Schémas propres et lisses sur $\mathbb{Z}$

by

Jean-Marc Fontaine

91 - 02

RÉSUMÉ : On se propose de prouver le résultat suivant (obtenu aussi indépendamment par Abrashkin) :

THÉORÈME. — *Soit X une variété propre et lisse sur $\mathbb{Q}$ ayant bonne réduction partout. Alors $H^j(X, \Omega^i_X) = 0$ si $i, j \in \mathbb{N}$ vérifient $i \neq j$ et $i + j \leq 3$.*

Ceci se déduit d'un théorème montrant que l'action de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ sur un sous-quotient tué par p d'une représentation cristalline à poids de Hodge-Tate entre 0 et $p-2$ n'est pas "trop ramifiée" (voir un énoncé précis plus bas) en utilisant le théorème de comparaison entre cohomologie cristalline et cohomologie étale p-adique d'une part et les majorations de discriminants à la Odlyzko d'autre part.

ABSTRACT : We prove the following results (see also Abrashkin [Ab5]) :

THEOREM 1. — *Let X be a proper and smooth variety over $\mathbb{Q}$. Assume X has good reduction everywhere. Then $H^j(X, \Omega^i_X) = 0$ if $i, j \in \mathbb{N}$ satisfy $i \neq j$ and $i + j \leq 3$.*

THEOREM 2. — *Let K be a field of* char. 0 *complete with respect to a discrete valuation, with perfect residue field of* char. $p > 0$, *absolutely unramified. Let $\overline{K}$ be an algebraic closure of K and $G_K = \mathrm{Gal}(\overline{K}/K)$. Let $r \in \mathbb{Z}$ satisfying $0 < r < p-1$ and V be a p-adic crystalline representation of G_K whose Hodge-Tate weights $\in [0, r]$. Let U a sub-quotient of V, stable under G_K and killed by p. Let H the kernel of the action of G_K on U and $L = \overline{K}^H$. If v_0 denote the valuation of L such that $v_0(p) = 1$ and if $\mathcal{D}_{L/K}$ is the different of the extension L/K, then*

$$v_0(\mathcal{D}_{L/K}) \leq 1 + r/(p-1).$$

Mots-clés : Représentations p-adiques, cohomologie cristalline, cohomologie étale, cohomologie de de Rham, discriminant, ramification.

Code matière AMS 1980 (version 1985) : 11 G 25, 11 G 35, 11 S 20, 14 F 30, 14 F 40, 14 G 20.

Schémas propres et lisses sur $\mathbb{Z}$

Jean-Marc FONTAINE

INTRODUCTION

On sait ([Ab1], [Fo1]) qu'il n'existe pas de schéma abélien sur $\mathbb{Z}$ non trivial. Ce texte reproduit une lettre adressée à William Messing dans laquelle je montre que, plus généralement, *si $\mathcal{X}$ est un schéma propre et lisse sur $\mathbb{Z}$ et si $X = \mathcal{X} \otimes \mathbb{Q}$, alors $H^j(X, \Omega^i_X) = 0$ si $i, j \in \mathbb{N}$ vérifient $i \neq j$ et $i + j \leq 3$* (et même un résultat un peu plus fort, cf. théorème 1 ci-dessous).

Ce résultat est obtenu comme une application de la théorie des périodes p-adiques (cf. le rapport [FI] dans ce volume). Plus précisément, soit K un corps de caractéristique 0, complet pour une valuation discrète, à corps résiduel parfait de caractéristique $p > 0$, absolument non ramifié. Soient $\overline{K}$ une clôture algébrique de K et $G_K = \mathrm{Gal}(\overline{K}/K)$. Utilisant le théorème de comparaison entre cohomologie cristalline et cohomologie étale p-adique que j'avais obtenu avec Bill Messing [FM] - théorème qui a été depuis considérablement généralisé par Faltings [Fa] - le résultat annoncé se déduit du résultat suivant (cf. théorème 2 ci-dessous) :

THÉORÈME. — *Soit $r \in \mathbb{Z}$ vérifiant $0 < r < p - 1$. Soit V une représentation p-adique de G_K qui est cristalline, à poids de Hodge-Tate $\in [0, r]$. Soit U un sous-quotient de V stable par G_K et tué par p. Soient H le noyau de l'action de G_K sur U et $L = \overline{K}^H$. Si v_0 désigne la valuation de L normalisée par $v_0(p) = 1$, et si $\mathfrak{D}_{L/K}$ est la différente de l'extension L/K, alors*

$$v_0(\mathfrak{D}_{L/K}) \leq 1 + r/(p-1).$$

Les théorèmes 1 et 2 ont été obtenus indépendamment par Abrashkin ([Ab2], [Ab3], [Ab4], [Ab5]) qui utilise essentiellement la même méthode. Abrashkin a obtenu depuis une jolie généralisation du théorème 2 ([Ab6]).

Afin de faciliter la lecture de la lettre qui suit, terminons cette introduction par quelques *rappels sur les modules de Dieudonné filtrés* ([FL], [Fo2]).

Notons k le corps résiduel du corps K introduit plus haut, $W = W(k)$ l'anneau des

vecteurs de Witt à coefficients dans k (c'est donc l'anneau des entiers de K) et σ le Frobenius absolu agissant sur k (via $x \longmapsto x^p$), W et K.

Pour tout entier $r \geq 0$, notons $\underline{MF}_W^{[0,r]}$ la catégorie suivante :

- un objet est un W-module M muni

a) d'une msuite décroissante de sous-W-modules

$$M = Fil^0 M \supset Fil^1 M \supset \cdots \supset Fil^i M \supset \cdots \supset Fil^r M,$$

b) pour tout entier i vérifiant $0 \leq i \leq r$, d'une application

$$\varphi_i : Fil^i M \longrightarrow M,$$

σ-semi-linéaire ; on demande que, si $0 \leq i < r$ et si $x \in Fil^{i+1} M$, alors $\varphi_i x = p\varphi_{i+1} x$;

- un morphisme est une application W-linéaire qui respecte la filtration et commute aux φ_i.

