SÉMINAIRE DE THÉORIE DES NOMBRES DE BORDEAUX

ANNE-MARIE BERGÉ

Groupe des classes projectives d'un ordre $\mathcal{D}$ de $\mathbb{Z}$ dans l'algèbre du groupe diédral d'ordre $2p$ sur Q

Séminaire de théorie des nombres de Bordeaux (1969-1970), exp. n° 4, p. 1-8

<http://www.numdam.org/item?id=STNB_1969-1970____A4_0>

Séminaire de Théorie des Nombres
Année 1969-1970 , exposé n° 4

9 Décembre 1969

GROUPE DES CLASSES PROJECTIVES D'UN ORDRE $\mathfrak{O}$ DE $\mathbb{Z}$ DANS L'ALGEBRE DU GROUPE DIEDRAL D'ORDRE 2p SUR $\mathbb{Q}$

par

Anne-Marie BERGÉ

-:-:-:-

INTRODUCTION

Soit G un groupe diédral d'ordre 2p , à 2 générateurs σ et τ liés par les conditions :

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

L'étude de l'anneau des entiers d'une extension diédrale de $\mathbb{Q}$ modérément ramifiée est liée à la structure des modules projectifs M de type fini, de rang 1 (c'est-à-dire tels que $\mathbb{Q} \underset{M}{\otimes} M$ soit $\mathbb{Q}[G]$-libre de rang 1) sur l'algèbre Z[G] (J. Martinet [2]).

Plus généralement, si l'on ne suppose plus l'extension modérément ramifiée, n est amené à introduire les ordres de $\mathbb{Z}$ dans $\mathbb{Q}[G]$ -c'est-à-dire les réseaux multiplicativement stables et contenant l'unité- contenant $\mathbb{Z}[G]$, et à étudier les modules projectifs de type fini, de rang r déterminé, sur un tel ordre.

Soit donc $\mathfrak{O}$ un ordre de $\mathbb{Z}$ dans $\mathbb{Q}[G]$ contenant $\mathbb{Z}[G]$. On dit que deux modules projectifs de type fini sur $\mathfrak{O}$ et de rangs déterminés, P et P' , sont équivalents s'il existe deux $\mathfrak{O}$-modules libres E et E' tels que $P \oplus E$ soit isomorphe à $P' \oplus E'$.

L'ensemble quotient est un groupe pour la loi induite par la somme directe, noté $\mathfrak{P}(\mathfrak{O})$ est appelé groupe des classes projectives de $\mathfrak{O}$.

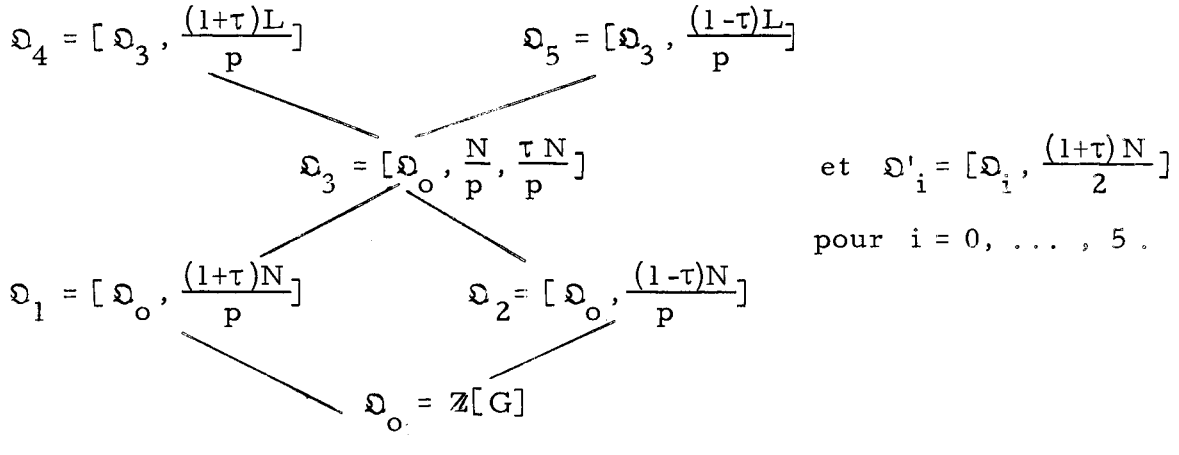
D. S. Rim [3] a démontré que $\mathfrak{P}(\mathbb{Z}[H])$ où H est un groupe cyclique d'ordre p, est isomorphe au groupe des classes d'idéaux du corps des racines $p^{\text{ièmes}}$ de l'unité.

