégalité (3) est vérifiée. Réciproquement, si (3) est vérifiée pour tout h , on montre, par récurrence, que $t_h \geq \frac{p^h e}{p-1} - 1$ pour tout h (remarquer que $t_h = \frac{pe - a - \lambda_h p}{p-1}$, où λ_h entier ≥ 0).

On a donc montré ainsi l'équivalence des conditions (i) et (ii).

L'équivalence des conditions (ii) et (iii) se démontre en utilisant les relations entre les nombres inférieurs de ramification données dans [5] .

Rappelons que les nombres supérieurs $u_1, u_2, \ldots, u_n$ de ramification d'une extension cyclique de degré p^n totalement ramifiée sont liés aux nombres inférieurs par :

$$u_1 = t_1, \ldots \; u_j = t_1 + \frac{t_2 - t_1}{p} + \ldots + \frac{t_j - t_{j-1}}{p^{j-1}}, \ldots .$$

Pour tout $j = 1, 2, \ldots, n-1$, on a :

a) si $u_j \geq \frac{e}{p-1}$, $u_{j+1} = u_j + e$,

b) si $u_j < \frac{e}{p-1}$, ou $u_{j+1} = pu_j$

ou $u_{j+1} = \frac{pe}{p-1}$

ou $pu_j < u_{j+1} < \frac{pe}{p-1}$, et $u_{j+1} \not\equiv 0 \bmod p$.

Supposons qu'il existe un entier $j : 1 \leq j \leq n$ tel que $t_j \geq \frac{p^j e}{p-1} - 1$.

Si $j < n$, considérons l'extension K_{j+1}/K_{j-1} ; cette extension, qui est cyclique de degré p^2 , admet comme nombres inférieurs de ramification t_j et t_{j+1} . On voit que la condition a) est vérifiée pour le 1er nombre inférieur, t_j , de cette extension ; on en déduit : $\frac{t_{j+1} - t_j}{p} + t_j = t_j + p^{j-1}e$, d'où : $t_{j+1} = t_j + p^j e \geq \frac{p^{j+1}e}{p-1} - 1$. On démontre aussi que, pour tout entier $h \geq j$, $t_h \geq \frac{p^h e}{p-1} - 1$.

Si $j > 1$, considérons l'extension K_j/K_{j-2} ; cette extension est cyclique de degré p^2 et a pour nombres inférieurs de ramification t_{j-1} et t_j . Si $t_{j-1} < \frac{e}{p-1}$, en utilisant la condition b) on trouve :

$$t_{j-1} + \frac{t_j - t_{j-1}}{p} \leq \frac{p^{j-1}e}{p-1} ,$$

d'où :

$$t_j \leq \frac{p^j e}{p-1} - (p-1)t_{j-1} < \frac{p^j e}{p-1} - 1 ,$$

ce qui est contraire à l'hypothèse. On a donc : $t_{j-1} \geq \frac{e}{p-1}$, et on en déduit (condition a)) : $t_j - t_{j-1} = p^{j-1}e$, d'où :

$$t_{j-1} = t_j - p^{j-1}e \geq \frac{p^j e}{p-1} - 1 - p^{j-1}e = \frac{p^{j-1}e}{p-1} - 1 .$$

On montre ainsi que pour tout entier $h < j$, $t_h \geq \frac{p^h e}{p-1} - 1$. Ceci achève la démonstration de l'équivalence des conditions (ii) et (iii).

Si la condition (iv) est vérifiée pour une valeur h , on a l'inégalité (3) pour la même valeur de h ; par suite, la condition (iii) est vraie pour un $h' > h$. D'autre part, il est clair que (i) implique (iv) . Ceci achève la démonstration de la proposition 5.

DEFINITION (cf.[6]). - Lorsque les conditions équivalentes de la proposition 5 sont vérifiées, on dit que la ramification de l'extension L/K est presque maximale.

Exemple : Si $e = 1$ (par exemple si $K = \mathbb{Q}_p$, cf.[1] , [6]), la ramification de L/K est nécessairement presque maximale, car $t_1 = a = 1$.

Remarque : Si la ramification de l'extension L/K est presque maximale, les nombres inférieurs de ramification de l'extension sont donnés par :

$$t_h = \frac{p^h e - a}{p-1} \quad , \quad 1 \leq h \leq n ,$$

et on a l'égalité : $e_h B = B_h$ (en effet μ_h vaut alors $(n-h)p^h e$) .

2.4. - Modules B décomposables.

THEOREME 1. - On suppose que B vérifie l'hypothèse d'invariance (H) . Le $A[G]$-module B est décomposable si et seulement si la ramification de l'extension L/K est presque maximale. Dans ce cas, pour tout entier i compris entre 0 et n , e_{χ_i} appartient à $\mathcal{O}(B)$; on a la décomposition : $B = \bigoplus_{0 \leq i \leq n} e_{\chi_i} B$.

Démonstration : Si la ramification est presque maximale, les idempotents e_h $(0 \leq h \leq n-1)$, et donc aussi (§ 2.2) les idempotents e_{χ_i} $(0 \leq i \leq n)$ appartiennent à $\mathcal{O}(B)$. D'où la décomposition : $B = \bigoplus_{0 \leq i \leq n} e_{\chi_i} B$.

Réciproquement, supposons le $A[G]$-module B décomposable, et la ramification de L/K non presque maximale.

LEMME. - Si la ramification de l'extension L/K n'est pas presque maximale, on a les inégalités :

$$v_L(e_{i+1}B) > v_L(e_iB) \text{ , pour } i = 0,1,2,\ldots,n-2 .$$

En effet, posant $\nu_i = v_L(e_iB)$, on a (§ 2.3) :

$$\nu_i = p^{n-i}(\mu_i-(n-i)ep^i) .$$

On en déduit

$$\nu_{i+1}-\nu_i = p^n e + p^{n-i-1}(\mu_{i+1}-p\mu_i) ;$$

d'où :

$$\nu_{i+1}-\nu_i > p^n e-(p-1)(t_{i+1}+1)p^{n-i-1}-p^{n-i-1} .$$

Comme la ramification n'est pas presque maximale, on a :

$$t_{i+1} \leq \frac{p^{i+1}e-a-p}{p-1} .$$

D'où : $\nu_{i+1}-\nu_i > ap^{n-i-1}$, ce qui entraîne le résultat du lemme.

