SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

MARIE-JOSÉE FERTON

Décomposition du Galois-module des entiers d'une extension diédrale de degré $2p$ d'un corps local d'un corps de nombres

Séminaire de théorie des nombres de Grenoble, tome 9 (1980-1981), exp. n° 6, p. 1-35
<http://www.numdam.org/item?id=STNG_1980-1981__9__A6_0>

© Institut Fourier – Université de Grenoble, 1980-1981, tous droits réservés.

L'accès aux archives du séminaire de théorie des nombres de Grenoble implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire de Théorie des Nombres
23 avril 1981
Grenoble

DECOMPOSITION DU GALOIS-MODULE DES ENTIERS D'UNE EXTENSION DIEDRALE DE DEGRE 2p D'UN CORPS LOCAL OU D'UN CORPS DE NOMBRES

par Marie-Josée FERTON

Soit A un anneau de Dedekind de corps des quotients K et soit L une extension galoisienne de K de groupe de Galois G. La clôture intégrale B de A dans L est un $A[G]$-module de rang 1. On cherche à décomposer B en une somme directe de sous $A[G]$-modules indécomposables, et on se propose ici de traiter les cas où K est un corps local ou un corps de nombres et où G est un groupe diédral d'ordre $2p$ (p nombre premier distinct de 2).

Lorsque le groupe G est un groupe abélien cette décomposition est unique. Elle a été déterminée dans certains cas par :

- H.W. Leopoldt [6] (lorsque K est le corps des rationnels) ;
- F. Bertrandias [2] et [2 bis] (lorsque G est une Γ-extension de degré p^n d'un corps local) ;
- Z.I. Borevich et S.V. Vostokov [3] (G cyclique de degré p, K corps local) ;

Dans d'autres cas, on sait seulement reconnaître si B est un $A[G]$-module décomposable ou non

- Y. Miyata [7] ;
- S.V. Vostokov [10] (G groupe abélien).

Dans la suite G sera toujours un groupe diédral, d'ordre $2p$. On notera σ et τ , deux générateurs de G tels que $\sigma^p = \tau^2 = 1$ et que $\sigma\tau = \tau\sigma^{-1}$; on notera H le sous-groupe cyclique de G d'ordre p engendré par σ .

Dans le §I , nous verrons des généralités sur la décomposition d'un $A[G]$-module M , de rang 1 .

Dans le §II , nous étudierons la décomposition du $A[G]$-module B dans le cas où le corps K est un corps local de caractéristique résiduelle p , et nous donnerons cette décomposition.

Dans le §III enfin, nous nous intéresserons à l'existence de cette décomposition dans le cas où K est un corps de nombres.

Ce travail s'inspire de la méthode employée par F. Bertrandias dans [2] .

§ I

I.1. DECOMPOSITIONS D'UN A(G)-MODULE DE RANG 1

Dans ce §I , A désigne un anneau de Dedekind de corps des quotients K ; nous ferons plus tard une hypothèse sur K . M est un $A[G]$-module à gauche de rang 1 tel que $A[G] \subset M \subset K[G]$. Notons $\mathrm{End}_{A[G]} M$ l'anneau des $A[G]$-endomorphismes de M . On sait, (cf. [2]) que trouver une décomposition de M en somme directe de sous-$A[G]$-modules indécomposables revient à trouver un système complet orthogonal d'idempotents primitifs de $\mathrm{End}_{A[G]} M$. Etudions donc $\mathrm{End}_{A[G]} M$.

PROPOSITION 1. - Si M est un $A[G]$-module à gauche de rang 1, le commutant de M, $\mathrm{End}_{A[G]} M$, est isomorphe à l'ordre à droite de M dans $K[G]$ noté $\mathcal{O}_d(M, K[G])$ et défini par :

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

Il suffit pour établir cette proposition de démontrer que l'application, qui à un λ de $\mathcal{O}_d(M, K[G])$ fait correspondre dans $\mathrm{End}_{A[G]} M$, la multiplication à droite par λ dans M, est un isomorphisme.

Trouver une décomposition de M en sous-$A[G]$-modules indécomposables c'est donc trouver un système complet orthogonal d'idempotents primitifs de $\mathcal{O}_d(M, K[G])$. Mais nous chercherons tout d'abord à décomposer M en somme directe de sous-modules "caractéristiques indécomposables".

DEFINITION 1. - Un sous-$A[G]$-module M' de M sera dit "caractéristique" si et seulement si pour tout f de $\mathrm{End}_{A[G]} M$, $f(M') \subset M'$.

DEFINITION 2. - Un sous-$A[G]$-module M' de M sera dit "caractéristique indécomposable" si il est caractéristique et si il ne peut se décomposer en somme directe de deux sous-modules caractéristiques non triviaux.

PROPOSITION 2. - Une décomposition de M en somme directe de sous-modules caractéristiques indécomposables correspond à un système complet orthogonal d'idempotents centraux primitifs de $\mathrm{End}_{A[G]} M$ ou de $\mathcal{O}_d(M, K[G])$. Nous appellerons une telle décomposition : "décomposition centrale".

PROPOSITION 3. - M étant un $A[G]$-module de rang 1, il existe une et une seule décomposition centrale de M.

Ce qui s'énonce aussi plus précisément par :

PROPOSITION 3 bis. - Il existe un seul système complet orthogonal d'idempotents centraux primitifs dans $\mathcal{O}_d(M, K[G])$. Ce système est l'ensemble de tous les idempotents centraux primitifs de $\mathcal{O}_d(M, K[G])$ non triviaux.

Démonstration. Soit $(E_i)_{1\leq i\leq k}$ un système complet d'idempotents centraux primitifs de $\mathcal{O}_d(M, K[G])$ et e un idempotent central primitif quelconque de cet ordre. On peut écrire $e = \sum_{1\leq i\leq k} eE_i = \sum_{1\leq i\leq k} E_i e$. Donc il existe un indice i , $1 \leq i \leq k$ tel que $e = eE_i = E_i e$ et $E_j e = 0$ pour tout $j \neq i$.

Ecrivons alors $E_i = e + (E_i - e)$; e et $E_i - e$ sont deux idempotents centraux orthogonaux, ce qui entraîne $E_i = e$.

L'ordre à droite de M dans $K[G]$ étant un sous-anneau de $K[G]$, les idempotents centraux de $\mathcal{O}_d(M, K[G])$ seront des idempotents centraux de $K[G]$. Le paragraphe suivant sera donc consacré au rappel de l'étude des idempotents centraux d'une algèbre $K[G]$ pour un groupe G diédral.

I.2. IDEMPOTENTS CENTRAUX DE L'ALGEBRE K(G)

Notations. Pour tout corps F et tout groupe g nous noterons $\mathrm{Irr}_F(g)$ l'ensemble des caractères irréductibles de g sur F , et $\mathrm{Irr}^*_F(g)$ l'ensemble des caractères irréductibles de g sur F distincts du caractère de la représentation unité.

Dans ce paragraphe, K est un corps local de caractéristique 0 et de caractéristique résiduelle p ou bien un corps de nombres. Nous noterons, k le corps $\mathbb{Q}_p$ ou bien le corps $\mathbb{Q}$ suivant que K est un corps local ou un corps de nombres . Si ζ est une racine primitive p-ième de

l'unité nous noterons k'_0 , K'_0 et E les corps suivants :

$$k'_0 = k(\zeta+\zeta^{-1}) ,$$
$$K'_0 = K(\zeta+\zeta^{-1}) ,$$
$$E = k'_0 \cap K .$$

En sachant que l'indice de Schur de tout caractère irréductible d'un groupe diédral G vaut 1 , on démontre que la décomposition de l'algèbre $K[G]$ (cf. [9 bis], chapitres [5] et [12].2) est :

$$K[G] = \underbrace{K \times K \times \mathbb{M}_2(K'_0) \times \ldots \times \mathbb{M}_2(K'_0)}_{\frac{p-1}{2\,\mathrm{Card}[K'_0:K]} \text{ fois}}$$

où $\mathbb{M}_2(K'_0)$ est l'anneau des matrices d'ordre 2 à coefficients dans K'_0 . Les caractères irréductibles de G sur K étant de plus à valeurs dans k'_0 , leur ensemble est celui des caractères irréductibles de G sur E . En particulier, les idempotents centraux primitifs de $K[G]$ sont ceux de l'algèbre $E[G]$.

PROPOSITION 1. - <u>Soit</u> $\mathcal{C}(K[G])$ <u>l'ensemble des idempotents centraux primitifs de</u> $K[G]$, <u>on a</u> :

$$\mathcal{C}(K[G]) = \{e_\chi , \chi \in \mathrm{Irr}_E(G)\}$$
$$= \{e_{\chi_0}, e_{\chi'_0} ; e_{\chi'} = \frac{1}{p}\sum_{i=0}^{p} \chi'(\sigma^{-i}) , \chi' \in \mathrm{Irr}^*_E(H)\}$$

<u>où on note</u> $T = \sum_{i=0}^{p-1} \sigma^i$, $e_{\chi_0} = \frac{T(1+\tau)}{2p}$, $e_{\chi'_0} = \frac{T(1-\tau)}{2p}$.

<u>Remarque</u> 1. Les $\frac{p-1}{2[K'_0:K]}$ idempotents correspondants aux représentations de degré supérieur à 1 sont les idempotents centraux primitifs de $E[H]$ distincts de $\frac{T}{p}$.

PROPOSITION 2. - <u>Tout idempotent central de</u> $K[G]$ <u>est une somme d'idempotents centraux primitifs de</u> $E[G]$.

Remarque 2. - Tout idempotent de $E[H]$ est un idempotent central de $E[G]$.

Remarque 3. - Si F et F' sont deux corps tels que $k \subset F \subset F' \subset E$, tout idempotent central primitif de $F[G]$, différent de $\frac{T(1+\tau)}{2p}$ et de $\frac{T(1-\tau)}{2p}$, est somme de $[F':F]$ idempotents centraux primitifs de $F'[G]$ permutés transitivement entre eux par $Gal(F'/F)$ (cf. définition du paragraphe I.3).

Remarque 4. - Tout idempotent central primitif de $K[G]$ est la somme de deux idempotents primitifs orthogonaux de $K[G]$, cette décomposition n'étant pas unique. En particulier, si e est un idempotent central primitif de $K[G]$, on peut écrire : $e = e\frac{1+\tau}{2} + e\frac{1-\tau}{2}$ où $e\frac{1+\tau}{2}$ et $e\frac{1-\tau}{2}$ sont des idempotents primitifs de $K[G]$ orthogonaux entre eux.

I.3. DECOMPOSITION CENTRALE D'UN A(G) MODULE DE RANG 1

PROPOSITION. - Soit $\mathcal{S}$ le système complet d'idempotents centraux primitifs de $\mathcal{O}_d(M, K[G])$; il existe une partition de $Irr_E(G)$, $Irr_E(G) = \bigcup_{1 \le i \le s} J_i$, telle que :

$\mathcal{S} = \{E_i , 1 \le i \le s\}$ avec $E_i = \sum_{\chi \in J_i} e_\chi$.

Cette proposition découle des remarques faites dans les paragraphes 1 et 2 .

DEFINITION. - Si φ est un élément du groupe de Galois de E/k et si $\lambda \in E(G)$, $\lambda = \sum_{g \in G} a_g g$, on définit l'action de φ sur $E[G]$ par :

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

HYPOTHESE H_1. - Nous dirons que M vérifie l'hypothèse H_1, si pour tout élément φ du groupe de Galois de E/k et pour tout idempotent central e de $\mathcal{O}_d(M, K[G]) \cap E[G]$, $\varphi(e)$ est encore un élément de $\mathcal{O}_d(M, K[G])$.

