Comptage des points d'une courbe hyperelliptique par des méthodes p-adiques, d'après Kedlaya

Amandine Pierrot, dirigée par Christine Huyghe

UFR de mathématiques et d'informatique de Strasbourg, master de mathématiques fondamentales 2013-2014

Table des matières

1 Introduction

L'objet de ce mémoire est de donner l'algorithme de Kedlaya, qui en un temps $O(g^{4+\epsilon}n^{3+\epsilon})$ et avec un espace de stockage $O(g^3n^3)$ permet de calculer le nombre de points d'une courbe hyperelliptique donnée à coordonnées dans un certain corps $\mathbb{F}_{q^m}$. Ce qui suit s'inspire très largement de l'article de Bas Edixhoven intitulé "Point counting after Kedlaya, EIDMA-Stieltjes Graduate course, Leiden" [1]. Le développement de l'algorithme va nécessiter le calcul de la cohomologie de Monsky-Washnitzer sur un certain anneau puis de l'action du Frobenius sur la cohomologie précédemment calculée. Tout cela sera développé plus en détail dans les sections 4 et 5 mais nous allons donner ici la motivation ainsi que l'explication de la légitimité de ce qui sera fait ultérieurement.

On considère V un anneau de valuation discrète complet. Cela signifie que V est muni d'une valuation v i.e d'une application $v : V \to \mathbb{R}$ vérifiant $v(xy) = v(x) + v(y)$, $v(x + y) \geq min(v(x), v(y))$ et $v(x) = \infty \Leftrightarrow x = 0$. De plus $Im(v) \subset \mathbb{R}$ est discret et V est complet pour la norme définie par v. On considère aussi $K = Frac(V)$ de caractéristique nulle, k un corps fini de caractéristique p et X_0 un schéma lisse sur k. On suppose qu'il existe F relèvement de Frobenius sur V. On peut prendre par exemple $k = \mathbb{F}_q$ et $V = \mathbb{Z}_q$.
Dans les années 90, Berthelot a construit une théorie de cohomologie, appelée cohomologie rigide, $H^*_{rig}(X_0)$ et $H^*_{rig,c}(X_0)$, c signifiant compacte. Les coefficients sont des K-espaces-vectoriels de dimension finie, i.e. à coefficients p-adiques. Cette théorie cohomologique développée par Berthelot possède les propriétés d'une cohomologie de Weil, ce qui donne en particulier la fonctorialité. Cette fonctorialité est essentielle dans la suite car c'est cela qui assurera que l'on a bien une action du Frobenius, en utilisant les théorèmes de Berthelot énoncés dans ce qui suit.

Théorème. 1.1. *Berthelot*
Supposons que $X_0 = Spec(A_0)$ avec $A_0 = k \otimes_V A^\dagger$ où $A^\dagger$ est une V-algèbre faiblement complète lisse. Dans ce cas, on dispose de la cohomologie de Monsky-Washnitzer et alors :

$$H^*_{MW}(X_0) \simeq H^*_{rig}(X_0)$$

cet isomorphisme étant canonique.

Théorème. 1.2. *Théorème de comparaison*
Si $X_0 = Spec(A_0)$ et si il existe A une V-algèbre lisse de type fini telle que $k \otimes_V A = A_0$ alors

$$H^*_{rig}(X_0) \simeq H^*_{DR}(X)$$

où $X = Spec(A)$.

Ce deuxième théorème est nécessaire car on ne sait pas calculer directement l'action de F sur la cohomologie de de Rham. En effet, on n'a généralement pas d'action de F sur X. C'est une conséquence du théorème d'Hurwitz énoncé plus loin. Par contre, le théorème de Monsky-Washnitzer assure l'existence d'un relèvement de F sur une algèbre faiblement complète. On a un morphisme de complexes :

$$\begin{array}{lccccccccc} C^\bullet : 0 & \to & A & \to & \Omega^1_A & ... & \to & \Omega^n_A & \to & ... \\ & & \downarrow & & \downarrow & & & \downarrow & & \\ D^\bullet : 0 & \to & A^\dagger & \to & \Omega^1_{A^\dagger} & ... & \to & \Omega^n_{A^\dagger} & \to & ... \end{array}$$

Ce morphisme induit $H^*(C^\bullet) \to H^*(D^\bullet)$ qui est un isomorphisme par le théorème de comparaison. L'action de F se lit alors uniquement sur $D^\bullet$.

Une fois la cohomologie et l'action du Frobenius calculées, on est alors à même de calculer le nombre de points de notre courbe à coordonnées dans le corps considéré en utilisant l'algorithme de Kedlaya qui sera détaillé dans la section 6. Cependant avant de développer ces trois points on commencera par une étude rapide de la courbe et on énoncera une conjecture de Weil sur la fonction zêta d'un schéma de type fini sur un corps fini.

2 Etude de la courbe

2.1 Description du problème

Soit $p \neq 2$ un nombre premier et soit $q = p^n$ avec n entier supérieur ou égal à 1. Soit $f \in \mathbb{F}_q[x]$ polynôme unitaire de degré impair $d = 2g + 1$. On suppose f sans racines multiples, f et f' sont donc premiers entre eux.
On souhaite étudier la courbe du plan affine sur $\mathbb{F}_q$ définie par l'équation

$$y^2 = f.$$

On la notera C_f.

2.2 Lissité

Remarque. 2.2.1. *Pour montrer la lissité à l'infini on utilise un résultat général, disponible dans Liu [2]. On énonce ici le cas particulier utilisé pour montrer la lissité à l'infini. Le résultat est donné sans démonstration.*

Proposition. 2.2.2. *Soit X une courbe hyperelliptique de genre g sur un corps k, $g : X \to \mathbb{P}^1_k$ morphisme séparable. On note s et t les coordonnées sur $\mathbb{P}^1_k$. Alors :*
(a) On a $K(X) = k(t)[y]$ avec la relation $y^2 = f(t)$.
(b) La courbe X est réunion de deux schémas affines ouverts

$$U' = Spec(k[t, y]/(y^2 - f(t))) \qquad V' = Spec(k[s, z]/(z^2 - f_1(t)))$$

où $f_1(s) = f(1/s)s^{2g+2}$ avec $t = 1/s$ et $y = t^{g+1}z$.
(c) g est ramifiée au point $s = 0 \in V'$.

Pour étudier la lissité de la courbe au point à l'infini, on se place sur l'ouvert V'.
Sur V' la courbe est définie par l'équation $z^2 = P_1(s)$ où $P_1(s) = f(1/s)s^{2g+2}$.
Le polynôme f étant unitaire de degré $d = 2g + 1$, on a

$$P_1(s) = s + s^2 f_{2g} + ... + s^{2g+1} f_1 + s^{2g+2} f_0.$$

Alors le Jacobien est donné par

$$J_{(z,s)} = \begin{pmatrix} 2z & -P_1'(s) \end{pmatrix}.$$

On cherche maintenant à contrôler la lissité au point à l'infini c'est-à-dire en $s = 0$. Or en $s = 0$ le polynôme $P_1'(s)$ vaut 1. On a donc $J_{(z,0)} = \begin{pmatrix} 2z & -1 \end{pmatrix}$ or il est clair que cette matrice est de rang maximal. La courbe est donc lisse en l'infini.

Proposition. 2.2.3. *La courbe affine C_f est lisse.*

Preuve. On commence par calculer la matrice Jacobienne. Elle est donnée par

$$J_{(y,t)} = \begin{pmatrix} 2y & -f'(t) \end{pmatrix}.$$

On cherche $V(J) \cap C_f$. On souhaite monter que cet ensemble est vide. Il est clair que $V(J)$ est donné par $2y = 0$ et $-f'(t) = 0$, ou encore $y = 0$ et $f'(t) = 0$.
Notons $A = k[t, y]/(y^2 - f(t))$ et posons $M = A/(2yA - f'(t)A)$. Montrer le résultat voulu revient à montrer que $M = 0$, soit $2yA - f'(t)A = A$.
Il est clair que $2yA - f'(t)A \subset A$, il suffit donc de montrer la seconde inclusion, c'est-à-dire que $1_A \in 2yA - f'(t)A$.
Comme A est un anneau local, on considère $Q \in Spec(A)$ l'unique idéal maximal et on va montrer que $1 \in 2yA_Q - f'(t)A_Q$, ce qui donnera le résultat voulu.
Si $b^2 = f(a)$, $Q = (t - a)A_Q + (y - b)A_Q$. Alors $1 \in 2yA_Q - f'(t)A_Q$ si et seulement si

$$\begin{cases} y & \neq & 0 \\ f'(t) & \neq & 0 \end{cases}$$

ces équations étant à considérer dans $k(Q) = A_Q/Q.A_Q$.
Or $2b = 0 \iff b = 0 \iff f(a) = 0$. Mais par hypothèse f et f' sont premiers entre eux donc si $f(a) = 0$ alors $f'(a) \neq 0$.
Cela établit donc le résultat souhaité, à savoir $V(J) \cap C_f = \varnothing$. Ainsi le Jacobien $J_{(y,t)}$ est de rang maximal (i.e. de rang 1) et la courbe est lisse. □

2.3 Ramification

Définition. 2.3.1. *On considère $f : X \to Y$ un morphisme séparable fini de courbes. Soit $P \in X$, $Q = f(P)$. Soit $t \in \mathcal{O}_Q$ un paramètre local en Q. On considère t comme élément de $\mathcal{O}_P$ via l'application naturelle $f^{\#} : \mathcal{O}_Q \to \mathcal{O}_P$. On définit l'indice de ramification e_P par $e_P = v_P(t)$ où v_P est la valuation associée à l'anneau de valuation $\mathcal{O}_P$.*

On dit que f est ramifiée en P si $e_P > 1$. Sinon on dit que f est non-ramifiée en P.

On suppose connues les notions de diviseur, de diviseur principal, de diviseur canonique, de degré d'un diviseur et de degré d'un morphisme. Les résultats suivants sont énoncés sans démonstration. Le lecteur intéressé pourra les trouver dans [3].

