SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

FRANÇOISE 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 de Grenoble, tome 5 (1975-1977), exp. n° 8, p. 1-23

<http://www.numdam.org/item?id=STNG_1975-1977__5__A8_0>

Séminaire de Théorie des Nombres
17 mars 1977
Grenoble

DECOMPOSITION DU GALOIS-MODULE DES ENTIERS D'UNE EXTENSION CYCLIQUE DE DEGRE PREMIER D'UN CORPS LOCAL OU D'UN CORPS DE NOMBRES.

par

Françoise BERTRANDIAS

Soit A un anneau de Dedekind, de corps des quotients K, et soit L une extension galoisienne finie de K, de groupe de Galois G. La clôture intégrale B de A dans L est un $A[G]$-module de rang 1 ; B est somme directe d'un nombre fini de sous-$A[G]$-modules indécomposables et, lorsque G est abélien, cette décomposition est unique ; elle a été déterminée, dans le cas où le corps K est le corps $\mathbb{Q}$ des rationnels, par H.W. Léopoldt [6].

On se propose ici de trouver la décomposition de B lorsque G est un groupe cyclique de degré premier, et K un corps local ou un corps de nombres.

Dans le paragraphe 1, on suppose G abélien et on étudie la décomposition d'un $A[G]$-module M de rang 1, en utilisant les idempotents de son commutant.

Dans le paragraphe 2, on se restreint au cas où G est cyclique de degré premier p, et où K est un corps local ou un corps de nombres.

Dans le paragraphe 3, on traite le cas où le module M est l'anneau B des entiers d'une extension cyclique L de degré p d'un corps local K. On verra en particulier que B est décomposable si et seulement si le nombre de ramifications t de l'extension L/K est "presque maximal" au

sens de Jabobinski [5] ; ce résultat avait été trouvé, indépendamment, par M.J. Ferton (1975, non publié) et par Y. Miyata [8].

Dans le paragraphe 4, on traite le cas où le module M est l'anneau B des entiers d'une extension cyclique de degré p d'un corps de nombres K.

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

1.1. Décompositions et idempotents.

On désignera par :

A un anneau commutatif intègre, de corps des quotients K,

G un groupe fini,

M un $A[G]$-module, de type fini et sans torsion sur A,

$C = \mathrm{End}_{A[G]}M$ le commutant de M.

On sait qu'il existe des décompositions de M en somme directe de sous-$A[G]$-modules indécomposables (utiliser par exemple le fait que l'application canonique de M dans $K \otimes_A M$ est injective).

Rappelons les relations qui lient les décompositions de M et les systèmes d'idempotents de C.

PROPOSITION 1. - *Soit* $M = \bigoplus_{1\le i\le k} M_i$ *une décomposition de* M *en somme directe de sous-*$A[G]$*-modules. On note* $e_i : M \to M_i$ *la projection canonique. Alors* $\{e_i \mid 1\le i\le k\}$ *est un système d'idempotents de* C *deux à deux orthogonaux et tel que :* $1_C = \sum_{1\le i\le k} e_i$ *(on désigne un tel système par : "système complet orthogonal d'idempotents"). Réciproquement, à tout système complet orthogonal* $\{e_i \mid 1\le i\le k\}$ *d'idempotents de* C *correspond la décomposition en somme directe :* $M = \bigoplus_{1\le i\le k} M_i$, *avec :* $M_i = e_iM$.

DEFINITION 1. - Un idempotent non nul e de C est dit primitif si l'égalité : $e = e' + e''$, où e' et e'' sont deux idempotents orthogonaux de C , entraîne : $e' = 0$ ou $e'' = 0$.

PROPOSITION 2. - Soit $M = \bigoplus_{1 \le i \le k} M_i$ une décomposition de M en somme directe de sous-A[G]-modules. Le module M_i est indécomposable si, et seulement si l'idempotent correspondant e_i est primitif.

On voit donc que trouver une décomposition de M en somme directe de sous-A[G]-modules M_i indécomposables revient à trouver un système complet orthogonal d'idempotents primitifs de C , qu'on notera fréquemment pour abréger : système d'idempotents c.o.p.

1.2. Cas d'un A[G]-module de rang 1 , G étant abélien.

Rappelons les définitions suivantes ([7]) :

On dit qu'un A[G]-module M est de rang 1 si M est de type fini et sans torsion sur A , et si le K[G]-module $K \otimes_A M$ est libre avec un générateur.

On appelle ordre associé à un A[G]-module M de rang 1 le sous-anneau $\mathcal{O}(M)$ de K[G] défini par :

$$\mathcal{O}(M) = \{\lambda \in K[G] \mid \lambda M \subset M\} .$$

Lorsque le groupe G est abélien, on a le résultat :

PROPOSITION 3. - Soit G un groupe abélien et soit M un A[G]-module de rang 1 . Le commutant C de M est canoniquement isomorphe à l'ordre associé à M .

Démonstration : pour tout λ élément de $\mathcal{O}(M)$, l'application $\varphi_\lambda : x \mapsto \lambda x$ de M dans lui-même est évidemment un A[G]-endomorphisme de M . D'autre part, on voit facilement que l'application qui, à tout λ de $\mathcal{O}(M)$, associe l'élément φ_λ de C est un homomorphisme injectif

d'anneaux. Il reste à montrer que cet homomorphisme est surjectif.

Soit donc φ un $A[G]$-endomorphisme de M. Désignons par θ un élément de M qui engendre $K \otimes_A M$ comme $K[G]$-module. On a :

$$\varphi(\theta) = \lambda\theta \text{ , avec } \lambda \in K[G] .$$

Pour tout x de M, on a : $x = \mu\theta$, avec $\mu \in K[G]$; il existe $d \in A$ tel que $d\mu \in A[G]$. Par suite :

$$\varphi(dx) = d\mu\varphi(\theta) = d\mu\lambda\theta = d\lambda\mu\theta = d\lambda x .$$

On en déduit : $\varphi(x) = \lambda x$, et donc : $\varphi = \varphi_\lambda$, ce qui achève la démonstration.

