

Thèse

INSTITUT DE
RECHERCHE
MATHÉMATIQUE
AVANCÉE

UMR 7501

Strasbourg

présentée pour obtenir le grade de docteur de
l'Université de Strasbourg
Spécialité MATHÉMATIQUES

Amandine Pierrot

**Calcul du φ -module filtré associé à certains
revêtements de la droite projective**

Soutenue le 21 décembre 2017
devant la commission d'examen

Christine Huyghe, directrice de thèse
Nathalie Wach, codirectrice de thèse
Xavier Caruso, rapporteur
Bernard Le Stum, rapporteur
Laurent Berger, examinateur
Ariane Mézard, examinatrice
Rutger Noot, examinateur
Jean-Pierre Wintenberger, examinateur

www-irma.u-strasbg.fr



Calcul du φ -module filtré associé à certains revêtements de la droite projective

Amandine Pierrot

Institut de Recherche Mathématique Avancée
Université de Strasbourg
7 rue René Descartes
67084 Strasbourg Cedex

Thèse de doctorat sous la direction de
Christine Huyghe et Nathalie Wach

Remerciements

Il serait impensable de ne pas le faire mais c'est en toute sincérité que je tiens à remercier ma directrice de thèse Christine HUYGHE, sans qui ce manuscrit n'aurait jamais vu le jour. Des balbutiements de mon mémoire de M2 jusqu'au point final de cette thèse elle a su être présente pour répondre à toutes mes questions, à plusieurs reprises si nécessaire, en gardant toujours une grande patience. Elle a su instaurer pour moi un climat studieux sans qu'il soit trop pesant, sachant "lâcher du lest" quand la situation l'exigeait. Lorsque ma confiance vacillait, peut-être trop souvent, elle a su m'encourager, parfois avec douceur, si nécessaire avec fermeté, et m'a permis de me remettre en selle quand les obstacles me semblaient insurmontables. Tout n'a pas toujours été sans heurts mais le chemin parcouru en valait la peine. Merci beaucoup.

Il me faut également remercier ma co-directrice, Nathalie WACH, qui déjà à l'époque du M2 était venue à la rescousse pour m'aider à préparer ma soutenance de mémoire. Je la remercie pour ses explications sur ce sujet obscur que sont les phi-modules et pour sa patience lors de nos entrevues. Le dernier chapitre de cette thèse lui doit beaucoup et n'existerait sans doute pas sans ses lumières. Par ailleurs elle a la charge, sans doute un peu ingrate, de la répartition des enseignements. C'est un travail que je devine ardu mais nécessaire et pour lequel je tiens également à la remercier.

Je remercie chaleureusement Xavier CARUSO d'avoir accepté le travail de relecture de cette thèse. Ses remarques précises et pertinentes m'ont aidé à l'améliorer et je l'en remercie. Le calcul explicite de la matrice doit également beaucoup à son ingénieuse astuce d'inversion. Par ailleurs lui présenter mes résultats dans une période de doutes profonds et voir l'intérêt qu'il semblait leur accorder m'a aidé à retrouver la motivation nécessaire à l'achèvement de mes travaux quand ceux-ci me semblaient vains, je lui dois donc plus qu'il ne le pense.

Je remercie également Bernard LE STUM qui a lui aussi accepté la tâche ardue de relire ma prose, parfois désastreuse. Je lui dois les premiers retours sur ce manuscrit, et s'ils ont été rudes ils étaient nécessaires. Son exigence m'a forcée à faire un véritable travail de fond, améliorant grandement la clarté et la présentation de mes résultats. J'espère pouvoir comprendre un jour les règles obscures de la typographie... Quoi qu'il en soit merci.

Je remercie également Laurent BERGER, Ariane MEZARD, Rutger NOOT et Jean-Pierre WINTENBERGER de me faire l'honneur de participer à mon jury.

Je remercie l'école doctorale MSII ainsi que le personnel administratif et enseignant de l'IRMA et de l'UFR de mathématiques et d'informatique pour leur efficacité et leur disponibilité. Je pense en particulier à Fabienne GRAUSS (dont tous les copains de M2 se souviennent !) qui a été d'un grand secours à de nombreuses reprises durant ma scolarité à l'UFR. Il y a également Marie-Jeanne THEOLO avec qui j'ai toujours grand plaisir à échanger quand l'occasion se présente et Myriam PEPINO que je souhaite remercier pour la gentillesse et la disponibilité dont elle a fait preuve lorsque j'ai fait appel à ses services.

Lorsque j'ai commencé les "vraies" mathématiques j'ai eu la chance d'être aidée dans ma tâche par deux enseignants aux qualités très différentes. Ils ont contribué à développer mon goût pour cette science, l'envie de trouver les solutions par moi-même, et ils ont aussi cru en moi à une période où je n'y croyais pas forcément moi-même. Je souhaite donc tout naturellement remercier mes deux professeurs de mathématiques de classe préparatoire, Christiane "Cricri" VINCENT et Jean-Denis EIDEN.

Cela fait plus de sept ans déjà que je suis arrivée à l'université de Strasbourg, dont quatre consacrés à mes études avant de commencer cette thèse. Les enseignants que j'y ai croisé ont contribué à ma réussite mais mes pensées aujourd'hui vont tout particulièrement vers deux d'entre eux. Tout d'abord Claude MITSCHI qui était responsable du parcours "magistère de mathématiques" que j'ai eu la chance de pouvoir suivre mais aussi Adriano MARMORA. C'est avec lui que j'ai fait mes premiers pas dans la recherche, lorsqu'il a encadré mon mémoire de L3 sur le Pyraminx, puis dans le domaine de la géométrie algébrique, puisqu'il a également encadré mon mémoire de M2 agrégation. Il a été patient et disponible à ces deux occasions et c'est toujours un plaisir d'échanger avec lui lorsque l'occasion se présente. Toutes mes félicitations encore pour votre habilitation à diriger des recherches je suis sûre que vous ferez un super encadrant !

Bien sûr je ne peux pas écrire de remerciements de thèse sans glisser un mot pour mes camarades doctorants ! Une thèse c'est à la fois une grande aventure stimulante et exaltante mais c'est parfois aussi un long cauchemar sans fin. C'est pourquoi les personnes que l'on fréquente au jour le jour sont d'une importance capitale. A Strasbourg nous avons la chance incroyable d'avoir une équipe de doctorants importante mais à taille humaine, soudée et toujours prête à rendre service en cas de besoin. Citer tout le monde serait long, fastidieux et risqué (gare si l'on en oublie un !) alors je vais me permettre de tricher et de lancer un merci général pour la bonne ambiance et les bières. Toutefois je souhaite ajouter un petit mot pour certains d'entre eux. Que ceux qui ne voient pas leur nom ne s'offusquent pas, j'ai toujours trouvé un peu artificielle cette interminable liste de noms que d'autres ont mis avant moi. Merci à Amaury pour sa bonne humeur, Antoine pour les longues discussions et les plaisanteries, Arnaud pour les discussions sur les jeux vidéos, Florian l'homme des bois qui me fait toujours bien rire et son adorable Claire, Frédéric avec qui je ne suis jamais d'accord mais que j'adore quand même, grand Guillaume pour les échanges passionnés, Jérôme "the big boss" qui a eu le parcours professionnel dont on rêvait tous et Xing dont je n'arriverai sans doute jamais à prononcer le nom correctement mais avec qui je partage non seulement mon goût pour les mathématiques mais aussi pour la danse et le tir à l'arc.

Je remercie également Audrey, qui me supporte depuis le M2 et qui arrive pourtant toujours à faire preuve de patience à mon égard, nos discussions m'ont été aussi précieuses qu'à toi ! Elle a repris la tête de l'équipe doctorante avec efficacité et sa gentillesse nous a tous conquis. Et puis bien sûr je remercie Thomas, lui qui a toujours fait partie du paysage pendant ma scolarité à l'UFR. L'agrég', le M2, la thèse, on a survécu à tout ça tous les deux et mine de rien ça compte.

Evidemment parmi les doctorants il y a le top du top, ceux qui partagent notre bureau ! On passe tellement de temps avec eux qu'il vaut mieux que le courant passe. En ce qui me concerne j'ai eu une chance incroyable. Le bureau 116 n'a été occupé que par des gens géniaux (bon peut-être pas tous... ;p) et ce n'est pas sans émotion que je repense aux moments que j'y ai passés. Je commencerai par Marie, qui vient seulement d'arriver mais qui est toujours dispo quand il s'agit de m'écouter raconter mes bêtises ou mes galères. Ça fait plaisir d'avoir quelqu'un qui travaille "avec" moi. Il y aussi Pierre, qui a rejoint le meilleur des bureaux il y a un an, mais que je connaissais déjà avant. Il fait semblant d'être une grosse brute mais tout le monde sait que c'est parce qu'il a un petit coeur de guimauve. Merci pour les discussions sérieuses (et moins sérieuses) pour le soutien moral et technique. Enfin lorsque j'ai débarqué dans ce bureau il y avait déjà deux locataires, avec qui je l'ai partagé pendant deux ans. Stéphane, qui me faisait un peu peur au début, qui a fait un tellement bon boulot sur ses cours qu'on les utilise encore honteusement après son départ, et à qui je dois d'avoir commencé la danse (et on sait tous les deux que je te dois beaucoup pour ça) et Ranine. Ma petite Poupette, sans ton soutien et ton amitié cette période de ma vie n'aurait pas eu la même saveur et je remercie la bonne fée responsable de l'attribution des bureaux (Pascale IGOT) de m'avoir fait atterrir dans le tien. Il m'arrive parfois de penser avec nostalgie à ces deux années que nous avons passées dans ce bureau tous les trois. J'ai un petit pincement au cœur quand je pense qu'elles sont biens finies et que bientôt mon nom aussi disparaîtra du petit papier à l'entrée.

Je prends mon temps mais on sait tous que cette partie est la seule que liront la plupart de ceux qui auront ce manuscrit entre les mains. Mais ne vous inquiétez pas, la fin est proche ! Je veux encore remercier les copains. Ceux qui ne font pas ou plus d'études en mathématiques et dont la présence est tout aussi indispensable que celle des doctorants. Et peut-être même plus puisqu'ils nous permettent de nous changer les idées et nous évitent peut-être de sombrer dans la monomanie ! Alors en vrac merci à Dédé presque coloc' et soutien indéfectible lors des coups durs. Merci à Charlotte "mon âme sœur de pensée" pour tout et plus encore. Merci aux copains et copines de la danse et surtout Elli, Manon et Pauline, on sait ce que je vous dois. Merci p'tit Benoît et Renaud mes deux cavaliers préférés (à une exception hors concours près !). Merci Yannick grâce à qui j'ai survécu à la prépa et qui a lui aussi soutenu il y a quelques jours. Merci à Pauline qui même de l'autre bout du monde pense à prendre des nouvelles et merci à Lucie et son Jimmy. Ma plus ancienne amie, celle grâce à qui je dessine, je regarde des dramas et sans doute plein d'autres choses qui font que je suis moi.

Je remercie ma famille. Les cousins, les tatas, les tontons et les grands-parents. J'ai la chance d'avoir un entourage formidable avec qui j'aime passer du temps. Dont je peux sentir l'intérêt

et l'affection qu'ils me portent et pour lesquels je les remercie chaleureusement. Un grand merci à mon neveu Yannick mon petit rayon de soleil, à mon frère Alain et à sa femme qui bien qu'habitant loin font toujours l'effort de faire partie du groupe. Merci à ma grande sœur Adeline qui m'a en quelque sorte montré la voie sur le chemin de la thèse et qui bien avant déjà m'avait servi de phare dans l'obscurité. Elle m'a appris à lire, à compter et je lui dois bien plus encore que je ne saurais dire. C'est une chance incroyable de l'avoir à mes côtés. Je remercie également son mari et le petit Bubulle simplement parce que ce qui la rend heureuse contribue à mon bien-être. Je remercie du fond du cœur mes parents. Je leur dois ce que je suis, je leur dois le simple fait d'écrire ces lignes et je les remercie de m'avoir guidée, d'avoir su me donner leur avis et leurs conseils sans me les imposer. Tout n'a pas été toujours facile mais vous avoir à mes côtés m'a été d'un grand secours. Je vous aime.

Enfin je terminerais ces remerciement par un mot pour toi, mon petit bonheur. C'est incroyable de voir ce que la vie peut parfois nous offrir, même quand on n'y croit pas. Ta simple présence me remplit de joie et me donne envie de sourire. Merci pour ton soutien, ta confiance, ta tendresse et ton amour. Je t'aime.

Table des matières

Introduction	1
1 Préliminaires	7
2 Modèle à deux ouverts d'un revêtement de degré n de \mathbb{P}^1	9
2.1 Définition de la courbe X	9
2.2 Une action sur la courbe X	13
3 Etude de la courbe X	17
3.1 Conventions	17
3.2 Etude de la lissité	17
3.3 Etude de la ramification de X_K et X_k	18
3.4 Calcul du genre	19
4 Une base de $H^0(X, \Omega_X^1)$	21
4.1 Calcul de la base	21
4.2 Décomposition de $H^0(X, \Omega_X^1)$ en composantes isotypiques	24
5 Calcul d'une base de $H_{DR}^1(X)$	25
5.1 Dégénérescence de la suite spectrale	25
5.2 Calcul des sections globales de $H^0(X, \mathcal{O}_X((2g-1)\infty))$	25
5.3 Calcul des sections globales de $H^0(X, \Omega_X^1(2g\infty))$	28
5.4 Calcul de $H_{DR}^1(X)$	34
6 Un scindage adapté de la filtration de Hodge	41
7 Mise en place du calcul du Frobenius divisé de la fibre spéciale	47
7.1 Rappels sur le Frobenius	47
7.2 Relèvements du Frobenius modulo p^2	49
7.3 Calcul du morphisme de Deligne-Illusie	53
7.4 Calcul de la matrice du Frobenius divisé sur $H_{DR}^1(X_k)$	58
7.5 Calcul des classes d'éléments de $\mathcal{O}_{X_k}(\overline{U}_k \cap W_k)$	60

8	Calcul de la matrice du Frobenius divisé de la fibre spéciale	65
8.1	Présentation de la matrice	65
8.2	Calcul de la matrice de Hasse-Witt	68
8.3	Calcul du bloc supérieur droit	69
8.4	Calcul du bloc inférieur gauche	71
8.5	Calcul de la matrice de Cartier	73
8.6	Le cas à paramètre	77
9	Un procédé algorithmique pour la décomposition de Jordan-Hölder des φ-modules filtrés	79
9.1	Mise en contexte	79
9.2	Description du cadre de travail	81
9.3	Obtention de la combinaison linéaire minimale	82
9.4	Obtention d'un sous-espace stable simple	84
9.5	Passage à l'étape suivante	84
A	Quelques exemples de résultats numériques	87
A.1	Courbe $y^2 = f(t)$, $\deg(f) = 5$, $p = 7$	87
A.2	Courbe $y^2 = (t - 1)(t - 2)(t - 3)(t - 4)(t - 5)(t - 6)(t - 7)$, $p = 11$	88
A.3	Courbe $y^3 = (t - 1)(t - 2)(t - 3)(t - 4)(t - 5)$, $5 < p < 100$ premier	89
A.3.1	Courbe $y^4 = (t - 1)(t - 2)(t - 3)(t - 4)(t - 5)(t - 6)(t - 7)$, $p = 13$	92
A.4	Application de l'algorithme de décomposition de Jordan-Hölder	92
A.4.1	Exemple explicite	92
A.4.2	Décomposition pour les exemples matriciels précédents	97
B	Invariant de Hasse des courbes elliptiques	99
C	Formulaire et index de notations	101
C.1	Formulaire	101
C.2	Notations	101
	Bibliographie	105

Introduction

Soit k un corps fini et X_k une courbe projective lisse sur $\text{Spec}(k)$. Il a été montré par Hasse [Has35] que le rang de la matrice de Hasse-Witt est un invariant important de X_k et donc de sa jacobienne. Lorsque le rang est minimal, c'est-à-dire nul, on dit que la courbe est supersingulière ; lorsqu'il est maximal et donc égal à g , genre de la courbe, elle est dite ordinaire. Dans le cas d'une courbe elliptique, définie par l'équation $y^2 = t(t-1)(t-\lambda)$, le calcul de cet invariant est déjà fait par Hasse en loc. cit. et il est donné, à un inversible modulo p près, par la formule $\sum_{i=0}^k \binom{k}{i}^2 \lambda^i$. Dans le cas des courbes hyperelliptiques et de certaines courbes de Fermat, le calcul a été fait par Gonzales [Gon97]. Par ailleurs pour les courbes hyperelliptiques on dispose depuis peu pour le calculer d'un algorithme en temps polynomial [HS14].

Parallèlement, Kedlaya [Ked01] s'est rendu compte que, lorsque X_k est une courbe hyperelliptique, il est possible de calculer la cohomologie rigide de l'ouvert complémentaire des points de ramification de X_k . On peut en déduire la fonction Zêta de cette courbe et donc le nombre de points de la courbe. Ce calcul a été généralisé par Tuitman dans le cas de revêtements séparables de degré n de la droite projective sur un corps fini [Tui16][Tui17]. Même si le contexte de notre travail est différent de celui de ces algorithmes, nous avons réutilisé certaines idées de Kedlaya, notamment celle qui consiste à se placer sur l'ouvert complémentaire du lieu de ramification pour trouver un relèvement explicite du Frobenius (cela sera explicité dans la section 7.2).

Considérons k un corps fini, $V = W(k)$ l'anneau des vecteurs de Witt de k et $K = \text{Frac}(V)$. On se propose dans cette thèse de calculer un invariant plus complet que l'invariant de Hasse-Witt pour une certaine classe de courbes projectives lisses. Ces courbes sont des revêtements séparables de degré n de la droite projective sur k , elles seront décrites plus précisément ci-dessous. Soit X une courbe projective lisse sur $\text{Spec}(V)$ qui est un revêtement séparable de degré n de la droite projective relative sur $\text{Spec}(V)$, notons X_k sa fibre spéciale et X'_k la courbe obtenue après changement de base par le Frobenius sur k . Commençons par quelques rappels sur l'invariant de X_k que nous souhaitons calculer. En 1987 Fontaine et Messing ont donné une construction du Frobenius divisé cristallin Ψ , qui est à valeurs dans le groupe de cohomologie cristalline, $H_{cris}^1(X_k)$ [FM87]. Or il se trouve que pour les courbes que nous considérons ici, $H_{cris}^1(X_k)$ est un V -module libre de rang fini égal à $2g$. Sous nos hypothèses on sait, grâce au théorème de comparaison de Berthelot [BO78], que le groupe $H_{cris}^1(X_k)$ s'identifie à $H_{DR}^1(X)$, et cet isomorphisme donne un isomorphisme modulo p

$$H_{cris}^1(X_k)/pH_{cris}^1(X_k) \simeq H_{DR}^1(X_k).$$

Finalement, modulo p , le Frobenius divisé Ψ donne un morphisme de k -espaces vectoriels

$$\Phi' : H^0(X'_k, \Omega_{X'_k}^1) \oplus H^1(X'_k, \mathcal{O}_{X'_k}) \rightarrow H_{DR}^1(X_k)$$

qui, sous nos hypothèses, est un isomorphisme. Par ailleurs, puisque le Frobenius sur k est un isomorphisme, la projection $X'_k \rightarrow X_k$ est un isomorphisme de schémas, et on en déduit des isomorphismes semi-linéaires par rapport au Frobenius sur k

$$H^0(X_k, \Omega_{X_k}^1) \simeq H^0(X'_k, \Omega_{X'_k}^1) \text{ et } H^1(X_k, \mathcal{O}_{X_k}) \simeq H^1(X'_k, \mathcal{O}_{X'_k}).$$

En composant l'isomorphisme précédent avec ces isomorphismes semi-linéaires, on en déduit un isomorphisme semi-linéaire de k -espaces vectoriels

$$\Phi : H^0(X_k, \Omega_{X_k}^1) \oplus H^1(X_k, \mathcal{O}_{X_k}) \rightarrow H_{DR}^1(X_k).$$

C'est cet isomorphisme dont on cherche à calculer la matrice dans une base adaptée au scindage. Par définition, dans la base que nous avons choisie pour la représenter, le quart inférieur droit de la matrice redonne la matrice de Hasse-Witt, tandis que le quart supérieur gauche redonne la matrice de l'opérateur de Cartier [Car57]. Il était déjà connu de Cartier que ces deux opérateurs se correspondent par la dualité de Serre sur X_k . L'intérêt de calculer ce nouvel invariant (la matrice du Frobenius divisé) est que cela permet, après application de l'algorithme de Wach [HW15][Wac97], de calculer le (φ, Γ) -module modulo p associé à la représentation galoisienne $H_{et}^1(X_{\overline{K}}, \mathbf{Q}_p)$, où \overline{K} est une clôture algébrique de K . Ce dernier point ne sera pas abordé ici. En revanche, en utilisant la classification des φ -modules filtrés simples via les suites finies d'entiers décrites par Fontaine-Laffaille [FL82], nous obtenons la liste des φ -modules filtrés simples (quotients de Jordan-Hölder) apparaissant dans la décomposition de $H_{DR}^1(X_k)$.

Pour mener à bien le calcul de la matrice du Frobenius divisé, nous utilisons un résultat récent de Huyghe-Wach [HW16] qui démontre que Φ' coïncide avec le morphisme construit par Deligne-Illusie en 1987 [DI87] pour démontrer la dégénérescence de la suite spectrale de Hodge vers de Rham. Le point remarquable de cette construction est qu'elle est complètement algorithmique, au moins dans certains cas, comme l'illustre notre travail. Signalons enfin qu'il est standard que Φ coïncide avec le Frobenius divisé de Mazur modulo p [Maz73a], qui est construit à partir d'un scindage de la filtration de Hodge, donnant un isomorphisme

$$H_{DR}^1(X) \simeq H^0(X, \Omega_X^1) \oplus H^1(X, \mathcal{O}_X).$$

Enfin nous obtenons au passage une formule générale pour calculer la matrice de Hasse-Witt pour la famille de courbes considérée, formule analogue à celle obtenue par Elkin pour l'opérateur de Cartier [Elk11].

Détaillons à présent notre travail. Tout d'abord puisque la construction du morphisme de Deligne-Illusie repose sur le calcul explicite du complexe de Čech associé au complexe de de Rham de la courbe X_k , nous nous sommes donné une classe de revêtements X sur $\text{Spec}(V)$ de degré n (avec $n \wedge p = 1$) admettant un recouvrement à deux ouverts généralisant ce qui se passe dans le cas des courbes hyperelliptiques. Notre première étape consiste alors à identifier une famille

de revêtements de degré n de \mathbb{P}^1 admettant un recouvrement à deux ouverts. Notre choix s'est porté sur des courbes X lisses (non planes) définies comme la réunion des deux ouverts affines U et W définis par

$$\begin{aligned} U &= \text{Spec}(V[t, y]/(y^n - f(t))) \\ W &= \text{Spec}(V[s, z]/(z^n - f_2(s))) \end{aligned}$$

avec $V = W(k)$, $f \in V[t]$, $f_2 \in V[s]$ polynômes de degré l et $l + 1$ respectivement ainsi que des conditions de recollement détaillées à la section 2.1. Ces revêtements cycliques définis par une équation $y^n = f(t)$ avec $n \wedge p = 1$ ont été appelés courbes superelliptiques par Gaudry-Gürel [GG01].

Soit X une courbe de cette famille. Lorsque k contient les racines n -ièmes de l'unité de $\overline{\mathbb{F}_p}$, une clôture algébrique de \mathbb{F}_p , i.e. $\mu_n(\overline{\mathbb{F}_p}) \subset k$, on peut définir une action de $\mu_n(\overline{\mathbb{F}_p})$ sur $V[t, y]$ (resp. $V[s, z]$) par $\delta : (t, y) \mapsto (t, [\zeta]^{-1}y)$ (resp. $\delta : (s, z) \mapsto (s, [\zeta]^{-1}z)$) où $[\zeta]$ est le représentant de Teichmüller de ζ , une racine primitive n -ième de l'unité. Les deux actions se recollent pour définir un morphisme sur X , puis sur les groupes de cohomologie. Il est alors naturel de considérer les composantes isotypiques associées à cette action. Par ailleurs, indépendamment du fait que k contienne $\mu_n(\overline{\mathbb{F}_p})$ on établit que X est de genre $g = (l - 1)(n - 1)/2$ (proposition 3.4.1) et si $p > 2g - 1$, alors on a un isomorphisme (théorème 5.4.1)

$$H_{DR}^1(X) \simeq \bigoplus_{j=1}^{n-1} \bigoplus_{i=0}^{rn-3} V \frac{t^i dt}{y^j}$$

avec $r = (l + 1)/n$. Afin de mener à bien le calcul de cet isomorphisme, nous commençons par twister le complexe de de Rham de X par une puissance assez grande du faisceau inversible associé au diviseur à l'infini. On obtient alors un complexe acyclique à partir duquel il est possible de calculer une base de $H_{DR}^1(X)$.

Soit maintenant $d : \mathcal{O}_X(U) \times \mathcal{O}_X(W) \rightarrow \mathcal{O}_X(U \cap W)$ avec $d(a, b) = (a - b)|_{U \cap W}$. A l'aide de l'identification $H^1(X, \mathcal{O}_X) = \mathcal{O}_X(U \cap W)/\text{Im}(d)$, on montre que le V -module $H^1(X, \mathcal{O}_X)$ admet pour base la famille $\overline{h_{i,j}}$ des classes des éléments $h_{i,j} = t^{-i}y^j \in \mathcal{O}_X(U \cap W)$ pour $1 \leq j \leq n - 1$ et $1 \leq i \leq rj - 1$ (proposition 6.0.4), soit encore

$$H^1(X, \mathcal{O}_X) = \bigoplus_{j=1}^{n-1} \bigoplus_{i=1}^{rj-1} V \overline{t^{-i}y^j}.$$

Toujours pour ces mêmes courbes, notons \mathcal{F} le recouvrement de X formé par U et W , Ω_X^\bullet le complexe de de Rham de X et $\check{C}(\mathcal{F}, \Omega_X^\bullet)$ le complexe de Čech de Ω_X relativement à \mathcal{F} . Pour pouvoir utiliser la construction de Deligne-Illusie il est essentiel de construire une application V -linéaire $[\tau] : H^1(X, \mathcal{O}_X) \rightarrow H^1(\check{C}(\mathcal{F}, \Omega_X^\bullet))$ qui est un scindage de la filtration de Hodge (proposition 6.0.6). Celle-ci sera explicitée en fonction des données de la courbe, à une section globale $\omega \in H^0(X, \Omega_X^1)$ près.

Il s'agit ensuite de calculer des relèvements du Frobenius modulo p^2 sur chaque ouvert. Nous émettons alors une nouvelle hypothèse. Nous supposons que 0 n'est pas racine du polynôme f permettant de définir la courbe sur U . Cette hypothèse peut sembler écarter le type de courbes

classiques comme par exemple la courbe elliptique définie sur U par $y^2 = t(t-1)(t-\lambda)$ mais il n'en est rien. Une simple translation $t' = t + u$ permet de ramener l'étude d'une telle courbe à l'étude d'une courbe vérifiant notre hypothèse. Celle-ci nous amène naturellement à considérer un nouveau recouvrement de X par

$$(U \cap D(f(t))) \cup W = \bar{U} \cup W$$

dont chacun des ouverts admet un relèvement du Frobenius modulo p^2 , celui-ci étant explicite sur \bar{U} (qui est l'ouvert de U complémentaire des points de ramification) et algorithmique sur W . Ceci étant fait nous pouvons alors donner explicitement l'image par le morphisme de Deligne-Illusie des éléments de la base de $H^1(X'_k, \mathcal{O}_{X'_k})$ et de $H^0(X'_k, \Omega_{X'_k}^1)$ et donc calculer la matrice du Frobenius divisé sur $H_{DR}^1(X_k)$. Nous décomposons ce morphisme dans les composantes isotypiques des modules considérés.

Ceci étant fait nous calculons alors des formules explicites donnant les coefficients de la matrice généralisant entre autre les formules de Gonzales [Gon97]. Cela nécessite entre autre l'utilisation d'une astuce d'inversion de f que nous devons à Xavier Caruso. Enfin nous fournissons un procédé algorithmique permettant d'obtenir la décomposition de Jordan-Hölder du φ -module filtré associé à cette matrice.

Pour illustrer cette introduction, considérons la courbe définie sur U par l'équation

$$y^3 = t(t-1)(t-2)(t-3)(t-4)$$

avec $p = 17$. Après avoir fait agir la translation $t' = t + 1$, il est possible d'appliquer les résultats algorithmiques développés dans cette thèse pour obtenir la matrice de ϕ dans une base adaptée au scindage

$$\left(\begin{array}{cccc|cccc} 0 & 12 & 16 & 6 & 6 & 0 & 0 & 0 \\ 8 & 0 & 0 & 0 & 0 & 15 & 1 & 11 \\ 9 & 0 & 0 & 0 & 0 & 7 & 0 & 12 \\ 7 & 0 & 0 & 0 & 0 & 1 & 4 & 15 \\ \hline 10 & 0 & 0 & 0 & 0 & 10 & 8 & 0 \\ 0 & 13 & 5 & 8 & 0 & 0 & 0 & 0 \\ 0 & 5 & 10 & 11 & 13 & 0 & 0 & 0 \\ 0 & 8 & 11 & 0 & 10 & 0 & 0 & 0 \end{array} \right)$$

ou encore dans une base adaptée aux composantes isotypiques des modules considérés

$$\left(\begin{array}{cccc|cccc} 0 & 0 & 0 & 0 & 12 & 16 & 6 & 6 \\ 0 & 0 & 0 & 0 & 13 & 5 & 8 & 0 \\ 0 & 0 & 0 & 0 & 5 & 10 & 11 & 13 \\ 0 & 0 & 0 & 0 & 8 & 11 & 0 & 10 \\ \hline 8 & 15 & 1 & 11 & 0 & 0 & 0 & 0 \\ 9 & 7 & 0 & 12 & 0 & 0 & 0 & 0 \\ 7 & 1 & 4 & 15 & 0 & 0 & 0 & 0 \\ 10 & 10 & 8 & 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

en gardant dans chaque sous-matrice une décomposition adaptée au scindage. Les quotients de Jordan-Hölder dans cet exemple sont de dimension 1 ou 2 ; ils sont au nombre de 6 et sont décrits par la liste suivante $(0, 0, 1, 1, (0, 1), (0, 1))$.

Nous commencerons par motiver le choix de la famille de revêtements étudiée et des conditions que nous souhaitons voir vérifiées (chapitre 2), ainsi que par une étude de la lissité, de la ramification et du genre (chapitre 3). Nous présenterons ensuite successivement un calcul d'une base de $H^0(X, \Omega_X^1)$ (chapitre 4) et de $H_{DR}^1(X)$ (chapitre 5). Nous expliciterons également le calcul d'un scindage du $H^1(X, \mathcal{O}_X)$ vers le premier espace de cohomologie du complexe de Čech du complexe de de Rham (chapitre 6) ainsi que le calcul du Frobenius divisé via un calcul de relèvements du Frobenius modulo p^2 sur chacun des ouverts et le calcul du morphisme de Deligne-Illusie (chapitre 7), ceci donnant lieu à des formules permettant de calculer la matrice associée (chapitre 8). A partir de cette matrice nous calculerons alors la décomposition de Jordan-Hölder du φ -module associé (chapitre 9). Enfin nous présenterons quelques exemples explicites (annexe A).

Chapitre 1

Préliminaires

Définition 1.0.1. On considère un corps l . On appelle courbe sur $\text{Spec}(l)$ un schéma intègre de dimension 1 propre sur $\text{Spec}(l)$ ([Liu02] 7.3).

Définition 1.0.2. Soit A un anneau de valuation discrète. On dit que $C \rightarrow \text{Spec}(A)$ est une courbe relative sur $\text{Spec}(A)$ si c'est un morphisme plat, propre dont les fibres sont des courbes ([Liu02] 8.3.1, 3.16).

Définition 1.0.3. On considère $C \rightarrow \text{Spec}(l)$ une courbe (au sens de la première définition), on définit le genre de C , noté $g(C)$, par $g(C) = \dim(H^0(C, \Omega_{C/\text{Spec}(l)}^1))$ ([Liu02] 7.3.2, 3.19).

Remarque 1.0.1. Si $C \rightarrow \text{Spec}(A)$ est une courbe, il est donc possible de calculer le genre de chacune de ses fibres qui sont des courbes sur $\text{Spec}(l)$ pour un certain corps l . Si ceux-ci sont tous égaux au même entier g alors on dira par abus de langage que la courbe C est de genre g .

Définition 1.0.4. Considérons C_1 et C_2 deux courbes sur un corps l . Notons $l(C_1)$ et $l(C_2)$ leurs corps de fonctions respectifs. On dit qu'un morphisme $f : C_1 \rightarrow C_2$ est un morphisme séparable si $l(C_2) \rightarrow l(C_1)$ est une extension séparable ([Liu02] 7.4.2). Par ailleurs si f est un morphisme fini on appelle degré de f le degré de l'extension de corps de fonctions $[l(C_1) : l(C_2)]$ ([Har77] IV.2).

Notation. Soient A un anneau de valuation discrète, l son corps résiduel, L son corps des fractions et $C \rightarrow \text{Spec}(A)$ une courbe. On note $C_l = C \times_{\text{Spec}(A)} \text{Spec}(l)$ la fibre spéciale de C et $C_L = C \times_{\text{Spec}(A)} \text{Spec}(L)$ la fibre générique de C . De la même manière on note \mathbb{P}_l^1 la fibre spéciale et \mathbb{P}_L^1 la fibre générique de \mathbb{P}_A^1 .

Définition 1.0.5. Considérons $A \rightarrow B$ un homomorphisme injectif d'anneaux de valuation discrète. Soit π_A (resp. π_B) une uniformisante de A (resp. sur B). On appelle indice de ramification de B sur A l'entier $e_{B/A} \geq 1$ vérifiant $\pi_A B = \pi_B^{e_{B/A}} B$. Par convention si $\pi_A = 0$ on pose

$e_{B/A} = 1$. On dit que B est modérément ramifié sur A si $B/\pi_B B$ est séparable sur $A/\pi_A A$ et si $e_{B/A}$ est premier à la caractéristique de $A/\pi_A A$ quand cette dernière est non nulle. ([Liu02] 7.4.2).

Définition 1.0.6. Soit $f : C_1 \rightarrow C_2$ un morphisme fini de courbes projectives normales ([Liu02] 4.1.1) sur un corps l . Pour tout point fermé x de C_1 on note e_x l'indice de ramification de $\mathcal{O}_{C_2, f(x)} \rightarrow \mathcal{O}_{C_1, x}$. On dit que f est ramifié en x ou que x est un point de ramification de f si f n'est pas étale en x (ce qui est équivalent à $e_x \geq 2$). L'ensemble des points de ramification de f est fini et est appelé lieu de ramification de f . On dit que f est modérément ramifié en x si $\mathcal{O}_{C_2, f(x)} \rightarrow \mathcal{O}_{C_1, x}$ est modérément ramifié ([Liu02] 7.4.2, 4.15).

Théorème 1.0.1 (Théorème d'Hurwitz). Soit $f : C_1 \rightarrow C_2$ un morphisme fini de courbes normales projectives lisses sur un corps l . Supposons que f est séparable de degré n , alors :

$$2g(C_1) - 2 = n(2g(C_2) - 2) + \sum_x (e'_x - 1)[l(x) : l]$$

où la somme est effectuée sur les points fermés x de C_1 et e'_x est un entier tel que $e'_x \geq e_x$, avec $e'_x = e_x$ si et seulement si f est modérément ramifié en x .

Preuve: Ce résultat est énoncé et démontré dans [Liu02] théorème 4.16, section 4, chapitre 7. □

Chapitre 2

Modèle à deux ouverts d'un revêtement de degré n de \mathbb{P}^1

2.1 Définition de la courbe X

Soient p un nombre premier et n un nombre entier tel que $n \wedge p = 1$. Soient k un corps fini de caractéristique p , $V = W(k)$ l'anneau des vecteurs de Witt et $K = \text{Frac}(V)$. Ainsi défini, V est un anneau de valuation discrète complet, d'inégale caractéristique $(0, p)$. De plus k est son corps résiduel. On écrit la droite projective \mathbb{P}_V^1 comme $\mathbb{P}_V^1 = A \cup B$ avec $A = \text{Spec}(V[t])$ et $B = \text{Spec}(V[s])$ où $s = 1/t$.

Soient l un entier congru à -1 modulo n , tel que l n'est pas multiple de p , $\alpha_i \in V$ pour $1 \leq i \leq l$, dont les classes sont toutes distinctes dans k et $f \in V[t]$ défini par $f(t) = \prod (t - \alpha_i)$, de degré l en tant que polynôme en t . Posons $r = (l + 1)/n$ et désignons par $f_2(s)$ la fraction rationnelle $f_2(s) = f(1/s)s^{rn} = f(1/s)s^{l+1}$. Enfin posons $z = s^r y$.

Remarque 2.1.1. Le fait que les classes des α_i soient distinctes dans k impose déjà la condition que l soit inférieur ou égal à p^m où m est tel que $k \simeq \mathbb{F}_{p^m}$. On souhaite cependant éviter le cas où l est un multiple de p qui pose des problèmes lorsque l'on souhaite manipuler la classe de la dérivée du polynôme f dans k . C'est ce qui justifie la condition sur l .

Par ailleurs pour simplifier les démonstrations dans l'étude de la lissité et de la ramification, il est utile de supposer que la classe d'aucun α_i est nulle dans k . Les résultats restent cependant vrais même si l'un des α_i a une classe nulle dans k .

Lemme 2.1.1. Notons $\mathbf{f}(t)$ et $\mathbf{f}'(t)$ respectivement les classes de $f(t)$ et $f'(t)$ dans $k[t]$. Alors $\mathbf{f}(t)$ et $\mathbf{f}'(t)$ (resp. $f(t)$ et $f'(t)$) sont premiers entre eux dans $k[t]$ (resp. dans $K[t]$). De plus $f(t)$ et $f'(t)$ engendrent l'idéal unité de $V[t]$, $V[t]$ étant factoriel on peut donc dire que $f(t)$ et $f'(t)$ sont premiers entre eux dans $V[t]$.

Preuve: Par hypothèse $f(t)$ n'a pas de racines doubles dans K donc $f(t)$ et $f'(t)$ sont premiers entre eux dans $K[t]$. De même puisque les α_i sont toutes distinctes dans k , $\mathbf{f}(t)$ est à racines simples dans $k[t]$ et donc $\mathbf{f}(t)$ et $\mathbf{f}'(t)$ sont premiers entre eux dans $k[t]$.

Puisque $f(t)$ et $f'(t)$ sont premier entre eux dans $K[t]$, il existe un entier m et des polynômes a et b de $V[t]$ tels que $p^m = a(t)f(t) + b(t)f'(t)$ dans $V[t]$. Prenons m minimal pour cette relation. Alors si $m > 1$ par passage à la classe dans $k[t]$ on obtient la relation $0 = \mathbf{a}(t)\mathbf{f}(t) + \mathbf{b}(t)\mathbf{f}'(t)$ dans $k[t]$. Supposons que $a(t)$ soit de classe nulle dans $k[t]$, comme $f'(t)$ est de classe non nulle dans $k[t]$ (on a pris soin que $l < p$) on en déduit que $b(t)$ est également de classe nulle dans $k[t]$ et cela contredit la minimalité de m . Par un argument similaire on peut également affirmer que la classe de $b(t)$ est non nulle dans $k[t]$. Alors la relation $0 = \mathbf{a}(t)\mathbf{f}(t) + \mathbf{b}(t)\mathbf{f}'(t)$ permet d'affirmer que la classe de $f(t)$ dans $k[t]$ est un diviseur de 0 dans $k[t]/\mathbf{f}'(t)$. Mais par ailleurs on sait que $\mathbf{f}(t)$ et $\mathbf{f}'(t)$ sont premiers entre eux dans $k[t]$ ce qui signifie que $f(t)$ est inversible dans $k[t]/\mathbf{f}'(t)$ ce qui est contradictoire. Ainsi $m = 0$ et donc $f(t)$ et $f'(t)$ engendrent l'idéal unité de $V[t]$. Enfin en tant qu'anneau de valuation discrète, V est principal, donc factoriel. Or on sait que pour tout anneau B factoriel, l'anneau des polynômes associé $B[t]$ est également factoriel (voir [Lan02] IV.2 2.4) donc $V[t]$ est factoriel. Cela a donc un sens de parler de polynômes premiers entre eux dans $V[t]$. □

Lemme 2.1.2. *La fraction rationnelle $f_2(s)$ définie par la relation $f_2(s) = f(1/s)s^{rn}$ est un polynôme de $V[s]$ à racines simples. Sa classe dans $k[s]$ est également un polynôme à racines simples.*

Preuve: Par définition on a

$$f_2(s) = s^{l+1} \prod_{i=1}^l (1/s - \alpha_i) = s \prod_{i=1}^l (1 - \alpha_i s)$$

il est donc évident que $f_2(s)$ est un polynôme en s . Par ailleurs les racines de ce polynôme sont les $1/\alpha_i$ (pour α_i non nul) et 0, qui sont tous distincts, donc $f_2(s)$ est à racines simples dans V . En ce qui concerne $\mathbf{f}_2(s)$ il est clair que c'est un élément de $k[s]$. De plus les α_i ont des classes distinctes dans k par hypothèse donc les $1/\alpha_i$ ont également des classes distinctes (et non nulles) dans k ce qui permet de conclure. □

Lemme 2.1.3. *Avec les notations précédentes, $\mathbf{f}_2(s)$ et $\mathbf{f}'_2(s)$ (resp. $f_2(s)$ et $f'_2(s)$) sont premiers entre eux dans $k[s]$ (resp. $K[s]$). De plus $f_2(s)$ et $f'_2(s)$ sont premiers entre eux dans l'anneau factoriel $V[s]$.*

Preuve: La démonstration est la même que dans le cas du lemme 2.1.1. □

On définit les polynômes en deux variables suivants :

$$F(Y, T) = Y^n - \prod_{i=1}^l (T - \alpha_i)$$

$$F_2(Y, T) = Y^n - T \prod_{i=1}^l (1 - \alpha_i T)$$

avec les α_i , $1 \leq i \leq l$ comme précédemment.

Théorème 2.1.1 (Critère d'Eisenstein). *Soit A un anneau factoriel, K son corps des fractions. Soit $f(S) = a_n S^n + \dots + a_0 \in A[S]$ un polynôme de degré $n \geq 1$. Soit \wp un élément premier de A tel que :*

$$a_n \not\equiv 0 [\wp], \quad \forall i < n \quad a_i \equiv 0 [\wp] \quad \text{et} \quad a_0 \not\equiv 0 [\wp^2]$$

alors $f(S)$ est irréductible sur $K[S]$.

Preuve: Voir le livre de Lang [Lan02] IV, 3.1. □

Lemme 2.1.4. *Les polynômes en deux variables, F et F_2 définis précédemment sont irréductibles.*

Preuve: Il suffit d'appliquer le théorème 2.1.1 en prenant $A = V[T]$, $K = K(T)$. En tant qu'anneau de valuation discrète, V est principal donc factoriel et alors l'anneau $A = V[T]$ considéré est factoriel (voir par exemple [Lan02] IV.2 2.4.). Chacun des polynômes considérés est un polynôme de $A[Y]$ de degré $n \geq 1$.

En ce qui concerne F on a $a_n = 1$, $a_0 = -\prod_{i=1}^l (T - \alpha_i)$ et $\forall 1 \leq k \leq n - 1$, $a_k = 0$. Posons $\wp = T - \alpha_1$. C'est un élément premier de A . De plus il est évident que $a_n \not\equiv 0 [\wp]$ et que $\forall i < n$ $a_i \equiv 0 [\wp]$. Enfin la dernière hypothèse est vérifiée car tous les α_i sont distincts. Ainsi par le théorème 2.1.1 F est un polynôme irréductible.

En ce qui concerne F_2 on a $a_n = 1$, $a_0 = -T \prod_{i=1}^l (1 - \alpha_i T)$ et $\forall 1 \leq k \leq n - 1$, $a_k = 0$. Posons $\wp = 1 - \alpha_1 T$. C'est un élément premier de A . On a $a_n \not\equiv 0 [\wp]$, $\forall i < n$ $a_i \equiv 0 [\wp]$ et la dernière hypothèse est vérifiée car tous les α_i sont distincts et $T \neq (1 - \alpha_i T)$ quel que soit α_i . Ainsi par le théorème 2.1.1 F_2 est un polynôme irréductible. □

Définition 2.1.1. *On conserve les notations précédentes. On définit un schéma affine U sur $A = \text{Spec}(V[t])$ par*

$$U = \text{Spec}(V[t, y]/(y^n - f(t)))$$

et $V[t] \rightarrow \mathcal{O}_U(U)$, $t \mapsto t$ ainsi qu'un ouvert affine W sur $B = \text{Spec}(V[s])$ par

$$W = \text{Spec}(V[s, z]/(z^n - f_2(s)))$$

et $V[s] \rightarrow \mathcal{O}_W(W)$, $s \mapsto s$.

