SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

DOMINIQUE DUVAL

Représentations entières de certains groupes finis. 2e partie : Représentations entières des groupes cycliques d'ordre premier

Séminaire de théorie des nombres de Grenoble, tome 3 (1973-1974), exp. n° 6, p. 1-9

<http://www.numdam.org/item?id=STNG_1973-1974__3__A6_0>

Séminaire de Théorie des Nombres VI - 1
14 février 1974
Grenoble

REPRESENTATIONS ENTIERES DE CERTAINS GROUPES FINIS

- 2e partie -

REPRESENTATIONS ENTIERES DES GROUPES CYCLIQUES D'ORDRE PREMIER

par Dominique DUVAL

I. INTRODUCTION.

Le but de cet exposé est l'étude des représentations indécomposables d'un groupe G cyclique d'ordre premier p sur l'anneau $\mathbb{Z}$ des entiers relatifs.

Convenons d'appeler, pour tout anneau commutatif S, $S[G]$-module tout $S[G]$-module à gauche, libre de type fini sur S. Nous étudions donc ici les $\mathbb{Z}[G]$-modules indécomposables.

Nous montrons d'abord, à l'aide de cohomologie de groupes, qu'il y a trois $\mathbb{Z}_p[G]$-modules indécomposables, à $\mathbb{Z}_p[G]$-isomorphisme près ($\mathbb{Z}_p$ étant l'anneau des entiers p-adiques).

Puis, utilisant ce résultat et un théorème démontré par L. Bouvier [2], nous montrons que le nombre de $\mathbb{Z}[G]$-modules indécomposables, à $\mathbb{Z}[G]$-isomorphisme près, est égal à $2h + 1$ (h étant le nombre de classes du corps cyclotomique $\mathbb{Q}^{(p)}$).

Le problème a déjà été traité par I. Reiner [4] et S.D. Berman et P. Gudivok [1].

RAPPELS : COHOMOLOGIE DES GROUPES ET EXTENSIONS DE MODULES.

Soient : G un groupe fini

S un anneau commutatif

X,Y deux $S[G]$-modules

$C(Y,X)$ l'ensemble des extensions de Y par X à équivalence près,

où on appelle extension de Y par X tout $S[G]$-module E tel que la suite $0 \to X \to E \to Y \to 0$ soit exacte sur $S[G]$ et scindée sur S, et où deux extensions E et E' de Y par X sont dites équivalentes s'il existe un $S[G]$-isomorphisme θ rendant le diagramme suivant commutatif :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X & \longrightarrow & E & \longrightarrow & Y & \longrightarrow & 0 \\ & & {\scriptstyle id_X}\downarrow & & {\scriptstyle\theta}\downarrow & & {\scriptstyle id_Y}\downarrow & & \\ 0 & \longrightarrow & X & \longrightarrow & E' & \longrightarrow & Y & \longrightarrow & 0 \end{array}$$

Soit $T_S = \mathrm{Hom}_S(Y,X)$, muni d'une structure de G-module grâce à l'opération : $t^g = gtg^{-1}$ pour tout t dans T_S et tout g dans G.

Alors E est isomorphe, comme S-module, à $X \oplus Y$, et l'action de G sur E est de la forme $g(x,y) = (gx+\lambda_g(gy),gy)$ (si g,x,y sont respectivement dans G,X,Y), où λ_g est un élément de T_S. On vérifie facilement que l'application λ de G dans T_S définie par $\lambda(g) = \lambda_g$ pour tout g de G est un 1-cocycle de G dans T_S. L'application ainsi obtenue, de l'ensemble des extensions de Y par X dans l'ensemble des 1-cocycles de G dans T_S, induit un isomorphisme de $C(Y,X)$ sur $H^1(G,T_S)$ (premier groupe de cohomologie de G dans T_S).

D'autre part, si G est un groupe cyclique d'ordre premier p, σ un générateur de G, et M un G-module, l'application qui fait correspondre, à tout 1-cocycle de G dans M, sa valeur en σ, est un homomorphisme de groupes qui induit un isomorphisme entre $H^1(G,M)$ et $\dfrac{\mathrm{Ker}\ \Phi_p(\sigma)}{(\sigma-1)M}$ (où Φ_p est le polynôme cyclotomique d'ordre p).

