Séminaire de théorie des nombres de Grenoble

Bruno Martel

Sur l'anneau des entiers d'une extension biquadratique d'un corps 2-adique

Séminaire de théorie des nombres de Grenoble, tome 3 (1973-1974), exp. nº 2, p. 1-15
<http://www.numdam.org/item?id=STNG_1973-1974__3__A2_0>

Séminaire de Théorie des Nombres
4 octobre 1973
Grenoble

SUR L'ANNEAU DES ENTIERS D'UNE EXTENSION BIQUADRATIQUE D'UN CORPS 2-ADIQUE

par Bruno MARTEL

L'objet de cette étude est de caractériser, à l'aide des nombres de ramification, les extensions biquadratiques d'une corps 2-adique dont l'anneau des entiers est libre sur l'ordre qui lui est associé.

1. GENERALITES.

Soit A l'anneau de valuation d'un corps local k de caractéristique nulle. Soit K une extension galoisienne finie de k, d'anneau de valuation B. Soit G le groupe de Galois de K/k, et $\mathfrak{O}$ l'ordre de A dans $k[G]$ associé à B par :

$$\mathfrak{O} = \{\lambda \in k[G] \; ; \; \lambda B \subset B\} .$$

On sait [4 et 5] que les assertions suivantes sont équivalentes :

(i) K/k modérément ramifiée.

(ii) $\mathfrak{O} = A[G]$.

(iii) B est un $A[G]$-module libre.

Soit θ un entier de K engendrant une base normale de K/k . On définit :

$$\mathfrak{A}_\theta = \{\lambda \in k[G] \; ; \; \lambda\theta \in B\} .$$

PROPOSITION 1.

a) $\mathfrak{A}_\theta$ <u>est un idéal à gauche de</u> $\mathfrak{O}$, <u>isomorphe à</u> B <u>en tant que</u> $\mathfrak{O}$-<u>module</u>.

b) $\mathfrak{O}$ <u>est l'ordre à gauche associé à</u> $\mathfrak{A}_\theta$.

c) <u>Les assertions suivantes sont équivalentes</u> :

(i) B <u>est un</u> $\mathfrak{O}$<u>-module libre</u> ;

(ii) <u>il existe</u> θ <u>tel que</u> $\mathfrak{A}_\theta$ <u>soit un anneau</u> (<u>et alors</u> $\mathfrak{A}_\theta = \mathfrak{O}$) ;

(iii) <u>pour tout</u> θ , $\mathfrak{A}_\theta$ <u>est un idéal à gauche principal de</u> $\mathfrak{O}$.

d) <u>Si</u> G <u>est abélien, et si</u> $\mathfrak{O}_m$ <u>désigne l'ordre maximal de</u> A <u>dans</u> $k[G]$, <u>les inclusions</u> $\mathfrak{A}_\theta \subset \mathfrak{A}_{\theta'} \subset \mathfrak{O}_m$ <u>entraînent</u> $\mathfrak{A}_\theta = \mathfrak{A}_{\theta'}$.

<u>Démontrons d)</u> (cf. [2] pour les trois premiers points).

Puisque $B = \mathfrak{A}_\theta \theta = \mathfrak{A}_{\theta'} \theta'$, il existe $\xi \in \mathfrak{A}_{\theta'}$ tel que $\theta = \xi\theta'$ et $\eta \in \mathfrak{A}_\theta$ tel que $\theta' = \eta\theta$. On a donc $\eta\xi = 1$.

Montrons que $\eta \in \mathfrak{O}$. Soit $\mu \in \mathfrak{A}_{\theta'}$, $\mu\eta \in \mathfrak{A}_\theta \subset \mathfrak{A}_{\theta'}$, donc η appartient à l'ordre associé à $\mathfrak{A}_{\theta'}$.

Montrons que $\xi \in \mathfrak{O}$. Puisque ξ est entier sur A il vérifie

$$\xi^n + a_{n-1}\xi^{n-1} + \ldots + a_o = 0 \qquad a_i \in A$$

$$\xi + a_{n-1} + \ldots + a_o \eta^{n-1} = 0 .$$

On en déduit que $\mathfrak{A}_{\theta'} \subset \mathfrak{A}_\theta$.

On suppose désormais que k est un corps 2-adique, et K une extension biquadratique de k . On note e l'indice de ramification absolu de k , f son degré résiduel, $(K_i)_{1 \leq i \leq 3}$ les trois extensions quadratiques de k contenues dans K , v_K (resp. v_{K_i}) la valuation normalisée de K (resp. K_i) , T (resp. T_i) la trace de l'extension K/k (resp. K/K_i) . On note π (resp. ω) une uniformisante de K (resp. k) .