Proposition 2.1.1. *Les courbes U et W définies précédemment se recollent au dessus de $A \cap B$. Par ailleurs les conditions de recollement sont données par $t = s^{-1}$ et $z = s^r y$.*

Preuve: Montrons que l'on peut définir des isomorphismes

$$\rho : V[t, t^{-1}] \otimes_{V[t]} \mathcal{O}_U(U) \rightarrow V[s, s^{-1}] \otimes_{V[s]} \mathcal{O}_W(W)$$

$$\tilde{\rho} : V[s, s^{-1}] \otimes_{V[s]} \mathcal{O}_W(W) \rightarrow V[t, t^{-1}] \otimes_{V[t]} \mathcal{O}_U(U)$$

inverses l'un de l'autre. Pour mémoire on a $V[t, t^{-1}] \otimes_{V[t]} \mathcal{O}_U(U) \simeq V[t, t^{-1}, y]/(y^n - f(t))$ et $V[s, s^{-1}] \otimes_{V[s]} \mathcal{O}_W(W) \simeq V[s, s^{-1}, z]/(z^n - f_2(s))$. Tout d'abord il existe un morphisme d'algèbres $V[t, t^{-1}, y] \rightarrow V[s, s^{-1}, z]$ qui envoie t sur s^{-1} et y sur $s^{-r}z = s^{-(l+1)/n}z$. Ce morphisme passe au quotient en un morphisme d'algèbres

$$\rho : V[t, t^{-1}] \otimes_{V[t]} \mathcal{O}_U(U) \rightarrow V[s, s^{-1}] \otimes_{V[s]} \mathcal{O}_W(W).$$

On définit de même le morphisme $\tilde{\rho} : V[s, s^{-1}] \otimes_{V[s]} \mathcal{O}_W(W) \rightarrow V[t, t^{-1}] \otimes_{V[t]} \mathcal{O}_U(U)$ avec $\tilde{\rho}(s) = t^{-1}$ et $\tilde{\rho}(z) = t^{-r}y$. Il est alors facile de vérifier que $\tilde{\rho} \circ \rho(t) = t$, $\tilde{\rho} \circ \rho(y) = y$ et $\rho \circ \tilde{\rho}(s) = s$, $\rho \circ \tilde{\rho}(z) = z$. Ainsi les ouverts U et W se recollent au dessus de l'ouvert $A \cap B$. □

Définition 2.1.2. *Avec les notations précédentes, on définit X comme le recollement des deux schémas U et W définis précédemment.*

Proposition 2.1.2. *Par construction on a un morphisme de schémas $\Pi : X \rightarrow \mathbb{P}_V^1$. Le morphisme Π est fini et plat. De plus les applications induites par Π sur les fibres, $\Pi_k : X_k \rightarrow \mathbb{P}_k^1$ et $\Pi_K : X_K \rightarrow \mathbb{P}_K^1$, sont des morphismes finis séparables de degré n .*

Preuve: Le fait que le morphisme $\Pi : X \rightarrow \mathbb{P}_V^1$ soit fini et plat est une propriété locale sur \mathbb{P}_V^1 , il suffit de montrer que $U \rightarrow \text{Spec}(V[t])$ et $W \rightarrow \text{Spec}(V[s])$ sont finis et plats, ce qui est équivalent à montrer que $V[t] \rightarrow \mathcal{O}_U(U)$ et $V[s] \rightarrow \mathcal{O}_W(W)$ sont finis et plats. Or $\mathcal{O}_U(U)$ est un $V[t]$ -module libre de rang n et de base $1, y, \dots, y^{n-1}$. De même $\mathcal{O}_W(W)$ est un $V[s]$ -module libre de rang n et de base $1, z, \dots, z^{n-1}$ ce qui permet de conclure.

En ce qui concerne le morphisme sur les fibres génériques c'est alors une conséquence de ce qui précède puisque platitude et finitude sont stables par changement de base. L'argument est le même pour le morphisme sur les fibres spéciales car k est de caractéristique p et qu'on a pris soin que n soit premier à p . □

Proposition 2.1.3. *Avec les notations précédentes, X est une courbe relative sur $\text{Spec}(V)$.*

Preuve: Grâce à la proposition 2.1.2, il suffit de montrer que $X \rightarrow \text{Spec}(V)$ est propre et que X_K et X_k sont intègres de dimension 1. Commençons par montrer que X_K et X_k sont intègres. Cela revient à montrer que $\mathcal{O}(U_K)$ et $\mathcal{O}(U_k)$ sont intègres et comme on est dans un anneau factoriel il suffit de montrer que les polynômes en deux variables $y^n - f(t)$ et $z^n - f_2(s)$ sont irréductibles sur K et sur k , ce qui a été établi dans le lemme 2.1.4. L'argument permettant de calculer la dimension de X_K et de X_k est le même. Traitons le cas de X_k , il suffit de montrer que U_k et W_k sont de dimension 1. On a un morphisme fini $U_k \rightarrow \text{Spec}(k[t]) = \mathbb{A}_k^1$ tel que $k[t] \rightarrow \mathcal{O}_{X_k}(U_k) = k[t, y]/(y^n - f(t))$ est injectif. On applique alors la proposition 2.5.10 de [Liu02] et on peut ainsi affirmer que $\dim(U_k) = \dim(\mathbb{A}_k^1) = 1$. On montre de la même manière que $\dim(W_k) = 1$ et on en conclut que $\dim(X_k) = 1$. De même $\dim(X_K) = 1$. Enfin on sait que le morphisme $\mathbb{P}_V^1 \rightarrow \text{Spec}(V)$ est propre. De plus par construction on a un morphisme fini $X \rightarrow \mathbb{P}_V^1$ de degré n or un morphisme fini est propre ([Har77] ex4.1) donc on a un morphisme propre $X \rightarrow \mathbb{P}_V^1$. Enfin la composée de deux morphismes propres est propre ([Har77] II, 4.8), et donc X est propre sur $\text{Spec}(V)$ ce qui permet de conclure. \square

Remarque 2.1.2. On se permettra désormais de parler de la courbe X au lieu de préciser courbe relative sur $\text{Spec}(V)$.

2.2 Une action sur la courbe X

On suppose dans cette partie que k contient les racines n -ièmes de l'unité de $\overline{\mathbb{F}_p}$, une clôture algébrique de \mathbb{F}_p , i.e. $\mu_n(\overline{\mathbb{F}_p}) \subset k$. Sous cette hypothèse, le polynôme $Q_n(X) = X^n - 1$ admet n racines distinctes dans k . Par ailleurs puisqu'on a supposé que $n \wedge p = 1$, si $Q_n(\alpha) = 0$ alors $Q'_n(\alpha) = n\alpha^{n-1} \neq 0$. Le lemme de Hensel assure alors que les éléments de $\mu_n(\overline{\mathbb{F}_p})$ se relèvent en n éléments distincts de $W(k) = V$ qui sont leurs représentants de Teichmüller. Le représentant de Teichmüller est multiplicatif donc si α et β sont dans k alors $[\alpha\beta] = [\alpha][\beta]$. Soit $\alpha \in k$ tel que $\alpha^n = 1$, alors $[\alpha]$ son représentant de Teichmüller dans V vérifie $[\alpha]^n = 1$. Enfin puisque k est un corps fini de caractéristique p , $k \simeq \mathbb{F}_q$ où $q = p^m$ pour un certain entier non nul m . Dans ce cas, $\mu_n(\overline{\mathbb{F}_p}) \subset k \Leftrightarrow n \mid p^m - 1$. Soit donc $\mu_n(\overline{\mathbb{F}_p})$ le groupe, cyclique, des racines n -ièmes de l'unité. Soit $\zeta \in \mu_n(\overline{\mathbb{F}_p})$ une racine primitive n -ième de l'unité, notons $[\zeta] \in V$ le représentant de Teichmüller de ζ .

On définit δ sur $V[t, y]$ par

$$\delta : (t, y) \mapsto (t, [\zeta]^{-1} y)$$

qui passe au quotient en

$$\begin{array}{ccc} \delta : \mathcal{O}_U(U) & \longrightarrow & \mathcal{O}_U(U) \\ t & \longmapsto & t \\ y & \longmapsto & [\zeta]^{-1} y \end{array}$$

de même on définit δ sur $V[s, z]$ par

$$\delta : (s, z) \mapsto (s, [\zeta]^{-1} z)$$

qui passe au quotient en

$$\begin{array}{ccc} \delta : \mathcal{O}_W(W) & \longrightarrow & \mathcal{O}_W(W) \\ s & \longmapsto & s \\ z & \longmapsto & [\zeta]^{-1} z \end{array}$$

et ces deux applications se recollent sur $U \cap W$. Donc δ induit un morphisme de $X \rightarrow X$ qui décrit l'action de $\mu_n(\overline{\mathbb{F}}_p)$ sur X . Par functorialité δ induit un morphisme sur $\Omega_{X/\text{Spec}(V)}^1$, noté δ^* . Cette action est déduite de la précédente par différentiation, on a donc la description suivante

$$\begin{array}{ccc} \delta^* : \Omega_{X/\text{Spec}(V)}^1(U) & \longrightarrow & \Omega_{X/\text{Spec}(V)}^1(U) \\ dt & \longmapsto & dt \\ dy & \longmapsto & [\zeta]^{-1} dy \end{array}$$

$$\begin{array}{ccc} \delta^* : \Omega_{X/\text{Spec}(V)}^1(W) & \longrightarrow & \Omega_{X/\text{Spec}(V)}^1(W) \\ ds & \longmapsto & ds \\ dz & \longmapsto & [\zeta]^{-1} dz \end{array}$$

Proposition 2.2.1. *Soient M un V -module libre de rang fini muni d'une action V -linéaire d'un endomorphisme u tel que $u^n = \text{Id}$ et ζ une racine primitive n -ième de l'unité. Posons*

$$M_j = \{x \in M \text{ tq } u(x) = [\zeta]^j x\}$$

où $[\zeta]$ désigne le représentant de Teichmüller de ζ , alors $M = \bigoplus M_j$.

Preuve: Tout d'abord $M \subset M \otimes_V K = M[1/p]$ car M est un V -module libre. De plus u induit une application K -linéaire u_K de M_K qui vérifie $u_K^n = \text{Id}_{M_K}$ et est donc diagonalisable sur M_K car $X^n - 1 = \prod (X - [\zeta]^j)$ est scindé à racines simples dans K . Notons $M_{j,K}$ la j -ième composante isotypique de u_K , alors clairement $M_j \subset M_{j,K}$ et donc les M_j sont en somme directe. Considérons $M' = \bigoplus M_j$ et montrons que $M = M'$. Il est clair que $M' \subset M$ montrons donc l'inclusion inverse. Soit $x \in M$ définissons $p_j : x \mapsto x_j \in M_j$ par

$$x_j = \sum_{k=0}^{n-1} [\zeta]^{-kj} u^k(x).$$

Montrons que les x_j ainsi définis sont bien dans les espaces considérés. On a

$$\begin{aligned} u(x_j) &= \sum_{k=0}^{n-1} [\zeta]^{-kj} u^{k+1}(x) = \sum_{k=1}^n [\zeta]^{-(k-1)j} u^k(x) = [\zeta]^j \sum_{k=1}^{n-1} [\zeta]^{-kj} u^k(x) + [\zeta]^{-(n-1)j} u^n(x) \\ &= [\zeta]^j \left(x + \sum_{k=0}^{n-1} [\zeta]^{-kj} u^k(x) \right) = [\zeta]^j x_j \end{aligned}$$

donc x_j est bien un élément de M_j pour tout $0 \leq j \leq n-1$. De plus $p_j \circ p_j = np_j$. En effet soit $x \in M_j$ alors

$$p_j \circ p_j(x) = p_j \left(\sum_{k=0}^{n-1} [\zeta]^{-kj} u^k(x) \right) = \sum_{k=0}^{n-1} [\zeta]^{-kj} u^k \left(\sum_{l=0}^{n-1} [\zeta]^{-lj} u^l(x) \right) = \sum_{k=0}^{n-1} \sum_{l=0}^{n-1} [\zeta]^{-(l+k)j} u^{k+l}(x)$$

effectuons le changement de variable $l' = k + l$ dans la seconde somme, on obtient

$$p_j \circ p_j(x) = \sum_{k=0}^{n-1} \sum_{l'=k}^{k+n-1} [\zeta]^{-l'j} u^{l'}(x)$$

mais comme $u^n = Id$ on a

$$p_j \circ p_j(x) = \sum_{k=0}^{n-1} \left(\sum_{l'=k}^{n-1} [\zeta]^{-l'j} u^{l'}(x) + \sum_{l'=n}^{k+n-1} [\zeta]^{-l'j} u^{l'-n}(x) \right)$$

soit en effectuant le changement de variable $l'' = l' - n$ dans la dernière somme

$$p_j \circ p_j(x) = \sum_{k=0}^{n-1} \left(\sum_{l'=k}^{n-1} [\zeta]^{-l'j} u^{l'}(x) + \sum_{l''=0}^{k-1} [\zeta]^{-(l''+n)j} u^{l''}(x) \right)$$

enfin comme $[\zeta]^n = 1$ on peut réunir à nouveau les deux sommes indexées par l et l'' et on obtient

$$p_j \circ p_j(x) = \sum_{k=0}^{n-1} \sum_{l=0}^{n-1} [\zeta]^{-lj} u^l(x)$$

mais les termes de la deuxième somme sont constants par rapport à k donc

$$p_j \circ p_j(x) = n \sum_{l=0}^{n-1} [\zeta]^{-lj} u^l(x) = np_j(x)$$

ce qui est bien le résultat annoncé. Enfin montrons que tout élément x de M pour s'exprimer comme somme d'éléments de M_j . Par définition de x_j , la matrice A associée au système

$$\begin{cases} p_0(x) = x + u(x) + \dots + u^{n-1}(x) \\ p_1(x) = x + [\zeta]^{-1}u(x) + \dots + [\zeta]^{-(n-1)}u^{n-1}(x) \\ \vdots \\ p_{n-1}(x) = x + [\zeta]^{-(n-1)}u(x) + \dots + [\zeta]^{-(n-1)(n-1)}u^{n-1}(x) \end{cases}$$

est une matrice de Van der Monde montrons qu'elle est inversible dans $\mathcal{M}_n(V)$. Notons \mathbf{D} son déterminant et D sa réduction modulo p , alors

$$D = \prod_{0 \leq i < j \leq n-1} (\zeta^{-j} - \zeta^{-i})$$

mais $\zeta^n = 1$ donc on peut multiplier chaque terme du produit par ζ^n puis effectuer le changement de variable $i' = n - i$ et $j' = n - j$ et on obtient alors

$$D = \prod_{0 \leq j' < i' \leq n-1} (\zeta^{j'} - \zeta^{i'}).$$

Par définition le discriminant du polynôme $X^n - 1 \in k[X]$ vaut

$$\Delta = 1^{2n-2} \prod_{0 \leq i < j \leq n-1} (\zeta^i - \zeta^j)^2 = D^2$$

or on sait que le discriminant d'un polynôme est non nul sur un corps k dès que le polynôme est séparable sur $k[X]$ ([Lan02]) ce qui est le cas puisqu'on a supposé que $n \wedge p = 1$. Ainsi D est inversible dans k et donc la matrice A est inversible dans $\mathcal{M}_n(V)$. Notons $A^{-1} = (b_{i,j}) \in \mathcal{M}_n(V)$ son inverse alors on déduit du système associé à A que

$$\begin{cases} x &= b_{0,0}p_0(x) + \dots + b_{0,n-1}p_{n-1}(x) \\ u(x) &= b_{1,0}p_0(x) + \dots + b_{1,n-1}p_{n-1}(x) \\ \vdots & \\ u^{n-1}(x) &= b_{n-1,0}p_0(x) + \dots + b_{n-1,n-1}p_{n-1}(x) \end{cases}$$

en particulier la première équation de ce système permet d'affirmer que x est un élément de $M' = \bigoplus M_j$ et donc de conclure que $M = M'$, ce qui achève la démonstration. \square

Proposition 2.2.2. *Soit $0 \rightarrow E_1 \rightarrow \dots \rightarrow E_k \rightarrow 0$ une suite exacte de V -modules libres de rang fini, munis d'une action de $\mu_n(\overline{\mathbb{F}}_p)$ et tels que les différentielles de la suite exacte commutent à l'action de $\mu_n(\overline{\mathbb{F}}_p)$. Alors pour tout $0 \leq j \leq n-1$ on a une suite exacte $0 \rightarrow E_{1,j} \rightarrow \dots \rightarrow E_{k,j} \rightarrow 0$ où $E_{l,j}$ désigne la j -ième composante isotypique de E_l .*

Preuve: C'est une conséquence immédiate du lemme précédent. \square

Définition 2.2.1. *Notons $H = H^0(X, \Omega_{X/\text{Spec}(V)}^1)$. Soit $\chi_j : \mu_n(\overline{\mathbb{F}}_p) \rightarrow K^*$, $\zeta \mapsto [\zeta^j] = [\zeta]^j$ pour $1 \leq j \leq n-1$. On pose $\mathcal{E}_j = \{\omega \in H : \forall \zeta \in \mu_n(\overline{\mathbb{F}}_p), \zeta \cdot \omega = \chi_j(\zeta)\omega\}$ ce sont les composantes isotypiques associées à δ .*

Chapitre 3

Etude de la courbe X

3.1 Conventions

Notation. Afin d'alléger les notations du faisceau des formes différentielles de degré 1 de X_k sur \mathbb{P}_k^1 (voir [Liu02] 6.1, 1.17) on notera désormais $\Omega_{X_k}^1 = \Omega_{X_k/\text{Spec}(k)}^1$. De même on notera $\Omega_{X_K}^1 = \Omega_{X_K/\text{Spec}(K)}^1$ et $\Omega_X^1 = \Omega_{X/\text{Spec}(V)}^1$.

Soient C_L une courbe lisse irréductible sur un corps L et Q un point de C_L . On suppose que Q correspond à un idéal premier, encore noté Q , d'un ouvert affine $\text{Spec}(B) \subset C_L$ et on désigne par $B_Q = \mathcal{O}_{C_L, Q}$ l'anneau local associé. Alors B_Q est un anneau de valuation discrète d'uniformisante ξ , un paramètre local de C_L en Q . Notons $L(Q) = \mathcal{O}_{C_L, Q}/\xi\mathcal{O}_{C_L, Q}$ le corps résiduel de C_L en Q , on a un morphisme canonique

$$\lambda_Q : B \rightarrow B/Q \rightarrow L(Q).$$

Soit $f \in B$ on utilisera le vocabulaire suivant

- $f(Q)$ pour $\lambda_Q(f)$
- f est inversible au voisinage de Q pour f est inversible dans l'anneau local B_Q
- v_Q pour la valuation ξ -adique de B_Q

par ailleurs on peut étendre v_Q à $\text{Frac}(B)$ le corps des fractions de la courbe C_L et on se permettra de la noter encore v_Q . Enfin on note $\Omega_{C_L, Q}^1$ le localisé en Q du module des différentielles $\Omega_{C_L}^1$ i.e. $\Omega_{C_L, Q}^1 = \mathcal{O}_{C_L, Q}.d\xi$ et si $\omega \in \Omega_{C_L, Q}^1$ avec $\omega = h.d\xi$ on posera $v_Q(\omega) = v_Q(h)$.

3.2 Etude de la lissité

Proposition 3.2.1. *La courbe relative X définie à la section 2.1 est lisse sur $\text{Spec}(V)$.*

Preuve: La démonstration se réalise en deux temps. On vérifie d'abord la lissité sur U puis sur W . Soit donc Q un idéal premier de $V[t, y]$ contenant $y^n - f(t)$ et notons $L(Q)$ le corps résiduel

de Q i.e. $L(Q) = \text{Frac}(V[t, y]/Q)$. Considérons $\lambda : V[t, y] \rightarrow L(Q)$, définie via la surjection et l'injection canonique $V[t, y] \rightarrow V[t, y]/Q \rightarrow L(Q)$. En vertu du critère Jacobien (cf [BLR90] II.2 prop 7(d)), pour vérifier que la courbe est lisse, il suffit de vérifier que $\lambda(ny^{n-1}) \neq 0$ ou $\lambda(f'(t)) \neq 0$. Comme n est inversible sur V il suffit donc de vérifier que $\lambda(y) \neq 0$ ou $\lambda(f'(t)) \neq 0$. Supposons que $\lambda(y) = 0$ alors $\lambda(f(t)) = 0$. Or f et f' sont premiers entre eux dans $V[t]$ (voir lemme 2.1.1) donc il existe a et b dans $V[t]$ tels que $af + bf' = 1$ et alors on en déduit que $\lambda(f'(t)) \neq 0$.

La lissité sur W repose sur les mêmes arguments en remplaçant t par s , y par z et f par f_2 . Alors le critère Jacobien permet de dire qu'il suffit de vérifier que $\lambda(nz^{n-1}) \neq 0$ ou $\lambda(f_2'(s)) \neq 0$ et comme on a également montré que f_2 et f_2' étaient premiers entre eux dans $V[s]$ (voir lemme 2.1.3) on peut conclure de la même manière. \square

Remarque 3.2.1. On a montré au passage que $U = D(y) \cup D(f')$.

3.3 Etude de la ramification de X_K et X_k

Proposition 3.3.1. *La courbe affine U_k (respectivement U_K) est ramifiée en les l points fermés correspondant aux idéaux maximaux $M_i = (t - \alpha_i)\mathcal{O}_{U_k}(U_k) + y\mathcal{O}_{U_k}(U_k)$ (respectivement $M_i = (t - \alpha_i)\mathcal{O}_{U_K}(U_K) + y\mathcal{O}_{U_K}(U_K)$) où α_i désigne la classe de α_i dans k . De plus le corps résiduel $k(M_i)$ (resp. $K(M_i)$) est égal à k (resp. K).*

Preuve: On va expliciter ici le calcul de la ramification sur U_k , des arguments semblables donneront le résultat annoncé sur U_K . On a $\Omega_U^1(U) = A dt \oplus A dy / (ny^{n-1}dy - \mathbf{f}'(t)dt)$ où on a noté $A = k[t, y]/(y^n - \prod(t - \alpha_i))$. Soient Q un idéal premier de A et A_Q le localisé de A en cet idéal, on cherche un paramètre local de A_Q i.e. un certain $u \in A_Q$ tel que du soit une base de $\Omega_{A_Q}^1$. Remarquons que puisque X est lisse, U_k est la réunion de $D(y)$ et $D(\mathbf{f}')$.

Supposons que $y \notin Q$ (i.e. $Q \in D(y)$), alors localement

$$dy = \frac{1}{ny^{n-1}} \mathbf{f}'(t) dt \in \Omega_{A_Q}^1$$

ainsi un paramètre local sur A_Q est t et l'application $\Pi^\# : \text{Spec}(A) \rightarrow \text{Spec}(k[t])$, est non ramifiée. Si $y \in Q$ (i.e. $Q \in V(y)$) alors $Q \in D(f')$ et il existe α_{i_0} tel que

$$\Pi(Q) = k[t] \cap Q = (t - \alpha_{i_0})k[t].$$

Alors $\Omega_{A_Q}^1 = A_Q dt \oplus A_Q dy / (ny^{n-1}dy - \mathbf{f}'(t)dt)$. Considérons $k(Q) = A_Q/Q$ le corps résiduel de Q , alors $k(Q) \otimes \Omega_{A_Q}^1 = k(Q)dt \oplus k(Q)dy / \mathbf{f}'(t)dt$ car $y = 0$ dans $k(Q)$. Mais on a $\mathbf{f} \wedge \mathbf{f}' = 1$ sur $k[t]$ (voir lemme 2.1.1) donc $\mathbf{f}'(t)$ est inversible et un paramètre local sur A_Q est y . Pour conclure il faut donc exprimer $t - \alpha_{i_0}$ en fonction de y dans A_Q car $t - \alpha_{i_0}$ est un paramètre local en le point fermé α_{i_0} de $\text{Spec}(k[t])$. On sait que

$$y^n = (t - \alpha_{i_0}) \prod_{\substack{i=0 \\ i \neq i_0}}^l (t - \alpha_i)$$

et comme le produit de droite est non nul en α_{i_0} , il est inversible, d'inverse h , dans A_Q . On a alors $t - \alpha_{i_0} = y^n \cdot h$ où h est un inversible de A_Q . La valuation de $t - \alpha_i$ est donc n et l'application $\Pi^\# : \text{Spec}(A) \rightarrow \text{Spec}(k[t])$, est ramifiée, d'indice de ramification n .

D'autre part il est clair que $k(M_i) = k[t, y]/(y^n - f(t), y, (t - \alpha_i)) \simeq k$, ce qui achève la démonstration. □

Proposition 3.3.2. *Supposons tous les α_i non nuls dans k , alors la courbe affine W_k (respectivement W_K) est ramifiée en les $l + 1$ points fermés correspondant aux idéaux maximaux $N_i = (1 - \alpha_i s)\mathcal{O}_{W_k}(W_k) + z\mathcal{O}_{W_k}(W_k)$ et $\infty = s\mathcal{O}_{W_k}(W_k) + z\mathcal{O}_{W_k}(W_k)$ (respectivement aux idéaux $N_i = (1 - \alpha_i s)\mathcal{O}_{W_K}(W_K) + z\mathcal{O}_{W_K}(W_K)$ et $\infty = s\mathcal{O}_{W_K}(W_K) + z\mathcal{O}_{W_K}(W_K)$) où α_i désigne la classe de α_i dans k . De plus les corps résiduels $k(N_i)$ et $k(\infty)$ (resp. $K(N_i)$ et $K(\infty)$) sont égaux à k (resp. K).*

Preuve: La démonstration sur W_k (et donc sur W_K) utilise les mêmes arguments que ceux de la proposition précédente. □

Remarque 3.3.1. Remarquons que si l'un des α_i est nul (resp. multiple de p) alors il n'y a non pas $l + 1$ mais seulement l points de ramification sur W_k et W_K (resp. W_k) car l'un des facteurs du polynôme $f_2(s)$ (resp. $\mathbf{f}_2(s)$) vaut en fait 1. Toutefois cela ne change rien au nombre de points de ramification sur X_k et X_K qui est énoncé dans la propositions suivante. Par ailleurs nous allons utiliser cette hypothèse plus loin, ce qui justifie le choix de l'énoncé précédent.

Proposition 3.3.3. *Notons α_i la classe de α_i dans k . Alors la courbe X_k (resp. X_K) est ramifiée en les $l + 1$ points fermés correspondant aux idéaux maximaux*

$$M_i = (t - \alpha_i)\mathcal{O}_{U_k}(U_k) + y\mathcal{O}_{U_k}(U_k) \text{ et } \infty = s\mathcal{O}_{W_k}(W_k) + z\mathcal{O}_{W_k}(W_k)$$

(resp. $M_i = (t - \alpha_i)\mathcal{O}_{U_K}(U_K) + y\mathcal{O}_{U_K}(U_K)$ et $\infty = s\mathcal{O}_{W_K}(W_K) + z\mathcal{O}_{W_K}(W_K)$). De plus les corps résiduels $k(M_i)$ et $k(\infty)$ (resp. $K(M_i)$ et $K(\infty)$) sont égaux à k (resp. K).

Preuve: C'est une synthèse des résultats des propositions 3.3.1 et 3.3.2. □

3.4 Calcul du genre

Proposition 3.4.1. *On conserve les notations précédentes. Les courbes X_k et X_K sont de même genre, g où*

$$g = \frac{(l-1)(n-1)}{2} = \frac{rn(n-1)}{2} - (n-1)$$

on définit donc le genre de la courbe X comme étant g (voir remarque 1.0.1).

Preuve: Grâce à ce qui précède, on sait que les courbes X_k et X_K sont lisses (voir proposition 3.2.1) or une courbe lisse est normale. De plus on a vu que $\Pi_K : X_K \rightarrow \mathbb{P}_K^1$ est un morphisme fini séparable de degré n , de même pour et $\Pi_k : X_k \rightarrow \mathbb{P}_k^1$ (voir proposition 2.1.2). Les conditions d'application du théorème d'Hurwitz (1.0.1) sont donc vérifiées.

Commençons par calculer le genre de X_K . Comme K est de caractéristique nulle X_K est modérément ramifiée. Par ailleurs en les points où la courbe est ramifiée, le degré de ramification est n . Pour un point x de X_k on a donc $e_x = 1$ ou $e_x = n$ mais lorsque $e_x = n$ on a $[K(x) : K] = 1$ (proposition 3.3.3), ainsi la formule d'Hurwitz donne $2g(X_K) - 2 = n(2g(\mathbb{P}_K^1) - 2) + \sum_{\alpha_i} (e_{\alpha_i} - 1)$. Or $g(\mathbb{P}_K^1) = 0$ et la somme contient $l + 1$ termes, on a donc $2g(X_K) = (l + 1)(n - 1) - 2(n - 1)$ d'où les deux égalités voulues puisque par ailleurs $l + 1 = rn$.

Pour le genre de X_k le raisonnement et les calculs sont les mêmes. En effet comme on a supposé que $n \wedge p = 1$ il n'y a pas de ramification sauvage pour X_k et à nouveau en les points où e_x est différent de 1 on a $[k(x) : k] = 1$ et on obtient à nouveau avec le théorème d'Hurwitz $2g(X_k) = (l + 1)(n - 1) - 2(n - 1)$ et donc $g(X_k)$ et $g(X_K)$ sont égaux.

□

Remarque 3.4.1. Si on fixe $n = 2$ on retrouve bien $r = g + 1$ valeur donnée par Liu ([Liu02] 7.4.3.).

Chapitre 4

Une base de $H^0(X, \Omega_X^1)$

4.1 Calcul de la base

Notation. On appelle point à l'infini le point de W_K (resp. W_k) correspondant à l'idéal engendré par s et z dans $K[s, z]/(z^n - f_2(s))$ (resp. $k[s, z]/(z^n - \mathbf{f}_2(s))$). De même il y a une section à l'infini définie par l'idéal premier engendré par s et z dans $V[s, z]/(z^n - f_2(s))$. Ceci définit un diviseur que l'on notera ∞

Théorème 4.1.1. *Le V -module $H^0(X, \Omega_X^1)$ est libre de rang g et admet pour base la famille*

$$\omega_{i,j} = \frac{t^i dt}{y^j} \text{ avec } 1 \leq j \leq n-1 \text{ et } 0 \leq i \leq rj-2$$

où pour mémoire $r = (l+1)/n$.

Preuve: Montrons d'abord que la famille $\omega_{i,j}$, $1 \leq j \leq n-1$, $0 \leq i \leq rj-2$ est une base de $H^0(X_K, \Omega_{X_K}^1)$. Comme X_K est propre et lisse (proposition 3.2.1) alors le faisceau $\Omega_{X_K}^1$ est localement libre et $H^0(X_K, \Omega_{X_K}^1)$ est un K -espace vectoriel de dimension finie. Par ailleurs le fait qu'il soit de dimension g est un résultat découlant directement du théorème de Riemann-Roch. Montrer que la famille $\omega_{i,j}$ est une famille d'éléments de $H^0(X_K, \Omega_{X_K}^1)$ revient à montrer que pour tout Q point de X_K , $v_Q(\omega_{i,j}) \geq 0$ (avec les notations de la section 3.1). Par ailleurs il est clair au vu de la démonstration de la lissité que $U_K = D(y) \cup D(f')$ et donc qu'un point de X_K est soit un point de $D(y)$, soit un point de ramification (contenu dans $D(f')$). Il est clair que $\omega_{i,j} \in \Omega_{X_K}^1(U_K \cap D(y))$ (sans condition sur j et avec $i \geq 0$) il n'y a donc plus qu'à considérer le cas où Q est un point de ramification de la courbe.

Si $Q \in V(y) \subset D(f')$ est un point de ramification de U_K , i.e si $\Pi_K(Q) = (t - \alpha_i)K[t]$ avec $\alpha \in \{\alpha_1, \dots, \alpha_l\}$, un paramètre local en Q est y (voir 3.3.1) il faut donc commencer par exprimer $\omega_{i,j}$ selon dy . Or on a la relation $y^n = f(t)$ donc $ny^{n-1}dy = f'(t)dt$ et on peut exprimer $\omega_{i,j}$ sur $D(f')$ par la formule

$$\omega_{i,j} = \frac{t^i y^{n-1-j}}{f'(t)} dy$$

alors $v_Q(\omega_{i,j}) = iv_Q(t) + (n-1-j)v_Q(y) - v_Q(f'(t)) = iv_Q(t) + n-1-j$. En effet $t = t - \alpha_i + \alpha_i$ donc $f'(t)$ est inversible dans A_Q . Si α_i est non nul alors $v_Q(t) = 0$, sinon $v_Q(t) = n$. Dans tous les cas pour $1 \leq j \leq n-1$ et $0 \leq i$ il est clair que $v_Q(\omega_{i,j}) \geq 0$.

Si maintenant Q est le point à l'infini défini précédemment, $\Pi_K(Q) = sK[s]$ et un paramètre local en Q est z . Il faut donc exprimer $\omega_{i,j}$ selon s, z et dz . On utilise les formules $t = 1/s$ et $y = s^{-r}z$ où pour mémoire $r = (l+1)/n$. On a alors

$$\omega_{i,j} = -\frac{s^{rj-2-i}}{z^j} ds = -ns^{rj-2-i} z^{n-1-j} dz$$

et $v_Q(\omega_{i,j}) = n(rj-2-i) + (n-1-j)$. Mais comme $i \leq rj-2$ et $j \leq n-1$ alors $v_Q(\omega_{i,j}) \geq 0$, ce qui achève de montrer que la famille considérée est une famille de $H^0(X_K, \Omega_{X_K}^1)$. Pour montrer que cette famille de $H^0(X_K, \Omega_{X_K}^1)$ est linéairement indépendante sur K , il suffit de montrer qu'elle l'est en restriction à $U_K \cap D(y)$. Or $\Omega_{X_K}^1(U_K \cap D(y))$ est un $\mathcal{O}_{X_K}(U_K \cap D(y))$ -module libre de base dt . Plus précisément $\Omega_{X_K}^1(U_K \cap D(y)) \simeq \bigoplus_{i=0}^{l-1} K[y, y^{-1}]t^i dt$. Alors en restriction à $U_K \cap D(y)$ les $\omega_{i,j}$ forment un K -module libre et la famille est donc libre dans $H^0(X_K, \Omega_{X_K}^1)$. Pour conclure il suffit de montrer qu'elle contient g éléments pour montrer que c'est une base de $H^0(X_K, \Omega_{X_K}^1)$. Or elle contient :

$$\sum_{j=1}^{n-1} (rj-1) = r \sum_{j=1}^{n-1} j - (n-1) = r \frac{(n-1)n}{2} - (n-1) = g$$

éléments, c'est donc bien une base du K -espace vectoriel considéré.

En ce qui concerne X , puisque c'est une courbe lisse (proposition 3.2.1), Ω_X^1 est localement libre et comme de plus X est propre $H^0(X, \Omega_X^1)$ est un V -module libre de rang fini. Mais $K \otimes_V H^0(X, \Omega_X^1) \simeq H^0(X_K, \Omega_{X_K}^1)$ car K est un V -module plat et donc $H^0(X, \Omega_X^1)$ est de rang g . Posons alors $M = \bigoplus V\omega_{i,j} = \bigoplus Vt^i y^{-j} dt$ avec $1 \leq j \leq n-1$ et $0 \leq i \leq rj-2$. Il est clair que $M \subset \Omega_X^1(U \cap D(y))$. De plus $M \otimes K \simeq \bigoplus K\omega_{i,j} \simeq H^0(X_K, \Omega_{X_K}^1)$ et M est donc un réseau de $H^0(X_K, \Omega_{X_K}^1)$. Pour conclure à l'aide du lemme 2.3 de [HW15] montrons que $\Omega_X^1(U \cap D(y))/M$ est sans torsion. Or $U \cap D(y) = \text{Spec}(V[t, y, y^{-1}]/(y^n - f(t)))$ on a donc $\Omega_X^1(U \cap D(y)) \simeq V[t, y, y^{-1}]/(y^n - f(t))dt$ et comme f est de degré l

$$\Omega_X^1(U \cap D(y)) \simeq \bigoplus_{i=0}^{l-1} V[y, y^{-1}]t^i dt. \quad (4.1)$$

Par ailleurs la puissance de t maximale apparaissant dans un $\omega_{i,j}$ est donnée par $j = n-1$ et $i = rj-2$ elle vaut donc $r(n-1)-2 = (l+1)(n-1)/n - 2 < l+1-2 = l-1$ et il est alors clair au vu de ce qui précède que $\Omega_X^1(U \cap D(y))/M$ est sans torsion. Ainsi $M = H^0(X, \Omega_X)$ ce qui achève la démonstration. \square

Proposition 4.1.1. *Le k -espace vectoriel $H^0(X_k, \Omega_{X_k}^1)$ est de dimension g et admet pour base la famille*

$$\omega_{i,j} = \frac{t^i dt}{y^j} \text{ avec } 1 \leq j \leq n-1 \text{ et } 0 \leq i \leq rj-2$$

où pour mémoire $r = (l + 1)/n$.

Preuve: Dans la démonstration précédente on établit que la famille $\omega_{i,j} = t^i dt/y^j$ où $1 \leq j \leq n-1$ et $0 \leq i \leq rj - 2$, $r = (l + 1)/n$, est une base de $H^0(X_K, \Omega_{X_K}^1)$. On montrerait de la même manière que c'est une base de $H^0(X_k, \Omega_{X_k}^1)$. □

Lemme 4.1.1. *On conserve les notations du théorème précédent. Alors*

$$(i) \Omega_X^1(U \cap D(y)) = H^0(X, \Omega_X^1) \oplus \left(\bigoplus_{i=0}^{l-1} V[y]t^i dt \oplus \bigoplus_{j \geq n} \bigoplus_{i=0}^{l-1} y^{-j} t^i dt \oplus \bigoplus_{j=1}^{n-1} \bigoplus_{i=rj-1}^{l-1} y^{-j} t^i dt \right)$$

$$(ii) \Omega_X^1(W) = H^0(X, \Omega_X^1) \oplus \left(V[s]ds \oplus \bigoplus_{j=1}^{n-1} \bigoplus_{i \geq rj-1} V s^i z^{-j} ds \right)$$

(iii) *Les énoncés analogues sont vrais sur X_k .*

Preuve: A la fin de la démonstration du théorème 4.1.1 on a établi que

$$\Omega_X^1(U \cap D(y)) \simeq \bigoplus_{i=0}^{l-1} V[y, y^{-1}]t^i dt$$

ce qui donne immédiatement la décomposition en somme directe du (i). Par ailleurs il est clair qu'on pourrait montrer de la même manière que

$$\Omega_{X_k}^1(U_k \cap D(y)) \simeq \bigoplus_{i=0}^{l-1} k[y, y^{-1}]t^i dt$$

et donc donner un résultat analogue sur $\Omega_{X_k}^1(U_k \cap D(y))$. En ce qui concerne le résultat sur $\Omega_X^1(W)$ commençons par montrer qu'il est libre, engendré par

$$-\omega_{r(n-1)-2, n-1} = -\frac{t^{r(n-1)-2} dt}{y^{n-1}} = \frac{ds}{z^n}$$

la dernière égalité étant évidente au vu des conditions de recollement. Dans $\Omega_X^1(W)$ on a la relation $nz^{n-1}dz - f_2'(s)ds = 0$, de plus comme X est lisse on a $W = D(z) \cup D(f_2'(s))$. Il est clair que $\omega_{r(n-1)-2, n-1} \in \Omega_X^1(W \cap D(z))$ et que $\Omega_X^1(W \cap D(z))$ est engendré par

$$ds = z^{n-1}(-\omega_{r(n-1)-2, n-1})$$

donc aussi par $(-\omega_{r(n-1)-2, n-1})$ le faisceau $\Omega_X^1(W \cap D(f_2'(s)))$ est quant à lui engendré par

$$dz = \frac{-1}{n} f_2'(s) \omega_{r(n-1)-2, n-1}$$

et donc aussi par $(-\omega_{r(n-1)-2, n-1})$ ce qui montre notre affirmation. De plus on a

$$\mathcal{O}_X(W) = V[s, z]/(z^n - f_2(s)) = \bigoplus_{j=0}^{n-1} V[s]z^j$$

4.2. DÉCOMPOSITION DE $H^0(X, \Omega_X^1)$ EN COMPOSANTES ISOTYPIQUES

et comme $\Omega_X^1(W)$ est libre engendré par $(-\omega_{r(n-1)-2, n-1})$ on a

$$\Omega_X^1(W) = \bigoplus_{j=0}^{n-1} V[s]z^j \frac{ds}{z^{n-1}} = \bigoplus_{j=0}^{n-1} V[s] \frac{ds}{z^j}$$

mais on a montré que

$$H^0(X, \Omega_X^1) = \bigoplus_{j=1}^{n-1} \bigoplus_{i=0}^{rj-2} V \frac{t^i dt}{y^j} = \bigoplus_{j=1}^{n-1} \bigoplus_{i=0}^{rj-2} V \frac{-s^{rj-2-i} ds}{z^j} = \bigoplus_{j=1}^{n-1} \bigoplus_{i=0}^{rj-2} V \frac{s^i ds}{z^j}$$

ce qui donne bien la décomposition en somme directe annoncée. Enfin puisque k est de caractéristique p avec $p \wedge n = 1$ tout ce qui a été fait peut s'appliquer à $\Omega_{X_k}^1(W_k)$ et donne donc un énoncé analogue sur X_k . □

4.2 Décomposition de $H^0(X, \Omega_X^1)$ en composantes isotypiques

Théorème 4.2.1. *Avec les notations précédentes, on a*

$$H^0(X, \Omega_X^1) = \bigoplus_{j=1}^{n-1} \bigoplus_{i=0}^{rj-2} V \frac{t^i dt}{y^j}.$$

Supposons maintenant que $\mu_n(\overline{\mathbb{F}}_p) \subset k$, alors si on note $\mathcal{D}_j = H^0(X, \Omega_X^1)_j$ la j -ième composante isotypique associée à l'action δ décrite dans le paragraphe 2.2 on a :

$$\mathcal{D}_0 = 0$$

$$\mathcal{D}_j = \bigoplus_{i=0}^{rj-2} V \frac{t^i dt}{y^j} \quad \forall 1 \leq j \leq n-1.$$

Preuve: C'est une conséquence immédiate du théorème 4.1.1 et de la définition de l'action δ définie à la section 2.2. □

Chapitre 5

Calcul d'une base de $H_{DR}^1(X)$

5.1 Dégénérescence de la suite spectrale

Soit X une courbe lisse sur $\text{Spec}(V)$. Elle vérifie les conditions de Mazur explicitées dans l'appendice de [Maz73b] si :

$$\forall i \in \{0, 1\}, \forall j \in \{0, 1\}, H^i(X, \Omega_X^j) \text{ est un } V\text{-module libre.}$$

Si ces conditions sont vérifiées alors la suite spectrale de Hodge vers de Rham dégénère.

Proposition 5.1.1. *Soit X la courbe définie précédemment, réunion des deux ouverts affines U et W où*

$$\begin{aligned} U &= \text{Spec}(V[t, y]/(y^n - f(t))) \\ W &= \text{Spec}(V[s, z]/(z^n - f_2(s))) \end{aligned}$$

alors la suite spectrale de Hodge vers de Rham dégénère.

Preuve: On a déjà montré que la courbe X était lisse (voir proposition 3.2.1). Il s'agit donc de vérifier que la condition de Mazur explicitée plus haut est vérifiée. Comme $X \rightarrow \text{Spec}(V)$ est plat, $H^0(X, \mathcal{O}_X)$ est un V -module de type fini sans torsion donc est un V -module libre. Par ailleurs X_K est une courbe projective lisse donc $H^0(X_K, \mathcal{O}_K) = K$ (voir [Liu02] 2.3.1) et $H^0(X, \mathcal{O}_X) = V$. On a vu au théorème 4.1.1 que $H^0(X, \Omega_X^1)$ est un V -module libre et par dualité de Poincaré $H^1(X, \mathcal{O}_X)$ est donc un V -module libre. Par dualité de Serre ([Har77] III.7) $H^1(X, \Omega_X^1)$ est le dual de $H^0(X, \Omega_X^1)$ et c'est donc également un V -module libre. Les conditions de Mazur sont donc vérifiées et la suite spectrale de Hodge vers de Rham dégénère. □

5.2 Calcul des sections globales de $H^0(X, \mathcal{O}_X((2g-1)\infty))$

On suppose désormais jusqu'à la fin de ce chapitre que $\mu_n(\overline{\mathbb{F}}_p) \subset k$ et on réalise un parallèle avec ce qui est fait dans le troisième paragraphe de [HW15].