Notons $\underline{MF}_{W,tf}^{[0,r]}$ (resp. $\underline{MF}_{W,f}^{[0,r]}$) la sous-catégorie pleine de $\underline{MF}_W^{[0,r]}$ formée des M qui sont des W-modules de type fini (resp. de longueur finie) tels que les $Fil^i M$ sont des facteurs directs de W et que

$$\sum_{0 \leq i \leq r} \varphi_i(Fil^i M) = M.$$

C'est une catégorie abélienne.

L'anneau A_{cris} (cf. [FI], n.1.3.1) est muni d'une filtration décroissante $(Fil^i A_{cris})_{i \in \mathbb{N}}$: on a $A_{cris} \subset B_{cris}^+ \subset B_{dR}$ et on prend $Fil^i A_{cris} = A_{cris} \cap Fil^i B_{dR}$. Pour $0 \leq i \leq p-1$, on a $\varphi(Fil^i A_{cris}) \subset p^i A_{cris}$; comme A_{cris} est sans p-torsion, on peut, pour tout $r \leq p-1$, munir A_{cris} d'une structure d'objet de $\underline{MF}_W^{[0,r]}$ en posant $\varphi_i(x) = p^{-i}\varphi x$, pour tout $x \in Fil^i A_{cris}$. Par réduction modulo p^n, on munit aussi l'anneau $A_{cris}/p^n A_{cris}$, *qui est noté* $\mathcal{O}_n^{cris}(\mathcal{O}_{\overline{K}})$ dans cette lettre, d'une structure d'objet de $\underline{MF}_W^{[0,r]}$.

le 15 janvier 1986

Cher Bill,

Je pense avoir fait quelques progrès en ce qui concerne tant les bornes pour le discriminant que les applications aux variétés algébriques sur $\mathbb{Q}$ ayant bonne réduction partout.

Plus précisément, je sais démontrer le théorème suivant :

THÉORÈME 1. — *Soit X une variété propre non singulière sur $\mathbb{Q}$. On suppose que X a bonne réduction partout. Alors, si $i,j \in \mathbb{N}$ vérifient $i \neq j$ et $i+j \leq 3$, on a $H^j(X, \Omega^i_X) = 0$.*

Remarques :

a) "bonne réduction partout" signifie que, pour tout nombre premier p, il existe un schéma propre et lisse Y sur $\mathbb{Z}_p$ tel que $Y \otimes_{\mathbb{Z}} \mathbb{Q}_p = X \otimes_{\mathbb{Z}} \mathbb{Q}_p$ (ce qui est a priori moins fort que l'existence d'un schéma propre et lisse sur $\mathbb{Z}$ qui prolonge X); en fait, j'ai seulement besoin de savoir que, pour tout p, il existe Z propre et lisse sur $W(\overline{\mathbb{F}}_p)$ tel que $Z \otimes Frac\ W(\overline{\mathbb{F}}_p) = X \otimes Frac\ W(\overline{\mathbb{F}}_p)$, mais j'imagine que les experts sont plus ou moins convaincus que si une variété sur un corps local acquiert bonne réduction après une extension non ramifiée, elle avait déjà bonne réduction au départ.

b) Le théorème implique que si $\dim X \leq 3$, toute sa cohomologie est algébrique.

c) La démonstration utilise Odlyzko et la méthode se casse la figure complètement pour $i+j \geq 4$.

Il y a deux parties bien distinctes dans la démonstration :

I : La conjecture pour la majoration du discriminant[1] est vraie pour $n = 1$ et $r < p-1$; plus précisément :

THÉORÈME 2. — *Soient k un corps parfait de caractérisation $p \neq 0$, $W = W(k)$. $K = Frac\ W$, $\overline{K}$ une clôture algébrique de K, r un entier vérifiant $0 < r < p-1$. Soit M un objet de $\underline{MF}^{[0,r]}_{W,tf}$ tué par p. Soient $U = \mathrm{Hom}_{\underline{MF}}(M, O^1_{cris}(O_{\overline{K}}))$[2] la représentation galoisienne associée*[3] *et H le noyau de l'action de $G_K = \mathrm{Gal}(\overline{K}/K)$ sur U. Soient $L = \overline{K}^H$, $\mathfrak{D}_{L/K}$ la différence de l'extension L/K, v_o la valuation de L normalisée par $v_o(p) = 1$. Alors*

$$v_o(\mathfrak{D}_{L/K}) < 1 + \frac{r}{p-1}.$$

---

[1] cf. [Fo1], n° 2.2, voir aussi [Ab6].

[2] Dans la suite, pour alléger l'écriture, j'écris $\mathrm{Hom}_{\underline{MF}}$ au lieu de $\mathrm{Hom}_{\underline{MF}^{[0,r]}_W}$, il n'y aura pas de risque de confusion sur r.

[3] On a $\dim_{\mathbb{F}_p} U = \dim_k M$ (cf. [FL], [Fo2]).

II : Le théorème 2 (avec bien sûr notre théorème de comparaison entre cohomologie étale et cohomologie cristalline) implique le théorème 1.

Plan :

§1 : Rappels sur les représentations cristallines

§2 : Le théorème 2 implique le théorème 1

§3 : Démonstration du théorème 1.

§1.– Rappels sur les représentations cristallines

Soient k, W, K, $\overline{K}$, p, r et G_K comme dans le théorème 2. Pour toute extension E de K contenue dans $\overline{K}$, $\mathfrak{O}_E$ désigne l'anneau des entiers de E.