Définition. 2.3.2. *Deux diviseurs sont dits linéairement équivalents si leur différence est un diviseur principal.*

Proposition. 2.3.3. *Sur une courbe non singulière complète X, un diviseur principal est de degré nul.*

Corollaire. 2.3.4. *Deux diviseurs linéairement équivalents ont même degré.*

Définition. 2.3.5. *On définit un homomorphisme $f^* : Div(Y) \to Div(X)$ du groupe des diviseurs de la manière suivante. En tout point Q de Y il est défini par $f^*(Q) = \sum_{P \to Q} e_P.P$. On l'étend par linéarité.*

Lemme. 2.3.6. *Soit D un diviseur et f un morphisme fini, alors*

$$deg(f^*D) = deg(f)deg(D).$$

Définition. 2.3.7. *Soit $f : X \to Y$ un morphisme séparable fini de courbes. On définit le diviseur de ramification de f par*

$$R = \sum_{P \in X} length(\Omega_{X/Y})_P.P.$$

Proposition. 2.3.8. *Soit $f : X \to Y$ un morphisme séparable fini de courbes. Soient K_X et K_Y les diviseurs canoniques de X et Y. Alors*

$$K_X \backsim f^*K_Y + R.$$

Théorème d'Hurwitz. 2.3.9. *Soit $f : X \to Y$ un morphisme séparable fini de courbes. Soit $n = deg(f)$. Alors*

$$2g(X) - 2 = n(2g(Y) - 2) + deg(R).$$

Preuve. Le résultat découle des résultats énoncés précédemment.
En effet, comme $K_X \backsim f^*K_Y + R$, en utilisant le lemme 2.3.4 on a

$$deg(K_X) = deg(f^*K_Y) + deg(R).$$

D'où par le lemme 2.3.6 $deg(K_X) = deg(f)deg(K_Y) + deg(R)$. En utilisant maintenant le résultat sur le degré du diviseur canonique on obtient finalement le résultat souhaité. □

Revenons maintenant à la courbe C_f. Ici $g(Y) = 0$ et $g(X) = g$. Donc dès que $g \neq 1$ le théorème d'Hurwitz assure l'existence de points de ramification (car $deg(R)$ ne peut pas être nul). La proposition 2.2.2 assure que f est ramifiée au point à l'infini. On souhaite savoir ce qu'il en est aux autres points.

Notons $V = \mathbb{Z}_{(p)}$, $B = V[t]$ et $A = V[t]/(y^2 - f(t))$. $f^{\#} : B \to A$, $t \mapsto t$. On cherche les points où $Spec(A) \longrightarrow Spec(B)$ est ramifié.

Proposition. 2.3.10. *L'application considérée est ramifiée en tout point où $f(t) = 0$, elle est non-ramifiée aux autres points.*

Preuve. La courbe étant lisse on a un seul paramètre local, donné par un générateur local de $\Omega^1_X = Xdt \oplus Xdy/(f'(t)dt - 2ydy)$.
Si f ne s'annule pas en t alors par définition de C_f on a également $y \neq 0$ et y est un inversible. On peut donc prendre dt comme paramètre sur Ω. On a alors $f^{\#}(t) = 1.t^1$ et il n'y a donc pas de ramification.
Dans le cas où $f(t) = 0$, on a par définition de C_f que y est nul également. D'où $\Omega^1_X = Xdt \oplus Xdy/(f'(t)dt - 2ydy) = Xdt \oplus Xdy/(f'(t)dt)$. Mais dans ce cas, par hypothèse sur f, $f'(t)$ est inversible et donc $\Omega^1_X = Ady$. Un paramètre local est donc y.
Les points de ramification correspondent aux idéaux maximaux de A contenant y. Soit donc $\mathcal{M}$ un idéal maximal de A contenant y. On note $\mathcal{P}$ l'idéal premier $\mathcal{M} \cap B$.
Soit $\mathcal{M}'$ un idéal maximal de B contenant $\mathcal{P}$. $B_{\mathcal{M}'}$ est local régulier et $\mathcal{M}'.B_{\mathcal{M}'}$ est engendré par un paramètre. Notons u ce paramètre. Comme

$y \in \mathcal{M}$, alors $f(t) \in \mathcal{P} \subset \mathcal{M}'$ donc $\exists g(t) \in B_{\mathcal{M}'}$ tel que $f(t) = u^a.g(t)$ avec a entier naturel non nul. La lissité de la courbe implique que a vaut 1.
En effet, notons $C = B_{\mathcal{M}'}[y]/(y^2 - f(t))$, alors $A_{\mathcal{M}} = C_{\mathcal{M}}$. Par définition, $\Omega^1_C = Cdy \oplus Cdu/(2ydy - \dfrac{d(f(t))}{du}du)$.
Or $\dfrac{d(f(t))}{du} = u^{a-1}\left(ag(t) + u\dfrac{dg(t)}{du}\right)$. Dans ce cas, si $a \geq 2$, Ω^1_C n'est pas libre au point $u = 0$ et $y = 0$ ce qui contredit le caractère lisse de la courbe. On a donc $a = 1$, ainsi $f(t) = ug(t)$. Regardons alors $B_{\mathcal{M}'} \to A_{\mathcal{M}}$, $u \mapsto u$. Comme $y^2 - f(t) = 0$, on a $y^2 = ug(t)$. Or $g(t)$ est inversible dans $B_{\mathcal{M}'}$ et donc $u \in y^2.A_{\mathcal{M}}$. On a ainsi $u \in y^2.A_{\mathcal{M}}$ et y étant notre paramètre, on en conclut que lorsque $f(t) = 0$, l'application $Spec(A) \longrightarrow Spec(B)$ est ramifiée, d'indice de ramification 2. □

3 Une conjecture de Weil

Soit $k = \mathbb{F}_q$ un corps fini à q éléments. Soit X un schéma de type fini sur k. Soit $\bar{k}$ la clôture algébrique de k et soit $\bar{X} = X \times_k \bar{k}$ le schéma correspondant sur $\bar{k}$. Pour tout entier $r \geq 1$, soit N_r le nombre de points de $\bar{X}$ rationnels sur le corps $k_r = \mathbb{F}_{q^r}$ à q^r éléments. En d'autres termes, N_r est le nombre de points de $\bar{X}$ dont les coordonnées sont dans k_r.

Définition. 3.1. *La fonction zêta de X est définie par :*

$$Z(t) = Z(X,t) = exp\left(\sum_{r=1}^{\infty} N_r \frac{t^r}{r}\right).$$

Par définition, c'est une série entière à coefficients rationnels : $Z(t) \in \mathbb{Q}[[t]]$.

Ex. 3.2. *Soit $X = \mathbb{P}^1$. Sur tout corps, $\mathbb{P}^1$ a un point de plus que le nombre d'éléments du corps donc $N_r = q^r + 1$. Ainsi la fonction zêta de X est la suivante :*

$$Z(\mathbb{P}^1,t) = exp\left(\sum_{r=1}^{\infty}(q^r+1)\frac{t^r}{r}\right) = exp\left(\sum_{r=1}^{\infty}\frac{(qt)^r}{r} + \sum_{r=1}^{\infty}\frac{t^r}{r}\right),$$

$$Z(\mathbb{P}^1,t) = exp(-log(1-qt))exp(-log(1-t)) = \frac{1}{1-qt}\frac{1}{1-t} = \frac{1}{(1-qt)(1-t)}.$$

En particulier, c'est une fonction rationnelle de t.

Conjecture de Weil. 3.3. *Soit X une variété projective lisse de dimension n sur $k = \mathbb{F}_q$.*
(1) Caractère rationnel : $Z(t)$ est une fonction rationnelle de t i.e. c'est un quotient de polynômes à coefficients rationnels.
(2) Equation fonctionnelle : soit E le nombre d'intersections de la diagonale Δ de $X \times X$. Alors $Z(t)$ satisfait l'équation fonctionnelle :

$$Z\left(\frac{1}{q^n t}\right) = \pm q^{nE/2} t^E Z(t).$$

(3) Analogue de l'hypothèse de Riemann : on peut écrire :

$$Z(t) = \frac{P_1(t)P_3(t)...P_{2n-1}(t)}{P_0(t)P_2(t)...P_{2n}(t)}$$

où $P_0(t) = 1-t$, $P_{2n}(t) = 1-q^n t$ et $\forall 1 \leq i \leq 2n-1$, $P_i(t)$ est un polynôme à coefficients entiers que l'on peut écrire sous la forme $P_i(t) = \prod(1-\alpha_{ij}t)$ où les α_{ij} sont des entiers algébriques avec $|\alpha_{ij}| = q^{i/2}$. (Cette dernière condition détermine les $P_i(t)$ de manière unique s'ils existent.)
(4) Nombres de Betti : en supposant (3) vrai, on peut définir le i-ième nombre de Betti $B_i = B_i(x)$ comme étant le degré de $P_i(t)$. Alors on a $E = \sum(-1)^i B_i$.

Ex. 3.4. *Dans le cas de $X = \mathbb{P}^1$, on a déjà vu que $Z(\mathbb{P}^1, t) = \dfrac{1}{(1-qt)(1-t)}$ est une fonction rationnelle de t.*
Dans ce cas, $E = 2$ et $n = 1$. On a de plus

$$Z\left(\frac{1}{qt}\right) = \frac{1}{1-1/t}\frac{1}{1-1/qt} = \frac{qt^2}{(t-1)(qt-1)} = qt^2 Z(t).$$

Le second point de la conjecture de Weil est donc également vérifié.
On a $P_0(t) = 1-t$, $P_2(t) = 1-qt$, on pose $P_1 = 1$. Alors $Z(t) = \dfrac{P_1(t)}{P_0(t)P_2(t)}$ et le troisième point de la conjecture de Weil est vérifié.
Enfin on a $deg(P_0) = deg(P_2) = 1$ et $deg(P_1) = 0$. On a donc

$$\sum(-1)^i B_i = B_0 - B_1 + B_2 = 1 - 0 + 1 = 2 = E$$

et le dernier point de la conjecture de Weil est lui aussi vérifié.

La théorie générale sur les fonctions zêta des courbes implique le théorème suivant dû à Weil. [3]

Theorème de Weil. 3.5. *Pour q et f comme précédemment, pour $\mathbb{F}_{q^m}$ une extension finie de $\mathbb{F}_q$, $\exists P_f$ polynôme unitaire à coefficients entiers, de degré $2g$, satisfaisant les propriétés suivantes :*
(1) Ses racines complexes α_i, $1 \leq i \leq 2g$ satisfont $|\alpha_i| = q^{1/2}$ et peuvent être numérotées de telle sorte que $\alpha_i \alpha_{g+i} = q$.
(2) Pour tout entier $m \geq 1$ on a $\#C_f(\mathbb{F}_{q^m}) = q^m - \sum \alpha_i^m$.
(3) Pour J_f variété jacobienne de C_f complétée avec un point non singulier on a $\#J_f(\mathbb{F}_q) = P_f(1)$.

Theorème de Kedlaya. 3.6. *Soit $p > 2$ un nombre premier. Pour $n \geq 1$ entier et $f \in \mathbb{F}_q[x]$ de degré $2g+1$ comme précédemment, P_f peut être calculé en un temps $\mathrm{O}(g^{4+\epsilon} n^{3+\epsilon})$.*

4 La cohomologie de Monsky-Washnitzer

4.1 Introduction

On conserve les notations précédentes, en particulier $q = p^n$.
Pour toute extension finie $\mathbb{F}_{q^m}$ de $\mathbb{F}_q$, on considère l'ensemble des points de C_f à coordonnées dans $\mathbb{F}_{q^m}$.

$$C_f(\mathbb{F}_{q^m}) = \{(a,b) \in \mathbb{F}_{q^m} \ tq \ b^2 = f(a)\}.$$

On souhaite calculer $\#C_f(\mathbb{F}_{q^m})$. L'idée est de faire intervenir une application pour laquelle C_f serait l'ensemble des points fixes. En effet, à condition de savoir calculer la cohomologie, la formule de la trace de Lefschetz donnerait alors directement le résultat cherché. Cette application sera l'application du Frobenius. Cela sera détaillé dans la section 5.

