Représentations galoisiennes et opérateurs de Bessel p-adiques.

par Yves André

Introduction.

Soit $\mathcal{G}$ le groupe de Galois absolu d'un corps local de caractéristique p. Suivant J.-M. Fontaine, on peut associer à toute représentation p-adique de $\mathcal{G}$ d'inertie finie un module différentiel p-adique sur une couronne, muni d'une structure de Frobenius. Les propriétés des représentations galoisiennes liées à la ramification se traduisent alors en termes différentiels.

Par ailleurs, dans un contexte tout à fait indépendant inspiré par la conjecture de l'indice de Robba, G. Christol et Z. Mebkhout ont développé une théorie générale des modules différentiels p-adiques sur une couronne et prouvé, avec leur théorie des pentes p-adiques [CM3], des analogues des propriétés de ramification ci-dessus dans un cadre beaucoup plus général (modules non nécessairement munis de structure de Frobenius, mais "solubles" en un bord fixé d'une couronne assez fine).

La question de savoir dans quelle mesure la théorie des modules différentiels p-adiques *avec structure de Frobenius* sur une couronne se ramène à la théorie des représentations galoisiennes est ouverte. Son importance, et son lien avec une version p-adique du théorème de monodromie locale de Grothendieck, ont été soulignés dans les travaux de R. Crew [Cr2]. À notre connaissance, la littérature n'offre aucun exemple d'un tel module différentiel qui ne soit quasi-unipotent, i.e. qui ne soit extension itérée de modules différentiels se déduisant d'une représentation finie de $\mathcal{G}$ par le procédé de Fontaine.

L'origine de cet article est une suggestion de Mebkhout (s'appuyant sur des calculs faits avec A. Arabia) selon laquelle le module différentiel considéré dans [CM3] 6.3.9 avec $p = 2$ pourrait être un tel exemple. Comme ce module est du type de Bessel (d'indice $2/3$), cette suggestion nous a incité à examiner systématiquement la question de la quasi-unipotence des opérateurs de Bessel p-adiques (normalisés à la Dwork). On sait depuis les travaux de Dwork [D] et Adolphson-Sperber [AS] que ceux-ci sont étroitement liés aux sommes exponentielles de Kloosterman, et sont munis d'une structure de Frobenius. Du point de vue différentiel, l'intérêt et la difficulté qu'offrent ces opérateurs résident dans l'irrégularité de leur singularité à l'infini, qui laisse une trace p-adique dans toute couronne $\mathcal{C}(]1, r[),\ r > 1$.

Commençons par préciser quelques notations. Soit K une extension finie de $\mathbf{Q}_p$, de corps résiduel $\mathbf{F}_q$. On note $\mathcal{R}_{x,K}$ l'"anneau de Robba à l'infini" formé des fonctions analytiques $\sum_{-\infty}^{\infty} a_n x^n$ $(a_n \in K)$ sur une couronne $\mathcal{C}(]1, r[)$ d'épaisseur

r non précisée. Le sous-anneau $\mathcal{E}^\dagger_{x,K}$ formé des séries à coefficients a_n bornés est un corps hensélien de corps résiduel $\mathbf{F}_q((\frac{1}{x}))$. Ses extensions finies non ramifiées sont de la forme $\mathcal{E}^\dagger_{y,K'}$, où K' est une extension finie non ramifiée de K et y une nouvelle variable, algébrique sur $\mathcal{E}^\dagger_{x,K}$; elles correspondent aux extensions finies séparables du corps local $\mathbf{F}_q((\frac{1}{x}))$. On a $\mathcal{R}_{y,K'} \cong \mathcal{R}_{x,K} \otimes_{\mathcal{E}^\dagger_{x,K}} \mathcal{E}^\dagger_{y,K'}$ [M1].

Un module différentiel M sur $\mathcal{R}_{x,K}$ est dit *quasi-unipotent* s'il existe une extension finie non ramifiée $\mathcal{E}^\dagger_{y,K'}$ telle que $M \otimes_{\mathcal{R}_{x,K}} \mathcal{R}_{y,K'}$ soit extension successive de modules différentiels triviaux [T2].

Notons $\Lambda_{\nu,x}$ l'opérateur de Bessel p-adique d'indice $\nu \in \mathbf{Q} \cap \mathbf{Z}_p$, normalisé à la Dwork: $\Lambda_{\nu,x} = (xd/dx)^2 - 4\pi^2 x^2 - \nu^2$ (il annule la série de Bessel $J_\nu(2\pi i\, x)$, où π désigne la constante p-adique de Dwork).

Théorème 0.1. *Le $\mathcal{E}^\dagger_{x,K}$-module différentiel attaché à $\Lambda_{\nu,x}$ ne dépend pas de ν à isomorphisme près. Il est quasi-unipotent, et même soluble dans une extension finie non ramifiée de $\mathcal{E}^\dagger_{x,K}$. Sa structure de Frobenius est supersingulière.*

Le cas p impair est peu significatif: la quasi-unipotence est aisée à établir directement, le quotient de $\mathcal{G}$ qui intervient étant cyclique d'ordre $2p$. En revanche, le cas $p = 2$ est beaucoup plus délicat (et en règle générale écarté de la littérature). Le résultat suivant explicite l'extension de $\mathcal{E}^\dagger_{x,K}$ qui trivialise $\Lambda_{\nu,x}$.

Théorème 0.2. *Prenons pour K l'extension quadratique non ramifiée de $\mathbf{Q}_2$. Soit E la courbe elliptique (supersingulière) sur $\mathbf{F}_4$ d'équation affine $Y^2 + Y = X^3 + \omega$, avec $\omega^3 = 1, \omega \neq 1$. Alors le revêtement $E \to E/Aut(E) \cong \mathbf{P}^1$ est totalement ramifié en l'origine de E, et définit une extension galoisienne non ramifiée de degré 24 de $\mathcal{E}^\dagger_{x,K}$, de groupe $Aut(E) \cong SL_2(\mathbf{Z}/3\mathbf{Z})$, dans laquelle les $\Lambda_{\nu,x}$ sont solubles.*

Nous démontrons ces résultats de manière indirecte(1), en combinant deux outils principaux: d'une part la théorie des pentes p-adiques de [CM3], et d'autre part la théorie de Galois différentielle. Au-delà du cas Bessel, c'est cette combinaison que nous avons cherché à illustrer dans cet article.

Les deux principaux résultats de la théorie de [CM3] utilisés ici sont le théorème de décomposition selon les pentes sur $\mathcal{R}$, et le théorème d'intégralité du polygône de Christol-Mebkhout (et ses corollaires immédiats d'irréductibilité). Le rôle de la théorie de Galois différentielle est double. D'une part, elle fournit un critère général commode de quasi-unipotence, ne faisant plus intervenir qu'un anneau différentiel au lieu du couple $(\mathcal{E}^\dagger_{x,K}, \mathcal{R}_{x,K})$ que met en jeu la définition:

Théorème 0.3. *Soit M un module différentiel sur l'anneau de Robba $\mathcal{R}_{x,K}$, muni d'une structure de Frobenius. Alors M est quasi-unipotent si et seule-*

(1) une fois "deviné" le résultat 0.2, une vérification directe de la quasi-unipotence diadique est en principe possible, mais semble mener à des calculs inextricables.

ment si son groupe de Galois différentiel, après passage au corps de fractions de $\mathcal{R}_{x,K}.\bar{K}$, est un groupe algébrique résoluble.

D'autre part, la théorie de Galois différentielle permet, dans une situation concrète, de restreindre les possibilités - plus ou moins a priori tout d'abord, puis en confrontation avec la théorie des pentes - et d'en dresser un catalogue fini. C'est ainsi, par élimination des cas résolubles, que nous prouvons la généralisation partielle de 0.1 qui suit (et dont nous déduisons 0.1, en fait):

Théorème 0.4. *Tout module différentiel M de rang ≤ 2 sur $\mathcal{R}_{x,K}$ admettant une structure de Frobenius, et de pentes p-adiques < 1, est quasi-unipotent.*

Résumons brièvement le contenu de l'article. Le §1 rappelle quelques faits de théorie de Galois différentielle avant d'analyser plus en détail le cas des modules différentiels de rang deux et de leurs petites puissances symétriques.

Le §2 montre que bien que l'anneau différentiel de Robba ne soit pas simple, on ne perd pas grand-chose en passant au corps de fractions.

Le §3 traite des pentes p-adiques; après un rappel des définitions et deux estimations élémentaires, on présente succinctement la théorie de Christol-Mebkhout qui joue un rôle fondamental dans la suite.

Le §4 traite des modules quasi-unipotents, selon Matsuda et Tsuzuki.

Le §5 contient la démonstration du critère de quasi-unipotence 0.3, et le §6 celle de 0.4. Ils forment le coeur de ce travail.

L'étude des opérateurs de Bessel p-adiques sur des couronnes fait l'objet du §7, où nous avons essayé de réduire les calculs au minimum. Signalons l'exemple 7.7 d'un opérateur algébrique à deux singularités $\{0, \infty\}$ admettant des exposants p-adiques qui ne "proviennent pas" des exposants formels de Turrittin en 0 ou en l'infini.

Dans le dernier paragraphe, nous élucidons la représentation galoisienne associée, pour $p = 2$; on y voit apparaître des courbes elliptiques supersingulières sur $\mathbf{F}_4$, et leur cohomologie cristalline.

Remerciements . Ce travail doit beaucoup à Z. Mebkhout: outre les commentaires dont il nous a fait part à propos du problème de la quasi-unipotence, il a attiré notre attention sur l'exemple [CM3] 6.3.9 comme on l'a dit, en nous le présentant comme un test important (et un contre-exemple potentiel); même si le test s'est finalement avéré positif, il a été précieux de pouvoir disposer d'un exemple aussi explicite et non trivial au commencement de nos recherches sur le sujet.

Nous remercions aussi G. Christol, Matsuda S. et Tsuzuki N. pour les discussions qui nous ont permis de nous familiariser avec leurs travaux respectifs.

1. Préliminaires de théorie de Galois différentielle.

Soit F un corps de caractéristique nulle, muni d'une dérivation ∂. On suppose que le corps des constantes $C = Ker\ \partial$ est algébriquement clos. La dérivation s'étend de manière unique à toute extension algébrique de F.

Soit M un F-module différentiel, i.e. un $F[\partial]$-module de dimension finie sur F. Fixons une extension de Picard-Vessiot $\mathcal{F}$ pour M. Rappelons qu'il s'agit d'une extension différentielle de F dans laquelle M est soluble, de corps de constantes égal à C, et minimale pour ces propriétés. On sait depuis Kolchin qu'il en existe, et qu'elle est unique à automorphisme non-unique près.

Les solutions de M dans $\mathcal{F}$ forment un C-espace vectoriel $V = Hom_\partial(M, \mathcal{F})$ de dimension égale à $\dim_F M$. Le groupe $G(\mathcal{F}/F)$ des automorphismes commutant à ∂, noté aussi $G(M, \mathcal{F})$, a une structure naturelle de sous-groupe algébrique de $GL(V)$. La donnée de $G(\mathcal{F}/F) \subset GL(V)$ permet de retrouver M: $M = Hom_{G(\mathcal{F}/F)}(V, \mathcal{F})$ (pour une introduction concise à la théorie de Galois différentielle, voir par exemple [Be] ou [P]).