Remarque 1. - L'idempotent e étant central, on peut remplacer dans cette hypothèse $\mathcal{O}_d(M, K[G])$ par l'ordre associé à gauche à M dans $K[G]$, $\mathcal{O}(M, K[G])$ défini par : $\mathcal{O}(M, K[G]) = \{\lambda \in K[G] , \lambda M \subset M\}$.

THEOREME. - Si M est un $A[G]$-module de rang 1 vérifiant l'hypothèse H_1 et si M a une décomposition centrale non triviale, nous appellerons F le plus petit sous-corps de E tel que le système $\mathcal{S}$ de $\mathcal{O}_d(M, K[G])$ soit contenu dans $F[G]$. On a alors deux groupes de possibilités :

1) Soit $F \supsetneq k$ et $\mathcal{S} = \left\{\frac{T(1+\tau)}{2p}, \frac{T(1-\tau)}{2p}; \{e_{\chi'}\}, \chi' \in \mathrm{Irr}_F^*(H)\right\} = \left\{e_\chi, \chi \in \mathrm{Irr}_F(G)\right\}$
ou $\mathcal{S} = \left\{e_{\chi'}, \chi' \in \mathrm{Irr}_F(H)\right\}$ (*)

2) Soit $F = k$ et $\mathcal{S} = \{\frac{T(1+\tau)}{2p}, \frac{T(1-\tau)}{2p}, 1-\frac{T}{p}\}$
ou $\mathcal{S} = \{\frac{T(1+\tau)}{2p}, 1-\frac{T(1+\tau)}{2p}\}$
ou $\mathcal{S} = \{\frac{T(1-\tau)}{2p}, 1-\frac{T(1-\tau)}{2p}\}$
ou $\mathcal{S} = \{\frac{T}{p}, 1-\frac{T}{p}\}$ (*) .

Remarque 2. - Les cas (*) ne peuvent se produire que si $\frac{1+\tau}{2} \notin \mathcal{O}_d(M, K[G])$ (cf. §I.4).

COROLLAIRE. - Soit M un $A[G]$-module de rang 1 vérifiant l'hypothèse H_1, M a une décomposition centrale non triviale si et seulement si un des idempotents $\frac{T(1+\tau)}{2p}$, $\frac{T(1-\tau)}{2p}$, $\frac{T}{p}$ au moins se trouve dans $\mathcal{O}_d(M, K[G])$ ou, ce qui revient au même dans $\mathcal{O}(M, K[G])$.

Démonstration du théorème. Supposons $\mathcal{S} \neq 1$.

- Si $F \supsetneq k$, soit f un générateur du groupe de Galois de F/k,

ce groupe $Gal(F/k)$ étant cyclique appelons r_F son ordre. D'après la définition de F, il existe $e \in \mathcal{S}$, $e \neq 1$, tel que les $f^i(e)$, $1 \leq i \leq r_F$ soient tous distincts. D'après l'hypothèse H_1, les $f^i(e)$ sont des idempotents centraux de $\mathcal{O}_d(M, K[G])$, ils sont primitifs et orthogonaux entre eux, ils coïncident donc d'après la proposition précédente et les remarques du §2, avec l'ensemble $\{e_{\chi'}, \chi' \in Irr_F^*(H)\}$. L'élément

$$\frac{T}{p} = 1 - \sum_{i=1}^{r_F} f^i(e) = 1 - \sum_{\chi' \in Irr_F^*(H)} e_{\chi'}$$

est un idempotent central dans $\mathcal{O}_d(M, K[G])$ et sa décomposition dans $F[G]$ est unique et égale à $\frac{T}{p} = \frac{T(1+\tau)}{2p} + \frac{T(1-\tau)}{2p}$, d'où les deux possibilités du théorème dans ce cas.

• Si $F = k$ comme $\mathcal{S} \neq 1$, $\mathcal{S}$ a deux ou trois éléments. Les idempotents centraux primitifs de $K[G]$ étant : $\frac{T(1+\tau)}{2p}$, $\frac{T(1-\tau)}{2p}$ et $1 - \frac{T}{p}$, la fin du théorème s'en déduit facilement.

<u>Remarque</u> 3. Si $F \not\supset k$, pour tout sous corps F' de E, tel que : $\{e_\chi, \chi \in Irr_H^*(F')\} \subset \mathcal{O}_d(M, K[G])$, on a : $F' \subset F$. Ceci résulte de l'unicité du système $\mathcal{S}$ de $\mathcal{O}_d(M, K[G])$.

Remarquons aussi que si L et L' sont deux sous-corps de $k(\zeta)$ tels que $L \subsetneq L' \subset k(\zeta)$, les idempotents centraux primitifs de $L'[G]$ autres que $\frac{T(1+\tau)}{2p}$ et $\frac{T(1-\tau)}{2p}$ n'appartiennent pas à $L[G]$.

I.4 DECOMPOSITION D'UN A(G) MODULE M DE RANG 1, EN SOUS-MODULES INDECOMPOSABLES

HYPOTHESE H_2. - Nous supposerons dans ce § que l'idempotent $\frac{1+\tau}{2}$ est un élément de $\mathcal{O}_d(M, K[G])$.

Nous dirons donc que M vérifie l'hypothèse H_2 si $M\frac{1+\tau}{2} \subset M$, ce qui implique $M\frac{1-\tau}{2} \subset M$.

L'hypothèse H_2 permet de décomposer tout idempotent central e de $\mathcal{O}_d(M, K[G])$, en une somme de deux idempotents orthogonaux dans $\mathcal{O}_d(M, K[G])$ de la manière suivante :

$$e = e\frac{1+\tau}{2} + e\frac{1-\tau}{2} .$$

Les deux modules $M\frac{1+\tau}{2}$ et $M\frac{1-\tau}{2}$ sont des $A[H]$-modules de rang 1, nous pourrons donc dans la suite leur appliquer les résultats de [2].

PROPOSITION 1. - Soit M un $A[G]$-module de rang 1 vérifiant H_2 et soit e un idempotent central de $\mathcal{O}_d(M, K[G])$; la décomposition de $e(\frac{1+\tau}{2})$ [respectivement $e(\frac{1-\tau}{2})$] en somme d'idempotents primitifs de $\mathcal{O}_d(M, K[G])$, deux à deux orthogonaux, se fait de manière unique sous la forme : $e(\frac{1+\tau}{2}) = \sum_{i\in I} \epsilon_i \frac{1+\tau}{2}$ (respectivement $e(\frac{1-\tau}{2}) = \sum_{j\in J} \delta_j \frac{1-\tau}{2}$), où I et J sont des ensembles finis et où pour tout $i \in I$ et tout $j \in J$ ϵ_i et δ_j sont des idempotents de $E[H]$.

Pour démontrer cette proposition et en particulier l'unicité de la décomposition, on utilise le lemme suivant très important dans la suite :

LEMME. - Soit ϵ un idempotent de $E[H]$, il est central dans $E[G]$. L'idempotent $\epsilon\frac{1+\tau}{2}$ est idempotent primitif dans $\mathcal{O}_d(M, K[G])$ si et seulement si ϵ est idempotent primitif dans $\mathcal{O}(M\frac{1+\tau}{2}, K[H])$ ordre associé à gauche dans $E[H]$ au $A[H]$-module $M\frac{1+\tau}{2}$.

HYPOTHESE H. - Nous dirons que M vérifie l'hypothèse H, si M vérifie H_2 et si pour tout idempotent e de $\mathcal{O}(M\frac{1+\tau}{2}, K[H]) \cap E[H]$ et pour tout élément φ de $Gal(E/k)$, $\varphi(e)$ est encore un élément de $\mathcal{O}(M\frac{1+\tau}{2}, K[H]) \cap E[H]$ (de même pour $\mathcal{O}(M\frac{1-\tau}{2}, K[H]) \cap E[H]$).

PROPOSITION 2. - Si M vérifie l'hypothèse H, M vérifie l'ensemble des deux hypothèses H_1 et H_2.

Cette proposition se démontre en utilisant le lemme précédent.

Dans la suite nous décomposerons l'idempotent 1 de $\mathcal{O}_d(M, K[G])$ en $1 = \frac{1+\tau}{2} + \frac{1-\tau}{2}$. Les décompositions de $\frac{1+\tau}{2}$ et $\frac{1-\tau}{2}$ se font de manière unique sous les formes :

$$\frac{1+\tau}{2} = \sum_{i\in I} \epsilon_i \frac{1+\tau}{2} \quad \text{et} \quad \frac{1-\tau}{2} = \sum_{j\in J} \delta_j \frac{1-\tau}{2} ,$$

et nous montrerons que les idempotents de $E[H]$, ϵ_i pour $i \in I$ et δ_j pour $j \in J$ sont en fait les idempotents primitifs d'algèbres $F'[H]$ et $F''[H]$ où F' et F'' sont des corps situés entre k et E. En faisant une démonstration analogue à celle du théorème du § 3, on démontre le théorème suivant :

THEOREME. - <u>Soit</u> M <u>un</u> $A[G]$-<u>module vérifiant l'hypothèse</u> H.

a) <u>Si</u> $M\frac{1+\tau}{2}$ <u>et</u> $M\frac{1-\tau}{2}$ <u>sont deux modules décomposables, il existe deux corps</u> F' <u>et</u> F'' <u>situés entre</u> k <u>et</u> E <u>tels qu'un système complet d'idempotents orthogonaux primitifs de</u> $\mathcal{O}_d(M, K[G])$ <u>soit composé des idempotents</u> $\{e_{\chi'} \frac{1+\tau}{2}, \chi' \in \mathrm{Irr}_{F'}(H)\}$ <u>et des idempotents</u> $\{e_{\chi''} \frac{1-\tau}{2}, \chi'' \in \mathrm{Irr}_{F''}(H)\}$.

b) <u>Si un de ces deux modules est indécomposable</u> (<u>par exemple</u> $M\frac{1-\tau}{2}$) $\{e_{\chi'} \frac{1+\tau}{2}, \chi' \in \mathrm{Irr}_{F'}(H)\} \cup \frac{1-\tau}{2}$ <u>sera un système complet d'idempotents primitifs de</u> $\mathcal{O}_d(M, K[G])$.

COROLLAIRE. - <u>Le</u> $A[H]$-<u>module</u> $M\frac{1+\tau}{2}$ (<u>respectivement</u> $M\frac{1-\tau}{2}$) <u>est décomposable si et seulement si l'idempotent</u> $\frac{T(1+\tau)}{2p}$ (<u>respectivement</u> $\frac{T(1-\tau)}{2p}$) <u>est dans</u> $\mathcal{O}_d(M, K[G])$.

<u>Remarque sur la démonstration du théorème</u>. Les corps F' et F'' sont définis en fait de la manière suivante : si $\frac{1+\tau}{2} = \sum_{i\in I} \epsilon_i \frac{1+\tau}{2}$, ϵ_i idempotent de $E[H]$ (cf. Proposition 1, § 4), F' est la plus petite extension de k dans E telle que tous les idempotents $\epsilon_i \frac{1+\tau}{2}$, $i \in I$, soient inclus dans l'algèbre $F'[G]$; de même pour le corps F''.

