

SUR LA REPRÉSENTATION INTÉGRALE DES GROUPES CYCLIQUES ET LES FACTEURS DE BASES

MOHAMED ELHASSANI CHARKANI ET MOHAMED BERTIT

RÉSUMÉ. Dans cet article, on utilise certains résultats profonds sur les résultants des polynômes cyclotomiques pour établir de nouveaux résultats sur la représentation intégrale. Plus précisément, pour tout groupe cyclique fini G , on étudie les idéaux premiers minimaux de l'anneau de groupe $\mathbf{Z}[G]$ et on donne certaines propriétés d'une importante famille de $\mathbf{Z}[G]$ -ordres et $\mathbf{Z}[G]$ -lattices M_Δ qui contient la famille de $\mathbf{Z}[G]$ -lattices appelés les facteurs de bases par E. Beneish [Bene 90]. Nous calculons aussi le premier groupe de cohomologie des $\mathbf{Z}[G]$ -lattices M_Δ et nous décrivons leur indécomposabilité en appliquant certains résultats récents de la théorie des graphes.

ABSTRACT. In this work we use some deep results on cyclotomic polynomials and their resultants to give some new results on integral representations. More precisely, for any finite cyclic group G , we study minimal prime ideals of the group ring $\mathbf{Z}[G]$ and exhibit some properties of an important family of $\mathbf{Z}$ -orders and $\mathbf{Z}[G]$ -lattices M_Δ which include the family of $\mathbf{Z}[G]$ -lattices called basic summands by E. Beneish [Bene 90]. We also calculate the first group of cohomology of the $\mathbf{Z}$ -orders M_Δ and by using graph theory, we describe their indecomposability.

1. Introduction. Dans tout ce travail on prend G un groupe cyclique d'ordre n et de générateur σ . On note par $D(n)$ l'ensemble des diviseurs de n et par d un élément de $D(n)$. Après avoir introduit les principales notations dans la section 2, on définit dans la section 3 le graphe $\mathcal{G}_n(M)$ associé à un $\mathbf{Z}[G]$ -lattice M et on donne certaines propriétés des graphes connexes. Dans la section 4, on montre le théorème 4.3 qui donne une condition nécessaire et suffisante sur Δ pour que M_Δ soit un $\mathbf{Z}[G]$ -module indécomposable. Le corollaire 4.5 montre que si Δ est saturé, M_Δ est un $\mathbf{Z}[G]$ -module indécomposable. Le corollaire 4.6 donne un critère sur le graphe $\mathcal{G}_n(M)$ pour tester si un $\mathbf{Z}[G]$ -lattice M est décomposable ou non.

La section 5 est consacrée à l'étude cohomologique; on dit qu'un $\mathbf{Z}[G]$ -lattice M est H^1 -trivial si pour tout sous-groupe A de G , $H^1(A, M) = 0$. Le résultat fondamental de cette section est la proposition 5.2 qui donne une condition nécessaire et suffisante sur Δ pour que le $\mathbf{Z}$ -ordre M_Δ soit un $\mathbf{Z}[G]$ -lattice H^1 -trivial. De la même manière, on déduit le corollaire 5.4 qui affirme que M_Δ est un $\mathbf{Z}[G]$ -module inversible si et seulement si

Reçu le 4 décembre 2003 et, sous forme définitive, le 17 février 2005.

Δ est saturé. Dans la section 6, on montre que l'utilisation des $\mathbf{Q}$ -caractères permet de donner une démonstration plus simple du théorème 1.1 (cité dans [Bene 90]), de même qu'une condition nécessaire et suffisante sur les coefficients des $\mathbf{Q}$ -caractères d'un $\mathbf{Q}[G]$ -module pour qu'il soit de permutation.

2. Préliminaires et notations. Soit G un groupe abélien fini. Un $\mathbf{Z}[G]$ -lattice est un $\mathbf{Z}[G]$ -module de type fini qui est libre sur $\mathbf{Z}$. Un $\mathbf{Z}[G]$ -module P est dit de permutation si P est un $\mathbf{Z}[G]$ -lattice qui admet pour base sur $\mathbf{Z}$ un G -ensemble fini. Un $\mathbf{Z}[G]$ -module M est dit inversible s'il est facteur direct d'un module de permutation.

Soit G un groupe cyclique d'ordre n et de générateur σ . On sait que l'ensemble $\mathcal{X}_{\mathbf{Q}}(G)$ des $\mathbf{Q}$ -caractères de G est identifié à l'ensemble $D(n)$ des diviseurs de n . Plus précisément,

$$\mathcal{X}_{\mathbf{Q}}(G) = \{\chi_d : d \text{ divise } n\}$$

où χ_d est le $\mathbf{Q}$ -caractère de G dont le noyau est le sous-groupe $G_d = \langle \sigma^d \rangle$ de G , associé au $\mathbf{Q}[G]$ -module $\mathbf{Q}[\zeta_d]$ (ζ_d étant une d^e racine primitive de l'unité). On note aussi par Ψ_d le $\mathbf{Q}$ -caractère $\mathbf{1}_{G_d}^G$ de G . Les $(\Psi_d)_{d|n}$ forment une base du groupe de Grothendieck $\mathcal{R}_{\mathbf{Q}}(G)$ de la catégorie des $\mathbf{Q}[G]$ -modules (voir [Ser 71], p. 119).

