Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Jean-Marc Fontaine

Extensions finies galoisiennes des corps valués complets à valuation discrète

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 9, n° 1 (1967-1968), exp. n° 6, p. 1-21

<http://www.numdam.org/item?id=SDPP_1967-1968__9_1_A6_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
9e année, 1967/68, n° 6

11 décembre 1967

EXTENSIONS FINIES GALOISIENNES DES CORPS VALUÉS COMPLETS À VALUATION DISCRÈTE

par Jean-Marc FONTAINE

0. Définitions. Notations.

On utilise, dans la mesure du possible, les notations de J.-P. SERRE ([7], en particulier chapitre IV).

0.1. - A_K est un anneau de valuation discrète v_K pour laquelle il est complet, K son corps des fractions, $\mathfrak{p}_K$ l'idéal maximal de A_K et $\overline{K} = A_K/\mathfrak{p}_K$ son corps résiduel.

L est une extension galoisienne finie de degré n de K, A_L la clôture intégrale de A_K dans L, v_L la valuation correspondant à A_L, $\mathfrak{p}_L$ l'idéal maximal de A_L, $\overline{L} = A_L/\mathfrak{p}_L$ son corps résiduel.

Si $\alpha \in A_K$ (resp. A_L), nous désignerons par $\overline{\alpha}$ sa classe modulo $\mathfrak{p}_K$ (resp. $\mathfrak{p}_L$).

π_K (resp. $\pi_L = \pi$) désigne une uniformisante de K (resp. L), c'est-à-dire un élément irréductible de l'anneau principal A_K (resp. A_L) ; x désigne un élément qui engendre A_L en tant que A_K-algèbre.

On note :

- $e_{L/K} = e = v_L(\pi_K) =$ indice de ramification de l'extension L/K.
- $f_{L/K} = f = [\overline{L} : \overline{K}] =$ degré de l'extension résiduelle $\overline{L}/\overline{K}$.

On a $n = ef$, et si $\mathrm{Car}\ \overline{K} = p$ est différente de 0, on pose $e = \ell p^k$, avec $(\ell, p) = 1$ et $k \geqslant 0$.

0.2. - On pose enfin :

(a) Si $p \neq 0$ et si $\overline{K}$ est un corps fini, $\mathrm{Card}\ \overline{K} = p^{f_0}$; et sinon $f_0 = +\infty$.

(b) Si $p \neq 0$ et si $\mathrm{Car}\ K = 0$, $v_K(p) = e_0$; et sinon $e_0 = +\infty$.

0.3. - Nous ferons de plus, dans tout l'exposé, l'hypothèse suivante :

(S) L'extension résiduelle $\overline{L}/\overline{K}$ est séparable

(ceci est toujours le cas si le corps résiduel $\overline{K}$ est parfait).

Dans ces conditions, l'extension L/K est dite :

- non ramifiée, si $e = 1$;
- simplement ramifiée, si $k = 0$ (c'est donc toujours le cas si $p = 0$) ;
- complètement ramifiée, si $f = 1$;
- complètement surramifiée, si $f = 1$ et si $\ell = 1$ (ceci ne peut se produire que si $p \neq 0$).

Nous désignerons par $G = G(L/K)$ le groupe de Galois de l'extension.

1. Décomposition canonique de l'extension.

1.1. Rappels.

Dans ces conditions, on sait [7] que :

LEMME. - Soit $s \in G$ et soit i un entier rationnel $\geqslant -1$. Les trois conditions suivantes sont équivalentes :

(a) s opère trivialement sur l'anneau quotient $A_L/\mathfrak{p}_L^{i+1}$;

(b) $v_L(s(a) - a) \geqslant i + 1$, $\forall\, a \in A_L$;

(c) $v_L(s(x) - x) \geqslant i + 1$.

On pose $\nu_G(s) = v_L(s(x) - x) - 1$ (1). ν_G est une application de G dans $\mathbb{Z}$.

On peut alors définir $G_i = \{s \in G ;\ \nu_G(s) \geqslant i\}$. G_i s'appelle le i-ième groupe de ramification de l'extension.

Les G_i forment une suite décroissante de sous-groupes invariants de G ; $G_{-1} = G$ et $G_i = \{1\}$ pour i assez grand. La connaissance de la fonction ν_G est équivalente à celle des G_i.

Les G_i forment une filtration de G au sens de Bourbaki [1]. Nous dirons que c'est la filtration associée à l'extension, et nous désignerons par K_i le corps des invariants de G_i. La fonction ν_G n'est autre que la fonction d'ordre de la filtration.

Si $G_i \neq G_{i+1}$, nous dirons que i est un saut de la filtration, ou encore un

---

(1) J.-P. SERRE utilise $i_G(s) = v_L(s(x) - x) = \nu_G(s) + 1$. Pour cet exposé, l'emploi de $\nu_G(s)$ est plus commode, car $\nu_G(s)$ est un nombre de ramification.

nombre de ramification. Si $i > 0$, nous dirons que ce nombre de ramification est propre.

1.2. Caractérisation des extensions à filtration triviale.

Définition. - Nous dirons qu'une extension est à filtration triviale, si la filtration ne comporte qu'un seul saut. Soit v cet unique nombre de ramification. On a alors :

$$G = G_i \quad \text{pour} \quad i \leqslant v \qquad \text{et} \qquad G_i = \{1\} \quad \text{pour} \quad i > v \ .$$

1.2.1. Cas $v = -1$. - On a $G_{-1} = G$, $G_0 = G_i = \{1\}$, $\forall\, i \geqslant 0$.

Ce cas est bien connu. On peut énoncer la proposition suivante :

PROPOSITION 1. - L'extension L/K est à filtration triviale, avec comme unique nombre de ramification $v = -1$, si, et seulement si, elle est non ramifiée $(n = f, e = 1)$. $G \simeq G(\overline{L}/\overline{K})$, et $\overline{L}/\overline{K}$ est aussi galoisienne. Si $\overline{L} = \overline{K}(\overline{\theta})$, quel que soit θ appartenant à la classe de $\overline{\theta}$ dans A_L , $L = K(\theta)$ et $A_L = A_K(\theta)$. Si $\overline{\varphi}(x)$ est le polynôme unitaire irréductible de $\overline{\theta}$ dans $\overline{K}$, quel que soit le polynôme $\varphi(x)$ appartenant à la classe de $\overline{\varphi}$ dans K , toute racine θ de φ engendre l'extension et engendre A_L en tant que A_K-algèbre.

1.2.2. Cas $v \geqslant 0$. - L'extension est alors complètement ramifiée. On a $L = K(\pi)$ et $A_L = A_K(\pi)$, où π est zéro d'un polynôme d'Eisenstein

$$\xi^e + \sum_0^{e-1} \alpha_i \, \xi^{e-i} \ , \qquad \alpha_i \in \mathfrak{p}_K \ , \quad \alpha_e \notin \mathfrak{p}_K^2 \ .$$

Nous allons caractériser complètement les polynômes d'Eisenstein qui engendrent une telle extension.

(a) Le cas $v = 0$.

PROPOSITION 2. - Pour que le corps de rupture d'un polynôme d'Eisenstein

$$\Phi(\xi) = \xi^e + \sum_0^{e-1} \alpha_i \, \xi^{e-i} \qquad (\alpha_i \in \mathfrak{p}_K \ , \quad \alpha_e \notin \mathfrak{p}_K^2)$$

soit une extension galoisienne à filtration triviale, avec comme unique nombre de ramification $v = 0$, il faut et il suffit que $(e \ , \ p) = 1$ et que $\overline{K}$ contienne une racine primitive e-ième de l'unité.

Le groupe de Galois de l'extension est alors un groupe cyclique isomorphe au groupe des racines e-ièmes de l'unité, c'est-à-dire au groupe multiplicatif des racines de $(\frac{1}{\pi^e}\Phi(\pi\eta))$ dans $\overline{L}$ (où π est un zéro de $\Phi(\xi)$).

