UNIVERSITÉ SCIENTIFIQUE ET MÉDICALE DE GRENOBLE
Laboratoire de Mathématiques Pures associé au C.N.R.S.

Jean-Marc Fontaine
INSTITUT
DE MATHÉMATIQUES PURES
Boîte Postale 116
38402 SAINT-MARTIN-D'HÈRES

Téléphone (76) 87-45-61 à 64

le 1° mars 1974

Cher Serre,

Voici, cette fois-ci, quelques résultats sur les points d'ordre fini des groupes formels ; et quelques indications sur les applications aux courbes elliptiques... le tout sans démonstrations !

Dans toute cette lettre, p est un nombre premier, K un corps local, de car. 0 , d'anneau des entiers A , de corps résiduel k (supposé parfait) de car. p . Je suppose que p est une uniformisante de A . Je note $\overline{K}$ une clôture algébrique de K , et $\overline{k}$ la clôture algébrique de k correspondante. Je désigne par v la valuation de $\overline{K}$ normalisée par $v(p) = 1$.

Je me donne un entier $h \geqslant 1$, et je pose $q = p^h$. Je note $\underline{Q}_q$ l'unique extension non ramifiée de $\underline{Q}_p$ de degré h contenue dans $\overline{K}$, $\underline{Z}_q$ l'anneau de ses entiers et $\underline{F}_q$ le corps résiduel.

Pour décrire commodément mon groupe de Galois je vais avoir besoin de décrire

1 - Certains groupes d'automorphismes des $\underline{Z}_q$-modules libres de rang un.

Grâce à Frobenius, le groupe $\underline{Z}/h\underline{Z}$ s'identifie canoniquement à $\mathrm{Gal}(\underline{Q}_q/\underline{Q}_p)$ et opère ainsi sur $\underline{Z}_q$. Soit M l'anneau des endomorphismes de $\underline{Z}_q$, considéré comme $\underline{Z}_p$-module. Il s'identifie à l'anneau non commutatif $\underline{Z}_q[\underline{Z}/h\underline{Z}]$, i.e. tout élément de M s'écrit d'une manière et d'une seule sous la forme

$$\sum_{i \in \underline{Z}/h\underline{Z}} b_i i \quad \text{(avec les } b_i \text{ dans } \underline{Z}_q \text{)},$$

et on a $b.i = i(b).i$ si $b \in \underline{Z}_q$, $i \in \underline{Z}/h\underline{Z}$.

Je vais maintenant définir une famille de sous-groupes de $G =$

$\mathrm{Aut}_{\underline{Z}_p}(\underline{Z}_q^h)$ ($\simeq GL_h(\underline{Z}_p)$).

Soit ν une application de $\underline{Z}/h\underline{Z}$ dans $\underline{N}^* \cup \{+\infty\}$ vérifiant

(i) $\nu(0) = 1$,

(ii) $\nu(i+j) \leq \nu(i) + \nu(j)$, pour i,j dans $\underline{Z}/h\underline{Z}$.

Je pose

$$H_\nu = \left\{ \sum_{i \in \underline{Z}/h\underline{Z}} b_i i \;\middle|\; \begin{array}{l} b_0 \text{ est une unité de } \underline{Z}_q \text{ ,} \\ v(b_i) \geq \nu(i) \text{ pour tout } i \neq 0 \end{array} \right\} .$$

Il est (presqu') immédiat que H_ν est un sous-groupe de G . Il est clair que H_ν est invariant par conjugaison par les éléments de $\underline{Z}/h\underline{Z}$ et que l'intersection de H_ν avec $\underline{Z}/h\underline{Z}$ est réduite à l'élément-neutre. Pour tout sous-groupe J de $\underline{Z}/h\underline{Z}$, je peux donc parler du produit semi-direct de H_ν par J : c'est encore un sous-groupe de G et je le note $H_\nu J$

Maintenant tu peux remarquer que les $H_\nu J$ sont invariants par conjugaison par les unités de $\underline{Z}_q$.