Aux représentations puissances symétriques (resp. extérieures) de V correspondent des modules différentiels $S^m M$ (resp. $\wedge^m M$). Par exemple, si $M = F[\partial]/F[\partial]\Lambda$ est le module différentiel attaché à l'opérateur $\Lambda = \partial^2 + P\partial + Q \in F[\partial]$, alors $S^2 M$ est le module différentiel attaché à l'opérateur

$$S^2\Lambda = \partial^3 + 3P.\ \partial^2 + (\partial(P) + 2P^2 + 4Q).\ \partial + (4PQ + 2\partial(Q)).$$

En effet, d'après un résultat classique d'Appell, les solutions de $S^2\Lambda$ sont les polynômes homogènes quadratiques en les solutions de Λ ([WW]XIV, ex. 10).

Proposition 1.1. *Supposons M de rang 2 sur F, $S^2 M$ irréductible, et $\wedge^2 M$ trivial. Alors*
i) ou bien M est absolument irréductible (i.e. ne se scinde sur aucune extension finie de F), de même que tous les $S^m M$,
ii) ou bien M est soluble dans une extension galoisienne de F de groupe binaire tétraédral $\tilde{A}_4$, binaire octaédral $\tilde{S}_4$, ou binaire icosaédral $\tilde{A}_5$.

Rappelons que les sous-groupes $\tilde{A}_4, \tilde{S}_4, \tilde{A}_5$ de SL_2 sont des extensions centrales par $\mathbf{Z}/2\mathbf{Z}$ des groupes alternés ou symétriques A_4, S_4, A_5 respectivement (sur ces groupes et leur géométrie, voir [Co] et [V]I.3).

Ici $\dim V = 2$. L'hypothèse que $\wedge^2 M$ est trivial se traduit par le fait que $G(\mathcal{F}/F)$ est un sous-groupe algébrique de SL_2.

Dire que M se scinde sur une extension finie de F se traduit par le fait que la composante neutre $G(\mathcal{F}/F)^0$ de $G(\mathcal{F}/F)$ est réductible (i.e. sa représentation naturelle sur V n'est pas irréductible), cf. e. g. [Be] 2.4.2. Par la correspondance de Galois différentielle, $G(\mathcal{F}/F)^0$ correspond à une extension galoisienne finie contenue dans $\mathcal{F}$. On est alors ramené au lemme standard de théorie des groupes suivant:

Lemme 1.2. *Soit G un sous-groupe algébrique de SL_{2C} non conjugué à $\tilde{A}_4, \tilde{S}_4, \tilde{A}_5$. Si S^2V est irréductible, alors $G = SL_2$ et tous les S^mV sont irréductibles.*

Plus généralement, en toute dimension, un sous-groupe algébrique G infini de $SL(W)$ tel que S^2W soit irréductible est soit $SL(W)$ soit $Sp(W)$ (et alors tous les S^mW sont irréductibles), cf. [Be] 3.2.5. En dimension 2, ceci se démontre bien plus simplement en utilisant le catalogue des sous-groupes réductifs de SL_2: SL_2, un tore de Cartan ou son normalisateur, ou un groupe fini.
On conclut en remarquant que les seuls sous-groupes finis de SL_2 tels que S^2V soit irréductible sont ceux indiqués (les autres sont cycliques ou dicycliques).

En fait, nous aurons à considérer toutes les puissances symétriques paires ≤ 8.

Proposition 1.3. *Soit $\tilde{G}$ l'un des groupes $\tilde{A}_4, \tilde{S}_4, \tilde{A}_5$, et V sa représentation plane standard. Alors $S^2V = V_3$ est irréductible, et les décompositions de S^4V et S^8V en irréductibles sont de la forme suivante (en notant en indice la dimension, et $\mathbf{1}$ la représentation triviale):*

$S^4V \cong V_1' \oplus V_1'' \oplus V_3$, $S^8V \cong \mathbf{1} \oplus V_1' \oplus V_1'' \oplus (V_3)^2$ *si* $\tilde{G} = \tilde{A}_4$ *(qui agit non trivialement sur V_1' et V_1'' à travers son quotient $\mathbf{Z}/3\mathbf{Z}$),*

$S^4V \cong V_2 \oplus V_3$, $S^8V \cong \mathbf{1} \oplus V_2 \oplus V_3 \oplus V_3'$ *si* $\tilde{G} = \tilde{S}_4$,

$S^4V \cong V_5$, $S^8V \cong V_4 \oplus V_5$ *si* $\tilde{G} = \tilde{A}_5$.

Preuve. On simplifie les calculs en remarquant que $\tilde{G}$ agit sur les puissances symétriques paires à travers $G = A_4, S_4$ ou A_5 respectivement, et que

$$S^2(S^2V) \cong S^4V \oplus \mathbf{1},\ S^2(S^4V) \cong S^8V \oplus S^4V \oplus \mathbf{1} \text{ (pléthisme pour } SL_2\text{, cf. [FH]11).}$$

De plus, le cas A_4 se déduit du cas S_4 par restriction. En utilisant la table de caractères de G et la formule $\chi_{S^2W}(g) = \frac{1}{2}(\chi_W^2(g) + \chi_W(g^2))$, on trouve que le caractère de S^4V (vue comme représentation de G) est donné par

Cas S_4: $\chi(1) = 5,\ \chi((12)) = 1,\ \chi((123)) = \chi((1234)) = -1,\ \chi((12)(34)) = 1$

A_4: $\chi(1) = 5,\ \chi((123)) = \chi((132)) = -1,\ \chi((12)(34)) = 1$

A_5: $\chi(1) = 5,\ \chi((123)) = -1,\ \chi((12)(34)) = 1,\ \chi((12345)) = \chi((21345)) = 0$,
(le carré de (12345) est conjugué à (21345))

tandis que le caractère de S^8V est donné par

S_4: $\chi(1) = 9,\ \chi((12)) = 1,\ \chi((123)) = 0,\ \chi((1234)) = \chi((12)(34)) = 1$

A_4: $\chi(1) = 9,\ \chi((123)) = \chi((132)) = 0,\ \chi((12)(34)) = 1$

A_5: $\chi(1) = 9,\ \chi((123)) = 0,\ \chi((12)(34)) = 1,\ \chi((12345)) = \chi((21345)) = -1$.

Pour conclure, on vérifie dans chaque cas que la décomposition (unique) annoncée dans la proposition donne lieu au même caractère.

2. Les anneaux différentiels $\mathcal{A}_I$, $\mathcal{R}$ et $\mathcal{E}^\dagger$.

Soient K une extension finie de $\mathbf{Q}_p$ et k son corps résiduel. Soit $I \subset]0,\infty[$ un intervalle ouvert. Notons $\mathcal{A}_I$ l'anneau des fonctions analytiques sur la couronne $\mathcal{C}(I)$, définies sur K. L'anneau de Robba à l'infini $\mathcal{R} = \mathcal{R}_{x,K}$ est la réunion des $\mathcal{A}_I$ lorsque I parcourt les intervalles de la forme $]1,r[$. C'est donc l'anneau des séries de Laurent $\sum_{-\infty}^{\infty} a_n x^n$ à coefficients dans K dont le polygône de Newton - c'est-à-dire l'enveloppe convexe des points $(n, ord_p(a_n))$ - est non vide et admet une direction asymptotique horizontale, qu'il surplombe et rejoint en $-\infty$. Le sous-anneau $\mathcal{E}^\dagger = \mathcal{E}^\dagger_{x,K}$ est formé des séries à coefficients bornés, ou ce qui revient au même, dont le polygône de Newton atteint l'asymptote. Comme une telle série non nulle ne s'annule pas près du bord intérieur de sa couronne de convergence, $\mathcal{E}^\dagger$ est un corps. Nous munissons une fois pour toutes ces anneaux de la dérivation

$$\partial = x\tfrac{d}{dx}.$$

Dans ce paragraphe, $\mathcal{A}$ désigne l'un des anneaux différentiels $\mathcal{A}_I$ ou $\mathcal{R}$, et $Q(\mathcal{A})$ désigne son corps des fractions. Une difficulté particulière que présente l'anneau différentiel $\mathcal{A}$ est qu'*il n'est pas simple*: il y a des idéaux propres non nuls stables sous ∂ (considérer l'idéal différentiel engendré par une fonction sur une couronne $\mathcal{C}(I)$ ayant des zéros de multiplicité non bornée). Pour contourner cette difficulté, on note tout d'abord le résultat suivant, prouvé dans [CM3]3.1.1 (voir aussi [Cr2]4.9):

Proposition 2.1. *L'anneau $\mathcal{A}$ est de Bézout, i.e. tout idéal de type fini de $\mathcal{A}$ est principal.*

Corollaire 2.2. *$\mathcal{A}$ est intégralement clos et cohérent. Tout $\mathcal{A}$-module de type fini est somme directe de son sous-module de torsion et d'un module libre.*

cf. [Bo] VII, 1 ex. 20, et 2 ex. 12 et 14 (ou [Cr2]4.9). La proposition suivante renforce certains résultats de [CM3] 3:

Proposition 2.3. *Tout module différentiel M sur $\mathcal{A}$ qui est de présentation finie (resp. de type fini et sans torsion) comme $\mathcal{A}$-module est en fait libre (et cohérent) sur $\mathcal{A}$.*

Preuve. Seule l'assertion concernant un module différentiel M de présentation finie ne découle pas immédiatement de 2.2. D'après 2.2, le sous-module de torsion est facteur direct, donc de présentation finie, et il est d'autre part clair qu'il est stable sous ∂. On est donc ramené à montrer qu'un module différentiel M de présentation finie et de torsion sur $\mathcal{A}$ est nul. Soit $\{m_i\}$ un ensemble fini de générateurs de M, et notons u_i l'homomorphisme $\mathcal{A} \to M$, $a \mapsto am_i$. Ce sont des homomorphismes de $\mathcal{A}$-modules cohérents, donc l'annulateur $\mathcal{I} = \cap_i Ker\ u_i$ de M dans $\mathcal{A}$ est de type fini ([Bo] I, 2, ex. 11). Comme $\mathcal{A}$ est de Bézout, on

peut écrire $\mathcal{I} = f.\mathcal{A}$. Or il est clair que cet annulateur est un idéal différentiel: pour tout $m \in M$, $(\partial f).m = \partial(fm) - f.\partial m = 0$. On a donc $\partial f/f \in \mathcal{A}$, ce qui entraîne que f n'a pas de zéro dans la couronne (resp. au bord intérieur de la couronne si $\mathcal{A} = \mathcal{R}$), et est donc une unité de $\mathcal{A}$, de sorte que $\mathcal{I} = \mathcal{A}$ et $M = 0$.

Remarque. On ne peut remplacer "de présentation finie" par "de type fini" dans l'énoncé, comme le montre l'exemple du quotient de $\mathcal{A}$ par un idéal différentiel non trivial.

Corollaire 2.4. *Soit M un $\mathcal{A}$-module différentiel de présentation finie. Soit $M'_{Q(\mathcal{A})}$ un sous-module différentiel de $M \otimes_{\mathcal{A}} Q(\mathcal{A})$, et posons $M' = M'_{Q(\mathcal{A})} \cap M$. Alors $M' \otimes_{\mathcal{A}} Q(\mathcal{A}) \cong M'_{Q(\mathcal{A})}$, et on a une suite exacte de modules différentiels*

$$0 \to M' \to M \to M/M' \to 0$$

dont les $\mathcal{A}$-modules sous-jacents sont libres. Si de plus $M'_{Q(\mathcal{A})}$ est facteur direct de $M_{Q(\mathcal{A})}$ comme module différentiel, alors M' est facteur direct de M comme module différentiel.

