ACTA ARITHMETICA
XLII (1983)

Théorème de densité de Tchebotareff et monogénéité de modules sur l'algèbre d'un groupe métacyclique

par

NICOLE MOSER (Grenoble)

Soit G un groupe métacyclique, c'est-à-dire un produit semi-direct de groupes cycliques. Le théorème de densité de Tchebotareff permet de démontrer la monogénéité de certains $\boldsymbol{Z}[G]$-modules construits à partir d'idéaux de corps cyclotomiques $\boldsymbol{Q}^{(d)}$, pour d diviseur de l'ordre de G. On en déduit une classification complète des $\boldsymbol{Z}[G]$-modules monogènes, dans le cas où G est un groupe diédral d'ordre $2p$, p premier. Une conséquence arithmétique intéressante de cette classification porte sur les unités de Minkowski. On rappelle qu'une extension galoisienne $K/\boldsymbol{Q}$, de groupe de Galois G, possède une unité de Minkowski si le $\boldsymbol{Z}[G]$-module quotient du groupe des unités de K par le sous-groupe des unités de torsion, est monogène. On sait déjà (voir [3]) que si le sous-corps réel maximal du p-ième corps cyclotomique $\boldsymbol{Q}^{(p)}$ est principal, toute extension diédrale imaginaire de degré $2p$ de $\boldsymbol{Q}$ admet une unité de Minkowski. Le résultat démontré dans cet article permet de supprimer l'hypothèse sur $\boldsymbol{Q}^{(p)}$: toute extension diédrale imaginaire de degré $2p$ de $\boldsymbol{Q}$ admet une unité de Minkowski. Les unités de Minkowski rencontrées dans les travaux antérieurs appartenaient au sous-corps réel de K, ou étaient de norme triviale sur ce sous-corps; on en construit ici de nouveaux types.

Tous les modules considérés dans cet article sont des $\boldsymbol{Z}$-modules sans torsion et de type fini; si Γ est un groupe fini, on utilise uniquement des structures de $\boldsymbol{Z}[\Gamma]$-modules à gauche. Enfin, pour tout entier d, on note ζ_d une racine primitive d-ième de l'unité, $\boldsymbol{Q}^{(d)} = \boldsymbol{Q}(\zeta_d)$ le d-ième corps cyclotomique, et A_d l'anneau des entiers de $\boldsymbol{Q}^{(d)}$.

1. Quelques lemmes généraux. Soit Γ un groupe fini; étudier les représentations entières de Γ, c'est déterminer les $\boldsymbol{Z}[\Gamma]$-modules indécomposables. Pour la construction de ces modules, on utilise les deux opérations de somme directe de sous-modules, et d'extension d'un sous-module par un autre. Le comportement de la propriété de $\boldsymbol{Z}[\Gamma]$-monogénéité, relativement à ces deux opérations, est décrit dans les lemmes ci-dessous:

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

(i) *Si M est $\mathbf{Z}[\Gamma]$-monogène, de générateur (α, β), alors N_1 (resp. N_2) est $\mathbf{Z}[\Gamma]$-monogène de générateur α (resp. β);*

(ii) *On suppose N_1 et N_2 $\mathbf{Z}[\Gamma]$-monogènes; soient α un générateur de N_1, d'annulateur $\mathscr{A}$ dans $\mathbf{Z}[\Gamma]$, et β un générateur de N_2. Les assertions suivantes sont équivalentes:*

(a) *(α, β) est générateur de M;*

(b) *$\mathscr{A}\cdot\beta = N_2$.*

Démonstration. L'assertion (i) est immédiate.

Si l'on suppose (α, β) générateur de M, quel que soit $(0, y)$ dans M, il existe λ élément de $\mathbf{Z}[\Gamma]$ tel que

$$\lambda(\alpha, \beta) = (0, y),$$

et $\mathscr{A}\cdot\beta$ est égal à N_2.

Réciproquement, si $\mathscr{A}\cdot\beta = N_2$, quel que soit $(x, y) \in M$, il existe λ dans $\mathbf{Z}[\Gamma]$ et μ dans $\mathscr{A}$ tels que

$$\lambda\cdot\alpha = x \quad \text{et} \quad \mu\cdot\beta = y - \lambda\beta,$$

et on a $(\lambda+\mu)(\alpha, \beta) = (x, y)$. ■

On considère ensuite le $\mathbf{Z}[\Gamma]$-module M, extension du $\mathbf{Z}[\Gamma]$-module N_2 par le $\mathbf{Z}[\Gamma]$-module N_1 construite à l'aide du cocycle $f \in Z^1\big(\Gamma, \mathrm{Hom}_{\mathbf{Z}}(N_2, N_1)\big)$. Une telle extension est notée (N_1, N_2, f), ou (N_1, N_2) lorsqu'il n'y a pas ambiguïté sur le choix du cocycle. On rappelle que (N_1, N_2, f) est le $\mathbf{Z}$-module $N_1 \oplus N_2$, sur lequel Γ agit de la manière suivante: quels que soient $x \in N_1$, $y \in N_2$, $\sigma \in \Gamma$, on a

$$\sigma(x, y) = \big(\sigma x + f_\sigma(\sigma y), \sigma y\big).$$

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 $\mathbf{Z}$-linéaire de $\mathbf{Z}[\Gamma]$ dans N_1 définie par:

$$\Phi_{f,\beta}\Big(\sum_{\sigma\in\Gamma} a_\sigma \sigma\Big) = \sum_{\sigma\in\Gamma} a_\sigma f_\sigma(\sigma\beta) \qquad (a_\sigma \in \mathbf{Z}).$$

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

(i) *Si M est $\mathbf{Z}[\Gamma]$-monogène, de générateur (α, β), N_2 est $\mathbf{Z}[\Gamma]$-monogène, de générateur β.*

(ii) *On suppose N_2 $\mathbf{Z}[\Gamma]$-monogène; soit β un générateur de N_2, d'annulateur $\mathscr{A}$ dans $\mathbf{Z}[\Gamma]$. Si $\Phi_{f,\beta}(\mathscr{A}) = N_1$, M est $\mathbf{Z}[\Gamma]$-monogène de générateur $(0, \beta)$.*

Démonstration. Le premier résultat provient de la définition de l'action de Γ sur M.