Comme le $A[G]$-module B est décomposable , et vérifie l'hypothèse (H) , il existe un idempotent e de $\mathcal{O}(B)$ de la forme :

$$e = \sum_{0\leq i\leq n} \delta_i e_{\chi_i} \text{ , avec } \delta_i = 0 \text{ ou } 1 \text{ (proposition 2, § 1.4).}$$

En utilisant les relations (1) du §2.2, on trouve :

$$e = \sum_{0\leq i\leq n-1} (\delta_i-\delta_{i+1})e_i + \delta_n .$$

Il existe donc dans $\mathcal{O}(B)$ un élément λ de la forme :

$$\lambda = \sum_{0\leq i\leq n-1} \delta'_i e_i \text{ , avec } \delta'_i = 0,1 \text{ ou } -1 .$$

Soit i_0 le plus petit entier tel que $\delta'_{i_0} \neq 0$, et soit x un élément de B tel que $v_L(e_{i_0}x) = v_L(e_{i_0}B)$. On a : $v_L(e_{i_0}B) < v_L(e_iB)$, si $i>i_0$, d'après le lemme ; par suite, $v_L(e_{i_0}x) < v_L(e_ix)$, si $i>i_0$.

On en déduit : $v_L(e_{i_0}x) = v_L(\lambda x) \geq 0$, et donc : $v_L(e_{i_0}B) \geq 0$, c'est-à-dire : e_{i_0} appartient à $\mathcal{O}(B)$. Donc, d'après la proposition 5, la ramification de l'extension L/K serait presque maximale. Par suite, si le module B est décomposable et vérifie (H) , la ramification est presque-maximale.

L'étude de la décomposition de B en somme de $A[G]$-modules indécomposables nécessite la détermination de l'ordre associé $\mathcal{O}(B)$.

3. ORDRE ASSOCIE A B .

On suppose l'extension L/K totalement ramifiée, et de ramification presque maximale.

Pour déterminer l'ordre associé $\mathcal{O}(B)$, on sera amené (§ 3.3 et § 3.4) à supposer l'indice e de ramification de K premier à p .

3.1. - Les modules B'_h et leurs ordres associés $\mathcal{O}'_h$.

Pour tout entier h compris entre 0 et n , on note :

$$e_{\chi_h} B = B'_h \quad , \quad \mathcal{O}(B)\, e_{\chi_h} = \mathcal{O}'_h \ .$$

On montre facilement :

PROPOSITION 6. - Si la ramification de l'extension L/K est presque maximale, le $A[G]$-module B (resp. le $A[G]$-module $\mathcal{O}(B)$) se décompose en somme directe de sous-$A[G]$-modules :

$$B = \bigoplus_{0 \leq h \leq n} B'_h \quad \text{(resp. } \mathcal{O}(B) = \bigoplus_{0 \leq h \leq n} \mathcal{O}'_h \text{) ;}$$

B'_h est le sous-module des éléments de B_h de trace nulle sur L_{h-1} , et $\mathcal{O}'_h$ est l'ordre associé à B'_h dans $K[G]\, e_{\chi_h}$.

La proposition 6 ramène l'étude du $A[G]$-module B et de son ordre associé $\mathcal{O}(B)$ à celle des modules B'_h et de leurs ordres associés $\mathcal{O}'_h$.

On a : $B'_0 = A$ et $\mathcal{O}'_0 = A$; si $h \geq 1$, l'extension L_h/K ayant une ramification presque-maximale, l'étude de B'_h et $\mathcal{O}'_h$ se conduit, pour le degré p^h , comme celle de B'_n et $\mathcal{O}'_n$, pour le degré p^n .

3.2. - La base (b_i) de $K[G]$.

Pour tout entier i compris entre 0 et p^n-1 , on note i_1, i_2 ,...,i_n les entiers compris entre 0 et $p-1$ tels que :

$$i = i_1 + pi_2 + p^2 i_3 + \ldots + p^{n-1} i_n \ .$$

On pose (σ étant un générateur de G) :

$$b_i = (\sigma-1)^{i_1} (\sigma^p-1)^{i_2} \ldots (\sigma^{p^{n-1}}-1)^{i_n} \ .$$

La famille b_i , $0 \leq i \leq p^n-1$, est une K-base de $K[G]$, puisque b_i , comme polynôme en σ , est de degré i .

Considérons, pour tout h compris entre 1 et $n-1$, la famille $b_i e_{\chi_h}$, $p^{h-1} \leq i \leq p^h$; c'est une famille génératrice de $K[G]\,e_{\chi_h}$ dont le cardinal vaut $p^h-p^{h-1}-1$, c'est-à-dire la dimension sur K de $K[G]\,e_{\chi_h}$. Par suite, la famille $b_i e_{\chi_h}$, $p^{h-1} \leq i \leq p^h$, est une K-base de $K[G]\,e_{\chi_h}$.

Pour tout couple (i,j) d'entiers compris entre p^{n-1} et p^n-1, on note :

$$s(i,j) = i+j - \left[\frac{i+j-p^{n-1}}{(p-1)p^{n-1}}\right](p-1)p^{n-1} \ ,$$

où, pour un réel x , $[x]$ désigne le plus grand entier $\leq x$.

LEMME. - Les produits $b_i b_j$, $p^{n-1} \leq i$, $j < p^n$ appartiennent à l'anneau $\mathbb{Z}[G] \cap K[G]\,e_{\chi_n}$ et vérifient dans cet anneau les congruences :

$$b_i b_j \equiv \begin{cases} b_{i+j} \mod pb_{i+j-(p-1)p^{n-2}} , & \text{si } i+j < p^n \\ -pb_{s(i,j)} \mod pb_{s(i,j)+p^{n-1}} , & \text{si } p^n \le i+j < 2p^n-2p^{n-1} \\ -pb_{s(i,j)} \mod p^2 b_{s(i,j)+2p^{n-1}-p^n} , & \text{si } 2p^n-2p^{n-1} \le i+j < 2p^n-p^{n-1} \\ p^2 b_{s(i,j)} \mod p^2 b_{s(i,j)+p^{n-1}} , & \text{si } i+j \ge 2p^n-p^{n-1} . \end{cases}$$

Démonstration : Si $i \ge p^{n-1}$, $\sigma^{p^{n-1}}-1$ divise b_i ; comme $(\sigma^{p^{n-1}}-1)e_{n-1} = 0$, $(\sigma^{p^{n-1}}-1)e_{\chi_n} = \sigma^{p^{n-1}}-1$; par suite, b_i appartient à $K[G]\,e_{\chi_n}$.