COROLLAIRE. - L'extension L/K est une extension à filtration triviale avec $v = 0$, comme unique nombre de ramification, si, et seulement si, elle est complètement simplement ramifiée.

Démonstration. - Soit π un zéro de $\Phi(\xi)$

$$\Phi(\pi) = 0 \implies \pi^e + \alpha_e \equiv 0 \pmod{\mathfrak{p}_L^{e+1}} .$$

$L = K(\pi)$. On a alors :

$$\Phi(\pi\eta) \equiv \pi^e(\eta^e + \frac{\alpha_e}{\pi^e}) \pmod{\mathfrak{p}_L^{e+1}} ,$$

donc $\psi(\eta) = \frac{1}{\pi^e}\Phi(\pi\eta) \equiv \eta^e - 1 \pmod{\mathfrak{p}_L}$.

On veut que $v_L(s\pi - \pi) = 1$, $\forall\, s \in G$, $s \neq 1$, c'est-à-dire que $v_L(\pi' - \pi) = 1$, $\forall\, \pi'$ zéro $\neq \pi$ de $\Phi(\xi)$.

Si on pose $\pi' = \pi\varepsilon'$, les ε' sont les racines différentes de 1 de $\psi(\eta)$, et il faut que $v_L(\varepsilon' - 1) = v_L(\pi' - \pi) - 1 = 0$, donc que $\varepsilon' \not\equiv 1 \pmod{\mathfrak{p}_L}$. 1 doit donc être racine simple de $\eta^e - 1 = 0$ dans $\overline{L}$. Il faut donc $(e , p) = 1$.

Le polynôme $\eta^e - 1$ étant alors séparable, les autres assertions sont évidentes.

Q. E. D.

(b) Le cas $v > 0$.

Ce cas ne peut se présenter que si $p \neq 0$. On peut énoncer la proposition suivante :

PROPOSITION 3. - Pour que le corps de rupture d'un polynôme d'Eisenstein

$$\Phi(\xi) = \xi^e + \sum_0^{e-1} \alpha_i \xi^{e-i} \qquad (\alpha_i \in \mathfrak{p}_K , \ \alpha_e \notin \mathfrak{p}_K^2)$$

soit une extension galoisienne à filtration triviale, avec comme unique nombre de ramification l'entier rationnel, strictement positif v , il faut que l'on ait :
- ou bien (a) : $(v , p) = 1$ et, si e_0 est fini, $v < \frac{e_0\, p}{p - 1}$. Soit, pour $s = 0 , 1 , \ldots , k - 1$, i_s l'unique entier compris entre 1 et $p^k - 1$ tel que $i_s = u_s\, p^s$ avec $(u_s , p) = 1$ et $p^{k-s} | (v - u_s)$.

Alors, il faut et il suffit que les quatre conditions suivantes soient réalisées :

(a.i) $e = p^k$ pour un certain entier positif k (ou encore $\ell = 1$) ;

(a.ii) $\alpha_i \in \mathfrak{p}_K^{\mu(i)}$ avec $\mu(i) = v - \frac{v-u}{p^{k-s}}$ si $i = up^s$ avec $(u , p) = 1$, pour $i = 1 , 2 , \dots , p^{k-1}$;

(a.iii) $\alpha_{i_0} \notin \mathfrak{p}_K^{\mu(i_0)+1}$;

(a.iv) le polynôme $\overline{P}(x) = x^{p^k} + \sum_{s=0}^{k-1} b_s x^{p^s}$ se décompose en facteurs linéaires dans $\overline{K}$, b_s désignant la classe modulo $\mathfrak{p}_K$ de $\binom{p^k - i_s}{p^s}(-1)^{\mu(i_s)} \frac{\alpha_{i_s}}{\alpha_e^{\mu(i_s)}}$.

- ou bien (b): e_0 est fini et $v = \frac{e_0 p}{p-1}$ (ce qui suppose que $(p-1) | e_0$).

Alors, il faut et il suffit que les trois conditions suivantes soient réalisées :

(b.i) $e = p$;

(b.ii) $\alpha_i \in \mathfrak{p}_K^{\mu(i)}$, avec la même définition de $\mu(i)$;

(b.iii) le polynôme $\overline{P}(x) = x^p - bx$ se décompose en facteurs linéaires dans $\overline{K}$, b désignant la classe modulo $\mathfrak{p}_K$ de $(-1)^{e_0} \frac{p}{\alpha_e^{e_0}}$.

COROLLAIRE 1. - G est alors un groupe abélien, produit direct de k groupes cycliques d'ordre p (dans le cas (b), $k = 1$), isomorphe au groupe additif des zéros de $\overline{P}(x)$ dans $\overline{K}$, ou encore des zéros de $(\frac{1}{\pi^{(v+1)e}} \Phi(\pi + \pi\eta))$ dans $\overline{L} = \overline{K}$ (π désignant un zéro de Φ).

COROLLAIRE 2. - Pour que l'extension L/K soit à filtration triviale avec comme unique nombre de ramification $v > 0$, il faut qu'elle soit complètement surramifiée.

La démonstration se fait soit directement en cherchant à résoudre l'équation $\Phi(\xi) = 0$ dans $L = K(\pi)$, soit en essayant de construire le polygone de Newton de $\psi(\eta) = \frac{1}{\pi^{(v+1)e}} \Phi(\pi + \pi^{v+1}\eta)$ (auquel cas, on peut utiliser des résultats dus à M. KRASNER [4]). On trouve ainsi que l'on doit avoir ou bien les conditions (a.i), (a.ii), (a.iii), ou bien (b.i), (b.ii).

On voit alors que :

- dans le cas (a) :

$$\pi^{(v+1)p^k} \psi(\eta) \equiv \pi^{(v+1)p^k} \eta^{p^k} + \sum_{s=0}^{k-1} \binom{p^k - i_s}{p^s} \alpha_{i_s} \pi^{p^k - i_s} \pi^{vp^s} \eta^{p^s} \pmod{\mathfrak{p}_L^{(v+1)p^k+1}}$$

$$\psi(\eta) \equiv \eta^{p^k} + \sum_{0}^{k-1} \binom{p^k - i_s}{p^s} \frac{\alpha_{i_s}}{\pi^{u(i_s)p^k}} \eta^{p^s} \pmod{\mathfrak{p}_L} .$$

Or

$$\Phi(\pi) = 0 \implies \pi^{p^k} + \alpha_e \equiv 0 \pmod{\mathfrak{p}_L^{p^k+1}}$$

et

$$\psi(\eta) \equiv \eta^{p^k} + \sum \binom{p^k - i_s}{p^s} (-1)^{\mu(i_s)} \frac{\alpha_{i_s}}{\alpha^{\mu(i_s)}} \eta^{p^s} \pmod{\mathfrak{p}_L} ,$$

ce qui montre que (a.iv) est bien une condition nécessaire et suffisante.

- dans le cas (b) :

$$\pi^{(v+1)p}\, \psi(\eta) \equiv \pi^p\, \pi^{vp}\, \eta^p + p\pi^p\, \pi^v\, \eta \pmod{\mathfrak{p}_L^{(v+1)p+1}} ,$$

$$\psi(\eta) \equiv \eta^p + \frac{p}{\pi^{v(p-1)}} \eta \equiv \eta^p + \frac{p}{\pi^{e_0 p}} \pmod{\mathfrak{p}_L} .$$

Or

$$\Phi(\eta) = 0 \implies \pi^p + \alpha_e \equiv 0 \pmod{\mathfrak{p}_L^{p+1}} ,$$

donc

$$\psi(\eta) \equiv \eta^p + (-1)^{e_0} \cdot \frac{p}{\alpha_e^{e_0}} \eta \pmod{\mathfrak{p}_L} ,$$

ce qui montre que (b.iii) est une condition nécessaire et suffisante.

Le corollaire 1 se déduit alors immédiatement des propriétés des racines du polynôme $x^{p^k} + \sum_{s=0}^{k-1} b_s x^{p^s}$ dans un corps de caractéristique p . Le corollaire 2 résulte de (a.i) et (b.i).

