Nicole Moser

Représentations entières de certains groupes finis. 3e partie : Représentations entières des groupes diédraux d'ordre $2p$

Séminaire de théorie des nombres de Grenoble, tome 3 (1973-1974), exp. n° 7, p. 1-14
<http://www.numdam.org/item?id=STNG_1973-1974__3__A7_0>

Séminaire de Théorie des Nombres
28 février 1974
Grenoble

REPRESENTATIONS ENTIERES DE CERTAINS GROUPES FINIS

- 3e partie -

REPRESENTATIONS ENTIERES DES GROUPES DIEDRAUX D'ORDRE 2p

par Nicole MOSER

I. INTRODUCTION.

Soit G un groupe diédral d'ordre $2p$, p nombre premier impair ; il est défini par deux générateurs σ et τ, liés par les relations :

$$\tau^2 = \sigma^p = 1 \quad \text{et} \quad \tau\sigma = \sigma^{-1}\tau .$$

Dans cet exposé, nous allons donner la classification des $\mathbb{Z}[G]$-modules sans torsion et de type fini sur $\mathbb{Z}$, établie par M.P. Lee dans [4], en utilisant une méthode de démonstration plus synthétique, où le foncteur Ext est remplacé par le foncteur H^1. Nous utiliserons le théorème suivant dû à Reiner (cf. L. Bouvier [1]) :

THEOREME 1. *Soit M un $\mathbb{Z}[G]$-module, sans torsion et de type fini sur $\mathbb{Z}$. Les deux assertions suivantes sont équivalentes* :

a) *M est $\mathbb{Z}[G]$-indécomposable ;*

b) *$M_{2p} = \mathbb{Z}_{(2p)} \otimes_{\mathbb{Z}} M$ est $\mathbb{Z}_{(2p)}[G]$-indécomposable.*
($\mathbb{Z}_{(2p)}$ est le localisé de $\mathbb{Z}$ en $2p$).

Notations : Pour toute la suite, S désignera soit $\mathbb{Z}$, soit l'un des localisés $\mathbb{Z}_{(2)}$, $\mathbb{Z}_{(p)}$ ou $\mathbb{Z}_{(2p)}$.

Posons : $\Phi_p(X) = 1+X+\ldots+X^{p-1}$

ζ : une racine primitive p-ième de l'unité

$A = S[\zeta]$

$K = \mathbb{Q}(\zeta)$

K_o : le sous-corps de K fixe par τ

$A_o = A \cap K_o$

h : le nombre de classes de A_o .

Désignons par $\mathfrak{a}$ le A-module $A[\tau]$, muni du produit défini par :

$$\tau(\lambda_1+\lambda_2\tau) = \bar{\lambda}_2 + \bar{\lambda}_1\tau ,$$

où les λ_i sont des éléments de A , et les $\bar{\lambda}_i$ les conjugués complexes des λ_i . Ainsi $\mathfrak{a}$ possède une structure d'algèbre, que l'on peut prolonger en structure de S[G]-module, en définissant l'action de σ comme la multiplication par ζ . Il est clair que l'application

$$\begin{aligned} \varphi : S[G] &\longrightarrow \mathfrak{a} \\ \sigma &\longmapsto \zeta \\ \tau &\longmapsto \tau \end{aligned}$$

se prolonge en S[G]-homomorphisme surjectif, de noyau $\Phi_p(\sigma)S[G]$. Donc $\mathfrak{a}$ et $S[G]/\Phi_p(\sigma)S[G]$ sont des S[G]-modules isomorphes.

Soit M un S[G]-module, sans torsion et de type fini sur S .

