Séminaire Delange-Pisot-Poitou. Théorie des nombres

Anne-Marie Berge

Sur l'arithmétique d'une extension diédrale

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 12 (1970-1971), exp. n° 14, p. 1-14

<http://www.numdam.org/item?id=SDPP_1970-1971__12__A9_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
12e année, 1970/71, n° 14, 14 p.

1er mars 1971

SUR L'ARITHMÉTIQUE D'UNE EXTENSION DIÉDRALE

par Anne-Marie BERGE

1. Introduction.

Rappelons d'abord quelques résultats relatifs aux extensions abéliennes. Soient E une extension abélienne de degré fini des rationnels, et G son groupe de Galois. Le théorème 132 de Hilbert peut s'énoncer de la manière suivante :

Si l'extension $E|\mathbb{Q}$ est modérément ramifiée, l'anneau des entiers de E est un $\mathbb{Z}[G]$-module libre.

LEOPOLDT [3] a étudié la structure de l'anneau des entiers de E sans hypothèse restrictive sur la ramification. On ne peut alors obtenir le même résultat. On démontre [4], en effet : Soient A un anneau de Dedekind, K son corps des fractions, E une extension galoisienne de K, G le groupe de Galois de E/K, B la clôture intégrale de A dans E ; alors B est un $A[G]$-module projectif si, et seulement si, l'extension E/K est modérément ramifiée.

Conservons les notations ci-dessus. Pour étudier l'anneau B dans le cas d'une ramification quelconque, on est amené à le considérer comme module, non plus sur $A[G]$, mais sur le sous-anneau de $K[G]$, noté $D(B)$, et égal à l'ensemble des éléments λ de $K[G]$ tels que, pour tout $x \in B$, λx appartienne à B. On verra que $D(B)$ est un ordre de A dans $K[G]$, et on l'appellera ordre associé à B.

On peut alors énoncer ainsi le résultat de LEOPOLDT :

L'anneau des entiers d'une extension abélienne des rationnels est un module libre sur l'ordre qui lui est associé dans $\mathbb{Q}[G]$.

La méthode employée pour les extensions abéliennes ne s'étend pas aux extensions galoisiennes quelconques. D'ailleurs, il n'y a pas de résultat général.

J. MARTINET [5] a construit une extension galoisienne des rationnels de groupe de Galois quaternionique d'ordre 8, qui est modérément ramifiée, et dont l'anneau des entiers n'est pas un $\mathbb{Z}[G]$-module libre.

On se propose d'exposer ici un résultat analogue à celui de LEOPOLDT, dans le cas d'une extension galoisienne non abélienne de degré $2p$ (où p est un nombre premier impair).

Dans toute la suite, on désigne par G un groupe diédral d'ordre $2p$, et par A

un anneau principal de corps de fractions K qui vérifie les hypothèses (H) suivantes :

(H_1) 2 est inversible dans A, ou bien tel que $A/2A$ soit un corps à 2 éléments ;

(H_2) p est inversible dans A, ou bien tel que A/pA soit un corps à p éléments ;

(H_3) Le polynôme $\sum_{i=0}^{i=p-1} X^i$ est irréductible dans $K[X]$.

Remarquons que les hypothèses (H) sont stables par localisation, et que, lorsque p n'est pas inversible dans H, (H_3) est une conséquence de (H_2) [4].

THÉORÈME. - *Si E est une extension galoisienne de K, dont le groupe de Galois est isomorphe à G, l'anneau des entiers de E est un module libre sur son ordre associé dans $K[G]$.*

Nous verrons que la nature de l'ordre associé à l'anneau B des entiers de E dépend de la ramification de E/K. Le résultat de J. MARTINET [4] sur les extensions diédrales modérément ramifiées apparaîtra ainsi comme un cas particulier du théorème.

L'étude de B comme module sur son ordre associé sera, suivant une suggestion de J.-P. SERRE, rattachée à la recherche d'invariants, pour les $A[G]$-modules de type fini et de "rang 1 ", qui permettent de caractériser ceux qui sont projectifs ou libres sur leurs "ordres associés" dans $K[G]$.

Il restera ensuite à calculer ces invariants pour l'anneau B.

2. Ordres de A dans $K[G]$ contenant $A[G]$.

On rappelle qu'un ordre de A dans $K[G]$ est un sous-anneau de $K[G]$ contenant une base de $K[G]$ sur K, et dont tous les éléments sont entiers sur A.

Notations. - Soient $H = \{1, \sigma, \ldots, \sigma^{p-1}\}$ et $g = \{1, \tau\}$ des sous-groupes de G d'ordres respectifs p et 2. On pose

$$N = \sum_{i=0}^{p-1} \sigma^i \qquad \text{et} \qquad L = (\sigma - \sigma^{-1})^{p-2} .$$

K' désigne l'extension de K obtenue par adjonction des racines p-ièmes de l'unité, K'_0 le sous-corps de K' de degré $(p-1)/2$, A'_0 la clôture intégrale de A dans K'_0.