Proposition 5.2.1. *Soit $m \in \mathbb{N}$ tel que $m \geq 2g - 1$. Le V -module $H^0(X, \mathcal{O}_X(m\infty))$ est libre de rang $m + 1 - g$. De plus pour $m \geq 2g - 1$ une base de $H^0(X, \mathcal{O}_X(m\infty))$ est donnée par*

$$t^i y^j, 0 \leq j \leq n - 1 \text{ et } 0 \leq i \leq \left\lfloor \frac{m + j}{n} \right\rfloor - jr$$

où $r = (l + 1)/n$.

Preuve: Comme pour la démonstration du théorème 4.1.1 il va d'abord falloir montrer le résultat analogue dans le cas de la courbe X_K . Pour $m \geq 2g - 1$ la formule de Riemann-Roch donne que $\dim(H^0(X, \mathcal{O}_X(m\infty))) = m + 1 - g$. Ceci permet de conclure à la première affirmation de la proposition en utilisant les mêmes arguments que dans la démonstration du théorème 4.1.1.

Vérifions que les éléments considérés sont des sections globales du module $H^0(X_K, \mathcal{O}_{X_K}(m\infty))$. Il est évident que ce sont des sections sur U_K pour $0 \leq i, j$ et ce sont des sections globales si ce sont des sections en l'infini i.e. si leur valuation en z est supérieure ou égale à $-m$. En effet si O est un ouvert affine tel que $\infty \in O$ alors $\mathcal{O}_{O, \infty}$ est un anneau local régulier, de dimension 1 et de paramètre z (voir la démonstration de 3.3.2). Commençons donc par exprimer t et y en fonction de z et s . On a le formulaire suivant :

$$\begin{cases} s = t^{-1} \\ z = s^r y \\ z^n = s R_1(s) \\ t = \frac{R_1(s)}{z^n} \end{cases}$$

avec $r = (l + 1)/n$ et R_1 est un polynôme en s dont 0 n'est pas racine. On a donc

$$t^i y^j = \frac{R_1(s)^{i+rj}}{z^{n(i+rj)-j}}$$

et comme 0 n'est pas racine de $R_1(s)$ alors $v_z(R_1(s)) = 0$ donc

$$v_z(t^i y^j) \geq -m \Leftrightarrow -n(i + rj) + j \geq -m \Leftrightarrow i \leq \frac{m - j(rn - 1)}{n}$$

ce qui donne la condition sur i annoncée puisque i est entier.

Il est clair que les $t^i y^j$ forment une famille libre de l'espace dès que $0 \leq j \leq n - 1$, il reste donc à vérifier que la famille \mathcal{F} considérée (i.e. en prenant les conditions $0 \leq j \leq n - 1$ et $0 \leq i \leq \lfloor (m + j)/n \rfloor - jr$) est bien une famille à $m + 1 - g$ éléments.

$$\#\mathcal{F} = \sum_{j=0}^{n-1} \left(1 - jr + \left\lfloor \frac{m + j}{n} \right\rfloor \right) = n - \frac{rn(n-1)}{2} + \sum_{j=0}^{n-1} \left\lfloor \frac{m + j}{n} \right\rfloor = 1 - g + \sum_{j=0}^{n-1} \left\lfloor \frac{m + j}{n} \right\rfloor$$

il suffit donc de vérifier que la somme, notée S , vaut bien m . Effectuons la division euclidienne de m par n . On a $m = an + b$ avec $0 \leq b \leq n - 1$ donc $m + j = an + b + j$ avec $0 \leq b + j \leq 2n - 1 < 2n$. Alors pour $0 \leq j \leq n - 1 - b$, $\lfloor (j + b)/n \rfloor = 0$ et pour $n - b \leq j \leq n - 1$, $\lfloor (j + b)/n \rfloor = 1$. Dans S il y a donc $n - b$ termes valant a et b termes valant $a + 1$. D'où $S = a(n - b) + (a + 1)b = an + b = m$

et $\#\mathcal{F} = m + 1 - g$. On a donc une base de $H^0(X_K, \mathcal{O}_{X_K}(m\infty))$. Par ailleurs $\mathcal{O}_{X_K}(m\infty)$ étant localement libre sur X alors le module $H^0(X, \mathcal{O}_X(m\infty))$ est un V -module libre de rang fini et on conclut en utilisant le lemme 2.3 de [HW15]. \square

Proposition 5.2.2. *Notons $k_j = r(n - j - 1) - 2$ où $r = (l + 1)/n$, alors :*

$$H^0(X, \mathcal{O}_X((2g - 1)\infty)) = \bigoplus_{j=0}^{n-2} \bigoplus_{i=0}^{k_j} Vt^i y^j.$$

Preuve: Tout d'abord remarquons que l'espace considéré correspond au cas particulier $m = 2g - 1$ de la proposition précédente. On sait donc qu'une base de l'espace est donnée par $t^i y^j$ avec $0 \leq j \leq n - 1$ et $0 \leq i \leq \lfloor (2g - 1 + j)/n \rfloor - jr$. Or $2g = rn(n - 1) - 2(n - 1)$ (voir proposition 3.4.1) d'où $\lfloor (2g - 1 + j)/n \rfloor - jr = r(n - j - 1) - 2 + \lfloor (j + 1)/n \rfloor$ cette dernière partie entière valant 0 dès que $j \neq n - 1$ et 1 sinon.

Pour $j = n - 1$ la condition sur i devient $0 \leq i \leq r(n - (n - 1) - 1) - 2 + 1 = -1$ il n'y a donc aucun élément du type $t^i y^{n-1}$ dans notre espace. Ce qui donne finalement la condition $0 \leq j \leq n - 2$ et $0 \leq i \leq r(n - j - 1) - 2 = k_j$ d'où la décomposition en somme directe. \square

Proposition 5.2.3. *La décomposition de $H^0(X, \mathcal{O}_X((2g - 1)\infty))$ en sous-espaces par l'action δ définie à la section 2.2 est donnée par :*

$$H^0(X, \mathcal{O}_X((2g - 1)\infty))_0 = \bigoplus_{i=0}^{r(n-1)-2} Vt^i,$$

$$H^0(X, \mathcal{O}_X((2g - 1)\infty))_1 = 0,$$

$$H^0(X, \mathcal{O}_X((2g - 1)\infty))_j = \bigoplus_{i=0}^{r(j-1)-2} Vt^i y^{n-j} \quad \forall 2 \leq j \leq n - 1$$

où $r = (l + 1)/n$.

Preuve: On rappelle que l'action δ est donnée par $t \mapsto t$ et $y \mapsto [\zeta]^{-1}y$ avec $([\zeta]^{-1})^n = 1$. De plus en effectuant le changement de variable $j = n - j$ dans la décomposition en somme directe donnée dans la proposition 5.2.2 on obtient :

$$H^0(X, \mathcal{O}_X((2g - 1)\infty)) = \bigoplus_{i=0}^{r(n-1)-2} Vt^i \oplus \bigoplus_{j=2}^{n-1} \bigoplus_{i=0}^{r(j-1)-2} Vt^i y^{n-j}$$

d'où le résultat. \square

5.3 Calcul des sections globales de $H^0(X, \Omega_X^1(2g\infty))$

Proposition 5.3.1. *On a une suite exacte longue de cohomologie :*

$$0 \rightarrow H^0(X, \Omega_X^1) \rightarrow H^0(X, \Omega_X^1(2g\infty)) \rightarrow \bigoplus_{i=1}^{2g} Vz^{-i}dz \rightarrow V \rightarrow 0.$$

Preuve: Considérons la suite exacte courte $0 \rightarrow \Omega_X^1 \rightarrow \Omega_X^1(2g\infty) \rightarrow \Omega_X^1(2g\infty)/\Omega_X^1 \rightarrow 0$ et notons $\mathcal{M} = \Omega_X^1(2g\infty)/\Omega_X^1$. Soit maintenant \mathcal{U} un ouvert contenant ∞ , muni d'une coordonnée z . Alors $\Omega_{\mathcal{U}}^1 \simeq \mathcal{O}_{\mathcal{U}}dz$ et $\Omega_{\mathcal{U}}^1(2g\infty) \simeq z^{-2g}\mathcal{O}_{\mathcal{U}}dz$ d'où

$$\Omega_{\mathcal{U}}^1(2g\infty)/\Omega_{\mathcal{U}}^1 \simeq z^{-2g}\mathcal{O}_{\mathcal{U}}dz/\mathcal{O}_{\mathcal{U}}dz$$

donc $\mathcal{M}_{\mathcal{U}} = z^{-2g}\mathcal{O}_{\mathcal{U}}dz/\mathcal{O}_{\mathcal{U}}dz$ et \mathcal{M} est un faisceau à support en ∞ . De plus \mathcal{M} est cohérent, c'est donc un $\mathcal{O}_{\mathcal{U}}/z\mathcal{O}_{\mathcal{U}}$ -module de type fini et comme $\mathcal{O}_{\mathcal{U}}/z\mathcal{O}_{\mathcal{U}} \simeq i_*V$, avec $i : \infty \hookrightarrow \mathcal{U}$, alors \mathcal{M} est un i_*V -module de type fini et $\mathcal{M} = i_*M$ ne dépend pas du choix de $\mathcal{U} \ni \infty$. D'où

$$\mathcal{M} = i_* \left(\varinjlim_{\mathcal{U} \ni \infty} \mathcal{M}(\mathcal{U}) \right) = z^{-2g}\mathcal{O}_{X,\infty}dz/\mathcal{O}_{X,\infty}dz$$

et on a la suite exacte courte

$$0 \rightarrow \Omega_X^1 \rightarrow \Omega_X^1(2g\infty) \rightarrow z^{-2g}\mathcal{O}_{X,\infty}dz/\mathcal{O}_{X,\infty}dz \rightarrow 0$$

qui donne la suite exacte longue de cohomologie suivante :

$$\begin{aligned} 0 \rightarrow H^0(X, \Omega_X^1) \rightarrow H^0(X, \Omega_X^1(2g\infty)) \rightarrow H^0(X, \mathcal{M}) \rightarrow H^1(X, \Omega_X^1) \\ \rightarrow H^1(X, \Omega_X^1(2g\infty)) \rightarrow H^1(X, \mathcal{M}) \rightarrow 0. \end{aligned}$$

Tout d'abord, comme \mathcal{M} est à support ponctuel, $H^i(X, \mathcal{M}) = 0$ dès que $i \neq 0$ de plus X est une courbe relative donc $H^i(X, \Omega_X^1) = 0$ et $H^i(X, \Omega_X^1(2g\infty)) = 0$ dès que $i \geq 2$. Par dualité de Poincaré, $H^1(X, \Omega_X^1(2g\infty)) \simeq H^0(\mathcal{O}_X(-2g\infty) \otimes \Omega_X^{1V} \otimes \Omega_X^1)$ or $\Omega_X^{1V} \otimes \Omega_X^1 \simeq \mathcal{O}_X$ donc $H^1(X, \Omega_X^1(2g\infty)) \simeq H^0(\mathcal{O}_X(-2g\infty))$. Comme $D = -2g\infty$ est un diviseur de degré strictement négatif, aucun diviseur effectif ne peut être linéairement équivalent à D et finalement $H^1(X, \Omega_X^1(2g\infty)) = 0$. Enfin $H^1(X, \Omega_X^1) \simeq V$. La suite exacte de cohomologie se réécrit donc

$$0 \rightarrow H^0(X, \Omega_X^1) \rightarrow H^0(X, \Omega_X^1(2g\infty)) \rightarrow H^0(X, \mathcal{M}) \rightarrow V \rightarrow 0.$$

Pour finir montrons que $H^0(X, \mathcal{M}) \simeq \bigoplus_{i=1}^{2g} Vz^{-i}dz$. Tout d'abord remarquons que

$$H^0(X, \mathcal{M}) = H^0(X, i_*M) = H^0(i^{-1}X, M) = H^0(\infty, M) = M = z^{-2g}\mathcal{O}_{X,\infty}dz/\mathcal{O}_{X,\infty}dz.$$

M est un A -module de type fini, où A est tel que $\infty = \text{Spec}(A)$, considérons \hat{M} le complété z -adique de M , alors $\hat{M} \simeq z^{-2g}V[[z]]dz/V[[z]]dz$ donc $\hat{M} \simeq \bigoplus_{i=1}^{2g} Vz^{-i}dz$. Pour conclure montrons que $M \simeq \hat{M}$. Or $M \twoheadrightarrow \hat{M}$ car $V[[z]] \subset \mathcal{O}_{X,\infty}$ et $z^{-2g}V[[z]]dz/V[[z]]dz \twoheadrightarrow z^{-2g}V[[z]]dz/V[[z]]dz \simeq \hat{M}$.

Calculons $N = Ker(M \rightarrow \hat{M})$; on a $N = \bigcap_{i \in \mathbb{N}} z^i M \subset M$ or il est clair que $zN \subset N$ et comme $M \cap zN = zN$ on a également $N \subset zN$ d'où $zN = N$ et d'après le lemme de Nakayama on en conclut que $N = 0$. Ainsi $M \hookrightarrow \hat{M}$ et donc M et \hat{M} sont isomorphes d'où la suite exacte de cohomologie annoncée. \square

Lemme 5.3.1. *La décomposition de $\bigoplus_{i=1}^{2g} Vz^{-i}dz$ en sous-espaces par l'action δ est donnée par :*

$$\begin{aligned} \left(\bigoplus_{i=1}^{2g} Vz^{-i}dz \right)_0 &= \bigoplus_{\alpha=0}^{r(n-1)-2} Vz^{-(1+\alpha n)}dz, \\ \left(\bigoplus_{i=1}^{2g} Vz^{-i}dz \right)_1 &= \bigoplus_{\alpha=0}^{r(n-1)-2} Vz^{-(2+\alpha n)}dz, \\ \left(\bigoplus_{i=1}^{2g} Vz^{-i}dz \right)_j &= \bigoplus_{\alpha=0}^{r(n-1)-3} Vz^{-(j+1+\alpha n)}dz \quad \forall 2 \leq j \leq n-1 \end{aligned}$$

où $r = (l+1)/n$.

Preuve: On rappelle que l'action de δ est donnée par $z \mapsto [\zeta]^{-1}z$ et $dz \mapsto [\zeta]^{-1}dz$ où $([\zeta]^{-1})^n = 1$. Soient $i \in \llbracket 1, 2g \rrbracket$ fixé et $\omega \in Vz^{-i}dz$, alors $\omega = v_0 z^{-i}dz$ d'où $\delta(\omega) = [\zeta]^{i-1}\omega$. Ainsi ω appartient à la j -ième composante isotypique associée à δ si et seulement si $i-1 \equiv j \pmod{n}$ i.e. si et seulement si $j+1-i = \alpha n$ avec $\alpha \in \mathbb{Z}$. On cherche maintenant la condition que doit satisfaire α . On sait que $1 \leq i \leq 2g$ donc $-j \leq -\alpha n \leq 2g-1-j$ d'où

$$\frac{-j}{n} \leq -\alpha \leq \frac{2g-1-j}{n}$$

mais $1 \leq j \leq n-1$ donc $-1 < -j/n \leq 0$ et comme α est entier, l'inégalité de gauche devient $0 \leq -\alpha$. De plus $2g = rn(n-1) - 2(n-1)$ donc $2g-1-j = rn(n-1) - 2n - j + 1$. Pour j valant 0 ou 1, $(1-j)/n$ vaut respectivement $1/n$ et 0 et dans ces deux cas l'inégalité de droite devient $-\alpha \leq r(n-1) - 2$. Dans le cas où $2 \leq j \leq n-1$ cette fois $0 > 1-j > -n$ et donc l'inégalité de droite devient $-\alpha \leq r(n-1) - 3$. Ainsi pour $j = 0, 1$, les valeurs prises par i sont les $1+j-\alpha n$ avec $0 \leq -\alpha \leq r(n-1) - 2$ et pour $2 \leq j \leq n-1$ les valeurs prises par i sont les $1+j-\alpha n$ avec $0 \leq -\alpha \leq r(n-1) - 3$ ce qui donne bien les espaces annoncés. \square

Lemme 5.3.2. *Soit $0 \leq j \leq n-1$, alors $t^i dt/y^j$ est une section globale de $H^0(X, \Omega_X^1(2g\infty))$ si et seulement si*

$$0 \leq i \leq r(n+j-1) - 3 + \left\lfloor \frac{1-j}{n} \right\rfloor$$

où $r = (l+1)/n$.

Preuve: On a vu dans la démonstration du théorème 4.1.1 qu'un tel élément est une section sur U_K dès que $0 \leq i$, c'est donc une section globale de $H^0(X_K, \Omega_{X_K}^1(2g\infty))$ si et seulement si c'est une section en l'infini. On commence donc par exprimer un tel élément en fonction de s et z . Comme $t = s^{-1}$ on a $dt = -s^{-2}ds$ de plus $y = s^{-r}z$, d'où

$$\frac{t^i dt}{y^j} = \frac{-s^{rj-i-2} ds}{z^{j-(n-1)} z^{n-1}}.$$

Par ailleurs le paramètre en ∞ est z , notons v_z la valuation en z . On a $nz^{n-1}dz = (sR_1(s))'ds$ avec $v_z((sR_1(s))') = 0$, ainsi l'élément considéré est une section globale sur $H^0(X_K, \Omega_{X_K}^1(2g\infty))$ si et seulement si

$$v_z \left(\frac{s^{rj-i-2}}{z^{j-(n-1)}} \right) \geq -2g.$$

On sait que $z^n = sR_1(s)$ et que $R_1(0) \neq 0$, c'est donc un inversible au voisinage de ∞ ainsi $v_z(s) = n$ et la condition devient $n(rj - i - 2) - j + (n - 1) = n(rj - 1 - i) - (j + 1) \geq -2g$ i.e. $i \leq rj - 1 + (2g - j - 1)/n$. Mais $2g = rn(n - 1) - 2(n - 1)$ donc l'inégalité devient $i \leq r(n + j - 1) - 3 + (1 - j)/n$ et comme i doit être entier, on trouve la condition annoncée sur i . Enfin comme le faisceau $\Omega_X^1(2g\infty)$ est localement libre sur X alors $H^0(X, \Omega_X^1(2g\infty))$ est un V -module libre et on conclut en utilisant à nouveau le lemme 2.3 de [HW15]. \square

Proposition 5.3.2. *Le V -module $H^0(X, \Omega_X^1(2g\infty))_0$ est libre de rang $r(n - 1) - 2$, de base :*

$$t^i dt, \quad \forall 0 \leq i \leq r(n - 1) - 3.$$

Preuve: Les éléments considérés sont bien des sections globales de $H^0(X, \Omega_X^1(2g\infty))$ en vertu du lemme 5.3.2. De plus il est évident que ce sont les seules sections globales invariantes par l'action de δ . Pour montrer que la famille est libre il suffit à nouveau de montrer qu'elle est libre en restriction à $U \cap D(y)$. Comme $U \cap D(y)$ est un ouvert ne contenant pas ∞ alors $\Omega_{U \cap D(y)}^1(2g\infty) = \Omega_{U \cap D(y)}^1$. Comme les sections considérées forment un sous- V -module libre de $(\Omega_{U \cap D(y)}^1)_0$ alors elles forment une famille libre, à $r(n - 1) - 2$ éléments de $H^0(X, \Omega_X^1(2g\infty))_0$. Posons

$$M = \bigoplus_{i=0}^{r(n-1)-3} t^i dt$$

c'est un V -module libre de $H^0(X, \Omega_X^1(2g\infty))_0$ qui est clairement de rang $r(n - 1) - 2$. Montrons que $H^0(X, \Omega_X^1(2g\infty))_0$ est également de rang $r(n - 1) - 2$. Pour cela on fait intervenir la suite exacte de cohomologie donnée dans la proposition 5.3.1. Par functorialité et par la proposition 2.2.2, l'action de δ sur cette suite exacte donne la suite exacte

$$0 \rightarrow H^0(X, \Omega_X^1)_0 \rightarrow H^0(X, \Omega_X^1(2g\infty))_0 \rightarrow \left(\bigoplus_{i=1}^{2g} V z^{-i} dz \right)_0 \rightarrow V_0 \rightarrow 0.$$

L'action sur V est triviale donc $V_0 = V$. On connaît une décomposition de $H^0(X, \Omega_X^1)$ en composantes isotypiques pour l'action de δ donnée par

$$H^0(X, \Omega_X^1) = \bigoplus_{j=0}^{n-1} \mathcal{D}_j$$

où les \mathcal{D}_j sont de dimension $d_j = rj - 1$ pour $1 \leq j \leq n - 1$ et 0 pour $j = 0$. Enfin le lemme 5.3.1 donne

$$\left(\bigoplus_{i=1}^{2g} Vz^{-i} dz \right)_0 = \bigoplus_{\alpha=0}^{r(n-1)-2} Vz^{-(1+\alpha n)} dz.$$

Finalement on a la suite exacte :

$$0 \rightarrow \mathcal{D}_0 \rightarrow H^0(X, \Omega_X^1(2g\infty))_0 \rightarrow \bigoplus_{\alpha=0}^{r(n-1)-2} Vz^{-(1+\alpha n)} dz \rightarrow V \rightarrow 0.$$

Pour finir ces modules étant des V -modules libres (ils sont sans torsion), la tensorisation de la suite exacte par K donne une suite exacte de K -espaces vectoriels à laquelle on peut appliquer le théorème du rang, ce qui permet finalement de calculer le rang du module cherché

$$rg(H^0(X, \Omega_X^1(2g\infty))_0) = 0 + (r(n-1) - 2 + 1) - 1 = r(n-1) - 2.$$

Enfin montrons que le quotient $H^0(U \cap D(y), \Omega_{U \cap D(y)}^1(2g\infty))_0 / M$ est sans torsion. Remarquons que $U \cap D(y)$ est un ouvert ne contenant par ∞ , ainsi

$$H^0(U \cap D(y), \Omega_{U \cap D(y)}^1(2g\infty))_0 = H^0(U \cap D(y), \Omega_{U \cap D(y)}^1)_0.$$

Par ailleurs on a établi dans la démonstration du théorème 4.1.1 la formule (4.1) dont on déduit clairement que

$$H^0(U \cap D(y), \Omega_{U \cap D(y)}^1)_0 = \bigoplus_{j \in n\mathbb{N}} \bigoplus_{i=0}^{l-1} t^i y^j dt$$

et comme $r(n-1) - 3 = l - 2 - 1/n < l - 1$ on en conclut que le quotient est sans p -torsion. Alors en vertu du (iii) du lemme 2.3 de [HW15] $M = H^0(X, \Omega_X^1(2g\infty))_0$ ce qui achève la démonstration. \square

Proposition 5.3.3. *Le V -module $H^0(X, \Omega_X^1(2g\infty))_1$ est libre de rang $rn - 2$, de base :*

$$\frac{t^i dt}{y}, \quad \forall 0 \leq i \leq rn - 3.$$

Preuve: A nouveau, ces éléments sont bien des sections globales de $H^0(X, \Omega_X^1(2g\infty))$ en vertu du lemme 5.3.2 et il est évident que ce sont les seules sections globales dans la première composante isotypique pour l'action δ . Enfin elles forment une famille libre à $rn - 2$ éléments pour les mêmes raisons que dans la démonstration précédentes. Posons

$$M = \bigoplus_{i=0}^{rn-3} t^i y^{-1} dt$$

c'est un V -module libre de $H^0(X, \Omega_X^1(2g\infty))_1$ de rang $rn - 2$. Pour conclure montrons que $H^0(X, \Omega_X^1(2g\infty))_1$ est de rang $rn - 2$ et que le quotient $H^0(U \cap D(y), \Omega_{U \cap D(y)}^1(2g\infty))_1/M$ est sans torsion. On fait à nouveau intervenir la suite exacte de cohomologie donnée dans la proposition 5.3.1. Par functorialité et par la proposition 2.2.2, l'action de δ sur cette suite exacte donne la suite exacte :

$$0 \rightarrow H^0(X, \Omega_X^1)_1 \rightarrow H^0(X, \Omega_X^1(2g\infty))_1 \rightarrow \left(\bigoplus_{i=1}^{2g} Vz^{-i} dz \right)_1 \rightarrow V_1 \rightarrow 0.$$

L'action sur V est triviale donc $V_1 = 0$. Comme précédemment $H^0(X, \Omega_X^1)_1 = \mathcal{D}_1$ où \mathcal{D}_1 est libre de rang $r - 1$. Enfin le lemme 5.3.1 donne

$$\left(\bigoplus_{i=1}^{2g} Vz^{-i} dz \right)_1 = \bigoplus_{\alpha=0}^{r(n-1)-2} Vz^{-(2+\alpha n)} dz.$$

Finalement on a la suite exacte :

$$0 \rightarrow \mathcal{D}_1 \rightarrow H^0(X, \Omega_X^1(2g\infty))_1 \rightarrow \bigoplus_{\alpha=0}^{r(n-1)-2} Vz^{-(2+\alpha n)} dz \rightarrow 0 \rightarrow 0.$$

A nouveau la tensorisation de la suite exacte par K donne une suite exacte de K -espaces vectoriels à laquelle on peut appliquer le théorème du rang, on en déduit

$$rg(H^0(X, \Omega_X^1(2g\infty))_1) = (r - 1) + (r(n - 1) - 2 + 1) - 0 = rn - 2.$$

Comme dans la démonstration précédente on utilise le fait que $U \cap D(y)$ ne contient pas ∞ ainsi que la formule (4.1) établie dans la démonstration du théorème 4.1.1 pour dire que

$$H^0(U \cap D(y), \Omega_{U \cap D(y)}^1(2g\infty))_1 = \bigoplus_{j \in n\mathbb{N}} \bigoplus_{i=0}^{l-1} t^i y^{j-1} dt$$

et comme $rn - 2 = l - 1$ on en conclut que le quotient par M est sans torsion et, à l'aide du (iii) du lemme 2.3 de [HW15], que $H^0(X, \Omega_X^1(2g\infty))_1 = M$. □

Proposition 5.3.4. *Soit $2 \leq j \leq n - 1$ fixé. Le V -module $H^0(X, \Omega_X^1(2g\infty))_j$ est libre de rang $r(n + j - 1) - 3$, de base :*

$$\frac{t^i dt}{y^j}, \quad \forall 0 \leq i \leq r(n + j - 1) - 4.$$

Preuve: Encore une fois, ces éléments sont des sections globales de $H^0(X, \Omega_X^1(2g\infty))$ en vertu du lemme 5.3.2 et il est évident que ce sont les seules sections globales dans la j -ième composante isotypique pour l'action δ . Enfin elles forment une famille libre, à $r(n + j - 1) - 3$ éléments toujours pour les raisons déjà évoquées. Posons alors

$$M_j = \bigoplus_{i=0}^{r(n+j-1)-4} t^i y^{-j} dt$$

qui est un V -module libre de rang $r(n+j-1) - 3$ de $H^0(X, \Omega_X^1(2g\infty))_j$. Pour conclure, comme dans les démonstrations précédentes, il s'agit de montrer que $H^0(X, \Omega_X^1(2g\infty))_j$ est de rang $r(n+j-1) - 3$ et que le quotient $H^0(U \cap D(y), \Omega_{U \cap D(y)}^1)_j / M_j$ est sans torsion. On fait encore intervenir la suite exacte de cohomologie donnée dans la proposition 5.3.1. Par functorialité et par la proposition 2.2.2, l'action de δ sur cette suite exacte donne la suite exacte

$$0 \rightarrow H^0(X, \Omega_X^1)_j \rightarrow H^0(X, \Omega_X^1(2g\infty))_j \rightarrow \left(\bigoplus_{i=1}^{2g} V z^{-i} dz \right)_j \rightarrow V_j \rightarrow 0.$$

L'action sur V est triviale donc $V_j = 0$. Comme avant $H^0(X, \Omega_X^1)_j = \mathcal{D}_j$ avec \mathcal{D}_j de rang $rj - 1$. Enfin le lemme 5.3.1 donne

$$\left(\bigoplus_{i=1}^{2g} V z^{-i} dz \right)_j = \bigoplus_{\alpha=0}^{r(n-1)-3} V z^{-(j+1+\alpha n)} dz.$$

Finalement on a la suite exacte

$$0 \rightarrow \mathcal{D}_j \rightarrow H^0(X, \Omega_X^1(2g\infty))_j \rightarrow \bigoplus_{\alpha=0}^{r(n-1)-3} V z^{-(j+1+\alpha n)} dz \rightarrow 0 \rightarrow 0.$$

Pour finir en tensorisant à nouveau par K on obtient

$$rg(H^0(X, \Omega_X^1(2g\infty))_1) = (rj - 1) + (r(n-1) - 3 + 1) - 0 = r(n+j-1) - 3.$$

Enfin pour conclure que la quotient est sans torsion il faut cette fois utiliser le fait que $y^n = f(t)$ et non plus $f(t) = y^n$ pour exprimer $\Omega_X^1(U \cap D(y)) \simeq V[t, y, y^{-1}]/(y^n - f(t))dt$. On obtient alors

$$\Omega_X^1(U \cap D(y)) = \bigoplus_{j=0}^{n-1} V[t, y^{-1}]y^j dt$$

qui permet d'affirmer que

$$H^0(U \cap D(y), \Omega_{U \cap D(y)}^1)_j = V[t]y^{-j} dt$$

et de conclure que le quotient est sans torsion, puis toujours à l'aide du (iii) du lemme 2.3 de [HW15] que $M = H^0(X, \Omega_X^1(2g\infty))_j$ ce qui achève la démonstration. \square

Proposition 5.3.5. *Avec les notations et les conditions précédentes,*

$$H^0(X, \Omega_X^1(2g\infty)) = \bigoplus_{i=0}^{r(n-1)-3} V t^i \oplus \bigoplus_{i=0}^{rn-3} V \frac{t^i dt}{y} \oplus \bigoplus_{j=2}^{n-1} \bigoplus_{i=0}^{r(n+j-1)-4} V \frac{t^i dt}{y^j}.$$

Preuve: C'est simplement une conséquence des résultats précédents. On sait par le théorème de Riemann-Roch que le K -espace vectoriel $H^0(X_K, \Omega_{X_K}^1(2g\infty))$ est de dimension $3g - 1$ et comme précédemment on en conclut que $H^0(X, \Omega_X^1(2g\infty))$ est un V -module libre de rang $3g - 1$. Il est clair par ce qui précède que l'espace de droite est inclus dans $H^0(X, \Omega_X^1(2g\infty))$, pour conclure montrons qu'ils sont de même rang. Notons R le rang de l'espace de droite, alors

$$R = (r(n-1) - 2) + (rn - 2) + \sum_{j=2}^{n-1} (r(n+j-1) - 3) = r(n-1) + rn - 4 + (rn-3)(n-2) + r \sum_{j=1}^{n-2} j$$

$$R = r(n-1) + rn(n-1) - 3(n-1) - 1 + \frac{r(n-2)(n-1)}{2} = 3g - 1$$

car pour mémoire $g = rn(n-1)/2 - (n-1)$. □

5.4 Calcul de $H_{DR}^1(X)$

On conserve les notations précédentes et on applique la méthode de Huyghe-Wach ([HW15]). Notons C le complexe de de Rham :

$$C : 0 \longrightarrow \mathcal{O}_X \longrightarrow \Omega_X^1 \longrightarrow 0.$$

Par définition, la cohomologie de de Rham de X est la cohomologie du complexe $R\Gamma(X, C)$. Si on considère D un diviseur relatif effectif de X et m un entier, notons $C(mD)$ le complexe de de Rham twisté de X :

$$C(mD) : 0 \longrightarrow \mathcal{O}_X((m-1)D) \longrightarrow \Omega_X^1(mD) \longrightarrow 0.$$

Proposition 5.4.1. *Notons z un paramètre de la courbe en ∞ . On a la suite exacte courte :*

$$0 \rightarrow V \rightarrow \text{Ker}(d) \rightarrow \text{Ker}(\Delta) \rightarrow H_{DR}^1(X) \rightarrow \text{Coker}(d) \rightarrow \text{Coker}(\Delta) \rightarrow V \rightarrow 0$$

où $d : \Gamma(\mathcal{O}_X((2g-1)\infty)) \rightarrow \Gamma(\Omega_X^1(2g\infty))$ et $\Delta : z^{-2g+1}V[[z]]/V[[z]] \rightarrow z^{-2g}V[[z]]/V[[z]]dz$ sont les différentielles usuelles.

Preuve: Tout d'abord, on a la suite exacte courte :

$$0 \longrightarrow C \longrightarrow C(2g\infty) \longrightarrow C(2g\infty)/C \longrightarrow 0$$

qui après application de $R\Gamma$ donne le triangle :

$$0 \longrightarrow R\Gamma(C) \longrightarrow R\Gamma(C(2g\infty)) \xrightarrow{+1} R\Gamma(C(2g\infty)/C)$$

et donc la suite exacte longue de cohomologie :

$$0 \rightarrow R^0\Gamma(C) \rightarrow R^0\Gamma(C(2g\infty)) \rightarrow R^0\Gamma(C(2g\infty)/C) \rightarrow R^1\Gamma(C) \rightarrow R^1\Gamma(C(2g\infty)) \\ \rightarrow R^1\Gamma(C(2g\infty)/C) \rightarrow R^2\Gamma(C) \rightarrow R^2\Gamma(C(2g\infty)) \rightarrow R^2\Gamma(C(2g\infty)/C) \rightarrow 0$$

car tous les termes $R^i\Gamma$ sont nuls pour $i \geq 3$. Par définition, $R^i\Gamma(C) = H_{DR}^i(X)$, de plus $H_{DR}^2(X) \simeq H^1(X, \Omega_X^1) = V$ et $H_{DR}^0(X) \simeq H^0(X, \mathcal{O}_X) = V$ par dégénérescence de la suite spectrale de Hodge vers de Rham. Par ailleurs, par dualité de Serre $H^1(X, \mathcal{O}_X(2g\infty))$ est le dual de $H^0(X, E)$ où $E = \mathcal{O}_X(-2g\infty) \otimes_{\mathcal{O}_X} \Omega_X^1$. Or E est localement libre donc $H^0(X, E)$ est sans torsion et on en déduit que $H^1(X, \mathcal{O}_X(2g\infty))$ est un V -module libre. On sait donc qu'il est nul si et seulement si la dimension de $H^1(X_K, \mathcal{O}_K(2g\infty)) = K \otimes H^1(X, \mathcal{O}_X(2g\infty))$ est nulle. Alors par [Har77] (IV.1, 1.3.2 et 1.3.3) $C(2g\infty)$ est à termes acycliques pour Γ donc

$$R\Gamma(C(2g\infty)) = 0 \rightarrow \Gamma(\mathcal{O}_X((2g-1)\infty)) \xrightarrow{d} \Gamma(\Omega_X^1(2g\infty)) \rightarrow 0$$

d'où $R^0\Gamma(C(2g\infty)) = \text{Ker}(d)$, $R^1\Gamma(C(2g\infty)) = \text{Coker}(d)$ et $R^2\Gamma(C(2g\infty)) = 0$. Enfin notons $\mathbb{B}^0 = \mathcal{O}_X((2g-1)\infty)/\mathcal{O}_X$ et $\mathbb{B}^1 = \Omega_X^1(2g\infty)/\Omega_X^1$, alors

$$C(2g\infty)/C = 0 \rightarrow \mathbb{B}^0 \rightarrow \mathbb{B}^1 \rightarrow 0$$

est à support ponctuel donc \mathbb{B}^0 et \mathbb{B}^1 sont acycliques pour Γ et donc

$$R\Gamma(C(2g\infty)/C) = 0 \rightarrow z^{-2g+1}V[[z]]/V[[z]] \xrightarrow{\Delta} z^{-2g}V[[z]]/V[[z]]dz \rightarrow 0$$

d'où $R^0\Gamma(C(2g\infty)/C) = \text{Ker}(\Delta)$, $R^1\Gamma(C(2g\infty)/C) = \text{Coker}(\Delta)$, $R^2\Gamma(C(2g\infty)/C) = 0$. Ce qui donne bien le résultat annoncé. □

On suppose jusqu'à la fin de cette partie que $p > 2g - 1$.

Lemme 5.4.1. *Soit $\Delta : z^{-2g+1}V[[z]]/V[[z]] \rightarrow z^{-2g}V[[z]]/V[[z]]dz$ avec z un paramètre de la courbe en ∞ , alors $\text{Ker}(\Delta) = 0$ et $\text{Coker}(\Delta) = V \frac{dz}{z}$.*

Preuve: Observons tout d'abord que

$$z^{-2g+1}V[[z]]/V[[z]] \simeq \bigoplus_{i=1}^{2g-1} Vz^{-i} \quad \text{et} \quad z^{-2g}V[[z]]/V[[z]]dz \simeq \bigoplus_{i=1}^{2g} Vz^{-i}dz$$

or $\Delta(z^{-i}) = (-i)z^{-i-1}$ il est donc clair que $\text{Ker}(\Delta) = 0$ puisqu'avec l'hypothèse sur p , $-i$ est inversible. Ensuite

$$\text{Im}(\Delta) = -\bigoplus_{i=2}^{2g} (i-1)Vz^{-i}dz \simeq \bigoplus_{i=1}^{2g} (i-1)Vz^{-i}dz$$

d'où

$$\text{Coker}(\Delta) \simeq \bigoplus_{i=1}^{2g-1} Vz^{-i} / \left(\bigoplus_{i=1}^{2g} (i-1)Vz^{-i}dz \right) \simeq \bigoplus_{i=1}^{2g} V / (i-1)Vz^{-i}dz.$$

Or $\forall 2 \leq i \leq 2g$, par hypothèse sur p , $i - 1$ est inversible et donc $(i - 1)V = V$. D'où

$$\bigoplus_{i=1}^{2g} V/(i-1)Vz^{-i}dz = V\frac{dz}{z}$$

ce qui donne le résultat annoncé sur le conoyau. □

Lemme 5.4.2. *Soit $d : \Gamma(\mathcal{O}_X((2g-1)\infty)) \rightarrow \Gamma(\Omega_X^1(2g\infty))$, alors $\text{Ker}(d) = V$ et*

$$\text{Coker}(d) = \bigoplus_{j=1}^{n-1} \bigoplus_{i=0}^{rn-3} V \frac{t^i dt}{y^j}.$$

Preuve: Notons $\mathcal{G}_j = H^0(X, \mathcal{O}_X((2g-1)\infty))_j$ pour $0 \leq j \leq n-1$, une expression explicite de \mathcal{G}_j a été donnée dans la proposition 5.2.3. Tout d'abord puisque d et δ commutent, on a $\text{Coker}(d)_j = H^0(X, \Omega_X^1(2g\infty))_j / \text{Im}(d|_{\mathcal{G}_j})$.

Si $j = 0$, on a

$$\mathcal{G}_0 = \bigoplus_{i=0}^{r(n-1)-2} Vt^i.$$

On calcule d sur les éléments de la base, $d(t^i) = it^{i-1}dt$ pour $0 \leq i \leq r(n-1) - 2$ et donc

$$\text{Im}(d|_{\mathcal{G}_0}) = \bigoplus_{i=0}^{r(n-1)-3} (i+1)Vt^i dt$$

d'où

$$\text{Coker}(d)_0 = \bigoplus_{i=0}^{r(n-1)-3} V/(i+1)Vt^i dt.$$

Or $2g = rn(n-1) - 2(n-1)$ donc $r(n-1) - 2 = 2(g-1)/n \leq g$ car $n \geq 2$, ainsi $\forall 0 \leq i \leq r(n-1) - 3$, $(i+1) \leq 2g - 1 < p$ et $i+1$ est inversible dans V donc $\text{Coker}(d)_0 = 0$.

Si $j = 1$, comme $\mathcal{G}_1 = 0$ on a simplement

$$\text{Coker}(d)_1 = H^0(X, \Omega_X^1(2g\infty))_1 = \bigoplus_{i=0}^{rn-3} V \frac{t^i dt}{y}.$$

Enfin soit $2 \leq j \leq n-1$ fixé. Sur l'ouvert U de la courbe X on a la relation $y^n = f(t)$ on peut donc écrire

$$\mathcal{G}_j = \bigoplus_{i=0}^{r(j-1)-2} Vt^i y^{n-j} = \bigoplus_{i=0}^{r(j-1)-2} Vf(t) \frac{t^i}{y^j}.$$

Notons $R = \text{Spec}(V[t, y]) = \mathbb{A}_V^2$ le plan affine sur $\text{Spec}(V)$. On a une immersion fermée $\iota : U \hookrightarrow R$ et $\iota^*\Omega_{\mathbb{A}^2}^1(R)/d(y^n - f(t)) \simeq \Omega_U^1(U)$. On a donc le diagramme commutatif suivant :

$$\begin{array}{ccc} V[t, y] & \xrightarrow{d} & i^*\Omega_{\mathbb{A}^2}^1(R) \\ \downarrow & \circlearrowleft & \downarrow \\ \mathcal{O}_U(U) & \xrightarrow{d} & \Omega_U^1(U) \end{array}$$

et on a des résultats similaires sur W ce qui justifie les calculs suivants.

Calculons donc d sur les éléments de la base. Soient $0 \leq i \leq r(j-1) - 2$ et $2 \leq j \leq n-1$ fixés, alors

$$d\left(f(t)\frac{t^i}{y^j}\right) = \frac{(f'(t)t^i + it^{i-1}f(t))y^j dt - jy^{j-1}f(t)t^i dy}{y^{2j}}$$

modulo $d(y^n - f(t))$. Or $y^n = f(t)$ donc $ny^{n-1}dy = f'(t)dt$ et ainsi $f(t)dy = yf'(t)dt/n$. D'où finalement

$$d\left(f(t)\frac{t^i}{y^j}\right) = \left(it^{i-1}f(t) + \frac{n-j}{n}f'(t)t^i\right)\frac{dt}{y^j} \in \Omega_U^1(U).$$

Dans l'expression entre parenthèses apparaît un polynôme en t de degré $i-1+l$ et de valuation $i-1$ (0 pour $i=0$). De plus le monôme de plus haut degré de ce polynôme est donné par $\left(i + l\frac{n-j}{n}\right)t^{i-1+l}$. Finalement on a

$$\text{Im}(d|_{\mathcal{G}_j}) = V\frac{n-j}{n}f'(t)\frac{dt}{y^j} \bigoplus_{i=0}^{r(j-1)-3} V\left((i+1)f(t) + \frac{n-j}{n}f'(t)t\right)\frac{t^i dt}{y^j}.$$

Tout d'abord remarquons que lorsque $i = r(j-1) - 2$, $i-1+l = r(j-1) + l - 3$. Or $l = rn - 1$ d'où $i-1+l = r(n+j-1) - 4$. Il s'agit maintenant de calculer

$$\bigoplus_{i=0}^{r(n+j-1)-4} \frac{t^i dt}{y^j} / \text{Im}(d|_{\mathcal{G}_j}).$$

Notons $E_j = \{P \in V[t] \mid \deg(P) \leq r(n+j-1) - 4\}$ alors $H^0(X, \Omega_X^1(2g\infty))_j \simeq E_j$. De plus par les calculs et les remarques précédentes, $\text{Im}(d|_{\mathcal{G}_j})$ peut être identifié au sous-module de E_j engendré par les éléments de la forme

$$\left(i + l\frac{n-j}{n}\right)t^{i-1+l} + P_i(t)$$

où P_i est un polynôme avec $\deg(P_i) < i-1+l$ avec $0 \leq i \leq r(j-1) - 2$. Or les coefficients dominants des polynômes considérés sont inversibles dès qu'ils sont strictement inférieurs à p . Le plus grand de ces coefficient à j fixé est $a_{M,j} = r(j-1) - 2 + l(n-j)/n$ or $l = rn - 1$ d'où $a_{M,j} = r(n-1) - 3 + j/n$ comme par ailleurs $j < n$ on a $a_{M,j} < r(n-1) - 2 < p$ comme cela a déjà été remarqué précédemment. Ainsi les $\left(i + l\frac{n-j}{n}\right)$ sont inversibles et le j -ième conoyau est isomorphe à

$$E_j / \left(t^{l-1} + P_{l-1}(t), t^l + P_l(t), \dots, t^{r(n+j-1)-4} + P_{r(n+j-1)-4}(t)\right) \simeq E_{l-2}.$$

Enfin $l - 2 = rn - 1 - 2 = rn - 3$ d'où

$$Coker(d)_j = \bigoplus_{i=0}^{rn-3} V \frac{t^i dt}{y^j}, \quad 2 \leq j \leq n-1$$

ce qui achève le calcul de $Coker(d)_j$. Par ailleurs il apparaît clairement au vu des calculs effectués que $Ker(d) = V$. □

Proposition 5.4.2. *Notons z un paramètre de la courbe en ∞ . En supposant que $p > 2g - 1$ on a la suite exacte courte :*

$$0 \rightarrow V \rightarrow V \rightarrow 0 \rightarrow H_{DR}^1(X) \rightarrow \bigoplus_{j=1}^{n-1} \bigoplus_{i=0}^{rn-3} V \frac{t^i dt}{y^j} \rightarrow V \frac{dz}{z} \rightarrow V \rightarrow 0$$

Preuve: Il s'agit simplement de remplacer dans la proposition 5.4.1 les valeurs de $Ker(d)$, $Ker(\Delta)$, $Coker(d)$ et $Coker(\Delta)$ par celles calculées dans les lemmes 5.4.1 et 5.4.2. □

Remarque 5.4.1. Sous les conditions de la proposition précédente on retrouve le fait que le module $H_{DR}^1(X)$ est de rang $2g$. En effet par les propriétés du rang dans une suite exacte on sait qu'ici le rang de $H_{DR}^1(X)$ est égal à celui de $Coker(d)$. Or le rang de $Coker(d)$ vaut $(n-1)(rn-2) = rn(n-1) - 2(n-1) = 2g$.

