

NICOLE MOSER

Classification des $\mathbb{Z}\mathbb{Z}[G]$ -modules monogènes, pour G diédral d'ordre $2p$

Séminaire de théorie des nombres de Grenoble, tome 10 (1981-1982), exp. n° 1, p. 1-9

http://www.numdam.org/item?id=STNG_1981-1982__10__A1_0

© Institut Fourier – Université de Grenoble, 1981-1982, 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

19 novembre 1981

Grenoble

CLASSIFICATION DES $\mathbb{Z}[\Gamma]$ -MODULES MONOGENES, POUR Γ DIEDRAL D'ORDRE $2p$

par Nicole MOSER

GENERALITES.

Soient Γ un groupe fini, et M un $\mathbb{Z}[\Gamma]$ -module ; sauf mention du contraire, les modules étudiés dans ce travail sont supposés sans \mathbb{Z} -torsion, et de type fini sur \mathbb{Z} . Le module M se décompose, pas nécessairement de manière unique, en somme directe de $\mathbb{Z}[\Gamma]$ -modules indécomposables et pour certains groupes finis, on connaît un système exact de représentants des classes d'isomorphisme des $\mathbb{Z}[\Gamma]$ -modules indécomposables ; c'est le cas lorsque Γ est cyclique d'ordre premier (I. Reiner, [3]), ou Γ diédral d'ordre $2p$, p premier impair (M.P. Lee [1]). Parmi les sommes directes de $\mathbb{Z}[\Gamma]$ -modules indécomposables, il est clair que seules celles dont le \mathbb{Z} -rang est inférieur ou égal au cardinal de Γ sont susceptibles d'être $\mathbb{Z}[\Gamma]$ -monogènes.

Les représentants des classes d'isomorphisme de $\mathbb{Z}[\Gamma]$ -modules indécomposables sont en général construits à partir d'idéaux de corps cyclotomiques, avec lesquels on effectue des sommes directes ou des extensions. Le comportement de la propriété de $\mathbb{Z}[\Gamma]$ -monogénéité relativement à ces deux opérations est décrit dans les lemmes ci-dessous, dont les démonstrations ne posent pas de problème :

LEMME 1. - Soient Γ un groupe fini, et M un $\mathbb{Z}[\Gamma]$ -module somme directe de deux sous- $\mathbb{Z}[\Gamma]$ -modules N_1 et N_2 .

- (i) Si M est $\mathbb{Z}[\Gamma]$ -monogène, de générateur (α, β) , alors N_1 (resp. N_2) est $\mathbb{Z}[\Gamma]$ -monogène de générateur α (resp. β).
- (ii) On suppose N_1 et N_2 $\mathbb{Z}[\Gamma]$ -monogènes ; soient α un générateur de N_1 , d'annulateur \mathcal{O} dans $\mathbb{Z}[\Gamma]$, et β un générateur de N_2 . Les assertions suivantes sont équivalentes :
- a) (α, β) est générateur de M ;
- b) $\mathcal{O} \cdot \beta = N_2$.

On considère ensuite le $\mathbb{Z}[\Gamma]$ -module M , extension du $\mathbb{Z}[\Gamma]$ -module N_2 par le $\mathbb{Z}[\Gamma]$ -module N_1 construite à l'aide du cocycle $f \in Z^1(\Gamma, \text{Hom}_{\mathbb{Z}}(N_2, N_1))$. Une telle extension est notée (N_1, N_2, f) ; c'est le module $N_1 \oplus N_2$, sur lequel Γ agit de la manière suivante :

$$\sigma(x, y) = (\sigma x + f_{\sigma}(oy), \sigma y)$$

pour tout $x \in N_1$, $y \in N_2$, $\sigma \in \Gamma$.

