

MÉMOIRES DE LA S. M. F.

JEAN-MARC FONTAINE

**Points d'ordre fini d'un groupe formel sur une
extension non ramifiée de \mathbb{Z}_p**

Mémoires de la S. M. F., tome 37 (1974), p. 75-79

<http://www.numdam.org/item?id=MSMF_1974__37__75_0>

© Mémoires de la S. M. F., 1974, tous droits réservés.

L'accès aux archives de la revue « Mémoires de la S. M. F. » (<http://smf.emath.fr/Publications/Memoires/Presentation.html>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

POINTS D'ORDRE FINI D'UN GROUPE FORMEL SUR
 UNE EXTENSION NON RAMIFIÉE DE \mathbb{Z}_p

par

Jean-Marc FONTAINE

--:--:--

1. Soit K un corps local de caractéristique 0 , dont le corps résiduel k est parfait de caractéristique $p \neq 0$. Soit \bar{K} une clôture algébrique de K . Soit A (resp. \bar{A}) l'anneau des entiers de K (resp. \bar{K}) et soit \mathfrak{m} (resp. $\bar{\mathfrak{m}}$) l'idéal maximal de A (resp. \bar{A}).

Soit $F(X, Y) \in A[[X, Y]]$ une loi de groupe formel à un paramètre définie sur A (cf. [2] pour les résultats classiques sur les groupes formels). On note $F(\bar{\mathfrak{m}})$ le groupe des points de F à valeurs dans $\bar{\mathfrak{m}}$ (i.e. l'ensemble $\bar{\mathfrak{m}}$ muni de la loi de groupe $(\alpha, \beta) \mapsto F(\alpha, \beta)$). C'est un groupe abélien d'élément-neutre 0 .

On suppose la hauteur h de F finie. Le groupe de torsion E de $F(\bar{\mathfrak{m}})$ est alors isomorphe à $(\mathbb{Q}_p/\mathbb{Z}_p)^h$ et le module de Tate de F , $T = \text{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, E)$ est un \mathbb{Z}_p -module libre de rang h . Le groupe $\mathfrak{G} = \text{Gal}(\bar{K}/K)$ opère continûment sur T , d'où un homomorphisme de \mathfrak{G} dans $\text{Aut}_{\mathbb{Z}_p}(T) (\simeq \text{GL}_h(\mathbb{Z}_p))$. L'image H de \mathfrak{G} par cet homomorphisme s'identifie au groupe de Galois de l'extension $L = K(E)$ de K engendrée par les points d'ordre fini de $F(\bar{\mathfrak{m}})$.

On s'intéresse à la question suivante : on se donne le corps K et on se fixe un entier h . Soit H' un sous-groupe de $\text{GL}_h(\mathbb{Z}_p)$. Quelles conditions doit vérifier H' pour que (avec les notations qui précèdent) il existe F , défini sur A , de hauteur h , tel que $H = \text{Gal}(L/K) \simeq H'$?

Le but de cet exposé est de donner, dans le cas où p est une uniformisante de A , des conditions nécessaires. Celles-ci sont également suffisantes lorsque $h = 1$ ou 2 . On renvoie à [1] pour des démonstrations complètes.

2. On conserve les notations et hypothèses qui précèdent et on suppose désormais que p est une uniformisante de A . On note \bar{T} la réduction de T modulo p et on pose

\bar{K}
 L } $M = \text{End}_{\mathbb{Z}_p}(T)$, $G = \text{Aut}_{\mathbb{Z}_p}(T)$, $\tilde{M} = \text{End}_{\mathbb{F}_p}(\tilde{T})$, $\tilde{G} = \text{Aut}_{\mathbb{F}_p}(\tilde{T})$.
 On munit le groupe G de sa filtration naturelle : on pose
 L_{n+1} } $G(n) = \{g \in G \mid g-1 \in p^n M\}$, pour tout entier $n \geq 0$.
 L_n } Pour $n \geq 0$, soit $E_n = \{\alpha \in E \mid p^n \alpha = 0\}$. Le corps $L_n = K(E_n)$ est
 le corps fixe de $H(n) = H \cap G(n)$. On a $L = \varprojlim L_n$ et $H = \varprojlim H/H(n)$.
 L_1 } C'est un sous-groupe fermé de $G = \varprojlim G/G(n)$. Le groupe $G/G(1)$
 $K=L_0$ } s'identifie à \tilde{G} et le groupe $J = \text{Gal}(L_1/K)$ s'identifie au sous-
 groupe $H/H(1)$ de \tilde{G} .

