ANNALES DE L'INSTITUT FOURIER

ANNE-MARIE BERGÉ

Sur l'arithmétique d'une extension diédrale

Annales de l'institut Fourier, tome 22, n° 2 (1972), p. 31-59

<http://www.numdam.org/item?id=AIF_1972__22_2_31_0>

Ann. Inst. Fourier, Grenoble
22, 2 (1972), 31-59.

SUR L'ARITHMÉTIQUE D'UNE EXTENSION DIÉDRALE

par Anne-Marie BERGÉ

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, complété par Speiser, peut s'énoncer de la manière suivante :

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

Léopoldt [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 $\mathfrak{O}(B)$, 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 $\mathfrak{O}(B)$ est un ordre de A dans K[G], et on l'appellera *ordre associé à* B.

On peut alors énoncer ainsi le résultat de Léopoldt :

L'anneau des entiers d'une extension abélienne des ration-

nels est un module libre sur l'ordre qui lui est associé dans $\mathbf{Q}[G]$.

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 quaternionien d'ordre 8, qui est modérément ramifiée, et dont l'anneau des entiers n'est pas un $Z[G]$-module libre.

On se propose d'exposer ici un résultat analogue à celui de Léopoldt, 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 suivantes :

1) 2 est inversible dans A, ou bien tel que $A/2A$ soit un corps à 2 éléments;

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

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

Remarquons que ces hypothèses sont stables par localisation, et que, lorsque p n'est pas inversible dans A, la troisième est une conséquence de la deuxième [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 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 localement libres 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* :

$$\mathfrak{O}_0 = A[G]; \ \mathfrak{O}_1 = [A[G], ((1+\tau)N)/p];$$
$$\mathfrak{O}_2 = [A[G], ((1-\tau)N)/p], \ \mathfrak{O}_3 = [A[G], N/p, \tau N/p];$$
$$\mathfrak{O}_4 = [\mathfrak{O}_3, ((1+\tau)L)/p]; \ \mathfrak{O}_5 = [\mathfrak{O}_3, ((1-\tau)L)/p],$$

et, pour tout i, $0 \leqslant i \leqslant 5$, $\mathfrak{O}'_i = [\mathfrak{O}_i, ((1+\tau)N)/2]$.

Démonstration. — Il est facile de vérifier que les A-modules $\mathfrak{O}_i$ et $\mathfrak{O}'_i$ 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. — $\mathfrak{O}'_4$ *et* $\mathfrak{O}'_5$ *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 $\mathfrak{O}'_4$ et $\mathfrak{O}'_5$ se ramène

à celui de A[G], grâce aux isomorphismes

$$\mathfrak{O}_4'/\mathrm{A}[\mathrm{G}] \simeq \mathfrak{O}_5'/\mathrm{A}[\mathrm{G}] \simeq \mathrm{A}/p\mathrm{A} \times \mathrm{A}/p\mathrm{A} \times \mathrm{A}/2p\mathrm{A}.$$

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 $\mathfrak{O}_0$ et $\mathfrak{O}_0'$ sont les seuls ordres de A dans K[G] contenant A[G] : tout ordre maximal doit en effet contenir l'entier du centre $((1 + \tau)\mathrm{N})/2$, donc, d'après le lemme 2.1, être égal à $\mathfrak{O}_0'$. On conclut en remarquant que le A-module $\mathfrak{O}_0'/\mathfrak{O}_0$ 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 $\mu \in \mathrm{K}[\mathrm{H}]$. Pour $\mu = \sum_{i=0}^{p-1} k_i\sigma_i$, $k_i \in \mathrm{K}$, 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 $\mathrm{K}[\mathrm{H}]/(\mathrm{N}) \simeq \mathrm{K}'$, de la forme $a\mathrm{N}/p + \alpha$, $a \in \mathrm{A}$, $\alpha \in \mathrm{A}[\mathrm{H}]$.

Soit $\mathfrak{O}$ un ordre de A dans K[G] contenant A[G], et soit $\lambda \in \mathfrak{O}$.

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

LEMME 2.2. — *Soient* $a, a' \in \mathrm{A}$, $\alpha, \alpha' \in \mathrm{A}[\mathrm{H}]$ *et* $\mu \in \mathrm{K}[\mathrm{H}]$ *tel que*

$$\mu + \bar{\mu} = a\mathrm{N}/p + \alpha \quad \textit{et} \quad \mu\sigma + \bar{\mu}\sigma^{-1} = a'\mathrm{N}/p + \alpha'.$$

Alors μ *est de la forme* $u\mathrm{N}/p + \nu\mathrm{L}/p + \beta$, $u, \nu \in \mathrm{A}$, $\beta \in \mathrm{A}[\mathrm{H}]$.

Il en résulte que λ est de la forme :

$$\lambda = u_\lambda \frac{(1+\tau)\mathrm{N}}{p} + u_\lambda' \frac{(1-\tau)\mathrm{N}}{p} + \nu_\lambda \frac{(1+\tau)\mathrm{L}}{p} + \nu_\lambda' \frac{(1-\tau)\mathrm{L}}{p} + \gamma, \quad (1)$$

$$u_\lambda, u_\lambda', \nu_\lambda, \nu_\lambda' \in \mathrm{A}, \quad \gamma \in \mathrm{A}\ [6].$$

Pour discuter les valeurs de u_λ, u'_λ, v_λ, v'_λ modulo p, on utilisera la remarque suivante :

Si une somme S

$$S = u\frac{(1+\tau)N}{p} + u'\frac{(1-\tau)N}{p} + v\frac{(1+\tau)L}{p} + v'\frac{(1-\tau)L}{p}$$

appartient à $\mathfrak{O}$, chacun de ses quatre termes appartient à $\mathfrak{O}$.

Il suffit en effet d'écrire $(1+\varepsilon\tau)S(1-\varepsilon'\tau) \in \mathfrak{O}$ avec $\varepsilon = +1$ ou -1, $\varepsilon' = +1$ ou -1, en tenant compte des relations

$$(1+\varepsilon\tau)L(1+\varepsilon\tau) = 0,\ (1+\varepsilon\tau)L(1-\varepsilon\tau) = 2(1+\varepsilon\tau)L.$$

De sorte qu'une condition telle que : « $\frac{(1+\tau)L}{p}$ n'appartient pas à $\mathfrak{O}$ » par exemple se traduira, dans la formule (1), par la condition « v_λ est congru à 0 modulo p pour tout λ », et donc par l'inclusion $\mathfrak{O} \subset \mathfrak{O}_5$.

On remarque par ailleurs que $\mathfrak{O}_4$ (resp. $\mathfrak{O}_5$) est le seul ordre $\mathfrak{O}$ qui contienne $\frac{(1+\tau)L}{p}$ $\left(\text{resp. } \frac{(1-\tau)L}{p}\right)$.

L'élément $L = (\sigma - \sigma^{-1})^{p-2}$ vérifie en effet la congruence $L(\sigma - \sigma^{-1}) \equiv N$ modulo p, d'où les implications :

$$\frac{(1+\tau)L}{p} \in \mathfrak{O} \begin{cases} \nearrow\ (\sigma-\sigma^{-1})\frac{(1+\tau)L}{p} \in \mathfrak{O} \Longrightarrow \frac{(1-\tau)N}{p} \in \mathfrak{O} \\ \searrow\ \frac{(1+\tau)L}{p}(\sigma-\sigma^{-1}) \in \mathfrak{O} \Longrightarrow \frac{(1+\tau)N}{p} \in \mathfrak{O} \end{cases} \Longrightarrow \mathfrak{O}_4 \subset \mathfrak{O} \Longrightarrow \mathfrak{O}_4 = \mathfrak{O}$$

On peut donc supposer que $\frac{(1+\tau)L}{p}$ et $\frac{(1-\tau)L}{p}$ n'appartiennent pas à $\mathfrak{O}$, c'est-à-dire que, dans la formule (1), v_λ et v'_λ sont congrus à 0 modulo p pour tout λ, soit encore : $\mathfrak{O} \subset \mathfrak{O}_3$. En discutant suivant l'appartenance à $\mathfrak{O}$ des éléments $\frac{(1+\tau)N}{p}$ et $\frac{(1-\tau)N}{p}$, $\left(\text{la condition } \frac{(1+\tau)N}{p} \in \mathfrak{O}\right.$ se traduit par l'inclusion $\mathfrak{O}_1 \subset \mathfrak{O}$, sa négation se traduit par l'inclusion $\mathfrak{O} \subset \mathfrak{O}_2$), on achève l'identification de $\mathfrak{O}$ avec l'un des ordres $\mathfrak{O}_i (i = 0, 1, 2, 3)$.