1.3. Décomposition canonique.

1.3.1. - Revenons au cas général. On sait alors que :

- G_0 est le groupe d'inertie de l'extension, c'est-à-dire que K_0 est la plus grande extension non ramifiée de K contenue dans L , et on a $G(K_0/K) \simeq G(\overline{L}/\overline{K})$ et $[K_0 : K] = f$.

- G_1 est le groupe de ramification de l'extension, c'est-à-dire que K_1 est la plus grande extension simplement ramifiée de K contenue dans L , et on a

$G(K_1/K_0) \simeq G_0/G_1$, groupe cyclique isomorphe au groupe des racines ℓ-ièmes de l'unité qui doit être continu dans $\overline{L} = \overline{K}_0$; $[K_1 : K_0] = \ell$.

- Alors

(a) si $\mathrm{Car}\ \overline{K} = \mathrm{Car}\ \overline{L} = 0$, $G_1 = \{1\}$ et G_0 est cyclique ;

(b) si $\mathrm{Car}\ \overline{K} = p \neq 0$, G_1 est un p-groupe, et les G_i/G_{i+1} sont des groupes abéliens, produits directs de groupes cycliques d'ordre p .

1.3.2. - Les extensions K_j/K_i $(j \geqslant i)$ sont toutes galoisiennes. L'extension K_{i+1}/K_i est

- ou bien triviale, si i n'est pas un nombre de ramification : $K_i = K_{i+1}$;

- ou bien non ; on peut alors montrer que K_{i+1}/K_i est une extension à filtration triviale dont l'unique nombre de ramification est précisément i , et nous pouvons énoncer le théorème suivant :

THÉORÈME 1. - Toute extension finie galoisienne d'un corps valué complet pour une valuation discrète, correspondant à une extension résiduelle séparable, se décompose d'une manière et d'une seule en une suite d'extensions

$$K = K_{v_0} - K_{v_1} - \ldots - K_{v_{m-1}} - K_{v_m} = K_\infty = L \ ,$$

chaque extension $K_{v_{i+1}}/K_{v_i}$ étant une extension à filtration triviale dont l'unique nombre de ramification est v_i , la suite des entiers v_i étant strictement croissante. C'est ce que nous appellerons la décomposition canonique de l'extension.

2. Propriétés de la filtration.

2.1. Un problème non résolu.

(a) Si $\mathrm{Car}\ \overline{K} = p \neq 0$, le groupe d'inertie G_0 est le produit semi-direct d'un sous-groupe cyclique d'ordre premier à p par un p-sous-groupe invariant. On peut montrer que, réciproquement, tout groupe possédant cette propriété peut être considéré comme le groupe d'inertie d'une extension du type L/K .

On peut essayer d'aller plus loin et se demander si l'on peut donner une caractérisation de G_0 muni de la filtration des G_i , ou, ce qui revient au même, muni de la fonction $v_G(s)$.

(b) Un certain nombre de problèmes sont liés dans une large mesure à celui-ci, en particulier la recherche d'une réciproque du théorème 1, ou la donnée d'un

procédé permettant de construire l'extension L/K la plus générale. A défaut de pouvoir donner des résultats complets, nous allons donner un certain nombre de conditions nécessaires.

2.2. Résultats classiques.

Soit U_L le groupe multiplicatif des éléments inversibles de A_L. U_L peut être muni de la filtration des $U_L^{(i)}$ définis par :

$$U_L^{(0)} = U_L \; ; \qquad U_L^{(i)} = 1 + \mathfrak{p}_L^i \quad \text{pour} \quad i > 0 \; .$$

On est alors conduit (cf. [7]) à introduire les applications θ_i définies par la proposition suivante :

PROPOSITION 4. - L'application qui, à $s \in G_i$ fait correspondre $\frac{s\pi}{\pi}$, définit par passage au quotient un isomorphisme θ_i du groupe quotient G_i/G_{i+1} sur un sous-groupe du groupe $U_L^{(i)}/U_L^{(i+1)}$. Cet isomorphisme ne dépend pas du choix de l'uniformisante π .

On peut alors montrer que :

PROPOSITION (A). - Soit $s \in G_0$ et soit $z \in G_i/G_{i+1}$, $i \geqslant 1$. On a

$$\theta_i(szs^{-1}) = \theta_0(s)^i \, \theta_i(z) \; .$$

PROPOSITION (B). - Si $s \in G_i$, $t \in G_j$ et i, $j \geqslant 1$, alors $sts^{-1} t^{-1} \in G_{i+j+1}$.

PROPOSITION (C). - Les nombres propres de ramification sont congrus entre eux modulo p ($\nu_G(s) > 0$, $\nu_G(t) > 0 \Longrightarrow \nu_G(s) \equiv \nu_G(t) \pmod p$) .

Les propositions (B) et (C) se déduisent simultanément du lemme suivant :

LEMME. - Si $s \in G_i$ et $t \in G_j$, on a $sts^{-1} t^{-1} \in G_{i+j}$ et

$$\theta_{i+j}(sts^{-1} t^{-1}) = (j - i) \, \theta_i(s) \, \theta_j(t) \; .$$

On en déduit alors que si les nombres propres de ramification sont congrus à 0 modulo p, le groupe de ramification G_1 est cyclique, d'ordre p^k. Si s est un générateur de G_1, on a

$$\nu_G(s) = \frac{e_0 \, p}{p - 1} \qquad \text{et} \qquad \nu_G(s^h) = \frac{e_0 \, p^{t(h)+1}}{p - 1}$$

(où $p^{t(h)}$ désigne la plus grande puissance de p qui divise h) pour $h = 1 , 2 , \ldots , p^k - 1$, ce qui détermine entièrement la filtration de G_1 . C'est le cas de $L = K(\pi_K^{1/p^k})$, K contenant une racine primitive p^k-ième de l'unité.

Dans le cas "régulier", c'est-à-dire si les nombres propres de ramification sont incongrus à 0 modulo p , on ne sait rien de plus en général. On connaît seulement des résultats plus précis dans le cas où G_0 est un groupe abélien.

Nous allons montrer, dans le paragraphe suivant, comment une étude directe des commutateurs d'éléments de G_1 permet de donner des résultats plus précis et comment, dans certains cas particuliers, on peut même calculer $\nu_G(sts^{-1} t^{-1})$ et $\theta_{\nu_G(sts^{-1}t^{-1})}(sts^{-1} t^{-1})$.

2.3. Étude directe des commutateurs de G_1 .

Dans ce paragraphe, nous remplaçons l'hypothèse (S), donnée initialement, par une hypothèse plus forte :

(S') $\overline{K}$ est un corps parfait ((S') ==> (S)) .

2.3.1. - Nous allons établir le théorème suivant :

THÉORÈME 2. - Soient, pour $i = 1 , 2 , 3 , s_i \in G_1$ avec $\nu_G(s_i) = v_i$. Soit p^r la puissance maximale de p qui divise $v_3 - v_1$. Soit

$$n_0 = \min(v_1 , (p^r - 1)v_2 , (p - 1)v_2 + p , v_3) .$$

Alors $\forall\ n \leqslant n_0$

$$\left\{ \begin{array}{l} \nu_G(s_1 s_3 s_1^{-1} s_3^{-1}) \geqslant v_1 + v_3 + n \\ \nu_G(s_2 s_3 s_2^{-1} s_3^{-1}) \geqslant v_2 + v_3 + n \end{array} \right\} \Longrightarrow \nu_G(s_1 s_2 s_1^{-1} s_2^{-1}) \geqslant v_1 + v_2 + n .$$

Soit v_M le plus grand nombre de ramification fini de l'extension, $G_{v_M} \subset Z_G$, centre du groupe. En appliquant le théorème 2 à $s , t \in G_1$ et $s_3 \in G_{v_M}$, on en déduit le résultat suivant, plus précis que la proposition (B) du paragraphe 2.2.