PROPOSITION 2.1. - Les ordres de A dans $K[G]$, qui contiennent $A[G]$, sont les sous-A-modules de $K[G]$ suivants :

$D_0 = A[G]$; $D_1 = [A[G], ((1+\tau)N)/p]$; $D_2 = [A[G], ((1-\tau)N)/p]$,

$D_3 = [A[G], N/p, \tau N/p]$; $D_4 = [D_3, ((1+\tau)L)/p]$; $D_5 = [D_3, ((1-\tau)L)/p]$,

et, pour tout i, $0 \leqslant i \leqslant 5$, $D_i' = [D_i, ((1+\tau)N)/2]$.

Démonstration. - Il est facile de vérifier que les A-modules D_i et D_i' sont, pour tout i, $0 \leqslant i \leqslant 5$, des ordres de A dans $K[G]$. Pour vérifier qu'il n'y en a pas d'autres, on démontre d'abord le lemme suivant.

LEMME 2.1. - D_4' et D_5' sont des ordres maximaux.

On peut, pour cela, utiliser la théorie des discriminants d'algèbres (discriminants relatifs à la forme bilinéaire trace) ; on sait, en effet, que pour qu'un ordre de A dans $K[G]$ soit maximal, il faut et il suffit que son discriminant soit égal au discriminant Δ de la K-algèbre $K[G]$. Le calcul de Δ se ramène, grâce à l'isomorphisme

$$K[G] \simeq K \times K \times \mathfrak{M}_2(K_0')$$

(où $\mathfrak{M}_2(K_0')$ est l'algèbre des matrices d'ordre 2 à coefficients dans K_0'), à celui du discriminant de l'ordre maximal $\mathfrak{M}_2(A_0')$ de A dans $\mathfrak{M}_2(K_0')$.

Le calcul des discriminants des ordres D_4' et D_5' se ramène à celui de $A[G]$, grâce aux isomorphismes

$$D_4'/A[G] \simeq D_5'/A[G] \simeq A/pA \times A/pA \times A/2pA \ .$$

On trouve comme valeur commune à Δ et à ces discriminants, $2^{2p-2} \times p^{2p-6}$, ce qui achève la démonstration du lemme.

Il est clair que l'on peut se borner, pour la démonstration de la proposition 2.1, aux cas où A est un anneau de valuation discrète d'idéal maximal mA, avec $m = 2$ ou $m = p$.

Dans le premier cas, on voit facilement que D_0 et D_0' sont les seuls ordres de A dans $K[G]$ contenant $A[G]$: Tout ordre maximal doit en effet contenir l'entier du centre $((1+\tau)N)/2$, donc, d'après le lemme 2.1, être égal à D_0'. On conclut en remarquant que le A-module D_0'/D_0 est simple.

On suppose désormais A local d'idéal maximal pA, et on étudie les entiers de $K[G]$ de la forme $(1+\varepsilon\tau)\mu$, avec $\varepsilon = \pm 1$ et $\mu \in K[H]$. Pour $\mu = \sum_{i=0}^{p-1} k_i \sigma_i$,

$k_i \in K$, on pose $\bar{\mu} = \sum_{i=0}^{p-1} k_i \sigma^{-i}$. On voit que, pour que $(1 + \varepsilon\tau)\mu$ soit entier sur A , il faut et il suffit que $\mu + \bar{\mu}$ soit entier sur A , donc, en raison de l'isomorphisme $K[H]/(N) \simeq K'$, de la forme $aN/p + \alpha$, $a \in A$, $\alpha \in A[H]$.

Soit D un ordre de A dans $K[G]$ contenant $A[G]$, et soit $\lambda \in D$.

En écrivant que $(1 + \varepsilon\tau)\lambda$ et $(1 + \varepsilon\tau)\lambda\sigma$ appartiennent à D , pour $\varepsilon = \pm 1$, on déterminera la forme de λ grâce au lemme suivant.

LEMME 2.2. - Soient a , $a' \in A$, α , $\alpha' \in A[H]$, et $\mu \in K[H]$ tel que

$$\mu + \bar{\mu} = aN/p + \alpha \qquad \text{et} \qquad \mu^{\sigma} + \bar{\mu}^{\sigma-1} = a'N/p + \alpha' \ .$$

Alors μ est de la forme $u\,N/p + v\,L/p + \beta$, u , $v \in A$, $\beta \in A[H]$.

On en déduit sans peine que D est égal à l'un des D_i , $0 \leqslant i \leqslant 5$.

Citons ici une propriété des ordres maximaux :

PROPOSITION 2.2. - Les D_3-modules D_4 et D_5 (respectivement D_3'-modules D_4' et D_5') sont projectifs.

Démonstration. - Nous verrons plus loin (théorème 4.1) qu'en fait le D_3-module $D_4 \oplus D_5$ est libre. Mais il nous suffit ici de vérifier cette propriété localement, et même dans le seul cas où A est un anneau de valuation discrète d'idéal maximal pA .

