Représentations galoisiennes associées aux courbes hyperelliptiques lisses*

C. Huyghe and N. Wach

May 21, 2014

Abstract

In 2003, Kedlaya gave an algorithm to compute the zeta function associated to a hyperelliptic curve over a finite field, by computing the rigid cohomology of the curve. Edixhoven remarked that it is actually possible to compute the crystalline cohomology of the curve, which is a lattice in the rigid cohomology. Following a method of Wach, we explain how to use this lattice to compute the (φ, Γ)-module associated to an hyperelliptic curve.

Résumé

En 2003, Kedlaya a donné un algorithme pour calculer la fonction zêta d'une courbe hyperelliptique sur un corps fini, en calculant la cohomologie rigide de la courbe. Edixhoven a remarqué qu'on pouvait en fait calculer la cohomologie cristalline de la courbe, qui est un réseau dans la cohomologie rigide. Nous expliquons comment utiliser ce réseau pour calculer le (φ, Γ)-module associé à une courbe hyperelliptique, en suivant une méthode due à Wach.

Table des matières

*Les deux auteurs ont bénéficié du soutien du projet CETHop : ANR-09-JCJC-0048-01, coordonné par Xavier Caruso, projet de l'Agence Nationale de la Recherche.

MSC classification 2010 : 11S23, 14F30, 14F40

Introduction

Soient k un corps fini de caractéristique p différente de 2, de cardinal p^n, $W = W(k)$, l'anneau des vecteurs de Witt de k, K le corps des fractions de W, S le schéma Spec W, X une courbe hyperelliptique lisse sur $W(k)$, de genre g, X_k, resp. X_K la fibre spéciale, resp. la fibre générique de X. Le but de ce texte est d'expliquer comment calculer modulo p^i le (φ, Γ)-module associé à la courbe X_K, c'est-à-dire le (φ, Γ)-module associé à la représentation galoisienne $H^1_{et}(X_{\overline{K}}, \mathbf{Q}_p)$.

La méthode générale modulo p^i exposée en 5.1 repose sur le calcul par Kedlaya [Ked01], de la cohomologie rigide d'une courbe hyperelliptique et de l'action du Frobenius sur cette cohomologie. Edixhoven a ensuite remarqué dans [Edi03] que l'on pouvait calculer un réseau (en fait la cohomologie cristalline) dans la cohomologie rigide des courbes hyperelliptiques, peut-être inspiré par un argument de Katz dans le cas des courbes elliptiques qu'on trouve dans A1.2 de [Kat73]. Bogaart a enfin donné la démonstration du résultat d'Edixhoven dans un preprint non publié [vdB08]. Cette approche a été systématisée par Lauder [Lau06], ainsi que par Abbott, Kedlaya et Roe [AKR10]. Même si on peut calculer la cohomologie cristalline d'une courbe hyperelliptique, on ne dispose pas cependant de calcul purement cristallin du Frobenius : pour ce faire, il faut utiliser la méthode de Kedlaya. Le calcul du (φ, Γ)-module associé à la courbe X_K fait intervenir un algorithme dû à Wach [Wac97] et nécessite de disposer d'un réseau stable par le Frobenius dans la cohomologie rigide de X_k, d'où l'intérêt de la remarque d'Edixhoven. Le résultat que nous prouvons est le suivant : connaissant la matrice du Frobenius dans une base adaptée à la filtration de Hodge de la cohomologie cristalline, il est possible de déterminer algorithmiquement le (φ, Γ)-module associé à la courbe X. Si la courbe est de genre g, la complexité de l'algorithme calculant le (φ, Γ)-module modulo (p^i, T^j) est au plus

$$O\big(((\log p)^{2+\varepsilon} g^2 + (\log p)^{1+\varepsilon} g^\omega) n^{1+\varepsilon} i^{2+\varepsilon} j\big),$$

où ω représente le plus petit exposant pour la multiplication des matrices. Il faut y rajouter la complexité de l'algorithme de Kedlaya pour calculer la matrice de Frobenius modulo p^{i+1} qui est $O(p^{1+\varepsilon} n^{1+\varepsilon} g^{2+\varepsilon} i^{2+\varepsilon})$ et celle d'un changement de base.

Voici le contenu de cet article. Après une première partie de notations, nous donnons dans une deuxième partie une stratégie générale pour calculer la cohomologie de de Rham d'une courbe projective lisse sur W. En effet, d'après le théorème de comparaison de Berthelot, cette cohomologie de de Rham est canoniquement isomorphe à la cohomologie cristalline de la courbe X_k. En particulier, cela nous donne un réseau stable par le Frobenius dans la cohomologie rigide de X_k. Cette stratégie de calcul reprend celle de Bogaart-Edixhoven et est exposée ici dans le cadre des catégories dérivées. L'argument est simple : si on twiste le

complexe de de Rham de X par une puissance suffisante du faisceau inversible associé au diviseur à l'infini, on obtient un complexe acyclique pour le foncteur sections globales. Et le quotient des deux complexes est un complexe à support au point à l'infini. Du coup, tout est facilement calculable dans la catégorie dérivée des complexes de W-modules, pourvu que l'on sache déterminer les sections globales du module des différentielles. C'est ce que nous faisons dans la troisième partie.

Dans la quatrième partie, nous détaillons comment trouver le (φ, Γ)-module associé à une courbe. On considère le produit tensoriel sur W de l'anneau $S = W[[T]]$ et du W-module $H^1_{cris}(X)$, sur lequel on définit une action naturelle de φ ; l'algorithme, déjà expliqué dans [Wac97], consiste à déterminer la matrice d'un générateur de Γ par dévissages modulo les puissances de p et les puissances de T. Il suffit alors de calculer l'inverse de la matrice du Frobenius divisé modulo p.

Nous appliquons ces résultats au cas des courbes hyperelliptiques dans la cinquième partie. L'algorithme donnant le (φ, Γ)-module à une précision (p^i, T^j) fixée reposant sur l'algorithme de Kedlaya est donné en 5.1.

Nous remercions le Referee pour ses remarques constructives sur divers aspects de ce texte, ainsi que Jérémy Leborgne, et Marcela Szopos qui nous ont aidées à éclaircir les problèmes de complexité.

1 Conventions, notations

Si X est un S-schéma, nous noterons X_0 la fibre spéciale et X_K la fibre générique.

Une courbe X sur S est par définition un S-schéma noetherien de dimension 1 qui est de type fini sur S, irréductible, dont les fibres sur S (c'est-à-dire la fibre spéciale et la fibre générique) sont réduites et connexes, géométriquement réduites et géométriquement connexes. On suppose de plus qu'il existe une section $i_s : S \hookrightarrow X$ correspondant à un diviseur relatif de degré 1 sur S.

Sous ces hypothèses (3.3.21 de [Liu02]), $H^0(X_0, \mathcal{O}_{X_0}) = k$ et $H^0(X_K, \mathcal{O}_{X_K}) = K$.

On dit qu'une courbe X est de genre g si la fibre générique et la fibre spéciale sont de genre arithmétique égal à g. Dans le cas où X est lisse, ce qui sera toujours le cas ici, l'égalité de ces deux nombres est automatique, par invariance de la caractéristique d'Euler Poincaré (5.3.28 de [Liu02]), et platitude de $\mathcal{O}_X$ sur W. De plus, si X est lisse, X est un schéma intègre.

Dans cet article, la catégorie $D^b(W)$ désignera la catégorie dérivée des complexes de W-modules sur une courbe X, à cohomologie bornée.

Nous disons qu'une courbe lisse X vérifie la condition de Mazur explicitées dans l'appendice de [Maz73], si

$$\forall i \in \{0,1\}, \forall j \in \{0,1\}\ H^i(X, \Omega^j_X) \text{ est un } W \text{ module libre .} \tag{1}$$

Si ces conditions sont vérifiées, alors, par définition, les modules $E_1^{j,i}$ de la suite spectrale de Hodge vers de Rham sont des W-modules libres et donc la suite spectrale de Hodge vers de Rham dégénère d'après loc. cit..

