Astérisque

ANNE-MARIE BERGE

Projectivité des anneaux d'entiers sur leurs ordres associés

Astérisque, tome 61 (1979), p. 15-28

<http://www.numdam.org/item?id=AST_1979__61__15_0>

Société Mathématique de France
Astérisque 61 (1979) p. 15-28

PROJECTIVITÉ DES ANNEAUX D'ENTIERS SUR LEURS ORDRES ASSOCIÉS

par

Anne-Marie BERGÉ

-:-:-:-

Soit F un corps de nombres, et soit N/F une extension galoisienne finie, de groupe de Galois G. Le groupe G opère de façon naturelle sur N, et on peut donc munir N d'une structure de module à gauche sur l'algèbre de groupe $F[G]$. D'après le théorème de la base normale, le $F[G]$-module N est libre, avec un générateur.

Notons $\mathbb{Z}_F$ et $\mathbb{Z}_N$ les anneaux d'entiers de F et N respectivement. Nous savons que $\mathbb{Z}_N$ est un module de rang 1 sur l'algèbre de groupe $\mathbb{Z}_F[G]$, projectif si et seulement si l'extension N/F est modérément ramifiée. Il est donc naturel de chercher si, dans le cas d'une extension non modérément ramifiée, $\mathbb{Z}_N$ vérifie une propriété analogue, à condition naturellement de substituer, à l'ordre $\mathbb{Z}_F[G]$, l'ordre $\mathfrak{O}(\mathbb{Z}_N, F[G])$ formé des $\lambda \in F[G]$ tels que $\lambda \mathbb{Z}_N$ soit inclus dans $\mathbb{Z}_N$.

Nous savons, par un théorème de Leopoldt ([6]), que, dans le cas des extensions abéliennes du corps $\mathbb{Q}$ des rationnels, l'anneau $\mathbb{Z}_N$ est libre sur l'ordre $\mathfrak{O}(\mathbb{Z}_N, \mathbb{Q}[G])$. Nous allons voir que, par contre, l'étude des extensions diédrales de $\mathbb{Q}$ fournit plusieurs types de contre-exemples à la projectivité de $\mathbb{Z}_N$ sur son ordre associé.

Par complétion pour les valuations $\mathfrak{p}$-adiques du corps F, on est immédiatement ramené, pour ce problème, au cas d'une algèbre galoisienne semi-locale sur un corps local. Cette algèbre est induite par une extension galoisienne du

corps local. Nous consacrons donc un premier paragraphe à l'étude de propriétés des ordres d'une algèbre de groupe relatives à l'induction. Nous faisons ainsi apparaître, dans le cas non abélien, des contraintes qui sont à l'origine d'un premier type de contre-exemples. Nous étudions, dans le deuxième paragraphe, les extensions cycliques ou diédrales de corps locaux. Dans le troisième paragraphe, nous appliquons ces résultats aux extensions diédrales de certaines classes de corps de nombres. Nous caractérisons celles pour lesquelles l'anneau d'entiers est projectif sur son ordre associé, par une condition sur la ramification, qui met en évidence l'aspect particulier des extensions de degré $2p$, où p est premier ([7], [1]).

§ .I. - Méthodes locales

Nous conservons les notations de l'introduction. De plus, si R est un anneau intègre, k son corps des fractions, et M un $R[G]$-module de rang 1, nous notons $\mathfrak{O}(M, k[G])$ l'ordre associé à M dans $k[G]$, c'est-à-dire l'ensemble des $\lambda \in k[G]$ vérifiant $\lambda M \subset M$.

1. - Complétion semi-locale

Pour tout idéal premier non nul $\mathfrak{p}$ de $\mathbb{Z}_F$, l'indice $\mathfrak{p}$ désigne la complétion pour la valuation $\mathfrak{p}$-adique.

PROPOSITION 1. - *Soient M un $\mathbb{Z}_F[G]$-module de rang 1, et $\mathfrak{O}$ son ordre associé dans $F[G]$. Alors :*

1) *Pour tout idéal premier $\mathfrak{p}$ de $\mathbb{Z}_F$, on a $\mathfrak{O}(M_{\mathfrak{p}}, F_{\mathfrak{p}}[G]) = \mathfrak{O}_{\mathfrak{p}}$.*

2) *Les conditions suivantes sont équivalentes :*

   i) *M est un $\mathfrak{O}$-module projectif,*

   ii) *Pour tout idéal premier $\mathfrak{p}$ de $\mathbb{Z}_F$, $M_{\mathfrak{p}}$ est projectif sur $\mathfrak{O}_{\mathfrak{p}}$.*

[L'implication (ii) ⇒ (i) résulte du "bon" comportement du foncteur $\mathrm{Ext}^1_{\mathfrak{O}}$ vis-à-vis de la complétion (cf. [3], exercice 11, p. 123).]

2. - Relation avec les complétions locales

Revenons à l'extension galoisienne N/F. Soit $\mathfrak{p}$ un idéal premier de $\mathbb{Z}_F$.