PROPOSITION 3. -

a) Dans les mêmes hypothèses que le a) du théorème précédent, le corps F relatif à la décomposition centrale de M (cf. théorème du paragraphe 3) est le corps : $F = F' \cap F''$.

b) Si seul un des modules, $M\frac{1+\tau}{2}$ par exemple, est décomposable le corps F est nécessairement le corps $\mathbb{Q}_p$ et le système $\mathcal{S}$ est le suivant : $\{\frac{T(1+\tau)}{2p}, 1-\frac{T(1+\tau)}{2p}\}$.

On utilise pour le démontrer la remarque 3 du § 3 et la proposition 1 du § 4 .

Dans le § II qui suit, l'hypothèse H énoncée ci-dessus sera satisfaite et nous déterminerons pour un corps local K les ordres, $\mathcal{O}(M\frac{1+\tau}{2}, K[H])$ et $\mathcal{O}(M\frac{1-\tau}{2}, K[H])$, pour trouver les corps F , F' et F'' .

§ II

DECOMPOSITION DU GALOIS MODULE DES ENTIERS D'UNE EXTENSION DIEDRALE (2p) D'UN CORPS LOCAL DE CARACTERISTIQUE RESIDUELLE p

Ce paragraphe utilise les résultats du chapitre II de [5] . Dans ce paragraphe K est un corps local de caractéristique 0 , de caractéristique résiduelle p , d'indice de ramification absolue e_K .

B est l'anneau des entiers d'une extension L de K galoisienne, de groupe de Galois G , où G est un groupe diédral d'ordre $2p$. Si A désigne l'anneau des entiers de K , B est un $A[G]$-module de rang 1 .

Si θ est un élément de B engendrant une base normale de L/K , nous noterons $M = \{\lambda \in K[G] \ , \ \lambda\theta \in B\}$, B et M sont deux $A[G]$-modules à gauche isomorphes.

Nous étudierons la décomposition en sous-$A[G]$-modules indécomposables du module M qui vérifie comme dans le §I , $A[G] \subset M \subset K[G]$.

On notera a le reste modulo p du deuxième nombre de ramification inférieure t de l'extension, $t = a_0 p + a$ avec $0 \leq a < p$. Le théorème que nous allons démontrer dans le §II est le suivant :

II.1. THEOREME

Soit L/K une extension diédrale de corps locaux.

1°) Si p ne divise pas la différente de L/K : B est un $A[G]$-module centralement indécomposable et $M = M\frac{1+\tau}{2} \oplus M\frac{1-\tau}{2}$ est une décomposition de M en deux sous-modules indécomposables.

2°) Si p divise la différente de L/K :

a) Si L/K est une extension totalement ramifiée avec a impair (a reste modulo p du 2ème nombre de ramification) : la décomposition centrale de B est la suivante

$$B = \frac{T(1+\tau)}{2p} B \oplus (1 - \frac{T(1+\tau)}{2p})B$$

et

$$M = M\frac{1-\tau}{2} \oplus M\frac{T(1+\tau)}{2p} \oplus M(1-\frac{T}{p})(\frac{1+\tau}{2})$$

est une décomposition de M en sous-$A[G]$-modules indécomposables.

b) Sinon (c'est-à-dire ou L/K non totalement ramifiée, ou L/K totalement ramifiée et a pair) :

b.1) Si $a \neq 0$ et si a ne divise pas $p-1$

$$B = \frac{T(1+\tau)}{2p} B \oplus \frac{T(1-\tau)}{2p} B + (1-\frac{T}{p})B$$

est la décomposition centrale de B .

$$M = M\frac{T(1+\tau)}{2p} \oplus M\frac{T(1-\tau)}{2p} \oplus M(1-\frac{T}{p})(\frac{1+\tau}{2}) \oplus M(1-\frac{T}{p})(\frac{1-\tau}{2})$$

est une décomposition de M en sous-$A[G]$-modules indécomposables.

b.2) <u>Si</u> $a = 0$ <u>où</u> a <u>divise</u> $p-1$

$B = \oplus e_\chi B$, $\chi \in \mathrm{Irr}_E(G)$ <u>est la décomposition centrale de</u> B .

$M = \oplus Me_\chi \frac{1+\tau}{2} \oplus Me_\chi \frac{1-\tau}{2}$, $\chi \in \mathrm{Irr}_E(H)$

<u>est une décomposition centrale de</u> M <u>en sous-</u>$A[G]$<u>-modules indécomposables.</u>

(On rappelle que $E = \mathbb{Q}_p(\zeta+\zeta^{-1}) \cap K$ où ζ est une racine p-ème de 1).

Pour la démonstration de ce théorème, nous devrons distinguer plusieurs cas suivant la ramification de l'extension L/K , et suivant la parité de a . Lorsque l'extension est sauvagement ramifiée, nous distinguons par **A** et **B** les deux cas suivants, cf. [5]

A , l'extension L/K est totalement ramifiée

B , l'extension L/K n'est pas totalement ramifiée.

L'élément θ de B est alors choisi suivant les cas comme dans [5] et nous connaissons des A-bases du $A[G]$-module M dans tous les cas. Nous noterons dans la suite $g = \sigma - \sigma^{-1}$, v_K la valuation d'un corps local K , $[x]$ et $\underset{\sim}{x}$ les parties entières et fractionnaires d'un réel x . D'après [5] , on a

$$M\frac{1-\tau}{2} = \left\{ \sum_{0\le i\le p-1} a_i \frac{g^i(1-\tau)}{2},\ a_i \in K \text{ et } v_K(a_i) \ge -\nu_i \right\}$$

$$M\frac{1+\tau}{2} = \left\{ \sum_{0\le i\le p-1} a_i \frac{g^i(1+\tau)}{2},\ a_i \in K \text{ et } v_K(a_i) \ge -\nu'_i \right\}$$

avec pour tout i , $0 \le i \le p-1$:

- dans le cas **A** , a impair $\nu_i = [\frac{it+a}{2p}]$, $\nu'_i = [\frac{it+a+p}{2p}]$;
- dans le cas **A** , a pair, $a \neq 0$ $\nu_i = [\frac{it+a+p}{2p}]$, $\nu'_i = [\frac{it+a}{2p}]$;
- dans le cas **A** , $a = 0$ $\nu_i = \nu'_i = [\frac{it}{2p}]$;
- dans le cas **B** , $\nu_i = \nu'_i = [\frac{it+a}{p}]$.

PROPOSITION 1. - p <u>divise la différente</u> $\mathcal{D}(L/K)$ <u>si et seulement si l'extension</u> L/K <u>est sauvagement ramifiée et que la ramification est presque maximale dans cette extension ou encore si et seulement si l'idempotent</u> $\frac{T}{p}$ <u>appartient à l'ordre</u> $\mathcal{O}(M^{\frac{1+\tau}{2}}, K[H])$.

Cette proposition se déduit très facilement des formules données dans [5] : la ramification est presque maximale dans les extensions sauvagement ramifiées si :

- dans le cas **A** , $\frac{2pe_K}{p-1} - 2 \leq t \leq \frac{2pe_K}{p-1}$
- dans le cas **B** , $\frac{pe_K}{p-1} - 1 \leq t \leq \frac{pe_K}{p-1}$,

et de la valuation de la différente donnée dans [9]

- cas **A** , $v_L(\mathcal{D}(L/K)) = 2p-1+t(p-1)$
- cas **B** , $v_L(\mathcal{D}(L/K)) = (p-1)(t+1)$.

<u>Remarque</u>.

a) Dans le cas **A** , a impair, l'idempotent $\frac{T(1-\tau)}{2p} \notin \mathcal{O}(M, K[G])$, cf. [5] , p. 66 et 67 , on peut donc dire que le module $M^{\frac{1-\tau}{2}}$ est indécomposable.

b) Dans le cas **A** , si a impair on a toujours : $t < \frac{2pe_K}{p-1} - 1$ et donc la ramification est presque maximale si et seulement si

$$\frac{2pe_K}{p-1} - 2 \leq t < \frac{2pe_K}{p-1} - 1 .$$

c) Dans le cas **A** , a pair, la ramification est presque maximale si et seulement si $t \geq \frac{2pe_K}{p-1} - 1$.

d) Dans le cas **A** , a impair, p ne peut diviser la différente de l'extension L/K_H (K_H corps fixe par le groupe H) en effet $v_L(\mathcal{D}(L/K_H)) = (t+1)(p-1)$ et $(t+1)(p-1) < 2pe_K$ d'après b) .

e) Dans le cas **A** , a pair, p divise $\mathcal{D}(L/K)$ est équivalent à p divise $\mathcal{D}(L/K_H)$ d'après c) .

PROPOSITION 2. - <u>L'hypothèse</u> H <u>du paragraphe</u> I.4 <u>est vérifiée dans tous les cas par le module</u> M .

En effet, si $e \in \mathcal{O}(M\frac{1+\tau}{2}, K[H]) \cap E[H]$ on vérifie que pour tout $\varphi \in Gal(E/k)$, $\varphi(e) \cdot M\frac{1+\tau}{2} \subset M\frac{1+\tau}{2}$, il suffit de vérifier que l'inclusion est vraie pour tout élément de la A-base de $M\frac{1+\tau}{2}$ donnée ci-dessus.

PROPOSITION 3 (cf. [5]). - <u>Pour tout corps</u> F , $\mathbb{Q}_p \subset F \subset E \subset \mathbb{Q}'_{p_0}$ <u>l'ordre maximal de l'algèbre</u> F[H] <u>noté</u> $\mathcal{M}_F$, <u>est donné par</u> (cf. [5])

$$\mathcal{M}_F = \left\{ \sum_{0 \le i \le p-1} a_i g^i \ , \ a_i \in F \ , \ v_F(a_i) \ge -[\frac{ie_F}{p-1}] \right\} .$$

<u>D'autre part,</u> $\mathcal{M}_F$ <u>est l'anneau engendré par</u> $A_F[H]$ (A_F <u>anneau des entiers de</u> F) <u>et par les idempotents</u> $\frac{T}{p}$ <u>et</u> $\{e_\chi\}$, $\chi \in Irr^*_H(F)$.

Dans la suite, nous allons chercher (d'après I.4) le plus grand corps F' , $\mathbb{Q}_p \subset F' \subset E$ tel que $\mathcal{M}_{F'} \subset \mathcal{O}(M\frac{1+\tau}{2}, K[H])$ (respectivement dans le cas **B** et le cas **A** a pair, le plus grand corps F'' , $\mathbb{Q}_p \subset F'' \subset E$ tel que $\mathcal{M}_{F''} \subset \mathcal{O}(M\frac{1-\tau}{2}, K[H])$. Puis nous en déduirons le corps F et la décomposition centrale de B d'après la proposition 3 de I.4. Cette étude nécessite de séparer les cas **B** , **A** a pair et **A** a impair, c'est ce que nous ferons dans la suite.

II.2. ETUDE DU CAS **B**

Définissons l'ensemble $\mathcal{E}(\frac{t}{p})$, (cf. [2 et 5])

$$\mathcal{E}(\tfrac{t}{p}) = \{h \text{ entier}, \ 1 \le h \le p-1 \ / \ \text{pour tout } h' \text{ entier}, \ 1 \le h' < h : \ h'\underset{\vee}{\frac{a}{p}} > h\underset{\vee}{\frac{a}{p}}\} .$$

D'après [5]

$$\mathcal{O}(M\frac{1+\tau}{2}, K[H]) = \mathcal{O}(M\frac{1-\tau}{2}, K[H]) =$$

$$= \left\{ \sum_{0\le i\le p-1} a_i g^i \ , \ a_i \in K \ , \ v_K(a_i) \ge -n_i \ \text{ où } \ n_i = [\frac{it}{p}] + \delta_i \right\}$$

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

Comme dans [2] on en déduit que si p divise la différente $\mathcal{D}(L/K)$ on a si $a=0$ ou si a divise $p-1$, $F = F' = F'' = E$, et sinon $F = F'' = F' = \mathbb{Q}_p$. D'où les décompositions données par le théorème dans ce cas-là.

