Journal de Théorie des Nombres
de Bordeaux **12** (2000), 483–488

Substitutions commutatives de séries formelles

par François LAUBIE

À Jacques Martinet

Résumé. L'étude des systèmes dynamiques non archimédiens initiée par J. Lubin conduit à déterminer la ramification de séries à coefficients dans un corps fini k, qui commutent entre elles pour la loi $\circ$. Dans cet article nous traîtons le cas des sous-groupes abéliens de $t + t^2k[[t]]$ qui correspondent par le foncteur *corps de normes* aux extensions abéliennes des extensions finies de $\mathbb{Q}_p$, dont la ramification se stabilise dès le début.

Abstract. In order to investigate the non-archimedian dynamical systems of J. Lubin, we are led to determine the ramification of series with coefficients in a finite field k, which commute for the law $\circ$. In this paper we study the case of Abelian subgroups of $t+t^2k[[t]]$ which corresponds, by means of the *norms field* functor, to Abelian extensions of finite extensions of $\mathbb{Q}_p$, whose ramification is stabilized from the ground field.

Dans [4], Lubin a proposé le sujet de recherche suivant : soit $\mathcal{O}$ l'anneau des entiers d'une extension finie de $\mathbb{Q}_p$; supposons qu'il existe deux séries formelles $f(t)$ et $g(t)$ dans $t\mathcal{O}[[t]]$ telles que $f \circ g = g \circ f$ avec $f(t)$ réversible (i.e. inversible pour o) et $f(t) \neq t$, $g(t)$ non réversible et $g(t) \neq 0$; existe-t-il une loi de groupe formel sur $\mathcal{O}$ susceptible de rendre compte de cette situation ?

Une faon d'aborder le problème est d'étudier les commutants pour la loi o des séries formelles de $\mathcal{O}/\pi\ \mathcal{O}[[t]]$ où π est une uniformisante de $\mathcal{O}$ et plus particulièrement les propriétés de ces commutants qui se conservent par relèvement dans $\mathcal{O}[[t]]$; cela a été fait [3] pour certaines séries en déterminant leur ramification et en appliquant le foncteur "corps des normes" de Fontaine et Wintenberger.

Soit k un corps parfait de caractéristique p et soit $\mathfrak{G}_k$ le groupe pour la loi o des séries $\sigma(t) \equiv t \bmod t^2k[[t]]$. Le but de cet article est de décrire une situation où le centralisateur dans $\mathfrak{G}_k$ d'un ensemble de séries $\sigma_1(t), \cdots \sigma_d(t)$

Manuscrit reçu le 24 février 2000.

qui commutent deux à deux, est presque complètement déterminé, en tant que groupe filtré, par les deux premiers nombres de ramification des séries. En fait cette situation correspond par le foncteur "corps des normes" au cas d'une extension abélienne d'une extension finie de $\mathbb{Q}_p$ dont la ramification se stabilise dès le début.

On désigne par corps local un corps complet pour une valuation discrète dont le corps résiduel est un corps parfait de caractéristique $p > 0$.

Soit k un corps parfait de caractéristique p et soit $K = k((t))$. Pour tout $\gamma \in \mathrm{Aut}_k(K)$, on pose $i(\gamma) = \mathrm{ord}_t((\gamma(t) - t)/t)$ et pour tout $m \geq 0$, $i_m(\gamma) = i(\gamma^{p^m})$.

Toute série $f(t)$ sauvagement ramifiée, c'est-à-dire telle que $\mathrm{ord}_t((f(t) - t)/t) \geq 1$, s'identifie à l'automorphisme $\gamma \in \mathrm{Aut}_k(K)$ défini par $\varphi(t)^\gamma = \varphi \circ f(t)$, pour tout $\varphi(t) \in k((t))$.

Soit $\mathfrak{G}$ le groupe $t + t^2k[[t]]$ pour la loi o; ainsi la puissance n-ième de f en tant qu'élément du groupe $\mathfrak{G}$ sera notée f^{on} et l'on pose également : $i_m(f) = \mathrm{ord}_t((f^{op^m}(t) - t)/t)$, pour tout $f \in \mathfrak{G}$ et tout $m \geq 0$.