Soient i et j deux entiers. On note :

$i_1+j_1 = r_1 + \varepsilon_1 p$, avec $\varepsilon_1 = 0$ ou 1 , $0 \le r_1 \le p-1$,

et, si $2 \le k \le n$:

$i_k+j_k+\varepsilon_{k-1} = r_k + \varepsilon_k p$, avec $\varepsilon_k = 0$ ou 1 , $0 \le r_k \le p-1$.

En utilisant les congruences : $b_{p^k}^p \equiv b_{p^{k+1}} \mod pb_{p^k}$, pour tout entier k compris entre 0 et $n-1$, et en remarquant que, si $i < j$, b_i divise b_j , on montre, par récurrence sur k , les congruences :

$$b_i b_j \equiv b_1^{r_1} b_p^{r_2} \ldots b_{p^{k-1}}^{r_k} b_{p^k}^{i_{k+1}+j_{k+1}+\varepsilon_k} b_{p^{k+1}}^{i_{k+2}+j_{k+2}} \ldots b_{p^{n-1}}^{i_n+j_n}$$

$$\mod pb_1^{r_1} b_p^{r_2} \ldots b_{p^{k-1}}^{r_k+1} b_{p^k}^{i_{k+1}+j_{k+1}} b_{p^{k+1}}^{i_{k+2}+j_{k+2}} \ldots b_{p^{n-1}}^{i_n+j_n} .$$

La congruence relative à l'indice $k = n-1$, s'écrit :

$$b_i b_j \equiv b_1^{r_1} \ldots b_{p^{n-2}}^{r_{n-1}} b_{p^{n-1}}^{i_n+j_n+\varepsilon_{n-1}} \mod pb_1^{r_1} \ldots b_{p^{n-2}}^{r_{n-1}+1} b_{p^{n-1}}^{i_n+j_n} .$$

Si $i+j < p^n$, on en déduit la congruence figurant dans l'énoncé du lemme.

Si $i+j > p^n$, utilisant la congruence : $b_{p^{n-1}}^p \equiv -pb_{p^{n-1}} \mod pb_{p^{n-1}}^2$, on trouve :

$$b_i b_j \equiv -pb_1^{r_1} \ldots b_{p^{n-2}}^{r_{n-1}} b_{p^{n-1}}^{r_n+1} \mod pb_1^{r_1} \ldots b_{p^{n-2}}^{r_{n-1}} b_{p^{n-1}}^{r_n+2} ;$$

le cas $r_n \le p-2$ équivaut à : $i+j < 2p^n - 2p^{n-1}$ et on a la congruence

énoncée dans le lemme. Si $r_n = p-2$ (resp. $r_n = p-1$), alors $2p^n - 2p^{n-1} \leq i+j < 2p^n - p^{n-1}$ (resp. $i+j \geq rp^n - p^{n-1}$) , et on obtient le résultat annoncé en remplaçant $b^p_{p^{n-1}}$ par $-pb_{p^{n-1}} \bmod pb^2_{p^{n-1}}$.

3.3. - L'ordre maximal de $K[G]$.

Soit $\mathcal{M}$ l'ordre maximal de A dans $K[G]$; l'ordre $\mathcal{M}$ se décompose en somme directe :

$$\mathcal{M} = \bigoplus_{0 \leq h \leq n} \mathcal{M} e_{\chi_h} ,$$

et $\mathcal{M} e_{\chi_h}$ est l'ordre maximal de A dans $K[G]\, e_{\chi_h}$.

PROPOSITION 7. - On suppose, si $n > 1$, l'indice e premier à p . Le A-module $\mathcal{M} e_{\chi_h}$ admet pour base :

$$b_i e_{\chi_h} / \varpi^{\left[\frac{ie}{(p-1)p^{h-1}}\right]} \quad , \quad p^{h-1} \leq i < p^h .$$

Démonstration : Notons $\mathcal{M}'_h$ le sous-A-module de $K[G]\, e_{\chi_h}$ engendré par les $b_i e_{\chi_h} / \varpi^{\left[\frac{ie}{(p-1)p^{h-1}}\right]}$, $p^{h-1} \leq i < p^h$.

Les algèbres $K[G]\, e_{\chi_h}$ et $K[X] / \Phi_{p^h}(X)$ sont K-isomorphes (cf. § 1.1). Comme e est premier à p , le polynôme $\Phi_{p^h}(X)$ se décompose en produit de r polynômes irréductibles (cf. § 1.1, remarque 2) ; on a $r = \frac{p-1}{m}$, avec $m = [K^{(p)} : K]$. Il existe un K-isomorphisme d'algèbres $f : K[G]\, e_{\chi_h} \to (K^{(p^h)})^r$; l'ordre $\mathcal{M} e_{\chi_h}$ est l'image par f^{-1} de $(A_{p^h})^r$, où A_{p^h} désigne l'anneau de valuation de $K^{(p^h)}$.

Les composantes dans les corps $K^{(p^h)}$ des $f(b_i e_{\chi_h})$ sont pour valuation $i e(K^{(p^h)} \mid \mathbb{Q}_p^{(p^h)})$ (où $e(F'|F)$ désigne l'indice de ramification d'une extension F'/F). On montre :

LEMME 1. - On note : $m = qd$ et $\frac{e}{r} = e'd$, où $d = \text{pgcd}(m, \frac{e}{r})$. Alors les indices de ramification des extensions $K^{(p)}/K$ et $K^{(p)}/\Phi_p^{(p)}$ sont donnés par :

$$e(K^{(p)}|K) = q \quad , \quad e(K^{(p)}|\Phi_p^{(p)}) = e' \ .$$

Par suite, $\varpi\,[\frac{ie}{(p-1)p^{h-1}}]$ a dans $K^{(p^h)}$ une valuation majorée par : $qp^{h-1}\frac{ie}{(p-1)p^{h-1}} = ie' = ie(K^{(p^h)}|\Phi_p^{(p^h)})$; on en déduit : $f(\mathcal{M}'_h) \subset (A_{p^h})^r$, et on a l'inclusion : $\mathcal{M}'_h \subset \mathcal{M} e_{\chi_h}$.

