ANNALES SCIENTIFIQUES DE L'É.N.S.

JACQUES MARTINET

Modules sur l'algèbre du groupe quaternionien

Annales scientifiques de l'É.N.S. 4^e série, tome 4, n° 3 (1971), p. 399-408

<http://www.numdam.org/item?id=ASENS_1971_4_4_3_399_0>

Ann. scient. Éc. Norm. Sup.,
4e série, t. 4, 1971, p. 399 à 408.

MODULES SUR L'ALGÈBRE DU GROUPE QUATERNIONIEN

PAR JACQUES MARTINET.

Soit G le groupe quaternionien d'ordre 8. Il est défini par deux générateurs σ et τ, liés par les relations $\sigma^4 = 1$, $\tau^2 = \sigma^2$, $\tau\sigma\tau^{-1} = \sigma^{-1}$.

Nous montrons, dans le paragraphe I, qu'il y a exactement deux classes d'isomorphismes de $\mathbf{Z}[G]$-modules projectifs de rang 1 (un module M sur l'algèbre $\mathbf{Z}[H]$ d'un groupe H est dit de rang r si $\mathbf{Q}\otimes_{\mathbf{Z}}M$ est libre sur $\mathbf{Q}[H]$ avec r générateurs). De plus, nous donnons une méthode permettant de déterminer effectivement la classe d'un module.

Dans le second paragraphe, on étudie les modules stablement libres sur $\mathbf{Z}[G]$, et l'on montre qu'ils sont en fait libres.

Le troisième paragraphe est consacré à l'étude des extensions N des rationnels, galoisiennes à groupe de Galois isomorphe à G, et modérément ramifiées. On étudie une décomposition du discriminant.

Dans le quatrième paragraphe, on applique les résultats des paragraphes I et III. On en déduit en particulier un exemple d'extension galoisienne modérément ramifiée des rationnels qui ne possède pas de base normale.

I. Les classes d'idéaux de $\mathbf{Z}[G]$

Le centre de G est le sous-groupe $\{1, \sigma^2\}$. Notons $\mathbf{Z}'$ (resp. $\mathbf{Z}''$) le quotient de $\mathbf{Z}[G]$ par l'idéal bilatère $(1 - \sigma^2)$ [resp. $(1 + \sigma^2)$]. Pour tout $\mathbf{Z}[G]$-module M, soit M′ (resp. M″) le sous-module annulé par $(1 - \sigma^2)$ [resp. $(1 + \sigma^2)$]; M′ (resp. M″) est muni canoniquement d'une structure de module sur $\mathbf{Z}'$ (resp. $\mathbf{Z}''$). Soient g le groupe d'ordre 4, produit direct de deux sous-groupes $\{1, s\}$ et $\{1, t\}$ d'ordre 2, et H le corps des quaternions « usuels » sur $\mathbf{Q}$, de base 1, i, j, k, avec $i^2 = j^2 = -1$, $ij = -ji = k$. L'anneau $\mathbf{Z}'$ est

isomorphe à $\mathbf{Z}[g]$ (on applique σ sur s et τ sur t), et l'anneau $\mathbf{Z}''$ est isomorphe au sous-anneau de H formé des quaternions à coefficients entiers (on applique σ sur i et τ sur j). Enfin, nous notons $\mathbf{F}_q$ le corps fini avec q éléments, et identifions $\mathbf{Z}'/2\,\mathbf{Z}'$ et $\mathbf{Z}''/2\,\mathbf{Z}''$ à $\mathbf{F}_2[g]$.

Soit a un entier impair. Notons P_a le $\mathbf{Z}[\mathrm{G}]$-module obtenu de la façon suivante : P_a est libre de rang 8 sur $\mathbf{Z}$, avec pour base un élément e_0 et 7 éléments e_s ($s \in \mathrm{G}$, $s \neq 1$), et G opère par $se_0 = e_0$, et, pour $t \neq 1$, $se_t = e_{st}$ si $t \neq s^{-1}$ et $se_{s^{-1}} = ae_0 - \sum_{t \neq 1} e_t$. On notera e_1 cet élément, si bien que $e_s = se_1$ pour tout $s \in \mathrm{G}$.