Citons ici une propriété des ordres maximaux :

PROPOSITION 2.2. — *Les $\mathfrak{O}_3$-modules $\mathfrak{O}_4$ et $\mathfrak{O}_5$ (respectivement $\mathfrak{O}'_3$-modules $\mathfrak{O}'_4$ et $\mathfrak{O}'_5$) sont projectifs.*

Démonstration. — Nous verrons plus loin (théorème 4.1) qu'en fait le $\mathfrak{O}_3$-module $\mathfrak{O}_4 \oplus \mathfrak{O}_5$ 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*

$$L' = \sum_{i=0}^{p-1} i\sigma^{2i} \quad \text{et} \quad L'_0 = ((p-1)/2)(\sigma^2 - 1) + N/p.$$

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 $\mathfrak{O}_3$-modules

$$0 \to \operatorname{Ker} f \to \mathfrak{O}_4 \oplus \mathfrak{O}_5 \xrightarrow{f} \mathfrak{O}_3 \to 0,$$

où f associe, à $(x, y) \in \mathfrak{O}_4 \oplus \mathfrak{O}_5$, $((x - y)L'_0)/(p-1)$. Il est facile de voir que Ker f est isomorphe à $\mathfrak{O}_3$, 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 $\mathfrak{O}'_4$ (respectivement $\mathfrak{O}'_5$) 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 :

$$\begin{cases} \chi_0 : G \to K^* \\ \qquad \text{défini par} \quad \chi_0(\sigma) = 1,\ \chi_0(\tau) = 1, \\ \chi_1 : G \to K^* \\ \qquad \text{défini par} \quad \chi_1(\sigma) = 1,\ \chi_1(\tau) = -1, \\ \chi : G \to (\mathfrak{M}_2(K'_0))^* \\ \qquad \text{défini par} \quad \chi(\sigma) = \begin{pmatrix} \omega + \omega^{-1} & -1 \\ 1 & 0 \end{pmatrix},\ \chi(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \end{cases}$$

L'image de $\mathfrak{O}'_5$ par ψ est un ordre maximal contenu dans $A \times A \times \mathfrak{M}_2(A'_0)$, donc lui est égal.

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

3. Invariants associés à un $\mathfrak{O}$-module.

On désignera désormais par $\mathfrak{O}$ un ordre de A dans K[G] contenant A[G] et par M un $\mathfrak{O}$-module vérifiant les hypothèses suivantes :

Hypothèses (H_0). — M *est de type fini sur* $\mathfrak{O}$, *sans torsion sur* A, *et son rang est défini* : rappelons que M est de rang r si le K[G]-module $M_K = K \underset{A}{\otimes} M$ est libre avec une base à r éléments.

M, étant sans A-torsion, sera considéré comme un sous-$\mathfrak{O}$-module du K[G]-module M_K.

Nous allons associer au $\mathfrak{O}$-module M vérifiant les hypothèses (H_0) deux invariants par isomorphisme $d(M)$ et $h(M)$, qui permettront de reconnaître si M est localement libre, puis s'il est libre, sur $\mathfrak{O}$.

1) 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 $R = A[\sigma + \sigma^{-1}]/(N)$. Ce R-module sera noté M^*.

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

Il est clair que, si M est un $\mathfrak{O}$-module libre, on a $h(M) = h(\mathfrak{O})$. Cette condition n'est évidemment pas suffisante pour que M soit libre, car elle ne fait intervenir que la structure sous-jacente de A[G]-module de M (de même d'ailleurs que les hypothèses (H_0)).

Montrons que $h(\mathfrak{O})$ *est la classe principale de* $\mathcal{K}(R)$. Soit i l'entier $0 \leqslant i \leqslant 5$ tel que $\mathfrak{O} = \mathfrak{O}_i$ ou $\mathfrak{O}'_i$ (proposition 2.1). On remarque d'abord que l'on a $h(\mathfrak{O}_i) = h(\mathfrak{O}'_i)$ pour tout i et que pour $i \neq 4$, le R-module $\mathfrak{O}_i^* = \dfrac{\mathfrak{O}_i^g}{\mathfrak{O}_i^G}$ admet pour base $\{[1 + \tau], [(1 + \tau)\sigma]\}$ où, pour $x \in M^g$, on note $[x]$ la classe de x modulo M^G,

Reste à vérifier que les classes $h(\mathfrak{O}_4)$ et $h(\mathfrak{O}_5)$ sont inverses dans $\mathcal{K}(R)$. On construit pour cela, comme pour la proposition 2.2, une suite exacte de R-modules :

$$0 \to \operatorname{Ker} F \to \mathfrak{O}_4^* \oplus \mathfrak{O}_5^* \xrightarrow{F} \mathfrak{O}_3^* \to 0$$

où F associe au couple $([x], [y])$, où x appartient à $\mathfrak{O}_4^g$ et y à $\mathfrak{O}_5^g$, l'élément $[x - y][\sigma^2 - 1]$. On achève en remarquant que Ker F est isomorphe à $\mathfrak{O}_3^*$, lequel est R-libre.

2) Pour permettre une étude locale du $\mathfrak{O}$-module M on lui associe un entier défini, lorsque p n'est pas inversible dans A, de la façon suivante :

Le A-module $M/pM + M^H$ peut être canoniquement muni d'une structure d'espace vectoriel sur A/pA. On définit alors une application f de M^* dans cet espace vectoriel :

Pour $X \in M^*$, $f(X)$ désigne la classe modulo $pM + M^H$ de l'élément Lx, où x est un représentant de X dans M^g (on vérifie aisément que l'élément Lx est indépendant du choix de ce représentant).

Cette application f vérifie la propriété suivante : pour tous

$X \in M^*$ $Y \in M^*$, $\alpha \in R$, $\beta \in R$, on a :

$$f(\alpha X + \beta Y) = \mathrm{Tr}\alpha f(X) + \mathrm{Tr}\beta f(Y),$$

où, pour $\alpha = \left[\sum_{i=0}^{p-1} a_i \sigma^i\right] \in R$, $\mathrm{Tr}\alpha$ désigne la classe modulo pA de $\sum_{i=0}^{p-1} a_i$. Nous dirons que f est une R-*application* de M^* dans le A/pA-espace vectoriel $M/pM + M^H$. Il en résulte que l'image $f(M^*)$ est un sous-espace vectoriel de $M/pM + M^H$, de dimension invariante par localisation en p, et donc inférieure ou égale à $2r$ (si M^* est R-libre de base $\mathcal{B}$, $f(M^*)$ sera engendré par $f(\mathcal{B})$).

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.

Pour plus de généralité dans l'énoncé de résultats, on posera $d(M) = 0$ lorsque p est inversible dans A.

L'entier $d(M)$ est invariant par isomorphisme et vérifie $d(M \oplus M') = d(M) + d(M')$, de sorte que, si M est localement libre sur $\mathfrak{O}$, on doit avoir

$$d(M) = rd(\mathfrak{O}).$$

Dans le cas général nous allons voir que quelques hypothèses rattachant M à $\mathfrak{O}$ permettent de limiter les valeurs prises par $d(M)$:

Introduisons pour cela quelques définitions :

DÉFINITION 3.3. — *Soit* h (*resp.* $\bar{h}$) *le plus grand entier* $m \in \{1, 2, p, 2p\}$ *tel que* $\dfrac{(1+\tau)N}{m}$ $\left(\text{resp. } \dfrac{(1-\tau)N}{m}\right)$ *appartienne à* $\mathfrak{O}$. *Nous posons*

$$T = \frac{(1+\tau)N}{h}, \quad \bar{T} = \frac{(1-\tau)N}{\bar{h}}.$$

DÉFINITION 3.4. — *L'ensemble* $\mathfrak{O}(M)$ *des éléments* $\lambda \in K[G]$ *tels que pour tout* $x \in M$, λx *appartienne à* M *est un ordre de* A *dans* K[G] *qui contient* $\mathfrak{O}$ *et que l'on appelle : ordre associé à* M.

Nous désignerons enfin par $\overline{M}^G$ le sous-A-module des éléments x de M qui vérifient $\tau x = -x$ et $\sigma x = x$.

Nous sommes maintenant en mesure d'énoncer, en nous bornant au cas où A est un anneau local d'idéal maximal pA, quelques résultats relatifs au signe de $d(M)$.

PROPOSITION 3.1. — *Soit* M *un* $\mathfrak{O}$ *module vérifiant les hypothèses suivantes :*

(H_0) M *est de type fini, sans* A *torsion, de rang défini et égal à* r.

(H_1) *Les applications* $x \to Tx$ *et* $x \to \overline{T}x$ *de* M *dans* M^G *et* $\overline{M}^G$ *respectivement sont surjectives.*

Alors

1) *si* $\dfrac{(1+\tau)N}{p}$ $\left(\text{resp. } \dfrac{(1-\tau)N}{p}\right)$ *n'appartient pas à* $\mathfrak{O}$, *on a* $d(M) \geqslant 0$ (*resp.* $d(M) \leqslant 0$).