Si (x, y) est un élément arbitraire de (N_1, N_2, f) sous les hypothèses de (ii), il existe λ dans $\mathbf{Z}[\Gamma]$ avec $\lambda\beta = y$, et μ dans $\mathscr{A}$ tel que

$$\Phi_{f,\beta}(\mu) = x - \Phi_{f,\beta}(\lambda).$$

Donc

$$(\lambda+\mu)(0, \beta) = (x, y). \ ■$$

Lorsque le $\mathbf{Z}$-rang de l'annulateur $\mathscr{A}$ de β est plus grand que celui de N_1, la structure de N_1 ne semble pas intervenir dans le fait que (N_1, N_2, f) soit monogène ou non.

LEMME 3. *Soient N_1, N_2 et N_3 des $\mathbf{Z}[\Gamma]$-modules. Si $N_1 \oplus N_2$ n'est pas $\mathbf{Z}[\Gamma]$-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 $\mathbf{Z}[\Gamma]$-monogène.*

Démonstration. D'après le lemme 1, il suffit d'examiner le cas où N_1 et N_2 sont $\mathbf{Z}[\Gamma]$-monogènes. Tout élément (γ, β) susceptible de fournir un générateur de (N_3, N_2, f) est construit à l'aide d'un générateur β de N_2 (lemme 2); l'annulateur de (γ, β) est un sous $\mathbf{Z}[\Gamma]$-module de l'annulateur $\mathscr{A}$ de β. Or, d'après le lemme 1, quel que soit le générateur α de N_1 considéré, $\mathscr{A}\cdot\alpha$ est un sous-module strict de N_1. ■

2. Où intervient le théorème de densité de Tchebotareff. Soit G un groupe métacyclique d'ordre $m \times n$, m et n entiers; il est engendré par deux éléments σ et τ liés par les relations

$$\sigma^m = \tau^n = 1 \quad \text{et} \quad \tau\sigma\tau^{-1} = \sigma^r,$$

où r est une racine n-ième de l'unité modulo m dont l'order l est un diviseur commun à n et à $\varphi(m)$; (φ désigne l'indicateur d'Euler). Si l est égal à 1, alors G est le produit direct de deux groupes cycliques. Tout élément de G s'écrit de manière unique $\sigma^i\tau^j$, ou $\tau^j\sigma^i$, avec $0 \leqslant i \leqslant m-1$ et $0 \leqslant j \leqslant n-1$.

Plusieurs auteurs ont étudié les représentations entières de groupes métacycliques particuliers, par exemple M. P. Lee ([2]), pour m premier et n égal à 2, ou S. Galovitch, I. Reiner et S. Ullom ([1]), pour m premier et r racine primitive n-ième de 1 modulo m. Les $\mathbf{Z}[G]$-modules indécomposables obtenus sont construits à partir d'idéaux de corps cyclotomiques munis de l'une des structures de $\mathbf{Z}[G]$-module décrites dans les propositions 4 et 5.

PROPOSITION 4. *Soient d un diviseur de n, et $\mathfrak{a}$ un idéal de $Q^{(d)}$. Lorsque σ opère trivialement sur $\mathfrak{a}$, et que τ agit par multiplication par ζ_d, le $\mathbf{Z}[G]$-module $\mathfrak{a}$ est monogène si et seulement si l'idéal $\mathfrak{a}$ est principal.*

Démonstration. Soit $\lambda=\sum_{j=0}^{n-1}\sum_{i=0}^{m-1} a_{ij}\sigma^i\tau^j$, $a_{ij}\in\mathbf{Z}$, un élément arbit de $\mathbf{Z}[G]$; pour α élément de $\mathfrak{a}$, on a

$$\lambda\cdot\alpha=\sum_{j=0}^{n-1}\Big(\sum_{i=0}^{m-1}a_{ij}\Big)\zeta_d^j\alpha.$$

Comme les éléments $\{1,\zeta_d,\ldots,\zeta_d^{\varphi(d)-1}\}$ constituent une $\mathbf{Z}$-base de A est donc clair que:

$$\mathbf{Z}[G]\cdot\alpha=A_d\alpha.$$

Le $\mathbf{Z}[G]$-module $\mathfrak{a}$ est monogène si et seulement si l'idéal $\mathfrak{a}$ est princ et les générateurs de $\mathfrak{a}$ en tant que $\mathbf{Z}[G]$-module sont les générateu l'idéal $\mathfrak{a}$ de $\boldsymbol{Q}^{(d)}$. ■

Proposition 5. *Soit δ un diviseur de m tel que l divise $\varphi(\delta)$. On s l'élément de* $\mathrm{Gal}(\boldsymbol{Q}^{(\delta)}/\boldsymbol{Q})$ *défini par* $s(\zeta_\delta)=\zeta_\delta^r$, *et* $\mathfrak{b}$ *un idéal non n* $\boldsymbol{Q}^{(\delta)}$ *fixe par* s, *sur lequel* σ *agit par multiplication par* ζ_δ, *et* τ *comme l'élé s. Si* r *est distinct de* 1, *le* $\mathbf{Z}[G]$*-module* $\mathfrak{b}$ *est monogène; un élément* $\beta\in$ *générateur de* $\mathfrak{b}$ *si et seulement si*

$$\beta A_\delta=\mathfrak{b}\mathfrak{q},$$

avec $\mathfrak{q}+\mathfrak{q}^s+\ldots+\mathfrak{q}^{s^{l-1}}=A_\delta$.