Preuve. D'après 2.3, M est libre (et cohérent). De même, M/M' est de type fini et sans torsion, donc libre (et cohérent). On en déduit que M' est aussi cohérent ([Bo] I, 2, ex 11), donc de présentation finie; il est donc aussi libre, par 2.3, et $M' \otimes_{\mathcal{A}} Q(\mathcal{A}) \cong M'_{Q(\mathcal{A})}$ ([Bo] I, 2, 6). Supposons ensuite que $M'_{Q(\mathcal{A})}$ admette un module différentiel supplémentaire $M''_{Q(\mathcal{A})}$, et posons $M'' = M''_{Q(\mathcal{A})} \cap M$. Alors $(M' \oplus M'') \otimes_{\mathcal{A}} Q(\mathcal{A}) \cong M_{Q(\mathcal{A})}$ et $M/(M' \oplus M'') = 0$ d'après ce qui précède.

Remarques. *a*) Ce résultat permet de définir de manière non ambigue le semi-simplifié de M.

b) Il faut prendre garde qu'un tel résultat ne se transpose pas sans précaution aux opérateurs différentiels. On trouve dans [CM3] 6.1.16 un exemple d'opérateur unitaire de rang deux sur $\mathcal{R}$ qui se factorise en produit de deux opérateurs de rang un sur $Q(\mathcal{R})$, mais pas sur $\mathcal{R}$ - bien que le module différentiel associé soit somme directe de modules différentiels de rang un sur $\mathcal{R}$.

3. Pentes p-adiques: la théorie de Christol-Mebkhout.

Soit M un module différentiel sur l'anneau $\mathcal{A}_{]1,r[}$ des fonctions analytiques sur une couronne $\mathcal{C}(]1,r[)$. On suppose M libre de type fini comme $\mathcal{A}_{]1,r[}$-module.

Pour tout $\rho \in]1,r[$, on note $R(M,\rho)$ le minimum de $1/\rho$ et des rayons de convergence des solutions de M au point générique de Dwork t_ρ du "disque" $|x| > \rho$.

On dit que M est *soluble au bord intérieur* si $lim_{\rho \to 1^+} R(M,\rho) = 1$. (Dans [CM3], il est plutôt question de solubilité au bord extérieur, mais la traduction est immédiate).

Soit $\lambda \in [0,\infty[$. On dit que M (supposé soluble au bord, et non nul) est *de plus grande pente* λ si pour tout $\rho > 1$ assez voisin de 1, on a $R(M,\rho) = \rho^{-\lambda-1}$.

On dit que M est *purement de pente* λ si pour tout $\rho > 1$ assez voisin de 1, et pour toute solution non nulle u de M au point t_ρ, le minimum de $1/\rho$ et du rayon de convergence de u est égal à $\rho^{-\lambda-1}$ (en particulier, M est de plus grande pente λ).

Ces définitions s'étendent immédiatement au cas d'un module différentiel libre de type fini sur l'anneau de Robba à l'infini $\mathcal{R}$ (et il n'y a plus lieu de préciser que le bord est intérieur). Plutôt que "pente", on dit "pente p-adique au bord", si on veut distinguer des pentes formelles ou de Frobenius.

Avant de rappeler les résultats de la théorie de Christol-Mebkhout qui nous seront utiles, commençons par deux résultats plus élémentaires sur les plus grandes pentes.

Proposition 3.1. *Soient l, m, n des entiers ≥ 1, avec m et n premiers entre eux. Supposons que $S^l M$ (resp. $S^{lm} M$, $S^{ln} M$) soit de plus grande pente λ (resp. λ', λ''). Alors $\lambda' \leq \lambda$, $\lambda'' \leq \lambda$, et $sup(\lambda', \lambda'') = \lambda$.*

Preuve. Pour tout entier naturel s, les solutions de $S^{ls} M$ s'expriment comme polynômes en les solutions de $S^l M$, ce qui montre que $R(S^{ls} M, \rho) \geq R(S^l M, \rho)$; en particulier $\lambda' \leq \lambda$, $\lambda'' \leq \lambda$. On veut ensuite démontrer que $R(S^l M, \rho) \geq inf(R(S^{lm} M, \rho), R(S^{ln} M, \rho))$ pour ρ assez proche de 1. On peut supposer que toutes les solutions de $S^l M$ en t_ρ ne convergent pas dans un disque de rayon $> 1/\rho$ (sinon l'énoncé est trivial: $\lambda = \lambda_m = \lambda_n = 0$). Comme les puissances l-ièmes des solutions de M engendrent celles de $S^l M$, on voit qu'il existe une solution de Λ en t_ρ dont la puissance l-ième g a pour rayon de convergence $R(S^l M, \rho)$. Choisissons des entiers r, s tels que $rm + sn = 1$. En écrivant $g = (g^m)^r.(g^n)^s$, on voit que g est méromorphe dans le disque $D(t_\rho, inf(R(S^{lm} M, \rho), R(S^{ln} M, \rho)))$. En passant à la puissance m-ième, on voit en outre que g n'a pas de pôle dans ce disque. D'où le résultat.

Proposition 3.2. *Supposons que M provienne d'un module différentiel sur le sous-anneau de $(K \cap \bar{\mathbf{Q}})((\frac{1}{x}))$ formé des séries convergeant dans la couronne $\mathcal{C}(]1, \infty[)$. Notons λ_∞ sa plus grande pente formelle à l'infini. Si M est de plus grande pente p-adique λ (au bord intérieur de la couronne), alors $\lambda \leq \lambda_\infty$.*

Preuve. Considérons la fonction $\rho \mapsto R(M, \rho)^{-1}$ sur $]1, \infty[$. En coordonnées logarithmiques, son graphe est celui d'une fonction *continue convexe non-décroissante*, cf. [CD] 2.4, 2.5 (mutatis mutandis). Au voisinage de l'abscisse 0 (qui correspond au point limite $\rho = 1$), ce graphe est une droite partant de 0 et de pente λ. Au voisinage de l'infini, le développement de Turrittin-Levelt p-adique montre que ce graphe a la forme d'une droite de pente λ_∞, cf. [Ba] prop. 4 (l'hypothèse sur l'algébricité des coefficients entraîne que les différences des exposants de Turrittin à l'infini ne sont pas des nombres de Liouville p-adiques, d'où la convergence du développement de Turrittin-Levelt). On conclut que $\lambda \leq \lambda_\infty$ par convexité.

Venons-en aux deux résultats fondamentaux de la théorie des pentes p-adiques.

Théorème de décomposition. *Tout module différentiel M sur $\mathcal{R}$ (libre de type fini) soluble au bord admet une filtration décroissante $M_{>\lambda}$ telle que le gradué associé $Gr_\lambda\ M$ est nul ou libre de type fini, purement de pente λ. En particulier M est de plus grande pente le maximum des λ pour lesquels $Gr_\lambda\ M$ est non nul.*

cf. [CM3]6.2.6. Ce théorème permet d'attacher un "polygône de Newton" à M, dont la longueur du segment de pente λ est le rang de $Gr_\lambda\ M$, et dont l'extrémité gauche est conventionnellement l'origine. Nous l'appellerons *polygône de Christol-Mebkhout.*

Théorème d'intégralité. *Les sommets du polygône de Christol-Mebkhout de tout module différentiel M sur $\mathcal{R}$ soluble au bord sont à coordonnées entières.*

cf. [CM3]8.3.6. Via le théorème de décomposition, ce théorème se déduit de l'interprétation de la hauteur du polygône de Christol-Mebkhout comme un indice, donc un nombre entier [CM3]8.3.1. Il en résulte que si M est purement de pente λ, celle-ci est rationnelle, et si son dénominateur ne divise pas le rang de M, alors M est irréductible.

Le cas de la pente nulle est analysé dans [CM2]. On suppose K muni d'un automorphisme continu σ. En caractéristique p, il induit $t \mapsto t^{p^f}$ pour un entier $f > 0$ convenable (non unique). On désigne par φ_f l'endomorphisme de Frobenius σ-linéaire de $\mathcal{R}$ induit par $x \mapsto x^{p^f}$. Notons que pour tout entier $s > 0$, la puissance φ_f^s n'est autre que l'endomorphisme σ^s-linéaire φ_{sf}.

On dit qu'un $\mathcal{R}$-module différentiel M (libre de type fini) a une *structure de Frobenius* d'ordre f si $\varphi_f^* M \cong M$. Par un argument bien connu de Dwork, ceci entraîne qu'il est soluble au bord (cf. [CM3] 6.3.11).

Nous citons pour référence le "théorème fuchsien" suivant, prouvé dans [CM2] (cf. [CM2] 5.5.3, 6.2.6).

Théorème 3.3. *Supposons M muni d'une structure de Frobenius, et de pente nulle. Alors M est extension successive de modules différentiels du type $(\mathcal{R}, \partial - \alpha)$ pour des nombres $\alpha \in \mathbf{Q} \cap \mathbf{Z}_p$ convenables.*

Ces nombres, bien définis à permutation et à l'addition d'un entier près, s'appellent les *exposants p-adiques* de M.

4. Représentations galoisiennes, pentes p-adiques et pentes de Frobenius: la théorie de Matsuda et Tsuzuki.

Muni de la valeur absolue discrète $|\sum_{-\infty}^{\infty} a_n x^n| = \sup_n |a_n|$, le corps $\mathcal{E}_{x,K}^\dagger$ est hensélien, de corps résiduel $k((\frac{1}{x}))$ [M1]. Si $k'((\frac{1}{y}))/k((\frac{1}{x}))$ est une extension

finie séparable, il lui correspond une extension finie non ramifiée [(1)] de $\mathcal{E}^\dagger_{x,K}$, qui est nécessairement de la forme $\mathcal{E}^\dagger_{y,K'}$, et qui se plonge donc dans $\mathcal{R}_{y,K'}$. Notons que σ a une extension naturelle à K' et que $K'^\sigma = K^\sigma$.

Lemme 4.1. *$\mathcal{E}^\dagger$ est algébriquement fermé dans $Q(\mathcal{R})$.*

Considérons une équation algébrique $g^N + \ldots + u_1 g + u_0 = 0$ à coefficients u_i dans $\mathcal{E}^\dagger$, avec $g \in Q(\mathcal{R})$. Comme $\mathcal{R}$ est intégralement clos (cf. 2.2), on voit que $g \in \mathcal{R}$. Or d'après [M2], $\mathcal{E}^\dagger$ est intégralement fermé dans $\mathcal{R}$. Rappelons l'argument: supposons g et les u_i analytiques sur la couronne $\mathcal{C}(]1,r[)$. Pour tout $h = \sum_{-\infty}^{\infty} a_n x^n \in \mathcal{A}_{]1,r[}$ et tout $R \in]1,r[$, posons $|h|_R = \sup_n |a_n| R^n$. On a $h \in \mathcal{E}^\dagger$ si et seulement si $\overline{\lim_{R\to 1^+}} |h|_R < \infty$. On a donc $\overline{\lim_{R\to 1^+}} |u_i|_R < \infty$, et il est facile de tirer de l'équation de g que $\overline{\lim_{R\to 1^+}} |g|_R < \infty$, i.e. $g \in \mathcal{E}^\dagger$.