2) *si* $\dfrac{(1+\tau)N}{p}$ $\left(\text{resp. } \dfrac{(1-\tau)N}{p}\right)$ *appartient à* $\mathfrak{O}$, *la condition* $d(M) = +r$ (*resp.* $d(M) = -r$] *est équivalente à* $\mathfrak{O}(M) = \mathfrak{O}_4$ (*resp.* $\mathfrak{O}_5$).

On déduit de cette proposition (qui sera démontrée au paragraphe 5) les valeurs de $d(\mathfrak{O})$ (nul pour $\mathfrak{O} \subset \mathfrak{O}_3$, égal à $+1$ pour $\mathfrak{O} = \mathfrak{O}_4$, à -1 pour $\mathfrak{O} = \mathfrak{O}_5$). On en déduit aussi que les conditions (H_0) et (H_1) suffisent, dans le cas des ordres $\mathfrak{O}_0$, $\mathfrak{O}_4$, $\mathfrak{O}_5$, à assurer la relation $d(M) = rd(\mathfrak{O})$. On va énoncer d'autres conditions suffisantes :

COROLLAIRE 3.1. — *Soit* M *un* $\mathfrak{O}$*-module projectif et vérifiant les hypothèses* (H_0). *Alors il vérifie la condition* (H_1), *et la relation* $d(M) = rd(\mathfrak{O})$ *sauf peut-être dans le cas* $\mathfrak{O} = \mathfrak{O}_3$ *pour lequel* $d(M)$ *peut prendre toutes valeurs entières* m *telles que* $-r \leqslant m \leqslant +r$.

La proposition 2.2. nous permet d'ailleurs de construire tout de suite un $\mathfrak{O}_3$-module projectif d'invariant m donné. Supposons par exemple $m > 0$. Le $\mathfrak{O}_3$-module

$$M = \underbrace{\mathfrak{O}_4 \oplus \cdots \oplus \mathfrak{O}_4}_{m} \oplus \underbrace{\mathfrak{O}_3 \oplus \cdots \oplus \mathfrak{O}_3}_{r-m}$$

est projectif de rang r, et d'invariant $d(M) = m$.

COROLLAIRE 3.2. — *Soit* M *un* $\mathfrak{O}$*-module vérifiant les hypothèses* (H_0), *de rang* 1 *et tel que* $\mathfrak{O}(M) = \mathfrak{O}$. *Alors il vérifie la propriété* (H_1) *et la relation* $d(M) = rd(\mathfrak{O})$ *sauf peut-être dans les cas suivants :*

$\mathfrak{O} = \mathfrak{O}_1$ *auquel cas on peut avoir* $d(M) = 0$ *ou* $d(M) = -1$,
$\mathfrak{O} = \mathfrak{O}_2$ *auquel cas on peut avoir* $d(M) = 0$ *ou* $d(M) = +1$.

Le cas d'un A[G]-module de rang 1, d'ordre associé $\mathfrak{O}_1$ non localement libre et même non projectif sur $\mathfrak{O}_1$ peut en effet se présenter : c'est le cas du A-module engendré par $\mathfrak{O}_1$ et $\frac{(1-\tau)L}{p}$.

Nous allons maintenant justifier le choix des invariants $h(M)$ et $d(M)$.

4. Résultats sur les $\mathfrak{O}$-modules.

THÉORÈME 4.1. — *Soient* $\mathfrak{O}$ *un ordre de* A *dans* K[G] *contenant* A[G] *et* M *un* $\mathfrak{O}$*-module de type fini sans* A*-torsion, de rang défini et égal à* r. *On suppose de plus que* M *vérifie les hypothèses suivantes :*

(H_1) *Les applications* $x \to Tx$ *et* $x \to \overline{T}x$ *de* M *dans* M^G *et* $\overline{M}^G$ *respectivement sont surjectives.*

(H_2) $d(M) = rd(\mathfrak{O})$.

(H_3) $h(M)$ *est la classe principale de* $\mathfrak{K}(R)$.

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

La conjonction des hypothèses (H_1) et (H_2) caractérise donc les $\mathfrak{O}$*-modules localement libres* (parmi ceux qui vérifient les hypothèses H_0), la condition (H_3) caractérisant parmi eux ceux qui sont *libres* sur $\mathfrak{O}$. Les corollaires 3.1. et 3.2. peuvent maintenant s'exprimer ainsi :

COROLLAIRE 4.1. — *Soit* M *un* $\mathfrak{O}$*-module projectif vérifiant les hypothèses* (H_0). *Alors, dans le cas* $\mathfrak{O} \neq \mathfrak{O}_3$ *et* $\mathfrak{O} \neq \mathfrak{O}'_3$, M *est localement libre, et dans les cas* $\mathfrak{O} = \mathfrak{O}_3$ *ou* $\mathfrak{O} = \mathfrak{O}'_3$ *il est localement libre s'il vérifie* $d(M) = 0$.

Le corollaire 4.1. sera utilisé au paragraphe 6 dans l'étude

du groupe des classes projectives de $\mathfrak{O}$. En arithmétique, nous utiliserons plutôt le résultat suivant :

COROLLAIRE 4.2. — *Soit* M *un* A[G]*-module de rang* 1 *et* $\mathfrak{O}$ *son ordre associé dans* K[G]. *Alors, dans les cas où* $\mathfrak{O}$ *est différent de* $\mathfrak{O}_1$, $\mathfrak{O}'_1$, $\mathfrak{O}_2$, $\mathfrak{O}'_2$, M *est localement libre sur* $\mathfrak{O}$. *Dans les autres cas, il en est ainsi si et seulement si* $d(M) = 0$.

On peut en déduire que les ordres $\mathfrak{O}'_3$, $\mathfrak{O}'_4$ et $\mathfrak{O}'_5$ sont *héréditaires* (pour $\mathfrak{O}'_3$ on utilise la proposition 2.2). Ce sont d'ailleurs les seuls possibles car les seuls à contenir les idempotents du centre $\dfrac{(1+\tau)N}{2p}$ et $\dfrac{(1-\tau)N}{2p}$.

5. Démonstrations de la proposition 3.1 et du théorème 4.1.

Désormais M désignera un $\mathfrak{O}$-module *vérifiant les hypothèses* (H_0) *et* (H_1).

A. — *Quelques propriétés du* R*-module* $M^* = M^g/M^G$.

LEMME 5.1. — *Soit* $X \in M^*$. *Alors :*

1) *Il existe* $x \in M$ *tel que* $X = [(1+\tau)x]$.

2) *Lorsque* $(1+\tau)x$ *décrit* X, Tx *décrit*

$$\begin{cases} M^G \text{ dans le cas où } \dfrac{(1+\tau)N}{p} \text{ appartient à } \mathfrak{O}; \\ \text{sa classe modulo } pM^G \text{ dans le cas contraire.} \end{cases}$$

Rappelons que la notation $[y]$ désigne l'image canonique dans M^g/M^G de l'élément y de M^g.

Démonstration du lemme 5.1. — Soit $y \in M^g$. L'égalité $2y = (1+\tau)y$ permet de supposer p inversible pour la recherche des représentants de X de la forme $(1+\tau)x$. L'identité : $p\tau = pN\tau + L'(1-\tau) - (1+\tau)L'$ (lemme 2.3) montre que y est congru modulo pM^G à un élément $(1+\tau)x$, $x \in M$, d'où 1.

Si on suppose de plus $y \in M^G$, et si l'on pose $h = u\wp$, avec $u = 1$ ou 2, $\wp = 1$ ou p, l'hypothèse (H_1) permet d'écrire : $uy = (1+\tau)y'$, $y' \in M^G$. De sorte que, pour tout $x \in M$,

tout $y \in M^G$, l'élément $(1+\tau)x + uy$ est de la forme $(1+\tau)x'$, où $x' \in M$ vérifie $Tx' = Tx + \frac{p}{\varphi} y$, ce qui prouve 2.

Notation. — Pour $x \in M$, on notera clx sa classe modulo pM.

DÉFINITION 5.1. — *Dans le cas où* $\frac{(1+\tau)N}{p}$ *n'appartient pas à* $\mathfrak{D}$, *on désigne par* g *l'application de* M^* *dans* M^G/pM^G *qui, à* $X = [(1+\tau)x]$ *associe* $cl(Tx)$.

Il est clair que g est une R-application, surjective grâce à l'hypothèse (H_1).

Les R-applications f (cf. paragraphe 3) et g vérifient les propriétés suivantes :

LEMME 5.2. — *Soit* $X \in M^*$, $(1+\tau)x$ *un de ses représentants dans* M^g.