Posons :

$$M' = \{m \in M \mid \Phi_p(\sigma)m = 0\} .$$

On peut considérer M' comme un $\mathfrak{a}$-module. Quant au quotient $M^* = M/M'$, il est annulé par $\sigma - 1$; donc sa structure en tant que S[G]-module est déterminée par celle de $S[\langle\tau\rangle]$-module. La classification des S[G]-modules s'étudie donc en trois étapes :

a) détermination des $\mathfrak{a}$-modules indécomposables ;

b) détermination des $S[\langle\tau\rangle]$-modules indécomposables ;

c) détermination des extensions indécomposables d'un $S[\langle\tau\rangle]$-module par un $\mathfrak{a}$-module.

II. DETERMINATION DES $\mathfrak{A}$-MODULES INDECOMPOSABLES.

Donnons d'abord la définition suivante :

DEFINITION. *Soient* B *un anneau unitaire, et* C *un sous-anneau de* B . *Un* B-*module est dit irréductible relativement à* C *s'il ne contient pas de sous*-B-*module non trivial facteur direct en tant que* C-*module*.

PROPOSITION 1. *Tout* $\mathfrak{A}$-*module indécomposable est irréductible relativement à* A .

La démonstration de cette proposition nécessite un lemme :

LEMME. *Tout* $\mathfrak{A}$-*module qui est* A-*projectif est aussi* $\mathfrak{A}$-*projectif.*

Démonstration du lemme : Soit M un $\mathfrak{A}$-module qui est projectif sur A . Désignons par $j : A \to \mathfrak{A}$ l'injection canonique de A dans $\mathfrak{A}$. Comme $\mathfrak{A}$ est libre et de type fini sur A , $M_j = \mathfrak{A} \otimes_A M$ est $\mathfrak{A}$-projectif. (cf. Cartan-Eilenberg, prop. 6.1 [2]). Considérons alors la suite exacte :

$$0 \to \operatorname{Ker} g \to M_j \underset{g}{\to} M \to 0$$

où g est l'application de M_j dans M définie par :

$$g(\lambda \otimes m) = \lambda m$$

pour tout λ de $\mathfrak{A}$ et tout m de M .

On vérifie facilement que l'application $f : M \to M_j$

$$m \longmapsto 1 \otimes \frac{\zeta}{\zeta+\bar{\zeta}} m + \tau \otimes \frac{\zeta}{\zeta+\bar{\zeta}} \tau m$$

est une section de g . Donc M , facteur direct d'un module $\mathfrak{A}$-projectif, est $\mathfrak{A}$-projectif. ∎

Démonstration de la proposition 1 : Soit M un $\mathfrak{A}$-module, et soit N un sous $\mathfrak{A}$-module non trivial, facteur direct de M en tant que A-module. Comme A est un anneau de Dedekind, N est sans torsion et de type fini sur A , donc il est A-projectif. D'après le lemme, N est $\mathfrak{a}$-projectif : c'est un facteur direct de M en tant que $\mathfrak{a}$-module, et M n'est pas un $\mathfrak{a}$-module indécomposable. ■

PROPOSITION 2. <u>Tout $\mathfrak{a}$-module irréductible par rapport à</u> A <u>est isomorphe à un idéal ambige de</u> A/A_o .

<u>Démonstration</u> : Considérons l'algèbre $\tilde{\mathfrak{a}} = K_o \otimes_{A_o} \mathfrak{a}$; elle est isomorphe à l'algèbre de matrices $\mathfrak{M}_2(K_o)$, donc c'est une algèbre simple et centrale, et tous les $\tilde{\mathfrak{a}}$-modules simples à gauche sont isomorphes ; parmi ceux-ci se trouve $K(1+\tau)$.

Donc tout $\mathfrak{a}$-module irréductible par rapport à A est un A-module de rang 1 , invariant par τ : il est isomorphe à un idéal ambige de A/A_o . ■

PROPOSITION 3. <u>Deux idéaux ambiges de</u> A/A_o <u>sont $\mathfrak{a}$-isomorphes si et seulement si l'un est produit de l'autre par un élément de</u> K_o .