DEFINITION 1. - Etant donné l'extension (N_1, N_2, f) , soit β un élément de N_2 . On appelle $\Phi_{f, \beta}$ l'application \mathbb{Z} -linéaire de $\mathbb{Z}[\Gamma]$ dans N_1 définie par

$$\Phi_{f, \beta} \left(\sum_{\sigma \in \Gamma} a_{\sigma} \sigma \right) = \sum_{\sigma \in \Gamma} a_{\sigma} f_{\sigma}(\sigma \beta), \quad a_{\sigma} \in \mathbb{Z}.$$

LEMME 2. - Soit M le $\mathbb{Z}[\Gamma]$ -module (N_1, N_2, f) , où $f \in Z^1(\Gamma, \text{Hom}_{\mathbb{Z}}(N_2, N_1))$.

- (i) Si M est $\mathbb{Z}[\Gamma]$ -monogène, de générateur (α, β) , N_2 est $\mathbb{Z}[\Gamma]$ -monogène, de générateur β .
- (ii) On suppose N_2 $\mathbb{Z}[\Gamma]$ -monogène ; soit β un générateur de N_2 , d'annulateur \mathcal{O} dans $\mathbb{Z}[\Gamma]$. Si les modules $\Phi_{f, \beta}(\mathcal{O})$ et N_1 sont égaux, M est $\mathbb{Z}[\Gamma]$ -monogène de générateur $(0, \beta)$.

On déduit des lemmes 1 et 2 le résultat suivant :

LEMME 3. - Soient N_1 , N_2 et N_3 trois $\mathbb{Z}[\Gamma]$ -modules. Si $N_1 \oplus N_2$ n'est pas $\mathbb{Z}[\Gamma]$ -monogène, quelle que soit l'extension (N_3, N_2, f) considérée, le module $N_1 \oplus (N_3, N_2, f)$ n'est pas $\mathbb{Z}[\Gamma]$ -monogène.

ETUDE DU CAS DIEDRAL.

Soient p un nombre premier impair, et G un groupe diédral d'ordre $2p$; le groupe G est engendré par deux éléments σ et τ liés par les relations :

$$\begin{aligned}\sigma^p &= \tau^2 = 1 \\ \tau\sigma\tau^{-1} &= \sigma^{p-1}.\end{aligned}$$

Si h désigne le nombre de classes du sous-corps réel maximal de $\mathbb{Q}^{(p)}$, M.P. Lee a dénombré dans [1], à isomorphisme près, $7h + 3$ $\mathbb{Z}[G]$ -modules indécomposables ; parmi ceux-ci, il en existe trois sur lesquels σ agit trivialement,

S_1 : \mathbb{Z} , sur lequel τ opère trivialement,

S_2 : \mathbb{Z} , sur lequel τ opère par multiplication par -1 ,

S_3 : $\mathbb{Z} + \mathbb{Z}\tau$, sur lequel τ opère par multiplication par τ .

PROPOSITION 4. -

- (i) Les trois $\mathbb{Z}[G]$ -modules S_1 , S_2 et S_3 sont $\mathbb{Z}[G]$ -monogènes. Tout générateur de S_1 (resp. S_2 , resp. S_3) admet comme annulateur dans $\mathbb{Z}[G]$ l'idéal $\mathbb{Z}[G](1-\sigma, 1-\tau)$, (resp. $\mathbb{Z}[G](1-\sigma, 1+\tau)$, resp. $\mathbb{Z}[G](1-\sigma)$).
- (ii) Si M est un $\mathbb{Z}[G]$ -module monogène, son écriture comporte au plus un des modules S_i .