Pour toute partie Δ de $D(n)$, on définit l'idéal

$$J_{\Delta} := \prod_{d \in \Delta} \Phi_d(\sigma) \mathbf{Z}[G]$$

où Φ_d est le d^e polynôme cyclotomique. Si Δ est vide on pose $J_{\Delta} = \mathbf{Z}[G]$. Lorsque Δ est réduit à un singleton $\{d\}$, on écrit tout simplement J_d au lieu de J_{Δ} et si $\Delta = D(n)$ alors J_{Δ} est l'idéal nul. Il est clair que si Δ est non vide alors $J_{\Delta} = \prod_{d \in \Delta} J_d$. Si Δ et Δ' sont deux parties disjointes de $D(n)$, alors $J_{\Delta} \cdot J_{\Delta'} = J_{\Delta \cup \Delta'}$. On note que J_d est un idéal premier minimal de $\mathbf{Z}[G]$ et que les seuls idéaux premiers minimaux de $\mathbf{Z}[G]$ sont les idéaux J_d . Ceci permet de voir que $J_{\Delta} \subseteq J_{\Delta'}$ si et seulement si $\Delta' \subseteq \Delta$.

De même, pour toute partie non vide Δ de $D(n)$, on définit le $\mathbf{Z}[G]$ -lattice $M_{\Delta} := e_{\Delta} \cdot \mathbf{Z}[G]$ où e_{Δ} est l'idempotent de $\mathbf{Q}[G]$ égal à $\sum_{d \in \Delta} e_d$, (où e_d est l'idempotent associé à χ_d). Si Δ est vide, on pose $M_{\Delta} = (0)$ l'idéal nul. On note que le $\mathbf{Z}[G]$ -lattice M_{Δ} est aussi un $\mathbf{Z}$ -ordre de $e_{\Delta} \mathbf{Q}[G]$.

3. Graphe associé à un $\mathbf{Z}[G]$ -lattice. On rappelle (voir [G-Y 99] ou [C 2002]) qu'un graphe $G = (V, E)$ est la donnée de deux ensembles V et E où E est un ensemble des paires d'éléments de V , $E \subseteq V^2$. Les éléments de V s'appellent les sommets et les éléments de E s'appellent les arêtes. Deux parties X et Y d'un graphe $G = (V, E)$ sont dites voisines dans G si X contient au moins un sommet qui a un sommet voisin dans Y . Dans le cas contraire, on dit que X et Y sont séparés dans G .

Pour tout entier n , on note par $D(n)$ l'ensemble des diviseurs de n . On définit sur l'ensemble $D(n)$ le graphe $\mathcal{D}_n = (D(n), E)$ par $[d, d'] \in E$ (où d et d' sont deux éléments de $D(n)$) s'il existe un entier premier p tel que $d' = p^s d$ ou $d = p^t d'$. Pour toute partie Δ de $D(n)$, on définit le graphe $\mathcal{D}_n(\Delta)$ comme étant le sous-graphe de $\mathcal{D}_n$ induit par Δ (voir la notion de sous-graphe induit dans [G-Y 99] et [C 2002]). De même pour tout entier n , on définit sur l'ensemble $D(n)$ le graphe $\mathcal{G}_n = (D(n), E)$ par $[d, d'] \in E$ (où d et d' sont deux éléments de $D(n)$) si $J_d + J_{d'} \neq \mathbf{Z}[G]$.

Une partie non vide Δ de $D(n)$ est dite *saturée* (ou *croissante*, voir [D-P 90]) si pour tout élément k de Δ , $D(k)$ est inclus dans Δ .

Lemme 3.1. *Soit $G = (V, E)$ un graphe d'ordre $n \geq 2$. Alors G est connexe si et seulement si pour toute partition non vide (I, K) de V , il existe (i_0, k_0) dans $I \times K$ tel que $(i_0, k_0) \in E$.*

Proposition 3.2. *Pour tout entier n le graphe $\mathcal{D}_n$ est connexe. En plus, pour toute partie saturée Δ de $D(n)$, $\mathcal{D}_n(\Delta)$ est connexe.*

Démonstration. En effet, on applique les résultats de [C 2003] et le critère de connexité donné par le lemme 3.1. $\square$

Soit M un $\mathbf{Z}[G]$ -lattice (c'est-à-dire que M est un $\mathbf{Z}[G]$ -module de type fini libre sur $\mathbf{Z}$); alors $\mathbf{Q} \otimes_{\mathbf{Z}} M$ est identifié à $\mathbf{Q} \cdot M$. On désigne par Δ_M l'ensemble des diviseurs k de n tels que $e_k \mathbf{Q} \cdot M \neq 0$:

$$\Delta_M = \{k|n : e_k \mathbf{Q} \cdot M \neq 0\}.$$

On désigne par $\mathcal{G}_n(M)$ ou tout simplement Δ_M le sous-graphe de $\mathcal{G}_n$ induit par Δ_M . Le graphe $\mathcal{G}_n(M)$ est dit le graphe associé à M .