2 Méthode de calcul du complexe de de Rham d'une courbe

Dans cette section X est une courbe lisse de genre g comme définie en 1. Si C est le complexe de de Rham

$$C: \ 0 \to \mathcal{O}_X \to \Omega_X^1 \to 0,$$

dont les termes sont en degré 0 et 1, la cohomologie de de Rham de X est la cohomologie du complexe $R\Gamma(X, C)$. Nous considérons aussi le complexe de de Rham twisté $C(nD)$ où D est un diviseur de X

$$C(nD): \ 0 \to \mathcal{O}_X((n-1)D) \to \Omega_X^1(nD) \to 0.$$

La filtration bête du complexe C induit la suite spectrale de Hodge vers de Rham. La proposition suivante rappelle un critère de dégénerescence standard.

Proposition 2.1. *(i) Sous nos hypothèses, la condition de Mazur 1 est vérifiée. En particulier, la suite spectrale de Hodge vers de Rham dégénère au niveau E_1. De plus $H^0(X, \mathcal{O}_X) = W$.*

(ii) Les modules $H^0_{DR}(X)$ et $H^2_{DR}(X)$ s'identifient à W, le module $H^1_{DR}(X)$ est un W-module libre.

Démonstration. Le terme général de la suite spectrale de Hodge vers de Rham est $E_1^{j,i} = H^i(X, \Omega_X^j)$, les différentielles de la suite spectrale proviennent des flèches canoniques $H^i(X, \Omega_X^j) \to H^i(X, \Omega_X^{j+1})$ et la dégenerescence de la suite spectrale équivaut, dans le cas d'une courbe lisse X, à la nullité de la flèche $H^1(X, \mathcal{O}_X) \to H^1(X, \Omega_X^1)$.

Montrons que les modules $H^i(X, \Omega_X^j)$ sont des W-modules libres. Ceci résulte par exemple du lemme 3.1 de [vdB08], dont nous reproduisons la démonstration ici. D'après le théorème de semi-continuité (5.3.20 de [Liu02]), il suffit de vérifier que les groupes de cohomologie $H^i(X_k, \Omega_{X_k}^j)$ et $H^i(X_K, \Omega_{X_K}^j)$ ont même dimension pour $i, j \in \{0, 1\}$. La caractéristique d'Euler-Poincaré des faisceaux $\mathcal{O}_{X_K}$ et $\mathcal{O}_{X_0}$ est la même. De plus, $H^0(X_0, \mathcal{O}_{X_0}) = k$ et $H^0(X_K, \mathcal{O}_{X_K}) = K$ ont même dimension sur k et K respectivement, de sorte que $H^1(X_0, \mathcal{O}_{X_0})$ et $H^1(X_K, \mathcal{O}_{X_K})$ ont aussi même dimension. Par dualité de Serre, les modules $H^i(X_0, \Omega_{X_0}^1)$ et $H^i(X_K, \Omega_{X_K}^1)$ ont aussi même dimension. Ainsi la courbe X vérifie la condition de Mazur.

Considérons maintenant $M = H^0(X, \mathcal{O}_X)$: c'est un W-module libre M tel que $M \otimes K$ est isomorphe à $H^0(X_K, \mathcal{O}_{X_K}) = K$, et qui est donc isomorphe à W. Par dualité de Serre (III, §11 de [Har66]) et compte tenu du fait que $H^1(X, \Omega_X^1)$ est un W-module libre, nous trouvons que $H^1(X, \Omega_X^1) \simeq W$. Ceci mis ensemble montre (i). La dégénerescence de la suite spectrale de Hodge vers de Rham implique que l'on a une suite exacte courte

$$0 \to H^0(X, \Omega_X^1) \to H^1_{DR}(X) \to H^1(X, \mathcal{O}_X) \to 0,$$

de sorte que le W-module $H^1_{DR}(X)$ est libre. De plus $H^0_{DR}(X) \simeq H^0(X, \mathcal{O}_X) \simeq W$, et $H^2_{DR}(X) \simeq H^1(X, \Omega^1_X) = W$. □

Considérons maintenant un diviseur relatif D sur X. Alors nous pouvons compléter la proposition précédente par la

Proposition 2.2. *i Si D est de degré > 0, alors $H^0(X, \Omega^1_X(D))$ est un W-module libre et $H^1(X, \Omega^1_X(D)) = 0$.*

ii Si D est de degré ≥ 1 et si n est un entier tel que $(n-1)deg(D) > 2g-2$, alors $H^0(X, \mathcal{O}_X((n-1)D))$ est un W-module libre et le complexe $C(nD)$ est à termes acycliques pour le foncteur Γ.

Démonstration. Là encore, nous suivons 3.1 de [vdB08]. Si D est de degré > 0, alors $dim\, H^0(X_0, \mathcal{O}_{X_0}(-D)) = dim\, H^0(X_K, \mathcal{O}_{X_K}(-D)) = 0$ et donc, par dualité de Serre, $dim\, H^1(X_0, \Omega^1_{X_0}(D)) = dim\, H^1(X_K, \Omega^1_{X_K}(D)) = 0$, ce qui entraîne comme précédemment que $H^1(X, \Omega^1_X(D)) = 0$ car ce module est un W-module de type fini. Par invariance de la caractéristique d'Euler-Poincaré, il y a donc aussi égalité des dimensions des $H^0(X_0, \Omega^1_{X_0}(D))$ et de $H^0(X_K, \Omega^1_{X_K}(D))$, d'où le fait que $H^0(X, \Omega^1_X(D))$ est un W-module libre et (i). En particulier, avec les hypothèses de (ii), on sait que $H^1(X, \Omega^1_X(nD)) = 0$. Le raisonnement est identique pour (ii), puisque $H^0(X_0, \Omega^1_{X_0}(-(n-1)D))$ (resp. $H^0(X_K, \Omega^1_{X_K}(-(n-1)D))$) est nul, car le degré de $\Omega^1(-(n-1)D)$ est < 0. Par dualité de Serre, $H^1(X_0, \mathcal{O}_{X_0}((n-1)D))$ (resp. $H^1(X_K, \mathcal{O}_{X_K}((n-1)D))$) est nul, et ceci montre que $H^1(X, \mathcal{O}_X((n-1)D)) = 0$. Par invariance de la caractéristique d'Euler-Poincaré, on obtient aussi que $H^0(X_0, \mathcal{O}_{X_0}((n-1)D))$ et $H^0(X_K, \mathcal{O}_{X_K}((n-1)D))$ ont même dimension et donc que $H^0(X, \mathcal{O}_X((n-1)D))$ est un W-module libre. □

Remarque. On notera que la différentielle

$$d_1^{\{0,0\}} : H^0(X, \mathcal{O}_X((n-1)D)) \to H^0(X, \Omega^1_X(nD)),$$

n'est pas nulle en général (par exemple pour $\mathbf{P}^1_S$, $n = 2$, D le point à l'infini) et donc que la suite spectrale associée à la filtration bête du complexe $C(nD)$ ne dégénère pas en général.

Fixons maintenant une section $i_s : S \hookrightarrow X$ correspondant à un diviseur relatif de degré ≥ 1 et n strictement supérieur à $2g-2$. La suite exacte de complexes

$$0 \to C \to C(nD) \to C(nD)/C \to 0,$$

donne lieu à un triangle distingué (T') dans $D^b(W)$.