On peut associer à C_f deux espaces vectoriels, $H_c^1(C_f)$ et $H_c^2(C_f)$ sur un corps de caractéristique nulle. On pose $C'_f = C_f - \{y = 0\}$. Les courbes C_f et C'_f ont un automorphisme $\beth$ d'ordre deux :

$$\beth : (a,b) \mapsto (a,-b).$$

Celui-ci induit un automorphisme de $H^1(C'_f)$ et $H^1(C_f)$, noté $\beth^*$ et cet automorphisme décompose $H^1(C'_f)$ et $H^1(C_f)$ en deux sous-espaces propres sur lesquels il agit comme 1 et -1. On note :

$$H^1(C'_f) = H^1(C'_f)^+ \oplus H^1(C'_f)^-,\ H^1(C_f) = H^1(C_f)^+ \oplus H^1(C_f)^-.$$

4.2 L'anneau $A^\dagger$

On souhaite construire le premier groupe de cohomologie de Monsky-Washnitzer des courbes de la forme C'_f comme précédemment. Pour cela on a besoin de se placer sur le corps $\mathbb{Q}_p$ des nombres p-adiques. On suppose connus les résultats sur les nombres p-adiques. Le lecteur pourra se rapporter à l'ouvrage de Koblitz [4].

Définition. 4.2.1. *Soit $\bar{f} \in \mathbb{F}_p[x]$ un polynôme unitaire et irréductible de degré n. Soit $f \in \mathbb{Z}_p[x]$ un relèvement unitaire de $\bar{f}$. On définit $\mathbb{Z}_q = \mathbb{Z}_p[x]/(f)$ et $\mathbb{Q}_q = \mathbb{Q}_p[x]/(f)$.*

On considère p un nombre premier impair et pour n entier naturel non nul on note $q = p^n$. Soit $\bar{Q} \in \mathbb{F}_q[x]$ un polynôme unitaire de degré impair, $d = 2g + 1$, tel que $\bar{Q} \wedge \bar{Q}' = 1$. Notons $\bar{A} = \mathbb{F}_q[x, y, y^{-1}]/(y^2 - \bar{Q})$. C'est l'anneau des fonctions de la courbe $C'_{\bar{Q}}$ que l'on souhaite étudier.

Lemme. 4.2.2. *L'anneau $\bar{A}$ vérifie :*

$$\bar{A} = \bigoplus_{0 \leq i < d,\ j \in \mathbb{Z}} \mathbb{F}_q x^i y^j.$$

Preuve. Comme y est inversible (car on a pris soin de se placer en dehors des zéros de y) $\bar{Q}$ l'est également. De plus on a $\bar{Q}^{-1} = (y^{-1})^2$.

$$\begin{aligned} \bar{A} &= \mathbb{F}_q[x, y, y^{-1}]/(y^2 - \bar{Q}) &&= (\mathbb{F}_q[x, \bar{Q}^{-1}])[y]/(y^2 - \bar{Q}) \\ &= \bigoplus_{\substack{0 \leq i < d,\ j \in \mathbb{Z} \\ 0 \leq k < 2}} \mathbb{F}_q x^i \bar{Q}^j y^k &&= \bigoplus_{0 \leq i < d,\ j \in \mathbb{Z}} \mathbb{F}_q x^i y^j. \end{aligned}$$

□

Soit $Q \in \mathbb{Z}_q[x]$ unitaire, un relèvement de $\bar{Q}$. On note :

$$A = \mathbb{Q}_q[x, y, y^{-1}]/(y^2 - Q) = \bigoplus_{0 \leq i < d,\ j \in \mathbb{Z}} \mathbb{Q}_q x^i y^j.$$

L'anneau A est l'anneau des fonctions de la courbe algébrique C'_Q sur $\mathbb{Q}_q$. Si $g > 0$ celui-ci dépend du choix du relèvement Q. Cependant on souhaite que ce ne soit pas le cas, il nous faut donc construire un autre anneau.

Définition. 4.2.3. *On définit*

$$A^\infty = \{\sum_{i,j} a_{i,j} x^i y^j \mid a_{i,j} \in \mathbb{Q}_q,\ |a_{i,j}| \to 0 \ lorsque\ |j| \to \infty\}$$

avec $0 \leq i < d$ *et* $j \in \mathbb{Z}$.

Les éléments de A^∞ sont les séries de la forme $f = \sum a_{i,j} x^i y^j$, $0 \leq i < d$, $j \in \mathbb{Z}$, ayant la propriété suivante : pour tout entier k, presque tout $a_{i,j}$ est dans $p^k \mathbb{Z}_q$. Si on note A^∞_+ la complétion p-adique de $\mathbb{Z}_q[x, y, y^{-1}]/(y^2 - Q)$, on peut encore voir A^∞ comme $\mathbb{Q}_q \otimes_{\mathbb{Z}_q} A^\infty_+$. On peut montrer que A^∞_+ ne dépend pas du choix du relèvement Q de $\bar{Q}$ et donc avec cette écriture que A^∞ est indépendant du choix du relèvement, à isomorphisme près. Cependant l'anneau A^∞ ne permet pas encore d'obtenir les résultats de cohomologie souhaités. Pour cela il nous faut faire intervenir un autre anneau, l'anneau dagger.

Définition. 4.2.4. *On définit l'anneau dagger par :*

$$A^\dagger = \{\sum_{i,j} a_{i,j} x^i y^j \mid a_{i,j} \in \mathbb{Q}_p,\ \liminf_{|j| \to \infty} v_p(a_{i,j})/|j| > 0\}$$

avec $0 \leq i < d$ *et* $j \in \mathbb{Z}$.

On peut montrer que l'anneau $A^\dagger$ ne dépend pas du choix du relèvement Q de $\bar{Q}$.

4.3 Cohomologie différentielle et cohomologie de de Rham

On commence par déterminer les formes différentielles sur C'_Q. Les fonctions considérées sur C'_Q sont les éléments de A. Tout élément f de A admet une différentielle df qui doit vérifier la règle de Leibniz et telle que $\forall a \in \mathbb{Q}_q$, $da = 0$. De plus les différentielles doivent former un A-module. Il existe une dérivation universelle $d : A \to \Omega$ telle que $\forall D : A \to M$ $\mathbb{Q}_q$-dérivation, $\exists! l : \Omega \to M$ application A-linéaire telle que $D = ld$. Nous allons décrire cette dérivation universelle.

Lemme. 4.3.1. *Le A-module Ω est un A-module libre. Une A-base de Ω est $(Q'dx)/2y$.*

Preuve. Tout d'abord Ω est engendré par les df avec f élément de A donc Ω est engendré par dx et dy. Cependant on a la relation $0 = y^2 - Q$ d'où $0 = 2ydy - Q'dx$. Comme y est inversible dans A on a donc $dy = \dfrac{Q'dx}{2y}$. Ainsi Ω est un A-module libre et $(Q'dx)/2y$ est une A-base. En d'autres termes, $\Omega = A.\dfrac{dx}{2y}$. □

On souhaite désormais écrire le complexe de de Rham de C'_Q. Pour cela il faut d'abord expliciter l'image par d des éléments de la forme $x^i y^j$ dans notre base.
On a $d(x^i y^j) = ix^{i-1}y^j dx + jx^i y^{j-1} dy = ix^{i-1}y^j dx + jx^i y^{j-1}\dfrac{Q'}{2y}dx$.
Ainsi le complexe de de Rham de C'_Q est :

$$0 \to A \xrightarrow{d} \Omega^1_A \to 0,$$

où l'application $A \xrightarrow{d} A.\dfrac{dx}{2y}$ est donnée par :

$$x^i y^j \mapsto (2ix^{i-1}y^{j+1} + jx^i Q' y^{j-1})\frac{dx}{2y}.$$

La cohomologie algébrique de de Rham est la cohomologie de ce complexe.

$$H^0_{dR}(C'_Q) = ker(d) = \{f \in A \mid df = 0\},$$
$$H^1_{dR}(C'_Q) = coker(d) = \left(A.\frac{dx}{2y}\right)/dA.$$

Proposition. 4.3.2. *On a* $H^0_{dR}(C'_Q) = \mathbb{Q}_q$.
Les classes $\left[x^i y^{-1}(dx)/y\right]$ *avec* $0 \leq i \leq 2g$ *forment une base de* $H^1_{dR}(C'_Q)^+$.
Les classes $\left[x^i(dx)/y\right]$ *avec* $0 \leq i < 2g$ *forment une base de* $H^1_{dR}(C'_Q)^-$.

Preuve. On commence par répartir le complexe en deux sous-espaces propres pour $\beth$. L'anneau A admet pour $\mathbb{Q}_q$-base les $x^i y^j$ avec $0 \leq i < d$ et $j \in \mathbb{Z}$. De plus $\beth x = x$ et $\beth y = -y$, il est donc clair que la décomposition de A en sous-espace propres pour $\beth$ est la suivante :

$$A^+ = \bigoplus_{\substack{0\leq i<d \\ j\in\mathbb{Z}}} \mathbb{Q}_q x^i y^{2j}, \qquad A^- = \bigoplus_{\substack{0\leq i<d \\ j\in\mathbb{Z}}} \mathbb{Q}_q x^i y^{2j+1}.$$

Soit encore $A^+ = \bigoplus_{\substack{0\leq i<d \\ j\in\mathbb{Z}}} \mathbb{Q}_q x^i Q^j = \mathbb{Q}_q[x, Q^{-1}]$ et $A^- = \bigoplus_{\substack{0\leq i<d \\ j\equiv 1[2]}} \mathbb{Q}_q x^i y^j$.
La décomposition de Ω en sous-espaces propres pour $\beth$ est la suivante :

$$\Omega^+ = \bigoplus_{\substack{0\leq i<d \\ j\equiv 1[2]}} \mathbb{Q}_q x^i y^j \frac{dx}{2y}, \qquad \Omega^- = \bigoplus_{\substack{0\leq i<d \\ j\equiv 0[2]}} \mathbb{Q}_q x^i y^j \frac{dx}{2y}.$$

On peut encore écrire la partie positive de manière plus explicite, la dernière égalité venant du fait que Q est un polynôme en x :

$$\Omega^+ = \bigoplus_{\substack{0\leq i<d \\ j\equiv 1[2]}} \mathbb{Q}_q x^i Q^{(j-1)/2} dx = \mathbb{Q}_q[x, Q^{-1}]dx.$$

On commence par déterminer la partie positive. En fait cette partie est le complexe de de Rham de l'anneau $\mathbb{Q}_q[x, Q^{-1}]$. On a :

$$0 \xrightarrow{\Phi} \mathbb{Q}_q[x, Q^{-1}] \xrightarrow{d} \mathbb{Q}_q[x, Q^{-1}]dx \xrightarrow{\Psi} 0.$$