L'algèbre galoisienne $N_\mathfrak{p}$ est composée directe d'extensions galoisiennes de $F_\mathfrak{p}$, sur l'ensemble desquelles le groupe $G = \mathrm{Gal}(N/F)$ opère transitivement. Soient L l'une de ces extensions, et D son groupe de Galois (groupe de décomposition d'un idéal premier au-dessus de $\mathfrak{p}$ dans N). On a $N_\mathfrak{p} = \bigoplus_s sL$, où s décrit un système de représentants de G/D. Autrement dit, $N_\mathfrak{p}$ est de la forme $F_\mathfrak{p}[G] \otimes L$, où le produit tensoriel est pris sur $F_\mathfrak{p}[D]$. De même, si l'on désigne par B l'anneau de valuation de L, on a $\mathbb{Z}_{N,\mathfrak{p}} \simeq \mathbb{Z}_{F,\mathfrak{p}}[G] \otimes B$, où le produit tensoriel est pris sur $\mathbb{Z}_{F,\mathfrak{p}}[D]$.

3. - Propriétés de l'induction

Soient K un corps local d'inégales caractéristiques, A son anneau de valuation, G un groupe fini, et D un sous-groupe de G. Soit enfin M un module de rang 1 sur l'algèbre A[D]. Nous désignons par $\mathfrak{O}$ l'ordre associé à M dans K[D]. Pour tout A[D]-module P de rang 1, nous notons $\mathrm{Ind}_D^G P$ le G-module induit, c'est-à-dire $A[G] \otimes P$, où le produit tensoriel est pris sur A[D].

PROPOSITION 2. - *Si $\mathrm{Ind}_D^G M$ est projectif sur $\mathfrak{O}(\mathrm{Ind}_D^G M, K[G])$, alors* M *est projectif sur* $\mathfrak{O}$.

Cela résulte de l'inclusion $\mathfrak{O}(\mathrm{Ind}_D^G M, K[G]) \subset \bigoplus_{s \in D\backslash G} \mathfrak{O}s$, grâce au critère suivant ([3]) :

LEMME 1. - *Soit* R *un anneau. Un* R*-module* P *est projectif si, et seulement si, il existe une famille $(x_i)_{i\in I}$ d'éléments de* P*, et une famille $(f_i)_{i\in I}$ de* R*-homomorphismes de* P *dans* R*, tels que, pour tout $x \in P$, on ait $x = \sum_{i\in I} f_i(x)\, x_i$, où presque tous les $f_i(x)$ sont nuls.*

Inversement, si M est libre sur $\mathfrak{O}$, le G-module $\mathrm{Ind}_D^G M$ est isomorphe au G-module $\mathrm{Ind}_D^G \mathfrak{O}$, mais ce dernier n'est généralement pas un anneau. En fait, l'ordre $\mathfrak{O}(\mathrm{Ind}_D^G M, K[G])$ est l'intersection des conjugués $s(\mathrm{Ind}_D^G \mathfrak{O})s^{-1}$ où s décrit G. Lorsqu'il est induit par un ordre de K[D], on obtient le résultat attendu :

PROPOSITION 3. - *Supposons le sous-groupe* D *distingué dans* G*, et considérons l'ordre $\mathfrak{O}^* = \bigcap_{s\in G} s\mathfrak{O}s^{-1}$ de* K[D]*. Alors :*

1) $\mathfrak{O}(\mathrm{Ind}_D^G M, K[G]) = \mathrm{Ind}_D^G \mathfrak{O}^*$

2) pour que $\mathrm{Ind}_D^G M$ soit projectif sur $\mathfrak{O}(\mathrm{Ind}_D^G M, K[G])$, il faut et il suffit que M soit projectif sur $\mathfrak{O}^*$.

Ainsi apparaît une contrainte qui s'explicite mieux lorsque l'algèbre $K[D]$ est commutative :

COROLLAIRE. - Supposons le sous-groupe D commutatif et distingué dans G . Alors les conditions suivantes sont équivalentes :

i) $\mathrm{Ind}_D^G M$ est projectif sur son ordre associé dans $K[G]$,

ii) $\mathrm{Ind}_D^G \mathfrak{O}$ est un anneau, et $\mathrm{Ind}_D^G M$ est libre sur $\mathrm{Ind}_D^G \mathfrak{O}$,

iii) M est libre sur $\mathfrak{O}$, et l'on a $s\mathfrak{O}s^{-1} = \mathfrak{O}$ pour tout $s \in G$.

§ .II. - Extension cyclique ou diédrale d'un corps local

1. - Hypothèses et notations

Soit K un corps local, de caractéristique 0 , et de caractéristique résiduelle $p \neq 0$. On note A l'anneau de valuation de K, et on suppose A absolument non ramifié. Soit G un groupe fini. Pour tout sous-groupe J de G , et tout caractère φ de J à valeurs dans K, on introduit l'idempotent de $K[J]$ suivant :

$$e_\varphi = \frac{1}{(J:1)} \sum_{s \in J} \varphi(s^{-1})\, s \ ,$$

noté plus simplement e_J lorsque $\varphi = 1_J$. Lorsque $(J:1) = p^i$, nous écrivons même e_i au lieu de e_J , si aucune confusion n'est possible. Enfin, si $(x_i)_{i \in I}$ est une famille d'éléments de $K[G]$, le symbole $\langle A[G], x_i \rangle_{i \in I}$ désigne la sous-A-algèbre de $K[G]$ engendrée par $A[G]$ et la famille $(x_i)_{i \in I}$.