Si t est un paramètre local définissant la section s, le complété de $\mathcal{O}_{X,t}$ pour la topologie t-adique s'identifie à l'anneau de séries formelles $W[[t]]$ (chap. 8, §5 Anneaux locaux réguliers, thm 2 de [Bou83]) et le complexe de faisceaux gratte-ciels $C(nD)/C$ au complexe

$$\bigoplus_{i=1}^{n-1} Wt^{-i} \xrightarrow{d} \bigoplus_{i=1}^{n} Wt^{-i}dt.$$

Comme $d(t^{-i}) = (-i)t^{-(i+1)}$, le complexe $R\Gamma(X, C(nD)/C)$ est concentré en degré 1, où il s'identifie à

$$coker(d) = \bigoplus_{i=1}^{n} (W/(i-1)W)t^{-i}dt. \tag{2}$$

En outre, le complexe $R\Gamma(X, C(nD))$ est représenté par le complexe

$$0 \to \Gamma(X, \mathcal{O}_X((n-1)D)) \to \Gamma(X, \Omega^1_X(nD)) \to 0.$$

Finalement, pour calculer la cohomologie de de Rham, on dispose d'un triangle distingué

$$R\Gamma(X, C) \to R\Gamma(X, C(nD)) \to R\Gamma(X, C(nD)/C) \xrightarrow{+} R\Gamma(X, C). \tag{3}$$

Le but de cet article est de décrire ce triangle dans le cas des courbes hyperelliptiques, pour D correspondant au point à l'infini et $n = 2g$, où g est le genre de la courbe. Pour les calculs, nous utiliserons le lemme suivant.

Lemme 2.3. *Soient U un ouvert affine de X, supposé irréductible, tel que U_0 soit un ouvert non vide de la fibre spéciale X_0, et $\mathcal{E}$ un faisceau localement libre de rang fini sur X.*

(i) Soit $f \in \mathcal{E}(U)$ tel qu'il existe $l \in \mathbf{N}$ tel que $p^l f \in \mathcal{E}(X)$, alors $f \in \mathcal{E}(X)$.

(ii) De plus $\mathcal{E}(X) \subset \mathcal{E}(U)$ et le quotient est sans p-torsion.

(iii) Soit M un réseau de $\mathcal{E}(X)$, tel que $\mathcal{E}(U)/M$ soit sans p-torsion, alors $M = \mathcal{E}(X)$.

Démonstration. Notons j l'inclusion de $U \hookrightarrow X$. Remarquons que, puisque X et X_0 sont des schémas intègres, les hypothèses impliquent que

$$\mathcal{E}/p\mathcal{E} \hookrightarrow j_*\mathcal{E}_{|U}/p\mathcal{E}_{|U}.$$

En effet, X_0 est recouvert par des ouverts affines sur lesquels $\mathcal{E}/p\mathcal{E}$ est un $\mathcal{O}_{X_0}$-module libre, si bien que l'assertion se ramène à la même assertion pour $\mathcal{E} = \mathcal{O}_X$, qui résulte de l'intégrité de X_0 et du fait que U_0 est dense dans X_0. En passant aux sections globales, et en tenant compte du fait que l'ouvert U est affine, on a une inclusion

$$r : \mathcal{E}(X)/p\mathcal{E}(X) \hookrightarrow \mathcal{E}(U)/p\mathcal{E}(U).$$

Soit $f \in \mathcal{E}(U)$ comme dans l'énoncé, tel que $p^l f \in \mathcal{E}(X)$ avec $l \geq 1$. Nous procédons par récurrence sur l, le cas $l = 0$ étant évident. Posons $f' = p^{l-1}f \in \mathcal{E}(U)$. Alors $h = pf' \in \mathcal{E}(X)$, et $r(h) = 0$, ce qui montre qu'il existe $h' \in \mathcal{E}(X)$ tel que $h = pf' = ph'$, or $\mathcal{E}(X)$ est sans p-torsion car $\mathcal{E}$ est localement libre, de sorte que ceci implique que $f' = h' \in \mathcal{E}(X)$. Ainsi $p^{l-1}f \in \mathcal{E}(X)$ et l'hypothèse de récurrence entraîne que $f \in \mathcal{E}(X)$. Le (ii) résulte du fait qu'on a une inclusion

$$\mathcal{E} \hookrightarrow j_*\mathcal{E}_{|U},$$

d'où l'inclusion des sections globales. Le fait que le quotient soit sans p-torsion est une simple traduction de (i). Le (iii) vient du fait que l'on a une injection $\mathcal{E}(X)/M \hookrightarrow \mathcal{E}(U)/M$, de sorte que $\mathcal{E}(X)/M$ est sans torsion et comme M est un réseau de $\mathcal{E}(X)$, on a l'égalité $M = \mathcal{E}(X)$. □

Nous aurons aussi besoin de quelques considérations de base à propos de l'action de l'involution hyperelliptique. Soient V une W-algèbre, M un V-module muni d'une action V-linéaire d'une involution u (telle que $u^2 = Id$). On pose alors :

$$M^- = \{x \in M \,|\, u(x) = -x\}, \quad M^+ = \{x \in M \,|\, u(x) = x\}.$$

Comme $car(k) \neq 2$, on a un isomorphisme canonique

$$M \xrightarrow{\sim} M^+ \bigoplus M^-$$

$$x \longmapsto (x + u(x), x - u(x)),$$

et le foncteur $M \mapsto M^-$ est exact, de même que $M \mapsto M^+$. Nous en déduisons le fait suivant. Soit $V \to V'$ un morphisme de W-algèbres. Si M est muni d'une involution V-linéaire, u, alors $1 \otimes u$ est une involution V'-linéaire du V'-module $M \otimes_V V'$, et le morphisme canonique $M^- \otimes_V V' \to (M \otimes_V V')^-$ est un isomorphisme (resp. avec M^+).

3 Cohomologie de de Rham des courbes hyperelliptiques

3.1 Equations

3.1.1 Données

Soit P un polynôme unitaire de $W[X]$ de degré impair $d = 2g + 1$, tel que P est séparable comme polynôme à coefficients dans K et tel que la classe de P dans $k[X]$ est aussi séparable. On note $P(X) = X^d + \sum_{l=1}^{d-1} a_l X^l$.

Définissons, suivant 7.4.24 de [Liu02], la courbe hyperelliptique X suivante. Soient $[u, v]$ les coordonnées projectives sur $\mathbf{P}^1_W$, $x = v/u$ une coordonnée fixée sur $D_+(u)$, $x_1 = u/v$ une autre fixée sur $D_+(v)$. La courbe X est un revêtement h de degré 2 de $\mathbf{P}^1_W$, réunion de deux ouverts affines $U = h^{-1}(D_+(u))$ et $W = h^{-1}(D_+(v))$ donnés par

$$U = \mathrm{Spec} W[x, y]/y^2 - P(x),$$

$$V = \mathrm{Spec} W[x_1, t]/t^2 - P_1(x_1),$$

où l'on a posé $P_1(x_1) = x_1^{d+1} P(1/x_1) = x_1 R_1(x_1)$, $t = y/x^{g+1}$.

Les conditions sur P assurent que la courbe X ainsi définie est lisse et irréductible. De même, les fibres génériques et spéciales sont lisses, connexes et géométriquement connexes.

Nous pouvons donc appliquer les résultats de 2. On note X_0 la fibre spéciale de X et X_K la fibre générique de X.

On vérifie facilement que comme dans le cas d'un corps le lieu de ramification de h est $V(P) \bigcup V(x_1)$.

Dans la suite nous noterons A (resp. A')la W-algèbre $W[x,y]/y^2 - P(x)$, qui est un $W[x]$-module libre de rang 2 de base 1, y.

L'application définie sur U par $\iota(x,y) = (x,-y)$ et sur V par $\iota(x_1,t) = (x_1,-t)$ définit une involution de X dont les points fixes sont le lieu de ramification de h.

3.1.2 Situation en l'infini

Par convention, le point à l'infini noté ∞ de $\mathbf{P}^1_W$ correspond à $x_1 = 0$, et le point à l'infini aussi noté ∞ de X est le point de V vérifiant $x_1 = 0$. Remarquons que $R_1(x_1) = 1 + \sum_{l=1}^{d} a_{d-l} x_1^l$ est de valuation 0 en x_1, en d'autres termes P_1' est inversible de l'anneau local $\mathcal{O}_{X,\infty}$. Un générateur du faisceau localement libre Ω^1_V est dx_1/t d'après 6.4.14 de [Liu02]. Dans le module $\Omega^1_{V,\infty}$ on a la relation $dx_1/2t = (P'(x_1)^{-1})dt$ de sorte que t est aussi un paramètre à l'infini sur X. Donnons quelques formules

$$\begin{aligned} \frac{dx}{2y} &= -\frac{x_1^{g-1}dx_1}{2t} \in \Omega^1_V, \\ x &= x_1^{-1} = \frac{1}{t^2}R_1(x_1), \\ R_1(x_1) &= x_1^{2g+1}P(x). \end{aligned} \tag{4}$$

Commençons par calculer les sections globales de Ω^1_X, $\Omega^1_X(2g\infty)$ et préciser l'action de l'involution hyperelliptique ι sur ces modules.