NOTATIONS :

Désormais, nous utiliserons les notations suivantes :

soient p un nombre premier ;

G un groupe cyclique d'ordre p ;

σ un générateur de G ;

Φ_p le polynôme cyclotomique d'ordre p ,
$\Phi_p(X) = \frac{X^{p-1}}{X-1} = X^{p-1} + X^{p-2} + \ldots + X + 1$;

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

$\mathbb{Q}_p$ le corps des nombres p-adiques, $\mathbb{Z}_p$ l'anneau des entiers de $\mathbb{Q}_p$;

$\mathbb{Q}$ le corps des nombres rationnels, $\mathbb{Z}$ l'anneau des entiers relatifs ;

$\mathbb{F}_p$ le corps fini à p éléments ;

h le nombre de classes du corps cyclotomique $\mathbb{Q}(\zeta)$.

II. REPRESENTATIONS INDECOMPOSABLES DE G SUR $\mathbb{Z}_p$.

1. Application des résulats connus sur $\mathbb{Q}_p$.

Nous savons que $\mathbb{Q}_p[G]$ est une algèbre semi-simple, qu'il y a deux types de $\mathbb{Q}_p[G]$-modules simples, à savoir $\mathbb{Q}_p$ et $\mathbb{Q}_p(\zeta)$, et que $\mathbb{Q}_p[G]$ est isomorphe, en tant que $\mathbb{Q}_p[G]$-module, à $\mathbb{Q}_p \oplus \mathbb{Q}_p(\zeta)$.

Soit M un $\mathbb{Z}_p[G]$-module, et $\hat{M}$ le $\mathbb{Q}_p[G]$-module égal à $\mathbb{Q}_p \oplus_{\mathbb{Z}_p} M$; M sera identifié à $1 \oplus_{\mathbb{Z}_p} M$ et considéré comme une partie de $\hat{M}$. Sur $\mathbb{Q}_p[G]$, décomposons $\hat{M}$ en somme directe de $\mathbb{Q}_p[G]$-modules simples ; appelons N_1 l'un de ces facteurs simples, π la projection canonique de $\hat{M}$ sur N_1 , et $N = \pi(M)$. Soit $\hat{N} = \mathbb{Q}_p \oplus_{\mathbb{Z}_p} N$.

LEMME 1. $\boxed{N_1 = \hat{N}}$

Démonstration : Il s'agit de montrer que tout élément de N_1 est dans $\hat{N}$; or tout élément n de N_1 s'écrit $\pi(a \oplus m)$ où $a \in \mathbb{Q}_p$, $m \in M$, c'est-à-dire $n = a.\pi(1 \oplus m)$; donc n est dans $\mathbb{Q}_p \oplus_{\mathbb{Z}_p} \pi(M) = \hat{N}$. Autrement dit, le diagramme suivant est commutatif, et $\hat{N}$ est un $\mathbb{Q}_p[G]$-module simple :

$$\begin{array}{ccccc} \hat{M} & \longrightarrow & \hat{N} & \longrightarrow & 0 \\ \uparrow & & \uparrow & & \\ M & \xrightarrow{\pi} & N & \longrightarrow & 0 \end{array}$$

Nous allons donc chercher les $\mathbb{Z}_p[G]$-modules N tels que $\hat{N}$ soit isomorphe à $\mathbb{Q}_p$ ou à $\mathbb{Q}_p(\zeta)$:

Si $\hat{N}$ est isomorphe à $\mathbb{Q}_p$ (comme $\mathbb{Q}_p[G]$-module), alors N est un $\mathbb{Z}_p$-sous-module de $\mathbb{Q}_p$; mais, $\mathbb{Z}_p$ étant principal, tous les $\mathbb{Z}_p$-sous-modules de $\mathbb{Q}_p$ sont isomorphes ; donc N est isomorphe à $\mathbb{Z}_p$ (comme $\mathbb{Z}_p[G]$-module).

Si $\hat{N}$ est isomorphe à $\mathbb{Q}_p(\zeta)$, comme $\mathbb{Z}_p[\zeta]$ est principal, le même raisonnement montre que N est isomorphe à $\mathbb{Z}_p[\zeta]$ (comme $\mathbb{Z}_p[G]$-module).

2. THEOREME 1.

A $\mathbb{Z}_p[G]$-isomorphisme près, les seuls $\mathbb{Z}_p[G]$-modules indécomposables sont $S_1 = \mathbb{Z}_p$, $S_2 = \mathbb{Z}_p[\zeta]$, $S_3 = \mathbb{Z}_p[G]$.