Soit alors V un $\underline{Z}_q$-module libre de rang un. Si je choisis un générateur α de V j'ai un ismomorphisme de $\underline{Z}_q$ sur V , donc un isomorphisme de G sur $G' = \mathrm{Aut}_{\underline{Z}_p}(V)$. Pour tout sous-groupe H de G je note H' son image dans G' . En général H' dépend du choix de α

Mais si je suppose que H est invariant par conjugaison par les unités de $\underline{Z}_q$, alors H' ne dépend plus du choix de α (seul l'isomorphisme de H sur H' en dépend). J'ai donc une façon canonique d'associer à un tel H un sous-groupe H' de G' .

Je crois que mainteaant je peux décrire mon groupe de Galois.

2 - Le groupe de Galois des points d'ordre fini : partie "directe".

Soit $\Gamma(X,Y)$ une loi de groupe formel à un paramètre, de hauteur finie h , définie sur A . Soit V le module de Tate. Le groupe $\mathrm{Gal}(\bar{K}/K)$ opère sur V et je note H' son image dans $\mathrm{Aut}_{\underline{Z}_p}(V)$. Je peux aussi considérer H' comme le groupe de Galois de l'extension K_Γ de K engendrée par les points d'ordre fini de Γ . Bien sûr, si Γ n'est pas un Lubin-Tate, je n'ai pas de structure canonique de $\underline{Z}_q$-module sur

V. Mais il y a des structures de $\mathbb{Z}_q$-module qui sont moins mauvaises q d'autres. Et j'ai le résultat suivant :

Théorème :

1) L'extension maximale non ramifiée de K contenue dans L est le corps obtenu en adjoignant à K les racines (q-1)-ièmes de l'unité. En particulier son groupe de Galois s'identifie à un sous-groupe J de $\mathbb{Z}/h\mathbb{Z}$.

2) Il existe une application ν (unique) : $\mathbb{Z}/h\mathbb{Z} \to \mathbb{N}^* \cup \{+\infty\}$, vérifian les conditions (i) et (ii) , et une structure de $\mathbb{Z}_q$-module libre de rang un sur V (qui n'est unique que dans le cas d'un Lubin-Tate) tel les que le groupe de Galois H' soit le groupe $(H_\nu J)'$ (le groupe d'inertie étant H'_ν).

3 - Le groupe de Galois des points d'ordre fini : partie "réciproque".

Comme je te l'ai dit dans ma précédente lettre, l'anneau $K[[X]]$ d séries formelles à coefficients dans K a une structure de module sur l'anneau non commutatif $A[[F]]$ (sauf que dans la dite lettre A s'a pelait W_k). Je te rappelle comment F opère :

$F(\sum b_i X^i) = \sum \sigma(b_i) X^{pi}$ (où σ est le Frobenius absolu).

Soit $\ell(X)$ le logarithme de Γ . Je te dirai dans une prochaine let tre pourquoi il existe un polynôme de la forme

$$P_\Gamma = p + a_1 F + .. + a_{h-1} F^{h-1} + a_h F^h$$

(avec les a_j dans A , $v(a_h) = 0$ et $v(a_j) \geqslant 1$ pour $1 \leqslant j \leqslant h-1$) et un seul tel que $P_\Gamma(\ell(X))$ soit une série formelle à coefficients dans A (en fait une série formelle à coeff. dans l'idéal maximal).

Ceci étant, avec des notations évidentes, et sauf erreur, j'ai

Théorème : On a $\inf_{i \neq 0} \nu(i) = \inf_{1 \leqslant j \leqslant h-1} v(a_j)$.

En tout cas, c'est à peu près évident que le premier est $\geqslant$ au secon Et dans le cas de hauteur 2 , j'en suis absolument certain : ça me don ne $\nu(0) = 1$, $\nu(1) = v(a_1)$ (le polynôme P_Γ est de la forme

$p + a_1 F + a_2 F^2$) et ça détermine complètement le groupe H' .