Proposition 3.3. *Soient d et d' deux diviseurs de n et δ leur pgcd ($\delta = (d, d')$). Alors $J_d + J_{d'} = \mathbf{Z}[G]$ si et seulement si ou bien $\delta \neq d$ et $\delta \neq d'$, ou bien $\delta = d$ et d'/d est composé, ou bien $\delta = d'$ et d/d' est composé.*

Démonstration. Soit δ le pgcd de d et d' . Alors d'après [Adn] (page 27), le résultant $\text{Res}(\Phi_d(X), \Phi_{d'}(X))$ des polynômes $\Phi_d(X)$ et $\Phi_{d'}(X)$ est égal à ± 1 si et seulement si ou bien $\delta \neq d$ et $\delta \neq d'$, ou bien $\delta = d$ et d'/d est composé, ou bien $\delta = d'$ et d/d' est composé. De plus, le corollaire 1 de [Bour 81] (chapitre 4 page 73) entraîne que $\Phi_d(X)$ et $\Phi_{d'}(X)$ vérifient l'identité de Bezout dans $\mathbf{Z}[X]$ si et seulement si $\text{Res}(\Phi_d(X), \Phi_{d'}(X)) = \pm 1$. Donc les deux polynômes $\Phi_d(X)$ et $\Phi_{d'}(X)$ vérifient l'identité de Bezout dans $\mathbf{Z}[X]$ si et seulement si ou bien $\delta \neq d$ et $\delta \neq d'$, ou bien $\delta = d$ et d'/d est composé, ou bien $\delta = d'$ et d/d' est composé. De plus, l'application

$$\begin{aligned} \mathbf{Z}[X] &\longrightarrow \mathbf{Z}[G] \\ P(X) &\longmapsto P(\sigma) \end{aligned}$$

est un homomorphisme d'anneaux surjectif dont le noyau est $(X^n - 1)\mathbf{Z}[X]$. Donc si $\Phi_d(X)$ et $\Phi_{d'}(X)$ vérifient l'identité de Bezout dans $\mathbf{Z}[X]$, alors $J_d + J_{d'} = \mathbf{Z}[G]$. Si $J_d + J_{d'} = \mathbf{Z}[G]$, alors il existe $P(X)$ et $P'(X)$ dans $\mathbf{Z}[X]$ tels que $\Phi_d(\sigma)P(\sigma) + \Phi_{d'}(\sigma)P'(\sigma) = 1$. Donc il existe $Q(X)$ dans $\mathbf{Z}[X]$ tel que

$$\Phi_d(X)P(X) + \Phi_{d'}(X)P'(X) + (X^n - 1)Q(X) = 1,$$

et comme $\Phi_d(X)$ divise $X^n - 1$ dans $\mathbf{Z}[X]$, alors $\Phi_d(X)$ et $\Phi_{d'}(X)$ vérifient l'identité de Bezout dans $\mathbf{Z}[X]$. $\square$

Corollaire 3.4. *Les graphes $\mathcal{D}_n$ et $\mathcal{G}_n$ sont isomorphes.*

4. Quelques propriétés de M_Δ . Soit Δ une partie de $D(n)$. On rappelle que G est un groupe cyclique d'ordre n et σ un générateur de G .

Proposition 4.1. (1) Pour toute partie Δ de $D(n)$, on a $J_\Delta = \text{Ann}_{\mathbf{Z}[G]} M_\Delta$ et par conséquent, l'isomorphisme $M_\Delta \cong \mathbf{Z}[G]/J_\Delta$.

(2) Pour tout diviseur d de n , on a $\tilde{G}_d = \sum_{k|d} e_k$ et par conséquent,

$$e_\Delta \tilde{G}_d = \frac{n}{d} e_{\Delta'}$$

où $\Delta' = \Delta \cap D(d)$ et $\tilde{G}_d$ est la somme des éléments du sous-groupe $G_d = \langle \sigma^d \rangle$ d'indice d de G .

Démonstration. (1) Il suffit d'appliquer le lemme 1.5 de [C 1992].

(2) Il suffit d'appliquer les propriétés des idempotents primitifs et le fait que $\frac{d}{n} \tilde{G}_d$ est l'idempotent associé à $\mathbf{Q}[G/G_d]$ (voir [B 1997]). $\square$

Corollaire 4.2. Soient d un diviseur de n et Δ un sous-ensemble non vide de $D(n)$. Si $\Delta' = \Delta \cap D(d)$, alors

$$(M_\Delta)_{\tilde{G}_d} = J_{\Delta'} M_\Delta.$$

Démonstration. On rappelle qu'on a déjà vu que $J_\Delta = \text{Ann}_{\mathbf{Z}[G]} M_\Delta$. Donc pour tout u dans $\mathbf{Z}[G]$, on a $e_\Delta u = 0$ si et seulement si $u \in J_\Delta$. Or $e_\Delta \tilde{G}_d = \frac{n}{d} e_{\Delta'}$. Par suite, $e_\Delta \tilde{G}_d u = 0$ si et seulement si $e_{\Delta'} u = 0$ si et seulement si $u \in J_{\Delta'}$. $\square$

Les propriétés des polynômes cyclotomiques (voir [Bour 81]) permettent aussi d'établir que

$$\tilde{G}_d = \prod_{k \notin D(d)} \Phi_k(\sigma).$$

De même, on peut établir que si d est un diviseur de n et $\Delta = D(d)$, alors $J_\Delta = I_d \mathbf{Z}[G]$ où I_d est l'idéal d'augmentation de $\mathbf{Z}[G_d]$. De plus, on a

$$M_\Delta \cong \prod_{d \in D(n) - \Delta} J_d = J_{\Delta^c}$$

où Δ^c est le complémentaire de Δ dans $D(n)$.