1) *Les conditions suivantes sont équivalentes :*

a) $f(x) = 0$;

b) Il existe $y \in M$ *tel que :* $X = [(1+\tau)(\sigma - \sigma^{-1})y]$;

c) il existe $z \in M$ *tel que :* $L(1+\tau)x \equiv (1-\tau)Nz$ *modulo* p.

2) *Si* $\frac{(1+\tau)N}{p}$ *n'appartient pas à* $\mathfrak{D}$, *la condition a) ci-dessus implique la condition :*

d) $g(X) = 0$.

Démonstration du lemme 5.2. — Les conditions *a)*, *c)* et *d)* sont invariantes par localisation en p, La relation

$$pX = \sum_{i=0}^{p-1} [(1+\tau)(1-\sigma^i)x]$$

montre qu'il en est de même pour *b)*.

Supposons donc 2 inversible dans A.

1. *a)* $\Longrightarrow$ *b)* se déduit de la congruence modulo $\mathfrak{D}_0$:

$$p(1+\tau) \sim (1+\tau)(\sigma - \sigma^{-1}) \frac{\sigma L'}{2} (1+\tau) \quad \text{(lemme 2.3)}$$

b) $\Longrightarrow$ *c)* se déduit de la congruence modulo p :

$$L(1+\tau)(\sigma - \sigma^{-1}) \equiv (1-\tau)N$$

$c) \Longrightarrow a)$ résulte de la définition de f.

2. $b) \Longrightarrow d)$ provient de $\mathrm{T}(\sigma - \sigma^{-1}) = 0$.

B. — *Démonstration de la proposition* 3.1.

1) Si $\dfrac{(1+\tau)\mathrm{N}}{p}$ *n'appartient pas à* $\mathfrak{O}$: la partie 2 du lemme 5.2. montre que l'on a $\dim f(\mathrm{M}^*) \geqslant \dim g(\mathrm{M}^*) = r$.

2) *Si* $\dfrac{(1-\tau)\mathrm{N}}{p}$ *appartient à* $\mathfrak{O}$. Soit

$$x \in \mathrm{M}, \qquad \text{et} \qquad \mathrm{X} = [(1+\tau)x].$$

On a

$$f(\mathrm{X}) = 0 \Longleftrightarrow (1-\tau)\mathrm{L}x \equiv 0\ (\mathrm{pM}) \quad \text{(lemme 5.2., partie 1).}$$

D'où les équivalences :

$$(d(\mathrm{M}) = -r) \Longleftrightarrow (f(\mathrm{X}) = 0 \quad \text{pour tout} \quad \mathrm{X} \in \mathrm{M}^*) \Longleftrightarrow \left(\frac{(1-\tau)\mathrm{L}}{p} \in \mathfrak{O}(\mathrm{M})\right).$$

3) Pour achever la démonstration de la proposition 3.1, introduisons l'automorphisme ψ de l'algèbre $\mathrm{K}[\mathrm{G}]$ définie par $\psi(\sigma) = \sigma$, $\psi(\tau) = -\tau$. Soit $\overline{\mathfrak{O}}$ l'ordre image de $\mathfrak{O}$ par ψ. On peut, grâce à ψ, munir le groupe additif sous-jacent de M d'une structure de $\overline{\mathfrak{O}}$ module notée $\overline{\mathrm{M}}$. Les $\mathfrak{O}$-module M et $\overline{\mathfrak{O}}$ module $\overline{\mathrm{M}}$ ont même structure. Montrons que l'on a $d(\mathrm{M}) = -d(\overline{\mathrm{M}})$ soit encore :

$$\dim f(\mathrm{M}^*) + \dim f(\overline{\mathrm{M}}^*) = 2r.$$

Considérons pour cela l'élément $\alpha = [(\sigma - \sigma^{-1})^{p-3}]$ de R et l'application $\varphi : \mathrm{M}^* \to \mathrm{M}^*/p\mathrm{M}^*$ qui à $\mathrm{X} \in \mathrm{M}^*$ associe $cl(\alpha \mathrm{X})$. On montre que c'est une R-application et que $\varphi(\mathrm{M}^*)$ a pour dimension $2r$ sur $\mathrm{A}/p\mathrm{A}$ (il suffit pour cela de localiser en p). La relation $\alpha[(1+\tau)(\sigma - \sigma^{-1}] = [\mathrm{L}(1-\tau)]$ conduit aux équivalences :

$$f(\mathrm{X}) = 0 \Longleftrightarrow (\text{il existe } x \in \mathrm{M} \text{ tel que } \mathrm{X} = [(1+\tau)(\sigma - \sigma^{-1})x]) \Longleftrightarrow (\varphi(\mathrm{X}) \text{ appartient à } \overline{f}\,(\overline{\mathrm{M}}^*)).$$

4) Supposons ici M projectif sur $\mathfrak{O}$: il existe un $\mathfrak{O}$-module M′ vérifiant les hypothèses (H_0) tel que l'on ait :

$$M \oplus M' \simeq \mathfrak{O}^k.$$

$\{T\}$ et $\{\overline{T}\}$ étant des A-bases de $\mathfrak{O}^G$ et $\overline{\mathfrak{O}}^G$, le $\mathfrak{O}$-module $\mathfrak{O}^k$ vérifie les hypothèses (H_1). Il est aisé d'en conclure qu'il en est de même pour M et M′.

Les hypothèses de la proposition 3.1. sont donc vérifiées par M et M′. Il suffit donc, pour démontrer le corollaire 3.1., d'examiner les cas $\mathfrak{O} = \mathfrak{O}_1$ et $\mathfrak{O} = \mathfrak{O}_2$. La relation :

$$d(M) + d(M') = kd(\mathfrak{O}) = 0,$$

et le fait que $d(M)$ et $d(M')$ ont le même signe, prouve $d(M) = d(M') = 0$.

5) On suppose ici que M est de rang 1 et vérifie $\mathfrak{O}(M) = \mathfrak{O}$.

Montrons par exemple que $x \to Tx$ est une surjection de M sur M^G. La relation : $2py = (1 + \tau)Ny$ pour tout $y \in M^G$ permet de se borner aux cas où A est local d'idéal maximal sur A, avec $m = 2$, ou $m = p$, et où $\dfrac{(1+\tau)N}{m}$ n'appartient pas à $\mathfrak{O}$. Le A-module libre de rang 1 M^G admet alors pour base tout élément de M^G non congru à 0 modulo m. L'hypothèse « $\dfrac{(1+\tau)N}{m}$ n'appartient pas à $\mathfrak{O}(M)$ » permet de trouver un tel élément de la forme $(1 + \tau)Nx$, avec $x \in M$.

M vérifie ainsi les hypothèses de la proposition 3.1. : il nous suffit donc, pour démontrer le corollaire 3.2., d'examiner le cas $\mathfrak{O} = \mathfrak{O}_3$. L'hypothèse $\mathfrak{O}(M) = \mathfrak{O}_3$ permet alors, d'après la partie 2 de la proposition 3.1., d'éliminer les cas

$$d(M) = +1 \qquad \text{et} \qquad d(M) = -1.$$

C. — *Une propriété du quotient* $M/\overline{M}^G$.

Le $\mathfrak{O}$*-module quotient* $M/\overline{M}^G$ peut être canoniquement muni d'une structure de module sur l'anneau $\mathfrak{O}/\overline{\mathfrak{O}}^G$, sans A-torsion, de « rang » r.

Nous nous proposons de montrer ici que *s'il est libre sur* $\mathfrak{O}/\overline{\mathfrak{O}}^G$, *alors* M *est libre sur* $\mathfrak{O}$.

Pour $x \in M$, nous noterons $\dot{x}$ sa classe modulo $\overline{M}^G$. Il s'agit de prouver que, si $(\dot{\theta}_1, \ldots, \dot{\theta}_r)$ est une base de $M/\overline{M}^G$ sur $\mathfrak{O}/\overline{\mathfrak{O}}^G$, il existe un système de représentants $(\varphi_1, \ldots, \varphi_r)$ de $(\dot{\theta}_1, \ldots, \dot{\theta}_r)$ dans M tel que les $(\overline{T}\varphi_i)_{i=1,\ldots,r}$ constituent une A-base de $\overline{M}^G$.

Soient $\{\bar{e}_i\}_{i=1,2,\ldots,r}$ une A-base de $\overline{M}^G$ fixée.