Le groupe $\mathfrak{G}$ est un pro-p-groupe et la filtration définie par la fonction d'ordre $i = i_0$ s'appelle sa filtration de ramification en numérotation inférieure. Lorsque $k = \mathbb{F}_p$, le groupe $\mathfrak{G}$ est parfois appelé le groupe de Nottingham [1].

Théorème. *Soit d un entier ≥ 2 et soient des séries $\sigma_1(t), \cdots, \sigma_d(t)$ qui commutent deux à deux dans $\mathfrak{G}$ et telles que :*

$$i(\sigma_1) < i(\sigma_2) < \cdots < i(\sigma_d) < i(\sigma_1^{op})$$

et

$$(*) \quad i(\sigma_1^{op}) < p^{d-1}(p^2 - p + 1)i(\sigma_1) - p^{d-2}(p-1)i(\sigma_2) - \cdots \\ - p(p-1)i(\sigma_{d-1}) - (p-1)\, i(\sigma_d)$$

Alors le sous-groupe G de $\mathfrak{G}$ engendré par $\{\sigma_1, \cdots, \sigma_d\}$ est isomorphe à $\mathbb{Z}_p^d$, il est d'indice fini dans son centralisateur dans $\mathfrak{G}$ et, pour tout $j = 1, \cdots, d$ on a :

$$i_n(\sigma_j) = i(\sigma_j) + (i_1(\sigma_j) - i(\sigma_j))(p^{nd} - 1)/(p^d - 1).$$

Démonstration. D'après la théorie du corps des normes, on sait qu'il existe un corps local F (unique à isomorphisme continu de corps près) et une extension abélienne E de F dont le groupe de Galois s'identifie à G, en tant que groupes filtrés par leur filtration de ramification. On note φ_G la fonction de Herbrand de E/F :

$$\varphi_G(x) = \int_0^x \frac{dt}{(G : G_t)}.$$

Rappelons que l'extension E/F étant arithmétiquement profinie au sens de Fontaine et Wintenberger [9] son groupe de galois G est naturellement muni d'une filtration de ramification en numérotation inférieure $(G_t)_{t\geq 0}$ respectant le théorème de Herbrand. Pour tout $x \in [0, i_1(\sigma_1)]$, on pose :

$$\varphi(x) = \begin{cases} x & \text{si } x \leq i(\sigma_1), \\ i(\sigma_1) + \dfrac{i(\sigma_2) - i(\sigma_1)}{p} + \cdots + \dfrac{i(\sigma_j) - i(\sigma_{j-1})}{p^{j-1}} + \dfrac{x - i(\sigma_j)}{p^j} & \\ & \text{si } x \in [i(\sigma_j), i(\sigma_{j+1})], \\ i(\sigma_1) + \dfrac{i(\sigma_2) - i(\sigma_1)}{p} + \cdots + \dfrac{x - i(\sigma_d)}{p^d} & \text{si } x \geq i(\sigma_d). \end{cases}$$

Lemme 1. *Pour tout $x \in [0, i_1(\sigma_1)]$ on a $\varphi_G(x) \leq \varphi(x)$, avec égalité si et seulement si toute série $\tau \in G$ de la forme $\tau = \sigma_j^{op^n}$ avec $n \geq 1$ et $j = 1, \cdots, d$ vérifie $i(\tau) \geq i_1(\sigma_1)$.*

Démonstration du lemme 1. Comme G est abélien, les sauts de sa filtration de ramification en numérotation inférieure sont les $i(\sigma_j^{op^n})$ où $j \in \{1, \cdots, d\}$ et $n \in \mathbb{N}$.

Si, parmi ces sauts, les seuls qui sont $< i_1(\sigma_1)$ sont les $i(\sigma_j)$ avec $j = 1, \cdots, d$ alors $\varphi_G(x) = \varphi(x)$ pour $x \leq i_1(\sigma_1)$; si l'un de ces sauts appartient à $]i(\sigma_{j-1}), i(\sigma_j)[$ alors $\varphi_G(i(\sigma_j)) < \varphi(i(\sigma_j))$ et si l'un de ces sauts est égal à $i(\sigma_j)$ alors, pour tout $\epsilon > 0$ assez petit, on a $\varphi'_G(i(\sigma_j)+\epsilon) \leq \dfrac{1}{p^2}\varphi'_G(i(\sigma_j)-\epsilon)$ alors que $\varphi'(i(\sigma_j)+\epsilon) = \dfrac{1}{p}\varphi'(i(\sigma_j)-\epsilon)$, donc $\varphi_G(i(\sigma_{j+1})) < \varphi(i(\sigma_{j+1}))$. □

Le lemme suivant est une formulation complète d'un résultat bien connu ; voir [5].