Démonstration :

a) S_1, S_2, S_3 sont indécomposables sur $\mathbb{Z}_p[G]$:

Si S_1 (resp. S_2) était décomposable sur $\mathbb{Z}_p[G]$, alors $\hat{S}_1$ (resp. $\hat{S}_2$) le serait sur $\mathbb{Q}_p[G]$; or $\hat{S}_1 = \mathbb{Q}_p$ et $\hat{S}_2 = \mathbb{Q}_p(\zeta)$ sont des $\mathbb{Q}_p[G]$-modules simples, donc indécomposables.

Si S_3 était décomposable sur $\mathbb{Z}_p[G]$, alors $\mathbb{F}_p \otimes_{\mathbb{Z}_p} S_3 \approx \mathbb{F}_p[G]$ le serait sur $\mathbb{F}_p[G]$. Le lemme suivant montre que c'est impossible.

LEMME 2. La représentation régulière de $\mathbb{F}_p$ est indécomposable.

Démontration : Soit Σ la multiplication par σ dans le $\mathbb{F}_p$-espace vectoriel $\mathbb{F}_p[G]$; son polynôme caractéristique est $X^p-1 = (X-1)^p$, donc Σ a une seule valeur propre égale à 1 et d'ordre p. La matrice de Σ dans la base $\{1,\sigma,\ldots,\sigma^{p-1}\}$ est :

$$\begin{pmatrix} 0 & & & 1 \\ 1 & \ddots & & \\ & \ddots & 0 & \\ 0 & & 0 & 0 \end{pmatrix}$$

donc tous les vecteurs propres sont colinéaires à $1 + \sigma + \ldots + \sigma^{p-1}$, par suite la réduite de Jordan de Σ est :

$$\begin{pmatrix} 1 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 1 \end{pmatrix},$$

et la représentation régulière de $\mathbb{F}_p$ est indécomposable. ∎

b) Tout $\mathbb{Z}_p[G]$-module indécomposable est isomorphe à S_1, S_2 ou S_3 :

Nous allons démontrer par récurrence sur le $\mathbb{Z}_p$-rang de M. Soit donc M un $\mathbb{Z}_p[G]$-module indécomposable, non nul, tel que tout $\mathbb{Z}_p[G]$-module de rang strictement inférieur à celui de M soit de la forme $S_1^{(i)} \oplus S_2^{(j)} \oplus S_3^{(k)}$, où $S_\nu^{(i)}$ désigne la somme directe de i exemplaires de S_ν ($\nu \in \{1,2,3\}$, $i \in \mathbb{N}$). Considérons $\hat{M} = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} M$, et sa décomposition en $\mathbb{Q}_p[G]$-modules simples.

α) Si $\mathbb{Q}_p$ n'intervient pas dans la décomposition de $\hat{M}$: alors $\mathbb{Q}_p(\zeta)$ intervient, donc, d'après ce qui précède, la projection de $\hat{M}$ sur $\mathbb{Q}_p(\zeta)$ induit une projection de M sur S_2 ; le noyau N de cette projection est de rang

strictement inférieur à celui de M, donc de la forme $S_1^{(i)} \oplus S_2^{(j)} \oplus S_3^{(k)}$. Mais alors, sur $\mathbb{Q}_p[G]$, $\hat{M}$ est isomorphe à $\hat{B} \oplus \hat{N}$, donc à $\mathbb{Q}_p^{(i+k)} \oplus \mathbb{Q}_p(\zeta)^{(j+k+1)}$; on en conclut que $i = k = 0$ et que la suite de $\mathbb{Z}_p[G]$-modules est exacte : $0 \to S_2^{(j)} \to M \to S_2 \to 0$.
Cette suite montre qu'ici, il revient au même de parler de $\mathbb{Z}_p[G]$-modules ou de S_2-modules. Mais S_2 est principal, donc M est isomorphe à $S_2^{(j+1)}$; et comme nous avons supposé M indécomposable, nous obtenons $j = 0$ et $M \approx S_2$.

