THÉORIE DES NOMBRES. — *Sur les extensions à groupe de Galois quaternionien.* Note (*) de M. **Jacques Martinet**, transmise par M. Henri Cartan.

Soit G le groupe quaternionien d'ordre 8, et soit N une extension galoisienne du corps **Q** des rationnels dont le groupe de Galois est isomorphe à G. On complète dans cette Note les résultats de ([3]) en étudiant la structure en tant que G-module de l'anneau des entiers de N lorsque l'extension n'est pas modérément ramifiée.

1. Notations. — On conserve les notations de ([3]). On note σ et τ deux générateurs de G, liés par les relations $\sigma^4 = 1$, $\tau^2 = \sigma^2$ et $\tau\sigma\tau^{-1} = \sigma^{-1}$; H désigne le sous-groupe de G engendré par σ, et $G' = \{1, \sigma^2\}$ est le centre de G. Soit $\mathbf{Z}'$ (resp. $\mathbf{Z}''$) l'anneau quotient de $\mathbf{Z}[G]$ par l'idéal bilatère $(1 - \sigma^2)$ [resp. $(1 + \sigma^2)$]. On identifie $\mathbf{Z}'$ à $\mathbf{Z}[g]$, où g désigne le groupe abélien engendré par deux éléments s et t d'ordre 2, en appliquant σ sur s et τ sur t, et $\mathbf{Z}''$ à l'ordre de base 1, i, j, k du corps des quaternions $\mathbf{H}$ sur $\mathbf{Q}$, où $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$.

Soit K le sous-corps biquadratique de N, k_i $(1 \leqq i \leqq 3)$ ses trois sous-corps quadratiques, k_1 étant supposé invariant par H. On suppose σ choisi de façon que :

a. Si K/**Q** n'est pas totalement ramifiée en 2, alors $k_1/\mathbf{Q}$ n'est pas ramifiée en 2;

b. Si K/**Q** est totalement ramifiée en 2, le saut de ramification de $k_1/\mathbf{Q}$ est alors égal à 1, ceux de k_2 et k_3 étant égaux à 2.

Les groupes de ramification que nous utilisons sont relatifs à un idéal premier de N au-dessus de 2. Enfin, pour tout corps de nombres L, on note Z_L la clôture intégrale de Z dans L.

2. Ramification et discriminant. — On suppose que l'extension N/**Q** n'est pas modérément ramifiée [pour le cas modéré, se reporter à ([3])]. Le groupe G_0 contient alors G'.

Proposition 1. — (*a*) *Si* K/**Q** *est non ramifiée en* 2, *le saut de ramification de* N/K *est égal à* 1 *ou* 2, *cas désignés respectivement par* A *et* B.

(*b*) *Si* K/**Q** *est ramifiée en* 2, $k_1/\mathbf{Q}$ *ne l'étant pas, l'extension* N/k_1 *possède deux sauts de ramification, qui sont les couples* (1, 3) *ou* (2, 4), *cas désignés respectivement par* C *et* D.

(c) *Si* N/**Q** *est totalement ramifiée en* 2, *la suite des groupes de ramification de* N/**Q** *est :* $G_i = G$ *pour* $i \leq 1$, $G_i = H$ *pour* $1 < i \leq 3$, $G_i = G'$ *pour* $3 < i \leq 7$, $G_i = \{1\}$ *pour* $i > 7$; *ce dernier cas sera désigné par* E.

Le dernier saut de ramification est majoré par l'indice de ramification de 2 dans N et le premier est minoré par 1, d'où (*a*). Les sauts de ramification étant congrus entre eux modulo 2 [([4]), chap. IV, prop. 11], on en déduit (*b*). Enfin, la démonstration de (*c*) se déduit aisément de la proposition 4.5 de ([1]).

Corollaire. — *L'exposant de 2 dans le discriminant de* N/**Q** *est respectivement dans chacun des cas* A *à* E : 8, 12, 16, 22, 24.

3. Les idéaux de l'anneau $\mathbf{Z}''$. — Soit $\mathbf{Z}''_1$ l'ordre maximal de **Z** dans **H** de base 1, i, j et $\varepsilon = (1 + i + j + k)/2$. Comme $\mathbf{Z}''$ et $\mathbf{Z}''_1$ coïncident localement en chaque nombre premier impair, l'algèbre **H** étant de plus ramifiée en 2, $\mathbf{Z}''_1$ est l'unique ordre maximal contenant $\mathbf{Z}''$.

Proposition 2. — *Soit* I *un idéal fractionnaire à gauche de* $\mathbf{Z}''$. *On est alors dans l'un ces cas suivants :*

(i) *L'ordre à gauche de* I *est* $\mathbf{Z}''$, *et* I *est un* $\mathbf{Z}''$*-module libre;*

(ii) *L'ordre à gauche de* I *est* $\mathbf{Z}''_1$, *et* I *est un* $\mathbf{Z}''$*-module isomorphe à* $\mathbf{Z}''_1$.

Les idéaux à gauche de $\mathbf{Z}''_1$ étant principaux, on peut, quitte à remplacer I par un idéal équivalent, supposer que $\mathbf{Z}''_1\, \mathrm{I} = \mathbf{Z}''_1$. Dans ces conditions, I contient le conducteur de $\mathbf{Z}''$ dans $\mathbf{Z}''_1$. L'examen des différentes possibilités prouve tout de suite la proposition.

4. Structure de l'anneau $\mathbf{Z}_N$. — Si L′ est une extension galoisienne finie d'un corps de nombre L, de groupe de Galois G, on appelle ordre associé à l'extension le sous-anneau de L [G] formé des $\lambda \in L[G]$ vérifiant $\lambda\, Z_{L'} \subset Z_{L'}$; notation : $\mathfrak{O}\,(L'/L)$.