THÉORÈME I.1 :

a. Le module P_a *est projectif de rang* 1 *sur* $\mathbf{Z}[\mathrm{G}]$.

b. Deux modules P_a *et* $\mathrm{P}_{a'}$ *sont isomorphes si et seulement si* $a \equiv \pm a' \bmod 8$.

c. Un $\mathbf{Z}[\mathrm{G}]$*-module projectif de rang* 1 *est isomorphe à* P_1 *ou* P_3.

THÉORÈME I.2. — *Soit* M *un* $\mathbf{Z}[\mathrm{G}]$*-module projectif de rang* 1.

a. Les modules M′ *et* M″ *sont libres de rang* 1 *respectivement sur* $\mathbf{Z}'$ et $\mathbf{Z}''$.

b. Une base de M′ *sur* $\mathbf{Z}'$ *(resp. de* M″ *sur* $\mathbf{Z}''$*) est déterminée de manière unique au signe près et à la conjugaison près par un élément de* G.

c. On peut trouver une base φ *de* M′ *sur* $\mathbf{Z}'$ *et une base* ψ *de* M″ *sur* $\mathbf{Z}''$ *de façon qu'une des congruences suivantes, qui s'excluent mutuellement, ait lieu :*

(i) $\qquad \psi \equiv \varphi \bmod 2\,\mathrm{M}$,

(ii) $\qquad \psi \equiv (\sigma + \tau + \tau\sigma)\,\varphi \bmod 2\,\mathrm{M}$.

Nous allons démontrer ensemble ces deux théorèmes. Considérons le module P_a. Le changement de base $e_0 \to e_0$, $e_s \to e_s - ke_0$ montre que P_a et P_{a+8k} sont isomorphes. Le changement de base $e_0 \to -e_0$, $e_s \to e_s$ montre que P_a est isomorphe à P_{-a}. Donc, P_a est isomorphe à P_1 ou à P_3. Le module P_1 est visiblement libre, de base e_1. Pour montrer que P_3 est projectif, il suffit de voir que ses localisés sont libres sur $\mathbf{Z}_{(p)}[\mathrm{G}]$ pour tout nombre premier p, $\mathbf{Z}_{(p)}$ désignant l'anneau local de $\mathbf{Z}$ en p. C'est clair pour $p \neq 3$, car 3 est alors inversible dans $\mathbf{Z}_{(p)}$, et P_1 et P_3 ont des localisés isomorphes. Pour $p = 3$, on fait un raisonnement analogue, en remarquant que P_3 est isomorphe à P_{-5}.

Passons maintenant à la démonstration du théorème I.2. Comme M est projectif, de rang 1 sur $\mathbf{Z}[\mathrm{G}]$, M′ (resp. M″) est projectif de rang 1 sur $\mathbf{Z}'$ (resp. $\mathbf{Z}''$). Il suffit de voir que tout module projectif de rang 1 sur $\mathbf{Z}'$ ou $\mathbf{Z}''$ est libre.

L'ordre maximal $\mathfrak{M}$ de $\mathbf{Z}$ dans $\mathbf{Q}[g]$, isomorphe à $\mathbf{Z}\times\mathbf{Z}\times\mathbf{Z}\times\mathbf{Z}$, jouit de cette propriété; $\mathbf{Z}[g]$ est inclus dans $4\,\mathfrak{M}$; comme tout élément inversible de $\mathbf{Z}/4\,\mathbf{Z}$ est image d'une unité de $\mathbf{Z}$, les modules projectifs de rang 1 sur $\mathbf{Z}'$ sont libres (*cf.* J. P. Serre [6], p. 23-16 et 23-17). Le résultat analogue pour $\mathbf{Z}''$ est bien connu.

Nous avons donc prouvé (*a*). Comme les unités de $\mathfrak{M}$ sont les quadruplets $(\pm 1, \pm 1, \pm 1, \pm 1)$, les unités de $\mathbf{Z}[g]$ sont $\pm 1, \pm s, \pm t, \pm st$; les unités de $\mathbf{Z}'$ sont donc les images des unités de $\mathbf{Z}[G]$. Le résultat analogue pour $\mathbf{Z}''$ est évident, d'où (*b*).