Montrons tout d'abord que $H^0_{dR}(C'_Q)^+ = \mathbb{Q}_q$.
Par définition, $H^0_{dR}(C'_Q)^+ = Ker(d)/Im(\Phi)$. Or $Im(\Phi) = 0$ il suffit donc de déterminer le noyau de l'application d. Il est clair que $\mathbb{Q}_q \subset Ker(d)$, on veut montrer que ces deux ensemble sont égaux. Soit donc M un élément de $\mathbb{Q}_q[x, Q^{-1}]$, montrons que $dM = 0 \Rightarrow M \in \mathbb{Q}_q$. L'élément M est de la forme

$M = \sum_{i=0}^{n}\sum_{j=0}^{m} a_{ij}x^iQ^{-j}$. On a donc $dM = \sum_{i=0}^{n}\sum_{j=0}^{m} a_{ij}(i-jxQ'Q^{-1})x^{i-1}Q^{-j}dx$.
On commence par remarquer que cette expression ne donne aucune information sur le terme a_{00} correspondant au coefficient de x^0Q^{-0} qui est donc quelconque. La partie en Q^{-0} est donnée par $\sum_{i=0}^{n} ia_{i0}x^{i-1}dx$. Cette expression est nulle si et seulement si $\forall 1 \leq i \leq n$, $a_{i0} = 0$. Soit maintenant $1 \leq j \leq m$ la partie en Q^{-j} est donnée par $\sum_{i=0}^{n}(ia_{ij} - (j-1)a_{ij-1}xQ')x^{i-1}dx$. Le terme de plus bas degré a pour coefficient a_{1j} qui doit donc être nul et de proche en proche on en déduit que $\forall 0 \leq i \leq n$ et $\forall 1 \leq j \leq m$, $a_{ij} = 0$. On a donc établi que $dM = 0 \Leftrightarrow M \in \mathbb{Q}_q$.

On montre maintenant que les $x^iQ^{-1}dx$ avec $0 \leq i < d$ forment une base de $H^1_{dR}(C'_Q)^+$.
On a par définition $H^1_{dR}(C'_Q)^+ = Ker(\Psi)/Im(d) = \mathbb{Q}_q[x, Q^{-1}]dx/Im(d)$. En réutilisant ce qui précède, on sait qu'un élément de $Im(d)$ est de la forme $dM = \sum_{i=0}^{n}\sum_{j=0}^{m} a_{ij}(i - jxQ'Q^{-1})x^{i-1}Q^{-j}dx$.
Tout d'abord il est clair qu'il est possible d'atteindre x^i pour tout i, il suffit de prendre $m = 0$ et $a_{k0} = \frac{1}{i+1}\delta_{i+1k}$. On va maintenant montrer qu'on a une relation entre Q^{-j} et $Q^{-(j+1)}$, $\forall j \geq 1$. Comme par ailleurs on sait qu'on a une relation entre Q et x^d et qu'il est clair que les éléments x^iQ^{-1} forment une famille libre, on aura alors le résultat voulu. On réalise la division euclidienne de x^iQ' par Q (cela sera détaillé plus tard) pour obtenir l'expression $x^iQ' = a_iQ + b_i$ où les a_i et les b_i sont des polynômes en x. Alors on peut réécrire l'expression des éléments de l'image de d. On a $dM = \sum_{i=0}^{n}\sum_{j=0}^{m} a_{ij}(ix^{i-1} - ja_i(x))Q^{-j}dx - \sum_{i=0}^{n}\sum_{j=0}^{m} ja_{ij}b_i(x)Q^{-(j+1)}$. D'où le résultat souhaité.

Il s'agit maintenant de déterminer la partie négative. Pour cela il va falloir définir un ordre sur les monômes x^iy^j où $0 \leq i < d$ et $j \in \mathbb{Z}$. On les ordonne de manière lexicographique en considérant d'abord l'exposant de y puis celui de x.
Pour $0 \leq i < d$ on considère la division euclidienne de x^iQ' par Q dans

$\mathbb{Q}_q[x]$. On a donc :

$$x^i Q' = a_i Q + b_i \quad avec \quad deg(b_i) < d.$$

Dans le cas $i = 0$, on réalise la division euclidienne d'un polynôme non nul par sa dérivée qui est donc de degré strictement inférieur. Ainsi $a_0 = 0$ et $b_0 = Q'$.
Dans le cas $1 \leq i < d$, comme Q est unitaire et que $deg(Q') = deg(Q) - 1$ on a $a_i = dx^{i-1} + ...$ et donc $deg(a_i) = i - 1$.
En injectant ce résultat dans l'expression de l'application d on obtient :

$$d : x^i y^j \mapsto (2ix^{i-1}y^{j+1} + jx^i Q' y^{j-1})\frac{dx}{2y} = (2ix^{i-1}y^{j+1} + ja_i y^{j+1} + jb_i y^{j-1})\frac{dx}{2y}.$$

Regardons maintenant ce qui se passe pour $0 \leq i < d$ et $j \equiv 1[2]$. On cherche à identifier le monôme le plus grand de $d(x^i y^j)$ (dans la relation d'ordre choisie précédemment).
Si $i = 0$, $d(x^i y^j) = (ja_0 y^{j+1} + jb_0 y^{j-1})\frac{dx}{2y} = (jQ' y^{j-1})\frac{dx}{2y}$. Comme $jd \neq 0$ le plus grand monôme est $x^{d-1}y^{j-1}$.
Si $1 \leq i < d$, comme j est impair, $2i + jd \neq 0$ et donc le plus grand monôme est $x^{i-1}y^{j+1}$.
Remarquons que comme Q et Q' sont premiers entre eux, la multiplication par Q' dans $\mathbb{Q}_q[x]/(Q)$ est un isomorphisme. Comme de plus les x^i forment une famille de degré échelonné, on en conclut que les b_i, $0 \leq i \leq d - 1$ forment une $\mathbb{Q}_q$-base de $\mathbb{Q}_q[x]_{<d}$. Ainsi le plus petit monôme de $d(x^i y^j)$ est de la forme $x^k y^{j-1}$ avec $0 \leq k < d$.
Ces considérations nous permettent de prouver immédiatement que
$H^0_{dR}(C'_Q)^- = ker(d : A^- \to \Omega^-) = 0$. En effet, ce qui précède assure que les $d(x^i y^j)$ avec $0 \leq i < d$ et $j \equiv 1[2]$ sont de degré échelonné, ils sont donc linéairement indépendants.
Cela permet enfin, avec le résultat déjà démontré sur la partie positive, d'établir le premier résultat énoncé dans la proposition.

Il s'agit pour finir de montrer que les classes $\left[x^i(dx)/y\right]$ avec $0 \leq i < 2g$ forment une base de $H^1_{dR}(C'_Q)^- = \Omega^-/dA^-$. La démonstration se fait en deux temps. On commence par montrer que ces éléments forment une famille libre, puis qu'ils forment une famille génératrice (le fait qu'ils soient dans l'espace considéré est clair).
Commençons par remarquer qu'il est clair que la famille $(x^i(dx)/y)$ est libre dans Ω^- puisqu'elle est de degré échelonné. Supposons qu'il existe une combinaison linéaire des classes $\left[x^i(dx)/y\right]$ dans Ω^-/dA^- qui soit nulle. Cela

signifie que cette combinaison linéaire est un élément de Ω^- appartenant à dA^-. Supposons donc que l'on ait :

$$\sum_{0\leq k<d} \lambda_k x^k (dx)/y = \sum_{\substack{0\leq i<d \\ j\equiv 1[2]}} \mu_{i,j} d(x^i y^j).$$

La relation étant valable dans Ω^- dont les $d(x^i y^j)$ sont des générateurs. Encore une fois on raisonne sur l'ordre des éléments intervenant dans cette somme.
On a déjà établi précédemment que les éléments $d(x^i y^j)$ étaient de la forme $(2ix^{i-1}y^{j+1} + jx^i Q' y^{j-1})\dfrac{dx}{2y}$. Or dans la somme de gauche les monômes en facteur de $\dfrac{dx}{y}$ sont des monômes en x et ne font intervenir aucune puissance non nulle de y. C'est pourquoi le facteur $\mu_{i,j}$ d'un $d(x^i y^j)$ intervenant dans le membre de droite est non nul si et seulement si j vaut 1 ou -1. Alors le monôme de plus grand ordre dans le membre de droite est donné par $j = 1$ et est de la forme $x^i y^{-1}$ et le monôme de plus petit ordre est donné par $j = -1$ et est de la forme $x^i y$, avec dans les deux cas $0 \leq i < d$. Cela est absurde car alors le plus petit monôme est plus grand que le plus grand monôme. Ainsi tous les $\mu_{i,j}$ sont nuls. On en conclut qu'une combinaison linéaire des $[x^i(dx)/y]$ est nulle dans $H^1_{dR}(C'_Q)^-$ si et seulement si elle est nulle dans Ω^-. Cependant il est clair que dans Ω^- cette famille est libre car c'est une famille de degré échelonné. La seule relation existant entre les $[x^i(dx)/y]$ est la relation triviale et la famille est donc libre.

Montrons maintenant que la famille est génératrice. Pour cela on donne un algorithme de réduction. Celui-ci permet de connaître une procédure explicite permettant d'écrire un élément quelconque $f(dx)/y$ de Ω^- comme somme d'un élément de dA^- et d'une combinaison linéaire des $x^i(dx)/y$.

Soit donc $f(dx)/y$. La première étape consiste à supprimer les puissances de y strictement négatives de f. La procédure est la suivante. Tant que f admet un monôme avec $j < 0$, soit m la plus petite puissance de y apparaissant dans f. Alors il existe une unique combinaison linéaire des $d(x^k y^{m+1})$ telle que $f(dx)/y - dg$ n'a pas de monôme de la forme $x^n y^m$. Comme le plus petit monôme de $d(x^k y^{m+1})$ est de la forme $x^n y^m$, le plus petit monôme de $f(dx)/y - dg$ est plus grand que le plus petit monôme de $f(dx)/y$. Comme de plus on a la condition que ce plus petit monôme doit avoir une puissance négative, l'algorithme est assuré de se terminer en un temps fini. On remplace dans la procédure $f(dx/y)$ par $f(dx)/y - dg$. Une fois qu'elle est achevée, f n'a plus de monômes avec une puissance négative de y.

On supprime maintenant les puissances de y strictement positives apparaissant dans f. La procédure est la suivante. Tant que f admet un monôme avec $j > 0$, soit m la plus grande puissance de y apparaissant dans f. Soit $x^i y^m$ le plus grand monôme de f, soit $x^k y^l$ le monôme tel que $d(x^k y^l)$ admet $x^i y^m$ comme plus grand monôme (les valeurs de k et l dépendent de la valeur de i). On remplace alors $f(dx)/y$ par $f(dx)/y$ moins un multiple approprié de $d(x^k y^l)$. Encore une fois la procédure diminue l'ordre du plus grand monôme et la condition $j > 0$ assure qu'elle s'achève en un temps fini. Une fois la procédure achevée, f n'a plus de monômes avec une puissance strictement positive de y. De plus, cette procédure ne rajoute pas de puissance strictement négative de y. Enfin on soustrait à $f(dx)/y$ un multiple approprié de dy pour que le monôme $x^{d-1}y$ n'apparaisse plus dans la différence.