2. - Algèbre $K[G]$

Nous étudions, lorsque G est cyclique ou diédral, certains ordres de $K[G]$ contenant $A[G]$, et notamment les ordres maximaux.

1) Supposons G cyclique. - On pose alors $G = U.V$, où V est le p-sous-groupe de Sylow de G , d'ordre p^n . Comme A est absolument non ramifié,

les idempotents primitifs centraux de $K[G]$ sont de la forme $e_\chi(e_i - e_{i+1})$, où χ est un caractère irréductible de U à valeurs dans K, et où i varie de 0 à n (avec la convention $e_{n+1}=0$), de sorte que l'ordre $\mathfrak{M} = \langle A[G], e_i \rangle_{1\leq i\leq n}$ est maximal.

PROPOSITION 4.- Soit $0\leq p\leq n$, et soit $\mathfrak{O} = \langle A[G], e_i \rangle_{0\leq i\leq p}$. Soit M un G-module de rang 1, d'ordre associé $\mathfrak{O}$. Alors M est libre sur $\mathfrak{O}$.

En effet, par récurrence sur p à partir de la relation $M = e_1 M \oplus (1-e_1)M$, où l'ordre associé à $(1-e_1)M$ est l'ordre maximal du corps $(1-e_1)K[G]$, on est ramené au cas $p=0$; nous utilisons alors un résultat plus général dû à S.M.J. Wilson :

LEMME 2.- On ne fait ici aucune hypothèse sur l'indice absolu de ramification de A. Soit G un groupe fini abélien. Alors, tout G-module de rang 1, d'ordre associé $A[G]$, est libre sur $A[G]$.

2) Le groupe G est diédral.- Nous désignons par σ et τ deux générateurs de G liés par les relations $\sigma^h = \tau^2 = 1$, $\tau\sigma\tau^{-1} = \sigma^{-1}$, et par H le sous-groupe de G engendré par σ. On pose $H = U.V$, où V est le p-sous-groupe de Sylow de H. Soit Φ l'ensemble des caractères irréductibles de H à valeurs dans K. La famille d'idempotents suivante constitue une base sur K du centre de $K[G]$:

$$\mathcal{B} = \{\tfrac{1}{2}(1\pm\tau)\, e_\varphi\ ,\ \varphi\in\Phi\ ,\ \varphi^2 = 1\} \cup \{e_\varphi\ ,\ \varphi\in\Phi\ ,\ \varphi^2\neq 1\}\ .$$

Soit $e\in\mathcal{B}$. Nous étudions l'ordre $eA[G]$ de la K-algèbre simple $eK[G]$. Lorsque $e = \frac{1}{2}(1\pm\tau)e_\varphi$, cet ordre est l'ordre maximal du corps $eK[G]$. Supposons donc $e = e_\varphi$, et notons K_φ le corps cyclotomique $e_\varphi K[H]$, K'_φ son sous-corps "réel" maximal, A_φ et A'_φ les anneaux de valuation respectifs de K_φ et K'_φ. Si l'on désigne par Γ le groupe de Galois de l'extension K_φ/K'_φ, l'ordre $eA[G]$ est isomorphe au "twisted group ring" $A_\varphi[\Gamma]$, donc est maximal si et seulement si K_φ/K'_φ est non ramifiée. Nous supposons donc l'extension K_φ/K'_φ ramifiée. Il existe alors deux ordres maximaux $\mathfrak{M}_1$ et $\mathfrak{M}_2$ contenant $eA[G]$, lequel est héréditaire si et seulement si la ramification de K_φ/K'_φ est modérée, c'est-à-dire si $p\neq 2$ ([8]).

Soit M un $eA[G]$-module de rang r. Nous allons lui associer deux invariants, de la façon suivante : désignons par σ_V un générateur du groupe V.

Comme $e(\sigma_V - 1)$ est une uniformisante de K_φ, le A-module quotient $(1+\tau)M/(\sigma_V-1)M \cap (1+\tau)M$ est un A/pA-espace vectoriel, de dimension finie $\leq 2r$. On pose :

$$d(M) = \dim_{A/pA}[(1+\tau)M/(\sigma_V-1)M \cap (1+\tau)M] ,$$

et de même, si $p \neq 2$:

$$d'(M) = \dim_{A/pA}[(1-\tau)M/(\sigma_V-1)M \cap (1-\tau)M] .$$

PROPOSITION 5. - Soit $e \in \mathcal{E}$ tel que l'ordre $eA[G]$ ne soit pas maximal, et soit M un $eA[G]$-module de rang r. Alors :

(i) si p est différent de 2, on a $d(M) + d'(M) = 2r$;

(ii) supposons $r = 1$. Le module M est libre sur $eA[G]$ si et seulement si $d(M)$ et $d'(M)$ sont non nuls.