Proposition 5.4.3. *Supposons $p > 2g - 1$, alors on a un isomorphisme*

$$H_{DR}^1(X) \simeq \bigoplus_{j=1}^{n-1} \bigoplus_{i=0}^{rn-3} V \frac{t^i dt}{y^j}$$

ou encore

$$H_{DR}^1(X) \simeq \bigoplus_{j=1}^{n-1} \bigoplus_{i=0}^{rj-2} V \frac{t^i dt}{y^j} \oplus \bigoplus_{j=1}^{n-1} \bigoplus_{i=rj-1}^{rn-3} V \frac{t^i dt}{y^j}.$$

Preuve: Le résultat se démontre en appliquant δ à la suite exacte donnée dans la proposition 5.4.2. En effet il est clair que dz/z est invariant par δ , il en est donc de même pour $Coker(\Delta)$. Après application de δ on obtient donc n suites exactes courtes

$$0 \rightarrow V \rightarrow V \rightarrow 0 \rightarrow H_{DR}^1(X)_0 \rightarrow 0 \rightarrow V \frac{dz}{z} \rightarrow V \rightarrow 0$$

et pour $1 \leq j \leq n-1$

$$0 \rightarrow 0 \rightarrow 0 \rightarrow 0 \rightarrow H_{DR}^1(X)_j \rightarrow \bigoplus_{i=0}^{rn-3} V \frac{t^i dt}{y^j} \rightarrow 0 \rightarrow 0 \rightarrow 0.$$

De la première suite exacte on conclut que $H_{DR}^1(X)_0 = 0$, de la seconde que $\forall 1 \leq j \leq n-1$,

$$H_{DR}^1(X)_j \simeq \bigoplus_{i=0}^{rn-3} V \frac{t^i dt}{y^j}$$

d'où le résultat annoncé. Pour mémoire, $2g = rn(n-1) - 2(n-1)$. Enfin la dernière égalité est simplement la décomposition de cette suite exacte selon $H^0(X, \Omega_X^1)$ car

$$H^0(X, \Omega_X^1) = \bigoplus_{j=1}^{n-1} \bigoplus_{i=0}^{rj-2} V \frac{t^i dt}{y^j}$$

(voir proposition 4.1.1).

□

Théorème 5.4.1. *Supposons que $p > 2g - 1$, alors indépendamment du fait que k contienne $\mu_n(\overline{\mathbb{F}}_p)$, on a un isomorphisme*

$$H_{DR}^1(X) \simeq \bigoplus_{j=1}^{n-1} \bigoplus_{i=0}^{rj-2} V \frac{t^i dt}{y^j} \oplus \bigoplus_{j=1}^{n-1} \bigoplus_{i=rj-1}^{rn-3} V \frac{t^i dt}{y^j} = \bigoplus_{j=1}^{n-1} \bigoplus_{i=0}^{rn-3} V \frac{t^i dt}{y^j}.$$

Preuve: Comme la suite spectrale de Hodge vers de Rham dégénère, on a un isomorphisme $H_{DR}^1(X) \simeq H^0(X, \Omega_X^1) \oplus H^1(X, \mathcal{O}_X)$. Soit maintenant $k \rightarrow k'$ une extension finie telle que $\mu_n(\overline{\mathbb{F}}_p) \subset k'$, alors on a une extension finie et plate $W(k) \rightarrow W(k')$ des anneaux des vecteurs de Witt. De plus les résultats précédents s'appliquent. Notons $\overline{X} = X \times_{\text{Spec}(V)} \text{Spec}(W(k'))$ alors comme l'extension est plate on a :

$$W(k') \otimes_{W(k)} H^0(X, \Omega_X^1) \simeq H^0(X, \Omega_{\overline{X}}^1)$$

$$W(k') \otimes_{W(k)} H^1(X, \mathcal{O}_X) \simeq H^1(X, \mathcal{O}_{\overline{X}})$$

mais les $t^i y^{-j} dt$ sont invariants par extension du corps donc on a bien une base de l'espace avant extension.

□

Chapitre 6

Un scindage adapté de la filtration de Hodge

On considère le complexe de Čech relatif au recouvrement $X = U \cup W$.

$$0 \longrightarrow \mathcal{O}_X(U) \times \mathcal{O}_X(W) \xrightarrow{d_{0,1}} \mathcal{O}_X(U \cap W) \longrightarrow 0$$

où l'application $d_{0,1}$ est donnée par $(a, b) \mapsto (a - b)|_{U \cap W}$. D'après le théorème 4.5 (III,4) de [Har77] $H^1(X, \mathcal{O}_X)$ est égal au premier espace de cohomologie de ce complexe de Čech et est donc égal à $\mathcal{O}_X(U \cap W)/\text{Im}(d_{0,1})$.

Lemme 6.0.3. *On a $H^1(X_k, \mathcal{O}_{X_k}) = k \otimes_V H^1(X, \mathcal{O}_X)$.*

Preuve: On a une suite exacte courte

$$0 \rightarrow \mathcal{O}_X \xrightarrow{\times p} \mathcal{O}_X \rightarrow \mathcal{O}_{X_k} \rightarrow 0$$

qui donne la suite exacte longue de cohomologie

$$\begin{aligned} 0 \rightarrow H^0(X, \mathcal{O}_X) \xrightarrow{\times p} H^0(X, \mathcal{O}_X) \rightarrow H^0(X_k, \mathcal{O}_{X_k}) \rightarrow H^1(X, \mathcal{O}_X) \xrightarrow{\times p} H^1(X, \mathcal{O}_X) \\ \rightarrow H^1(X_k, \mathcal{O}_{X_k}) \rightarrow 0 \end{aligned}$$

or $H^0(X, \mathcal{O}_X) = V$, $H^0(X_k, \mathcal{O}_{X_k}) = k$ et $k \simeq V/pV$, on obtient donc la suite exacte courte

$$0 \rightarrow H^1(X, \mathcal{O}_X) \xrightarrow{\times p} H^1(X, \mathcal{O}_X) \rightarrow H^1(X_k, \mathcal{O}_{X_k}) \rightarrow 0$$

qui permet de conclure que $H^1(X_k, \mathcal{O}_{X_k}) = H^1(X, \mathcal{O}_X)/pH^1(X, \mathcal{O}_X) = k \otimes_V H^1(X, \mathcal{O}_X)$ et montre le lemme. □

Proposition 6.0.4. *Le V -module $H^1(X, \mathcal{O}_X)$ est libre de rang g , de plus il admet pour base les classes $\overline{h_{i,j}}$ des éléments $h_{i,j} \in \mathcal{O}_X(\overline{U} \cap W)$ où*

$$h_{i,j} = \frac{y^j}{t^i} = \frac{z^j}{s^{rj-i}}, \quad 1 \leq j \leq n-1, \quad 1 \leq i \leq rj-1$$

soit encore

$$H^1(X, \mathcal{O}_X) = \bigoplus_{j=1}^{n-1} \bigoplus_{i=1}^{rj-1} V \overline{t^{-i}y^j} = \bigoplus_{j=1}^{n-1} \bigoplus_{i=1}^{r(n-j)-1} V \overline{t^{-i}y^{n-j}}.$$

Par ailleurs supposons que $\mu_n(\overline{\mathbb{F}}_p) \subset k$. Alors si on note $H^1(X, \mathcal{O}_X)_j$ la j -ième composante isotypique associée à l'action de δ alors on a :

$$\begin{aligned} H^1(X, \mathcal{O}_X)_0 &= 0 \\ H^1(X, \mathcal{O}_X)_j &= \bigoplus_{i=1}^{r(n-j)-1} V \overline{t^{-i}y^{n-j}} \quad \forall 1 \leq j \leq n-1. \end{aligned}$$

Preuve: Comme X est propre on sait que $H^1(X, \mathcal{O}_X)$ est un V -module de type fini. Par ailleurs par dualité de Poincaré on a $H^1(X, \mathcal{O}_X) \simeq H^0(X, \Omega_X^1)$. Mais on a établi au théorème 4.1.1 que ce dernier module était libre de rang g ce qui donne le résultat sur $H^1(X, \mathcal{O}_X)$. De plus $\mathcal{O}_X(U) = V[t, y]/(y^n - f(t))$ et $\mathcal{O}_X(W) = V[s, z]/(z^n - f_2(t))$ et donc

$$\mathcal{O}_X(U \cap W) = V[t, y, t^{-1}]/(y^n - f(t)) = V[s, z, s^{-1}]/(z^n - f_2(t)).$$

Une base de $\mathcal{O}_X(U \cap W)$ comme V -module est donc $t^i y^j$ avec $i \in \mathbb{Z}$ et $0 \leq j \leq n-1$ ou encore $s^i z^j$ avec $i \in \mathbb{Z}$ et $0 \leq j \leq n-1$. De même une base de $\mathcal{O}_X(U)$ (respectivement $\mathcal{O}_X(W)$) est $t^i y^j$ avec $i \geq 0$ et $0 \leq j \leq n-1$ (respectivement $s^i z^j$ avec $i \geq 0$ et $0 \leq j \leq n-1$). Par définition de $d_{0,1}$, tout élément $t^i y^j$ avec $i \geq 0$ et $0 \leq j \leq n-1$ est dans l'image de $d_{0,1}$. De la même manière tout élément du type $s^i z^j$ avec $i \geq 0$ et $0 \leq j \leq n-1$ est dans l'image de $d_{0,1}$. Or sur $U \cap W$ on a $s = 1/t$ et $z = s^r y$ d'où $s^i z^j = t^{-(i+rj)} y^j$. Par ailleurs lorsque j vaut 0, $i+rj$ prend toutes les valeurs entières lorsque i est dans \mathbb{N} et lorsque j est non nul, $i+rj$ prend toutes les valeurs supérieures ou égales à rj . Posons donc $B = \{Vt^i y^j, 0 \leq j \leq n-1, i \in \mathbb{N}\} \cup \{Vt^{-i} y^j, 0 \leq j \leq n-1, i \geq rj\}$, alors $\text{Im}(d) \supset B$. On sait également grâce à la description de $\mathcal{O}_X(U \cap W)$ donnée plus haut que $H^1(X, \mathcal{O}_X) = \sum V \overline{t^i y^j}$ pour $0 \leq j \leq n-1$ et i élément de \mathbb{Z} et les considérations précédentes permettent alors de dire que

$$H^1(X, \mathcal{O}_X) = \sum_{\substack{1 \leq j \leq n-1 \\ 1 \leq i \leq rj-1}} V \overline{t^{-i} y^j}. \quad (1)$$

On établirait de la même manière que

$$H^1(X_k, \mathcal{O}_{X_k}) = \sum_{\substack{1 \leq j \leq n-1 \\ 1 \leq i \leq rj-1}} \widehat{kt^{-i} y^j} \quad (2)$$

où $\widehat{t^{-i} y^j}$ désigne la classe de $t^{-i} y^j$ dans $H^1(X_k, \mathcal{O}_{X_k})$. Notons $e_{i,j} = \overline{t^{-i} y^j}$ pour $1 \leq j \leq n-1$ et $1 \leq i \leq rj-1$, $L = \bigoplus V e_{i,j}$ le V -module libre et $\varphi : L \rightarrow H^1(X, \mathcal{O}_X)$ l'application qui envoie $e_{i,j}$ sur $\overline{h_{i,j}}$. Remarquons tout d'abord que L est de rang g , en effet son rang vaut

$$\sum_{j=1}^{n-1} (rj-1) = r \sum_{j=1}^{n-1} j - (n-1) = r \frac{(n-1)n}{2} - (n-1) = g.$$

On sait que φ est surjective par le (1) et elle induit une surjection $\oplus k\widehat{e}_{i,j} \rightarrow H^1(X_k, \mathcal{O}_{X_k})$ via $\widehat{e}_{i,j} \mapsto \widehat{t^{-i}y^j}$. Notons maintenant \mathcal{K} le noyau de φ . C'est un V -module de type fini et on a une suite exacte courte

$$0 \rightarrow \mathcal{K} \rightarrow L \xrightarrow{\varphi} H^1(X, \mathcal{O}_X) \rightarrow 0$$

alors comme $H^1(X, \mathcal{O}_X)$ est un V -module libre, on a une suite exacte courte

$$0 \rightarrow \mathcal{K}/p\mathcal{K} \rightarrow L/pL \xrightarrow{\bar{\varphi}} k \otimes_V H^1(X, \mathcal{O}_X) \rightarrow 0.$$

Or $\bar{\varphi}$ est surjectif par le (2), c'est donc une application k -linéaire surjective entre deux k -espaces vectoriels de même dimension, ainsi $\bar{\varphi}$ est bijective et donc $\mathcal{K}/p\mathcal{K} = 0$. Le lemme de Nakayama permet alors d'affirmer que \mathcal{K} est nul et que φ induit un isomorphisme $L \simeq H^1(X, \mathcal{O}_X)$. En particulier les éléments $\overline{h_{i,j}}$ forment une base de $H^1(X, \mathcal{O}_X)$ d'où l'expression de $H^1(X, \mathcal{O}_X)$. La seconde étant donnée par le changement d'indice $j' = n - j$.

Pour finir rappelons que l'action de δ est donnée par $t \mapsto t$ et $y \mapsto [\zeta]^{-1}y$ et donc δ appliquée à $h_{i,j}$ donne $[\zeta]^{-j}h_{i,j} = [\zeta]^{n-j}h_{i,j}$ et $\delta(h_{i,n-j}) = [\zeta]^{-n+j}h_{i,n-j} = [\zeta]^j h_{i,n-j}$ d'où le résultat annoncé sur les $H^1(X, \mathcal{O}_X)_j$. □

Proposition 6.0.5. *Le k -espace vectoriel $H^1(X_k, \mathcal{O}_{X_k})$ est de dimension g et admet pour base les classes $\overline{h_{i,j}}$ des éléments $h_{i,j} \in \mathcal{O}_{X_k}(\overline{U}_k \cap \overline{W}_k)$ où*

$$h_{i,j} = \frac{y^j}{t^i} = \frac{z^j}{s^{rj-i}}, \quad 1 \leq j \leq n-1, \quad 1 \leq i \leq rj-1$$

soit encore

$$H^1(X_k, \mathcal{O}_{X_k}) = \bigoplus_{j=1}^{n-1} \bigoplus_{i=1}^{rj-1} \overline{kt^{-i}y^j} = \bigoplus_{j=1}^{n-1} \bigoplus_{i=1}^{r(n-j)-1} \overline{kt^{-i}y^{n-j}}.$$

Par ailleurs supposons que $\mu_n(\overline{\mathbb{F}}_p) \subset k$. Alors si on note $H^1(X_k, \mathcal{O}_{X_k})_j$ la j -ième composante isotypique associée à l'action de δ alors on a :

$$H^1(X_k, \mathcal{O}_{X_k})_0 = 0$$

$$H^1(X_k, \mathcal{O}_{X_k})_j = \bigoplus_{i=1}^{r(n-j)-1} \overline{kt^{-i}y^{n-j}} \quad \forall 1 \leq j \leq n-1.$$

Preuve: La démonstration fait appel aux mêmes arguments que ceux utilisés pour démontrer la proposition précédente. □

Remarque 6.0.2. Au vu de la démonstration de la proposition 6.0.4, il y a une identification naturelle d'un élément $\overline{h_{i,j}}$ de la base de $H^1(X, \mathcal{O}_X)$ avec le représentant $h_{i,j}$ élément de $\mathcal{O}_{U \cap W}$. Par la suite on notera simplement $t^{-i}y^j$ le représentant de la classe $\overline{t^{-i}y^j} \in H^1(X, \mathcal{O}_X)$ lorsqu'on voudra le regarder comme élément de $\mathcal{O}_{U \cap W}$. Cette remarque est également valable dans le cas de X_k .

Notons Ω_X^\bullet le complexe de de Rham associé à Ω_X^1 et \mathcal{F} le recouvrement de X par U et W alors on note $\check{C}(\mathcal{F}, \Omega_X^\bullet)$ le complexe de Čech associé au complexe de de Rham. Il est donné par

$$\begin{array}{ccccccc} & & 0 & & 0 & & \\ & & \uparrow & & \uparrow & & \\ 0 & \rightarrow & \Omega_X^1(U) \times \Omega_X^1(W) & \rightarrow & \Omega_X^1(U \cap W) & \rightarrow & 0 \\ & & \uparrow & & \uparrow & & \\ 0 & \rightarrow & \mathcal{O}_X(U) \times \mathcal{O}_X(W) & \rightarrow & \mathcal{O}_X(U \cap W) & \rightarrow & 0 \\ & & \uparrow & & \uparrow & & \\ & & 0 & & 0 & & \end{array}$$

on peut lui associer le complexe simple

$$0 \rightarrow \mathcal{O}_X(U) \times \mathcal{O}_X(W) \rightarrow \Omega_X^1(U) \times \Omega_X^1(W) \oplus \mathcal{O}_X(U \cap W) \rightarrow \Omega_X^1(U \cap W) \rightarrow 0$$

et le groupe de cohomologie $H_{DR}^1(X)$ s'identifie alors aux classes des éléments

$$(\omega_U, \omega_W, h) \in \Omega_X^1(U) \oplus \Omega_X^1(W) \oplus \mathcal{O}_X(U \cap W)$$

tels que $\omega_W - \omega_U + dh = 0$, modulo les éléments de la forme $(dh_U, -dh_W, h)$ où $h = h_U + h_W$, $h_U \in \mathcal{O}_X(U)$, $h_W \in \mathcal{O}_X(W)$. Dans la suite on notera $H^1(\check{C}(\mathcal{F}, \Omega_X^\bullet))$ le premier espace de cohomologie associé au complexe simple considéré ici.

Proposition 6.0.6. *On conserve les notations précédentes, alors :*

- (i) L'image de $\omega \in H^0(X, \Omega_X^1)$ dans $H^1(\check{C}(\mathcal{F}, \Omega_X^\bullet))$ est la classe de l'élément $(\omega|_U, \omega|_W, 0)$.
- (ii) Soient $1 \leq j \leq n-1$ et $1 \leq i \leq rj-1$. Notons λ_k le coefficient de t^k dans $f(t)$ et posons $a_j = (n-j)r-2$,

$$\alpha_{i,j}^U = \left[\sum_{k=i+1}^l \frac{jk-in}{n} \lambda_k t^{k-(i+1)} \right] y^{j-1} \frac{dt}{y^{n-1}},$$

$$\alpha_{i,j}^W = \left[\sum_{k=0}^i \frac{in-jk}{n} \lambda_k s^{i+1+a_j-k} \right] z^{j-1} \frac{ds}{z^{n-1}}.$$

Alors $\alpha_{i,j}^U \in \Omega_X^1(U)$, $\alpha_{i,j}^W \in \Omega_X^1(W)$, $dh_{i,j} = \alpha_{i,j}^U + \alpha_{i,j}^W$ et on a une application V -linéaire :

$$[\tau] : \begin{array}{ccc} H^1(X, \mathcal{O}_X) & \longrightarrow & H^1(\check{C}(\mathcal{F}, \Omega_X^\bullet)) \\ \overline{h_{i,j}} & \longmapsto & [(\alpha_{i,j}^U, -\alpha_{i,j}^W, h_{i,j})] \end{array}$$

qui est un scindage de la filtration de Hodge. Les $\alpha_{i,j}$ sont déterminés, à une section globale $\omega \in H^0(X, \Omega_X^1)$ près.

Preuve: (i) Cela résulte de l'inclusion naturelle $H^0(X, \Omega_X^1) \subset H^1(\check{C}(\mathcal{F}, \Omega_X^\bullet)) \simeq H_{DR}^1(X)$.

(ii) Rappelons tout d'abord que $dt/y^{n-1} \in H^0(X, \Omega_X^1)$ (voir théorème 4.1.1) et de même pour ds/z^{n-1} . Soient $1 \leq j \leq n-1$ et $1 \leq i \leq rj-1$ fixés, calculons $dh_{i,j}$.

$$dh_{i,j} = \frac{jy^{j-1}dy}{t^i} - \frac{iy^j dt}{t^{i+1}} \text{ mod } \mathcal{O}_X(U \cap W) [ny^{n-1}dy - f'(t)dt]$$

Par ailleurs on a la relation $y^n = f(t)$ dans $\mathcal{O}_X(U \cap W)$ et donc

$$dh_{i,j} = \frac{jf'(t)y^{j-1}}{nt^i} \frac{dt}{y^{n-1}} - \frac{iy^j y^{n-1}}{t^{i+1}} \frac{dt}{y^{n-1}} = \left(\frac{jf'(t)}{nt^i} - \frac{if(t)}{t^{i+1}} \right) y^{j-1} \frac{dt}{y^{n-1}} \in \Omega_X^1(U \cap W).$$

On rappelle que

$$\Omega_X^1(U) \supset (V[t, y]/(y^n - f(t))) \frac{dt}{y^{n-1}}$$

$$\Omega_X^1(W) \supset (V[s, z]/(z^n - f_2(s))) \frac{ds}{z^{n-1}}.$$

donc pour montrer le résultat voulu montrons que l'on peut écrire

$$dh_{i,j} = R_{i,j}(t, y) \frac{dt}{y^{n-1}} + S_{i,j}(s, z) \frac{ds}{z^{n-1}}$$

avec $R_{i,j} \in V[y, t]$ et $S_{i,j} \in V[z, s] \forall 1 \leq j \leq n-1, \forall 1 \leq i \leq rj-1$. Remarquons qu'avec ces conditions, $i \leq rj-1 \Rightarrow i \leq r(n-1)-1 = rn-1-r = l-r < l$. Notons $f(t) = \sum \lambda_k t^k$ alors $f'(t) = \sum k \lambda_k t^{k-1}$ (pour mémoire $\lambda_k \in V$), alors

$$dh_{i,j} = \left[\frac{j}{n} \frac{1}{t^i} \sum_{k=1}^l k \lambda_k t^{k-1} - i \frac{1}{t^{i+1}} \sum_{k=0}^l \lambda_k t^k \right] y^{j-1} \frac{dt}{y^{n-1}} \in \Omega_X^1(U \cap W)$$

$$dh_{i,j} = \left[\frac{j}{n} \sum_{k=1}^i k \lambda_k t^{k-(i+1)} - i \sum_{k=0}^i \lambda_k t^{k-(i+1)} \right] y^{j-1} \frac{dt}{y^{n-1}} + \left[\frac{j}{n} \sum_{k=i+1}^l k \lambda_k t^{k-(i+1)} - i \sum_{k=i+1}^l \lambda_k t^{k-(i+1)} \right] y^{j-1} \frac{dt}{y^{n-1}}.$$

Il est clair que le second terme de cette expression est un élément de $V[y, t]/(y^n - f(t)) \frac{dt}{y^{n-1}}$, on le note $\alpha_{i,j}^U$. Pour conclure montrons que le premier terme, noté $\alpha_{i,j}^W$, est un élément de $V[z, s]/(z^n - f_2(s)) \frac{ds}{z^{n-1}}$.

$$y^{j-1} \frac{dt}{y^{n-1}} = \frac{-s^{-(j-1)r} z^{j-1} s^{-2} ds}{s^{-(n-1)r} z^{n-1}} = -s^{(n-j)r-2} z^{j-1} \frac{ds}{z^{n-1}} \in \Omega_X^1(U \cap W).$$

Notons $a_j = (n-j)r-2$, comme $1 \leq j \leq n-1$ alors $r-2 \leq a_j \leq (n-1)r-2$. Mais $r = (l+1)/n$ avec $l \equiv -1 [n]$ et $l \geq 0$ donc $r \geq 1$ et $-1 \leq a_j \leq (n-1)r-2$.

$$\alpha_{i,j}^W = \left[-\frac{j}{n} \sum_{k=1}^i k \lambda_k s^{i+1+a_j-k} + i \sum_{k=0}^i \lambda_k s^{i+1+a_j-k} \right] z^{j-1} \frac{ds}{z^{n-1}}.$$

Comme $i-k \geq 0$ et que par les considérations précédentes $1+a_j \geq 0$, alors $\alpha_{i,j}^W$ est bien dans l'espace désiré. Par linéarité cela définit une application τ qui à $h_{i,j}$ associe $(\alpha_{i,j}^U, -\alpha_{i,j}^W, h_{i,j})$ dans $\Omega_X^1(U) \oplus \Omega_X^1(W) \oplus \mathcal{O}_X(U \cap W)$ qui donne $[\tau]$ par passage au quotient dans $H^1(\check{C}(\mathcal{F}, \Omega_X^\bullet))$ ce qui achève la démonstration. \square

Remarque 6.0.3. On peut également définir $[\tau] : H^1(X_k, \mathcal{O}_{X_k}) \longrightarrow H^1(\check{C}(\mathcal{F}_k, \Omega_{X_k}^\bullet))$ où \mathcal{F}_k désigne le recouvrement de X_k par U_k et W_k . Il est facile de voir que la démonstration resterait la même et donc que les formules permettant d'exprimer $\alpha_{i,j}^{U_k}$ et $\alpha_{i,j}^{W_k}$ sont identiques à conditions de remplacer les coefficients par leur classe modulo p dans k .

Proposition 6.0.7. *On conserve les notations de la proposition précédente. Supposons que $\mu_n(\overline{\mathbb{F}_p}) \subset k$, alors τ envoie la j -ième composante isotypique de $H^1(X, \mathcal{O}_X)$ sur la j -ième composante isotypique de $\Omega_X^1(U) \oplus \Omega_X^1(W) \oplus \mathcal{O}_X(U \cap W)$. De même $[\tau]$ envoie la j -ième composante isotypique de $H^1(X, \mathcal{O}_X)$ sur la j -ième composante isotypique de $H^1(\check{C}(\mathcal{F}, \Omega_X^\bullet))$.*

Preuve: Soit $1 \leq j \leq n-1$ fixé, et soit τ comme dans la proposition précédente. Alors l'élément $\overline{h_{i,j}}$ est envoyé par τ sur un triplet du type $(\alpha_U(t)y^{-(n-j)}dt, \alpha_W(t)y^{-(n-j)}dt, h(t)y^j)$. Comme l'action de δ est donnée par $\delta(t) = t$ et $\delta(y) = [\zeta]^{-1}y$ (voir section 2.2), l'image de $\overline{h_{i,j}} = \overline{t^{-i}y^j}$, élément de la $(n-j)$ -ième composante isotypique de $H^1(X, \mathcal{O}_X)$, est dans la $(n-j)$ -ième composante isotypique de $\Omega_X^1(U) \oplus \Omega_X^1(W) \oplus \mathcal{O}_X(U \cap W)$ ce qui donne bien le résultat annoncé. Le résultat sur $[\tau]$ s'en déduit par passage aux classes d'équivalence. □

Chapitre 7

Mise en place du calcul du Frobenius divisé de la fibre spéciale

7.1 Rappels sur le Frobenius

Définition 7.1.1. Soit σ_k le Frobenius sur k (i.e. l'élevation à la puissance p), alors σ_k induit un morphisme de schémas $\text{Spec}(k) \rightarrow \text{Spec}(k)$. Si Y est un schéma sur $\text{Spec}(k)$ on notera Y'_k le schéma $\text{Spec}(k) \times_{\text{Spec}(k)} Y$, où le produit fibré est pris au-dessus de σ_k .

Soit σ un relèvement du Frobenius sur $\text{Spec}(V/p^2V)$, alors σ induit un morphisme de schémas $\text{Spec}(V/p^2V) \rightarrow \text{Spec}(V/p^2V)$. Si Y_1 est un schéma sur $\text{Spec}(V/p^2V)$ on notera Y'_1 le schéma $\text{Spec}(V/p^2V) \times_{\text{Spec}(V/p^2V)} Y$, où le produit fibré est pris au-dessus de σ .

Définition 7.1.2. Soit σ le Frobenius sur V/p^2V qui relève le Frobenius sur k . Considérons $Q(T) = \sum b_k T^k$ un polynôme à coefficients dans V/p^2V , on note $Q^\sigma(T) = \sum \sigma(b_k) T^k$.

Par la propriété des vecteurs de Witt, le Frobenius sur k (qui est l'élevation à la puissance p) se relève en un isomorphisme $\sigma : V \rightarrow V$.

On a le diagramme suivant de schémas sur $\text{Spec}(k)$:

$$\begin{array}{ccccc}
 & & F_{abs} & & \\
 & \curvearrowright & & \curvearrowleft & \\
 X_k & \xrightarrow{F} & X'_k & \xrightarrow{pr} & X_k \\
 & & \downarrow & & \downarrow \\
 & & \text{Spec}(k) & \xrightarrow{\bar{\sigma}} & \text{Spec}(k)
 \end{array}$$

où F_{abs} est le Frobenius absolu, F le Frobenius relatif factorisant F_{abs} , pr la projection de X'_k sur X_k et $\bar{\sigma} : \text{Spec}(k) \rightarrow \text{Spec}(k)$ est le morphisme induit par le Frobenius sur k .

Soit $U'_k \simeq U_k$ (comme \mathbb{Z} -schéma) l'analogue de U_k sur X'_k , on a $U_k = \text{Spec}(k[t, y]/(y^n - f(t)))$ et donc $U'_k = \text{Spec}(k[t, y]/(y^n - f^\sigma(t)))$ (voir définition 7.1.2). En restreignant le diagramme à l'ouvert U_k on obtient

$$\begin{array}{c}
 \xrightarrow{F_{abs}^\#} \\
 k[t, y]/(y^n - f(t)) \xrightarrow{pr^\#} k[t, y]/(y^n - f^\sigma(t)) \xrightarrow{F^\#} k[t, y]/(y^n - f(t))
 \end{array}$$

où $F_{abs}^\#(h) = h^p$, $pr^\#(h) = h^\sigma$, $F^\#(y) = y^p$ et $F^\#(t) = t^p$.

Par ailleurs $F_{abs}^\#$ est semi-linéaire par rapport à σ , $pr^\#$ est un isomorphisme d'anneaux également semi-linéaire par rapport à σ et $F^\#$ est un morphisme de k -algèbres.

Par functorialité on a alors

$$\begin{array}{c}
 \xrightarrow{F_{abs}} \\
 H_{cris}^1(X_k) \longrightarrow H_{cris}^1(X'_k) \xrightarrow{F} H_{cris}^1(X_k)
 \end{array}$$

où F_{abs} est un morphisme semi-linéaire et F un morphisme K -linéaire qui factorise F_{abs} . De plus, Berthelot ayant construit un isomorphisme $H_{cris}^1(X_k) \simeq H_{DR}^1(X)$ (et $H_{cris}^1(X'_k) \simeq H_{DR}^1(X')$, voir [BO78]), on obtient par identification

$$\begin{array}{c}
 \xrightarrow{F_{abs}} \\
 H_{DR}^1(X) \xrightarrow{pr} H_{DR}^1(X') \xrightarrow{F} H_{DR}^1(X)
 \end{array}$$

avec F_{abs} semi-linéaire, pr isomorphisme de groupes semi-linéaire par rapport à σ et F qui factorise F_{abs} .

Supposons que l'on ait un scindage $sc : H^1(X', \mathcal{O}_{X'}) \oplus H^0(X', \Omega_{X'}^1) \rightarrow H_{DR}^1(X)$ ainsi que l'application F décrite précédemment. On peut alors construire le Frobenius divisé modulo p , $\varphi' : H^1(X'_k, \mathcal{O}_{X'_k}) \oplus H^0(X'_k, \Omega_{X'_k}^1) \rightarrow H_{DR}^1(X_k)$ qui est k -linéaire (voir définition 7.3.1).

On sait pas un théorème de Huyghe-Wach que φ' est donné par le morphisme de Deligne-Illusie. Il s'agit en fait de calculer $H^1(X_k, \mathcal{O}_{X_k}) \oplus H^0(X_k, \Omega_{X_k}^1) \rightarrow H_{DR}^1(X_k)$, le Frobenius divisé de Mazur modulo p , qui décrit le φ -module filtré modulo p associé à X_k . Cette application est la composée

$$\begin{array}{c}
 \xrightarrow{\phi} \\
 H^1(X_k, \mathcal{O}_{X_k}) \oplus H^0(X_k, \Omega_{X_k}^1) \xrightarrow{pr^\#} H^1(X'_k, \mathcal{O}_{X'_k}) \oplus H^0(X'_k, \Omega_{X'_k}^1) \xrightarrow{\phi'} H_{DR}^1(X_k)
 \end{array}$$

avec ϕ semi-linéaire.

Proposition 7.1.1. *Une base de $H^1(X'_k, \mathcal{O}_{X'_k})$ est donnée par $\overline{h'_{i,j}} = \overline{t^{-i}y^j}$ pour $1 \leq j \leq n-1$ et $1 \leq i \leq rj-1$.*

Une base de $H^0(X_k, \Omega_{X_k}^1)$ est donnée par $\omega'_{i,j} = t^i y^{-j} dt$ pour $1 \leq j \leq n-1$ et $0 \leq i \leq rj-2$.

CHAPITRE 7. MISE EN PLACE DU CALCUL DU FROBENIUS DIVISÉ DE LA FIBRE SPÉCIALE

Preuve: On dispose déjà d'une base de $H^1(X_k, \mathcal{O}_{X_k})$ et $H^0(X_k, \Omega_{X_k}^1)$ donnée par la proposition 6.0.5 ainsi que par la proposition 4.1.1, dont les éléments sont respectivement $\overline{h_{i,j}} = t^{-i}y^j$ pour $1 \leq j \leq n-1$ et $1 \leq i \leq rj-1$ et $\omega_{i,j} = t^i y^{-j} dt$ pour $1 \leq j \leq n-1$ et $0 \leq i \leq rj-2$. Au vu des démonstrations de ces deux résultats et par définition de X'_k , il est clair qu'on obtient bien les bases proposées pour $H^1(X'_k, \mathcal{O}_{X'_k})$ et $H^0(X'_k, \Omega_{X'_k}^1)$. \square

Remarque 7.1.1. On dispose d'une base de $H^1(X_k, \mathcal{O}_{X_k}) \oplus H^0(X_k, \Omega_{X_k}^1) \simeq H_{DR}^1(X_k)$ donnée par les propositions 6.0.5 et 4.1.1 (ou encore par la proposition 5.4.1). Alors $pr^\#(\omega_{i,j}) = \omega'_{i,j}$ et $pr^\#(\overline{h_{i,j}}) = \overline{h'_{i,j}}$ et donc $\phi(\omega_{i,j}) = \phi'(\omega'_{i,j})$ et $\phi(\overline{h_{i,j}}) = \phi'(\overline{h'_{i,j}})$. Ainsi la matrice de ϕ est donnée par les $\phi'(\omega'_{i,j})$ et $\phi'(\overline{h'_{i,j}})$ exprimés dans les bases $(\omega_{i,j})$ et $(\overline{h_{i,j}})$. Par ailleurs la base $((\omega_{i,j}), (\overline{h_{i,j}}))$ est adaptée à la filtration et on peut donc, de façon abusive, considérer cette base au départ et à l'arrivée de ϕ .

7.2 Relèvements du Frobenius modulo p^2

Notation. On se donne des polynômes f, f', f_2 et f'_2 dans $V[t]$ et $V[s]$ comme précédemment. Par abus de notation, on notera de la même façon f, f', f_2 et f'_2 leurs classes modulo $p^2V[t]$ et $p^2V[s]$ respectivement. Enfin on notera f, f', f_2 et f'_2 les classes de f, f', f_2 et f'_2 dans $k[t]$ et $k[s]$ respectivement.

Remarque 7.2.1. Toute translation de la droite projective transforme X_k en une courbe Y_k isomorphe à X_k . En effet soit X_k définie comme précédemment et supposons qu'elle soit définie sur U_k par l'équation $y^n = f(t) = t \prod (t - \alpha_i)$. Son corps des fonctions est alors $k(t, y)/(y^n - f(t))$. Soit $t' = t + u$, alors $f(t) = (t' - u) \prod (t' - (u + \alpha_i)) = g(t')$ et $k(t, y)/(y^n - f(t)) \simeq k(t', y)/(y^n - g(t'))$. En choisissant judicieusement u (en fait tel que $u + \alpha_i \neq 0 \forall i$) et quitte à faire une extension finie du corps de base, on peut donc se ramener à l'étude de la courbe $Y_k \simeq X_k$ définie comme la réunion des deux ouverts affines U'_k et W'_k où $U'_k = \text{Spec}(k[t', y]/(y^n - g(t')))$ et telle que 0 n'est pas racine de g . Or pour ce que nous souhaitons calculer, à savoir la matrice du Frobenius divisé sur le premier espace de cohomologie de de Rham, on travaille modulo p i.e. sur X_k ce qui est équivalent à travailler sur Y_k . On peut donc supposer que t ne divise pas $f(t)$ dans $k[t]$ ce qui sera utile plus tard dans la section 7.2.

Afin de relever le Frobenius, on va modifier les ouverts U et W qui ont été définis à la section 2.1. On suppose désormais dans tout ce qui va suivre que 0 n'est pas racine de f dans $k[t]$ i.e. $\alpha_i \neq 0$ dans $k, \forall 1 \leq i \leq l$. Posons $\overline{U} = U \cap D(y)$ et notons $\overline{\mathcal{F}}$ le recouvrement associé aux deux ouverts \overline{U} et W .

Lemme 7.2.1. *Le recouvrement $\overline{\mathcal{F}}$ est un recouvrement de X .*

Preuve: Il suffit de montrer l'égalité des fibres spéciales et génériques i.e.

$$X_k = \bar{U}_k \cup W_k$$

$$X_K = \bar{U}_K \cup W_K.$$

On traite le cas de la fibre spéciale. Soit donc \bar{k} une clôture algébrique de k . On va montrer que $X_k(\bar{k}) = \bar{U}_k(\bar{k}) \cup W_k(\bar{k})$. Par définition

$$X_k(\bar{k}) = \left\{ (t, y) \in \bar{k}^2 \mid tq y^n = f(t) \right\} \cup \left\{ (s, z) \in \bar{k}^2 \mid tq z^n = f_2(s) \right\}$$

où $ts = 1$, $z = s^r y$ et $f_2(s) = f(t)s^{rn}$. Par ailleurs

$$U_k(\bar{k}) = \bar{U}_k(\bar{k}) \cup \left\{ (t, 0) \in \bar{k}^2 \mid tq \cdot 0 = f(t) \right\}$$

or par hypothèse, si $f(t) = 0$ alors $t \neq 0$ et donc

$$\left\{ (t, 0) \in \bar{k}^2 \mid tq \cdot 0 = f(t) \right\} \subset W_k(\bar{k})$$

et donc on a bien l'égalité souhaitée. On montrerait de la même manière le résultat sur la fibre générique ce qui achève la démonstration. \square

Remarque 7.2.2. Puisque y et $\mathbf{f}(t)$ sont liés par $y^n = \mathbf{f}(t)$ il est clair que $\bar{U} = U \cap D(\mathbf{f}(t))$. Par ailleurs puisque $t \wedge \mathbf{f}(t) = 1$ dans $V[t]$, l'inverse de $\mathbf{f}(t)$ est en fait un élément de $V[[t]]$. En effet $\mathbf{f}(t) = \lambda_0 + tw(t) = \lambda_0(1 + a_0^{-1}tw(t))$ avec $\lambda_0 \neq 0$ et $\mathbf{f}(t)^{-1} = \lambda_0^{-1} \sum (-1)^k \lambda_0^{-k} t^k w^k(t) \in V[[t]]$ et on a donc

$$\mathcal{O}_U(U)[\mathbf{f}(t)^{-1}] = V[t, y, \mathbf{f}(t)^{-1}] / (y^n - \mathbf{f}(t)) \subset \bigoplus_{j=1}^{n-1} V[[t]] y^j$$

comme $V[t]$ -module.

On se place désormais sur $X_1 = X \times_{\text{Spec}(V)} \text{Spec}(V/p^2V)$. Alors X_1 est la réunion des deux ouverts affines

$$\begin{aligned} \bar{U}_1 &= \bar{U} \times_{\text{Spec}(V)} \text{Spec}(V/p^2V) \\ W_1 &= W \times_{\text{Spec}(V)} \text{Spec}(V/p^2V). \end{aligned}$$

Le Frobenius de X_k (fibre spéciale de X) admet un relèvement modulo p^2 sur chacun des deux ouverts \bar{U}_1 et W_1 par lissité de ces deux ouverts.

Remarque 7.2.3. La multiplication par p induit une bijection entre $k[t]$ et $pV/p^2V[t]$. Dans toute la suite lorsque Q sera un polynôme de $k[t]$ on fera l'abus d'écrire $pQ(t)$ pour désigner l'image de $Q(t)$ sous cette bijection.

Proposition 7.2.1. *Il existe un relèvement du Frobenius $\bar{U}_1 \rightarrow \bar{U}'_1$, et un polynôme $\mathcal{P}(t)$ de $k[t]$, tel que le relèvement modulo p^2 du Frobenius*

$$F_U : V/p^2V[t, y, y^{-1}]/(y^n - \mathbf{f}^\sigma(t)) \longrightarrow V/p^2V[t, y, y^{-1}]/(y^n - \mathbf{f}(t))$$

soit déterminé par

$$\begin{aligned} F_U(t) &= t^p \\ F_U(y) &= y^p + py^p \left(\frac{\mathcal{P}(t)}{n} y^{-np} \right) \end{aligned}$$

où $\mathcal{P}(t) = (\mathbf{f}^\sigma(t^p) - \mathbf{f}(t)^p) / p$.