Démonstration. D'après le théorème de densité de Tchebotare densité analytique des idéaux de degré résiduel 1 et d'indice de rami tion 1, appartenant à une classe d'idéaux fixée de $\boldsymbol{Q}^{(\delta)}$, est non nulle particulier, il existe un tel idéal $\mathfrak{q}$ dans la classe de $\mathfrak{b}^{-1}$, et l'idéal $\mathfrak{b}$ principal; soit β un de ses générateurs, et soit $\lambda=\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}a_{ij}\sigma^i\tau^j$ un élé de $\mathbf{Z}[G]$:

$$\lambda\cdot\beta=\sum_{j=0}^{n-1}\Big(\sum_{i=0}^{m-1}a_{ij}\zeta_\delta^i\Big)s^j(\beta).$$

Donc

$$\mathbf{Z}[G]\beta=\sum_{j=0}^{n-1}A_\delta s^j(\beta)=\mathfrak{b}\mathfrak{q}+(\mathfrak{b}\mathfrak{q})^s+\ldots+(\mathfrak{b}\mathfrak{q})^{s^{n-1}}$$
$$=\mathfrak{b}(\mathfrak{q}+\mathfrak{q}^s+\ldots+\mathfrak{q}^{s^{l-1}})=\mathfrak{b}.$$

Ce calcul permet aussi de caractériser les générateurs du $\mathbf{Z}[G]$-mc $\mathfrak{b}$. ■

Proposition 6. *On suppose que m est un nombre premier p, e r est distinct de* 1. *Soient* $\mathfrak{p}$ *l'idéal premier de* $\boldsymbol{Q}^{(p)}$ *au-dessus de* p, $\mathfrak{a}$ *et* $\mathfrak{b}$ *idéaux du sous-corps de* $\boldsymbol{Q}^{(p)}$ *fixe par* $s(\zeta\to\zeta^r)$, *et* e *un entier tel que* $\leqslant l-1$. *On munit les idéaux* $\mathfrak{p}^e\mathfrak{a}$ *et* $\mathfrak{p}^e\mathfrak{b}$ *de la structure de* $\mathbf{Z}[G]$*-module dé*

à la proposition 5, *pour* $\delta=p$. *Alors, le* $\mathbf{Z}[G]$*-module* $\mathfrak{p}^e\mathfrak{a}\oplus\mathfrak{p}^e\mathfrak{b}$ *n'est pas monogène.*

Démonstration. A $\mathbf{Z}[G]$-isomorphisme près, seules comptent les classes des idéaux $\mathfrak{a}$ et $\mathfrak{b}$; on peut donc choisir ces idéaux premiers à p. D'après la proposition 5, le module $\mathfrak{p}^e\mathfrak{a}$ est $\mathbf{Z}[G]$-monogène; soit $(1-\zeta)^e u$ un de ses générateurs: u n'appartient pas à $\mathfrak{p}$. Soit $\lambda=\sum_{i=0}^{p-1}\sum_{j=0}^{n-1}a_{ij}\sigma^i\tau^j$ un élément de $\mathbf{Z}[G]$. Si l'on pose $A_j=\sum_{i=0}^{p-1}a_{ij}\zeta^i$, on a:

$$\lambda\cdot(1-\zeta)^e u=\sum_{j=0}^{n-1}A_j s^j[(1-\zeta)^e u]=\sum_{j=0}^{n-1}A_j(1-\zeta^{r^j})^e s^j(u).$$

On note η_{rj} l'unité $(1-\zeta^{r^j})(1-\zeta)^{-1}$; comme $s^j(u)$ est congru à u mod $\mathfrak{p}$, si λ appartient à l'annulateur de $(1-\zeta)^e u$, on a:

$$\sum_{j=0}^{n-1}A_j\eta_{rj}^e\equiv 0\bmod\mathfrak{p}.$$

Tout générateur de $\mathfrak{p}^e\mathfrak{b}$ est de la forme $(1-\zeta)^e\cdot v$, où v n'appartient pas à $\mathfrak{p}$. Si λ est dans l'annulateur de $(1-\zeta)^e u$,

$$\lambda\cdot(1-\zeta)^e v=(1-\zeta)^e\sum_{j=0}^{n-1}A_j\eta_{rj}^e s^j(v).$$

Comme $s^j(v)-v$ appartient à $\mathfrak{p}$, $\lambda\cdot(1-\zeta)^e v$ appartient à $\mathfrak{p}^{e+1}$, et d'après le lemme 1, $\mathfrak{p}^e\mathfrak{a}\oplus\mathfrak{p}^e\mathfrak{b}$ ne peut être $\mathbf{Z}[G]$-monogène. ■

3. Application au cas G diédral d'ordre $2p$. Si G est un groupe diédral d'ordre $2p$, p nombre premier impair, il est engendré par deux éléments σ et τ vérifiant les relations:

$$\sigma^p=\tau^2=1,$$
$$\tau\sigma=\sigma^{-1}\tau.$$

Un $\mathbf{Z}[G]$-module monogène M est un $\mathbf{Z}$-module de rang inférieur ou égal à $2p$; il se décompose en somme directe (non nécessairement unique) de $\mathbf{Z}[G]$-modules indécomposables. Or M. P. Lee a dénombré, à isomorphisme près, $7h+3$ $\mathbf{Z}[G]$-modules indécomposables, où h désigne le nombre de classes du sous-corps réel maximal de $\boldsymbol{Q}^{(p)}$ (cf. [2]). Dans cette classification, on rencontre d'abord trois $\mathbf{Z}[G]$-modules sur lesquels σ agit trivialement:

$S_1=\mathbf{Z}$, sur lequel τ opère trivialement;
$S_2=\mathbf{Z}$, sur lequel τ opère par multiplication par -1;
$S_3=\mathbf{Z}+\mathbf{Z}\tau$, sur lequel τ opère par multiplication par τ.