Démonstration. - Il suffit de calculer les invariants d et d' relatifs aux ordres $\mathfrak{M}_1$, $\mathfrak{M}_2$, $\mathfrak{M}_1 \cap \mathfrak{M}_2$ et $eA[G]$. Pour cela, nous utilisons un isomorphisme de $eK[G]$ sur l'algèbre de matrices $M_2(K'_\varphi)$ tel que l'image de $eA[G]$ soit contenue dans l'ordre héréditaire suivant, où $\mathfrak{p}'$ est l'idéal premier de A'_φ :

$$\begin{pmatrix} A'_\varphi & \mathfrak{p}' \\ A'_\varphi & A'_\varphi \end{pmatrix} .$$

3. - Ramification

Pour toute la suite du paragraphe, L/K désigne une extension cyclique ou diédrale, et on pose $q = |A/pA|$.

Notons G_i, $i \geq 0$, les sous-groupes de ramification de $G = Gal(L/K)$. On sait que G_1 est le p-sous-groupe de Sylow du groupe d'inertie G_o ([9]). Posons $r = (G_o : G_1)$. Remarquons que, puisque les groupe G_i/G_{i+1} $(i \geq 1)$ sont de type $(p, p, \ldots, p)$, il nous suffit de préciser les sous-groupes G_i non cycliques, ainsi que la suite $(t_i)_{i \geq 1}$ des indices inférieurs de ramification.

Si le groupe G_1 est cyclique, d'ordre p^n, les t_i vérifient :

$$(1) \qquad t_i = \frac{1}{p-1} rp^i - \left(\frac{rp}{p-1} - t_1\right) \qquad 1 \leq i \leq n .$$

Si de plus G_o est cyclique, on a $t_1 = r$ sauf peut-être lorsque $p = 2$, auquel cas on peut aussi avoir $t_1 = 2r$. En outre r divise $q-1$ ou $q+1$ selon que G est cyclique ou diédral ([2]).

Si G_1 n'est pas cyclique, ce qui suppose $p = 2$, nous utilisons les résultats de Fontaine relatifs aux 2-extensions diédrales ([4]). Résumons les différentes possibilités pour une extension diédrale :

PROPOSITION 6. - On suppose G diédral, et l'on note H (*) le sous-groupe cyclique d'indice 2 de G, et V le p-sous-groupe de Sylow de H. Soit enfin u l'indice de H dans V. Alors u divise $q+1$, et on a $G_o = H$ sauf peut-être lorsque $u \leq 2$, auquel cas on peut aussi avoir la situation suivante :

1) si $p \neq 2$, G_o est diédral d'indice u dans G, $G_1 = H \cap G_o$, et les t_i sont donnés par la formule (1) avec $r = 2$ et $t_1 = 1$ sauf peut être pour $p = 3$ où l'on peut avoir $t_1 = 3$,

2) si $p = 2$, $G_o = G$ sauf peut-être lorsque G est d'ordre 8 (auquel cas G_o peut être diédral d'indice 2), $G_1 = G_o$, et l'un des trois cas suivants :

(I) $G_2 = H \cap G_1$, les t_i vérifient (1) avec $r = t_1 = 1$,

(II) G_2 d'indice 2 dans $H \cap G_1$, et $t_i = 2^{i+1} - 3$ pour $i \geq 1$,

(III) G_2 est diédral d'indice 2 dans G_1, $G_3 = G_2$, $G_4 = H \cap G_2$, et, pour $i \geq 3$, $t_i = 2^i - 3$.

Remarque. - Par la théorie du corps de classes local, on montre que tous les cas énumérés ci-dessus se présentent effectivement. Cependant, si on se limite à $K = \mathbb{Q}_p$, il faut ajouter, lorsque $p = 2$, les restrictions suivantes : lorsque G_o est cyclique, le cas $t_1 = r$ suppose G_1 d'ordre 2. Lorsque G_o est diédral, le cas (II) exige $(G:1) = 8$ et $(G_o:1) = 4$.

Ramification presque-maximale. - Soit J un sous-groupe de G. On note L^J le sous-corps de L fixe par J, B^J son anneau de valuation, et v_J la valuation de L^J. L'idéal fractionnaire $e_J B$ de L^J contient B^J. S'il est entier pour tout sous-groupe J compris entre deux groupes de ramification consécutifs, on dit que la ramification de L/K est presque-maximale ([5]).

(*) lorsque G est d'ordre 4, on suppose H convenablement choisi.

La connaissance de la suite $(G_i)_{i\geq 0}$ permet de calculer les valuations $v_J(e_J B)$, ([9]), et nous obtenons en particulier :

COROLLAIRE. - On suppose l'extension L/K (cyclique ou diédrale) sauvagement ramifiée. La ramification est presque-maximale si et seulement si l'une des conditions suivantes est vérifiée :

(i) le groupe G_o est cyclique d'ordre rp^n (avec r premier à p), et l'on a $r \leq p-1$, ou alors $p=2$ et $t_1 = 2r$,

(ii) le groupe G_o est diédral, et l'on a $p=3$ et $t_1 = 3$, ou alors $p=2$ avec une ramification de type (I).