Le théorème 4.3 donne une condition nécessaire et suffisante sur Δ pour que M_Δ soit un $\mathbf{Z}[G]$ -module indécomposable.

Théorème 4.3. Le $\mathbf{Z}[G]$ -module M_Δ est un $\mathbf{Z}[G]$ -module indécomposable si et seulement si $\mathcal{G}_n(\Delta)$ est connexe.

Avant de montrer le théorème 4.3, on a besoin du lemme suivant qui caractérise quand deux idéaux J_I et J_K sont étrangers dans $\mathbf{Z}[G]$.

Lemme 4.4. Soient I et K deux sous-ensembles non vides de $D(n)$. Alors $J_I + J_K = \mathbf{Z}[G]$ si et seulement si pour tout couple (i, k) dans $I \times K$ on a $J_i + J_k = \mathbf{Z}[G]$.

Démonstration. Si $\prod_{i \in I} J_i + \prod_{k \in K} J_k = \mathbf{Z}[G]$, alors il est clair que pour tout couple (i, k) de $I \times K$ on a $J_i + J_k = \mathbf{Z}[G]$. Inversement, supposons que pour tout couple

(i, k) de $I \times K$ on a $J_i + J_k = \mathbf{Z}[G]$. Donc pour tout couple (i, k) de $I \times K$, il existe u_i et v_k dans $\mathbf{Z}[G]$ tels que $u_i \Phi_i(\sigma) + v_k \Phi_k(\sigma) = 1$; ainsi, en calculant le produit

$$\prod_{i \in I} (u_i \Phi_i(\sigma) + v_k \Phi_k(\sigma)) = 1,$$

on aura

$$\left(\prod_{i \in I} u_i \right) \prod_{i \in I} \Phi_i(\sigma) + \Phi_k(\sigma) v_k \sum_{j \in I} \left(\prod_{i \in I - \{j\}} (u_i \Phi_i(\sigma)) \right) = 1.$$

Donc pour tout k dans K , il existe x_k et y_k dans $\mathbf{Z}[G]$ tels que

$$x_k \left(\prod_{i \in I} \Phi_i(\sigma) \right) + y_k \Phi_k(\sigma) = 1.$$

De même, l'égalité

$$\prod_{k \in K} \left(x_k \left(\prod_{i \in I} \Phi_i(\sigma) \right) + y_k \Phi_k(\sigma) \right) = 1$$

entraîne que

$$\left(\prod_{k \in K} y_k \right) \prod_{k \in K} \Phi_k(\sigma) + x_k \left(\prod_{i \in I} \Phi_i(\sigma) \right) \left(\sum_{j \in K} \prod_{j \in K - \{k\}} y_j \Phi_j(\sigma) \right) = 1.$$

D'où $J_I + J_K = \mathbf{Z}[G]$. $\square$

Démonstration du théorème 4.3. $(\Rightarrow)$ On va montrer que pour toute partition non vide (I, K) de Δ , il existe (i_0, k_0) dans $I \times K$ tel que $J_{i_0} + J_{k_0} \neq \mathbf{Z}[G]$. S'il existe $I, K \neq \emptyset$ tels que la réunion disjointe $I \cup K = \Delta$ et que pour tout $(i, k) \in I \times K$, $J_i + J_k = \mathbf{Z}[G]$, alors $J_I + J_K = \mathbf{Z}[G]$. Par suite, $J_I \cap J_K = J_I J_K = J_\Delta$. Comme les J_i sont des idéaux premiers de $\mathbf{Z}[G]$ et que le couple (I, K) forme une partition disjointe non vide de Δ , alors $J_I \neq J_\Delta$ et $J_K \neq J_\Delta$. Donc

$$\mathbf{Z}[G]/J_\Delta \cong \frac{J_I}{J_\Delta} \oplus \frac{J_K}{J_\Delta}$$

constitue une décomposition non triviale, ce qui est absurde car $M_\Delta \cong \mathbf{Z}[G]/J_\Delta$ et M_Δ est indécomposable.

$(\Leftarrow)$ Supposons qu'il existe deux idéaux L_1 et L_2 de $\mathbf{Z}[G]$ tels que $L_1 + L_2 = \mathbf{Z}[G]$ et $L_1 \cap L_2 = J_\Delta$. Soit $I_j = \{i \in \Delta \mid L_j \subseteq J_i\}$, avec $j = 1, 2$. D'une part, on a $L_1 \cdot L_2 \subseteq L_1 \cap L_2 = J_\Delta$; donc pour tout d dans Δ , on a $L_1 \subseteq J_d$ ou $L_2 \subseteq J_d$. Ainsi tout élément de Δ est un élément de $I_1 \cup I_2$ et par suite $I_1 \cup I_2 = \Delta$. D'autre part, si $d \in I_1 \cap I_2$, alors $J_d \supseteq L_1 + L_2 = \mathbf{Z}[G]$, ce qui est absurde. Donc $I_1 \cap I_2 = \emptyset$. Si I_1 et I_2 sont tous les deux non vides, alors par hypothèse il existe (i_0, k_0) dans $I_1 \times I_2$ tel que $J_{i_0} + J_{k_0} \neq \mathbf{Z}[G]$. Or $L_1 + L_2 = \mathbf{Z}[G]$ et $J_{i_0} + J_{k_0} \supseteq L_1 + L_2$, ce qui est absurde. Donc I_1 ou I_2 est vide (car $I_1 \cap I_2 = \emptyset$ et $I_1 \cup I_2 = \Delta$). Si $I_1 = \emptyset$ alors $I_2 = \Delta$. Par suite, $L_2 = J_\Delta = L_1 \cap L_2 \subseteq L_1$. Donc $L_1 = L_1 + L_2 = \mathbf{Z}[G]$. Si $I_2 = \emptyset$ alors $I_1 = \Delta$ et par suite, $L_1 = J_\Delta = L_1 \cap L_2 \subseteq L_2$. Donc $L_2 = L_1 + L_2 = \mathbf{Z}[G]$. Donc $\mathbf{Z}[G]/J_\Delta$ est un $\mathbf{Z}[G]$ -module indécomposable. $\square$