PROPOSITION 2. <u>L'ordre maximal</u> $\mathfrak{D}_m$ <u>de</u> A <u>dans</u> k[G] <u>est engendré comme</u> A-<u>module par</u> :

$$1 \, , \, \frac{T_1}{2} \, , \, \frac{T_2}{2} \, , \, \frac{T}{4} \, .$$

En effet $1 \, , \, \frac{T_1}{2} \, , \, \frac{T_2}{2} \, , \, \frac{T}{4}$ est une base de k[G] sur k . Soit $\lambda \in k[G]$, déterminons la matrice, relativement à cette base, de l'endomorphisme m_λ de k[G] , multiplication par λ . Si $\lambda = a_o + a_1 \frac{T_1}{2} + a_2 \frac{T_2}{2} + a_3 \frac{T}{4}$, on obtient la matrice triangulaire :

$$\begin{pmatrix} a_o & 0 & 0 & 0 \\ a_1 & a_o+a_1 & 0 & 0 \\ a_2 & 0 & a_o+a_2 & 0 \\ a_3 & a_2+a_3 & a_1+a_3 & \sum_i a_i \end{pmatrix} .$$

Le polynôme caractéristique de m_λ est donc : $(X-a_o)\circ(X-(a_o+a_1))\circ(X-(a_o+a_2))\circ(X-\sum_i a_i)$. Or λ est entier sur A si et seulement si ce polynôme est à coefficients dans A [1].

2. NOMBRES DE RAMIFICATION.

On définit [6] la suite $(G_i)_{i\geq -1}$ des sous-groupes de ramification de G par :

$$G_i = \{g \in G \; ; \; \forall x \in G \quad v_K(g-1)x \geq i+1\} \, .$$

Un nombre t est dit nombre de ramification de l'extension si $G_t \neq G_{t+1}$.

2.1. Si l'extension K/k a un seul nombre de ramification, t . Alors : $f > 1$ et t vérifie : (1) t nombre impair, $0 < t < 2e$.

En effet, $G = G_t/G_{t+1}$ se plonge dans le groupe additif du corps résiduel de K , donc de k . D'autre part, t est le nombre de ramifications des extensions quadratiques intermédiaires. On en déduit que

[6] : $t \leq 2e$, avec égalité si t est pair. Montrons que t est impair. Soit σ_1 le générateur du groupe de Galois de K/K_1 , $T_1\pi = (\sigma_1 - 1)\pi + 2\pi$, donc $v_K T_1 \pi = t+1 \equiv 0 \mod 2$.

Réciproquement, étant donné un corps 2-adique k de degré résiduel $f > 1$, il existe des extensions biquadratiques de k avec un seul nombre de ramification vérifiant (1). Plus généralement :

PROPOSITION 3. <u>Soit</u> k <u>un corps p-adique d'indice de ramification absolu</u> e , <u>de degré résiduel</u> f . <u>Soit</u> (r,t) <u>un couple d'entiers vérifiant</u> : $0 < r \leq f$, $0 < t < \frac{pe}{p-1}$ <u>et</u> $t \not\equiv 0 \mod p$. <u>Il existe une extension abélienne de</u> k <u>à groupe de Galois</u> $(Z/pZ)^r$, <u>ayant</u> t <u>comme seul nombre de ramification</u>.

On ne restreint pas le problème en supposant $r = f$. On note $\mathfrak{p}$ l'idéal maximal de l'anneau des entiers de k et, pour tout entier i , $U^i = 1 + \mathfrak{p}^i$. On sait que les $(U^i)_{i \geq 0}$ forment une suite décroissante de sous-groupe de k^* , et on s'intéresse à la suite $(U^i k^{*p})_{i \geq 0}$. Le groupe $k^*/U^{t+1}k^{*p}$ est un p-groupe abélien élémentaire, on peut le considérer comme un espace vectoriel sur $\mathbb{F}_p$. En choisissant un supplémentaire du sous-espace $U^t k^{*p}/U^{t+1}k^{*p}$, on met en évidence un sous-groupe N de k^* qui vérifie :

$$N \cap U^t k^{*p} = U^{t+1}k^{*p} \quad \text{et} \quad N.U^t k^{*p} = k^* .$$

Utilisons les résultats de la théorie du corps de classe local [6]. Soit K l'extension abélienne de k dont N est le groupe des normes, G le groupe de Galois de K/k . On a :

$$G \simeq k^*/N = N.U^t k^{*p}/N \simeq U^t k^{*p}/U^{t+1}k^{*p} .$$

Le calcul des indices $(U^i k^{*p} : U^{i+1}k^{*p})$ provient de [3] § 15. En particulier, si $0 < i < \frac{pe}{p-1}$ et $i \not\equiv 0 \mod p$, l'indice est égal à p^f . On rappelle que l'application de réciprocité, de noyau N , qui envoie k^* sur G , envoie la suite $(U^i)_{i \geq 0}$ sur la suite $(G^i)_{i \geq 0}$ des groupes de ramification de G en notation supérieure. En utilisant les théorèmes d'homomorphisme ; on obtient :

$$G/G^{t} \simeq k^{*}/NU^{t} = \{1\}$$
$$G/G^{t+1} \simeq k^{*}/NU^{t+1} = k^{*}/N = G$$

K est donc une extension abélienne de k, à groupe de Galois $(\mathbb{Z}/p\mathbb{Z})^{f}$ ayant t comme seul nombre de ramification.