Pour tout $n \in \mathbb{N}$, et pour $0 \leq i \leq r$, on dispose d'une application φ_i : $Fil^i\mathcal{O}_n^{cris}(\mathfrak{O}_{\overline{K}}) \longrightarrow \mathcal{O}_n^{cris}(\mathfrak{O}_{\overline{K}})$ et, par passage à la limite, d'une application φ_i : $Fil^i\mathcal{O}_\infty^{cris}(\mathfrak{O}_{\overline{K}}) \longrightarrow \mathcal{O}_\infty^{cris}(\mathfrak{O}_{\overline{K}})$ (où $\mathcal{O}_\infty^{cris}(\mathfrak{O}_{\overline{K}})$ est la limite *inductive* des $\mathcal{O}_n^{cris}(\mathfrak{O}_{\overline{K}})$).

Pour tout M dans $\underline{M}_{W,f}^{[O,r]}$, je pose $\underline{U}^*(M) = \mathrm{Hom}_{\underline{MF}}(M, \mathcal{O}_\infty^{cris}(\mathfrak{O}_{\overline{K}}))$ (on a $\underline{U}^*(M) = \mathrm{Hom}_{\underline{MF}}(M, \mathcal{O}_n^{cris}(\mathfrak{O}_{\overline{K}}))$, si M est tué par p^n. Alors $\underline{U}^*$ est un foncteur contravariant additif qui induit une anti-équivalence entre la catégorie $\underline{MF}_{W,f}^{[0,r]}$ et la catégorie des *"représentations cristallines finies à poids compris entre* 0 *et* r*"*. i.e. la sous-catégorie pleine de la catégorie des représentations linéaires et continues de G_K à valeurs dans les groupes abéliens finis d'ordre une puissance de p dont les objets sont ceux qui sont isomorphes à un sous-quotient d'une représentation p-adique cristalline[4] dont les poids de la décomposition de Hodge-Tate sont compris entre 0 et r[5].

§2.– Le théorème 2 implique le théorème 1

2.1.– Je choisis $K = \mathbb{Q}_7$ et $\overline{\mathbb{Q}}$ = la fermeture algébrique de $\mathbb{Q}$ dans $\overline{\mathbb{Q}}_7 = \overline{K}$, ce qui me permet d'identifier $G_7 = \mathrm{Gal}(\overline{\mathbb{Q}}_7/\mathbb{Q}_7)$ à un sous-groupe de $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

PROPOSITION 1. — *Soit V une représentation 7-adique de G (de dimension finie, bien sûr); on suppose que V est non ramifiée en dehors de 7 et que, en tant que représentation de G_7, V est cristalline, avec les poids de la décomposition de Hodge-Tate appartenant à $0, 1, 2, 3$. Si l'on pose $V_4 = 0$, et, pour $i = 3, 2, 1, 0$, $V_i = \{v \in V | gv - \chi^i(g)v \in V_{i+1}$, pour tout $g \in G\}$ (où χ est le caractère cyclotomique), on a $V_o = V$.*

Bien sûr, cette proposition implique le théorème 1 : Soient $m \in \{1, 2, 3\}$ et $V' = H^m_{\text{ét}}(X \otimes \overline{\mathbb{Q}}, \mathbb{Q}_7)$: les hypothèses faites (et notre théorème) impliquent que le dual V de V' satisfait les hypothèses de la proposition; les conjectures de Weil impliquent que $V' = 0$, sauf peut-être pour $m = 2$, auquel cas $V' \simeq (\mathbb{Q}_7(-1))^{n_1}$. Le théorème 1 s'en déduit immédiatement[6].

---

[4] cf. par exemple, [FI], n° 2.2.3.

[5] C'est essentiellement le résultat principal de [FL], voir aussi [Fo2].

[6] Parce que, si $\mathbb{C}_7$ désigne le complété de $\overline{\mathbb{Q}}_7$, le théorème de comparaison entre cohomologie étale p-adique et cohomologie cristalline implique que, si $\widehat{X} = X \otimes \mathbb{Q}_7$, alors $H^j(\widehat{X}, \Omega^i_{\widehat{X}/\mathbb{Q}_7})$ s'identifie à

Remarque :

a) Conjecturalement[7], la représentation 7-adique associée à Δ devrait fournir un exemple de représentation semi-simple non "stupide" de G, non ramifiée en dehors de 7 et cristalline en 7; mais, ses poids dans la décomposition de Hodge-Tate sont 0 et 11.

b) Il me semble que l'on peut démontrer aussi la proposition 1 en remplaçant 7 par 5; je n'ai pas tout vérifié.

c) En se fatigant un peu plus, on devrait pouvoir décrire explicitement toutes les représentations du type de celles considérées dans la proposition 1; par exemple, si V est de ce type et est une extension non triviale de $\mathbb{Q}_7(i)$ par $\mathbb{Q}_7(j)$, on a nécessairement $i = 0$ et $j = 3$.

d) En se fatigant nettement plus, la même méthode devrait permettre de montrer que si X est une surface sur $\mathbb{Q}(\sqrt{3})$ ayant bonne réduction partout, alors sa cohomologie est algébrique.

2.2.– Dans la suite de ce paragraphe, j'appelle *module galoisien* la donnée d'un groupe abélien fini d'ordre une puissance de 7, muni d'une action linéaire et continue de G, non ramifiée en dehors de 7. Ils forment une catégorie abélienne C.

Pour tout module galoisine U, je pose $U_4 = 0$ et, pour $i = 3, 2, 1, 0$, $U_i = \{u \in U / gu - \chi^i(g)u \in U_{i+1}$, pour tout $g \in G\}$;
je pose aussi $g_iU = \{u \in U / gu = \chi^i(g)u$, pour tout $g \in G\}$.

Je note $C_{cris}^{[0,3]}$ la sous-catégorie pleine de C formée des U vérifiant :

il existe M objet de $\underline{MF}_f^{[0,3]}$ tel que $U \simeq \underline{U}^*(M)$ (en tant que G_7-module) (et où $\underline{MF}_f^{[0,3]} = \underline{MF}_{\mathbb{Z}_7,f}^{[0,3]}$).