Corollaire 4.5. *Si Δ est un sous-ensemble non vide saturé de $D(n)$, alors M_Δ est un $\mathbf{Z}[G]$ -module indécomposable.*

Démonstration. En effet, d'après la proposition 3.2, toute partie saturée du graphe $\mathcal{D}_n$ est connexe. $\square$

La réciproque n'est pas vraie. En effet, soit k un diviseur de n . Le théorème 4.3 entraîne que $e_k \cdot \mathbf{Z}[G]$ est un $\mathbf{Z}[G]$ -module indécomposable; par contre, l'ensemble $\{k\}$ n'est pas saturé par définition.

Soit M un $\mathbf{Z}[G]$ -lattice de type fini. Alors $\mathbf{Q} \otimes_{\mathbf{Z}} M$ est identifié à $\mathbf{Q} \cdot M$. On désigne par Δ_M le graphe associé à M .

Corollaire 4.6. *Soit M un $\mathbf{Z}[G]$ -lattice de type fini. Si M est un $\mathbf{Z}[G]$ -lattice indécomposable, alors le graphe $\mathcal{G}_n(M)$ est connexe.*

Démonstration. Soit M un $\mathbf{Z}[G]$ -lattice indécomposable. Alors on va montrer que pour toute partition non vide (I, K) de Δ_M , il existe (i_0, k_0) dans $I \times K$ tel que $J_{i_0} + J_{k_0} \neq \mathbf{Z}[G]$. En effet, supposons qu'il existe une partition disjointe non vide (I, K) de Δ_M telle que pour tout élément (i, k) de $I \times K$ on a $J_i + J_k = \mathbf{Z}[G]$. Alors

$$M_1 = (J_I) \cdot M \quad \text{et} \quad M_2 = (J_K) \cdot M.$$

(1) Si m est un élément de $M_1 \cap M_2$, alors il existe m_1 et m_2 dans M tels que

$$m = \left(\prod_{d \in I} \Phi_d(\sigma) \right) \cdot m_1 = \left(\prod_{d \in K} \Phi_d(\sigma) \right) \cdot m_2.$$

Donc pour tout d dans Δ_M , on a $e_d \cdot m = 0$ et comme $\sum_{k \in D(n)} e_k = 1$, alors $m = \sum_{k \in D(n)} e_k \cdot m$; ainsi $m = 0$. D'où $M_1 \cap M_2 = (0)$.

(2) On a $J_I + J_K = \mathbf{Z}[G]$. Alors il existe a_1 dans J_I et a_2 dans J_K tels que $a_1 + a_2 = 1$. Donc pour tout m dans M , on a $m = a_1 \cdot m + a_2 \cdot m \in M_1 + M_2$. Ainsi M est un $\mathbf{Z}[G]$ -lattice décomposable. D'où par contraposée, si M est indécomposable, alors pour toute partition non vide (I, K) de Δ_M , il existe (i_0, k_0) dans $I \times K$ tels que $J_{i_0} + J_{k_0} \neq \mathbf{Z}[G]$. $\square$

5. Étude du groupe de cohomologie $H^1(G_d, M_\Delta)$. On considère toujours un groupe cyclique G d'ordre n et σ un générateur de G . Soient d un diviseur de n et Δ un sous-ensemble non vide de $D(n)$. Soit $G_d = \langle \sigma^d \rangle$ le sous-groupe de G d'indice d . Comme G est cyclique, alors on a $H^1(G_d, M_\Delta) = H^{-1}(G_d, M_\Delta)$ (voir [Wei 69] et [Bab 72]). Donc pour tout diviseur d de n , le premier groupe de cohomologie est défini par

$$H^1(G_d, M_\Delta) = \frac{(M_\Delta)_{\tilde{G}_d}}{I_d M_\Delta},$$

où $(M_\Delta)_{\tilde{G}_d} = \{m \in M_\Delta \mid \tilde{G}_d m = 0\}$ et où I_d est l'idéal d'augmentation de $\mathbf{Z}[G_d]$.