PROPOSITION 5. - Soient i et j des entiers $\geqslant 1$. Soit p^r la puissance maximale de p qui divise $v_M - i$. Soit

$$n(i , j) = n = \min(i , (p^r - 1)j , (p - 1)j + p) .$$

Si $s \in G_i$, $t \in G_j$, alors $sts^{-1} t^{-1} \in G_{i+j+n}$.

Nous montrerons de plus la proposition suivante :

PROPOSITION 6. - Soient i et j des entiers $\geqslant 1$, tels que $(p-1)j < i$. Alors, $\forall\, s \in G_i$, $t \in G_j$, on a

$$(1) \qquad \theta_{i+pj}(sts^{-1}\, t^{-1}) \equiv \frac{v_M - 1}{p}\, \theta_i(s)\, \theta_j^p(t) \ .$$

En particulier, si $i \not\equiv v_M \pmod{p^2}$,

$$\left.\begin{matrix} \nu_G(s) = i \\ \nu_G(t) = j \end{matrix}\right\} \Longrightarrow \nu_G(sts^{-1}\, t^{-1}) = i + pj \ .$$

C'est ce dernier résultat qui est le plus intéressant. Nous en donnerons des exemples simples d'application un peu plus loin.

Pour démontrer ce théorème, nous allons d'abord établir un lemme.

2.3.2. Lemme préliminaire.

Soit A un domaine d'intégrité de caractéristique 0 ou p. $\forall\, a, b \in A$, nous poserons $a \equiv b \pmod{p}$, ou plus simplement $a \equiv b$ si :

$$a = b \qquad \text{si Car } A = p \ .$$

$$p \mid (a - b) \qquad \text{si Car } A = 0 \ .$$

Si P_t est une matrice carrée d'ordre $t+1$ à coefficients dans A et si $\xi_0, \xi_1, \dots, \xi_t$; $\eta_0, \eta_1, \dots, \eta_t$ sont $2(t+1)$ éléments de A, nous poserons $P_t = \langle p_{k,\ell}^{(t)} \rangle$ et

$$\langle \xi_k \,|P_t|\, \eta_\ell \rangle = (\xi_0, \xi_1, \dots, \xi_t) P_t \begin{pmatrix} \eta_0 \\ \eta_1 \\ \vdots \\ \eta_\ell \end{pmatrix} = \sum_{k=0}^{t} \sum_{\ell=0}^{t} \xi_k\, p_{k,\ell}^{(t)}\, \eta_\ell \ .$$

Nous pouvons énoncer alors le lemme suivant :

LEMME. - Soit A un domaine d'intégrité de caractéristique 0 ou p.

Soient $\lambda_0, \lambda_1, \dots, \lambda_i$; $\mu_0, \mu_1, \dots, \mu_i$; $\nu_0, \nu_1, \dots, \nu_i$ des éléments de A avec $(\nu_0, p) = 1$.

Soient, pour $t = 0, 1, \dots, i$, D_t et N_t des matrices carrées d'ordre $t+1$ vérifiant :

$$D_t = \langle d_{k,\ell}^{(t)} \rangle \qquad \text{avec} \begin{cases} d_{k,t-k}^{(t)} \equiv t - 2k \\ d_{k,\ell}^{(t)} \equiv 0 \quad \text{si} \quad \ell \neq t - k \end{cases}$$

$$N_t = \langle n_{k,\ell}^{(t)} \rangle \qquad \underline{\text{avec}} \quad \begin{cases} n_{k,\ell}^{(t)} \equiv 0 \quad \underline{\text{si}} \quad k + \ell \geqslant t \\ n_{k,\ell}^{(t)} \equiv n_{k-p,\ell}^{(t-p)} \ , \quad \forall\ k \geqslant p \ , \quad t \geqslant p \ . \end{cases}$$

Alors, si, pour $t = 0 , 1 , \ldots , i$, on a

$$\begin{cases} \alpha_t = \langle \nu_k \ |D_t| \ \lambda_\ell \rangle \equiv 0 \\ \beta_t = \langle \nu_k \ |D_t + N_t| \ \mu_\ell \rangle \equiv 0 \end{cases}$$

on a aussi : $\gamma_t = \langle \lambda_k \ |D_t + N_t| \ \mu_\ell \rangle \equiv 0$ pour $t = 0 , 1 , \ldots , i$.

Remarque. - Plus précisément, nous démontrerons que si on a $\alpha_t \equiv 0$, pour $t = 0 , \ldots , i$ et $\beta_t \equiv 0$ pour $t = 0 , \ldots , i - p$, alors $\nu_0 \gamma_t \equiv \lambda_0 \beta_t$ pour $t = 0 , 1 , \ldots , i$.

Démonstration du lemme. - En changeant ν_i en ν_i/ν_0 , et en divisant tout par ν_0 (ce qui est possible, puisque on suppose $(\nu_0 , p) = 1$), on peut se ramener au cas où $\nu_0 = 1$.

(a) $\alpha_0 \equiv \beta_0 \equiv \gamma_0 \equiv 0$.

$\alpha_1 \equiv 0$ s'écrit $\lambda_1 \equiv \lambda_0 \nu_1$.

$\alpha_2 \equiv 0$ s'écrit $2\lambda_2 - 2\lambda_0 \nu_2 \equiv 0$, ou, si $p \neq 2$, $\lambda_2 \equiv \lambda_0 \nu_2$.

Supposons que pour $0 , 1 , \ldots , i - 1$, on ait montré que $\lambda_t \equiv \lambda_0 \nu_t$. Alors $\alpha_i \equiv 0$ s'écrit

$$\sum_{k=0}^{i} (i - 2k)\nu_k \lambda_{i-k} \equiv 0 \ ,$$

ou

$$i\lambda_i - i\lambda_0 \nu_i + \sum_{1}^{i-1} (i - 2k)\nu_k \lambda_{i-k} \equiv 0$$

ou

$$i\lambda_i - i\lambda_0 \nu_i + \lambda_0 \sum_{1}^{i-1} (i - 2k)\nu_k \nu_{i-k} \equiv 0$$

ou

$$i\lambda_i - i\lambda_0 \nu_i \equiv 0 \ .$$

Donc, si $(i , p) = 1$, il faut $\lambda_i \equiv \lambda_0 \nu_i$. On a donc, pour $i = 1 , 2 , \ldots , p-1$

$$\lambda_i \equiv \lambda_0 \nu_i \ ,$$

et, pour $i = p$,

$$\alpha_p \equiv p\lambda_p - p\lambda_0\ \nu_p \equiv 0 , \qquad \forall\ \lambda_p \text{ et } \nu_p .$$

Si donc on suppose que, pour $t = 1 , 2 , \ldots , i$, avec $i \leqslant p - 1$, on a $\alpha_i \equiv 0$, on a aussi

$$\gamma_t = \langle \lambda_k \,|D_t + N_t|\, \mu_\ell \rangle \equiv \lambda_0 \langle \nu_k \,|D_t + N_t|\, \mu_\ell \rangle .$$

donc $\gamma_t \equiv \lambda_0\ \beta_t$ pour $t = 0 , 1 , \ldots , i$.

Pour $i = p$,

$$\gamma_p = \langle \lambda_k \,|D_p + N_p|\, \mu_\ell \rangle$$
$$\equiv \lambda_0 \langle \nu_k \,|D_p + N_p|\, \mu_\ell \rangle + \langle (0, \ldots , 0 , \lambda_p - \lambda_0\ \nu_p) |D_p + N_p|\, \mu_\ell \rangle$$

$$\gamma_p \equiv \lambda_0\ \beta_p - p(\lambda_p - \lambda_0\ \nu_p)\ \mu_0 \equiv \lambda_0\ \beta_p .$$

Le lemme est donc démontré pour $t = 0 , 1 , 2 , \ldots , p$.