<u>Démonstration</u> : Deux idéaux $\mathfrak{a}$-isomorphes sont A-isomorphes, donc dans la même classe d'idéaux de A . Le coefficient multiplicatif doit être invariant par τ . ■

<u>Conclusion</u> : Dans A/A_o , il y a au plus un idéal ramifié, celui au-dessus de p . Donc les idéaux ambiges sont les étendus des idéaux de A_o , et leur produit par $1-\zeta$.

Si S est l'un des localisés $\mathbb{Z}_{(2)}$, $\mathbb{Z}_{(p)}$, ou $\mathbb{Z}_{(2p)}$, A_o est principal. Il y a donc deux $\mathfrak{a}$-modules indécomposables, A et $(1-\zeta)A$.

Si $S = \mathbb{Z}$, soient h le nombre de classes de A_o , et $\{\mathfrak{A}_i\}_{1\leq i\leq h}$ un système de représentants des classes de A_o . A isomorphisme près, il y a $2h$ $\mathfrak{a}$-modules indécomposables :

$$\mathfrak{A}_i A \quad \text{et} \quad (1-\zeta)\mathfrak{A}_i A \quad \text{avec} \quad 1\leq i\leq h .$$

Tout $\mathfrak{a}$-module est donc isomorphe à une somme directe :

$$\mathfrak{A}_{i_1} A \oplus \dots \oplus \mathfrak{A}_{i_k} A \oplus (1-\zeta)\mathfrak{A}_{i_{k+1}} A \oplus \dots \oplus (1-\zeta)\mathfrak{A}_{i_{k+\ell}} A$$

où les indices i_j appartiennent à l'ensemble $\{1,\dots,h\}$. Il est caractérisé, à isomorphisme près, par les entiers k et ℓ , et la classe dans A_o de l'idéal $\prod_{j=1}^{k+\ell} \mathfrak{A}_{i_j}$.

III. DETERMINATION DES $S[\langle\tau\rangle]$-MODULES INDECOMPOSABLES.

Désignons par :

S_1 l'ensemble S sur lequel τ agit trivialement,

S_2 l'ensemble S sur lequel τ agit comme la multiplication par -1

et S_3 $S[\langle\tau\rangle]$ lui-même.

D'après les résultats de Reiner, exposés par D. Duval dans [3], si $S = \mathbb{Z}$, $\mathbb{Z}_{(2)}$ ou $\mathbb{Z}_{(2p)}$, il y a trois $S[\langle\tau\rangle]$-modules indécomposables, S_1 , S_2 , S_3 . Par contre si $S = \mathbb{Z}_{(p)}$, il n'y en a que deux, à isomorphisme près, S_1 et S_2 .

IV. EXTENSIONS DES $S[\langle\tau\rangle]$-MODULES PAR DES $\mathcal{O}$-MODULES.

Soient M^* un $S\langle\tau\rangle$-module, et M' un $\mathcal{O}$-module : ce sont en particulier deux $S[G]$-modules. Une extension M de M^* par M' est définie par une suite exacte de $S[G]$-modules :

$$0 \to M' \to M \to M^* \to 0 ,$$

qui est une suite scindée de S-modules.

Deux extensions M_1 et M_2 de M^* par M' sont équivalentes s'il existe entre elles un $S[G]$-isomorphisme β tel que le diagramme suivant soit commutatif :

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r] \arrow[d, "1_{M'}"] & M_1 \arrow[r] \arrow[d, "\beta"] & M^* \arrow[r] \arrow[d, "1_{M^*}"] & 0 \\
0 \arrow[r] & M' \arrow[r] & M_2 \arrow[r] & M^* \arrow[r] & 0
\end{tikzcd}$$

Chaque classe d'équivalence d'extensions est caractérisée par un élément ε de $H^1(G,T_S)$, où $T_S = \mathrm{Hom}_S(M^*,M')$ sur lequel G agit de la manière suivante :

$$\begin{aligned} g : T_S &\longrightarrow T_S \\ t &\longmapsto gtg^{-1} \end{aligned} \quad . \text{ (cf. [3])}$$

Pour construire un représentant de cette classe d'équivalence, on munit la somme directe de S-modules $M' \oplus M^*$ d'une structure de S[G]-module, à l'aide d'un cocycle $\lambda : G \to T_S$ d'image ε dans $H^1(G,T_S)$:

$$g(x,y) = (gx + \lambda_g(gy), gy)$$

pour tout g de G , tout x de M' et tout y de M^* .