Preuve: Ce résultat est inspiré du relèvement du Frobenius donné par Kedlaya dans [Ked01] pour les courbes hyperelliptiques et par Gaudry-Gürel dans [GG01] dans le cas superelliptique. On rappelle que $\mathcal{O}_{X_1}(\bar{U}_1) = V/p^2V[t, \mathbf{f}(t)^{-1}, y]/(y^n - \mathbf{f}(t))$. On cherche un relèvement du Frobenius de la forme $t \mapsto F_U(t) = t^p$ et $y \mapsto F_U(y)$ tels que

$$(F_U(y))^n = \mathbf{f}^\sigma(F_U(t)).$$

Comme $\mathbf{f}^\sigma(t^p) - \mathbf{f}(t)^p \in p(V/p^2V[t])$ l'élément $\mathcal{P}(t) = (\mathbf{f}^\sigma(t^p) - \mathbf{f}(t)^p) / p$ est bien définie et est un polynôme de $k[t]$. On a clairement $\mathbf{f}^\sigma(F_U(t)) = \mathbf{f}^\sigma(t^p) = \mathbf{f}(t)^p + p\mathcal{P}(t)$. Comme y est inversible sur \bar{U}_1 , on peut poser

$$F_U(y) = y^p \left(1 + p \frac{\mathcal{P}(t)}{n} y^{-np} \right).$$

Alors on a

$$(F_U(y))^n = \left(y^p \left(1 + p \frac{\mathcal{P}(t)}{n} y^{-np} \right) \right)^n = y^{np} \sum_{k=0}^n \binom{n}{k} \left(\frac{1}{n} p \mathcal{P}(t) y^{-np} \right)^k.$$

Réduisons maintenant cette expression modulo V/p^2V , alors

$$(F_U(y))^n \equiv \mathbf{f}(t)^p \left(1 + n \left(\frac{1}{n} p \mathcal{P}(t) y^{-np} \right) \right) \equiv \mathbf{f}(t)^p (1 + p \mathcal{P}(t) \mathbf{f}(t)^{-p}) \equiv \mathbf{f}(t)^p + p \mathcal{P}(t).$$

Et donc $(F_U(y))^n = \mathbf{f}^\sigma(F_U(t))$. Reste à vérifier que $F_U(y)$ est inversible, ce qui est simple à faire. En effet dans $\mathcal{O}_{X_1}(\bar{U}_1)$ on a

$$\left(1 + p \frac{\mathcal{P}(t)}{n} y^{-np} \right) \left(1 - p \frac{\mathcal{P}(t)}{n} y^{-np} \right) = 1 - \left(p \frac{\mathcal{P}(t)}{n} y^{-np} \right)^2 = 1$$

donc

$$F_U(y^{-1}) = F_U(y)^{-1} = y^{-p} \left(1 - p \frac{\mathcal{P}(t)}{n} y^{-np} \right) \in \mathcal{O}_{X_1}(\bar{U}_1)$$

ce qui établit que F_U défini par $F_U(t) = t^p$ et $F_U(y) = y^p + py^p (\mathcal{P}(t)/ny^{-np})$ est un endomorphisme d'algèbres qui passe au quotient et montre l'énoncé. □

Proposition 7.2.2. *On conserve les notations précédentes et on note b le reste de la division euclidienne de pj par n pour $1 \leq j \leq n-1$ fixé. Supposons que $\mu_n(\overline{\mathbb{F}_p}) \subset k$ alors le morphisme $F_U : \mathcal{O}_{X_1}(\overline{U_1}) \rightarrow \mathcal{O}_{X_1}(\overline{U_1})$ envoie la j -ième composante isotypique de $\mathcal{O}_{X_1}(\overline{U_1})$ sur la b -ième composante isotypique de $\mathcal{O}_{X_1}(\overline{U_1})$. De plus l'application $j \mapsto b$ est une bijection de $\{1, \dots, n-1\}$.*

Preuve: Soit $1 \leq j \leq n-1$ fixé. On a $F_U(y^j) = y^{pj}(1 + p\mathcal{P}(t)y^{-npj}/n) \in \mathcal{O}_{X_1}(\overline{U_1})$ et donc si on effectue la division euclidienne $pj = an + b$ on a $F_U(y^j) = \mathbf{f}(t)^a y^b (1 + p\mathcal{P}(t)y^{-np}/n)$. Ainsi un élément de la $(n-j)$ -ième composante isotypique est envoyé sur un élément de la $(n-b)$ -ième composante isotypique puisque t et y^n sont invariants par cette action. Par ailleurs comme p est premier à n et que j est strictement inférieur à n , l'application qui à j associe b est bien une bijection. \square

Proposition 7.2.3. *Il existe un relèvement du Frobenius $W_1 \rightarrow W_1'$ et deux polynômes $v(s), b(s)$ de $k[s]$ tels que le relèvement modulo p^2 du Frobenius*

$$F_W : V/p^2V[s, z]/(z^n - \mathbf{f}_2^\sigma(s)) \longrightarrow V/p^2V[s, z]/(z^n - \mathbf{f}_2(s))$$

soit déterminé par

$$\begin{aligned} F_W(s) &= s^p + pv(s) \\ F_W(z) &= z^p + pz^p b(s) \end{aligned}$$

où v et b sont reliés par la relation :

$$\mathbf{f}_2(s)^p - \mathbf{f}_2^\sigma(s^p) = p(v(s)\mathbf{f}_2'(s)^p - nb(s)\mathbf{f}_2(s)^p).$$

Preuve: Par définition on a $\mathbf{f}_2^\sigma(s^p) \equiv \mathbf{f}_2(s)^p$ modulo $p(V/p^2V[s])$ (voir définition 7.1.2) donc il existe un polynôme $Q(s) \in k[s]$ tel que $\mathbf{f}_2(s)^p - \mathbf{f}_2^\sigma(s^p) = pQ(s)$ dans $V/p^2V[s]$. De plus $\mathbf{f}_2 \wedge \mathbf{f}_2' = 1$ dans $k[s]$ (voir lemme 2.1.3) donc il existe deux polynômes, $v_0(s), b_0(s) \in k[s]$ tels que

$$v_0(s)\mathbf{f}_2'(s)^p + b_0(s)\mathbf{f}_2(s)^p = 1$$

et on peut donc trouver deux polynômes $v(s), b(s) \in k[s]$ tels que

$$Q(s) = v(s)\mathbf{f}_2'(s)^p - nb(s)\mathbf{f}_2(s)^p$$

(qui est bien la relation annoncée sur v et b) en posant $v(s) = Q(s)v_0(s)$ et $nb(s) = -Q(s)b_0(s)$. Posons $F_W(s) = s^p + pv(s)$ et $F_W(z) = z^p + pz^p b(s)$ et montrons que cela définit bien un relèvement du Frobenius sur W_1 i.e. que $F_W(z)^n = \mathbf{f}_2^\sigma(F_W(s))$ dans $\mathcal{O}_{X_1}(W_1)$. Avec cette définition $F_W(z)^n = z^{pn}(1 + pb(s))^n = \mathbf{f}_2(s)^p(1 + pb(s))^n$. On utilise alors la formule du binôme de Newton pour développer le second terme et comme on travaille modulo V/p^2V on a finalement $F_W(z)^n = \mathbf{f}_2(s)^p(1 + npb(s)) = \mathbf{f}_2(s)^p + npb(s)\mathbf{f}_2(s)^p = \mathbf{f}_2(s)^p + npb(s)\mathbf{f}_2(s)^p$ car dans V/p^2V on a $p\mathbf{f}_2(s) = \mathbf{f}_2(s)$. En utilisant la relation établie précédemment entre v et b on a donc $F_W(z)^n = \mathbf{f}_2^\sigma(s^p) + pv(s)\mathbf{f}_2'(s)^p \in \mathcal{O}_{X_1}(W_1)$.

Calculons alors $\mathbf{f}_2^\sigma(F_W(s)) = \mathbf{f}_2^\sigma(s^p + pv(s))$. Il est aisé en utilisant la formule du binôme de Newton de montrer que dans $V/p^2V[s]$ on a $(s^p + pv(s))^m = (s^p)^m + pv(s)m(s^p)^{m-1}$ pour tout entier m et donc de montrer que dans V/p^2V on a

$$\mathbf{f}_2^\sigma(s^p + pv(s)) = \mathbf{f}_2^\sigma(s^p) + pv(s)\mathbf{f}'_2^\sigma(s^p) = \mathbf{f}_2^\sigma(s^p) + pv(s)f'_2(s^p).$$

Comme par ailleurs $f'_2(s^p) = f'_2(s)^p$ dans $k[s]$ on a finalement

$$\mathbf{f}_2^\sigma(F_W(s)) = \mathbf{f}_2^\sigma(s^p) + pv(s)f'_2(s)^p = F_W(z)^n \in \mathcal{O}_{X_1}(W_1)$$

ce qui achève la démonstration □

Proposition 7.2.4. *On conserve les notations précédentes et on note b le reste de la division euclidienne de pj par n pour $1 \leq j \leq n-1$ fixé. Supposons que $\mu_n(\overline{\mathbb{F}_p}) \subset k$ alors le morphisme $F_W : \mathcal{O}_{X_1}(W_1) \rightarrow \mathcal{O}_{X_1}(W_1)$ envoie la j -ième composante isotypique de $\mathcal{O}_{X_1}(W_1)$ sur la b -ième composante isotypique de $\mathcal{O}_{X_1}(W_1)$. De plus l'application $j \mapsto b$ est une bijection de $\{1, \dots, n-1\}$.*

Preuve: Soit $1 \leq j \leq n-1$ fixé. On a $F_W(z^j) = z^{pj}(1 + pb(s))$ et donc si on effectue la division euclidienne $pj = an + b$ on a $F_W(z^j) = \mathbf{f}_2(s)^a z^b (1 + pb(s))$. Comme s est invariant par δ on a bien le résultat annoncé. Par ailleurs comme p est premier à n et que j est strictement inférieur à n , l'application qui à j associe b est bien une bijection. □

Proposition 7.2.5. *Considérons $v(s)$ tel que défini dans la proposition 7.2.3, alors*

$$f_2(s)^{p-1} | (v'(s) + s^{p-1})$$

dans $k[s]$.

Preuve: On a $pQ(s) = \mathbf{f}_2(s)^p - \mathbf{f}_2^\sigma(s^p)$ donc $pQ'(s) = p\mathbf{f}'_2(s)\mathbf{f}_2(s)^{p-1} - p s^{p-1}\mathbf{f}'_2^\sigma(s^p)$ dans $V/p^2V[s]$. Soit après simplification par p , $Q'(s) = f'_2(s)f_2(s)^{p-1} - s^{p-1}f'_2^\sigma(s^p)$ dans $k[s]$. D'autre part $Q'(s) = v'(s)f'_2(s)^p - nb'(s)f_2(s)^p$ dans $k[s]$ et comme $f'_2^\sigma(s^p) = f'_2(s^p) = f'_2(s)^p$ dans $k[s]$ on obtient

$$f_2(s)^{p-1}(f'_2(s) + nb'(s)f_2(s)) = f'_2(s)^p(v'(s) + s^{p-1}) \in k[s]$$

mais $f_2 \wedge f'_2 = 1$ dans $k[s]$ (voir lemme 2.1.3) et donc $f_2(s)^{p-1} | (v'(s) + s^{p-1})$ dans $k[s]$. □

7.3 Calcul du morphisme de Deligne-Illusie

Notation. Dans la suite si \mathcal{E} est un faisceau sur X , si x est une section locale de \mathcal{E} sur un ouvert \mathcal{U} de X on notera $x \in \mathcal{E}$.

On rappelle que $\overline{\mathcal{F}}_k$ est le recouvrement de la courbe X_k par les deux ouverts \overline{U}_k et W_k . Alors le complexe de Čech associé est :

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \uparrow & & \uparrow & & \\
 0 & \rightarrow & \Omega_{X_k}^1(\overline{U}_k) \times \Omega_{X_k}^1(W_k) & \rightarrow & \Omega_{X_k}^1(\overline{U}_k \cap W_k) & \rightarrow & 0 \\
 & & \uparrow & & \uparrow & & \\
 0 & \rightarrow & \mathcal{O}_{X_k}(\overline{U}_k) \times \mathcal{O}_{X_k}(W_k) & \rightarrow & \mathcal{O}_{X_k}(\overline{U}_k \cap W_k) & \rightarrow & 0 \\
 & & \uparrow & & \uparrow & & \\
 & & 0 & & 0 & &
 \end{array}$$

auquel on peut associer le complexe simple suivant :

$$0 \rightarrow \mathcal{O}_{X_k}(\overline{U}_k) \times \mathcal{O}_{X_k}(W_k) \rightarrow \Omega_{X_k}^1(\overline{U}_k) \times \Omega_{X_k}^1(W_k) \oplus \mathcal{O}_{X_k}(\overline{U}_k \cap W_k) \rightarrow \Omega_{X_k}^1(\overline{U}_k \cap W_k) \rightarrow 0.$$

De la même manière on a un complexe double et un complexe simple associés au recouvrement $\overline{\mathcal{F}}_1$ (resp. $\overline{\mathcal{F}}$) de X_1 (resp. X) par \overline{U}_1 et W_1 (resp. \overline{U} et W). On se place ici sur la fibre spéciale X_k . Ainsi on considère les ouverts \overline{U}_k et W_k et on travaille donc modulo p .

Le choix d'un relèvement de Frobenius sur les deux ouverts affines \overline{U}_1 et W_1 permet de construire un morphisme $\mathcal{O}_{X'_k}$ -linéaire

$$DI : \bigoplus_{i=0}^1 \Omega_{X'_k}^i[-i] \rightarrow F_* \check{C}(\overline{\mathcal{F}}_k, \Omega_{X_k}^\bullet)$$

en suivant la méthode donnée par Illusie dans [Ill96] au paragraphe 5.1. On notera Φ le morphisme induit $\Phi : H^1(X'_k, \mathcal{O}_{X'_k}) \oplus H^0(X'_k, \Omega_{X'_k}^1) \rightarrow H_{DR}^1(X_k)$.

Définition 7.3.1. Soit F_U un relèvement du Frobenius modulo p^2 . Il induit $U_1 \rightarrow U'_1$ et donc une application $F_U^{-1} : \mathcal{O}_{U'_1} \rightarrow \mathcal{O}_{U_1}$ et $dF_U : F_U^* \Omega_{U'_1}^1 \rightarrow \Omega_{U_1}^1$.

Or d'après la proposition 3.8 (c) de [Ill96], comme F_U relève le Frobenius relatif en caractéristique $p > 0$, l'image de cette application est à valeurs dans $p\Omega_{U_1}^1$ et on peut donc considérer l'application $p^{-1}dF_U : F_{U_1}^* \Omega_{U'_1}^1 \rightarrow \Omega_{U_k}^1$ qui se factorise en une application $f_U : F_{rel} \Omega_{U'_k}^1 \rightarrow \Omega_{U_k}^1$ appelée Frobenius divisé différentiel.

Définition 7.3.2. Soient $F : X_k \rightarrow X'_k$ le Frobenius relatif, X_1 un relèvement de X_k sur V/p^2V et $\mathcal{F} = (\mathcal{U}_i)$ un recouvrement d'ouverts de X_k tel que pour chaque i on ait un relèvement Z_i de \mathcal{U}_i sur V/p^2V et un relèvement $G_i : Z_i \rightarrow X_1$ de $F|_{\mathcal{U}_i}$. Alors pour chaque i on dispose d'un Frobenius divisé différentiel

$$f_i : \Omega_{\mathcal{U}'_i}^1 \rightarrow F_* \Omega_{\mathcal{U}_i}^1$$

et pour chaque couple (i, j) de l'homomorphisme

$$h_{i,j} : \Omega_{X'}^1 \rightarrow F_* \mathcal{O}_{\mathcal{U}_i \cap \mathcal{U}_j}$$

liés par $\forall \omega \in \Omega_{X'}^1$,

$$f_j(\omega|_{\mathcal{U}'_j}) - f_i(\omega|_{\mathcal{U}'_i}) = dh_{ij}(\omega)|_{\mathcal{U}_i \cap \mathcal{U}_j} \text{ sur } \mathcal{U}_i \cap \mathcal{U}_j \quad (7.1)$$

$$h_{i,j}(\omega) + h_{j,k}(\omega) = h_{i,k}(\omega) \text{ sur } \mathcal{U}_i \cap \mathcal{U}_j \cap \mathcal{U}_k \quad (7.2)$$

qui permettent de construire le morphisme $\mathcal{O}_{X'_k}$ -linéaire évoqué plus haut.

Remarque 7.3.1. Dans notre cas les choses sont plus simples puisqu'on dispose d'un recouvrement à deux ouverts de X_1 par \bar{U}_1 et W_1 sur lesquels nous avons déjà calculé un relèvement du Frobenius (voir propositions 7.2.1 et 7.2.3). Il n'y a alors qu'à construire f_1 et f_2 , qui sont en fait f_U et f_W le Frobenius divisé sur \bar{U}_k respectivement W_k (voir définition 7.3.1) et h devant vérifier la conditions 7.1.

Proposition 7.3.1. En degré 0, $DI_0 : \mathcal{O}_{X'_k} \rightarrow F_*\mathcal{O}_{\bar{U}_k} \oplus F_*\mathcal{O}_{W_k}$ est donné par le Frobenius relatif F i.e. $DI_0(\alpha) = (F(\alpha)|_{\bar{U}_k}, F(\alpha)|_{W_k})$.

En degré 1,

$$\begin{aligned} DI_1 : \quad \Omega_{X'_k}^1 &\longrightarrow F_*\Omega_{\bar{U}_k}^1 \oplus F_*\Omega_{W_k}^1 \oplus F_*\mathcal{O}_{\bar{U}_k \cap W_k} \\ \omega = \alpha_0 dt = \alpha_1 ds &\longmapsto (\alpha_0^p f_U(dt), \alpha_1^p f_W(ds), \alpha_0^p h(dt)) \end{aligned}$$

où f_U est le Frobenius divisé différentiel sur \bar{U}_k , f_W est le Frobenius divisé différentiel sur W_k (voir définition 7.3.1) correspondants aux relèvement du Frobenius donnés par les propositions 7.2.1 et 7.2.3 et h vérifie la condition 7.1. On remarque que

$$\begin{aligned} f_U(dt) &= t^{p-1} dt \\ f_W(ds) &= (s^{p-1} + v'(s)) ds \\ h(dt) &= t^{2p} v(s) \end{aligned}$$

où v est le polynôme du relèvement du Frobenius sur W_1 (voir proposition 7.2.3).

Preuve: En ce qui concerne le degré 0 il n'y a rien à montrer. En degré 1, f_U (resp. f_W) est simplement le Frobenius divisé associé au relèvement du Frobenius sur \bar{U}_1 (resp. W_1).

On rappelle que sur \bar{U}_1 le relèvement du Frobenius (modulo p^2) choisi vérifie $F_U(t) = t^p$. Alors on a $F_U(dt) = dF_U(t) = d(t^p) = pt^{p-1} dt$. Or par définition

$$f_U(dt) = \frac{F_U(dt)}{p} = \frac{pt^{p-1} dt}{p} = t^{p-1} dt \in \Omega_{X'_k}^1.$$

Sur W_1 , $F_W(s) = s^p + pv(s)$. Alors $F_W(ds) = dF_W(s) = d(s^p + pv(s)) = p(s^{p-1} + v'(s)) ds$. D'où

$$f_W(ds) = \frac{F_W(ds)}{p} = \frac{p(s^{p-1} + v'(s)) ds}{p} = (s^{p-1} + v'(s)) ds \in \Omega_{X'_k}^1.$$

Par définition h est une application définie sur $\bar{U}_k \cap W_k$ vérifiant $f_U(dt) - f_W(dt) = dh(dt)$.

On rappelle que t est un paramètre sur $\bar{U}_k \cap W_k$. Calculons $f_W(dt)$. Comme $t = s^{-1}$ alors $dt = -s^{-2} ds$, d'où

$$f_W(dt) = f_W(-s^{-2} ds) = (-s^{-2})^p f_W(ds) = -s^{-2p} (s^{p-1} + v'(s)) ds.$$

On a donc $dh(dt) = f_U(dt) - f_W(dt) = t^{p-1}dt - (-s^{-2p}(s^{p-1} + v'(s))ds)$. Utilisons à nouveau les relations entre s et t pour simplifier cette expression :

$$dh(dt) = t^{p-1}dt - (-t^{2p}(t^{1-p} + v'(1/t)))(-t^{-2}dt) = -t^{2p-2}v'(1/t)dt = t^{2p}(-1/t^2)v'(1/t)dt \text{ d'où}$$

$$dh(dt) = t^{2p}(v(1/t))'.$$

Enfin X_k étant un k -schéma, on a $(t^{2p})' = 2pt^{2p-1}dt = 0$ d'où $(t^{2p}v(s))' = t^{2p}(v(1/t))'$ sur $\bar{U}_k \cap W_k$ et donc $h(dt) = t^{2p}v(s)$. Par définition il est clair que sur $\bar{U}_k \cap W_k$ la relation $f_W - f_U + dh$ est vérifiée.

Enfin la construction du morphisme de Deligne et Illusie garantit que $f_U(\omega) \in F_*\Omega_{X_k}^1(\bar{U}_k)$, $f_W(\omega) \in F_*\Omega_{X_k}^1(W_k)$ et $h(\omega) \in F_*\mathcal{O}_{X_k}(\bar{U}_k \cap W_k)$, $\forall \omega \in \Omega_{X'_k}^1(X'_k)$. □

Remarque 7.3.2. Une base de $H^0(X'_k, \Omega_{X'_k}^1)$ est donnée par $\omega'_{i,j} = t^i y^{-j} dt$ avec $1 \leq j \leq n-1$ et $0 \leq i \leq rj-2$ (voir proposition 7.1.1). On a donc

$$\begin{aligned} f_U(\omega'_{i,j}) &= \frac{t^{p(i+1)-1}}{y^{pj}} dt \in \Omega_{X_k}^1(\bar{U}_k) \\ f_W(\omega'_{i,j}) &= -s^{p(rj-(i+2))} \frac{(s^{p-1} + v'(s))}{z^{pj}} ds \in \Omega_{X_k}^1(W_k) \\ h(\omega'_{i,j}) &= \frac{t^{p(i+2)}}{y^{pj}} v(s) \in \mathcal{O}_{X_k}(\bar{U}_k \cap W_k). \end{aligned}$$

Soit encore, en notant a le quotient de la division euclidienne de pj par n et b son reste (non nul puisque $n \wedge p = 1$ et $1 \leq j \leq n-1$)

$$\begin{aligned} f_U(\omega'_{i,j}) &= \frac{t^{p(i+1)-1}}{f(t)^a} \frac{dt}{y^b} \\ f_W(\omega'_{i,j}) &= -s^{p(rj-(i+2))} \frac{(s^{p-1} + v'(s))}{f_2(s)^a} \frac{ds}{z^b} \\ h(\omega'_{i,j}) &= \frac{t^{p(i+2)}}{f(t)^{a+1}} v(s) y^{n-b}. \end{aligned}$$

Enfin grâce à la proposition 7.2.5 on constate qu'on a bien

$$f_W(\omega'_{i,j}) \in k[s] \frac{ds}{z^b} \subset \Omega_W^1 = \bigoplus_{i=0}^n k[s] \frac{ds}{y^j}.$$

En effet $a < p$ car si on avait $a \geq p$ alors $pj = an + b \geq pn + b \geq pn > p(n-1) \geq pj$ ce qui est absurde. Ainsi $f_2(s)^a | f_2(s)^{p-1}$ dans $k[s]$ et on conclut grâce à la proposition 7.2.5.

Lemme 7.3.1. Notons \mathcal{F}'_k le recouvrement de X'_k par les deux ouverts \bar{U}'_k et W'_k et $\check{C}(\mathcal{F}'_k, \mathcal{O}_{X'_k})$ le complexe de Čech de $\mathcal{O}_{X'_k}$ relativement à \mathcal{F}'_k .

(i) Le morphisme DI_0 induit par functorialité un morphisme de complexes

$$\alpha : \check{C}(\mathcal{F}'_k, \mathcal{O}_{X'_k}) \rightarrow \check{C}(\mathcal{F}_k, \Omega_{X_k}^\bullet)$$

CHAPITRE 7. MISE EN PLACE DU CALCUL DU FROBENIUS DIVISÉ DE LA FIBRE SPÉCIALE

donné par

$$\begin{array}{ccccccc}
 0 & \longrightarrow & \mathcal{O}_{X'_k}(\overline{U}'_k) \times \mathcal{O}_{X'_k}(W'_k) & \longrightarrow & \mathcal{O}_{X'_k}(\overline{U}'_k \cap W'_k) & \longrightarrow & 0 \\
 & & \downarrow \alpha_0 & & \downarrow \alpha_1 & & \downarrow \\
 0 & \longrightarrow & \mathcal{O}_{X_k}(\overline{U}_k) \times \mathcal{O}_{X_k}(W_k) & \longrightarrow & \Omega^1_{X_k}(\overline{U}_k) \times \Omega^1_{X_k}(W_k) \oplus \mathcal{O}_{X_k}(\overline{U}_k \cap W_k) & \longrightarrow & \Omega^1_{X_k}(\overline{U}_k \cap W_k) \longrightarrow 0
 \end{array}$$

avec $\alpha_0(h_1, h_2) = (F^\#(h_1), F^\#(h_2))$ et $\alpha_1(h) = (0, 0, F^\#(h))$.

(ii) Le morphisme induit par $DI_0, H^1(X'_k, \mathcal{O}_{X'_k}) \rightarrow H^1_{DR}(X_k)$ est donc induit par le morphisme de complexes α précédent.

Preuve: Il est clair que α ainsi défini est bien un morphisme de complexes. □

Proposition 7.3.2. *On conserve les notations précédentes. Soit $1 \leq j \leq n - 1$ fixé, notons b le reste de la division euclidienne de pj par n . Enfin supposons que $\mu_n(\overline{\mathbb{F}_p}) \subset k$, alors le morphisme de Deligne-Illusie induit un isomorphisme*

$$(H^0(X_k, \Omega^1_{X_k}))_j \oplus (H^1(X_k, \mathcal{O}_{X_k}))_j \simeq (H^1_{DR}(X))_{\lfloor pj/n \rfloor}$$

où l'indexation par j désigne le sous-espace correspondant à la j -ième composante isotypique.

Preuve: Les arguments de la démonstration sont à nouveau sensiblement les mêmes que pour les propositions 6.0.7, 7.2.2 et 7.2.4. Par définition du Frobenius relatif, il est évident qu'en degré 0 un élément de la j -ième composante isotypique de $\mathcal{O}_{X'_k}$ est envoyé sur un élément de la b -ième composante isotypique de $F_*\mathcal{O}_{\overline{U}_k} \oplus F_*\mathcal{O}_{W_k}$ où b est le reste de la division euclidienne de pj par n .

En degré 1, grâce aux formules explicites données dans la remarque précédente on peut dire également qu'un élément de la j -ième composante isotypique de $H^0(X_k, \Omega^1_{X_k})$ est envoyé sur un élément de la b -ième composante isotypique de $F_*\Omega^1_{\overline{U}_k} \oplus F_*\Omega^1_{W_k} \oplus F_*\mathcal{O}_{\overline{U}_k \cap W_k}$ avec toujours b reste de la division euclidienne de pj par n .

Les mêmes arguments que précédemment permettent d'affirmer que $j \mapsto b$ est une permutation. Enfin puisque le morphisme de Deligne-Illusie est un isomorphisme, cela donne un isomorphisme au niveau de composantes isotypiques. □

Remarque 7.3.3. Plus généralement même lorsque la condition $\mu_n(\overline{\mathbb{F}_p}) \subset k$ n'est pas vérifiée, définissons $(H^0(X_k, \Omega^1_{X_k}))_j$ comme étant le sous-espace de $H^0(X_k, \Omega^1_{X_k})$ engendré par $t^i y^{-j} dt$ pour $0 \leq i \leq rj - 2$ et $(H^1(X_k, \mathcal{O}_{X_k}))_j$ comme étant le sous-espace de $H^1(X_k, \mathcal{O}_{X_k})$ engendré par $t^{-i} y^{n-j}$ pour $1 \leq i \leq r(n - j) - 1$, c'est-à-dire ce que l'on pourrait appeler par abus de langage la j -ième composante isotypique de ces espaces respectifs. Alors comme précédemment on peut montrer que le morphisme de Deligne-Illusie induit un isomorphisme

$$(H^0(X_k, \Omega^1_{X_k}))_j \oplus (H^1(X_k, \mathcal{O}_{X_k}))_j \simeq (H^1_{DR}(X))_{\lfloor pj/n \rfloor}$$

où $(H^1_{DR}(X))_j$ j désigne le sous-espace qui correspondrait à la j -ième composante isotypique. Cela nous permet de conclure qu'il y a une permutation des "composantes isotypiques" par le

morphisme de Deligne-Illusie et donc que la matrice du Frobenius présentera des blocs de zéros et $n - 1$ blocs inversibles de taille $rn - 2 = l - 1$ (qui correspond bien à une matrice de taille $(n - 1)(l - 1) = 2g$). Il est donc possible de choisir une présentation de la matrice à la fois adaptée à cette permutation et à la filtration. Pour des raisons de simplicité d'écriture on choisira cependant une présentation uniquement adaptée à la filtration (voir section 8.1).

7.4 Calcul de la matrice du Frobenius divisé sur $H_{DR}^1(X_k)$

Ce qui suit repose sur le lemme suivant.

Lemme 7.4.1. *Soit V un anneau, soit $0 \rightarrow E \xrightarrow{i} F \xrightarrow{s} G \rightarrow 0$ une suite exacte de V -modules et soit $\tau : G \rightarrow F$ un scindage de la suite exacte. Alors on déduit de τ un isomorphisme :*

$$\begin{aligned} E \oplus G &\xrightarrow{\sim} F \\ (x, y) &\longmapsto i(x) + \tau(y). \end{aligned}$$

Dans notre cas, $E = H^0(X_k, \Omega_{X_k}^1)$, $G = H^1(X_k, \mathcal{O}_{X_k})$ et $F = H_{DR}^1(X_k)$. Par ailleurs nous avons déjà calculé un scindage de cette suite exacte dans la proposition 6.0.6. Dans la suite, on calcule Φ le Frobenius divisé, qui a été défini à la section 7.1, sur $H^0(X'_k, \Omega_{X'_k}^1) \oplus H^1(X'_k, \mathcal{O}_{X'_k})$. On utilise le scindage construit au chapitre 6 pour identifier $H_{DR}^1(X_k)$, qui est isomorphe à $H^1(\check{C}(\mathcal{F}, \Omega_{X_k}^\bullet))$, à $H^1(X_k, \mathcal{O}_{X_k}) \oplus H^0(X_k, \Omega_{X_k}^1)$.

Définition 7.4.1. *On rappelle quelques définitions et notations qui serviront dans toute cette section. L'identification de $H^1(X_k, \mathcal{O}_{X_k})$ à $\mathcal{O}_{X_k}(\overline{U}_k \cap W)/\text{Im}(d_{0,1})$ induit (voir remarque 6.0.4)*

$$\iota : H^1(X_k, \mathcal{O}_{X_k}) \rightarrow \mathcal{O}_{X_k}(\overline{U}_k \cap W)$$

ainsi que

$$\overline{\dots} : \mathcal{O}_{X_k}(\overline{U}_k \cap W) \rightarrow H^1(X_k, \mathcal{O}_{X_k}).$$

Par ailleurs on a construit à la proposition 6.0.3

$$\tau : H^1(X_k, \mathcal{O}_{X_k}) \rightarrow \Omega_{X_k}^1(\overline{U}_k) \times \Omega_{X_k}^1(W_k) \times \mathcal{O}_{X_k}(\overline{U}_k \cap W)$$

et enfin on note

$$[\dots] : \Omega_{X_k}^1(\overline{U}_k) \times \Omega_{X_k}^1(W_k) \times \mathcal{O}_{X_k}(\overline{U}_k \cap W) \rightarrow H^1(\check{C}(\mathcal{F}, \Omega_{X_k}^\bullet)).$$

On notera enfin P_1 (resp. P_2) la projection de $H^1(X_k, \mathcal{O}_{X_k}) \oplus H^0(X_k, \Omega_{X_k}^1)$ sur le premier (resp. le second) facteur.

CHAPITRE 7. MISE EN PLACE DU CALCUL DU FROBENIUS DIVISÉ DE LA FIBRE SPÉCIALE

Proposition 7.4.1. *Soit $\omega_{i,j} = t^i y^{-j} dt \in H^0(X_k, \Omega_{X_k}^1)$ un élément de la base (donnée à la proposition 4.1.1), posons $h = h(\omega'_{i,j}) - \iota(\overline{h(\omega'_{i,j})}) \in \mathcal{O}_{X_k}(\overline{U}_k \cap W_k)$. Il existe $h_U \in \mathcal{O}_{X_k}(\overline{U}_k)$ et $h_W \in \mathcal{O}_{X_k}(W_k)$ tels que $h = h_U + h_W$. Enfin notons $(\beta_U^{ij}, -\beta_W^{ij}, \iota(\overline{h(\omega'_{i,j})})) = \tau(\overline{h(\omega'_{i,j})})$, alors*

$$P_1(\Phi(\omega_{i,j})) = \overline{h(\omega'_{i,j})}$$

$$P_2(\Phi(\omega_{i,j})) = f_W(\omega'_{i,j}) + \beta_W^{ij} + dh_W.$$

Preuve: On a vu à la section 7.1 que $\Phi(\omega_{i,j}) = \Phi'(\omega'_{i,j})$ et $\Phi(\overline{h(\omega'_{i,j})}) = \Phi'(\overline{h(\omega'_{i,j})})$. Or sur $H^0(X'_k, \Omega_{X'_k}^1)$ on a $\Phi'(\omega) = [DI_1(\omega)]$ donc $P_1(\Phi(\omega_{i,j})) = P_1(\Phi'(\omega'_{i,j})) = \overline{h(\omega'_{i,j})}$.

En ce qui concerne le second point il s'agit en fait de calculer la classe de $DI_1(\omega'_{i,j})$ dans $H^1(\check{C}(\mathcal{F}, \Omega_{X_k}^\bullet))$. En utilisant les notations de l'énoncé on a

$$\begin{aligned} DI_1(\omega'_{i,j}) &= (f_U(\omega'_{i,j}), f_W(\omega'_{i,j}), h(\omega'_{i,j})) = (\beta_U^{ij}, -\beta_W^{ij}, \iota(\overline{h(\omega'_{i,j})})) \\ &\quad + (dh_U, -dh_W, h_U + h_W) + (f_U(\omega'_{i,j}) - \beta_U^{ij} - dh_U, f_W(\omega'_{i,j}) + \beta_W^{ij} + dh_W, 0) \end{aligned}$$

Or le triplet $(dh_U, -dh_W, h_U + h_W)$ est clairement un bord du complexe de Čech puisqu'il est l'image de $(h_U, -h_W)$ par l'application

$$\begin{aligned} \mathcal{O}_{X_k}(\overline{U}_k) \oplus \mathcal{O}_{X_k}(W_k) &\rightarrow \Omega_{X_k}^1(\overline{U}_k) \oplus \Omega_{X_k}^1(W_k) \oplus \mathcal{O}_{X_k}(\overline{U}_k \cap W_k) \\ (a, b) &\mapsto (da, db, (a - b)|_{\mathcal{O}_{X_k}(\overline{U}_k \cap W_k)}) \end{aligned}$$

et est donc de classe nulle dans $H^1(\check{C}(\mathcal{F}, \Omega_{X_k}^\bullet))$.

En ce qui concerne le dernier triplet on a $f_U(\omega'_{i,j}) - \beta_U^{ij} - dh_U - (f_W(\omega'_{i,j}) + \beta_W^{ij} + dh_W) = 0$ ce qui signifie donc que $f_W(\omega'_{i,j}) + \beta_W^{ij} + dh_W$ (resp. $f_U(\omega'_{i,j}) - \beta_U^{ij} - dh_U$) définit une section globale de $H^0(X_k, \Omega_{X_k}^1)$ qui est donc l'image recherchée de la projection de $\Phi(\omega_{i,j})$ sur $H^0(X_k, \Omega_{X_k}^1)$. Ce qui achève la démonstration.

Par ailleurs on a choisi d'exprimer cette section globale sur l'ouvert W_k pour des questions de calcul pratique qui seront détaillées plus loin. □

Définition 7.4.2. *Par définition $\overline{U}_k = U_k \cap D(y)$ donc la décomposition en somme directe de $\Omega_{X_k}^1(\overline{U}_k)$ et $\Omega_{X_k}^1(W_k)$ donnée par le lemme 4.1.1 permet de définir les projecteurs suivants :*

$$q_U : \Omega_{X_k}^1(\overline{U}_k) \rightarrow H^0(X_k, \Omega_{X_k}^1)$$

$$q_W : \Omega_{X_k}^1(W_k) \rightarrow H^0(X_k, \Omega_{X_k}^1)$$

qui vont servir par la suite.

Remarque 7.4.1. On sait que $f_W(\omega'_{i,j}) + \beta_W^{ij} + dh_W$ est une section globale de $H^0(X_k, \Omega_{X_k}^1)$ par la démonstration de la proposition précédente. Ce n'est pas le cas de $f_W(\omega'_{i,j})$, β_W^{ij} et dh_W qui sont seulement des éléments de $\Omega_{X_k}^1(W_k)$. Cependant on a

$$f_W(\omega'_{i,j}) + \beta_W^{ij} + dh_W = q_W(f_W(\omega'_{i,j}) + \beta_W^{ij} + dh_W) = q_W(f_W(\omega'_{i,j})) + q_W(\beta_W^{ij}) + q_W(dh_W)$$

ce qui signifie que pour les calculs effectifs il suffit de calculer les projections de $f_W(\omega'_{i,j})$, β_W^{ij} et dh_W sur $H^0(X_k, \Omega_{X_k}^1)$.

Proposition 7.4.2. *Soit $\overline{h_{i,j}} = \overline{t^{-i}y^j} \in H^1(X_k, \mathcal{O}_{X_k})$ un élément de la base (donnée à la proposition 6.0.5), posons $h = h_{i,j}^p - \iota(\overline{h_{i,j}}) \in \mathcal{O}_{X_k}(\overline{U}_k \cap W_k)$. Il existe $h_U \in \mathcal{O}_{X_k}(\overline{U}_k)$ et $h_W \in \mathcal{O}_{X_k}(W_k)$ tels que $h = h_U + h_W$. Enfin notons $(\beta_U^{ij}, -\beta_W^{ij}, \iota(\overline{h_{i,j}})) = \tau(\overline{h_{i,j}})$, alors*

$$\begin{aligned} P_1(\Phi(\overline{h_{i,j}})) &= \overline{h_{i,j}^p} \\ P_2(\Phi(\overline{h_{i,j}})) &= -\beta_U^{ij} - dh_U. \end{aligned}$$

Preuve: On utilise à nouveau le fait que $\Phi(\omega_{i,j}) = \Phi'(\omega'_{i,j})$ et $\Phi(\overline{h_{i,j}}) = \Phi'(\overline{h'_{i,j}})$. Par le lemme 7.3.1, sur $H^1(X_k, \mathcal{O}_{X_k})$ on a $\Phi'(\overline{h'_{i,j}}) = [(0, 0, h_{i,j}^p)]$ donc $P_1(\Phi(\overline{h_{i,j}})) = \overline{h_{i,j}^p}$.

En ce qui concerne le second point il s'agit à nouveau de calculer la classe de $DI_0(\overline{h'_{i,j}})$ dans $H^1(\check{C}(\mathcal{F}, \Omega_{X_k}^\bullet))$. Toujours à l'aide du lemme 7.3.1 et en utilisant les notation de l'énoncé on a donc :

$$(0, 0, h_{i,j}^p) = (\beta_U^{ij}, -\beta_W^{ij}, \iota(\overline{h_{i,j}})) + (dh_U, -dh_W, h_U + h_W) + (-\beta_U^{ij} - dh_U, \beta_W^{ij} + dh_W, 0).$$

A nouveau le triplet $(dh_U, -dh_W, h_U + h_W)$ est un bord du complexe de Čech et est donc de classe nulle dans $H^1(\check{C}(\mathcal{F}, \Omega_{X_k}^\bullet))$.

En ce qui concerne le dernier triplet on a $-\beta_U^{ij} - dh_U - (\beta_W^{ij} + dh_W) = 0$ ce qui signifie donc que $-\beta_U^{ij} - dh_U$ (resp. $\beta_W^{ij} + dh_W$) définit une section globale de $H^0(X_k, \Omega_{X_k}^1)$ qui est donc l'image recherchée de la projection de $\Phi(\overline{h_{i,j}})$ sur $H^0(X_k, \Omega_{X_k}^1)$. Ce qui achève la démonstration. \square

Remarque 7.4.2. On sait que $-\beta_U^{ij} - dh_U$ est une section globale de $H^0(X_k, \Omega_{X_k}^1)$ grâce à la démonstration de la proposition précédente. Ce n'est pas le cas de β_U^{ij} et dh_U qui sont seulement des éléments de $\Omega_{X_k}^1(\overline{U}_k)$. Mais

$$-\beta_U^{ij} - dh_U = q_U(-\beta_U^{ij} - dh_U) = -q_U(\beta_U^{ij}) - q_U(dh_U)$$

et pour les calculs effectifs il suffit de calculer les projections de β_U^{ij} et dh_U sur $H^0(X_k, \Omega_{X_k}^1)$.

Remarque 7.4.3. Pour pouvoir effectivement calculer la matrice de Φ il ne reste plus qu'à expliciter pour chaque élément de $\mathcal{O}_{X_k}(\overline{U}_k \cap W_k)$ sa classe d'équivalence dans $H^1(X_k, \mathcal{O}_{X_k})$.

7.5 Calcul des classes d'éléments de $\mathcal{O}_{X_k}(\overline{U}_k \cap W_k)$

On considère l'application

$$\begin{aligned} d : \mathcal{O}_{X_k}(\overline{U}_k) \times \mathcal{O}_{X_k}(W_k) &\rightarrow \mathcal{O}_{X_k}(\overline{U}_k \cap W_k) \\ (a, b) &\mapsto a - b|_{\overline{U}_k \cap W_k}. \end{aligned}$$

CHAPITRE 7. MISE EN PLACE DU CALCUL DU FROBENIUS DIVISÉ DE LA FIBRE SPÉCIALE

alors $H^1(X_k, \mathcal{O}_{X_k}) = \mathcal{O}_{X_k}(\overline{U}_k \cap W_k)/\text{Im}(d)$. On commence par expliciter d sur les éléments de la base de $\mathcal{O}_{X_k}(\overline{U}_k) \times \mathcal{O}_{X_k}(W_k)$. Pour cela montrons que toutes ces algèbres se plongent dans l'algèbre $A = k[[t]][t^{-1}][y]/(y^n - f(t))$ (où $k[[t]][t^{-1}]$ est l'algèbre des séries de Laurent).

Remarque 7.5.1. Comme $k[[t]]$ -module,

$$A = \bigoplus_{j=0}^{n-1} k[[t]][t^{-1}]y^j.$$

Lemme 7.5.1. On a $\mathcal{O}_{X_k}(\overline{U}_k) \subset A$ et plus précisément

$$\mathcal{O}_{X_k}(\overline{U}_k) \subset \bigoplus_{j=0}^{n-1} k[[t]]y^j$$

comme $k[[t]]$ -module.

Preuve: Comme $\overline{U}_k = U_k \cap D(y) = U_k \cap D(f(t))$, alors $\overline{U}_k = \text{Spec}(k[t, y, f(t)^{-1}]/y^n - f(t))$. Par ailleurs, $f(t)$ admet un inverse dans $k[[t]]$ (car $t \wedge f(t) = 1$ dans $k[t]$ voir lemme 2.1.1) et on a donc

$$\mathcal{O}_{X_k}(\overline{U}_k) \subset k[[t]][y]/(y^n - f(t))$$

ce qui donne clairement le résultat annoncé (et donc l'inclusion dans A). □

Lemme 7.5.2. On a $\mathcal{O}_{X_k}(W_k) \subset A$ et plus précisément

$$\mathcal{O}_{X_k}(W_k) = \bigoplus_{j=0}^{n-1} k[t^{-1}]t^{-rj}y^j$$

et

$$\mathcal{O}_{X_k}(W_k) = \bigoplus_{j=0}^{n-1} \bigoplus_{\alpha \geq rj} kt^{-\alpha}y^j$$

comme k -espace vectoriel

Preuve: Par définition $W_k = \text{Spec}(k[s, z]/(z^n - f_2(s)))$ d'où

$$\mathcal{O}_{X_k}(W_k) = \bigoplus_{j=0}^{n-1} k[s]z^j.$$

Par ailleurs sur $\overline{U}_k \cap W_k$ on a les relations $s = t^{-1}$, $z = t^{-r}y$ et alors par abus de notations on peut écrire

$$\mathcal{O}_{X_k}(W_k) = \bigoplus_{j=0}^{n-1} k[t^{-1}]t^{-rj}y^j$$

ce qui donne la première égalité, la seconde en est une conséquence immédiate. L'inclusion dans A est alors évidente. □

Lemme 7.5.3. *On a $\mathcal{O}_{X_k}(\overline{U}_k \cap W_k) \subset A$ et plus précisément comme k -espace vectoriel on a*

$$\mathcal{O}_{X_k}(\overline{U}_k \cap W_k) = \mathcal{O}_{X_k}(\overline{U}_k) \oplus \left(\bigoplus_{\alpha > 0} kt^{-\alpha} \oplus \bigoplus_{j=1}^{n-1} \bigoplus_{\alpha=1}^{rj-1} kt^{-\alpha} y^j \oplus \bigoplus_{j=1}^{n-1} \bigoplus_{\alpha \geq rj} kt^{-\alpha} y^j \right)$$

ou encore

$$\mathcal{O}_{X_k}(\overline{U}_k \cap W_k) = \mathcal{O}_{X_k}(\overline{U}_k) \oplus \widehat{\mathcal{O}_{X_k}(W_k)} \oplus \bigoplus_{j=1}^{n-1} \bigoplus_{\alpha=1}^{rj-1} kt^{-\alpha} y^j$$

où l'on a posé

$$\widehat{\mathcal{O}_{X_k}(W_k)} = \bigoplus_{\alpha > 0} kt^{-\alpha} \oplus \bigoplus_{j=1}^{n-1} \bigoplus_{\alpha \geq rj} kt^{-\alpha} y^j$$

De plus $\mathcal{O}_{X_k}(W_k) = k \oplus \widehat{\mathcal{O}_{X_k}(W_k)}$.