A tout r-uple $(x_1, \ldots, x_r)$ d'éléments de M on peut associer la matrice $\mathfrak{A} = (a_{ij})_{\substack{1\leqslant i\leqslant r\\ 1\leqslant j\leqslant r}}$ de $\mathfrak{M}_r(A)$ définie par

$$\overline{T}x_i = \sum_{j=1}^{j=r} a_{ij}\bar{e}_j.$$

Lorsque x_i décrit sa classe modulo $\overline{M}^G$, chaque a_{ij} décrit sa classe modulo $\frac{2p}{h}A$ (cf. définition 3.3). Nous sommes amenés à introduire les notations suivantes :

Deux matrices $\mathfrak{A} = (a_{ij})_{\substack{1\leqslant i\leqslant r\\ 1\leqslant j\leqslant r}}$ et $\mathfrak{B} = (b_{ij})_{\substack{1\leqslant i\leqslant r\\ 1\leqslant j\leqslant r}}$ sont équivalentes — relation notée $\mathfrak{A} \sim \mathfrak{B}$ — si l'on a

$$a_{ij} \equiv b_{ij} \text{ modulo } \frac{2p}{h} \text{ pour tous } i, j \in \{1, \ldots, r\}.$$

La classe de $\mathfrak{A}$ sera notée $\tilde{\mathfrak{A}}$ et représentée par une matrice d'ordre r à coefficients dans $A/\frac{2p}{h}A$.

Ainsi, on peut à tout r-uple $(\dot{x}_1, \ldots, \dot{x}_r)$ de $M/\overline{M}^G$ associer une classe $\tilde{\mathfrak{A}}$ de matrices telle que :

Pour qu'il existe un système $(\xi_1, \ldots, \xi_r)$ de représentants dans M de ce r-uple tel que les $(\overline{T}\xi_i)_{i=1,\ldots,r}$ soient linéairement indépendants sur A (respectivement constituent une A-base de $\overline{M}^G$) il faut et il suffit qu'il existe dans la classe $\tilde{\mathfrak{A}}$ une matrice régulière (respectivement inversible).

L'étude de telles conditions pour $\tilde{\mathfrak{A}}$ nous conduit au résultat suivant :

LEMME 5.3. — *Soit* $\tilde{\mathfrak{A}}$ *une classe de matrices. Alors :*

1) *Il existe une matrice régulière équivalente à* $\mathfrak{A}$.

2) *Si* $\mathfrak{A}$ *est inversible dans* $\mathfrak{M}_r\left(\mathrm{A}/\frac{2p}{\overline{h}}\,\mathrm{A}\right)$, *alors il existe une matrice* $\mathfrak{P}$ *inversible dans* $\mathfrak{M}_r(\mathrm{A})$, *et* r *entiers* $n_1, \ldots, n_r$ *tels que*

$$\begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix} \mathfrak{A} \to \mathfrak{B}.$$

Ces propriétés, triviales dans le cas $\overline{h} = 2p$, sont dans le cas $r = 1$, conséquences immédiates des hypothèses : $\mathrm{A}/_{2\mathrm{A}} \simeq \mathrm{Z}/_{2\mathrm{Z}}$ (pour $\overline{h} \not\equiv 0(2)$) et $\mathrm{A}/p\mathrm{A} \simeq \mathrm{Z}/p\mathrm{Z}$ (pour $\overline{h} \not\equiv 0(p)$). Notons que cette dernière hypothèse n'intervient que dans cette démonstration.

Le lemme se démontre dans le cas général par récurrence sur r.

Pour interpréter la classe de matrices $\widetilde{\begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix}}\,\mathfrak{A}$, on utilise une propriété de l'algèbre A[G] démontrée par J. Martinet [4].

Pour tout $n \in \mathrm{Z}$ inversible modulo $2p$ il existe $\omega_n \in \mathfrak{O}_0$, inversible modulo $\overline{\mathfrak{O}}_0^{\mathrm{G}}$ et tel que l'on ait $\overline{\mathrm{T}}\omega_n = n\overline{\mathrm{T}}$.

De sorte que si la classe $\mathfrak{A}$ est associée au r-uple $(\dot{x}_1, \ldots, \dot{x}_r)$, la classe $\widetilde{\begin{pmatrix} \vdots \\ n_r \end{pmatrix}}\,\mathfrak{A}$ est associée au r-uple $(\widehat{\omega_{n_1}\dot{x}_1}, \ldots, \widehat{\omega_{n_r}\dot{x}_r})$ (les n_i, $1 \leqslant i \leqslant r$ sont en effet inversibles modulo $\frac{2p}{\overline{h}}$ donc $2p$).

Supposons maintenant que le $\mathfrak{O}/\overline{\mathfrak{O}}^{\mathrm{G}}$-module $\mathrm{M}/\overline{\mathrm{M}}^{\mathrm{G}}$ soit libre et admette pour base : $(\dot{\theta}_1, \ldots, \dot{\theta}_r)$. La classe de matrices $\mathfrak{A}$ associée au r-uple $(\dot{\theta}_1, \ldots, \dot{\theta}_r)$ est inversible : il suffit pour s'en assurer d'écrire sur $(\dot{\theta}_1, \ldots, \dot{\theta}_r)$ les éléments $\dot{y}_j \in \mathrm{M}/\overline{\mathrm{M}}^{\mathrm{G}}$ tels que l'on ait $\overline{\mathrm{T}}y_j = \bar{e}_j (j = 1, \ldots, r)$ (nous utilisons ici l'hypothèse (H_1)).

D'après l'étude faite ci-dessus, il existe r éléments ω_i de $\mathfrak{O}/\overline{\mathfrak{O}}^{\mathrm{G}}$, inversibles, tels que la classe de matrice associée au r-uple $(\widehat{\omega_1\theta_1}, \ldots, \widehat{\omega_1\theta_r})$ admette un représentant $\mathfrak{B}$ inversible. Ce r-uple, qui constitue une base de $\mathrm{M}/\overline{\mathrm{M}}^{\mathrm{G}}$, admettra alors un système de représentants $(\varphi_1, \ldots, \varphi_r)$ tels que les

$(\overline{T}\varphi_i)_{i=1,\ldots,r}$ soient une base de $\overline{M}^G$, donc constituant une $\mathfrak{O}$-base de $\mathbf{M}$.

Remarquons que si $\dfrac{(1-\tau)N}{p}$ appartient à $\mathfrak{O}$, on peut prendre $\omega_i = 1$ pour tout i.

Nous allons maintenant montrer que, si $\mathbf{M}$ vérifie les hypothèses (H_2) et (H_3), le $\mathfrak{O}/\overline{\mathfrak{O}}^G$-module $\mathbf{M}/\overline{\mathbf{M}}^G$ est libre, ce qui achèvera la démonstration du théorème 4.1.

Nous allons, pour cela, construire des bases particulières de $\mathbf{M}^*$.

D. — *Bases normales et semi-normales de* $\mathbf{M}^* = \mathbf{M}^g/\mathbf{M}^G$.

1) Soit $\{[\lambda_1],]\lambda_2]\}$ une R-base de $\mathfrak{O}^* = \mathfrak{O}^g/\mathfrak{O}^G$.

Une base de $\mathbf{M}^*$ sur R est *semi-normale* si elle est de la forme $\{X_i, Y_i\}_{i=1,\ldots,r}$, où l'on a, pour tout $i \in \{1, \ldots, r\}$, $X_i = [\lambda_1 x_i]$, les x_i étant des éléments de $\mathbf{M}$ tels que $(Tx_1, \ldots, Tx_r)$ soit une A-base de $\mathbf{M}^G$.

Une base de $\mathbf{M}^*$ sur R est *normale* si elle est de la forme $\{X_i, Y_i\}_{i=1,\ldots,r}$, où l'on a pour tout

$$i \in \{1, \ldots, r\} : X_i = [\lambda_1\theta_i],\ Y_i = [\lambda_2\theta_i]$$

les θ_i étant des éléments de $\mathbf{M}$ tels que $(T\theta_1, \ldots, T\theta_r)$ soit une A-base de $\mathbf{M}^G$.

La notion de base normale est indépendante du choix de la base $([\lambda_1], [\lambda_2])$ de $\mathfrak{O}^*$, et signifie que *tout* $x \in \mathbf{M}^g$ *s'écrit d'une façon unique sous la forme* $x = \sum_{i=1}^{i=r} \mu_i\theta_i$, $\mu_i \in \mathfrak{O}$ *pour tout* i.

Nous serons amenés, pour construire une telle base, à distinguer le cas des ordres $\mathfrak{O}_4$ et $\mathfrak{O}'_4$.

Pour $\mathfrak{O} \neq \mathfrak{O}_4$, $\mathfrak{O} \neq \mathfrak{O}'_4$, nous choisirons $\lambda_1 = 1 + \tau$, $\lambda_2 = (1 + \tau)\sigma$.