Lemme 2 (Conditions de Marshall). *Soit F un corps local d'indice de ramification absolu e avec $e = \infty$ si F est d'égale caractéristique. Soit $(u_n)_{n\geq 0}$ une suite d'entiers strictement positifs. On dit que la suite satisfait les conditions de Marshall $\mathfrak{M}_F$ si :*

- dans le cas où F ne contient pas les racines primitives p-ièmes de l'unité, (en particulier si $\mathrm{car}(F) = p$*), on a :*

$\mathfrak{M}_{F,1}$ $\quad 1 \leq u_0 \leq ep/(p-1)$ *et* $p \nmid u_0$,

$\mathfrak{M}_{F,2}$ $\quad u_m < e/(p-1) \Longrightarrow u_{m+1} = pu_m$ *ou* $pu_m < u_{m+1} < ep/(p-1)$ *et* $p \nmid u_{m+1}$,

$\mathfrak{M}_{F,3}$ $\quad u_m \geq e/(p-1) \Longrightarrow u_{m+1} = u_m + e$;

- dans le cas où F contient une racine primitive p-ième de l'unité, on adjoint à $\mathfrak{M}_{F,1}$ l'éventualité : $u_0 = ep/(p-1)$, on adjoint à $\mathfrak{M}_{F,2}$ l'éventualité : $u_m < e/(p-1)$ et $u_{m+1} = ep/(p-1)$. La suite des sauts de ramification en numérotation supérieure d'une $\mathbb{Z}_p$-extension totalement ramifiée de F satisfait les conditions de Marshall $\mathfrak{M}_F$.

Réciproquement, si $\mathrm{car}(F) = p$, *ou si F ne contient pas de racines primitives p-ièmes de l'unité, ou si le corps résiduel de F est algébriquement clos, (ou plus généralement si le groupe de Galois de la pro-p-extension abélienne maximale de F est pro-p-libre) alors toute suite d'entiers satisfaisant $\mathfrak{M}_F$ est la suite des sauts de ramification en numérotation supérieure d'une $\mathbb{Z}_p$-extension de F ; voir* [5].

Corollaire. *Si (u_n) est la suite des sauts de ramification en numérotation supérieure d'une $\mathbb{Z}_p$-extension du corps local F et s'il existe un entier $m \geq 0$ tel que $u_{m+1} < pu_m$ alors* $\mathrm{car}(F) = 0$, *l'indice de ramification absolu de F est $e = u_{m+1} - u_m$ et pour tout $n \geq m$, $u_n = u_m + (n-m)e$.*

Pour tout $j \in \{1, 2, \cdots, d\}$, on note H_j le sous-groupe fermé de G engendré par $\{\sigma_1, \cdots, \sigma_d\} \backslash \{\sigma_j\}$; H_j s'identifie à un sous-groupe fermé de $\mathrm{Gal}(E/F)$ dont le corps des invariants M_j est une $\mathbb{Z}_p$-extension totalement ramifiée de F contenue dans E [9] et le groupe de Galois de M_j/F est engendré par l'image $\overline{\sigma_j}$ de σ_j dans G/H_j.

D'après le théorème de Herbrand [8, Ch. 4, Prop. 14] les deux premiers sauts de ramfication de M_1/F en numérotation supérieure sont $i(\sigma_1) = \varphi_G(i(\sigma_1))$ et $\varphi_G(i_1(\sigma_1))$. Or on vérifie facilement que la condition $(*)$ du théorème est équivalente à :

$$\varphi(i_1(\sigma_1)) < pi(\sigma_1).$$

Comme $\varphi_G(i_1(\sigma_1)) \leq \varphi(i_1(\sigma_1))$ (lemme 1), on a, d'après le corollaire au lemme 2, que : $\mathrm{car}(F) = 0$, l'indice de ramification absolu de F est $e = \varphi_G(i_1(\sigma_1)) - i(\sigma_1))$, avec $i(\sigma_1) \geq e/(p-1)$ et donc que les sauts de ramification en numérotation supérieure de M_1/F sont en progression arithmétique de raison e.