PROPOSITION 7. (i) *Les trois $\mathbf{Z}[G]$-modules S_1, S_2 et S_3 sont monogè*
Tout générateur de S_1 (resp. S_2, resp. S_3) admet comme annulateur d
$\mathbf{Z}[G]$ l'idéal $\mathbf{Z}[G](1-\sigma, 1-\tau)$ (resp. $\mathbf{Z}[G](1-\sigma, 1+\tau)$, resp. $\mathbf{Z}[G](1-$

(ii) *Si M est un $\mathbf{Z}[G]$-module monogène, son écriture comporte au p*
un des modules S_i.

Démonstration. (i) Les modules S_1 et S_2 vérifient les hypothè de la proposition 4; ils sont $\mathbf{Z}[G]$-monogènes, et admettent uniquem comme générateurs $+1$ et -1. Soit ε l'un de ces générateurs et soi $= \sum_{i=0}^{p-1} \sigma^i(a_i + b_i\tau)$ un élément arbitraire de $\mathbf{Z}[G]$.

Si λ appartient à l'annulateur de ε, générateur de S_1, on a:

$$\lambda \cdot \varepsilon = \sum_{i=0}^{p-1} (a_i + b_i)\varepsilon = 0;$$

donc $\lambda = \sum_{i=0}^{p-1} a_i(\sigma^i - \tau\sigma^{p-1}) + \sum_{i=0}^{p-2} b_i\tau(\sigma^i - \sigma^{p-1})$; or $\sigma^i - \tau\sigma^{p-1} = \sigma(\sigma^{i-1} -$ $= \sigma(\sigma^{i-1} - 1 + 1 - \tau)$. Donc λ appartient à $\mathbf{Z}[G](1-\sigma, 1-\tau)$; la récipro est évidente.

Si l'on considère ensuite ε comme générateur de S_2, et si $\lambda\varepsilon =$ on a:

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

$$\lambda = \sum_{i=0}^{p-1} a_i(\sigma^i + \tau\sigma^{p-1}) + \sum_{i=0}^{p-2} b_i\tau(\sigma^i - \sigma^{p-1})$$

$$= \sum_{i=0}^{p-1} a_i\sigma(\sigma^{i-1} - 1 + 1 + \tau) + \sum_{i=0}^{p-2} b_i\tau(\sigma^i - \sigma^{p-1}).$$

Donc λ est un élément de $\mathbf{Z}[G](1-\sigma, 1+\tau)$; il est clair que cet idéal inclus dans l'annulateur de ε.

Enfin, par définition de l'action de G sur S_3, 1 engendre le $\mathbf{Z}[$ module S_3; supposons que $x+y\tau$, x et y dans $\mathbf{Z}$, soit un autre génerat de S_3: il existe $\lambda = \sum_{i=0}^{p-1} \sigma^i(a_i + b_i\tau)$ dans $\mathbf{Z}[G]$ tel que $\lambda(x+y\tau) = 1$. posant $A = \sum_{i=0}^{p-1} a_i$ et $B = \sum_{i=0}^{p-1} b_i$, on obtient le système

$$\begin{cases} Ax + By = 1, \\ Ay + Bx = 0. \end{cases}$$

Donc $1 = (Ax+By)^2 - (Ay+Bx)^2 = (A^2 - B^2)(x^2 - y^2)$, d'où $x^2 -$ $= \pm 1$.

Donc l'un des deux entiers x et y vaut 0, et l'autre ± 1. Les seuls générateurs de S_3 sont 1, -1, τ et $-\tau$; soit g l'un d'eux.

Soit $\lambda = \sum_{i=0}^{p-1} \sigma^i(a_i + b_i\tau)$ un élément de l'annulateur de g:

$$\sum_{i=0}^{p-1} \sigma^i(a_i + b_i\tau)g = \sum_{i=0}^{p-1} a_i g + \sum_{i=0}^{p-1} b_i\tau g;$$

$$\lambda = \sum_{i=0}^{p-2} [a_i(\sigma^i - \sigma^{p-1}) + b_i\tau(\sigma^i - \sigma^{p-1})].$$

Donc λ appartient à l'idéal $\mathbf{Z}[G](1-\sigma)$; inversement, cet idéal annule g.

(ii) On suppose que deux des modules S_i interviennent dans l'écriture du $\mathbf{Z}[G]$-module M. D'après les résultats de M. P. Lee [2], on rencontre soit la somme directe $S_i \oplus S_j$, soit la somme directe de S_i et d'une extension de S_j par un module N, $S_i \oplus (N, S_j)$. Comme on vient de montrer que l'annulateur d'un générateur de S_i est en fait l'annulateur du module, d'après les lemmes 1 et 2, le cas $i = j$ est exclu pour M monogène.

D'autre part, l'annulateur de S_3 est contenu dans l'annulateur de S_1 et dans celui de S_2, donc toujours d'après les mêmes lemmes, l'écriture d'un module M $\mathbf{Z}[G]$-monogène ne peut contenir S_3 en même temps que S_1 ou S_2.

Enfin, on élimine les cas $(i,j) = (1,2)$ et $(i,j) = (2,1)$ en utilisant les deux inclusions

$$\mathbf{Z}[G](1-\sigma, 1-\tau)S_2 \subset 2S_2 \quad \text{et} \quad \mathbf{Z}[G](1-\sigma, 1+\tau)S_1 \subset 2S_1. \blacksquare$$

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; $A = \mathbf{Z}[\zeta]$; $\mathfrak{p} = (1-\zeta)A$; $h =$ nombre de classes du sous-corps réel maximal de $\mathbf{Q}^{(p)}$; $\{\mathfrak{a}_i\}_{1 \leqslant i \leqslant h}$ = un système de représentants des classes d'idéaux du sous-corps réel maximal de $\mathbf{Q}^{(p)}$, formé d'idéaux premiers à p. Les $7h$ $\mathbf{Z}[G]$-modules indécomposables restant sont:

