SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

BRUNO MARTEL

De l'anneau des entiers d'une extension de type (p, p) d'un corps p-adique

Séminaire de théorie des nombres de Grenoble, tome 8 (1979-1980), exp. n° 2, p. 1-26

<http://www.numdam.org/item?id=STNG_1979-1980__8__A2_0>

Séminaire de Théorie des Nombres
8 novembre 1979
Grenoble

DE L'ANNEAU DES ENTIERS D'UNE EXTENSION DE TYPE (p,p) D'UN CORPS p-ADIQUE

par

Bruno MARTEL

1. - INTRODUCTION

Soit A l'anneau des entiers d'un corps p-adique k, B celui d'une extension galoisienne finie K, et $G = Gal(K/k)$. B est un $A[G]$-module, il est libre si et seulement si K/k est modérément ramifiée [8]. Lorsque K/k est sauvagement ramifiée, on introduit l'ordre de A dans $k[G]$ associé à B par : $\mathfrak{O} = \{\lambda \in k[G] ; \lambda B \subset B\}$. Un problème ouvert est : B est-il un $\mathfrak{O}$-module libre ? ($\mathfrak{O}$ est le seul ordre de $k[G]$ sur lequel B puisse être libre). La réponse est connue lorsque K/k est : cyclique de degré p [2], diédrale de degré $2p$ [4], cyclique et k absolument non ramifié [1]. Dans tous ces cas, la réponse ne dépend que des nombres de ramification de K/k.

On va donner quelques résultats, partiels, lorsque K/k est bicyclique de degré p^2, p impair, et montrer que la réponse au problème posé ne dépend plus que des seuls nombres de ramification de K/k.

Madame Bertrandias a une large part dans les résultats obtenus.

2. - NOMBRES DE RAMIFICATION

Soit v_K la valuation normalisée de K, la suite $(G_i)_{i\geq -1}$ des groupes de ramification de G est définie par : $G_i = \{\sigma \in G ; \forall x \in B$,

$v_K(\sigma-1)x \geq i+1\}$. Un entier t est dit nombre de ramification de K/k si $G_t \neq G_{t+1}$. On utilisera plusieurs fois le résultat suivant :

LEMME 0. - Si $t > 0$ et ssi $\sigma \in G_t \backslash G_{t+1}$, alors, pour tout $x \in B$
$v_K(\sigma-1)x = v_K(x) + t$ si $v_K x \not\equiv 0 \mod p$
$v_K(\sigma-1)x > v_K x + t$ sinon.

On suppose désormais K/k bicyclique de degré p^2 , p impair. On note e l'indice de ramification absolu de k , F son degré résiduel.

2.1. Si K/k a un seul nombre de ramification t , alors $F > 1$ et t vérifie : $t \not\equiv 0 \mod p$ et $0 < t < \frac{pe}{p-1}$.

Il est clair que $t > 0$. On sait ([9] ch.4) que $G = G_t/G_{t+1}$ se plonge dans le groupe additif du corps résiduel de K , donc de k . On en déduit : $F > 1$. D'autre part, t est le nombre de ramification des extensions cycliques intermédiaires de k . On en déduit que : $t \leq \frac{pe}{p-1}$, avec égalité si $t \equiv 0 \mod p$ (ce qui exige que k contienne les racines p-èmes de 1) [6]. Montrons que $t \not\equiv 0 \mod p$. Soit $\sigma \in G$, σ distinct du neutre, K_1 le corps fixe par σ . Soit π une uniformisante de K . Posons $f = \sigma - 1$ et supposons que $t \equiv 0 \mod p$. Alors, pour tout entier $i > 0$, $v_K f^i \pi = it + 1$ (lemme 0). En particulier, $v_K f^{p-1} \pi = (p-1)t+1$. Or, dans $\mathbb{Z}[X]$, $(X-1)^{p-1} \equiv \sum_{j=0}^{p-1} X^j \mod p$. Il existe donc $h \in \mathbb{Z}[\sigma]$ tel que $\mathrm{Tr}_{K/K_1} \pi = f^{p-1}\pi + ph\pi$. Or $v_K \mathrm{Tr}_{K/K_1} \pi \equiv 0 \mod p$, et $v_K(f^{p-1}\pi + ph\pi) = (p-1)t+1$ puisque $v_K p = p^2 e \geq p(p-1)t$. On obtient une contradiction.

Réciproquement, étant donné un corps p-adique k de degré résiduel $F > 1$, il existe des extensions de k de type (p,p) avec un seul nombre de ramification t vérifiant : $t \not\equiv 0 \mod p$ et $t < \frac{pe}{p-1}$. On peut le montrer en utilisant la théorie du corps de classe local, on

verra ultérieurement des constructions explicites à l'aide de polynômes d'Artin-Schreier (cf.5).

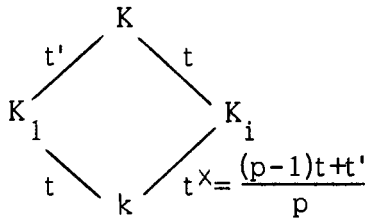
2.2. Si K/k a deux nombres de ramification $t < t'$, ils vérifient :

$t = -1$, $0 < t' \leq \frac{pe}{p-1}$ avec égalité ssi $t' \equiv 0 \mod p$

ou

$t \equiv t' \not\equiv 0 \mod p$, $t^{\chi} = \frac{(p-1)t+t'}{p} \leq \frac{pe}{p-1}$ avec égalité ssi $t^{\chi} \equiv 0 \mod p$.

Si l'extension est non totalement ramifiée $(t = -1)$, t' est le nombre de ramification des extensions cycliques intermédiaires de k , distinctes du corps d'inertie. Sinon, soit K_1 le corps fixe par $G_{t'}$, les nombres de ramification sont donnés par le schéma suivant ([9] ch.4) :



, $i = 2,\ldots,p+1$

On en déduit l'inégalité $t^{\chi} \leq \frac{pe}{p-1}$, avec égalité ssi $t^{\chi} \equiv 0 \mod p$. On sait que $t \equiv t' \mod p$, et $t \not\equiv 0 \mod p$, sinon $t = \frac{pe}{p-1} < t^{\chi}$.

Réciproquement, il existe des extensions bicycliques de degré p^2 de k avec deux nombres de ramification $t < t'$ vérifiant les conditions précédentes. Il suffit de composer deux extensions cycliques de degré p ayant -1 et t' ou t et t^{χ} comme nombres de ramification.

3. - ORDRE MAXIMAL DE A DANS k[G]

Soient σ et τ deux générateurs de G . On pose $f = \sigma - 1$ et $g = \tau - 1$. Soit ω une uniformisante de k . Pour tout couple d'entiers (i,j) du segment $[0,n-1]$, on définit l'entier $n_{i,j} = [\frac{(i+j)e}{p-1}]$.

PROPOSITION 1. - L'ordre maximal $\mathfrak{S}_m$ de A dans k[G] est le réseau de base $(\frac{f^i g^j}{\omega^{n_{ij}}})_{i,j}$.

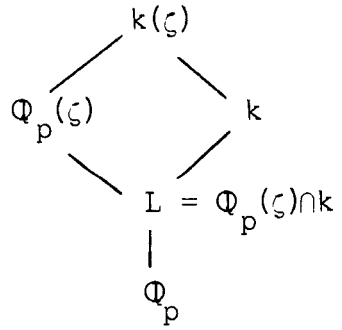
On définit le discriminant d'un réseau de k[G] comme celui vis à vis de la forme bilinéaire symétrique non dégénérée : $(\lambda,\mu) \longrightarrow Tr(\lambda\mu)$

LEMME 1. - Le discriminant de A[G] est engendré par p^{2p^2} .

Pour tout $\rho \in G$, $Tr(\rho)$ est égale à l'ordre de G si ρ est le neutre de G , et à zéro sinon. Prenons comme base de A[G] la famille $(\sigma^i\tau^j)_{i,j}$ ordonnée lexicographiquement. Le discriminant de A[G] est engendré par celui de la matrice carrée d'ordre p^2 suivante :

$$\begin{pmatrix} A & 0 & \dots & 0 \\ 0 & 0 & \dots & A \\ & & & \\ 0 & A & \dots & 0 \end{pmatrix}$$, où A est la matrice d'ordre p : $$\begin{pmatrix} p^2 & 0 & \dots & 0 \\ 0 & 0 & \dots & p^2 \\ & & & \\ 0 & p^2 & \dots & 0 \end{pmatrix}$$.

Soit ζ une racine primitive p-ème de 1 dans une clôture algébrique de k . On a le schéma suivant :



On note r le degré de L/Φ_p ,
q l'indice de ramification de $k(\zeta)/k$,
d son degré résiduel.
Donc : $p-1 = rdq$.

LEMME 2. - $d = (\frac{p-1}{r}, \frac{e}{r})$.

Soit $d_o = (\frac{p-1}{r}, \frac{e}{r})$, posons $\frac{p-1}{r} = d_o q_o$ et $\frac{e}{r} = d_o q'$. L'indice de ramification de $\Phi_p(\zeta)/L$ divise celui de $k(\zeta)/L$, on en déduit que q_o divise q . Soit Λ l'extension de degré d_o de L contenue dans $\Phi_p(\zeta)$, ν une uniformisante de Λ , ρ un générateur de $Gal(\Lambda k/k)$. Puisque Λ/L est modérément ramifiée, $v_\Lambda(\rho-1)\nu = 1$. Soit ε l'unité de Λk définie par $\varepsilon = \frac{\nu}{\omega^{q'}}$, alors $v_{\Lambda k}(\rho-1)\varepsilon = 0$. On en déduit que

k_o/k est non ramifiée et donc d_o divise d .