Proposition 5.1. *Supposons donné un groupe cyclique G d'ordre n et de générateur σ . Soient d un diviseur de n et Δ un sous-ensemble non vide de $D(n)$. Si $\Delta' = \Delta \cap D(d)$, alors*

$$H^1(G_d, M_\Delta) \cong \frac{J_{\Delta'}}{\prod_{k|d} J_k + J_\Delta}.$$

Démonstration. En effet, d'après le corollaire 4.2, on a $(M_\Delta)_{\tilde{G}_d} = J_{\Delta'} M_\Delta$. Or d'après la partie (1) de la proposition 4.1, on a $M_\Delta \cong \mathbf{Z}[G]/J_\Delta$, ce qui entraîne que $J_{\Delta'} M_\Delta \cong J_{\Delta'}/J_\Delta$ car $J_\Delta \subseteq J_{\Delta'}$. Donc pour achever la preuve, il suffit d'appliquer le fait que $I_d M_\Delta = (\sigma^d - 1)M_\Delta$ et qu'alors $I_d M_\Delta \cong (\prod_{k|d} J_k + J_\Delta)/J_\Delta$. $\square$

On rappelle qu'un $\mathbf{Z}[G]$ -lattice M est dit H^1 -trivial si pour tout sous-groupe A de G , on a $H^1(A, M) = 0$.

Proposition 5.2. *Soit G un groupe cyclique d'ordre n et de générateur σ , et Δ un sous-ensemble non vide de $D(n)$. Alors M_Δ est H^1 -trivial si et seulement si Δ est saturé.*

Pour la preuve on démontre tout d'abord le lemme suivant.

Lemme 5.3. *Soient d un diviseur de n et Δ un sous-ensemble non vide de $D(n)$. Si Δ et $D(d)$ ne sont pas comparables, alors $H^1(G_d, M_\Delta) = 0$ si et seulement si Δ et $D(d)$ sont séparés dans le graphe $\mathcal{D}_n$.*

Démonstration. En effet, $H^1(G_d, M_\Delta) = 0$ si et seulement si $J_{\Delta'} = \prod_{k|d} J_k + J_\Delta$ si et seulement si $\mathbf{Z}[G] = J_{D(d) - \Delta'} + J_{\Delta - \Delta'}$. Donc $J_{D(d) - \Delta'}$ et $J_{\Delta - \Delta'}$ sont étrangers dans $\mathbf{Z}[G]$. Autrement dit, d'après le lemme 4.4, $H^1(G_d, M_\Delta) = 0$ si et seulement si Δ et $D(d)$ sont séparés dans le graphe $\mathcal{D}_n$. $\square$

Démonstration de la proposition 5.2. Si $\Delta \subseteq D(d)$ ou $D(d) \subseteq \Delta$, alors $J_{\Delta'} = \prod_{k|d} J_k + J_\Delta$. Par suite, $H^1(G_d, M_\Delta) = 0$. Si Δ et $D(d)$ ne sont pas comparables, on applique le résultat de [C 2003] qui affirme que Δ et $D(d)$ sont séparés dans le graphe $\mathcal{D}_n$ si et seulement si Δ est saturé. $\square$

Corollaire 5.4. *Soit G un groupe cyclique d'ordre n et Δ un sous-ensemble non vide de $D(n)$. Alors M_Δ est un $\mathbf{Z}[G]$ -module inversible si et seulement si Δ est saturé.*

Démonstration. D'après le lemme 4.1 de [Bene 90], M_Δ est un $\mathbf{Z}[G]$ -module inversible si et seulement si M_Δ est H^1 -trivial. Donc la proposition 5.2 entraîne que M_Δ est inversible si et seulement si Δ est saturé. $\square$

6. Caractère associé à un module de permutation. Soit P un $\mathbf{Z}[G]$ -lattice. On note par $\mathbf{Q}P$ le $\mathbf{Q}[G]$ -module $\mathbf{Q} \otimes_{\mathbf{Z}} P$. Rappelons qu'un $\mathbf{Z}[G]$ -module P est dit de permutation si P est un $\mathbf{Z}[G]$ -lattice qui admet pour base sur $\mathbf{Z}$ un G -ensemble fini. Nous présentons le résultat suivant, cité dans [Bene 93] et pour lequel nous donnons une démonstration plus simple.

Théorème 6.1. *Soit G un groupe cyclique d'ordre n et de générateur σ . Soient P et P' deux $\mathbf{Z}[G]$ -modules de permutation. Alors P et P' sont isomorphes si et seulement si P et P' ont le même $\mathbf{Q}$ -caractère (c'est-à-dire $\mathbf{Q}P \cong \mathbf{Q}P'$).*

Démonstration. (1) Si P est $\mathbf{Z}[G]$ -isomorphe à P' , alors $\mathbf{Q}P$ est $\mathbf{Q}[G]$ -isomorphe à $\mathbf{Q}P'$. Donc P et P' ont le même $\mathbf{Q}$ -caractère associé.