Il est clair que $C_{cris}^{[0,3]}$ est stable par sous-objet, quotient, somme directe.

La proposition 1 résulte bien évidemment de :

PROPOSITION 1'. — *Si U est un objet de $C_{cris}^{[0,3]}$, on a $U_o = U$.*

2.3.– LEMME 1. — *Si*

$$0 \longrightarrow U' \longrightarrow U \longrightarrow U'' \longrightarrow 0$$

est une suite exacte de $C_{cris}^{[0,3]}$ et si G opère trivialement sur U' et U'', alors G opère trivialement sur U.

En effet, cette suite exacte induit une suite exacte

$$0 \longrightarrow M'' \longrightarrow M \longrightarrow M' \longrightarrow 0$$

$(H^j(X \otimes \overline{\mathbb{Q}}, \mathbb{Q}_7) \otimes \mathbb{C}_7(i))^{G_7}$ qui est nul si $i + j = 1$ ou 3 et aussi si $i + j = 2$ avec $i \neq j$ car $(\mathbb{C}_7(i))^{G_7} = 0$ si $i \neq 0$ [Ta].

[7] C'est un théorème, conséquence des théorèmes de comparaison entre cohomologie étale et cohomologie cristalline ([Fa], [FM], voir aussi [Sc]).

d'objets de $\underline{MF}_f^{[0,3]}$ et $Fil^1 M' = Fil^1 M'' = 0$, donc $Fil^1 M = 0$, donc U est non ramifiée en 7 [8], donc partout, donc triviale.

LEMME 2. — *A isomorphisme près, la catégorie $C_{cris}^{[0,3]}$ n'a que 4 objets simples qui sont les $\mathbb{F}_7(i)$, pour $i = 0, 1, 2, 3$.*

Démonstration : Soit U un objet simple, soient H le noyau de l'action de G sur U, $E = \overline{\mathbb{Q}}^H$, $F = E(\sqrt[7]{1})$, $n = 6n' = [F : \mathbb{Q}]$ (et donc $n' = [F : \mathbb{Q}(\sqrt[7]{1})]$. On a $F = \overline{\mathbb{Q}}^{H'}$ en notant H' le noyau de l'action de G sur $U \oplus \mathbb{F}_7(1)$. Comme $U \oplus \mathbb{F}_7(1)$ est un objet tué par 7 de $C_{cris}^{[0,3]}$, le théorème 2 implique

$$|d_F|^{1/n} < 7^{1+(3/6)} = 7^{1.5} < 18.52026$$

et les tables de Diaz y Diaz ([Di], méthode d'Odlyzko-Poitou-Serre) impliquent $n \leq 208$.

Si $F/\mathbb{Q}$ n'est pas modérée, on a $n' = 7n''$ avec $n'' \in \{1, 2, 3, 4\}$. Il en résulte que le 7-Sylow de $\mathrm{Gal}(F/\mathbb{Q}(\sqrt[7]{1}))$ est unique et donc invariant ; le sous-corps F' de F fixe par ce 7-Sylow est donc une extension modérément ramifiée de $\mathbb{Q}$, non ramifiée en dehors de 7, donc $|d_{F'}|^{1/[F':\mathbb{Q}]} < 7$, donc d'après Diaz y Diaz

$$6n'' = [F' : \mathbb{Q}] \leq 10, \quad \text{d'où} \quad n'' = 1.$$

Mais un groupe d'ordre 6×7 ne peut pas opérer simplement sur un $\mathbb{F}_7$-vectoriel sans que le sous-groupe d'ordre 7 opère trivialement et $F/\mathbb{Q}$ est modérée, d'où $6n' \leq 10$, d'où $n' = 1$ et $\mathbb{F} = \mathbb{Q}(\sqrt[7]{1})$. Ceci implique que U est isomorphe à un et un seul $\mathbb{F}_7(i)$, avec $0 \leq i \leq 6$; mais U objet de $C_{cris}^{[0,3]}$ implique alors $0 \leq i \leq 3$.

Remarque : Tu remarqueras que l'on a en fait démontré un peu plus : si U est un objet de $C_{cris}^{[0,3]}$ tué par 7, le degré de l'extension $E/\mathbb{Q}$ (où $E = \overline{\mathbb{Q}}^H$, H = noyau de l'action de G sur U) divise 42. En regardant les choses un peu plus soigneusement, on peut vérifier que $E \subset E_o(\sqrt[7]{1})$, où E_o est l'unique extension diédrale d'ordre 14 de $\mathbb{Q}$ non ramifiée en dehors de 7 (et le lemme 3 va dans ce sens).

2.5. LEMME 3. — *Dans $C_{cris}^{[0,3]}$, toute extension tuée par 7 de $\mathbb{F}_7(i)$ par $\mathbb{F}_7(j)$ est scindée sauf peut-être si on a simultanément $i = 0$ et $j = 3$.*

Si $i = j$, je peux, quitte à tordre par $\mathbb{F}_7(-i)$, supposer $i = j = 0$ et cela résulte du lemme 1.

Si $i > j$, et si je note M_i (resp. M_j) le module filtré associé à $\mathbb{F}_7(i)$ (resp. $\mathbb{F}_7(j)$), j'observe qu'il n'y a pas d'extension tuée par 7 non triviale de M_j par M_i et qu'il n'y a pas non plus d'extension cyclique de degré 7 de $\mathbb{Q}(\sqrt[7]{1})$ non ramifiée partout et je gagne.

[8] Si $Fil^1 M = 0$, $U = U^*(M)$ s'identifie, en tant que G_7-module, à $\mathrm{Hom}_{W[\varphi]}(M, \overline{k})$ et est non ramifiée.