Corollaire. - Les indices de ramification q et q' de $k(\zeta)/k$ et $k(\zeta)/\mathbb{Q}_p(\zeta)$ sont premiers entre eux.

LEMME 3. - Le discriminant du réseau $\mathfrak{O}'$ de base $(\frac{f^i g^j}{\omega^{n_{ij}}})_{i,j}$ est engendré par $\omega^{(p+1)rd(q-1)}$.

D'après le lemme 1, le discriminant de $\mathfrak{O}'$ est engendré par $p^{2p^2} \cdot \omega^{-2\sum_{i,j} n_{i,j}}$. Or :

$$\sum_{\substack{i\le p-1\\ j\le p-1}} n_{i,j} = \sum_{k=1}^{p-1} (k+1)[\frac{ke}{p-1}] + \sum_{k=1}^{p-1} (p-k)[\frac{(p-1+k)e}{p-1}]$$

$$= (p+1) \sum_{k=1}^{p-1} [\frac{ke}{p-1}] + e \sum_{k\le p-1} k = p^2 e - (p+1) \sum_{k=1}^{p-1} \langle \frac{ke}{p-1} \rangle$$

où $\langle x \rangle$ désigne la partie fractionnaire de x . Or :

$$\sum_{k=1}^{p-1} \langle \frac{ke}{p-1} \rangle = \sum_{k=1}^{p-1} \langle \frac{kq'}{q} \rangle = rd \sum_{k=1}^{q-1} \langle \frac{kq'}{q} \rangle = rd \frac{q-1}{2}$$

car q et q' sont premiers entre eux. Donc $\sum_{i,j} n_{i,j} = p^2 e - \frac{p+1}{2} rd(q-1)$ et le discriminant de $\mathfrak{O}'$ est engendré par $p^{2p^2} \omega^{-2p^2 e} \omega^{(p+1)rd(q-1)}$ i.e. $\omega^{(p+1)rd(q-1)}$.

LEMME 4. - Les réseaux $\mathfrak{O}_m$ et $\mathfrak{O}'$ ont le même discriminant.

La décomposition de l'algèbre $k[G]$ en composantes simples est de la forme : $k[G] \simeq k \times (k(\zeta))^{r(p+1)}$, puisque $[k(\zeta):k] = \frac{p-1}{r}$. Donc $\mathfrak{O}_m \simeq A \times (A_1)^{r(p+1)}$, où A_1 est l'anneau des entiers de $k(\zeta)$. Or le discriminant de A_1 est engendré par $\omega^{d(q-1)}$, puisque $k(\zeta)/k$ est modérément ramifiée, d'indice de ramification q et de degré résiduel d . Les réseaux $\mathfrak{O}_m$ et $\mathfrak{O}'$ ayant même discriminant, il suffit, pour démontrer la proposition, de montrer que $\mathfrak{O}'$ est inclus dans $\mathfrak{O}_m$, c'est-à-dire que l'image de $\frac{f^i g^j}{\omega^{n_{i,j}}}$ dans $k(\zeta)$ est un entier. Or $\zeta - 1$

est une uniformisante de $\mathbb{Q}_p(\zeta)$, et l'indice de ramification de $k(\zeta)/\mathbb{Q}_p(\zeta)$ est égal à $\frac{qe}{p-1}$. Donc

$$v_{k(\zeta)} \frac{(\zeta-1)^{i+j}}{\omega^{n_{i,j}}} = (i+j)\frac{qe}{p-1} - q\left[\frac{(i+j)e}{p-1}\right] \geq 0 .$$

4. - CONDITION NECESSAIRE POUR QUE B SOIT UN $\mathfrak{O}$-MODULE LIBRE

4.1. Soit M une extension abélienne de k de groupe de Galois G fini. Soit θ un entier de M engendrant une base normale de M/k . On définit $\mathfrak{A}_\theta = \{\lambda \in k[G] \ ; \ \lambda\theta \in B\}$.

PROPOSITION 2. - [2] , $\mathfrak{A}_\theta$ est un idéal de l'ordre $\mathfrak{O}$, isomorphe à B comme $\mathfrak{O}$-module. B est libre sur $\mathfrak{O}$ ssi il existe θ tel que $\mathfrak{A}_\theta$ soit un anneau (et alors $\mathfrak{A}_\theta = \mathfrak{O}$) . Les inclusions $\mathfrak{A}_\theta \subset \mathfrak{A}_{\theta'} \subset \mathfrak{O}_m$ entraînent $\mathfrak{A}_\theta = \mathfrak{A}_{\theta'}$.

Si l'on remplace l'anneau B par l'un de ses idéaux $\mathfrak{a}$, on a une proposition analogue pour l'ordre $\mathfrak{O}(\mathfrak{a})$ associé à $\mathfrak{a}$ et l'idéal de $\mathfrak{O}(\mathfrak{a})$ associé à un élément de $\mathfrak{a}$ qui engendre une base normale de M/k . Soit H un sous-groupe de G , L le corps fixe par H , $\bar{G} = G/H$ le groupe de Galois de L/k . L'homomorphisme canonique de G sur $\bar{G}$ se prolonge en un k-homomorphisme d'algèbre : $\lambda \longrightarrow \bar{\lambda}$ de $k[G]$ sur $k[\bar{G}]$. L'action de $k[\bar{G}]$ sur L est définie par $\bar{\lambda}x = \lambda x$. On note T la trace de M à L , B l'anneau des entiers de M .

LEMME 5. - Soit θ un entier de M qui engendre une base normale de M/k . Alors $T\theta$ engendre une base normale de L/k . Soit $\mathfrak{A}_{T\theta}(TB) = \{\Lambda \in k[\bar{G}] \ ; \ \Lambda T\theta \in TB\}$ alors $\mathfrak{A}_{T\theta}(TB) = \overline{\mathfrak{A}_\theta(B)}$.

Soit $(g_i)_{1\leq i\leq r}$ un système exact de représentants des classes de G mod H . Les éléments $(\bar{g}_i T\theta)_{i\leq r}$ sont k-linéairement indépendants, puisque, pour tout $(x_i) \in k^r$, on a : $\sum_{i\leq r} x_i \bar{g}_i T\theta = \sum_{i\leq r} x_i g_i T\theta = \sum_{\substack{i\leq r \\ h\in H}} x_i g_i h\theta$.

L'inclusion $\overline{\mathfrak{A}_\theta(B)} \subset \mathfrak{A}_{T\theta}(TB)$ est claire. Soit $\Lambda \in \mathfrak{A}_{T\theta}(TB)$. Il existe $b \in B$ tel que $\Lambda T\theta = Tb$, et il existe $\lambda \in \mathfrak{A}_\theta(B)$ tel que $b = \lambda\theta$. On obtient $\Lambda T\theta = \lambda T\theta = \bar{\lambda} T\theta$, et donc $\Lambda = \bar{\lambda}$ puisque $T\theta$ engendre une base normale de L/k .

COROLLAIRE. - Si B est libre sur son ordre associé dans $k[G]$, l'idéal TB est libre sur son ordre associé dans $k[\bar{G}]$.

En effet, si B est libre sur son ordre, il existe θ tel que $\mathfrak{A}_\theta(B)$ soit un anneau. Donc $\mathfrak{A}_{T\theta}(TB)$ est un anneau et l'idéal TB est libre sur son ordre (prop. 2).

4.2. On va appliquer ce corollaire à une extension K/k bicyclique de degré p^2 . On obtient ainsi une condition nécessaire pour que B soit libre sur son ordre : en effet, si L est une extension intermédiaire (cyclique de degré p) d'anneau d'entiers C , on sait caractériser les idéaux de C qui sont libres sur leur ordre [4] .

Si K/k est non totalement ramifiée, on choisit L distinct du corps d'inertie. Alors $TB = C$ et t' est le nombre de ramification de L/k . On obtient :

PROPOSITION 3. - Si K/k est non totalement ramifiée, pour que B soit un $\mathfrak{O}$-module libre, il est nécessaire que $t' = \frac{pe}{p-1}$ ou, si $t' < \frac{pe}{p-1} - 1$, que le reste de la division de t' par p divise $p-1$.

Si K/k est totalement ramifiée, soit $\mathfrak{p}$ l'idéal maximal de L , $\mathfrak{d}$ la différente de K/L . Le nombre de ramification de K/L est t (ou t'). Donc $v_K\mathfrak{d} = (p-1)(t+1)$ et $TB = \mathfrak{p}^{t-[t/p]}$. Le nombre de ramification de L/k est t^χ (ou t). Que l'idéal TB soit libre sur son ordre ou non dépend des congruences mod p des entiers $t-[\frac{t}{p}]$ et t^χ (ou $t'-[\frac{t'}{p}]$ et t). Si les nombres de ramification t et t' sont non congrus mod p^2 , on obtient des conditions différentes selon que l'on

choisit pour L le corps fixe par $G_{t'}$ ou non. Sinon, on obtient la même condition.

On suppose désormais que les nombres de ramification sont congrus mod p^2 .

On note a le reste de la division de t par p^2 , $a = \alpha + \beta p$ son écriture en base p , $\frac{\alpha}{p} = [\alpha_1, \ldots, \alpha_n]$ le développement en fraction continue de $\frac{\alpha}{p}$ (avec $\alpha_n > 1$). On obtient :

PROPOSITION 3'. - Si K/k est totalement ramifiée et ses nombres de ramification congrus mod p^2 , pour que B soit un $\mathfrak{O}$-module libre, sous l'hypothèse que $t < \frac{pe}{p-1} - 2$, il est nécessaire que :

$\beta \leq \frac{p-1}{2}$ si $\alpha = 1$

$\beta = 0$ ou α_n si $\alpha > 1$ et n pair

$\beta \leq \frac{1}{2}\alpha_n$ si $\alpha > 1$ et n impair.