Un module différentiel M libre de type fini sur $\mathcal{R}_{x,K}$ est dit *quasi-unipotent* s'il existe une extension galoisienne $k'((\frac{1}{y}))/k((\frac{1}{x}))$ telle que M devienne extension successive de modules triviaux sur l'extension correspondante $\mathcal{R}_{y,K'}/\mathcal{R}_{x,K}$. Notons que $\mathcal{R}_{y,K'} \cong \mathcal{E}^\dagger_{y,K'} \otimes_{\mathcal{E}^\dagger_{x,K}} \mathcal{R}_{x,K}$ par 4.1. Il est facile de voir que si pour une extension finie K_1/K, $M \otimes_K K_1$ est quasi-unipotent, alors M est déjà quasi-unipotent (passer au semi-simplifié pour simplifier, cf. 2.4).

Proposition 4.2. *Si M est de rang un et muni d'une structure de Frobenius, alors il est quasi-unipotent. De plus, tant M que sa structure de Frobenius sont définis sur $\mathcal{E}^\dagger$.*

cf. [T2] 4.1.4 , et aussi [Cr1] 4.11 (la seconde assertion découle du fait que $\mathcal{R}^\times = (\mathcal{E}^\dagger)^\times$).

Proposition 4.3. *Supposons M quasi-unipotent, et de rang μ. Alors quitte à remplacer K par une extension finie non ramifiée, le semi-simplifié M^{ss} est de la forme $Hom_G(W, \mathcal{R}_{y,K'})$, pour une extension finie galoisienne de $k'((\frac{1}{y}))/k((\frac{1}{x}))$ de groupe G et une représentation K-linéaire fidèle convenable W de G de dimension μ.*

cf. [M2] 6.4, 4.4. L'idée d'associer des modules différentiels sur $\mathcal{E}^\dagger$ aux représentations de $Gal(k((\frac{1}{x}))^{sep}/k((\frac{1}{x})))$ d'image finie est dûe à Fontaine [F].

Le formalisme des groupes de ramification en numérotation supérieure ([S2] IV 3, [K2] 1) permet de définir la décomposition de W suivant les "sauts". Via 4.3, tout module différentiel quasi-unipotent hérite d'une telle décomposition ([M2] 7.1). On a alors:

[(1)] rappelons qu'une extension finie de corps à valuation discrète est non ramifiée si l'indice de ramification est un, et si l'extension résiduelle est séparable [S2] p.26

Théorème 4.4. *Cette décomposition coïncide avec la décomposition selon les pentes de Christol-Mebkhout.*

cf. [M2] 7.7, [T1].

Soit M un $\mathcal{R}$-module différentiel muni d'une structure de Frobenius. Un $\mathcal{E}^\dagger$-réseau de M est un $\mathcal{E}^\dagger$-module différentiel N muni d'une structure de Frobenius tel que M se déduit de N par $\otimes_{\mathcal{E}^\dagger}\mathcal{R}$. Une généralisation de la théorie de Dieudonné-Manin ([T2] 3.1.6) mène à la notion de *filtration par les pentes de Frobenius* pour le $\mathcal{E}[\varphi_f]$-module $N \otimes_{\mathcal{E}^\dagger} \mathcal{E}$, où $\mathcal{E}$ désigne le complété de $\mathcal{E}^\dagger$ pour sa valeur absolue naturelle. On dispose donc d'un polygône de Newton-Frobenius ([T2] 3.1.5).

Theorème 4.5. *Soit M un $\mathcal{R}$-module différentiel muni d'une structure de Frobenius. Alors M est quasi-unipotent si et seulement si il existe une filtration croissante finie exhaustive et séparée (indexée par les rationnels) par des sous-modules différentiels stables sous la structure de Frobenius, telle que le gradué d'indice μ admette un $\mathcal{E}^\dagger$-réseau purement de pente de Frobenius μ.*
Une telle filtration est alors unique.

Ceci est démontré dans [T2] 5.2.1, 5.1.5.

Le cas de la pente frobeniusienne nulle est analysé dans [T3]:

Théorème 4.6. *Supposons que k contienne $\mathbf{F}_{p^f}$ et que $K = K^\sigma \otimes_{W(\mathbf{F}_q)} W(k)$ (voir 3.3). Alors la catégorie des représentations K^σ-linéaires continues de $Gal(k((\frac{1}{x}))^{sep}/k((\frac{1}{x})))$, dont l'image de l'inertie est finie, est équivalente à celle des $\mathcal{E}^\dagger$-modules différentiels munis d'une structure de Frobenius de pente nulle.*

Nous ferons usage du corollaire suivant de la théorie:

Corollaire 4.7. *Soit N un $\mathcal{E}^\dagger$-module différentiel muni d'une structure de Frobenius. Les conditions suivantes sont équivalentes:*
a) $N \otimes_{\mathcal{E}^\dagger} \mathcal{R}$ est irréductible et quasi-unipotent,
b) N est irréductible et a une seule pente de Frobenius,
c) N est irréductible et soluble dans une extension finie non ramifiée de $\mathcal{E}^\dagger$.

Preuve. *a)* $\Rightarrow$ *b)* découle de 4.5. Pour les autres implications, il est commode de remarquer d'emblée qu'il suffit, par descente galoisienne, de les démontrer après remplacement de K par une extension finie non ramifiée. Cela permet de supposer que $N \otimes_K K'$ est irréductible pour toute extension finie non ramifiée de K. Supposons *b)*. Quitte à remplacer σ par une puissance et la structure de Frobenius par un multiple d'une puissance convenable, on peut supposer sa pente nulle. Or par 4.6 (voir aussi [T1] 7.3.2), un tel module différentiel est soluble dans une extension galoisienne $\mathcal{E}^\dagger_{y,K'}/\mathcal{E}^\dagger_{x,K}$ de groupe G, et est de la forme $Hom_G(W, \mathcal{E}^\dagger_{y,K'})$ pour une représentation K-linéaire fidèle convenable W de G. D'où *b)* $\Rightarrow$ *c)*. Notons d'ailleurs que la représentation W est irréductible

et le reste si on remplace K par une extension finie non ramifiée quelconque. Par 4.3, on voit que $N \otimes_{\mathcal{E}^\dagger} \mathcal{R} = Hom_G(W, \mathcal{R}_{y,K'})$ est irréductible. D'où $c) \Rightarrow a)$.

Exemples. $a)$ Pour $p \equiv 1$ mod. 4, notons π une racine $(p-1)$-ième de $-p$ fixée, et posons $K = \mathbf{Q}_p(\pi^2)$, $\sigma = id$.
Le module différentiel $N = \mathcal{E}^\dagger/\mathcal{E}^\dagger(d^2/dx^2 + \pi^2)$ est irréductible et soluble dans l'extension galoisienne $\mathcal{E}^\dagger[\cos \pi x, \pi \sin \pi x]/\mathcal{E}^\dagger$ de groupe μ_p. La représentation correspondante envoie un générateur ζ_p sur la matrice $\begin{pmatrix} \cos 2\pi/p & \pi \sin 2\pi/p \\ -\frac{1}{\pi} \sin 2\pi/p & \cos 2\pi/p \end{pmatrix}$ à coefficients dans K définis par $\cos 2\pi/p = \frac{\zeta_p + \zeta_p^{-1}}{2}$, $\pi \sin 2\pi/p = \frac{\pi}{2i}(\zeta_p - \zeta_p^{-1})$.

$b)$ L'exemple de [CM3] 6.1.16 déjà cité fournit un cas de module différentiel de rang deux sur $\mathcal{E}^\dagger$ muni d'une structure de Frobenius, quasi-unipotent, qui est irréductible sur $\mathcal{E}^\dagger$ mais pas sur $\mathcal{R}$. La filtration par les pentes p-adiques de Christol-Mebkhout coïncide dans cet exemple avec la filtration par les pentes de Frobenius-Tsuzuki.

5. Un critère de quasi-unipotence.

Lemme 5.1. *Toute extension galoisienne finie de $\mathcal{E}^\dagger$ est résoluble.*

Preuve. Soit E' une extension galoisienne du corps à valuation discrète hensélien $\mathcal{E}^\dagger$. Notons $\mathcal{E}$ (resp. $\hat{E}'$) le complété de $\mathcal{E}^\dagger$ (resp. E') une extension galoisienne de $\mathcal{E}^\dagger$. Alors $Gal(E'/\mathcal{E}^\dagger) \cong Gal(\hat{E}'/\mathcal{E})$. Désignons par $k((\frac{1}{y}))$ l'extension séparable maximale du corps résiduel $k((\frac{1}{x}))$ de $\mathcal{E}$ contenue dans le corps résiduel de $\hat{E}'$. Comme $\mathcal{E}$ est un corps à valuation discrète complet, $Gal(\hat{E}'/\mathcal{E})$ est extension du groupe $Gal(k((\frac{1}{y}))/k((\frac{1}{x})))$ par le groupe d'inertie, et ce dernier est résoluble, cf. [S2] I.7 (p. 32) et IV.2 (p. 76). Comme $k((\frac{1}{x}))$ est un corps à valuation discrète complet à corps résiduel fini, $Gal(k((\frac{1}{y}))/k((\frac{1}{x})))$ est résoluble ([S2] I.7, cor. 5).

On note F le corps différentiel $Q(\mathcal{R}).\bar{K} = Q(\mathcal{R}.\bar{K})$ (par ce compositum, on entend la réunion des corps de fractions des $\mathcal{R}_{x,K'}$, $K \subset K'$ qui s'envoient canoniquement les uns dans les autres). Son corps des constantes est $C = \bar{K}$.

Théorème 5.2. *Soit M un module différentiel sur l'anneau de Robba $\mathcal{R}$, muni d'une structure de Frobenius. Alors M est quasi-unipotent si et seulement si le groupe de Galois différentiel de $M \otimes_{\mathcal{R}} F$ est un groupe algébrique résoluble.*

Preuve. Notons H le quotient du groupe de Galois différentiel de $M \otimes_{\mathcal{R}} F$ par son radical unipotent.

Rappelons que toute représentation ρ de dimension finie sur $\bar{K}$ du groupe de Galois différentiel de M sur F définit un module différentiel sur F qui est sous-quotient d'une construction tensorielle mixte sur $M \otimes_{\mathcal{R}} F$. Quitte à remplacer K par une extension finie, un tel module différentiel provient d'un sous-quotient M_ρ d'une construction tensorielle mixte sur M d'après 2.4. Les représentations

ρ qui se factorisent à travers H correspondent aux modules différentiels M_ρ qui sont semi-simples.

Supposons que M soit quasi-unipotent, et démontrons que le groupe de Galois différentiel de $M \otimes_{\mathcal{R}} F$ est résoluble. Il suffit de faire voir que H est résoluble. Pour cela, on peut remplacer M par le module différentiel semi-simple M_ρ correspondant à une représentation fidèle de H. Alors M se trivialise sur une extension galoisienne de $\mathcal{R}_{x,K}$ du type $\mathcal{R}_{y,K'} \cong \mathcal{E}^\dagger_{y,K'} \otimes_{\mathcal{E}^\dagger_{x,K}} \mathcal{R}_{x,K}$ (cf. 4.1). On conclut par 5.1.