Si $i < j$, je peux, quitte à tordre par $\mathbb{F}_7(-i)$, supposer $i = 0$. J'obtiens alors une représentation de Galois dans $GL_2(\mathbb{F}_7)$ du type

$$\begin{pmatrix} \chi^j & * \\ 0 & 1 \end{pmatrix}.$$

Si je pose $H = \text{Ker}$ de cette représentation, $E = \overline{\mathbb{Q}}^H$, $F = E(\sqrt[7]{1})$, un calcul facile me montre que, si l'extension n'est pas scindée, alors $F/\mathbb{Q}(\sqrt[7]{1})$ est cyclique de degré 7, non ramifiée en dehors de 7 et totalement ramifiée en 7 avec j comme unique nombre de ramfication (i.e. localement en 7, si π est une uniformisante du complété 7-adique de F et z un élément non trivial de $\text{Gal}(F/\mathbb{Q}(\sqrt[7]{1}))$, alors l'idéal engendré par $(z\pi - \pi)/\pi$ est l'idéal engendré par π^j.

On en déduit $|d_F| = 7^{(42-7)+6(j+1)} = 7^{41+6j} \leq 7^{53}$ si $j \leq 2$, donc $|d_F|^{1/[F:\mathbb{Q}]} = 7^{53/42} < 11.66$, d'où, d'après Diaz y Diaz $[F : \mathbb{Q}] \leq 28$, ce qui contredit $[F : \mathbb{Q}] = 42$.

2.6. Lemme 4. — *Si U est un objet de $C_{cris}^{[0,3]}$ qui n'a pas de quotient isomorphe à $\mathbb{F}_7$ (comme module galoisien), alors $U = \bigoplus_{i=0}^{3} g_i U$.*

Démonstration : D'abord, c'est clair si U est cyclique comme groupe abélien, parce que l'action de G sur U se fait à travers un caractère dont la restriction au sous-groupe d'inertie de G_7 est la restriction d'un χ^i, avec $i \in \{0, 1, 2, 3\}$, ce qui implique que c'est χ^i, donc que $U = g_i U$ (et les autres $g_j U$ sont nuls).

On termine par récurrence sur l'ordre de U (c'est clair si U est d'ordre 7); d'après les lemme 2, je peux trouver une suite exacte courte de la forme

$$0 \longrightarrow U' \longrightarrow U \longrightarrow \mathbb{F}_7(j) \longrightarrow 0$$

où $j \in \{1, 2, 3\}$. Je prétend que U' n'a pas non plus de quotient isomorphe à $\mathbb{F}_7$; sinon U aurait un quotient $\overline{U}$ qui serait une extension de $\mathbb{F}_7(j)$ par $\mathbb{F}_7$; comme $\overline{U}$ ne peut pas être cyclique, $\overline{U}$ est tué par 7; d'après le lemme 3, cette extension est scindée, donc $\overline{U}$, quotient de U, est isomorphe à $\mathbb{F}_7 \oplus \mathbb{F}_7(j)$ et U aurait un quotient isomorphe à $\mathbb{F}_7$.

Par hypothèse de récurrence, $U' = \bigoplus_{i=0}^{3} g_i U'$, en particulier, U' est soit décomposable, soit cyclique.

Si U' est décomposable, $U' = U'_1 \oplus U'_2$, avec U'_1 et U'_2 non réduits à 0; l'hypothèse de récurrence implique que U/U'_1 et U/U'_2 vérifient le lemme 4, donc aussi leur somme-directe et aussi U qui s'injecte dedans.

Si U' est cyclique, j'ai une suite exacte du type

$$0 \longrightarrow (\mathbb{Z}/7^n\mathbb{Z})(i) \longrightarrow U \longrightarrow \mathbb{F}_7(j) \longrightarrow 0,$$

avec $i \in \{1, 2, 3\}$.

Si l'extension n'est pas scindée comme suite exacte de groupes, U est cyclique et j'ai gagné; si elle est scindée, en regardant les noyaux de la multiplication par 7, j'obtiens une suite exacte

$$0 \longrightarrow \mathbb{F}_7(i) \longrightarrow U_7 \longrightarrow \mathbb{F}_7(j) \longrightarrow 0.$$

Comme $j \neq 0$, cette suite est scindée (lemme 3), ce qui implique $U \simeq (\mathbb{Z}/7^n\mathbb{Z})(i) \oplus \mathbb{F}_7(j)$ et j'ai gagné.

2.7.– Fin de la démonstration de la proposition 1

On procède par récurrence sur l'ordre de U (le cas où U est d'ordre 7 est clair). Si U n'a pas de quotient isomorphe à $\mathbb{F}_7$, c'est gagné d'après le lemme 4. Supposons donc que l'on ait une suite exacte

$$0 \longrightarrow U' \longrightarrow U \longrightarrow \mathbb{F}_7 \longrightarrow 0.$$

Par hypothèse de récurrence on a $U' = U'_0$. Soit $\overline{U} = U/U'_1$; on a une suite exacte courte

$$0 \longrightarrow U'/U'_1 \longrightarrow U/U'_1 \longrightarrow \mathbb{F}_7 \longrightarrow 0.$$

Il est clair que G opère trivialement sur le sous-truc et sur le quotient; le lemme 1 implique que G opère non moins trivialement sur U/U'_1. Comme $U_1 = U'_1$, on voit que $U = U_0$. Ca y est !