3.2 Calculs de sections globales

Proposition 3.2.1. *Le W-module $H^0(X,\Omega^1_X)$ est libre de rang g de base*

$$\omega_i = \frac{x^i dx}{y} = -\frac{x_1^{g-1-i}dx_1}{t},\ 0 \le i \le g-1.$$

Sur un corps, cela résulte de 7.4.26 de [Liu02]. D'après 6.4.14 de [Liu02], le faisceau Ω^1_U (resp. Ω^1_V) est libre, engendré par ω_0 (resp. ω_{g-1}) de sorte que les éléments considérés sont clairement des éléments linéairement indépendants de $H^0(X,\Omega^1_X)$. Soit maintenant M le sous-module des sections globales engendré par les ω_i pour $0 \le i \le g-1$, qui est a priori un réseau de $H^0(X,\Omega^1_X)$. Alors $\Omega^1_X(U)/M$ est libre sur W, de base les $x^j\omega_0$ pour $j \ge g$ et les $x^j y\omega_0$ pour $j \ge 0$, si bien que $M = H^0(X,\Omega^1_X)$ d'après le lemme 2.3.

En particulier, ι agit par $-Id$ sur les sections globales de Ω^1_X. On en déduit le

Corollaire 3.2.2. *L'involution ι agit par $-Id$ sur $H^1_{DR}(X)$.*

Démonstration. D'après la dégénérescence de la suite spectrale de Hodge vers de Rham, on a une suite exacte courte $0 \to H^0(X, \Omega^1_X) \to H^1_{DR}(X) \to H^1(X, \mathcal{O}_X) \to 0$. Nous venons de voir que ι agit par $-Id$ sur $H^0(X, \Omega^1_X)$. Le module $H^1(X, \mathcal{O}_X)$ est le dual de Poincaré de $H^0(X, \Omega^1_X)$ et donc ι agit aussi par $-Id$ sur ce module. Il s'ensuit que ι agit par $-Id$ sur $H^1_{DR}(X)$. □

Proposition 3.2.3. *(i) Soit $n \in \mathbf{N}$ tel que $n \geq 2g-1$, le W-module $H^0(X, \mathcal{O}_X(n\infty))$ est libre de base les x^i pour $i \in \{0, \ldots, [n/2]\}$ et les yx^i pour $i \in \{0, \ldots, [(n-1)/2] - g\}$.*

(ii) En particulier, le W-module $H^0(X, \mathcal{O}_X((2g-1)\infty))$ est libre de base les x^i pour $i \in \{0, \ldots, g-1\}$ et

$$H^0(X, \mathcal{O}_X((2g-1)\infty)^- = 0.$$

Démonstration. Comme le faisceau $\mathcal{O}_X(n\infty)$ est localement libre, le module $H^0(X, \mathcal{O}_X((2g-1)\infty))$ est un W-module libre. Pour $n \geq 2g-1$, la formule de Riemann Roch donne qu'il est de rang $n+1-g = [n/2]+1+[(n-1)/2]-g+1$, qui est le nombre d'éléments considérés. Ces éléments sont bien des sections globales de $H^0(X, \mathcal{O}_X(n\infty))$ puisque, en vertu de 4,

$$\begin{cases} \text{si } 0 \leq i \leq \left[\frac{n}{2}\right], \ x^i = \frac{R_1(x_1)^i}{t^{2i}} \\ \text{si } 0 \leq i \leq \left[\frac{n}{2}\right] - g - 1, \ x^i y = \frac{R_1(x_1)^{g+1+i}}{t^{2(i+g)+1}}. \end{cases}$$

Notons alors M le sous W-module de $H^0(X, \mathcal{O}_X(n\infty))$ engendré par ces sections. Comme $\mathcal{O}_X(U)/M$ est un W-module libre, on voit grâce à 2.3, que $M = H^0(X, \mathcal{O}_X(n\infty))$. L'assertion (ii) n'est qu'un cas particulier de (i). □

Nous en déduisons le corollaire.

Corollaire 3.2.4.

$$\forall 0 \leq i \leq g-2, \ x^i dx \in \Gamma(X, \Omega^1_X(2g\infty))^+.$$

Démonstration. En dérivant les sections globales de $\mathcal{O}_X((2g-1)\infty)$, on trouve des sections globales de $\Omega^1_X(2g\infty)$, lesquelles sont invariantes sous l'action de l'involution ι. De plus, en appliquant le lemme 2.3, on voit que si $ix^{i-1}dx \in \Gamma(X, \Omega^1_X(2g\infty))$, alors $x^{i-1}dx \in \Gamma(X, \Omega^1_X(2g\infty))$. □

Remarque. Au passage, on constate que si la suite spectrale associée au complexe filtré $C(2g\infty)$ ne dégénère pas, la suite spectrale obtenue à partir de celle-ci après application de $\iota = -Id$ dégénère car $car(k) \neq 2$. L'aboutissement de cette suite spectrale est la partie de $R\Gamma(X, C(2g\infty))$ sur laquelle ι agit par $-Id$.

Proposition 3.2.5. *Le W-module $H^0(X, \Omega^1_X(2g\infty))^-$ est libre de rang $2g$ de base*

$$\omega_i = \frac{x^i dx}{y} = -x_1^{2g-1-i} R_1(x_1)^g \frac{1}{t^{2g}} \frac{dx_1}{t}, \ 0 \leq i \leq 2g-1.$$

Démonstration. Les éléments considérés sont clairement des sections globales de $\Omega^1_X(2g\infty))$, qui est un W-module sans torsion, puisque le faisceau $\Omega^1_X(2g\infty))$ est localement libre de rang 1. Calculons le rang de ce module. En passant à la suite exacte longue de cohomologie de la suite exacte courte

$$0 \to \Omega^1_X \to \Omega^1_X(2g\infty) \to t^{-2g}\mathcal{O}_{X,\infty}dt \,/\mathcal{O}_{X,\infty}dt \to 0,$$

et en appliquant le foncteur exact $\iota = -Id$, on trouve la suite exacte

$$0 \to H^0(X,\Omega^1_X) \to H^0(X,\Omega^1_X(2g\infty))^- \xrightarrow{v} \left(\bigoplus_{j=1}^{2g} W\, t^{-j}dt\right)^- \to H^1(X,\Omega^1_X)^-. \tag{5}$$

Le terme $H^1(X,\Omega^1_X)$ est dual de $H^0(X,\mathcal{O}_X) = W$ et donc ι agit trivialement sur ce module si bien que le dernier terme de la suite est nul. Le troisième terme de cette suite exacte est $\bigoplus_{i=1}^{g} W.t^{-2i}dt$ puisque $\iota(dt) = -dt$. Le rang cherché est donc $2g$.

Notons M le sous-module engendré par les éléments ω_i, ce module est de rang $2g$ car les ω_i sont linéairement indépendants sur W dans $\Omega^1_X(U)$. Le même raisonnement que précédemment montre que $M = H^0(X,\Omega^1_X(2g\infty))$ et finalement que le rang de $H^0(X,\Omega^1_X(2g\infty))$ est $2g$. □

Remarquons que $v(\omega_i) = 0$ si $0 \le i \le g-1$.

Dans tous les cas portant sur la caractéristique de k, le module $M = H^0(X,\Omega^1_X(2g\infty))$ est libre de rang $3g-1$ par le théorème de Riemann-Roch et l'énoncé qui suit se démontre exactement de la même façon que le précédent.