Démonstration. - L'assertion (i) est presque évidente. Pour vérifier l'assertion (ii), on utilise les lemmes 1, 2 et 3 après avoir remarqué qu'on a les relations

$$\mathbb{Z}[G](1-\sigma)S_i = 0 \quad \text{pour } i = 1, 2 \text{ ou } 3 ,$$

$$\mathbb{Z}[G](1-\sigma, 1-\tau)S_2 \subset 2S_2$$

$$\mathbb{Z}[G](1-\sigma, 1+\tau)S_1 \subset 2S_1 . \blacksquare$$

Pour écrire les autres modules indécomposables obtenus par M.P. Lee, on utilise les notations suivantes :

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

$$A = \mathbb{Z}[\zeta] ;$$

$$\mathbb{Q}^{(p)} = \mathbb{Q}(\zeta) ;$$

$$\mathfrak{P} = (1-\zeta)A ;$$

$\{\alpha_i\}_{1 \leq i \leq h}$: un système de représentants des classes d'idéaux du sous-corps réel maximal de $\mathbb{Q}^{(p)}$, formé d'idéaux premiers à p .

Les $7h$ $\mathbb{Z}[G]$ -modules indécomposables autres que S_1 , S_2 et S_3 sont :

- $\alpha_i A$ et $\alpha_i \mathfrak{P}$, $1 \leq i \leq h$, où σ agit par multiplication par ζ , et τ comme la conjugaison complexe, notée s .

- $(\alpha_i A, S_2, f)$, avec $f \in Z^1(G, \text{Hom}_{\mathbb{Z}}(S_2, \alpha_i A))$ et $f_\sigma(1) \in \alpha_i A \setminus \alpha_i \mathfrak{P}$;

- $(\alpha_i \mathfrak{P}, S_1, g)$, avec $g \in Z^1(G, \text{Hom}_{\mathbb{Z}}(S_1, \alpha_i \mathfrak{P}))$ et $g_\sigma(1) \in \alpha_i \mathfrak{P} \setminus \alpha_i \mathfrak{P}^2$;

- $(\alpha_i A, S_3, f')$ avec $f' \in Z^1(G, \text{Hom}_{\mathbb{Z}}(S_3, \alpha_i A))$ et $f'_\sigma(1) \in \alpha_i A \setminus \alpha_i \mathfrak{P}$;

- $(\alpha_i \mathfrak{P}, S_3, g')$ avec $g' \in Z^1(G, \text{Hom}_{\mathbb{Z}}(S_3, \alpha_i \mathfrak{P}))$ et $g'_\sigma(1) \in \alpha_i \mathfrak{P} \setminus \alpha_i \mathfrak{P}^2$;

- $(A \oplus \alpha_i \mathfrak{P}, S_3, f' + g')$.

PROPOSITION 5. - Si e est un entier valant 0 ou 1, et α un idéal du sous-corps réel maximal de $\mathbb{Q}^{(p)}$, le $\mathbb{Z}[G]$ -module $\mathfrak{P}^e \alpha$ est $\mathbb{Z}[G]$ -monogène.

Démonstration. - Soit x un élément de $\mathfrak{P}^e \alpha$; tout élément de λ de $\mathbb{Z}[G]$ s'écrit $\sum_{i=0}^{p-1} \sigma^i(a_i + b_i \tau)$, où a_i et b_i sont des éléments de \mathbb{Z} , et l'on a :

$$\lambda \cdot x = \sum_{i=0}^{p-1} a_i \zeta^i x + \sum_{i=0}^{p-1} b_i \zeta^i s(x) .$$

Donc $\mathbb{Z}[G] \cdot x = Ax + As(x)$.

Or, d'après le théorème de densité d'Artin-Tchebotareff, dans chaque classe d'idéaux d'un corps de nombres K , il existe un idéal premier au-dessus d'un nombre premier totalement décomposé dans K . Soit \mathfrak{q} un tel idéal, appartenant à la classe de l'idéal $\alpha^{-1} \mathfrak{P}^{-e}$ de $\mathbb{Q}^{(p)}$; l'idéal $\mathfrak{P}^e \alpha \mathfrak{q}$ est donc un idéal entier principal de $\mathbb{Q}^{(p)}$, et si x désigne un de ses générateurs, on a :

$$\begin{aligned} \mathbb{Z}[G] \cdot x &= xA + s(x)A \\ &= \mathfrak{P}^e \alpha \mathfrak{q} + \mathfrak{P}^e \alpha s(\mathfrak{q}) = \mathfrak{P}^e \alpha . \blacksquare \end{aligned}$$

COROLLAIRE. - Toute extension diédrale imaginaire K de degré $2p$ de \mathbb{Q} admet une unité de Minkowski.

