Canad. Math. Bull. Vol. **47** (2), 2004 pp. 237–245

Ramification des séries formelles

François Laubie

Abstract. Let p be a prime number. Let k be a finite field of characteristic p. The subset $X + X^2k[[X]]$ of the ring $k[[X]]$ is a group under the substitution law $\circ$ sometimes called the Nottingham group of k; it is denoted by $\mathcal{R}_k$. The ramification of one series $\gamma \in \mathcal{R}_k$ is caracterized by its lower ramification numbers: $i_m(\gamma) = \operatorname{ord}_X\big(\gamma^{p^m}(X)/X - 1\big)$, as well as its upper ramification numbers:

$$u_m(\gamma) = i_0(\gamma) + \frac{i_1(\gamma) - i_0(\gamma)}{p} + \cdots + \frac{i_m(\gamma) - i_{m-1}(\gamma)}{p^m}, \quad (m \in \mathbb{N}).$$

By Sen's theorem, the $u_m(\gamma)$ are integers. In this paper, we determine the sequences of integers (u_m) for which there exists $\gamma \in \mathcal{R}_k$ such that $u_m(\gamma) = u_m$ for all integer $m \geq 0$.

1 Introduction

Soit k un corps fini de caractéristique $p > 0$. Soit γ un automorphisme continu du corps des séries formelles $K = k((X))$. Pour tout $\varphi(X) \in k((X))$ notons $\varphi(X)^\gamma$ l'image de $\varphi(X)$ sous l'action de γ ; alors $\varphi(X)^\gamma = \varphi \circ \gamma(X)$ où $\gamma(X)$ désigne la série X^γ. L'automorphisme γ (ou la série $\gamma(X)$) est dit sauvagement ramifié si $\gamma(X) \in X + X^2k[[X]]$. Le groupe des automorphismes sauvagement ramifiés de $k((X))$ est anti-isomorphe au groupe des séries de la forme $X + a_2X^2 + \cdots + a_iX^i + \cdots$ pour la loi $\circ$ de composition. Ce groupe est noté $\mathcal{R}_k$.

L'intérêt du groupe $\mathcal{R}_k$ réside dans les deux propriétés suivantes :

– tout pro-p-groupe de type fini se plonge dans $\mathcal{R}_k$ (théorème de Camina [1]),

– tout groupe de Galois d'une extension galoisienne totalement ramifiée d'un corps local à corps résiduel k qui est un pro-p-groupe de Lie p-adique se plonge dans $\mathcal{R}_k$ en tant que groupe filtré par sa filtration de ramification (théorème de Wintenberger [10]).

Soit $\gamma \in \mathcal{R}_k$; désormais nous ne distinguerons pas la série $\gamma(X)$ de l'automorphisme γ de K. On note $i(\mathrm{id}_K) = +\infty$ et $i(\gamma) = v\big(\gamma(X)/X - 1\big)$ où $v = \operatorname{ord}_X$ désigne la valuation de K normalisée par $v(X) = 1$. Pour tout entier m premier à p on a $i(\gamma^{mp^n}) = i(\gamma^{p^n})$ et la suite $i(\gamma^{p^n})$ est trictement croissante tant que $\gamma^{p^n} \neq \mathrm{id}_K$; les $i_n(\gamma) = i(\gamma^{p^n})$ s'appellent les nombres de ramification de γ en numérotation inférieure.

Pour tout entier $n \geq 0$, soit $u_n(\gamma) = i_o(\gamma) + \frac{i_1(\gamma)-i_o(\gamma)}{p} + \cdots + \frac{i_n(\gamma)-i_{n-1}(\gamma)}{p^n}$; les $u_n(\gamma)$ s'appellent les nombres de ramification de γ en numérotation supérieure. On sait que les $u_n(\gamma)$ sont entiers et que la suite $(u_n(\gamma))$ est strictement croissante tant

Reçu par la rédaction le 12 juillet 2002; revu le 20 février 2003.
Classification (AMS) par sujet: 11S15, 20E18.
Mots clés: ramification, Nottingham group.

que $u_n(\gamma) < +\infty$ [7]. Par ailleurs la donnée des $u_n(\gamma)$ est équivalente à celle des $i_n(\gamma)$ car :

$$i_n(\gamma) = u_0(\gamma) + p\big(u_1(\gamma) - u_0(\gamma)\big) + \cdots + p^n\big(u_n(\gamma) - u_{n-1}(\gamma)\big).$$

Supposons que γ soit un élément d'ordre fini du groupe $\mathcal{R}_k$; γ engendre alors un sous-groupe fini G de $\mathcal{R}_k$ qui s'identifie au groupe de Galois de l'extension cyclique K/K^G. La suite $(i_n(\gamma))$ (resp. $u_n(\gamma)$) est alors la suite des nombres de ramification de l'extension K/K^G en numérotation inférieure (resp. en numérotation supérieure). Les suites finies de nombres de ramification des extensions cycliques des corps locaux d'égale caractéristique sont connues [4].