M. P. Lée [1] a montré que $\mathfrak{P}[\mathbb{Z}[G]]$ est isomorphe au groupe des classes d'idéaux du sous-corps réel maximal du corps des racines $p^{\text{ièmes}}$ de l'unité. Il s'agit ici de généraliser ce résultat à un ordre $\mathfrak{O}$ quelconque.

I. - LISTE DES ORDRES DE $\mathbb{Z}$ DANS $\mathbb{Q}[G]$ CONTENANT $\mathbb{Z}[G]$

En écrivant qu'un tel ordre est formé d'entiers de $\mathbb{Q}[G]$ et qu'il est multiplicativement stable, on établit la liste des douze ordres notés $\mathfrak{O}_i$ et $\mathfrak{O}'_i$ $(i = 0, \ldots, 5)$ suivante :

Notations. On pose $N = \sum_{i=0}^{p-1} \sigma_i$, $L = (\sigma - \sigma^{-1})^{p-2}$ et $[\mathfrak{O}, \alpha]$ désigne le $\mathbb{Z}$-module engendré par $\mathfrak{O}$ et α dans $\mathbb{Q}[G]$:



On remarque qu'il existe deux ordres maximaux $\mathfrak{O}'_4$ et $\mathfrak{O}'_5$, conjugués dans le $K[G]$ automorphisme : $\sigma \to \sigma$, $\tau \to -\tau$. De même $\mathfrak{O}_1$ et $\mathfrak{O}_2$, $\mathfrak{O}'_1$ et $\mathfrak{O}'_2$, $\mathfrak{O}_4$ et $\mathfrak{O}_5$ sont conjugués dans ce même automorphisme.

Il suffira donc d'étudier $(\mathfrak{O}_i)$ et $\mathfrak{P}(\mathfrak{O}'_i)$ pour $i = 0, 1, 3, 5$.

II. - INVARIANTS ASSOCIES A UN $\mathfrak{O}$ - MODULE

Pour toute la suite, $\mathfrak{O}$ désigne l'un des ordres ci-dessus, et M un $\mathfrak{O}$-module projectif, de type fini, de rang r (c'est-à-dire tel que le $\mathbb{Q}[G]$ module $\mathbb{Q} \underset{\mathbb{Z}}{\otimes} M$ admette une base formée de r éléments).

Remarquons que $\mathfrak{O}$ étant sans torsion sur $\mathbb{Z}$, M étant projectif sur $\mathfrak{O}$, M est sans torsion sur $\mathbb{Z}$. On peut donc plonger M dans $\mathbb{Q} \underset{\mathbb{Z}}{\otimes} M$ et identifier alors $\mathbb{Q} \underset{\mathbb{Z}}{\otimes} M$ au "produit" $\mathbb{Q}M$.

On désigne par M^g, M^H, M^G, $\bar{M}^G$ les sous $\mathbb{Z}$-modules de M ainsi définis :

$$M^g = \{ x \in M \ / \ \tau x = x \}$$

$$M^H = \{ x \in M \ / \ \sigma x = x \}$$

$$M^G = \{ x \in M \ / \ \tau x = x, \ \sigma x = x \}$$

$$\bar{M}^G = \{ x \in M \ / \ \tau x = -x, \ \sigma x = x \} .$$

Considérons le sous-anneau $\mathbb{Z}[\sigma+\sigma^{-1}]$ de $\mathbb{Z}[G]$ engendré par $\sigma+\sigma^{-1}$, et dans ce sous-anneau l'idéal (N) engendré par $N = 1+\sigma+\ldots+\sigma^{p-1}$. On désigne par A l'anneau quotient $\mathbb{Z}[\sigma+\sigma^{-1}]/_{(N)}$. $\sigma+\sigma^{-1}$ appartenant au centre de $\mathbb{Q}[G]$, M^g est un $\mathbb{Z}[\sigma+\sigma^{-1}]/_{(N)}$ module admettant M^G pour sous-module.

$M^g/_{M^G}$, qui est annulé par N, est donc muni d'une structure de A-module, sans torsion, de type fini, et de rayon 2r.