En effet, on sait d'après [2] que le quotient du groupe des unités de K par le sous-groupe des unités de torsion est $\mathbb{Z}[G]$ -isomorphe à un module de la forme $\mathfrak{P}^e \alpha$.

PROPOSITION 6. - Les $4h$ $\mathbb{Z}[G]$ -modules indécomposables de \mathbb{Z} -rang p ou $p+1$ sont $\mathbb{Z}[G]$ -monogènes.

Démonstration. - On considère l'extension $(\alpha_1 A, S_2, f)$. Si α est un générateur de $\alpha_1 A$, α n'appartient pas à \mathfrak{P} , et l'idéal de A qu'il engendre s'écrit $\alpha_1 b$, b idéal de A étranger à $s(b)$. On peut

donc choisir comme cocycle f celui qui est défini par

$$f_{\sigma}(1) = \alpha .$$

Pour expliciter l'application $\Phi_{f,1}$ de la définition 1, on rappelle qu'un élément $x \in G$ agit sur $\psi \in \text{Hom}_{\mathbb{Z}}(S_2, \alpha_i A)$ de la manière suivante :

$$x * \psi = x \psi x^{-1} ,$$

donc :

$$\sigma * \psi = \zeta \psi , \quad \tau * \psi = -\text{so}\psi .$$

Si l'on pose $\eta_i = 1 + \zeta + \dots + \zeta^{i-1}$, on a :

$$f_{\sigma}^i(1) = \eta_i \alpha \quad \text{avec } 1 \leq i \leq p-1$$

$$f_{\tau}(1) = \frac{s(\alpha) + \eta_{p-1} \alpha}{1 - \zeta^{p-1}} = \beta$$

$$f_{\sigma \tau}^i(1) = \zeta^i \beta + \eta_i \alpha \quad \text{avec } 1 \leq i \leq p-1 .$$

Soit $\lambda = \sum_{i=0}^{p-1} \sigma^i(a_i + b_i \tau)$ un élément de $\mathbb{Z}[G]$;

$$\Phi_{f,1}(\lambda) = \sum_{i=1}^{p-1} (a_i - b_i) \eta_i \alpha - \sum_{i=0}^{p-1} b_i \zeta^i \beta .$$

Si l'on impose à λ d'appartenir à l'annulateur \mathcal{O} de S_2 , on a :

$$\sum_{i=0}^{p-1} (a_i - b_i) = 0$$

et

$$\Phi_{f,1}(\lambda) = \sum_{i=1}^{p-1} [(a_i - b_i) \eta_i \alpha - (b_i - b_0) \zeta^i \beta] .$$

Comme les η_i , pour $1 \leq i \leq p-1$, constituent une \mathbb{Z} -base de A , on obtient l'égalité :

$$\Phi_{f,1}(\mathcal{O}) = A\alpha + A\beta .$$

Si β est nul, les idéaux $A\alpha$, $As(\alpha)$ et $\alpha_i A$ sont identiques. Si β est non nul, on vérifie facilement qu'il est entier, et qu'il engendre un idéal de la forme $\alpha_i c$, avec $(c, b) = 1$. Dans tous les cas, $\Phi_{f,1}(\mathcal{O})$ est égal à $\alpha_i A$, et d'après le lemme 2, $(\alpha_i A, S_2, f)$ est $\mathbb{Z}[G]$ -monogène de générateur $(0, 1)$.

Les démonstrations sont analogues dans les autres cas. ■

PROPOSITION 7. - Tout $\mathbb{Z}[G]$ -module monogène de \mathbb{Z} -rang $2p$ est $\mathbb{Z}[G]$ -isomorphe à $(A \oplus \mathfrak{P}, S_3, f'+g')$.