Remarque : Je reviens au cas où h est quelconque. Je sais montrer que l'anneau A' des endomorphismes absolus de Γ (i.e. l'anneau des endomorphismes de Γ sur l'anneau des entiers d'une extension finie K assez grosse) est formé des a entiers dans l'extension maximale non ramifiée de K qui vérifient $aP_\Gamma = P_\Gamma a$. Soit I le sous-groupe de $\underline{Z}/h\underline{Z}$ engendré par les images des entiers j tels que $a_j \neq 0$. Alors A' est l'anneau des entiers de $\underline{Q}_q^I$. Le fait que H' est ouvert dans $\mathrm{Aut}_{A'}(V)$ revient alors à dire que

$$I = \{ i \in \underline{Z}/h\underline{Z} \mid \nu(i) \neq +\infty \} ,$$

chose que je crois savoir démontrer directement. Ceci donne à penser que même pour $h \neq 2$, on doit pouvoir relier simplement les $\nu(i)$ aux $v(a_j)$.

4 - La ramification.

Ici $h = 2$. J'écarte Lubin-Tate pour cause de trivialité, et je suppose donc que $\nu(1) = v(a_1) = r$ est fini.

Je vais énoncer un résultat, puis te dire ce qu'il faut en penser :

"Théorème" : La suite des nombres supérieurs de ramification de l'extension est

$0, 1/(p+1) , 1 , 1 + p/(p+1) , 2 , .. , n , n + p/(p+1) , ..$

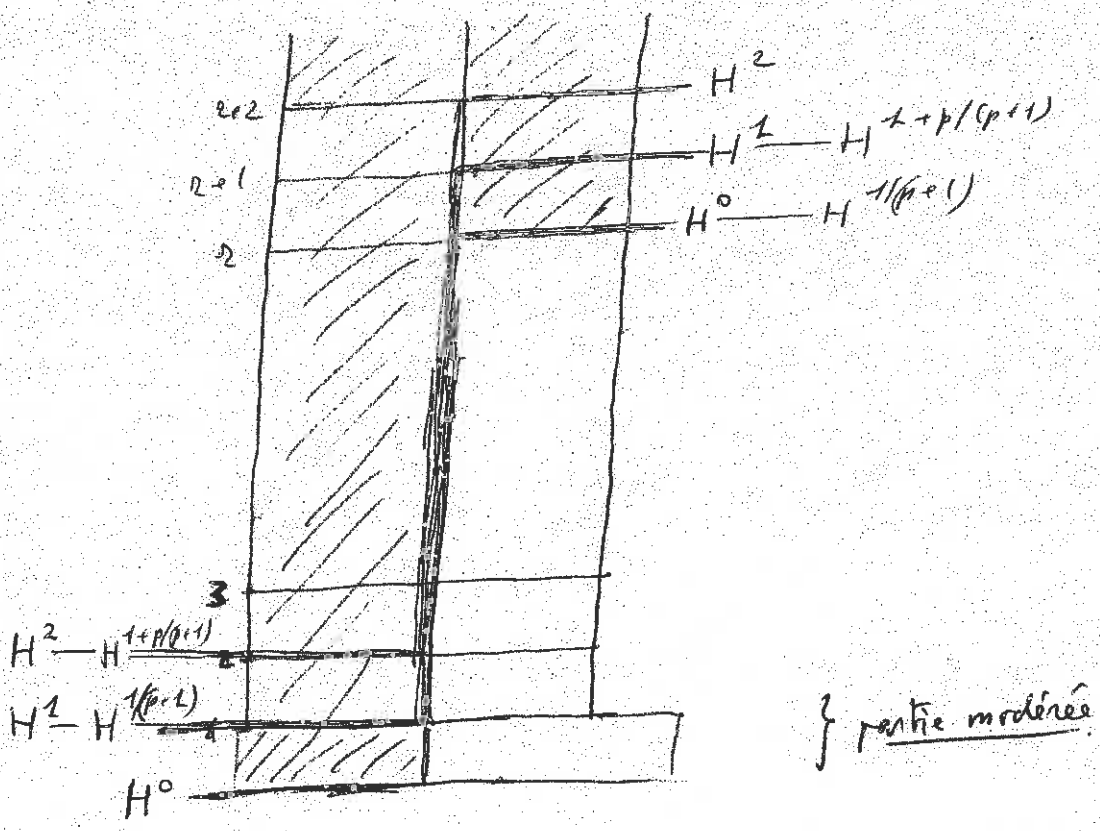
(voir le dessin qui est préférable à un long discours pour expliquer à quels sous-groupes ça correspond).