Pour un réseau M de $K[G]\,e_{\chi_h}$, on note $\Delta(M)$ le discriminant de M , par rapport à la forme bilinéaire associée à la trace de $K[G]\,e_{\chi_h}$. On a : $\Delta(\mathcal{M} e_{\chi_h}) = \delta^r$, où δ désigne le discriminant de l'extension $K^{(p^h)}/K$.

LEMME 2. - La valuation dans K du discriminant δ de l'extension $K^{(p^h)}/K$ est donnée par :

$$v_K(\delta) = d(p^{h-1}q - 1) + \frac{e}{r}\left((h-1)p^h - hp^{h-1} + 1\right) \ .$$

Le lemme 2 se démontre en remarquant que les nombres inférieurs de ramification de l'extension $K^{(p^h)}/K^{(p)}$ sont égaux à $(p^k-1)e'$, $1 \leq k \leq h-1$; on en déduit la valuation de la différente de l'extension $K^{(p^h)}/K$:

$$v_{K^{(p^h)}}(\mathcal{D}(K^{(p^h)}|K)) = p^{h-1}q - 1 + e'((h-1)p^h - hp^{h-1} + 1) \ .$$

La valuation du discriminant δ en résulte en prenant la norme.

D'autre part, on a :

$$\Delta(\mathcal{M}'_h) = \Delta(A[G] \cap K[G]\,e_{\chi_h})\,\varpi^{-2c} \ ,$$

avec $c = \sum_{p^{h-1} \leq i < p^h} [\frac{ie}{(p-1)p^{h-1}}]$. On montre :

$$\Delta(A[G] \cap K[G]\,e_{\chi_h}) = p^{hp^h - (h-1)p^{h-1}} A$$

$$c = \frac{e}{2}(p^h+p^{h-1}-1) - \frac{rd}{2}(p^{h-1}q - 1) \ .$$

On en déduit : $\Delta(\mathfrak{m}'_h) = \Delta(\mathfrak{m} e_{\chi_h})$, et par suite : $\mathfrak{m}'_h = \mathfrak{m} e_{\chi_h}$.

3.4. - Description des $A[G]$-modules B'_h (cas $a \neq 0$).

Pour tout entier i compris entre 0 et p^n-1 , on pose :

$$S(i) = i_1+i_2+\ldots+i_n \ , \quad \varepsilon(i) = 1 + [\frac{S(i)-1}{p-1}]$$

$$T(i) = i_1t_1+i_2t_2+\ldots+i_nt_n \ , \quad T'(i) = T(i)+a\varepsilon(i) \ .$$

On montre facilement les propriétés suivantes :

(1) $T'(i) \equiv a(S(i)+\varepsilon(i)) \bmod p$.

(2) Si x , $0 \leq x \leq p-2$, désigne le reste de la division de $S(i)$ par $p-1$, on a :

$$S(i)+\varepsilon(i) \equiv \begin{cases} 0 \bmod p \ , \text{ si } x = 0 \\ x+1 \bmod p \ , \text{ si } x \neq 0 \ . \end{cases}$$

(3) $$T'(i) = \frac{pie}{p-1} + \frac{(p-2)a}{p-1} - a\underbrace{\frac{S(i)-1}{p-1}}$$

en notant, pour tout réel x , $\underbrace{x} = x-[x]$.

PROPOSITION 8. - On suppose a non nul. Pour tout entier i compris entre 0 et p^n-1 , on a : $v_L(b_i\pi_n^a) = T'(i)$.

Démonstration : On remarque que

$$v_L(b_{p^h}x) = v_L(x) + t_{h+1} \quad \text{si} \quad v_L(x) \not\equiv 0 \bmod p$$

$$\geq v_L(x) + t_{h+1} \quad \text{si} \quad v_L(x) \equiv 0 \bmod p \ .$$

Il en résulte facilement :

$$v_L(b_i\pi_n^a) = T'(i) \ , \text{ si } S(i) \leq p-1 \ .$$

On fait l'hypothèse suivante, qu'on suppose vérifiée si $S(i) \leq h(p-1)$:

a) $v_L(b_i \pi_n^a) = T'(i)$;

b) si $S(i) \equiv 0 \bmod (p-1)$ il existe des unités u et v de A telles que : $b_i \pi_n^a \equiv \pi_{n-1}^{T'(i)/p}(u+v\pi_n^a) \bmod \pi_n^{T'(i)+a+1}$.

Soit i un entier tel que $S(i) = h(p-1)+1$, et soit k tel que $i_k \geq 1$; posons $j = i-p^{k-1}$. On a : $S(j) = h(p-1)$. En appliquant b) pour la valeur j , on trouve :

$$v_L(b_i \pi^a) = v_L(b_{p^{k-1}} b_j \pi^a) = T'(j)+a+t_k \ .$$

Utilisant alors la propriété (3), on montre :

$$T'(j)+a+t_k = T'(i) \ .$$

Par suite, un entier i tel que $S(i) = h(p-1)+1$ vérifie a) ; on en déduit alors facilement la propriété a) pour tous les entiers i tels que $S(i) \leq (h+1)(p-1)$.

Supposons alors $S(i) = (h+1)(p-1)$, et notons $i^* = \max(i_1,\ldots,i_n)$. Montrons d'abord la propriété b) lorsque $i^* = p-1$.

Soit k le plus grand entier tel que $i_k = p-1$.

Si $k < n$, on pose $j = i+p^{k-1}$; alors $S(j) = S(i)-(p-2) < (h+1)(p-1)$. On a : $b_i \pi_n^a = \pi_{n-1}^{T'(i)/p}(u_0+u_1\pi_n+\ldots+u_a\pi_n^a+\ldots)$, où les u_i appartiennent à un système de représentants dans A du corps résiduel de K . En remarquant que $v_L(b_{p^{k-1}} \pi_{n-1}^{T'(i)/p}) \geq T'(i) + pt_k$,

$$v_L(b_{p^{k-1}} \pi_n^{T'(i)+\ell} = T'(i)+\ell+t_k \quad (\text{si} \quad 1 \leq \ell \leq p-1) \ ,$$

et de plus que $T'(i)+a+t_k = T'(j)$, on trouve :

$u_1, u_2, \ldots, u_{a-1}$ sont nuls, et u_a est une unité de A .