Exemples numériques.

$p = 3$, $t \equiv t' \bmod 9$ et $t < \frac{3e}{2} - 2$. B n'est pas libre sur son ordre si, mod 9, $t \in \{5,7\}$.

$p = 5$, $t \equiv t' \bmod 25$ et $t < \frac{5e}{4} - 2$. B n'est pas libre sur son ordre si, mod 25, $t \in \{7,9,13,14,16,17,18,19,21,22,23\}$.

4.3. Il résulte de la proposition 2 que si un entier θ engendre une base normale, et si $\mathfrak{A}_\theta$ est inclus dans $\mathfrak{O}_m$, il est nécessaire que $\mathfrak{A}_\theta = \mathfrak{O}$ pour que B soit libre sur $\mathfrak{O}$. C'est cette condition que l'on va désormais exploiter.

PROPOSITION 4. - Soit θ un entier de K de valuation a . Alors θ engendre une base normale de K/k et, si $t^\times \leq \frac{pe}{p-1} - \beta$, $\mathfrak{A}_\theta \subset \mathfrak{O}_m$.

LEMME 6. - Soit M une extension abélienne non cyclique de k. Un élément θ de M engendre une base normale de M/k ssi, pour toute extension intermédiaire stricte L, l'élément $\mathrm{Tr}_{M/L}\theta$ engendre une base normale de L/k.

La condition est nécessaire (lemme 5). Montrons qu'elle est suffisante. Si l'annulateur de θ dans $k[G]$ n'était pas réduit à 0, il contiendrait un idéal minimal. Il suffit donc de montrer que, pour tout caractère irréductible χ de $G = \mathrm{Gal}(M/k)$ sur k, $e_\chi\theta \neq 0$, où e_χ est l'idempotent primitif de $k[G]$ associé à χ. Soit ρ une représentation de G sur k, de module V. On sait que l'image par ρ de $k[G]$ dans $\mathrm{End}_k V$ coïncide avec le bicommutant du module V, puisque $k[G]$ est semi-simple [3]. Supposons de plus ρ irréductible (de caractère χ), le bicommutant de V est un corps puisque G est abélien, et donc $\rho(G)$ est un groupe cyclique. Soit H le noyau de ρ, L le corps fixe par H. L est une extension intermédiaire stricte, car H n'est pas réduit au neutre, G étant non cyclique. Soit $(g_i)_{1\leq i\leq r}$ un système exact de représentants des classes de G mod H. On a : $e_\chi\theta = \frac{1}{|G|}\sum_{g\in G}\chi(g^{-1})g\theta = \frac{1}{|G|}\sum_{\substack{i\leq r\\ h\in H}}\chi(g_i^{-1})g_i h\theta$. Donc $e_\chi\theta = \frac{1}{|G|}\sum_{i\leq r}\chi(g_i^{-1})g_i\,\mathrm{Tr}_{M/L}\theta \neq 0$ puisque $\mathrm{Tr}_{M/L}\theta$ engendre une base normale de L/k.

Application. Un entier θ de K de valuation a engendre une base normale de K/k.

On note $(K_h)_{1\leq h\leq p+1}$ les extensions intermédiaires de degré p sur k, K_1 étant le corps fixe par $G_{t'}$, T_h la trace de K/K_h. Soit σ un générateur de $G_{t'}$ et $f = \sigma - 1$. Pour tout entier i, tel que $0 \leq i \leq p-1$, on a (lemme 0) : $v_K f^i\theta = it' + a \equiv (i+1)a \bmod p^2$. En particulier, $v_K f^{p-1}\theta = (p-1)t' + a$. Il existe $h \in \mathbb{Z}[\sigma]$ tel que $T_1\theta = f^{p-1}\theta + ph\theta$. Comme $v_K p = p^2 e > (p-1)t'$, on obtient : $v_{K_1} T_1\theta = \frac{(p-1)t'+a}{p} \equiv a \bmod p$. Le nombre de ramification t de K_1/k

étant congru à a mod p , on sait que $T_1\theta$ engendre une base normale de K_1/k . On montre de même, pour $h > 1$, que $T_h\theta$ engendre une base normale de K_h/k (dont le nombre de ramification t^χ est congru à a mod.p).

LEMME 7. - Soit λ un élément de $k[G]$, λ appartient à $\mathfrak{D}_m$ ssi, pour tout $h \leq p+1$, $\lambda \frac{T_h}{p} \in \mathfrak{D}_m$.

La condition est nécessaire puisque $\frac{T_h}{p}$ appartient à $\mathfrak{D}_m$. La condition suffisante résulte de l'égalité : $p = \sum_{h\leq p+1} T_h - T$.

Application. Si $t^\chi \leq \frac{pe}{p-1} - \beta$, $\mathfrak{A}_\theta \subset \mathfrak{D}_m$.

Soit τ un générateur de $\mathrm{Gal}(K/K_2)$ et $g = \tau - 1$. Pour tout entier j , tel que $0 \leq j \leq p-1$, on a : $v_K g^j\theta = jt + a$. En particulier, $v_K g^{p-1}\theta = (p-1)t + a$. On obtient, comme ci-dessus,

$$v_{K_2} T_2\theta = \frac{(p-1)t + a}{p} \equiv a \bmod p.$$

On en déduit que, pour tout entier $i \leq p-1$, $v_{K_2} f^i T_2\theta = it^\chi + \frac{(p-1)t + a}{p}$.

Soit $\lambda = \sum_{i,j=0}^{p-1} a_{i,j} f^i g^j$, $a_{ij} \in k$, un élément de $\mathfrak{A}_\theta$. On a : $\frac{\lambda T_2}{p} = \frac{1}{p} \sum_{i=0}^{p-1} a_{i,o} f^i T_2$. On a montré que $\mathfrak{D}_m$ est le réseau de base $\frac{f^i g^j}{\omega^{n_{i,j}}}$, où $n_{i,j} = [\frac{(i+j)e}{p-1}]$. On peut remplacer les p éléments $\frac{f^i g^{p-1}}{\omega^{n_{i,p-1}}}$ par les éléments $\frac{f^i T_2}{p\omega^{n_{i,o}}}$. On obtient ainsi la condition : $\frac{\lambda T_2}{p} \in \mathfrak{D}_m$ ssi, pour tout $i \leq p-1$, $v_k a_{i,o} + [\frac{ie}{p-1}] \geq 0$. Montrons que cette condition est satisfaite si $t^\chi \leq \frac{pe}{p-1} - \beta$. Puisque $\lambda \in \mathfrak{A}_\theta$, $\lambda T_2\theta \in T_2 B = \wp_2^{t-[\frac{t}{p}]}$. Or $\lambda T_2\theta = \sum_{i=0}^{p-1} a_{i,o} f^i T_2\theta$ et $v_{K_2} f^i T_2\theta = it^\chi + \frac{(p-1)t + a}{p} \equiv (i+1)a \bmod p$. On obtient : pour tout $i \leq p-1$, $pv_k a_{i,o} + it^\chi + \frac{(p-1)t + a}{p} \geq t - [\frac{t}{p}]$ i.e. $v_k a_{i,o} \geq -\frac{it^\chi + \beta}{p}$. La condition est satisfaite pour $i = 0$ ($a_{o,o}$ entier), elle l'est pour $i > 0$ si $\frac{t^\chi + \beta}{p} \leq \frac{e}{p-1}$. On montre de même que, si

$t \leq \frac{pe}{p-1} - \beta$, $\frac{\lambda T_1}{p} \in \mathfrak{O}_m$ si $\lambda \in \mathfrak{A}_\theta$.

Remarque : pour $p = 3$, on peut construire une base de $\mathfrak{A}_\theta$ assez explicite pour vérifier l'inclusion $\mathfrak{A}_\theta \subset \mathfrak{O}_m$ (au moins pour $a = 1$) sans condition sur les nombres de ramification. Cette inclusion est-elle vraie pour tout p , sans condition ?

5. - EXTENSION D'ARTIN-SCHREIER

Soit t un entier positif premier à p , Δ un élément de k de valuation $-t$. Le polynôme $X^p-X-\Delta$, dit d'Artin-Schreier, est irréductible sur k . Si x est une de ses racines (dans une extension de k), l'extension $K = k(x)/k$ est ramifiée, et $v_K x = -t$. Si de plus t vérifie : $t < \frac{pe}{p-1}$, alors K/k est cyclique, de nombre de ramification t .

Réciproquement, toute extension de k , cyclique de degré p , ramifiée, dont le nombre de ramification t vérifie : $t < \frac{pe}{p-1}$, est obtenue par adjonction d'une racine d'un polynôme d'Artin-Schreier [6] . Donc K/k étant une extension de type (p,p) , totalement ramifiée, à nombres de ramification t et t' congrus mod p^2 , on peut supposer que (notations du paragraphe précédent) :

$K_1 = k(\ell)$, ℓ racine de $X^p-X-\delta\omega^{-t}$

$K_2 = k(m)$, m racine de $X^p-X-\varepsilon\omega^{-t^\chi}$, δ, ε unités de k .