3. En regardant la série formelle qui donne la multiplication par p pour la loi F , on constate que les points d'ordre p sont les racines d'un polynôme d'Eisenstein de degré p^h-1 à coefficients dans A . On en déduit que L_1 est l'extension totalement et modérément ramifiée de degré p^h-1 du corps obtenu en adjoignant à K les racines (p^h-1) -ièmes de l'unité.

Dans toute la suite, on suppose que K contient déjà les racines (p^h-1) -ièmes de l'unité. On pose $q = p^h$ et on note \mathbb{F}_q l'unique sous-corps de k ayant q éléments. L'extension L_1/K est alors totalement et modérément ramifiée de degré $q-1$ et J s'identifie (cf. [3], p.75) au groupe multiplicatif \mathbb{F}_q^\times de \mathbb{F}_q . D'où un plongement de \mathbb{F}_q^\times dans \tilde{G} qui se prolonge en un plongement du corps \mathbb{F}_q dans l'anneau \tilde{M} .

4. Pour $n \geq 1$, le groupe $G/G(n+1)$ opère par conjugaison sur $G(n)/G(n+1)$. On voit tout de suite que $G(1)/G(n+1)$ opère trivialement ; par passage au quotient, $G(n)/G(n+1)$ devient un \tilde{G} -module, donc a fortiori un J -module. Il est clair que $H(n)/H(n+1)$ est un sous- J -module de $G(n)/G(n+1)$.

Le groupe J opère également sur \tilde{M} par conjugaison. L'application, qui à g dans $G(n)$ fait correspondre $(g-1)/p^n$, définit, par passage au quotient, un isomorphisme du J -module $G(n)/G(n+1)$ sur \tilde{M} . Finalement, $\text{Gal}(L_{n+1}/L_n)$ s'identifie à un sous- J -module \tilde{H}_n de \tilde{M} .

5. La structure du J -module \tilde{M} se trouve être très simple. On vérifie que la décomposition de \tilde{M} en somme directe de ses composants isotypiques peut se mettre sous la forme

$$\tilde{M} = \bigoplus_{i \in \mathbb{Z}/h\mathbb{Z}} \tilde{M}_i ,$$

la structure de chaque \tilde{M}_i étant donnée par :

- le groupe \tilde{M}_i peut s'identifier au groupe additif de \mathbb{F}_q ;
- si $\epsilon \in J = \mathbb{F}_q^\times$ et si $\lambda \in \tilde{M}_i$, ϵ opère sur \tilde{M}_i par $\epsilon : \lambda \mapsto \epsilon^{1-p^i} \lambda$.

En particulier, J opère trivialement sur \tilde{M}_0 ; et les \tilde{M}_i , pour $i \neq 0$, sont des J -modules simples deux à deux non isomorphes.

6. A l'aide d'un argument de ramification, on montre que, pour tout $n \geq 1$, $\tilde{M}_0 \subset \tilde{H}_n$. On voit donc que \tilde{H}_n est la somme directe de certains des \tilde{M}_i .

De plus, il est immédiat que si $\tilde{M}_i \subset \tilde{H}_n$, alors $\tilde{M}_i \subset \tilde{H}_{n+1}$ (pour $p \neq 2$ ou pour $p = 2$ et $n \geq 2$, cela résulte de ce que l'élévation à la puissance p -ième définit, par passage aux quotients, un isomorphisme de $G(n)/G(n+1)$ sur $G(n+1)/G(n+2)$ qui, après identification de ces deux groupes avec \tilde{M} , devient l'identité ; pour $p = 2$ et $n = 1$ il faut regarder un peu plus en détail l'élévation au carré).

La suite des sous-groupes \tilde{H}_n est donc complètement déterminée par la fonction $v_H : \mathbb{Z}/h\mathbb{Z} \rightarrow \mathbb{N}^* \cup \{+\infty\}$ définie par

$$v_H(i) = \text{le plus petit entier } n \geq 1 \text{ tel que } \tilde{M}_i \subset \tilde{H}_n ;$$

on a en effet, pour $n \geq 1$: $\tilde{H}_n = \bigoplus_{v_H(i) \leq n} \tilde{M}_i$.