(b) Supposons le donc vrai pour $t = 0 , 1 , \ldots , i$. Montrons alors que

$$\left\{ \begin{array}{l} \alpha_t \equiv 0 \quad \text{pour} \quad t = 0 , 1 , \ldots , i + p \\ \beta_t \equiv 0 \quad \text{pour} \quad t = 0 , 1 , \ldots , i \end{array} \right\} \Longrightarrow \gamma_{i+p} \equiv \lambda_0\ \beta_{i+p} .$$

Posons $\lambda'_t = \lambda_{p+t} - \lambda_0\ \nu_{p+t}$,

$\alpha_{t+p} \equiv 0$ pour $t = 0 , 1 , \ldots , i$ s'écrit $\langle \nu_k \,|D_{t+p}|\, \mu_\ell \rangle \equiv 0$.

Comme D_{t+p} est antisymétrique, $\langle \nu_k \,|D_{t+p}|\, \nu_\ell \rangle \equiv 0$, donc

$$\langle \nu_k \,|D_{t+p}|\, \lambda_\ell - \lambda_0\ \nu_\ell \rangle \equiv 0$$

ou encore

$$\langle (\nu_0 , \ldots , \nu_{t+p}) |D_{t+p}| (0 , \ldots , 0 , \lambda'_0 , \ldots , \lambda'_t) \rangle \equiv 0 ,$$

ou, comme tous les termes de D_{t+p} , sauf ceux de "l'antidiagonale", sont nuls :

$$\langle (\nu_0 , \ldots , \nu_t , 0 , \ldots , 0) |D_{t+p}| (0 , \ldots , 0 , \lambda'_0 , \ldots , \lambda'_t) \rangle \equiv 0 ,$$

ou encore, comme $d^{(t+p)}_{k,t+p-k} \equiv t + p - 2k \equiv t - 2k \equiv d^{(t)}_{k,t-k}$

$$\alpha'_t = \langle \nu_k \,|D_t|\, \lambda'_\ell \rangle \equiv 0 \qquad \text{pour} \quad t = 0 , 1 , \ldots , i .$$

Comme $\beta_t = \langle \nu_k \,|D_t + N_t|\, \mu_\ell \rangle \equiv 0$ pour $t = 0 , 1 , \ldots , i$, on déduit de l'hypothèse de récurrence que :

$$\langle \lambda'_k \,|D_t + N_t|\, \mu_\ell \rangle \equiv 0 \qquad \text{pour} \quad t = 0 , 1 , \ldots , i .$$

Or,

$$\begin{aligned} \gamma_{i+p} - \lambda_0 \beta_{i+p} &\equiv \langle \lambda_k \,|D_{i+p} + N_{i+p}|\, \mu_\ell \rangle - \lambda_0 \langle \nu_k \,|D_{i+p} + N_{i+p}|\, \mu_\ell \rangle \\ &\equiv \langle \lambda_k - \lambda_0 \nu_k \,|D_{i+p} + N_{i+p}|\, \mu_\ell \rangle \\ &\equiv \langle 0 , \ldots , 0 , \lambda'_0 , \ldots , \lambda'_t \,|D_{i+p} + N_{i+p}|\, \mu_\ell \rangle . \end{aligned}$$

$\langle (0 , \ldots , 0 , \lambda'_0 , \ldots , \lambda'_t) | D_{i+p} |\, \mu_\ell \rangle \equiv \langle \lambda'_k \,|D_i|\, \mu_\ell \rangle$ puisque tous les termes de D_{i+p} , sauf ceux de l'antidiagonale, sont nuls et que

$$d^{(i+p)}_{k+p,i+p-(k+p)} \equiv i + p - 2(k + p) \equiv i - 2k \equiv d^{(i)}_{k,i-k} .$$

$\langle (0,\ldots,0,\lambda'_0,\ldots,\lambda'_t) | N_{i+p} | \mu_\ell \rangle \equiv \langle (0,\ldots,0,\lambda'_0,\ldots,\lambda'_t) | N_{i+p} | (\mu_0,\ldots,\mu_t , 0,\ldots,0) \rangle$ (puisque $n^{(t+p)}_{k,\ell} \equiv 0$ pour $k + \ell \geqslant t + p$).

$$\equiv \langle \lambda'_k \,|N_i|\, \mu_\ell \rangle \qquad \text{puisque} \quad n^{(i+p)}_{k+p,\ell} \equiv n^{(i)}_{k,\ell} .$$

Finalement, $\gamma_{i+p} - \lambda_0 \beta_{i+p} \equiv \langle \lambda'_k \,|D_i + N_i|\, \mu_\ell \rangle \equiv 0$ et $\gamma_{i+p} \equiv \lambda_0 \beta_{i+p}$.

Q. E. D.

2.3.3. Démonstration du théorème 2.

(a) Soient, pour $i = 1 , 2 , 3 , \ldots , v_{i+1}$, $s_i \in G_1$ avec $\nu_G(s_i) = v_i$. Posons $s_i \pi = \pi_i$. π_i peut s'écrire $\pi_i = \pi + \pi^{v_i+1} \rho_i$ avec $\rho_i \in U_L$. Comme on a supposé $\overline{K}$ parfait :

1° Si Car K = 0 , il existe un sous-corps de L , k_L qui est le plus grand sous-corps absolument non ramifié de L . $L = k_L(\pi)$, le corps résiduel de k_L est $\overline{k}_L = \overline{L}$, $v_{k_L}(p) = 1$, $[L : k_L] = e e_0$.

On peut alors choisir un système R de représentants de $\overline{k}_L = \overline{L}$ dans k_L , contenant 0 , tel que

$$\forall\ \theta \in A_L , \qquad \theta = \sum_{k=0}^{\infty} a_k \pi^k , \qquad a_k \in R \subset k_L .$$

2° Si Car K = p , alors $A_L \simeq \overline{L}[[T]]$, et on peut choisir un système R de représentants de $\overline{L}$ dans A_L qui est un corps isomorphe à $\overline{L}$ tel que

$$\forall\ \theta \in A_L , \qquad \theta = \sum_{0}^{\infty} a_k \pi^k , \qquad a_k \in R .$$

Choisissons un tel système R et posons, pour $i = 1, 2, 3$,

$$\rho_i = \sum_0^\infty a_k^{(i)} \pi^k , \qquad a_k^{(i)} \in R .$$

On a, pour $i, j = 1, 2, 3$,

$$\nu_G(s_i s_j s_i^{-1} s_j^{-1}) = v_L(s_i s_j s_i^{-1} s_j^{-1} \pi' - \pi') - 1 ,$$

où π' est une uniformisante quelconque.

Prenons $\pi' = s_j s_i \pi$; $\nu_G(s_i s_j s_i^{-1} s_j^{-1}) = v_L(s_i s_j \pi - s_j s_i \pi) - 1$. Or $s_i s_j \pi = s_i(\pi + \pi^{v_j+1} \sum_{k=0}^\infty a_k^{(j)} \pi^k) = \pi_i + \sum_{k=0}^\infty a_k^{(j)} \pi_i^{v_j+1+k}$ (puisque s_i est continu).

$$s_i s_j \pi = \pi_i + \pi_j - \pi + \sum_{k=0}^\infty a_k^{(j)} (\pi_i^{v_j+1+k} - \pi^{v_j+1+k})$$

$$= \pi_i + \pi_j - \pi + \sum_{k=0}^\infty \pi^{v_j+1+k} a_k^{(j)} [(\frac{\pi_j}{\pi})^{v_j+1+k} - 1]$$

$$= \pi_i + \pi_j - \pi + \pi^{v_j+1} \sum_{k=0}^\infty a_k^{(j)} \pi^k [(1 + \pi^{v_i} \sum_{\ell=0}^\infty a_\ell^{(i)} \pi^\ell)^{v_j+1+k} - 1]$$

ou finalement

$$s_i s_j \pi = \pi_i + \pi_j - \pi + \pi^{v_i+v_j+1} r_{i,j} \tag{2}$$

avec $r_{i,j} \in A_L$ et

$$r_{i,j} = \frac{1}{\pi^{v_i}} \sum_{k=0}^\infty a_k^{(j)} \pi^k [(1 + \pi^{v_i} \sum_{\ell=0}^\infty a_\ell^{(i)} \pi^\ell)^{v_j+1+k} - 1] \tag{3}$$

On a donc

$$s_i s_j \pi - s_j s_i \pi = \pi^{v_i+v_j+1} (r_{i,j} - r_{j,i}) \tag{4}$$

et

$$\nu_G(s_i s_j s_i^{-1} s_j^{-1}) = v_i + v_j + v_L(r_{i,j} - r_{j,i}) . \tag{5}$$

(b) Calcul de $r_{i,j}$. - Posons $A_s^{(i,m)}$ = coefficient de π^s dans le développement de $(\sum_{k=0}^\infty a_k^{(i)} \pi^k)^m$.