Réciproquement, supposons que le groupe de Galois différentiel soit résoluble. Alors H admet une filtration $H = H_0 \triangleright H_1 \ldots \triangleright H_m = 1$, chaque H_{i+1} étant normal et fermé dans H_i, et les quotients H_i/H_{i+1} étant soit $\mathbf{G}_m$, soit un groupe cyclique μ_n. Soit L_1 le module différentiel provenant d'une représentation fidèle de dimension un de H/H_1 (il en existe). Il est muni d'une structure de Frobenius en vertu de la proposition 5.3 ci-dessous. Il découle alors de 4.2 que L_1 devient trivial après une extension du type $\mathcal{R}_{x_1,K_1}/\mathcal{R}_{x,K}$. Une fois cette extension faite, le quotient du nouveau groupe de Galois différentiel par son radical unipotent est contenu dans H_1. En itérant cette construction d'extensions, on se ramène au cas où H est trivial, c'est-à-dire où le groupe de Galois différentiel est unipotent. Mais M est alors extension successive de modules différentiels triviaux, et 5.2 s'ensuit.

Proposition 5.3. *Si L est un sous-quotient de rang un d'un $\mathcal{R}$-module différentiel N admettant une structure de Frobenius, alors L admet une structure de Frobenius.*

Écrivons $L = N'/N''$ avec $N'' \subset N' \subset N$. Comme on a $L \cong \wedge^{max} N' \otimes (\wedge^{max} N'')^\vee$, on se ramène à traiter les cas de $\wedge^{max} N'$ et $\wedge^{max} N''$. Cela permet de supposer d'emblée que $L \subset N$. Soit *soc* N le socle de N, i.e. la somme des sous-$\mathcal{R}$-modules différentiels irréductibles de N (ce qui a un sens grâce à 2.4). Il est clair que la structure de Frobenius de N en induit une sur *soc* N: $(\varphi_f^*)(soc\ N) \cong soc\ N$. D'autre part, $L \subset soc\ N$. On peut donc remplacer N par son socle, ce qui nous permet de supposer N semi-simple. Soit $N = \oplus_1^s N_i$ la décomposition isotypique du module différentiel N (ceci a un sens grâce à 2.4). Alors la structure de Frobenius de N induit une permutation des N_i et il est alors clair que $(\varphi_f^*)^{s!} L = \varphi_{s!f}^* L \cong L$.

Remarques. *a*) Le même argument montre que si N' est un sous-module différentiel semi-simple de N, il admet une structure de Frobenius.

b) En combinant 5.2, 4.4, et le théorème de Hasse-Arf ([S2] V.7), on voit que les pentes p-adiques de tout $\mathcal{R}$-module différentiel muni d'une structure de Frobenius et dont le groupe de Galois différentiel est abélien sont entières. Cela peut bien entendu aussi se voir plus directement en se ramenant au cas d'un opérateur différentiel d'ordre un.

6. Modules différentiels de rang deux et de pente p-adique $1/2$.

Soit M un $\mathcal{R}[\partial]$-module, libre de rang deux sur $\mathcal{R}$. On fait les hypothèses suivantes:

H_1) le déterminant $\wedge^2 M$ est trivial,
H_2) M admet une structure de Frobenius,
H_3) M est *purement de pente p-adique* $1/2$.

Lemme 6.1. *M est irréductible sur le corps différentiel $F = Q(\mathcal{R}.\bar{K})$.*

Par H_3) et par le théorème d'intégralité, M est irréductible. Par le corollaire 2.4, il en est de même sur $Q(\mathcal{R})$. Comme ceci ne dépend pas du choix de K, il en est encore de même sur $F = Q(\mathcal{R}).\bar{K} = Q(\mathcal{R}.\bar{K})$.

Lemme 6.2. *On a l'alternative suivante:*
a) S^2M admet une solution de la forme $x^\alpha.g$, $g \in \mathcal{R} \setminus 0$, $\alpha \in \mathbf{Q} \cap \mathbf{Z}_p$ (i.e. $Hom_\partial(M, x^\alpha.\mathcal{R}) \neq 0$).
b) S^2M est purement de pente p-adique $1/3$.
Le cas b) a lieu si et seulement si S^2M est irréductible sur F.

Les pentes de S^2M sont inférieures ou égales à celle de M, c'est-à-dire $1/2$, cf. 3.1. Le théorème d'intégralité ne laisse que les possibilités (0), $(0, 1/2)$, $(1/3)$ pour les pentes. D'après le résultat rappelé en 3.3 (et compte tenu de H_2)), les deux premières possibilités correspondent au cas a) (et la troisième au cas b) bien entendu). La dernière assertion se déduit aisément du théorème de décomposition et de 2.4, comme en 6.1.

Théorème 6.3. *Sous les hypothèses H_i), M est quasi-unipotent, et n'a qu'une seule pente de Frobenius dans la couronne $(]1, r[)$ pour r assez voisin de 1. Il est soluble dans une extension entière finie $\mathcal{R}_{y,K'}/\mathcal{R}_{x,K}$ galoisienne de groupe dicyclique dans le cas a), de groupe binaire tétraédral $\tilde{A}_4 = SL_2(\mathbf{Z}/3\mathbf{Z})$ dans le cas b).*
En outre, si M admet un $\mathcal{E}^\dagger_{x,K}$-réseau (stable sous Frobenius, cf. 4.5), il est soluble dans l'extension finie non ramifiée $\mathcal{E}^\dagger_{y,K'}/\mathcal{E}^\dagger_{x,K}$.

On commence par traiter le cas a) de 6.2. Comme la représentation fondamentale V du groupe de Galois différentiel $G(\mathcal{F}/F)$ est irréductible, mais pas son carré symétrique, $G(\mathcal{F}/F)$ est contenu dans le normalisateur d'un tore de Cartan de SL_2 (compte tenu de H_1)). En particulier, $G(\mathcal{F}/F)$ est résoluble et il découle de 5.2 que M est quasi-unipotent. Par 6.1, on voit que $G(\mathcal{F}/F)$ est un groupe dicyclique. On conclut que M est soluble dans une extension (entière finie) $\mathcal{R}_{y,K'}/\mathcal{R}_{x,K}$. On termine la preuve de 6.3 dans le cas a) en invoquant 4.7.

On se place maintenant dans le cas b) de 6.2.

Lemme 6.4. *L'un des opérateurs S^4M et S^6M est réductible.*

Par le théorème de décomposition, il suffit de voir que l'un des deux a au moins deux pentes distinctes. Supposons S^4M isocline. Sa pente, qui est $\leq 1/3$

(la pente de S^2M) est donc $1/5$ par le théorème d'intégralité. Alors d'après 3.1, la plus grande pente de S^6M est $1/3$, et donc S^6M a au moins deux pentes par le théorème d'intégralité. Il est donc réductible.

En appliquant la proposition 1.1, on déduit de 6.4 que le groupe de Galois différentiel $G(\mathcal{F}/F)$ est l'un des groupes finis $\tilde{A}_4$, $\tilde{S}_4$ ou $\tilde{A}_5$. La proposition 1.3 donne les possibilités pour les décompositions de S^4V et S^8V. D'après 2.4, ces décompositions correspondent à des décompositions des $\mathcal{R}$-modules différentiels S^4M et S^8M (quitte à remplacer K par une extension finie).

Confrontons cela avec ce que donne la théorie des pentes. Du fait que la plus grande pente de l'opérateur d'ordre cinq S^4M est au plus celle de S^2M, c'est-à-dire $1/3$, on trouve a priori trois polygônes de Christol-Mebkhout possibles. Leurs pentes sont $(1/5), (1/4, 0), (1/3, 0)$ respectivement. Compte tenu de ce que les modules de pente 0 se décomposent (cf. 3.3), on élimine directement $\tilde{S}_4$.

Pour éliminer $\tilde{A}_5$, on considère S^4V et S^8V. Comme la représentation S^4V de $\tilde{A}_5$ est irréductible, la pente de S^4M est de la forme $m/5$; comme cette pente est $\leq 1/3$ (la pente de S^2M), on a $m = 1$. Or de la décomposition de S^8V prescrite en 1.3, on déduit que les deux pentes sont de la forme $n/4$ et $m/5$. Comme $1/4 > 1/5$, c'est impossible. On conclut donc que $G(\mathcal{F}/F)$ est le groupe résoluble $\tilde{A}_4$. On termine comme dans le cas a) la preuve de 6.3.

Corollaire 6.5. *Tout module différentiel M de rang ≤ 2 sur $\mathcal{R}$ admettant une structure de Frobenius, et de pentes p-adiques < 1, est quasi-unipotent.*

Preuve. Le cas de rang 1 découle de 4.2. Supposons donc M de rang 2. Par le théorème d'intégralité, M est purement de pente 0 ou $1/2$. Le premier cas ressort de 3.3 et 4.2. Plaçons-nous dans le second. Comme $\wedge^2 M$ est de rang un et de pente $\leq 1/2$, il est en fait de pente nulle; puisqu'il admet une structure de Frobenius, il est donc de la forme $(\mathcal{R}, \partial - \alpha)$, $\alpha \in \mathbf{Q} \cap \mathbf{Z}_p$. Si $\alpha \in 2\mathbf{Z}_p$, on peut remplacer M par $M \otimes (\mathcal{R}, \partial + \alpha/2)$, ce qui nous ramène aux hypothèses H_i). Si $\alpha \notin 2\mathbf{Z}_p$ (donc $p = 2$), on peut appliquer Frobenius $x \mapsto x^2$ et se ramener au cas précédent.

7. Opérateurs de Bessel p-adiques.

Notre objectif est maintenant d'étudier des exemples d'opérateurs différentiels dont les modules différentiels associés vérifient les hypothèses H_i) du paragraphe précédent.

On fixe $\nu \in \mathbf{Q} \cap \mathbf{Z}_p$, et pour tout entier naturel n, on définit le symbole de Pochhammer $(\nu + 1)_n = (\nu + 1)(\nu + 2) \ldots (\nu + n)$. On note f le plus petit entier > 0 tel que le dénominateur de ν divise $p^f - 1$ (il en existe). On note $\mathbf{Q}_{p^f}$ l'extension non ramifiée de $\mathbf{Q}_p$ de degré résiduel f. On note π une racine $(p-1)$-ième de $-p$ dans $\bar{\mathbf{Q}}_p$. On prend $K = \mathbf{Q}_{p^f}(\pi)$, avec $\sigma = id$ et $|p| = 1/p$.

On considère la série de Bessel

$$I_\nu(x) = x^\nu \sum_0^\infty \frac{x^{2n}}{4^n n!(\nu+1)_n} \quad (= (-4)^{\nu/2}\Gamma(\nu+1)J_\nu(\sqrt{-1}.x) \ )$$

et la série hypergéométrique confluente ${}_0F_1(\nu+1 \mid x) = \sum_0^\infty \frac{x^n}{n!(\nu+1)_n}$, qui sont reliées par la formule

$$x^{-\nu/2} I_\nu(2\pi\sqrt{x}) = {}_0F_1(\nu+1 \mid \pi^2 x).$$

D'après [AS], c'est cette dernière série p-adique, convergente dans $D(0,1^-)$, qui est directement liée aux sommes exponentielles de Kloosterman tordues par la puissance $(p^f-1)\nu$-ième du caractère de Teichmuller (voir [B] pour une formulation limpide en cohomologie rigide). De cette interprétation découle l'existence d'une structure de Frobenius sur $\mathcal{E}^\dagger$ (via φ_f) pour l'opérateur différentiel

$$\Upsilon_{\nu,x} = x^2 \tfrac{d^2}{dx^2} + (1+\nu)x\tfrac{d}{dx} - \pi^2 x = \partial^2 + \nu\partial - \pi^2 x$$

annulant ${}_0F_1(\nu+1 \mid \pi^2 x)$. De plus (loc. cit. 4.6), la structure de Frobenius sur l'équation du wronskien est donnée par $\pm p^f.x^{fa}$ pour $a \in \mathbf{Z}$ convenable.