On a donc démontré dans ce cas la propriété b) .

Si $k=n$, $b_{p^{n-1}} b_i \equiv pb_{i+2p^{n-1}-p^n} \bmod pb_{i+3p^{n-1}-p^n}$, d'après le lemme du §3.2. On pose $j = i+2p^{n-1}-p^n$; alors

$S(j) = S(i) - (p-2) < (h+1)(p-1)$. On démontre alors la propriété b) pour l'entier i par une démonstration analogue à la démonstration précédente, en utilisant l'égalité :

$$T'(i) + a + t_n = p^n e + T'(j) ,$$

égalité qui résulte de la propriété (3) .

Ceci achève la démonstration de la propriété b) lorsque $S(i) = (h+1)(p-1)$, et $i^* = \max(i_1,\dots,i_n) = p-1$. On termine la démonstration par récurrence sur i^* . Supposons que b) soit vérifiée pour $i^* = p-1 , p-2 ,\dots,\alpha+1$, et soit i tel que $i^* = \alpha$; il existe un indice k tel que $i_k = \alpha$, et un indice h tel que $i_h \geq 1$. Soit $j = i + p^{k-1} - p^{h-1}$; on a : $S(i) = S(j)$, et $j^* = \alpha+1$. L'indice j vérifie la propriété b) ; on montre qu'il en est de même pour i , en calculant la valuation de $b_{i+p^{h-1}} = b_{j+p^{k-1}}$ et en remarquant, grâce à la propriété (3) que : $T'(i)+a+t_k = T'(j)+a+t_h$.

Ceci achève la démonstration de la proposition 8.

THEOREME 1. - <u>On suppose</u> a <u>non nul et</u>, <u>si</u> $n>1$, e <u>premier à</u> p . <u>Le</u> A-<u>module</u> B'_h <u>admet pour base</u> : $b_i \pi_h^a / \varpi^{[T'(i)/p^h]}$, $p^{h-1} \leq i < p^h$.

<u>Démonstration</u> : Il suffit de faire la démonstration pour le cas $h = n$ (cf. § 3.1) . Pour i compris entre p^{n-1} et p^n-1 , on a : $b_i = b_i e_{\chi_n}$, et donc : $b_i \pi_n^a = b_i e_{\chi_n} \pi_n^a$. Par suite, les éléments $b_i \pi_n^a$, $p^{n-1} \leq i < p^n$, forment une K-base de $e_{\chi_n} L$ (cf. § 3.2). Notons $\beta_i = b_i \pi_n^a / \varpi^{[T'(i)/p^n]}$; d'après la proposition 8, pour tout i : $p^{n-1} \leq i < p^n$, β_i a une valuation positive et donc appartient à $B'_n = e_{\chi_n} B$. De plus, on a : $v_L(\beta_i) = T'(i) - p^n[T'(i)/p^n] < p^n$. On va montrer que les valuations $v_L(\beta_i)$ sont toutes distinctes.

LEMME. - On suppose, si $n>1$, e premier à p . Si les entiers i,j , compris entre p^{n-1} et p^n-1 , sont distincts, alors $T'(i) \not\equiv T'(j) \bmod p^n$.

En effet, d'après la propriété (3), la congruence $T'(i) \equiv T'(j) \bmod p^n$ équivaut à : $pie - a(p-1)\underbrace{\frac{S(i)-1}{p-1}} \equiv pje - a(p-1)\underbrace{\frac{S(j)-1}{p-1}} \bmod p^n$. Ceci entraîne $S(i) \equiv S(j) \bmod (p-1)$, d'où $i = j$, si $n = 1$. Si $n > 1$, on a de plus : $ie = je \bmod p^{n-1}$, et donc $i \equiv j \bmod p^{n-1}$. On en déduit $i = j$.

La famille β_i , $p^{n-1} \leq i < p^n$, est une K-base de $e\chi_n L$, et les β_i ont des valuations distinctes, comprises entre 0 et p^n-1 ; c'est donc une A-base de B'_n .

Remarque : Le lemme ci-dessus montre que, lorsque i varie de p^{n-1} à p^n-1 , $T'(i)$ prend modulo p^n toute valeur non congrue à a modulo p .

Dans toute la suite, on supposera, si $n > 1$, l'indice e premier à p .

3.5. - Description des ordres $\mathcal{O}'_h$.

DEFINITIONS. -

1. Pour tout réel x , $\mathcal{E}(x)$ désigne l'ensemble des entiers j positifs tels que, pour tout entier j' vérifiant : $1 \leq j' < j$, on ait : $\underbrace{j'x} > \underbrace{jx}$.

2. Soit un entier h compris entre 1 et n ; $\mathcal{E}_h(a/p)$ désigne l'ensemble des entiers i , $p^{h-1} \leq i < p^h$, satisfaisant l'une des conditions a) ou b) suivantes :

   a) $1 - \underbrace{\frac{T(i)}{p^h}} < \frac{a}{p^h}(\varepsilon(i)-1)$,

   b) $\frac{a}{p^h}(\varepsilon(i)-1) < 1 - \underbrace{\frac{T(i)}{p^h}} \leq \frac{a}{p^h}\varepsilon(i)$ et $(p-1)(1 - \underbrace{\frac{S(i)-1}{p-1}}) \in \mathcal{E}(a/p)$.

THEOREME 3. - L'ordre $\mathcal{O}'_h$ admet pour A-base la famille

$$b_i e_{\chi_h} / \varpi^{[T(i)/p^h] + \delta_h(i)} \quad , \quad p^{h-1} \leq i < p^h \ ,$$

où $\delta_h(i)$ vaut 1 ou 0 suivant que i appartient ou non à $\mathcal{E}_h(a/p)$.

Démonstration : Il suffit de démontrer ce résultat lorsque $h = n$.