4. - Structure de B sur son ordre associé $\mathfrak{O}$ dans $K[G]$

Pour déterminer l'ordre $\mathfrak{O}$, on peut supposer l'extension totalement ramifiée, grâce à un résultat de Jacobinski ([5]) :

LEMME 3. - Soit L/K une extension galoisienne finie du corps local K. L'ordre $\mathfrak{O}$ est induit de G_o à G par l'ordre $\mathfrak{O}_o$ associé à B dans l'algèbre $K[G_o]$.

Ainsi, supposons par exemple l'extension L/K cyclique avec une ramification presque-maximale. L'ordre $\mathfrak{O}_o$ est alors l'ordre maximal de $K[G_o]$ (cf. I), et, d'après la proposition 4, B est libre sur $\mathfrak{O} = \langle A[G], e_{G_i} \rangle_{i\geq 1}$.

Nous caractérisons maintenant les extensions diédrales pour lesquelles B est projectif sur $\mathfrak{O}$:

PROPOSITION 7. - On suppose G diédral. Alors le $\mathfrak{O}$-module B est projectif si et seulement si l'une des conditions suivantes est vérifiée :

(i) la ramification est presque-maximale. On a alors :

$$\mathfrak{O} = \langle A[G], e_{G_i} \rangle_{i\geq 1},$$

(ii) la ramification n'est pas presque-maximale, et le groupe G_o est diédral d'ordre 2p. On a alors :

$$\mathfrak{O} = \langle A[G], 2e_{G_o} \rangle.$$

Dans les deux cas, le $\mathfrak{O}$-module B est libre.

Démonstration. - Nous nous bornons au cas où G_o est diédral (pour les autres cas, voir [2]). Nous conservons les notations de I. De plus, si V_i, $0 \leq i \leq n$, désigne le sous-groupe cyclique d'ordre p^i de H, nous écrivons L_i, B_i, v_i au lieu de L^{V_i}, B^{V_i}, v_{V_i}. Supposons d'abord que la ramification est presque-maximale, donc que l'on a $\mathfrak{O} \supset <A[G], e_{G_i}>_{i \geq 1}$. Pour montrer l'égalité, nous supposons $G = G_o$ (lemme 3). Soit $e \in \mathcal{S}$ un idempotent central primitif de $K[G]$; il appartient à $\mathfrak{O}$ sauf peut-être lorsque $p = 2$. Si e appartient à $\mathfrak{O}$, le facteur eB est libre sur $eA[G]$ (proposition 5). En effet, lorsque $eA[G]$ n'est pas maximal, les invariants $d(eB)$ et $d'(eB)$ ne sont pas nuls ($\sigma_V \in G_3$, $\tau \notin G_2$). Lorsque $p = 2$, on a :

$$\bigoplus_{e \notin \mathfrak{O}} e\mathfrak{O} = (e_{n-1} - e_n) A[G] \simeq A[\mathbb{Z}/2\mathbb{Z}],$$

et on conclut grâce au lemme 2. D'après la proposition 5, il reste à étudier, dans le cas $p = 2$ et $G \neq G_o$, les composantes $\frac{1}{2}(1 \pm \tau) e_1 B$, ce qui est immédiat (lemme 2).

Désormais, nous supposons que la ramification n'est pas presque-maximale. Traitons d'abord le cas $p \neq 2$. Le groupe G_o est alors d'ordre $2p^n$. On montre (en utilisant la proposition 6) que :

$$\mathfrak{O} = <A[G], \frac{1+\tau}{2} e_i, (\sigma_V - 1) e_i>_{i \geq 1}.$$

Cet ordre est donc contenu dans l'ordre :

$$\mathfrak{O}^* = <A[G], e_i>_{i \geq 1} = <A[G], e>_{e \in \mathcal{S}}.$$

LEMME 4. - *Soit* M *un* $\mathfrak{O}$*-module projectif de rang* r, *et soit* M^* *le* $\mathfrak{O}^*$*-module* $\mathfrak{O}^* M$. *Soit* $e \in \mathcal{S}$ *tel que l'ordre* $eA[G]$ *ne soit pas maximal. Alors on a* $d(eM^*) = r$.