§3.– Démonstration du théorème 2

3.1.– Je vais appeler π un élément de $\mathfrak{O}_{\overline{K}}$ tel que $\pi^p = -p$ et α l'image de π dans $\widetilde{\mathfrak{O}}_{\overline{K}} = \mathfrak{O}_{\overline{K}}/p\mathfrak{O}_{\overline{K}}$. Je te rappelle[9] que $\mathcal{O}_1^{cris}(\mathfrak{O}_{\overline{K}}) = \bigoplus_{m=0}^{\infty} \widetilde{\mathfrak{O}}_{\overline{K}} \cdot \gamma_{pm}(\alpha)$ et que, pour $0 \leq i < p-1$, on a $Fil^i\mathcal{O}_1^{cris}(\mathfrak{O}_{\overline{K}}) = \widetilde{\mathfrak{O}}_{\overline{K}} \cdot \alpha^i + \bigoplus_{m=1}^{\infty} \widetilde{\mathfrak{O}}_{\overline{K}} \cdot \gamma_{pm}(\alpha)$ et

$$\varphi_i(a\alpha^i + \sum_{m=1}^{\infty} a_m \gamma_{pm}(\alpha)) = a^p(1 - \gamma_p(\alpha))^i.$$

3.2.– Pour toute extension algébrique E de K, je note v_o la valuation de E normalisée par $v_o(p) = 1$, $\mathfrak{b}_E$ l'idéal de $\mathfrak{O}_E$ formé des x vérifiant $v_o(x) > r/(p-1)$ et $A_E = \mathfrak{O}_E/\mathfrak{b}_E$. Je munis A_E d'une structure de φ-module filtré en posant

$$Fil^i A_E = \{x \in \mathfrak{O}_E | v_o(x) \geq i/p\}/\mathfrak{b}_E, \quad \text{pour} \quad 0 \leq i \leq r$$

et $\varphi_i x =$ l'image dans A_E de $\widehat{x}^p/(-p)^i$, où $\widehat{x}$ est un relèvement dans $\mathfrak{O}_E$ de x (tu vérifieras facilement que ça ne dépend pas du choix de $\widehat{x}$ et que c'est bien σ-semi-linéaire).

---

[9] C'est un calcul facile, compte tenu de ce que $\mathcal{O}_1^{cris}(\mathfrak{O}_{\overline{K}})$ est l'enveloppe à puissances divisées de $\widetilde{\mathfrak{O}}_{\overline{K}}$ relativement à l'idéal engendré par α.

Bien sûr, si tu y tiens, je peux convenir que $Fil^i A_E = 0$ si $i > r$. J'ai un homomorphisme de $\mathcal{O}_1^{cris}(\mathfrak{O}_{\overline{K}})$ sur $A_{\overline{K}}$ qui envoie $a + \sum_{m=1}^{\infty} a_m \gamma_{pm}(\alpha)$ sur l'image $\overline{a}$ de a dans $A_{\overline{K}}$; il commute avec les Fil^i et les φ_i, pour $0 \leq i \leq r$, et induit un homomorphisme

$$\underline{U}^*(M) = \mathrm{Hom}_{\underline{MF}}(M, \mathcal{O}_1^{cris}(\mathfrak{O}_{\overline{K}})) \longrightarrow \mathrm{Hom}_{\underline{MF}}(M, A_{\overline{K}}),$$

pour tout objet M de $\underline{MF}_{k,f}^{[0,r]}$ (sous-catégorie pleine de $\underline{MF}_{W,f}^{[0,r]}$ formée des objets tués par p).

3.3. Lemme 1. — *L'application* $\underline{U}^*(M) \longrightarrow \mathrm{Hom}_{\underline{MF}}(M, A_{\overline{K}})$ *définie ci-dessus est un isomorphisme*

Je pourrais le démontrer par dévissage, dans le style Fontaine-Laffaille. Je préfère le déduire d'un autre lemme qui me reservira une autre fois.

3.4.– Pour cela, j'ai besoin de quelques notations : je peux toujours trouver une base $(e_1, e_2, \ldots, e_d)$ de M sur k et des entiers $i_1, i_2, \ldots, i_d \in [0, r]$, tels que $Fil^i M = \bigoplus_{i_s \geq i} k e_s$. Si je pose $\varphi_{i_t} e_t = \sum_s \lambda_{s,t} e_s$, la matrice des λ_{st} est dans $GL_d(k)$.

Pour toute extension algébrique E de K, je pose $J(E) = \mathrm{Hom}_{\underline{MF}}(M, A_E)$. Il est clair que $J(E)$ s'identifie au sous-groupe des $(a_1, a_2, \ldots, a_d) \in A_E^d$ tels que $a_s \in Fil^{i_s} A_E$, pour tout s et $\varphi_{i_t} a_t = \sum_s \lambda_{s,t} a_s$. Je choisis des relèvements $\widehat{\lambda}_{s,t}$ des $\lambda_{s,t}$ dans $\mathfrak{O}_E$ et je note $\widehat{J}(E)$ l'ensemble des $(x_1, x_2, \ldots, x_d) \in \mathfrak{O}_E^d$ vérifiant

$$x_t^p = (-p)^i (\sum_s \widehat{\lambda}_{s,t} x_s), \quad \text{pour tout} \quad t.$$

J'ai une application évidente de $\widehat{J}(E)$ dans $J(E)$.

Lemme 2. — *L'application* $\widehat{J}(E) \longrightarrow J(E)$ *définie ci-dessus est bijective.*

Démonstration : Comme $\widehat{J}(E)$ (resp. $J(E)$) est la réunion des $\widehat{J}(E)$ (resp. $J(E')$), pour E' parcourant les extensions finies de K contenues dans E, il suffit de le démontrer lorsque E/K est finie. Je vais noter $\mathfrak{m}$ l'idéal maximal de $\mathfrak{O}_E$ et e l'indice de ramification absolu de E. Il est clair qu'il suffit de vérifier le

Sous-lemme. — *Si n est un entier $> re/(p-1)$ et si $x_1, \ldots, x_d$ sont des éléments de $\mathfrak{O}_E$ vérifiant*

$$x_t^p/(-p)^{i_t} \equiv \sum_s \widehat{\lambda}_{s,t} x_s (\mathrm{mod}\, \mathfrak{m}^n), \quad \text{pour tout} \quad t,$$

il existe $y_1, \ldots, y_d \in \mathfrak{m}^n$, uniquement déterminés $\mathrm{mod}\, \mathfrak{m}^{n+1}$ *tels que*

$$(x_t + y_t)^p/(-p)^{i_t} \equiv \sum_s \widehat{\lambda}_{st}(x_s + y_s) \ (\mathrm{mod}\, \mathfrak{m}^{n+1}).$$