II.3. ETUDE DU CAS A , a impair

Rappelons que dans ce cas $M\frac{1-\tau}{2}$ est un module indécomposable et que $M\frac{1+\tau}{2}$ est décomposable si et seulement si $\frac{2pe_K}{p-1} - 2 \le t < \frac{2pe_K}{p-1} - 1$. Introduisons l'ensemble

$$\mathcal{E}'(\frac{t}{2p}) = \left\{ h \text{ entier}, \ 1 \le h \le p-1 / \text{pour tout } h' \text{ entier}, \ 1 \le h' < h : \underset{\vee}{\frac{h'a+p}{2p}} > \underset{\vee}{\frac{ha+p}{2p}} \right\}$$

ce qui équivaut à

$$\mathcal{E}'(\frac{t}{2p}) = \left\{ h \text{ entier}, \ 1 \le h \le p-1 / \underset{\vee}{\frac{ha}{2p}} > \frac{1}{2} \text{ et } \forall h' , \ 1 \le h' < h \text{ ou bien } \underset{\vee}{\frac{h'a}{2p}} < \frac{1}{2} \text{ ou bien } \underset{\vee}{\frac{h'a}{2p}} > \underset{\vee}{\frac{ha}{2p}} \right\} .$$

PROPOSITION 1. - <u>Si la ramification est presque maximale c'est-à-dire si</u> $e_K = \frac{(p-1)a_0}{2} + \frac{a+1}{2}$ <u>on a</u>

$$\mathcal{O}(M\frac{1+\tau}{2}, K[H]) = \left\{ \sum_{0\le i\le p-1} a_i g^i \ , \ a_i \in K \ , \ v_K(a_i) \ge -n'_i \ \underline{\text{où}} \ n'_i = [\frac{it}{2p}] + \delta'_i \ \underline{\text{avec}} \ \delta'_i = \begin{cases} 1 & \underline{\text{si}} \ p-i \in \mathcal{E}'(\frac{t}{2p}) \\ 0 & \underline{\text{sinon}} \end{cases} \right\} .$$

La démonstration de cette proposition est analogue à celle de la proposition de [5], page 19 .

PROPOSITION 2. - <u>Si la ramification est presque maximale et si</u> $a = 1$ <u>on a</u> $\mathfrak{M}_E \subset \mathcal{O}(M^{\frac{1+\tau}{2}}, K[H]) \cap E[H]$.

<u>Démonstration</u>. Nous avons dans ce cas $e_K = \frac{(p-1)a_0}{2} + 1$, e_E divisant à la fois $p-1$ et e_K est nécessairement égal à 1 et donc $E = k = \mathbb{Q}_p$. Par suite $\mathcal{E}'(\frac{t}{2p}) = \{1\}$ et $n'_i = \frac{ia_0}{2}$ pour tout i , $0 \leq i < p-1$. L'inclusion est ensuite facile à vérifier.

PROPOSITION 3. - <u>Si la ramification est presque maximale et si</u> $a \neq 1$ <u>pour tout sous-corps</u> F <u>de</u> E , $\mathbb{Q}_p \subsetneq F \subseteq E$ <u>on a</u>

$\mathfrak{M}_F \not\subset \mathcal{O}(M^{\frac{1+\tau}{2}}, K[H]) \cap F[H]$.

<u>Démonstration</u>. Si F est un sous-corps de E , $\mathbb{Q}_p \subsetneq F \subseteq E$, on peut dire que $2e_F$ divise $a+1$ en effet $2e_K = (p-1)a_0 + a + 1$ et $2e_F$ divise $2e_K$ et $a_0(p-1)$. Si

$$\mathfrak{M}_F \subset \mathcal{O}(M^{\frac{1+\tau}{2}}, K[H]) \cap F[H] = \left\{ \sum_{0 \leq i \leq p-1} a_i g^i \ , \ a_i \in F \ , \ v_F(a_i) \geq -\frac{n'_i e_F}{e_K} \right\}$$

c'est qu'en particulier pour les indices $i_k = k\frac{p-1}{e_F}$, $1 \leq k \leq e_F - 1$, (ici $e_F > 1$) on a :

$$n'_{i_k} \geq [\frac{i_k e_F}{p-1}] \times \frac{e_K}{e_F} \quad \text{pour} \quad 1 \leq k \leq e_F - 1$$

ce qui équivaut à $\delta'_{i_k} \geq 1$ pour $1 \leq k \leq e_F - 1$ ou à $p - i_k \in \mathcal{E}'(\frac{t}{2p})$ pour $1 \leq k \leq e_F - 1$ or ceci est impossible, en effet :

- si $a > \frac{a+p}{e_F}$ on a $p < \frac{(e_F - 1)(a+p)}{e_F} < 2p$ et les indices $h_k = p - i_k = p - \frac{k(p-1)}{e_F}$ pour $1 \leq k \leq e_F - 1$ vérifient $\frac{h_k a}{2p} = \frac{p + k(\frac{a+p}{e_F})}{2p}$ en particulier $\frac{h_{e_F - 1} a}{2p} < \frac{1}{2}$ donc $p - i_{e_F - 1} \notin \mathcal{E}'(\frac{t}{2p})$.

- si $a < \frac{a+p}{e_F}$ alors $h_1 = p - \frac{p-1}{e_F} \notin \mathcal{E}'(\frac{t}{2p})$ en effet, il existe h' tel que $(h'-1)a < p < h'a$ et cet h' vérifie $2 \leq h' < h$ avec $\frac{h'a}{2p} > \frac{1}{2}$ et

$$\frac{h'a}{2p} = \frac{1+a}{2p} < \frac{h_1 a}{2p} .$$

La partie du théorème de II.1 relative aux extensions de cas **A** , a impair, est donc démontrée car d'après les propositions 2 et 3 $F' = F = \mathbb{Q}_p$.

II.4. ETUDE DU CAS **A** , a pair

Rappelons dans ce cas que les modules $M\frac{1+\tau}{2}$ et $M\frac{1-\tau}{2}$ sont décomposables si et seulement si $t \geq \frac{2pe_K}{p-1} - 1$ c'est-à-dire si $e_K = \frac{(p-1)a_0}{2} + \frac{a}{2}$. Plaçons-nous dans cette hypothèse.

<u>Notations</u>.

$$\mathcal{E}_1(\frac{t}{2p}) = \left\{ h \text{ entier, } 0<h\leq p-1 / \forall h' \text{ entier } 0<h'<h \text{ , } \frac{h'(a+p)}{2p} > \frac{h(a+p)+p}{2p} \right\}$$

et

$$\mathcal{E}'_1(\frac{t}{2p}) = \left\{ h \text{ entier, } 0<h\leq p-1 / \forall h' \text{ entier } 0<h'<h \text{ , } \frac{h'(a+p)+p}{2p} > \frac{h(a+p)+p}{2p} \right\} .$$

Notons aussi pour tout i , $0 \leq i \leq p-1$, n_i (respectivement n'_i) le plus grand entier tel que pour $a_i \in K$, $a_i g^i \in \mathcal{O}(M\frac{1-\tau}{2}, K[H])$ (respectivement $a_i g^i \in \mathcal{O}(M\frac{1+\tau}{2}, K[H]))$ si et seulement si $v_K(a_i) \geq -n_i$ (respectivement $v_K(a_i) \geq -n'_i$) .

PROPOSITION 1. - <u>Pour tout</u> i , $0 \leq i \leq p-1$ <u>on a</u> :

a) $n'_i = [\frac{it}{2p}] + \delta'_i = \frac{i(a_0-1)}{2} + [\frac{i(a+p)}{2p}] + \delta'_i$

<u>avec</u> $\delta'_i = \begin{cases} 1 & \underline{\text{si}} \quad p-i \in \mathcal{E}'_1(\frac{t}{2p}) \\ 0 & \underline{\text{sinon.}} \end{cases}$

b) $n_i \leq [\frac{it}{2p}] + \delta_i$

<u>avec</u> $\delta_i = \begin{cases} 1 & \underline{\text{si}} \quad p-i \in \mathcal{E}_1(\frac{t}{2p}) \\ 0 & \underline{\text{sinon.}} \end{cases}$

De plus, pour les indices $i_k = k\frac{p-1}{e_E}$, $1 \leq k \leq e_E$ on a
$n_{i_k} = [\frac{i_k t}{2p}] + \delta_{i_k}$.

PROPOSITION 2. - Si p divise la différente $\mathcal{D}(L/K)$ et si a est non nul et ne divise pas $p-1$, quel que soit le sous-corps F de E , $\mathbb{Q}_p \subsetneq F \subseteq E$, $\mathfrak{M}_F$ n'est inclus ni dans $\mathcal{O}(M\frac{1+\tau}{2}, K[H])$ ni dans $\mathcal{O}'(M\frac{1-\tau}{2}, K[H])$.

Démonstration. Soit F un sous-corps de E , distinct de $\mathbb{Q}_p$, on a comme dans II.2

$$\mathfrak{M}_F = \left\{ \sum_{i=0}^{p-1} a_i g^i \ , \ a_i \in F \ , \ v_F(a_i) \geq -[\frac{ie_F}{p-1}] \right\} .$$

Considérons l'indice $j = \frac{p-1}{e_F}$, ici $e_F > 1$; si $a_j \in F$ avec $v_F(a_j) = -[\frac{je_F}{p-1}] = -1$, $a_j g^j$ est un élément de $\mathfrak{M}_F$. Montrons que $a_j g^j \notin \mathcal{O}(M\frac{1-\tau}{2}, K[H])$ et $a_j g^j \notin \mathcal{O}(M\frac{1+\tau}{2}, K[H])$ c'est-à-dire que $v_K(a_j) = v_F(a_j)\frac{e_K}{e_F} < -n'_j$ et $v_K(a_j) < -n_j$.

Il est facile de voir que ces deux inégalités proviennent de ce que pour $j = \frac{p-1}{e_F}$, $\delta_j = \delta'_j = 0$. Pour démontrer que $\delta_j = \delta'_j = 0$ on trouve des indices h' , $h' < p-j$, à l'aide des dénominateurs des réduites successives du développement en fraction continue de $\frac{a}{p}$, qui d'après les définitions précédentes entraînent que $p-j \notin \mathcal{E}_1(\frac{t}{2p})$ et $p-j \notin \mathcal{E}'_1(\frac{t}{2p})$.

Cette proposition signifie que dans ce cas $F = F' = F'' = \mathbb{Q}_p$.

PROPOSITION 3. - Si p divise $\mathcal{D}(L/K)$ et si $a = 0$ ou si a divise $p-1$, alors $\mathfrak{M}_E \subset \mathcal{O}(M\frac{1+\tau}{2}, K[H])$ et $\mathfrak{M}_E \subset \mathcal{O}(M\frac{1-\tau}{2}, K[H])$.