IV. 1. Calcul de $H^1(G,T_S)$, lorsque M' et M^* sont indécomposables.

PROPOSITION 4. Pour $S = \mathbb{Z}_{(2p)}$:

$$H^1(G,\mathrm{Hom}_S(S_1,A)) \simeq H^1(G,\mathrm{Hom}_S(S_2,(1-\zeta)A)) \simeq \{0\}$$

$$H^1(G,\mathrm{Hom}_S(S_1,(1-\zeta)A)) \simeq H^1(G,\mathrm{Hom}_S(S_2,A)) \simeq \mathbb{Z}/p\mathbb{Z}$$

$$H^1(G,\mathrm{Hom}_S(S_3,A)) \simeq H^1(G,\mathrm{Hom}_S(S_3,(1-\zeta)A)) \simeq \mathbb{Z}/p\mathbb{Z}$$

Démonstration : Il est facile de voir que chacun de ces groupes de cohomologie comporte 1 , p ou p^2 éléments. En effet, le sous-groupe cyclique $H = \langle\sigma\rangle$ est un sous-groupe distingué de G , donc on peut construire la suite exacte :

$$0 \longrightarrow H^1(G/H,T_S^H) \xrightarrow{\mathrm{Inf}} H^1(G,T_S) \xrightarrow{\mathrm{Res}} H^1(H,T_S)$$

où T_S désigne l'un des groupes d'homomorphismes de l'énoncé. On vérifie que dans chacun des cas, σ agit sur T_S comme la multiplication par ζ ; donc l'ensemble des points de T_S fixes par H , T_S^H , est réduit à 0 , et la restriction de $H^1(G,T_S)$ à $H^1(H,T_S)$ est une injection. Comme H est cyclique, ce dernier groupe se calcule facilement :

$$H^1(H,T_S) \simeq \mathrm{Ker}\,\Phi_p(\sigma)/(1-\sigma)T_S \simeq T_S/(1-\zeta)T_S \;.$$

Lorsque M^* est égal à S_1 ou S_2, T_S est un $S[H]$-module isomorphe à M', donc $H^1(H,T_S) = \mathbb{Z}/p\mathbb{Z}$. Lorsque M^* vaut S_3, T_S est $S[H]$-isomorphe à $M' \times M'$, et l'on obtient $H^1(H,T_S) = (\mathbb{Z}/p\mathbb{Z})^2$.

Calculons complètement $H^1(G,\mathrm{Hom}_S(S_2,A))$. Comme S_2 est un S-module de rang 1, $\mathrm{Hom}_S(S_2,A)$ est S-isomorphe à A ; l'action de σ correspond à la multiplication par ζ, et celle de τ à l'opposée de la conjugaison complexe ; notons $\hat{A}$ cette structure de $S[G]$-module. Nous avons donc à déterminer $H^1(G,\hat{A})$.

Soit u un élément de $Z^1(G,\hat{A})$:

$$u(gg') = gu(g') + u(g)$$

quels que soient g et g' dans G. Posons $u(\tau) = \alpha$ et $u(\sigma) = \beta$, et transcrivons les relations liant les générateurs de G :

$$u(\tau^2) = 0 = \tau u(\tau) + u(\tau) = -\bar{\alpha} + \alpha$$
$$u(\sigma^2) = \sigma u(\sigma) + u(\sigma) = (\zeta+1)\beta .$$

De proche en proche :

$$u(\sigma^i) = \sigma u(\sigma^{i-1}) + u(\sigma) = (\zeta^{i-1}+\zeta^{i-2}+\ldots+1)\beta .$$