Dans le cas $\mathfrak{O} = \mathfrak{O}_4$ ou $\mathfrak{O}'_4$, on montre qu'on peut supposer $\lambda_1 \in A[G]$, ce que nous ferons. Nous utiliserons les propriétés suivantes d'une telle base :

LEMME 5.4. — 1) *Il existe* μ_1 *et* ν *appartenant à* $A[G]$ *tels que :*

$$(1 + \tau) \sim \lambda_1\mu_1 \quad \textit{et} \quad 0 \sim \lambda_1\nu.$$

2) *Dans le cas des ordres* $\mathfrak{O}_4$ *ou* $\mathfrak{O}'_4$, *il existe* $\mu_2 \in A[G]$ *tel que*

$$1 + \tau \sim \lambda_2 \nu \mu_2$$

(*tous les symboles* $\sim$ *désignent des congruences modulo* $\mathfrak{O}^G$).

Démonstration. — Pour $\mathfrak{O} \neq \mathfrak{O}'_4$ et $\mathfrak{O} \neq \mathfrak{O}'_4$, on prendra $\mu_1 = 1$ et $\nu = 1 - \tau$. Supposons $\mathfrak{O} = \mathfrak{O}_4$ ou $\mathfrak{O} = \mathfrak{O}'_4$, et posons

$$[1 + \tau] = \alpha_1[\lambda_1] + \alpha_2[\lambda_2]$$
$$[(1 + \tau)\sigma] = \beta_1[\lambda_1] + \beta_2[\lambda_2]$$

où $\alpha_1\alpha_2\beta_1\beta_2$ appartiennent à R.

On montre que l'on peut choisir :

$$\mu_1 \sim (\alpha_1\sigma^{-1} - \beta_1)\frac{(1-\tau)L'\sigma}{p}; \quad \nu \sim \frac{\alpha_2\sigma^{-1} - \beta_2}{(\sigma - \sigma^{-1})^2}(1 - \tau)$$

et

$$\mu_2 \sim (\sigma - \sigma^{-1})^2 \frac{L'\sigma}{p}.$$

2) Supposons maintenant que M vérifie l'hypothèse (H_3), c'est-à-dire que M^* soit libre sur R, et construisons une R-base semi-normale. Pour cela, étudions la condition « il existe $x \in M$ tel que $X = [\lambda_1 x]$ et $Tx = e$ » où $X \in M^*$ et $e \in M^G$ sont donnés.

Cette condition est toujours vérifiée si $\dfrac{(1+\tau)N}{p}$ appartient à $\mathfrak{O}$ cela résulte, dans le cas $\mathfrak{O} \neq \mathfrak{O}_4, \mathfrak{O}'_4$, du lemme 5.1, et dans le cas $\mathfrak{O} = \mathfrak{O}_4$ ou $\mathfrak{O} = \mathfrak{O}'_4$ des lemmes 5.1. et 5.4 : soient en effet $x_1 \in M$ tel que $X = [(1 + \tau)x_1]$, et $x_2 \in M$ tel que $Tx_2 = e - T(\mu_1 x_1)$. Alors l'élément $x = \mu_1 x_1 + \dfrac{N}{p} x_2$ de M convient.

Donc si $\dfrac{(1+\tau)N}{p}$ appartient à $\mathfrak{O}$, toute R-base de M^* est semi-normale.

Supposons que $\dfrac{(1+\tau)N}{p}$ n'appartienne pas à $\mathfrak{O}$. La condition $X = [(1 + \tau)x]$, $Tx = e$ équivaut, d'après le lemme 5.1, à $g(X) = cl(e)$. Soit alors $\{E_k\}_{1 \leqslant k \leqslant 2r}$ une R-base de M^* numérotée de façon que $\{g(E)_k\}_{r+1 \leqslant k \leqslant 2r}$ soit une A/pA-base de M^G/pM^G. Si $\{e_i\}_{1 \leqslant i \leqslant r}$ est une A-base de M^G,

écrivons :

$$cl(e_i) - g(E_i) = \sum_{j=1}^{j=r} cl(a_{ij}) g(E_{r+j}) \quad i \in \{1, \ldots, r\}$$

où $a_{ij} \in A$.

Alors on obtient une R-base semi-normale de M^* en prenant

$$X_i = E_i + \sum_{j=1}^{r} a_{ij} E_{r+j} \quad \text{pour} \quad i = 1, \ldots, r.$$
$$Y_i = E_{r+i}.$$

3) Supposons maintenant qu'en outre M vérifie l'hypothèse $d(M) \leqslant r\, d(\mathfrak{O})$; nous allons construire une R-base normale de M^*.

Soit $(X_i, Y_i)_{1 \leqslant i \leqslant r}$ une base semi-normale de M^*, avec $X_i = [\lambda_1 x_i]$, et posons $Z_i = [\lambda_2 x_i]$ pour $i = 1, \ldots, r$.

Il est facile de voir que si $Y_i - Z_i$ est de la forme $[\lambda_2 \nu y_i]$ avec $y_i \in M$ pour tout i, la base $(X_i, Y_i)_{1 \leqslant i \leqslant r}$ est une base normale (si ν est l'élément introduit dans le lemme 5.4., $\theta_i = x_i + \nu y_i$ vérifie en effet $X_i = [\lambda_1 \theta_i]$, $Y_i = [\lambda_2 \theta_i]$, $T\theta_i = Tx_i$).

Étudions donc la condition « il existe $x \in M$ tel que $X = [\lambda_2 \nu x]$, X étant donné ».

La congruence $1 + \tau \sim \lambda_2 \nu \mu_2$ du lemme 5.4., jointe au lemme 5.1, montre qu'elle est toujours vérifiée dans le cas $\mathfrak{O} = \mathfrak{O}_4$ ou $\mathfrak{O}'_4$. Dans les autres cas, on a

$$\lambda_2 \nu = (1 + \tau)(\sigma - \sigma^{-1})$$

et donc la condition ci-dessus équivaut à $f(X) = 0$.

D'où il résulte que, dans le cas des ordres $\mathfrak{O}_4$, $\mathfrak{O}'_4$, $\mathfrak{O}_5$ et $\mathfrak{O}'_5$ toute R-base de M^* est normale. On suppose désormais $\mathfrak{O} \subset \mathfrak{O}'_3$, et on est alors amenés à construire une R-base semi-normale $(X_i, Y_i) i = 1, \ldots . r$ telle que $f(X_i) = f(Y_i)$ pour tout $i = 1, \ldots, r$. Soit donc $(X'_i, Y'_i)_{1 \leqslant i \leqslant r}$ une R-base semi-normale quelconque de M^*.

— Si $\dfrac{(1 + \tau)N}{p}$ n'appartient pas à $\mathfrak{O}$, les éléments $(g(X'_i)_{i=1, \ldots, r}$ sont linéairement indépendants sur A/pA et donc aussi les $(f(X'_i)_{i=1, \ldots, r}$ (lemme 5.2).

— Dans le cas contraire, les X'_i et Y'_i jouent le même rôle. L'hypothèse $d(M) \leqslant 0$ permet donc, dans tous les cas, de considérer que les $(f(X'_i))_{i=1, \ldots, r}$ engendrent $f(M^*)$: il

existe donc des éléments a_{ij} de A tels que l'on ait

$$f(X'_i) - f(Y'_i) = \sum_{j=1}^{j=r} cl(a_{ij}) f(X'_j) \quad i = 1, \ldots, r.$$

On obtient alors une base normale en posant

$$X_i = X'_i$$
$$Y_i = Y'_i + \sum_{j=1}^{j=r} a_{ij} X'_j.$$

4) Supposons enfin que M vérifie en outre $d(M) \geqslant rd(\mathfrak{O})$. Soit $(X_i, Y_i)_{i=1,\ldots,r}$ une base normale de M^*. Les conditions :

$$X_i = [\lambda_1 \theta_i], \quad Y_i = [\lambda_2 \theta_i], \quad T\theta_i = e_i \quad i = 1, \ldots, r$$

ne définissent θ_i que modulo $\overline{M}^G$. A la base normale (X_i, Y_i) est donc associé en fait un r-uple $(\dot{\theta}_1, \ldots, \dot{\theta}_r)$ de $M/\overline{M}^G$. Nous allons montrer que c'est une base de $M/\overline{M}^G$ sur $\mathfrak{O}/\overline{\mathfrak{O}}^G$.

Pour cela, choisissons-en un système de représentants $(\varphi_1, \ldots, \varphi_r)$ tel que les $(T\varphi_i)_{i=1,\ldots,r}$ soient linéairement indépendants sur A (lemme 5.3).

Tout $x \in M^g$ s'écrit de façon unique sous la forme :

$$x = \sum_{i=1}^{r} \mu_i \varphi_i \qquad \text{avec} \qquad \mu_i \in \mathfrak{O}. \tag{1}$$

Soit une relation $\sum_{i=1}^{r} \alpha_i \varphi_i = 0$, avec $\alpha_i \in \mathfrak{O}$.