[Cela étant évident lorsque M est libre sur $\mathfrak{O}$, il suffit de vérifier, pour M projectif sur $\mathfrak{O}$, l'inégalité $d'(eM^*) \geq r$. Soit $M' = \{x \in M ; \sigma_V(x) = x \text{ et } \tau x = -x\}$. On montre, en se ramenant au cas $M = \mathfrak{O}$, que l'application $(1-\tau) ey \longrightarrow (1-\tau) e_n y$ induit une application A/pA-linéaire et surjective de l'espace vectoriel $(1-\tau) eM^* / (\sigma_V - 1) eM^* \cap (1-\tau) eM^*$ sur l'espace M'/pM', qui est de dimension r.] Supposons alors $n > 1$, et montrons que, pour $e = e_{n-1} - e_n$, on a $d(eB^*) = 0$, c'est-à-dire $\frac{1+\tau}{2} eB \subset (\sigma_V - 1) eB$. Il suffit de prouver l'inclusion entre les ensembles de valuations correspondants. Or, puisque $n > 1$, on a $v_{n-1}(e_{n-1} B) = -1$,

et donc tout entier ≥ 0 non congru à 1 modulo p appartient à l'ensemble $v_{n-1}((\sigma_V - 1)eB)$ (car $\sigma_V \in G_1 \setminus G_2$). Par ailleurs, dans $(1+\tau)eB$, les valuations sont paires et non congrues à 1 modulo p (les éléments de eB ont une trace nulle sur L_n). Ainsi, d'après le lemme 4, le $\mathfrak{O}$-module B n'est pas projectif dans le cas $n>1$. Par contre, on montre que, lorsque $n=1$, il est libre (on se ramène au cas $G=G_o$ traité dans [1]). Plaçons-nous désormais dans le cas $p=2$. Le groupe G_o est alors d'ordre 2×2^n. Lorsque $n=1$ (G est alors d'ordre 4 ou 8, et $G_2=(1)$), on vérifie que tout élément $x \in B$ tel que $e_{G_o} x$ ne soit pas entier est une base de B sur l'ordre $\mathfrak{O} = <A[G], 2e_{G_o}>$. Lorsque n est supérieur à 1, B n'est pas projectif sur $\mathfrak{O}$. Montrons-le par exemple lorsque la ramification est de type (II) ($G = G_o = G_1$, $G_2 = V_{n-1}$). Alors on a $2e_G B = 2e_G B_{n-1} = B_n$. On en conclut que tout $\mathfrak{O}$-module M projectif, de rang déterminé, vérifie $e_G M^{V_{n-1}} \subset M$, (et donc que B n'est pas projectif). En effet, il suffit de prouver cette inclusion pour $M = \mathfrak{O}$. Choisissons $x_1 \in B_{n-1}$ tel que $v_n(2e_G x_1) = 0$, et $x_2 \in B$ tel que $v_n(2e_G x_2) > 0$ et $v_{n-1}((1+\tau)e_{n-1}x_2) = 0$. Soit alors $\lambda \in \mathfrak{O}^{V_{n-1}}$: cet élément appartient à l'ordre maximal $Ae_G \oplus A\frac{1-\tau}{2}e_n \oplus A\frac{1+\tau}{2}(e_{n-1}-e_n) \oplus A\frac{1-\tau}{2}(e_{n-1}-e_n)$ de l'algèbre $e_{n-1}K[G]$. En appliquant $(1+\tau)\lambda$ à x_1 et x_2, on prouve qu'en fait $e_G \lambda \in 2Ae_G$. Le cas de la ramification de type (III) se traite de façon analogue (avec $\frac{1}{2}(\sigma_V - 1)$ au lieu de e_G).

§ . 3. - Extension diédrale d'un corps de nombres

Notations et hypothèses

Soit F un corps de nombres, et soit N/F une extension diédrale, de groupe de Galois G. On note $\mathbb{Z}_F$ et $\mathbb{Z}_N$ les anneaux d'entiers de F et N. Soit $\mathfrak{p}$ un idéal premier de $\mathbb{Z}_F$, absolument non ramifié, et non modérément ramifié dans l'extension N/F. On désigne par $(G_i)_{i\geq 0}$ les sous-groupes de ramification d'un idéal premier $\mathfrak{P}$ de $\mathbb{Z}_N$ au-dessus de $\mathfrak{p}$. Soit H le sous-groupe cyclique d'indice 2 de G (lorsque G est d'ordre 4, on suppose H convenablement choisi). On pose $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$.

THÉORÈME. - *Le complété $\mathbb{Z}_{N,\mathfrak{P}}$ est projectif sur son ordre associé dans $F_{\mathfrak{p}}[G]$ si et seulement si l'une des trois conditions suivantes est vérifiée* :

(i) la ramification est presque-maximale et G_1 est inclus dans H . Alors $\mathbb{Z}_{N,\mathfrak{p}}$ est libre sur l'ordre $<\mathbb{Z}_{F,\mathfrak{p}}[G], e_{G_i}>_{i\geq 1}$;

(ii) la ramification est presque-maximale, G_1 n'est pas inclus dans H , G_2 est inclus dans H , et l'indice de G_o dans G n'est pas divisible par 4 . Alors $\mathbb{Z}_{N,\mathfrak{p}}$ est libre sur l'ordre $<\mathbb{Z}_{F,\mathfrak{p}}[G], e_J, e_{G_i}>_{i\geq 2}$ où J est le plus petit sous-groupe distingué de G contenant G_o ;

(iii) la ramification n'est pas presque-maximale, le groupe G_o est d'ordre 2p et d'indice 1 ou 2 dans G . Alors $\mathbb{Z}_{N,\mathfrak{p}}$ est libre sur l'ordre $<\mathbb{Z}_{F,\mathfrak{p}}[G], 2e_{G_o}>$.