L'objet de cet article est de décrire parmi les suites strictement croissantes d'entiers celles qui sont de la forme $(u_n(\gamma))$ pour un $\gamma \in \mathcal{R}_k$ d'ordre infini. La méthode consiste à utiliser le foncteur "corps de normes" de Fontaine et Wintenberger pour établir un dictionnaire entre les propriétés des automorphismes d'ordre infini, sauvagement ramifiés de K et les propriétés des $\mathbb{Z}_p$-extensions totalement ramifiées des corps locaux à corps résiduel k.

Désormais on désigne par corps local un corps muni d'une valuation discrète pour laquelle il est complet et admet un corps résiduel fini de caractéristique p.

2 Ramification des $\mathbb{Z}_p$-extensions des corps locaux

Dans cette section, on détaille un par un les résultats connus sur les suites de nombres de ramification supérieurs des $\mathbb{Z}_p$-extensions totalement ramifiées des corps locaux.

Etant donné un corps local F, on note $e = e_F$ son indice de ramification absolu avec la convention $e_F = +\infty$ si F est d'égale caractéristique ; on note ζ_n une racine primitive p^n-ème de l'unité dans une clôture séparable $\bar{F}$ fixée et $s = s_F$ le plus grand entier n tel que $\zeta_n \in F$.

E. Maus [5] a décrit les suites finies d'entiers $u_0 < u_1 < \cdots < u_m$ qui sont les suites de nombres de ramification supérieurs des extensions cycliques E des corps locaux F d'inégales caractéristiques dans les deux cas suivants : $\zeta_1 \notin F$ ou $\mathrm{ord}_F(\zeta_s - 1) \not\equiv 0 \bmod p$.

B. Wyman [14] et J. Tate [9] ont montré que si (u_n) est la suite de nombres supérieurs de ramification d'une $\mathbb{Z}_p$-extension totalement ramifiée d'un corps local F d'inégales caractéristiques alors $u_{n+1} = u_n + e$ pour tout entier $n \geq n_0$ où n_0 ne dépend que de F.

M. A. Marshall [4] et J.-M. Fontaine [2] ont complété les conditions nécessaires sur (u_n) pour que (u_n) soit la suite de nombres de ramification supérieurs d'une $\mathbb{Z}_p$-extension totalement ramifiée d'un corps local F.

M. A. Marshall [4] a montré que ces dernières conditions (voir le théorème A ci-dessous) étaient aussi suffisantes dans le cas où le groupe de Galois de la pro-p-extension maximale de F est pro-p-libre ; cela se produit par exemple si $\mathrm{car}(F) = 0$ et $\zeta_1 \notin F$ (théorème B) ou si $\mathrm{car}(F) = p$ (théorème C).

Enfin H. Miki [6] a donné une réponse complète à la question à l'aide de paramètres assez sophistiqués ne dépendant que du corps F. Nous n'aurons à utiliser qu'un cas particulier du théorème de Miki (théorème D).

Théorème A **(Marshall [4], Fontaine [2])** *Soit F un corps local d'inégales caractéristiques et d'indice de ramification absolu e. Si $(u_n)_{n\geq 0}$ est la suite des nombres de ramification supérieurs d'une $\mathbb{Z}_p$-extension totalement ramifiée de F alors (u_n) satisfait les conditions $(\mathcal{M}_e)$ suivantes :*

– *ou bien $u_0 < ep/(p-1)$ et $p \nmid u_0$, ou bien $u_0 = ep/(p-1)$;*
– *si $u_n < e/(p-1)$ alors : ou bien $u_{n+1} = pu_n$, ou bien $pu_n < u_{n+1} < ep/(p-1)$ et $p \nmid u_{n+1}$, ou bien $u_{n+1} = ep/(p-1)$;*
– *si $u_n \geq e/(p-1)$ alors $u_{n+1} = u_n + e$.*

Théorème B **(Marshall [4])** *Soit F un corps local d'inégales caractéristiques tel que $\zeta_1 \notin F$ et soit e l'indice de ramification absolu de F. Pour qu'une suite d'entiers $(u_n)_{n\geq 0}$ soit la suite des nombres de ramification supérieurs d'une $\mathbb{Z}_p$-extension totalement ramifiée de F, il faut et il suffit qu'elle satisfasse les conditions $(\mathcal{M}'_e)$ suivantes :*