Traitons d'abord le cas $a = 0$; dans ce cas $\mathcal{E}_h(a/p)$ est vide et $\frac{T(i)}{p^n} = \frac{ie}{(p-1)p^{n-1}}$. Il s'agit donc de montrer que $\mathcal{O}'_n$ coïncide avec l'ordre maximal $\mathfrak{M} e_{\chi_n}$ (proposition 7). Ceci résulte de l'inégalité suivante, valable pour tout x de B :

$$v_L(b_i x) \geq v_L(x) + i_1 t_1 + \ldots + i_n t_n \ ;$$

comme $a = 0$, $i_1 t_1 + \ldots + i_n t_n = \frac{i_1 pe}{p-1} + \ldots + \frac{i_n p^n e}{p-1} = \frac{pie}{p-1}$, d'où : $v_L((b_i/\varpi^{[T(i)/p^n]})x) \geq 0$, et donc $b_i/\varpi^{[T(i)/p^n]} \in \mathcal{O}'_n$. L'ordre $\mathcal{O}'_n$ contient donc l'ordre maximal $\mathfrak{M} e_{\chi_n}$ et par suite coïncide avec lui.

Supposons maintenant $a \neq 0$. Notons :

$$\nu(i) = \left[\frac{T'(i)}{p^n}\right] \quad , \quad \nu'(i+j) = \nu(s(i,j)) + e\left[\frac{i+j-p^{n-1}}{(p-1)p^{n-1}}\right] \ .$$

LEMME 1. - Soit un entier j compris entre p^{n-1} et $p^n - 1$. Le A-module B'_n admet pour base la famille $b_i b_j \pi_n^a / \varpi^{\nu'(i+j)}$, $p^{n-1} \leq i < p^n$.

En effet, on montre que les $s(i,j)$ prennent toutes les valeurs comprises entre p^{n-1} et $p^n - 1$, quand i varie de p^{n-1} à $p^n - 1$; les congruences du lemme du §3.2 montrent que $b_i b_j \pi_n^a / \varpi^{\nu'(i+j)}$ a même valuation que $b_{s(i,j)} \pi_n^a / \varpi^{\nu(s(i,j))}$. Le lemme 1 résulte alors de la démonstration du théorème 2.

LEMME 2. - On pose : $\gamma(i) = \mathrm{Min}\{\nu'(i+j) - \nu(j) \ ; \ p^{n-1} \leq i < p^n\}$.

L'ordre $\mathcal{O}'_n$ admet pour A-base la famille $b_i / \varpi^{\gamma(i)}$, $p^{n-1} \leq i < p^n$.

Ceci résulte immédiatement du théorème 3, et du lemme 1.

LEMME 3 (dû à J.P. Bertrandias). - Pour tout entier i, $p^{n-1} \leq i < p^n$, on a : $\gamma(i) = [\frac{T(i)}{p^n}] + \delta_n(i)$, où $\delta_n(i)$ vaut 1 ou 0 suivant que i appartient ou non à $\mathfrak{e}_n(a/p)$.

En évaluant la différence $\nu'(i+j) - \nu(j)$, on trouve :

$$\nu'(i+j) - \nu(j) = \frac{T(i)}{p^n} + \underbrace{\frac{T'(j)}{p^n}} + \frac{a}{p^n}(\varepsilon(i) - 1 + \delta'_{i,j}) - \underbrace{\frac{T'(i+j)}{p^n}}$$

où $\delta'_{i,j} = \begin{cases} 0 & , \text{ si } \underbrace{\frac{S(i)-1}{p-1}} + \underbrace{\frac{S(j)-1}{p-1}} \leq \frac{p-3}{p-1} \\ 1 & , \text{ dans le cas contraire.} \end{cases}$

D'après le lemme 2, on en déduit :

$$\gamma(i) = [\frac{T(i)}{p^n}] + \delta_n(i) ,$$

où $\delta_n(i) = \underset{p^{n-1} \leq j < p^n}{\text{Min}} \{ \underbrace{\frac{T(i)}{p^n}} + \underbrace{\frac{T'(j)}{p^n}} + \frac{a}{p^n}(\varepsilon(i)-1+\delta'_{i,j}) - \underbrace{\frac{T'(i+j)}{p^n}} \}$.

Si $\underbrace{\frac{T(i)}{p^n}} + \frac{a}{p^n}\varepsilon(i) < 1$, on peut choisir j pour que $\underbrace{\frac{T'(j)}{p^n}} = 0$ (prendre $j = (p-1)p^{n-1}$) ; par suite $\delta_n(i) = 0$.

Si $\underbrace{\frac{T(i)}{p^n}} + \frac{a}{p^n}(\varepsilon(i)-1) \geq 1$, il est clair que $\delta_n(i) \geq 1$; en choisissant $j = (p-1)p^{n-1}$, on voit que $\delta_n(i) = 1$.

Supposons $1 - \frac{a}{p^n}\varepsilon(i) \leq \underbrace{\frac{T(i)}{p^n}} < 1 - \frac{a}{p^n}(\varepsilon(i)-1)$.

L'entier $\delta_n(i)$ est égal à 0 si et seulement si il existe un entier j, $p^{n-1} \leq j < p^n$ tel que l'on ait les 2 inégalités :

(1) $$\underbrace{\frac{S(i)-1}{p-1}} + \underbrace{\frac{S(j)-1}{p-1}} \leq \frac{p-3}{p-1}$$

(2) $$\underbrace{\frac{T'(j)}{p^n}} < \underbrace{\frac{a - T'(i)}{p^n}}$$

(en effet d'après les hypothèses faites, $\underbrace{\frac{T'(i)}{p^n}} = \underbrace{\frac{T(i)}{p^n}} + \frac{a}{p^n}\varepsilon(i) - 1 < \frac{a}{p^n}$).

L'inégalité (1) s'écrit aussi :

$$(p-1)\frac{S(j)-1}{p-1}+2 \leq (p-1)(1-\frac{S(i)-1}{p-1}) ,$$

c'est-à-dire, en posant :

$$q_i = (p-1)(1-\frac{S(i)-1}{p-1}) \quad , \quad q'_j = (p-1)\frac{S(j)-1}{p-1}+2 ,$$

(1') $\qquad q'_j \leq q_i$.

L'inégalité (2) entraîne :

$$(S(j)+\varepsilon(j))\frac{a}{p} < (1-S(i)-\varepsilon(i))\frac{a}{p} ,$$

ce qui s'écrit aussi :

(2') $\qquad q'_j\frac{a}{p} < q_i\frac{a}{p}$.

Si $\delta_n(i) = 0$, les inégalités (1') et (2') sont vérifiées pour un certain entier j ; ceci entraîne : $q_i \notin \mathcal{E}(a/p)$.