(2) Supposons maintenant que P et P' ont le même $\mathbf{Q}$ -caractère χ . Or P et P' sont deux $\mathbf{Z}[G]$ -modules de permutation. Donc il existe $(a_i)_{1 \leq i \leq r}$ et $(b_i)_{1 \leq i \leq r'}$ des entiers

naturels tels que

$$P \cong \bigoplus_{i=1}^r (\mathbf{Z}[G/H_i])^{a_i} \quad \text{et} \quad P' \cong \bigoplus_{j=1}^{r'} (\mathbf{Z}[G/H'_j])^{b_j}$$

où les $(H_i)_{1 \leq i \leq r}$ sont des sous-groupes distincts de G (de même pour les $(H_j)_{1 \leq j \leq r}$). Comme G est cyclique, alors pour tout $i = 1, 2, \dots, r$, il existe un diviseur d_i de n tel que $H_i = G_{d_i}$. De même, pour tout $j = 1, 2, \dots, r'$, il existe un diviseur d'_j de n tel que $H'_j = G_{d'_j}$. Or les $(H_i)_{1 \leq i \leq r}$ (resp. $(H'_j)_{1 \leq j \leq r'}$) sont distincts deux à deux. Donc les $(d_i)_{1 \leq i \leq r}$ (resp. $(d'_j)_{1 \leq j \leq r'}$) sont aussi distincts deux à deux. Donc

$$\chi = \sum_{1 \leq i \leq r} a_i \Psi_{d_i} \quad \text{et} \quad \chi = \sum_{1 \leq j \leq r'} b_j \Psi_{d'_j}.$$

Comme les $(\Psi_d)_{d|n}$ forment une base de $\mathcal{R}_{\mathbf{Q}}(G)$, alors $r = r'$ et il existe une permutation δ de l'ensemble $\{1, 2, \dots, r\}$ telle que $d'_i = d_{\delta(i)}$ et $b_i = a_{\delta(i)}$. Donc P est $\mathbf{Z}[G]$ -isomorphe à P' . $\square$

Lemme 6.2. Soient G un groupe cyclique d'ordre n et de générateur σ , M un $\mathbf{Q}[G]$ -module de caractère $\chi = \sum_{d|n} b_d \cdot \Psi_d$. Alors M est un $\mathbf{Q}[G]$ -module de permutation si et seulement si pour tout d divisant n , $b_d \geq 0$.

Démonstration. Si M est un $\mathbf{Q}[G]$ -module de permutation, alors il existe $\alpha_1, \alpha_2, \dots, \alpha_r$ dans $\mathbf{N}$, et H_i ($1 \leq i \leq r$) des sous-groupes de G tels que

$$M \cong \bigoplus_{i=1}^r \mathbf{Q}[G/H_i]^{\alpha_i}.$$

Or pour tout $i = 1, 2, \dots, r$, il existe un d_i divisant n tel que $H_i = G_{d_i}$; donc

$$M \cong \bigoplus_{i=1}^r \mathbf{Q}[G/G_{d_i}]^{\alpha_i}.$$

Ainsi le $\mathbf{Q}$ -caractère de M est $\chi = \sum_{i=1}^r \alpha_i \Psi_{d_i}$. D'où

$$\chi = \sum_{d|n} b_d \Psi_d$$

où $b_d = \alpha_i$ si $d = d_i$ et $b_d = 0$ sinon. Réciproquement, si M est un $\mathbf{Q}[G]$ -module de caractère

$$\chi = \sum_{d|n} b_d \cdot \Psi_d$$

avec $b_d \in \mathbf{N}$ pour tout $d|n$, alors

$$M \cong \bigoplus_{d|n} \mathbf{Q}[G/G_d]^{b_d}.$$

Donc M est un $\mathbf{Q}[G]$ -module de permutation. $\square$

English extended abstract. Let G be a cyclic group of order n and let σ be a generator of G . We denote by $D(n)$ the set of all divisors d of n . For any subset Δ of $D(n)$, we define the principal ideal

$$J_\Delta := \prod_{d \in \Delta} \Phi_d(\sigma) \mathbf{Z}[G]$$

where Φ_d is the d -th cyclotomic polynomial. If Δ is an empty set we put $J_\Delta = \mathbf{Z}[G]$. When Δ is reduced to a singleton $\{d\}$, we simply write J_d instead of J_Δ ; if $\Delta = D(n)$ then J_Δ is (0) . It is clear that if Δ is not empty, then $J_\Delta = \prod_{d \in \Delta} J_d$. If Δ and Δ' are two disjoint subsets of $D(n)$, then $J_\Delta \cdot J_{\Delta'} = J_{\Delta \cup \Delta'}$. Note that J_d is a minimal prime ideal of $\mathbf{Z}[G]$ and that the only minimal prime ideals of $\mathbf{Z}[G]$ are the ideals J_d . Therefore $J_\Delta \subseteq J_{\Delta'}$ if and only if $\Delta' \subseteq \Delta$.

Similarly for any non-empty subset Δ of $D(n)$, we define the $\mathbf{Z}[G]$ -lattice M_Δ by

$$M_\Delta := e_\Delta \cdot \mathbf{Z}[G]$$

where e_Δ is the idempotent $\sum_{d \in \Delta} e_d$ of $\mathbf{Q}[G]$ (e_d being the idempotent associated to χ_d). If Δ is empty, we put $M_\Delta = (0)$. Note that the $\mathbf{Z}[G]$ -lattice M_Δ is also a $\mathbf{Z}$ -order of $e_\Delta \mathbf{Q}[G]$ and $J_\Delta = \text{Ann}_{\mathbf{Z}[G]} M_\Delta$.

We define on $D(n)$ the graph $\mathcal{D}_n = (D(n), E)$ by $[d, d'] \in E$ (where d and d' are two elements of $D(n)$) if there exists a prime integer p such that $d' = p^s d$ or $d = p^t d'$. For any subset Δ of $D(n)$, we denote by $\mathcal{D}_n(\Delta)$ the subgraph of $\mathcal{D}_n$ induced by Δ (see the notion of induced subgraph by a set in [G-Y 99]).