Donc, quel que soit β, $u(\sigma^p) = 0$.

$$u(\sigma\tau) = \sigma u(\tau) + u(\sigma) = \zeta\alpha + \beta$$
$$\begin{aligned} u(\tau\sigma^{p-1}) &= \tau u(\sigma^{p-1}) + u(\tau) \\ &= -\overline{(\zeta^{p-2}+\ldots+1)}\bar{\beta} + \alpha \\ &= \zeta\bar{\beta} + \alpha . \end{aligned}$$

Donc, les relations à vérifier par α et β se résument en :

(i) $\alpha - \bar{\alpha} = 0$

(ii) $(\zeta-1)\alpha = \zeta\bar{\beta} - \beta = (\zeta-1)\bar{\beta} + \bar{\beta} - \beta$.

Comme l'idéal au-dessus de p, dans A, est principal, la condition (ii) impose à β de vérifier

$$\bar{\beta} - \beta \in (\zeta-1)A .$$

Les éléments 1 et ζ constituent une A_o-base de A ; posons :

$$\beta = \lambda + \mu\zeta \qquad \lambda \text{ et } \mu \text{ dans } A_o$$
$$\bar{\beta} = \lambda + \mu\bar{\zeta} \ .$$

Donc :

$$\begin{aligned} \bar{\beta} - \beta &= \mu(\bar{\zeta}-\zeta) = \mu\zeta(\zeta^{p-2}-1) \\ &= \mu\zeta(\zeta-1)(\zeta^{p-3}+\ldots+1) \ , \end{aligned}$$

et $\bar{\beta} - \beta$ appartient toujours à $(\zeta-1)A$. D'après (ii), on obtient l'égalité :

$$\begin{aligned} \alpha &= \lambda + \mu\zeta^{p-1} - \mu\zeta(\zeta^{p-2}+\zeta^{p-1}) \\ &= \lambda + \mu\zeta^{p-1} - \mu\zeta^{p-1} - \mu = \lambda - \mu \in A_o \ . \end{aligned}$$

Pour déterminer un cocycle, il suffit donc de se donner sa valeur β en σ : l'égalité (ii) permet de calculer α , qui vérifie toujours (i). On obtient donc le $\mathbb{Z}$-homomorphisme :

$$Z^1(G,\hat{A}) \simeq \hat{A} \ .$$

Un cobord v de $B^1(G,\hat{A})$ est tel qu'il existe un $a \in A$ vérifiant pour tout g de G :

$$v(g) = g.a - a \ .$$

L'image de σ par un cobord est donc de la forme $(\zeta-1)a$, et l'isomorphisme de $Z^1(G,\hat{A})$ sur $\hat{A}$ transforme $B^1(G,\hat{A})$ en $(1-\zeta)\hat{A}$. D'où :

$$H^1(G,\hat{A}) \simeq \hat{A}/(1-\zeta)\hat{A} \simeq \mathbb{Z}/p\mathbb{Z} \ .$$

On termine la démonstration, pour les autres cas, à l'aide de calculs analogues. ■

PROPOSITION 5. Supposons $S = \mathbb{Z}_{(2p)}$, et soient M' un $\mathfrak{a}$-module indécomposable, et M^* un $S[\langle\tau\rangle]$-module indécomposable. Posons $T_S = \mathrm{Hom}_S(M^*,M')$. Si $H^1(G,T_S)$ n'est pas nul, toutes les extensions de M^* par M' correspondant à des éléments non nuls de $H^1(G,T_S)$ sont des $S[G]$-modules isomorphes.

Démonstration : Soit $\tilde{\beta}$ un élément non nul de $\mathbb{Z}/p\mathbb{Z}$; comme $\mathbb{Z}/p\mathbb{Z}$ est isomorphe à $M'/(1-\zeta)M'$, pour construire une extension M associée à $\tilde{\beta}$, il suffit de choisir un relèvement β de $\tilde{\beta}$ dans M' . L'action de G sur M est alors définie par :

$$\sigma(a,b) = (\sigma a + b\beta , b)$$

pour tout a de M' et tout b de M^* .