Réciproquement, supposons : $q_i \notin \mathcal{E}(a/p)$. Soit un entier x compris entre 1 et a tel que $\frac{x}{p} = q'\frac{a}{p}$, avec $2 \leq q' < q_i$. D'après la remarque du § 3.4, il existe un entier j compris entre p^{n-1} et p^n-1 tel que : $\frac{T'(j)}{p^n} = \frac{x}{p^n}$; on a alors $(S(j)+\varepsilon(j))\frac{a}{p} = \frac{x}{p} = q'\frac{a}{p}$, et on en déduit : $q' = q_j$. Les inégalités (1) et (2) sont donc satisfaites pour cet entier j ; d'où $\delta_n(i) = 0$.

Ceci achève la démonstration du lemme 3, et du théorème 3 .

3.6. - L'hypothèse d'invariance (H) .

Le théorème 3 admet le corollaire suivant :

COROLLAIRE. - *Si l'extension* L/K *a une ramification presque maximale, le* $A[G]$*-module* B *vérifie l'hypothèse d'invariance* (H) .

En effet, tout élément λ de $\mathcal{O}(B)$ s'écrit :

$$\lambda = \sum_{\substack{0\leq h\leq n \\ p^{h-1}\leq i<p^h}} \lambda_{i,h} b_i e_{\chi_h} \quad , \text{ où } \lambda_{i,h} \in K ,$$

avec : $v_K(\lambda_{i,h}) \geq -[\frac{T'(i)}{p^h}] + \delta_h(i)$. Comme les éléments b_i et e_{χ_h} appartiennent à $\mathbb{Q}_p[G]$, il est clair que $\mathcal{O}(B) \cap E[G]$ est globalement invariant par tout $\mathbb{Q}_p$-automorphisme φ de $E[G]$.

3.7. - Etude des différences $[\frac{T'(i)}{p^h}] - ([\frac{T(i)}{p^h}] + \delta_h(i))$.

LEMME. - On suppose $a \neq 0$, soit un entier h compris entre 1 et n, et soit i un entier compris entre p^{h-1} et p^h-1 . La différence $[\frac{T'(i)}{p^h}] - ([\frac{T(i)}{p^h}] + \delta_h(i))$ vaut 0 ou 1 ; elle vaut 1 si et seulement si :

$$\frac{a}{p^h}(\varepsilon(i)-1) < 1 - \frac{T(i)}{p^h} < \frac{a}{p^h}\varepsilon(i) \text{ , et } (p-1)(1-\frac{S(i)-1}{p-1}) \notin \mathcal{E}(a/p) .$$

En effet, on trouve :

$$[\frac{T'(i)}{p^h}] - [\frac{T(i)}{p^h}] - \delta_h(i) = \frac{T(i)}{p^h} - \frac{T'(i)}{p^h} + \frac{a}{p^h}\varepsilon(i) - \delta_h(i)$$

$$= \begin{cases} 0 & \text{, si } 1 - \frac{T(i)}{p^h} > \frac{a}{p^h}\varepsilon(i) \\ 1 - \delta_h(i) & \text{, si } 1 - \frac{T(i)}{p^h} \leq \frac{a}{p^h}\varepsilon(i) \end{cases}$$

on en déduit le résultat annoncé.

PROPOSITION 9. - Si l'entier a est nul ou divise p-1 , B est un $\mathcal{O}$-module libre.

Démonstration : Si $a = 0$, $\mathcal{O}$ coïncide avec l'ordre maximal de $K[G]$, et donc B est libre sur $\mathcal{O}$ [7] . Si a divise p-1 , on montre qu'un entier q , $0<q<p$, tel que $q\frac{a}{p} < \frac{a}{p}$, appartient à $\mathcal{E}(a/p)$. Soit alors i tel que $\frac{a}{p^h}(\varepsilon(i)-1) < 1 - \frac{T(i)}{p^h} < \frac{a}{p^h}\varepsilon(i)$; on a : $\frac{-T(i)-a(\varepsilon(i)-1)}{p^h} < \frac{a}{p^h}$, d'où $p^{h-1}\frac{-T(i)-a(\varepsilon(i)-1)}{p^h} = ((p-1)\varepsilon(i)-S(i)+1)\frac{a}{p} < \frac{a}{p}$; or $(p-1)\varepsilon(i) - S(i) + 1 = (p-1)(1-\frac{S(i)-1}{p-1})$; le lemme ci-dessus entraîne donc : $\delta_h(i) = 0$, pour tout i .

On en déduit : $B'_h = \mathcal{O}'_h \pi_h^a$, pour $1 \leq h \leq n$ et donc : $B = \mathcal{O}\theta$, en posant $\theta = e_{\chi_n} \pi_n^a + e_{\chi_{n-1}} \pi_{n-1}^a + \ldots + e_{\chi_h} \pi_h^a + \ldots + e_{\chi_0} 1$.

4. DECOMPOSITION D'UN A[G] -MODULE D'ENTIERS B DANS LE CAS DE RAMIFICATION PRESQUE MAXIMALE.

4.1. - Comme dans le § 3 , L/K désigne une extension cyclique totalement ramifiée de corps locaux, le groupe de Galois G de l'extension étant d'ordre p^n . On suppose que la ramification de l'extension est presque maximale (cf. § 2.3), et que l'indice absolu de ramification de K , e, est premier à p ($si\ n > 1$).

Rappelons (§ 3.1) que le A[G] -module B se décompose en somme directe : $B = \bigoplus_{0 \leq h \leq n} B'_h$, avec $B'_h = e_{\chi_h} B$. Trouver la décomposition de B en somme directe de sous-A[G] -modules indécomposables revient à trouver la décomposition des A[G] -modules B'_h . Ce problème est équivalent à la recherche des idempotents primitifs de $\mathcal{O}'_h$.

4.2. - Enoncé du résultat.

Rappelons que, pour tout corps K , on note I_K l'ensemble des caractères irréductibles de G sur K .

On montre :

THEOREME 4. - On note $I = \begin{cases} I_K & , \text{ si } a = 0 \text{ ou } a \text{ divise } p-1 \\ I_{\mathbb{Q}_p} & , \text{ dans le cas contraire.} \end{cases}$

1) L'ensemble des idempotents primitifs de $\mathcal{O}(B)$ est $\{e_\chi ; \chi \in I\}$;

2) La décomposition de B en somme directe de sous-A[G] -modules indécomposables s'écrit :

$B = \bigoplus_{\chi \in I} e_\chi B$.