Exemple : Soit $k = \mathbb{Q}_2(\zeta)$, ζ racine cubique de l'unité . Soit $K = k(\sqrt{-1}, \sqrt{1-2\zeta})$. L'extension biquadratique K/k admet 1 comme seul saut de ramification.

2.2. Si l'extension K/k a deux nombres de ramification, $t < t'$. Ils vérifient :

(2) $t = -1$, $t' \leq 2e$ avec égalité si t' est pair,

ou

(3) t et t' impairs, $t+t' \leq 4e$ avec égalité si $t+t' \equiv 0 \mod 4$.

En effet, si l'extension est non totalement ramifiée, en notant K_3 le corps d'inertie, t' est le nombre de ramification des extensions $(K_i/k)_{i=1,2}$. Si l'extension est totalement ramifiée, notons K_3 le corps fixe par $G_{t'}$. Alors t est le nombre de ramification de K_3/k , $\frac{t+t'}{2}$ celui de $(K_i/k)_{i=1,2}$. La même démonstration qu'en 2.1. montre que t est impair.

Réciproquement, étant donné un corps 2-adique k , il existe des extensions biquadratiques de k avec deux nombres de ramification vérifiant (2) ou (3). Il suffit de composer deux extensions quadratiques ayant -1 et t' ou $\frac{t+t'}{2}$ et t comme nombres de ramification.

Exemples : -1 et 2 sont les nombres de ramification de $\mathbb{Q}_2(\sqrt{5},\sqrt{2})/\mathbb{Q}_2$, 1 et 3 ceux de $\mathbb{Q}_2(\sqrt{3},\sqrt{2})/\mathbb{Q}_2$.

2.3. On utilisera ultérieurement les deux résultats suivants :

LEMME 1. Soit K/k une extension galoisienne totalement ramifiée de corps p-adique. Soit $(G_i)_{i\geq -1}$ la suite des groupes de ramification, et v_K la valuation normalisée de K. Soit $x \in K$ et $\sigma \in G_t \backslash G_{t+1}$, alors :

$$v_K(\sigma-1)x = v_K(x) + t \quad \text{si} \quad v_K(x) \not\equiv 0 \bmod p$$

$$v_K(\sigma-1)x \geq v_K(x) + t + 1 \quad \text{sinon.}$$

LEMME 2. Soit K/k une extension de corps p-adique d'indice de ramification relatif e'. Soit $\mathfrak{P}$ (resp. $\mathfrak{p}$) l'idéal maximal de l'anneau des entiers de K (resp. k). Soit m la valuation de la différente $\mathfrak{D}_{K/k}$.

a) Pour tout entier $r \geq 0$, $\operatorname{Tr} \mathfrak{P}^r = \mathfrak{p}^{[\frac{m+r}{e'}]}$.

b) Si l'extension est totalement ramifiée, et si u est un saut de la suite des idéaux $(\operatorname{Tr} \mathfrak{P}^r)_{r\geq 0}$, alors les entiers de K de valuation u ont pour trace des entiers de valuation dans k celle de $\operatorname{Tr} \mathfrak{P}^u$.

En effet,

a) Posons $\operatorname{Tr} \mathfrak{P}^r = \mathfrak{p}^s$. s est le plus grand entier n tel que $\mathfrak{p}^n \supset \operatorname{Tr} \mathfrak{P}^r$. Or, $\operatorname{Tr} \mathfrak{P}^r \subset \mathfrak{p}^n \rightleftharpoons \mathfrak{P}^r \subset \mathfrak{p}^n \mathfrak{D}_{K/k}^{-1} \rightleftharpoons ne' - m \leq r \rightleftharpoons n \leq \frac{m+r}{e'}$.

b) Supposons que $\mathfrak{p}^s = \operatorname{Tr} \mathfrak{P}^u \supsetneq \operatorname{Tr} \mathfrak{P}^{u+1}$. Soit x de valuation s dans k. Il existe y de valuation u dans K tel que $\operatorname{Tr} y = x$. Soit z de valuation u dans K. Il existe a, unité de k, telle que $v_K(y+az) > u$. Alors, $v_k \operatorname{Tr}(y+az) = v_k(\operatorname{Tr} y + a \operatorname{Tr} z) > s$. Donc $v_k \operatorname{Tr} z = s$.

3. EXTENSION NON TOTALEMENT RAMIFIEE.

PROPOSITION 4. Si l'extension K/k est non totalement ramifiée, B est un $\mathfrak{O}$-module libre.