(3) s'écrit encore

$$r_{i,j} = \Big(\sum_{\ell=0}^{\infty} a_\ell^{(i)} \pi^\ell\Big)\Big\{\sum_{k=0}^{\infty} a_k^{(j)} \pi^k\Big[v_j + 1 + k + \sum_{m=1}^{v_j+k} \pi^{mv_i}\binom{v_j + 1 + k}{m + 1}\Big(\sum_{\ell'=0}^{\infty} a_{\ell'}^{(i)} \pi^{\ell' m}\Big]\Big\}$$

$$= \Big(\sum_{\ell=0}^{\infty} a_\ell^{(i)} \pi^\ell\Big)\Big[\sum_{k=0}^{\infty} a_k^{(j)} \pi^k (v_j + 1 + k)\Big]$$

$$+ \Big(\sum_{\ell=0}^{\infty} a_\ell^{(i)} \pi^\ell\Big)\Big\{\sum_{k=0}^{\infty} a_k^{(j)} \pi^k\Big[\sum_{m=1}^{v_j+k} \pi^{mv_i}\binom{v_j + 1 + k}{m + 1}\Big(\sum_{n=0}^{\infty} a_n^{(i)} \pi^n\Big)^m\Big]\Big\}$$

ou

$$r_{i,j} = \sum_0^\infty \alpha_t^{(i,j)} \pi^t \qquad \text{avec} \quad \alpha_t^{(i,j)} = \langle a_k^{(j)} \,|D_t^{(i,j)} + P_t^{(i,j)}|\, a_\ell^{(i)} \rangle$$

avec $D_t^{(i,j)} = \langle d_{k,\ell}^{(t;i,j)} \rangle$;

$$\begin{cases} d_{k,\ell}^{(t;i,j)} = 0 & \text{si} \quad \ell \neq t - k \\ d_{k,t-k}^{(t;i,j)} = v_j + 1 + k \end{cases}$$

avec $P_t^{(i,j)} = \langle p_{k,\ell}^{(t;i,j)} \rangle$;

$$\begin{cases} p_{k,\ell}^{(t;i,j)} = 0 & \text{si} \quad k + \ell > t - v_i \\ p_{k,\ell}^{(t;i,j)} = \sum\limits_{m \geqslant 1} \binom{v_j + 1 + k}{m + 1} A_{t-mv_i-(k+\ell)}^{(i,m)} \end{cases}$$

(en particulier $P_t^{(i,j)} = 0$, pour $t < v_i$).

(c) <u>Calcul de</u> $r_{j,i} - r_{i,j}$. - On a donc $r_{j,i} - r_{i,j} = \sum\limits_0^\infty (\alpha_t^{(j,i)} - \alpha_t^{(i,j)})\pi^t$ avec

$$\alpha_t^{(j,i)} - \alpha_t^{(i,j)} = \langle a_k^{(j)} \,|\overline{D}_t^{(j,i)} - D_t^{(i,j)} + \overline{P}_t^{(j,i)} - P_t^{(i,j)}|\, a_\ell^{(i)} \rangle ,$$

en désignant par $\overline{P}$ la matrice transposée de la matrice P . Dans $\overline{D}_t^{(j,i)} - D_t^{(i,j)}$, tous les termes sont nuls sauf ceux de l'antidiagonale qui sont de la forme

$$(v_i + 1 + t - k) - (v_j + 1 + k) = v_i - v_j + t - 2k \equiv t - 2k \pmod p$$

puisque v_i et v_j étant des nombres propres de ramification, $v_i \equiv v_j \pmod p$.

Donc $\overline{D}_t^{(j,i)} - D_t^{(i,j)} \equiv D_t \pmod p$, où D_t est la matrice définie dans l'énoncé du lemme

Soit $v = \min(v_1 , v_3)$. On a

$$r_{3,1} - r_{1,3} \equiv \sum_0^{v-1} \alpha_t \pi^t \pmod{\mathfrak{p}_L^v} \qquad \text{avec} \quad \alpha_t = \alpha_t^{(3,1)} - \alpha_t^{(1,3)}$$

$$r_{3,2} - r_{2,3} \equiv \sum_0^{v-1} \beta_t \pi^t \pmod{\mathfrak{p}_L^v} \qquad \text{avec} \quad \beta_t = \alpha_t^{(3,2)} - \alpha_t^{(2,3)}$$

$$r_{1,2} - r_{2,1} \equiv \sum_0^{v-1} \gamma_t \pi^t \pmod{\mathfrak{p}_L^v} \qquad \text{avec} \quad \gamma_t = \alpha_t^{(1,2)} - \alpha_t^{(2,1)} \quad .$$

Pour connaître ces expressions $\pmod{\mathfrak{p}_L^v}$, il suffit de connaître α_t , β_t , γ_t modulo p .

[En effet, ou bien Car K = p , et ceci signifie qu'on les connaît complètement ; ou bien Car K = 0 , et alors $v_L(p) = e_0 e$ et v , étant un nombre propre de ramification, correspond à une extension à filtration triviale d'un corps strictement contenu dans L , L en étant une extension complètement surramifiée. Ce corps a donc un indice de ramification absolu $\leqslant \frac{e_0 e}{p}$, $v \leqslant \frac{e_0 e}{p} \cdot \frac{p}{p-1} = \frac{e_0 e}{p-1} = \frac{v_L(p)}{p-1}$, et $v_L(p) \geqslant (p-1)v \geqslant v$, donc $p \in \mathfrak{p}_L^v$.]

Compte tenu de ce que $P_t^{(i,j)} = 0$ pour $t < v_i$, on peut alors écrire, pour $t = 0 , 1 , \ldots , v - 1$,

$$\alpha_t \equiv \langle a_k^{(3)} \, | D_t | \, a_\ell^{(1)} \rangle \pmod p$$

$$\beta_t \equiv \langle a_k^{(3)} \, | D_t + N_t | \, a_\ell^{(2)} \rangle \pmod p$$

$$\gamma_t \equiv \langle a_k^{(1)} \, | D_t + N'_t | \, a_\ell^{(2)} \rangle \pmod p$$

en posant $N_t = \langle n_{j,k}^{(t)} \rangle = - P_t^{(2,3)}$ et $N'_t = \langle n'^{(t)}_{j,k} \rangle = - P_t^{(2,1)}$.

De plus :

(i) $$n_{k,\ell}^{(t)} = - p_{k,\ell}^{(t;2,3)} = - \sum_{m=1}^{[(t-(k+\ell))/v_2]} \binom{v_3 + 1 + k}{m + 1} A_{t-mv_2-(k+\ell)}^{(2,m)}$$

$$n'^{(t)}_{k,\ell} = - p_{k,\ell}^{(t;2,1)} = - \sum_{m=1}^{[(t-(k+\ell))/v_2]} \binom{v_1 + 1 + k}{m + 1} A_{t-mv_2-(k+\ell)}^{(2,m)}$$

et si $\binom{v_3 + 1 + k}{m + 1} \equiv \binom{v_1 + 1 + k}{m + 1}$, $\forall\, m = 1 , \ldots , [\frac{t - (k + \ell)}{v_2}]$, on a $n_{k,\ell}^{(t)} \equiv n'^{(t)}_{k,\ell} \pmod p$.