LEMME 2.3. - On pose

$$L' = \sum_{i=0}^{p-1} i\sigma^{2i} \qquad \text{et} \qquad L_0' = ((p-1)/2)(\sigma^2 - 1) + N/p \ .$$

Alors L' est congru à $-L$ modulo $pA[H]$, et on a $L'L_0' = p((p-1)/2)$.

On peut alors construire une suite exacte et scindée de D_3-modules

$$0 \longrightarrow \operatorname{Ker} f \longrightarrow D_4 \oplus D_5 \xrightarrow{f} D_3 \longrightarrow 0 \ ,$$

où f associe, à $(x , y) \in D_4 \oplus D_5$, $((x - y)L_0')/(p - 1)$. Il est facile de voir que $\operatorname{Ker} f$ est isomorphe à D_3 , d'où la proposition 2.2.

Remarque. - On peut construire une représentation φ (respectivement ψ) de $K[G]$ sur $K \times K \times \mathfrak{M}_2(K_0')$, qui envoie l'ordre D_4' (respectivement D_5') sur $A \times A \times \mathfrak{M}_2(A_0')$:

Soit ω une racine p-ième primitive de l'unité. Définissons ψ à partir des

caractères χ_0 , χ_1 , χ suivants :

$$\begin{cases} \chi_0 : G \to K^* & \text{défini par} \quad \chi_0(\sigma) = 1 \ , \ \chi_0(\tau) = 1 \ , \\ \chi_1 : G \to K^* & \text{défini par} \quad \chi_1(\sigma) = 1 \ , \ \chi_1(\tau) = -1 \ , \\ \chi : G \to (\mathfrak{M}_2(K_0'))^* & \text{défini par} \quad \chi(\sigma) = \begin{pmatrix} \omega + \omega^{-1} & -1 \\ 1 & 0 \end{pmatrix} , \ \chi(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} . \end{cases}$$

L'image de D_5' par ψ est un ordre maximal contenu dans $A \times A \times \mathfrak{M}_2(A_0')$, donc lui est égale.

(Pour φ , on remplace χ par χ' : $\chi'(\sigma) = \chi(\sigma)$, $\chi'(\tau) = -\chi(\tau)$.)

3. Invariants associés à un $A[G]$-module.

Tous les $A[G]$-modules à gauche considérés sont de type fini, sans A-torsion, de rang défini.

Soit M un tel $A[G]$-module. Rappelons qu'il est de rang r , si le $K[G]$-module $M_K = K \otimes_A M$ est libre avec une base à r éléments. Puisque M est sans A-torsion, il sera désormais considéré comme sous-$A[G]$-module de M_K .

Pour tout sous-groupe G' de G , nous notons $M^{G'}$ le sous-A-module de M invariant par G' . Considérons en particulier les A-modules M^g et M^G . On a clairement $M^g \supset M^G$.

Les générateurs σ et τ de G étant liés par $\tau\sigma = \sigma^{-1}\tau$, on voit que $\sigma + \sigma^{-1}$ appartient au centre de $A[G]$. M^g et M^G sont donc des sous-$A[\sigma + \sigma^{-1}]$-modules de M (où $A[\sigma + \sigma^{-1}]$ désigne la sous-A-algèbre de $A[G]$ engendrée par $\sigma + \sigma^{-1}$).

De plus, il est clair que, pour tout $x \in M^g$, Nx appartient à M^G .

Le A-module quotient M^g/M^G peut donc être canoniquement muni d'une structure de module sur l'anneau quotient $R = A[\sigma + \sigma^{-1}]/(N)$.

Or R est un anneau de Dedekind. Plus précisément, il est isomorphe à l'anneau d'entiers A_0' (un tel isomorphisme n'est pas canonique : il y a autant d'isomorphismes que de couples (χ , χ^{-1}) de caractères non triviaux de H dans K^* , c'est-à-dire $(p-1)/2$).

Comme le R-module M^g/M^G est sans torsion, de type fini, et de rang $2r$, il est isomorphe à une somme directe $R^{2r-1} \oplus \mathfrak{A}$, où $\mathfrak{A}$ est un idéal de R que cette condition détermine, à la multiplication par un idéal principal près [1].

DÉFINITION 3.1. - On notera $\{M\}$ la classe, dans le groupe $\mathcal{K}(R)$ des classes d'idéaux de R , d'un idéal $\mathfrak{A}$ de R tel que M^g/M^G soit isomorphe à $R^{2r-1} \oplus \mathfrak{A}$.

Soit $\mathfrak{O}$ un ordre de A dans $K[G]$ contenant $A[G]$. On vérifie facilement que $\{\mathfrak{O}\}$ est la classe principale de $\mathcal{K}(R)$.

Mais la proposition 2.2 donne un exemple de $\mathfrak{O}_3$-module projectif de rang 1, à savoir $M = \mathfrak{O}_4$ ou $M = \mathfrak{O}_5$, pour lequel $\{M\}$ est la classe principale, et qui n'est pas libre sur $\mathfrak{O}_3$.