Démonstration : Les nombres de ramification sont -1 et t'. Soient ω une uniformisante de k, K_3 le corps d'inertie de l'extension, ξ une unité de K_3 telle que $T_1\xi = 1$.

Si $t' \equiv 1 \mod 2$, posons $t' = 2q' + 1$.

Comme $v_{K_1}\mathfrak{D}_{K_1/k} = t' + 1 = 2q' + 2$, toute uniformisante π_1 de K_1 est telle que $v_k T_3 \pi_1 = q' + 1$ (lemme 2). Soit π une uniformisante de K de la forme $\pi = \xi\pi_1$. Alors :

$$T_1\pi = \pi_1 \ , \quad T_3\pi = \xi u \omega^{q'+1} \quad (\ u \text{ unité de } k\ ), \quad T\pi = u\omega^{q'+1} \ .$$

Donc π engendre une base normale de K/k, et $\mathfrak{A}_\pi$ est le sous A-module de $k[G]$ engendré par :

$$1 \ , \quad T_1 \ , \quad \frac{T_3}{\omega^{q'+1}} \ , \quad \frac{T}{\omega^{q'+1}} \ .$$

Comme $t' < 2e$, $\dfrac{2}{\omega^{q'+1}} \in A$, et $\mathfrak{A}_\pi$ est un anneau. Donc $\mathfrak{A}_\pi = \mathfrak{O}$ et B est libre sur $\mathfrak{O}$ (proposition 1).

Si $t' \equiv 0 \mod 2$, soit $t' = 2e$.

Comme $v_{K_1}\mathfrak{D}_{K_1/k} = 2e + 1$, il existe une uniformisante π_1 de K_1 telle que $v_k T_3 \pi_1 = e + 1$. Soit π l'uniformisante de K définie par $\pi = \xi\pi_1$.

Comme ci-dessus, π engendre une base normale de K/k, et $\mathfrak{A}_\pi$ est le sous A-module de $k[G]$ engendré par :

$$1 \ , \quad T_1 \ , \quad \frac{T_3}{2\omega} \ , \quad \frac{T}{2\omega} \ .$$

$\mathfrak{A}_\pi$ n'est pas un anneau. On détermine facilement l'ordre $\mathfrak{O}$. C'est le sous A-module de $k[G]$ engendré par :

$$1 \ , \ T_1 \ , \ \frac{T_3}{2} \ , \ \frac{T}{2} \ .$$

On vérifie que $\mathfrak{A}_\pi$ est l'idéal principal de $\mathfrak{O}$ engendré par $1 + \frac{T_3}{2\omega}$. Donc B est libre sur $\mathfrak{O}$ (proposition 1).

4. EXTENSION TOTALEMENT RAMIFIEE.

On suppose l'extension K/k totalement ramifiée. On note t et t' les deux nombres de ramification (éventuellement égaux) de l'extension, q la partie entière de $\frac{t+1}{4}$, q' celle de $\frac{t'-1}{4}$. Lorsque $t < t'$, on définit K_3 comme le corps fixe par $G_{t'}$. On note toujours ω une uniformisante de k . L'énoncé des résultats dépend des congruences de t et t' modulo 4 .

PROPOSITION 5. <u>On suppose</u> $t \equiv t' \equiv 1 \bmod 4$ (resp. 3 mod 4). <u>Tout entier</u> θ <u>de</u> K <u>de valuation</u> 1 (resp. 3) <u>engendre une base normale de</u> K/k , <u>et il existe des entiers</u> a <u>et</u> b <u>de</u> k <u>tels que</u> :

(i) $\mathfrak{A}_\theta$ <u>soit le sous A-module de</u> $k[G]$ <u>engendré par</u> :

$$1 \ , \ \frac{T_1}{\omega^q} \ , \ \frac{T}{\omega^{2q+q'+1}} \ , \ S = \frac{T_2+aT_1}{\omega^\alpha} + b\frac{T}{\omega^{3q+q'}} \ .$$

(ii) $\mathfrak{O}$ <u>soit le sous A-module de</u> $k[G]$ <u>engendré par</u> :

$$1 \ , \ \frac{T_1}{\omega^q} \ , \ \frac{T}{\omega^{2q+q'+1}} \ , \ \omega^\beta S$$

<u>avec</u> $\alpha = q+q'$ (resp. $q+q'+1$)

$\beta = \mathrm{Max}\{0, 2q+q'-e\}$ (resp. $\mathrm{Max}\{0, 2q+q'+1-e\}$).

