UNIVERSITÉ CHEIKH ANTA DIOP

École Doctorale Mathématiques et Informatique

N^0 d'ordre : · · · ·

THÈSE DE DOCTORAT UNIQUE

Mention : **Mathématiques et Modélisation**

Spécialité : **Codage, Cryptologie, Algèbre et Applications**

RELÈVEMENT CANONIQUE DE SURFACES ABÉLIENNES

Présentée et soutenue le 24 Juin 2022
par

ABDOULAYE MAÏGA

Pour obtenir le grade de

Docteur de l'Université Cheikh Anta Diop de Dakar

COMPOSITION DU JURY:

Président:	Cheikh Tiécoumba GUEYE	Prof. Titulaire CAMES	UCAD, Sénégal
Rapporteurs:	Jean-Marc COUVEIGNES	Prof. Titulaire des Universités	Univ. de Bordeaux, France
	Omar KIHEL	Prof. Titulaire	Univ. de Brock, Canada
Examinateurs:	Abdoul Aziz CISS	Maître de Conférence CAMES	EPT de Thiès, Sénégal
	Amadou Lamine FALL	Maître de Conférence CAMES	UCAD, Sénégal
	Ismaïla DIOUF	Maître de Conférence CAMES	UCAD, Sénégal
Directeurs de thèse:	Djiby SOW	Prof. Titulaire CAMES	UCAD, Sénégal
	Damien ROBERT	Prof. Titulaire (HDR)	Univ. de Bordeaux, France

À ma mère, ma maman,
À madame MAÏGA Kouthoum TANDINA.
À l'enseignante spéciale, celle qui m'a appris les opérations de divisions entre les nombres entiers depuis les petites classes au primaire. 🍃🍃🍃

À toutes ces merveilleuses personnes: père , frères et sœurs, amis et collaborateurs qui m'ont soutenu pendant ces moments remplis d'expériences inoubliables. 🍃🍃🍃

Dakar-SENEGAL
24 Juin 2022 – classicthesis v4.6

ABSTRACT

Let $\mathcal{M}_2(\mathbb{F}_q)$ be the moduli space of the genus 2 curves defined over $\mathbb{F}_q$. We first compute modular polynomials with good reduction in any characteristic using Igusa's arithmetic invariants. Using the Kronecker condition on these modular polynomials, we give a method to compute the canonical lift of any ordinary genus 2 curves over $\mathbb{F}_q$. Let p be a prime and $\mathfrak{A}_{g,\Gamma_0(p)}$ be the Siegel moduli space with $\Gamma_0(p)$-level structure. We give the general statement of the *Kronecker conditions* on the ordinary locus of $\mathfrak{A}_{g,\Gamma_0(p)}$, which extends the well known result in dimension 1 under the same name. We extend the computation of the canonical lift to several types of invariants (Theta invariants and Gundlach invariants). In each case, we introduced a Newton method for lifting the Verschiebung over $\mathbb{Z}_q$. Using these results, we give an algorithm to compute the characteristic polynomial of genus 2 curves in quadratic time complexity using Siegel polynomials and Hilbert polynomials. Further one can use these methods to lift modular forms associated to genus 2 curves.
In other hand we propose a new method for computing the canonical lift in general without modular polynomial, and in dimension 1 we succed to reduce efficiently these computations to $\widetilde{O}(pn^2)$. We give a detailed description with the necessary optimizations for an efficient implementation.

Keywords: Abelian variety, Arithmetic invariants of genus 2 curves, Modular polynomials, Canonical lift, Point counting.

RÉSUMÉ

Nous avons calculé des polynômes modulaires en dimension 2 avec bonne réduction en toute caractéristique en fonction des invariants arithmétiques d'Igusa. En utilisant les conditions de Kronecker sur ces polynômes modulaires, nous donnons une méthode pour calculer le relevé canonique de toute courbe ordinaire de genre 2 en caractéristique paire. Soient p un nombre premier et $\mathfrak{A}_{g,\Gamma_0(p)}$ l'espace de module de Siegel des variétés abéliennes, muni d'une structure de niveau $\Gamma_0(p)$. Nous avons établi l'énoncé des *conditions de Kronecker* sur le lieu $\mathfrak{A}^{(0)}_{g,\Gamma_0(p)}$ des points ordinaires de $\mathfrak{A}_{g,\Gamma_0(p)}$; cette propriété généralise le résultat bien connu en dimension 1 sous le même nom. D'un autre côté, nous avons introduit des méthodes de Newton pour calculer le relevé du Verschiebung sur $\mathbb{Z}_q$ dans chaque cas. Ces résultats nous ont permis de déterminer le polynôme caractéristique d'une courbe de genre 2 en $\widetilde{O}(n^2)$ opérations sur $\mathbb{F}_p$, en utilisant des polynômes de Siegel et des polynômes de Hilbert en fonction des invariants Thêta et invariants de Gundlach. En outre, on peut utiliser ces méthodes pour calculer les formes modulaires (vectorielles) associées à ces courbes.
Nous avons réduit considérablement les complexités dans les calculs de relevé canonique en proposant des méthodes qui n'utilisent pas de polynômes modulaires et en dimension 1 nous proposons un algorithme qui calcule le relevé canonique en $\widetilde{O}(pn^2)$. Nous donnons une description détaillée avec les optimisations nécessaires pour des implémentations éfficaces.

Mots-clés: Variétés Abéliennes, Invariants arithmétiques en genre 2, Polynômes Modulaires, Relèvement Canonique, Comptage de Points.