Précisons les calculs dans le même cas particulier qu'à la proposition 4. Les éléments $u_i = 1 + \zeta + \ldots + \zeta^i$, pour $0 \leq i \leq p-2$, constituent un système de représentants des classes non nulles de A modulo $(1-\zeta)A$. Il en est de même pour les $x_i = |u_i\bar{u}_i|^{1/2}$. Remarquons que si l'on choisit x_i comme représentant, le cocycle considéré donne la même image de σ et de τ , d'après la relation (ii) de la démonstration précédente.

Considérons donc l'extension M_1 correspondant à $x_1 = 1$, et l'extension M_i correspondant à x_i . Définissons les deux $S[G]$-automorphismes suivants :

a) la multiplication par x_i dans M' , notée x_i ;
b) l'identité dans M^* , notée 1_{M^*} .

Ces automorphismes permettent la construction d'une application $(x_i, 1_{M^*})$ de M_1 dans M_i , qui est un S-isomorphisme. Relativement à l'action de G , on obtient :

$$\begin{aligned}
(x_i , 1_{M^*})[\sigma(a,b)] &= (x_i, 1_{M^*})(\sigma a+b , b) \\
&= (x_i\sigma a + bx_i , b) \\
&= \sigma(x_i, 1_{M^*})(a,b) \\
(x_i , 1_{M^*})[\tau(a,b)] &= (x_i, 1_{M^*})(\tau a+b, b) \\
&= (x_i\tau a + bx_i , b) \\
&= \tau(x_i, 1_{M^*})(a,b) ,
\end{aligned}$$

car x_i est égal à son conjugué complexe. Donc tous les M_i sont isomorphes à M_1 , comme $S[G]$-modules. On procède de manière analogue dans les autres cas.

Notations : Lorsqu'il existe une extension indécomposable de M^* par M', nous la noterons (M',M^*) . ■

IV.2. Extensions indécomposables de modules décomposables.

Pour mettre en évidence de telles extensions, rappelons le résultat suivant, dû à Swan [5] :

THEOREME II. Soient π un groupe fini, et R un anneau de Dedekind de caractéristique 0 . Supposons qu'aucun diviseur de $|\pi|$ ne soit une unité de R . Alors tout module de type fini, projectif sur $R[\pi]$, est la somme directe d'un $R[\pi]$-module libre, et d'un idéal projectif I de $R[\pi]$. De plus, I est un $R[\pi]$-module indécomposable, et $rg_R I = rg_R R[\pi]$.

Appliquons ce théorème au cas où R est l'anneau $\mathbb{Z}_{(2p)}$, et où π est un groupe diédral G . Le $\mathbb{Z}_{(2p)}[G]$-module indécomposable obtenu, I , est de rang sur $\mathbb{Z}_{(2p)}$ égal à $2p$; il n'a donc pas encore été cité. Précisons dans la proposition suivante :

PROPOSITION 6. Lorsque $S = \mathbb{Z}_{(2p)}$, il existe à isomorphisme près une seule extension indécomposable de modules décomposables, $(A \oplus (1-\zeta)A, S_3)$.

Démonstration : L'idéal I du théorème II est $S[G]$-projectif, donc $S[G]$-isomorphe à $S[G]$. Donc I' est isomorphe à $\mathfrak{a}$, c'est-à-dire à $A \oplus (1-\zeta)A$. Quant à I^* , c'est un module de rang 2 sur S ; en étudiant l'action de τ , on vérifie que I^* est isomorphe à S_3 , donc

$$I \underset{S[G]}{\simeq} (A \oplus (1-\zeta)A, S_3)$$

Vérifier que $(A \oplus (1-\zeta)A, S_3$ est, à isomorphisme près, la seule extension indécomposable de modules décomposables, nécessite des calculs longs et fastidieux que l'on pourra trouver dans [4].