<u>Démonstration</u> : Désormais V désigne un système de représentants du corps résiduel de k , et σ_i un générateur du groupe de Galois de K/K_i . Traitons par exemple le cas où $t = 4q+1$ et $t' = 4q'+1$. Comme

$v_K \mathfrak{D}_{K/k} = 3(t+1) + t' - t = 8q + 4q' + 6$, toute uniformisante π de K est telle que $v_k T\pi = 2q + q' + 1$ (lemme 2). Pour $i = 1$ ou 2, $v_K T_i \pi = t+1$, car $v_K(\sigma_i - 1)\pi = t+1$ (lemme 1) et $v_K 2 = 4e > t+t'$. De même, $v_K(T_2+T_1)\pi = v_K T_3 \pi = t'+1$. Posons $t'-t = 4r$, il existe $a_r \in V^{\cdot}$ tel que $v_K(T_2+T_1+a_r\omega^r T_1)\pi \geq t'+2$. Appliquons $\sigma_1 - 1$,

$$v_K(\sigma_1-1)(T_2+T_1+a_r\omega^r T_1)\pi = 2v_{K_2}(\sigma_1-1)T_2\pi = 2(\frac{t+1}{2}+\frac{t+t'}{2}) .$$

On en déduit (lemme 1) que :

$$v_K(T_2+T_1+a_r\omega^r T_1)\pi \text{ est } \begin{cases} \text{ou paire, inférieure à } t+t' \\ \text{ou impaire, égale à } t+t'+1 \end{cases} .$$

Comme $v_K \frac{T\pi}{\omega^{2q}} = t'+3$, le même raisonnement montre qu'il existe une unité a et un entier b de k tels que $v_K(T_2+aT_1+b\frac{T}{\omega^{2q}})\pi = t+t'+1$. On obtient donc une base du A-module B formée des entiers π , $\frac{T_1\pi}{\omega^q}$, $\frac{T\pi}{\omega^{2q+q'+1}}$, $\frac{1}{\omega^{q+q'}}(T_2+aT_1+b\frac{T}{\omega^{2q}})\pi$. La première partie de la proposition en résulte. L'ordre $\mathfrak{O}$ contient les éléments 1 , $\frac{T_1}{\omega^q}$, $\frac{T}{\omega^{2q+q'+1}}$. Donc un élément de $\mathfrak{A}_\pi$ de la forme $\alpha + \beta\frac{T_1}{\omega^q} + \gamma\frac{T}{\omega^{2q+q'+1}} + \delta S$ ($\alpha, \beta, \gamma, \delta$ entiers de k) appartient à $\mathfrak{O}$ si et seulement si $\delta S^2\pi$ est entier. On montre que $v_K(T_2 + a^2 T_1)\pi = t'+1$, puisque $v_K S^2\pi = 4e + 5 - 2t - t'$. La deuxième partie s'en déduit.

PROPOSITION 6. <u>On suppose</u> $t \equiv 1 \bmod 4$ <u>et</u> $t' \equiv 3 \bmod 4$. <u>Sauf dans le cas où</u> $t' = t+2$ <u>et</u> $f = 1$, <u>il existe une uniformisante</u> π <u>de</u> K <u>telle que</u> :

$$v_K(\frac{T_3\pi}{\omega^{q'+1}} - 1) = 2 \quad \underline{\text{et}} \quad v_K\frac{T\pi}{\omega^{2q+q'+2}} = 0 .$$

<u>Une telle uniformisante engendre une base normale de</u> K/k , <u>et il existe des unités</u> a <u>et</u> b <u>de</u> k <u>telles que</u> :

(i) $\mathfrak{A}_\pi$ <u>soit le sous</u> A-<u>module de</u> $k[G]$ <u>engendré par</u> :

$$1 \ , \ \frac{T_1}{\omega^q} \ , \ \frac{T}{\omega^{2q+q'+2}} \ , \ S = \frac{T_3}{\omega^{q+q'+1}} + a\,\frac{T_1}{\omega^{2q}} + b\,\frac{T}{\omega^{3q+q'+2}} \ .$$

(ii) $\mathfrak{O}$ soit le sous A-module de $k[G]$ engendré par :

$$1 \ , \ \frac{T_1}{\omega^q} \ , \ \frac{T}{\omega^{2q+q'+2}} \ , \ \omega^q S \ .$$

Démonstration : Soit $t = 4q+1$, $t' = 4q'+3$, donc $e = q+q'+1$. Comme $v_K \mathfrak{D}_{K/K_3} = t'+1$, pour toute unité u de k et toute uniformisante π_3 de K_3 , il existe une uniformisante π de K telle que $T_3\pi = \omega^{q'+1}(1+u\pi_3)$. Alors $T\pi = \omega^{q'+1}(2+uT_1\pi_3)$, et $v_k T_1 \pi_3 = \frac{t+1}{2} = 2q+1$. A condition, si $q' = q$, de supposer le degré résiduel $f > 1$ et de bien choisir u , l'uniformisante π satisfait aux conditions de l'énoncé.