– *$u_0 < ep/(p-1)$ et $p \nmid u_0$;*
– *si $u_n < e/(p-1)$ alors : ou bien $u_{n+1} = pu_n$, ou bien $pu_n < u_{n+1} < ep/(p-1)$ et $p \nmid u_{n+1}$;*
– *si $u_n \geq e/(p-1)$ alors $u_{n+1} = u_n + e$.*

Remarques 1 - Les conditions $(\mathcal{M}_e)$ contiennent strictement les conditions $(\mathcal{M}'_e)$.
2 - Une suite d'entiers (u_n) satisfaisant $(\mathcal{M}_e)$ satisfait nécessairement $(\mathcal{M}'_e)$ dans les deux cas suivants : - $ep/(p-1)$ n'est pas un terme de la suite (u_n), - $e/(p-1)$ est un terme de la suite (u_n).

Théorème C **(Marshall [4])** *Soit F un corps local d'égale caractéristique. Pour qu'une suite d'entiers (u_n) soit la suite des nombres supérieurs de ramification d'une $\mathbb{Z}_p$-extension totalement ramifiée de F, il faut et il suffit qu'elle satisfasse les conditions $(\mathcal{M}_\infty)$ suivantes :*

– *$p \nmid u_0$,*
– *ou bien $u_{n+1} = pu_n$; ou bien $u_{n+1} > pu_n$ et $p \nmid u_{n+1}$.*

Remarque - En fait $(\mathcal{M}_\infty)$ n'est autre que la réécriture de $(\mathcal{M}_e)$ pour $e = +\infty$.

Théorème D **(Maus [5], Satz 6.1' revu par Miki [6] 4.1 corollarie 1)** *Soit F un corps local d'inégales caractéristiques, d'indice de ramification absolu e. On suppose que $\zeta_1 \in F$ et que $\operatorname{ord}_F(\zeta_s - 1) \not\equiv 0 \bmod p$. Pour qu'une suite $(u_n)_{n\geq 0}$ soit la suite des nombres de ramification supérieurs d'une $\mathbb{Z}_p$-extension totalement ramifiée de F, il faut et il suffit qu'elle satisfasse $(\mathcal{M}_e)$ dans les deux cas suivants :*

1-er cas : *le corps résiduel de F n'est pas le corps premier $\mathbb{F}_p$*

2-ème cas : *le corps résiduel de F est $\mathbb{F}_p$ et $\operatorname{ord}_F(\zeta_s - 1)$ n'est pas l'un des termes de la suite (u_n).*

https://doi.org/10.4153/CMB-2004-023-6 Published online by Cambridge University Press

3 Application du foncteur "corps de normes"

Etant donnée une $\mathbb{Z}_p$-extension E d'un corps local F, la filtration de ramification de $\mathrm{Gal}(E/F)$ est définie a priori en numérotation supérieure et tout sous-groupe fermé de $\mathrm{Gal}(E/F)$ est un groupe de ramification. En fait la filtration de ramification de $\mathrm{Gal}(E/F)$ est aussi définie en numérotation inférieure : si (u_n) est la suite des nombres de ramification supérieurs de E/F alors les nombres de ramification inférieurs de E/F sont les

$$i_n = u_0 + p(u_1 - u_0) + \cdots + p^n(u_n - u_{n-1}), \quad (n \in \mathbb{N}).$$

Etant donné un corps k fini de caractéristique p et un sous-groupe fermé G de $\mathcal{R}_k$, la filtration de ramification de G est définie a *priori* en numérotation inférieure. En fait dans le cas où G est isomorphe à $\mathbb{Z}_p$, on peut définir les nombres de ramification supérieurs de G à partir de ses nombres de ramification inférieurs i_n par :

$$u_n = i_0 + \frac{i_1 - i_0}{p} + \cdots + \frac{i_n - i_{n-1}}{p^n}, \quad (n \in \mathbb{N}).$$

On sait [7] que (u_n) est une suite strictement croissante d'entiers. Le foncteur "corps de normes" associe à toute $\mathbb{Z}_p$-extension totalement ramifiée E d'un corps local F de corps résiduel k, un isomorphisme ϕ de $\mathrm{Gal}(E/F)$ sur un sous-groupe Γ du groupe $\mathcal{R}_k$ des automorphismes sauvagement ramifiés de $K = k((X))$; en outre ϕ applique la filtration de ramification en numérotation inférieure (resp. supérieure) de $\mathrm{Gal}(E/F)$ sur la filtration de ramification en numérotation inférieure (resp. supérieure) de Γ, (voir [12]). Réciproquement une série $\sigma(X) \in X + X^2k[[X]]$ qui est d'ordre infini dans le groupe $\mathcal{R}_k$ engendre un sous-groupe fermé Γ de $\mathcal{R}_k$ isomorphe à $\mathbb{Z}_p$. Le foncteur inverse du foncteur "corps de normes" associe à un tel sous-groupe Γ de $\mathcal{R}_k$ une $\mathbb{Z}_p$-extension totalement ramifiée E d'un corps local F et un isomorphisme ϕ de $\mathrm{Gal}(E/F)$ sur Γ qui préserve les filtrations de ramification, (voir [11] et [13]). De ce qui précède et des théorèmes A, B, C et D, on tire les conséquences suivantes :