L'unicité de la forme (1) montre que l'on a $\mu\alpha_i = 0$ pour tout $i = 1, \ldots, r$, et pour tout $\mu \in \mathfrak{O}^g$, et donc que α_i est de la forme $\alpha_i = a_i \overline{T}$, avec $a_i \in A$ pour tout i. Ainsi le choix des représentants $(\varphi_i)_{i=1,\ldots,r}$ assure leur indépendance linéaire sur $\mathfrak{O}$. Ils constituent donc une K[G] base de KM : tout $x \in M$ peut s'écrire $x = \sum_{i=1}^{r} \xi_i \varphi_i$ avec $\xi_i \in K[G]$ pour tout i.

Soit $\mu \in \mathfrak{O}^g$. L'écriture de μx sous la forme (1) prouve que $\mu\xi_i$ appartient à $\mathfrak{O}$ pour tout i. ξ_i est donc de la forme :

$$\xi_i = \mu_i + \frac{a_i}{p}(1 - \tau)L + k_i(1 - \tau)N,$$

avec $\mu_i \in \mathfrak{O}$, $k_i \in K$, $a_i \in A$ et $a_i \equiv 0(p)$ sauf peut-être dans les cas $\mathfrak{O} = \mathfrak{O}_1, \mathfrak{O}'_1, \mathfrak{O}_3, \mathfrak{O}'_3$. Montrons que l'hypothèse $d(M) \geqslant 0$ permet de conclure, dans ces cas aussi, $a_i \equiv 0(p)$.

L'élément x appartenant à M, les a_i vérifient :

$$\sum_{i=1}^{r} a_i L(1+\tau)\varphi_i \equiv 0 \text{ modulo } pM + \overline{M}^G,$$

soit encore

$$\sum_{i=1}^{r} cl(a_i) f(X_i) = 0.$$

Or on a $f(X_i) = f(Y_i)$ pour tout i. L'hypothèse $\dim f(M^*) \geqslant r$ montre donc que les $(f(X_i))_{i=1,\ldots,r}$ constituent une base de $f(M^*)$ d'où la conclusion.

On en déduit aisément que les $(\varphi_i)_{i=1,\ldots,r}$ sont une $\mathfrak{O}/\overline{\mathfrak{O}}^G$-base de $M/\overline{M}^G$.

6. Groupe des classes projectives d'un ordre $\mathfrak{O}$.

Soit $\mathfrak{O}$ un ordre de A dans K[G] contenant A[G].

Deux $\mathfrak{O}$-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 $\mathfrak{T}(\mathfrak{O})$, et que le théorème 4.1., complété du corollaire 4.1., nous permet de décrire en distinguant le cas des ordres $\mathfrak{O}_3$ et $\mathfrak{O}'_3$.

THÉORÈME 6.1. — *L'application* $[M] \to h(M)$ *est, dans le cas* $\mathfrak{O} \neq \mathfrak{O}_3$ *et* $\mathfrak{O} \neq \mathfrak{O}'_3$, *un isomorphisme de groupes de* $\mathfrak{T}(\mathfrak{O})$ *sur* $\mathfrak{K}(R)$.

L'application $[M] \to \{h(M), d(M)\}$ *est, dans le cas* $\mathfrak{O} = \mathfrak{O}_3$ *ou* $\mathfrak{O} = \mathfrak{O}'_3$, *un isomorphisme de groupes de* $\mathfrak{T}(\mathfrak{O})$ *sur* $\mathfrak{K}(R) \times Z$.

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 Z[G] tels que $J \oplus Z[G]$ soit isomorphe à $Z[G] \oplus Z[G]$.

Démonstration du théorème 6.1. — Le théorème 4.1, complété du corollaire 4.1, montre que la classe neutre de $\mathfrak{L}(\mathfrak{O})$ est composée de $\mathfrak{O}$-modules libres, et que les applications $[M] \to h(M)$ et $[M] \to (h(M), d(M))$ 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 $h(I)$ soit la classe de $\mathfrak{A}$ dans $\mathfrak{K}(R)$.

Nous utiliserons pour cela les remarques suivantes :

1° On peut se borner aux cas où $\mathfrak{O}$ est un ordre maximal : Soient en effet $\mathfrak{O}'$ et $\mathfrak{O}''$ deux ordres tels que : $\mathfrak{O}' \subset \mathfrak{O}''$.

Si $\mathfrak{J}(\mathfrak{O}')$ (resp. $\mathfrak{J}(\mathfrak{O}'')$) désigne l'ensemble des idéaux à gauche localement libres de $\mathfrak{O}'$ (resp. $\mathfrak{O}''$), on sait que l'application $I \to \mathfrak{O}''I$ est une surjection de $\mathfrak{J}(\mathfrak{O}')$ sur $\mathfrak{J}(\mathfrak{O}'')$. On a de plus $h(I) = h(\mathfrak{O}''I)$ si toutefois l'élément $\dfrac{(1+\tau)L}{p}$ n'appartient à $\mathfrak{O}''$ que s'il appartient à $\mathfrak{O}'$.

2° Soient φ et ψ les isomorphismes de K[G] sur $K \times K \times \mathfrak{M}_2(K_0')$ 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 $\Omega = A \times A \times \mathfrak{M}_2(A_0')$.

Soit $\mathfrak{J}$ le sous-ensemble des éléments $\left[a, b, \begin{pmatrix} u & \rho \\ w & h \end{pmatrix}\right]$ 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 $\mathfrak{K}(R)$:

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

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 $h(I')$ la classe de $\mathfrak{A}$ dans $\mathfrak{K}(R)$.

Dans le cas $\mathfrak{O} = \mathfrak{O}_3$ ou $\mathfrak{O} = \mathfrak{O}_3'$, on achève la démonstration de la surjectivité de $[M] \to (h(M), d(M))$ en utilisant le corollaire 3.1.

Remarque.

M. P. Lee a montré que $\mathfrak{X}(Z[G])$ est isomorphe au groupe $\mathfrak{K}(Z'_0)$ des classes d'idéaux de Z'_0 (anneau des entiers du sous-corps réel maximal de $\mathbf{Q}'$) [2].

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

7. 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]. Nous allons d'abord déterminer, suivant la ramification de l'extension E/K en p et 2, l'ordre $\mathfrak{O}(B)$.

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 7.1. — *L'ordre associé à* B *dans* K[G] *est de type* $\mathfrak{O}_i$ *ou* $\mathfrak{O}'_i$, *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 7.1. — 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 $m = p$.

L'extension E/K est modérément ramifiée si et seulement

si l'on a $\mathrm{Tr}_{E/K}(B) = A$ [4], donc si et seulement si $\frac{(1+\tau)N}{m}$ n'appartient pas à $\mathfrak{O}(B)$.

De plus, si l'extension E/K est modérément ramifiée, l'existence d'une application $f \in \mathrm{End}_A(B)$ telle que pour tout $x \in B$ on ait $x = \sum_{s \in G} sf(s^{-1}x)$ [4] implique que $\frac{(1-\tau)N}{m}$ n'appartient pas à $\mathfrak{O}(B)$. Ces remarques permettent de se borner désormais au cas où A est un anneau de valuation discrète d'idéal maximal pA, et où l'extension E/K n'est pas modérément ramifiée. On vient de voir qu'alors $\frac{(1+\tau)N}{p}$ appartient à $\mathfrak{O}(B)$.

Désignons par $\mathfrak{D}_{B/C}$ la différente de B par rapport à C. Des relations

$$\begin{cases} \nu_{\mathfrak{P}}(\mathfrak{D}_{B/C}) = (t+1)(p-1) \quad \text{pour tout idéal maximal } \mathfrak{P} \text{ de B [7]} \\ \text{et} \\ \mathrm{Tr}_{E/F}(B) \subset pC \Longleftrightarrow B \subset p\mathfrak{D}_{B/C}^{-1} \end{cases}$$

on déduit que N/p appartient à $\mathfrak{O}(B)$ si et seulement si l'on a $(t+1)(p-1) \geqslant \nu_{\mathfrak{P}}(p)$, c'est-à-dire si l'extension E/K ou bien n'est pas totalement ramifiée, ou bien est totalement ramifiée dans le cas $p = 3$, $t = 3$.

Pour montrer qu'alors l'ordre $\mathfrak{O}(B)$ n'est pas maximal, nous utiliserons les lemmes suivants (où l'on suppose seulement l'extension E/K non modérément ramifiée), qui précisent la ramification en $\mathfrak{P}$ de l'extension quadratique E/F′ et de l'extension cyclique de degré pE/F.