On va construire un élément de K de valuation a . Soit n l'entier défini par $t'-t = np^2$. Puisque $v_K\omega^n m = v_K \ell = -pt$, il existe une unité μ de k telle que $v_K(\omega^n m + \mu\ell) > -pt$. Appliquant $f = \sigma-1$ à cet élément (K_1 fixe par σ), on obtient un élément de valuation $t'-t$. Donc la valuation de $\omega^n m + \mu\ell$ ou bien est égale à $-t$, ou bien est inférieure mais multiple de p (lemme 0) . Comme $v_K \ell^i = -pit$ décrit l'ensemble des multiples de p mod p^2 , le raisonnement précédent prouve l'existence d'une unité γ de k et d'éléments z et $(y_i)_{2 \leq i \leq p-1}$

de k tels que : $x = \omega^n m + \gamma\ell + z + \sum_{i=2}^{p-1} y_i \ell^i$ soit de valuation $-t$. Alors $v_K(\ell x)^{p-1} = -(p^2-1)t \equiv t \bmod p^2$, et $\theta = \omega^{\frac{(p^2-1)t+a}{p^2}} (\ell x)^{p-1}$ est de valuation a .

PROPOSITION 5. - Si les nombres de ramification sont égaux, l'unité γ définie ci-dessus vérifie les conditions : $\gamma^p + \frac{\varepsilon}{\delta} \equiv 0 \bmod \omega$ et $\gamma^{p-1} \not\equiv 1 \bmod \omega$.

Soit y' l'élément de K_1 défini par : $x = m + \gamma\ell + y'$ $(n=0)$. Puisque x est de degré p sur K_1 , son polynôme minimal est : $(X-\gamma\ell-y')^p - (X-\gamma\ell-y') - \varepsilon\omega^{-t}$. En prenant sa norme, on obtient : $v_{K_1}((\gamma\ell+y')^p-(\gamma\ell+y')+\varepsilon\omega^{-t}) = -t$. Si $y' = 0$,

$$v_{K_1}((\gamma\ell)^p-\gamma\ell+\varepsilon\omega^{-t}) = v_{K_1}(\gamma(\gamma^{p-1}-1)\ell+(\gamma^p\delta+\varepsilon)\omega^{-t}) = -t .$$

On en déduit que : $v_k(\gamma^p+\frac{\varepsilon}{\delta}) > \frac{(p-1)t}{p}$ et $\gamma^{p-1} \not\equiv 1 \bmod \omega$. Si $y' \neq 0$, $(\gamma\ell+y')^p - (\gamma\ell+y') + \varepsilon\omega^{-t} = \gamma^p\ell^p + \sum_{i=1}^{p-1} \binom{p}{i} (\gamma\ell)^{p-i} y'^i + y'^p - \gamma\ell - y' + \varepsilon\omega^{-t}$. Par construction, $v_{K_1} y' > -t$, donc $v_{K_1} \binom{p}{i} (\gamma\ell)^{p-i} y'^i > pe - pt > -t$. Donc $v_{K_1}(\gamma(\gamma^{p-1}-1)\ell+(\gamma^p\delta+\varepsilon)\omega^{-t}+y'^p) = -t$. Par construction, $v_K y' < v_K x$, donc $v_{K_1} y'^p < -t$. On en déduit que : $v_{K_1} y'^p = v_{K_1}(\gamma^p\delta+\varepsilon)\omega^{-t}$ i.e. $v_k(\gamma^p+\frac{\varepsilon}{\delta}) = t + v_{K_1} y'$. En particulier : $v_k(\gamma^p+\frac{\varepsilon}{\delta}) > 0$.

Posons $y'^p = \sum_{i=0}^{p-1} a_i \ell^i$, $a_i \in k$, alors :

$$v_{K_1}(\gamma(\gamma^{p-1}-1)\ell + (\gamma^p\delta+\varepsilon)\omega^{-t} + a_o + a_1\ell + \ldots + a_{p-1}\ell^{p-1}) = -t .$$

Il suffit de montrer que $v_k(a_1) > 0$ pour prouver que $\gamma^{p-1} \not\equiv 1 \bmod \mathfrak{x}$. Or $y'^p = z^p + \sum_{i=2}^{p-1} (y_i\ell^i)^p + p. \sum_{\substack{n_o+\ldots+n_{p-1}=p \\ n_j \neq 0}} \text{entier}. z^{n_o} \ldots (y_{p-1}\ell^{p-1})^{n_{p-1}}$.

Comme $v_{K_1} pz^{n_o} \ldots (y_{p-1}\ell^{p-1})^{n_{p-1}} > pe-pt > -t$, il suffit de regarder la participation de $(y_i\ell^i)^p$ à ℓ . Or $(y_i\ell^i)^p = y_i^p(\ell+\delta\omega^{-t})^i$ a pour composante sur ℓ l'élément $iy_i^p(\delta\omega^{-t})^{i-1}$ dont la valuation est strictement

positive, puisque $v_{K_1} y_i \ell^i > -t$.

Cette proposition admet une réciproque partielle, que l'on peut énoncer ainsi :

PROPOSITION 5'. - Soit t un entier positif, premier à p, vérifiant $t < \frac{pe}{p-1}$. Soient $K_1 = k(\ell)$, ℓ racine de $X^p - X - \delta\omega^{-t}$, et $K_2 = k(m)$, m racine de $X^p - X - \varepsilon\omega^{-t}$ deux extensions d'Artin-Schreier de k . On suppose qu'il existe une unité γ de k qui vérifie : $v_k(\gamma^p + \frac{\varepsilon}{\delta}) > \frac{(p-1)t}{p}$ et $\gamma^{p-1} \not\equiv 1 \bmod \omega$. Alors $K = K_1K_2$ est une extension de degré p^2 de k , admettant t comme seul nombre de ramification, et l'élément $x = m + \gamma\ell$ est de valuation $-t$ dans K .

L'élément x vérifie : $(x-\gamma\ell)^p - (x-\gamma\ell) - \varepsilon\omega^{-t} = 0$ i.e.

$$x^p + \sum_{i=1}^{p-2} \binom{p}{i}(-1)^i(\gamma\ell)^i x^{p-i} + (p(\gamma\ell)^{p-1} - 1)x - \gamma(\gamma^{p-1} - 1)\ell - (\gamma^p\delta + \varepsilon)\omega^{-t} = 0 .$$

Soit $\lambda_o = \gamma(\gamma^{p-1} - 1)\ell + (\gamma^p\delta + \varepsilon)\omega^{-t}$, $v_{K_1}\lambda_o = -t$ grâce à l'hypothèse sur γ . Donc x est racine d'un polynôme P de $K_1[X]$ de la forme : $P = X^p - \sum_{i=1}^{p} \lambda_{p-i} X^{p-i}$, avec $v_{K_1}\lambda_o = -t$ et $v_{K_1}\lambda_i \geq 0$ pour $i \geq 1$ puisque $t < \frac{pe}{p-1}$. Or un tel polynôme est irréductible sur K_1 et, si x est une de ses racines, l'extension $K = K_1(x)/K_1$ est ramifiée et $v_K x = -t$ (même démonstration que pour un polynôme d'Artin-Schreier). Il reste à montrer que t est le seul nombre de ramification de K/k . Il suffit de vérifier que c'est celui de K/K_1 (cf. 2). Or $v_K fx = v_K fm = 0$ et $v_K fx = v_K x + t_{K/K_1} = -t + t_{K/K_1}$ (lemme 0).

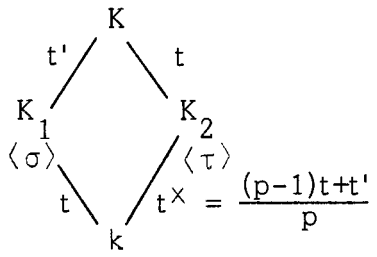
Remarque : La condition γ unité telle que $\gamma^{p-1} \not\equiv 1 \bmod \omega$ exige que le degré résiduel F de k vérifie $F > 1$. Si cette condition est vérifiée, la proposition précédente permet de construire explicitement des extensions bicycliques de degré p^2 de k avec un seul nombre de ramification.

6. - CONDITION NECESSAIRE POUR QUE $\mathfrak{A}_\theta = \mathfrak{O}$

6.1. Soit ϑ un entier de valuation a . Reprenons les notations des paragraphes précédents résumées par le schéma :

$t' \equiv t \equiv a \bmod p^2$, $t'-t = np^2$

$f = \sigma - 1$, $g = \tau - 1$.



Pour tout entier i , tel que $0 \le i \le p-1$, on a (cf. 4) :

$$v_K f^i\theta = it' + a \ , \ v_{K_1} T_1\theta = \frac{(p-1)t'+a}{p} \ , \ v_{K_1} g^i T_1\theta = \frac{(p-1)t'+a}{p} + it$$

$$v_K g^i\theta = it + a \ , \ v_{K_2} T_2\theta = \frac{(p-1)t+a}{p} \ , \ v_{K_2} f^i T_2\theta = \frac{(p-1)t+a}{p} + it^\chi \ .$$

Puisque $v_K T_2\theta = v_K \dfrac{T_1\theta}{\omega^{(p-1)n}} = (p-1)t+a$, il existe une unité μ de k telle que $v_K(T_2 + \mu \dfrac{T_1}{\omega^{(p-1)n}})\theta > (p-1)t + a$. Appliquant f à cet élément, on obtient $fT_2\theta$, de valuation $2(p-1)t + a + t'$.

Définissons l'entier J par : $J = \mathrm{Max}\{v_K(T_2 + \mu \dfrac{T_1}{\omega^{(p-1)n}})\theta \ ; \ \mu$ unité de $k\}$. Il résulte du lemme 0 que, ou bien J est égal à $2(p-1)t + a$, ou bien J est multiple de p , strictement compris entre $(p-1)t + a$ et $2(p-1)t + a$, et non congru à $ap \bmod p^2$ (puisque $v_K T_1\theta \equiv ap \bmod p^2$). Notons mp^2 le plus grand multiple de p^2 inférieur à $2(p-1)t + a$, $c(t)$ l'entier défini par : $c(t) = p - 2\alpha$ si $2\alpha < p$ et $c(t) = p - \alpha$ sinon (α reste de la division de t par p).