THEOREME III. <u>Soit</u> h <u>le nombre de classes de</u> A_o . <u>Il existe, à isomorphisme près,</u> $7h+3$ $\mathbb{Z}[G]$-<u>modules indécomposables. Si</u> $\{\mathfrak{A}_i\}$, <u>pour</u> $1 \leq i \leq h$, <u>désigne un système de représentants des classes de</u> A_o , <u>on peut les écrire comme suit</u> :

$$\mathfrak{A}_i A \quad , \quad (1-\zeta)\mathfrak{A}_i A$$

$$S_1 \quad , \quad S_2 \quad , \quad S_3$$

$$(\mathfrak{A}_i A , S_2) \quad , \quad ((1-\zeta)\mathfrak{A}_i A , S_1) \quad , \quad (\mathfrak{A}_i A , S_3)$$

$$((1-\zeta)\mathfrak{A}_i A, S_3) \quad , \quad (\mathfrak{A}_i A \oplus (1-\zeta)A, S_3) \ .$$

<u>Démonstration</u> : Les résultats des paragraphes II et III donnent les $2h+3$ modules $\mathfrak{A}_i A$, $(1-\zeta)\mathfrak{A}_i A$, S_1 , S_2 et S_3 . Il reste donc à dénombrer les extensions indécomposables M d'un $\mathbb{Z}[\langle\tau\rangle]$-module non trivial M^* par un $\mathfrak{a}$-module non trivial M' .

D'après le théorème I, si M est $\mathbb{Z}[G]$-indécomposable, $M_{2p} = \mathbb{Z}_{(2p)} \otimes_{\mathbb{Z}} M$ est $\mathbb{Z}_{(2p)}[G]$-indécomposable. Posons $M'_{2p} = \mathbb{Z}_{(2p)} \otimes_{\mathbb{Z}} M'$, et $M^*_{2p} = \mathbb{Z}_{(2p)} \otimes_{\mathbb{Z}} M^*$. De la suite exacte

$$(\alpha) \qquad 0 \to M' \to M \to M^* \to 0$$

on déduit la suite exacte

$$(\beta) \qquad 0 \to M'_{2p} \to M_{2p} \to M^*_{2p} \to 0 \ .$$

Donc M_{2p} est une extension de M^*_{2p} par M'_{2p} . Les $\mathbb{Z}_{(2p)}[G]$-modules indécomposables sont énumérés dans les propositions 5 et 6 . Etudions la première éventualité :

$$M^*_{2p} = (\mathbb{Z}_{(2p)})_1 \quad ; \quad \text{comme} \quad rg_{\mathbb{Z}_{(2p)}} M^*_{2p} = rg_{\mathbb{Z}} M^* \ ,$$

et que l'action de τ est la même pour les deux modules, nécessairement $M^* = (\mathbb{Z})_1$.

$M'_{2p} = (1-\zeta)A_{2p}$; donc M' est un $\mathfrak{a}$-module de rang sur $\mathbb{Z}$ égal à $p-1$: c'est un idéal ambige de A , de la forme $(1-\zeta)\mathfrak{A}_i A$.

On obtient ainsi, pour chaque $\mathbb{Z}_{(2p)}[G]$-module indécomposable obtenu comme extension de M^* par M', M^* et M' non triviaux, h $\mathbb{Z}[G]$-modules indécomposables. ■

V. A PROPOS DU THEOREME DE KRULL-SCHMIDT.

On trouve dans [4] la démonstration du théorème de Krull-Schmidt sour la forme suivante :

THEOREME IV. Dans toute décomposition d'un $\mathbb{Z}_{(p)}[G]$-module M_p en somme directe de modules indécomposables, les facteurs sont déterminés de manière unique par M_p, à un $\mathbb{Z}_{(p)}[G]$-isomorphisme près, et à l'ordre des facteurs près.