Il existe alors $b_o \in V^{\cdot}$ tel que $R\pi = (\frac{T_3}{\omega^{q'+1}} + b_o \frac{T}{\omega^{2q+q'+2}})\pi$ soit une uniformisante de K_3 . Comme $v_K \frac{T_1\pi}{\omega^q} = 2$, il existe $a_o \in V^{\cdot}$ tel que $v_K(R + a_o \frac{T_1}{\omega^q})\pi \geq 3$. Appliquons $\sigma_1 - 1$:

$$v_K(\sigma_1 - 1)(R + a_o \frac{T_1}{\omega^q})\pi = 2v_{K_3}(\sigma_1 - 1)R\pi = 2(t+1) \ .$$

On en déduit que :

$$v_K(R + a_o \frac{T_1}{\omega^q})\pi \quad \text{est} \quad \begin{cases} \text{ou paire, inférieure à } t+1 \\ \text{ou impaire, égale à } t+2 \end{cases} .$$

Les mêmes techniques montrent l'existence d'unités a et b de k telles que $v_K(\frac{T_3}{\omega^{q'+1}} + a\frac{T_1}{\omega^q} + b\frac{T}{\omega^{2q+q'+2}})\pi = t+2$. On obtient une base du A-module B formée des entiers π , $\frac{T_1\pi}{\omega^q}$, $\frac{T\pi}{\omega^{2q+q'+2}}$, $(\frac{T_3\pi}{\omega^{q+q'+1}} + a\frac{T_1\pi}{\omega^{2q}} + b\frac{T\pi}{\omega^{3q+q'+2}})$

La première partie de la proposition en résulte. L'ordre $\mathfrak{O}$ contient les éléments 1 , $\frac{T_1}{\omega^q}$, $\frac{T}{\omega^{2q+q'+2}}$, et la recherche de $\mathfrak{O}$ se ramène, comme précédemment, au calcul de la valuation de $S^2\pi$. On montre que $v_K S^2\pi = 1-t$. La deuxième partie s'en déduit.

Remarque : Si $t' = t+2$ et $f = 1$, il existe une uniformisante π de K telle que

$$v_K\left(\frac{T_3\pi}{\omega^{q+1}} - 1\right) = 2 \quad \text{et} \quad v_K \frac{T\pi}{\omega^{3q+3}} = 0 .$$

Les mêmes méthodes montrent que π engendre une base normale de K/k , et qu'il existe des unités a et b de k telles que $\mathfrak{A}_\pi$ (resp. $\mathfrak{O}$) soit le A-module engendré par 1 , $\frac{T_1}{\omega^q}$, $\frac{T}{\omega^{3q+3}}$, $S = \frac{T_3}{\omega^{2q+1}} + a\frac{T_1}{\omega^{2q}} + b\frac{T}{\omega^{4q+3}}$ (resp. 1 , $\frac{T_1}{\omega^q}$, $\frac{T}{\omega^{3q+2}}$, $\frac{T_3}{\omega^{q+1}}$) .

PROPOSITION 7. <u>On suppose</u> $t \equiv 3 \bmod 4$ <u>et</u> $t' \equiv 1 \bmod 4$. <u>Sauf dans le cas où</u> $t' = t+2$ <u>et</u> $f = 1$, <u>il existe une uniformisante</u> π <u>de</u> K <u>telle que</u> :

$$v_K\left(\frac{T_1\pi}{\omega^q} - 1\right) = v_K\left(\frac{T_2\pi}{\omega^q} - 1\right) = 2 .$$

<u>Une telle uniformisante engendre une base normale de</u> K/k , <u>et il existe des entiers</u> a <u>et</u> b <u>de</u> k <u>tels que</u> :

(i) $\mathfrak{A}_\pi$ <u>soit le sous</u> A-<u>module de</u> $k[G]$ <u>engendré par</u> :

$$1 , \frac{T_1}{\omega^q} , \frac{T}{\omega^{2q+q'}} , S = \frac{T_2+aT_1}{\omega^{q+q'}} + b\frac{T}{\omega^{2q+2q'}} .$$

(ii) $\mathfrak{O}$ <u>soit le sous</u> A-<u>module de</u> $k[G]$ <u>engendré par</u> :

$$1 , \frac{T_1}{\omega^q} , \frac{T}{\omega^{2q+q'}} , \omega^q S .$$

Démonstration : Soit $t = 4q-1$ et $t' = 4q'+1$, donc $e = q+q'$. Comme $v_K\mathfrak{D}_{K/K_1} = t+1 = 4q$, pour toute uniformisante π_1 de K_1 , il existe une uniformisante π de K telle que $\frac{T_1\pi}{\omega^q} = 1+\pi_1$. Soit π_2 une uniformisante de K_2 , écrivons le développement de Hensel de $\frac{T_2\pi}{\omega^q} = \beta_o + \beta_1\pi_2 + \dots$, $\beta_i \in V$, $\beta_o \neq 0$. Comme

$$v_K \frac{T_2+T_1}{\omega^q}\pi = v_K \frac{T_3\pi}{\omega^q} = t'-t ,$$

on en déduit que $\beta_o = 1$ et $\beta_1 \neq 0$ si $t'-t > 2$. Supposons que $t'-t = 2$ et que $\beta_1 = 0$ (cas défavorable). Soit π^* une uniformisante de K de la forme $\pi^* = \pi + u\pi^3$, u unité de k . On a :

$$\frac{T_1\pi^*}{\omega^q} = 1 + \pi_1 + u\frac{T_1\pi^3}{\omega^q} \quad , \text{ et } \quad \frac{T_2\pi^*}{\omega^q} = 1 + u\,\frac{T_2\pi^3}{\omega^q} + \dots .$$