- $\mathfrak{a}_i A$ et $\mathfrak{a}_i\mathfrak{p}$, où σ agit par multiplication par ζ, et τ comme la conjugaison complexe, notée s;
- $(\mathfrak{a}_i A, S_2, f)$, avec $f \in Z^1\big(G, \mathrm{Hom}_{\mathbf{Z}}(S_2, \mathfrak{a}_i A)\big)$, tel que $f_\sigma(1) \in \mathfrak{a}_i A \setminus \mathfrak{a}_i\mathfrak{p}$;
- $(\mathfrak{a}_i\mathfrak{p}, S_1, g)$, avec $g \in Z^1\big(G, \mathrm{Hom}_{\mathbf{Z}}(S_1, \mathfrak{a}_i\mathfrak{p})\big)$, tel que $g_\sigma(1) \in \mathfrak{a}_i\mathfrak{p} \setminus \mathfrak{a}_i\mathfrak{p}^2$;
- $(\mathfrak{a}_i A, S_3, f_1)$, avec $f_1 \in Z^1\big(G, \mathrm{Hom}_{\mathbf{Z}}(S_3, \mathfrak{a}_i A)\big)$ tel que $f_{1\sigma}(1) \in \mathfrak{a}_i A \setminus \mathfrak{a}_i\mathfrak{p}$;
- $(\mathfrak{a}_i\mathfrak{p}, S_3, g_1)$, avec $g_1 \in Z^1\big(G, \mathrm{Hom}_{\mathbf{Z}}(S_3, \mathfrak{a}_i\mathfrak{p})\big)$ tel que $g_{1\sigma}(1) \in \mathfrak{a}_i\mathfrak{p} \setminus \mathfrak{a}_i\mathfrak{p}^2$;
- $(A \oplus \mathfrak{a}_i\mathfrak{p}, S_3, f_1 + g_1)$.

PROPOSITION 8. *Si G est un groupe diédral d'ordre $2p$, tous les $\mathbf{Z}[G]$-modules indécomposables de $\mathbf{Z}$-rang inférieur ou égal à $p+1$ sont monogènes.*

Démonstration. Le travail est fait dans la proposition 7 pour S_1, S_2 et S_3. La proposition 5 donne la monogénéité des modules $\mathfrak{a}_i A$ et $\mathfrak{a}_i \mathfrak{p}$.

Soit α un générateur du $\mathbf{Z}[G]$-module $\mathfrak{a}_i A$:

$$\alpha A = \mathfrak{a}_i \mathfrak{b}, \quad \mathfrak{b}+\mathfrak{b}^s = A;$$

donc α n'appartient pas à $\mathfrak{a}_i\mathfrak{p}$, et l'extension de S_2 par $\mathfrak{a}_i A$ construite à l'aide du cocycle défini par $f_\sigma(1) = \alpha$ est indécomposable. Par définition de l'action de G sur $\mathrm{Hom}_{\mathbf{Z}}(S_2, \mathfrak{a}_i A)$, pour tout $x \in G$ et tout $\psi \in \mathrm{Hom}_{\mathbf{Z}}(S_2, \mathfrak{a}_i A)$, on a:

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

en particulier:

$$\sigma*\psi = \zeta\psi \quad \text{et} \quad \tau*\psi = -s\circ\psi.$$

Donc $f_{\sigma^i}(1) = (1+\zeta+\ldots+\zeta^{i-1})\alpha = \eta_i\alpha$ si $1 \leqslant i \leqslant p-1$, et de l'égalité $\tau\sigma = \sigma^{p-1}\tau$, on déduit:

$$\tau * f_\sigma + f_\tau = \sigma^{p-1} * f_\tau + f_{\sigma^{p-1}},$$

et

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

Enfin, pour $1 \leqslant i \leqslant p-1$,

$$f_{\sigma^i\tau}(1) = \sigma^i f_\tau(1) + f_{\sigma^i}(1) = \zeta^i\beta + \eta_i\alpha.$$

L'image de l'élément $\lambda = \sum_{i=0}^{p-1} \sigma^i(a_i+b_i\tau)$ de $\mathbf{Z}[G]$ par l'application $\Phi_{f,1}$ de la définition 1 est égale à:

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

On suppose que λ appartient à l'annulateur $\mathscr{A}$ de S_2; alors:

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

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 $1 \leqslant i \leqslant p-1$, constituent une $\mathbf{Z}$-base de A, on en déduit que:

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

Comme $s(\alpha)+\eta_{p-1}\alpha$ appartient à $\mathfrak{p}$, β appartient à A; ce dernier est aussi un élément de $\mathfrak{a}_i A$, et grâce à la condition $\mathfrak{b}+\mathfrak{b}^s = A$, on vérifie qu'il n'est dans aucun diviseur premier de $\mathfrak{b}$. Donc si $\beta \neq 0$:

$$A\beta = \mathfrak{a}_i\mathfrak{q}, \quad \text{avec} \quad (\mathfrak{q}, \mathfrak{b}) = 1,$$

et

$$\Phi_{f,1}(\mathscr{A}) = \mathfrak{a}_i A.$$

D'après le lemme 2, $(0, 1)$ est générateur de $(\mathfrak{a}_i A, S_2, f)$. (Si β est nul, les idéaux $A\alpha$ et $As(\alpha)$ sont identiques, donc $\mathfrak{b} = A$, et le résultat est encore vrai.)