Cette proposition signifie que si $a = 0$ ou a divise $p-1$ on a $F = F' = F'' = E$. Le cas $a = 0$ est immédiat d'après [5] car

$$\mathfrak{M}_E = \mathcal{O}(M\frac{1+\tau}{2}, K[H]) = \mathcal{O}(M\frac{1-\tau}{2}, K[H]) .$$

Le cas $a/p-1$ se déduit des deux lemmes suivants :

LEMME 1. - $\mathfrak{M}_E \subset \mathcal{O}(M\frac{1+\tau}{2}, E[H])$ (respectivement $\mathfrak{M}_E \subset \mathcal{O}(M\frac{1-\tau}{2}, E[H])$) si et seulement si la suite $p - k\frac{p-1}{e_E}$, $1 \leq k \leq e_E$ est dans $\mathcal{E}'_1(\frac{t}{2p})$ (respectivement $\mathcal{E}_1(\frac{t}{2p})$).

Démonstration. $\mathfrak{M}_E \subset \mathcal{O}(M\frac{1+\tau}{2}, K[H])$ si et seulement si $e_K[\frac{ie_E}{p-1}] \leq e_E n'_i$ pour tout i, $0 \leq i \leq p-1$. Pour les indices i vérifiant $k\frac{p-1}{e_E} < i < (k+1)\frac{p-1}{e_E}$, $0 \leq k \leq e_E-1$, il est facile de voir que ces inégalités sont toujours vérifiées. Pour les indices $k\frac{p-1}{e_E}$, $0 \leq k \leq e_E$ elles ne le sont que si $\delta'_{k\frac{p-1}{e_E}} = 1$.

LEMME 2. - Si a divise $p-1$, la suite $p - k\frac{p-1}{e_E}$ est dans $\mathcal{E}'_1(\frac{t}{2p})$ (respectivement $\mathcal{E}_1(\frac{t}{2p})$).

Démonstration. Si a divise $p-1$ posons $d = \frac{p-1}{a}$. D'autre part, e_E qui divise e_K et $p-1$ divise aussi a d'après l'égalité $2e_K = (p-1)a_0+a$. Par suite, si nous posons $a = re_E$, on obtient $2e_K = re_E(da_0+1)$, on montre facilement que d'après le choix du corps E, r est un entier pair.

Soit $1 \leq k \leq e_E$ l'entier $p - k\frac{p-1}{e_E}$ s'écrit alors

$$p - k\frac{p-1}{e_E} = p - krd = 1 + d(a-kr) .$$

Par suite,

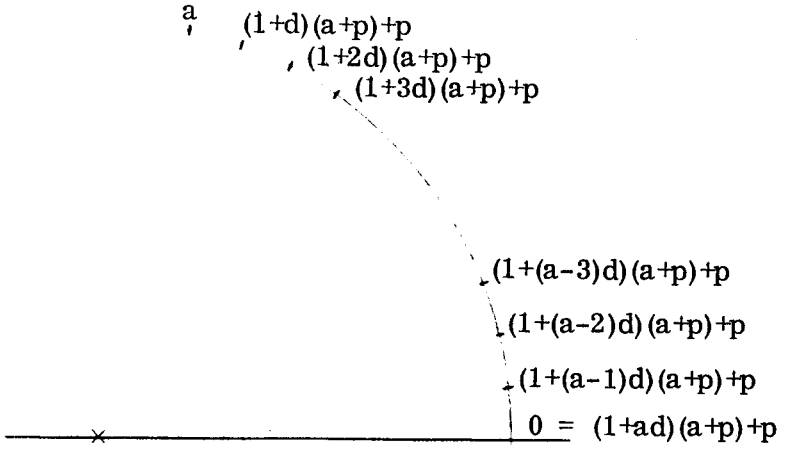
$$\frac{(p-k\frac{p-1}{e_E})a}{\underset{\vee}{2p}} = \frac{kr}{2p} \quad \text{et} \quad \frac{(p-k\frac{p-1}{e_E})(a+p)+p}{\underset{\vee}{2p}} = \frac{kr}{2p} .$$

D'autre part, suivant que d est pair ou impair on a :

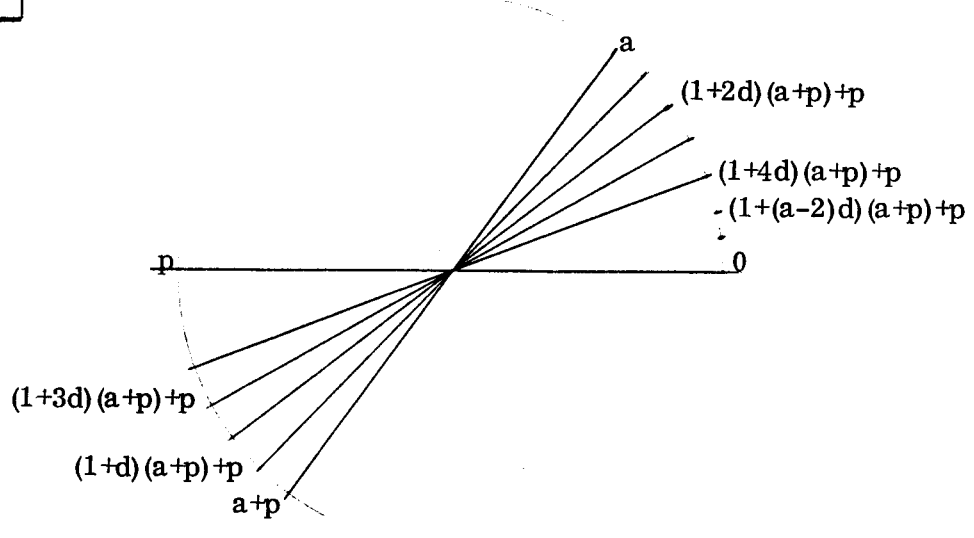
$$\frac{\{1+(a-kr+1)d\}(a+p)+p}{\underset{\vee}{2p}} \quad \text{qui vaut} \quad \frac{kr-1+p}{2p} \quad \text{ou} \quad \frac{kr-1}{2p} .$$

Comme $ja \equiv j'_a \pmod p$ est impossible si j et j' sont des entiers distincts compris entre 0 et $p-1$, il est clair d'après les représentations sur le cercle modulo $2p$ que la suite, $p - krd$, $1 \leq k \leq e_E$ se trouve à la fois dans $\mathcal{E}'_1(\frac{t}{2p})$ et $\mathcal{E}_1(\frac{t}{2p})$.

CAS d impair



CAS d pair



N.B. : le point noté x sur le cercle représente le reste modulo 2p de l'entier x.

Les propositions précédentes permettent de démontrer le théorème dans le cas d'une extension de type **A** avec a pair.

Il nous reste à regarder le cas où l'extension est modérément ramifiée. C'est le cas le plus simple, car nous pouvons alors choisir un élément θ de B tel que $B = A[G]\cdot\theta$, par suite $M = A[G]$ et $\mathcal{O}_d(M, K[G]) = A[G]$.

Donc dans ce cas aussi M vérifie l'hypothèse H et d'après le §I , B et M sont des modules centralement indécomposables. D'autre part, les sous-modules $M\frac{1+\tau}{2}$ et $M\frac{1-\tau}{2}$ de M sont indécomposables car les idempotents $\frac{T(1+\tau)}{2p}$ et $\frac{T(1-\tau)}{2p}$ ne sont pas dans $\mathcal{O}_d(M, K[G])$ (cf. corollaire du théorème I.4). Une décomposition de M en sous-$A[G]$-modules indécomposables est donc dans ce cas :

$$M = M\frac{1+\tau}{2} \oplus M\frac{1-\tau}{2} .$$

Rappelons que lorsque l'extension n'est pas sauvagement ramifiée p ne divise pas la différente de L/K . Ceci achève la démonstration du théorème cité au début du §II .

§ III

DECOMPOSITION DU GALOIS-MODULE DES ENTIERS D'UNE EXTENSION DIEDRALE D'UN CORPS DE NOMBRES

Dans ce paragraphe, K désigne un corps de nombres et L une extension galoisienne de K avec $Gal(L/K) = G$, groupe diédral d'ordre $2p$. B et A désignent respectivement les anneaux d'entiers de L et de K . Nous nous intéresserons tout d'abord à la décomposition centrale du $A[G]$-module de rang 1 , B , décomposition que l'on sait unique (cf. §I) .

III.1 DECOMPOSITION CENTRALE

Dans ce paragraphe, nous démontrerons le théorème suivant :

THEOREME. - <u>Soit</u> L/K <u>une extension diédrale de corps de nombres, une condition nécessaire et suffisante pour que le</u> $A[G]$-<u>module</u> B <u>des entiers de</u> L <u>soit décomposable centralement est qu'il existe un sous-corps</u> F <u>de</u> L , $K \subseteq F \subsetneq L$, <u>galoisien sur</u> K <u>tel que</u> $[L:F]$ <u>divise la différente de</u> L/F .

Pour la démonstration de ce théorème, nous allons tout d'abord voir comment l'ordre associé à B dans $K[G]$, $\mathcal{O}(B, K[G])$ se déduit des ordres associés des extensions locales.

III.1.1. Lien entre les divers ordres associés.

Soit $\mathcal{P}$ l'ensemble des idéaux premiers de A . On note $K_{\mathfrak{p}}$ le complété de K pour un idéal $\mathfrak{p} \in \mathcal{P}$, $A_{\mathfrak{p}}$ l'anneau des entiers de $K_{\mathfrak{p}}$ et $B_{\mathfrak{p}} = A_{\mathfrak{p}}[G] \underset{A[G]}{\otimes} B$. On a alors la propriété suivante : pour un λ de $K[G]$, λ est dans $\mathcal{O}(B, K[G])$ si et seulement si pour tout idéal $\mathfrak{p}$ de $\mathcal{P}$, λ est dans $\mathcal{O}(B_{\mathfrak{p}}, K_{\mathfrak{p}}[G])$.

Choisissons ensuite un idéal $\mathfrak{P}$ premier de B au-dessus de $\mathfrak{p} \in \mathcal{P}$; notons D le groupe de décomposition de $\mathfrak{P}$ et $\mathcal{R}$ un système de représentants de G/D . Le complété $L_{\mathfrak{P}}$ de L pour la valuation $\mathfrak{P}$-adique est une extension galoisienne de $K_{\mathfrak{p}}$ de groupe de Galois D , et si $B_{\mathfrak{P}}$ est l'anneau des entiers de $L_{\mathfrak{P}}$ on a :

$$B_{\mathfrak{p}} = \bigoplus_{s \in \mathcal{R}} s\, B_{\mathfrak{P}}$$

et

$$(*) \qquad \mathcal{O}(B_{\mathfrak{p}}, K_{\mathfrak{p}}[G]) = \bigcap_{s \in \mathcal{R}} s\,(\oplus t\,\mathcal{O}(B_{\mathfrak{P}}, K_{\mathfrak{p}}[D]))\,s^{-1} \qquad \text{(cf. [1], chapitre 4).}$$

On note $\mathcal{S}$ l'unique système complet d'idempotents centraux primitifs orthogonaux de $\mathcal{O}(B, K[G])$. Pour tout $\mathfrak{p} \in \mathcal{P}$, $\mathcal{S}$ est aussi contenu dans $\mathcal{O}(B_{\mathfrak{p}}, K_{\mathfrak{p}}[G])$.

III.1.2. Condition nécessaire pour une décomposition centrale.