On peut alors énoncer :

PROPOSITION 4. - (unicité de la décomposition).
Soit G un groupe abélien et soit M un $A[G]$-module de rang 1.

1) Il existe un unique système S complet orthogonal d'idempotents primitifs dans l'ordre $\mathcal{O}(M)$; S est l'ensemble des idempotents primitifs de $\mathcal{O}(M)$.

2) La décomposition : $M = \bigoplus_{e \in S} eM$ est l'unique décomposition de M en somme directe de sous-$A[G]$-modules indécomposables.

Démonstration : on sait que M se décompose en somme directe de sous-$A[G]$-modules indécomposables. Par suite (§ 1.1) il existe au moins un système d'idempotents c.o.p. dans C, et donc aussi dans $\mathcal{O}(M)$ qui lui est isomorphe. L'unicité d'un tel système est assurée par le lemme suivant (dont la démonstration est analogue à celle du lemme 5.7 de [10], ch. III) :

LEMME. - Soit R un anneau commutatif possédant un système S d'idempotents c.o.p. Alors tout autre système d'idempotents c.o.p. de R coïncide avec S.

L'unicité de la décomposition de M en résulte, d'après l'étude du § 1.1.

Soit e' un idempotent primitif de $\mathcal{O}(M)$. Notons $S = \{e_1,\ldots,e_k\}$. On a : $e' = e'e_1 + e'e_2 +\ldots+ e'e_k$. Pour tout i , $1 \leq i \leq k$, $e'e_i$ est un idempotent ; si $i \neq j$, $e'e_i$ et $e'e_j$ sont orthogonaux. Il existe donc un indice i tel que $e' = e'e_i$ et $e'e_j = 0$ $(i \neq j)$. Ecrivant alors $e_i = e' + (e_i - e')$, on vérifie que e' et $e_i - e'$ sont orthogonaux, et il en résulte : $e' = e_i$. Ceci achève la démonstration de la proposition 4.

1.3. Idempotents de $K[G]$ et idempotents de $\mathcal{O}(M)$.

L'ordre $\mathcal{O}(M)$ étant un sous-anneau de $K[G]$, ses idempotents vont s'exprimer à l'aide des idempotents de $K[G]$.

Rappelons comment s'obtiennent les idempotents primitifs de $K[G]$, (cf. [3]).

Soit G un groupe abélien et soit K un corps de caractéristique 0 . Pour tout caractère irréductible χ de G sur K , on pose :

$$e_\chi = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1})g \ .$$

Notant I l'ensemble des caractères irréductibles de G sur K , on a les résultats suivants :

(1) pour tout $\chi \in I$, e_χ est un idempotent primitif de $K[G]$ et $K[G]e_\chi$ est un corps,

(2) $K[G] = \bigoplus_{\chi \in I} K[G]e_\chi$,

(3) $\{e_\chi \mid \chi \in I\}$ est l'ensemble des idempotents primitifs de $K[G]$.

On en déduit :

PROPOSITION 5. - Tout idempotent e de $K[G]$ s'écrit : $e = \sum_{\chi \in J} e_\chi$, où J est un ensemble de caractères irréductibles de G sur K .

En effet, on a : $e = \sum_{\chi \in I} ee_\chi$; l'égalité $e^2 = e$ entraîne : $(ee_\chi)^2 = ee_\chi$, pour tout $\chi \in I$. Comme ee_χ est un élément du corps

$K[G]e_\chi$, dont l'élément unité est e_χ , ceci équivaut à : $ee_\chi = 0$ ou $ee_\chi = e_\chi$.

Remarque : si le groupe G est d'exposant n , les valeurs prises par un caractère χ appartiennent au corps $\mathbb{Q}^{(n)}$ engendré par les racines $n^{\text{èmes}}$ de 1 sur le coprs $\mathbb{Q}$ des rationnels. Par suite, les idempotents e_χ , et donc aussi tous les idempotents de $K[G]$, appartiennent à $\mathbb{Q}^{(n)}[G]$.

Revenons à l'étude des idempotents de l'ordre $\mathcal{O}(M)$ et supposons dorénavant le corps K de caractéristique 0 .

La proposition 5 entraîne immédiatement :

PROPOSITION 6. - Soit $\{e_i \mid 1 \le i \le k\}$ l'ensemble des idempotents primitifs de $\mathcal{O}$. Il existe une partition de l'ensemble I des caractères irréductibles de G sur K : $I = \bigcup_{1 \le i \le k} J_i$, telle que, pour tout i : $1 \le i \le k$, on ait :

$$e_i = \sum_{\chi \in J_i} e_\chi \ .$$

2. CAS OU G CYCLIQUE D'ORDRE PREMIER ET K CORPS LOCAL OU CORPS DE NOMBRES.

Dans toute la suite (§ 2,3,4) G sera supposé cyclique d'ordre premier p . Dans ce paragraphe 2, K désigne, soit un corps local (de caractéristique 0 et de caractéristique résiduelle p), soit un corps de nombres.

On désignera par k soit le corps $\mathbb{Q}_p$ des rationnels p-adiques (si K corps local), soit le corps $\mathbb{Q}$ des rationnels (si K corps de nombres).

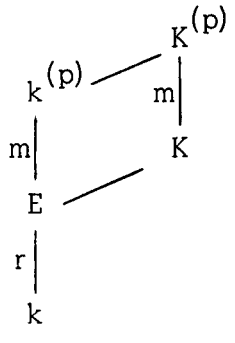
2.1. Les caractères irréductibles de G sur K .

Notons, dans une clôture algébrique du corps k :

$k^{(p)}$ (resp. $K^{(p)}$) le corps engendré sur k (resp. K) par les racines p-èmes de 1 ,

$E = k^{(p)} \cap K$.

Soit $X^p - 1 = (X-1)P_1(X)\dots P_r(X)$ la décomposition du polynôme $X^p - 1$ en produit de polynômes irréductibles de $K[X]$. Les polynômes $P_i(X)$ $(1 \leq i \leq r)$ ont tous le même degré m et on a : $m = [K^{(p)} : K] = \frac{p-1}{r}$.