Puisque pour tout $j \in \{1, 2, \cdots, d\}$, $\varphi_G(i(\sigma_j)) > i(\sigma_1) \geq e/(p-1)$, les sauts de ramification en numérotation supérieure de la $\mathbb{Z}_p$-extension M_j/F sont également en progression arithmétique de raison e ; en particulier $i_1(\sigma_j) > i_1(\sigma_1)$ et les seuls sauts de ramification en numérotation inférieure de G qui sont $< i_1(\sigma_1)$ sont $i(\sigma_1) < i(\sigma_2) < \cdots < i(\sigma_d)$.

Donc $\varphi_G(x) = \varphi(x)$ pour tout $x \in [0, i_1(\sigma_1)]$.

Il reste à calculer $i_n(\sigma_j)$ pour $j \in \{1, 2, \cdots, d\}$ et $n \in \mathbb{N}$.

Posons $u_j = \varphi_G(i(\sigma_j))$ de sorte que la suite des sauts de ramification en numérotation supérieure de E/F soit $u_1, u_2, \cdots, u_d, u_1+e, u_2+e, \cdots, u_i+e, \cdots, u_1 + 2e, \cdots$.

Soit ψ_G la fonction réciproque de φ_G. On a :

$$\begin{aligned}
i_n(\sigma_1) &= \psi_G(u_1+ne)\\
&= u_1+p(u_2-u_1)+\cdots+p^{d-1}(u_d-u_{d-1})+p^d(u_1+e-u_d)+p^{d+1}(u_2-u_1)+\cdots\\
&\quad +p^{2d-1}(u_d-u_{d-1})+\cdots+p^{(n-1)d}(u_1+e-u_d)+p^{(n-1)d+1}(u_2-u_1)+\cdots\\
&\quad +p^{nd-1}(u_d-u_{d-1})+p^{nd}(u_1+e-u_d)
\end{aligned}$$

$$\begin{aligned}
&= u_1+\frac{p^{(n+1)d}-p^d}{p^d-1}(u_1+e-u_d)+p\frac{p^{nd}}{p^d-1}(u_2-u_1)+\cdots\\
&\quad +p^{d-1}\frac{p^{nd}}{p^d-1}(u_d-u_{d-1})\\
&= u_1+\frac{p^{nd}-1}{p^d-1}\Big(p(u_2-u_1)+p^2(u_3-u_2)+\cdots\\
&\quad +p^{d-1}(u_d-u_{d-1})+p^d(u_1+e-u_d)\Big).
\end{aligned}$$

Mais $p^j(u_{j+1}-u_j)=i(\sigma_{j+1})-i(\sigma_j)$ pour $j=1,\cdots,d-1$ et $p^d(u_1+e-u_d)=i_1(\sigma_1)-i(\sigma_d)$, donc

$$i_n(\sigma_1)=i(\sigma_1)+\frac{p^{nd}-1}{p^d-1}(i_1(\sigma_1)-i(\sigma_1)).$$

Comme l'indice de ramification absolu e de F est $\leq (p-1)\varphi_G(i(\sigma_j))$ la même démonstration donne, d'après le corollaire au lemme 2 :

$$i_n(\sigma_j)=i(\sigma_j)+\frac{p^{nd}-1}{p^d-1}(i_1(\sigma_j)-i(\sigma_j)) \text{ pour tout } j\in\{1,2,\cdots,d\}.$$