1 – Pour toute série $\sigma(X) \in X + X^2k[[X]]$ qui est d'ordre infini dans le groupe $\mathcal{R}_k$, il existe $e \in \mathbb{N}^* \cup \{+\infty\}$ tel que la suite des nombres de ramification supérieurs de σ satisfait les conditions $(\mathcal{M}_e)$; (Théorèmes A et C).

2 – Soit $(u_n)_{n\geq 0}$ une suite d'entiers satisfaisant $(\mathcal{M}_\infty)$ et soit k un corps fini de caractéristique p ; il existe une $\mathbb{Z}_p$-extension totalement ramifiée de $k((X))$ dont la suite des nombres de ramification supérieurs est (u_n) (Théorème C) et par application du foncteur "corps de normes" il existe une série $\sigma \in \mathcal{R}_k$ dont la suite des nombres de ramification supérieurs est (u_n).

3 – Soit $(u_n)_{n\geq 0}$ une suite d'entiers satisfaisant les conditions $(\mathcal{M}'_e)$ pour un entier $e \geq 1$. Pour tout corps fini k de caractéristique $p \geq 3$ il existe un corps local F de caractéristique 0, de corps résiduel k, d'indice de ramification absolu e et qui ne contient pas de racine primitive p-ème de l'unité. Alors (Théorème B) il existe une $\mathbb{Z}_p$-extension totalement ramifiée de F dont la suite des nombres supérieurs de ramification est (u_n). Par application du foncteur "corps de normes", il existe une série $\sigma(X) \in X + X^2k[[X]]$ d'ordre infini dans le groupe $\mathcal{R}_k$ dont la suite de nombre supérieur de ramification est (u_n).

https://doi.org/10.4153/CMB-2004-023-6 Published online by Cambridge University Press

4 – Soit $(u_n)_{n\geq 0}$ une suite d'entiers satisfaisant les conditions $(\mathcal{M}_e)$ avec $u_0 = ep/(p-1)$ pour un entier $e \geq 1$ c'est-à-dire avec $p|u_0$. Alors $p-1|e$ et, pour tout $n \geq 0$, $u_n = ep/(p-1) + ne$. En outre la série $\sigma(X) = X + X^{1+ep/(p-1)}$ admet la suite (u_n) pour suite de nombres supérieurs de ramification.

5 – Pour $p \geq 3$ il reste à considérer le cas d'une suite d'entiers $(u_n)_{n\geq 0}$ satisfaisant les conditions $(\mathcal{M}_e)$ pour un entier $e \geq 1$ et tel qu'il existe $m \geq 0$ avec $u_m < e/p-1$ et $u_{m+1} = ep/p-1$. Alors $p-1|e$; on pose $e = \eta(p-1)p^{s-1}$ avec $s \geq 1$, $\eta \geq 1$ et $p \nmid \eta$. Remarquons que si $s = 1$ alors $\eta = e/(p-1)$ n'est pas un nombre de ramification. Soit $F_0 = \mathbb{Q}_p(\zeta_s)$ où ζ_s est une racine primitive p^s-ème de l'unité et soit F une extension totalement ramifiée de F_0 de degré η (éventuellement $\eta = 1$ et $F = F_0$). Alors $\mathrm{ord}_F(\zeta_s - 1) = \eta$ et si pour tout $n \geq 0$, $\eta \neq u_n$ alors d'après le théorème D il existe une $\mathbb{Z}_p$-extension totalement ramifiée de F dont la suite des nombres supérieurs de ramification est (u_n). Le foncteur "corps de normes" fournit alors une série $\sigma(X) \in X + X^2\mathbb{F}_p[[X]]$ dont la suite des nombres supérieurs de ramification est (u_n).

6 – En outre pour tout p premier, pour tout corps fini k de caractéristique p avec $k \neq \mathbb{F}_p$ et pour toute suite (u_n) satisfaisant les conditions $(\mathcal{M}_e)$ pour un $e \in \mathbb{N}^*$, le même argument qu'en 5-fournit une série $\sigma \in \mathcal{R}_k$ dont la suite des nombres de ramification supérieurs est (u_n).