L'extension $k^{(p)} | E$ étant galoisienne, on a :

$[k^{(p)} : E] = [K^{(p)} : K] = m$.

Par suite, les polynômes $P_i(X)$ $(1 \leq i \leq r)$ appartiennent à $E[X]$.

On a les isomorphismes :

$$K[G] \simeq K[X]/X^p-1 \simeq K[X]/X-1 \times K[X]/P_1(X) \times \dots \times K[X]/P_r(X) .$$

Le groupe G possède donc $r+1$ représentations irréductibles sur K : une représentation de degré 1 et r représentations de degré m . Comme les polynômes $P_i(X)$ appartiennent à $E[X]$, les $r+1$ représentations irréductibles de G sur K proviennent, par extension des scalaires, des représentations irréductibles de G sur E . Pour tout caractère irréductible χ de G sur K , l'idempotent e_χ appartient donc à $E[G]$ (cf. remarque du § 1.3).

Notations :

On notera : χ_o le caractère de la représentation de degré 1 ,

χ_i $(1 \leq i \leq r)$ le caractère de la représentation $K[X]/P_i(X)$,

$T = \sum_{g \in G} g$

$e_{\chi_o} = \frac{T}{p}$.

2.2. Action du groupe de Galois de l'extension $E|k$.

L'extension $E|k$ est cyclique de degré r et $Gal(E|k)$ opère sur l'ensemble des représentations irréductibles de G sur E , ainsi que sur leurs caractères χ_i $(0\leq i\leq r)$. On voit facilement que χ_o est invariant et que les caractères χ_i $(1\leq i\leq r)$ sont permutés transitivement.

On montre facilement :

PROPOSITION 7. - Pour tout φ appartenant à $Gal(E|k)$, et tout $\lambda = \sum_{g\in G} a_g g$ appartenant à $E[G]$, on pose :

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

On définit ainsi une opération du groupe $Gal(E|k)$ sur $E[G]$; à tout élément de $Gal(E|k)$ est associé ainsi un automorphisme de k-algèbre de $E[G]$.

Remarque : $Gal(E|k)$ laisse invariant l'idempotent e_{χ_o} et permute transitivement les idempotents e_{χ_i} $(1\leq i\leq r)$.

2.3. Hypothèse d'invariance.

Revenons à l'étude des idempotents de l'ordre $\mathcal{O}(M)$ associé dans $K[G]$ au $A[G]$-module M de rang 1 .

On va faire l'hypothèse suivante :

Hypothèse d'invariance (H) .

On considère $\mathcal{O}(M) \cap E[G]$ qui est un ordre de A dans $E[G]$, et on suppose que cet ordre est globalement invariant par tout élément de $Gal(E|k)$.

On obtient alors :

THEOREME 1. - Soit M un $A[G]$-module de rang 1 décomposable, dont l'ordre associé $\mathcal{O}(M)$ vérifie l'hypothèse d'invariance (H) .

Soit F le plus petit corps intermédiaire entre k et E tel que $F[G]$ contienne tous les idempotents de $\mathcal{O}(M)$. Alors $F[G]$ et $\mathcal{O}(M)$ ont les mêmes idempotents.

Démonstration : soit S l'ensemble des idempotents primitifs de $\mathcal{O}(M)$ ($S \neq \{1\}$ par hypothèse). On sait que S est contenu dans $E[G]$. Soit F le plus petit sous-corps de E (contenant k) tel que S soit contenu dans $F[G]$.

Notons $r_F = [F:k]$ et τ un générateur du groupe cyclique $\mathrm{Gal}(F|k)$. D'après le choix du corps F, il existe un idempotent e de S tel que les éléments $\tau^i(e)$, $0 \leq i < r$, soient tous distincts. Ces éléments $\tau^i(e)$ sont des idempotents ; ils appartiennent à $\mathcal{O}(M)$ (hypothèse (H)) et sont nécessairement primitifs dans $\mathcal{O}(M)$. Or, deux idempotents primitifs distincts de $\mathcal{O}(M)$ sont orthogonaux, car ils appartiennent tous les deux à l'unique système S d'idempotents c.o.p. L'ensemble

$$\{\tau^i(e) \mid 0 \leq i \leq r_F - 1\} \cup \{1 - \sum_{0 \leq i \leq r_F - 1} \tau^i(e)\}$$

est alors un système complet orthogonal d'idempotents de $\mathcal{O}(M)$. Or, on constate qu'il a le même nombre d'éléments, $r_F + 1$, que le système S' d'idempotents c.o.p. de $F[G]$: il ne peut donc que coïncider avec celui-ci et donc aussi avec S.

2.4. Modules décomposables.

Le théorème 1 entraîne immédiatement :

PROPOSITION 8. - Soit M un $A[G]$-module dont l'ordre associé $\mathcal{O}(M)$ vérifie l'hypothèse d'invariance (H). Si M est décomposable, l'idempotent $\frac{T}{p}$ appartient à $\mathcal{O}(M)$, et on a la décomposition :

$$M = \frac{T}{p}M \oplus (1 - \frac{T}{p})M \quad .$$

Remarque : l'idempotent $\frac{T}{p}$ est primitif dans $K[G]$, donc dans $\mathcal{O}(M)$ et par suite le module $\frac{T}{p}M$ est indécomposable.

3. DECOMPOSITION DE L'ANNEAU DES ENTIERS D'UNE EXTENSION CYCLIQUE DE DEGRE PREMIER D'UN CORPS LOCAL.

Dans ce paragraphe, on suppose que K est un corps local de caractéristique 0 et de caractéristique résiduelle p et que A est l'anneau des entiers de K. Soit L une extension cyclique de degré p de K. On se propose d'appliquer les résultats des paragraphes 1 et 2 au module $M = B$, $A[G]$-module des entiers de L $(G = Gal(L/K))$.