Comme $v_K\,\frac{T_1\pi^3}{\omega^q} = v_K\,\frac{T_2\pi^3}{\omega^q} = 2$, on peut, en supposant le degré résiduel $f > 1$, choisir u afin que π^* convienne. Alors $v_k\,\frac{T\pi}{\omega^{2q+q'}} = 0$, et il existe $b_o \in V^{\cdot}$ tel que $R\pi = (\frac{T_1}{\omega^q} + b_o\,\frac{T}{\omega^{2q+q'}})\pi$ soit une uniformisante de K_1 . Posons $t'-t = 4r+2$, il existe $a_r \in V^{\cdot}$ tel que

$$v_K(\frac{T_1+T_2}{\omega^q} + a_r\omega^r R)\pi > t'-t \; .$$

En appliquant σ_1-1 , on montre que

$$v_K(\frac{T_1+T_2}{\omega^q} + a_r\omega^r R)\pi \;\text{ est }\begin{cases}\text{ou paire, inférieure à } t'+1\\ \text{ou impaire, égale à } t'+2\end{cases} .$$

Les mêmes méthodes montrent qu'il existe des entiers a et b de k tels que : $v_K(\frac{T_2}{\omega^q} + a\,\frac{T_1}{\omega^q} + b\,\frac{T}{\omega^{2q+q'}})\pi = t'+2$. On obtient une base du A-module B formée des entiers π , $(\frac{T_1}{\omega^q} + b_o\,\frac{T}{\omega^{2q+q'}})\pi$, $\frac{T\pi}{\omega^{2q+q'}}$, $(\frac{T_2+aT_1}{\omega^{q+q'}} + b\,\frac{T}{\omega^{2q+2q'}})\pi$. La première partie de la proposition en résulte.
L'ordre $\mathfrak{D}$ contient les éléments 1 , $\frac{T_1}{\omega^q}$, $\frac{T}{\omega^{2q+q'}}$, et la recherche de $\mathfrak{D}$ se ramène au calcul de la valuation de $S^2\pi$. On montre que $vS^2\pi = 1-t$.

Remarque : Si $t' = t+2$ et $f = 1$, il existe un entier θ de K de valuation 3 tel que :

$$v_K(\frac{T_3\theta}{\omega^{q+1}} - 1) = 2 \quad \text{et} \quad v_K\,\frac{T\theta}{\omega^{3q+2}} = 0 \; .$$

Les mêmes méthodes montrent que θ engendre une base normale de K/k et qu'il existe des unités a et b de k telles que $\mathfrak{A}_\theta$ (resp. $\mathfrak{O}$) soit le A-module engendré par 1, $\frac{T_1}{\omega^q}$, $\frac{T}{\omega^{3q+2}}$, $S = \frac{T_3}{\omega^{2q+1}} + a\frac{T_1}{\omega^{2q}} + b\frac{T}{\omega^{4q+2}}$ (resp. 1, $\frac{T_1}{\omega^q}$, $\frac{T}{\omega^{3q}}$, $\frac{T_3}{\omega^q}$).

THEOREME. <u>Si l'extension</u> K/k <u>est totalement ramifiée,</u> B <u>est</u> $\mathfrak{O}$-<u>module libre si et seulement si l'on a</u> :

$$\begin{cases} t = 1 & \underline{\text{si}} \quad t \not\equiv t' \bmod 4 \\ 2t+t' \leq 4e+3(-1)^{\frac{t-1}{2}} & \underline{\text{si}} \quad t \equiv t' \bmod 4 . \end{cases}$$

<u>Démonstration</u> : Dans le cas général, on a mis en évidence un entier θ engendrant une base normale de K/k tel que $\mathfrak{A}_\theta$ soit contenu dans l'ordre maximal $\mathfrak{O}_m$. D'après la proposition 1, B est un $\mathfrak{O}$-module libre si et seulement si $\mathfrak{A}_\theta = \mathfrak{O}$. On obtient donc comme critère : $q = 0$ si $t' \not\equiv t \bmod 4$, $\beta = 0$ si $t' \equiv t \bmod 4$.