PROPOSITION 6. - <u>Si</u> $J \equiv 0 \bmod p$, <u>une condition nécessaire pour que</u> $\mathfrak{A}_\theta = \mathfrak{O}$ <u>est</u> : $J \ge mp^2 - pc(t)$.

On suppose donc $J \equiv 0 \bmod p$. On note $\nu_i = v_K g^i T_1\theta = ipt + (p-1)t' + a \equiv (i+1)ap \bmod p^2$, i entier du segment $[0, p-1]$.

Si $J \equiv 0 \bmod p^2$. Il existe une unité μ de k telle que $v_K(T_2 + \mu \frac{T_1}{\omega^{(p-1)n}})\theta = J \equiv \nu_{p-1}$. Un raisonnement analogue à celui de 5 montre qu'il existe des éléments $(x_i)_{0 \le i \le p-1}$ de k tels que : $v_k x_o = 0$, $v_k x_{p-1} = \frac{J - \nu_{p-1}}{p^2}$ et $v_K(T_2 + x_o \frac{T_1}{\omega^{(p-1)n}} + \sum_{i=2}^{p-1} x_i g^i T_1)\theta = 2(p-1)t + a$. Il résulte de la définition de m que l'élément φ de $k[G]$ défini par : $\varphi = \frac{1}{\omega^m}(T_2 + x_o \frac{T_1}{\omega^{(p-1)n}} + \sum_{i=2}^{p-1} x_i g^i T_1)$ appartient à $\mathfrak{A}_\theta$. Soit $\mathfrak{f}$ le conducteur de $\mathfrak{O}$ dans $A[G]$, i.e. $\mathfrak{f} = \{x \in k \, ; \, x\mathfrak{O} \subset A[G]\}$. On sait [5] que c'est l'idéal TB , engendré par $\omega^{\frac{1}{p^2}\nu_{p-1}}$. Une condition nécessaire pour que $\mathfrak{A}_\theta = \mathfrak{O}$ est que $\varphi \in \mathfrak{O}$, donc que $\omega^{\frac{1}{p^2}\nu_{p-1}} \varphi \in A[G]$, en particulier que $\omega^{\frac{1}{p^2}\nu_{p-1}} \frac{x_{p-1}}{\omega^m} \in A$, i.e. que $J \ge mp^2$.

Donc, si $J \equiv 0 \bmod p^2$, une condition nécessaire pour que $\mathfrak{A}_\theta = \mathfrak{O}$ est : $J = mp^2$.

Si $J \not\equiv 0 \bmod p^2$. Soit r l'entier compris entre 2 et $p-1$ tel que $J \equiv rap \bmod p^2$. Il existe une unité μ de k telle que $v_K(T_2 + \mu \frac{T_1}{\omega^{(p-1)n}})\theta = J \equiv \nu_{r-1} \bmod p^2$. Comme ci-dessus, on montre qu'il existe des éléments $(x_i)_{0 \le i \le p-1}$ de k tels que : $v_k x_o = 0$, $v_k x_{r-1} = \frac{J - \nu_{r-1}}{p^2}$, et $\varphi = \frac{1}{\omega^m}(T_2 + x_o \frac{T_1}{\omega^{(p-1)n}} + \sum_{i=1}^{p-1} x_i g^i T_1) \in \mathfrak{A}_\theta$. Une condition nécessaire pour que $\mathfrak{A}_\theta = \mathfrak{O}$ est que $\varphi \in \mathfrak{O}$, en particulier que $\varphi\theta_1\theta - \theta_1\varphi\theta \in B$ quel que soit l'entier θ_1 de K_1 (la condition relative au conducteur est satisfaite).

Or $\frac{1}{\omega^m}(T_2\theta_1\theta - \theta_1 T_2\theta) \in B$. On montre en effet, par récurrence, que, pour $i \le p-1$, $g^i\theta_1\theta \equiv \theta_1 g^i\theta \bmod \theta_1 \pi^{(p+i-1)t+a}$ (π uniformisante de K) . On en déduit que $T_2\theta_1\theta \equiv \theta_1 T_2\theta \bmod \theta_1 \pi^{2(p-1)t+a}$. Donc

$\varphi \in \mathfrak{D}$ exige : $\frac{1}{\omega^m} \sum_{i=1}^{p-1} x_i(g^i T_1 \theta_1 \theta - \theta_1 g^i T_1 \theta) \in B$. Or $v_K(g^i T_1 \theta_1 \theta - \theta_1 g^i T_1 \theta) \geq v_K \theta_1 + \nu_i$ et on peut choisir θ_1 tel qu'il y ait égalité pour $i = r-1$. En effet, $v_K \theta_1 g^i T_1 \theta = v_K \theta_1 + \nu_i$, $v_K g^i T_1 \theta_1 \theta = p v_{K_1} g^i \theta_1 T_1 \theta$, $v_{K_1} \theta_1 \cdot T_1 \theta = v_{K_1} \theta_1 + \frac{\nu_0}{p} \equiv v_{K_1} \theta_1 + \alpha \bmod p$ donc $v_{K_1} g^i \theta_1 \cdot T_1 \theta \geq v_{K_1} \theta_1 + \frac{\nu_0}{p} + it$ avec inégalité stricte si $v_{K_1} \theta_1$ est congrue mod p à l'un des entiers $-\alpha$, -2α ,..., $-i\alpha$. Choisissons un tel entier θ_1 , alors : $v_K \frac{1}{\omega^m} x_{r-1}(g^{r-1} T_1 \theta_1 \theta - \theta_1 g^{r-1} T_1 \theta) = J + v_K \theta_1 - mp^2$, et pour $i \neq r-1$, $v_K \frac{1}{\omega^m} x_i(g^i T_1 \theta_1 \theta - \theta_1 g^i T_1 \theta) \geq v_K x_i + v_K \theta_1 + \nu_i - mp^2 > J + v_K \theta_1 - mp^2$, car $v_K x_i g^i T_1 \theta > J$. Donc $\varphi \in \mathfrak{D}$ exige : $J \geq mp^2 - p v_{K_1} \theta_1$.

Si $r = 2$, toute uniformisante vérifie la condition : $v_K(gT_1 \theta_1 \theta - \theta_1 g T_1 \theta) = v_K \theta_1 + \nu_1$, car $g\theta_1 T_1 \theta = \theta_1 \cdot g T_1 \theta + g\theta_1 \cdot T_1 \theta + g\theta_1 \cdot g T_1 \theta$.

Si $r > 2$, tout entier de K_1 dont la valuation dans K_1 est congrue mod p à l'un des entiers $-\alpha, -2\alpha, \ldots, -(r-1)\alpha$ vérifie la condition : $v_K(g^{r-1} T_1 \theta_1 \theta - \theta_1 g^{r-1} T_1 \theta) = v_K \theta_1 + \nu_{r-1}$.

Notons $d(r)$ l'entier défini pour $2 \leq r \leq p-1$ par : $d(2) = 1$ et $d(r) = \mathrm{Min}\{d ; 0 < d \leq p-1, d \equiv -\alpha, -2\alpha, \ldots, -(r-1)\alpha \bmod p\}$ si $r > 2$.

Alors si $J \equiv \mathrm{rap} \bmod p^2$, une condition nécessaire pour que $\mathfrak{A}_{\mathfrak{G}} = \mathfrak{D}$ est : $J \geq mp^2 - pd(r)$.

Pour obtenir une condition nécessaire indépendante de r , on introduit l'entier $c(t)$ défini précédemment : $c(t) = 1$ si $p = 3$, $c(t) = d(3)$ si $p > 3$.

6.2. On va désormais évaluer l'entier J lorsque θ est l'entier de valuation a construit en 5 , et utiliser la proposition précédente pour obtenir :

PROPOSITION 7. - Soit θ l'entier de K de valuation a construit en 5 . Si les nombres de ramification de K/k vérifient

$$\frac{pt+t'}{p} \geq \frac{pe}{p-1} + \frac{p+c(t)}{p-1} \qquad (I)$$

alors $\mathfrak{A}_\theta \neq \mathfrak{O}$.

COROLLAIRE. - Si $\mathfrak{A}_\theta \subset \mathfrak{O}_m$, par exemple si $\frac{(p-1)t+t'}{p} \leq \frac{pe}{p-1} - \beta$, la condition (I) entraîne que l'anneau des entiers B n'est pas libre sur son ordre $\mathfrak{O}$.