Notons que le cas (ii) suppose $p=2$.

Remarque. - Ainsi, si $\mathbb{Z}_N$ est projectif sur son ordre associé $\mathfrak{O}$, il est localement libre sur $\mathfrak{O}$ (puisque cela est vrai aussi en tout $\mathfrak{p}$ modérément ramifié dans N). On peut conjecturer que ce résultat est général.

Exemples. - Prenons $F=\mathbb{Q}$.

1) Si G est le groupe diédral d'ordre 2ℓ , ℓ premier, alors l'extension $N/\mathbb{Q}$ vérifie, pour tout premier p , les conditions du théorème. En fait, $\mathbb{Z}_N$ est alors libre sur son ordre associé ([2], [7], [6]).

2) Si G est le groupe diédral d'ordre 4ℓ , ℓ premier, il est possible que $\mathbb{Z}_{N,2}$ ne soit pas projectif sur son ordre associé, soit parce que la structure locale n'est pas triviale [exemple (avec $\ell=3$) : $N=\mathbb{Q}(\sqrt[12]{1}, \sqrt{2})$], soit parce que l'induction ne conserve pas la projectivité [citons l'exemple (avec $\ell=2$) $\mathbb{Q}(\sqrt{-7}, \sqrt{\frac{-1+\sqrt{-7}}{2}}, \sqrt{\frac{-1-\sqrt{-7}}{2}})$ dû à S.M.J. Wilson].

3) Soit p un nombre premier impair. On peut construire une extension diédrale $N/\mathbb{Q}$, de degré $2p^n$ par exemple, qui ne vérifie pas, pour p , les conditions du théorème : considérons le corps quadratique imaginaire $k=\mathbb{Q}(\sqrt{-p})$ lorsque $p\neq 3$, $k=\mathbb{Q}(\sqrt{-6})$ lorsque $p=3$, et soit $\mathfrak{p}$ l'idéal premier de k au-dessus de p ; la théorie du corps de classes montre qu'il existe une extension N/k , cyclique de degré p^2 , de conducteur $\mathfrak{p}^{2n}$, qui convient.

La suite du paragraphe est consacrée à la démonstration du théorème. Nous posons $K=F_{\mathfrak{p}}$, $L=N_{\mathfrak{P}}$, et nous reprenons les notations du paragraphe 2 . Notons $\mathfrak{O}_o$ l'ordre associé à B dans $K[G_o]$. Lorsque $\mathbb{Z}_{N,\mathfrak{p}}$ est projectif sur son

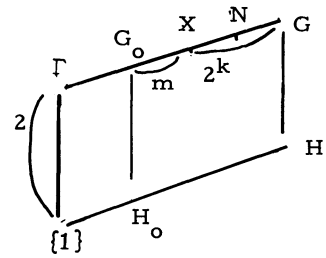
ordre associé dans $K[G]$, il est isomorphe au G-module $\mathrm{Ind}_{G_o}^{G} \mathfrak{O}_o$ (propositions 2 et 7, et lemme 3). Nous allons donc étudier ce module, en nous bornant aux cas où la structure locale est triviale, et où G est d'ordre supérieur à 4. Dans le cas (i), l'ordre $\mathfrak{O}_o$ est engendré, dans $K[G_o]$, par des idempotents e_J tels que J soit distingué dans G. Le G-module $\mathrm{Ind}_{G_o}^{G} \mathfrak{O}_o$ est donc l'anneau engendré dans $K[G]$ par les e_J, ce qui achève l'étude du cas (i). Supposons maintenant que l'extension locale L/K soit cyclique, avec une ramification non presque-maximale. La structure locale peut être triviale (voir [2]), mais l'ordre $\mathfrak{O}_o$ n'est pas invariant par conjugaison par un élément $\tau \in G \setminus H$ (cf. [2], théorème 1 et lemme 5). L'induction ne conserve donc pas la projectivité. Nous supposons désormais G_o non inclus dans H. Il est alors produit semi-direct du groupe $H_o = H \cap G_o$ par un groupe Γ d'ordre 2. D'après la proposition 7, il nous reste à examiner les trois cas suivants :

α) $p=2$ et $\mathfrak{O}_o = \langle A[G_o], e_{G_o}, e_{H'} \rangle_{H' \subset H_o}$

β) $p=2$, $(G_o:1)=4$, et $\mathfrak{O}_o = \langle A[G_o], e_{G_o}, e_\Gamma \rangle$

γ) $(G_o:1)=2p$, et $\mathfrak{O}_o = \langle A[G_o], 2e_{G_o} \rangle$.