Pour que $\mathcal{S} \neq 1$, regardons d'abord les ordres $\mathcal{O}(B_{\mathfrak{p}}, K_{\mathfrak{p}}[G])$ pour des idéaux $\mathfrak{p}$ de A situés au-dessus du nombre premier p .

Si $\mathfrak{p}$ est au-dessus de p , les possibilités pour l'extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$

et pour l'ordre $\mathcal{O}(B_{\mathfrak{p}}, K_{\mathfrak{p}}[G])$ sont les suivantes :

a) $\mathfrak{p}$ est un idéal totalement décomposé dans $L_{\mathfrak{P}}/K_{\mathfrak{p}}$; c'est-à-dire $D = \{1\}$. Dans ce cas $\mathcal{O}(B_{\mathfrak{p}}, K_{\mathfrak{p}}[G]) = A_{\mathfrak{p}}[G]$;

b) $\mathfrak{p}$ est un idéal de A décomposé en p-idéaux dans $L_{\mathfrak{P}}/K_{\mathfrak{p}}$, D est alors un sous-groupe d'ordre 2 de G ; l'extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ est modérément ramifiée et $\mathcal{O}(B_{\mathfrak{p}}, K_{\mathfrak{p}}[G]) = A_{\mathfrak{p}}[G]$.

Dans les cas a) et b) le seul système complet d'idempotents centraux est 1 .

c) $\mathfrak{p}$ est un idéal non décomposé, c'est-à-dire $D = G$, on a alors $\mathcal{O}(B_{\mathfrak{p}}, K_{\mathfrak{p}}[G]) = \mathcal{O}(B_{\mathfrak{P}}, K_{\mathfrak{p}}[G])$, l'extension locale étant soit totalement ramifiée, soit ramifiée dans la partie de degré p (cf. §II).

D'après le §II, $\mathcal{O}(B_{\mathfrak{P}}, K_{\mathfrak{p}}[G])$ possède dans ce cas un système d'idempotents centraux non trivial si et seulement si la ramification est presque maximale dans l'extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$.

d) $\mathfrak{p}$ se décompose en 2 idéaux, c'est-à-dire $D = H$ et l'extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ est cyclique d'ordre p . On a $B_{\mathfrak{p}} = B_{\mathfrak{P}} \oplus \tau B_{\mathfrak{P}}$.

La formule (*) dans ce cas, montre que l'hypothèse H_1 du §I.3 est vérifiée pour le $A_{\mathfrak{p}}[G]$-module $B_{\mathfrak{p}}$. D'après le corollaire du théorème de I.3, on voit que $\mathcal{O}(B_{\mathfrak{p}}, K_{\mathfrak{p}}[G])$ a un système d'idempotents centraux non trivial seulement si il contient un des idempotents $\frac{T}{p}$, $\frac{T(1+\tau)}{2p}$, $\frac{T(1-\tau)}{2p}$. On montre que ceci n'est possible que si $\frac{T}{p} \in \mathcal{O}(B_{\mathfrak{P}}, K_{\mathfrak{p}}[D])$, c'est-à-dire que si l'extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ est ramifiée avec une ramification presque maximale (cf. [5]).

En résumé, une condition nécessaire pour que $\mathcal{O}(B, K[G])$ possède un système $\mathcal{S}$, $\mathcal{S} \neq 1$, est que les idéaux $\mathfrak{p}$ de A au-dessus de p se comportent tous comme dans les cas c) et d) avec une ramification presque maximale. Cette condition s'exprime facilement à l'aide de la différente de l'extension L/K : $\mathcal{D}(L/K)$. Il suffit dans chaque cas de calculer les valuations $\mathfrak{P}$-adique de la différente sachant que $v_{\mathfrak{P}}(\mathcal{D}(L/K)) = \sum_{i=0}^{\infty} \mathrm{Card}(G_i) - 1$ (cf. [9])

(les G_i étant les groupes de ramification successifs de l'extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$) .

LEMME. - Une condition nécessaire pour qu'il existe une décomposition centrale non triviale du $A[G]$-module B est que p divise la différente $\mathcal{D}(L/K)$ de l'extension L/K .

III. 1. 3. Condition suffisante.

Supposons que p divise la différente $\mathcal{D}(L/K)$; notons K_H le sous-corps de L fixe par H . Deux cas sont possibles :

i) p divise aussi la différente de L/K_H , $\mathcal{D}(L/K_H)$. Toutes les extensions locales de degré $2p$ ont alors un nombre de ramification $t_{\mathfrak{P}}$ supérieur ou égal à $\frac{2p\, e_{K_{\mathfrak{p}}}}{p-1} - 1$ et il n'y a pas d'extension locale totalement ramifiée avec a impair (cf. la remarque d) du paragraphe II. 1). Par suite, d'après II, tous les ordres locaux contiennent l'idempotent $\frac{T}{p}$ et donc $\frac{T}{p} \in \mathcal{O}(B, K[G])$ et B a une décomposition centrale non triviale.

ii) p divise la différente $\mathcal{D}(L/K)$ mais ne divise pas $\mathcal{D}(L/K_H)$. On démontre qu'il existe alors nécessairement une extension locale au-dessus de p , de degré $2p$, totalement ramifiée avec a impair (cf. remarque du §II. 1) . Les seuls systèmes $\mathcal{S} \neq 1$, possibles contiennent $\frac{T(1+\tau)}{2p}$ d'après le théorème de II , il faut donc regarder dans quelles conditions $\frac{T(1+\tau)}{2p}$ appartient aux ordres $\mathcal{O}(B_{\mathfrak{p}}, K_{\mathfrak{p}}[G])$ où $\mathfrak{p}$ décrit l'ensemble des idéaux $\mathfrak{p} \in \mathcal{P}$ au-dessus de 2 .

Si $\mathfrak{p}$ est un idéal au-dessus de 2 , les possibilités pour l'extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ et pour l'ordre $\mathcal{O}(B_{\mathfrak{p}}, K_{\mathfrak{p}}[G])$ sont les suivantes :

a') $\mathfrak{p}$ est non décomposé, c'est-à-dire $D = G$ ou $\mathfrak{p}$ est décomposé en deux idéaux et $D = H$ ou $\mathfrak{p}$ est totalement décomposé et $D = 1$. Dans ces trois cas, $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ est modérément ramifiée ou non ramifiée et

$\mathcal{O}(B_{\mathfrak{p}}, K_{\mathfrak{p}}[G]) = A_{\mathfrak{p}}[G]$.

b') $\mathfrak{p}$ est décomposé en p-idéaux, D est un sous-groupe d'ordre 2 et $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ est une extension cyclique d'ordre 2 .

On choisit pour $\mathfrak{P}$ l'idéal au-dessus de $\mathfrak{p}$ qui correspond au groupe D engendré par 1 et τ , $D = (1, \tau)$. D'après le début du §III (*)

$$\mathcal{O}(B_{\mathfrak{p}}, K_{\mathfrak{p}}[G]) = \bigcap_{0 \le i \le p-1} \sigma^{i} \left[\oplus \sigma^{j} \mathcal{O}(B_{\mathfrak{P}}, k_{\mathfrak{p}}[D]) \right] \sigma^{-i} .$$

On voit que $\frac{T(1+\tau)}{2p} \in \mathcal{O}(B_{\mathfrak{p}}, K_{\mathfrak{p}}[G])$ si et seulement si $\frac{1+\tau}{2} \in \mathcal{O}(B_{\mathfrak{P}}, K_{\mathfrak{p}}[D])$ donc si et seulement si la ramification dans $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ est presque maximale ou encore si et seulement si 2 divise la différente de L/K . Ceci termine la démonstration du théorème cité au début de ce paragraphe en effet dans le cas i) p divise $\mathcal{D}(L/K_H)$ dans le cas ii) $2p$ divise $\mathcal{D}(L/K)$.

On remarquera que si l'on connait précisément tous les nombres de ramification des idéaux au-dessus de 2 et de p d'une extension L/K , on peut donner exactement la décomposition centrale du $A[G]$-module B , par exemple :

PROPRIETE. - Si $2p$ divise la différente de L/K , $\mathcal{D}(L/K)$, et si p ne divise pas la différente $\mathcal{D}(L/K_H)$ la décomposition centrale de B est la suivante :

$$B = \frac{T(1+\tau)}{2p} B \oplus \left(1 - \frac{T(1+\tau)}{2p}\right) B$$ (cf. remarque d) du §II.1 et théorème du II)

III.2 DECOMPOSITION EN SOUS-MODULES INDECOMPOSABLES

THEOREME. - Soit L/K une extension diédrale de corps de nombres, A et B étant les anneaux d'entiers des corps K et L et G le groupe de Galois $G(L/K)$, une condition nécessaire et suffisante pour

<u>le</u> $A[G]$-<u>module</u> B <u>soit décomposable est que l'un des deux diviseurs de l'ordre de</u> G , 2 <u>ou</u> p , <u>divise la différente</u> $\mathcal{D}(L/K)$.

Soit θ un élément de B qui engendre une base normale de L/K on note $M = \{\lambda \in K[G] \ , \ \lambda\cdot\theta \in B\}$, c'est-à-dire le $A[G]$-module à gauche de rang 1 qui vérifie $B = M\cdot\theta$. Nous savons alors que B est un $A[G]$-module décomposable si et seulement si il existe un idempotent e , $e \neq 0$, $e \neq 1$, dans l'ordre à droite de M dans $K[G]$: $\mathcal{O}_d(M, K[G])$. Nous allons, pour démontrer le théorème cité ci-dessus nous intéresser tout d'abord au choix de cet élément θ .

III.2.1. LEMME. - <u>Si</u> K' <u>est un corps local d'anneau des entiers</u> A' , <u>si</u> L' <u>est une extension galoisienne de</u> K' <u>d'anneau des entiers</u> B' <u>et</u> α <u>un élément de</u> B' <u>engendrant une base normale de</u> L'/K' , <u>notons</u> $M_\alpha = \{\lambda \in K'[G] \ , \lambda\alpha \in B'\}$. <u>Il existe un entier positif</u> N <u>tel que si</u> β <u>est un élément de</u> B' <u>vérifiant</u> $v_{L'}(\alpha-\beta) > N$ <u>alors le module</u> $M_\beta = \{\lambda \in K'[G] \ , \ \lambda\beta \in B'\}$ <u>est égal au module</u> M_α ($v_{L'}$ désigne la valuation du corps L') .

<u>Démonstration</u>. - Si e et f désignent respectivement l'indice de ramification et le degré résiduel de L'/K' , on peut choisir une A' base de B' du type $\{E_i\pi^j \ , \ 1 \leq i \leq f \ , \ 0 \leq j \leq e-1\}$ où π est une uniformisante de K' et où $(E_i)_{1\leq i\leq f}$ est une famille d'unités de B' telle que $(\overline{E}_i)_{1\leq i\leq f}$ soit une $\overline{K}'$ base de $\overline{L}'$ (corps résiduel). Pour tout couple i,j il existe alors un élément λ_{ij} de M_α tel que $\lambda_{ij}\alpha = E_i\pi^j$. Les λ_{ij} forment donc une A'-base de M_α . Il existe alors un entier N tel que si $v_{L'}(\alpha-\beta) > N$ pour un β de B' on puisse écrire

$$v_{L'}(\lambda_{ij}\alpha - \lambda_{ij}\beta) > e+1 \ .$$

Ceci entraîne que $\lambda_{ij}\beta$ est un élément de même valuation que $E_i\pi^j$ et s'écrit donc : $\lambda_{ij}\beta = E'_i\pi^j$ avec E'_i unité de B' vérifiant $\overline{E}'_i = \overline{E}_i$. Par suite les λ_{ij} forment une A'-base de M_β et $M_\alpha = M_\beta$.