L'entier θ de K de valuation a construit en 5 est de la forme $\theta = \omega^{\frac{(p^2-1)t+a}{p^2}} (\ell x)^{p-1}$, où $x = \omega^n m + \gamma\ell + z + \sum_{i=2}^{p-1} y_i \ell^i$ est de valuation $-t$. On pose $y = \sum_{i=2}^{p-1} y_i \ell^i$ et $\ell^X = \gamma\ell + z + y$. Pour les calculs de trace, on utilise le lemme suivant :

LEMME 8. - Soit ℓ une racine d'un polynôme d'Artin-Schreier sur k : $X^p - X - \Delta$. Soit T la trace dans l'extension $k(\ell)/k$. Soit i un entier > 0 écrit sous la forme $i = (p-1)h + r$, $0 \leq r < p-1$. Alors, si $h \leq p-1$,

$$T\ell^i = \begin{cases} p-1 & \text{si } r = 0 \\ c\Delta^r \text{ , } c \text{ entier de } k \text{ , si } & 0 < r < h \\ p\Delta^r & \text{si } r = h \\ 0 & \text{si } r > h \text{ .} \end{cases}$$

La démonstration se fait par récurrence sur l'entier h .
Puisque $x = \omega^n m + \ell^X$, $x^{p-1} = (\omega^n m + \ell^X)^{p-1}$ et, d'après le lemme,

$$T_1 x^{p-1} = (p-1)\omega^{n(p-1)} + p(\ell^X)^{p-1} \text{ .}$$

Donc $$\frac{T_1(\ell x)^{p-1}}{\omega^{(p-1)n}} = (p-1)\ell^{p-1} + \frac{p\ell^{p-1}}{\omega^{(p-1)n}} (\gamma\ell + z + y)^{p-1}$$

$$(\ell x)^{p-1} = \ell^{p-1}(\omega^n m + z + \gamma\ell + y)^{p-1} = \ell^{p-1} \sum_{k=0}^{p-1} \binom{p-1}{k} (\omega^n m + z)^{p-1-k} (\gamma\ell + y)^k$$

$$T_2(\ell x)^{p-1} = \sum_{k=0}^{p-1} \binom{p-1}{k} (\omega^n m + z)^{p-1-k} T_2 \ell^{p-1} (\gamma\ell + y)^k \ .$$

D'après le lemme, $T_2 \ell^{p-1}(\gamma\ell+y) = \gamma p\Delta + y_{p-1}(p-1)$, où $\Delta = \ell^p - \ell$.

Donc $T_2(\ell x)^{p-1} = (p-1)(\gamma\ell+y-x)^{p-1} - (p-1)(\gamma\ell+y-x)^{p-2}(\gamma p\Delta + y_{p-1}(p-1)) + \sum_{k=2}^{p-1} u_k$,

où $u_k = (-1)^k \binom{p-1}{k} (\gamma\ell+y-x)^{p-1-k} T_2 \ell^{p-1} (\gamma\ell+y)^k$. Définissons u_o et u_1 par : $u_o = (p-1)(\gamma\ell+y-x)^{p-1} - (p-1)(\gamma\ell)^{p-1}$,

$$u_1 = -(p-1)(\gamma\ell+y-x)^{p-2}(\gamma p\Delta + y_{p-1}(p-1)) - \frac{p(\gamma\ell)^{p-1}}{\omega^{(p-1)n}} (\gamma\ell+z+y)^{p-1} \ .$$

Alors :

$$(T_2 - \gamma^{p-1} \frac{T_1}{\omega^{(p-1)n}})(\ell x)^{p-1} = \sum_{k=0}^{p-1} u_k \ .$$

Etudions d'abord le cas particulier où $y = 0$

$$u_o = (p-1)((\gamma\ell - x)^{p-1} - (\gamma\ell)^{p-1}) \ , \ v_K u_o = v_K \ell^{p-2} x = -(p-1)^2 t$$

$$u_1 = \gamma^{p-1} p\, \ell^{2p-2} (1 - \frac{\gamma^{p-1}}{\omega^{(p-1)n}}) + \text{termes de valuation} \rangle .$$

$v_K u_1 = v_K \dfrac{p\ell^{2p-2}}{\omega^{(p-1)n}}$, même lorsque $n = 0$ (i.e. $t' = t$) puisque $\gamma^{p-1} \not\equiv 1 \bmod \omega$ (cf. 5) ; $v_K u_1 = p^2 e - (p-1)(pt+t') - (p-1)^2 t$.

$u_k = 0$ si $2 \le k < p-1$ et $u_{p-1} = \gamma^{p-1}(p-1)$.

On obtient donc pour $\theta = \omega^{\frac{(p^2-1)t+a}{p^2}} (\ell x)^{p-1}$:

$$v_K(T_2 - \gamma^{p-1} \frac{T_1}{\omega^{(p-1)n}})\theta = \text{Min}\left(2(p-1)t+a \ , \ 2(p-1)t+a+p^2 e-(p-1)(pt+t')\right) \ .$$

D'où le résultat dans ce cas particulier :

si $pt+t' < \dfrac{p^2 e}{p-1}$, $J = 2(p-1)t + a$

si $pt+t' > \dfrac{p^2 e}{p-1}$, $J = 2(p-1)t + a + p^2 e - (p-1)(pt+t') \equiv 2ap \bmod p^2$.

Une condition nécessaire pour que $\mathfrak{A}_\theta = \mathfrak{D}$ est alors : $J \ge mp^2 - p$.

Cette condition n'est pas satisfaite si $\beta+1 \le 2\alpha < p-1$ ou si $2\alpha \ge \beta+p+1$, car le segment $[mp^2-p, 2(p-1)t+a]$ ne contient alors pas d'entier congru à $2ap \bmod p^2$.

Plus généralement, elle n'est pas satisfaite si $J \leq 2(p-1)t+a-p^2-p$ i.e. si $\frac{pt+t'}{p} \geq \frac{pe}{p-1} + \frac{p+1}{p-1}$.

Etudions maintenant le cas où $y \neq 0$.

$k \geq 2$, $v_K u_k \equiv v_K \ell^{p-1-k} \equiv (k+1)ap \bmod p^2$

$u_1 = \gamma^{p-1} p\ell^{2p-2} - (\gamma\ell)^{p-2} y_{p-1} - \frac{p(\gamma\ell)^{2p-2}}{\omega^{(p-1)n}}$ + termes de valuation $\rangle$

$v_K y_{p-1} \ell^{p-1} > v_K \ell$ par construction de x , donc $v_K y_{p-1} \ell^{p-2} > 0$. On suppose désormais qu'est réalisée la condition suivante :

$$v_K \frac{p(\gamma\ell)^{2p-2}}{\omega^{(p-1)n}} < 0 \text{ , i.e. } \frac{pt+t'}{p} > \frac{pe}{p-1} - \frac{(p-1)t}{p} \text{ .} \qquad \text{(II)}$$

Alors, comme dans le cas particulier,

$$v_K u_1 = p^2 e - (p-1)(pt+t') - (p-1)^2 t \equiv 2\,ap \bmod p^2 \text{ .}$$

$$u_o = (p-1)^2(\gamma\ell)^{p-2}(y-x) + \text{termes de valuation} \rangle \text{ .}$$

Soit ν l'entier, compris entre 2 et p-1 , tel que $v_K y = v_K y_\nu \ell^\nu$. Alors $v_K u_o = v_K \ell^{p-2} y_\nu \ell^\nu \equiv (p-\nu+2)ap \equiv v_K u_{p-\nu+1} \bmod p^2$ $(2 \leq p-\nu+1 \leq p-1)$. On pose $u_o + u_{p-\nu+1} = u'_o + u'_{p-\nu+1}$, avec $u'_o = -(p-1)^2(\gamma\ell)^{p-2}x$.

LEMME 9. - $v_K u'_{p-\nu+1} = v_K u_{p-\nu+1}$.

Montrons que ce lemme entraîne la proposition 7 .

$$v_K(T_2 - \gamma^{p-1}\frac{T_1}{\omega^{(p-1)n}})(\ell x)^{p-1} = \text{Min}(v_K u'_o , v_K u_i ,\ i>0) \text{ .}$$

Supposons que $\frac{pt+t'}{p} > \frac{pe}{p-1}$, alors la condition (II) est vérifiée, $v_K u_1 < v_K u'_o$, et on obtient pour $\theta = \omega^{\frac{(p^2-1)t+a}{p^2}} (\ell x)^{p-1}$:

$$v_K(T_2 - \gamma^{p-1}\frac{T_1}{\omega^{(p-1)n}})\theta = \text{Min}((p^2-1)t + a + v_K u_i \ ,\ i>0) \text{ .}$$

Donc l'entier J est congru à 0 mod p et au plus égal à $2(p-1)t + a + p^2 e - (p-1)(pt+t')$. Une condition nécessaire pour que

$\mathfrak{U}_\theta = \mathfrak{O}$ est alors : $J \geq mp^2 - pc(t)$. Elle n'est pas satisfaite si $(p-1)(pt+t') \geq p^2 e + p^2 + pc(t)$ i.e. $\frac{pt+t'}{p} \geq \frac{pe}{p-1} + \frac{p+c(t)}{p-1}$.

LEMME 10. -

$T_2 \varepsilon^{p-1}(\gamma\varepsilon+y)^{p-\nu+1} = T_2 \varepsilon^{p-1}(p-\nu+1)(\gamma\varepsilon)^{p-\nu} y_\nu \varepsilon^\nu + \text{termes de valuation} \rangle$.

Montrons que ce lemme entraîne le précédent.

$u_{p-\nu+1} = (-1)^\nu \binom{p-1}{\nu-2}(\gamma\varepsilon+y-x)^{\nu-2} T_2 \varepsilon^{p-1}(\gamma\varepsilon+y)^{p-\nu+1}$. Utilisons le lemme 9 .

$u_{p-\nu+1} = (-1)^\nu \binom{p-1}{\nu-2}(\gamma\varepsilon)^{\nu-2}(p-\nu+1)\gamma^{p-\nu} y_\nu T_2 \varepsilon^{2p-1} + \text{termes de val.} \rangle$

$u_{p-\nu+1} = (-1)^\nu \binom{p-1}{\nu-2}(p-\nu+1)\gamma^{p-2} y_\nu (2p-1)\varepsilon^{p+\nu-2} + \text{termes de val.} \rangle$

Or $u_o - u'_o = (\gamma\varepsilon)^{p-2} y_\nu \varepsilon^\nu + \text{termes de val.} \rangle$. Donc

$u'_{p-\nu+1} = \gamma^{p-2} y_\nu \varepsilon^{p+\nu-2}(1+(-1)^{\nu+1}\binom{p-1}{\nu-2}(p-\nu+1)) + \text{termes de val.} \rangle$ où

$1 + (-1)^{\nu+1}\binom{p-1}{\nu-2}(p-\nu+1) \equiv \nu \bmod p$.