7 – Pour $p = 2$, si (u_n) est une suite d'entiers satisfaisant $(\mathcal{M}_e)$ on pose $e = \eta 2^{s-1}$ avec $\eta \geq 1$ impair et $s \geq 1$. Alors si $\forall n \geq 0$, $u_n \neq \eta$ le même argument qu'en 5-fournit une série $\sigma(X) \in X + X^2\mathbb{F}_2[[X]]$ dont la suite des nombres de ramification supérieurs est (u_n).

Contre-exemple : pour $p = 2$ et $e = 1$, il n'existe qu'une seule suite d'entiers (u_n) satisfaisant les conditions $(\mathcal{M}_1)$ tel qu'il existe une série $\sigma(X) \in X + X^2\mathbb{F}_2[[X]]$ avec $u_n(\sigma) = u_n$ pour tout $\eta \geq 0$; c'est la suite des entiers ≥ 2 ; c'est-à-dire la suite des nombres de ramification supérieurs des $\mathbb{Z}_2$-extensions totalement ramifiées de $\mathbb{Q}_2$. Ainsi quoique la suite des entiers ≥ 1 satisfasse les conditions $(\mathcal{M}_1)$ elle n'est pas la suite des nombres supérieurs de ramification d'une série $\in X + X^2\mathbb{F}_2[[X]]$.

L'ensemble de toutes ces remarques ne donne une réponse complète à la question de déterminer les suites de nombres de ramification supérieurs des séries de $X + X^2k[[X]]$ que lorsque $k \neq \mathbb{F}_p$.

Lorsque $k = \mathbb{F}_p$, il reste à considérer les suites $(u_n)_{n\geq 0}$ d'entiers positifs satisfaisant les condition $(\mathcal{M}_e)$ avec, comme précédemment, $e = \eta(p-1)p^r$, $r \geq 1$ et $p \nmid \eta$ telles que :

– si $p = 2$, η est l'un des entiers u_n,

– si $p \neq 2$, η et ηp^{r+1} sont des termes de la suite (u_n) alors que ηp^r n'en est pas un.

4 Etude du cas particulier $k = \mathbb{F}_p$

Dans cette section, k est le corps premier $\mathbb{F}_p$, F est une extension finie totalement ramifiée de $\mathbb{Q}_p$ de degré $e = \eta(p-1)p^r$ avec $p \nmid \eta$, $\mathcal{O} = \mathcal{O}_F$ est l'anneau des entiers de F, $\pi = \pi_F$ est une uniformisante de F, $U^n = U_F^n$ est le groupe des unités de F de la forme $1 + a\pi^n$ avec $a \in \mathcal{O}$ et $s = s_F$ est le plus grand entier tel que F contienne

https://doi.org/10.4153/CMB-2004-023-6 Published online by Cambridge University Press

une racine primitive p^s-ème de l'unité ζ_s. On note également $\lambda_e(x) = \min(px, x+e)$ et on désigne par $\mathbf{p}$ l'opérateur d'élévation à la puissance p : $\mathbf{p}^n(G) = G^{p^n}$ pour tout groupe multiplicatif G et tout entier $n \geq 1$.

Lemme 1 *Pour tout entier $n \geq 1$, on a :*

- *le groupe U^n/U^{n+1} est cyclique d'ordre p,*
- $\mathbf{p}(U^n) \subset U^{\lambda_e(n)}$,
- *si $n \neq e/(p-1)$, $\mathbf{p}$ induit un isomorphisme $\mathbf{p}_n$ de U^n/U^{n+1} sur $U^{\lambda_e(n)}/U^{\lambda_e(n)+1}$.*

En outre, lorsque $p-1|e$, $\mathbf{p}_{e/(p-1)}$ est aussi un isomorphisme si et seulement si $s = 0$.

C'est un cas particulier d'un résultat bien connu. Une preuve issue de la théorie du corps de classes local "géométrique" de J.-P. Serre se trouve dans [4]*.

Supposons désormais que $s \geq 1$; donc $p-1|e$. Soit I l'ensemble des entiers $i \in [1, ep/(p-1)]$ premiers à p auquel on adjoint $ep/(p-1) = \eta p^{r+1}$. Pour tout $i \in I$, on se donne une unité $y_i \in U^i \backslash U^{i+1}$. Il résulte du lemme 1 que $S = \{y_i \; ; i \in I\}$ est un système de générateurs topologiques minimal du pro-p-groupe U^1 ; il a $e+1$ éléments et $U^1/\langle\zeta_s\rangle$ est un pro-p-groupe abélien libre de rang e.

Posons $S^n = \{y_i^{p^{n(i)}} \; ; i \in I\}$ où $n(i)$ désigne le plus petit entier tel que $n \leq \lambda_e^{n(i)}(i)$. D'après le lemme 1, il est clair que S^n est un système de générateurs topologiques de U^n pour tout entier $n \geq 1$ (voir [4], proof of theorem 5).