3.1. L'ordre associé à B.

Il dépend du nombre de ramification t de l'extension L/K. Si l'extension L/K est non ramifiée, on a [9] :

$$\mathcal{O}(B) = A[G] .$$

Si l'extension L/K est ramifiée, $\mathcal{O}(B)$ a été déterminé précédemment ([1], [2], [4]). Pour énoncer le résultat, introduisons les notations et définitions suivantes :

(1) Pour tout réel x :

$[x]$ est le plus grand entier $\leq x$

$\underset{\vee}{x} = x - [x]$

$\mathcal{E}(x) = \{h \text{ entier} \geq 1 \mid 1 \leq h' < h \quad h' \text{ entier entraîne : } h'\underset{\vee}{x} > h\underset{\vee}{x}\}$.

(2) Si K est un corps local :

v_K désigne la valuation normalisée de K.

(3) σ désigne un générateur du groupe cyclique G.

PROPOSITION 9. - L'ordre $\mathcal{O}(B)$ associé à B est défini par :

$$\mathcal{O}(B) = \{ \sum_{0\le i\le p-1} a_i(\sigma-1)^i \mid a_i \in K \text{ et } v_K(a_i) \ge -n_i \} \quad \text{avec} \quad n_i = [\frac{it}{p}] + \delta_i$$

où $\delta_i = \begin{cases} 1 & \text{si } p-i \in \mathcal{E}(\frac{t}{p}) \\ 0 & \text{sinon} \end{cases}$.

On peut alors énoncer :

PROPOSITION 10. - L'ordre $\mathcal{O}(B)$ vérifie l'hypothèse d'invariance (H).

Démonstration : si L/K est non ramifiée, $\mathcal{O}(B) = A[G]$, d'où : $\mathcal{O}(B) \cap E[G] = E[G]$; donc $\mathcal{O}(B) \cap E[G]$ est globalement invariant par tout élément de $Gal(E/\mathbb{Q}_p)$.

Si L/K est ramifiée, on a :

$$\mathcal{O} \cap E[G] = \{ \sum_{0\le i\le p-1} a_i(\sigma-1)^i \mid a_i \in E \text{ et } v_E(a_i) \ge -\frac{n_i}{e(K|E)} \}$$

en notant $e(K|E)$ l'indice de ramification de l'extension $K|E$. Comme un $\mathbb{Q}_p$ automorphisme de E transforme un élément de E en un élément de même valuation, $Gal(E|\mathbb{Q}_p)$ laisse globalement invariant l'ordre $\mathcal{O} \cap E[G]$.

3.2. Modules B décomposables.

THEOREME 2. - (M.J. Ferton (non publié) Y. Miyata [7]).
Le A[G]-module B est décomposable si et seulement si l'une des conditions équivalentes suivantes est vérifiée :

(1) l'idempotent $\frac{T}{p}$ appartient à $\mathcal{O}(B)$

(2) le nombre de ramification t de l'extension L/K vérifie :

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

DEFINITION. - Le nombre de ramifications t de l'extension L/K est dit "presque maximal" (cf. [5]) si l'une ou l'autre des conditions équivalentes (1) ou (2) est vérifiée.

Démonstration du théorème : l'ordre $\mathcal{O}(B)$ vérifie l'hypothèse d'invariance (H) . Donc (proposition 8, § 2.4) B est décomposable si et seulement si $\frac{T}{p} \in \mathcal{O}(B)$. L'équivalence des conditions (1) et (2) résulte facilement de la description de l'ordre $\mathcal{O}(B)$ (cf. [4]).

3.3. Décomposition de B . Enoncé des résultats.

Dans le paragraphe précédent, on a utilisé uniquement le fait que l'ordre $\mathcal{O}(B)$ vérifie l'hypothèse d'invariance pour caractériser les modules B décomposables. On va maintenant donner la décomposition de B en somme directe de sous-modules indécomposables.

Notations.

a désigne le reste de la division de t par p

I désigne l'ensemble des caractères irréductibles de G sur K .

THEOREME 3. - Soit L|K une extension cyclique de degré p de corps locaux, dont le nombre de ramification est presque maximal.

1) L'ensemble des idempotents primitifs de $\mathcal{O}(B)$ est égal à :

$\{e_\chi \mid \chi \in I\}$ si a est nul ou divise p-1

$\{\frac{T}{p}, 1-\frac{T}{p}\}$ dans le cas contraire.

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

$B = \bigoplus_{\chi \in I} e_\chi B$ si a est nul ou divise p-1

$B = \frac{T}{p}B \oplus (1-\frac{T}{p})B$ dans le cas contraire.

Remarque : un A[G]-module N , de type fini sans torsion sur A , est A-irréductible si $K \otimes_A N$ est un K[G]-module simple ([3]).

Pour tout $\chi \in I$, $e_\chi B$ est A-irréductible ; en particulier $\frac{T}{p}B$ est A-irréductible. Par contre $(1-\frac{T}{p})B$ est A-irréductible si, et seulement si, le corps K et $\mathbb{Q}_p^{(p)}$ sont linéairement disjoints sur $\mathbb{Q}_p$ $(r=1)$.

Le théorème 3 montre donc que B est décomposable en somme directe de sous-$A[G]$-modules A-irréductibles si et seulement si :

1) t est presque maximal

2) $a = 0$, ou a divise $p-1$, ou $r = 1$.

3.4. Démonstration du théorème 3.

On considère une extension $L|K$ de degré p , dont le nombre de ramifications t est presque maximal. B est décomposable et on sait (théorème 1) que l'ensemble des idempotents primitifs de $\mathcal{O}(B)$ coïncide avec celui de l'algèbre $F[G]$, où F est le plus petit corps intermédiaire entre k et E tel que $F[G]$ contienne tous les idempotents de $\mathcal{O}(M)$. Il reste à déterminer le corps F . La démonstration comprend plusieurs étapes.

LEMME 1. - F est le plus grand sous-corps F de E tel que :
(1) $\{e_\chi \mid \chi$ caractère irréductible de G sur $F\} \subset \mathcal{O}(B)$.