Si on pose $v_3 - v_1 = \lambda p^r$ avec $(\lambda , p) = 1$, on voit que

$$(1 + x)^{v_3+1+k} = (1 + x)^{v_1+1+k} (1 + x)^{\lambda p^r} \equiv (1 + x)^{v_1+1+k} (1 + x^{p^r})^{\lambda} \pmod p$$

donc

$$\sum \binom{v_3 + 1 + k}{m + 1} x^{m+1} \equiv \sum \binom{v_1 + 1 + k}{m + 1} x^{m+1} + \lambda x^{p^r} + \dots$$

et

$$\binom{v_3 + 1 + k}{m + 1} \equiv \binom{v_1 + 1 + k}{m + 1} \qquad \text{tant que } m < p^r - 1$$

et

$$\binom{v_3 + 1 + k}{(p^r - 1) + 1} \equiv \binom{v_1 + 1 + k}{(p^r - 1) + 1} + \lambda .$$

Donc, pour $t < (p^r - 1)v_2$, on a $[\frac{t - (k + \ell)}{v_2}] \leqslant \frac{t}{v_2} < p^r - 1$ et $N_t \equiv N'_t$ pour $t = 0 , 1 , \dots , (p^r - 1)v_2 - 1$.

Pour $t = (p^r - 1)v_2$, $n_{k,\ell}^{(p^r-1)v_2} \equiv n'^{(p^r-1)v_2}_{k,\ell}$ sauf si $k + \ell = 0$, auquel cas on a

$$n'^{(p^r-1)v_2}_{0,0} = n_{0,0}^{(p^r-1)v_2} + \lambda A_0^{(2,(p^r-1))} ,$$

$$n'^{(p^r-1)v_2}_{0,0} \equiv n_{0,0}^{(p^r-1)v_2} + \lambda a_0^{(2)} p^r - 1 . \tag{6}$$

(ii) Un calcul analogue montre que $n_{k,\ell}^{(t)} \equiv n_{k-p,\ell}^{(t-p)} \pmod p$ tant que $m < p - 1$, c'est-à-dire tant que $[\frac{t - (k + \ell)}{v_2}] < p - 1$. Or, $k \geqslant p \implies [\frac{t - (k + \ell)}{v_2}] \leqslant \frac{t - p}{v_2}$.

On a donc $n_{k,\ell}^{(t)} \equiv n_{k-p,\ell}^{(t-p)} \pmod p$, $\forall\ k \geqslant p$ pour $t < (p - 1)v_2 + p$.

(d) Fin de la démonstration du théorème 2. - Pour $j < n_0$, les α_t , β_t et γ_t vérifient les définitions du lemme.

Supposons alors que s_1 , s_2 , s_3 vérifient les hypothèses du théorème. On a alors

$$\sum_0^{n-1} \alpha_t \pi^t \equiv 0 \pmod{\mathfrak{p}_L^n} . \tag{7}$$

Les α_t sont des expressions polynomiales des $a_k^{(i)}$ à coefficients dans le corps premier de L . Donc :

(i) Si Car K = 0 , $a_k^{(i)} \in R \subset k_L$ et $\alpha_t \in k_L$. Donc

$$\alpha_t \equiv 0 \pmod{\mathfrak{p}_L} \iff \alpha_t \equiv 0 \pmod{p} . \tag{8}$$

(ii) Si Car K = p , $a_k^{(i)} \in R$ et R est un corps, donc $\alpha_t \in R$. Or, le seul élément de R , congru à 0 modulo $\mathfrak{p}_L$, est 0 . Donc, ici encore,

$$\alpha_t \equiv 0 \pmod{\mathfrak{p}_L} \iff \alpha_t \equiv 0 \pmod{p} . \tag{8}$$

La formule (8), toujours valable, appliquée à (7), compte tenu de ce que $p \in \mathfrak{p}_L^n$, montre que $\alpha_t \equiv 0 \pmod{p}$, $\forall\ t = 0 , 1 , \dots , n - 1$.

Le même raisonnement s'applique aux β_t , et on en déduit que $\beta_t \equiv 0 \pmod{p}$, $\forall\ t = 0 , 1 , \dots , n - 1$.

Il résulte alors du lemme, en prenant $\lambda_k = a_k^{(1)}$, $\mu_k = a_k^{(2)}$, $\nu = a_k^{(3)}$, que $\gamma_t \equiv 0 \pmod{p}$ pour $t = 0 , 1 , 2 , \dots , n - 1$, donc que

$$\sum_0^{n-1} \gamma_t \pi^t \equiv 0 \pmod{\mathfrak{p}_L^n} ,$$

ce qui compte tenu de (5), démontre le théorème 2.

Q. E. D.

(e) Fin de la démonstration de la proposition 6. - Dans le cas où l'on prend $v_3 = v_M$ et où $(p - 1)v_2 < v_1$, le lemme s'applique encore à l'ordre $(p - 1)v_2$:

- si $r > 1$, c'est-à-dire si $v_M \equiv v_1 \pmod{p^2}$, $N'_{(p-1)v_2} = N_{(p-1)v_2}$ et $\gamma_{(p-1)v_2} \equiv 0$, ce qui entraîne que $\theta_{v_1+pv_2}(s_1\ s_2\ s_1^{-1}\ s_2^{-1}) = 0$. On peut écrire

$$\theta_{v_1+pv_2} = \frac{v_M - v_1}{p}\, \theta_{v_1}(s_1)\, \theta^p_{v_2}(s_2) . \tag{9}$$

- si $r = 1$, on a

$$\gamma_{(p-1)v_2} \equiv \langle a_k^{(1)} \,|D_{(p-1)v_2} + N_{(p-1)v_2}|\, a_\ell^{(2)} \rangle + a_0^{(1)} (n'^{(p-1)v_2}_{0,0} - n^{(p-1)v_2}_{0,0})\, a_0^{(2)}$$
$$\equiv \lambda a_0^{(1)}\, a_0^{(2)p} \not\equiv 0 \qquad \text{si } a_0^{(1)} \text{ et } a_0^{(2)} \text{ sont différents de } 0 ,$$

donc $\nu_G(s_1\ s_2\ s_1^{-1}\ s_2^{-1}) = v_1 + v_2 + (p - 1)v_2 = pv_2 + v_1$.

De plus,

$$\frac{s_1\,\pi}{\pi} \equiv 1 + a_0^{(1)}\, \pi^{v_1} \pmod{\mathfrak{p}_L^{v_1+1}} \qquad \text{et} \qquad \frac{s_2\,\pi}{\pi} \equiv 1 + a_0^{(2)}\, \pi^{v_2} \pmod{\mathfrak{p}_L^{v_2+1}}$$

entraînent

$$\frac{s_1\, s_2\, \pi - s_2\, s_1\, \pi}{\pi} \equiv \lambda a_0^{(1)}\, a_0^{(2)} p\, \pi^{pv_2+v_1} \pmod{\mathfrak{p}_L^{pv_2+v_1+1}} .$$

Si on applique ceci à $\pi' = s_1^{-1}\, s_2^{-1}\, \pi$

$$s_1\, \pi' = s_1\, s_1^{-1}\, s_2^{-1}\, \pi = s_2^{-1}\, \pi ,$$

et on vérifie facilement que si

$$\frac{s_1\, \pi}{\pi} \equiv 1 + a\pi^{v_1} \pmod{\mathfrak{p}_L^{v_1+1}} \qquad \text{et} \qquad \frac{s_2\, \pi}{\pi} \equiv 1 + b\pi^{v_2} \pmod{\mathfrak{p}_L^{v_2+1}}$$

on a $a \equiv a_0^{(1)}$ et $b \equiv a_0^{(2)}$.

