Séminaire Delange-Pisot-Poitou. Théorie des nombres

Jean-Marc Fontaine

Un résultat de Sen sur les automorphismes dans les corps locaux

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 11, n° 1 (1969-1970), exp. n° 6, p. 1-13

<http://www.numdam.org/item?id=SDPP_1969-1970__11_1_A3_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
11e année, 1969/70, n° 6, 13 p.

15 décembre 1969

UN RÉSULTAT DE SEN SUR LES AUTOMORPHISMES DANS LES CORPS LOCAUX

par Jean-Marc FONTAINE

Dans [3], Shankar SEN établit un résultat, conjecturé par GROTHENDIECK, qui généralise le théorème de Hasse-Arf pour les extensions cycliques. La première partie de cet exposé est consacrée à la démonstration de ce théorème. C'est donc un démarquage des premières pages de [3].

Dans la deuxième partie, on énonce, sans démonstration, un certain nombre de résultats sur les automorphismes dans les corps locaux qui précisent le théorème de Sen. Dans la troisième partie, on démontre l'un de ces résultats.

1. Généralisation du théorème de Hasse-Arf.

Soit K un corps local, c'est-à-dire un corps muni d'une valuation discrète pour laquelle il est complet. Soit A l'anneau des entiers de K, soit M l'idéal maximal de A, et soit $k = A/M$ le corps résiduel. On suppose que k est de caractéristique p non nulle. On note v la valuation de K normalisée de telle sorte que $v(K) = \mathbb{Z}$.

Supposons, pour le moment, k parfait. Soit σ un automorphisme sauvagement ramifié de K, c'est-à-dire un automorphisme de K tel que $v((\sigma - 1)x) > 1$ pour tout x dans A. On est dans l'un des deux cas suivants :

Ou bien la caractéristique de K est nulle. L'anneau A est alors une extension finie totalement ramifiée de $W(k)$, anneau des vecteurs de Witt à coefficients dans K. L'automorphisme σ induit l'identité sur k ; on en déduit que la restriction de σ à $W(k)$ est l'identité et, par conséquent, que σ est d'ordre fini.

Ou bien la caractéristique de K est p. Le corps K est alors isomorphe à un corps de séries formelles sur k, et σ peut être d'ordre fini ou infini.

Dans les deux cas, il existe une section multiplicative f, et une seule, de k dans A. Comme σ induit l'identité sur k, σf est encore une section de k dans A. Comme σf est une application multiplicative, on voit que σf est encore une section multiplicative de k dans A, et, d'après l'unicité de cette section, on a $\sigma f = f$. Si on pose $C = f(k)$, on voit que σ vérifie la propriété :

(S) Il existe un système de représentants C de k dans A, contenant 0, tel que $\sigma c = c$, pour tout c dans C.

C'est, en fait, la seule propriété que l'on utilisera et, dans toute la suite de ce paragraphe, K est un corps local dont le corps résiduel est de caractéristique p non nulle, et σ est un automorphisme de K vérifiant (S). Il est clair que, pour tout entier μ, σ^μ vérifie aussi (S).

Soit π une uniformisante de l'anneau des entiers A de K (c'est-à-dire un élément dont la valuation est égale à 1). On pose

$$(1) \qquad i(\sigma) = \begin{cases} v((\sigma - 1)\pi/\pi) , & \text{si } \sigma \neq 1 , \\ +\infty , & \text{si } \sigma = 1 . \end{cases}$$

Si π' est une autre uniformisante de A, elle est de la forme $\pi' = \sum_1^\infty c_\mu \pi^\mu$, avec $c_\mu \in C$, et $c_1 \neq 0$. On a

$$v((\sigma - 1)\pi) = i(\sigma) + 1 ,$$

tandis que

$$v((\sigma - 1)\pi^\mu) > v((\sigma - 1)\pi) , \qquad \text{pour } \mu > 1 .$$

On en déduit que $i(\sigma)$ est indépendant du choix de π.

Si $\sigma(\pi) \equiv \pi + a\pi^{i+1} \pmod{M^{i+2}}$, avec $a \in C$, on voit que, pour tout entier μ, $\sigma^\mu(\pi) \equiv \pi + \mu a\pi^{i+1} \pmod{M^{i+2}}$. Par conséquent :

On a $i(\sigma^\mu) = i(\sigma)$ si p ne divise pas μ. Plus généralement, soit $p^{0(\mu)}$ la plus grande puissance de p qui divise μ ; en appliquant ce qui précède à $\sigma^{p^{0(\mu)}}$, on voit que $i(\sigma^\mu)$ ne dépend que de $0(\mu)$.