Finalement f n'a plus que des monômes ayant une puissance nulle de y. On a donc écrit $f(dx)/y$ comme une combinaison linéaire des $x^i(dx)/y$ avec $0 \leq i < d-1$ plus un élément de dA^-. Cela achève de montrer que les classes considérées forment une famille génératrice et prouve donc la troisième assertion de la proposition. □

Pour obtenir un opérateur de Frobenius, cela ne suffit pas. Il nous faut encore calculer la cohomologie de l'anneau $A^\dagger$.
Par définition, le complexe de de Rham de $A^\dagger$ est le suivant :

$$0 \to A^\dagger \xrightarrow{d} \Omega^1_{A^\dagger} \to 0,$$

où l'application d est donnée par :

$$\sum_{i,j} a_{i,j} x^i y^j \mapsto \sum_{i,j} a_{i,j}(2ix^{i-1}y^{j+1} + jx^i Q' y^{j-1})\frac{dx}{2y}.$$

Il est en effet possible de vérifier que si $\liminf_{|j|\to\infty} v_p(a_{i,j})/|j| > 0$ alors il en est de même pour les coefficients de $\sum_{i,j} a_{i,j}(2ix^{i-1}y^{j+1} + jx^i Q' y^{j-1})$.

On note $H^i(C'_{\bar{Q}})$ les groupes de cohomologie de ce complexe, qui sont des $\mathbb{Q}_q$ espaces vectoriels. Comme précédemment, l'automorphisme $\sqsupset$ les scinde en deux sous-espaces. On va identifier plus précisément la partie négative. Pour ce faire on aura besoin de deux lemmes techniques dont la démonstration ne sera pas donnée ici. Elle est disponible dans [1] et repose en grande partie sur l'algorithme de réduction énoncé dans la preuve de la proposition précédente.

Lemme. 4.3.3. *Soit $\omega = ay^{-m}(dx)/y$, avec $m > 0$, $m \equiv 0$ [2] et $a \in \mathbb{Z}_q[x]$ vérifiant $deg(a) < d$. Alors : $\exists! b \in \mathbb{Q}_q[x]$ avec $deg(b) < d$, $\exists! f \in A^-$ tels que*

$$w = ay^{-m}(dx)/y = b(dx)/y + df,$$

avec $f = \sum_{j=-m+1}^{-1} f_j y^j$, $f_j \in \mathbb{Q}_q[x]$, $deg(f_j) < d$. Alors on a :

$$p^{\lfloor log_p(m-1) \rfloor} b \in \mathbb{Z}_q[x] \quad et \quad p^{\lfloor log_p(m-1) \rfloor} f_j \in \mathbb{Z}_q[x] \quad \forall j.$$

Lemme. 4.3.4. *Soit $\omega = ay^{m}(dx)/y$, avec $m > 0$, $m \equiv 0$ [2] et $a \in \mathbb{Z}_q[x]$ vérifiant $deg(a) < d$. Alors : $\exists! b \in \mathbb{Q}_q[x]$ avec $deg(b) < d$, $\exists! f \in A^-$ tels que*

$$w = ay^{-m}(dx)/y = b(dx)/y + df,$$

avec $f = \sum_{j=1}^{m-1} f_j y^j$, $f_j \in \mathbb{Q}_q[x]$, $deg(f_j) < d$. Alors on a :

$$p^{\lfloor log_p(dm+d-2) \rfloor} b \in \mathbb{Z}_q[x] \quad et \quad p^{\lfloor log_p(dm+d-2) \rfloor} f_j \in \mathbb{Z}_q[x] \quad \forall j.$$

Proposition. 4.3.5. *Les classes $\left[x^i(dx)/y\right]$ avec $0 \leq i < d-1$ forment une base de $H^1(C'_{\bar{Q}})^-$.*

Preuve. Commençons par montrer que ces éléments forment une famille génératrice. Soit donc $\sum_m a_m y^m(dx)/y$, $a_m \in \mathbb{Q}_q[x]$, $deg(a_m) < d$, un élément de $A^\dagger(dx)/y$. Par définition, il existe une certaine puissance n_0 de p pour laquelle $\forall m$, $p^{n_0} a_m \in \mathbb{Z}_q[x]$.
Les deux lemmes énoncés précédemment nous donnent, pour tout m non nul, un polynôme $b_m \in \mathbb{Q}_q[x]$ avec $deg(b_m) < d-1$ et un élément $f_m \in A^-$ tels que $p^{n_0} a_m y^m(dx)/y = b_m(dx)/y + df_m$. Il s'agit maintenant de montrer qu'une telle relation est valable dans $A^\dagger$. On sait qu'il existe un certain $\epsilon > 0$ et un entier m_0 tels que a_m est divisible par $p^{\lfloor \epsilon |m| \rfloor}$ dès que $|m| > m_0$. Ainsi on a dans $A^\dagger$ la relation suivante :

$$\sum_m a_m y^m(dx)/y = a_0(dx)/y + \left(\sum_{m \neq 0} b_m \right) (dx)/y + d\left(\sum_m f_m \right).$$

Cependant il est possible qu'apparaisse dans cette somme un monôme du type x^{d-1}. On peut faire disparaitre un tel terme en utilisant la relation $dy = Q'\dfrac{dx}{y} = (dx^{d-1} + ...)\dfrac{dx}{2y}$. Cela achève de montrer que la famille considérée est bien génératrice.

La démonstration de la liberté de cette famille est sensiblement la même que dans le cas de $H^1_{dR}(C'_Q)^-$. Supposons en effet que l'on ait une relation entre les éléments de cette famille. Il est alors possible de trouver une puissance de p adaptée pour que cette relation soit à coefficients entiers. En réduisant alors cette relation selon une puissance arbitrairement grande de p on est alors dans une situation semblable à celle de la liberté de la famille $\left[x^i(dx)/y\right]$ dans le cas de $H^1_{dR}(C'_Q)^-$ et le processus est le même. Cela achève la démonstration de la proposition. □

5 Relèvement du Frobenius

5.1 Motivation

On souhaite que $X_0 \mapsto H^1_c(X_0)$ soit fonctoriel en X_0 c'est pourquoi on va introduire le Frobenius.

Soit $\mathbb{F}$ une clôture algébrique de $\mathbb{F}_q$. On note $F : \mathbb{F} \to \mathbb{F}$, $a \mapsto a^p$, l'application puissance p de Frobenius. C'est un automorphisme du corps $\mathbb{F}$. On note F_q l'application définie par F^n, la puissance q de Frobenius.

Lemme. 5.1.1. *Pour tout entier naturel m non nul,*

$$\mathbb{F}_{q^m} = \{a \in \mathbb{F} \mid F_q^m(a) = a\}.$$

Preuve. C'est une conséquence directe de la démonstration de l'existence d'un corps fini à p^m éléments, pour tout nombre premier p et pour tout entier naturel non nul m. Un tel corps est en effet un corps de décomposition sur $\mathbb{F}_p$ du polynôme $x^{p^m} - x$. Or $q^m = p^{nm}$ et $F_q^m = (F^n)^m$ et donc $F_q^m(a) = a$ pour a appartenant à $\mathbb{F}$ si et seulement si a est une racine du polynôme $x^{p^{nm}} - x$. □

Comme le polynôme f définissant C_f est à coefficients dans $\mathbb{F}_q$, l'application F_q donne également une application appelée puissance q de Frobenius sur C_f. On notera encore cette application F_q.

$$F_q : C_f(\mathbb{F}) \to C_f(\mathbb{F}),\ (a,b) \mapsto (F_q(a), F_q(b)).$$

Proposition. 5.1.2. *L'ensemble $C_f(\mathbb{F}_{q^m}) = Hom(Spec(\mathbb{F}_{q^m}), C_f)$ est exactement l'ensemble des points fixes de l'application $F_q^m : C_f(\mathbb{F}) \to C_f(\mathbb{F})$.*

Preuve. Ce résultat est une conséquence directe de la définition de l'ensemble $C_f(\mathbb{F}_{q^m})$ et du lemme 5.1.1.
On a $C_f(\mathbb{F}_{q^m}) = \left\{(a,b) \in \mathbb{F}_{q^m}^2 \mid b^2 = f(a)\right\}$ et $\mathbb{F}_{q^m} = \left\{a \in \mathbb{F} \mid F_q^m(a) = a\right\}$. Un élément de $C_f(\mathbb{F})$ est un point fixe de l'application si et seulement si $(a,b) \in \mathbb{F}^2$ et $(a,b) = (F_q^m(a), F_q^m(b))$. C'est-à-dire si et seulement si $(a,b) \in \mathbb{F}^2$ et $a = F_q^m(a)$ et $b = F_q^m(b)$. Comme de plus on considère l'application F_q^m sur $C_f(\mathbb{F})$ un point fixe de cette application doit vérifier la relation $b^2 = f(a)$ et donc aussi $F_q^m(b)^2 = F_q^m(a)$. Ainsi l'ensemble des points fixes de $F_q^m : C_f(\mathbb{F}) \to C_f(\mathbb{F})$ est l'ensemble $C_f(\mathbb{F}_{q^m})$. □

On peut associer à C_f deux espaces vectoriels, $H_c^1(C_f)$ et $H_c^2(C_f)$ sur un corps de caractéristique nulle, tels que F_q induise un endomorphisme $F_q^* : H_c^i(C_f) \to H_c^i(C_f)$ pour $i = 1, 2$. Et que l'on ait le résultat suivant.

Théorème. 5.1.3. *On a :*

$$\#C_f(\mathbb{F}_{q^m}) = Tr((F_q^m)^* \mid H_c^2(C_f)) - Tr((F_q^m)^* \mid H_c^1(C_f)).$$

Preuve. C'est une conséquence immédiate de la proposition précédente et du théorème de la trace de Lefschetz. □

Ici l'indice c signifie que la cohomologie considérée est à support compact. Dans la formule de théorème 3.5, q^m est la trace sur H_c^2 et la somme des α_i^m est la trace sur H_c^1. En particulier, le polynôme P_f est le polynôme caractéristique de F_q^* agissant sur $H_c^1(C_f)$. Cependant la cohomologie à support compact peut être difficile à calculer. On utilise donc la dualité de Poincaré qui nous dit que le produit usuel

$$H_c^1(C_f) \times H^1(C_f) \to H_c^2(C_f)$$

est non dégénéré. Cela implique que P_f est le polynôme caractéristique de $q(F_q^*)^{-1}$ sur $H^1(C_f)$. C'est ce qui a motivé le calcul de la cohomologie dans la section 4.

L'espace vectoriel $H^1_{dR}(C'_Q)^- = \bigoplus_{0\leq i<d-1} \mathbb{Q}_q x^i(dx)/y$ nous donnera le polynôme $P_{\bar{Q}}$. Cependant nous n'avons pas dans ce contexte l'opérateur de Frobenius dont $P_{\bar{Q}}$ est le polynôme caractéristique. En fait il est généralement impossible de relever l'endomorphisme de Frobenius F_q de $C'_{\bar{Q}}$ sur C'_Q. C'est pour cela que l'on a fait intervenir l'anneau $A^\dagger$.