Démonstration : il est clair que (1) est vérifié par F et par tout sous-corps de F . Par ailleurs, si $F \subsetneq E' \subset E$, E' ne peut vérifier (1) car alors un idempotent e_χ , où χ caractère irréductible de G sur E' , ne serait pas primitif dans $\mathcal{O}(B)$, puisqu'il serait somme non triviale d'idempotents de $F[G]$.

Notations.

A_F est l'anneau des entiers du corps local F

$\mathfrak{m}_F$ est l'ordre maximal de l'algèbre $F[G]$

e_F est l'indice de ramification absolu de F

$e(K|F) = \dfrac{e_K}{e_F}$

m_F désigne le degré $[\mathbb{Q}_p^{(p)} : F]$, si F est contenu dans $\mathbb{Q}_p^{(p)}$.

LEMME 2. - Soit F un corps local contenu dans $\mathbb{Q}_p^{(p)}$. L'ordre maximal $\mathfrak{m}_F$ est l'anneau engendré par $A_F[G]$ et par les idempotents e_χ, où χ parcourt l'ensemble des caractères irréductibles de G sur F.

Démonstration : on a la décomposition en somme directe :

$$F[G] = \bigoplus_\chi F[G]e_\chi .$$

Pour tout χ, $F[G]e_\chi$ est isomorphe à $\mathbb{Q}_p^{(p)}$ et, dans un tel isomorphisme, σe_χ a pour image ζ, racine primitive p-ème de 1. Comme l'anneau des entiers de $\mathbb{Q}_p^{(p)}$ est l'anneau $A_F[\zeta]$, on a :

$$\mathfrak{m}_F = \bigoplus_\chi A_F[G]e_\chi .$$

LEMME 3. - Soit F un corps local. L'ordre maximal $\mathfrak{m}_F$ est vérifié :

$$\mathfrak{m}_F = \left\{ \sum_{0\le i\le p-1} a_i(\sigma-1)^i \mid a_i \in F \text{ et } v_F(a_i) \ge -\left[\frac{ie_F}{p-1}\right] \right\} .$$

La démonstration de ce résultat se trouve dans [4].

LEMME 4. - E' est le plus grand sous-corps F de E tel que, pour tout i : $0 \le i \le p-1$, on ait :

$$(2) \qquad e(K|F)\underbrace{\frac{i}{\mathfrak{m}_F}} - \underbrace{\frac{ia}{p}} - \frac{ia}{p(p-1)} + \delta_i \ge 0$$

où δ_i vaut 1 ou 0 suivant que $p-i$ appartient à $\mathcal{E}(\frac{t}{p})$ ou non.

Démonstration : E' est le plus grand sous-corps F de E tel que $\mathfrak{m}_F \subset \mathcal{O}(B) \cap F[G]$ (lemmes 1 et 2). D'après la proposition 9, on a :

$$\mathcal{O}(B) \cap F[G] = \left\{ \sum_{0\le i\le p-1} a_i(\sigma-1)^i \mid a_i \in F \text{ et } v_F(a_i) \ge -\frac{n_i}{e_{K|F}} \right\} .$$

Par suite (lemme 3) E' est le plus grand sous-corps F de E tel que :

$$\frac{n_i}{e(K|F)} \ge \left[\frac{ie_F}{p-1}\right] \qquad (0\le i\le p-1) .$$

Posons $t = a + \lambda p$ $(0\le a\le p-1)$. Comme t est presque maximal, on a (4) : $e_K = a + \lambda(p-1)$.

On montre facilement (remarquer que $p-1 = e_F m_F$) :

$$n_i - e(K|F)\left[\frac{ie_F}{p-1}\right] = e(K|F)\underbrace{\frac{i}{m_F}} - \frac{ia}{p} - \frac{ia}{p(p-1)} + \delta_i \ .$$

D'où le lemme 4.

LEMME 5. - *Si* $a = 0$, *on a* : $F = E$. *Si* $a \neq 0$, F *est le plus grand sous-corps de* E *tel que l'ensemble* $\{p - jm_F \mid 1 \leq j \leq e_F\}$ *soit contenu dans* $\mathcal{E}(\frac{t}{p})$.

Démonstration : Si $a = 0$, (2) est vérifiée pour tout sous-corps F de E . Supposons $a \neq 0$. Soit F un sous-corps quelconque de E , et soit i un entier non multiple de m_F . On a les inégalités :

$$e(K|F)\underbrace{\frac{i}{m_F}} \geq e_{K|F}\frac{1}{m_F} = \frac{e_K}{p-1}$$

$$\frac{e_K}{p-1} = \frac{a}{p-1} + \lambda \geq \frac{a}{p-1} \ .$$

D'où :

$$e(K|F)\underbrace{\frac{i}{m_F}} - \frac{ia}{p(p-1)} \geq \frac{a}{p-1} - \frac{ia}{p(p-1)} > 0 \ .$$

Par suite (2) est vérifiée.

Si i est multiple de m_F , (2) est vérifiée si, et seulement si, $\delta_i = 1$ (remarquer que le 1er membre de (2), étant entier, est ≥ 0 si, et seulement si, il est > -1).

Le lemme en résulte.

LEMME 6. - *Soit* d *un diviseur de* $p-1$, $d < p-1$. *Les entiers* $p - jd$, $1 \leq j \leq \frac{p-1}{d}$, *appartiennent à* $\mathcal{E}(\frac{t}{p})$ *si, et seulement si,* a *divise* $p-1$, $a \neq 1$, *et* $\frac{p-1}{a}$ *divise* d .