On est ainsi amenés, pour caractériser les $\mathfrak{O}$-modules localement libres, à associer à M un deuxième invariant, défini, lorsque p n'est pas inversible dans A, de la façon suivante : Le A-module quotient $M/(pM + M^H)$ peut être canoniquement muni d'une structure d'espace vectoriel sur A/pA. On définit une application f de M^g/M^G dans $M/(pM + M^H)$: soit $X \in M^g/M^G$. L'identité

$$p\tau = pN\tau + L'(1 - \tau) - (1 + \tau)L'$$

montre que X admet un représentant dans M^g de la forme $(1 + \tau)x$, $x \in M$. La classe modulo $pM + M^H$ de l'élément $L(1 + \tau)x$, qui ne dépend pas du choix de ce représentant, est notée $f(X)$.

On vérifie que $f(M^g/M^G)$ est un sous-A/pA-espace vectoriel de $M/(M^H + pM)$, de dimension inférieure ou égale à $2r$.

DÉFINITION 3.2. - On note $d(M)$ l'entier défini de la façon suivante : Lorsque p n'est pas inversible dans A, on pose

$d(M) = n - r$, où n est la dimension de $f(M^g/M^G)$, et r le rang de M.

Lorsque p est inversible dans A, on pose

$d(M) = 0$.

Soit $\mathfrak{O}$ un ordre de A dans $K[G]$ contenant $A[G]$. Lorsque p n'est pas inversible dans A, on peut calculer $d(\mathfrak{O})$: si i, $0 \leqslant i \leqslant 5$, est l'entier défini par $\mathfrak{O} = \mathfrak{O}_i$ ou $\mathfrak{O}_i'$, on trouve

$$d(\mathfrak{O}) = 0, \quad \text{pour } i \leqslant 3,$$

$$d(\mathfrak{O}) = +1, \quad \text{pour } i = 4,$$

$$d(\mathfrak{O}) = -1, \quad \text{pour } i = 5.$$

En vue de l'application arithmétique annoncée dans le paragraphe 1, on associe à tout $A[G]$-module de rang $r = 1$ un ordre de A dans $K[G]$:

DÉFINITION 3.3. - Soit M un $A[G]$ de rang 1. L'ensemble $\mathfrak{O}(M)$ des éléments λ de $K[G]$, tels que, pour tout $x \in M$, λx appartienne à M, est appelé ordre associé à M dans $K[G]$.

(Il est en effet facile de vérifier que $D(M)$ est un ordre de A dans $K[G]$.)

Lorsque M est un $A[G]$-module de rang 1, la valeur de l'entier $d(M)$ ($-1 \leqslant d(M) \leqslant +1$) est liée à la nature de l'ordre $D(M)$. Comme $d(M)$ est invariant par localisation pour p, il suffit de le calculer lorsque A est local d'idéal maximal pA.

PROPOSITION 3.1. - *Soient M un $A[G]$-module de rang 1, $D(M)$ son ordre associé dans $K[G]$, et i, $0 \leqslant i \leqslant 5$, l'entier tel que $D(M) = D_i$.*

Alors on a $d(M) = d[D(M)]$, sauf peut-être pour $i = 1$ (auquel cas on peut avoir $d(M) = 0$ ou $d(M) = -1$) et pour $i = 2$ (auquel cas on peut avoir $d(M) = 0$ ou $d(M) = +1$).

Remarquons que le cas $d(M) \neq d[D(M)]$ peut effectivement se présenter. Le sous-$A[G]$-module de $K[G]$, engendré par D_1 et $((1 - \tau)L)/p$, a pour ordre associé D_1, et pour invariant $d = -1$.

On va voir (proposition 4.1) qu'il n'est pas projectif sur son ordre associé.

4. Résultats sur les $A[G]$-modules.

Nous utiliserons, pour l'étude de l'arithmétique d'une extension diédrale, le résultat suivant :

PROPOSITION 4.1. - *Soient M un $A[G]$-module de type fini, de rang 1, et $D(M)$ l'ordre qui lui est associé dans $K[G]$. Alors :*

1° M est projectif sur $D(M)$ si, et seulement si, l'on a $d(M) = d[D(M)]$;

2° Si cette condition est vérifiée, M est libre sur $D(M)$ si, et seulement si, $\{M\}$ est la classe principale de $K(R)$.

On déduit cette proposition, par globalisation pour le 1° et comme cas particulier pour le 2°, du théorème suivant :

THÉORÈME 4.1. - *Soient D un ordre de A dans $K[G]$ qui contient $A[G]$, M un D-module de type fini de rang r, tel que $\{M\}$ soit la classe principale de $K(R)$. On suppose en outre que M vérifie l'une des deux hypothèses suivantes : M est projectif sur D, ou bien M est de rang 1 et D est son ordre associé.*

Alors M est libre sur D si, et seulement si, $d(M) = rd(D)$.