Démonstration. - Comme on ne considère que des modules sans \mathbb{Z} -torsion, tout module monogène de \mathbb{Z} -rang $2p$ est isomorphe à $\mathbb{Z}[G]$, et d'après M.P. Lee [1], $\mathbb{Z}[G]$ est isomorphe à $(A \oplus \mathfrak{P}, S_3, f'+g')$. ■

THEOREME. - Tout $\mathbb{Z}[G]$ -module monogène est isomorphe à l'un, et à l'un seul, des $8h+7$ modules ci-dessous :

$S_1, S_2, S_3, (A \oplus \mathfrak{P}, S_3, f'+g'), \alpha_i A, \mathfrak{P} \alpha_i,$
 $(\alpha_i A, S_2, f), (\alpha_i \mathfrak{P}, S_1, g), (\alpha_i A, S_3, f'), (\alpha_i \mathfrak{P}, S_3, g'),$
 $\alpha_i A \oplus S_2, \alpha_i \mathfrak{P} \oplus S_1$
 (l'indice i variant entre 1 et h), et $A \oplus \mathfrak{P}, (\mathfrak{P}, S_1, g) \oplus \mathfrak{P},$
 $(A, S_2, f) \oplus A$.

Démonstration. - D'après la proposition 4, l'écriture d'un module M monogène comporte au plus un S_i , donc les seuls $\mathbb{Z}[G]$ -modules monogènes de rang inférieur ou égal à $p-1$ sont indécomposables.

Les $\mathbb{Z}[G]$ -modules monogènes de rang p ou $p+1$ sont soit indécomposables, soit somme directe d'un module de la forme $\mathfrak{P}^e \alpha_i$ et d'un S_j . Dans le cas où $j=1$, l'annulateur de S_1 est $\mathbb{Z}[G](1-\sigma, 1-\tau)$. On note α un générateur de $\mathfrak{P}^e \alpha_i$; alors on a :

$$\begin{aligned} \mathbb{Z}[G](1-\sigma, 1-\tau)\alpha &= \mathbb{Z}[G](1-\sigma)\alpha + \mathbb{Z}[G](1-\tau)\alpha \\ &= \mathfrak{P}^{e+1} \alpha_i + A[\alpha - s(\alpha)]. \end{aligned}$$

Quel que soit l'élément α de A , $\alpha - s(\alpha)$ appartient à \mathfrak{P} ; donc si $e=0$, on a l'inclusion

$$\mathbb{Z}[G](1-\sigma, 1-\tau)\alpha \subset \mathfrak{P} \alpha_i,$$

et d'après le lemme 1, les modules $\alpha_i A \oplus S_1$ ne peuvent être monogènes. Mais si e est égal à 1, on écrit α sous la forme $(1-\zeta)\beta$, avec $\beta \notin \mathfrak{P}$;

$$\alpha - s(\alpha) = (1-\zeta)(\beta + \zeta^{p-1}s(\beta))$$

et l'élément $\beta + \zeta^{p-1}s(\beta)$ n'appartient pas à \mathfrak{P} . Donc l'idéal $A[\alpha - s(\alpha)]$ s'écrit $\mathfrak{P}\alpha_i b$, avec $(b, \mathfrak{P}) = 1$, l'idéal $\mathbb{Z}[G](1-\sigma, 1-\tau)\alpha$ est égal à $\mathfrak{P}\alpha_i$, et les modules $\alpha_i^{\mathfrak{P}} \oplus S_1$ sont $\mathbb{Z}[G]$ -monogènes. Les cas $j=2$ et $j=3$ se traitent de manière analogue.