Pour l'extension $(\mathfrak{a}_i\mathfrak{p}, S_1, g)$, on utilise des calculs analogues, en remarquant que τ agit sur $\psi \in \mathrm{Hom}_{\mathbf{Z}}(S_1, \mathfrak{a}_i\mathfrak{p})$ par:

$$\tau*\psi = s\circ\psi.$$

On définit le cocycle g par l'égalité:

$$g_\sigma(1) = (1-\zeta)\alpha, \quad \text{avec} \quad (1-\zeta)\alpha A = \mathfrak{a}_i\mathfrak{p}\mathfrak{b}, \quad \text{et} \quad \mathfrak{b}+\mathfrak{b}^s = A.$$

Donc:

$$g_{\sigma^i}(1) = (1+\zeta+\ldots+\zeta^{i-1})(1-\zeta)\alpha = \eta_i(1-\zeta)\alpha \quad \text{si} \quad 1 \leqslant i \leqslant p-1;$$

$$g_\tau(1) = \alpha - s(\alpha) = \beta.$$

Si λ est un élément de l'annulateur $\mathscr{A}'$ de S_1, on a:

$$\lambda = \sum_{i=0}^{p-1} \sigma^i(a_i+b_i\tau), \quad \sum_{i=0}^{p-1} (a_i+b_i) = 0,$$

$$\Phi_{g,1}(\lambda) = \sum_{i=0}^{p-1} [(a_i+b_i)\eta_i(1-\zeta)\alpha + (b_i-b_0)\zeta^i\beta].$$

Donc $\Phi_{g,1}(\mathscr{A}') = (1-\zeta)\alpha A + \beta A = \mathfrak{p}\mathfrak{a}_i$, et $(0, 1)$ est générateur de $(\mathfrak{a}_i\mathfrak{p}, S_1, g)$.

On considère enfin un cocycle j de $Z^1\big(G, \mathrm{Hom}_{\mathbf{Z}}(S_3, \mathfrak{a}_i\mathfrak{p}^e)\big)$, égal à f_1 si $e = 0$, et à g_1 si $e = 1$. Comme σ agit par multiplication par ζ, $H^1\big(G, \mathrm{Hom}_{\mathbf{Z}}(S_3, \mathfrak{a}_i\mathfrak{p}^e)\big)$ est isomorphe à $H^1\big(\langle\sigma\rangle, \mathrm{Hom}_{\mathbf{Z}}(S_3, \mathfrak{a}_i\mathfrak{p}^e)\big)^{G/\langle\sigma\rangle}$; donc j est déterminé si l'on connait j_σ. En posant par exemple:

$$j_\sigma(1) = \alpha, \quad \text{avec} \quad \alpha A = \mathfrak{p}^e\mathfrak{a}_i\mathfrak{b} \quad \text{et} \quad \mathfrak{b}+\mathfrak{b}^s = A,$$

$$j_\sigma(\tau) = -\zeta s(\alpha),$$

on vérifie qu'on obtient un représentant d'une classe non triviale fixe par τ. Le calcul de j_τ se fait à partir de la relation:

$$\tau*j_\sigma + j_\tau = \sigma^{p-1}*j_\tau + j_{\sigma^{p-1}}.$$

Quels que soient a et b dans $\mathbf{Z}$, on a:

$$(1-\zeta^{p-1})j_\tau(a+b\tau) = j_{\sigma^{p-1}}(a+b\tau) - s[j_\sigma(b+a\tau)]$$
$$= a\eta_{p-1}\alpha - \zeta b\eta_{p-1}s(\alpha) - bs(\alpha) + \zeta^{p-1}a\alpha = 0.$$

Soit $\lambda = \sum_{i=0}^{p-1} \sigma^i(a_i+b_i\tau)$ un élément de l'annulateur $\mathscr{A}''$ de S_3:

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

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

Donc

$$\Phi_{j,1}(\mathscr{A}'') = A\alpha + As(\alpha) = \mathfrak{a}_i\mathfrak{p}^e.$$

D'après le lemme 2, les $2h$ $\mathbf{Z}[G]$-modules $(\mathfrak{a}_iA, S_3, f_1)$ et $(\mathfrak{a}_i\mathfrak{p}, S_3, g_1)$ sont monogènes. ■

PROPOSITION 9. (i) *Les modules* $\mathfrak{a}_iA\oplus S_2$ *et* $\mathfrak{a}_i\mathfrak{p}\oplus S_1$ *sont* $\mathbf{Z}[G]$*-monogènes.*

(ii) *Les modules* $\mathfrak{a}_iA\oplus S_1$, $\mathfrak{a}_i\mathfrak{p}\oplus S_2$, $\mathfrak{a}_iA\oplus S_3$ *et* $\mathfrak{a}_i\mathfrak{p}\oplus S_3$ *ne sont pas* $\mathbf{Z}[G]$*-monogènes.*

Démonstration. Par définition de l'action de G sur les idéaux de la forme $\mathfrak{a}_i\mathfrak{p}^e$, pour tout élément x d'un tel idéal, on a:

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

On choisit un élément α tel que:

$$\alpha A = \mathfrak{p}^e\mathfrak{a}_i\mathfrak{b}, \quad \mathfrak{b}+\mathfrak{b}^s = A.$$

Alors:

$$\mathbf{Z}[G](1-\sigma)\alpha = \mathfrak{p}^{e+1}\mathfrak{a}_i\mathfrak{b} + \mathfrak{p}^{e+1}\mathfrak{a}_i\mathfrak{b}^s = \mathfrak{p}^{e+1}\mathfrak{a}_i.$$

D'après la proposition 7 et le lemme 1, les modules $\mathfrak{a}_iA\oplus S_3$ et $\mathfrak{a}_i\mathfrak{p}\oplus S_3$ ne sont pas $\mathbf{Z}[G]$-monogènes.

Toujours pour le même élément α, on a:

$$(1-\tau)\alpha = \alpha - s(\alpha) \quad \text{et} \quad \mathbf{Z}[G](1-\tau)\alpha = A\big(\alpha - s(\alpha)\big).$$

Il est clair que $\alpha - s(\alpha)$ appartient à $\mathfrak{a}_i$ et à $\mathfrak{p}$, donc:

$$A\big(\alpha - s(\alpha)\big) = \mathfrak{p}\mathfrak{a}_i\mathfrak{c}.$$

Si $e=0$, $\mathbf{Z}[G](1-\sigma, 1-\tau)\alpha = \mathfrak{p}\mathfrak{a}_i$, et les modules $\mathfrak{a}_iA\oplus S_1$ ne sont pas monogènes. Si $e=1$, on pose:

$$\alpha = (1-\zeta)\beta, \quad \beta\notin\mathfrak{p};$$

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

L'élément $\beta+\zeta^{p-1}s(\beta)$ n'appartient pas à $\mathfrak{p}$, et:

$$A\big(\alpha - s(\alpha)\big) = \mathfrak{p}\mathfrak{a}_i\mathfrak{c}, \quad \text{avec} \quad (\mathfrak{c},\mathfrak{p}) = 1.$$

D'où $\mathbf{Z}[G](1-\sigma, 1-\tau)\alpha = \mathfrak{a}_i\mathfrak{p}$, et les modules $\mathfrak{a}_i\mathfrak{p}\oplus S_1$ sont $\mathbf{Z}[G]$-monogènes.