III.2.2. Choix de l'élément θ de B qui engendre une base normale de L/K .

a) Premier cas. Il existe un idéal $\mathfrak{q}$ de A non décomposé dans L/K , c'est-à-dire il existe une extension locale $L_{\mathfrak{Q}}/K_{\mathfrak{q}}$ de degré $2p$, $\mathfrak{Q}\cap A = \mathfrak{q}$. Alors pour tout idéal $\mathfrak{p}$ de A au-dessus de 2 ou de p nous choisissons dans $B_{\mathfrak{P}}$ $(\mathfrak{P}\cap A = \mathfrak{p})$ un $\theta_{\mathfrak{P}}$ de façon que l'on connaisse le module $M_{\mathfrak{P}}$ de $K_{\mathfrak{p}}[D]$ (D groupe de décomposition de $\mathfrak{P}$ dans L/K) qui vérifie : $B_{\mathfrak{P}} = M_{\mathfrak{P}}\cdot\theta_{\mathfrak{P}}$ (choix précisé dans [5]). De plus, si l'idéal $\mathfrak{q}$ n'est ni au-dessus de p ni au-dessus de 2 , choisissons un $\theta_{\mathfrak{Q}}$ dans $B_{\mathfrak{Q}}$, tel que $B_{\mathfrak{Q}} = A[G]\cdot\theta_{\mathfrak{Q}}$ puisque l'extension $L_{\mathfrak{Q}}/K_{\mathfrak{q}}$ est forcément modérément ramifiée.

D'après le lemme d'approximation, il existe alors un élément θ de B tel que pour tous les $\mathfrak{p}$ cités au-dessus $v_{\mathfrak{P}}(\theta-\theta_{\mathfrak{P}}) > N_{\mathfrak{P}}$ ($N_{\mathfrak{P}}$ entier défini par le lemme précédent).

Ce θ engendre une base normale de L/K , car l'extension $L_{\mathfrak{Q}}/K_{\mathfrak{q}}$ est de degré $2p$ et dans les algèbres $K_{\mathfrak{p}}[D]$ citées ci-dessus, on a $B_{\mathfrak{P}} = M_{\mathfrak{P}}\cdot\theta = M_{\mathfrak{P}}\cdot\theta_{\mathfrak{P}}$, d'après le lemme précédent.

b) Deuxième cas. Pas d'extensions locales de degré $2p$ mais il existe au moins un idéal $\mathfrak{p}$ de A au-dessus de 2 ou de p qui se décompose en deux idéaux $\mathfrak{P}$ et $\overline{\mathfrak{P}}$. Choisissons dans $B_{\mathfrak{P}}$ un élément $\theta_{\mathfrak{P}}$ qui engendre une base normale de $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ et tel que l'on connaisse le $A_{\mathfrak{p}}[H]$-module $M_{\mathfrak{P}}$ vérifiant $B_{\mathfrak{P}} = M_{\mathfrak{P}}\cdot\theta_{\mathfrak{P}}$.

LEMME. - Il existe des entiers N et M tels que si $\theta \in L$ vérifie $v_{\mathfrak{P}}(\theta-\theta_{\mathfrak{p}}) > N$ et $v_{\mathfrak{P}}(\theta) \geq M$ alors θ engendre une base normale de $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ et on a $B_{\mathfrak{P}} = M_{\mathfrak{P}}\cdot\theta = M_{\mathfrak{P}}\cdot\theta_{\mathfrak{P}}$ dans $K_{\mathfrak{p}}[H]$ comme dans le lemme du 2.1.

Dans ce cas, on choisit donc θ grâce au lemme d'approximation en lui imposant les mêmes conditions que dans le premier cas, plus les conditions du lemme du 2.2.

c) Troisième cas. Pas d'extensions locales de degré $2p$ et tous les idéaux au-dessus de 2 et de p se décomposent en p idéaux. Alors il est facile de voir que tout θ de B qui engendre une base normale de L/K engendre aussi une base normale de toutes les extensions locales de degré 2. Dans ce troisième cas, θ est choisi de cette façon là.

Remarque. Dans les deux premiers cas, chaque fois que l'extension locale est soit modérément ramifiée, soit non ramifiée le $\theta_{\mathfrak{P}}$ choisi localement est tel que $B_{\mathfrak{P}} = A_{\mathfrak{p}}[D] \cdot \theta_{\mathfrak{P}}$ c'est-à-dire que $M_{\mathfrak{P}} = A_{\mathfrak{p}}[D]$.

Récapitulons : pour un idéal $\mathfrak{p}$ donné de A, si $\mathfrak{P}$ est un idéal de B, $\mathfrak{P} \cap A = \mathfrak{p}$, de groupe de décomposition D et si $\mathcal{R}$ est un système de représentants de G/D, on note $B_{\mathfrak{p}} = A_{\mathfrak{p}}[G] \underset{A[G]}{\otimes} B$ et on a

$$B_{\mathfrak{p}} = \bigoplus_{g \in \mathcal{R}} gB_{\mathfrak{P}} .$$

Si θ est choisi comme précédemment pour ce θ on pose $B = M \cdot \theta$ et $M_{\mathfrak{p}} = A_{\mathfrak{p}}[G] \underset{A[G]}{\otimes} M$ et si $B_{\mathfrak{P}} = M_{\mathfrak{P}} \cdot \theta$ on a : $M = \bigcap_{\mathfrak{p} \in \mathcal{P}} M_{\mathfrak{p}}$ et on a alors quatre cas possibles suivant les ramifications de l'idéal $\mathfrak{p}$.

α) $\mathfrak{p}$ est non décomposé alors $B_{\mathfrak{p}} = B_{\mathfrak{P}}$ et $M_{\mathfrak{p}} = M_{\mathfrak{P}}$.

β) $\mathfrak{p}$ est décomposé en deux idéaux : $M_{\mathfrak{p}} = M_{\mathfrak{P}} \oplus \tau M_{\mathfrak{P}}$.

γ) $\mathfrak{p}$ est décomposé en p idéaux : $M_{\mathfrak{p}} = \bigoplus_{0 \leq i \leq p-1} \sigma^i M_{\mathfrak{P}}$.

δ) $\mathfrak{p}$ est totalement décomposé : $B_{\mathfrak{p}} = M_{\mathfrak{p}} = A_{\mathfrak{p}}[G]$.

Rappelons que B est décomposable si et seulement si il existe un idempotent e de $K[G]$ distinct de 1 et de 0 dans $\mathcal{O}_d(M, K[G])$ c'est-à-dire si il existe un idempotent e, $e \neq 1$, $e \neq 0$, vérifiant $e \in \mathcal{O}_d(M_{\mathfrak{p}}, K_{\mathfrak{p}}[G])$ pour tout idéal $\mathfrak{p} \in \mathcal{P}$.

III. 2. 3. Condition suffisante pour que le $A[G]$-module M soit décomposable.

Rappelons tout d'abord le résultat suivant de Reiner [4] p. 580. Soit $\mathcal{P}_1$ l'ensemble des idéaux premiers de A qui sont soit au-dessus de 2 soit au-dessus de p. Pour tout $\mathfrak{p}$ de $\mathcal{P}_1$ on note $\check{A}_{\mathfrak{p}}$ le localisé de A en $\mathfrak{p}$. $\check{M}_{\mathfrak{p}} = \check{A}_{\mathfrak{p}} \otimes_A M$, $\check{A} = \bigcap_{\mathfrak{p}\in\mathcal{P}_1} \check{A}_{\mathfrak{p}}$ et $\check{M} = \check{A} \otimes_A M$ c'est-à-dire $\check{M} = \bigcap_{\mathfrak{p}\in\mathcal{P}_1} \check{M}_{\mathfrak{p}}$.

D'après [4], M est un $A[G]$-module décomposable si et seulement si $\check{M}$ est un $\check{A}[G]$-module décomposable.

PROPOSITION. - Soit M est un $A[G]$-module de rang 1 contenu dans $K[G]$, il est décomposable si et seulement si il existe un idempotent e de $K[G]$, $e \neq 1$, $e \neq 0$ appartenant à tous les ordres $\mathcal{O}_d(M_{\mathfrak{p}}, K_{\mathfrak{p}}[G])$ pour $\mathfrak{p} \in \mathcal{P}_1$.

En effet, si pour tout $\mathfrak{p} \in \mathcal{P}_1$, $e \in \mathcal{O}_d(M_{\mathfrak{p}}, K_{\mathfrak{p}}[G])$ on a $\check{M}_{\mathfrak{p}} e \subset \check{M}_{\mathfrak{p}}$, on en déduit $e \in \mathcal{O}_d(\check{M}, K[G])$ et d'après le théorème de Reiner M est décomposable.

Réciproquement, si il existe $e \in \mathcal{O}_d(\check{M}, K[G])$, $e \neq 1$, $e \neq 0$ c'est que $e \in \mathcal{O}_d(\check{M}_{\mathfrak{p}}, K[G])$ pour tout $\mathfrak{p}$ de $\mathcal{P}_1$ et par complétion $M_{\mathfrak{p}} e \subset M_{\mathfrak{p}}$ pour tout $\mathfrak{p}$ de $\mathcal{P}_1$.

LEMME. - Si 2 divise la différente $\mathcal{D}(L/K)$, B est un $A[G]$-module décomposable.

Démonstration. Nous allons montrer que si 2 divise la différente de L/K, l'idempotent $\frac{1+\tau}{2}$ appartient à tous les ordres $\mathcal{O}_d(M_{\mathfrak{p}}, K_{\mathfrak{p}}[G])$ pour tout $\mathfrak{p} \in \mathcal{P}_1$.

Regardons tout d'abord les idéaux $\mathfrak{p}$ au-dessus de 2. Si 2 divise la différente de L/K, toutes les extensions locales relatives à des $\mathfrak{p}$ au-dessus de 2 sont de degré 2 et elles sont ramifiées avec une ramification presque maximale. (cf. [5], [2], [10]).

Pour ces extensions, on a :

$$M_{\mathfrak{p}} = \bigoplus_{0\leq i\leq p-1} \sigma^i M_{\mathfrak{P}}$$

et d'après [2] si la ramification est presque maximale, on a $\frac{1+\tau}{2} \in \mathcal{O}_d(M_{\mathfrak{P}}, K_{\mathfrak{p}}(D)) = \mathcal{O}(B_{\mathfrak{P}}, K_{\mathfrak{p}}[D])$. Par suite, pour ces idéaux $\mathfrak{p}$, $\frac{1+\tau}{2} \in \mathcal{O}_d(M_{\mathfrak{p}}, K_{\mathfrak{p}}[G])$.

Regardons alors les extensions locales pour des idéaux $\mathfrak{p}$ au-dessus de p .

1er cas. - $M_{\mathfrak{p}} = M_{\mathfrak{P}}$. L'extension locale est soit modérément ramifiée et d'après le choix de $\theta_{\mathfrak{P}}$: $M_{\mathfrak{P}} = A_{\mathfrak{p}}[G]$ (voir remarque 2.2), et donc $\frac{1+\tau}{2} \in \mathcal{O}_d(A_{\mathfrak{p}}[G], K_{\mathfrak{p}}[G])$; soit ramifiée et toujours d'après le choix de $\theta_{\mathfrak{P}}$, on vérifie d'après [5] que $\frac{1+\tau}{2} \in \mathcal{O}_d(M_{\mathfrak{P}}, K_{\mathfrak{p}}[G])$.