Proposition. 5.1.4. *Le polynôme P_f du théorème 3.5 est le polynôme caractéristique de F_q^* sur $H^1(C'_f)^-$.*

On a défini précédemment le morphisme $F_q : C'_{\bar{Q}} \to C'_{\bar{Q}}$ comme une application de $C_{\bar{Q}}(\mathbb{F})$ sur lui-même, où $\mathbb{F}$ est une clôture algébrique de $\mathbb{F}_q$. Voyons de quelle façon on peut l'interpréter comme un morphisme de la $\mathbb{F}_q$-algèbre $\bar{A} = \mathbb{F}_q[x, y, y^{-1}]/(y^2 - \bar{Q})$ sur elle-même.
Le morphisme F_q envoie un élément $(a, b) \in C_{\bar{Q}}(\mathbb{F})$ sur (a^q, b^q). Par définition de $\bar{A}$ on a $C_{\bar{Q}}(\mathbb{F}) = Hom_{\mathbb{F}_q}(\bar{A}, \mathbb{F})$, où (a, b) correspond au morphisme envoyant x sur a et y sur b. Alors l'application $(a, b) \mapsto (a^q, b^q)$ est induite par le morphisme de $\mathbb{F}_q$-algèbre $F_q : \bar{A} \to \bar{A}$ qui envoie x sur x^q et y sur y^q. Pour les calculs, il est intéressant de travailler avec $F_p : \bar{A} \to \bar{A}$. Cependant F_p n'est pas un morphisme de $\mathbb{F}_q$-algèbre si $n > 1$. On a le diagramme suivant :

$$\begin{array}{ccc} \bar{A} & \xrightarrow{F_p} & \bar{A} \\ \uparrow & & \uparrow \\ \mathbb{F}_q & \xrightarrow{\sigma} & \mathbb{F}_q \end{array}$$

en notant $\sigma : \mathbb{F}_q \to \mathbb{F}_q$, $a \mapsto a^p$ l'application de Frobenius usuelle sur $\mathbb{F}_q$.

Dans ce qui suit, on va montrer que l'endomorphisme de Frobenius $F_q : C'_{\bar{Q}} \to C'_{\bar{Q}}$ peut être relevé sur $A^\dagger$.

5.2 Relèvement sur $A^\dagger$

On commence par relever σ en un automorphisme de $\mathbb{Z}_q$ sur lui-même. Cela peut-être fait de manière unique. On note encore σ cet automorphisme.

Comme $\mathbb{Q}_q = \mathbb{Z}_q[1/p]$, on peut étendre σ, de manière unique, en un automorphisme de $\mathbb{Q}_q$ que l'on désignera encore une fois par σ. Enfin on étend σ en $F_p : \mathbb{Z}_q[x] \to \mathbb{Z}_q[x]$ en envoyant x sur x^p.

Proposition. 5.2.1. *L'endomorphisme F_p peut être étendu de manière unique en un endomorphisme F_p de A^∞, p-adiquement continu et compatible avec la structure de $\mathbb{Q}_q[x]$-algèbre de A^∞. En d'autres termes, F_p applique le sous-anneau $A^\infty_+ = (\mathbb{Z}_q[x,y,z]/(y^2 - Q, yz - 1))^\wedge$ sur lui-même et $\forall m \geq 0$ la restriction de F_p de $\mathbb{Z}_q[x,y,z]/(y^2 - Q, yz - 1, p^m)$ à $\mathbb{Z}_q[x]/(p^m)$ est égale à la réduction modulo p^m de F_p défini précédemment.*

Construire une extension de F_p à A^∞_+ comme nous le voulons signifie que F_p doit vérifier les hypothèses suivantes :

1. $F_p a = \sigma a$, $\forall a \in \mathbb{Z}_q$.
2. $F_p x = x^p$.
3. $F_p y \in A^\infty_+$ satisfait $(F_p y)^2 = F_p Q$ et a pour image y^p dans $\bar{A}$.
4. $F_p z \in A^\infty_+$ et satisfait $(F_p y)^2 (F_p z)^2 = 1$.

Construisons donc notre relèvement de F_p de façon à ce que ces hypothèses soient vérifiées.
Si on note $Q = x^d + Q_{d-1}x^{d-1} + ... + Q_0$, alors on a :

$$F_p Q = x^{pd} + \sigma(Q_{d-1})x^{p(d-1)} + ... + \sigma(Q_0).$$

Comme F_p relève l'endomorphisme puissance p de Frobenius de $\mathbb{F}_q[x]$, $F_p Q$ et Q^p ont la même image dans $\mathbb{F}_q[x]$ et donc leur différence est divisible par p dans $\mathbb{Z}_q[x]$. Notons $E = \dfrac{F_p Q - Q^p}{p} \in \mathbb{Z}_q[x]$.
On a alors dans A^∞_+ :

$$F_p Q = Q^p + pE = y^{2p} + pE = y^{2p}(1 + pEz^{2p})$$

(puisque dans notre anneau on a la relation $yz = 1$). La condition 3 justifie alors de poser

$$F_p y = y^p (1 + pEz^{2p})^{1/2}.$$

On utilise alors l'écriture en série entière de $(1+x)^\alpha$ et on a

$$F_p y = y^p \sum_{k \geq 0} \binom{1/2}{k} p^k E^k z^{2pk}$$

où l'on a pris la convention que $\binom{1/2}{k}$ est le polynôme $\frac{t(t-1)...(t-k+1)}{k!}$ évalué en $t = 1/2$.

Remarque. 5.2.2. *On a* $v_p\left(\binom{1/2}{k}\right) \geq 0$ *et donc* $\binom{1/2}{k} \in \mathbb{Z}_q$.
Le fait que cet élément a une valuation p-adique positive peut se montrer explicitement en utilisant les propriétés d'une valuation. Tout d'abord rappelons que $\binom{1/2}{k}$ *vaut par convention* $\frac{1/2(1/2-1)...(1/2-k+1)}{k!}$. *Comme p est impair,* $v_p(1/2) = 0$ *d'où* $v_p\left(\binom{1/2}{k}\right) = v_p\left(\frac{1(1-2)...(1-2(k-1))}{k!}\right)$. *De plus la valuation d'un nombre et celle de son opposé sont égales, d'où* $v_p\left(\binom{1/2}{k}\right) = v_p\left(\frac{(2(k-1)-1)...3.1}{k!}\right)$. *Utilisons les propriétés d'une valuation pour simplifier l'expression. On a* $v_p\left(\binom{1/2}{k}\right) = v_p\left(\frac{(2(k-1))!}{2.k!(k-1)!}\right)$ *et p étant impair, on peut enlever le facteur 2 au dénominateur. Alors* $v_p\left(\binom{1/2}{k}\right) = v_p\left(\frac{(2(k-1))!}{k!(k-1)!}\right) = v_p\left(\frac{1}{k}\binom{2(k-1)}{k-1}\right)$. *Comme la valuation p-adique d'un nombre entier est positive, si p ne divise pas k alors clairement on a* $v_p\left(\binom{1/2}{k}\right) \geq 0$. *Reste le cas où k est un multiple de p. Dans ce cas, utilisons les propriétés d'addition de la valuation p-adique. On a* $v_p\left(\frac{1}{k}\binom{2(k-1)}{k-1}\right) = \sum_{i=1}^{2(k-1)} v_p(i) - 2\sum_{i=1}^{k-1} v_p(i) - v_p(k) = \sum_{i=k+1}^{2(k-1)} v_p(i) - \sum_{i=1}^{k-1} v_p(i)$. *Il s'agit maintenant de montrer que cette différence est positive. Concrètement, la valuation p-adique évalue le nombre de divisions par p qu'il est possible d'effectuer. Or, en mettant de côté le dernier terme de la seconde somme, on évalue ce nombre sur* $k-2$ *entiers et les mêmes entiers, translatés de k, qui est un multiple de p, il y a donc le même nombre de multiples de p dans les deux sommes et si les puissances ne sont pas les mêmes, alors elles sont forcément plus élevées dans la somme de gauche. De plus comme k est un multiple de p, alors* $k-1$ *n'en est pas un et le terme que nous avons mis de côté dans la seconde somme ne compte pas car sa valuation p-adique est nulle. Ainsi on a donc bien montré que* $v_p\left(\binom{1/2}{k}\right) \geq 0$.

L'hypothèse 4 permet de déduire l'expression de $F_p z$ à partir de celle de

$F_p y$ donnée précédemment. On pose :

$$F_p z = z^p (1 + pEz^{2p})^{-1/2} = z^p \sum_{k \geq 0} \binom{-1/2}{k} p^k E^k z^{2pk}.$$

On a ainsi étendu F_p à A_+^∞ et donc à A^∞. Il s'agit maintenant d'étendre F_p à $A^\dagger$.

Soit donc $a = \sum_{\substack{0 \leq i < d \\ j \in \mathbb{Z}}} a_{i,j} x^i y^j \in A^\dagger$. Alors on a :

$$F_p a = \sum_{i,j} \sigma(a_{i,j}) x^{pi} (F_p y)^j$$

où $(F_p y)^j = (F_p z)^{-j}$ si $j < 0$.

Remarque. 5.2.3. *L'élément $F_p a$ ainsi défini est bien un élément de $A^\dagger$. En effet on a $F_p y = y^p \sum_{k \geq 0} \binom{1/2}{k} p^k E^k z^{2pk}$. Comme $yz = 1$, la plus grande puissance de y apparaissant dans $F_p y$ est y^p (obtenue pour $k = 0$) et donc à j fixé, la plus grande puissance de y apparaissant dans $F_p a$ est y^{pj}. Ainsi si on montre que $\liminf_{|j| \to \infty} \frac{v_p(b_{i,j})}{p|j|} > 0$ où b_{ij} est le coefficient du terme en $x^{pi} y^{pj}$ de $F_p a$, on aura alors que $F_p a \in A^\dagger$.*
On a $b_{ij} = \sigma(a_{ij}) c_{ij}$ où c_{ij} fait intervenir des termes de la forme $\binom{1/2}{k} p^k E^k$ pour certaines valeurs de k. Or $\sigma(a_{ij}) = a_{ij}^p$ d'où $v_p(\sigma(a_{ij})) = p v_p(a_{ij})$, on a déjà montré dans la remarque 5.2.2 que $v_p\left(\binom{1/2}{k}\right) \geq 0$, $v_p(p^k) = k \geq 0$ et enfin par définition $v_p(E^k) = k v_p(E) \geq 0$ car E est dans $\mathbb{Z}_q[x]$. Ainsi $v_p(b_{ij}) \geq v_p(a_{ij})$.
On en conclut que $\liminf_{|j| \to \infty} \frac{v_p(b_{i,j})}{p|j|} \geq \liminf_{|j| \to \infty} \frac{p v_p(a_{i,j})}{p|j|} = \liminf_{|j| \to \infty} \frac{v_p(a_{i,j})}{|j|} > 0$.
Ainsi l'élément $F_p a$ construit précédemment est bien dans $A^\dagger$.

