

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 $\mathbb{Q}$**

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

© Université Bordeaux 1, 1969-1970, tous droits réservés.

L'accès aux archives du séminaire de théorie des nombres de Bordeaux implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

GRUPE DES CLASSES PROJECTIVES D'UN ORDRE
 Ω 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 :

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

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 $\mathbb{Q} \otimes M$ soit $\mathbb{Q}[G]$ -libre de rang 1) sur l'algèbre $\mathbb{Z}[G]$ (J. Martinet [2]).

Plus généralement, si l'on ne suppose plus l'extension modérément ramifiée, on 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 Ω un ordre de $\mathbb{Z}$ dans $\mathbb{Q}[G]$ contenant $\mathbb{Z}[G]$. On dit que deux modules projectifs de type fini sur Ω et de rangs déterminés, P et P' , sont équivalents s'il existe deux Ω -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 $\mathfrak{P}(\mathfrak{Q})$ est appelé groupe des classes projectives de $\mathfrak{Q}$.

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 $\mathfrak{Q}$ quelconque.

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

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

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

$$\begin{array}{ccc}
 \mathfrak{Q}_4 = [\mathfrak{Q}_3, \frac{(1+\tau)L}{p}] & & \mathfrak{Q}_5 = [\mathfrak{Q}_3, \frac{(1-\tau)L}{p}] \\
 & \swarrow \quad \searrow & \\
 & \mathfrak{Q}_3 = [\mathfrak{Q}_0, \frac{N}{p}, \frac{\tau N}{p}] & \\
 & \swarrow \quad \searrow & \\
 \mathfrak{Q}_1 = [\mathfrak{Q}_0, \frac{(1+\tau)N}{p}] & & \mathfrak{Q}_2 = [\mathfrak{Q}_0, \frac{(1-\tau)N}{p}] \\
 & \swarrow \quad \searrow & \\
 & \mathfrak{Q}_0 = \mathbb{Z}[G] &
 \end{array}
 \quad \text{et } \mathfrak{Q}'_i = [\mathfrak{Q}_i, \frac{(1+\tau)N}{2}]$$

pour $i = 0, \dots, 5$.

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

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

II. - INVARIANTS ASSOCIES A UN $\mathbb{Q}$ - MODULE

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

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

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

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

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

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

$$\overline{M}^G = \{ x \in M \mid \tau x = -x, \sigma x = x \}.$$

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 $N = 1 + \sigma + \dots + \sigma^{p-1}$. 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 $\mathbb{Z}'_0$ des entiers du sous-corps réel maximal $\mathbb{Q}'_0$ 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 $\frac{M^g}{M^G}$ 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 $\mathfrak{P}(\mathfrak{Q})$ ont même classe et que l'application φ qui à $[M] \in \mathfrak{P}(\mathfrak{Q})$ associe $\{M\} \in \mathfrak{K}(A)$ est un homomorphisme du groupe $\mathfrak{P}(\mathfrak{Q})$ dans le groupe $\mathfrak{K}(A)$.

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

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 :

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

On vérifie que si M et M' sont deux modules équivalents dans $\mathfrak{P}(\mathfrak{Q})$, 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 $\mathfrak{P}(\mathfrak{Q})$ dans $\mathbb{Z}$ qui à $[M]$ associe $d_{(M)}$ est un homomorphisme de groupes.

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

On a vu que l'on peut supposer $\mathfrak{Q} \neq \mathfrak{Q}_4$ et $\mathfrak{Q} \neq \mathfrak{Q}'_4$, 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 $\mathfrak{Q}$ -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 $\mathfrak{Q} = \mathfrak{Q}_3$ ou $\mathfrak{Q} = \mathfrak{Q}'_3$, $d = 0$.

Alors M est libre sur $\mathfrak{Q}$.