Soit x un élément de M″; alors $x + \sigma^2 x = 0$. Comme M est projectif, $\hat{\mathrm{H}}^0(\{1, \sigma^2\}, \mathrm{M}) = 0$. Il existe alors $y \in \mathrm{M}$, vérifiant $x = y - \sigma^2 y$; $x = y + \sigma^2 y - 2\,\sigma^2 y$ est congru modulo 2 M à un élément de M′. Cela s'applique en particulier à une base ψ de M″ sur $\mathbf{Z}''$. Si φ désigne une base de M′ sur $\mathbf{Z}'$, on peut écrire $\psi \equiv \lambda\varphi$, où $\lambda \in \mathbf{Z}'$ a une image inversible dans $\mathbf{F}_2[g]$. Quitte à remplacer φ par un de ses conjugués, on peut supposer que l'on a $\psi \equiv \varphi \bmod 2\,\mathrm{M}$ ou $\psi \equiv (\sigma + \tau + \tau\sigma)\,\varphi \bmod 2\,\mathrm{M}$. Il est clair que l'on ne peut pas trouver des bases φ, φ' de M′ sur $\mathbf{Z}'$ et ψ, ψ' de M″ sur $\mathbf{Z}''$ de façon que l'on ait $\psi \equiv \varphi$ et $\psi' \equiv (\sigma + \tau + \tau\sigma)\,\varphi' \bmod 2\,\mathrm{M}$.

Revenons maintenant au théorème I.1. Dans le cas du module P_1, on peut prendre $\varphi = (1 + \sigma^2)\,e_1$ et $\psi = (1 - \sigma^2)\,e_1$, d'où $\psi \equiv \varphi \bmod 2\,\mathrm{P}_1$. Dans le cas de P_3, on peut prendre $\varphi = e_0 - e_1 - e_{\sigma^2}$ et $\psi = e_1 - e_{\sigma^2}$; on a alors $\psi \equiv (\sigma + \tau + \tau\sigma)\,\varphi \bmod 2\,\mathrm{P}_3$, ce qui prouve que P_1 et P_3 ne sont pas isomorphes.

Si M est un $\mathbf{Z}[G]$-module projectif, vérifiant, avec les notations du théorème I.2, $\psi \equiv \varphi \bmod 2\,\mathrm{M}$, l'application qui associe $e_1 + e_{\sigma^2}$ à φ et $e_1 - e_{\sigma^2}$ à ψ se prolonge immédiatement en un isomorphisme de M sur P_1. Un raisonnement analogue montre qu'un module pour lequel

$$\psi \equiv (\sigma + \tau + \tau\sigma)\,\varphi \bmod 2\,\mathrm{M}$$

est isomorphe à P_3.

Remarques. — 1° Le fait qu'il y ait dans $\mathbf{Z}[G]$ au moins deux classes d'isomorphismes de modules projectifs de rang 1 était connu de Swan (lettre de Swan à Payan); il prouvait que l'idéal (3, N) de $\mathbf{Z}[G]$, avec $\mathrm{N} = \sum_{s\in G} s$ était projectif et non libre. Cet idéal est visiblement isomorphe à P_3. Le fait que ce soit un idéal bilatère prouve en outre que les modules projectifs de rang 1 ont des anneaux d'endomorphismes isomorphes.

2° On pourrait conduire des raisonnements analogues en remplaçant G par le groupe diédral G′ d'ordre 8, avec deux générateurs σ' et τ', liés

par les relations $\sigma'^4 = \tau'^2 = 1$, $\tau'\sigma'\tau'^{-1} = \sigma'^{-1}$. L'anneau $\mathbf{Z}''$ est alors isomorphe à un sous-anneau de l'anneau des matrices d'ordre 2 à coefficients dans $\mathbf{Z}$. Comme l'image dans $\mathbf{Z}''$ de $\sigma' + \tau' + \tau'\sigma'$ est inversible, on en déduit que tout module projectif de rang 1 sur $\mathbf{Z}[G']$ est libre.