7. On a le résultat suivant :

THEOREME. - Soit $v : \mathbb{Z}/h\mathbb{Z} \rightarrow \mathbb{N}^* \cup \{+\infty\}$ vérifiant $v(0) = 1$. Pour qu'il existe un sous-groupe fermé H de $GL_h(\mathbb{Z}_p)$ vérifiant (avec des conventions évidentes)

$$\tilde{H} = \mathbb{F}_q \quad \text{et} \quad \tilde{H}_n = \bigoplus_{v(i) \leq n} \tilde{M}_i$$

il faut et il suffit que la fonction v vérifie

$$v(i+j) \leq v(i) + v(j) \quad \text{pour } i, j \text{ dans } \mathbb{Z}/h\mathbb{Z}.$$

Le groupe H est alors unique à isomorphisme près.

On montre que la condition est nécessaire en regardant l'application de $(G(m)/G(m+1)) \times (G(n)/G(n+1))$ dans $G(m+n)/G(m+n+1)$ définie par passage aux quotients à partir du commutateur d'un élément de $G(m)$ et d'un élément de $G(n)$.

Pour voir que la condition est suffisante, on peut introduire l'anneau R

des entiers de l'extension non ramifiée de \mathbb{Q}_p de degré h et utiliser le fait que l'anneau des matrices carrées d'ordre h à coefficients dans \mathbb{Z}_p est isomorphe à l'anneau

$$D = R + Rf + \dots + Rf^{h-1}$$

dans lequel la multiplication est définie par

$$\begin{cases} f \cdot a = \varphi(a) \cdot f & \text{si } a \in R \text{ (} \varphi = \text{Frobenius)} \\ f^h = 1 & . \end{cases}$$

Si on pose

$$H = \left\{ a_0 + a_1 f + \dots + a_{h-1} f^{h-1} \mid \begin{array}{l} a_0 \text{ est une unité,} \\ \text{pour } i \neq 0, a_i \text{ est divisible par } p^{\nu(i)} \end{array} \right\}$$

on vérifie que H est un sous-groupe du groupe multiplicatif des unités de D qui répond à la question.

8. Réciproquement, on peut se poser la question suivante : soit A l'anneau des entiers d'un corps local de caractéristique 0, à corps résiduel de caractéristique $p \neq 0$, absolument non ramifié ; soit h un entier ≥ 1 et soit ν une application de $\mathbb{Z}/h\mathbb{Z}$ dans $\mathbb{N}^* \cup \{+\infty\}$ vérifiant les hypothèses du théorème ; on suppose que A contient les racines $(p^h - 1)$ -ièmes de l'unité ; existe-t-il une loi de groupe formel F définie sur A , à un paramètre et de hauteur h , telle que, avec les notations précédentes, $\nu_H = \nu$? La réponse est oui si $h = 1$ ou 2 (et trivialement si $h = 1$). Pour $h \geq 3$ c'est un problème ouvert.

Dans le cas $h = 2$, on voit que la donnée de ν est équivalente à celle de $\nu(1)$. On sait associer à toute loi de groupe formel F de hauteur 2 sur A un polynôme d'Eisenstein de degré 2 à coefficients dans A (cf. [1] ; si $A = \mathbb{Z}_p$, c'est simplement le polynôme caractéristique du Frobenius de la réduction de F modulo p). On peut montrer que $\nu(1)$ est égal à la valuation du terme de degré 1 de ce polynôme. On peut aussi, mais c'est assez pénible, calculer explicitement les nombres de ramification de l'extension $K(E)/K$.

BIBLIOGRAPHIE

- [1] J.M. FONTAINE. - Groupes formels lisses sur un anneau de vecteurs de Witt (à paraître).
- [2] A. FRÖHLICH. - Formal Groups, Lecture Notes in Maths 74, Springer 1968.
- [3] J.P. SERRE. - Corps locaux, 2e édition, Hermann 1968.

--:--:--

Université scientifique et médicale de
Grenoble
Laboratoire de Mathématiques Pures
associé au C.N.R.S. n° 188
BP 116
38402 ST MARTIN D'HERES