Il reste à démontrer le lemme 10.

$$(\gamma\varepsilon + \sum_{i=2}^{p-1} y_i \varepsilon^i)^{p-\nu+1} = \sum_{\substack{a_i \geq 0 \\ \sum a_i = p-\nu+1}} \binom{p-\nu+1}{a_1,\ldots,a_{p-1}} (\gamma\varepsilon)^{a_1} \ldots (y_{p-1}\varepsilon^{p-1})^{a_{p-1}}$$

$$T_2 \varepsilon^{p-1}(\gamma\varepsilon+y)^{p-\nu+1} = \sum_{\substack{a_i \geq 0 \\ \sum a_i = p-\nu+1}} \epsilon\, y_2^{a_2} \ldots y_{p-1}^{a_{p-1}} T_2 \varepsilon^{p-1+j}$$

avec ϵ unité de k (dépendant de $a_1,\ldots,a_{p-1}$) et $j = \sum_{i=1}^{p-1} i a_i$.

On privilégie le terme associé à : $a_1 = p-\nu$ et $a_\nu = 1$, i.e. $(p-\nu+1)\gamma^{p-\nu} \cdot y_\nu T_2 \varepsilon^{2p-1}$, dont la valuation est celle de $y_\nu \varepsilon^p$ ($T_2 \varepsilon^{2p-1} = (2p-1)\Delta$) . On montre que tous les autres termes de la somme ont une valuation strictement supérieure. Pour cela, on écrit $p-1+j$ sous la forme $(p-1)q+r$, $0 \leq r < p-1$ et on utilise les résultats du lemme 8 . On remarque que $2p-\nu \leq p-1+j \leq (p-1)(p-\nu+2)$.

Si $r = 0$.

Ou bien $q < p$, alors $T_2\ell^{(p-1)q} = p-1$. Il faut montrer que $vy_2^{a_2}\dots y_{p-1}^{a_{p-1}} > vy_\nu\ell^p$. Or $vy_i\ell^i > v\ell$, donc $pv_k y_i > (i-1)t > 0$ et $vy_\nu\ell^\nu < vx$, donc $p^2 v_k y_\nu < (\nu p-1)t$, $vy_\nu\ell^p < 0$.

Ou bien $q = p$. Cela n'est possible que si $\nu = 2$ et pour le terme associé à : $a_{p-1} = p-1$. Alors $T_2\ell^{(p-1)p} = p-1+p\Delta^{p-1}$. Il faut montrer que $vy_{p-1}^{p-1}p\ell^{p(p-1)} > vy_2\ell^p$ i.e. $(p-1)pv_k y_{p-1}+pe-p(p-2)t-pv_k y_2 > 0$. Or $vy_{p-1}\ell^{p-1} \geq vy_2\ell^2$ et $pe > (p-1)t$, donc

$$(p-1)pv_k y_{p-1} + pe > (p-1)pv_k y_2 + (p-1)(p-2)t .$$

L'inégalité est donc satisfaite si : $(p-2)(pv_k y_2 - t) \geq 0$, et cette dernière l'est.

Si $r = q$.

Alors $T_2\ell^{pq} = p\Delta^q$. Il faut montrer que $vy_2^{a_2}\dots y_{p-1}^{a_{p-1}}p\ell^{pq} > vy_\nu\ell^p$ i.e. $\sum_{i=2}^{p-1} a_i pv_k y_i + pe - p(q-1)t - pv_k y_\nu > 0$. Or $vy_i\ell^i \geq vy_\nu\ell^\nu$ donc $pv_k y_i \geq pv_k y_\nu + (i-\nu)t$. Soit $s = \sum_{i=2}^{p-1} a_i$, alors

$$\sum_{i=2}^{p-1} a_i pv_k y_i \geq spv_k y_\nu + (j-a_1)t - s\nu t .$$

L'inégalité est donc satisfaite si : $(s-1)pv_k y_\nu + (j-a_1)t - s\nu t + (p-1)t - p(q-1)t \geq 0$ i.e. $(s-1)pv_k y_\nu + (p-a_1-s\nu)t \geq 0$, soit $(s-1)(pv_k y_\nu - (\nu-1)t) \geq 0$. Cette dernière l'est car $pv_k y_\nu > (\nu-1)t$ et $s > 0$.

Si $r < q$.

Alors $T_2\ell^{(p-1)q+r} = c\Delta^r$, c entier de k . Il faut montrer que : $vy_2^{a_2}\dots y_{p-1}^{a_{p-1}}\ell^{pr} > vy_\nu\ell^p$ i.e. $\sum_{i=2}^{p-1} a_i pv_k y_i - p(r-1)t - pv_k y_\nu > 0$. Comme précédemment, l'inégalité est satisfaite si $(s-1)pv_k y_\nu + (j-a_1)t - s\nu t - p(r-1)t > 0$, soit $(s-1)(pv_k y_\nu - (\nu-1)t) + (p-1)(q-r-1)t > 0$. Cette dernière l'est si $s > 1$, et $s = 1$ n'est obtenu que pour le terme privilégié.

7. - CONCLUSION, SOUS FORME DE REMARQUES

7.1. Pour $p = 2$ et $t \equiv t' \equiv 1 \bmod 4$ par exemple, on sait que B (anneau des entiers d'une extension biquadratique d'un corps 2-adique) n'est pas libre sur son ordre $\mathfrak{O}$ ssi $2t+t' \geq 4e+7$ [7] . L'analogie avec la condition (I) de la proposition 7 est claire.

7.2. Pour $p = 3$ et $t = t' \equiv 1 \bmod 9$, la proposition 7 s'énonce : si $8t > 9e+8$, B n'est pas libre sur $\mathfrak{O}$ (car $\mathfrak{A}_\theta \subset \mathfrak{O}_m$) . Or il existe des extensions qui vérifient : $8t < 9e+8$ et B libre sur $\mathfrak{O}$.

PROPOSITION. - Soit t un entier qui vérifie $t \equiv 1 \bmod 9$ et $t < \frac{3e}{2}$, soit $K_1 = k(\ell)$, ℓ racine de $X^3-X-\delta\omega^{-t}$ (δ unité de k), soit $K_2 = k(m)$, m racine de $X^3-X-\varepsilon\omega^{-t}$. On suppose qu'il existe une unité γ de k telle que : $v_k(\gamma^3+\frac{\varepsilon}{\delta}) > \frac{2t}{3}$ et $\gamma^2 \not\equiv 1 \bmod \omega$. Alors $K = K_1K_2$ est une extension de degré 9 de k , admettant t comme seul nombre de ramification, et telle que B soit libre sur $\mathfrak{O}$ si $8t < 9e$.

On sait que K/k est de degré 9 , admet t comme seul nombre de ramification, et que $x = m+\gamma\ell$ est de valuation $-t$ dans K (cf. 5). Soit $\theta = \omega^{\frac{8t+1}{9}}(\ell x)^2$, c'est une uniformisante de K . Lorsque $8t < 9e$, on va construire une A-base de $\mathfrak{A}_\theta$ et montrer que $\mathfrak{A}_\theta = \mathfrak{O}$. $g\ell = (\tau-1)\ell$ est racine du polynôme primitif de $K_1[X]$: $X^2+3\ell X+3\ell^2-1$. On peut supposer que $g\ell$ est une unité principale de K_1 et poser $g\ell = 1+r$. La méthode de Newton montre que $v_{K_1} r = v_{K_1} 3\ell^2$. On pose de même $fm = 1+s$, $v_{K_2} s = v_{K_2} 3m^2$. Des calculs simples montrent, sous l'hypothèse $9e-8t > 0$, que l'on a, modulo des termes de valuation strictement supérieure à $-5t$:

$$f(\ell x)^2 \equiv 2\ell^2 x + \ell^2$$

$$g(\ell x)^2 \equiv 2\gamma\ell^2 x + \gamma^2\ell^2 + 2\ell x^2$$

$$T_1(\ell x)^2 \equiv 2\ell^2 \quad .$$

Donc $v_K(\gamma f - g + \gamma(1-\gamma)T_1)(\ell x)^2 = -5t$. Soit $\varphi = \gamma f - g + \gamma(1-\gamma)T_1$. Posons $t = 9\lambda+1$, alors $v_K \frac{\varphi\theta}{\omega^{3\lambda}} = 4$ et $v_K \frac{f\varphi\theta}{\omega^{4\lambda}} = 5$. De même, sous l'hypothèse $9e - 8t > 0$, on a, modulo des termes de valuation strictement supérieure à $-2t$:

$$T_1(\ell x)^2 \equiv 2\ell^2 + 3\gamma^2\ell^4$$

$$T_2(\ell x)^2 \equiv 2\gamma^2\ell^2 + 3\gamma^2\ell^4 - 4\gamma\ell x + 2x^2$$

$$fg(\ell x)^2 \equiv 2\gamma\ell^2 + 2\gamma\ell^2(r+s) + 4\ell x + 2(1-\gamma)\ell$$