3.5. *Démonstration du lemme* : Je vais montrer que tout élément de $\mathrm{Hom}_{\underline{MF}}(M, A_{\overline{K}}) = J(\overline{K})$ se relève de manière unique en un élément de $\overline{U}^*(M)$. Tout d'abord si je munis $\mathfrak{O}_{\overline{K}}$ d'une structure de φ-module filtré "de la même manière que $A_{\overline{K}}$", le lemme précédent (ou plutôt la démonstration, j'exagère) montre que tout élément de $\mathrm{Hom}_{\underline{MF}}(M, A_{\overline{K}})$ se relève de manière unique en un élément de $\mathrm{Hom}_{\underline{MF}}(M, \widetilde{\mathfrak{O}}_{\overline{K}})$. Si l'image de e_s par cet élément est x_s, l'image de e_s dans le relèvement doit être $x_s + \sum_{m\geq 1} x_{s,m}\gamma_{pm}(\alpha)$. Mais il est clair que $\varphi_{i_t}(x_t + \sum_{m\geq 1} x_{t,m}\gamma_{pm}(\alpha)) = \varphi_{i_t}(x_t) = \sum_s \lambda_{st}x_s(1-\gamma_p(\alpha))^{i_t}$ qui peut encore s'écrire

$$\sum_s \lambda_{s,t}x_s + \sum_{m=1}^{\infty} a_{tm}\gamma_{pm}(\alpha),$$

où les a_{tm} sont des éléments de $\widetilde{\mathfrak{O}}_{\overline{K}}$, presque tous nuls, qui ne dépendent pas du choix des $x_{s,m}$ dans $\widetilde{\mathfrak{O}}_{\overline{K}}$. On a donc à résoudre, pour tout $m \geq 1$, le système linéaire de d équations à d inconnues

$$\sum_s \lambda_{s,t}x_{t,m} = a_{t,m} \quad (\text{pour} \quad t = 1, \ldots, d)$$

qui a une solution et une seule et on a gagné.

3.6.– Je reprends les notations du théorème 1, et, comme au n° 3.4, pour toute extension algébrique E de K, je pose $J(E) = \mathrm{Hom}_{\underline{MF}}(M, A_E)$.

LEMME 3. — *Soit $d = \dim_k M$. Alors, pour toute extension algébrique E de K, on a $\#J(E) \leq p^d$, avec l'égalité si et seulement s'il existe un K-plongement de L dans E.*

Démonstration : Si l'on choisit un plongement de E dans $\overline{K}$, il induit une application injective de A_E dans $A_{\overline{K}}$, donc de $J(E)$ dans $J(\overline{K})$, donc $\#J(E) \leq \#J(\overline{K}) = \#\underline{U}^*(M) = p^d$ puisque $\underline{U}^*(M)$ est un $\mathbb{F}_p$-espace vectoriel de dimension d. Si maintenant $H' = \mathrm{Gal}(\overline{K}/E)$, on a $J(E) = \widehat{J}(E) = \widehat{J}(\overline{K}^{H'}) = (\widehat{J}(\overline{K}))^{H'} = (J(\overline{K}))^{H'}$ qui est égal à $\underline{U}^*(M) = J(\overline{K})$ si et seulement si $H' \subset H$, i.e. si $E \supset L$.

3.7.– Comme dans [Fo1], n° 1.5, pour tout nombre réel $m \geq 0$, je dis que L/K satisfait la propriété (P_m) si

pour toute extension algébrique E de K, s'il existe un homomorphisme (de $\mathfrak{O}_K$-algèbres) de $\mathfrak{O}_L$ dans $\mathfrak{O}_E/\mathfrak{a}^m_{E/K}$, alors il existe un K-plongement de L dans E

(où $\mathfrak{a}^m_{E/K} = \{x \in \mathfrak{O}_E | v_o(x) \geq m\}$).

LEMME 4. — *Pour tout $m > 1 + \frac{r}{p-1}$, L satisfait la propriété (P_m).*

Preuve : Pour simplifier, je suppose que E et K ont le même corps résiduel ; c'est facile de se ramener à ce cas là et, en plus, j'aurais très bien pu supposer k algébriquement clos dans tout ce paragraphe.

Soient e l'indice de ramification absolu de E, a une uniformisante de E et $P(X) = X^e + p\Big(\sum_{t=0}^{e-1} u_t X^t\Big)$ le polynôme minimal de a sur $\mathfrak{O}_K$.

Soit $\eta : \mathfrak{O}_L \longrightarrow \mathfrak{O}_E/\mathfrak{a}_{E/K}^m$ un homomorphisme de $\mathfrak{O}_K$-algèbres. Le fait que $m > 1$ implique que η induit un homomorphisme injectif

$$\overline{\eta} : A_L \longrightarrow A_E$$

qui vérifie $\overline{\eta}(Fil^i A_L) \subset Fil^i A_E$, pour $i = 0, 1, \ldots, r$.

Je prétends que, pour tout $x \in Fil^i A_L$, $\overline{\eta}(\varphi_i x) = \varphi_i(\overline{\eta} x)$. Soit en effet b un relèvement de $\overline{\eta}(\overline{a})$ (ou $\overline{a}$ = image de a dans A_L) dans $\mathfrak{O}_E$; j'ai $v_o(P(b)) > 1 + \frac{r}{p-1}$ et je peux donc écrire $P(b) = pc$ avec $c \in \mathrm{Ker}(\mathfrak{O}_E \longrightarrow \mathfrak{A}_E)$.