β) Si $\mathbb{Q}_p$ intervient dans la décomposition de $\hat{M}$: alors nous obtenons une suite exacte de $\mathbb{Z}_p[G]$-modules de la forme : $0 \to N \to M \to S_1 \to 0$, où N est isomorphe à $S_1^{(i)} \oplus S_2^{(j)} \oplus S_3^{(k)}$. Appliquons maintenant les rappels de cohomologie des groupes : $C(S_1, N)$ est isomorphe à $H^1(G,T)$ où $T = \mathrm{Hom}_{S_1}(S_1, N)$ est isomorphe à N comme S_1-module (rappelons que $S_1 = \mathbb{Z}_p$!). Donc $C(S_1, N)$ est isomorphe à $(H^1(G,S_1))^{(i)} \oplus (H^1(G,S_2))^{(j)} \oplus (H^1(G,S_3))^{(k)}$.
Admettons un instant le lemme suivant :

LEMME 3. $H^1(G,S_1) = 0$

$H^1(G,S_3) = 0$

$H^1(G,S_2)$ <u>est isomorphe à</u> $\mathbb{F}_p$, <u>et toutes les extensions de</u> S_1 <u>par</u> S_2 <u>correspondant à un élément non nul de</u> $\mathbb{F}_p$ <u>sont isomorphes à</u> S_3.

D'après ce lemme, $C(S_1, N)$ est isomorphe à $(H^1(G,S_2))^{(j)}$. Si l'image de M dans $(H^1(G,S_2))^{(j)}$ est nulle, alors la suite exacte $0 \to N \to M \to S_1 \to 0$ est scindée et M isomorphe à S_1 (car M est indécomposable).

Sinon, notons $N = N' \oplus S_2$ pour mettre en évidence le facteur S_2 tel que l'image de M dans le $H^1(G,S_2)$ correspondant soit non nulle.

LEMME 4. Alors la suite $0 \to N' \to M \to S_3 \to 0$ est exacte.

En effet, sur $\mathbb{Z}_p$, M est isomorphe à $N' \oplus S_2 \oplus S_1$, et en explicitant l'action de σ sur un élément de M, on voit que M peut être considéré comme une extension de S_3 par N'.

Donc nous avons une suite exacte de $\mathbb{Z}_p[G]$-modules : $0 \to N' \to M \to \mathbb{Z}_p[G] \to 0$. Or $\mathbb{Z}_p[G]$ est libre sur lui-même, donc la suite est scindée ; et M est indécomposable, d'où : $N' = 0$ et $M \approx S_3$. ∎

Démonstration du lemme 3 : Nous utiliserons l'isomorphisme de $H^1(G,S)$ sur $\frac{\text{Ker } \Phi_p(\sigma)}{(\sigma-1)S}$ (où S est un G-module quelconque).

Si $S = S_1 = \mathbb{Z}_p$, l'action de $\Phi_p(\sigma)$ sur S est la multiplication par p, donc $\text{Ker } \Phi_p(\sigma) = 0$ et $H^1(G,S_1) = 0$.

Si $S = S_3 = \mathbb{Z}_p[G]$, et si y est un élément de $\mathbb{Z}_p[G]$, alors $\Phi_p(\sigma)(y)$ est nul si et seulement si y est de la forme $(\sigma-1)y_1$, où y_1 appartient à $\mathbb{Z}_p[G]$; donc $\text{Ker } \Phi_p(\sigma) = (\sigma-1)S_3$, et $H^1(G,S_3) = 0$.

Si $S = S_2 = \mathbb{Z}_p[\zeta]$, l'action de $\Phi_p(\sigma)$ est la multiplication par $\Phi_p(\zeta)$ qui est nul. Donc $H^1(G,S_2) \approx \frac{\mathbb{Z}_p[\zeta]}{(\zeta-1)\mathbb{Z}_p[\zeta]}$; or $\mathbb{Z}_p[\zeta]$ est l'anneau des entiers de $\mathbb{Q}_p(\zeta)$, et l'extension $\mathbb{Q}_p(\zeta)$ sur $\mathbb{Q}_p$ est totalement ramifiée, d'uniformisante $(\zeta-1)$, donc $H^1(G,S_2) \approx \mathbb{F}_p$.