On a $i(\sigma^\mu) > i(\sigma)$ si p divise μ, et, plus généralement, $i(\sigma^{\mu'}) > i(\sigma^\mu)$ si $0(\mu') > 0(\mu)$ en appliquant ceci à $\sigma^{p^{0(\mu)}}$.

Si on pose $i(\sigma^\mu) = i_{0(\mu)}$, on obtient ainsi une suite d'entiers positifs

$$(2) \qquad i_0 < i_1 < i_2 < \ldots < i_n < \ldots ,$$

strictement croissante tant que $i_n \neq +\infty$; on l'appelle <u>la suite des nombres de ramification de l'automorphisme</u> σ. Le théorème de Hasse-Arf se généralise de la manière suivante (ce résultat n'était connu que pour σ d'ordre fini) :

THÉORÈME 1. - <u>Soit</u> σ <u>un automorphisme de</u> K <u>vérifiant</u> (S). <u>Pour tout entier</u> n <u>strictement positif, on a</u>

$$(3) \qquad i(\sigma^{p^{n-1}}) \equiv i(\sigma^{p^n}) \pmod{p^n}$$

((3) <u>signifie que, ou bien les deux membres sont finis et la congruence est satisfaite, ou bien l'un des deux membres au moins est infini</u>).

Avant de démontrer ce théorème, nous allons établir trois lemmes.

LEMME 1. - Pour tout entier μ dans $\mathbb{Z}$, il existe un élément x_μ de K tel que $v(x_\mu) = \mu$, et $v((\sigma - 1)x_\mu) = \mu + i(\sigma^\mu)$.

Démonstration. - Soit π une uniformisante de A. Si $\mu \geqslant 0$, posons

$$x_\mu = \prod_{i=0}^{\mu-1} \sigma^i(\pi) \quad .$$

On a $v(x_\mu) = \mu$. D'autre part, $\sigma(x_\mu)/x_\mu = \sigma^\mu(\pi)/\pi$, donc

$$(\sigma - 1)x_\mu = x_\mu.(\sigma^\mu - 1)\pi/\pi \qquad \text{et} \qquad v((\sigma - 1)x_\mu) = \mu + i(\sigma^\mu) \quad .$$

Si $\mu < 0$, il suffit de poser $x_\mu = 1/x_{-\mu}$.

LEMME 2. - Tout élément x de K peut s'écrire sous la forme

$$x = \sum_{\mu=v(x)}^{+\infty} x_\mu \quad , \tag{4}$$

expression dans laquelle chaque x_μ, ou bien a la propriété du lemme 1, ou bien est nul.

Démonstration. - Il est clair que tout x de K peut s'écrire sous la forme $x = \sum_{\mu \geqslant v(x)} c_\mu x_\mu$, où chaque x_μ a la propriété du lemme 1, et où chaque c_μ est dans C. Il résulte alors de la propriété (S) que chaque $c_\mu x_\mu$ vérifie bien les conditions exigées de x_μ dans l'énoncé du lemme.

LEMME 3. - Soit n un entier strictement positif tel que $i_{n-1} = i(\sigma^{p^{n-1}})$ soit fini. Si, pour tout entier j strictement compris entre 0 et n, les congruences $i_{j-1} \equiv i_j \pmod{p^j}$ sont satisfaites, alors les entiers $\mu + i(\sigma^\mu)$, avec $0(\mu) < n$, sont tous distincts. Ils sont aussi différents de i_{n-1}.

Démonstration.

Si $0(\lambda) = 0(\mu)$, alors $i(\sigma^\lambda) = i(\sigma^\mu)$; donc, si $\lambda + i(\sigma^\lambda) = \mu + i(\sigma^\mu)$, $\lambda = \mu$.

Si $0(\lambda) \neq 0(\mu)$, alors $0(\lambda - \mu) = \min\{0(\lambda), 0(\mu)\}$. Or, par hypothèse, $0(i(\sigma^\lambda) - i(\sigma^\mu)) > \min\{0(\lambda), 0(\mu)\}$ si ce minimum est strictement inférieur à n. On a donc $\lambda + i(\sigma^\lambda) \neq \mu + i(\sigma^\mu)$.

Si $0(\mu) < n$, alors $0(i_{n-1} - i(\sigma^\mu)) > 0(\mu)$ et $i_{n-1} - i(\sigma^\mu) \neq \mu$.