On a ainsi le relèvement du Frobenius F_p sur $A^\dagger$. Nous allons maintenant regarder son action sur l'espace de cohomologie $H^1_{dR}(C'^{-}_{\bar{Q}})$, ce qui va nous donner le polynôme $P_{\bar{Q}}$ que nous cherchons.
Comme l'espace de cohomologie est donné par une base explicite (voir la proposition 4.3.5), calculer l'action de F_q signifie calculer sa matrice dans

cette base. Le polynôme $P_{\bar{Q}}$ que nous voulons est alors le polynôme caractéristique.

5.3 Action sur la cohomologie

Pour finir il faut encore déterminer l'action sur H^1 du Frobenius que l'on vient de relever. Ce relèvement du Frobenius sur $A^\dagger$ induit un endomorphisme σ-linéaire sur le complexe de de Rham sur $A^\dagger$ et donc un endomorphisme σ-linéaire sur le $\mathbb{Q}_q$-espace vectoriel $H^1(C_{\bar{Q}})^-$. Or la proposition 4.3.5 nous donne une base explicite de cet espace. Donner l'action du Frobenius sur $H^1(C'_{\bar{Q}})^-$ revient donc à donner son action sur les éléments de la base. C'est ce que nous allons décrire.
Tout d'abord on a $F_p(dx) = d(F_p(x)) = d(x^p) = px^{p-1}dx$ et
$F_p(1/y) = 1/F_p(y) = F_p(y)^{-1}$. D'où :

$$F_p : x^i(dx)/y \mapsto px^{pi+p-1}y(F_py)^{-1}(dx)/y = px^{p(i+1)-1}y(F_pz)(dx)/y.$$

Dans ce qui précède on a donné une expression explicite de F_pz et on a (en utilisant yz=1) :

$$y(F_pz) = y^{-p+1}\sum_{k\geq 0}\binom{-1/2}{k}p^kE^ky^{-2pk}.$$

Ainsi l'action du Frobenius sur un élément de la base est donné par :

$$F_p(x^i(dx)/y) = \sum_{k\geq 0}\binom{-1/2}{k}p^{k+1}E^kx^{p(i+1)-1}y^{-(2k+1)p+1}.(dx)/y.$$

Cette expression n'est cependant pas encore celle que nous cherchons. On souhaite en effet une expression explicite dans la base donnée par la proposition 4.3.5.
Par définition de E, son degré est au plus $pd-1$. Ainsi le degré de $E^kx^{p(i+1)-1}$ est au plus $k(pd-1)+p(d-1)-1$ (car $i < d-1$). On utilise maintenant la relation existant entre y et Q, et donc entre y et x^d pour réécrire chaque terme de cette somme, en remarquant que $\dfrac{k(pd-1)+p(d-1)-1}{d} < (k+1)p$. On a $\forall k \geq 0$:

$$\binom{-1/2}{k}E^kx^{p(i+1)-1}y^{-(2k+1)p+1} = \sum_{-(2k+1)p<j<p} c_{i,k,j}y^j$$

où $c_{i,k,j}$ est un élément de $\mathbb{Z}_q[x]$ tel que $deg(c_{i,k,j}) < d$. D'où

$$F_p(x^i(dx)/y) = \sum_{\substack{k\geq 0 \\ -(2k+1)p<j<p}} p^{k+1} c_{i,k,j}.(dx)/y.$$

On utilise maintenant les lemmes 4.3.3 et 4.3.4 pour écrire l'élément $[F_p(x^i(dx)/y)]$ dans la base donnée par la proposition 4.3.5. On trouve :

$$[F_p(x^i(dx)/y)] = \left[\sum_{k\geq 0} p^{k+1} c'_{i,k}(dx)/y\right]$$

avec $c'_{i,k} \in \mathbb{Q}_q[x]$, $deg(c'_{i,k}) < d$ et $p^{m_k} c'_{i,k} \in \mathbb{Z}_q[x]$
où $m_k = max(\lfloor log_p((2k+1)p)\rfloor, \lfloor log_p(pd-2)\rfloor)$.

Cependant l'élément $F_p(x^i(dx)/y)$ n'est pas encore complètement réduit car il est possible qu'un terme $x^{d-1}(dx)/y$ apparaisse encore dans la formule. La dernière étape de la réduction fait intervenir une division par d. Si d n'est pas divisible par p alors la division par d donne un résultat entier et la matrice de l'action du Frobenius sur $H^1(C'_{\bar{Q}})$ est à coefficients dans $\mathbb{Z}_q$. Dans le cas contraire, soit $c''_{i,k} \in \mathbb{Q}_q[x]$ avec $deg(c''_{i,k}) < d-1$ tel que $[c'_{i,k}(dx)/y] = [c''_{i,k}(dx)/y]$. Alors :

$$[F_p(x^i(dx)/y)] = \left[\sum_{k\geq 0} p^{k+1} c''_{i,k}(dx)/y\right]$$

avec $c''_{i,k} \in \mathbb{Q}_q[x]$, $deg(c''_{i,k}) < d-1$ et $p^{m_k+v_p(d)} c''_{i,k} \in \mathbb{Z}_q[x]$.

On souhaite regarder la n-ième puissance de F_p agissant sur $H^1(C'_{\bar{Q}})^-$, c'est pourquoi il peut être utile de savoir si le $\mathbb{Z}_q$-module $\bigoplus_{\leq i<d-} \mathbb{Z}_q x^i(dx)/y$ est stable par F_p i.e. si la matrice de F_p dans la base décrite dans la proposition 4.3.5 est à coefficients dans $\mathbb{Z}_q$. Cela permettrait en effet de ne pas avoir à se préoccuper de la croissance des dénominateurs pendant le calcul de l'action de F_p^n. Cependant la plupart du temps, les coefficients de la matrice ne sont pas tous dans $\mathbb{Z}_q$. La proposition suivante, énoncée sans démonstration (celle-ci est rédigée dans l'article [1]), permet de ne pas se préoccuper du dénominateur.

Proposition. 5.3.1. *Soit t un paramètre au point ∞ à l'infini tel que $\beth t = -t$. Soit L le sous-$\mathbb{Z}_q$-module de $\bigoplus_{0\leq i<d-1} \mathbb{Z}_q x^i(dx)/y$ composé des éléments ω dont l'image dans $\frac{t^{-2g}\mathbb{Z}_q[[t]]dt}{t^{-1}\mathbb{Z}_q[[t]]dt}$ peut être intégrée i.e. les éléments qui sont dans l'image de*

$$d : \frac{t^{-2g+1}\mathbb{Z}_q[[t]]dt}{\mathbb{Z}_q[[t]]dt} \longrightarrow \frac{t^{-2g}\mathbb{Z}_q[[t]]dt}{t^{-1}\mathbb{Z}_q[[t]]dt}.$$

Alors l'action de F_p sur $H^1(C_{\bar{Q}'})^-$ laisse stable le $\mathbb{Z}_q$-module L. De plus il y a un isomorphisme

$$\frac{\bigoplus_{0\leq i<d-1} \mathbb{Z}_q.x^i(dx)/y}{L} \longrightarrow \bigoplus_{\substack{-(2g-1)\leq i<0 \\ i\equiv 1[2]}} \mathbb{Z}_q/i\mathbb{Z}_q,$$

et donc le quotient $\frac{\bigoplus_{0\leq i<d-1} \mathbb{Z}_q.x^i(dx)/y}{L}$ est tué par $p^{\lfloor log_p(2g-1)\rfloor}$.

Soit maintenant $e = (e_1, ..., e_{2g})$ une $\mathbb{Z}_q$-base de L et soit m la matrice de l'action de F_p sur L dans cette base. En d'autres termes, $F_p e_j = \sum_i m_{i,j} e_i$.

Remarque. 5.3.2. *La proposition 5.3.1 montre que m est à coefficients dans $\mathbb{Z}_q$.*

Comme F_p est σ-linéaire, on a pour $\lambda_j \in \mathbb{Z}_q$:

$$F_p \sum_j \lambda_j e_j = \sum_{i,j} \sigma(\lambda_j) m_{i,j} e_i.$$

Proposition. 5.3.3. *La matrice dans la base e de l'endomorphisme linéaire $F_q = F_p^n$ de $H^1(C'_{\bar{Q}})^-$ est donnée par :*

$$(matF_q)_e = m.(\sigma m)...(\sigma^{n-1} m).$$

Preuve. La démonstration se fait par récurrence sur n.
Soient a et b deux endomorphismes σ-linéaires d'un $\mathbb{Q}_q$-espace vectoriel V de base e. Montrons que $mat(ab)_e = (mat\, a)_e(\sigma(mat\, b))_e$.

$$ab(e_j) = a(b(e_j)) = a\left(\sum_i b_{i,j}e_i\right) = \sum_i \sigma(b_{i,j})a(e_i) = \sum_i \sigma(b_{i,j}) \sum_k a_{k,i}e_k$$

On a donc $ab(e_j) = \sum_k \left(\sum_i a_{k,i}\sigma(b_{i,j})e_k\right)$. D'où le résultat voulu. En prenant le cas particulier $a = b = F_p$ on a donc l'initialisation.
L'hérédité est tout aussi immédiate. Comme $F_p^n = F_pF_p^{n-1}$ en utilisant la propriété générale démontrée précédemment avec $a = F_p$ et $b = F_p^{n-1}$ et l'hypothèse de récurrence on a alors $(matF_p^n)_e = (matF_p)_e(matF_p^{n-1})_e$ et $(matF_p^n)_e = m.\sigma(m.(\sigma m)...(\sigma^{n-2}m)) = m.(\sigma m)...(\sigma^{n-1}m)$. □

Théorème. 5.3.4. *Le polynôme caractéristique de F_p^n sur le $\mathbb{Q}_q$-espace vectoriel $H^1(C'_{\bar{Q}})^-$ est le polynôme de $\mathbb{Z}[t]$*

$$P_{\bar{Q}} = \prod_{i=1}^{2g}(t - \alpha_i) = t^{2g} - a_1t^{2g-1} + ... - a_{2g-1}t + a_{2g}$$

du théorème 3.5. De plus $a_{2g-i} = q^{g-i}a_i$, $|a_i| \leq 2^{2g}q^{i/2}$.