Tous les $\mathbb{Z}[G]$ -modules monogènes de rang supérieur à $p+1$ s'écrivent avec au moins deux modules de la forme $\mathfrak{P}^e \alpha_i$. On étudie d'abord les modules $\mathfrak{P}^e \alpha_i \oplus \mathfrak{P}^e$; soient $(1-\zeta)^e \alpha$, $\alpha \notin \mathfrak{P}$, un générateur de $\mathfrak{P}^e \alpha_i$, et $\lambda = \sum_{i=0}^{p-1} \sigma^i(a_i + b_i \tau)$ un élément de son annulateur dans $\mathbb{Z}[G]$; si l'on pose :

$$X = \sum_{i=0}^{p-1} a_i \zeta^i \quad \text{et} \quad Y = \sum_{i=0}^{p-1} b_i \zeta^i,$$

on a :

$$X\alpha - \zeta^{p-e} Y s(\alpha) = 0$$

d'où

$$X - Y \equiv 0 \quad \text{modulo } \mathfrak{P}.$$

Quel que soit le générateur $(1-\zeta)^e \beta$, $\beta \notin \mathfrak{P}$, choisi pour \mathfrak{P}^e , on a :

$$\lambda \cdot (1-\zeta)^e \beta = (1-\zeta)^e [X\beta - \zeta^{p-e} Y s(\beta)]$$

et $X\beta - \zeta^{p-e} Y s(\beta) \in \mathfrak{P}$.

D'après le lemme 1, la somme directe $\mathfrak{P}^e \alpha_i \oplus \mathfrak{P}^e$ n'est donc pas $\mathbb{Z}[G]$ -monogène. On montre ensuite facilement que pour que $A \oplus \alpha_i^{\mathfrak{P}}$ soit $\mathbb{Z}[G]$ -monogène, il faut que l'idéal $\alpha_i^{\mathfrak{P}}$ soit principal, et on vérifie que $A \oplus \mathfrak{P}$ est effectivement monogène, de générateur $(1, 1-\zeta)$.

Restent les modules de \mathbb{Z} -rang $2p-1$. Grâce au lemme 3, il suffit d'étudier ceux de la forme $A \oplus (\alpha_i A, S_2, f)$ ou $\mathfrak{P} \oplus (\alpha_i^{\mathfrak{P}}, S_1, g)$. Or, tous les modules $A \oplus (\alpha_i A, S_2, f)$ sont annulés par $(1+\tau)(1+\sigma+\dots+\sigma^{p-1})$, et tout $\mathbb{Z}[G]$ -module monogène de \mathbb{Z} -rang $2p-1$, annulé par $(1+\tau)(1+\sigma+\dots+\sigma^{p-1})$, est isomorphe à $\mathbb{Z}[G]/\mathbb{Z}[G](1+\tau)(1+\sigma+\dots+\sigma^{p-1})$; donc parmi les h modules considérés, un seul est monogène, et il est

facile de voir que celui qui est monogène est $A \oplus (A, S_1, f)$. Pour les modules $\mathcal{P} \oplus (\alpha_i^{\mathcal{P}}, S_2, g)$, on procède de manière analogue en remarquant qu'ils sont tous annulés par $(1-\tau)(1+\sigma+\dots+\sigma^{p-1})$.

Enfin, on vérifie qu'il n'existe pas de $\mathbb{Z}[G]$ -isomorphisme entre deux quelconques des $8h+7$ modules cités, en étudiant les \mathbb{Z} -rangs et les sous-modules annulés par $1 + \sigma + \dots + \sigma^{p-1}$. ■

BIBLIOGRAPHIE

- [1] M.P. LEE, Integral representations of dihedral groups of order $2p$.
Trans. Amer. Math. Soc. 110 (1964) 213-231.
- [2] N. MOSER, Unités et nombre de classes d'une extension galoisienne
diédrale de \mathbb{Q} . Abh. Math. Sem. Univ. Hamburg, 48 (1979)
54-75.
- [3] I. REINER et C. CURTIS, Representation theory of finite groups and
associative algebras. Interscience (1962).