Démonstration du théorème 4.1. - Pour simplifier l'exposé, nous supposerons $D \neq D_4$ et D_4' (le choix de l'invariant $\{M\}$ introduit en effet une dissymétrie), et $r = 1$.

1° On étudie d'abord les A-modules libres de rang 1 , M^G et $\overline{M}^G$ ($\overline{M}^G$ désigne l'ensemble des éléments x de M^H tels que $\tau x = -x$). Soient $\{T\}$ et $\{\overline{T}\}$ des A-bases de D^G et $\overline{D}^G$ (par exemple, pour D_1' , $T = ((1+\tau)N)/2p$, $\overline{T} = ((1-\tau)N)/2$). On montre que les applications $x \to Tx$ et $x \to \overline{T}x$ sont des surjections de M sur M^G et $\overline{M}^G$.

2° On remarque que le R-module D^g/D^G admet pour base $[(1+\tau)]$ et $[(1+\tau)\sigma]$.

On dira qu'une R-base de M^g/M^G est normale, si elle est de la forme $\{[(1+\tau)\theta] , [(1+\tau)\sigma\theta]\}$, où $\theta \in M$ est tel que $\{T\theta\}$ soit une A-base de M^G .

Une base $\{X , Y\}$ de M^g/M^G sera dite semi-normale, si X est de la forme $[(1+\tau)x]$, avec $x \in M$ tel que $\{Tx\}$ soit une A-base de M^G .

On montre facilement que, si $((1+\tau)N)/p$ appartient à D , toute R-base de M^g/M^G est semi-normale. Si $((1+\tau)N)/p$ n'appartient pas à D , il existe une base semi-normale $\{X , Y\}$ de M^g/M^G , et alors $f(X)$ n'est pas nul (f désigne l'application citée dans la définition 3.2).

Cette application f intervient dans la recherche des bases normales de la façon suivante :

LEMME 4.1. - Soit $X \in M^g/M^G$. Pour que X admette un représentant de la forme $(1+\tau)(\sigma - \sigma^{-1})x$, $x \in M$, il faut et il suffit que l'on ait $f(X) = 0$.

Les bases normales de M^g/M^G apparaissent donc comme les bases semi-normales $\{X , Y\}$ telles que $f(X) = f(Y)$, et on aboutit à la condition suivante :

Pour qu'il existe une R-base normale de M^g/M^G , il faut et il suffit que l'on ait $d(M) \leqslant 0$ (rappelons que l'on a écarté le cas $D = D_4$).

3° L'intérêt des bases normales est lié à la remarque suivante :

Il est clair qu'à une base normale $\{[(1+\tau)\theta] , [(1+\tau)\sigma\theta]\}$ est associé en fait une classe de générateurs θ modulo $\overline{M}^G$ (soit $\alpha \in \overline{M}^G$: on a $(1+\tau)\alpha = 0$, $(1+\tau)\sigma\alpha = 0$, $T\alpha = 0$).

Or le A-module quotient $M/\overline{M}^G$ peut être canoniquement muni d'une structure de module sur l'anneau quotient $D/\overline{D}^G$. Pour $x \in M$, on désigne par $\dot{x}$ sa classe dans $M/\overline{M}^G$.

LEMME 4.2. - Supposons ici $d(M) = d(D)$. Alors $\theta \in M$ engendre une R-base normale de M^g/M^G , si, et seulement si, $\{\dot{\theta}\}$ est une base de M/M^G sur $D/\overline{D}^G$.

Pour illustrer la nécessité de l'hypothèse $d(M) = d(D)$, remarquons que, si l'on a $d = -1$, avec $D \neq D_5$ et $D \neq D_5'$, alors $(((1 - \tau)L)/p)\dot{\theta}$ appartient à M/M^G sans que $((1 - \tau)L)/p$ appartienne à $D/\bar{D}^G$.

4° Il reste alors à choisir une base $\{\dot{\theta}\}$ de $M/\bar{M}^G$ sur $D/\bar{D}^G$, telle qu'il existe un représentant θ de $\dot{\theta}$ pour lequel $\{\bar{T}\theta\}$ soit une A-base de $\bar{M}^G$.

On voit facilement que cette condition est toujours vérifiée si $((1 - \tau)N)/p$ appartient à D .

Dans les autres cas, on sera amené à faire un changement de base dans $M/\bar{M}^G$. Remarquons que le nombre d'éléments de A/pA n'intervient que dans cette question.

5. Groupe des classes projectives d'un ordre D .

Soit D un ordre de A dans $K[G]$ contenant $A[G]$.

Deux D-modules projectifs de type fini, de rangs définis, M_1 et M_2 , sont dits équivalents, s'il existe deux modules libres L_1 et L_2 de type fini tels que $M_1 \oplus L_1$ soit isomorphe à $M_2 \oplus L_2$.

L'ensemble quotient muni de la loi induite par la somme directe est un groupe abélien, que l'on notera $\mathcal{P}(D)$, et que le théorème 4.1 nous permet de décrire.