Lemme 2 *Soit e un entier ≥ 1 et soit Γ un groupe isomorphe à $\mathbb{Z}_p$ muni d'une filtration $(\Gamma^n)_{n\geq 0}$ telle que $\forall n \geq 0$, $\mathbf{p}^n(\Gamma) = \Gamma^{u_n}$ où $(u_n)_{n\geq 0}$ est une suite strictement croissante d'entiers ≥ 1. Alors les assertions suivantes sont équivalentes :*

(i) *la suite (u_n) satisfait les conditions $(\mathcal{M}_e)$;*

(ii) *pour tout entier $n \geq 1$, on a $\mathbf{p}(\Gamma^n) \subset \Gamma^{\lambda_e(n)}$ et, si $n \neq e : (p-1)$, $\mathbf{p}$ induit un homomorphisme surjectif $\mathbf{p}_n$ de Γ^n/Γ^{n+1} sur $\Gamma^{\lambda_e(n)}/\Gamma^{\lambda_e(n)+1}$.*

Démonstration L'assertion (ii) est équivalente à la suivante : si $\lambda_e(n)$ est un saut de la filtration alors n est aussi un saut de la filtration sauf si $n = e/(p-1)$ (dans ce cas $\lambda_e(n) = ep/(p-1)$) ; il est immédiat de vérifier que c'est bien équivalent aux conditions $(\mathcal{M}_e)$ pour la suite (u_n)*.

Supposons que les conditions du lemme 2 soient vérifiées. Pour tout $i \in I \cap \{u_n\}_{n\geq 0}$, on se donne $\gamma_i \in \Gamma^i \setminus \Gamma^{i+1}$, on pose $S_\Gamma = \{\gamma_i \; ; \; i \in I \cap \{u_n\}_{n\geq 0}\}$ et $S_\Gamma^n = \{\gamma_i^{p^{n(i)}} \; ; i \in I \cap \{u_n\}_{n\geq 0}\}$ où $n(i)$ est défini comme précédemment. Alors les propriétés de surjectivité des $\mathbf{p}_n$ font que S_Γ^n engendre Γ^n pour tout entier $n \geq 1$.

On note également $S_\Gamma^* = \{\gamma_i \in S_\Gamma \; ; i \neq ep/(p-1)\}$.

Lemme 3 *Les entiers $r \geq s \geq 1$ étant donnés, il existe une extension finie F de $\mathbb{Q}_p$, totalement ramifiée de degré $e = \eta(p-1)p^r$ avec $\zeta_s \in F$, $\zeta_{s+1} \notin F$ et telle qu'on puisse choisir $y_{ep/(p-1)} = \zeta_s y_\eta^{p^{r-s+1}}$.*

Démonstration Soit F_0 une extension totalement ramifiée de degré η de $\mathbb{Q}_p(\zeta_s)$. Soit y une unité de F_0 telle que $\mathrm{ord}_{F_0}(y-1) = \eta p^s$; on note $z = (\zeta_s y)^{1/p^{r-s+1}}$ et

$F = F_0(z)$. On a $\mathrm{ord}_{F_0}(\zeta_s y - 1) = \mathrm{ord}_{F_0}(\zeta_s - 1) = \eta$. Comme $p \nmid \eta$, l'extension F/F_0 est totalement ramifiée de degré p^{r-s+1} donc $\mathrm{ord}_F(y-1) = \eta p^{r+1}$ et $\mathrm{ord}_F(z-1) = \eta$. L'indice de ramification absolu de F est bien $e = \eta(p-1)p^r$ et comme $\mathrm{ord}_F(y-1) = ep/(p-1)$, on peut choisir $y_\eta = z$ et $y_{ep/(p-1)} = y = \zeta_s^{-1} y_\eta^{p^{r-s+1}}$. En outre $\zeta_{s+1} \notin F$ car sinon $y = \zeta_{s+1}^{-p} y_\eta^{p^{r-s+1}}$ serait une puissance p-ème dans F, en contradiction avec le lemme $1^\star$.

Etant donnée une suite (u_n) d'entiers positifs satisfaisant les conditions $\mathcal{M}_e$ pour $e = \eta(p-1)p^r$ comme ci-dessus, soit t le plus petit entier tel que $\eta p^t \notin \{u_n\}_{n\geq 0}$; on suppose que $1 \leq t \leq r$ c'est-à-dire : $\eta \in \{u_n\}_{n\geq 0}$ et $e/(p-1) \notin \{u_n\}_{n\geq 0}$. Soit n_0 tel que $u_{n_0} = \eta p^{t-1}$ et soit n_1 le plus grand entier tel que $u_{n_1} \leq \eta p^{r+1} = ep/(p-1)$. Alors $1 \leq n_1 - n_0 \leq r - t + 1$. Dorénavant on choisit $s = r - n_1 + n_0 + 1$ de sorte que $t \leq s \leq r$ et on considère un corps local F satisfaisant les conditions du lemme 3.