Preuve: Par définition on sait que $\overline{U}_k \cap W_k = \text{Spec}(k[t, t^{-1}, f(t)^{-1}, y]/(y^n - f(t)))$ et on a donc $\mathcal{O}_{X_k}(\overline{U}_k \cap W_k) = k[t, t^{-1}, f(t)^{-1}, y]/(y^n - f(t))$ et $\mathcal{O}_{X_k}(\overline{U}_k \cap W_k) \simeq \bigoplus_{j=0}^{n-1} k[t][f(t)^{-1}][t^{-1}]y^j$ comme $k[t]$ -module. Mais $t \wedge f(t) = 1$ dans $k[t]$ donc $f(t)^{-1} \in k[[t]]$ et $\mathcal{O}_{X_k}(\overline{U}_k \cap W_k) \subset A$.

En ce qui concerne les trois égalités, la dernière est une évidence au regard du lemme 7.5.2 et la seconde n'est qu'une réécriture de la première. Par ailleurs il est clair par définition des différents espaces que le membre de droite de la première égalité est bien inclus dans $\mathcal{O}_{X_k}(\overline{U}_k \cap W_k)$ il reste donc à prouver l'inclusion réciproque.

Soit $B = k[[t]][y]/(y^n - f(t))$ alors $B \simeq \bigoplus_{j=0}^{n-1} k[[t]]y^j$ comme $k[[t]]$ -module. Posons également $E = k[t, y]/(y^n - f(t))$, alors $E \simeq \bigoplus_{j=0}^{n-1} k[t]y^j$ comme $k[t]$ -module. Comme $k[t]$ est noethérien, le complété de E pour la topologie t -adique est $k[[t]] \otimes_{k[t]} E$. Or $k[[t]]$ est un $k[t]$ -module plat et E est séparé pour la topologie t -adique donc $E \hookrightarrow k[[t]] \otimes_{k[t]} E \simeq B$.

Par définition $\mathcal{O}_{X_k}(\overline{U}_k) = E[y^{-1}] = E[f(t)^{-1}]$ et alors $\mathcal{O}_{X_k}(\overline{U}_k) \hookrightarrow B[f(t)^{-1}]$ car la localisation est plate. Par ailleurs $B[f(t)^{-1}] \simeq B$ car $f(t)^{-1} \in k[[t]]$ et $\mathcal{O}_{X_k}(\overline{U}_k) \hookrightarrow B$ par platitude de la localisation.

Par définition $\mathcal{O}_{X_k}(\overline{U}_k \cap W_k) = \mathcal{O}_{X_k}(\overline{U}_k)[t^{-1}] = E[f(t)^{-1}][t^{-1}]$ et $\mathcal{O}_{X_k}(\overline{U}_k \cap W_k) \hookrightarrow B[t^{-1}]$. Pour conclure montrons le lemme suivant :

Lemme 7.5.4. $B \cap \mathcal{O}_{X_k}(\overline{U}_k \cap W_k) = \mathcal{O}_{X_k}(\overline{U}_k)$.

Preuve: Rappelons tout d'abord que l'on a les inclusions d'anneaux compatibles à l'action de δ

$$\mathcal{O}_{X_k}(\overline{U}_k) \stackrel{i_1}{\subset} B \stackrel{i_2}{\subset} A$$

$$\mathcal{O}_{X_k}(\overline{U}_k \cap W_k) = \mathcal{O}_{X_k}(\overline{U}_k)[f^{-1}] \stackrel{i_3}{\subset} A$$

notons $B_j = k[[t]]y^j$ et $A_j = k[[t]][t^{-1}]y^j$ pour $1 \leq j \leq n-1$, les sous-espaces de A et B tels que $B = \bigoplus B_j$ et $A = \bigoplus A_j$. Alors $i_1(\mathcal{O}_{X_k}(\overline{U}_k)_j) \subset B_j$, $i_2(B_j) \subset A_j$ et $i_3(\mathcal{O}_{X_k}(\overline{U}_k \cap W_k)_j) \subset A_j$. Ainsi il suffit de montrer que pour tout $0 \leq j \leq n-1$ on a $B_j \cap \mathcal{O}_{X_k}(\overline{U}_k \cap W_k)_j = \mathcal{O}_{X_k}(\overline{U}_k)_j$ c'est-à-dire $k[[t]]y^j \cap k[t, t^{-1}, f^{-1}]y^j = k[t, f^{-1}]y^j$ ce qui revient à montrer que

$$k[[t]] \cap k[t, t^{-1}, f^{-1}] = k[t, f^{-1}].$$

CHAPITRE 7. MISE EN PLACE DU CALCUL DU FROBENIUS DIVISÉ DE LA FIBRE SPÉCIALE

Or l'algèbre $k[[t]]$ est munie de la valuation t -adique, v_t , qui s'étend à $k[[t]][t^{-1}]$. De plus $v_t(f)$ est non nulle car $f(0) \neq 0$. Soit u un élément de $k[[t], f^{-1}]$, alors il s'écrit $u = af^{-n}$ avec $a \in k[[t]]$ et $v_t(u) = v_t(af^{-n}) = v_t(a) \geq 0$. Soit w dans $k[[t]] \cap k[[t], t^{-1}, f^{-1}]$, alors $w = af^{-n}$ avec $a \in k[[t], t^{-1}]$. Comme w est un élément de $k[[t]]$ alors $v_t(w) = v_t(a) \leq 0$ et donc a est un élément de $k[[t]]$ ce qui signifie que w est dans $k[[t], f^{-1}]$ et montre donc le lemme. \square

Montrons maintenant l'inclusion

$$\mathcal{O}_{X_k}(\overline{U}_k \cap W_k) \subset \mathcal{O}_{X_k}(\overline{U}_k) \oplus \left(\bigoplus_{\alpha > 0} kt^{-\alpha} \oplus \bigoplus_{j=1}^{n-1} \bigoplus_{\alpha=1}^{rj-1} kt^{-\alpha} y^j \oplus \bigoplus_{j=1}^{n-1} \bigoplus_{\alpha \geq rj} kt^{-\alpha} y^j \right)$$

Considérons maintenant $h \in \mathcal{O}_{X_k}(\overline{U}_k \cap W_k)$ et regardons-le comme élément de A (puisque $\mathcal{O}_{X_k}(\overline{U}_k \cap W_k) \subset A$), alors $\forall 0 \leq j \leq n-1$, $\exists h_j \in k[[t]][t^{-1}]$ tel que $h = \sum h_j y^j$. Par définition, pour j fixé on peut écrire

$$h_j = \sum_{s=-a}^0 \lambda_s^j t^s + \sum_{s \geq 0} \lambda_s^j t^s$$

avec $\lambda_i^j \in k$. Posons

$$H_j = \sum_{s=-a}^0 \lambda_s^j t^s$$

$$K_j = \sum_{s \geq 0} \lambda_s^j t^s$$

alors $h = \sum (H_j + K_j) y^j$. Or $\sum H_j y^j \in \mathcal{O}_{X_k}(\overline{U}_k \cap W_k)$ et comme c'est également le cas de h on en déduit que $\sum K_j y^j \in \mathcal{O}_{X_k}(\overline{U}_k \cap W_k)$ et d'après le lemme $\sum K_j y^j \in \mathcal{O}_{X_k}(\overline{U}_k)$. On a donc décomposé un élément de $\mathcal{O}_{X_k}(\overline{U}_k \cap W_k)$ selon le second membre de la première égalité de l'énoncé ce qui prouve la seconde inclusion voulue et achève donc la démonstration. \square

Remarque 7.5.2. A l'aide de ce dernier lemme on retrouve clairement le résultat déjà établi à la proposition 6.0.5 qui est l'expression d'une base de $H^1(X_k, \mathcal{O}_{X_k})$. Cependant on voit que pour obtenir la classe d'un élément du type $f(t)^{-at^b} y^j$ avec $a \in \mathbb{N}$, $b \in \mathbb{Z}$ et $1 \leq j \leq n-1$ il est nécessaire de connaître l'expression de l'inverse de f dans $k[[t]]$. Cela pose plusieurs problèmes et il est notamment peu raisonnable d'espérer gérer une telle donnée algorithmiquement. Cependant il existe une astuce, due à Xavier Caruso que l'on détaille dans le lemme suivant.

Lemme 7.5.5. *Rappelons que l'on note $\overline{\dots}$ les classes des éléments de $\mathcal{O}_{X_k}(\overline{U}_k \cap W_k)$ dans $H^1(X_k, \mathcal{O}_{X_k})$, soient $a, b \in \mathbb{N}$, $1 \leq j \leq n-1$ alors :*

$$\overline{f(t)^{-at^b} y^j} = 0$$

$$\overline{f(t)^{-at^b} y^j} = \overline{I_b^a t^{-b} y^j}$$

où I_b est l'inverse de f à l'ordre $b+1$ (donc dans $k[t]/t^{b+1}$) i.e. $f(t)I_b(t) = 1 + t^{b+1}P(t)$ avec $P \in k[t]$.

Preuve: Il est évident au vu de ce qui précède que $f(t)^{-a}t^b y^j$ est un élément de $\mathcal{O}_{X_k}(\overline{U}_k)$ ce qui donne le premier résultat.

En ce qui concerne le second. Soit I l'inverse de f dans $k[[t]]$ et soit I_b sa troncature à l'ordre b . On a donc $I = I_b + t^{b+1}R(t)$ où $R(t) \in k[[t]]$.

Alors $f(t)^{-a}t^{-b}y^j = I^a t^{-b}y^j = (I_b + t^{b+1}R(t))^a t^{-b}y^j$. En utilisant la formule du binôme de Newton on obtient finalement $f(t)^{-a}t^{-b}y^j = (I_b^a + t^{b+1}\tilde{R}(t))t^{-b}y^j = I_b^a t^{-b}y^j + t\tilde{R}(t)y^j$. Le second terme de la somme étant clairement dans $Im(d)$, la classe de l'élément considéré est la classe de $I_b^a t^{-b}y^j$ d'où le résultat voulu. \square

Lemme 7.5.6. Notons λ_k le coefficient du monôme t^k dans f . On peut construire récursivement une suite $(I_N(t))$ de polynômes de $k[t]$ tels que I_N soit l'inverse de f à l'ordre t^{N+1} i.e. $I_N(t)f(t) = 1 + t^{N+1}P_N(t)$ et $I_{N+1}(t) = I_N(t) + a_{N+1}t^{N+1}$. On a

$$\begin{aligned} a_0 &= \frac{1}{\lambda_0} & P_0(t) &= \sum_{k=1}^l \frac{\lambda_k}{\lambda_0} t^{k-1} \\ a_{N+1} &= \frac{-P_N(0)}{\lambda_0} & P_{N+1}(t) &= \frac{\lambda_0 P_N(t) - P_N(0)f(t)}{\lambda_0 t}. \end{aligned}$$

Preuve: Tout d'abord il est clair que a_0 et P_0 ainsi définis conviennent. En effet soit $I_0 = a_0$ alors $I_0(t)f(t) = a_0 \sum \lambda_k t^k$. D'où

$$I_0(t)f(t) = \sum_{k=0}^l \frac{\lambda_k}{\lambda_0} t^k = 1 + \sum_{k=1}^l \frac{\lambda_k}{\lambda_0} t^k = 1 + tP_0(t).$$

Supposons que I_N soit un inverse de f à l'ordre t^{N+1} (i.e. $I_N(t)f(t) = 1 + t^{N+1}P_N(t)$) et cherchons I_{N+1} inverse de f à l'ordre t^{N+2} sous la forme $I_N(t) + a_{N+1}t^{N+1}$. Alors

$$I_{N+1}(t)f(t) = I_N(t)f(t) + a_{N+1}t^{N+1}f(t) = 1 + t^{N+1}(P_N(t) + a_{N+1}f(t)).$$

Mais $P_N(t) = P_N(0) + (P_N(t) - P_N(0))$, $f(t) = f(0) + (f(t) - f(0))$ avec $(P_N(t) - P_N(0))$ et $f(t) - f(0)$ dans $tk[t]$. D'où

$$I_{N+1}(t)f(t) = 1 + t^{N+1}(P_N(0) + a_{N+1}f(0)) + t^{N+2} \left(\frac{P_N(t) - P_N(0)}{t} + a_{N+1} \frac{f(t) - f(0)}{t} \right).$$

Par ailleurs on souhaite que cette dernière expression soit égale à $1 + t^{N+2}P_{N+1}(t)$. On a donc directement l'expression de a_{N+1} puisque $f(0) = \lambda_0$. Il reste donc à exprimer $P_{N+1}(t)$. On a

$$P_{N+1}(t) = \frac{P_N(t) - P_N(0)}{t} - \frac{P_N(0)}{\lambda_0} \frac{f(t) - f(0)}{t} = \frac{P_N(t)}{t} - \frac{P_N(0)}{t} \left(1 + \frac{f(t)}{\lambda_0} - \frac{f(0)}{\lambda_0} \right)$$

qui est bien l'expression donnée après simplification. \square

Chapitre 8

Calcul de la matrice du Frobenius divisé de la fibre spéciale

Ce qui précède permet le calcul de la matrice du Frobenius divisé

$$\Phi : H^0(X_k, \Omega_{X_k}^1) \oplus H^1(X_k, \mathcal{O}_{X_k}) \rightarrow H_{DR}^1(X_k)$$

défini à la section 7.1. On a donné dans les propositions 4.1.1 et 6.0.5 des bases de $H^0(X_k, \Omega_{X_k}^1)$ et $H^1(X_k, \mathcal{O}_{X_k})$ qui par abus de notation donnent une base de $H_{DR}^1(X_k)$ (voir remarque 7.1.1). La matrice donnée par les formules présentées plus loin est exprimée dans cette base, on donne donc la matrice de

$$\Phi : H^0(X_k, \Omega_{X_k}^1) \oplus H^1(X_k, \mathcal{O}_{X_k}) \rightarrow H^0(X_k, \Omega_{X_k}^1) \oplus H^1(X_k, \mathcal{O}_{X_k}).$$

8.1 Présentation de la matrice

On fait le choix de présentation suivant, l'image des éléments de la base de $H^0(X_k, \Omega_{X_k}^1)$ se lit dans les g premières colonnes de la matrice et l'image des éléments de la base de $H^1(X_k, \mathcal{O}_{X_k})$ dans les g dernières colonnes. Cela permet de respecter la filtration. Soit maintenant un élément de la base de $H^0(X_k, \Omega_{X_k}^1) \oplus H^1(X_k, \mathcal{O}_{X_k})$ la projection de son image sur $H^0(X_k, \Omega_{X_k}^1)$ se lit dans les g premières lignes et la projection de son image sur $H^1(X_k, \mathcal{O}_{X_k})$ dans les g dernières lignes. Ceci ne fait pas apparaître le découpage par composantes isotypiques comme présenté dans la proposition 7.3.2 et la remarque 7.3.3 mais si on découpe la matrice en 4 blocs de taille $g \times g$ alors le bloc supérieur gauche correspond à la matrice de Cartier et le bloc inférieur droit à la matrice de Hasse-Witt. Par ailleurs pour chaque bloc on ordonne les éléments dans l'ordre lexicographique en prenant d'abord en compte la puissance de y puis celle de t afin de respecter les composantes isotypiques au sein de chaque bloc. En d'autres termes la matrice se présente de la manière suivante

$$\begin{array}{l}
 y^{-1}dt \\
 \vdots \\
 t^{r-2}y^{-1}dt \\
 y^{-2}dt \\
 \vdots \\
 t^{r(n-1)-2}y^{-(n-1)}dt \\
 t^{-1}y \\
 \vdots \\
 t^{r-1}y \\
 t^{-1}y^2 \\
 \vdots \\
 t^{-(r(n-1)-1)}y^{n-1}
 \end{array}
 \begin{pmatrix}
 y^{-1}dt & \dots & t^{r(n-1)-2}y^{-(n-1)}dt & t^{-1}y & \dots & t^{-(r(n-1)-1)}y^{n-1} \\
 * & \dots & * & * & \dots & * \\
 * & \dots & * & * & \dots & * \\
 * & \dots & * & * & \dots & * \\
 * & \dots & * & * & \dots & * \\
 * & \dots & * & * & \dots & * \\
 * & \dots & * & * & \dots & * \\
 * & \dots & * & * & \dots & * \\
 * & \dots & * & * & \dots & * \\
 * & \dots & * & * & \dots & * \\
 * & \dots & * & * & \dots & * \\
 * & \dots & * & * & \dots & * \\
 * & \dots & * & * & \dots & *
 \end{pmatrix}$$

Lemme 8.1.1. Soit $\omega_{i,j} = t^i y^{-j} dt$, $1 \leq j \leq n-1$, $0 \leq i \leq rj-2$ un élément de la base de $H^0(X_k, \Omega_{X_k}^1)$ (voir proposition 4.1.1). Alors l'image de $\omega_{i,j}$ par Φ se lit dans la colonne

$$\frac{(rj-2)(j-1)}{2} + i + 1$$

de la matrice.

Preuve: Vu la manière dont on remplit la matrice, l'élément $y^{-1}dt$ est dans la colonne 1, $ty^{-1}dt$ dans la colonne $1+1, \dots$, $t^{r-2}y^{-1}dt$ dans la colonne $1+r-2$, $y^{-2}dt$ dans la colonne $r-2+2, \dots$, $t^{2r-2}y^{-2}dt$ dans la colonne $r-2+2+2r-2$ et ainsi de suite. On en déduit que l'image de l'élément $t^i y^{-j} dt$ se lit dans la colonne

$$\sum_{k=1}^{j-1} (rj-2) + j + i = r \frac{(j-1)j}{2} - 2(j-1) + (j-1) + 1 + i = \frac{(rj-2)(j-1)}{2} + i + 1$$

ce qui est bien le résultat annoncé. \square

Lemme 8.1.2. Soit $\overline{h_{i,j}} = \overline{t^{-i}y^j}$, $1 \leq j \leq n-1$, $1 \leq i \leq rj-1$ un élément de la base de $H^1(X_k, \mathcal{O}_{X_k})$ (voir proposition 6.0.5). Alors l'image de $\overline{h_{i,j}}$ par Φ se lit dans la colonne

$$g + \frac{(rj-2)(j-1)}{2} + i$$

de la matrice.

CHAPITRE 8. CALCUL DE LA MATRICE DU FROBENIUS DIVISÉ DE LA FIBRE SPÉCIALE

Preuve: Tout d'abord vu la manière dont on remplit la matrice, l'image de $H^1(X_k, \mathcal{O}_{X_k})$ se lit dans les colonnes g à $2g$. L'image de $\overline{t^{-1}y}$ dans la colonne $g+1, \dots$ celle de $\overline{t^{-(r-2)}y}$ dans la colonne $g+r-2$, celle de $\overline{t^{-1}y^2}$ dans la colonne $g+r-2+1, \dots$ celle de $\overline{t^{-(2r-2)}y^2}$ dans la colonne $g+r-2+2r-2$ et ainsi de suite. On en déduit que l'image de l'élément $\overline{t^{-i}y^j}$ se lit dans la colonne

$$g + \sum_{k=1}^{j-1} (rj-1) + i = g + r \frac{j(j-1)}{2} - (j-1) + i = g + \frac{(rj-2)(j-1)}{2} + i$$

ce qui est bien le résultat annoncé. □

De manière évidente on a le résultat symétrique suivant.

Lemme 8.1.3. *Soit e un élément de la base de $H^0(X_k, \Omega_{X_k}^1) \oplus H^1(X_k, \mathcal{O}_{X_k})$. Alors le coefficient en $t^i y^{-j} dt$ de $\Phi(e)$ se lit dans la ligne*

$$\frac{(rj-2)(j-1)}{2} + i + 1$$

et le coefficient en $\overline{t^{-i}y^j}$ dans la ligne

$$g + \frac{(rj-2)(j-1)}{2} + i$$

de la matrice.

Définition. *On rappelle qu'on utilise les notations suivantes dans tout ce chapitre. L'identification de $H^1(X_k, \mathcal{O}_{X_k})$ à $\mathcal{O}_{X_k}(\overline{U}_k \cap W)/\text{Im}(d_{0,1})$ induit (voir remarque 6.0.4)*

$$\iota : H^1(X_k, \mathcal{O}_{X_k}) \rightarrow \mathcal{O}_{X_k}(\overline{U}_k \cap W)$$

ainsi que

$$\overline{\dots} : \mathcal{O}_{X_k}(\overline{U}_k \cap W) \rightarrow H^1(X_k, \mathcal{O}_{X_k}).$$

Par ailleurs on a construit à la proposition 6.0.3

$$\tau : H^1(X_k, \mathcal{O}_{X_k}) \rightarrow \Omega_{X_k}^1(\overline{U}_k) \times \Omega_{X_k}^1(W_k) \times \mathcal{O}_{X_k}(\overline{U}_k \cap W)$$

et on note

$$[\dots] : \Omega_{X_k}^1(\overline{U}_k) \times \Omega_{X_k}^1(W_k) \times \mathcal{O}_{X_k}(\overline{U}_k \cap W) \rightarrow H^1(\check{C}(\mathcal{F}, \Omega_{X_k}^\bullet)).$$

On a également défini les projecteurs suivants (définition 7.4.2)

$$q_U : \Omega_{X_k}^1(\overline{U}_k) \rightarrow H^0(X_k, \Omega_{X_k}^1)$$

$$q_W : \Omega_{X_k}^1(W_k) \rightarrow H^0(X_k, \Omega_{X_k}^1)$$

et on notera P_1 (resp. P_2) la projection de $H^1(X_k, \mathcal{O}_{X_k}) \oplus H^0(X_k, \Omega_{X_k}^1)$ sur le premier (resp. le second) facteur.

8.2 Calcul de la matrice de Hasse-Witt

La matrice de Hasse-Witt correspond au quart inférieur droit de la matrice du Frobenius divisé que nous sommes en train de calculer, c'est en fait $\Phi : H^1(X_k, \mathcal{O}_{X_k}) \rightarrow H^1(X_k, \mathcal{O}_{X_k})$. En vertu de la proposition 7.4.2 on l'obtient tout simplement en calculant la classe de $h_{i,j}^p$ dans $H^1(X_k, \mathcal{O}_{X_k})$.

Proposition 8.2.1. *Soit $\overline{h_{i,j}}$ un élément de la base de $H^1(X_k, \mathcal{O}_{X_k})$ (voir proposition 6.0.5). Soient a le quotient et b le reste de la division euclidienne de pj par n . Notons $F(t) = f(t)^a$ et $F[k]$ le coefficient de t^k de F . Alors $1 \leq b \leq n-1$ et*

$$P_1(\Phi(\overline{h_{i,j}})) = \overline{h_{i,j}^p} = \sum_{k=1}^{rb-1} F[pi-k] \overline{t^{-k}y^b} = \sum_{k=1}^{rb-1} F[pi-k] \overline{h_{k,b}}$$

dans $H^1(X_k, \mathcal{O}_{X_k})$.

Preuve: Par définition $0 \leq b \leq n-1$. Par ailleurs $b \neq 0$ car $p \wedge n = 1$ et $1 \leq j \leq n-1$ donc n ne divise pas le produit pj . Soient $1 \leq j \leq n-1$, $1 \leq i \leq rj-1$, par abus de notation notons $DI_0(t^{-i}y^j)$ l'élément $(t^{-i}y^j)^p \in \mathcal{O}_{X_k}(\overline{U}_k)$ alors

$$DI_0(t^{-i}y^j) = t^{-pi}y^{pj} = t^{-pi}f(t)^a y^b = t^{-pi}F(t)y^b = \sum_{k=0}^d F[k]t^{-(pi-k)}y^b$$

où d désigne le degré de F en tant que polynôme en t . Réalisons le changement de variable $k' = pi - k$, alors

$$DI_0(t^{-i}y^j) = \sum_{k'=pi-d}^{pi} F[pi-k']t^{-k'}y^b.$$

Or $\forall \alpha \in \mathbb{N}$, $\overline{t^\alpha y^b} = 0$ et $\overline{t^{-\alpha} y^b} = \overline{h_{\alpha,b}} \forall 1 \leq \alpha \leq rb-1$ et $\overline{t^{-\alpha} y^b} = 0$ sinon. D'où

$$\overline{DI_0(t^{-i}y^j)} = \sum_{k'=1}^{rb-1} F[pi-k'] \overline{t^{-k'}y^b}$$

ce qui est le résultat annoncé. Par ailleurs notons que si $pi-d > 1$ ou $pi < rb-1$ la somme contient à priori plus de termes qu'elle ne devrait. Dans le premier cas un tel terme k vérifie $pi-k > d$ et donc $F[pi-k] = 0$ puisque $d = \deg(F)$. Dans le second cas k vérifie $pi-k < 0$ et donc $F[pi-k] = 0$ puisque F est un polynôme. □

Remarque 8.2.1. Dans le cas hyperelliptique, on a toujours $j = 1$ et comme p est impair alors $a = (p-1)/2$ et $b = 1$, de plus $g = r-1$. Ainsi la formule devient

$$P_1\left(\Phi(\overline{t^{-i}y})\right) = \sum_{k=1}^g f^{(p-1)/2}[pi-k] \overline{t^{-k}y}$$

dans $H^1(X_k, \mathcal{O}_{X_k})$ et le coefficient en $\overline{t^{-j}y}$ vaut donc $f^{(p-1)/2}[pi-j]$. On retrouve bien le résultat cité dans [HS14] (à transposition près).

8.3 Calcul du bloc supérieur droit

Ce bloc correspond à $\Phi : H^1(X_k, \mathcal{O}_{X_k}) \rightarrow H^0(X_k, \Omega_{X_k}^1)$. On utilise donc la proposition 7.4.2 pour calculer $P_2(\Phi(\overline{h_{i,j}})) = -\beta_U^{ij} - dh_U$ or clairement $q_U(P_2(\Phi(\overline{h_{i,j}}))) = P_2(\Phi(\overline{h_{i,j}}))$ et donc $P_2(\Phi(\overline{h_{i,j}})) = -q_U(\beta_U^{ij}) - q_U(dh_U)$. Dans ce qui suit nous procédons au calcul de ces deux termes.

Lemme 8.3.1. *Soit $\overline{h_{i,j}}$ un élément de la base de $H^1(X_k, \mathcal{O}_{X_k})$ (voir proposition 6.0.5). Soient a le quotient et b le reste de la division euclidienne de pj par n . Notons $F(t) = f(t)^a$, $F[k]$ le coefficient de t^k de F et $\beta_{ij}^U \in \Omega_{X_k}^1(\overline{U}_k)$ la première composante de $\tau(\overline{h_{i,j}^p})$ (voir proposition 6.0.6). Alors $1 \leq b \leq n-1$ et*

$$q_U(\beta_{ij}^U) = \sum_{m=0}^{r(n-b)-2} \left(\sum_{k=1}^{rb-1} \frac{b(m+k+1) - kn}{n} F[pi - k] f[m+k+1] \right) \frac{t^m dt}{y^{n-b}}$$

dans $H^0(X_k, \Omega_{X_k}^1)$.

Preuve: En ce qui concerne la condition sur b l'argument est le même que dans la démonstration précédente. Par ailleurs la formule proposée vient tout simplement de la linéarité du scindage τ et de la formule donnée à la proposition 8.2.1. En effet le terme que nous cherchons à calculer est le β_{ij}^U de la proposition 7.4.2 qui est donné par la première composante de $\tau(\overline{t^{-k}y^b})$ et qui vaut $\sum_{m=k+1}^l (bm - kn)/n f[m] t^{m-(k+1)} dt / y^{n-b}$ (voir proposition 6.0.6). On a donc

$$\beta_{ij}^U = \sum_{k=1}^{rb-1} \sum_{m=k+1}^l \frac{bm - kn}{n} F[pi - k] f[m] \frac{t^{m-(k+1)} dt}{y^{n-b}} \in \Omega_{X_k}^1(\overline{U}_k)$$

et en réalisant le changement de variable $m' = m - (k+1)$ on obtient

$$\beta_{ij}^U = \sum_{k=1}^{rb-1} \sum_{m'=0}^{l-(k+1)} \frac{b(m'+k+1) - kn}{n} F[pi - k] f[m'+k+1] \frac{t^m dt}{y^{n-b}}.$$

Par la remarque 7.4.2 il suffit de calculer $q_U(\beta_{ij}^U)$ et pour cela on considère uniquement les termes de cette somme tels que $0 \leq m' \leq r(n-b) - 2$ (voir lemme 4.1.1) ce qui achève la démonstration. Encore une fois on pourrait penser que si $r(n-b) - 2 > l - (k+1)$ la somme contient plus de termes qu'elle ne devrait. Cependant un tel terme vérifie $m' > l - (k+1)$ donc $m' + k + 1 > l$ et $f[m' + k + 1] = 0$ puisque $\deg(f) = l$. □

Lemme 8.3.2. *Soit $\overline{h_{i,j}}$ un élément de la base de $H^1(X_k, \mathcal{O}_{X_k})$ (voir proposition 6.0.5). Soient a le quotient et b le reste de la division euclidienne de pj par n . Notons $F(t) = f(t)^a$, $F[k]$ le coefficient de t^k de F et $d = \deg(F)$. Soit $h = h_{i,j}^p - \iota(\overline{h_{i,j}^p})$ et notons $h_U \in \mathcal{O}_{X_k}(\overline{U}_k)$ et*

$h_W \in \mathcal{O}_{X_k}(W_k)$ tels que $h = h_U + h_W$ (voir proposition 7.4.2). Alors $1 \leq b \leq n-1$ et

$$q_U(dh_U) = \sum_{m=0}^{r(n-b)-2} \left(\sum_{k=pi-d}^0 \frac{b(m+k+1) - kn}{n} F[pi-k] f[m+k+1] \right) \frac{t^m dt}{y^{n-b}}$$

dans $H^0(X_k, \Omega_{X_k}^1)$. Où par convention la somme est nulle si $pi-d > 0$.

Preuve: Pour la condition sur b l'argument est toujours le même. Dans la démonstration de la proposition 8.2.1 on a établi la formule suivante

$$DI_0(t^{-i}y^j) = \sum_{k=pi-d}^{pi} F[pi-k] t^{-k} y^b$$

et on a donc

$$h = \sum_{k=pi-d}^0 F[pi-k] t^{-k} y^b + \sum_{k=rb}^{pi} F[pi-k] t^{-k} y^b$$

et clairement h_U correspond à la première somme et h_W à la seconde grâce au lemme 7.5.3. Dans le cas où $pi-d > 0$ la première somme est vide donc $h_U = 0$ et $dh_U = 0$. Dans le cas contraire on obtient par différentiation

$$dh_U = \sum_{k=pi-d}^0 F[pi-k] \left(-kt^{-k-1} y^b dt + t^{-k} b y^{b-1} dy \right) \in \Omega_{X_k}^1(\bar{U}_k)$$

cette relation étant valable modulo $ny^{n-1}dy - f'(t)dt$ puisque sur \bar{U}_k on a la relation $y^n = f(t)$. Ainsi

$$\begin{aligned} dh_U &= \sum_{k=pi-d}^0 F[pi-k] \left(-kt^{-k-1} y^n y^{b-n} dt + t^{-k} b y^{b-1} \frac{f'(t)dt}{ny^{n-1}} \right) \\ &= \sum_{k=pi-d}^0 F[pi-k] \left(-kt^{-k-1} f(t) + \frac{bt^{-k} f'(t)}{n} \right) \frac{dt}{y^{n-b}}. \end{aligned}$$

On remplace alors $f(t)$ et $f'(t)$ par leur expression en fonction des $f[k]$ et on obtient

$$\begin{aligned} dh_U &= \sum_{k=pi-d}^0 F[pi-k] \left(-kt^{-k-1} \sum_{m=0}^l f[m] t^m + \frac{bt^{-k}}{n} \sum_{m=0}^l m f[m] t^{m-1} \right) \frac{dt}{y^{n-b}} \\ &= \sum_{k=pi-d}^0 F[pi-k] \left(-k \sum_{m=0}^l f[m] t^{m-k-1} + \frac{b}{n} \sum_{m=0}^l m f[m] t^{m-1-k} \right) \frac{dt}{y^{n-b}} \\ &= \sum_{k=pi-d}^0 \sum_{m=0}^l \frac{bm - kn}{n} F[pi-k] f[m] \frac{t^{m-k-1} dt}{y^{n-b}}. \end{aligned}$$

CHAPITRE 8. CALCUL DE LA MATRICE DU FROBENIUS DIVISÉ DE LA FIBRE SPÉCIALE

On réalise le changement de variable $m' = m - k - 1$, alors

$$dh_U = \sum_{k=pi-d}^0 \sum_{m'=-k+1}^{l-(k+1)} \frac{b(m'+k+1) - kn}{n} F[pi-k] f[m'+k+1] \frac{t^{m'} dt}{y^{n-b}}.$$

Par la remarque 7.4.2 il suffit de calculer $q_U(dh_U)$ et pour cela on considère uniquement les termes de cette somme tels que $0 \leq m' \leq r(n-b) - 2$ (voir lemme 4.1.1) ce qui achève la démonstration. De plus si $r(n-b) - 2 > l - (k+1)$ la somme ne contient pas plus de termes qu'elle ne devrait puisqu'on aurait $m' > l - (k+1)$ et donc $f[m'+k+1] = 0$ car $\deg(f) = l$. \square

Proposition 8.3.1. *Soit $\overline{h_{i,j}}$ un élément de la base de $H^1(X_k, \mathcal{O}_{X_k})$ (voir proposition 6.0.5). Soient a le quotient et b le reste de la division euclidienne de pi par n . Notons alors $F(t) = f(t)^a$, $F[k]$ le coefficient de t^k de F et $d = \deg(F)$. Alors $1 \leq b \leq n-1$ et*

$$P_2(\Phi(\overline{h_{i,j}})) = \sum_{m=0}^{r(n-b)-2} \left(\sum_{k=pi-d}^{rb-1} \frac{kn - b(m+k+1)}{n} F[pi-k] f[m+k+1] \right) \frac{t^m dt}{y^{n-b}}$$

dans $H^0(X_k, \Omega_{X_k}^1)$.

Preuve: Cette proposition est tout simplement une conséquence de la proposition 7.4.2 et des lemmes 8.3.1 et 8.3.2. Remarquons que dans le lemme 8.3.2 on avait dû considérer séparément les cas où $pi - d \leq 0$ et $pi - d > 0$. Dans le premier cas il est clair qu'on a la somme proposée, dans le second cas on a $dh_U = 0$ mais en fait cela signifie également que la formule donnée dans le lemme 8.3.1 présente des termes nuls jusqu'à ce que $k = pi - d$ ce qui fait qu'on obtient bien la même formule dans les deux cas. \square

8.4 Calcul du bloc inférieur gauche

Ce bloc correspond à $\Phi : H^0(X_k, \Omega_{X_k}^1) \rightarrow H^1(X_k, \mathcal{O}_{X_k})$. On utilise donc la proposition 7.4.1. Calculons la classe de $h(\omega'_{i,j})$ dans $H^1(X_k, \mathcal{O}_{X_k})$ pour $1 \leq j \leq n-1$ et $0 \leq i \leq rj-2$.

Lemme 8.4.1. *Soit $\omega'_{i,j}$, $1 \leq j \leq n-1$, $0 \leq i \leq rj-2$ un élément de la base de $H^0(X'_k, \Omega_{X'_k}^1)$ (voir proposition 7.1.1). Soit $v(s)$ le polynôme intervenant dans le relèvement du Frobenius modulo p^2 sur W_1 (voir proposition 7.2.3). Notons $d = \max\{0, \deg(v) - 2p\}$. Alors*

$$\overline{h(\omega'_{i,j})} = \overline{t^{p(i+2)} v(s) I_d(t)^{a+1} y^{n-b}}$$

dans $H^1(X_k, \mathcal{O}_{X_k})$ où I_d est l'inverse de f à l'ordre $d+1$ (voir lemme 7.5.6).

Preuve: Tout d'abord on a vu à la remarque 7.3.2 que

$$h(\omega'_{i,j}) = \frac{t^{p(i+2)}}{f(t)^{a+1}} v(s) y^{n-b}.$$

Par ailleurs en vertu du lemme 7.5.5 on sait qu'il suffit de connaître la puissance négative maximale en t pouvant apparaître dans cette expression et que celle-ci nous donne l'ordre d'inversion de f suffisant pour calculer la classe de $h(\omega'_{i,j})$. Comme $s = t^{-1}$ la puissance négative maximale en t apparaissant dans $t^{p(i+2)}v(s)$ est donc $\deg(v) - p(i+2)$.

Or $0 \leq i \leq rj - 1$ donc $\deg(v) - p(i+2) \geq \deg(v) - 2p$, $\forall 0 \leq i \leq rj - 1$. Ainsi la puissance maximale en t^{-1} est $\deg(v) - 2p$ et ce quel que soit j . Soit donc $d = \deg(v) - 2p$ alors connaître l'inverse de f à l'ordre $d+1$ est suffisant pour obtenir la classe cherchée. \square

Remarque 8.4.1. On a déjà vu que puisqu'il était nécessaire de ne considérer qu'une estimation de l'inverse de f il fallait mener les calculs non pas sur \bar{U}_k mais sur W_k . On utilise donc les relations entre (t, y) et (s, z) qui sont pour mémoire $s = t^{-1}$ et $z = t^{-r}y$ où $r = (l+1)/n$. Clairement $\forall 1 \leq j \leq n-1, \forall 1 \leq i \leq rj-1, t^{-i}y^j = s^{-(rj-i)}z^j$ et $\forall 1 \leq j \leq n-1, \forall 0 \leq i \leq rj-2, t^i y^{-j} dt = -s^{rj-(i+2)} z^{-j} ds$. Donc la base de $H^1(X_k, \mathcal{O}_{X_k})$ peut s'écrire $s^{-i}z^j$ avec $1 \leq j \leq n-1$ et $1 \leq i \leq rj-1$ et celle de $H^0(X_k, \Omega_{X_k}^1)$ peut s'écrire $s^i z^{-j} ds$ avec $1 \leq j \leq n-1$ et $0 \leq i \leq rj-2$.

Proposition 8.4.1. Soit $\omega_{i,j} \in H^0(X_k, \Omega_{X_k}^1)$ un élément de la base (voir proposition 4.1.1). Soient $v(s)$ le polynôme du relèvement du Frobenius modulo p^2 sur W_1 (voir proposition 7.2.3), $d = \max\{0, \deg(v) - 2p\}$, I_d l'inverse de f à l'ordre $d+1$ (voir lemme 7.5.6), a le quotient et b le reste de la division euclidienne de pj par n . Notons $IP(t) = I_d(t)^{a+1}$, $dIP = \deg(IP)$, $IP[k]$ le coefficient du monôme t^k dans $IP(t)$ et $v[m]$ le coefficient du monôme s^m dans $v(s)$. Alors $1 \leq b \leq n-1$ et

$$P_1(\Phi(\omega_{i,j})) = \overline{h(\omega'_{i,j})} = \sum_{m=1}^{r(n-b)-1} \left(\sum_{k=0}^{dIP} IP[k] \cdot v[p(i+2) + k + m] \right) \overline{t^{-m}y^{n-b}}$$

dans $H^1(X_k, \mathcal{O}_{X_k})$.

Preuve: Tout d'abord on rappelle qu'en vertu du lemme 8.4.1 on sait que

$$\overline{h(\omega'_{i,j})} = \overline{t^{p(i+2)}v(s)I_d(t)^{a+1}y^{n-b}} = \overline{t^{p(i+2)}v(s)IP(t)y^{n-b}}.$$

Par ailleurs

$$v(s) = \sum_{m=0}^{d+2p} v[m]s^m \quad \text{et} \quad IP(t) = \sum_{k=0}^{dIP} IP[k]t^k = \sum_{k=0}^{dIP} IP[k]s^{-k}$$

D'où

$$t^{p(i+2)}IP(t)v(s)y^{n-b} = \sum_{m=0}^{d+2p} \sum_{k=0}^{dIP} v[m] \cdot IP[k] \cdot s^{m-k-p(i+2)} s^{-r(n-b)} z^{n-b} \in \mathcal{O}_{X_k}(\bar{U}_k \cap W_k)$$

et en faisant le changement de variable $m' = p(i+2) + r(n-b) + k - m$ on a alors

$$t^{p(i+2)} IP(t)v(s)y^{n-b} = \sum_{k=0}^{dIP} \sum_{m'=pi+r(n-b)+k-d}^{p(i+2)+r(n-b)+k} IP[k] \cdot v[p(i+2) + r(n-b) + k - m'] \cdot s^{-m'} z^{n-b}.$$

Or tous les éléments $s^{-m'} z^{n-b}$ ne vérifiant pas $1 \leq m' \leq r(n-b) - 1$ ont une classe nulle dans $H^1(X_k, \mathcal{O}_{X_k})$. On obtient donc

$$\overline{h(\omega'_{i,j})} = \sum_{k=0}^{dIP} \sum_{m'=1}^{r(n-b)-1} IP[k] \cdot v[p(i+2) + r(n-b) + k - m'] \cdot \overline{s^{-m'} z^{n-b}}$$

et à nouveau la somme ne contient pas plus de termes qu'elle ne devrait et ce même si on a $pi + r(n-b) + k - d > 1$ ou $p(i+2) + r(n-b) + k < r(n-b) - 1$. Dans le premier cas un tel terme vérifierait $p(i+2) + r(n-b) + k - m > 2p + d = \deg(v)$ et son coefficient est donc nul. Dans le second cas on a $p(i+2) + r(n-b) + k - m < 0$ et le coefficient est également nul puisque v est un polynôme.

On utilise alors la condition de recollement pour exprimer cette égalité selon t et y et on a

$$\overline{h(\omega'_{i,j})} = \sum_{k=0}^{dIP} \sum_{m'=1}^{r(n-b)-1} IP[k] \cdot v[p(i+2) + r(n-b) + k - m'] \cdot \overline{t^{m'} t^{-r(n-b)} y^{n-b}}$$

puis avec le changement de variable $m = r(n-b) - m'$ on obtient finalement

$$\overline{h(\omega'_{i,j})} = \sum_{k=0}^{dIP} \sum_{m=1}^{r(n-b)-1} IP[k] \cdot v[p(i+2) + k + m] \cdot \overline{t^{-m} y^{n-b}}$$

ce qui achève la démonstration. □

8.5 Calcul de la matrice de Cartier

La matrice de Cartier correspond au quart supérieur gauche de la matrice du Frobenius divisé que nous sommes en train de calculer, c'est en fait $\Phi : H^0(X_k, \Omega_{X_k}^1) \rightarrow H^0(X_k, \Omega_{X_k}^1)$. On utilise donc la proposition 7.4.1 pour calculer $P_2(\Phi(\omega_{i,j})) = f_W(\omega'_{i,j}) + \beta_{ij}^W + dh_W$ or clairement $q_W(P_2(\Phi(\omega_{i,j}))) = P_2(\Phi(\omega_{i,j}))$ et donc $P_2(\Phi(\omega_{i,j})) = q_W(f_W(\omega'_{i,j})) + q_W(\beta_{ij}^W) + q_W(dh_W)$. Dans ce qui suit on va donc procéder au calcul de ces trois termes.

Lemme 8.5.1. *Soit $\omega'_{i,j} \in H^0(X'_k, \Omega_{X'_k}^1)$ un élément de la base (voir proposition 7.1.1). Soient a le quotient et b le reste de la division euclidienne de pj par n . Soient $v(s)$ le polynôme du relèvement du Frobenius modulo p^2 sur W_1 (voir proposition 7.2.3) et $Q(s)$ la fraction rationnelle $(s^{p-1} + v'(s))/f_2(s)^a$. Alors $1 \leq b \leq n-1$, Q est un polynôme en s et si l'on note $Q[k]$ le coefficient du monôme s^k dans Q et dQ le degré de Q , alors*

$$q_W(f_W(\omega'_{i,j})) = \sum_{\mu=0}^{rb-2} Q[rb-2 + p(i+2-rj) - \mu] \frac{t^\mu dt}{y^b}$$

dans $H^0(X_k, \Omega_{X_k}^1)$. Pour mémoire $f_W(\omega'_{i,j})$ désigne la deuxième composante de $DI_1(\omega'_{i,j})$ (voir proposition 7.3.1).