Ce qu'il faut en penser !

D'abord j'ai bien écrit ce que je voulais écrire (le premier qui n'est pas entier est bien $1/(p+1)$, et, pour les autres, c'est bien $p/(p+1)$ qu'il faut rajouter).

Ensuite, si $r = 1$, je ne sais pas le démontrer (et je n'ai pas de sentiment, comme tu dirais !).

Enfin, pour $r \neq 1$, je n'en donnerais pas ma tête à couper : j'ai confiance car mon calcul est vraiment complet. Mais autrefois j'étais convaincu qu'on a $n + 1/(p+1)$ au lieu de $n + p/(p+1)$. Mais si on réfléchit au sens dans lequel il est le plus facile de se tromper, je


2=2
2=1
2
3
H^2
$H^1 - H^{1+p/(p+1)}$
$H^0 - H^{1/(p+1)}$
$H^2 - H^{1+p/(p+1)}$
$H^1 - H^{1/(p+2)}$
H^0
} partie modérée

crois vraiment, qu'à condition de rajouter $r \neq 1$, on peut laisser tomber les guillemets dans mon théorème.

5 - Les courbes elliptiques.

Je suppose maintenant $p \neq 2$ et je considère une courbe elliptique E définie sur A. Je peux toujours supposer que E est donnée par une équation de la forme

$$y^2 = R(x)$$

où $R(x)$ est un polynôme du troisième degré, à coeff. dans A, dont réduction modulo p est un polynôme du troisième dégré dont les racin dans $\bar{k}$, sont simples.

Si je choisis une coordonnée X, la composante connexe de $E(p)$ e une loi de groupe formel Γ à unparamètre, de hauteur $h = 1$ ou 2. je note encore $\ell(X)$ le logarithme de Γ.

Pour tout entier $s \geq 0$, je pose

H_s = coefficients de x^{p^s-1} dans $(R(x))^{(p^s-1)/2}$

(H comme Hasse, tu ne confondras pas les coeff. H_s avec les groupe H_y du n° 3 que j'aurais dû appeler autrement !).

Exemple: si $R(x) = 4x^3 - g_2x - g_3$, on a

$$H_s = \sum_{2m+3n=(p^s-1)/2} (-1)^{m+n} 4^{((p^s-1)/2)-m-n} \frac{((p^s-1)/2)!}{m!n!(((p^s-1)/2)-m-n)!} g_2^m g_3^n$$

(c'est pas beau, mais c'est on ne peut plus explicite).

Le point c'est que l'on peut choisir la coordonnée X pour que

$$\ell(X) = \sum_{n \geq 0} p^{-n} H_n X^{p^n} .$$

Il est alors facile de calculer h et de dire comment calculer le polynôme P_Γ défnit au n° 3 (si $c \in K$, je note c^σ son image par Frobenius).

Premier cas : $h = 1$. Ceci se produit si et seulement si la réduction modulo p de H_1 (qui est, bien sûr, l'invariant de Hasse) n'est pas nulle. Alors $P_\Gamma = p + a_1 F$, où a_1 est une unité de A.

Tous les H_n sont alors des unités de A et on a

$$H_n + a_1 H_{n-1}^{\sigma} \equiv 0 \pmod{p^n} \text{ , pour tout } n \geqslant 1 \text{ ,}$$

ce qui fait que la connaissance de H_n et H_{n-1} détermine a_1 modulo p^n et que

$$a_1 = -\lim_{n\to\infty} H_n / H_{n-1}^{\sigma} \text{ .}$$

Deuxième cas : $h = 2$. Donc $v(H_1) \geqslant 1$. Alors $P_\Gamma = p + a_1 F + a_2 F^2$ (avec a_1 et a_2 dans A , $v(a_1) \geqslant 1$, $v(a_2) = 0$). Je dois avoir

$$H_n + a_1 H_{n-1}^{\sigma} + p a_2 H_{n-2}^{\sigma^2} \equiv 0 \pmod{p^n} \text{ , pour } n \geqslant 1 \text{ .}$$