Soit $V = U^1/T$ où $T = \langle \zeta_s \rangle$ est le sous-groupe de torsion de $U^1 = U_F^1$. La filtration quotient sur V est donnée par $V^n = U^n T/T$; V est un pro-p-groupe abélien libre et il résulte du lemme 3 que l'image $S_V^* = \{\bar{y}_i \ ; \ i \in I \setminus \{ep/(p-1)\}\}$ de $S \setminus \{ep/(p-1)\}$ dans V est un système de générateurs topologiques libre de V à e éléments parceque $\bar{y}_{ep/(p-1)} = \bar{y}_\eta^{p^{r-s+1}}$.

Soit Γ un groupe isomorphe à $\mathbb{Z}_p$ filtré comme dans le lemme 2 : $\mathbf{p}^n(\Gamma) = \Gamma^{u_n}$. Soit φ l'application de S_V^* dans $S_\Gamma^* \cup \{1\}$ défini par $\varphi(\bar{y}_i) = \gamma_i$ si $i \in I \cap \{u_n\}_{n\geq 0}$ et $\varphi(\bar{y}_i) = 1$ sinon ; c'est une surjection de S_V^* sur S_Γ^* ou sur $S_\Gamma^* \cup \{1\}$.

Comme V est un pro-p-groupe abélien libre de $\mathbb{Z}_p$-base S_V^*, φ se prolonge en un homomorphisme surjectif de groupes $\tilde{\varphi}$ de V sur Γ tel que $\tilde{\varphi}(\bar{y}_{ep/(p-1)}) = \gamma_\eta^{p^{r-s+1}} = \gamma_\eta^{p^{n_1-n_0}}$; si $u_{n_1} = ep/(p-1)$, alors $\tilde{\varphi}(\bar{y}_{ep/(p-1)}) \in \Gamma^{ep/(p-1)} \setminus \Gamma^{ep/(p-1)+1}$. Donc, dans tous les cas, on a $\tilde{\varphi}(S_V) = S_\Gamma$ (ou $S_\Gamma \cup \{1\}$), $\tilde{\varphi}(S_V^n) = S_\Gamma^n$ (ou $S_\Gamma^n \cup \{1\}$) et $\tilde{\varphi}(V^n) = \Gamma^n$.

Ainsi Γ s'identifie, en tant que groupe filtré, à un quotient de U_F^1 et, par la théorie du corps de classes local, au groupe de Galois d'une $\mathbb{Z}_p$-extension totalement ramifiée de F.

Le foncteur "corps de normes" fournit donc une série de $X + X^2\mathbb{F}_p[[X]]$ dont la suite des nombres de ramification supérieurs (u_n) satisfait les conditions $(\mathcal{M}_e)$ avec $\eta \in \{u_n\}_{n\geq 0}$ et $\eta p^r = e/(p-1) \notin \{u_n\}_{n\geq 0}$.

Remarquons pour finir que, dans le cas où le corps résiduel du corps local F est $\mathbb{F}_2$, le degré e de F sur $\mathbb{Q}_2$ n'est jamais un saut de la filtration $(V^n)_{n\in\mathbb{N}}$ du groupe $V = U_F^1/\langle \zeta_s \rangle$ car $\mathrm{ord}_F(\zeta_1 - 1) = \mathrm{ord}_F(2) = e$. Il n'existe donc pas de $\mathbb{Z}_2$-extension totalement ramifiée de F dont e soit un saut de ramification supérieur ni de série de $X + X^2\mathbb{F}_2[[X]]$ dont la suite des nombres de ramification supérieurs satisfasse les conditions $(\mathcal{M}_e)$ tout en contenant e.

5 Conclusion

Donnons d'abord des formulations équivalentes des conditions $(\mathcal{M}_e)$:

Proposition *Soit (u_n) une suite strictement croissante d'entiers ≥ 1. Les assertions suivantes sont équivalentes :*

https://doi.org/10.4153/CMB-2004-023-6 Published online by Cambridge University Press

(i) *il existe* $e \in \mathbb{N}^* \cup \{+\infty\}$ *tel que* (u_n) *satisfait les conditions* $(\mathcal{M}_e)$ *;*