Dans les cas particuliers où $t' = t+2$ et $f = 1$, on étudie l'application A-linéaire de $\mathfrak{O}$ dans $\mathfrak{A}_\theta$ définie comme la multiplication par un élément λ de $\mathfrak{A}_\theta$. Soit m_λ cette application, $\mathfrak{A}_\theta$ est un idéal principal de $\mathfrak{O}$ si et seulement s'il existe λ tel que le déterminant de m_λ soit une unité de A. Or ceci est impossible sauf si $k = \mathbb{Q}_2$ et $t = 1$. Traitons par exemple le cas où $t = 4q+1$ (cf. proposition 6, remarque). Choissons comme A-base de $\mathfrak{O}$ (resp. $\mathfrak{A}_\pi$) les éléments 1, $\frac{T_3}{\omega^{q+1}}$, $\frac{T_1}{\omega^q}$, $\frac{T}{\omega^{3q+2}}$ (resp. 1, S, $\frac{T_1}{\omega^q}$, $\frac{T}{\omega^{3q+3}}$). Soit $\lambda = \alpha + \beta S + \gamma\frac{T_1}{\omega^q} + \delta\frac{T}{\omega^{3q+3}}$.
La matrice de m_λ est triangulaire inférieure, l'élément de la 2e ligne et 2e colonne étant $(\alpha + \frac{2}{\omega^{2q+1}}\beta)\omega^q$.

<u>Remarques</u> :

1. L'anneau des entiers d'une extension quadratique d'un corps 2-adique est toujours libre sur l'ordre qui lui est associé [2]. Donc, la propriété, pour une extension galoisienne de corps locaux, que l'anneau des

entiers soit libre sur l'ordre qui leur est associé, ne se conserve pas par composition.

2. Les mêmes méthodes permettent d'étudier les idéaux de B comme module sur l'ordre qui lui est associé. On obtient des cas où aucun des idéaux n'est libre ; par exemple si l'extension K/k a un seul nombre de ramification $t \equiv 1 \bmod 4$ et si $3t > 4e+3$.

3. L'ordre $\mathfrak{O}$ ne dépend pas seulement des nombres de ramification de l'extension K/k. Par exemple, soit $k = \mathbb{Q}_2(\sqrt[4]{2}, j)$, j racine primitive cubique de 1. Soit $\omega = \sqrt[4]{2}$, $x = 1+\omega$, $y = 1+\omega^3$, $y' = 1+j\omega^3$. Les corps $K = k(\sqrt{x}, \sqrt{y})$ et $K' = k(\sqrt{x}, \sqrt{y'})$ sont deux extension biquadratiques distinctes de k admettant 5 et 9 comme nombres de ramification. On montre que l'ordre $\mathfrak{O}$ (resp. $\mathfrak{O}'$) est le sous A-module de $k[G]$ engendré par 1, $\frac{T_1}{\omega}$, $\frac{T}{\omega^5}$, $\frac{T_3+\omega T_1}{\omega^3}$ (resp. $\frac{T_3+j^2\omega T_1}{\omega^3}$). Détaillons un peu les calculs relatifs à l'extension K/k. Soit $\lambda = \sqrt{x}-1$, c'est une uniformisante de $K_1 = k(\sqrt{x})$, qui vérifie $\lambda^2 + 2\lambda - \omega = 0$. On écrit
$y = 1+\omega^3 = 1+\lambda^3(\lambda+2)^3 = (1+\lambda^3)^2 + 6\lambda^3(1+\lambda)^2 = (1+\lambda^3)^2.z$. Donc
$K = K_1(\sqrt{y}) = K_1(\sqrt{z})$ avec $z = 1+u_1\lambda^{11}$, u_1 unité de K_1. $\sqrt{z}-1$ est un élément de K de valuation 11, et on peut prendre comme uniformisante de K : $\pi = \frac{\lambda}{\omega}(\sqrt{y}-1-\lambda^3)$. On a alors : $T_1\pi \equiv \lambda\omega \bmod \pi^7$ et
$T_3\pi \equiv \lambda^3\omega \bmod \pi^{11}$. On en déduit que $v_K(T_3+\omega T_1)\pi > 10$, et on est assuré de l'existence d'un élément de valuation 15 de la forme $(T_3+\omega T_1 + \cdot\frac{T}{\omega^2} + \cdot\omega^2 T_1)\pi$.
On en déduit des générateurs de $\mathfrak{A}_\pi$ et donc de $\mathfrak{O}$.

-o-o-

BIBLIOGRAPHIE

[1] DEURING M. - Algebren, Springer Verlag, 1935.

[2] FERTON M.J. - Thèse de 3e cycle, Grenoble, 1972.

[3] HASSE H. - Zahlentheorie, Akademie Verlag, 1963.

[4] MARTINET J. - Bull. Soc. math. Fr., mémoire 25, 1971.

[5] NOETHER E. - J. reine angew, Math., 167, 1932.

[6] SERRE J.P. - Corps locaux, Hermann, 1962.

-o-o-