Démonstration : On utilise le développement en fraction continue de $\frac{t}{p}$, en notant $q_o = 1$, $q_1, \ldots, q_i = a_i q_{i-1} + q_{i-2}, \ldots, q_n = p$ les dénominateurs des réduites de $\frac{t}{p}$ (on suppose $a_n > 1$). On montre ([4]) :

$$\mathcal{E}(\frac{t}{p}) = \{p\} \cup \{q_{2i} + xq_{2i+1} \mid 0 \leq i < \frac{n-1}{2} \text{ et } 0 \leq x \leq a_{2i+2}\} .$$

Supposons que $p-d$ et $p-2d$ appartiennent à $\mathcal{E}(\frac{t}{p})$; il existe des entiers i,j,x,y tels que :

$$p - d = q_{2i} + xq_{2i+1}$$

$$p - 2d = q_{2j} + yq_{2j+1}$$

$$0 \leq i,j < \frac{n-1}{2} , \quad 0 \leq x \leq a_{2i+2} , \quad 0 \leq y \leq a_{2j+2} .$$

On en déduit :

$$p = 2(q_{2i} + xq_{2i+1}) - (q_{2j} + yq_{2j+1}) .$$

D'où :

$$p < 2q_{2i+2} .$$

Comme $p = a_n q_{n-1} + q_{n-2} > 2q_{n-1}$, on a : $2i + 2 > n - 1$, et donc : $2i = n - 2$.

Par suite : $p = a_{2i+2}q_{2i+1} + q_{2i}$.

On en déduit : $d = (a_{2i+2} - x)q_{2i+1}$.

Ceci entraîne : q_{2i+1} divise d et donc divise $p - 1$.

Mais $p - 1 = a_{2i+2}q_{2i+1} + q_{2i} - 1$.

D'où q_{2i+1} divise $q_{2i} - 1$ et donc $q_{2i} = 1$.

Par suite $i = 0$ et $n = 2$. On en déduit : a divise $p-1$, $a \neq 1$. Posons $a = \frac{p-1}{q}$; on a $q_1 = q$ et $a_2 = a$.

D'où :

$$\mathcal{E}(\frac{t}{p}) = \{1 + xq \mid 0 \leq x \leq a\} = \{p - jq \mid 0 \leq j \leq a\} .$$

On en déduit le résultat annoncé.

On peut alors terminer la démonstration du théorème 3.

Le corps F cherché est caractérisé par le lemme 5.

Si $a = 0$, on a vu que $F = E$. Supposons donc $a \neq 0$. Puisque F est un sous-corps de E, m_F est un multiple de m. D'autre part, si a divise $p-1$, m_F est un multiple de $\frac{p-1}{a}$; en effet, on a $m_F = \frac{p-1}{a}\frac{a}{e_F}$, et e_F, divisant e_K et $p-1$, divise $a = e_K - \lambda(p-1)$.

Si $a = 1$, on a : $m_F = p-1$ et $e_F = 1$ pour tout sous-corps F de E. Par suite $F = \mathbb{Q}_p = E$; les caractères irréductibles de G sont les mêmes sur $\mathbb{Q}_p$ ou sur K. Le système d'idempotents c.o.p. de $\mathcal{O}(B)$ peut donc s'écrire sous la forme $\{e_\chi | \chi \in I\}$ indiquée dans le théorème 3.

Si a divise $p-1$, $a \neq 1$, pour tout sous-corps F de E $\{p-jm_F | 1 \leq j \leq e_F\}$ est contenu dans $\mathcal{E}(\frac{t}{p})$, puisque m_F est multiple de $\frac{p-1}{a}$ (lemme 6). Donc $F = E$, et on a le résultat énoncé dans le théorème 3.

Si a ne divise pas $p-1$, le lemme 6 montre que nécessairement $m_F = p-1$, $e_F = 1$. Il en résulte $F = \mathbb{Q}_p$, ce qui achève la démonstration de la première partie du théorème. La deuxième partie en résulte immédiatement, compte-tenu des résultats du paragraphe 1.

4. DECOMPOSITION DE L'ANNEAU DES ENTIERS D'UNE EXTENSION CYCLIQUE DE DEGRE PREMIER p D'UN CORPS DE NOMBRES.

Dans ce paragraphe, A est l'anneau des entiers d'un corps de nombres K. On se propose d'utiliser les résultats des paragraphes 1 et 2 pour trouver la décomposition du $A[G]$-module B, anneau des entiers d'une extension L, cyclique de degré p, du corps K. On utilisera également les résultats obtenus dans le paragraphe 3 pour le cas local.

4.1. Notations.

Pour tout idéal premier $\mathfrak{P}$ de B, on note :

- $L_{\mathfrak{P}}$ un complété de L pour la valuation $\mathfrak{p}$-adique
- $B_{\mathfrak{p}}$ l'anneau des entiers de $L_{\mathfrak{p}}$
- $\mathfrak{p} = \mathfrak{P} \cap A$
- $K_{\mathfrak{p}}$ le complété de K dans $L_{\mathfrak{p}}$ pour la valuation $\mathfrak{p}$-adique
- $A_{\mathfrak{p}}$ l'anneau des entiers de $K_{\mathfrak{p}}$
- $v_{\mathfrak{P}}$ (resp. $v_{\mathfrak{p}}$) la valuation $\mathfrak{P}$-adique (resp. $\mathfrak{p}$-adique) normalisée de $L_{\mathfrak{P}}$ (resp. $K_{\mathfrak{p}}$)
- σ un générateur du groupe $G = \mathrm{Gal}(L|K)$.

Si $\mathfrak{p}$ est un idéal premier de K, la factorisation de $\mathfrak{p}B$ en idéaux premiers de B est de l'une des 3 formes suivantes :

a) $\mathfrak{p}B = \mathfrak{P}^p$ ($\mathfrak{p}$ ramifié)

b) $\mathfrak{p}B = \mathfrak{P}$ ($\mathfrak{p}$ inerte)

c) $\mathfrak{p}B = \mathfrak{P}\sigma\mathfrak{P}\ldots\sigma^{p-1}\mathfrak{P}$ ($\mathfrak{p}$ décomposé).

Si $\mathfrak{p}$ est ramifié et si de plus $\mathfrak{p}$ est au-dessus de p, on dira que $\mathfrak{p}$ est sauvagement ramifié.

Si $\mathfrak{p}$ n'est pas décomposé, l'extension $L_{\mathfrak{P}}|K_{\mathfrak{p}}$ est cyclique de degré p ; on identifie son groupe de Galois à G.