Enonçons d'abord un résultat analogue à celui de la proposition 3.1.

PROPOSITION 5.1. - *Si M est un D-module projectif de rang r , on a $d(M) = rd(D)$, sauf peut-être pour $D = D_3$ ou D_3' , auxquels cas $d(M)$ peut prendre l'une quelconque des valeurs entières comprises entre $-r$ et $+r$.*

Précisons le cas $D = D_3$, par exemple. Soit $0 < h \leqslant r$. Considérons le D_3-module M_h :

$$M_h = \underbrace{D_4 \oplus \dots \oplus D_4}_{h} \oplus \underbrace{D_3 \oplus \dots \oplus D_3}_{r-h} ,$$

M_h est D_3-projectif, d'après la proposition 2.2, et on a $d(M_h) = h$ (pour $h < 0$, on échange les rôles de D_4 et D_5).

La proposition 5.1, nous conduit à distinguer le cas singulier $D = D_3$ ou D_3' (cas où il existe des D-modules projectifs non localement libres).

THÉORÈME 5.1. - *L'application $[M] \to \{M\}$ est, dans le cas $D \neq D_3$ et $D \neq D_3'$, un isomorphisme de groupes $\mathcal{P}(D)$ sur $\mathcal{K}(R)$.*

L'application $[M] \to \{\{M\}, d(M)\}$ est, dans le cas $D = D_3$ ou $D = D_3'$, un isomorphisme de groupes de $\mathcal{P}(D)$ sur $\mathcal{K}(R) \times \mathbb{Z}$.

De plus, toute relation $M \oplus L_1 \simeq L_2$, où L_1 et L_2 sont des $\mathfrak{O}$-modules libres, implique que M est libre.

Remarque. - SWAN [8] a construit un groupe G (groupe des quaternions généralisés d'ordre 32) pour lequel il existe des idéaux non libres J de $\mathbb{Z}[G]$ tels que $J \oplus \mathbb{Z}[G]$ soit isomorphe à $\mathbb{Z}[G] \oplus \mathbb{Z}[G]$.

Démonstration du théorème 5.1. - Le théorème 4.1, complété par la proposition 5.1, montre que la classe neutre de $\mathcal{P}(\mathfrak{O})$ est composée de $\mathfrak{O}$-modules libres, et que les applications $[M] \to \{M\}$ et $[M] \to (\{M\}, d(M))$ sont injectives.

Soit $\mathfrak{A}$ un idéal de R. On se propose de construire un idéal à gauche I de $\mathfrak{O}$, qui soit projectif sur $\mathfrak{O}$, et pour lequel $\{I\}$ soit la classe de $\mathfrak{A}$ dans $\mathcal{K}(R)$.

Nous utiliserons pour cela les remarques suivantes dues à J. MARTINET.

1° On peut se borner aux cas où $\mathfrak{O}$ est un ordre maximal : soient, en effet, $\mathfrak{O}$ un ordre quelconque, $\mathfrak{O}^*$ un ordre maximal qui le contient, I^* un idéal à gauche de $\mathfrak{O}^*$ étranger au conducteur de $\mathfrak{O}^*$ dans $\mathfrak{O}$ (on montre que, dans toute classe d'isomorphismes d'idéaux à gauche de $\mathfrak{O}^*$, il existe un tel idéal).

Alors l'intersection $I = \mathfrak{O} \cap I^*$ est un idéal à gauche de $\mathfrak{O}$, localement libre, donc projectif sur $\mathfrak{O}$, et qui vérifie $\mathfrak{O}^* I = I^*$.

De cette dernière relation, on déduit $\{I\} = \{I^*\}$, pourvu toutefois que, si $((1 + \tau)L)/p$ appartient à $\mathfrak{O}^*$, il appartienne aussi à $\mathfrak{O}$.

2° Soient φ et ψ les isomorphismes de $K[G]$ sur $K \times K \times \mathbb{M}_2(K_0')$, décrits à la fin du paragraphe 2, et $\mathfrak{B}$ l'idéal de A_0' image de $\mathfrak{A}$ par l'isomorphisme de R sur A_0' associé à φ et ψ. On a vu que $\varphi(\mathfrak{O}_4')$ et $\psi(\mathfrak{O}_5')$ sont égaux à l'ordre $\Omega = A \times A \times \mathbb{M}_2(A_0')$.

Soit $\mathfrak{J}$ le sous-ensemble des éléments $[a, b\begin{pmatrix} u & v \\ w & h \end{pmatrix}]$ de Ω, où u et w appartiennent à $\mathfrak{B}$. C'est un idéal à gauche de Ω.

Montrons que l'idéal à gauche $I = \varphi^{-1}(\mathfrak{J})$ de $\mathfrak{O}_4'$ admet pour invariant $\{I\}$ la classe de $\mathfrak{A}$ dans $\mathcal{K}(R)$:

Il est immédiat de voir que $\varphi(I^G)$ est défini, dans $\mathfrak{J}$, par les relations $b = 0$, $w = -u$, et $h = -v$, et que $\varphi(I^G)$ est défini, dans $\mathfrak{J}$, par $b = 0$, $w = u = h = v = 0$.