Proposition 3.2.6. *Si $g \ge 2$*

$$H^0(X,\Omega^1_X(2g\infty)) = \bigoplus_{i=0}^{2g-1} W \cdot \frac{x^i dx}{y} \bigoplus \bigoplus_{i=0}^{g-2} W \cdot x^i dx.$$

Pour une courbe elliptique, seul le premier terme apparaît. On remarquera que les éléments $x^i dx$ sont invariants par l'involution hyperelliptique ι.

3.3 Calcul explicite de la cohomologie de de Rham des courbes hyperelliptiques

3.3.1 Calcul du passage au complété de l'anneau local en l'infini

Décrivons d'abord explicitement l'homomorphisme d'anneaux locaux

$$\mathcal{O}_{X\infty} \to W[[t]].$$

Notons $C = \mathcal{O}_{X\infty}$ l'anneau local en ∞ de la courbe X, de sorte que

$$C = \left[W[x_1,t]\,/t^2 - x_1R_1(x_1)\right]_{(pW[x_1,t]+tW[x_1,t])},$$

c'est-à-dire que C est obtenu en localisant l'algèbre $W[x_1,t]/t^2 - x_1R_1(x_1)$ par l'idéal maximal engendré par t et p. Le complété de $\widehat{C}$ pour la topologie t-adique est isomorphe à $W[[t]]$ via une application $\mu : W[[t]] \to \widehat{C}$. On note λ l'application $C \to W[[t]]$ qui s'obtient comme $\mu^{-1} \circ Can$ où Can est l'application canonique $C \to \widehat{C}$, et par abus de notation on continue de noter x_1 l'élément $\lambda(x_1)$. Cherchons x_1 sous la forme $x_1(t) = t^2U(t)$ avec $U(t) = \sum_i q_i t^i \in W[[t]]$. L'élément U doit vérifier l'équation

$$(F) \quad t^2 = (t^2U(t))\left[R_1(t^2U(t))\right],$$

c'est-à-dire $1 = U(t)R_1(t^2U(t))$. Notons $f(X) = X(R_1(t^2X)) - 1 \in W[[t]][X]$, l'image de f dans le corps résiduel k de $W[[t]]$ est $R_1(0)X - 1 = X - 1$ dont 1 est une racine simple de sorte qu'on peut appliquer le lemme de Hensel et voir qu'il existe un unique $U(t)$ de W[[t]] (inversible) satisfaisant $f(U(t)) = 0$, et donc aussi un unique $x_1(t) = t^2U(t) \in W[[t]]$ vérifiant l'équation (F).

Remarquons de plus que $P_1'(x_1) \in 1 + tW[[t]]$ est inversible dans $W[[t]]$, dont l'inverse sera noté $V(t)$. On a alors

$$\frac{dx_1}{2t} = \frac{dt}{P_1'(x_1)},$$

soit encore

$$\frac{dx_1}{2t} = V(t)dt.$$

Avec ces notations, du fait que $R_1(x_1) = U(t)^{-1}$ on voit que dans $\widehat{\Omega}^1_{X,\infty} = W[[t]] \otimes \widehat{\Omega}^1_{X,\infty}$, on a l'égalité, en reprenant les notations de 3.2.5

$$\omega_i = -2t^{2(g-1-i)}U(t)^{g-1-i}V(t)dt.$$

Notons

$$\forall\, 0 \leq i \leq g-1,\ 2U(t)^{-1-i}V(t) \quad = \quad 2 + \sum_l u_{i,l}t^l,\ u_{i,l} \in W. \tag{6}$$

Alors, nous calculons $v(\omega_{g+i})$ où v est l'application définie en 5 :

$$\begin{aligned}
\forall\, 0 \leq i \leq g-1,\ v(\omega_{g+i}) &= -t^{-2(1+i)}\left(2 + \sum_{l=1}^{2i+1} u_{i,2l}t^{2l}\right)dt, \\
v(\omega_{g+i}) &= -2t^{-2(i+1)}dt - \sum_{l=1}^{i} u_{i,2l}t^{2(l-i-1)}dt, \\
&= -2t^{-2(i+1)}dt - \sum_{l=i}^{1} u_{i,2(i+1-l)}t^{-2l}dt
\end{aligned}$$

puisque les $v(\omega_{g+i})$ sont anti-invariants pour ι et que $\iota(t) = -t$. Pour terminer nous avons besoin du corollaire suivant.

Corollaire 3.3.1.1. *(Bogaart-Edixhoven, [vdB08],[Edi03]) On a une suite exacte courte*

$$(E) \quad 0 \to H^1_{DR}(X) \to H^0(X, \Omega^1_X(2g\infty))^- \xrightarrow{v'} \bigoplus_{j=1}^{g} (W/(2j-1)W)\ t^{-2j}dt \to 0.$$

Démonstration. Reprenons le triangle (3) de 2 avec D correspondant à la section à l'infini, et $n = 2g-1$. On trouve le complexe exact

$$0 \to H^0_{DR}(X) \to R^0\Gamma(X, C(2g\infty)) \to 0 \to H^1_{DR}(X) \to R^1\Gamma(X, C(2g\infty)) \\ \to coker(d) \to H^2_{DR}(X) \to 0. \quad (7)$$

Appliquons maintenant $\iota = -Id$ à ce complexe. Par dégénerescence de la suite spectrale de Hodge vers de Rham, $H^2_{DR}(X)$ s'identifie à $H^1(X, \Omega^1_X) = W$ sur lequel ι agit trivialement et donc $H^2_{DR}(X)^-$ est nul, tout comme $H^0_{DR}(X)^-$.

Le complexe $R\Gamma(X, C(2g\infty))$ est le complexe (2.2)

$$H^0(X, \mathcal{O}_X(2g-1)\infty) \xrightarrow{d} H^0(X, \Omega^1_X(2g\infty)),$$

de sorte que $R^1\Gamma(X, C(2g\infty))^-$ se réduit à $H^0(X, \Omega^1_X(2g\infty))^-$ d'après 3.2.3.

Il reste à calculer $coker(d)^-$. Le conoyau $coker(d)$ est $\left(\bigoplus_{j=1}^{2g} W/(j-1)W\, t^{-j}dt\right)$.

En passant à la partie $-$ de ce module, seuls subsistent les termes correspondant à j pair, d'où l'énoncé. □

Reprenons les notations de 6.

Dans les bases $(\omega_0, \ldots, \omega_{2g-1})$ et $t^{-2l}dt$ pour $1 \leq l \leq g$, la matrice de l'application v (5) qui est dans $M_{g,2g}(W)$ la suivante. Notons $V = (v_{2l,i})$ avec $v_{2l,i} \in W$, avec $i \in \{0, \ldots, 2g-1\}$, $l \in \{1, \ldots, g\}$ cette matrice. Les coefficients sont

$$\begin{aligned} \forall i \leq g-1,\ \forall l,\ v_{2l,i} &= 0 \\ \forall 0 \leq i \leq g-1,\ v_{2(i+1),g+i} &= -2 \\ \forall 0 \leq i \leq g-1,\ \forall l \leq i,\ v_{2l,g+i} &= -u_{i,2(i+1-l)} \\ \forall 0 \leq i \leq g-1,\ \forall l \geq i+1,\ v_{2l,g+i} &= 0. \end{aligned}$$

La matrice V est donc

$$V = \begin{pmatrix} 0 & \cdots & 0 & -2 & -u_{1,2} & -u_{2,4} & \cdots & -u_{g-1,4g-1} \\ 0 & \cdots & 0 & 0 & -2 & -u_{2,2} & \cdots & -u_{g-1,4g-3} \\ \vdots & & \vdots & 0 & 0 & -2 & & \vdots \\ \vdots & & \vdots & \vdots & \vdots & \ddots & & -u_{g-1,2} \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & -2 \end{pmatrix}$$

et l'application v' s'obtient à partir de v par passage au quotient via la surjection canonique

$$\bigoplus_{i=0}^{g-1} Wt^{-2(i+1)}dt \twoheadrightarrow \bigoplus_{i=0}^{g-1} W/(2i+1)Wt^{-2(i+1)}dt.$$