LEMME 7.1. — *Soit e l'indice de ramification de $\mathfrak{P}$ dans l'extension* E/F′. *Alors il existe deux éléments x_{-1} et x_1 de* B *tels que*

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

La *démonstration du lemme* 7.1. repose sur le fait que l'extension E/F′ est modérément ramifiée en $\mathfrak{P}$:

Si on désigne par $\mathfrak{D}_{E/F'}$ la différente de B par rapport à C′ et par $\mathfrak{p}'$ la trace de $\mathfrak{P}$ sur C′, on a :

$$\nu_{\mathfrak{P}}(\mathfrak{D}_{E/F'}) = e - 1, \quad \text{d'où} \quad \nu_{\mathfrak{p}'}[\mathrm{Tr}_{E/F'}(\mathfrak{P})] = 1.$$

Il existe donc bien dans $\mathfrak{P}$ un élément x_1 tel que $v_{\mathfrak{P}'}[(1+\tau)x_1] = 1$, soit : $v_{\mathfrak{P}}[(1+\tau)x_1] = e$.

Soit $(g_i)_{i\leqslant -1}$ la suite des groupes de ramification de $\mathfrak{P}$ dans g; on a $g_1 = (1)$ car l'extension E/F′ est modérément ramifiée. La nature de g_0 dépend de la valeur de e : si $e = 1$, τ n'appartient pas à g_0; il existe donc $x \in B$ tel que $v_{\mathfrak{P}}[(1-\tau)x] = 0$. On choisira alors, pour le lemme; $x_{-1} = \omega x$ où ω est un élément de F′ tel que $v_{\mathfrak{P}}(\omega) = 1$. Si $e = 2$, τ appartient à g_0 et on a $v_{\mathfrak{P}}[(1-\tau)x] \geqslant 1$ pour tout $x \in B$. En écrivant que τ n'appartient pas à g_1 on trouve un élément $x_{-1} \in B$ tel que $v_{\mathfrak{P}}(1-\tau)x_{-1} = 1$.

LEMME 7.2. — *Soit* $x \in B$ *tel que* :

$$1 \leqslant v_{\mathfrak{P}}(x) < p.$$

Alors on a

$$v_{\mathfrak{P}}[(\sigma - \sigma^{-1})x] = t + v_{\mathfrak{P}}(x).$$

Démonstration. — Cette propriété de la ramification de $\mathfrak{P}$ dans l'extension totalement ramifiée E/F est invariante par localisation de C en $\mathfrak{p} = \mathfrak{P} \cap C$. Nous supposerons donc que C et B sont des anneaux de valuation discrète d'idéaux maximaux $\mathfrak{p}$ et $\mathfrak{P}$ respectivement, et nous désignerons par π une uniformisante de $\mathfrak{P}$. Posons $y = (\sigma - \sigma^{-1})(\pi)$.

Par définition de t et par choix de π on a

$$v_{\mathfrak{P}}(y) = t + 1.$$

Calculons, pour n entier, $1 \leqslant n < p$, $v_{\mathfrak{P}}[(\sigma - \sigma^{-1})(\pi^n)]$: si on pose $\sigma^{-1}(\pi) = z$, on a :

$$(\sigma - \sigma^{-1})[\pi^n] = \sum_{k=1}^{n} C_n^k y^k z^{n-k}.$$

L'hypothèse $n < p$ implique que C_n^k est premier à p, et on a donc

$$v_{\mathfrak{P}}(C_n^k y^k z^{n-k}) = kt + n \quad \text{pour tout } k$$

d'où

$$v_{\mathfrak{P}}[(\sigma - \sigma^{-1})(\pi^n)] = v_{\mathfrak{P}}[C_n^1 y z^{n-1}] = t + n.$$

Soit alors $x = u\pi^n$ où u est une unité de B.

La relation :

$$(\sigma - \sigma^{-1})(x) = (\sigma - \sigma^{-1})(u) \times \sigma(\pi^n) + \sigma^{-1}(u) \times (\sigma - \sigma^{-1})(\pi^n)$$

et l'inégalité

$$v_{\mathfrak{P}}[(\sigma - \sigma^{-1})(u)] \geqslant t + 1$$

permettent d'achever la démonstration.

Nous pouvons maintenant calculer la valuation en $\mathfrak{P}$ de l'élément $L(1 + \varepsilon)x_\varepsilon$ où, pour $\varepsilon = \pm 1$, x_ε est défini dans le lemme 7.1.

On déduit en effet du lemme 7.2., par récurrence sur l'entier h, que, pour tout $x \in B$ vérifiant

$$1 \leqslant v_{\mathfrak{P}}(x) < p - (h - 1)t,$$

on a

$$v_{\mathfrak{P}}[(\sigma - \sigma^{-1})^h(x)] = ht + v_{\mathfrak{P}}(x).$$

Pour $h = p - 2$, on a $p - (h - 1)t = 3$ dans tous les cas, d'où l'on déduit la formule :

$$\underline{v_{\mathfrak{P}}L(1 + \varepsilon\tau)x_\varepsilon = (p - 2)t + v_{\mathfrak{P}}[(1 + \varepsilon\tau)x_\varepsilon].} \qquad (1)$$

Nous sommes maintenant en mesure d'achever la détermination de l'ordre $\mathfrak{O}(B)$ dans les cas où il contient N/p, c'est-à-dire $e = 1$ ou bien $e = 2$, $t = 3$, $p = 3$:

La formule (1) et le lemme 7.1. donnent alors :

$$\begin{array}{ll} \text{pour } e = 1 & v_{\mathfrak{P}}[L(1 + \varepsilon\tau)x_\varepsilon] = p - 1 \\ \text{pour } e = 2 & v_{\mathfrak{P}}[L(1 + \varepsilon\tau)x_\varepsilon] \leqslant 5 \end{array}$$

et dans tous les cas $v_{\mathfrak{P}}[L(1 + \varepsilon\tau)x_\varepsilon] < ep = v_{\mathfrak{P}}(p)$.

Les deux éléments $L(1 + \tau)x_1$ et $L(1 - \tau)x_{-1}$ ne sont donc pas congrus à 0 modulo p, et l'ordre $\mathfrak{O}(B)$ n'est donc ni $\mathfrak{O}_5$ ni $\mathfrak{O}_4$: $\mathfrak{O}(B) = \mathfrak{O}_3$.

Nous allons maintenant appliquer à l'étude du $\mathfrak{O}(B)$-module B les résultats du paragraphe 4.

1° B *est localement libre sur* $\mathfrak{O}(B)$.

D'après le corollaire 4.2, il suffit de vérifier que, dans le cas $\mathfrak{O}(B) = \mathfrak{O}_1$ ou $\mathfrak{O}_1'$, on a $d(B) \neq -1$: supposons donc que A soit un anneau de valuation, discrète d'idéal maximal pA, l'extension E/K étant totalement ramifiée avec $t = 1$.

Désignons par m un élément de A tel que $F = K[\sqrt{m}]$, par $\mathfrak{P}$ l'idéal maximal de B, par x_{-1} l'élément défini par le lemme 7.1., et par x l'élément $x = \sqrt{m}x_{-1}$.

On a :

$$L(1 + \tau)x = \sqrt{m} \times [L(1 - \tau)x_{-1}]$$

et, d'après la formule (1) :

$$v_{\mathfrak{P}}[L(1 - \tau)x_{-1}] = p - 1,$$

d'où

$$v_{\mathfrak{P}}[L(1 + \tau)x] = 2p - 1.$$

Or, tout $y \in C$ a une valuation $v_{\mathfrak{P}}(y)$ congrue à 0 modulo p.

L'élément x considéré est donc tel que $L(1 + \tau)x$ ne soit pas congru modulo p à un élément de C. L'application f introduite au paragraphe 3 n'est donc pas nulle, d'où

$$d(B) \neq -1.$$

2° B *est libre sur* $\mathfrak{O}(B)$.

Le théorème 4.1. montre qu'il suffit, pour s'en assurer, de déterminer $h(B)$. C'est la classe principale de $\mathfrak{K}(R)$ comme le montre le résultat de J. Martinet suivant :

THÉORÈME 7.2. [4]. — La clôture intégrale C′ de A dans F′ admet une base sur A de la forme

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

Cela achève la démonstration du théorème énoncé dans l'introduction.

BIBLIOGRAPHIE

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

[2] M. P. LEE, Intetral reprensentations of dihedral groups of order 2p. *Trans. Amer. math. Soc.*, t. 110, (1964), 213-231.

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

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

[5] J. MARTINET, Modules sur l'algèbre du groupe quaternionien (à paraître aux *Annales de l'E.N.S.*).

[6] D. S. Rim, Modules over finite groups, *Annals of Math.*, Series 2, t. 69, 1959, 700-712.

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

[8] G. Swan, Projective modules over groups rings and maximal orders, *Annals of Math.*, séries 2, t. 76, (1962), 55-61.

Manuscrit reçu le 10 juillet 1971.
accepté par J. L. Koszul.

Anne-Marie Bergé,
Université de Bordeaux 1,
U.E.R. de Mathématiques et d'Informatique,
351, cours de la Libération,
33-Talence.