In the same way, for any integer n we define on $D(n)$ the graph $\mathcal{G}_n = (D(n), E)$ by $[d, d'] \in E$ if $J_d + J_{d'} \neq \mathbf{Z}[G]$. We also denote the graph $\mathcal{G}_n(\Delta)$ as being the subgraph of $\mathcal{G}_n$ induced by Δ . A non-empty subset Δ of $D(n)$ is said to be *saturated* or *increasing* (see [D-P 90]) if for any element k of Δ , $D(k)$ is a subset in Δ .

If M is a finitely generated $\mathbf{Z}[G]$ -lattice, we denote by $\mathcal{G}_n(M)$ (or simply Δ_M) the subgraph of $\mathcal{G}_n$ induced by Δ_M , where Δ_M is the set of divisors k of n such that $e_k \mathbf{Q} \cdot M \neq 0$. The graph $\mathcal{G}_n(M)$ is said to be the graph associated to the $\mathbf{Z}[G]$ -lattice M . If $M = M_\Delta$ then $\Delta_M = \Delta$. In this case we write $\mathcal{G}_n(\Delta)$ instead of $\mathcal{G}_n(M)$.

In this work we use some properties of graphs to describe some properties of the $\mathbf{Z}[G]$ -lattices M_Δ . Indeed we establish three important results. The first is that for any saturated subset Δ of $D(n)$, the graph $\mathcal{D}_n(\Delta)$ is connected. The second is that the graphs $\mathcal{D}_n$ and $\mathcal{G}_n$ are isomorphic graphs. The third (and the main) result is Theorem 4.3 which gives a necessary and sufficient condition on Δ under which M_Δ is an indecomposable $\mathbf{Z}[G]$ -module. More precisely, we prove that a $\mathbf{Z}[G]$ -module M_Δ is an indecomposable $\mathbf{Z}[G]$ -module if and only if the graph $\mathcal{G}_n(\Delta)$ is a connected graph. A consequence of this result is that if Δ is a saturated subset of $D(n)$, then M_Δ is an indecomposable $\mathbf{Z}[G]$ -module. In general, we have only a necessary condition (the connectivity of the graph $\mathcal{G}_n(M)$ associated to M) for a finitely generated $\mathbf{Z}[G]$ -lattice M to be an indecomposable $\mathbf{Z}[G]$ -lattice.

Finally some deep properties of cyclotomic polynomials and the idempotents e_Δ allow us to calculate the first group of cohomology of M_Δ :

$$H^1(G_d, M_\Delta) \cong \frac{J_{\Delta'}}{\prod_{k|d} J_k + J_\Delta}$$

where $\Delta' = \Delta \cap D(d)$. It follows from the previous result that M_Δ is H^1 -trivial (i.e., $H^1(H, M) = 0$ for any subgroup H of G) if and only if Δ is saturated.

BIBLIOGRAPHIE

- [Adn] F. El Adnani, *Polynômes cyclotomiques et invariants liés à l'élimination*, Thèse de 3^e cycle; Rabat, Faculté des Sciences, Université Mohamed V.
- [Bab 72] A. Babakhanian, *Cohomological Methods in Group Theory*, Dekker, New York, 1972.
- [Bene 90] E. Beneish, *Invertible modules*, J. Algebra **128** (1990), 101–125.
- [B 1997] M. Bertit, Thèse de doctorat; Fès, Université Sidi Mohamed Ben Abdellah, 1997.
- [Bour 81] N. Bourbaki, *Algèbre*; Chapitres 4 à 7, Masson, Paris, 1981.
- [C 1992] M. E. Charkani, *Sur la structure galoisienne du groupe des unités*, Thèse de doctorat; Québec, Université Laval, 1992.
- [C 2002] M. E. Charkani, *Graphes et leurs applications*, Cours CEA Informatique avancée (2002-03).
- [C 2003] M. E. Charkani, *A study of a particular graph*; En préparation.
- [C-R 81] C. W. Curtis et I. Reiner, *Methods of Representation Theory*, vol. 1, John Wiley & Sons, Inc., New York, 1981.
- [C-W 90] G. Cliff et A. Weiss, *Summands of permutation lattices for finite groups*, Proc. Amer. Math. Soc. **110** (1990); no. 1, 17–20.
- [D-P 90] B. A. Davey et H.A. Priestley, *Introduction to lattices and order*, Cambridge Mathematical Textbooks, Cambridge University Press, Cambridge, 1990.
- [G-Y 99] J. Gross et J. Yellen, *Graph Theory and its Applications*, CRC Press, 1999.
- [Ser 71] J.-P. Serre, *Représentations linéaires des groupes finis*, Hermann, Paris, 1971.
- [Wei 69] E. Weiss, *Cohomology of Groups*, Pure and Applied Mathematics, vol. 34, Academic Press, New York-London, 1969.

M. E. CHARKANI ET M. BERTIT

DÉPARTEMENT DE MATHÉMATIQUES

FACULTÉ DES SCIENCES DHAR-MAHRAZ

B. P. 1796, FÈS, MAROC

COURRIEL : mcharkani@fsdmfes.ac.ma

m.bertit@caramail.com