Démonstration du théorème 1. - On procède par récurrence. Supposons que, pour tout automorphisme τ de K vérifiant (S), et pour tout entier j strictement compris entre 0 et n, on ait

$$i(\tau^{p^{j-1}}) \equiv i(\tau^{p^j}) \pmod{p^j} .$$

Supposons qu'en revanche il existe un automorphisme σ de K vérifiant (S) tel que $i(\sigma^{p^{n-1}}) \not\equiv i(\sigma^{p^n}) \pmod{p^n}$. On va en déduire une contradiction.

L'hypothèse de récurrence appliquée à σ^p montre que $i_{n-1} \equiv i_n \pmod{p^{n-1}}$. On en déduit que, si on pose $s = i_{n-1} - i_n$, on a $0(s) = n - 1$. Le lemme 1, appliqué à l'automorphisme σ^p et à l'entier s, montre qu'il existe un élément z de K tel que $v(z) = s$ et $v((\sigma^p - 1)z) = s + i(\sigma^{ps}) = s + i_n = i_{n-1}$.

Soit $x = (1 + \sigma + \ldots + \sigma^{p-1})z$. On a $1 + \sigma + \ldots + \sigma^{p-1} \equiv (\sigma - 1)^{p-1} \pmod{p}$. Comme, pour tout élément u de K, $v((\sigma - 1)u) > v(u)$, on voit que $v(x) > v(z) = s$. Posons $y = (\sigma - 1)x$. On a $y = (\sigma^p - 1)z$; donc $v(y) = i_{n-1}$.

Appliquons le lemme 2 à x. On a

$$x = \sum_{\mu=v(x)}^{+\infty} x_\mu , \qquad \text{avec } v(x_\mu) = \mu \text{ ou } x_\mu = 0 .$$

Posons $y_\mu = (\sigma - 1)x_\mu$. Alors

$$y = \sum y_\mu , \qquad \text{avec } v(y_\mu) = \mu + i(\sigma^\mu) , \quad \text{si } x_\mu \text{ n'est pas nul} .$$

On peut encore écrire

$$y = \sum_{0(\mu) \geqslant n} y_\mu + \sum_{0(\mu) < n} y_\mu .$$

Pour $0(\mu) \geqslant n$, $v(y_\mu) = \mu + i_{0(\mu)} \geqslant \mu + i_n > s + i_n = i_{n-1}$ car, si y_μ n'est pas nul, μ est strictement supérieur à s puisque $v(x) > s$.

On doit donc avoir $v\left(\sum_{0(\mu)<n} y_\mu\right) = i_{n-1}$. Dans cette somme les $v(y_\mu) = \mu + i(\sigma^\mu)$, pour x_μ non nul, sont tous distincts d'après la première partie du lemme 3. La valuation de la somme est donc égale au minimum des $\mu + i(\sigma^\mu)$ pour $0(\mu) < n$ et x_μ non nul. Il doit donc exister un entier μ vérifiant $0(\mu) < n$ tel que $\mu + i(\sigma^\mu) = i_{n-1}$, ce qui contredit la deuxième partie du lemme 3.

C. Q. F. D.

2. Propriétés des nombres de ramification (énoncé de résultats).

Avec les notations du paragraphe précédent, si σ est un automorphisme de K vérifiant (S), et si on pose

$$(5)\qquad \begin{cases} u_0 = i_0 \ , \\ u_n = i_0 + (i_1 - i_0)/p + \ldots + (i_n - i_{n-1})/p^n \ , \quad \text{pour} \quad n \in \underset{\sim}{N} - \{1\} \ , \end{cases}$$

le théorème 1 revient à dire que les u_n sont des entiers rationnels. La suite

$$(6)\qquad u_0 < u_1 < u_2 < \ldots < u_n < \ldots$$

s'appelle la suite des nombres supérieurs de ramification de σ. La connaissance des i_n est équivalente à celle des u_n.

Etant donnée une suite strictement croissante d'entiers positifs, on peut se demander à quelle condition il existe un automorphisme σ de K vérifiant la condition (S) dont c'est la suite des nombres supérieurs de ramification. Pour plus de commodité, nous supposerons désormais que le corps résiduel k de K est parfait. Tous les automorphismes envisagés vérifieront (S), ce qui revient alors à dire qu'ils sont sauvagement ramifiés.

Lorsque le corps local K est de caractéristique 0, les automorphismes sauvagement ramifiés sont d'ordre fini, et le problème peut se ramener à celui de la détermination des nombres de ramification des p-extensions cycliques totalement ramifiées des corps locaux de caractéristique 0. Cette détermination a été étudiée par E. MAUS ([2], § 6).