On voit donc que v induit une bijection notée $\overline{v}$

$$\bigoplus_{l=1}^{g} Wt^{-2l} \simeq \bigoplus_{i=0}^{g-1} Wt^{-2(i+1)}dt,$$

dont la matrice sera notée $\overline{V}$, et qui est triangulaire supérieure dans les bases choisies. Un élément $\omega \in \bigoplus_{i=0}^{g-1} Wt^{-2(i+1)}dt$ est dans $Ker(v')$ si et seulement si $\omega \in \overline{v}^{-1}(Ker(s))$. Or on a l'identification

$$Ker(s) = \bigoplus_{i=0}^{g-1}(2i+1)Wt^{-2(i+1)}dt.$$

Pour $i \in \{0, \ldots, g-1\}$, définissons

$$\omega'_{g+i} = \overline{V}^{-1} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ (2i+1)t^{-2(i+1)}dt \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in (2i+1)\omega_{g+i} \bigoplus_{l \leq i} W\omega_{g+l}.$$

Nous avons alors la

Proposition 3.3.2. *Le W-module $H^1_{DR}(X)$ est libre de rang $2g$ de base des éléments*

$$\begin{array}{ll} \dfrac{x^i dx}{y} & pour\, 0 \leq i \leq g-1, \\ \omega'_{g+i} & pour\, 0 \leq i \leq g-1. \end{array}$$

Si $p > 2g-1$ le terme de droite de la suite exacte 3.3.1.1 est nul, ce qui donne l'énoncé suivant.

Corollaire 3.3.3. *Si $p > 2g-1$ on a un isomorphisme*

$$H^1_{DR}(X) \simeq H^0(X, \Omega^1_X(2\infty))^-.$$

En particulier, si X est une courbe elliptique, on a toujours cet isomorphisme.

4 Action du Frobenius et (φ, Γ)-module associé

4.1 Action du Frobenius

Rappelons qu'un φ-module filtré sur W est la donnée d'un W-module muni d'un endomorphisme φ semi-linéaire par rapport au Frobenius de W et d'une filtration par des sous-W-modules, décroisssante, exhaustive et séparée.

La cohomologie de De Rham $H^1_{DR}(X)$ d'une courbe X projective et lisse de genre g est un W-module libre de rang $2g$, muni de la filtration de Hodge :

$$\begin{aligned} \mathrm{Fil}^r H^1_{DR}(X) &= H^1_{DR}(X) && \text{pour } r \leq 0, \\ &= H^0(X, \Omega^1_X) && \text{pour } r = 1, \\ &= 0 && \text{pour } r \geq 2. \end{aligned}$$

De plus, la cohomologie de De Rham de X s'identifie à la cohomologie cristalline $H^1_{cris}(X_k)$ de X_k [Ber74] ; elle est donc munie d'un endomorphisme de Frobenius, induit par l'action du Frobenius sur X_k. On obtient ainsi un φ-module filtré.

Lorsque les W-modules $H^p(X, \Omega^q_X)$ sont des W-modules libres et que la suite spectrale associée dégénère (Proposition 2.1 pour une courbe hyperelliptique), on sait, par une application d'un théorème de Mazur [Maz73] et [Fon83], que le φ-module filtré $H^1_{DR}(X)$ est un réseau fortement divisible de $H^1_{DR}(X_K)$: pour tout entier r, chaque $\mathrm{Fil}^r H^1_{DR}(X)$ est un facteur direct de $H^1_{DR}(X)$, on a

$$\varphi(\mathrm{Fil}^r H^1_{DR}(X)) \in p^r H^1_{DR}(X)$$

et

$$\sum_{r \in \mathbf{Z}} \frac{1}{p^r} \varphi(\mathrm{Fil}^r H^1_{DR}(X)) = H^1_{DR}(X).$$

Considérons $(e_i)_{1 \leq i \leq 2g}$ une base de $H^1_{DR}(X)$ adaptée à la filtration [Wac97] ; soit r_i le plus grand entier tel que $e_i \in \mathrm{Fil}^{r_i} H^1_{DR}(X)$ et pour tout entier $r \geq 0$, posons $\varphi_r = \frac{1}{p^r} \varphi_{|\mathrm{Fil}^r}$. On a ainsi, pour $1 \leq i \leq 2g$, si

$$e_i \in \mathrm{Fil}^1 H^1_{DR}(X), \quad r_i = 1, \quad \text{et} \quad \varphi_1(e_i) = \frac{1}{p} \varphi(e_i)$$

et, sinon,

$$r_i = 0 \quad \text{et} \quad \varphi_0(e_i) = \varphi(e_i).$$

Ecrivons, pour $1 \leq j \leq 2g$,

$$\varphi_{r_j}(e_j) = \sum_{i=1}^{2g} a_{ij} e_i$$

l'expression de $\varphi_{r_j}(e_j)$ dans la base (e_i). Le φ-module filtré $H^1_{DR}(X)$ étant fortement divisible, les applications φ_r sont bien définies, et la matrice $A = (a_{ij})$ est une matrice à coefficients dans W, qui est inversible ([Wac97], 2.2.2).

4.2 (φ, Γ)-module associé

Considérons la $\mathbf{Z}_p$-extension cyclotomique K_∞ de K contenue dans $\bar{K}$, notons Γ le groupe de Galois de K_∞ / K, qui est isomorphe à $\mathbf{Z}_p$, et choisissons-en un générateur topologique, noté γ. On munit l'anneau $S = W[[T]]$ d'une action de Γ telle que $\gamma(T) - T = \alpha(p + T)T$, où α est une unité de S, qui est congrue à une unité de $\mathbf{Z}_p$ modulo T et à 1 modulo (p, T). Dans ces conditions, il existe une unique action de Frobenius, notée φ, commutant à l'action de Γ,

compatible avec le Frobenius sur W, qui relève l'élévation à la puissance p modulo p et telle que $\varphi(T) = u(p+T)^{p-1}T$, où $u \equiv 1$ modulo pS (pour un exposé détaillé des propriétés de S, voir [Fon90], 3.2, [Fon94], ou [Wac97], 3.1.1.).

Pour une courbe projective et lisse X vérifiant les hypothèses du théorème de Mazur [Maz73], on définit sur le module $N = S \otimes_W H^1_{DR}(X)$ une action de φ par

$$\varphi(1 \otimes e_j) = (p+T)^{r_j} \sum_{i=1}^{2g} a_{ij}(1 \otimes e_i),$$

l'action de Γ étant induite par la proposition suivante (cf [Wac97], 3.1.4, théorème 3) :

Proposition 4.2.1. *Il existe sur N une unique action de Γ commutant à φ et triviale modulo T.*

Démonstration. Nous reproduisons ici la démonstration de *op.cit*, adaptée au cas particulier d'une courbe.

Il suffit de connaître la matrice du générateur γ dans la base $(1 \otimes e_i)_{1 \leq i \leq 2g}$, notée simplement $(e_i)_{1 \leq i \leq 2g}$; la démonstration se fait par dévissages modulo T et modulo p en déformant la matrice de l'identité I_{2g}, qui induit sur N une action de γ triviale modulo T, mais ne commutant pas à φ a priori. Notons ρ cette action :

$$\begin{aligned} \rho(\varphi(e_j)) - \varphi(\rho(e_j)) &= (\gamma(p+T)^{r_j} - (p+T)^{r_j}) \textstyle\sum_{i=1}^{2g} a_{ij} e_i \\ &= (p+T)^{r_j} \alpha_j T \textstyle\sum_{i=1}^{2g} a_{ij} e_i \end{aligned}$$

si α_j est l'unique élément de S tel que

$$\gamma(p+T)^{r_j} = (p+T)^{r_j}(1 + T\alpha_j) \quad .$$

Comme S est complet pour la topologie T-adique, il suffit de vérifier le lemme suivant :

Lemme 4.2.2. *Soient $l \in \mathbf{N}$ et ρ un endomorphisme de N, semi-linéaire par rapport à l'action de γ sur S tel que $\rho(e_j) \equiv e_j \mod T$ et*

$$\rho(\varphi(e_j)) \equiv \varphi(\rho(e_j)) \mod T^l(p+T)^{r_j} N$$

pour tout j ; alors, il existe un endomorphisme ρ' de N, uniquement déterminé modulo T^{l+1}, semi-linéaire par rapport à l'action de γ sur S tel que, pour tout j :

$$\begin{aligned} &\rho'(e_j) \equiv \rho(e_j) \mod T^l N \\ \textit{et} \quad &\rho'(\varphi(e_j)) \equiv \varphi(\rho'(e_j)) \mod T^{l+1}(p+T)^{r_j} N \quad . \end{aligned}$$

Démontrons la proposition. On pose, pour tout j, $1 \leq j \leq 2g$:

$$\rho(\varphi(e_j)) - \varphi(\rho(e_j)) = T^l(p+T)^{r_j} b_j$$

où b_j est un élément de N et on cherche la matrice G' de ρ' dans la base (e_i) sous la forme $G' = G + T^l X$ où G est la matrice de ρ et X une matrice à coefficients dans W.