On en déduit que l'opérateur différentiel

$$\Lambda_{\nu,x} = \partial^2 - (4\pi^2 x^2 + \nu^2)$$

qui annule $I_{\pm\nu}(2\pi x)$ vérifie aussi H_2), i.e. admet aussi une structure de Frobenius (via φ_f). Il en est de même, si $p \neq 2$ ou bien si $\nu \in 2\mathbf{Z}_2$, de l'opérateur différentiel

$$\Lambda_{\nu,\sqrt{x}} = \partial^2 - (\pi^2 x + \tfrac{\nu^2}{4})$$

qui annule $I_{\pm\nu}(2\pi\sqrt{x})$. L'avantage des deux derniers opérateurs sur $\Upsilon_{\nu,x}$ est que leur wronskien est rationnel (ils vérifient H_1)).

Remarque. L'opérateur de [CM3] 6.3.9 annule $I_{\pm 2/3}(4\ x^{-1/2}/3\sqrt{-3})$; il est proportionnel à $\Lambda_{\frac{2}{3},\sqrt{-1/27x}}$.

Commençons par la quasi-unipotence, qui ne nécessite aucun calcul p-adique sur ces opérateurs.

Proposition 7.1. *L'opérateur $\Upsilon_{\nu,x}$ et l'opérateur de Bessel $\Lambda_{\nu,x}$ sont quasi-unipotents.*

Preuve. Le cas de $\Lambda_{\nu,x}$ se déduit de celui de $\Upsilon_{\nu,x}$. À l'infini, $\Upsilon_{\nu,x}$ est purement de pente formelle 1/2. D'après 3.2, sa plus grande pente p-adique est donc $\leq 1/2$. On conclut par 6.5.

Remarque. Le cas particulier de 7.1 où $p \neq 2$, $\nu = 0$ était établi dans [T2]6.2.6. En fait, le cas p impair se traite directement: $\Lambda_{\nu,x}$ est irréductible sur $\mathcal{E}^\dagger$, mais deux solutions "formelles" en l'infini sont données par

$$x^{-1/2} e^{\pm 2\pi x}.{}_2F_0(\tfrac{\nu+1}{2}, \tfrac{-\nu+1}{2} \mid \tfrac{\pm 1}{4\pi x}) \quad \text{(cf. [WW] 17.7)}$$

et ${}_2F_0(\frac{\nu+1}{2}, \frac{-\nu+1}{2} \mid \frac{\pm 1}{4\pi x})$ converge dans $|x| > 1$ (et y est même bornée). On voit directement que $\Lambda_{\nu,x}$ est soluble dans l'extension non ramifiée cyclique de degré $2p$ de $\mathcal{E}^\dagger$ engendrée par les éléments y, z avec $z^2 = x,\ y^p - y = x$.

Les lemmes suivants précisent la situation, au prix de quelques calculs p-adiques.

Lemme 7.2. *i)* $\Lambda_{\nu,\sqrt{x}}$ *est soluble dans le disque générique* $D(t_1, 1^-)$ *si et seulement si* $p \neq 2$ *ou* $\nu \in 2\mathbf{Z}_2$. *Il est alors purement de pente* p*-adique* $1/2$.
ii) $\Lambda_{\nu,x}$ *est soluble dans le disque générique* $D(t_1, 1^-)$. *Il est purement de pente* p*-adique* $1/2$ *si* $p = 2$, *purement de pente* 1 *si* $p \neq 2$.

Preuve. Compte tenu de ce que $\nu \in \mathbf{Z}_p$, en comparant l'opérateur soluble $\Upsilon_{\nu,x}$ et $\Lambda_{\nu,\sqrt{x}}$, on voit que $\Lambda_{\nu,\sqrt{x}}$ est soluble dans le disque générique $D(t_1, 1^-)$ si et seulement si $\partial - \nu/2$ l'est, c'est-à-dire si $p \neq 2$ ou bien si $\nu \in 2\mathbf{Z}_2$. On voit aussi que $\Lambda_{\nu,x}$ est soluble.

On a vu que la plus grande pente p-adique de $\Upsilon_{\nu,x}$ est $\leq 1/2$. Par le théorème d'intégralité, $\Upsilon_{\nu,x}$ est donc purement de pente p-adique $1/2$ ou bien 0. Pour éliminer ce dernier cas, il suffit, en vertu de 3.3, de voir que $\Upsilon_{\nu,x}$ n'a pas de solution de la forme $x^\alpha.g$, où $g = \sum_{-\infty}^{\infty} a_n x^n$ est dans $\mathcal{R} \setminus 0$, et $\alpha \in \mathbf{Q} \cap \mathbf{Z}_p$. Or on voit facilement que les coefficients de g vérifieraient la récurrence

$$(n + \alpha)(n + \alpha + \nu).a_n = \pi^2.a_{n-1}$$

et, de là, qu'ils ne peuvent définir un élément de l'anneau de Robba (la série tronquée $\sum_{n>0} a_n x^n$ n'est pas surconvergente).

Les autres assertions concernant les pentes en découlent aisément ([CM3] 6.3.7-8). On précise ensuite dans quel cas de 6.3 on est:

Lemme 7.3. $S^2\Upsilon_{\nu,x}$ *est purement de pente* $1/3$ *si et seulement si* $p = 2$.

Preuve. On a $S^2\Upsilon_{\nu,x} = \partial^3 - 3\nu\partial^2 + (2\nu^2 - 4\pi^2 x)\partial - 2\pi^2(2\nu + 1)x$ (cf. 1). D'après 6.2, il s'agit de voir que $S^2\Upsilon_{\nu,x}$ a une solution de la forme $x^\alpha.g$, $g = \sum_{-\infty}^{\infty} a_n x^n \in \mathcal{R}$, $\alpha \in \mathbf{Q} \cap \mathbf{Z}_p$ si et seulement si $p \neq 2$. L'équation $S^2\Upsilon_{\nu,x}(x^\alpha.g) = 0$ équivaut à la récurrence

$$(n + \alpha)(n + \alpha - \nu)(n + \alpha - 2\nu).a_n = 2\pi^2(2n + 2\alpha + 2\nu - 1).a_{n-1}.$$

Si $p \neq 2$, on trouve une solution convergente dans $|x| > 1$ avec $\alpha = 1/2 - \nu$ et $g = \sum_{n<0} a_n x^n$. Si $p = 2$, on trouve au contraire que la série tronquée $\sum_0^\infty a_n x^n$ ne peut être nulle, et n'est pas surconvergente.

L'application de 6.3 (et de la remarque suivant 7.1) mène alors au résultat suivant:

Théorème 7.4. *L'opérateur de Bessel* p*-adique* $\Lambda_{\nu,x}$ *est supersingulier dans la couronne* $(]1, r[)$ *pour* r *assez voisin de* 1.
Si p *est impair, il est soluble dans une extension non ramifiée cyclique de degré* $2p$ *de* $\mathcal{E}^\dagger$.
Si $p = 2$, *il est soluble dans galoisienne non ramifiée de* $\mathcal{E}^\dagger$ *de groupe binaire tétraédral ou octaédral (selon le choix de* K*).*

(La supersingularité signifie qu'il y a une seule pente de Frobenius, qui est 1/2 - avec la normalisation de [T2] - compte tenu de la structure de Frobenius du wronskien).

En fait, il n'y a qu'*un seul* opérateur de Bessel sur $\mathcal{E}^\dagger$:

Proposition 7.5. *Les $\mathcal{E}^\dagger$-modules différentiels attachés aux opérateurs de Bessel $\Lambda_{\nu,x}$ et $\Lambda_{\nu',x}$ sont isomorphes. Les $\mathcal{E}^\dagger$-modules différentiels attachés aux opérateurs $\Lambda_{\nu,\sqrt{x}}$ et $\Lambda_{\nu',\sqrt{x}}$ sont isomorphes, sauf si $p=2$ et $\nu-\nu'\notin 2\mathbf{Z}_2$.*

Commençons par un lemme d'algèbre différentielle:

Lemme 7.6. *Soient $Q\neq Q'$ deux éléments d'un corps différentiel de caractéristique nulle F. Posons $\Lambda=\partial^2+Q$, $\Lambda'=\partial^2+Q'$ et notons $\Lambda\otimes\Lambda'$ l'opérateur différentiel unitaire dont les solutions sont engendrées par les produits d'une solution de Λ par une solution de Λ'. On a*

$$S^4\Lambda=\partial^5+20Q.\partial^3+30\partial(Q).\partial^2+(18\partial^2(Q)+64Q^2).\partial+(4\partial^3(Q)+64Q\partial(Q)),$$

$$\Lambda\otimes\Lambda'=\partial^4-\tfrac{\partial(Q-Q')}{Q-Q'}.\partial^3+2(Q+Q').\partial^2+\tfrac{\partial(Q)(Q-5Q')-\partial(Q')(Q'-5Q)}{Q-Q'}.\partial+$$
$$[\partial^2(Q)+\partial^2(Q')+(Q-Q')^2-\tfrac{\partial(Q-Q')}{Q-Q'}.\partial(Q+Q')].$$

Preuve de 7.6. Comme les puissances quatrièmes engendrent l'espace des polynômes quartiques, cela résulte du calcul mécanique suivant: si $\partial^2u=-Qu$, alors

$$\partial(u^4)=4u^3\partial u,\ \ \partial^2(u^4)=-4Qu^4+12u^2(\partial u)^2,$$
$$\partial^3(u^4)=-4\partial(Q).u^4-40Q.u^3\partial u+24u(\partial u)^3,$$
$$\partial^4(u^4)=[-4\partial^2(Q)+40Q^2].u^4-56\partial(Q).u^3\partial u-192Q.u^2(\partial u)^2+24(\partial u)^4,$$
$$\partial^5(u^4)=[-4\partial^3(Q)+136Q\partial(Q)].u^4+[-72\partial^2(Q)+544Q^2].u^3\partial u$$
$$-360\partial(Q).u^2(\partial u)^2-480u(\partial u)^3\ \text{ et}$$

$$[\partial^5+20Q.\partial^3+30\partial(Q).\partial^2+(18\partial^2(Q)+64Q^2).\partial+(4\partial^3(Q)+64Q\partial(Q))](u^4)=0.$$

De même, si v est une solution de Λ', on a

$$\partial(uv)=\partial uv+u\partial v,\ \partial^2(uv)=-(Q+Q')uv+2\partial u.\partial v,$$
$$\partial^3(uv)=-(\partial(Q)+\partial(Q')).uv-(3Q+Q')u\partial v-(Q+3Q')\partial uv,$$
$$\partial^4(uv)=[-\partial^2(Q)-\partial^2(Q')+6QQ'+Q^2+Q'^2].uv$$
$$-(4\partial(Q)+2\partial(Q'))u\partial v-(4\partial(Q')+2\partial(Q))v\partial u-4(Q+Q')\partial u.\partial v$$

et $\Lambda\otimes\Lambda'(uv)=0$.