Enfin, $\mathbf{Z}[G](1+\tau)\alpha = A\big(\alpha+\beta(\alpha)\big)$. Si $e=0$, $\alpha+s(\alpha)$ appartient à $\mathfrak{a}_i$, mais non à $\mathfrak{p}$, donc:

$$A\big(\alpha+s(\alpha)\big) = \mathfrak{a}_i\mathfrak{c}, \quad (\mathfrak{c},\mathfrak{p}) = 1,$$

$$\mathbf{Z}[G](1-\sigma, 1+\tau)\alpha = \mathfrak{p}\mathfrak{a}_i + \mathfrak{a}_i\mathfrak{c} = \mathfrak{a}_iA;$$

les $\mathbf{Z}[G]$-modules $\mathfrak{a}_iA\oplus S_2$ sont monogènes. Si $e=1$, on pose encore:

$$\alpha = (1-\zeta)\beta, \quad \beta\notin\mathfrak{p},$$

$$\alpha+s(\alpha) = (1-\zeta)\big(\beta+\eta_{p-1}s(\beta)\big);$$

comme $\beta+\eta_{p-1}s(\beta)$ appartient à $\mathfrak{p}$, on a:

$$A\big(\alpha+s(\alpha)\big) = \mathfrak{a}_i\mathfrak{p}^2\mathfrak{c},$$

et

$$\mathbf{Z}[G](1-\sigma, 1+\tau)\alpha = \mathfrak{a}_i\mathfrak{p}^2 + \mathfrak{a}_i\mathfrak{p}^2\mathfrak{c} = \mathfrak{a}_i\mathfrak{p}^2;$$

les $\mathbf{Z}[G]$-modules $\mathfrak{a}_i\mathfrak{p}\oplus S_2$ ne sont pas monogènes. ■

PROPOSITION 10. *Parmi les modules* $(A\oplus\mathfrak{a}_i\mathfrak{p}, S_3, f_1+g_1)$ *(resp.* $A\oplus(\mathfrak{a}_iA, S_2, f)$, *resp.* $\mathfrak{p}\oplus(\mathfrak{a}_i\mathfrak{p}, S_1, g)$*), il existe un, et un seul,* $\mathbf{Z}[G]$*-module monogène* $(A\oplus\mathfrak{p}, S_3, f_1+g_1)$ *(resp.* $A\oplus(A, S_2, f)$, *resp.* $\mathfrak{p}\oplus(\mathfrak{p}, S_1, g)$*).*

Démonstration. Il est clair que tout $\mathbf{Z}[G]$-module monogène de $\mathbf{Z}$-rang $2p$ est $\mathbf{Z}[G]$-isomorphe à $\mathbf{Z}[G]$. Comme M. P. Lee a démontré dans [2] que $\mathbf{Z}[G]$ est isomorphe à $(A\oplus\mathfrak{p}, S_3, f_1+g_1)$, la première partie de la proposition est justifiée.

Les h $\mathbf{Z}[G]$-modules $A\oplus(\mathfrak{a}_iA, S_2, f)$ sont de $\mathbf{Z}$-rang $2p-1$; on vérifie facilement qu'ils sont annulés par $(1+\tau)(1+\sigma+\ldots+\sigma^{p-1})$; or, tout $\mathbf{Z}[G]$-module monogène de rang $2p-1$, annulé par $(1+\tau)(1+\sigma+\ldots+\sigma^{p-1})$, est isomorphe à $\mathbf{Z}[G]/\mathbf{Z}[G](1+\tau)(1+\sigma+\ldots+\sigma^{p-1})$. Parmi les modules considérés, il y a au plus un $\mathbf{Z}[G]$-module monogène.

D'après les calculs de la proposition 8, si l'on pose $f_\sigma(1) = \alpha = 1+\zeta$, on a:

$$\beta = f_\tau(1) = 0.$$

L'élément $(0,1)$ de (A, S_2, f) est un générateur, et on voit facilement que tout élément λ de son annulateur $\mathscr{A}$ s'écrit:

$$\lambda = \sum_{i=0}^{p-1} a_i\sigma^i(1+\tau).$$

Comme l'extension $Q^{(p)}/Q$ est modérément ramifiée, la trace est une surjection de A sur l'anneau des entiers du sous-corps réel maximal de $Q^{(p)}$; soit $\gamma \in A$ un élément de trace 1 sur ce sous-corps; il est clair que γ engendre le $\mathbf{Z}[G]$-module A, et que $\mathscr{A}\cdot\gamma = A$. Donc le $\mathbf{Z}[G]$-module $A \oplus (A, S_1, f)$ est monogène.

On procède de même pour les modules $\mathfrak{p} \oplus (\mathfrak{a}_i\mathfrak{p}, S_1, g)$: ils ont pour $\mathbf{Z}$-rang $2p-1$, sont annulés par $(1-\tau)(1+\sigma+\ldots+\sigma^{p-1})$; tout $\mathbf{Z}[G]$-module monogène possédant ces propriétés est isomorphe à $\mathbf{Z}[G]/\mathbf{Z}[G](1-\tau)(1+\sigma+\ldots+\sigma^{p-1})$.