Comme $\dfrac{s_1\, s_2\, \pi' - s_2\, s_1\, \pi'}{\pi} = \dfrac{s_1\, s_2\, s_1^{-1}\, s_2^{-1}\, \pi - \pi}{\pi} \times \dfrac{\pi}{\pi'}$ et $\dfrac{\pi}{\pi'} \equiv 1 \pmod{\mathfrak{p}_L}$, on en déduit que

$$\frac{s_1\, s_2^{-1}\, s_1^{-1}\, s_2^{-1}\, \pi}{\pi} \equiv 1 + \lambda a b^p\, \pi^{pv_2+v_1} \pmod{\mathfrak{p}_L^{pv_2+v_1+1}} .$$

Il suffit alors de passer au quotient pour obtenir la formule (9).

Q. E. D.

2.3.4. Remarques et exemples d'applications.

(a) Remarque : Dans le cas où on ne suppose pas $\overline{K}$ parfait, et où on ne fait que l'hypothèse (S), si Car K = 0 (resp. p), le corps k_L (resp. R) n'existe pas nécessairement. On peut cependant faire le même calcul modulo $\mathfrak{p}_{K_0} = \mathfrak{p}_K$ au lieu de modulo p . Mais alors, il faut remplacer $v_L(p) = e_{L/k_L} = ee_0$ ou $+\infty$ par $e_{L/K_0} = e_{L/K} = e = v_L(\pi_K)$, et il se peut que l'on ait $e < v(i)$. Il faut donc rajouter e dans l'énumération des limitations imposées à n .

(b) La proposition 6 reste vraie si l'on remplace v_M par $v > v_1$ et appartenant à l'ensemble des nombres de ramification des éléments de Z_{G_1} , centre du groupe de ramification. Comme la formule (9) doit toujours donner le même résultat, on peut énoncer :

COROLLAIRE 1. - S'il existe deux nombres propres de ramification v_1 et v_2 tels que $(p-1)v_2 < v_1$, les nombres de ramification des éléments du centre du groupe de ramification, supérieurs ou égaux à v_1 sont congrus entre eux modulo p^2

$(\forall\, s\, ,\, s' \in Z_{G_1}\, ,\ v_G(s) \geqslant v_1\, ,\ v_G(s') \geqslant v_1 \implies v_G(s) \equiv v_G(s') \pmod{p^2})$.

En particulier :

COROLLAIRE 2. - Si l'extension L/K est abélienne et si v_0 est le plus petit nombre propre de ramification de L/K, $\forall\ s, s' \in G$ avec $\nu_G(s), \nu_G(s') \geq (p-1)v_0$ on a $\nu_G(s) \equiv \nu_G(s') \pmod{p^2}$.

Par exemple, si 1 est un nombre de ramification de l'extension L/K, on voit que tous les nombres propres de ramification des éléments du centre (dans le cas abélien $Z_G = G$), sauf peut-être éventuellement 1 lui-même, sont congrus entre eux modulo p^2.

(c) Si l'on se donne une suite R finie d'entiers positifs, pour qu'il existe une extension du type L/K telle que R soit l'ensemble des nombres propres de ramification de l'extension, il est nécessaire que $\forall\ v, v' \in R$, $v \equiv v' \pmod{p}$. La proposition 6 montre que ceci n'est pas suffisant.

En particulier, si $1 \in R$ et si $v_M = \ell p + 1$, alors si $v_i = ip + 1 \in R$, il faut aussi que $v_j = jp + 1 \in R$, $\forall\ j = i, i+1, \ldots, i+s$, où s est le reste de la division par p de $\ell - i$.

Par exemple, si $1 \in R$, $p+1 \in R$ et $v_M = (p-1)p + 1$, on voit qu'il faut $R = \{ip + 1 ;\ i = 0, 1, \ldots, p-1\}$.

(d) Soit $\sigma \in G_i/G_{i+1}$. Soit s un représentant de σ dans G_i. Il résulte du paragraphe 1.2.2 (Prop. 3, Cor. 1) que l'application θ_i' de G_i/G_{i+1} dans $\overline{L}$ définie par $\theta_i'(\sigma) = \overline{[\frac{1}{i}(\frac{s\pi}{\pi} - 1)]}$ est un isomorphisme de G_i/G_{i+1} sur le groupe additif des racines de $\overline{P}(x)$.

On déduit alors immédiatement de la formule (1) de la proposition 6, le corollaire suivant :

COROLLAIRE 3. - Soient i et j deux nombres de ramification tels que $(p-1)j < i$. Soient $\sigma \in G_i/G_{i+1}$, $\tau \in G_j/G_{j+1}$. Soit s (resp. t) un représentant de σ (resp. τ) dans G. Soit ρ_τ (resp. ρ'_σ) l'application de G_i/G_{i+1} (resp. G_j/G_{j+1}) dans G_{i+pj}/G_{i+pj+1} qui, à σ (resp. τ) fait correspondre la classe de $sts^{-1}t^{-1}$. Cette définition a toujours un sens et cette application est :

- l'application nulle, si $i \equiv v_M \pmod{p^2}$ ou si σ (resp. τ) $= 1$;

- sinon, un isomorphisme de G_i/G_{i+1} (resp. G_j/G_{j+1}) sur un sous-groupe de G_{i+pj}/G_{i+pj+1} et si $\sigma \neq \sigma'$, $\rho'_\sigma \neq \rho'_{\sigma'}$; si $\tau \neq \tau'$, $\rho_\tau \neq \rho_{\tau'}$.

[La dernière affirmation provient du fait que l'application $b \to b^p$ est un isomorphisme du groupe des racines de $\overline{P}(x)$ sur un sous-groupe additif de $\overline{K}$.]

(e) Soit, pour $i \geqslant 1$, $p^{k_i} = \mathrm{Ord}(G_i/G_{i+1})$. On a $\sum_1^\infty k_i = k$ et $k_i \neq 0 \Longleftrightarrow i \in R$. Comme p^{k_i} est aussi l'ordre d'un sous-groupe additif de $\overline{K}$, si $\overline{K}$ est fini, on doit avoir $k_i \leqslant f_0$, $\forall\, i$.

Le corollaire 3 montre que ces conditions sur les k_i ne sont pas suffisantes. Si i et j sont deux nombres propres de ramification tels que $(p-1)j < i$ et si $i \not\equiv v_M \pmod{p^2}$, il faut aussi que $k_{pj+i} \geqslant \max(k_i, k_j)$.

(f) La restriction $(p-1)j < i$ dans la proposition 6 qui provient de $n_0 \leqslant v_1$ dans le théorème 2 semble être trop forte. Mais alors la même démonstration ne s'applique plus car on ne peut plus exprimer linéairement les $(p-1)$-premiers $a_j^{(1)}$ en fonction des $a_j^{(3)}$.

BIBLIOGRAPHIE

[1] BOURBAKI (Nicolas). - Algèbre commutative. Chapitre 3 : Graduations, filtrations et topologies. - Paris, Hermann, 1961 (Act. scient. et ind., 1293 ; Bourbaki, 28).

[2] BOURBAKI (Nicolas). - Algèbre commutative. Chapitre 6 : Valuations. - Paris, Hermann, 1964 (Act. scient. et ind., 1308 ; Bourbaki, 30).

[3] HASSE (Helmut). - Zahlentheorie, 2te Auflage. - Berlin, Akademie-Verlag, 1963.

[4] KRASNER (Marc). - Sur la primitivité des corps p-adiques. Mathematica, Cluj, t. 13, 1937, p. 72-191.

[5] KRASNER (Marc). - La loi de Jordan-Hölder dans les hypergroupes et les suites génératrices des corps de nombres p-adiques, Duke math. J., t. 6, 1940, p. 120-140 et t. 7, 1940, p. 121-135.

[6] ÖRE (Öystein). - Abriss einer arithmetischen Theorie der Galoisschen Körper, Math. Annalen, t. 100, 1928, p. 650-673.

[7] SERRE (Jean-Pierre). - Corps locaux. - Paris, Hermann, 1962 (Act. scient. et ind., 1296 ; Publ. Inst. Math. Univ. Nancago, 8).

[8] SPEISER (Andreas). - Die Zerlegungsgruppe, J. für die reine und angew. Math., t. 149, 1919, p. 174-188.