Posons $(G:G_o) = m2^k$, où m est impair, et soient X le sous-groupe d'indice 2^k de G contenant G_o, et N le normalisateur de X dans G :



Enfin, nous notons s le plus petit entier tel que $se_{G_o} \in \mathfrak{O}_o$ ($s=1$ ou 2).

a) Etudions l'induction de G_o à X. Dans le cas α), posons $(G_o:1)=2^{n+1}$, et montrons, par récurrence sur $n \geq 0$, que $\mathrm{Ind}_{G_o}^{X} \mathfrak{O}_o$ est libre sur l'ordre $\langle A[X], e_X, e_{H'} \rangle_{H' \subset G_o}$: on utilise la relation $\mathfrak{O}_o = e_1 \mathfrak{O}_o \oplus (1-e_1)\mathfrak{O}_o$, où le X-module $\mathrm{Ind}_{G_o}^{X} (1-e_1)\mathfrak{O}_o$ est un ordre de $(1-e_1)K[X]$. On est ainsi ramené au cas $n=0$, pour lequel $\mathrm{Ind}_{G_o}^{X} \mathfrak{O}_o$ est égal à l'ordre maximal $\langle A[X], e_X \rangle$ de $K[X]$ (voir II). Dans les cas β) et γ) au contraire, l'idempotent e_{H_o} n'appartient

pas à $\mathfrak{O}_o$. L'ordre $\mathfrak{x}$ associé à $\mathrm{Ind}_{G_o}^{X} \mathfrak{O}_o$ dans $K[X]$ possède donc la propriété suivante : $\mathfrak{x}^{G_o} \subset \mathrm{Ams}\, e_X + 2p e_{G_o} A[X]$. Supposons alors que $\mathrm{Ind}_{G_o}^{X} \mathfrak{O}_o$ soit projectif sur $\mathfrak{x}$. D'après le lemme 1 , l'élément $s e_{G_o}$ peut s'écrire

$$s e_{G_o} = \sum_{i=1,\ldots,k} \lambda_i x_i \text{ , avec } \lambda_i \in \mathfrak{x}^{G_o} \text{ , } x_i \in \mathrm{Ind}_{G_o}^{X} \mathfrak{O}_o \text{ .}$$

On en déduit que e_{G_o} appartient à $\mathrm{Am}\, e_X + p \sum_{x \in X} A e_{G_o} x$, d'où $X = G_o$.

b) Nous étudions l'induction de X à N de l'ordre $\mathfrak{x}$ égal à $\langle A[X], e_X, e_{H'} \rangle_{H' \subset G_o}$ dans le cas α), à $\langle A[X], e_X, e_\Gamma \rangle$ dans le cas β), et à $\langle A[X], e_X \rangle$ dans le cas γ), le groupe X étant d'ordre $2p$ dans les cas β) et γ). Dans le cas β), le N-module $\mathrm{Ind}_X^N \mathfrak{x}$ n'est projectif sur son ordre associé que lorsque $N = X$, et donc $G = X$ (proposition 3). Dans les cas α) et γ) par contre, $\mathrm{Ind}_X^N \mathfrak{x}$ est un ordre, que nous notons $\mathfrak{N}$, et dont nous étudions l'inductions de N à G .

c) Pour montrer que, si $N \neq G$, $\mathrm{Ind}_N^G \mathfrak{N}$ n'est pas projectif sur son ordre associé, on peut se borner au cas où N est d'indice 2 dans G ; il suffit alors de vérifier que $\mathfrak{N}$ n'est pas projectif sur l'ordre $\mathfrak{N}^* = \bigcap_{s \in G} s \mathfrak{N} s^{-1}$ de $K[N]$. Pour cela, on procède comme dans a), à partir de l'inclusion

$$(\mathfrak{N}^*)^X \subset 2s A e_N + ps e_X A[X] \text{ .}$$

-:-:-:-

BIBLIOGRAPHIE

[1] A.-M. BERGÉ, Sur l'arithmétique d'une extension diédrale, Ann. Inst. Fourier, 22, 2 (1972), 31-59.

[2] A.-M. BERGÉ, Arithmétique d'une extension galoisienne à groupe d'inertie cyclique, Ann. Inst. Fourier, 28, 4 (1978), 17-44.

[3] H. CARTAN and S. EILENBERG, Homological Algebra, Princeton Univ. 1956.

[4] J.-M. FONTAINE, Groupes de ramification et représentations d'Artin, Ann. Scient. Ec. Norm. Sup., 4e série, t. 4 (1971), 337-392.

[5] H. JACOBINSKI, Über die Hauptordnung eines Körpers als Gruppenmodul, J. reine angew. Math. 213 (1963), 151-164.

[6] H.W. LEOPOLDT, Über die Hauptordnung der ganzen Elementen eines abelschen Zahlkörpers, J. reine angew. Math. 201 (1959), 119-149.

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

[8] M. ROSEN, Representations of twisted group rings, Ph. D. Thesis, Princeton Univ., 1963.

[9] J.-P. SERRE, Corps locaux, 2e éd., Hermann, Paris, 1968.

-:-:-:-

Anne-Marie BERGÉ
U.E.R. de Mathématiques
et d'Informatique de
l'Université de Bordeaux I
351, cours de la Libération
33405 TALENCE CEDEX