Dans la suite interviendront les ordres : $\mathcal{O}(B)$, ordre associé à B dans $K[G]$ et, si $\mathfrak{P} \cap A$ n'est pas complètement décomposé, $\mathcal{O}(B_{\mathfrak{P}})$ ordre associé à $B_{\mathfrak{P}}$ dans $K_{\mathfrak{P}}[G]$.

Si $\mathfrak{p}$ n'est pas décomposé, $t_{\mathfrak{p}}$ désignera le nombre de ramification de l'extension $L_{\mathfrak{P}}|K_{\mathfrak{p}}$.

4.2. L'ordre $\mathcal{O}(B)$.

PROPOSITION 11. -

$$\mathcal{O}(B) = \left\{ \sum_{0\le i\le p-1} a_i(\sigma-1)^i \,\middle|\, a_i \in K \text{ et } v_p(a_i) \ge -n_{p,i} \text{ , pour tout idéal premier } p \text{ de } A \text{ et tout entier } i : 0\le i\le p-1 \right\} ,$$

les entiers $n_{p,i}$ étant donnés par :

- si p non sauvagement ramifié, $n_{p,i} = 0$
- si p sauvagement ramifié, $n_{p,i} = [\frac{it_p}{p}] + \delta_i$, avec

$$\delta_i = \begin{cases} 1 & \text{si } p-i \in \mathcal{E}(\frac{t_p}{p}) \\ 0 & \text{sinon.} \end{cases}$$

Démonstration : Soit $\lambda \in K[G]$; λ appartient à $\mathcal{O}(B)$ si et seulement si, pour tout $x \in B$ et pour tout $\mathfrak{P}$ idéal premier de B , on a :

$$v_{\mathfrak{P}}(\lambda x) \ge 0 .$$

1) Si $\mathfrak{P} \cap A$ n'est pas décomposé dans L , la condition : "pour tout $x \in B$, $v_{\mathfrak{P}}(\lambda x) \ge 0$ " équivaut, puisque B est dense dans $B_{\mathfrak{P}}$, à : "pour tout $x \in B_{\mathfrak{P}}$, $v_{\mathfrak{P}}(\lambda x) \ge 0$ ", c'est-à-dire : "$\lambda \in \mathcal{O}(B_{\mathfrak{P}})$ ". Ecrivant alors un λ de $K[G]$ sous la forme, $\lambda = \sum_{0\le i\le p-1} a_i(\sigma-1)^i$, l'étude du cas local (proposition 9) montre que $\lambda \in \mathcal{O}(B_{\mathfrak{P}})$ si, et seulement si $v_p(a_i) \ge -n_{p,i}$ $(0\le i\le p-1)$.

2) Si $p = \mathfrak{P} \cap A$ est décomposé dans L , notons $\lambda = \sum_{0\le i\le p-1} b_i\sigma^i$ un élément de $K[G]$. Il est clair que les inégalités : $v_p(b_i) \ge 0$ $(0\le i\le p-1)$ entraînent : $v_{\mathfrak{P}}(\lambda x) \ge 0$, pour tout $x \in B$.

Réciproquement, supposons $v_{\mathfrak{P}}(\lambda x) \ge 0$, pour tout $x \in B$. Soit i_o un entier fixé, compris entre 0 et $p-1$ et soit, pour tout $i \ne i_o$, $0\le i\le p-1$, $\nu_i = \max(0, -v_p(b_i))$.

D'après le théorème des restes chinois, il existe un élément x_o de B vérifiant les congruences :

$$x_o \equiv 0 \mod(\sigma^{-i}\mathfrak{P})^{\nu_i} \quad \text{si} \quad i \neq i_o \ , \quad 0 \leq i \leq p-1$$

$$x_o \equiv 1 \mod \sigma^{-i_o}\mathfrak{P} \ .$$

On en déduit $v_{\mathfrak{P}}(b_{i_o}\sigma^{i_o}x_o) \geq \mathrm{Min}\left(v_{\mathfrak{P}}(\lambda x_o), v_{\mathfrak{P}}\left(\sum_{\substack{i\neq i_o \\ 0\leq i\leq p-1}} b_i\sigma^i x_o\right)\right) \geq 0$.

D'où,

$$v_{\mathfrak{p}}(b_{i_o}) \geq 0 \ .$$

Donc, si $\lambda = \sum_{0\leq i\leq p-1} b_i\sigma^i$ vérifie : $v_{\mathfrak{P}}(\lambda x) \geq 0$, pour tout x de B , on a : $v_{\mathfrak{P}}(b_i) \geq 0$, pour tout i : $0 \leq i \leq p-1$.

Comme la matrice de passage de la base $(\sigma^i)_{0\leq i\leq p-1}$ du K-espace vectoriel $K[G]$ à la base $((\sigma-1)^i)_{0\leq i\leq p-1}$ a pour déterminant 1 , on en déduit :

Une condition nécessaire et suffisante pour que $\lambda = \sum_{0\leq i\leq \sigma-1} a_i(\sigma-1)^i$ élément de $K[G]$ vérifie $v_{\mathfrak{P}}(\lambda x) \geq 0$ pour tout x de B est :

$$v_{\mathfrak{p}}(a_i) \geq 0 \qquad (0\leq i\leq p-1) \ .$$

Ceci achève la démonstration de la proposition 11.

PROPOSITION 12. - <u>L'ordre</u> $\mathcal{O}(B)$ <u>vérifie l'hypothèse d'invariance</u> (H) .

<u>Démonstration</u> : $\mathcal{O}(B) \cap E[G]$ est l'ensemble des éléments $\sum_{0\leq i\leq p-1} a_i(\sigma-1)^i$ de $E[G]$, où la valuation des a_i est ≥ 0 en tout idéal premier de E , sauf, éventuellement, pour l'unique idéal premier $\mathfrak{p}'$ au-dessus de p et pour lequel :

$$v_{\mathfrak{p}'}(a_i) \geq -\min_{\mathfrak{p}} \frac{n_{\mathfrak{p},i}}{e(K_{\mathfrak{p}}|E_{\mathfrak{p}'})} \ ,$$

$\mathfrak{p}$ décrivant l'ensemble des idéaux premiers de K au-dessus de p .