Lorsque K est de caractéristique $p \neq 0$, c'est-à-dire lorsque K est un corps de séries formelles, il existe des automorphismes d'ordre fini, et d'autres d'ordre infini. On peut démontrer les résultats suivants.

PROPOSITION 2.1. - Soit

$$(6')\qquad u_0 < u_1 < \ldots < u_{n-1} < u_n$$

une suite finie croissante d'entiers strictement positifs. Pour qu'il existe un automorphisme sauvagement ramifié d'ordre fini de K, dont la suite (6') soit la suite des nombres supérieurs de ramification, il faut et il suffit que les conditions suivantes soient réalisées :

$$(P)\qquad \begin{cases} \text{(i)} \quad u_0 \not\equiv 0 \pmod{p} \ ; \\ \text{(ii) pour} \quad j = 1 \ , \ 2 \ , \ \ldots \ , \ n \ , \quad u_j = p u_{j-1} \\ \qquad\qquad\qquad\qquad \text{ou} \quad u_j > p u_{j-1} \quad \text{et} \quad u_j \not\equiv 0 \pmod{p} \ . \end{cases}$$

Soit $\Gamma_S(K)$ le groupe des automorphismes sauvagement ramifiés de K. Si σ et τ sont des éléments de $\Gamma_S(K)$, on pose

$$d(\sigma , \tau) = i(\sigma\tau^{-1}) \quad . \tag{7}$$

On vérifie facilement que, si π est une uniformisante de K,

$$d(\sigma , \tau) = v(\sigma\pi - \tau\pi) - 1 \quad .$$

L'application d a toutes les propriétés d'une distance, et munit $\Gamma_S(K)$ d'une structure de groupe ultramétrique complet. On a alors les résultats suivants.

PROPOSITION 2.2. - Soit σ un automorphisme sauvagement ramifié de K d'ordre infini. Pour que σ soit limite d'automorphismes d'ordre fini, il faut et il suffit que les nombres supérieurs de ramification de σ vérifient (P) pour tout n.

PROPOSITION 2.3. - Soit

$$u_0 < u_1 < u_2 < \ldots < u_n < \ldots \tag{6"}$$

une suite infinie croissante d'entiers strictement positifs. Pour qu'il existe un automorphisme σ sauvagement ramifié de K, qui soit limite d'automorphismes d'ordre fini tel que la suite (6") soit la suite des nombres supérieurs de ramification de σ, il faut et il suffit que, pour tout n, u_n vérifie (P).

PROPOSITION 2.4. - Supposons $p \neq 2$. Soit σ un automorphisme sauvagement ramifié de K qui n'est pas limite d'automorphismes d'ordre fini. Soit n_0 le plus petit entier positif tel que le nombre supérieur de ramification u_{n_0} de σ ne vérifie pas (P). Alors, il existe un entier positif e tel que, pour tout entier n strictement supérieur à n_0, les nombres supérieurs de ramification de σ vérifient $u_{n+1} - u_n = e$.

Soit E un corps local dont le corps résiduel est de caractéristique p. Soit $(F_n)_{n\in\mathbb{N}}$ une famille d'extensions galoisiennes de E telle que :

Pour tout n, F_n/E est une extension cyclique totalement ramifiée de degré p^n ;

Pour tout n, F_n est contenue dans F_{n+1}.

Soit $F = \bigcup_1^\infty F_n$. L'extension F/E s'appelle une Γ-extension totalement ramifiée. On peut définir la suite des nombres supérieurs de ramification

$$u_0 < u_1 < u_2 < \ldots < u_n < \ldots$$

d'une telle extension. C'est une suite strictement croissante d'entiers positifs.

Si on cherche à quelles conditions il existe une Γ-extension totalement ramifiée d'un corps local E, dont la suite des nombres supérieurs de ramification soit une suite donnée, on trouve :

Si E est de caractéristique p, les conditions de la proposition 2.3 ;

Si E est de caractéristique 0, des conditions analogues à celles de la proposition 2.4 : il doit exister un entier n_0 tel que la suite des u_n vérifie les conditions de la proposition 2.4, l'entier e n'étant plus arbitraire mais désignant l'indice de ramification absolu de E ; de plus, u_{n_0} et u_{n_0+1} doivent remplir certaines conditions supplémentaires (cf. [2], § 6, et [5]). C'est ce qui fait l'intérêt du théorème suivant.