Preuve. Le fait que P_f est le polynôme caractéristique de F_p est une conséquence de la formule du point fixe de Lefschetz appliquée dans le cadre de la cohomologie de Monsky-Washnitzer.
L'identité $\alpha_i\alpha_{g+i} = q$ découle de la dualité de Poincaré. Cela implique que $a_{2g-i} = q^{q-i}a_i$ avec les relations coefficients-racines du polynôme P_f.
Enfin on sait par la conjecture de Weil (voir le paragraphe 3) que $|\alpha_i| = q^{1/2}$. Cela nous permet d'établir le dernier résultat, $|a_i| \leq 2^{2g}q^{i/2}$. En effet

$$|a_i| = |\sum_{j_1<...<j_{2g}} \alpha_{j_1}...\alpha_{j_i}| \leq \sum_{j_1<...<j_{2g}} |\alpha_{j_1}...\alpha_{j_i}| = \binom{2g}{i}q^{i/2} \leq 2^{2g}q^{i/2}.$$

□

Ce théorème nous permet d'affirmer qu'il suffit de calculer les a_i pour $1 \leq i \leq g$ comme éléments de $\mathbb{Z}_q/p^N\mathbb{Z}_q$ où N est un entier choisi tel que $p^N > 2.2^{2g}.q^{g/2}$. On peut désormais passer à l'algorithme proprement dit.

6 L'algorithme de Kedlaya

6.1 Description de l'algorithme

L'algorithme que nous allons détailler dans ce qui suit prend en entrée les éléments suivants : un corps fini $\mathbb{F}_q$, défini par un nombre premier $p > 2$, un entier $n \geq 1$ et un polynôme unitaire $\bar{f} \in \mathbb{F}_p[x]$ de degré n, un entier impair $d = 2g + 1 \geq 1$ et un polynôme unitaire $\bar{Q} \in \mathbb{F}_q[x]$ de degré d tel que $\bar{Q} \wedge \bar{Q}' = 1$.
L'algorithme donne en sortie le polynôme $P_{\bar{Q}} \in \mathbb{Z}[t]$ donné dans le théorème 3.5.

6.1.1 Initialisation

La première étape consiste à relever $\bar{f}$ en $f \in \mathbb{Z}[x]$ en relevant ses coefficients dans $\{0, 1, ..., p-1\}$.
Notons $\mathbb{Z}_q = \mathbb{Z}_p[z]/(f)$. La seconde étape consiste à relever $\bar{Q}$ en $Q \in \mathbb{Z}_q[x]$ de la manière suivante :

$$Q = x^d + Q_{d-1}x^{d-1} + ... + Q_0$$

avec $Q_i = \sum_{0 \leq j < n} Q_{i,j} z^j \in \mathbb{Z}_q \in \mathbb{Z}_p 1 \oplus ... \oplus \mathbb{Z}_p x^{n-1}$, les $Q_{i,j}$ étant des éléments de $\{0, 1..., p-1\}$.
On pose

$$N = \lceil log_p(2^{2g+1} q^{g/2}) \rceil, \text{ tel que } p^N > 2^{2g+1}.q^{g/2},$$
$$N_1 = N + v_p(d) + \lfloor log_p(d - 2/p) \rfloor + \lfloor log_p(2g-1) \rfloor.$$

Enfin soit M le plus petit entier tel que $M - \lfloor log_p(2M+1) \rfloor \geq N_1$.

6.1.2 Calcul du Frobenius sur les différentielles

Ce qui suit utilise les résultats énoncés dans le paragraphe 5.3.
Pour $0 \leq i < d-1$ on calcule :

$$\sum_{0 \leq k < M} \binom{-1/2}{k} p^{k+1} E^k x^{p(i+1)-1} y^{-(2k+1)p+1} = \sum_{\substack{0 \leq k < M \\ -(2k+1)p < j < p}} p^{k+1} c_{i,k,j} y^j$$

comme élément de $\mathbb{Z}_q[x, y, y^{-1}]/(y^2 - Q) = \bigoplus_{\substack{0 \leq k < d \\ l \in \mathbb{Z}}} \mathbb{Z}_q x^k y^l$, avec une précision de N_1 chiffres, en d'autres termes modulo p^{N_1}.

Pour mémoire $E = \dfrac{F_pQ - Q^p}{p}$ et les $c_{i,k,j} \in \mathbb{Z}_q[x]$ sont de degré strictement inférieur à d.

6.1.3 Application de l'algorithme de réduction

On utilise l'algorithme de réduction donné dans la démonstration de la proposition 4.3.2 pour calculer :

$$\sum_{\substack{0\leq k<M \\ -(2k+1)p<j<p}} p^{k+1}c_{i,k,j}y^j.(dx)/y \equiv \tilde{\mathrm{m}}_i.(dx)/y,$$

avec $\tilde{\mathrm{m}}_i \in \mathbb{Z}_q[x]$ et $deg(\tilde{m}_i) < d-1$. On travaille ici avec N_1 chiffres à gauche de la virgule. Si une division par p est nécessaire, on décale simplement les chiffres d'une place vers la droite et on ajoute le nombre que l'on veut à gauche.
Soit $\tilde{m}$ la matrice dont les colonnes sont les $\tilde{m}_i$. C'est une matrice carrée de taille $2g$.
On calcule maintenant une $\mathbb{Z}_q$-base e du $\mathbb{Z}_q$-module L défini comme dans la proposition 5.3.1, avec une précision de N chiffres, et on calcule la matrice m de F_p dans la base e.

6.1.4 Calcul du polynôme caractéristique

On calcule maintenant $m' = m.(\sigma m)(\sigma^2 m)...(\sigma^{n-1}m) \in M_{2g}(\mathbb{Z}_q)$. Puis $det(t.I_{2g} - m) = P = t^{2g} + P_{2g-1}t^{2g-1} + ... + P_0 \in \mathbb{Z}_q[t]$.
Pour $1 \leq i \leq g$, soit a_i l'unique entier vérifiant $|a_i| \leq 2^{2g}q^{i/2}$ et tel que $a_i = (-1)^i P_i$ dans $\mathbb{Z}/p^N\mathbb{Z}$. Pour $g < i \leq 2g$ on pose $a_i = q^{i-g}a_{2g-i}$. Enfin on a :

$$P_{\bar{Q}} = t^{2g} - a_1t^{2g-1} + ... - a_{2g-1}t + a_{2g}.$$

6.2 Calcul de complexité

Tout d'abord on remarque que $N_1 = \mathrm{O}(gn)$, qu'un élément de $\mathbb{Z}_q/p^{N_1}\mathbb{Z}_q$ nécessite un espace de stockage en $\mathrm{O}(gn^2)$ et que toutes les opérations dans l'anneau $\mathbb{Z}_q/p^{N_1}\mathbb{Z}_q$ peuvent être réalisées en un temps $\mathrm{O}(g^{1+\epsilon}n^{2+\epsilon})$ en utilisant le procédé de multiplication d'entiers rapide.

Pour $0 \leq k < n$, la matrice de l'automorphisme σ^k de
$\mathbb{Z}_q/p^{N_1}\mathbb{Z}_q = (\mathbb{Z}_q/p^{N_1}\mathbb{Z}_q)[z]/(f)$ peut être calculée en un temps $\mathrm{O}(g^{1+\epsilon}n^{3+\epsilon})$ en effectuant le calcul dans $\mathbb{F}_q$, puis en relevant le résultat en utilisant la méthode de Newton.

On remarque que $M = \mathrm{O}(gn)$, $deg(E) = \mathrm{O}(g)$ et $d = deg(Q) = \mathrm{O}(g)$. L'étape 6.1.2 peut être effectuée en un temps $\mathrm{O}(g^{3+\epsilon}n^{3+\epsilon})$ et nécessite un espace de stockage en $\mathrm{O}(g^3n^3)$. En fait cette étape consiste à calculer un polynôme de degré $\mathrm{O}(g^2n)$ en x et à l'écrire comme un polynôme en Q à coefficients de degré strictement inférieur à d.

Pour l'étape 6.1.3 il n'y a pas besoin d'espace de stockage supplémentaire et le calcul peut être effectué en un temps $\mathrm{O}(g^{4+\epsilon}n^{3+\epsilon})$. En effet il nous faut réduire g formes, chacune nécessitant $M = \mathrm{O}(gn)$ multiplications par $(Q')^{-1}$ dans $\mathbb{Z}_q[x]/(Q, p^N)$.

Enfin l'étape 6.1.4 ne nécessite pas d'espace de stockage supplémentaire et peut être effectuée en un temps $\mathrm{O}(g^{4+\epsilon}n^{2+\epsilon}) + \mathrm{O}(g^{3+\epsilon}n^{3+\epsilon})$. On calcule $m' = m.(\sigma m)(\sigma^2 m)...(\sigma n - 1m)$ de la manière suivante : $m_1 = m.(\sigma m)$, $m_2 = m_1.(\sigma^2 m_1)$, etc. De cette manière, on effectue $\mathrm{O}(log\, n)$ multiplications de matrices carrées de taille $2g$, à coefficients de taille gn^2, et $\mathrm{O}(g^2 log\, n)$ applications d'une certaine puissance de σ. Enfin on calcule le polynôme caractéristique de m' en choisissant un élément v et en calculant les vecteurs v, $m'v$, $(m')^2v$,... jusqu'à ce que ceux-ci soient linéairement dépendants. Cela nécessite $\mathrm{O}(g^3)$ opérations.

L'étape dominante de cet algorithme est l'étape de réduction. Le temps total d'exécution est $\mathrm{O}(g^{4+\epsilon}n^{3+\epsilon})$ et il nécessite un espace de stockage en $\mathrm{O}(g^3n^3)$.

7 Remerciements

Je remercie tout d'abord ma directrice de mémoire, Christine Huyghe, pour la disponibilité et la patience dont elle a fait preuve à mon égard. J'ai bénéficié d'excellentes conditions d'encadrement et je ne l'en remercierai sans doute jamais assez.

Je souhaite également remercier Nathalie Wach qui a bien voulu consacrer un peu de son temps à m'aider à préparer ma soutenance.

Je tiens à remercier Fabienne Grauss sans qui ma scolarité à l'UFR aurait sans doute été bien plus stressante. Pour votre optimisme, votre sympathie et votre volonté de nous aider contre vents et marées, merci beaucoup.

Enfin je remercie mes camarades de M2 avec lesquels j'ai passé une année agréable et plus particulièrement Charlotte Debargue, Olivier Duong, Thomas Richez et Audrey Vonseel grâce à qui cette année parfois difficile s'est déroulée dans la bonne humeur.

Références

[1] Bas Edixhoven. Point counting after Kedlaya, EIDMA-Stieltjes graduate course, Leiden. September 22-26, 2003.

[2] Qing Liu. Algebraic geometry and arithmetic curves.

[3] Robin Hartshorne. Algebraic geometry.

[4] Neal Koblitz. p-adic numbers, p-adic analysis, and zeta-functions. *Seconde édition*.

[5] P. Monsky and G. Washnitzer. Formal cohomology : I. *The annals of mathematics*, Vol. 88 :181–217, September 1968.

[6] P. Monsky. Formal cohomology : II. the cohomology sequence of a pair. *The annals of mathematics*, Vol. 88 :218–238, September 1968.

[7] P. Monsky. Formal cohomology : III. fixed point theorems. *The annals of mathematics*, Vol. 93 :315–343, Mars 1971.

[8] Kiran S. Kedlaya. Counting Points on Hyperelliptic Curves using Monsky-Washnitzer Cohomology. November 20, 2001.