Preuve: L'argument pour la condition sur b est toujours le même. De plus on a vu à la remarque 7.3.2 que l'entier a était toujours strictement inférieur à p et donc en vertu de la proposition 7.2.5 Q est bien un polynôme en s . On utilise la formule de la remarque 7.3.2 pour f_W et on a

$$f_W(\omega'_{i,j}) = -s^{p(rj-(i+2))} Q(s) \frac{ds}{z^b} = \sum_{\mu=0}^{dQ} -Q[\mu] s^\mu s^{p(rj-(i+2))} \frac{ds}{z^b}$$

ce qui donne par le changement de variable $\mu' = p(rj - (i + 2)) + \mu$ l'expression

$$f_W(\omega'_{i,j}) = \sum_{\mu'=p(rj-(i+2))}^{p(rj-(i+2))+rb-2} -Q[\mu' - p(rj - (i + 2))] s^{\mu'} \frac{ds}{z^b}.$$

Grâce au lemme 4.1.1 on sait que pour calculer $q_W(f_W(\omega'_{i,j}))$ on ne garde que les valeurs de μ' pour lesquelles $0 \leq \mu' \leq rb - 2$ et on obtient ainsi

$$q_W(f_W(\omega'_{i,j})) = \sum_{\mu'=0}^{rb-2} -Q[\mu' - p(rj - (i + 2))] s^{\mu'} \frac{ds}{z^b}$$

où la somme ne contient pas de termes supplémentaires puisque $p(rj - (i + 2)) \geq 0$ et donc $p(rj - (i + 2)) + rb - 2 \geq rb - 2$ et par ailleurs pour μ' compris entre 0 et $p(rj - (i + 2))$ on a $\mu' - p(rj - (i + 2)) < 0$ et comme Q est un polynôme $Q[\mu' - p(rj - (i + 2))] = 0$. En utilisant la condition de recollement on a

$$q_W(f_W(\omega'_{i,j})) = \sum_{\mu'=0}^{rb-2} -Q[\mu' - p(rj - (i + 2))] t^{-\mu'} \frac{-t^{-2} dt}{t^{-rb} y^b} = \sum_{\mu'=0}^{rb-2} Q[\mu' - p(rj - (i + 2))] t^{rb-2-\mu'} \frac{dt}{y^b}$$

soit par le changement de variable $\mu = rb - 2 - \mu'$

$$q_W(f_W(\omega'_{i,j})) = \sum_{\mu=0}^{rb-2} Q[rb - 2 - p(rj - (i + 2)) - \mu] \frac{t^\mu dt}{y^b}$$

ce qui achève la démonstration. □

Lemme 8.5.2. Soit $\omega'_{i,j} \in H^0(X'_k, \Omega_{X'_k}^1)$ un élément de la base (voir proposition 7.1.1). Notons β_{ij}^W la deuxième composante de $\tau(\overline{h(\omega'_{i,j})})$ (voir proposition 6.0.6). Alors

$$q_W(\beta_{ij}^W) = 0$$

dans $H^0(X_k, \Omega_{X_k}^1)$.

CHAPITRE 8. CALCUL DE LA MATRICE DU FROBENIUS DIVISÉ DE LA FIBRE SPÉCIALE

Preuve: On sait par la proposition 8.4.1 que dans $H^1(X_k, \mathcal{O}_{X_k})$ on a l'égalité

$$\overline{h(\omega'_{i,j})} = \sum_{m=1}^{r(n-b)-1} \left(\sum_{k=0}^{dIP} IP[k]v[p(i+2) + k + m] \right) \overline{t^{-m}y^{n-b}}$$

et alors par linéarité du scindage il suffit de calculer la deuxième composante de $\tau(\overline{t^{-m}y^{n-b}})$ qui est égale à $-\beta_{ij}^W$ où

$$\beta_{ij}^W = \sum_{\mu=0}^m \frac{mn - (n-b)\mu}{n} f[\mu] s^{m+rb-1-\mu} \frac{ds}{z^b},$$

(voir proposition 6.0.6) et donc

$$\beta_{ij}^W = \sum_{m=1}^{r(n-b)-1} \sum_{k=0}^{dIP} IP[k]v[p(i+2) + k + m] \sum_{\mu=0}^m \frac{mn - (n-b)\mu}{n} f[\mu] s^{m+rb-1-\mu} \frac{ds}{z^b}.$$

On constate que puisque $\mu \leq m$ alors $m + rb - 1 - \mu \geq rb - 1$ et donc dans cette somme la puissance en s est toujours strictement supérieure à $rb - 2$. Mais grâce au lemme 4.1.1 on sait que pour calculer $q_W(\beta_{ij}^W)$ on ne conserve que les termes dont la puissance en s est comprise entre 0 et $rb - 2$ et on obtient donc le résultat annoncé. \square

Lemme 8.5.3. Soit $\omega'_{i,j} \in H^0(X'_k, \Omega_{X'_k}^1)$ un élément de la base (voir la proposition 7.1.1). Soient $v(s)$ le polynôme intervenant dans le relèvement du Frobenius modulo p^2 sur W_1 (voir la proposition 7.2.3), $d = \max\{0, \deg(v) - 2p\}$, I_d l'inverse de f à l'ordre $d + 1$ (voir le lemme 7.5.6). Soient a le quotient et b le reste de la division euclidienne de pj par n . Notons $IP(t) = I_d(t)^{a+1}$, $dIP = \deg(IP)$, $IP[k]$ le coefficient du monôme t^k dans $IP(t)$ et $v[m]$ le coefficient du monôme s^m dans $v(s)$. Soit $h = h(\omega'_{i,j}) - \iota(h(\omega'_{i,j}))$ et notons $h_U \in \mathcal{O}_{\overline{U}_k}$ et $h_W \in \mathcal{O}_{W_k}$ tels que $h = h_U + h_W$ (voir proposition 7.4.1). Posons $\nu_{m,k} = p(i+2) + k + m$, alors $1 \leq b \leq n - 1$ et

$$q_W(dh_W) = \sum_{\mu=0}^{rb-2} \left(\sum_{k=0}^{dIP} \sum_{m=r(n-b)}^{d-(pi+k)} \frac{n(\mu+1) - b(\mu+m+1)}{n} IP[k] \cdot f[\mu+m+1] \cdot v[\nu_{m,k}] \right) \frac{t^\mu dt}{y^b}$$

dans $H^0(X_k, \Omega_{X_k}^1)$. Où par convention la somme est nulle si $r(n-b) > d - (pi+k)$.

Preuve: Dans la démonstration de la proposition 8.4.1 on a obtenu l'égalité suivante

$$t^{p(i+2)} IP(t)v(s)y^{n-b} = \sum_{k=0}^{dIP} \sum_{m=pi+r(n-b)+k-d}^{p(i+2)+r(n-b)+k} IP[k] \cdot v[p(i+2) + r(n-b) + k - m] \cdot s^{-m} z^{n-b}.$$

Clairement si $pi + r(n-b) + k - d > 0$ i.e $r(n-b) > d - (pi+k)$ cette somme ne contient aucun terme polynômial en s et donc $h_W = 0$ ce qui implique que $dh_W = 0$. Dans le cas contraire notons on a alors

$$h_W = \sum_{k=0}^{dIP} \sum_{m=pi+r(n-b)+k-d}^0 IP[k] \cdot v[p(i+2) + r(n-b) + k - m] \cdot s^{-m} z^{n-b}$$

et en utilisant les conditions de recollement

$$h_W = \sum_{k=0}^{dIP} \sum_{m=pi+r(n-b)+k-d}^0 IP[k] \cdot v[p(i+2) + r(n-b) + k - m] \cdot t^m t^{-r(n-b)} y^{n-b}.$$

Posons $m' = r(n-b) - m$ on a alors

$$h_W = \sum_{k=0}^{dIP} \sum_{m'=r(n-b)}^{d-(pi+k)} IP[k] \cdot v[p(i+2) + k + m'] \cdot t^{-m'} y^{n-b}.$$

Par différentiation on obtient

$$dh_W = \sum_{k=0}^{dIP} \sum_{m'=d-(pi+k)}^{r(n-b)} IP[k] \cdot v[p(i+2) + k + m'] \left(-m' t^{-m'-1} y^{n-b} dt + (n-b) t^{-m'} y^{n-b-1} dy \right)$$

qui est donc un élément de $\Omega_{X_k}^1(W_k)$, alors comme $y^n = f(t)$ et $ny^{n-1}dy = f'(t)dt$

$$dh_W = \sum_{k=0}^{dIP} \sum_{m'=d-(pi+k)}^{r(n-b)} IP[k] \cdot v[p(i+2) + k + m'] \left(-m' t^{-m'-1} f(t) + (n-b) t^{-m'} \frac{f'(t)}{n} \right) \frac{dt}{y^b}.$$

Or on a

$$\begin{aligned} -m' t^{-m'-1} f(t) + (n-b) t^{-m'} \frac{f'(t)}{n} &= \sum_{\mu=0}^l -m' f[\mu] t^{\mu-m'-1} + \sum_{\mu=0}^l \frac{n-b}{n} \mu f[\mu] t^{\mu-1-m'} \\ &= \sum_{\mu=0}^l \frac{\mu(n-b) - m'n}{n} f[\mu] t^{\mu-m'-1} \end{aligned}$$

d'où

$$dh_W = \sum_{k=0}^{dIP} \sum_{m'=d-(pi+k)}^{r(n-b)} \sum_{\mu=0}^l \frac{\mu(n-b) - m'n}{n} IP[k] \cdot v[p(i+2) + k + m'] \cdot f[\mu] \frac{t^{\mu-m'-1} dt}{y^b}.$$

On réalise le changement de variable $\mu' = \mu - m' - 1$ et on pose $\nu_{m',k} = p(i+2) + k + m'$, alors

$$dh_W = \sum_{k=0}^{dIP} \sum_{m'=d-(pi+k)}^{r(n-b)} \sum_{\mu'=-m'+1}^{l-(m'+1)} \frac{n(\mu'+1) - b(\mu'+m'+1)}{n} IP[k] \cdot v[\nu_{m',k}] \cdot f[\mu'+m'+1] \frac{t^{\mu'} dt}{y^b}.$$

Enfin grâce au lemme 4.1.1 on sait que pour calculer $q_W(dh_W)$ on ne conserve que les termes tels que $0 \leq \mu' \leq rb - 2$ ce qui donne la formule annoncée. Par ailleurs il n'y a pas de termes supplémentaires car si $-(m'+1) > 0$ ou $l - (m'+1) < rb - 2$ alors dans le premier cas on aura un terme avec $\mu' < -(m'+1)$ et donc $\mu' + m' + 1 < 0$ et le coefficient sera nul puisque f est un polynôme. Dans le second cas $\mu' + m' + 1 > l$ et comme $\deg(f) = l$ le coefficient sera à nouveau nul.

□

CHAPITRE 8. CALCUL DE LA MATRICE DU FROBENIUS DIVISÉ DE LA FIBRE SPÉCIALE

Proposition 8.5.1. Soit $\omega_{i,j} \in H^0(X_k, \Omega_{X_k}^1)$ un élément de la base (voir proposition 4.1.1). Soient $v(s)$ le polynôme intervenant dans le relèvement du Frobenius modulo p^2 sur W_1 (voir proposition 7.2.3), $d = \max\{0, \deg(v) - 2p\}$ et I_d l'inverse de f à l'ordre $d+1$ (voir lemme 7.5.6). Soient a le quotient et b le reste de la division euclidienne de pj par n , notons $IP(t) = I_d(t)^{a+1}$, $dIP = \deg(IP)$, $IP[k]$ le coefficient du monôme t^k dans $IP(t)$ et $v[m]$ le coefficient du monôme s^m dans $v(s)$. Soit $Q(s)$ le polynôme $(s^{p-1} + v'(s))/f_2(s)^a$ (voir lemme 8.5.1), notons $Q[k]$ le coefficient du monôme s^k dans Q et dQ le degré de Q . Alors $1 \leq b \leq n - 1$ et si on note $\nu_{m,k} = p(i+2) + k + m$,

$$P_2(\Phi(\omega_{i,j})) = \sum_{\mu=0}^{rb-2} \left(\sum_{k=0}^{dIP} \sum_{m=r(n-b)}^{d-(pi+k)} \frac{n(\mu+1) - b(\mu+m+1)}{n} IP[k] \cdot f[\mu+m+1] \cdot v[\nu_{m,k}] + Q[rb-2 + p(i+2-rj) - \mu] \right) \frac{t^\mu dt}{y^b}$$

dans $H^0(X_k, \Omega_{X_k}^1)$. Où par convention la double somme est nulle si $r(n-b) > d - (pi+k)$.

Preuve: Cette proposition est tout simplement une conséquence de la proposition 7.4.1 et des lemmes 8.5.1, 8.5.2 et 8.5.3. □

8.6 Le cas à paramètre

Il peut être intéressant d'effectuer les calculs dans le cas à paramètre. Par exemple l'une des familles de courbes étudiées par Noot-de Jong dans [dJN91] est $y^3 = t(t-1)(t-\lambda)(t-\mu)(t-\nu)$. Cette famille vérifie bien la condition $l \equiv -1 \pmod{n}$ et quitte à réaliser une translation on peut la transformer en une famille de courbe telle que 0 n'est pas racine de f et qui correspond donc à notre cadre de travail.

Cependant le paramètre peut poser des problèmes pour la machine notamment pour le calcul du relèvement du Frobenius sur W_1 qui nécessite le calcul d'une relation de Bezout. On peut cependant utiliser le résultant pour calculer le polynôme v intervenant dans ce relèvement (voir proposition 7.2.3).

Lemme 8.6.1. Notons M la matrice de Sylvester associée à $f_2(s)$ et $f_2'(s)$, $M_{i,2l+1}$ le mineur d'ordre $i, 2l+1$ de M . Soient U et V les polynômes tels que $Uf_2 + Vf_2' = \text{Res}(f_2, f_2')$, alors V est donné par l'expression

$$V(s) = \sum_{k=0}^l (-1)^{l+k} M_{l+1+k, 2l+1} s^{l-k}.$$

Preuve: Tout d'abord on sait que le résultant de f_2 et f_2' est donné par le déterminant de la matrice de Sylvester de $f_2(s)$ et $f_2'(s)$. Par ailleurs une astuce connue afin d'obtenir les polynômes U et

V est d'effectuer l'opération sur les colonnes

$$C_{2l+1} \leftarrow C_{2l+1} + \sum_{j=1}^{2l} s^{2l+1-j} C_j$$

qui laisse inchangées les $2l$ premières colonnes et transforme la dernière colonne en

$$\begin{pmatrix} s^{l-1} f_2 \\ \vdots \\ f_2 \\ s^l f'_2 \\ \vdots \\ f'_2 \end{pmatrix}$$

puis à développer le déterminant par rapport à la dernière colonne. Or le développement par rapport à la dernière colonne donne pour les l premières ligne les coefficients de U et pour les $l + 1$ suivantes les coefficients de V . Ce qui permet de déduire la formule donnée, la puissance de -1 étant déduite du fait que le coefficient de la toute dernière ligne est $+1$ or il correspond à $k = l$.

□

Proposition 8.6.1. *Le polynôme v du relèvement du Frobenius modulo p^2 sur W_1 de la proposition 7.2.3 est donné par la formule*

$$v(s) = \frac{V(s)^p}{\text{Res}(f_2, f'_2)^p} \frac{f_2(s)^p - f_2(s^p)}{p}$$

où $V(s)$ est le polynôme donné par le lemme 8.6.1

Preuve: Tout d'abord puisqu'on est dans le cas où $f_2 \wedge f'_2 = 1$ alors $\text{Res}(f_2, f'_2) \neq 0$ et donc on a la relation

$$\frac{U(s)}{\text{Res}(f_2, f'_2)} f_2(s) + \frac{V(s)}{\text{Res}(f_2, f'_2)} f'_2(s) = 1.$$

Par ailleurs puisqu'on est sur un corps de caractéristique p alors

$$\left(\frac{U(s)}{\text{Res}(f_2, f'_2)} f_2(s) + \frac{V(s)}{\text{Res}(f_2, f'_2)} f'_2(s) \right)^p = \frac{U(s)^p}{\text{Res}(f_2, f'_2)^p} f_2(s)^p + \frac{V(s)^p}{\text{Res}(f_2, f'_2)^p} f_2'^p(s) = 1$$

enfin pour trouver le polynôme v il suffit de multiplier cette relation par $(f_2(s)^p - f_2(s^p))/p$ toujours en vertu de la proposition 7.2.3 ce qui donne le résultat annoncé.

□

Chapitre 9

Un procédé algorithmique pour la décomposition de Jordan-Hölder des φ -modules filtrés

Le groupe de cohomologie $H_{DR}^1(X_k)$ muni de la filtration de Hodge et du Frobenius divisé a une structure de φ -module filtré sur k au sens de Fontaine-Laffaille [FL82]. Ce qui suit est consacré à un procédé algorithmique fournissant une description des φ -modules filtrés simples apparaissant comme quotients de Jordan-Hölder de $H_{DR}^1(X_k)$. Celui-ci se base sur la démonstration du lemme 4.8 de *op cit.*

9.1 Mise en contexte

Définition 9.1.1. *Un φ -module filtré sur k est un k -espace vectoriel de dimension finie \mathcal{M} , muni d'une filtration décroissante par des sous-espaces vectoriels $Fil^r \mathcal{M}$ et d'une application ϕ , appelée Frobenius divisé, semi-linéaire, bijective, définie sur le gradué*

$$Gr \mathcal{M} = \bigoplus_{r \in \mathbb{Z}} Fil^r \mathcal{M} / Fil^{r+1} \mathcal{M}$$

et à valeurs dans \mathcal{M} .

Soit X_k une courbe définie comme précédemment (section 2.1), posons $\mathcal{M} = H_{DR}^1(X_k)$. Alors muni de la filtration $Fil^0 \mathcal{M} = \mathcal{M}$, $Fil^1 \mathcal{M} = H^0(X_k, \Omega_{X_k}^1)$, $Fil^2 \mathcal{M} = 0$ et de ϕ , application dont la matrice a été calculée précédemment dans une base adaptée à la filtration (section 7.4), $\mathcal{M} = H_{DR}^1(X_k)$ est un φ -module filtré sur k .

Les φ -modules filtrés simples de dimension m sur un corps algébriquement clos \bar{k} sont bien connus depuis [FL82] proposition 4.4. Ils sont de la forme $\mathcal{M}(i_0, \dots, i_{h-1})$ où la suite $(i_r)_{0 \leq r \leq h-1}$ n'est pas périodique. Ils sont décrits explicitement de la manière suivante.

Soit $\mathcal{M} = \bar{k}^h$ et soit $(e_r)_{0 \leq r \leq h-1}$ la base canonique. Définissons la filtration par

$$Fil^r \mathcal{M} = \bigoplus_{i_m \geq r} e_m$$

et pour x élément de \mathcal{M} notons \bar{x} sa projection dans $Gr\mathcal{M}$. Si r est le plus grand entier tel que x soit dans $Fil^r \mathcal{M}$, alors $\bar{x} \in Fil^r \mathcal{M} / Fil^{r+1} \mathcal{M}$. Enfin l'application φ est définie sur la base par $\varphi(\bar{e}_r) = e_{r+1}$ pour $0 \leq r \leq h-2$ et $\varphi(\bar{e}_{h-1}) = e_0$.

Dans notre cas on a $Fil^0 \mathcal{M} = \mathcal{M}$ et $Fil^2 \mathcal{M} = 0$ donc les termes de la suite (i_r) sont des 0 ou des 1. On peut par exemple voir apparaître le module trivial sur k , représenté par la suite (0) , où $Fil^0 = \langle e_0 \rangle$, $Fil^1 = Fil^2 = 0$ et $\phi(e_0) = e_0$. De même on peut voir apparaître le module sur k noté $k(1)$ et représenté par la suite (1) où $Fil^0 = Fil^1 = \langle e_0 \rangle$, $Fil^2 = 0$ et $\phi(e_0) = e_0$. Il est bien évidemment possible d'avoir des modules de dimension supérieure. Dans les exemples traités plus loin (section A.4.1) on voit notamment apparaître un module que l'on représente par la suite $(0, 1)$ et pour lequel $Fil^0 = \langle e_0, e_1 \rangle$, $Fil^1 = \langle e_0 \rangle$, $Fil^2 = 0$ et $\phi(e_0) = e_1$, $\phi(e_1) = e_0$.

Remarque 9.1.1. On a vu dans ce qui précède que le calcul de l'application ϕ nécessite de se placer dans le gradué qui dans notre cas sera $Fil^0 / Fil^1 \oplus Fil^1$. Notons ϕ_{gr} l'application définie par $\phi_{gr}(x) = \phi(\bar{x})$ i.e. si x est dans Fil^1 alors $\phi_{gr}(x) = \phi(x)$, sinon $\phi_{gr}(x) = \phi(\bar{x})$. Alors $\phi_{gr}^2(x) = \phi(\phi(\bar{x}))$ et on définit de la même manière $\phi_{gr}^r(x)$. Il est important de noter que ϕ_{gr} n'est pas additive.

La démonstration de la proposition de 4.4 de [FL82] sur laquelle repose la classification des φ -modules filtrés simples utilise un lemme (lemme 4.8 *op cit*) que nous énonçons ici avec les notations de notre cadre de travail. Nous donnons également les grandes lignes de la démonstration puisque c'est à partir de celle-ci que l'on développe le procédé algorithmique présenté dans ce texte.

Lemme 9.1.1. *Soit \mathcal{M} un φ -module filtré non nul et soit m la dimension du k -espace vectoriel sous-jacent, supposons k algébriquement clos. Alors il existe un entier h vérifiant $1 \leq h \leq m$ tel que l'ensemble des éléments x de \mathcal{M} vérifiant $\phi_{gr}^h(x) = x$ ne soit pas réduit à 0.*

Preuve: On reprend les résultats principaux de la démonstration originale. Considérons l'ensemble des relations suivant

$$\mathcal{J} = \left\{ \sum_{j \in J} a_j \phi_{gr}^j(x) = 0, x \in \mathcal{M}, x \neq 0, J \subset \mathbb{N}, J \neq \emptyset, a_j \in k^*, \forall j \in J \right\}$$

qui est non vide puisque \mathcal{M} est un k -espace vectoriel de dimension finie.

Définissons une relation d'ordre sur les sous-ensembles finis non vides de \mathbb{N} . Pour cela associons à un tel J le couple d'entiers (m_J, n_J) où $m_J = \sup\{j, j \in J\}$ et $n_J = \#J$ et munissons $\mathbb{N} \times \mathbb{N}$

CHAPITRE 9. UN PROCÉDÉ ALGORITHMIQUE POUR LA DÉCOMPOSITION DE JORDAN-HÖLDER DES φ -MODULES FILTRÉS

de la relation d'ordre lexicographique. Choisissons alors une relation de \mathcal{J} pour laquelle le couple (m_J, n_J) soit minimal.

Il est alors possible de montrer que dans ce cas $0 \in J$ et que par ailleurs tous les $\phi_{gr}^j(x)$ avec $j \in J$ sont dans le même cran i_0 de la filtration.

Notons alors h le pgcd des éléments de J , h' l'entier tel que $m_J = hh'$ et définissons N comme étant le sous- k -espace vectoriel de base $\phi_{gr}^{hn}(x)$ pour $0 \leq n \leq h' - 1$. Comme tous les $\phi_{gr}^{hn}(x)$ sont dans $Fil^{i_0}\mathcal{M}$, on peut montrer que $N \subset Fil^{i_0}\mathcal{M}$ et $N \cap Fil^{i_0+1}\mathcal{M} = 0$ puis que $\phi_{gr}^h|_N$ s'identifie à une application bijective de N dans N qui est σ^h -semi-linéaire, où σ désigne le Frobenius sur k . En utilisant un résultat dû à Jacobson (chapitre 2 théorème 15 de [Jac43]) on peut alors affirmer qu'il existe y dans N non nul et $a \in k$ tels que $\phi_{gr}^h(y) = ay$. Enfin comme k est algébriquement clos, quitte à multiplier y par une constante non nulle, on peut supposer que $\phi_{gr}^h(y) = y$. Par ailleurs puisque $hh' = m_j$ et $1 \leq m_j \leq m$ on a bien $1 \leq h \leq m$ d'où le lemme. □

Remarque 9.1.2. La mise en place des étapes de la démonstration nécessite non seulement de faire varier J mais également x afin de trouver un élément de \mathcal{J} minimal. Supposons que l'on fixe x et que l'on fasse uniquement varier J , on peut alors se trouver avec une relation, minimale pour x fixé, mais pour laquelle les $\phi_{gr}^j(x)$ ne seraient pas tous dans le même cran de la filtration. Cependant dans notre cas la filtration n'ayant que deux crans on peut alors séparer la relation en deux sommes. L'une contenant les termes étant dans Fil^1 et l'autre contenant ceux de Fil^0 . En appliquant ϕ_{gr} à cette relation et en notant $x' = \phi_{gr}(x)$ on obtient alors une nouvelle relation (sur x' cette fois) avec $m_{J'} \leq m_J$ et $n_{J'} < n_J$. En itérant cette opération il est alors possible d'obtenir une relation dont tous les éléments sont bien dans le même cran de la filtration. Par ailleurs cette opération se termine en un nombre fini d'opérations puisque le nombre n_J d'éléments intervenant dans la relation diminue toujours au moins de 1. Enfin il est possible que cette relation ne fasse pas intervenir x , mais en posant $m = \min\{j \in J\}$ et $x' = \phi_{gr}^m(x)$ on obtient finalement une relation telle que l'ensemble J contienne 0 et que tous les termes soient dans le même cran de la filtration. Cela nous permet d'appliquer le résultat de Jacobson. Cela signifie qu'on peut faire fonctionner la démonstration du lemme en fixant tout d'abord x et en faisant seulement varier J quitte à modifier x , tout d'abord afin que les $\phi_{gr}^j(x)$ successifs soient dans le même cran de la filtration, puis de manière à ce que 0 soit dans J . C'est ce que nous faisons dans le procédé algorithmique présenté dans ce qui suit.

9.2 Description du cadre de travail

On va présenter ici le cas d'une filtration à deux crans quelconque qui est celui qui correspond à notre problème.

Soit donc \mathcal{M} un k -module, $E_0 = Fil^1\mathcal{M}$ et F_0 supplémentaire de E_0 dans \mathcal{M} . Notons m_0 la dimension de l'espace vectoriel sous-jacent à E_0 , n_0 la dimension de l'espace vectoriel sous-jacent à F_0 et alors la dimension de l'espace vectoriel sous-jacent à \mathcal{M} est $m_0 + n_0$.

Notons $\mathcal{E} = (e_1, \dots, e_{m_0}, e_{m_0+1}, \dots, e_{m_0+n_0})$ une base de \mathcal{M} adaptée à la filtration (i.e. (e_1, \dots, e_{m_0}) est une base de $Fil^1\mathcal{M} = E_0$ et $(e_{m_0+1}, \dots, e_{m_0+n_0})$ est une base de F_0). Soit ϕ une application

semi-linéaire sur \mathcal{M} et M_ϕ sa matrice dans la base \mathcal{E} .

Le principe du procédé algorithmique que nous allons présenter est le suivant. Il prend en entrée E_0, F_0, m_0, n_0 et M_ϕ et donne en sortie une liste correspondant à la liste des sous-modules simples successifs apparaissant dans la décomposition de Jordan-Hölder. La procédure est itérative, on commence par trouver un sous-module simple puis on passe au quotient ce qui permet d'obtenir E_1, F_1, m_1, n_1 et M_ϕ^1 et il s'agit alors de répéter la procédure jusqu'à obtenir un espace simple. Le procédé algorithmique est assuré de se terminer puisque à chaque cran m_i , ou n_i diminue. Nous allons présenter ici la manière d'obtenir un sous-module simple puis quelles transformations opérer sur les données d'entrée pour obtenir les nouvelles données sur lesquelles recommencer le procédé algorithmique.

Notons que dans la démonstration du lemme, k est un corps algébriquement clos. Cela ne sert que pour la dernière étape du procédé algorithmique pour assurer que l'on peut trouver un vecteur propre. Cependant il n'est pas forcément nécessaire que k soit algébriquement clos et il suffit généralement de prendre une extension bien choisie de k . Dans les exemples traités en A.4.1 il n'y a même pas besoin d'extension et tout se fait sur \mathbb{F}_p .

9.3 Obtention de la combinaison linéaire minimale

Dans la démonstration du lemme 4.8 de [FL82] la première étape consiste à prendre $x \in \mathcal{M}$ non nul quelconque et à considérer l'ensemble \mathcal{J} des relations de la forme

$$\sum_{j \in J} a_j \phi_{gr}^j(x) = 0$$

avec $J \subset \mathbb{N}$ non vide et $\forall j \in J, a_j \in k$ non nul. On pose $m_J = \sup\{j, j \in J\}$, $n_J = \text{Card}(J)$ et on munit les sous-ensembles finis non vides $J \subset \mathbb{N}$ d'une relation d'ordre en considérant l'ordre lexicographique sur les couples (m_J, n_J) . L'idée est de trouver un ensemble J de \mathcal{J} qui soit minimal selon cette relation d'ordre.

Tout d'abord remarquons que puisque l'espace vectoriel sous-jacent à \mathcal{M} est de dimension $m_0 + n_0$ alors si J est l'ensemble tel que (m_J, n_J) soit minimal, $m_J \leq m_0 + n_0$. Afin de trouver J il faut commencer par trouver m_J minimal. Pour cela remarquons que cela signifie simplement qu'on cherche le plus petit entier r tel que la famille $(x, \phi_{gr}(x), \dots, \phi_{gr}^r(x))$ soit liée. Pour trouver m_J il suffit donc de calculer les images successives de x par ϕ_{gr} et à chaque nouvel élément de vérifier si la famille obtenue est liée. Le nombre d'itérations de ϕ_{gr} correspondant est alors m_J .

L'étape suivante consiste à trouver une relation minimale entre les éléments de cette famille, c'est-à-dire faisant intervenir le moins de coefficients non nuls possibles. En fait comme \mathcal{M} est de rang $m_0 + n_0$ et que $m_J \leq m_0 + n_0$ l'équation $\sum a_j \phi_{gr}^j(x) = 0$ va donner un système de $m_0 + n_0$ équations à $m_J \leq m_0 + n_0$ inconnues. Ces équations sont liées et comme la famille $(\phi_{gr}^j(x))_{0 \leq j \leq m_J-1}$ est libre, l'espace des solutions est donc de dimension 1. Alors tout élément de l'espace considéré admettra le même nombre de coefficients non nuls donc n'importe lequel pourra convenir.

Voici un algorithme donnant une matrice A dont les colonnes sont $x, \phi_{gr}(x), \dots, \phi_{gr}^{m_J}(x)$ respectivement. La commande "A.right_kernel()" permet alors d'obtenir les générateurs du noyau à

CHAPITRE 9. UN PROCÉDÉ ALGORITHMIQUE POUR LA DÉCOMPOSITION DE JORDAN-HÖLDER DES φ -MODULES FILTRÉS

droite de A i.e. des $m_{J+1} - \text{uplet}$ (a_0, \dots, a_{m_J}) correspondant aux coefficients d'une combinaison linéaire nulle. Comme il est de dimension 1 le générateur convient.

```
def Iteration(M,m,n,x) :
    A=x
    Res=x
    l=1
    u=zero_vector(n)
    while rank(A)==1 :
        for i in range(n) :
            u[i]=Res[i+m,0]
        if u==0 :
            Res=M*Res
        else :
            for i in range(m) :
                Res[i,0]=0
            Res=M*Res
        A=block_matrix([[A,Res]])
        l=l+1
    return A
```

Remarquons que le test "if u==0" permet de déterminer si l'élément dont on souhaite déterminer l'image est dans Fil^1 ou non. Dans le premier cas son image est simplement donnée par la produit avec la matrice de ϕ . Dans le cas contraire son image est donnée par le produit de M_ϕ et de sa classe dans Fil^0/Fil^1 , obtenue simplement en mettant à zéro les composantes sur (e_0, \dots, e_{m_0}) . Supposons obtenue la relation $\sum_{j \in J} a_j \phi_{gr}^j(x) = 0$. Il nous faut contrôler si tous les termes de cette relation sont dans le même cran de la filtration. Dans le cas contraire, on définit les ensembles $J^1 = \{j \in J \text{ tq } \phi_{gr}^j(x) \in Fil^1\}$ et $J^0 = J - J^1$. On applique alors ϕ_{gr} à la relation : par définition

$$\phi_{gr} \left(\sum_{j \in J} a_j \phi_{gr}^j(x) \right) = \phi \left(\overline{\sum_{j \in J} a_j \phi_{gr}^j(x)} \right) = \phi \left(\overline{\sum_{j \in J^0} a_j \phi_{gr}^j(x)} \right)$$

et comme ϕ est additive sur Fil^0/Fil^1 on obtient

$$\phi \left(\overline{\sum_{j \in J^0} a_j \phi_{gr}^j(x)} \right) = \sum_{j \in J^0} a_j \phi \left(\overline{\phi_{gr}^j(x)} \right)$$

et puisque par définition sur Fil^0/Fil^1 on a $\phi(\bar{u}) = \phi_{gr}(u)$, en posant $x' = \phi_{gr}(x)$, on obtient alors la relation $\sum_{j \in J^0} a_j \phi_{gr}^j(x') = 0$. Si tous les termes sont dans le même cran de la filtration on passe à l'étape suivante, sinon on réitère le procédé.

Enfin on pose $\min = \min \{j \in J\}$. Si $j = 0$ on peut passer à l'étape suivante, sinon on pose $x' = \phi_{gr}^{\min}(x)$ ce qui transforme la relation en une relation telle que $0 \in J'$.

9.4 Obtention d'un sous-espace stable simple

On suppose maintenant donnée une relation

$$\sum_{j \in J} a_j \phi_{gr}^j(x) = 0$$

répondant au problème initial où J est un sous-espace de \mathbb{N} contenant 0 et où chaque terme de la somme est dans le même cran de la filtration. Notons h le pgcd des éléments de J et h' l'entier tel que $m_J = hh'$. Enfin appelons N le sous- k -espace vectoriel engendré par la famille $(\phi_{gr}^{hi}(x))$ pour $0 \leq i \leq h' - 1$ (qui en est donc une base puisqu'elle est libre). On sait, par Jacobson [Jac43], que

$$\exists y \in N \setminus \{0\}, \exists a \in k \text{ tq } \phi_{gr}^h(y) = ay.$$

L'espace engendré par $(y, \phi_{gr}(y), \dots, \phi_{gr}^{h-1}(y))$ est donc un sous-espace stable par ϕ . Cependant il n'est pas nécessairement simple.

Afin de vérifier la simplicité, associons au h -uplet $(y, \phi_{gr}(y), \dots, \phi_{gr}^{h-1}(y))$ un h -uplet de $\{0, 1\}^h$ défini de la manière suivante. Si $\phi_{gr}^i(y) \in Fil^1$ alors la $(i + 1)$ -ième composante est un 1, un 0 sinon. Enfin pour tout d diviseur strict de h vérifions que ce h -uplet n'est pas périodique de période d . S'il n'admet aucune période l'espace engendré par $(y, \phi_{gr}(y), \dots, \phi_{gr}^{h-1}(y))$ est simple, sinon il admet un sous-espace stable de dimension d et il faut donc recommencer la procédure avec $(y, \phi_{gr}(y), \dots, \phi_{gr}^{h-1}(y))$.

Cela implique un résultat assez intuitif, si n_0 est nul alors la liste que doit renvoyer le procédé algorithmique est tout simplement un n_0 -uplet de 1 (i.e. on n'a que des sous-espaces simples de Fil^1 et de dimension 1) et si m_0 est nul alors on a un m_0 -uplet de 0.

9.5 Passage à l'étape suivante

On suppose désormais que l'on a $(y, \phi_{gr}(y), \dots, \phi_{gr}^{h-1}(y))$ famille génératrice du sous-espace stable obtenu noté \mathcal{M}_1 . On a alors une suite exacte de k -espaces vectoriels

$$0 \rightarrow \mathcal{M}_1 \rightarrow \mathcal{M} \rightarrow \overline{\mathcal{M}} \rightarrow 0.$$

On définit la filtration sur \mathcal{M}_1 par $Fil^1 \mathcal{M}_1 = Fil^1 \mathcal{M} \cap \mathcal{M}_1$ et sur $\overline{\mathcal{M}}$ par $Fil^1 \overline{\mathcal{M}} = Im(Fil^1 \mathcal{M})$. Alors les morphismes sont strictement compatibles et on a la suite exacte

$$0 \rightarrow Fil^1 \mathcal{M}_1 \rightarrow Fil^1 \mathcal{M} \rightarrow Fil^1 \overline{\mathcal{M}} \rightarrow 0.$$

Il s'agit maintenant d'obtenir E_1, F_1, m_1, n_1 et M_ϕ^1 . En fait $E_1 = Fil^1 \overline{\mathcal{M}}$ et F_1 est un supplémentaire bien choisi dans $\overline{\mathcal{M}}$ il s'agit donc de trouver des bases de ces deux espaces.

Pour m_1 et n_1 on commence par calculer m_N et n_N qui sont respectivement le nombre de 1 et de 0 du h -uplet de $\{0, 1\}^h$ associé à $(y, \phi_{gr}(y), \dots, \phi_{gr}^{h-1}(y))$. Alors $m_1 = m_0 - m_N$ et $n_1 = n_0 - n_N$. L'étape suivante consiste à obtenir une base de E_0 et F_0 adaptée au passage au quotient par le sous-espace stable. On donne ici l'exemple de E_0 . Notons y_1, \dots, y_{m_N} les éléments de $(y, \phi_{gr}(y), \dots, \phi_{gr}^{h-1}(y))$ appartenant à Fil^1 . Alors ils forment une famille libre de E_0 que

CHAPITRE 9. UN PROCÉDÉ ALGORITHMIQUE POUR LA DÉCOMPOSITION DE
 JORDAN-HÖLDER DES φ -MODULES FILTRÉS

l'on peut compléter en une base de E_0 . Le plus simple consiste à remplacer des éléments de la base de E_0 (pour mémoire (e_1, \dots, e_{m_0})) par les y_i . Afin d'être certain d'obtenir une base après remplacement, l'idée générale est de remplacer par y_i l'élément e_j où j est le plus petit entier tel que le coefficient de e_j dans y_i soit non nul et tel que e_j n'ait pas déjà été remplacé par un $y_{i'}$. Cela n'est pas tout à fait systématique car si par exemple $y_1 = e_1 + e_2$ et $y_2 = e_1$ alors la procédure décrite remplacerait e_1 par y_1 et il n'y aurait plus de possibilité pour y_2 . On note E'_0 l'espace engendré par les y_j , i.e. $E'_0 = E_0 \cap \mathcal{M}_1 = \text{Fil}^1 \mathcal{M}_1$. On procède de manière similaire pour trouver une base de F_0 adaptée au passage au quotient par le sous-espace stable et on note F'_0 l'espace $F_0 \cap \mathcal{M}_1$. Remarquons que dans ce cas on a $\mathcal{M}_1 = \text{Fil}^1 \mathcal{M}_1 \oplus F'_0 = E'_0 \oplus F'_0$. Notons E'_1 l'espace dont la base est donnée en supprimant les y_j de la base de E_0 . A priori une base de E_1 est donnée par l'image des éléments de la base de E'_1 dans $\overline{\mathcal{M}}$. On définirait de même F'_1 et une base de F_1 serait l'image des éléments de la base de F'_1 dans $\overline{\mathcal{M}}$. Mais $\text{Fil}^1 \mathcal{M} = E'_0 \oplus E'_1$ et $F_0 = F'_0 \oplus F'_1$, donc par passage au quotient on obtient $\text{Fil}^1 \overline{\mathcal{M}} \simeq E'_1$ et $\overline{F_0} \simeq F'_1$ ce qui permet d'identifier E_1 à E'_1 et F_1 à F'_1 .

Enfin pour M_ϕ^1 il s'agit simplement d'écrire la matrice de ϕ dans la nouvelle base et de supprimer les lignes et les colonnes correspondant aux éléments de la base du sous-espace stable.

Notons \mathcal{B}_1 la base initiale adaptée à la filtration et \mathcal{B}_2 la base adaptée au passage au quotient. Notons C la matrice de passage de \mathcal{B}_1 à \mathcal{B}_2 (i.e. exprimant les éléments de \mathcal{B}_2 dans \mathcal{B}_1). Notons \overline{C} la matrice obtenue de C par passage au gradué (i.e. si dans une colonne les n_0 derniers coefficients sont non nuls alors on met à 0 les m_0 premiers coefficients). Alors la matrice de ϕ dans la nouvelle base est donnée par la formule

$$M'_\phi = C^{-1} M_\phi \overline{C}.$$

Annexe A

Quelques exemples de résultats numériques

A.1 Courbe $y^2 = f(t)$, $\deg(f) = 5$, $p = 7$

On donne ici six exemples numériques.

Pour $f(t) = (t-1)(t-2)(t-3)(t-4)(t-5)$, la matrice du Frobenius est

$$\begin{pmatrix} 0 & 1 & 5 & 1 \\ 2 & 4 & 4 & 3 \\ 5 & 1 & 3 & 6 \\ 1 & 6 & 0 & 4 \end{pmatrix}$$

Pour $f(t) = (t-1)(t-2)(t-3)(t-4)(t-6)$, la matrice du Frobenius est

$$\begin{pmatrix} 2 & 3 & 5 & 4 \\ 3 & 4 & 2 & 6 \\ 0 & 0 & 3 & 3 \\ 5 & 2 & 0 & 4 \end{pmatrix}$$

Pour $f(t) = (t-1)(t-2)(t-3)(t-5)(t-6)$, la matrice du Frobenius est

$$\begin{pmatrix} 2 & 0 & 5 & 5 \\ 1 & 3 & 6 & 5 \\ 5 & 2 & 4 & 5 \\ 1 & 6 & 0 & 3 \end{pmatrix}$$

Pour $f(t) = (t-1)(t-2)(t-4)(t-5)(t-6)$, la matrice du Frobenius est

$$\begin{pmatrix} 5 & 0 & 5 & 2 \\ 1 & 4 & 1 & 5 \\ 5 & 5 & 3 & 5 \\ 6 & 6 & 0 & 4 \end{pmatrix}$$

Pour $f(t) = (t-1)(t-3)(t-4)(t-5)(t-6)$, la matrice du Frobenius est

$$\begin{pmatrix} 5 & 3 & 5 & 3 \\ 3 & 3 & 5 & 6 \\ 0 & 0 & 4 & 3 \\ 2 & 2 & 0 & 3 \end{pmatrix}$$

Pour $f(t) = (t-2)(t-3)(t-4)(t-5)(t-6)$, la matrice du Frobenius est

$$\begin{pmatrix} 0 & 1 & 5 & 6 \\ 2 & 3 & 3 & 3 \\ 5 & 6 & 4 & 6 \\ 6 & 6 & 0 & 3 \end{pmatrix}$$

Pour $f(t) = (t-1)(t-2)(t-3)(t-4)(t-L)$ la matrice de Hasse-Witt est

$$\begin{pmatrix} 3L^2 + 2L + 2 & 3L^2 + 6L + 6 \\ 6L^3 + 5L^2 + L + 2 & 6L^3 + L^2 + 3L + 5 \end{pmatrix}$$

Remarque A.1.1. Si on prend $L = 5$ et $L = 6$ respectivement on obtient pour la matrice de Hasse-Witt

$$\begin{pmatrix} 3 & 6 \\ 0 & 4 \end{pmatrix} \quad \begin{pmatrix} 3 & 3 \\ 0 & 4 \end{pmatrix}$$

qui coïncident bien avec les quarts inférieurs droits des deux premières matrices calculées.

A.2 Courbe $y^2 = (t-1)(t-2)(t-3)(t-4)(t-5)(t-6)(t-7)$, $p = 11$

La matrice du Frobenius est

$$\left(\begin{array}{ccc|ccc} 10 & 7 & 3 & 6 & 2 & 2 \\ 8 & 5 & 5 & 6 & 1 & 7 \\ 2 & 8 & 6 & 6 & 6 & 2 \\ \hline 9 & 3 & 8 & 9 & 6 & 0 \\ 3 & 9 & 8 & 5 & 6 & 5 \\ 4 & 3 & 6 & 2 & 8 & 7 \end{array} \right)$$

par ailleurs le déterminant de la matrice de Hasse-Witt est nul.