II. Stabilité

Soit A un anneau. On dit qu'un A-module M, de type fini, est stablement libre (ou stablement trivial) s'il existe deux A-modules libres de type fini L_1 et L_2 et un isomorphe de $M \oplus L_1$ sur L_2; un module stablement libre est bien entendu projectif.

THÉORÈME II.1. — *Un $\mathbf{Z}[G]$-module stablement libre est libre.*

Démonstration. — Soit P un $\mathbf{Z}[G]$-module stablement libre, qui n'est pas libre. On sait que le rang de P est défini, et que, en notant r son rang, P est isomorphe à la somme directe d'un module libre de rang $r-1$ et d'un module projectif de rang 1 (Swan [7]). On a donc un isomorphisme de P sur $P_1'^{r-1} \oplus P_3$, et, de plus, il existe un entier r' tel que $P_1'^{r'+r-1} \oplus P_3$ soit libre. Tout revient donc à montrer que, quel que soit r, $Q = P_1'^{r-1} \oplus P_3$ n'est jamais libre.

Notons φ_i (resp. ψ_i) $(1 \leqq i \leqq r-1)$, un générateur de la $i^{\text{ième}}$ copie de P_1' (resp. P_1'') et φ' (resp. ψ') un générateur de P_3' (resp. P_3''). Dire que Q est libre revient à dire qu'il existe des matrices M' et M'' d'ordre r à coefficients dans $\mathbf{Z}[G]$, telles que les images de M' modulo $(1-\sigma^2)$ et de M'' modulo $(1+\sigma^2)$ soient inversibles dans $M_r(\mathbf{Z}')$ et $M_r(\mathbf{Z}'')$ respectivement, et vérifient en outre la condition

$$M'\begin{pmatrix}\varphi_i\\ \varphi'\end{pmatrix} \equiv M''\begin{pmatrix}\psi_i\\ \psi'\end{pmatrix} \bmod 2\,Q.$$

Compte tenu des congruences $\psi_i \equiv \varphi_i \bmod 2P$, et $\psi' \equiv (\sigma+\tau+\tau\sigma)\varphi' \bmod P_3$, on voit, en travaillant modulo l'idéal $(2, 1-\sigma^2) = (2, 1+\sigma^2)$ de $\mathbf{Z}[G]$ et en identifiant les anneaux $\mathbf{Z}'/2\,\mathbf{Z}'$ et $\mathbf{Z}''/2\,\mathbf{Z}''$ à l'algèbre $\mathbf{F}_2[g]$ de g sur le corps à deux éléments, que le théorème II.1 est une conséquence de la

PROPOSITION II.2. — *Soient m' et m'' deux matrices de $M_r(\mathbf{F}_2[g])$, vérifiant la relation $m' = m''\begin{pmatrix}I_{r-1} & 0\\ 0 & s+t+st\end{pmatrix}$, où I_{r-1} est la matrice unité de dimension $r-1$. Soit M' (resp. M'') une matrice de $M_r(\mathbf{Z}')$ [resp. $M_r(\mathbf{Z}'')$], ayant m' (resp. m'') comme image modulo 2. Alors, l'une au plus des matrices M', M'' est inversible.*

Démonstration. — On a la relation dét $(m') = (s + t + st)$ dét (m''). Il suffit de montrer que si une matrice de $M_r(\mathbf{Z}')$ ou de $M_r(\mathbf{Z}'')$ est inversible, le déterminant de son image modulo 2 est l'un des éléments 1, s, t, st de $\mathbf{F}_2[g]$. C'est clair si $M \in M_r(\mathbf{Z}')$, car le déterminant de l'image de M dans $M_r(\mathbf{F}_2[g])$ est l'image dans $\mathbf{F}_2[g]$ du déterminant de M.

Soit alors M une matrice inversible de $M_r(\mathbf{Z}'')$, et soit m son image modulo 2. Notons N la norme réduite, relativement au corps $\mathbf{Q}$ des rationnels, de l'algèbre centrale simple $M_r(H)$. Bien entendu, N applique $M_r(\mathbf{Z}'')$ dans $\mathbf{Z}$.