Rappelons que $\varphi(T) = uT(p+T)^{p-1}$ avec u une unité de S ; alors,

$$\begin{aligned}\rho'(\varphi(e_j)) &= \rho'((p+T)^{r_j}\textstyle\sum_{i=1}^{2g} a_{ij}e_i)\\ &= \rho(\varphi(e_j)) + (p+T)^{r_j}(1+T\alpha_j)T^l\textstyle\sum_{1\le i,k\le 2g} a_{kj}x_{ik}e_i\end{aligned}$$

et

$$\begin{aligned}\varphi(\rho'(e_j)) &= \varphi(\rho(e_j)) + \varphi(T^l)\textstyle\sum_{i=1}^{2g}\varphi(x_{ij})\varphi(e_i)\\ &= \varphi(\rho(e_j)) + T^l(p+T)^{l(p-1)}u^l\textstyle\sum_{1\le i,k\le 2g}\varphi(x_{kj})(p+T)^{r_k}a_{ik}e_i \quad .\end{aligned}$$

On obtient une équation matricielle à résoudre

$$(*) \qquad B = u^l A' X'_\varphi - XA,$$

où B est la matrice modulo T du système (b_j) dans la base (e_i), $A' = (p^{r_j}a_{ij})$ et $X'_\varphi = (p^{l(p-1)-r_j}\varphi(x_{ij}))$.

Ces matrices sont toutes à coefficients dans W, qui est complet pour la topologie p-adique ; on commence par résoudre ce système modulo p.

Dans notre cas, $r_j = 0$ ou 1, donc pour $p > 2$, on a $l(p-1) - r_j > 0$ et l'équation devient :

$$B \equiv -XA \mod p$$

et on conclut en utilisant le fait que la matrice A est inversible.

Notons X_m une solution de $B = u^l A' X'_\varphi - XA$ modulo p^m et $p^m B_m = B - u^l A' X'_{m,\varphi} + X_m A$. Relevons X_m en $X_{m+1} = X_m + p^m Y_m$ solution modulo p^{m+1}. L'équation vérifiée par Y_m est à nouveau $B_m = -Y_m A$ modulo p, qui se résout en inversant la matrice A. □

4.3 Complexité

La démonstration ci-dessus fournit un algorithme permettant d'obtenir l'action de Γ à une précision modulo p^i et modulo T^j souhaitée.

Rappelons que calculer le produit de deux matrices carrées de taille l ou l'inverse d'une matrice à coefficients dans un anneau nécesite un nombre d'opérations dans l'anneau d'au plus $O(l^\omega)$, où ω est le plus petit exposant connu pour la multiplication des matrices ([BCS97] chapitres 15-16 ou [CW90]). Chaque multiplication dans k, de cardinal p^n, se fait en $O((\log p)^{1+\varepsilon}n^{1+\varepsilon})$ opérations. La matrice A modulo p, dont il faut calculer l'inverse, est élément de $\mathcal{M}_{2g}(k)$, d'où une complexité de $O((\log p)^{1+\varepsilon}n^{1+\varepsilon}g^\omega)$ pour ce calcul.

Pour effectuer la $m^{\text{ième}}$ étape du dévissage modulo p, il faut d'abord calculer la matrice B_m. On commence par choisir un relèvement modulo p^{m+1} de X_m, que l'on note encore X_m ; il s'agit alors de calculer la matrice $X'_{m,\varphi}$ modulo p^{m+1}, ce qui se fait en $O((\log p)^{2+\varepsilon}n^{1+\varepsilon}g^2m^{1+\varepsilon})$ opérations ([Hub10], pour la complexité du calcul de φ). Puis $B - u^l A' X'_{m,\varphi} + X_m A$ s'obtient comme deux produits et sommes de matrices modulo p^m, calcul de complexité totale de l'ordre de $O\big(((\log p)^{2+\varepsilon}g^2 + (\log p)^{1+\varepsilon}g^\omega)n^{1+\varepsilon}m^{1+\varepsilon}\big)$.

Cette étape se répétant pour m variant entre 1 et i, la complexité totale du dévissage modulo p est $O\big(((\log p)^{2+\varepsilon}g^2 + (\log p)^{1+\varepsilon}g^\omega)n^{1+\varepsilon}i^{2+\varepsilon}\big)$.

Calculons à présent la complexité du dévissage modulo T : à chaque étape, on effectue un dévissage modulo p, de complexité calculée ci-dessus. Il faut aussi calculer la matrice B, qui repose sur le calcul de $X'_{i,\varphi}$, effectué lors du dévissage modulo p. Puisqu'il y a j étapes, la complexité totale de l'algorithme pour déterminer la matrice de Γ modulo p^i et T^j est donc au plus

$$O\big(((\log p)^{2+\varepsilon} g^2 + (\log p)^{1+\varepsilon} g^{\omega}) n^{1+\varepsilon} i^{2+\varepsilon} j\big).$$

5 Application au cas des courbes hyperelliptiques

Dans cette partie, X est une courbe hyperelliptique et nous reprenons les notations de 3. La méthode générale précedente 4 met en jeu le calcul du Frobenius divisé sur la cohomologie de De Rham de X. Nous allons donner dans la suite un algorithme pour calculer le (φ, Γ)-module mod p^i associé à $H^1_{et}(X_{\overline{K}}, \mathbf{Q}_p)$ basé sur l'algorithme de Kedlaya pour calculer la fonction zêta de X_0. Dans notre article [HW13], nous donnerons une autre méthode, basée sur le morphisme de Deligne-Illusie pour calculer ce (φ, Γ)-module modulo p.

5.1 Calcul du (φ, Γ)-module associé aux courbes hyperelliptiques via l'algorithme de Kedlaya

La base $((\frac{x^i dx}{y})_{0 \leq i \leq g-1}, (\omega'_i)_{g \leq i \leq 2g-1})$ présentée dans le corollaire 3.3.2 est une base adaptée à la filtration. Notons $e_i = \frac{x^{i-1} dx}{y}$ (respectivement $e_i = \omega'_{i-1}$) pour $1 \leq i \leq g$ (respectivement pour $g+1 \leq i \leq 2g$) les éléments de cette base. On a bien, pour $1 \leq i \leq g$,

$$e_i \in \mathrm{Fil}^1 H^1_{DR}(X) \quad \text{et} \quad \varphi_1(e_i) = \frac{1}{p}\varphi(e_i)$$

et, pour $g+1 \leq i \leq 2g$,

$$e_i \in \mathrm{Fil}^0 H^1_{DR}(X), \quad r_i = 0 \quad \text{et} \quad \varphi_0(e_i) = \varphi(e_i).$$

Notons $X' = \operatorname{Spec} A'$ la courbe obtenue en enlevant les points de ramification du revêtement $h : X \to \mathbf{P}^1_W$ et X'_k sa fibre spéciale. Kedlaya [Ked01] décrit un algorithme qui permet de calculer l'action du Frobenius sur la cohomologie rigide à coefficients dans K de la courbe X'_k. Cette cohomologie s'identifie à la cohomologie de de Rham (cf [BC94]) de X'_K et le K-espace vectoriel $H^1_{DR}(X'_K)$ se trouve ainsi muni d'une action de Frobenius. L'inclusion $X' \hookrightarrow X$ induit des applications $H^1_{DR}(X) \to H^1_{DR}(X')$ et $H^1_{DR}(X_K) \to H^1_{DR}(X'_K)$ qui sont injectives et équivariantes par l'action de Frobenius (cf [vdB08]). Nous pouvons donc utiliser cet algorithme pour calculer la matrice de φ et, après changement de base dans la base formée des vecteurs (e_i), en déduire la matrice A.