Soit alors φ un Φ_p-automorphisme de E ; a_i et $\varphi(a_i)$ ont même valuation $\mathfrak{p}'$-adique, car $\mathfrak{p}'$ est invariant par φ ; a_i et $\varphi(a_i)$ sont simultanément entiers pour tous les idéaux premiers $\mathfrak{q} \neq \mathfrak{p}'$, car φ permute ces idéaux.

Par suite $\mathcal{O} \cap E[G]$ est globalement invariant par φ .

4.3. Modules B décomposables.

THEOREME 4. - Le A[G]-module B est décomposable si et seulement si l'une des conditions équivalentes suivantes est vérifiée :

(1) l'idempotent $\frac{T}{p}$ appartient à $\mathcal{O}(B)$

(2) tout idéal premier $\mathfrak{p}$ de A au-dessus de p est ramifié dans L et le nombre de ramification correspondant $t_{\mathfrak{p}}$ est presque maximal, c'est-à-dire :

$$\frac{p}{p-1} e_{K_{\mathfrak{p}}} - 1 \leq t_{\mathfrak{p}} \leq \frac{p}{p-1} e_{K_{\mathfrak{p}}} .$$

Démonstration : Le fait que la condition (1) est nécessaire et suffisante pour que B soit décomposable résulte de la proposition 8 du paragraphe 2, et du fait que $\mathcal{O}(B)$ vérifie l'hypothèse d'invariance (H).

L'équivalence des conditions (1) et (2) résulte de la description de l'ordre $\mathcal{O}(B)$ (§ 4.2) et de l'étude locale (§ 3.2, théorème 2).

4.4. Décomposition de B .

Notations.

I désigne l'ensemble des caractères irréductibles de G sur K

$a_{\mathfrak{p}}$ désigne le reste de la division de $t_{\mathfrak{p}}$ par p .

THEOREME 5. - Soit L/K une extension cyclique de degré p de corps de nombres telle que tout idéal premier $\mathfrak{p}$ de K au-dessus de p soit ramifié et que le nombre de ramification correspondant $t_{\mathfrak{p}}$ soit presque maximal.

1) L'ensemble des idempotents primitifs de $\mathcal{O}(B)$ est donné par :

$\{e_\chi \mid \chi \in I\}$ si, pour tout $\mathfrak{p}$, $a_{\mathfrak{p}}$ est nul ou divise p-1

$\{\frac{T}{p}, 1-\frac{T}{p}\}$ dans le cas contraire.

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

$B = \bigoplus_{\chi \in I} e_\chi B$ si, pour tout $\mathfrak{p}$ au-dessus de p, $a_\mathfrak{p}$ est nul ou divise $p-1$

$B = \frac{T}{p}B \oplus (1-\frac{T}{p})B$ dans le cas contraire.

Démonstration : On s'est placé dans le cas où le module B est décomposable. On sait (théorème 1, §2.3) que le système d'idempotents c.o.p. de $\mathcal{O}(B)$ coïncide avec celui d'une algèbre $E'[G]$, où le sous-corps E' de E reste à déterminer (rappelons que $E = K \cap \mathbb{Q}^{(p)}$).

La description de $\mathcal{O}(B)$ (proposition 11, §4.2) montre qu'un idempotent e de $K[G]$ appartient à $\mathcal{O}(B)$ si, et seulement si, pour tout idéal $\mathfrak{P}$ de L au-dessus de p, e appartient à $\mathcal{O}(B_\mathfrak{P})$.

Soit $\mathfrak{p}$ un idéal de K au-dessus de p, et $\mathfrak{P}$ l'idéal de L au-dessus de $\mathfrak{p}$. Notons $\mathbb{Q}_p^{(p)} \cap K_\mathfrak{p} = E(\mathfrak{p})$. Si $a_\mathfrak{p} = 0$ ou $a_\mathfrak{p}$ divise $p-1$, on sait, d'après l'étude locale (théorème 3, §3.3), que tout idempotent de $E(\mathfrak{p})[G]$ appartient à $\mathcal{O}(B_\mathfrak{P})$; donc tout idempotent de $E[G]$ appartient à $\mathcal{O}(B_\mathfrak{P})$. Par contre, si $a_\mathfrak{p} \neq 0$ et $a_\mathfrak{p}$ ne divise pas $p-1$, le système d'idempotents c.o.p. de $\mathcal{O}(B_\mathfrak{P})$ est $\{\frac{T}{p}, 1-\frac{T}{p}\}$.

La première partie du théorème en résulte ; la deuxième partie s'en déduit, compte-tenu des résultats du paragraphe 1.

Remarque : (cf. remarque du §3.3).

On voit que B est décomposable en somme directe de sous-A[G]-modules A irréductibles si et seulement si :

1) tout idéal premier $\mathfrak{p}$ de K au-dessus de p est ramifié dans L, le nombre de ramification $t_\mathfrak{p}$ correspondant étant presque ma maximal

2) $a_\mathfrak{p}$ est nul ou divise $p-1$ (pour tout $\mathfrak{p}$ au-dessus de p), ou $\mathbb{Q}^{(p)} \cap K = \mathbb{Q}$.

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, p. 1330-1333.

[2] F. BERTRANDIAS, J.P. 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, p. 1388-1391.

[3] C.W. CURTIS, I. REINER - Representation theory of finish groups and associative algebras. Interscience.

[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 de Doctorat de 3e cycle. Grenoble 1972.

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

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

[7] J. MARTINET - Anneau des entiers d'un extension galoisienne considérée comme module sur l'algèbre du groupe de Galois. Colloque Théorie des Nombres, Bordeaux 1969. Bull. soc. math. Fr., Mémoire 25, (1971), p. 123-126.

[8] Y. MIYATA - On the module structure of the ring of all integers of a $\mathfrak{P}$ adic number field. Nagoya Math. J., vol. 54 (1974), p. 53-59.

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

[10] K.W. ROGGENKAMP, V. HUBER DYSON - Lattices over orders I. Lecture Notes in Mathematics 115, Springer Verlag.

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)