Pour tout $y \in \mathfrak{O}_L$ (resp. $\mathfrak{O}_E$), je note $\overline{y}$ son image dans A_L (resp. A_E). Il est clair que $Fil^i A_L$ est engendré comme $\mathfrak{O}_K$-module par les $\overline{a}^j$, pour $j \geq ie/p$, et il suffit de le vérifier pour x égal à un tel $\overline{a}^j$. Si je pose $pj = ie + j'$, j'ai $(a^j)^p = a^{pj} = a^{j'} \cdot (a^e)^i = a^{j'} \cdot (-p)^i \cdot (\sum u_t a^t)^i$ et $\varphi_i(\overline{a}^j) = \overline{a}^{j'} \cdot (\sum u_t \overline{a}^t)^i$, donc $\overline{\eta}(\varphi_i(\overline{a}^j)) = \overline{b}^{j'} \cdot (\sum u_t \overline{b}^t)^i$.

D'autre part $\overline{\eta}(\overline{a}^j) = \overline{b}^j$ se relève en b^j et j'ai

$$(b^j)^p = b^{pj} = b^{j'} \cdot (b^e)^i = b^{j'} \cdot (-p)^i \cdot ((\sum u_t b^t) - c)^i$$

et

$$\varphi_i(\overline{\eta}(\overline{a}^j)) = \overline{b}^{j'} \cdot (\sum u_t \overline{b}^t)^i = \overline{\eta}(\varphi_i(\overline{a}^j)).$$

Autrement dit $\overline{\eta} : A_L \longrightarrow A_E$ est un monomorphisme de φ-modules filtrés : il induit donc une application injective de $J(L) = \mathrm{Hom}_{\underline{MF}}(M, A_L)$ dans $J(E) = \mathrm{Hom}_{\underline{MF}}(M, A_E)$. On a donc $\#J(E) \geq \#J(L)$, ce qui, d'après le lemme 3, implique l'existence d'un plongement de L dans E.

3.8.– Fin de la démonstration du théorème 2

C'est clair si l'extension L/K est non ramifiée ; sinon avec les notations du § 1 de [Fo1], on a (loc. cit. prop. 1.5) $u_{L/K} - e^{-1} < m$, pour tout $m > 1 + \frac{r}{p-1}$, donc $u_{L/K} - e^{-1} \leq 1 + \frac{r}{p-1}$ et en étant un peu plus soigneux (cf. l'argument de la fin du n° 1.8 de loc. cit.), on en déduit que

$$u_{L/K} \leq 1 + \frac{r}{p-1},$$

d'où (loc. cit. prop. 1.3) $v_o(\mathfrak{D}_{L/K}) = u_{L/K} - i_{L/K} < u_{L/K} \leq 1 + \frac{r}{p-1}$.

Remarque : Si l'on a la flemme d'être soigneux, on a $u_{L/K} - e^{-1} \leq 1 + \frac{r}{p-1}$, d'où $v_o(\mathfrak{D}_{L/K}) \leq 1 + \frac{r}{p-1}$, puisque $i_{L/K} \leq e^{-1}$ (du moins si l'extension est sauvagement ramifiée; mais sinon la majoration est triviale). On récupère l'inégalité large qui suffit pour les applications. Mais l'inégalité stricte se déduit de l'inégalité large, car si on a l'égalité cela implique $i_{L/K} = e^{-1}$; on en déduit que le p-Sylow du groupe d'inertie a un seul nombre de ramification et un calcul direct montre que l'égalité est impossible.

BIBLIOGRAPHIE

[Ab1] V.A. ABRASHKIN. — Galois moduli of period p group schemes over a ring of Witt vectors, *Math. USSR Izvestiya* **31**, (1988), 1-46.

[Ab2] V.A. ABRASHKIN. — Modular crystalline representations, *Russian Math. Surveys* **43**, (1988), 195-232.

[Ab3] V.A. ABRASHKIN. — Modular crystalline representations and generalization of the Shafarevich conjecture, *UINITI* **6418**, (1988), 1135-1182, traduction anglaise à paraître.

[Ab4] V.A. ABRASHKIN. — Modification of the Fontaine-Laffaille functor, *Math. USSR Izvestiya* **34**, (1990), 467-516.

[Ab5] V.A. ABRASHKIN. — Crystalline representations and generalization of the Shafarevich conjecture, *Izv. Akad. Nauk. USSR* **53**, (1989), 1135-1182, traduction anglaise à paraître in Math. USSR Izv.

[Ab6] V.A. ABRASHKIN. — Ramification in étale cohomology, *Inv. Math.* **101**, (1990), 631-640.

[Di] F. DIAZ Y DIAZ. — *Tables minorant la racine n-ième du discriminant d'un corps de degré n*, Publ. Math. d'Orsay, 1980.

[Fa] G. FALTINGS. — Crystalline cohomology and p-adic étale cohomology, Algebraic Analysis, Geometry and Number Theory, *The Johns Hopkins Univ. Press* , (1989), 25-80.

[Fo1] J.-M. FONTAINE. — Il n'y a pas de variétés abéliennes sur $\mathbb{Z}$, *Inv. Math.* **81**, (1985), 515-538.

[Fo2] J.-M. FONTAINE. — Cohomologie de de Rham, cohomologie cristalline et représentations p-adiques, in *Algebraic Geometry Tokyo-Kyoto, Lecture Notes in Math, Springer, Berlin* **1016**, (1983), 86-108.

[FI] J.-M. FONTAINE and L. ILLUSIE. — *p-adic periods : a survey*, ce volume.

[FL] J.-M. FONTAINE et G. LAFAILLE. — Construction de représentations p-adiques, *Ann. Scient. E.N.S., 4ème série* **15**, (1982), 547-608.

[FM] J.-M. FONTAINE and W. MESSING. — p-adic Periods and p-adic étale Cohomology, *Contemporary Mathematics* **67**, (1987), 179-207.

[Sc] T. SCHOLL. — Motives for modular forms, *Invent. Math.* **100**, (1990), 419-430.

[Ta] J. TATE. — p-divisible Groups, in Proc. of a conf. on local Fields, *NUFFIC Summer School, Driebergen, Springer, Berlin* , (1967), 158-183.