Lorsque $S = \mathbb{Z}_{(2)}$ ou $\mathbb{Z}_{(p)}$, les paragraphes II et III donnent les $\mathfrak{a}$-modules indécomposables, ainsi que les $S[\langle\tau\rangle]$-modules indécomposables. Une étude analogue à celle conduite au paragraphe IV donne les extensions qui sont $S[G]$-indécomposables. Dressons un tableau dans la première colonne duquel figurent les $\mathbb{Z}_{(2p)}[G]$-modules indécomposables. La deuxième colonne donne les localisés en p de chacun d'eux, et la troisième les localisés en 2 .

$(\mathbb{Z}_{(2p)})_1$	$(\mathbb{Z}_{(p)})_1$	$(\mathbb{Z}_{(2)})_1$
$(\mathbb{Z}_{(2p)})_2$	$(\mathbb{Z}_{(p)})_2$	$(\mathbb{Z}_{(2)})_2$
$(\mathbb{Z}_{(2p)})_3$	$(\mathbb{Z}_{(p)})_1 \oplus (\mathbb{Z}_{(p)})_2$	$(\mathbb{Z}_{(2)})_3$
A_{2p}	A_p	A_2
$(1-\zeta)A_{2p}$	$(1-\zeta)A_p$	$(1-\zeta)A_2$
$(A_{2p}, (\mathbb{Z}_{(2p)})_2)$	$(A_p, (\mathbb{Z}_{(p)})_2)$	$A_2 \oplus (\mathbb{Z}_{(2)})_2$
$((1-\zeta)A_{2p}, (\mathbb{Z}_{(2p)})_1)$	$((1-\zeta)A_p, (\mathbb{Z}_{(p)})_1)$	$(1-\zeta)A_2 \oplus (\mathbb{Z}_{(2)})_1$
$(A_{2p}, (\mathbb{Z}_{(2p)})_3)$	$(A_p, (\mathbb{Z}_{(p)})_2) \oplus (\mathbb{Z}_{(p)})_1$	$A_2 \oplus (\mathbb{Z}_{(2)})_3$
$((1-\zeta)A_{2p}, (\mathbb{Z}_{(2p)})_3)$	$((1-\zeta)A_p, (\mathbb{Z}_{(p)})_1) \oplus (\mathbb{Z}_{(p)})_2$	$(1-\zeta)A_2 \oplus (\mathbb{Z}_{(2)})_3$
$(A_{2p} \oplus (1-\zeta)A_{2p}, (\mathbb{Z}_{(2p)})_3)$	$(A_p, (\mathbb{Z}_{(p)})_2) \oplus ((1-\zeta)A_p, (\mathbb{Z}_{(p)})_1)$	$A_2 \oplus (1-\zeta)A_2 \oplus (\mathbb{Z}_{(2)})_3$

Considérons alors les $\mathbb{Z}[G]$-modules :

$$M = (A \oplus (1-\zeta)A , S_3) \oplus S_1 \oplus S_2$$

$$\text{et} \quad N = (A, S_2) \oplus ((1-\zeta)A, S_1) \oplus S_3 \ .$$

Leurs localisés en p et en 2 sont isomorphes. Ils sont donc $\mathbb{Z}[G]$-isomorphes. (cf. [1])

Conclusion : Même dans le cas où $h = 1$, la décomposition d'un $\mathbb{Z}[G]$-module en somme directe de modules indécomposables n'est pas toujours unique.

-o-o-o-

BIBLIOGRAPHIE

[1] L. BOUVIER - Séminaire de Théorie des Nombres. Grenoble 1973-1974.

[2] H. CARTAN et S. EILENBERG - Homological Algebra. Princeton University Press, 1956.

[3] D. DUVAL - Séminaire de Théorie des Nombres. Grenoble 1973-1974.

[4] M.P. LEE - Integral Representations of Dihedral Groups of order 2p . Trans. AMS 110 (1964).

[5] R.G. SWAN - Induced Representations and projective modules. Ann. of Math. (2) 70 (1960).

-o-o-o-