Premier invariant associé à M

A est isomorphe à l'anneau $\mathbb{Z}'_o$ des entiers du sous-corps réel maximal $\mathbb{Q}'_o$ du corps $\mathbb{Q}'$ des racines $p^{\text{ièmes}}$ de 1. C'est donc un anneau de Dédekind dont on désignera par $\mathcal{K}(A)$ le groupe des classes d'idéaux.

On sait que le A-module projectif $\dfrac{M^g}{M^G}$ est entièrement déterminé -à un isomorphisme près- par son rang 2r et sa classe dans $\mathcal{K}(A)$, classe que nous noterons $\{M\}$.

Il est facile de vérifier que deux modules équivalents dans $\mathfrak{P}(\mathfrak{O})$ ont même classe et que l'application φ qui à $[M] \in \mathfrak{P}(\mathfrak{O})$ associe $\{M\} \in \mathfrak{K}(A)$ est un homomorphisme du groupe $\mathfrak{P}(\mathfrak{O})$ dans le groupe $\mathfrak{K}(A)$.

Deuxième invariant dans le cas $\mathfrak{O} = \mathfrak{O}_3$ ou $\mathfrak{O}'_3$

Soit $L = (\sigma - \sigma^{-1})^{p-2}$ l'élément de $\mathbb{Z}[G]$ défini dans I. La multiplication par L (à gauche) induit un homomorphisme f de groupes additifs de $M^g/_{M^G}$ dans $M/M^H/_{(p)}$ ainsi défini : à la classe de $(1+\tau)x$ modulo M^G $(x \in M)$ f associe la classe de $L(1+\tau)x$ modulo M^H et modulo p.

On démontre que l'image $f(\frac{M^g}{M^G})$ est un $\mathbb{Z}/_{p\mathbb{Z}}$ espace vectoriel de dimension finie n, et on pose :

$$d_{(M)} = n - r \quad .$$

On vérifie que si M et M' sont deux modules équivalents dans $\mathfrak{P}(\mathfrak{O})$, on a $d_{(M)} = d_{(M')}$ et que l'on a $d(P \oplus P') = d(P) + d(P')$.

De sorte que, l'application ψ de $\mathfrak{P}(\mathfrak{O})$ dans $\mathbb{Z}$ qui à $[M]$ associe $d_{(M)}$ est un homomorphisme de groupes.

III. ETUDE DES APPLICATIONS φ ET (φ, ψ) DE $\mathfrak{P}(\mathfrak{O})$ DANS $\mathfrak{K}(A)$ ET $\mathfrak{K}(A) \times \mathbb{Z}$.

On a vu que l'on peut supposer $\mathfrak{O} \neq \mathfrak{O}_4$ et $\mathfrak{O} \neq \mathfrak{O}'_4$, ce que nous ferons désormais pour simplifier l'exposé.

L'étude des noyaux de φ et (φ, ψ) résulte de la proposition 1

PROPOSITION 1. *Soit* M *un* $\mathfrak{O}$*-module projectif, de type fini, de rang déterminé, tel que le* A*-module* $M^g/_{M^G}$ *soit libre, et vérifiant en outre dans le cas* $\mathfrak{O} = \mathfrak{O}_3$ *ou* $\mathfrak{O} = \mathfrak{O}'_3$, $d = 0$.

Alors M *est libre sur* $\mathfrak{O}$.

La construction d'une base de M se fait par les étapes suivantes :

1) Il existe une base de $M^g/_{M^G}$ sur A de la forme

$$\{[(1+\tau)\,\theta_i],\ [(1+\tau)\sigma\,\theta_i]\}_{i=1,\ldots,r}$$

avec $\theta_i \in M$ tel que de plus les r éléments $(\frac{(1+\tau)N}{h}\theta_i)_{i=1,\ldots,r}$ constituent une $\mathbb{Z}$-base de M^G.

(h désigne l'entier 1 , 2 , p ou 2p suivant l'ordre $\mathfrak{O}$ considéré).

2) De tels éléments $(\theta_1,\ldots,\theta_r)$ sont caractérisés par la propriété suivante : leurs r classes modulo $\overline{M}^G$ constituent une base de $M/_{\overline{M}^G}$ sur l'anneau quotient $\mathfrak{O}/_{\overline{\mathfrak{O}}^G}$.