(ii) *il existe* $e \in \mathbb{N}^* \cup \{+\infty\}$ *tel que* $\forall n \geq 0$, $u_{n+1} \geq \lambda_e(u_n)$ *et* $\lambda_e(\mathbb{N}^*) \cap \{u_n\}_{n\geq 0} \subset \lambda_e(\{u_n\}_{n\geq 0}) \cup \{ep/(p-1)\}$ *;*

(iii) *il existe* $e \in \mathbb{N}^* \cup \{+\infty\}$ *tel que* (u_n) *satisfait les conditions :*

- *ou bien* $u_{n+1} \geq pu_n$ *pour tout entier* $n \geq 0$*, ou bien,* $\big((2p-1)/p\big)\, u_{n_0} \leq u_{n_0+1} < pu_{n_0}$ *pour* $n_0 = \min_{u_{n+1}<pu_n} n$ *et* $u_{n+1} - u_n = u_{n_0+1} - u_{n_0}$*, pour tout entier* $n \geq n_0$ *;*
- *si* $p|u_n$ *alors ou bien* $n \geq 1$ *et* $u_n \leq pu_{n-1}$*, ou bien* $n = n_0$ *et* $u_{n_0+1} = \big((2p-1)/p\big)\, u_{n_0}$.

Démonstration Ce n'est qu'un exercice : l'équivalence (i) $\Leftrightarrow$ (ii) est immédiate et l'équivalence (i) $\Leftrightarrow$ (iii) est démontrée dans [3]*.

Les résultats obtenus peuvent se formuler ainsi :

Théorème *Soit* k *un corps fini de caractéristique* $p > 0$.

- *Si* $k \neq \mathbb{F}_2$*, les suites d'entiers* $(u_n)_{n\geq 0}$ *pour lesquelles il existe* $\gamma(X) \in X + X^2k[[X]]$ *vérifiant* $u_n(\gamma) = u_n$ *pour tout* $n \geq 0$*, sont les suites satisfaisant les conditions* $(\mathcal{M}_e)$ *avec* $e \in \mathbb{N}^* \cup \{+\infty\}$ *;*
- *Si* $k = \mathbb{F}_2$*, les suites d'entiers* $(u_n)_{n\geq 0}$ *pour lesquelles il existe* $\gamma(X) \in X + X^2k[[X]]$ *vérifiant* $u_n(\gamma) = u_n$ *pour tout* $n \geq 0$*, sont les suites satisfaisant les conditions* $(\mathcal{M}_e)$ *avec* $e \in \mathbb{N}^* \cup \{+\infty\}$ *mais* $e \notin \{u_n\}_{n\geq 0}$.

Remerciements Ce sont les suggestions du référé anonyme qui ont permis d'établir un résultat complet.

Références

[1] R. D. Camina, *Subgroups of the Nottingham group*. J. Algebra **196**(1997), 101–113.

[2] J.-M. Fontaine, *Groupes de ramification et représentation d'Artin*. Ann. Sci. École Norm. Sup **4**(1971), 337–392.

[3] F. Laubie and M. Saine, *Ramification of some automorphisms of local fields*. J. Number Theory **72**(1998), 174–182.

[4] M. A. Marshall, *Ramification groups of Abelian local field extensions*. Canad. J. Math. **23**(1971), 271–281.

[5] E. Maus, *Existenz* $\mathfrak{p}$*-adischer Zahlkörper zu Vorgegebenem Verzweigungsverhalten*. Dissertation, Hamburg, 1965.

[6] H. Miki, *On the ramification numbers of cyclic* p*-extensions over local fields*. J. Reine Angew. Math. **328**(1981), 99–115.

[7] S. Sen, *On automorphisms of local fields*. Ann. of Math **90**(1969), 33–46.

[8] J.-P. Serre, *Corps locaux*. 2-ème ed., Hermann, Paris, 1968.

[9] J. Tate, p*-divisible groups*. Proc. of a conference on local fields, Driebergen, 1966.

[10] J.-P. Wintenberger, *Extensions de Lie et groupes d'automorphismes des corps locaux de caractéristique* p. C. R. Acad. Sci. Sér. A **288**(1979) 477–479.

[11] ———, *Extensions abéliennes et groupes d'automorphismes de corps locaux*. C. R. Acad. Sci. Paris Sér. A–B **290**(1980), 201–203.

[12] ———, *Le corps des normes de certaines extensions infinies de corps locaux ; applications*. Ann. Sci. École Norm. Sup. **16**(1983), 59–89.

[13] ———, *Automorphismes de corps locaux de caractéristique* p. (2002), preprint.
[14] B. F. Wyman, *Wildly ramified gamma extensions.* Amer. J. Math. **91**(1969), 135–152.

UMR6090 CNRS
Université de Limoges
Département de Mathématiques
123 Av. Albert Thomas
87060 Limoges Cedex
France
e-mail: laubie@unilim.fr