LEMME II.3. — *Soit* $M' \in M_r(Z'')$. *Si* $M' \equiv M \bmod 2$, *alors*

$$N(M) \equiv N(M') \bmod 4.$$

Soit $M'' \in M_r(\mathbf{Z}'')$, définie par $M'M^{-1} = 1 + 2M''$, et soit

$$P = X^{2r} + \sum_{i=0}^{2r-1} a_i X^i$$

le polynôme caractéristique réduit de M''. Le coefficient a_{2r-1}, qui est la trace réduite de M'', est pair (puisque la trace réduite d'un élément de Z'' est un entier pair). Le polynôme caractéristique réduit de 2 M'', égal à $X^{2r} + \sum_{i=0}^{2r-1} 2^{2r-i} a_i X^i$, est donc congru modulo à 4 à X^{2r}, ce qui entraîne la congruence cherchée.

Par passage au quotient, on déduit du lemme ci-dessus, un homomorphisme f de $Gl_r(\mathbf{F}_2[g])$ dans $(\mathbf{Z}/4\mathbf{Z})^*$. Soit $f' : \mathbf{F}_2[g]^* \to (\mathbf{Z}/4\mathbf{Z})^*$, l'homomorphisme défini par $f'(s) = f'(t) = 1$ et $f'(s + t + st) = -1$, et soit $h : Gl_r(\mathbf{F}_2[g]) \to (\mathbf{Z}/4\mathbf{Z})^*$ l'homomorphisme $f' \circ$ dét.

LEMME II.4. — *Les homomorphismes f et h sont identiques.*

Démonstration. — Les homomorphismes f et h coïncident sur les matrices triangulaires (la norme réduite est dans ce cas le produit des normes réduites des éléments de la diagonale) et sur les matrices dont les éléments sont dans $\mathbf{Z}$ (la norme réduite est dans ce cas le carré du déterminant).

Par ailleurs, on ne change pas la définition de f si l'on remplace $\mathbf{Z}$ par l'anneau local $\mathbf{Z}_2$ de $\mathbf{Z}$ en 2. Comme 2 est ramifié dans H, l'anneau des combinaisons linéaires à coefficients dans $\mathbf{Z}_2$ des éléments 1, i, j, k est local, et le lemme II.4 est une conséquence du

LEMME II.5. — *Soit* A *un anneau local (non nécessairement commutatif), et n un entier positif. Le groupe* $Gl_n(A)$ *est engendré par le groupe triangulaire supérieur et par les matrices de permutation.*

En effet, soit $(a_{i,j}) \in Gl_n(A)$. L'un des éléments $a_{j,1}$ au moins n'appartient pas à l'idéal maximal de A. Quitte à multiplier par une matrice de permutation, on peut supposer que $a_{11} \not\equiv 0$. Il est alors immédiat que $(a_{i,j})$ est le produit d'une matrice triangulaire et d'une matrice pour laquelle $a_{j,1} = 0$ quel que soit $j \not\equiv 1$. Un raisonnement par récurrence permet de conclure.

Démonstration de la proposition II.2. — Soit $M \in Gl_r(Z'')$. Le lemme II.5, appliqué avec A = Q, montre que N(M) est un nombre positif. Comme N(M) doit être inversible dans **Z**, on a N(M) = + 1, d'où $f(M) = 1$. Alors, $h(M) = 1$, et le déterminant de l'image de M dans $Gl_r(\mathbf{F}_2[g])$ est bien égal à l'un des éléments 1, s, t, st de $\mathbf{F}_2[g]$.

III. Discriminants des extensions modérément ramifiées

Dans les paragraphes III et IV, on note N une extension galoisienne de **Q**, de groupe de Galois G, K son sous-corps bi-quadratique, k_1, k_2, k_3 ses trois sous-corps quadratiques, d_i le discriminant de k_i. Soit A la clôture intégrale de **Z** dans **N**. On suppose l'extension modérément ramifiée; cette hypothèse équivaut à la suivante : A est **Z**[G]-projectif ([3], théorème II.1). La clôture intégrale de **Z** dans K est alors l'ensemble noté A′ dans les paragraphes précédents. Notons encore D le discriminant de K, Δ celui de N. Soient φ et ψ des bases respectives de A′ sur **Z**′ et A″ sur **Z**″.