3) Soit $(\mathring{\theta}_1,\ldots,\mathring{\theta}_r)$ une base de $M/_{\overline{M}^G}$ sur $\mathfrak{O}/_{\overline{\mathfrak{O}}^G}$. Il existe r éléments $(\mathring{\omega}_1,\ldots,\mathring{\omega}_r)$ inversibles de $\mathfrak{O}_o/_{\overline{\mathfrak{O}}_o^G}$ tels que la base $(\widehat{\omega_1\,\theta_1},\ldots,\widehat{\omega_r\,\theta_r})$ admette un système de représentants $(\varphi_1,\ldots,\varphi_r)$ tels que si on pose $\overline{T} = \frac{(1-\tau)N}{h'}$, (où h' vaut 1 , 2 , p ou 2p suivant les r éléments $(\overline{T}\varphi_1,\ \ldots,\ \overline{T}\varphi_2)$ soient une base sur $\mathbb{Z}$ de $\overline{M}^G$.

Il est clair que $(\varphi_1,\ldots,\varphi_r)$ est alors une base de M sur $\mathfrak{O}$.

Conséquence de la proposition 1.

Les homomorphismes de groupes suivants :

φ de $\mathfrak{P}(\mathfrak{O})$ dans $\mathcal{K}(A)$: $[P]\xrightarrow{\varphi}\{P\}$ pour $\mathfrak{O}\neq\mathfrak{O}_3$, $\mathfrak{O}'_3$

(φ,ψ) de $\mathfrak{P}(\mathfrak{O})$ dans $\mathcal{K}(A)\times\mathbb{Z}$: $[P]\xrightarrow{(\varphi,\psi)}(\{P\},d(P))$ pour $\mathfrak{O}=\mathfrak{O}_3$ ou $\mathfrak{O}=\mathfrak{O}'_3$

sont donc injectifs.

De plus, un module P appartient à la classe $[O]$ de $\mathfrak{P}(\mathfrak{O})$ si et seulement si il est libre.

Il reste à étudier l'image de $\mathfrak{P}(\mathfrak{O})$ par l'application φ ou l'application $(\varphi;\psi)$. Nous allons déduire cette étude du résultat démontré par M. P. Lée [1].

PROPOSITION 2. Pour tout idél $\mathfrak{A} \in \mathcal{K}(A)$, il existe un $\mathfrak{O}$-module projectif de type fini de rang déterminé P tel que l'on ait : $\{P\} = \mathfrak{A}$.

Démonstration. Rappelons que tout $\mathbb{Z}[G]$-module projectif de type fini est de rang déterminé, d'après un théorème de Swann.

M. P. Lée a démontré que $\mathfrak{P}(\mathbb{Z}[G])$ est un groupe isomorphe au groupe fini $\mathcal{K}(\mathbb{Z}'_o)$ lui-même isomorphe à $\mathcal{K}(A)$.

$\mathfrak{P}(\mathbb{Z}[G])$ et $\mathcal{K}(A)$ ont donc même cardinal fini et l'injection :

$$\varphi : \mathfrak{P}[\mathbb{Z}[G]] \to \mathcal{K}(A)$$

est une surjection.

Soit alors $\mathfrak{A}$ un élément de $\mathcal{K}(A)$. Il existe un $\mathbb{Z}[G]$-module projectif de type fini (et de rang déterminé) P_o tel que l'on ait :

$$\{P_o\} = \mathfrak{A} .$$

Puisque l'on se place dans le cas $\mathfrak{O} \neq \mathfrak{O}_4$ et $\mathfrak{O} \neq \mathfrak{O}'_4$, il est facile de voir que le $\mathfrak{O}$-module projectif de type fini, de même rang que P_o :

$$\mathfrak{O} \underset{\mathbb{Z}}{\otimes} P_o = \mathfrak{O} P_o ,$$

vérifie :

$$\{\mathfrak{O} P_o\} = \mathfrak{A} .$$

Etudions mainteant deux $\mathfrak{O}_3$-modules importants. On démontre la proposition suivante :

PROPOSITION 3. Les $\mathfrak{O}_3$ (resp. $\mathfrak{O}'_3$)-modules $\mathfrak{O}_4$ (resp. $\mathfrak{O}'_4$) et $\mathfrak{O}_5$ (resp. $\mathfrak{O}'_5$) sont projectifs de rang 1 , et on a :

$$\begin{cases} d_{\mathfrak{O}_4} = d_{\mathfrak{O}'_4} = +1 , \\ d_{\mathfrak{O}_5} = d_{\mathfrak{O}'_5} = -1 , \\ \{\mathfrak{O}_4\} = \{\mathfrak{O}'_4\} = \{\mathfrak{O}_5\} = \{\mathfrak{O}'_5\} = \{1\} . \end{cases}$$

Remarquons que la proposition 2 permet alors d'affirmer que $\mathfrak{O}_4 \oplus \mathfrak{O}_5$ est un $\mathfrak{O}_3$-module libre.