Enfin, le fait que G soit d'indice fini dans son centralisateur dans $\mathfrak{G}$ provient du caractère pleinement fidèle du foncteur "corps de normes" [10] : si $\tau_1(t)$ est une série de $\mathfrak{G}$ qui commute avec les éléments de G alors le sous-groupe fermé G_1 de $\mathfrak{G}$ engendré par $G\cup\{\tau_1\}$ s'identifie au groupe de Galois de l'extension E/F_1 où F_1 est une extension de $\mathbb{Q}_p$ contenue dans F ; si $\tau_2(t)$ est une série de $\mathfrak{G}$ qui commute avec les élémemts de G_1 alors le sous-groupe fermé G_2 de $\mathfrak{G}$ engendré par $G_1\cup\{\tau_2\}$ s'identifie au groupe de Galois de l'extension E/F_2 où F_2 est une extension de $\mathbb{Q}_p$ contenue dans F_1 et ainsi de suite. Il existe donc un entier n_0 tel que G_{n_0} soit le centralisateur de G dans $\mathfrak{G}$ et G est d'indice fini dans G_{n_0}.

Remarque 1. Il convient de noter que la situation envisagée dans les hypothèses du théorème n'est pas exceptionnelle : soit e un entier ≥ 1 et soit K une extension finie de $\mathbb{Q}_p$ d'indice de ramification e ; étant donnés des entiers $u_1<u_2<\cdots<u_d$ avec $u_1\geq e/(p-1)$, $u_d<ep/(p-1)$ et

$p \nmid u_j$, il existe (lemme 2) d $\mathbb{Z}_p$-extensions $L_1, L_2, \cdots, L_d$ dont les premiers sauts de ramification sont respectivement $u_1, u_2, \cdots, u_d$. Il en résulte que la suite des sauts de ramification supérieurs de L_j/K est $(u_j + ne)$, pour tout $j = 1, 2, \cdots, d$. Soit M l'extension abélienne composée par toutes les $\mathbb{Z}_p$-extensions L_j. Comme ces $\mathbb{Z}_p$-extensions sont arithmétiquement disjointes au sens de Maus [6], l'ensemble des sauts de ramification supérieurs de M est exactement la réunion des d progressions arithmétiques $(u_j + ne)$, $j = 1, 2, \cdots, d$. Le foncteur corps des normes applique alors le groupe de Galois de M/K sur un groupe d'automorphismes de $k((t))$ (où k est le corps résiduel de K) dont la ramification satisfait les conditions du théorème.

Remarque 2. D'après le théorème, si une série formelle σ fait partie d'un système $\mathbb{Z}_p$-indépendants de d séries formelles commutant deux à deux en ce sens que le groupe fermé qu'elles engendrent est isomorphe à $\mathbb{Z}_p^d$, alors $i_{n+1}(\sigma) \equiv i_n(\sigma) \bmod p^{nd+1}$ pour n assez grand, cela précise un résultat bien connu de S. Sen [7]. Ce résultat est également une conséquence de la généralisation par Wintenberger du théorème de Hasse-Arf [10].

Bibliographie

[1] I. FESENKO, *On just infinite pro-p-groups and arithmetically profinite extensions of local fields.* J. Reine Angew. Math. **517** (1999), 61–80.

[2] F. LAUBIE, M. SAÏNE, *Ramification of some automorphisms of local fields.* J. Number Theory **72** (1998), 174–182.

[3] F. LAUBIE, A. MOVAHHEDI, A. SALINIER, *Systèmes dynamiques non archimediens et corps des normes.* Preprint.

[4] J. LUBIN, *Nonarchimedean dynamical systems.* Comp. Math. **94** (1994), 321–346.

[5] M.A. MARSHALL, *Ramification groups of Abelian local field extensions.* Canad. J. Math. **23** (1971), 278–281.

[6] E. MAUS, *Arithmetische dijunkte Krper.* J. Reine Angew. Math. **226** (1967), 184–203.

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

[8] J.-P. SERRE, *Corps locaux.* Hermann, Paris (1962).

[9] J.-P. WINTENBERGER, *Le corps des normes de certaines extensions finies des corps locaux ; applications.* Ann. Sci. Ecole Norm. Sup. **16** (1983), 59–89.

[10] J.-P. WINTENBERGER, *Extensions abéliennes et groupes d'automorphismes des corps locaux.* C.R. Acad. Sci. Paris **290** (1980), 201–203.

François LAUBIE
LACO et INRIA de Rocquencourt
Département de Mathématiques
123, avenue Albert-Thomas
87060 Limoges Cedex
France
E-mail : laubie@unilim.fr