PROPOSITION III.1. : $\Delta = D\,[\mathrm{Tr}_{K/Q}(\psi^2)]^4$.

L'extension N est soit totalement réelle, soit totalement imaginaire, donc possède un nombre pair de couples de conjugués imaginaires.

Par conséquent, Δ est positif. Il en est de même de D; en fait, K est totalement réelle, puisque, si N est imaginaire, K est le sous-corps réel maximal de N. Les deux membres de l'égalité sont positifs. Il suffit de voir qu'ils engendrent le même idéal dans **Z**.

Soient T, T′ et T″ les trois formes bilinéaires suivantes, respectivement sur N, N′ = K et N″ = Ker $(x \to (1 + \sigma^2)x)$:

$$T(xy) = \mathrm{Tr}_{N/Q}(xy); \qquad T'(x, y) = \mathrm{Tr}_{K/Q}(xy); \qquad T''(x, y) = \mathrm{Tr}_{K/Q}(xy).$$

La dernière égalité a un sens, puisque $\sigma^2(xy) = \sigma^2 x . \sigma^2 y = (-x)(-y) = xy$.

Étant donné une forme bilinéaire θ sur un espace vectoriel V sur Q et un réseau M de $\mathbf{Z}$ dans V, on sait définir le discriminant de θ sur M (J.-P. Serre [5], chap. III).

Ici, $\frac{1}{2}T = (T' \oplus T'')$, car, pour tout $x \in N$, $x = \frac{1}{2}[(x+\sigma^2 x) + (x - \sigma^2 x)]$. Comme $A' \oplus A''$ est d'indice 2^4 dans A, on a

$$\Delta_T(A) = \frac{1}{2}8\,\Delta_{T'\oplus T''}(A) = \Delta_{T'\oplus T''}(A' \oplus A'') = \Delta_{T'}(A')\,\Delta_{T''}(A'').$$

Mais $\Delta_T(A) = \Delta$, $\Delta_{T'}(A') = D$, et il n'y a plus qu'à expliciter le terme $\Delta_{T''}(A'')$. En considérant la base ψ, $\sigma\psi$, $\tau\psi$, $\tau\sigma\psi$ de A'' sur $\mathbf{Z}$, on voit que $\Delta_{T''}(A'') = \text{dét}\,[\mathrm{Tr}_{K/Q}(s\psi.t\psi)]$, s et t parcourant des éléments 1, σ, τ, $\tau\sigma$ de G. Les termes de la diagonale sont de la forme

$$\mathrm{Tr}_{K/Q}(s\,\psi^2) = \mathrm{Tr}_{K/Q}(\psi^2),$$

et les autres termes du déterminant sont nuls, d'où la proposition.

PROPOSITION III.2 : $\mathrm{Tr}_{K/Q}(\psi^2) = \varepsilon \prod_{p \mid \Delta} p$, *avec* $\varepsilon = +1$ *si* N *est réelle*, $\varepsilon = -1$ *si* N *est imaginaire.*

Démonstration. — Si N est réelle, ψ^2 est un élément totalement positif de K, et sa trace est positive. Si N est imaginaire, comme $N = K(\psi)$, K étant totalement réel, ψ^2 est totalement négatif, et sa trace est négative. Il reste à voir que les deux membres de l'égalité engendrent le même idéal dans $\mathbf{Z}$. Le membre de gauche n'est divisible que par les facteurs premiers de Δ, et ceux-ci sont impairs, puisque l'extension $N/\mathbf{Q}$ est modérément ramifiée. Soit p un facteur premier de Δ. Si p divise D, p est non ramifié dans un des sous-corps quadratiques, soit k_i; les facteurs premiers de p dans k_i sont ramifiés dans K/k_i, donc aussi dans N/k_i qui est cyclique. L'exposant de p est alors 1 (respectivement 3) dans le discriminant de K (resp. de N) par rapport à k_i. L'exposant de p dans D (resp. Δ) est donc 2 (resp. 6), et la proposition III.1 montre que l'exposant de p dans $\mathrm{Tr}_{K/Q}(\psi^2)$ est 1.