Si l'on choisit $g_\sigma(1) = 1-\zeta$, $g_\tau(1)$ est nul. Le générateur $(0,1)$ de $(\mathfrak{p}, S_1, g)$ admet comme annulateur l'idéal $\mathscr{A}'$ de $\mathbf{Z}[G]$ formé des éléments λ s'écrivant:

$$\lambda = \sum_{i=0}^{p-1} a_i \sigma^i (1-\tau).$$

$$\mathbf{Z}[G](1-\tau)(1-\zeta) = A(1-\zeta)(1+\zeta^{p-1}) = \mathfrak{p}.$$

Donc $\mathfrak{p} \oplus (\mathfrak{p}, S_1, g)$ est $\mathbf{Z}[G]$-monogène. ■

Théorème. *Soient G un groupe diédral d'ordre $2p$, et h le nombre de classes du sous-corps réel maximal de $Q^{(p)}$. Tout $\mathbf{Z}[G]$-module monogène M est isomorphe à l'un, et à l'un seul, des $8h+7$ modules ci-dessous:*

S_1, S_2, S_3,

$\mathfrak{a}_i A$, $\mathfrak{p}\mathfrak{a}_i$, $(\mathfrak{a}_i A, S_2, f)$, $(\mathfrak{a}_i\mathfrak{p}, S_1, g)$,

$\mathfrak{a}_i A \oplus S_2$, $\mathfrak{p}\mathfrak{a}_i \oplus S_1$, $(\mathfrak{a}_i A, S_3, f_1)$, $(\mathfrak{a}_i\mathfrak{p}, S_3, g_1)$,

$A \oplus \mathfrak{p}$, $(\mathfrak{p}, S_1, g) \oplus \mathfrak{p}$, $(A, S_2, f) \oplus A$, $(A \oplus \mathfrak{p}, S_3, f_1 + g_1)$.

Démonstration. D'après la proposition 7, l'écriture d'un module M monogène comporte au plus un S_i, donc les seuls $\mathbf{Z}[G]$-modules monogènes de rang inférieur ou égal à $p-1$ sont indécomposables, et l'on utilise la proposition 8.

Les $\mathbf{Z}[G]$-modules monogènes de rang p ou $p+1$ sont soit indécomposables (voir proposition 8), soit somme d'un module de rang $p-1$ et d'un S_i (voir proposition 9).

Tous les modules restant contiennent au moins deux sous $\mathbf{Z}[G]$-modules indécomposables de rang $p-1$. Parmi ceux de rang $2(p-1)$, d'après la proposition 6, les seuls susceptibles d'être monogènes sont de la forme $A \oplus \mathfrak{a}_i\mathfrak{p}$. Soit α un générateur de A:

$$\alpha A = \mathfrak{b} \quad \text{avec} \quad \mathfrak{b} + \mathfrak{b}^s = A.$$

Pour tout élément $\lambda = \sum_{i=0}^{p-1} \sigma^i(a_i + b_i\tau)$ de $\mathbf{Z}[G]$, on pose

$$x = \sum_{i=0}^{p-1} a_i\zeta^i \quad \text{et} \quad y = \sum_{i=0}^{p-1} b_i\zeta^i;$$

par définition de l'action de G sur A, l'élément $\lambda\cdot\alpha$ est égal à $x\alpha + ys(\alpha)$. Comme α et $s(\alpha)$ engendrent deux idéaux étrangers, pour que λ appartienne à l'annulateur $\mathrm{ann}(\alpha)$ de α, il faut et il suffit qu'il existe $z \in A$ tel que

$$x = zs(\alpha) \quad \text{et} \quad y = -z\alpha.$$

Donc quel que soit le générateur β de $\mathfrak{a}_i\mathfrak{p}$ choisi,

$$\mathrm{ann}(\alpha)\cdot\beta = A[s(\alpha)\beta - \alpha s(\beta)].$$

D'après le lemme 1, pour que $A \oplus \mathfrak{a}_i\mathfrak{p}$ soit monogène, il faut que $\mathfrak{a}_i\mathfrak{p}$ soit principal. Réciproquement, il est facile de vérifier que $A \oplus \mathfrak{p}$ est monogène, en choisissant pour α la valeur 1, et pour β, $1-\zeta$; on a alors

$$\mathrm{ann}(\alpha) = \mathbf{Z}[G](1-\tau, 1+\sigma+\ldots+\sigma^{p-1}),$$

et

$$\mathbf{Z}[G](1-\tau)\beta = \mathfrak{p}.$$

Quant aux modules de rang $2p-1$ ou $2p$, on montre grâce au lemme 3 et aux propositions 8 et 9 qu'il suffit d'étudier ceux de la proposition 10.

Enfin, il n'existe pas de $\mathbf{Z}[G]$-isomorphisme entre deux quelconques des $8h+7$ modules cités: c'est clair pour les modules de rang inférieur ou égal à $p-1$; pour les modules de rang supérieur, on détermine le sous-ensemble annulé par $1+\sigma+\ldots+\sigma^{p-1}$. ■

Corollaire. *Toute extension diédrale imaginaire K/Q, de degré $2p$, admet une unité de Minkowski.*

Démonstration. D'après la proposition III.1 de [3], le quotient du groupe des unités de K par le sous-groupe des unités de torsion est un $\mathbf{Z}[G]$-module isomorphe soit à $\mathfrak{a}_i A$, soit à $\mathfrak{a}_i\mathfrak{p}$; c'est donc un $\mathbf{Z}[G]$-module monogène.

Le résultat de la proposition 5 donne tous les types d'unités de Minkowski possibles. ■

Bibliographie

[1] S. Galovitch, I. Reiner et S. Ullom, *Class groups for integral representations of metacyclic groups*, Mathematika 19 (1972), pp. 105–111.

[2] M. P. Lee, *Integral representations of dihedral groups of order 2p*, Trans. Amer. Math. Soc. 110 (1964), pp. 213–231.

[3] N. Moser, *Unités et nombre de classes d'une extension galoisienne diédrale de Q*, Abh. Math. Sem. Univ. Hamburg 48 (1979), pp. 54–75.

Reçu le 7. 12. 1981 (1283)