Proposition 3. — *L'ordre* $\mathfrak{O}$ (N/**Q**) *contient les idempotents* $(1 + \sigma^2)/2$ *et* $(1 - \sigma^2)/2$ *de* Q [G].

En effet, il résulte de la proposition 1 que, si $x \in \mathbf{Z}_N$, alors $x - \sigma^2 x \in 2\,\mathbf{Z}_N$.

On en déduit que $\mathbf{Z}_N$ est somme directe de ses deux sous-Z [G]-modules $\mathbf{Z}'_N$ et $\mathbf{Z}''_N$, et que l'ordre associé à N/**Q** s'identifie au produit $\mathfrak{O}' \times \mathfrak{O}''$, où $\mathfrak{O}'$ est l'ordre associé à l'extension K/**Q** et $\mathfrak{O}''$ est l'ordre à gauche de $\mathbf{Z}''_N$ considéré comme module sur $\mathbf{Z}''$.

Théorème. — (*a*) *L'ordre associé à l'extension* N/**Q** *est canoniquement isomorphe au produit* $\mathfrak{O}' \times \mathbf{Z}''$, *où l'ordre* $\mathfrak{O}'$ *est défini ainsi :*

(i) *Si* K/**Q** *est non ramifiée en* 2, $\mathfrak{O}' = \mathbf{Z}[g]$;

(ii) *Si* K/**Q** *est ramifiée en* 2 *et si* k_1/**Q** *ne l'est pas,* $\mathfrak{O}'$ *est l'ordre de base sur* **Z** : 1, t, $(1 + s)/2$, $(t + st)/2$;

(iii) *Si* $K/\mathbf{Q}$ *est totalement ramifiée en* 2, $\mathfrak{O}'$ *est l'ordre de base sur* $\mathbf{Z}$: 1, $(1+s)/2$, $(1+t)/2$ $(1+s+t+st)/4$.

(*b*) *L'anneau* $\mathbf{Z}_N$ *des entiers de* N *est libre sur son ordre associé.*

Démonstration. — La détermination de $\mathfrak{O}'$ et le fait que $\mathbf{Z}'_N = \mathbf{Z}_K$ est libre sur $\mathfrak{O}'$ résultent de ([2]). Le fait que $\mathbf{Z}''_N$ est libre sur $\mathfrak{O}''$ résulte de la proposition 2. Il reste à montrer l'égalité $\mathfrak{O}'' = \mathbf{Z}''$. Soit T la forme bilinéaire sur N définie par $T(x, y) = \mathrm{Tr}_{N/\mathbf{Q}}(xy)$. On a l'égalité $(1/2)\, T = T' \oplus T''$, où T' et T'' sont les formes bilinéaires sur N' et N'' définies par

$$T'(x, y) = \mathrm{Tr}_{K/\mathbf{Q}}(xy) \quad \text{et} \quad T''(x, y) = \mathrm{Tr}_{K/\mathbf{Q}}(xy).$$

On sait par ailleurs définir le discriminant d'une forme bilinéaire sur un réseau [([4]), chap. III]. On a l'égalité

$$\Delta(Z''_N) = \frac{1}{2^8}\, \Delta(N/Q)\, (\Delta(K/Q))^{-1},$$

où $\Delta(Z''_N)$ est le discriminant de T'' sur Z''_N, et $\Delta(N/Q)$ et $\Delta(K/Q)$ sont les discriminants respectifs des extensions N/Q et K/Q. L'exposant de 2 dans $\Delta(K/Q)$ est dans chacun des cas A, B, C, D, E respectivement 0, 0, 4, 6, 8; les valeurs de l'exposant de 2 dans $\Delta(Z''_N)$ sont donc respectivement 0, 4, 4, 8, 8.

Soit ψ un élément non nul de Z''_N. On vérifie [*cf.* ([3]), § III] que le discriminant du $\mathbf{Z}$-module engendré par ψ et ses conjugués est l'idéal de $\mathbf{Z}$ engendré par $\mathrm{Tr}_{K/Q}(\psi^2)^4$. Si l'ordre à gauche de $\mathbf{Z}''_N$ était égal à $\mathbf{Z}''_1$, $\mathbf{Z}''_N$ possèderait une $\mathbf{Z}$-base du type ψ, $\sigma\psi$, $\tau\psi$, $\varepsilon\psi$; le discriminant de cette base serait alors $(1/2^2)\, \mathrm{Tr}_{K/Q}(\psi^2)^4$, et l'exposant de 2 dans $\Delta(Z''_N)$ ne serait pas divisible par 4.

C. Q. F. D.

Remarque. — Soit F le conducteur d'Artin du caractère irréductible de degré 2 de G. La formule $\Delta(N/Q) = \Delta(K/Q)\, F^2$ permet d'écrire F sous la forme $F = 2^4\, \mathrm{Tr}_{K/Q}(\psi^2)^2$, expression dans laquelle ψ désigne une base de $\mathbf{Z}''_N$ sur l'anneau de $\mathbf{Z}''$.

(*) Séance du 13 mars 1972.

([1]) J. M. FONTAINE, *Ann. scient. Éc. Norm. Sup.*, 4e série, 4, fasc. 3, 1971, p. 337-392.
([2]) H. W. LEOPOLDT, *J. reine angew. Math.*, 201, 1959, p. 119-149.
([3]) J. MARTINET, *Ann. scient. Éc. Norm. Sup.*, 4e série, 4, fasc. 3, 1971, p. 399-408.
([4]) J. P. SERRE, *Corps locaux*, Hermann, Paris, 1962.

U. E. R. de Mathématiques
et d'Informatique,
Université de Bordeaux I,
351, cours de la Libération,
33-Talence,
Gironde.