Revenons à 7.5. Comme le wronskien de $\Lambda_{\nu,x}$ (resp. $\Lambda_{\nu,\sqrt{x}}$) est rationnel, le $\mathbf{Q}(x)$-module différentiel associé est isomorphe à son propre dual. De plus, on a vu qu'il est irréductible sur $\mathcal{E}^\dagger$ (et même sur $\mathcal{R}$). On voit par là qu'il suffit de montrer que $\Lambda_{\nu,x}\otimes\Lambda_{\nu',x}$ (resp. $\Lambda_{\nu,\sqrt{x}}\otimes\Lambda_{\nu',\sqrt{x}}$) a au moins une solution non nulle $g=\sum_{-\infty}^{\infty}a_nx^n$ dans $\mathcal{E}^\dagger$ (resp. sauf si $p=2$ et $\nu-\nu'\notin 2\mathbf{Z}_2$). par 7.6, on a $\Lambda_{\nu,x}\otimes\Lambda_{\nu',x}=\prod_{\epsilon,\epsilon'=\pm1}(\partial+\epsilon\nu+\epsilon'\nu')-2\pi^2x(2\partial^2+3\partial+1)$, et dire que g est solution se

ramène à la récurrence $\prod_{\epsilon,\epsilon'=\pm 1}(n+\epsilon\nu+\epsilon'\nu').a_n = \pi^2.2n(2n-1).a_{n-1}$. On trouve une solution convergente de la forme $\sum_{n<0} a_n x^n$, bornée dans $D(\infty, 1-)$ (pour p impair, cela se voit directement du reste: une telle solution est donnée par

$\frac{1}{x}\ {}_2F_0(\frac{\nu+1}{2}, \frac{-\nu+1}{2} \mid \frac{1}{4\pi x}).{}_2F_0(\frac{\nu'+1}{2}, \frac{-\nu'+1}{2} \mid \frac{-1}{4\pi x})\ )$.

Pour $\Lambda_{\nu,\sqrt{x}} \otimes \Lambda_{\nu',\sqrt{x}}$, on obtient la récurrence $\prod_{\epsilon,\epsilon'=\pm 1}(n+\frac{1}{2}(\epsilon\nu+\epsilon'\nu')).a_n = (\pi^2/2)n(2n-1).a_{n-1}$ et on peut conclure de même, sauf dans le cas où $p=2$ et $\nu-\nu' \notin 2\mathbf{Z}_2$. Cela achève la preuve de 7.5 (et conjointement à 7.4, celle de 0.1).

Terminons ce paragraphe par un exemple d'opérateur unitaire $\Lambda \in \mathbf{Q}[x,\partial]$ admettant des exposants p-adiques qui ne "proviennent" pas des exposants formels à l'origine ou à l'infini:

Proposition 7.7. *Les exposants formels de Turrittin aux singularités de*

$$\partial^5 - 80.\partial^3 - 120.\partial^2 + 8x(2^7x-9).\partial + 16x(2^6x-1)$$

sont entiers ou demi-entiers, mais cet opérateur diadique est soluble au bord intérieur d'une couronne $\mathcal{C}(]1,r[)$ dans laquelle il admet les exposants diadiques $\pm 1/3$.

Preuve. Cet opérateur n'est autre que $S^4\Lambda_{0,\sqrt{x}}$ (cf. 7.6). L'assertion sur les exposants formels est sans mystère: à l'origine, la singularité est régulière à exposants nuls; en l'infini, les solutions formelles sont combinaisons linéaires de

$$x^{-1}e^{8(n-2)\sqrt{x}}.[{}_2F_0(\tfrac{1}{2},\tfrac{1}{2} \mid \tfrac{1}{8\sqrt{x}})^n.{}_2F_0(\tfrac{1}{2},\tfrac{1}{2} \mid \tfrac{-1}{8\sqrt{x}})^{(4-n)}],\ n=0,\dots,4.$$

Considérons à présent le $\mathcal{R}$-module différentiel M attaché à $\Lambda_{0,\sqrt{x}}$. D'après 1.3, la représentation S^4V du groupe de Galois différentiel $\tilde{A}_4$ admet un facteur de rang deux de la forme $V_1' \oplus V_1''$, somme de deux représentations inéquivalentes où $\tilde{A}_4$ agit à travers son quotient $\mathbf{Z}/3\mathbf{Z}$. Ces représentations correspondent à des facteurs de rang un de S^4M. Étant de pente au plus $1/2$, on voit qu'ils sont en fait de pente nulle, et isomorphes à $(\mathcal{R}, \partial - 1/3)$ et $(\mathcal{R}, \partial + 1/3)$ respectivement. On en conclut que $S^4\Lambda_{0,\sqrt{x}}$ admet des solutions de la forme $x^{\pm 1/3}.g$, $g \in \mathcal{R}\setminus 0$.

8. Représentation galoisienne attachée à l'opérateur de Bessel diadique.

On a vu que les opérateurs de Bessel diadiques sur $\mathcal{E}^\dagger$ correspondent à une représentation d'image finie de $Gal(\mathbf{F}_2((\frac{1}{x}))^{sep}/\mathbf{F}_2((\frac{1}{x})))$. Nous nous proposons d'expliciter cette représentation, en nous inspirant de [S1]5.

Fixons $\omega \in \mathbf{F}_4,\ \omega^3 = 1, \omega \neq 1$. Soit E la courbe elliptique sur $\mathbf{F}_4$ d'équation affine $Y^2+Y = X^3+\omega$. Elle est isomorphe à sa conjuguée $Y^2+Y = X^3+\omega^2$ (au moyen de la transformation $Y \mapsto Y+X,\ X \mapsto X+1$). Soit d'autre part E_0 la courbe elliptique sur $\mathbf{F}_4$ d'équation affine $Y^2+Y = X^3$.

Ce sont deux courbes elliptiques supersingulières d'invariant $j = 0$, non isomorphes (mais qui deviennent isomorphes sur $\mathbf{F}_{16}$), cf. [H] p. 325.

Tous les automorphismes de E comme de E_0 sont définis sur $\mathbf{F}_4$: il sont de la forme $\alpha_{v,r,t}$: $X \mapsto vX + r,\ Y \mapsto Y + r^2vX + t,$ où $v \in \mathbf{F}_4^\times,\ (r,t) \in (\mathbf{F}_4^\times \times \{\omega, \omega^2\}) \cup (\{0\} \times \{0,1\})$, avec la loi de composition

$$\alpha_{v,r,t} \circ \alpha_{v',r',t'} = \alpha_{vv',vr'+r,t+t'+r^2r'v}$$

cf. [H] 3.6.2 , et p. 324. Ils forment un groupe isomorphe à $\tilde{A}_4 \cong SL_2(\mathbf{F}_3)$. Le lemme suivant se vérifie grâce aux formules de *loc. cit.*, en testant la liste des dix-huit courbes elliptiques (à isomorphisme près) définies sur $\mathbf{F}_4$ donnée dans [H] p. 325:

Lemme 8.1. *Les courbes elliptiques sur $\mathbf{F}_4$ dont le groupe des $\mathbf{F}_4$-automorphismes contient $\tilde{A}_4$ sont isomorphes à E ou E_0 sur $\mathbf{F}_4$.*

On considère à présent le revêtement galoisien ramifié $E \to E/Aut(E) \cong \mathbf{P}^1$. L'origine de E (c'est-à-dire le point de coordonnées $X = Y = \infty$) est fixée par $Aut(E)$, donc ce revêtement est totalement ramifié en ce point. Pour aller plus avant, on dévisse $\tilde{A}_4$: son 2-Sylow est un sous-groupe normal Q qui n'est autre que le groupe quaternionien $\{\pm 1, \pm i, \pm j, \pm k\}$. Le centre $Z = \{\pm id_E\}$ de $\tilde{A}_4$ est aussi celui de Q. Ce sont là les seuls sous-groupes propres normaux de $\tilde{A}_4$. On a $Q/Z = (\mathbf{Z}/2\mathbf{Z})^2,\ \tilde{A}_4/Q = \mathbf{Z}/3\mathbf{Z}$. Il n'est pas difficile d'en déduire une présentation du revêtement ramifié $E \to E/Aut(E) \cong \mathbf{P}^1$ comme une tour[(1)] dont les étages, galoisiens sur la base, sont

1) un revêtement cubique kummérien $\mathbf{P}^1 \xrightarrow{t \mapsto t^3} \mathbf{P}^1$,

2) un revêtement biquadratique $\mathbf{P}^1 \to \mathbf{P}^1$ formé de deux revêtements d'Artin-Schreier en parallèle $u^2 + u = t, v^2 + v = \omega t$,

3) au sommet, le quotient $E \to E/Z \cong \mathbf{P}^1 : (X,Y) \mapsto X$.

De plus, on peut supposer et on supposera que l'origine de E s'envoie sur le point à l'infini de la base $\mathbf{P}^1$.

Rappelons que nous notons $\mathbf{Q}_4$ l'extension quadratique non ramifiée de $\mathbf{Q}_2$.

Théorème 8.2. *L'extension minimale de $\mathcal{E}^\dagger_{x,\mathbf{Q}_4}$ dans laquelle l'opérateur de Bessel $\Lambda_{\nu,x}$ est soluble est de la forme $\mathcal{E}^\dagger_{y,\mathbf{Q}_4}/\mathcal{E}^\dagger_{x,\mathbf{Q}_4}$. L'extension de corps résiduels s'obtient par localisation-complétion au-dessus de l'infini dans le revêtement $E \to E/Aut(E) \cong \mathbf{P}^1$.*

Preuve. En vertu de 7.5, on peut se limiter à $\Lambda_{0,x}$. Cela nous permet de choisir dans un premier temps $f = 1, k = \mathbf{F}_2$. Il sera commode de prendre $K = \mathbf{Q}_2(i),\ \sigma = id$: en effet, en divisant la structure de Frobenius par $i - 1$, on peut la supposer de pente nulle. Le $\mathcal{E}^\dagger$-module différentiel attaché à $\Lambda_{0,x}$ correspond alors (cf. [M2] 4.4) à une représentation $\mathbf{Q}_2(i)$-linéaire τ de

(1) on a la même présentation pour E_0.

$Gal(\mathbf{F}_2((\frac{1}{x}))^{sep}/\mathbf{F}_2((\frac{1}{x})))$ de dimension deux, et d'image finie G. Son carré exterieur est trivial, i.e. $G \subset SL_2(K)$. L'extension définie par l'image de τ est donc de la forme $\mathbf{F}_{2^m}((\frac{1}{y}))/\mathbf{F}_2((\frac{1}{x}))$.
Il suit de 7.4 (voir aussi 6.3) que le sous-groupe normal $Gal(\mathbf{F}_{2^m}((\frac{1}{y}))/\mathbf{F}_{2^m}((\frac{1}{x})))$ de G n'est autre que $\tilde{A}_4$. On a donc $m \leq 2$, et $G = \tilde{A}_4$ ou bien $\tilde{S}_4$. Dans les deux cas, Q est un sous-groupe normal de G. En observant le quotient G/Q et en remarquant que la seule extension galoisienne cubique de $\mathbf{F}_2((\frac{1}{x}))$ est $\mathbf{F}_8((\frac{1}{x}))$, on voit que $G = \tilde{S}_4$ et $m = 2$.