Si p ne divise pas D, les différents facteurs premiers de p dans K divisent avec l'exposant 1 le discriminant de N par rapport à K; l'exposant de p dans Δ est alors 4, et on conclut comme ci-dessus.

IV. **Bases normales**

On conserve les notations du paragraphe III. On trouvera des détails sur les extensions quaternioniennes, par exemple dans P. Damey et J.-J. Payan [1].

THÉORÈME IV.1. — *L'anneau* A *est libre sur* $\mathbf{Z}[G]$ *si*

$$\mathrm{Tr}_{K/Q}(\psi^2) \equiv \mathrm{Tr}_{K/Q}(\varphi^2) \bmod 4,$$

et est un $\mathbf{Z}[G]$*-module isomorphe à* P_3 *si*

$$\mathrm{Tr}_{K/Q}(\psi^2) \equiv -\mathrm{Tr}_{K/Q}(\varphi^2) \bmod 4.$$

Remarque. — On peut prendre pour φ n'importe lequel des éléments $\frac{\pm 1 \pm \sqrt{d_1} \pm \sqrt{d_2} \pm \sqrt{d_3}}{4}$ de A′. Dans tous les cas, on trouve

$$\mathrm{Tr}_{K/Q}(\varphi^2) = \frac{1 + d_1 + d_2 + d_3}{4}.$$

En utilisant la valeur de $\mathrm{Tr}_{K/Q}(\psi^2)$ donnée par la proposition III.2, on obtient un moyen effectif de déterminer la structure de A comme $\mathbf{Z}[G]$-module.

Démonstration. — Si A est libre, on a $\psi \equiv \varphi \bmod 2$, d'où $\psi^2 \equiv \varphi^2 \bmod 4$, et $\mathrm{Tr}_{K/Q}(\psi^2) \equiv \mathrm{Tr}_{K/Q}(\varphi^2) \bmod 4$.

Si A est isomorphe à P_3, on a $\psi \equiv \sigma\varphi + \tau\varphi + \tau\sigma\varphi \bmod 2$, donc $\psi \equiv \pm 1 - \varphi \bmod 2$, d'où $\psi^2 \equiv 1 + \varphi^2 \pm 2\varphi \bmod 4$, et

$$\mathrm{Tr}_{K/Q}(\psi^2) \equiv \mathrm{Tr}_{K/Q}(\varphi^2) \pm 2 \equiv -\mathrm{Tr}_{K/Q}(\varphi^2) \bmod 4.$$

Exemple 1. — Soit $k_1 = Q(\sqrt{5})$, $k_2 = Q(\sqrt{21})$, $M = \frac{5+\sqrt{5}}{2}\frac{21+\sqrt{21}}{2}$. $N = K(\sqrt{M})$. On a $k_3 = Q(\sqrt{105})$. La norme sur k_1 de M est égale à $21 \times 5 \times \left(\frac{5+\sqrt{5}}{2}\right)^2$. C'est un nombre de la forme $d_3\lambda_1^2$, avec $\lambda_1 \in k_1$. Comme $K = k_1(\sqrt{d_3})$, l'extension N/k_1 est cyclique d'ordre 4. On vérifie de même que N est cyclique sur k_2 et k_3. Il en résulte que N est une extension galoisienne de $\mathbf{Q}$, et que son groupe de Galois est isomorphe à G (le groupe quaternionien est l'unique groupe d'ordre 8 possédant trois sous-groupes cycliques d'ordre 4).

On vérifie immédiatement les congruences $\frac{5+\sqrt{5}}{2} \equiv -\left(\frac{1-\sqrt{5}}{2}\right)^2 \bmod 4$ et $\frac{21+\sqrt{21}}{2} \equiv -\left(\frac{1-\sqrt{21}}{2}\right)^2 \bmod 4$. On a donc $M \equiv \left(\frac{1-\sqrt{5}}{2}\frac{1-\sqrt{21}}{2}\right)^2 \bmod 4$, ce qui prouve que 2 est non ramifié dans N/K (Hecke [2], théorème 119). L'extension $N/\mathbf{Q}$ est donc modérément ramifiée.