Cette matrice est la donnée de l'algorithme décrit en 4.2 et nous pouvons donc en déduire la matrice de Γ à une précision modulo p^i et modulo T^j arbitraire.

5.2 Estimations de la complexité de l'algorithme

Nos résultats sont résumés par la

Proposition 5.2.1. *Sous les hypothèses de 3. Notons n le degré de l'extension k sur $\mathbf{F}_p$, et ω l'exposant de la multiplication des matrices*

i La complexité du calcul du (φ, Γ)-module associé à $H^1_{DR}(X_K)$ mod (p^i, T^j) est inférieure à $O(p^{1+\varepsilon} n^{1+\varepsilon} g^\omega i^{2+\varepsilon} j)$.

ii Lorsque $i = 1$, la complexité du calcul du (φ, Γ)-module associé à $H^1_{DR}(X_K)$ mod (p, T^j) est inférieure à $O(p^{1+\varepsilon} n^{1+\varepsilon} g^\omega j)$.

Rappelons que la complexité de l'algorithme permettant d'obtenir l'action de Γ a été évaluée comme au plus

$$O\big(((\log p)^{2+\varepsilon} g^2 + (\log p)^{1+\varepsilon} g^\omega) n^{1+\varepsilon} i^{2+\varepsilon} j\big).$$

Il convient de rajouter la complexité de l'algorithme permettant de calculer la matrice A modulo p^i, à savoir $O(p^{1+\varepsilon} n^{1+\varepsilon} g^{2+\varepsilon} i^{2+\varepsilon})$ pour déterminer la matrice du Frobenius modulo p^{i+1} via l'algorithme de Kedlaya (cf [Ked01]).

Une fois la matrice trouvée, il faut effectuer encore un changement de base pour déterminer la matrice A dans une base du réseau $H^1_{DR}(X)$. La matrice du changement de base se déduit des calculs de 3.3.1 : les vecteurs de la base appartenant à $H^0(X, \Omega^1_X)$ sont simplement multipliés par 2, en revanche les autres vecteurs de la base adaptée à la filtration sont des combinaisons linéaires de tous les vecteurs de la base utilisée par Kedlaya. L'opération de changement de base revient alors à multiplier des matrices carrées de taille g à coefficients modulo p^i ; il n'a finalement pas d'influence sur la complexité.

La complexité totale est majorée par

$$O(p^{1+\varepsilon} n^{1+\varepsilon} g^\omega i^{2+\varepsilon} j).$$

Pour le calcul du (φ, Γ)-module modulo (p, T^j), il suffit de considérer $i = 2$ dans la complexité ci-dessus.

Références

[AKR10] Timothy G. Abbott, Kiran S. Kedlaya, and David Roe. Bounding Picard numbers of surfaces using p-adic cohomology. In *Arithmetics, geometry, and coding theory (AGCT 2005)*, volume 21 of *Sémin. Congr.*, pages 125–159. Soc. Math. France, Paris, 2010.

[BC94] Francesco Baldassarri and Bruno Chiarellotto. Algebraic versus rigid cohomology with logarithmic coefficients. In *Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991)*, volume 15 of *Perspect. Math.*, pages 11–50. Academic Press, San Diego, CA, 1994.

[Ber74] Pierre Berthelot. *Cohomologie cristalline des schémas de caractéristique $p > 0$*. Lecture Notes in Mathematics, Vol. 407. Springer-Verlag, Berlin, 1974.

[Bern08] Daniel J. Bernstein. *Fast multiplication and its applications*. In *Algorithmic number theory : lattices, number fields, curves and cryptography* volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 325–384. Cambridge Univ. Press, Cambridge, 2008

[Bou83] Nicolas. Bourbaki. *Éléments de mathématique. Algèbre commutative. Chapitres 8 et 9*. Masson, Paris, 1983.

[BCS97] Peter Bürgisser, Michael Clausen et M. Amin Shokrollahi, *Algebraic complexity theory*. Grundlehren der Mathematischen Wissenschaften, Vol. 315. Springer-Verlag, Berlin, 1997.

[CW90] Coppersmith, Don et Winograd, Shmuel. Matrix multiplication via arithmetic progressions. *Journal of Symbolic Computation*, 9(3) :251–280, 1990

[DI87] Pierre Deligne et Luc Illusie. Relèvements modulo p^2 et décomposition du complexe de de Rham. *Invent. Math.*, 89(2) :247–270, 1987.

[Edi03] Bas Edixhoven. Point counting after kedlaya. eidma-stieltjes graduate course, 2003.

[FM87] Jean-Marc Fontaine and William Messing. p-adic periods and p-adic étale cohomology. In *Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985)*, volume 67 of *Contemp. Math.*, pages 179–207. Amer. Math. Soc., Providence, RI, 1987.

[Fon83] Jean-Marc Fontaine. Cohomologie de de Rham, cohomologie cristalline et représentations p-adiques. In *Algebraic geometry (Tokyo/Kyoto, 1982)*, volume 1016 of *Lecture Notes in Math.*, pages 86–108. Springer, Berlin, 1983.

[Fon90] Jean-Marc Fontaine. Représentations p-adiques des corps locaux. I. In *The Grothendieck Festschrift, Vol. II*, volume 87 of *Progr. Math.*, pages 249–309. Birkhäuser Boston, Boston, MA, 1990.

[Fon94] Jean-Marc Fontaine. Le corps des périodes p-adiques. *Astérisque*, (223) :59–111, 1994. With an appendix by Pierre Colmez, Périodes p-adiques (Bures-sur-Yvette, 1988).

[Har66] Robin Hartshorne. *Residues and duality*. Lecture notes of a seminar on the work of A. Grothendieck, given at Harvard 1963/64. With an appendix by P. Deligne. Lecture Notes in Mathematics, No. 20. Springer-Verlag, Berlin, 1966.

[Hub10] Hendrik Hubrechts. Fast arithmetic in unramified p-adic fields. *Finite Fields and Their Applications*, 16 :155–162, 2010.

[HW13] Christine Huyghe et Nathalie Wach. Interprétation cristalline de l'isomorphisme de deligne-illusie (cas des courbes). *soumis pour publication*, pages 1–48, 2013.

[Kat73] Nicholas M. Katz. p-adic properties of modular schemes and modular forms. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 69–190. Lecture Notes in Mathematics, Vol. 350. Springer, Berlin, 1973.

[Ked01] Kiran S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16(4) :323–338, 2001.

[Lau06] Alan G. B. Lauder. A recursive method for computing zeta functions of varieties. *LMS J. Comput. Math.*, 9 :222–269, 2006.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, 2002.

[Maz73] Barry Mazur. Frobenius and the Hodge filtration (estimates). *Ann. of Math. (2)*, 98 :58–95, 1973.

[vdB08] Theo van den Bogaart. About the choice of a basis in Kedlaya's algorithm. *http ://arxiv.org/abs/math/0505178v3*, pages 1–19, 2008.

[Wac97] Nathalie Wach. Représentations cristallines de torsion. *Compositio Math.*, 108(2) :185–240, 1997.

Christine Huyghe et Nathalie Wach
IRMA
Université Louis Pasteur
7, rue René Descartes
67084 STRASBOURG cedex FRANCE
mél huyghe@math.unistra.fr, wach@math.unistra.fr, http ://www-irma.u-strasbg.fr/~huyghe, http ://www-irma.u-strasbg.fr/~wach