Pour aller plus loin, il nous faut analyser la ramification de l'extension à déterminer $\mathbf{F}_4((\frac{1}{y}))/\mathbf{F}_{2^m}((\frac{1}{x}))$. On voit d'emblée que le groupe d'inertie $G_0 = G^0$ est $\tilde{A}_4$, et que le groupe d'inertie sauvage G_1 est son 2-Sylow Q. Au-delà, on dispose du théorème 4.4 qui relie les groupes de ramification aux pentes p-adiques. On a vu que $\Lambda_{0,x}$ est de pente $1/2$, et son carré symétrique de pente $1/3$. Via 4.4, le formalisme de la décomposition suivant les "sauts" ([K2] 1) montre que $1/2$ et $1/3$ figurent parmi les sauts de la filtration par les groupes de ramification en numérotation supérieure $G^r \triangleleft G$ (voir aussi [S2] IV). Comme les seuls sous-groupes propres normaux de G sont $Z, Q, \tilde{A}_4$, on a

$G^r = Q$ si $0 < r < 1/3$, $G^r = Z$ si $1/3 < r < 1/2$, $G^r = \{1\}$ si $r > 1/2$.

En numérotation inférieure, cela donne: $G_1 = Q$, $G_2 = G_3 = Z$, $G_4 = \{1\}$.

Pour exploiter cette information sous forme géométrique, nous ferons appel à la théorie des extensions canoniques de Katz-Gabber ([K1] 1.4). Elle montre que l'extension $\mathbf{F}_4((\frac{1}{y}))/\mathbf{F}_2((\frac{1}{x}))$ provient d'un revêtement étale de $\mathbf{G}_m = \mathbf{P}^1 \setminus \{0, \infty\}$. Plus précisément, compte tenu de ce que le 2-Sylow de $\tilde{A}_4$ est normal, il existe un revêtement étale galoisien $f : C \to \mathbf{G}_{m,\mathbf{F}_4}$ de groupe $\tilde{A}_4$ totalement ramifié à l'infini et modérément ramifié au-dessus de 0, tel que le revêtement $Spec\, \mathbf{F}_4((\frac{1}{y}))/Spec\, \mathbf{F}_2((\frac{1}{x}))$ provienne du revêtement composé

$$C \to \mathbf{G}_{m,\mathbf{F}_4} \to \mathbf{G}_{m,\mathbf{F}_2}$$

par localisation-complétion à l'infini. Connaissant les groupes de ramification à l'infini, on trouve que f est une tour dont les étages, galoisiens sur la base $\mathbf{G}_{m,\mathbf{F}_4}$, sont

$1'$) un revêtement cubique kummérien $\mathbf{G}_m \xrightarrow{t \mapsto t^3} \mathbf{G}_m$,

$2'$) un revêtement biquadratique $\mathbf{G}_m \to \mathbf{G}_m$ formé de deux revêtements d'Artin-Schreier en parallèle $u^2 + u = t, v^2 + v = \omega t$,

$3'$) au sommet, le quotient $C \to C/Z \cong \mathbf{G}_m$, revêtement d'Artin-Schreier du type $Y^2 + Y = P(X)$, où P est un polynôme cubique (cf. [S2] IV, 2, ex. 5).
La complétion projective $\bar{C}$ de C est donc une courbe elliptique sur $\mathbf{F}_4$, et il suit du lemme 8.1 que $\bar{C} = E$ ou bien $\bar{C} = E_0$.

Pour trancher, examinons l'action de $G = \tilde{S}_4$ sur $\bar{C}$ (vue comme courbe sur $\mathbf{F}_2$). Le 2-Sylow de $\tilde{S}_4$ est le groupe quaternionien généralisé à seize éléments, dont le seul élément d'ordre exactement 2 est $-1 \in Z$. Cela entraîne que le quotient $Gal(\mathbf{F}_4/\mathbf{F}_2)$ de G ne se relève pas, ce qui exclut la courbe elliptique E_0

qui est définie sur $\mathbf{F}_2$ (le groupe du revêtement composé $E_0 \to \mathbf{P}^1_{\mathbf{F}_4} \to \mathbf{P}^1_{\mathbf{F}_2}$ est $GL_2(\mathbf{Z}/3\mathbf{Z})$ et non $\tilde{S}_4$). Ceci achève la preuve de 8.2.

Remarque. La situation que nous rencontrons ici est un analogue géométrique de celle de [S1] 4.

Au lieu du choix ci-dessus de (K, σ, f) (qui nous a permis de trancher entre E et E_0), il paraît plus naturel de prendre $K = \mathbf{Q}_4,\ \sigma = id,\ f = 2$. En divisant la structure de Frobenius (relative à $x \mapsto x^4$) par 2, on se ramène au cas de pente frobeniusienne nulle. D'après 4.6, le $\mathcal{E}^\dagger_{x,\mathbf{Q}_4}$-module différentiel attaché à $\Lambda_{0,x}$ (ou $\Lambda_{\nu,x}$, peu importe) muni de cette nouvelle structure de Frobenius correspond à une représentation $\mathbf{Q}_4$-linéaire ρ de $Gal(\mathbf{F}_4((\frac{1}{x}))^{sep}/\mathbf{F}_4((\frac{1}{x})))$ de dimension deux et d'image $Aut(E) = SL_2(\mathbf{Z}/3\mathbf{Z})$.

Proposition 8.3. *Cette représentation ρ est la représentation naturelle de $Aut(E)$ dans le groupe de cohomologie cristalline $H^1_{cris}(E/\mathbf{Q}_4)$.*

Preuve. Nous allons comparer leurs caractères, en commençant par remarquer:

Lemme 8.4. *Il existe un unique caractère de $SL_2(\mathbf{Z}/3\mathbf{Z})$ de degré deux à valeurs dans $\mathbf{Q}_2$ (il est en fait à valeurs dans $\mathbf{Z}$).*

En effet, des trois caractères de $SL_2(\mathbf{Z}/3\mathbf{Z})$ de degré deux, seul celui noté X_ϕ dans [FH] p. 72 est à valeurs dans $\mathbf{Q}_2$.

Il est bien connu que le caractère de la représentation naturelle de $Aut(E)$ dans $H^1_{cris}(E/\mathbf{Q}_4)$ est à valeurs dans $\mathbf{Z}$. Il reste à voir que le caractère de ρ est à valeurs dans $\mathbf{Q}_2$. Un résultat de [T1] 3.4.6 sur le changement de coefficients montre que ρ et la restriction de τ à $Gal(\mathbf{F}_4((\frac{1}{x}))^{sep}/\mathbf{F}_4((\frac{1}{x})))$ deviennent isomorphes sur $\mathbf{Q}_4(i)$. Leur caractère commun est donc à valeurs dans $\mathbf{Q}_2(i) \cap \mathbf{Q}_4 = \mathbf{Q}_2$, d'où l'assertion.

Remarque. On a une "formule de Weil" reliant la représentation d'Artin de $Gal(\mathbf{F}_4((\frac{1}{y}))/\mathbf{F}_4((\frac{1}{x})))$ à la cohomologie rigide de la courbe E privée des neuf points de ramification du revêtement $E \to \mathbf{P}^1_{\mathbf{F}_4}$, cf. [M2] 7.17 et [Hy].

Bibliographie

[AS] A. Adolphson, S. Sperber, *Twisted Kloosterman sums and p-adic Bessel functions*, Amer. J. Math. **106** (1984), 549-591.

[Ba] F. Baldassarri, *Differential modules and singular points of p-adic differential equations*, Advances in Math. **44** (1982), 155-179.

[B] P. Berthelot, *Cohomologie rigide et théorie de Dwork: le cas des sommes exponentielles*, in S.M.F. Astérisque **119-120** (1984), 17-49.

[Be] F. Beukers, *Differential Galois theory*, chap. 8 de "From Number Theory to Physics", Springer-Verlag ed. (1995).

[Bo] N. Bourbaki, *Algèbre commutative*, chapitres I, VII, Masson (1985).

[CD] G. Christol, B. Dwork, *Modules différentiels sur des couronnes*, Ann. Inst. Fourier, Grenoble **44** (1994), 663-701.

[CM2] G. Christol, Z. Mebkhout, *Sur le théorème de l'indice des équations différentielles p-adiques II*, Ann. of Maths **146** (1997), 345-410.

[CM3] G. Christol, Z. Mebkhout, *Sur le théorème de l'indice des équations différentielles p-adiques III*, Ann. of Maths **151** (2000), 385-457.

[Co] H.S.M. Coxeter, *Complex regular polytopes*, 2e éd., Cambridge Univ. press (1991).

[Cr1] R. Crew, *F-isocrystals and p-adic representations*, in *Algebraic Geometry - Bowdoin 1985*, Proc. Symp. Pure Math. XLVI (2) (1987), 111-138.

[Cr2] R. Crew, *Finiteness theorems for the cohomology of an overconvergent isocrystal on a curve*, Ann. scient. Éc. Norm. Sup. **31** (1998), 717-763.

[D] B. Dwork, *Bessel functions as p-adic functions of their argument*, Duke Math. J. **41** (1974), 711-738.

[F] J.M. Fontaine, *Représentations p-adiques des corps locaux*, Grothendieck Festschrift II, Progress in Math. **87**, Birkhauser (1990), 249-309.

[FH] W. Fulton, J. Harris, *Representation theory*, Springer GTM **129** (1991).

[H] D. Husemoller, *Elliptic curves*, (appendix by R. Lawrence), Springer GTM **111** (1987).

[Hy] Hyodo O., *A cohomological construction of Swan representations over the Witt ring II*, Proc. Japan Acad. **64A** (1988), 350-351.

[K1] N. Katz, *Local-to-global extensions of representations of fundamental groups*, Ann. Inst. Fourier, Grenoble **36** (1986), 69-106.

[K2] N. Katz, *Gauss sums, Kloosterman sums, and monodromy groups*, Annals of math. studies **116**, Princeton (1988).

[M1] Matsuda S., *Local indices of p-adic differential operators corresponding to Artin-Schreier-Witt coverings* , Duke Math. J. **77** (1995), 607-625.

[M2] Matsuda S., *Katz correspondence for quasi-unipotent overconvergent isocrystals*, manuscrit (1997).

[P] M. van der Put, *Galois theory of differential equations, algebraic groups and Lie algebras,* J. symbolic computation **28** (1999), 441-472.

[S1] J.P. Serre, *Sur la rationalité des représentations d'Artin*, Ann. of Maths **72** (1960), 406-420.

[S2] J.P. Serre, *Corps locaux*, Hermann, 1968.

[T1] Tsuzuki N., *The local index and the Swan conductor*, Compos. Math. **111** (1998), 245-288.

[T2] Tsuzuki N., *Slope filtration of quasi-unipotent overconvergent F-isocrystals*, Ann. Inst. Fourier, Grenoble **48** (1998), 379-412.

[T3] Tsuzuki N., *Finite local monodromy of overconvergent unit-root F-isocrystal on a curve*, Amer. J. Math. **120** (1998), 1165-1190.

[V] M.F. Vignéras, *Arithmétique des algèbres de quaternions*, Lect. Notes 800, Springer (1980).

[WW] E. Whittaker, G. Watson, *A course of modern analysis*, 4e éd., réimpression, Cambridge Univ. press (1996).