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

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

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

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

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

2) De tels éléments $(\theta_1, \dots, \theta_r)$ 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 $(\dot{\theta}_1, \dots, \dot{\theta}_r)$ une base de $M/\overline{M}^G$ sur $\mathfrak{O}/\overline{\mathfrak{O}}^G$. Il existe r éléments $(\dot{w}_1, \dots, \dot{w}_r)$ inversibles de $\mathfrak{O}_0/\overline{\mathfrak{O}}_0^G$ tels que la base $(\widehat{w}_1\theta_1, \dots, \widehat{w}_r\theta_r)$ admette un système de représentants $(\varphi_1, \dots, \varphi_r)$ tels que si on pose $\overline{T} = \frac{(1-\tau)N}{h'}$, (où h' vaut 1, 2, p ou $2p$ suivant les r éléments $(\overline{T}\varphi_1, \dots, \overline{T}\varphi_r)$ soient une base sur $\mathbb{Z}$ de $\overline{M}^G$.

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

Conséquence de la proposition 1.

Les homomorphismes de groupes suivants :

$$\begin{aligned} \varphi \quad \text{de } \mathfrak{P}(\mathfrak{Q}) \text{ dans } \mathcal{K}(A) & : [P] \xrightarrow{\varphi} \{P\} \quad \text{pour } \mathfrak{Q} \neq \mathfrak{Q}_3, \mathfrak{Q}'_3 \\ (\varphi, \psi) \quad \text{de } \mathfrak{P}(\mathfrak{Q}) \text{ dans } \mathcal{K}(A) \times \mathbb{Z} & : [P] \xrightarrow{(\varphi, \psi)} (\{P\}, d(P)) \quad \text{pour } \mathfrak{Q} = \mathfrak{Q}_3 \text{ ou } \mathfrak{Q} = \mathfrak{Q}'_3 \end{aligned}$$

sont donc injectifs.

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

Il reste à étudier l'image de $\mathfrak{P}(\mathfrak{Q})$ 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 idéal $\mathfrak{U} \in \mathcal{K}(A)$, il existe un $\mathfrak{D}$ -module projectif de type fini de rang déterminé P tel que l'on ait : $\{P\} = \mathfrak{U}$.

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 $\mathcal{K}(\mathbb{Z}'_0)$ lui-même isomorphe à $\mathcal{K}(A)$.

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

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

est une surjection.

Soit alors $\mathfrak{U}$ un élément de $\mathcal{K}(A)$. Il existe un $\mathbb{Z}[G]$ -module projectif de type fini (et de rang déterminé) P_0 tel que l'on ait :

$$\{P_0\} = \mathfrak{U}.$$

Puisque l'on se place dans le cas $\mathfrak{D} \neq \mathfrak{D}_4$ et $\mathfrak{D} \neq \mathfrak{D}'_4$, il est facile de voir que le $\mathfrak{D}$ -module projectif de type fini, de même rang que P_0 :

$$\mathfrak{D} \otimes_{\mathbb{Z}} P_0 = \mathfrak{D} P_0,$$

vérifie :

$$\{\mathfrak{D} P_0\} = \mathfrak{U}.$$

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

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

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

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

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

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

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

$\mathbb{Z}'_0$ l'anneau des entiers du sous-corps réel maximal du corps des racines $p^{\text{ièmes}}$ de l'unité,

$\mathcal{K}(\mathbb{Z}'_0)$ le groupe des classes d'idéaux de $\mathbb{Z}'_0$.

Alors le groupe des classes projectives $\mathfrak{P}(\mathfrak{D})$ de l'anneau $\mathfrak{D}$ est isomorphe à $\mathcal{K}(\mathbb{Z}'_0)$ sauf dans le cas des ordres $\mathfrak{D}_3$ et $\mathfrak{D}'_3$ auxquels cas il est isomorphe au groupe produit $\mathcal{K}(\mathbb{Z}'_0) \times \mathbb{Z}$.

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

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

$\mathfrak{P}(\mathfrak{D}) \rightarrow \mathcal{K}(A)$ 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 :

$\mathfrak{P}(\mathfrak{D}) \rightarrow \mathcal{K}(\mathbb{Z}'_0)$ qui en résulte dépendra alors du choix d'un caractère de $\mathbb{Q}[G]$ dans $\mathbb{Q}'$.

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

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

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

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

$$\text{si } d' = 0 : M = P$$

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

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

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 finite groups. Ann. of Math. 69 (1959) p. 700-712.

-:-:-:-