THÉORÈME 2. - *Soit E un corps local à corps résiduel fini contenu dans le corps résiduel de K. Soit F une Γ-extension totalement ramifiée de E. Alors il existe un automorphisme sauvagement ramifié σ de K, dont la suite des nombres supérieurs de ramification est la même que celle de l'extension F/E.*

En fait, il paraît raisonnable de penser que les conditions suffisantes de la proposition précédente sont aussi nécessaires. Dans tous les cas particuliers que j'ai étudiés, les conditions sur u_{n_0} et u_{n_0+1}, qui sont contenues implicitement dans le théorème précédent sans l'être dans la proposition 2.4, étaient satisfaites. Quant au fait que je n'ai pas pu démontrer la proposition 2.4, pour $p = 2$, il semble que cela soit plutôt dû à la nature de la démonstration qu'à une différence réelle dans les résultats.

3. Démonstration du théorème 2.

3.1. - Rappelons tout d'abord le résultat suivant (cf. [1]).

PROPOSITION 3.1. - *Soit L un corps local à corps résiduel parfait de caractéristique p non nulle. Soit L' une extension cyclique totalement ramifiée de degré p de L. Soit i le nombre de ramification de l'extension L'/L. Soit v la valuation de L normalisée de telle sorte que $v(L) = \mathbb{Z}$. Soit $e = v(p)$ l'indice de ramification absolu de L (fini ou non). Alors :*

- Ou bien $i = ep/(p-1)$, et L' est le corps de rupture d'un polynôme de Kummer $P(\xi) = \xi^p - \alpha$, avec $\alpha \in L$ et $v(\alpha) = 1$;

- Ou bien $0 < i < ep/(p-1)$, $i \not\equiv 0 \pmod p$, et L' est le corps de rupture d'un polynôme d'Artin-Schreier $P(\xi) = \xi^p - \xi - \alpha$, avec $\alpha \in L$ et $v(\alpha) = -i$.

Nous allons déduire de cette proposition le lemme suivant.

LEMME 1. - Avec les hypothèses et les notations de la proposition 3.1, soit x une uniformisante de L, et soit v' la valuation de L' normalisée de telle sorte que $v(L') = \mathbb{Z}$. Alors il existe une uniformisante x' de L' telle que

$$v'(x - x'^p) \geqslant p + (p-1)i \ .$$

Démonstration. - Soit S un système de représentants, contenant 0, de k, corps résiduel de L, dans L. L'ensemble $S^p = \{s^p \mid s \in S\}$ est encore un système de représentants de k dans L. Supposons qu'il existe une uniformisante x_0 de L, et une uniformisante x'_0 de L', telles que l'on ait

$$v'(x_0 - x_0'^p) \geqslant p + (p-1)i \ .$$

L'uniformisante x peut s'écrire

$$x = \sum_{n \geqslant 1} c_n^p x_0^n \ , \qquad \text{avec } c_n \in S \text{ et } c_1 \neq 0 \ .$$

Posons $x' = \sum_{n \geqslant 1} c_n x_0'^n$. L'élément x' est une uniformisante de L'. Comme, pour $j = 1, 2, \ldots, p-1$, $\binom{p}{j}$ est divisible par p, et comme $v'(p) = ep$, la formule du binôme montre que

$$x - x'^p \equiv \sum_{n \geqslant 1} c_n^p (x_0^n - x_0'^{pn}) \pmod{\mathfrak{p}^{p+ep}} \ ,$$

en désignant par $\mathfrak{p}$ l'idéal maximal de l'anneau des entiers de L'. Comme $p + ep \geqslant p + (p-1)i$, on en déduit que $v'(x - x'^p) \geqslant p + (p-1)i$. Il ne reste donc plus qu'à établir l'existence de x_0 et x'_0.

(a) Si $i = ep/(p-1)$: Il résulte de la proposition 3.1 qu'il existe une uniformisante x_0 de L, et une uniformisante x'_0 de L', telles que $x_0 = x_0'^p$; on a donc

$$v'(x_0 - x_0'^p) = +\infty \geqslant p + (p-1)i \ .$$

(b) Si $i < ep/(p-1)$: Il résulte de la proposition 3.1 qu'il existe un élément θ de L', et un élément α de L, tels que $\theta^p - \theta = \alpha$ et $v'(\theta) = -i$. L'élément θ est donc de la forme $1/ax_0'^i$, où x'_0 est une uniformisante de L' et a un élément de S. On a alors $1/a^p x_0'^{pi} - 1/ax_0'^i = \alpha$. L'élément α est donc de la forme $1/a^p x_0^i$, où x_0 est une uniformisante de L. On a

$$v'(x_0^{-i} - x_0'^{-pi}) = v'(a^{p-1} x_0'^{-i}) = -i \ .$$

Comme $i \not\equiv 0 \pmod{p}$, si $x_0 = x_0'^p + \beta$, alors

$$x_0^{-i} = x_0'^{-pi} - i x_0'^{p(-i-1)} \beta + \dots \ .$$

On en déduit que $v'(\beta) - p(i+1) = -i$, ou encore que $v'(\beta) = p + (p-1)i$.