Le A_0'-module quotient $\varphi(I^G)/\varphi(I^G)$ est donc isomorphe à $\mathfrak{B} \oplus A_0'$.

On montre de même que l'idéal à gauche $I' = \psi^{-1}(\mathfrak{J})$ de $\mathfrak{O}_5'$ admet pour invariant $\{I'\}$ la classe de $\mathfrak{A}$ dans $\mathcal{K}(R)$.

Dans le cas $D = D_3$ ou $D = D_3'$, on achève la démonstration de la surjectivité de $[M] \to (\{M\}, dM)$ en utilisant la proposition 5.1.

Remarque. - M. P. LEE a montré que $\mathcal{P}(Z[G])$ est isomorphe au groupe $\mathcal{K}(Z_0')$ des classes d'idéaux de Z_0' (anneau des entiers du sous-corps réel maximal de $\underset{\sim}{Q}'$) [2].

Dans le cas où H est un groupe cyclique d'ordre premier p, D. S. RIM a montré que $\mathcal{P}(Z[H])$ est isomorphe au groupe $\mathcal{K}(Z')$, où Z' est l'anneau d'entiers de $\underset{\sim}{Q}'$ [6].

6. Application à l'arithmétique.

Soient E/K une extension galoisienne, dont le groupe de Galois est isomorphe à G, et B la clôture intégrale de A dans E.

D'après le théorème de la base normale, B est un A[G]-module de rang 1 [4]. Pour lui appliquer la proposition 4.1, nous allons d'abord déterminer, suivant la ramification de l'extension E/K en p et 2, l'ordre $\mathcal{O}(B)$.

Notations. - Soient F et F' les sous-corps de E invariants par H et g respectivement, et C et C' les clôtures intégrales de A dans F et F'.

Supposons ici p non inversible dans A. Pour tout idéal maximal $\mathfrak{P}$ de B au-dessus de l'idéal pA, nous désignerons par $v_{\mathfrak{P}}$ la valuation de E correspondante, et par H_i, $-1 \leqslant i$, la suite des sous-groupes de ramification de $\mathfrak{P}$ dans H [7].

Nous définirons enfin l'entier t par $H_t = H$, $H_{t+1} = \{1\}$. On montre que, lorsque l'extension E/K n'est pas modérément ramifiée en p, on a $t = 1$, sauf peut-être pour $p = 3$ dans le cas où l'extension E/K est totalement ramifiée : on peut, en effet, avoir alors $t = 1$ ou $t = 3$ [4].

THÉORÈME 6.1. - *L'ordre associé à B dans K[G] est de type D_i ou D_i', suivant que l'extension E/K est ou n'est pas modérément ramifiée en 2, avec $i = 0$ si elle est modérément ramifiée en p, $i = 1$ si elle est totalement ramifiée en p avec $t \neq 3$, $i = 3$ dans tous les autres cas.*

Démonstration du théorème 6.1. - Il est clair qu'on peut se borner aux cas où A est un anneau de valuation discrète d'idéal maximal mA, avec $m = 2$ et $m = p$.

On sait que l'on a les équivalences suivantes :

(L'extension E/K est modérément ramifiée) $\Longleftrightarrow$ (B est un $A[G]$-module relativement projectif) $\Longleftrightarrow$ (il existe $f \in \mathrm{End}_A(B)$ tel que, pour tout $x \in B$, on ait $x = \sum_{s \in G} sf(s^{-1}x)$ [4]).

D'où on déduit l'équivalence :

(E/K est modérément ramifiée) $\Longleftrightarrow$ $(((1+\tau)N)/m$ n'appartient pas à $\mathfrak{D}(B))$,

et l'implication :

(E/K est modérément ramifiée) $\Longrightarrow$ $(((1-\tau)N)/m$ n'appartient pas à $\mathfrak{D}(B))$.

Ceci achève l'étude dans le cas $m = 2$.

Supposons donc que A est un anneau de valuation discrète d'idéal maximal pA, et que E/K n'est pas modérément ramifiée. On vient de voir qu'alors $\mathfrak{D}(B)$ contient $\mathfrak{D}_1$.

Si $\mathfrak{W}_{B/C}$ est la différence de B sur C, les relations

$$v_{\mathfrak{P}}(\mathfrak{W}_{B/C}) = (t+1)(p-1), \qquad \text{pour tout idéal maximal } \mathfrak{P} \text{ de } B \text{ [7]},$$

$$(\mathrm{Tr}_{E/F}(B) \subset pC) \Longleftrightarrow (B \subset p(\mathfrak{W}_{B/C})^{-1}),$$

montrent que N/p appartient à $\mathfrak{D}(B)$ si, et seulement si, l'extension E/K, ou bien n'est pas totalement ramifiée, ou bien est totalement ramifiée dans le cas $p = 3$, $t = 3$.