On voit d'abord que ceci implique

$$v(H_{2n}) = n \text{ , } v(H_{2n+1}) \geqslant n+1 \text{ .}$$

Et puis cela permet de calculer a_1 et a_2 . On peut écrire :

$$a_1 \equiv \frac{H_{2n} H_{2n-1}^{\sigma^2} - H_{2n+1} H_{2n-2}^{\sigma^2}}{H_{2n-2}^{\sigma^2} H_{2n}^{\sigma} - H_{2n-1}^{\sigma+\sigma^2}} \pmod{p^{n+1}}$$

$$a_2 \equiv p^{-1} \cdot \frac{H_{2n+1}^{1+\sigma} - H_{2n}^{\sigma} H_{2n+2}}{H_{2n}^{\sigma+\sigma^2} - H_{2n-1}^{\sigma^2} H_{2n+1}^{\sigma}} \pmod{p^{n+1}} \text{ .}$$

Maintenant si tu veux savoir quand le groupe de Galois se remplit, il faut calculer ce que j'ai appelé $\gamma(1)$ dans le n° 3 , ou encore $r = v(a_1)$.

Soit n un entier fixé et soit B le numérateur de la fraction qui donne a_1 modulo p^{n+1} dans la formule ci-dessus. On voit tout de suite que $B = p^{2n} C$, avec C entier sur A et que

- si $v(C) < n$, $r = v(C) + 1$,
- si $v(C) \geqslant n$, $r \geqslant n+1$.

Exemple : $p = 5$ et $R(x) = 4x^3 - g_2 x - g_3$.

On voit tout de suite que $h = 2$ si et seulement si $g_2 \equiv 0 \pmod 5$ et qu'on a alors bonne réduction modulo 5 si et seulement si g_3 est une unité. Le calcul des H_n est relativement simple car les termes des grosses puissances de g_2 sont divisibles par de grosses puissances de 5 . J'ai calculé le numérateur de la fraction indiquée pour $n = 2$ (je ne pense pas m'être trompé, il y a des moyens de contrôle !) :

$$C \equiv \tfrac{1}{2}\left(g^{\sigma^2}.g_3^{104+20\sigma^2} - g g_3^{520+4\sigma^2} \right) \pmod{25} ,$$

ce qui fait que $r = 1$, 2 ou est ≥ 3 suivant que l'expression entre parenthèses est de valuation 0, 1 ou ≥ 2 (dans cette expression, j'ai posé $g_2 = 5g$).

Par exemple, $r = 1$ si et seulement si g et g_3 sont des unités vérifiant $g^{24} \not\equiv g_3^{16} \pmod 5$.

En outre, on vérifie que si g et g_3 sont dans $\underline{Z}_p$, ou si $g = 0$ alors $C \equiv 0 \pmod{25}$: c'est conforme à ce que l'on sait par ailleurs dans les deux cas, on a affaire à un Lubin-Tate.

*

Et bien je ne te "dois" plus qu'une lettre sur les groupes formels. Elle devrait se faire attendre un peu plus : j'ai pas mal de boulot (innombrables réunions, un séminaire qui va m'obliger à regarder d'assez près Brauer et les représentations modulaires,...). J'ai un peu en vie de rejeter un oeil sur ces calculs sur les courbes elliptiques (pa exemple, il ne devrait pas être très difficile de montrer que, si $h = 2$ et E est définie sur $\underline{Z}_p$, la suite des $p^{-n}H_{2n}$ et celle des $p^{-n}H_{2n+1}$ convergent. Cela entrainerait $a_1 = 0$ et $a_2 = -1$: Lubin-Tate !). Et je ne dis pas que je vais attendre le 20 mars pour faire du ski, d'autant plus que le temps semble s'y prêter !

J'espère que la digestion de ces deux lettres ne te sera pas trop pénible. A part quelques problèmes justement d'ordre digestif, le sentiment filial (resp. maternel, resp. paternel) d'Isabelle (resp. Laurence, resp. moi) semble se développer normalement.

On vient d'avoir ~~attend~~ de tes nouvelles (Val-d'Isère ?). Merci !

Amitiés

Jean-Pierre Serre

P.S. : Même le n° 5 de ma précédente lettre ne te dit pas grand chose ?