A.3 Courbe $y^3 = (t-1)(t-2)(t-3)(t-4)(t-5)$, $5 < p < 100$ premier

$$p = 7 \quad \det(A4) = 4$$

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 4 & 3 & 4 \\ 0 & 5 & 3 & 4 & 5 & 0 & 0 & 0 \\ 0 & 5 & 1 & 5 & 1 & 0 & 0 & 0 \\ 0 & 5 & 5 & 1 & 2 & 0 & 0 & 0 \\ \hline 0 & 0 & 3 & 4 & 5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 1 & 1 \\ 6 & 0 & 0 & 0 & 0 & 0 & 6 & 3 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{array} \right)$$

$$p = 11 \quad \det(A4) = 0$$

$$\left(\begin{array}{cccc|cccc} 0 & 7 & 4 & 3 & 9 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 7 & 0 & 0 & 0 & 0 & 5 & 8 & 6 \\ 8 & 0 & 0 & 0 & 0 & 9 & 7 & 10 \\ \hline 3 & 0 & 0 & 0 & 0 & 3 & 10 & 0 \\ 0 & 4 & 1 & 10 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 7 & 8 & 0 & 0 & 0 \\ 0 & 10 & 7 & 9 & 4 & 0 & 0 & 0 \end{array} \right)$$

$$p = 13 \quad \det(A4) = 12$$

$$\left(\begin{array}{cccc|cccc} 9 & 0 & 0 & 0 & 0 & 6 & 0 & 7 \\ 0 & 0 & 11 & 0 & 9 & 0 & 0 & 0 \\ 0 & 6 & 10 & 4 & 10 & 0 & 0 & 0 \\ 0 & 12 & 2 & 4 & 3 & 0 & 0 & 0 \\ \hline 0 & 0 & 8 & 9 & 10 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 8 & 6 & 12 \\ 11 & 0 & 0 & 0 & 0 & 12 & 9 & 10 \\ 1 & 0 & 0 & 0 & 0 & 6 & 2 & 8 \end{array} \right)$$

$$p = 17 \quad \det(A4) = 0$$

$$\left(\begin{array}{cccc|cccc} 0 & 12 & 16 & 6 & 6 & 0 & 0 & 0 \\ 8 & 0 & 0 & 0 & 0 & 15 & 1 & 11 \\ 9 & 0 & 0 & 0 & 0 & 7 & 0 & 12 \\ 7 & 0 & 0 & 0 & 0 & 1 & 4 & 15 \\ \hline 10 & 0 & 0 & 0 & 0 & 10 & 8 & 0 \\ 0 & 13 & 5 & 8 & 0 & 0 & 0 & 0 \\ 0 & 5 & 10 & 11 & 13 & 0 & 0 & 0 \\ 0 & 8 & 11 & 0 & 10 & 0 & 0 & 0 \end{array} \right)$$

$$p = 19 \quad \det(A4) = 9$$

$$\left(\begin{array}{cccc|cccc} 11 & 0 & 0 & 0 & 0 & 7 & 7 & 5 \\ 0 & 11 & 11 & 1 & 18 & 0 & 0 & 0 \\ 0 & 9 & 4 & 5 & 14 & 0 & 0 & 0 \\ 0 & 8 & 9 & 16 & 3 & 0 & 0 & 0 \\ \hline 0 & 0 & 15 & 14 & 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 15 & 7 \\ 10 & 0 & 0 & 0 & 0 & 6 & 5 & 2 \\ 3 & 0 & 0 & 0 & 0 & 10 & 7 & 0 \end{array} \right)$$

$$p = 23 \quad \det(A4) = 0$$

$$\left(\begin{array}{cccc|cccc} 0 & 14 & 20 & 15 & 14 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 22 & 15 & 6 \\ 22 & 0 & 0 & 0 & 0 & 13 & 8 & 10 \\ 20 & 0 & 0 & 0 & 0 & 20 & 13 & 6 \\ \hline 3 & 0 & 0 & 0 & 0 & 9 & 20 & 0 \\ 0 & 20 & 14 & 18 & 0 & 0 & 0 & 0 \\ 0 & 14 & 8 & 11 & 11 & 0 & 0 & 0 \\ 0 & 18 & 11 & 21 & 20 & 0 & 0 & 0 \end{array} \right)$$

$$p = 29 \quad \det(A4) = 0$$

$$\left(\begin{array}{cccc|cccc} 0 & 26 & 9 & 13 & 0 & 0 & 0 & 0 \\ 8 & 0 & 0 & 0 & 0 & 7 & 4 & 2 \\ 16 & 0 & 0 & 0 & 0 & 11 & 24 & 6 \\ 23 & 0 & 0 & 0 & 0 & 7 & 14 & 28 \\ \hline 6 & 0 & 0 & 0 & 0 & 24 & 21 & 0 \\ 0 & 28 & 26 & 9 & 0 & 0 & 0 & 0 \\ 0 & 26 & 27 & 11 & 10 & 0 & 0 & 0 \\ 0 & 9 & 11 & 27 & 2 & 0 & 0 & 0 \end{array} \right)$$

$$p = 31 \quad \det(A4) = 8$$

$$\left(\begin{array}{cccc|cccc} 21 & 0 & 0 & 0 & 0 & 8 & 2 & 4 \\ 0 & 17 & 19 & 25 & 8 & 0 & 0 & 0 \\ 0 & 14 & 10 & 16 & 30 & 0 & 0 & 0 \\ 0 & 8 & 8 & 14 & 20 & 0 & 0 & 0 \\ \hline 0 & 0 & 16 & 3 & 11 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 9 & 11 & 24 \\ 28 & 0 & 0 & 0 & 0 & 8 & 29 & 10 \\ 13 & 0 & 0 & 0 & 0 & 29 & 15 & 9 \end{array} \right)$$

$$p = 37 \quad \det(A4) = 12$$

$$\left(\begin{array}{cccc|cccc} 27 & 0 & 0 & 0 & 0 & 35 & 18 & 36 \\ 0 & 20 & 1 & 18 & 30 & 0 & 0 & 0 \\ 0 & 24 & 22 & 24 & 12 & 0 & 0 & 0 \\ 0 & 33 & 13 & 22 & 33 & 0 & 0 & 0 \\ \hline 0 & 0 & 12 & 35 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 18 & 13 & 4 \\ 9 & 0 & 0 & 0 & 0 & 8 & 5 & 12 \\ 17 & 0 & 0 & 0 & 0 & 36 & 21 & 18 \end{array} \right)$$

$$p = 41 \quad \det(A4) = 0$$

$$\left(\begin{array}{cccc|cccc} 0 & 1 & 31 & 30 & 36 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 & 0 & 37 & 27 & 14 \\ 34 & 0 & 0 & 0 & 0 & 27 & 9 & 6 \\ 8 & 0 & 0 & 0 & 0 & 14 & 6 & 40 \\ \hline 33 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 36 & 26 & 4 & 0 & 0 & 0 & 0 \\ 0 & 26 & 6 & 31 & 0 & 0 & 0 & 0 \\ 0 & 4 & 31 & 38 & 0 & 0 & 0 & 0 \end{array} \right)$$

$$p = 43 \quad \det(A4) = 23$$

$$\left(\begin{array}{cccc|cccc} 33 & 0 & 0 & 0 & 0 & 40 & 19 & 28 \\ 0 & 38 & 30 & 16 & 16 & 0 & 0 & 0 \\ 0 & 9 & 22 & 0 & 34 & 0 & 0 & 0 \\ 0 & 20 & 31 & 36 & 35 & 0 & 0 & 0 \\ \hline 0 & 0 & 29 & 2 & 8 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 34 & 33 & 16 \\ 12 & 0 & 0 & 0 & 0 & 12 & 0 & 5 \\ 29 & 0 & 0 & 0 & 0 & 1 & 19 & 34 \end{array} \right)$$

$$p = 47 \quad \det(A4) = 0$$

$$\left(\begin{array}{cccc|cccc} 0 & 5 & 17 & 19 & 15 & 0 & 0 & 0 \\ 18 & 0 & 0 & 0 & 0 & 32 & 38 & 0 \\ 26 & 0 & 0 & 0 & 0 & 19 & 19 & 1 \\ 35 & 0 & 0 & 0 & 0 & 13 & 28 & 39 \\ \hline 12 & 0 & 0 & 0 & 0 & 34 & 20 & 0 \\ 0 & 28 & 37 & 34 & 0 & 0 & 0 & 0 \\ 0 & 37 & 35 & 22 & 30 & 0 & 0 & 0 \\ 0 & 34 & 22 & 44 & 39 & 0 & 0 & 0 \end{array} \right)$$

$$p = 53 \quad \det(A4) = 0$$

$$\left(\begin{array}{cccc|cccc} 0 & 3 & 2 & 49 & 46 & 0 & 0 & 0 \\ 14 & 0 & 0 & 0 & 0 & 11 & 11 & 4 \\ 26 & 0 & 0 & 0 & 0 & 27 & 23 & 11 \\ 1 & 0 & 0 & 0 & 0 & 46 & 50 & 7 \\ \hline 52 & 0 & 0 & 0 & 0 & 11 & 14 & 0 \\ 0 & 46 & 32 & 37 & 0 & 0 & 0 & 0 \\ 0 & 32 & 32 & 45 & 48 & 0 & 0 & 0 \\ 0 & 37 & 45 & 14 & 23 & 0 & 0 & 0 \end{array} \right)$$

$$p = 59 \quad \det(A4) = 0$$

$$\left(\begin{array}{cccc|cccc} 0 & 42 & 53 & 6 & 11 & 0 & 0 & 0 \\ 31 & 0 & 0 & 0 & 0 & 9 & 8 & 9 \\ 40 & 0 & 0 & 0 & 0 & 48 & 18 & 11 \\ 19 & 0 & 0 & 0 & 0 & 3 & 13 & 8 \\ \hline 40 & 0 & 0 & 0 & 0 & 6 & 57 & 0 \\ 0 & 57 & 53 & 40 & 0 & 0 & 0 & 0 \\ 0 & 53 & 6 & 28 & 46 & 0 & 0 & 0 \\ 0 & 40 & 28 & 27 & 40 & 0 & 0 & 0 \end{array} \right)$$

$$p = 61 \quad \det(A4) = 19$$

$$\left(\begin{array}{cccc|cccc} 56 & 0 & 0 & 0 & 0 & 3 & 45 & 38 \\ 0 & 48 & 20 & 59 & 41 & 0 & 0 & 0 \\ 0 & 0 & 39 & 7 & 35 & 0 & 0 & 0 \\ 0 & 0 & 53 & 0 & 10 & 0 & 0 & 0 \\ \hline 0 & 0 & 8 & 48 & 51 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 14 & 0 & 0 \\ 8 & 0 & 0 & 0 & 0 & 11 & 51 & 0 \\ 48 & 0 & 0 & 0 & 0 & 5 & 39 & 14 \end{array} \right)$$

$$p = 67 \quad \det(A4) = 9$$

$$\left(\begin{array}{cccc|cccc} 53 & 0 & 0 & 0 & 0 & 42 & 62 & 29 \\ 0 & 46 & 16 & 29 & 14 & 0 & 0 & 0 \\ 0 & 0 & 33 & 56 & 25 & 0 & 0 & 0 \\ 0 & 0 & 8 & 27 & 4 & 0 & 0 & 0 \\ \hline 0 & 0 & 59 & 19 & 63 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 51 & 0 & 0 \\ 59 & 0 & 0 & 0 & 0 & 31 & 63 & 0 \\ 19 & 0 & 0 & 0 & 0 & 52 & 5 & 51 \end{array} \right)$$

$$p = 71 \quad \det(A4) = 0$$

$$\left(\begin{array}{cccc|cccc} 0 & 8 & 59 & 15 & 35 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 0 & 48 & 64 & 63 \\ 1 & 0 & 0 & 0 & 0 & 48 & 51 & 27 \\ 33 & 0 & 0 & 0 & 0 & 29 & 62 & 31 \\ \hline 38 & 0 & 0 & 0 & 0 & 34 & 36 & 0 \\ 0 & 40 & 49 & 2 & 0 & 0 & 0 & 0 \\ 0 & 49 & 10 & 36 & 1 & 0 & 0 & 0 \\ 0 & 2 & 36 & 47 & 6 & 0 & 0 & 0 \end{array} \right)$$

$$p = 73 \quad \det(A4) = 35$$

$$\left(\begin{array}{cccc|cccc} 41 & 0 & 0 & 0 & 0 & 52 & 33 & 60 \\ 0 & 51 & 61 & 1 & 60 & 0 & 0 & 0 \\ 0 & 0 & 20 & 33 & 27 & 0 & 0 & 0 \\ 0 & 0 & 31 & 18 & 71 & 0 & 0 & 0 \\ \hline 0 & 0 & 42 & 33 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 63 & 0 & 0 \\ 42 & 0 & 0 & 0 & 0 & 37 & 2 & 0 \\ 33 & 0 & 0 & 0 & 0 & 3 & 72 & 63 \end{array} \right)$$

$$p = 79 \quad \det(A4) = 51$$

$$\left(\begin{array}{cccc|cccc} 46 & 0 & 0 & 0 & 0 & 37 & 55 & 50 \\ 0 & 53 & 20 & 28 & 61 & 0 & 0 & 0 \\ 0 & 39 & 50 & 70 & 35 & 0 & 0 & 0 \\ 0 & 33 & 68 & 25 & 63 & 0 & 0 & 0 \\ \hline 0 & 0 & 31 & 28 & 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 71 & 26 & 22 \\ 2 & 0 & 0 & 0 & 0 & 57 & 51 & 66 \\ 12 & 0 & 0 & 0 & 0 & 70 & 44 & 71 \end{array} \right)$$

$$p = 83 \quad \det(A4) = 0$$

$$\left(\begin{array}{cccc|cccc} 0 & 5 & 25 & 81 & 80 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 & 70 & 8 & 68 \\ 12 & 0 & 0 & 0 & 0 & 7 & 66 & 72 \\ 1 & 0 & 0 & 0 & 0 & 36 & 55 & 71 \\ \hline 82 & 0 & 0 & 0 & 0 & 32 & 17 & 0 \\ 0 & 7 & 21 & 55 & 0 & 0 & 0 & 0 \\ 0 & 21 & 4 & 60 & 7 & 0 & 0 & 0 \\ 0 & 55 & 60 & 70 & 42 & 0 & 0 & 0 \end{array} \right)$$

$$p = 89 \quad \det(A4) = 0$$

$$\left(\begin{array}{cccc|cccc} 0 & 64 & 75 & 76 & 85 & 0 & 0 & 0 \\ 53 & 0 & 0 & 0 & 0 & 62 & 37 & 41 \\ 15 & 0 & 0 & 0 & 0 & 82 & 24 & 47 \\ 55 & 0 & 0 & 0 & 0 & 65 & 39 & 7 \\ \hline 34 & 0 & 0 & 0 & 0 & 65 & 8 & 0 \\ 0 & 30 & 1 & 21 & 0 & 0 & 0 & 0 \\ 0 & 1 & 35 & 77 & 18 & 0 & 0 & 0 \\ 0 & 21 & 77 & 21 & 19 & 0 & 0 & 0 \end{array} \right)$$

$$p = 97 \quad \det(A4) = 35$$

$$\left(\begin{array}{cccc|cccc} 37 & 0 & 0 & 0 & 0 & 35 & 28 & 48 \\ 0 & 48 & 59 & 0 & 12 & 0 & 0 & 0 \\ 0 & 48 & 47 & 3 & 77 & 0 & 0 & 0 \\ 0 & 89 & 36 & 20 & 51 & 0 & 0 & 0 \\ \hline 0 & 0 & 37 & 28 & 46 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 54 & 35 & 75 \\ 34 & 0 & 0 & 0 & 0 & 85 & 66 & 31 \\ 10 & 0 & 0 & 0 & 0 & 70 & 24 & 54 \end{array} \right)$$

A.3.1 Courbe $y^4 = (t-1)(t-2)(t-3)(t-4)(t-5)(t-6)(t-7)$, $p = 13$

$$\left(\begin{array}{cccccccc|cccccccc} 10 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 8 & 1 & 8 & 6 \\ 0 & 4 & 9 & 6 & 0 & 0 & 0 & 0 & 0 & 6 & 8 & 10 & 0 & 0 & 0 & 0 \\ 0 & 10 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 0 & 8 & 0 & 0 & 0 \\ 0 & 1 & 8 & 8 & 0 & 0 & 0 & 0 & 0 & 0 & 8 & 9 & 10 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 9 & 5 & 6 & 2 & 12 & 6 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 11 & 3 & 9 & 6 & 12 & 7 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 & 1 & 2 & 0 & 12 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 6 & 12 & 0 & 8 & 2 & 11 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 8 & 10 & 6 & 7 & 10 & 5 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 5 & 7 & 0 & 10 & 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 9 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 9 & 11 & 10 & 0 & 0 & 0 \\ 0 & 5 & 4 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 4 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 12 & 1 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 10 & 7 & 7 \\ 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 10 & 8 & 10 \\ 10 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & 10 & 1 \\ 11 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 11 & 1 & 7 \\ 5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & 1 & 4 \end{array} \right)$$

A.4 Application de l'algorithme de décomposition de Jordan-Hölder

A.4.1 Exemple explicite

On prend les exemples de la courbe $y^3 = (t-1)(t-2)(t-3)(t-4)(t-5)$ avec $p = 7$ et $p = 11$.

$$p = 7$$

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 4 & 3 & 4 \\ 0 & 5 & 3 & 4 & 5 & 0 & 0 & 0 \\ 0 & 5 & 1 & 5 & 1 & 0 & 0 & 0 \\ 0 & 5 & 5 & 1 & 2 & 0 & 0 & 0 \\ \hline 0 & 0 & 3 & 4 & 5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 1 & 1 \\ 6 & 0 & 0 & 0 & 0 & 0 & 6 & 3 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{array} \right)$$

La matrice donnée est M_ϕ , $m_0 = n_0 = 4$, $E_0 = \langle e_1, e_2, e_3, e_4 \rangle$ et $F_0 = \langle e_5, e_6, e_7, e_8 \rangle$.

Tout d'abord m_0 et n_0 sont non nuls, on passe donc à la recherche de J minimal. Afin de réaliser quelque chose de systématique, on prend toujours $x = e_1$ pour faire tourner l'algorithme. Pour mémoire la matrice du Frobenius a été obtenue sur $k = \mathbb{F}_p$.

On fait tourner l'algorithme décrit au paragraphe 9.3 et on obtient la matrice A

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 6 & 4 \\ 0 & 1 & 3 \end{pmatrix}$$

qui est donc donnée par $(x, \phi_{gr}(x), \phi_{gr}^2(x))$. L'espace des solutions de $AY = 0$ et de dimension 1 sur le corps fini à 7 éléments. Il est engendré par $(1, 2, 4)$. On a donc $x + 2\phi_{gr}(x) + 4\phi_{gr}^2(x) = 0$. Comme $x \in Fil^1$ et $\phi_{gr}(x), \phi_{gr}^2(x) \notin Fil^1$ il faut donc appliquer ϕ_{gr} à la relation. En posant $x' = \phi_{gr}(x)$ on obtient alors $2\phi_{gr}(x') + 4\phi_{gr}^2(x') = 0$. Cette fois les deux termes sont dans le même cran de la filtration. Enfin comme on souhaite que 0 soit dans J on pose $x'' = \phi_{gr}(x')$ et on obtient finalement la relation $2x'' + 4\phi_{gr}(x'') = 0$. L'espace J recherché est $\{0, 1\}$ et donc $h = 0 \wedge 1 = 1$, $m_J = 1$, $h' = 1$ et on a $N = \langle x'' \rangle$.

Ainsi il existe $y \in N$ non nul tel que $\phi_{gr}(y) = \lambda y$ pour un certain λ . Bien évidemment $y = x'' = e_1 + 4e_7 + 3e_8$ convient et on a $\phi_{gr}(y) = 3y$. On a donc un sous-espace stable, $S = \langle y \rangle$, qui est simple de type (0).

Une base de E_0 adaptée au quotient par S est (e_1, e_2, e_3, e_4) et une base de F_0 adaptée au quotient par S est (e_5, e_6, y, e_8) . On a donc $E_1 = E_0$, $F_1 = \langle e_5, e_6, e_8 \rangle$, $m_1 = 4$ et $n_1 = 3$. Reste enfin à obtenir M_ϕ^1 . Pour cela on commence par obtenir C , la matrice de changement de base, \bar{C} , la matrice par passage au gradué, et C^{-1} .

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & 1 \end{pmatrix} \quad C^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 5 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Ici \bar{C} est tout simplement obtenue en mettant à zéro la composante (1, 7). On applique donc la formule de changement de base pour l'application semi-linéaire donnée au paragraphe 9.5 et la

A.4. APPLICATION DE L'ALGORITHME DE DÉCOMPOSITION DE JORDAN-HÖLDER

matrice de ϕ dans la base adaptée au quotient par S est donc

$$\begin{pmatrix} 3 & 0 & 0 & 0 & 0 & 4 & 0 & 5 \\ 0 & 5 & 3 & 4 & 5 & 0 & 0 & 0 \\ 0 & 5 & 1 & 5 & 1 & 0 & 0 & 0 \\ 0 & 5 & 5 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 3 & 4 & 5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 0 & 1 \\ 5 & 0 & 0 & 0 & 0 & 0 & 3 & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 \end{pmatrix}$$

d'où finalement

$$M_\phi^1 = \begin{pmatrix} 3 & 0 & 0 & 0 & 0 & 4 & 5 \\ 0 & 5 & 3 & 4 & 5 & 0 & 0 \\ 0 & 5 & 1 & 5 & 1 & 0 & 0 \\ 0 & 5 & 5 & 1 & 2 & 0 & 0 \\ 0 & 0 & 3 & 4 & 5 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 6 \end{pmatrix}$$

matrice obtenue après passage au quotient.

Dans cet exemple, les itérations successives vont donner à chaque fois un sous-espace stable de dimension 1, il n'est donc pas intéressant de détailler tous les calculs ici. Par ailleurs à l'issue de la sixième itération, la liste obtenue est $(0, 1, 1, 0, 1, 1)$ et on a les valeurs $m_6 = 0$ et $n_6 = 2$. Cela signifie donc que tous les éléments sont dans le même cran de la filtration. Il n'est donc pas utile de faire d'itérations supplémentaires pour compléter la liste car il ne peut pas y avoir de sous-espace stable de dimension supérieure à 1. Ainsi la liste des quotients successifs obtenue dans le cas $p = 7$ est $(0, 1, 1, 0, 1, 1, 0, 0)$.

$$p = 11$$

$$\left(\begin{array}{cccc|cccc} 0 & 7 & 4 & 3 & 9 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 7 & 0 & 0 & 0 & 0 & 5 & 8 & 6 \\ 8 & 0 & 0 & 0 & 0 & 9 & 7 & 10 \\ \hline 3 & 0 & 0 & 0 & 0 & 3 & 10 & 0 \\ 0 & 4 & 1 & 10 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 7 & 8 & 0 & 0 & 0 \\ 0 & 10 & 7 & 9 & 4 & 0 & 0 & 0 \end{array} \right)$$

La matrice donnée est M_ϕ , $m_0 = n_0 = 4$, $E_0 = \langle e_1, e_2, e_3, e_4 \rangle$ et $F_0 = \langle e_5, e_6, e_7, e_8 \rangle$.

Tout d'abord m_0 et n_0 sont non nuls, on passe donc à la recherche de J minimal. Afin de réaliser quelque chose de systématique, on prend toujours $x = e_1$ pour faire tourner l'algorithme. Pour

mémoire la matrice du Frobenius a été obtenue sur $k = \mathbb{F}_p$.

On fait tourner l'algorithme décrit au paragraphe 9.3 et on obtient la matrice A

$$\begin{pmatrix} 1 & 0 & 5 & 0 & 4 \\ 0 & 5 & 0 & 1 & 0 \\ 0 & 7 & 0 & 0 & 0 \\ 0 & 8 & 0 & 2 & 0 \\ 0 & 3 & 0 & 9 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 6 \\ 0 & 0 & 1 & 0 & 3 \end{pmatrix}$$

qui est donnée par $(x, \phi_{gr}(x), \phi_{gr}^2(x), \phi_{gr}^3(x), \phi_{gr}^4(x))$. L'espace des solutions de $AY = 0$ est de dimension 1 sur le corps fini à 11 éléments. Il est engendré par $(0, 0, 1, 0, 7)$ et on a donc la relation $\phi_{gr}^2(x) + 7\phi_{gr}^4(x) = 0$. Comme $\phi_{gr}^2(x), \phi_{gr}^4(x) \notin Fil^1$ il n'est pas nécessaire d'appliquer à nouveau ϕ_{gr} à cette relation. Cependant on souhaite que 0 soit dans J posons $x' = \phi_{gr}^2(x)$. Alors on a la relation $x' + 7\phi_{gr}^2(x') = 0$. D'où $J = \{0, 2\}$ et donc $h = 0 \wedge 2 = 2$, $m_J = 2$, $h' = 1$ et on a $N = \langle x' \rangle$.

Il existe $y \in N$ non nul tel que $\phi_{gr}^2(y) = \lambda y$ pour un certain λ . Clairement $y = x' = 5e_1 + 2e_7 + e_8$ convient et vérifie $\phi_{gr}^2(y) = 3y$. Un sous-espace stable est donc $\langle y, \phi_{gr}(y) \rangle$. Cependant le 2-uplet associé à cet espace est $(0, 0)$ qui est 1-périodique donc $\exists u \in \langle y, \phi_{gr}(y) \rangle$ non nul tel que $\phi_{gr}(u) = \lambda u$ pour un certain λ .

On sait que u est de la forme $5ae_1 + be_2 + 2be_4 + 9be_5 + 2ae_7 + ae_8$ et donc $u \in F_0$ donc

$$\phi_{gr}(u) = 9b^p\phi(e_5) + 2a^p\phi(e_7) + a^p\phi(e_8) = 4b^pe_1 + a^pe_2 + 2a^pe_4 + 9a^pe_5 + 6b^pe_7 + 3b^pe_8$$

ce qui donne le système d'équations

$$\begin{cases} 4b^p = 5\lambda a \\ a^p = \lambda b \\ 2a^p = 2\lambda b \\ 9a^p = 9\lambda b \\ 6b^p = 2\lambda a \\ 3b^p = \lambda a \end{cases}$$

qui est en fait un système à deux équations puisque les deuxième, troisième et quatrième et les première, cinquième et sixième sont égales modulo $p = 11$.

Il se trouve que ce système admet des solutions sur \mathbb{F}_p qui sont $\lambda = 5$, $b = 1$ et $a = 5$. On a donc $u = 3e_1 + e_2 + 2e_4 + 9e_5 + 10e_7 + 5e_8 \in F_0$ et $\phi_{gr}(u) = 5u$. On a donc un sous-espace stable $S = \langle u \rangle$, qui est simple de type (0).

Une base de E_0 adaptée au quotient par S est (e_1, e_2, e_3, e_4) et une base de F_0 adaptée au quotient par S est (u, e_6, e_7, e_8) . On a donc $E_1 = E_0$, $F_1 = \langle e_6, e_7, e_8 \rangle$, $m_1 = 4$ et $n_1 = 3$. Reste enfin à

A.4. APPLICATION DE L'ALGORITHME DE DÉCOMPOSITION DE JORDAN-HÖLDER

obtenir M_ϕ^1 . La matrice de ϕ dans la nouvelle base est

$$\begin{pmatrix} 10 & 7 & 4 & 3 & 0 & 10 & 4 & 0 \\ 1 & 0 & 0 & 0 & 0 & 7 & 5 & 1 \\ 7 & 0 & 0 & 0 & 0 & 5 & 8 & 6 \\ 0 & 0 & 0 & 0 & 0 & 1 & 6 & 10 \\ 4 & 0 & 0 & 0 & 5 & 4 & 6 & 0 \\ 0 & 4 & 1 & 10 & 0 & 0 & 0 & 0 \\ 4 & 1 & 1 & 7 & 0 & 4 & 6 & 0 \\ 2 & 10 & 7 & 9 & 0 & 2 & 3 & 0 \end{pmatrix}$$

d'où finalement

$$M_\phi^1 = \begin{pmatrix} 10 & 7 & 4 & 3 & 10 & 4 & 0 \\ 1 & 0 & 0 & 0 & 7 & 5 & 1 \\ 7 & 0 & 0 & 0 & 5 & 8 & 6 \\ 0 & 0 & 0 & 0 & 1 & 6 & 10 \\ 0 & 4 & 1 & 10 & 0 & 0 & 0 \\ 4 & 1 & 1 & 7 & 4 & 6 & 0 \\ 2 & 10 & 7 & 9 & 2 & 3 & 0 \end{pmatrix}$$

matrice obtenue après passage au quotient.

Après la troisième itération, la liste est $(0,0,1)$, on a $m_3 = 3$, $n_3 = 2$, $E_3 = \langle e_2, e_3, e_4 \rangle$, $F_3 = \langle e_6, e_8 \rangle$ et

$$M_\phi^3 = \begin{pmatrix} 6 & 2 & 10 & 7 & 1 \\ 9 & 3 & 4 & 5 & 6 \\ 0 & 0 & 0 & 1 & 10 \\ 4 & 1 & 10 & 0 & 0 \\ 4 & 1 & 0 & 0 & 0 \end{pmatrix}$$

On fait tourner l'algorithme décrit au paragraphe 9.3 et on obtient la matrice A

$$\begin{pmatrix} 1 & 6 & 10 \\ 0 & 9 & 0 \\ 0 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 4 & 0 \end{pmatrix}$$

qui est donnée par $(x, \phi_{gr}(x), \phi_{gr}^2(x))$. L'espace des solutions de $AY = 0$ est de dimension 1 sur le corps fini à 11 éléments. Il est engendré par $(1,0,1)$. On a donc $x + \phi_{gr}^2(x) = 0$. Ces deux éléments sont dans Fil^1 et 0 est bien dans J d'où $J = \{0,2\}$ et donc $h = 0 \wedge 2 = 2$, $m_J = 2$, $h' = 1$ et donc $N = \langle x \rangle$.

Ainsi il existe $y \in N$ non nul tel que $\phi_{gr}^2(y) = \lambda y$ pour un certain λ . Ici clairement $y = x$ convient puisque $\phi_{gr}^2(x) = 10x$. Un sous-espace stable est donc $\langle y, \phi_{gr}(y) \rangle$. Le 2-uplet associé à cet espace est $(1,0)$ qui n'est pas périodique donc $\langle y, \phi_{gr}(y) \rangle$ est simple.

Une base de E_3 adaptée au quotient par S est (y, e_3, e_4) et une base de F_3 adaptée au quotient

par S est $(\phi_{gr}(y), e_8)$. On a donc $E_4 = \langle e_3, e_4 \rangle$, $F_4 = \langle e_8 \rangle$, $m_4 = 2$ et $n_4 = 1$. Enfin

$$M_\phi^4 = \begin{pmatrix} 9 & 9 & 6 \\ 0 & 0 & 10 \\ 0 & 1 & 0 \end{pmatrix}$$

et la liste est donc $(0, 0, 1, (0, 1))$.

On a $\phi_{gr}(e_3) = 9e_3$ donc $\langle e_3 \rangle$ est un sous-espace stable. Ainsi $E_5 = \langle e_4 \rangle$, $F_5 = F_4 = \langle e_8 \rangle$, $m_5 = 1$, $n_5 = n_4 = 1$ de plus

$$M_\phi^5 = \begin{pmatrix} 0 & 10 \\ 1 & 0 \end{pmatrix}$$

et la liste est $(0, 0, 1, (0, 1), 1)$.

On fait tourner l'algorithme décrit au paragraphe 9.3 et on obtient la matrice A

$$\begin{pmatrix} 1 & 0 & 10 \\ 0 & 1 & 0 \end{pmatrix}$$

qui est donc donnée par $(x, \phi_{gr}(x), \phi_{gr}^2(x))$. L'espace des solutions de $AY = 0$ est de dimension 1 sur le corps fini à 11 éléments. Il est généré par $(1, 0, 1)$. On a donc $x + \phi_{gr}^2(x) = 0$. On a $J = \{0, 2\}$ et donc $h = 0 \wedge 2 = 2$, $m_J = 2$, $h' = 1$ et on a $N = \langle x \rangle$.

Ainsi il existe $y \in N$ non nul tel que $\phi_{gr}^2(y) = \lambda y$ pour un certain λ . Ici clairement $y = x$ convient puisque $\phi_{gr}^2(x) = 10x$. Un sous-espace stable est donc $\langle y, \phi_{gr}(y) \rangle$. Le 2-uplet associé à cet espace est $(1, 0)$ qui n'est pas périodique donc $\langle y, \phi_{gr}(y) \rangle$ est simple.

On va avoir $m_6 = n_6 = 0$ donc l'algorithme est terminé.

La liste des quotient successifs est $(0, 0, 1, (0, 1), 1, (0, 1))$.

A.4.2 Décomposition pour les exemples matriciels précédents

En ce qui concerne les courbes hyperelliptiques dont les matrices sont données dans la section A.1, dans les 6 cas, la liste est $(0, 0, 1, 1)$.

En ce qui concerne les revêtements de degré 3 dont les matrices sont données dans la section A.3 l'algorithme proposé dans le chapitre 9 donne en sortie la liste

- $(0, 1, 1, 0, 1, 1, 0, 0)$ pour $p \in \{7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97\}$
- $(0, 0, 1, (0, 1), 1, (0, 1))$ pour $p \in \{11, 17, 23, 29, 47, 53, 59, 71, 83, 89\}$
- $((0, 1), (0, 1), (0, 1), (0, 1))$ pour $p = 41$.

Notons que dans le premier cas $n \mid p - 1$ et le déterminant de la matrice de Hasse-Witt est non nul, dans le second cas $n \nmid p - 1$ et le déterminant de la matrice de Hasse-Witt est nul. Enfin dans le dernier cas on est dans les mêmes conditions que dans le second cas mais de plus la matrice de Hasse-Witt est nulle.

Annexe B

Invariant de Hasse des courbes elliptiques

Au début de la section 7.2 on a fait l'hypothèse que 0 n'était pas racine du polynôme f afin d'avoir un relèvement explicite du Frobenius modulo p^2 sur l'ouvert \overline{U}_1 . Cependant lorsque l'on calcule explicitement le morphisme de Deligne et Illusie au paragraphe 7.3, en ce qui concerne DI_0 (voir la proposition 7.3.1) on remarque que le Frobenius divisé n'intervient pas. En fait on peut calculer le bloc inférieur droit de la matrice (qui correspond à la matrice de Hasse-Witt de la courbe) sans connaître de relèvement explicite du Frobenius. On va donc donner ici l'invariant de Hasse d'une courbe elliptique en fonction d'un paramètre λ . On considère le cas $f(t) = t(t-1)(t-\lambda)$.

Proposition B.0.1. *L'invariant de Hasse de la courbe X définie à l'aide de $f(t)$ est donné par la formule :*

$$H \equiv (-1)^{f_p} \sum_{k=0}^{f_p} \binom{f_p}{k}^2 \lambda^k$$

$$\text{où } f_p = \frac{p-1}{2}.$$

Preuve: On sait qu'une base de $H^1(X_k, \mathcal{O}_{X_k})$ est $\overline{t^{-1}y}$ (voir proposition 6.0.5). Il s'agit donc de calculer $Q(DI_0(t^{-1}y))$. Or $DI_0(t^{-1}y) = t^{-p}y^p = t^{-p}f(t)^{f_p}y$ puisque $y^2 = f(t)$ et que p est impair.

En ce qui concerne Q on sait que tout monôme du type $t^\alpha y$ est envoyé sur 0 sauf pour $\alpha = -1$ où il est envoyé sur lui-même. Pour connaître l'invariant de Hasse associé à X_k il s'agit donc d'identifier le monôme en t de degré $p-1$ dans $f(t)^{f_p}$.

$$\begin{aligned}
f(t)^{f_p} &= (t(t-1))^{f_p} (t-\lambda)^{f_p} = t^{f_p} \left(\sum_{l=0}^{f_p} \binom{f_p}{l} (-1)^{f_p-l} t^l \right) \left(\sum_{k=0}^{f_p} \binom{f_p}{k} (-1)^k \lambda^k t^{f_p-k} \right) \\
&= \sum_{l=0}^{f_p} \sum_{k=0}^{f_p} \binom{f_p}{l} \binom{f_p}{k} (-1)^{f_p+k-l} \lambda^k t^{p-1+l-k}
\end{aligned}$$

Le monôme de degré $p-1$ est donc donné par tout élément tel que $l-k=0$ i.e $k=l$. D'où finalement la formule annoncée. □

Remarque B.0.1. On connaissait déjà l'invariant de Hasse d'une courbe elliptique à un inversible près (voir par exemple IV.4, corollaire 4.22 [Har77]). Ici on a une petite information supplémentaire qui est donc cet inversible qui vaut $(-1)^{\frac{p-1}{2}}$.

Annexe C

Formulaire et index de notations

C.1 Formulaire

Dans ce document les relations suivantes sont vérifiées :

$$\begin{aligned}y^n &= f(t) \\z^n &= f_2(s) \\r &= \frac{l+1}{n} \\t &= s^{-1} \\z &= s^r y \\f_2(s) &= f(t)s^{rn}\end{aligned}$$

C.2 Notations

Dans ce document on a les notations suivantes :

$$\begin{aligned}U &= \text{Spec}(V[t, y]/(y^n - f(t))) \\ \bar{U} &= U \cap D(y) \\ W &= \text{Spec}(V[s, z]/(z^n - f_2(s))) \\ X &= U \cup W = \bar{U} \cup W \\ X_k &= X \times_{\text{Spec}(V)} \text{Spec}(V/pV) \\ \bar{U}_k &= \bar{U} \times_{\text{Spec}(V)} \text{Spec}(V/pV) \\ W_k &= W \times_{\text{Spec}(V)} \text{Spec}(V/pV) \\ X_1 &= X \times_{\text{Spec}(V)} \text{Spec}(V/p^2V) \\ \bar{U}_1 &= \bar{U} \times_{\text{Spec}(V)} \text{Spec}(V/p^2V) \\ W_1 &= W \times_{\text{Spec}(V)} \text{Spec}(V/p^2V)\end{aligned}$$

Bibliographie

- [BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990.
- [BO78] Pierre Berthelot and Arthur Ogus. *Notes on crystalline cohomology*. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1978.
- [Bor03] Niels Borne. Une formule de Riemann-Roch équivariante pour les courbes. *Canad. J. Math.*, 55(4) :693–710, 2003.
- [Car57] Pierre Cartier. Une nouvelle opération sur les formes différentielles. *C. R. Acad. Sci. Paris*, 244 :426–428, 1957.
- [DI87] Pierre Deligne and Luc Illusie. Relèvements modulo p^2 et décomposition du complexe de de Rham. *Invent. Math.*, 89(2) :247–270, 1987.
- [dJN91] Johan de Jong and Rutger Noot. Jacobians with complex multiplication. 89 :177–192, 1991.
- [dJR11] Robin de Jong and Gaël Rémond. Conjecture de Shafarevitch effective pour les revêtements cycliques. *Algebra Number Theory*, 5(8) :1133–1143, 2011.
- [Elk11] Arsen Elkin. The rank of the Cartier operator on cyclic covers of the projective line. *J. Algebra*, 327 :1–12, 2011.
- [FL82] Jean-Marc Fontaine and Guy Laffaille. Construction de représentations p -adiques. *Ann. Sci. École Norm. Sup. (4)*, 15(4) :547–608 (1983), 1982.
- [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.
- [GG01] Pierrick Gaudry and Nicolas Gürel. An extension of Kedlaya’s point-counting algorithm to superelliptic curves. In *Advances in cryptology—ASIACRYPT 2001 (Gold Coast)*, volume 2248 of *Lecture Notes in Comput. Sci.*, pages 480–494. Springer, Berlin, 2001.
- [Gon97] Josep González. Hasse-Witt matrices for the Fermat curves of prime degree. *Tohoku Math. J. (2)*, 49(2) :149–163, 1997.
- [Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

-
- [Has35] Helmut Hasse. Existenz separabler zyklischer unverzweigter erweiterungskörper vom primzahlgrade p über elliptischen funktionenkörpern der charakteristik p . *Journal für die reine und angewandte Mathematik*, 172 :77–85, 1935.
- [HS14] David Harvey and Andrew V. Sutherland. Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time. *LMS J. Comput. Math.*, 17(suppl. A) :257–273, 2014.
- [HW15] Christine Huyghe and Nathalie Wach. Représentations galoisiennes associées aux courbes hyperelliptiques lisses. *Q. J. Math.*, 66(1) :171–189, 2015.
- [HW16] Christine Huyghe and Nathalie Wach. Interprétation cristalline du morphisme de Deligne-Illusie. *Soumis pour publication*, 2016.
- [Ill96] Luc Illusie. Frobenius et dégénérescence de Hodge. In *Introduction à la théorie de Hodge*, volume 3 of *Panor. Synthèses*, pages 113–168. Soc. Math. France, Paris, 1996.
- [Jac43] Nathan Jacobson. *The Theory of Rings*. American Mathematical Society Mathematical Surveys, vol. II. American Mathematical Society, New York, 1943.
- [Jac85] Nathan Jacobson. *Basic algebra. I*. W. H. Freeman and Company, New York, second edition, 1985.
- [Kat70] Nicholas M. Katz. Nilpotent connections and the monodromy theorem : Applications of a result of Turrittin. *Inst. Hautes Études Sci. Publ. Math.*, (39) :175–232, 1970.
- [Ked01] Kiran S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16(4) :323–338, 2001.
- [Koo91] Ja Kyung Koo. On holomorphic differentials of some algebraic function field of one variable over \mathbf{C} . *Bull. Austral. Math. Soc.*, 43(3) :399–405, 1991.
- [Laf74] Jean-Pierre Lafon. *Les formalismes fondamentaux de l’algèbre commutative*. Hermann, Paris, 1974. Collection Enseignement des Sciences, No. 20.
- [Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.
- [Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Ern e, Oxford Science Publications.
- [Maz73a] B. Mazur. Frobenius and the Hodge filtration (estimates). *Ann. of Math. (2)*, 98 :58–95, 1973.
- [Maz73b] B. Mazur. Frobenius and the Hodge filtration (estimates). *Ann. of Math. (2)*, 98 :58–95, 1973.
- [Mir95] Rick Miranda. *Algebraic curves and Riemann surfaces*, volume 5 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1995.
- [Ser68] Jean-Pierre Serre. *Corps locaux*. Hermann, Paris, 1968. Deuxi me  dition, Publications de l’Universit  de Nancago, No. VIII.
- [Ser71] Jean-Pierre Serre. *Repr sentations lin aires des groupes finis*. Hermann, Paris, 1971. Deuxi me  dition, refondue.

BIBLIOGRAPHIE

- [Sza09] Tamás Szamuely. *Galois groups and fundamental groups*, volume 117 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2009.
- [Tui16] Jan Tuitman. Counting points on curves using a map to \mathbf{P}^1 . *Math. Comp.*, 85(298) :961–981, 2016.
- [Tui17] Jan Tuitman. Counting points on curves using a map to \mathbf{P}^1 , II. *Finite Fields Appl.*, 45 :301–322, 2017.
- [Wac97] Nathalie Wach. Représentations cristallines de torsion. *Compositio Math.*, 108(2) :185–240, 1997.

Dans cette thèse, on considère des revêtements séparables à deux ouverts de la droite projective sur un corps fini k de caractéristique $p > 0$ et on donne un calcul explicite de la matrice du Frobenius divisé sur le premier espace de cohomologie de de Rham de X_k , fibre spéciale du revêtement X étudié. On fournit également un procédé algorithmique permettant d'obtenir la décomposition de Jordan-Hölder du φ -module filtré associé à cette matrice.

Dans un premier temps on motive le choix de la famille de revêtements considérés et après une étude rapide de la lissité, du genre et de la ramification on donne le calcul d'une base des espaces de cohomologie $H^0(X, \Omega_X)$, $H^1(X, \mathcal{O}_X)$ et $H^1_{DR}(X)$.

Dans un second temps on calcule le Frobenius divisé modulo p en utilisant un résultat récent de Huyghe-Wach comparant cette application de Frobenius divisé sur $H^1_{DR}(X'_k)$ avec le morphisme construit par Deligne et Illusie en 1987, où X'_k est obtenue après changement de base par le Frobenius sur k . Afin de mener à bien ce calcul, il sera alors nécessaire de calculer un relèvement du Frobenius modulo p^2 sur chacun des ouverts permettant de définir X'_k . Puis grâce au calcul explicite d'un scindage de $H^1(X, \mathcal{O}_X)$ vers le premier espace de cohomologie de de Rham on donne des formules explicites pour la matrice du Frobenius divisé sur $H^1_{DR}(X_k)$.

Pour finir à l'aide de résultats dus à Wach et à Fontaine-Lafaille on calcule la décomposition de Jordan-Hölder du φ -module associé à cette matrice. Ce procédé algorithmique est illustré sur quelques exemples explicites.



UNIVERSITÉ DE STRASBOURG



ISSN 0755-3390

INSTITUT DE RECHERCHE MATHÉMATIQUE AVANCÉE
UMR 7501
Université de Strasbourg et CNRS
7 Rue René Descartes
67 084 STRASBOURG CEDEX

Tél. 03 68 85 01 29
 Fax 03 68 85 03 28

www-irma.u-strasbg.fr
irma@math.unistra.fr

IRMA 2017/010
<https://tel.archives-ouvertes.fr/tel-01655254>