Reste à montrer que, si l'une de ces conditions est réalisée, l'ordre $\mathfrak{D}(B)$ n'est jamais un ordre maximal : Pour construire des éléments x_ε de B tels que $L(1+\varepsilon\tau)x_\varepsilon$ ne soient pas congrus à 0 modulo p, on utilise les lemmes suivants (où l'on suppose seulement l'extension E/K non modérément ramifiée).

LEMME 6.1. - *Soient $\mathfrak{P}$ un idéal maximal de B, $v_{\mathfrak{P}}$ la valuation de E associée. Pour tout x tel que $1 \leqslant v_{\mathfrak{P}}(x) + (p-3)t < p$, on a*

$$v_{\mathfrak{P}}(Lx) = (p-2)t + v_{\mathfrak{P}}(x).$$

(Le lemme 6.1 se déduit de la relation $v_{\mathfrak{P}}[(\sigma - \sigma^{-1})x] = t + v_{\mathfrak{P}}(x)$.)

LEMME 6.2. - *Soit e l'indice de ramification E/F' de $\mathfrak{P}$ (on a $e = 1$ ou $e = 2$). Il existe $x_{-1} \in B$ et $x_1 \in B$ tels que l'on ait*

$$v_{\mathfrak{P}}[(1+\tau)x_1] = 1, \qquad 1 \leqslant v_{\mathfrak{P}}[(1-\tau)x_{-1}] \leqslant e.$$

Ce lemme 6.2, qui précise la ramification de l'extension E/F' en $\mathfrak{P}$, se démontre par l'étude de l'idéal $\mathrm{Tr}_{E/F'}(\mathfrak{P})$ et par celle des sous-groupes de ramification

de $\mathfrak{P}$ dans g .

On achève aisément la démonstration du théorème 6.1.

Nous sommes maintenant en mesure d'étudier le $D(B)$-module B :

1° B est projectif sur $D(B)$.

D'après la proposition 4.1, il suffit de démontrer que, lorsque A est un anneau de valuation discrète d'idéal maximal pA , et lorsque l'extension E/K est totalement ramifiée avec $t = 1$, on a $d(B) \neq -1$.

Il s'agit donc de construire un élément $x \in B$ tel que $L(1 + \tau)x$ ne soit pas congru, modulo p , à un élément de C . Soit $m \in A$ tel que $F = K[\sqrt{m'}]$.

Alors l'élément $x = \sqrt{m'}\, x_{-1}$ (où x_{-1} est défini dans le lemme 6.2) vérifie

$$v_{\mathfrak{P}}[L(1 + \tau)x] = 2p - 1 \qquad (\text{où } \mathfrak{P} \text{ est l'idéal maximal de } B) ,$$

ce qui rend impossible toute congruence modulo p de $L(1 + \tau)x$ avec un élément de C .

2° B est libre sur $D(B)$.

Il nous suffit, d'après la proposition 4.1, de montrer que $\{B\}$ est la classe principale de $\mathcal{K}(R)$. Cela résulte du théorème suivant :

THÉORÈME 6.2 (J. MARTINET [4]). - La clôture intégrale C' de A dans F' admet une base sur A de la forme

$$1 , \varphi , \psi , (\sigma^i + \sigma^{-i})\varphi , (\sigma^i + \sigma^{-i})\psi , \qquad 1 \leqslant i \leqslant (p - 3)/2 .$$

BIBLIOGRAPHIE

[1] BOURBAKI (N.). - Algèbre commutative. Chapitre 7. - Paris, Hermann, 1965 (Act. scient. et ind., 1314 ; Bourbaki, 31).

[2] LEE (Myrna Pike). - Integral representations of dihedral groups of order $2p$, Trans. Amer. math. Soc., t. 110, 1964, p. 213-231.

[3] LEOPOLDT (Heinrich-Wolfgang). - Über die Hauptordnung der ganzen Elementen eines abelschen Zahlkörpers, J. für reine und angew. Math., t. 201, 1959, p. 119-149.

[4] MARTINET (Jacques). - Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre $2p$, Ann. Inst. Fourier, Grenoble, t. 19, 1969, p. 1-80 (Thèse Fac. Sc. Grenoble, 1968).

[5] MARTINET (Jacques). - Modules sur l'algèbre du groupe quaternionique (à paraître).

[6] RIM (Dock Sang). - Modules over finite groups, Annals of Math., Series 2, t. 69, 1959, p. 700-712.

[7] SERRE (Jean-Pierre). - Corps locaux. - Paris, Hermann, 1962 (Act. scient. et ind., 1296 ; Publ. Inst. math. Univ. Nancago, 8).

[8] SWAN (Richard G.). - Projective modules over group rings and maximal orders, Annals of Math., Series 2, t. 76, 1962, p. 55-61.

(Texte reçu le 31 mars 1971)

Anne-Marie BERGE
Faculté des Sciences de Bordeaux
UER Mathématiques et Informatique
351 cours de la Libération
33 - TALENCE