2ème cas. - $M_{\mathfrak{p}} = M_{\mathfrak{P}} \oplus \tau M_{\mathfrak{P}}$, l'extension locale est de degré p . D'après le choix du $\theta_{\mathfrak{P}}$, on vérifie que $M_{\mathfrak{P}}\tau = \tau M_{\mathfrak{P}}$ et donc que $\frac{1+\tau}{2} \in \mathcal{O}_d(M_{\mathfrak{p}}, K_{\mathfrak{p}}[G])$.

3ème cas. - $M_{\mathfrak{p}} = \bigoplus_{0\leq i\leq p-1} \sigma^i M_{\mathfrak{P}}$, l'extension locale est de degré 2, donc modérément ramifiée ; par suite, $\frac{1+\tau}{2} \in \mathcal{O}(B_{\mathfrak{P}}, K_{\mathfrak{p}}[D]) = \mathcal{O}_d(M_{\mathfrak{P}}, K_{\mathfrak{p}}[D])$ et on en déduit $\frac{1+\tau}{2} \in \mathcal{O}_d(M_{\mathfrak{p}}, K_{\mathfrak{p}}[G])$.

En utilisant la proposition précédente (§2.3), on a démontré que si 2 divise la différente de L/K , B est un $A[G]$-module décomposable.

LEMME. - Si p divise la différente $\mathcal{D}(L/K)$, B est un $A[G]$-module décomposable.

Démonstration. - Nous allons montrer que si p divise la différente de L/K , l'idempotent $e = \left(\frac{(p-1)T}{2p} - (\sigma+\sigma^2+\ldots+\sigma^{\frac{p-1}{2}})\right)(1+\tau)$ appartient à

tous les ordres $\mathcal{O}_d(M_{\mathfrak{p}}, K_{\mathfrak{p}}[G])$ pour tout $\mathfrak{p} \in \mathcal{P}_1$.

Regardons tout d'abord les idéaux $\mathfrak{p}$ au-dessus de p , si p divise la différente de L/K , toutes les extensions locales relatives à des $\mathfrak{p}$ au-dessus de p sont de degré $2p$ ou p et elles sont ramifiées avec une ramification presque maximale (cf. [5]) . Donc deux cas se présentent :

1er cas. - $M_{\mathfrak{p}} = M_{\mathfrak{P}}$. D'après le choix de $\theta_{\mathfrak{P}}$ et d'après les résultats de [5] donnant une A-base de $M_{\mathfrak{P}}$ on démontre que $e \in \mathcal{O}_d(M_{\mathfrak{p}}, K_{\mathfrak{p}}[G])$.

2ème cas. - $M_{\mathfrak{p}} = M_{\mathfrak{P}} + \tau M_{\mathfrak{P}}$ l'extension locale est de degré p , ramifiée avec une ramification presque maximale ; on sait d'après le choix de $\theta_{\mathfrak{P}}$ et d'après [5] que $M_{\mathfrak{P}} \frac{T}{p} \subset M_{\mathfrak{P}}$, que $M_{\mathfrak{P}} \cdot A_{\mathfrak{p}}[H] \subset M_{\mathfrak{P}}$ et que $M_{\mathfrak{P}}\tau = \tau M_{\mathfrak{P}}$. Donc $e \in \mathcal{O}_d(M_{\mathfrak{p}}, K_{\mathfrak{p}}[G])$.

Pour les idéaux $\mathfrak{p}$ au-dessus de 2 , on remarque que $e \in A_{\mathfrak{p}}[G]$. D'autre part, soit l'extension locale est modérément ramifiée et par suite $M_{\mathfrak{p}} e \subset M_{\mathfrak{p}}$, soit elle est de degré 2 et il est facile de vérifier que $M_{\mathfrak{p}} e \subset M_{\mathfrak{p}}$ puisqu'on a une base de $M_{\mathfrak{P}}$ d'après [5] .

III. 2. 4. Condition nécessaire pour que le $A[G]$-module B soit décomposable.

PROPOSITION (cf. [8]). - *Soit A un anneau intègre de caractéristique 0 , K son corps des quotients et G un groupe fini, Card $G = n$. Si $e = \sum_{g \in G} a_g g$ est un idempotent de $K[G]$, $e \neq 0$ et $e \neq 1$ alors on a : $a_1 = \frac{q}{n}$ avec q un entier, $0 < q < n$.*

En particulier, si G est un groupe diédral, a_1 , mis sous forme irréductible, admet forcément un 2 ou un p au dénominateur ou les deux.

LEMME. - *Si ni 2 ni p ne divise la différente $\mathcal{D}(L/K)$, B est un $A[G]$-module indécomposable.*

<u>Démonstration</u>. Pour démontrer ce lemme nous utiliserons la proposition précédente et nous montrerons qu'il ne peut pas exister d'idempotent e, $e \neq 1$, $e \neq 0$, tel que $e \in \mathcal{O}_d(M_{\mathfrak{p}}, K_{\mathfrak{p}}[G])$ pour tout $\mathfrak{p} \in \mathcal{P}_1$ car pour cet idempotent e, $e = \sum_{g \in G} a_g g$, a_1 ne peut avoir ni 2 ni p au dénominateur.

En effet, si 2 ne divise pas la différente $\mathcal{D}(L/K)$, c'est que les extensions locales au-dessus de 2 sont

- soit de degré 2 avec une ramification qui n'est pas presque maximale. Mais alors si on écrit $M_{\mathfrak{p}} = \bigoplus_{0 \leq i \leq p-1} \sigma^i M_{\mathfrak{P}}$, ni $M_{\mathfrak{P}}$ ni l'ordre $\mathcal{O}(M_{\mathfrak{P}}, K_{\mathfrak{p}}[D]) = \mathcal{O}(B_{\mathfrak{P}}, K_{\mathfrak{p}}[D])$ ne contiennent $\frac{1+\tau}{2}$ et comme $a_1 + a_\tau \tau$ (de l'écriture $e = \sum_{g \in G} a_g g$) est dans $M_{\mathfrak{P}}$, a_1 ne peut avoir de 2 au dénominateur ;

- soit de degré autre que 2, mais elles sont alors modérément ramifiées et a_1 n'aura pas non plus de 2 au dénominateur.

On montre de la même façon que si p ne divise pas la différente $\mathcal{D}(L/K)$, a_1 ne peut avoir de p au dénominateur et par suite B est un $A[G]$-module indécomposable.

La démonstration du théorème cité au début du paragraphe III.2 résulte immédiatement des lemmes des paragraphes 2.3 et 2.4 précédents.

Remarquons que la donnée précise, pour une extension L/K, des nombres de ramification des extensions locales permet souvent d'écrire une décomposition en sous-$A[G]$-modules indécomposables du $A[G]$-module M.

Par exemple, si p ne divise pas $\mathcal{D}(L/K_H)$ et si 2 divise $\mathcal{D}(L/K)$ une décomposition de M en sous-$A[G]$-modules indécomposables est $M = M\frac{1+\tau}{2} \oplus M\frac{1-\tau}{2}$.

III. 2. 5. Etude du cas $K = \mathbb{Q}$.

Dans le cas d'une extension diédrale $L/\mathbb{Q}$, les résultats se simplifient un peu, nous les résumons de la manière suivante, en notant L_H le sous-corps de L fixe par le sous-groupe H .

- Si 2 ne divise pas $\mathcal{D}(L/\mathbb{Q})$ et si p ne divise pas $\mathcal{D}(L/\mathbb{Q})$, B est un $A[G]$-module indécomposable.

- Si 2 ne divise pas $\mathcal{D}(L/\mathbb{Q})$, si p divise $\mathcal{D}(L/\mathbb{Q})$ mais ne divise pas $\mathcal{D}(L/L_H)$, B est indécomposable centralement, mais B est un $A[G]$-module décomposable.

- Si 2 ne divise pas $\mathcal{D}(L/\mathbb{Q})$ et si p divise $\mathcal{D}(L/L_H)$, $B = \frac{T}{p}B + (1-\frac{T}{p})B$ est la décomposition centrale de B .

- Si 2 divise $\mathcal{D}(L/\mathbb{Q})$ et que p divise $\mathcal{D}(L/L_H)$, $B = \frac{T(1+\tau)}{2p}B \oplus \frac{T(1-\tau)}{2p}B \oplus (1-\frac{T}{p})B$ est la décomposition centrale de B et $M = M\frac{T(1+\tau)}{2p} \oplus M\frac{T(1-\tau)}{2p} \oplus M(1-\frac{T}{p})(\frac{1+\tau}{2}) \oplus M(1-\frac{T}{p})(\frac{1-\tau}{2})$ est une décomposition totale de M .

- Si 2 divise $\mathcal{D}(L/\mathbb{Q})$ et que p ne divise pas $\mathcal{D}(L/L_{\mathbb{Q}})$, B est indécomposable centralement et $M = M\frac{1+\tau}{2} \oplus M\frac{1-\tau}{2}$ est une décomposition de M en sous-$A[G]$-modules indécomposables.

- Si $2p$ divise $\mathcal{D}(L/\mathbb{Q})$ et que p ne divise pas $\mathcal{D}(L/L_H)$, $B = \frac{T(1+\tau)}{2p}B \oplus (1-\frac{T(1+\tau)}{2p})B$ est la décomposition centrale de B et $M = M\frac{T(1+\tau)}{2p} \oplus M(1-\frac{T}{p})(\frac{1+\tau}{2}) \oplus M\frac{1-\tau}{2}$ est une décomposition totale de M .

BIBLIOGRAPHIE

[1] A.M. BERGE - Anneaux d'entiers et ordres associés. Thèse de doctorat Bordeaux, avril 1979.

[2] F. BERTRANDIAS - Décomposition de Galois-module des entiers d'une extension cyclique de degré premier d'un corps de nombres ou d'un corps local. Extrait des annales de l'Institut Fourier, Tome XXIX, Fascicule 1, pp. 33-48 (1979).

[2bis] F. BERTRANDIAS - Décomposition du Galois-module des entiers d'une p-extension cyclique d'un corps local. Séminaire de théorie des nombres, Grenoble, nov. 1977.

[3] Z.I. BOREVICH et S.V. VOSTOKOV - The ring of integral elements of an extension of prime degree of a local field as a Galois-module. Zap. Nauĉn. Sem. Leningrad. Otdel. Mat. Inst. Steklov (LOMI) 31, pp. 24-37 (1973).

[4] C.W. CURTIS and I. REINER - Representation theory of finish groups and associative algebras. Interscience, New York (1962).

[5] 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 3e cycle, Grenoble (1972).

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

[7] Y. MIYATA - On the module structure of a p-extension over a p-adic number field. Nagoya Math. J. 77 (1980), pp. 13-23.

[8] I. REINER - K.W. ROGGENKAMP - Integral representations. Lecture Notes 744 Springer (1979), p. 73.

[9] J.P. SERRE - Corps locaux. Hermann (1962).

[9bis] J.P. SERRE - Représentations linéaires de groupes finis. Hermann (1971).

[10] S.V. VOSTOKOV - The ring of integral elements of an algebraic number field as a Galois-module. Zap. Nauĉn, Sem. Leningrad Otdel. Mat. Inst. Steklov (LOMI), 71 (1977), pp. 80-84, 284.