$$gT_1(\ell x)^2 \equiv 4\ell \ .$$

Donc $(\gamma^2 T_1 + T_2 + \gamma fg + \gamma(1-\gamma)gT_1)(\ell x)^2 \equiv \gamma^2\ell^2(3(\gamma^2+1)\ell^2 - (r+s)) + 2x^2$. La méthode de Newton montre que $r \equiv 3\ell^2 + 3\ell \bmod (3\ell^2)^2$, on en déduit, sous l'hypothèse $9e-8t > 0$, que $v_K(3(\gamma^2+1)\ell^2 - (r+s)) = v_K 3\ell x$. Soit $\psi = \gamma^2 T_1 + T_2 + \gamma fg + \gamma(1-\gamma)gT_1$, alors $v_K\psi(\ell x)^2 = -2t$, donc $v_K \frac{\psi\theta}{\omega^{6\lambda}} = 7$ et $v_K \frac{f\psi\theta}{\omega^{7\lambda}} = 8$. On peut choisir comme A-base de $\mathfrak{A}_\theta$ les éléments : 1 , $\frac{f}{\omega^\lambda}$, $\frac{T_1}{\omega^{2\lambda}}$, $\frac{\varphi}{\omega^{3\lambda}}$, $\frac{f\varphi}{\omega^{4\lambda}}$, $\frac{gT_1}{\omega^{5\lambda}}$, $\frac{\psi}{\omega^{6\lambda}}$, $\frac{f\psi}{\omega^{7\lambda}}$, $\frac{T}{\omega^{8\lambda+1}}$. Comme les éléments 1 , $\frac{f}{\omega^\lambda}$, $\frac{T_1}{\omega^{2\lambda}}$, $\frac{gT_1}{\omega^{5\lambda}}$, $\frac{T}{\omega^{8\lambda+1}}$ appartiennent à l'ordre $\mathfrak{O}$, pour démontrer l'inclusion de $\mathfrak{A}_\theta$ dans $\mathfrak{O}$, il suffit de montrer que $\frac{\varphi}{\omega^{3\lambda}}$ et $\frac{\psi}{\omega^{6\lambda}}$ appartiennent à $\mathfrak{O}$. On vérifie pour cela que $\frac{\varphi^2\theta}{\omega^{6\lambda}}$, $\frac{\varphi\psi\theta}{\omega^{9\lambda}}$, $\frac{\psi^2\theta}{\omega^{12\lambda}}$ sont des entiers.

7.3. Pour $p = 3$ et $t = t' \equiv 1 \bmod 9$, il existe des extensions qui vérifient : $10t > 9e + 10$ et B n'est pas libre sur $\mathfrak{O}$.

PROPOSITION. - Soit t un entier tel que : $t \equiv 1 \bmod 9$ et $t < \frac{3e}{2}$. On suppose que k contient les racines cubiques de 1 . Soit $K_1 = k(\sqrt[3]{a})$, $a = 1 + \alpha\omega^{\frac{3e}{2}-t}$ (α unité de k) , soit $K_2 = k(\sqrt[3]{b})$, $b = 1 + \beta\omega^{\frac{3e}{2}-t}$. On suppose qu'il existe une unité γ de k qui vérifie : $v_k(\gamma^3 + \frac{\beta}{\alpha}) > \frac{2t}{3}$ et $\gamma^2 \not\equiv 1 \bmod \omega$. Alors $K = K_1K_2$ est

une extension de degré 9 de k admettant t comme seul nombre de ramification ; si $10t > 9e+10$, l'anneau B n'est pas libre sur son ordre.

Les extensions K_1/k et K_2/k sont cycliques de degré 3 , et de nombre de ramification t . Soit $\ell = \sqrt[3]{a} - 1$, il vérifie : $\ell^3+3\ell^2+3\ell = \alpha\omega^{\frac{3e}{2}-t}$ et $v_{K_1}(\ell) = \frac{3e}{2} - t$. Définissons c par $\gamma^3+\frac{\beta}{\alpha} = c$; on a : $b = 1+\frac{\beta}{\alpha}(\ell^3+3\ell^2+3\ell) = 1+(c-\gamma^3)(\ell^3+3\ell^2+3\ell) =$

$= (1-\gamma\ell)^3+3\ell(\gamma(1-\gamma^2)+c)-3\ell^2(\gamma^2(1+\gamma)-c)+c\ell^3 = (1-\gamma\ell)^3\lambda$, avec $v_{K_1}\lambda = \frac{9e}{2}-t$ grâce à l'hypothèse faite sur γ . On en déduit que $K = K_1(\sqrt[3]{\lambda})$ est une extension cyclique de degré 3 , et de nombre de ramification t . De plus $\sqrt[3]{\lambda} - 1$ est de valuation $\frac{9e}{2}-t$ dans K . Soit $m = \sqrt[3]{b} - 1$ et $x = m+\gamma\ell$, alors $v_K x = \frac{9e}{2}-t$. Il reste à montrer que B n'est pas libre sur son ordre si $10t > 9e+10$. Soit $\theta = \omega^{\frac{8t+1}{9}}(\frac{\ell x}{3})^2$, c'est une uniformisante de K . Des calculs de trace donnent : $T_1(\ell x)^2 = 3\ell^2(1-\gamma\ell)^2$, $T_2(\ell x)^2 \equiv 3(m^2-\gamma^2\ell^3-\gamma m\ell^3) \bmod 9$, $(T_2-\gamma^2T_1)(\ell x)^2 \equiv 3((m-\gamma\ell)x-\gamma^2(\gamma+1)\ell^3-\gamma\ell^3(m+\gamma^3\ell))$. On en déduit que $v_K(T_2-\gamma^2T_1)\theta = \mathrm{Min}(4t+1\ ,\ 4t+1+\frac{9e}{2}-5t)$. Si $10t > 9e$, l'entier J défini en 6 vérifie $J \equiv \frac{9e}{2}-t+1 \equiv 0 \bmod 9$. Si $10t > 9e+10$, $\mathfrak{O} \neq \mathfrak{A}_\theta$ et B n'est pas libre sur $\mathfrak{O}$.

Cet exemple et le précédent montrent qu'il ne dépend pas que des seuls nombres de ramification que B soit libre sur son ordre ou non.

7.4. Pour p quelconque et $t < p$, la condition nécessaire de la proposition 3' est satisfaite, la condition (I) de la proposition 7 ne l'est pas. Peut-on spéculer que B est libre sur son ordre ? On a le résultat suivant :

PROPOSITION. - Lorsque $t = 1$, B est un $\mathfrak{O}$-module libre.

Posons $t' = \lambda' p^2+1$. Soit θ une uniformisante de K et soient i et j des entiers du segment $[0,p-1]$. On a : $v_K f^i g^j \theta \geq it'+j+1$ avec égalité si $i+j \leq p-1$ (lemme 0) , et $v_K f^i g^{p-1} \theta = pit^{\chi}+p$. On montre que les entiers $(\frac{f^i g^j \theta}{\omega^{i\lambda'}})(i,j) \neq (p-1,p-1)$ et $\frac{f^{p-1} g^{p-1} \theta}{\omega^{(p-1)\lambda'+1}}$ forment une A-base de B .

On utilise le lemme suivant : des éléments de B forment une A-base ssi leurs images dans $B/\omega B$ forment une $A/\omega A$-base .

Supposons que $\sum_{i,j}' a_{ij} \frac{f^i g^j \theta}{\omega^{i\lambda'}} + a_{p-1,p-1} \frac{f^{p-1} g^{p-1} \theta}{\omega^{(p-1)\lambda'+1}} \in \omega B$, $a_{ij} \in A$. Comme $\frac{f^{p-1} g^{p-1} \theta}{\omega^{(p-1)\lambda'+1}}$ est la seule unité parmi les entiers considérés, $a_{p-1,p-1} \in \omega A$. On montre ensuite, par récurrence sur j , que $a_{i,j} \in \omega A$. Pour $j = 0$ par exemple, on fait agir g^{p-1} , on obtient :

$$\sum_{i=0}^{p-1} a_{i,o} \frac{f^i g^{p-1} \theta}{\omega^{i\lambda'}} + g^p \sum_{\substack{i=0 \\ j=1}}^{p-1} \frac{f^i g^{j-1} \theta}{\omega^{i\lambda'}} \in \omega g^{p-1} B .$$

Or $v_K \frac{f^i g^{p-1} \theta}{\omega^{i\lambda'}} = (i+1)p$, $g^p = pgh$, $h \in Z[g]$, et $v_K \omega g^{p-1} x \geq p^2+p$ pour tout $x \in B$. On en déduit que $a_{i,o} \in \omega A$ pour tout $i \in [0,p-1]$.

On obtient donc comme A-base de $\mathfrak{A}_\theta$: $(\frac{f^i g^j}{\omega^{i\lambda'}})_{(i,j)\neq(p-1,p-1)}$ et $\frac{f^{p-1} g^{p-1}}{\omega^{(p-1)\lambda'+1}}$. Or ces éléments appartiennent à $\mathfrak{D}$.

---

[1] A.M. BERGE - Ann. Inst. Fourier, (1978), 4, p.17.

[2] F. BERTRANDIAS et M.J. FERTON - Comptes rendus 274, série A (1972), p. 1330.

[3] N. BOURBAKI - Algèbre , Ch.8, Hermann.

[4] M.J. FERTON - Comptes rendus 274, série A (1972), p.1529 et 276, série A (1973), p.1483.

[5] H. JACOBINSKI - Jour. reine angew Math. 213 (1964), p.151.

[6] R.E. MAC KENZIE and G. WHAPLES - Amer. J. of Maths 78 (1956), p.473.

[7] B. MARTEL - Comptes rendus 278, série A (1974), p.117.

[8] E. NOETHER - Jour. reine angew Math. 167 (1932), p.147.

[9] J.P. SERRE - Corps locaux, Hermann.