4.3. - Démonstration du théorème 4.

On sait que l'ordre $\mathcal{O}(B)$ vérifie l'hypothèse d'invariance (H) (§ 3.6). On peut donc utiliser les résultats du § 1.4.

Comme l'indice e est supposé premier à p, tous les corps $E_i = K \cap \mathbb{Q}_p^{(p^i)}$ coïncident avec $E = K \cap \mathbb{Q}_p^{(p)}$ (remarque 2 du § 1.1).

Pour tout corps F contenu dans $\mathbb{Q}_p^{(p)}$, on note :

$$m_F = [\mathbb{Q}_p^{(p)} : F] \quad , \quad r_F = [F : \mathbb{Q}_p] \ .$$

On désigne par F_h le corps compris entre $\mathbb{Q}_p$ et E tel que $F_h[G]$ et $\mathcal{O}'_h = \mathcal{O}(B)\, e_{\chi_h}$ aient même idempotents (proposition 3 du § 1.4).

LEMME 1. - *F_h est le plus grand sous-corps de E tel que, pour tout i compris entre p^{h-1} et $p^h - 1$, on ait :*

$$e(K|F_h)\,\underbrace{\frac{i}{m_{F_h}\, p^{h-1}}} - \frac{a\, S(i)}{p^h(p-1)} - \underbrace{\frac{T(i)}{p^h}} + \delta_h(i) \geq 0 \ .$$

En effet, d'après le corollaire § 1.4, F_h est le plus grand sous-corps de E tel que $\mathcal{O}'_h \cap F_h[G]$ contienne $\mathfrak{m}_{F_h} e_{\chi_h}$, ordre maximal de $F_h[G]\, e_{\chi_h}$. On a (cf. § 3.3 et § 3.5)

$$\mathcal{O}'_h \cap F_h[G] = \sum_{i=p^{h-1}}^{p^h-1} a_i b_i e_{\chi_h} \ ; \ a_i \in F_h \text{ et } v_{F_h}(a_i) \geq -\frac{1}{e(K|F_h)}\left(\left[\frac{T(i)}{p^h}\right] + \delta_h(i)\right)$$

$$\mathfrak{m}_{F_h} e_{\chi_h} = \sum_{i=p^{h-1}}^{p^h-1} a_i b_i e_{\chi_h} \ ; \ a_i \in F_h \text{ et } v_{F_h}(a_i) \geq -\left[\frac{ir_F}{p^{h-1}(p-1)}\right] \ .$$

Par suite, F_h est le plus grand sous-corps de E tel que :

$$\left[\frac{T(i)}{p^h}\right] + \delta_h(i) \leq e(K|F_h)\left[\frac{ir_F}{p^{h-1}(p-1)}\right] \ ,$$

inégalité équivalente à celle qui figure dans le lemme 1 ; on remarque que le premier membre de cette inégalité est un entier.

LEMME 2. - *Si a est nul ou divise $p-1$, on a : $F_h = E$.*

Si $a = 0$, l'inégalité du lemme 1 est satisfaite quel que soit le corps F_h . D'où $E = F_h$.

Si a divise $p-1$, on sait (§ 3.7) que $[\frac{T(i)}{p^h}] + \delta_j(i) = [\frac{T'(i)}{p^h}]$; l'inégalité du lemme 1 s'écrit alors :

$$e(K|F_h)\underbrace{\frac{i}{m_{F_h} p^{h-1}}} + \frac{a}{p^h}(\frac{p-2}{p-1} - \underbrace{\frac{S(i)-1}{p-1}}) \geq 0 ,$$

inégalité satisfaite pour tout i , quel que soit le corps F_h . On a donc : $F_h = E$.

LEMME 3. - (On suppose $a \neq 0$). Une condition nécessaire pour que l'inégalité du lemme 1 soit satisfaite pour tout i est que les entiers $p - km_F$, $1 \leq k \leq r_F$, appartiennent à $\mathcal{E}(a/p)$.

En effet, si i est un multiple de $m_F p^{h-1}$, c'est-à-dire si $i_1 = \ldots = i_{n-1} = 0$ et $i_n = km_F$, on doit avoir $\delta_h(i) = 1$, et donc $(p-1)(1 - \underbrace{\frac{S(i)-1}{p-1}}) = p - km_F$ doit appartenir à $\mathcal{E}(a/p)$. Or on sait (cf. [4]) :

LEMME 4. - Soit d un diviseur de $p-1$. Les entiers $p - jd$, $1 \leq j \leq \frac{p-1}{d}$, appartiennent à $\mathcal{E}(a/p)$ si et seulement si a divise $p-1$ et $\frac{p-1}{a}$ divise d .

Les lemmes 3 et 4 montrent donc que, si $a \neq 0$ et a ne divise pas $p-1$, on a : $F_h = \Phi_p$, ce qui achève la démonstration du théorème 4.

BIBLIOGRAPHIE

[1] A.M. BERGE - Sur l'arithmétique d'une extension cyclique totalement ramifiée d'un corps local, C.R.Acad. Sc. Paris, 281, (1975), 67-70.

[2] 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, 274 (1972), 1330-1333.

[3] F. BERTRANDIAS, J.P. BERTRANDIAS et M.J. FERTON - Même titre, C.R. Acad. Sc. Paris, 274 (1972), 1388-1391.

[4] F. BERTRANDIAS - Décomposition du Galois-module des entiers d'une extension cyclique de degré premier d'un corps local ou d'un corps de nombres. Séminaire de Théorie des Nombres, Grenoble, 1977.

[5] J.M. FONTAINE - Groupes de ramification et représentation d'Artin. Ann. Scient. Ec. Norm. Sup., t.4 (1971), fasc.3, 337-392.

[6] H. JACOBINSKI - Uber die Hauptordnung eines Körpers als Gruppen modul. J. reine angew. Math., 213 (1964), 151-164.

[7] I. REINER - Maximal orders, Academic Press, London, 1975.

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

Laboratoire de Mathématiques Pures - Institut Fourier
dépendant de l'Université Scientifique et Médicale de Grenoble
associé au C.N.R.S.
B.P. 116
38402 ST MARTIN D'HERES (France)