C. Q. F. D.

3.2. - Soit K un corps local de caractéristique p , et soit k son corps résiduel. Soit X une uniformisante de K . Alors on peut identifier K et le corps des séries formelles $k((X))$. L'anneau A des entiers de K est l'anneau $k[[X]]$, et son idéal maximal $\mathfrak{p}$ est l'idéal engendré par X . A tout élément α de $\mathfrak{p}$, on peut associer un élément σ du groupe $\Gamma_S(K)$ des automorphismes sauvagement ramifiés de K , et un seul, défini par

$$(8) \qquad \begin{cases} \sigma(X) = X(1+\alpha) \ , \\ \sigma(a) = a \ , \quad \text{pour tout} \quad a \quad \text{dans} \quad k \ ; \end{cases}$$

et réciproquement, tout élément de $\Gamma_S(K)$ est de cette forme, et on a

$$(9) \qquad i(\sigma) = v(\alpha) \ ,$$

en désignant par v la valuation normalisée de K .

Si k' est une extension de k , et si $K' = k'((X))$, tout élément de $\Gamma_S(K)$ se prolonge d'une manière, et d'une seule, en un élément de $\Gamma_S(K')$ qui a le même nombre de ramification. Il suffit donc de démontrer le théorème 2 lorsque E et K ont même corps résiduel k fini.

3.3. - Soit $(L_j)_{j \in \mathbb{N}}$ une famille de corps locaux ayant tous k comme corps résiduel. Soient, pour tout entier positif j , A_j l'anneau des entiers de L_j , $\mathfrak{p}_j$ l'idéal maximal de A_j , s_j une section de k dans A_j , v_j la valuation de L_j normalisée de telle sorte que $v_j(L_j) = \mathbb{Z}$, $e_j = v_j(p)$ l'indice de ramification absolu de L_j . On suppose que les e_j tendent vers l'infini.

Pour tout entier positif j , choisissons une uniformisante π_j de A_j , et un entier positif m_j inférieur ou égal à e_j , de telle manière que la suite

$$(10) \qquad m_0 \ , m_1 \ , \dots \ , m_j \ , \dots$$

soit une suite croissante d'entiers tendant vers l'infini.

Pour tout j , tout élément α de A_j s'écrit d'une manière, et d'une seule, sous la forme

$$(11) \qquad \alpha = \sum_{\ell=0}^{\infty} s_j(c_\ell) \pi_j^\ell \ , \qquad \text{avec, pour tout} \quad \ell \ , \quad c_\ell \in k \ .$$

Pour tout couple d'entiers positifs j et j' vérifiant $j \geqslant j'$, considérons l'application $\theta_j^{j'}$ de A_j dans $A_{j'}$, définie par

$$(12) \qquad \theta_j^{j'}(\alpha) = \sum_{\ell=0}^{\infty} s_{j'}(c_\ell)\pi_{j'}^{\ell}, \qquad \text{si} \quad \alpha = \sum_{\ell=0}^{\infty} s_j(c_\ell)\pi_j^{\ell} .$$

L'application $\theta_j^{j'}$ définit, par passage au quotient, un épimorphisme $\overline{\theta_j^{j'}}$ de l'anneau valué $\overline{A_j} = A_j/p_j^{m_j}$ sur $\overline{A_{j'}} = A_{j'}/p_{j'}^{m_{j'}}$, indépendant du choix des sections s_j et $s_{j'}$. On obtient ainsi un système projectif $(\overline{A_j}, \overline{\theta_j^{j'}})$, et sa limite est un anneau de séries formelles que l'on peut identifier à A :

$$(13) \qquad A = k[[X]] = \varprojlim \overline{A_j} .$$

Si σ_j est un automorphisme sauvagement ramifié de L_j, et si

$$\sigma_j(\pi_j) = \sum_{\ell=1}^{\infty} s_j(c_{\ell,j})\pi_j^{\ell} ,$$

alors σ_j est entièrement déterminé par $c_j = (c_{\ell,j})_{\ell \in \underset{\sim}{N}^*} \in k^{\underset{\sim}{N}^*}$. Par passage au quotient, σ_j définit un automorphisme $\overline{\sigma_j}$ de $\overline{A_j}$. Si on a défini un automorphisme σ_j pour tout entier j, la famille des $\overline{\sigma_j}$ définira un automorphisme du système projectif, donc de A, si, et seulement si,

$$(14) \qquad \forall\, j \in \underset{\sim}{N}, \qquad c_{\ell,j+1} = c_{\ell,j}, \quad \text{pour} \quad \ell = 1, 2, \ldots, m_j - 1 .$$