Nous sommes maintenant en mesure de démontrer le théorème suivant qui donne la structure de $\mathfrak{P}(\mathfrak{O})$

THEOREME. Soient G le groupe diédral d'ordre 2p (où p est un nombre premier impair)

$\mathfrak{O}$ un ordre de $\mathbb{Z}$ dans $\mathbb{Q}[G]$ contenant $\mathbb{Z}[G]$,

$\mathbb{Z}'_o$ l'anneau des entiers du sous-corps réel maximal du corps des racines $p^{\text{ièmes}}$ de l'unité,

$\mathcal{K}(\mathbb{Z}'_o)$ le groupe des classes d'idéaux de $\mathbb{Z}'_o$.

Alors le groupe des classes projectives $\mathfrak{P}(\mathfrak{O})$ de l'anneau $\mathfrak{O}$ est isomorphe à $\mathcal{K}(\mathbb{Z}'_o)$ sauf dans le cas des ordres $\mathfrak{O}_3$ et $\mathfrak{O}'_3$ auxquels cas il est isomorphe au groupe produit $\mathcal{K}(\mathbb{Z}'_o) \times \mathbb{Z}$.

Démonstration. (On suppose $\mathfrak{O} \neq \mathfrak{O}_4$, $\mathfrak{O} \neq \mathfrak{O}'_4$).

Dans le cas $\mathfrak{O} \neq \mathfrak{O}_3$, $\mathfrak{O} \neq \mathfrak{O}'_3$, l'application φ :

$\mathfrak{P}(\mathfrak{O}) \to \mathcal{K}(A)$ qui à $[M]$ associe la classe de $M^g/_{M^G}$ dans $\mathcal{K}(A)$ est un isomorphisme en vertu des propositions 1 et 2.

Bien entendu, l'isomorphisme :

$\mathfrak{P}(\mathfrak{O}) \to \mathcal{K}(\mathbb{Z}'_o)$ qui en résulte dépendra alors du choix d'un caractère de $\mathbb{Q}[G]$ dans $\mathbb{Q}'$.

Dans le cas $\mathfrak{O} = \mathfrak{O}_3$ (resp. $\mathfrak{O}'_3$) , soit $(d, \mathfrak{A}) \in \mathcal{K}(A)$.

D'après la proposition 2, il existe un $\mathfrak{O}$-module projectif et de type fini, de rang déterminé P tel que l'on ait :

$$\{P\} = \mathfrak{A} .$$

Posons alors $d' = d - d_P$, et considérons l'un des 3 modules M ainsi définis :

si $d' = 0$: $M = P$

si $d' > 0$: $M = P \oplus \underbrace{\mathfrak{Q}_4 \oplus \ldots \oplus \mathfrak{Q}_4}_{d'}$ (resp. $P \oplus \underbrace{(\mathfrak{Q}'_4 \oplus \ldots \oplus \mathfrak{Q}'_4)}_{d'}$)

si $d' < 0$: $M = P \oplus \underbrace{\mathfrak{Q}_5 \oplus \ldots \oplus \mathfrak{Q}_5}_{-d'}$ (resp. $P \oplus \underbrace{(\mathfrak{Q}'_5 \oplus \ldots \oplus \mathfrak{Q}'_R)}_{-d'}$) .

La proposition 3 prouve alors que l'on a :

$$\begin{cases} d_M = d \\ \{M\} = \{P\} = \mathfrak{U} \end{cases} .$$

-:-:-:-

BIBLIOGRAPHIE

[1] M. P. LEE. - Integral representation of dihedral groups of order 2p . Trans. Amer. Math. Soc. 110 (1964) p. 213-231.

[2] J. MARTINET. - Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre 2p. Thèse, Ann. Inst. Fourier, Grenoble, 19, 1 (1969) 80 p.

[3] D. S. RIM. - Modules over finites groups. Ann. of. Math. 69 (1959) p. 700-712.

-:-:-:-