Les seuls facteurs premiers de $N_{K/Q}(M)$ sont 3, 5 et 7, et ils sont ramifiés dans K. Ce sont donc les diviseurs premiers de Δ.

En outre, N est un corps totalement réel, puisque M est totalement positif. On a donc

$$\mathrm{Tr}_{K/Q}(\psi^2) = 3\times5\times7 \qquad \text{et} \qquad \mathrm{Tr}_{K/Q}(\varphi^2) = \frac{1+5+21+105}{4}.$$

La différence est $105 - 33 = 72 \equiv 0 \bmod 4$.

L'anneau A des entiers de N est donc libre sur $Z[G]$.

Remarque. — On a $\mathrm{Tr}_{K/Q}(\varphi^2) = \mathrm{Tr}_{K/Q}(M)$, et $\sqrt{M} \in A''$. On en déduit que l'on peut prendre pour ψ l'un des conjugués de $\pm\sqrt{M}$.

Exemple 2. — On conserve le même corps biquadratique que dans l'exemple ci-dessus, et l'on prend $N = K(\sqrt{M'})$ avec $M' = -3M$. Les calculs faits pour l'exemple 1 montrent immédiatement que $N/\mathbf{Q}$ est galoisienne, de groupe de Galois isomorphe à G, et est modérement ramifiée. Les seuls facteurs premiers de Δ sont donc encore 3, 5 et 7. Mais N est cette fois imaginaire. L'anneau A des entiers de N n'est donc pas libre sur $\mathbf{Z}[G]$. Cet exemple donne une réponse négative à la question posée dans [4].

Exemple 3. — Soit $k_1 = Q(\sqrt{5})$, $k_2 = Q(\sqrt{41})$, $M = \frac{5+\sqrt{5}}{2}\,\frac{41+\sqrt{5.41}}{2}$.

On vérifie par des calculs analogues à ceux de l'exemple 1 que $N = K(\sqrt{M})$ est une extension quaternionienne modérément ramifiée, totalement réelle. Les nombres premiers ramifiés dans N sont ici 5 et 41. Alors,

$$\mathrm{Tr}_{K/Q}(\psi^2) = 5\times41 = 205 \qquad \text{et} \qquad \mathrm{Tr}_{K/Q}(\varphi^2)$$
$$= \frac{1+5+41+205}{4} = 63 \equiv -\mathrm{Tr}_{K/Q}(\psi^2) \bmod 4.$$

On obtient ainsi un exemple d'extension totalement réelle dont l'anneau des entiers n'est pas libre sur $\mathbf{Z}[G]$.

Remarque. — Il en résulte du théorème I.1 que l'on peut, dans tous les cas, choisir une base de A sur $\mathbf{Z}$ formée de 1 et des conjugués $s\theta$ ($s \in G$, $s \neq 1$) d'un entier convenable de N.

BIBLIOGRAPHIE

[1] P. Damey et J.-J. Payan, *Existence et construction des extensions galoisiennes et non abéliennes de degré 8 d'un corps de caractéristique différente de 2* (*J. reine angew. Math.*, vol. 244, 1970, p. 37-54).

[2] E. Hecke, *Vorlesungen über die theorie der algebraischen Zahlen*, Leipzig, 1923. Réimpression : New-York, 1948.

[3] J. MARTINET, *Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre* 2 *p* (*Ann. Inst. Fourier*, Grenoble, t. 19, n° 1, 1969, p. 1 à 80).
[4] J. MARTINET, *Sur l'anneau des entiers d'une extension galoisienne*, (Communication individuelle au *Congrès international des Mathématiciens*, Nice, 1970, p. 41).
[5] J.-P. SERRE, *Corps locaux*, Hermann, Paris, 1962.
[6] J.-P. SERRE, *Modules projectifs et espaces fibrés à fibre vectorielle* (*Séminaire Dubreuil*, exposé n° 23, 1968, p. 23-01 à 23-18).
[7] R. G. SWAN, *Induced representations and projective modules* (*Ann. of Math.*, vol. 71, 1960, p. 552-578).

(Manuscrit reçu le 2 mai 1971.)

Jacques MARTINET,
351, cours de la Libération,
33-Talence.