Il est alors immédiat que la suite des nombres de ramification de $\sigma = \varprojlim \overline{\sigma_j}$ est la limite de la suite des nombres de ramification de σ_j.

3.4. - Soit E un corps local de corps résiduel k fini. Soit $q = p^r$ le nombre des éléments de k. Soit F une Γ-extension sauvagement ramifiée de E. Soit

$$i_0 < i_1 < i_2 < \ldots < i_n < \ldots$$

la suite des nombres de ramification de l'extension, et soit

$$u_0 < u_1 < u_2 < \ldots < u_n < \ldots$$

la suite des nombres supérieurs de ramification de l'extension.

Soit, pour tout entier positif n, E_n l'unique extension de degré p^n de E contenue dans F. Si τ_n est un automorphisme qui engendre le groupe de Galois de l'extension E_n/E, la suite des nombres supérieurs de ramification de τ_n est (cf. [4], proposition 14, p. 81, et remarque 1, p. 83)

$$u_0 < u_1 < \ldots < u_{n-1} .$$

L'extension E_{n+1}/E_n est une extension cyclique de degré p, dont l'unique nombre de ramification est i_n (cf. [4], proposition 2, p. 70, et corollaire à la proposition 3, p. 71).

Soit v'_n la valuation normalisée de E_n, et soit e'_n l'indice de ramification absolu de E_n. On a $e'_n = p^n e'_0$. Il résulte du lemme 1 que l'on peut choisir, dans chaque E_n, une uniformisante x_n de telle manière que, pour tout entier n positif, on ait

$$v'_{n+1}(x_n - x_{n+1}^p) \geqslant p + (p-1)i_n \quad . \tag{15}$$

Soit s une section de k dans E. Pour tout entier j positif, posons

$$L_j = E_{rj} \; ; \qquad \pi_j = x_{rj} \; ; \qquad s_j = s \; ; \qquad m_j = (p-1)i_{rj}/p \quad . \tag{16}$$

Avec les notations de 3.3, on a $e_j = e'_{rj} = p^{rj} e'_0$, et alors $m_j \leqslant e_j$, et la suite des m_j tend vers l'infini.

LEMME 2. - <u>On a</u> $v_{j+1}(\pi_j - \pi_{j+1}^q) \geqslant q(1 + m_j)$.

<u>Démonstration</u>. - On a

$$\pi_j - \pi_{j+1}^q = \sum_{\ell=0}^{r-1} (x_{rj+\ell}^{p^\ell} - x_{rj+\ell+1}^{p^{\ell+1}}) \quad .$$

Comme, pour tout entier strictement positif ℓ et pour $\mu = 1, 2, \ldots, p^\ell - 1$, p divise $\binom{p^\ell}{\mu}$, il résulte de la formule du binôme que

$$\pi_j - \pi_{j+1}^q \equiv \sum_{\ell=0}^{r-1} (x_{rj+\ell} - x_{rj+\ell+1}^p)^{p^\ell} \pmod{p_{j+1}^{q+e_{j+1}}} \quad .$$

Or $q + e_{j+1} \geqslant q(1 + m_j)$, et

$$v_{j+1}((x_{rj+\ell} - x_{rj+\ell+1}^p)^{p^\ell})$$

$$= p^\ell \, v_{j+1}(x_{rj+\ell} - x_{rj+\ell+1}^p) = p^\ell \, p^{r(j+1)-(rj+\ell+1)} \, v'_{rj+\ell+1}(x_{rj+\ell} - x_{rj+\ell+1}^p)$$

$$= p^{r-1} \, v'_{rj+\ell+1}(x_{rj+\ell} - x_{rj+\ell+1}^p) \geqslant p^{r-1}(p + (p-1)i_{rj+\ell}) \quad ,$$

d'après (15). Comme, pour tout entier ℓ positif,

$$p^{r-1}(p + (p-1)i_{rj+\ell}) \geqslant q(1 + (p-1)i_{rj}/p) = q(1 + m_j) \quad ,$$

on a $v_{j+1}(\pi_j - \pi_{j+1}^q) \geqslant q(1 + m_j)$.