L'extension de $\mathbb{Z}_p$ par $\mathbb{Z}_p[\zeta]$ correspondant à 0 dans $\mathbb{F}_p$ est décomposable, et il existe au moins une extension indécomposable, à savoir $S_3 = \mathbb{Z}_p[G]$. Or, on vérifie que deux extensions correspondant à deux éléments non nuls de $\mathbb{F}_p$ sont isomorphes ; d'où le lemme 3. ∎

III. REPRESENTATIONS INDECOMPOSABLES DE G SUR $\mathbb{Z}$.

Rappel : L. Bouvier a démontré [2] la proposition suivante :

Un $\mathbb{Z}[G]$-module M est $\mathbb{Z}[G]$-indécomposable si et seulement si le $\mathbb{Z}_p[G]$-module $\mathbb{Z}_p \otimes_{\mathbb{Z}} M$ est $\mathbb{Z}_p[G]$-indécomposable.

Donc M est $\mathbb{Z}[G]$-indécomposable si et seulement si $\mathbb{Z}_p \otimes_{\mathbb{Z}} M$ est isomorphe, sur $\mathbb{Z}_p[G]$, à $\mathbb{Z}_p$ ou $\mathbb{Z}_p[\zeta]$ ou $\mathbb{Z}_p[G]$.

a) Si $\mathbb{Z}_p \otimes_{\mathbb{Z}} M$ est isomorphe à $\mathbb{Z}_p$ comme $\mathbb{Z}_p[G]$-module, alors G agit trivialement sur $\mathbb{Z}_p \otimes_{\mathbb{Z}} M$, donc sur M , et M est un $\mathbb{Z}$-module ; le rang de M sur $\mathbb{Z}$ est égal au rang de $\mathbb{Z}_p \otimes_{\mathbb{Z}} M$ sur $\mathbb{Z}_p$, c'est-à-dire à 1 . Or, $\mathbb{Z}$ est principal, donc tous les $\mathbb{Z}$-modules de rang 1 , c'est-à-dire tous les idéaux fractionnaires de $\mathbb{Q}$, sont isomorphes. Dans ce cas, il y a une seule possibilité pour M : M est isomorphe au $\mathbb{Z}[G]$-module $\mathbb{Z}$.

b) Si $\mathbb{Z}_p \otimes_{\mathbb{Z}} M$ est isomorphe à $\mathbb{Z}_p[\zeta]$, alors M est annulé par $\Phi_p(\sigma)$ donc M est un $\mathbb{Z}[\zeta]$-module de rang 1 .

Or $\mathbb{Z}[\zeta]$ est un anneau de Dedekind, donc deux $\mathbb{Z}[\zeta]$-modules de rang 1 sont isomorphes si et seulement si, en tant qu'idéaux fractionnaires de $\mathbb{Q}(\zeta)$, ils sont dans la même classe.

Dans ce cas, il y a h possibilités pour M .

c) Si $\mathbb{Z}_p \otimes_{\mathbb{Z}} M$ est isomorphe à $\mathbb{Z}_p[G]$, c'est-à-dire si $\mathbb{Z}_p \otimes_{\mathbb{Z}} M$ est une extension non triviale de $S_1 = \mathbb{Z}_p$ par $S_2 = \mathbb{Z}_p[\zeta]$, alors M est une extension non triviale de S'_1 par S'_2 , où S'_ν est défini par $S_\nu \approx \mathbb{Z}_p \otimes_{\mathbb{Z}} S'_\nu$ $(\nu = 1,2)$; d'après a) et b), il y a 1 manière de choisir S'_1 et h manières de choisir S'_2 . Or, à chaque choix de S'_1 et S'_2 correspond une seule extension non triviale M .

Dans ce cas, il y a encore h possibilités pour M .

Le résultat est donc le suivant :

THEOREME 2. Le nombre de représentations non isomorphes d'un groupe cyclique d'ordre p sur $\mathbb{Z}$ est égal à $2h+1$, si h est le nombre de classes du corps cyclotomique $\mathbb{Q}^{(p)}$.

(Il y a une extension de degré 1, h de degré (p-1), et h de degré p).

-o-o-o-

BIBLIOGRAPHIE

[1] S.D. BERMAN et P.M. GUDIVOK - Indecomposable representations of finite groups over the ring of p-adic integers. Izv. Akad. Nauk, SSSR Ser. Mat. 28 (1964) pp. 875-910. English transl., Amer. Math. Soc. Transl. (2) 50 (1966), pp. 77-113.

[2] L. BOUVIER - Séminaire de théorie des nombres. Grenoble, 1973-1974.

[3] I. REINER - On the class number of representations of an order. Canadian Journal of Mathematics, Vol. 11 (1959), pp. 660-672.

-o-o-o-