C. Q. F. D.

3.5. - Choisissons, pour chaque entier j positif, un automorphisme σ_j de L_j de la manière suivante :

σ_0 est l'identité sur L_0 ;

Si σ_0 , σ_1 , ... , σ_{j-1} sont choisis, on prend pour σ_j un générateur du groupe de Galois de l'extension L_j/E , dont la restriction à L_{j-1} est σ_{j-1} .

Pour achever la démonstration du théorème 2, il ne reste plus qu'à établir le lemme suivant.

LEMME 3. - Avec les notations de 3.3, on a

$$\forall\ j\ , \qquad c_{\ell,j+1} = c_{\ell,j}\ , \quad \text{pour}\ \ \ell = 1\ ,\ 2\ ,\ \ldots\ ,\ m_j - 1\ .$$

Démonstration. - Posons $\pi_j = \pi_{j+1}^q + \alpha_{j+1}$. D'après le lemme 2, on a

$$v_{j+1}(\alpha_{j+1}) \geqslant q(1 + m_j)\ .$$

Or

$$\sigma_j(\pi_j) = \sum_{\ell\geqslant 1} s(c_{\ell,j})\pi_j^{\ell} = \sum_{\ell\geqslant 1} s(c_{\ell,j})(\pi_{j+1}^q + \alpha_{j+1})^{\ell} \equiv \sum_{\ell\geqslant 1} s(c_{\ell,j})\pi_{j+1}^{\ell q} \pmod{p_{j+1}^{q(1+m_j)}}\ .$$

Mais

$$\sigma_j(\pi_j) = \sigma_{j+1}(\pi_j) = \sigma_{j+1}(\pi_{j+1}^q) + \sigma_{j+1}(\alpha_{j+1}) \equiv (\sigma_{j+1}(\pi_{j+1}))^q \pmod{p_{j+1}^{q(1+m_j)}}\ .$$

Il résulte encore de la formule du binôme que

$$(\sigma_{j+1}(\pi_{j+1}))^q = \Big(\sum_{\ell\geqslant 1} s(c_{\ell,j+1})\pi_{j+1}^{\ell}\Big)^q \equiv \sum_{\ell\geqslant 1} (s(c_{\ell,j+1}))^q\, \pi_{j+1}^{\ell q} \pmod{p_{j+1}^{q+e_{j+1}}}\ .$$

Comme $q + e_{j+1} \geqslant q(1 + m_j)$, on voit alors que

$$\sum_{\ell\geqslant 1} s(c_{\ell,j})\pi_{j+1}^{\ell q} \equiv \sum_{\ell\geqslant 1} (s(c_{\ell,j+1}))^q\, \pi_{j+1}^{\ell q} \pmod{p_{j+1}^{q(1+m_j)}}\ .$$

Comme $e_{j+1} \geqslant qm_j$, on en déduit que $c_{\ell,j} = c_{\ell,j+1}^q$, pour $\ell = 1\ ,\ 2\ ,\ \ldots\ ,\ m_j - 1$. Or les $c_{\ell,j+1}$ appartiennent à k qui a q éléments. On a donc $c_{\ell,j+1} = c_{\ell,j+1}^q$ et, par conséquent, $c_{\ell,j} = c_{\ell,j+1}$ pour $j = 1\ ,\ 2\ ,\ \ldots\ ,\ m_j - 1$.

C. Q. F. D.

BIBLIOGRAPHIE

[1] MACKENZIE (R.) and WHAPLES (G.). - Artin-Schreier equations in characteristic zero, Amer. J. of Math., t. 78, 1956, p. 473-485.

[2] MAUS (E.). - Existenz p-adischer Zahlkörper zu vorgegebenem Verzweigungsverhalten, Dissertation, Hamburg, 1965.

[3] SEN (S.). - On automorphisms of local fields, Annals of Math., t. 90, 1969, p. 33-46.

[4] SERRE (J.-P.). - Corps locaux. - Paris, Hermann, 1968 (Act. scient. et ind., 1296 ; Publ. Inst. Math. Univ. Nancago, 8).

[5] WYMAN (B.). - Wildly ramified gamma extensions, Amer. J. of Math., t. 91, 1969, p. 135-152.

(Texte reçu le 16 mars 1970)

Jean-Marc FONTAINE
6 rue Gounod
75 - PARIS 17