REMERCIEMENTS

Par la Grâce du Tout Miséricordieux, qui m'a donné du temps, et une bonne santé pour aborder ces travaux de recherches doctorales, je suis très reconnaissant envers toutes les personnes et toutes collaborations qui m'ont assisté pendant ces années fastidieuses. Je m'en vais à travers ces quelques lignes exprimer ce qui m'est revenu en mémoire au moment où j'écrivais cette page. Ces mots ne pourront pas exprimer toute ma réconnaissance et les bénéfices de mes expériences vécues: que l'on me pardonne l'omission du nom de certaines merveilleuses personnes.

Je remercie sincèrement mes deux co-directeurs Djiby Sow et Damien Robert qui m'ont donné une opportunité de m'épanouïr scientifiquement dans l'un des domaines des mathématiques les plus en vu de notre siècle. Les rencontres avec ces deux chercheurs ont changé ma façon de regarder les mathématiques. Je suis très reconnaissant envers Marie Francoise Roy, David Lubicz et Emmanuel Fouotsa qui m'ont permis de rencontrer Damien Robert à Rennes: une très belle opportunité ! Son exigeance au travail m'a permis d'aller très loin aussi bien dans la lecture que dans les idées et la rédaction: sa manière de faire des mathématiques est, véritablement, une source d'inspiration pour moi. Je le remercie chaleuresement d'une part pour ce sujet fascinant et d'autre part pour avoir écouté puis répondu avec patience et gentillesse, à toutes les questions que j'ai pu lui poser durant ces années.

Il me faut également remercier Jean-Marc Couveignes et Omar Kihel pour avoir accepter d'être mes rapporteurs. Je les suis redevable pour leur lecture très attentive de ma thèse.

J'exprime ma profonde gratitude à tous les membres du jury : son président Cheikh Thiécoumba Guèye et les examinateurs Abdoul Aziz Ciss, Ismaïla Diouf et Amadou Lamine Fall pour l'honneur qu'ils me font en acceptant de sièger dans le jury de cette thèse.

À travers mes travaux de recherches doctoriales, j'ai courtoiyé plusieurs groupes de chercheurs desquels je garde des bénéfices et de très bons souvenirs. Je remercie tous les membres du laboratoire LACGAA de Dakar à travers son fondateur Pr. Mamadou Sangharé et les responsables Pr. Cheikh T. Gueye et Pr. Oumar Diankha: j'ai trouvé les séminaires très intéressants. Je remercie très particulièrement tous les membres de l'équipe ASCII dirigée par Pr. Djiby Sow où j'ai bénéficié d'un bon cadre de travail (avec des échanges très animés...) sous l'assistance de Boubacar Sow et dans le voisinage de Aminata Ngom, Guy Wamba, Michel Seck, Mohamadou et Moussa Sall, Yatma Diop, Soda Diop, Sakha, Clément et Sidouane. Mes remerciements s'adressent aussi au Département Mathématiques Informatique de la FST- UCAD dirrigé en ma présence successivement par les professeurs Mamadou Barry et Ismaïla Diouf: Merci à Fatou Kiné et Gnima Camara.

J'ai fait plusieurs séjours scientifiques à l'IMB de Bordeaux financés par le projet FAST-LIRIMA et ANR-CIAO. Je remercie l'IMB et l'INRIA de Bordeaux pour l'accueil dans de très bonnes conditions de travail: Merci à Sabrina Blondel Duthil ! Pendant ces séjours j'ai profité d'un côté de l'assistance technique de Bill Allombert et Enea Millio sur les outils pari-gnump.multiprecision de PARI/GP et PlaFRIM et d'un autre côté de discussions très animées (surtout pendant la pause-thé du jeudi soir) avec les membres de l'équipe LFANT.

```
{ ssh plafrim-ext
  cp resamiriel resamiriel-long
        sinfo|less }
```

Je remercie chaleuresement mon père Abdou-Kader, ma mère Kouthoum Tandina, ma sœur Fatim, ma Diata 🕊, ma petite Dina 🕊, mon frère Alassane depuis Sikasso (Mali), Mme Sow Fatima Gaye à Keur-Massar, Mme Ciss Aminata Diallo à Thiès, maman Aminata Faye à Médina, mes amis Ahmed Maïga et Mamadou Pouye pour leur soutien moral et leurs bénédictions.

Enfin, je rends un vibrant hommage aux professeurs Niamanto Diarra, Karim Samaké, Gana Blaise Togo et feu Moustaphe Soumaré qui m'ont beaucoup encouragé et ont nourri mes intérêts pour les Mathématiques et en particulier pour l'Algèbre depuis mes débuts à la FAST de l'Université de Bamako.

... Dieure Dieuff ... Yalnala yAllah sameu ...

- Alhamdoulilah Rabbi alAAalamine -

We have seen that computer programming is an art,
because it applies accumulated knowledge to the world,
because it requires skill and ingenuity, and especially
because it produces objects of beauty.

Donald E. Knuth

En mathématiques*, on ne comprend pas les choses, on s'y habitue.*

John Von Neumann

Le Savoir est une perception argumentée de La Vérité.

Abdoulaye MAÏGA

Ce document est produit à l'aide de LaTeX, de la classe KOMA-Script avec des packages additionels biber/biblatex, cleveref, hyperref, mathtools, ntheorem, tikz. Le style est repris des packages classicthesis v4.6 .

Dakar-SENEGAL
24 Juin 2022 – classicthesis v4.6

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ALGORITHMES

LISTE DES EXEMPLES ALGORITHMIQUES

NOTATIONS ET CONVENTIONS

— $\Bbbk$ et $\mathbb{K}$ corps commutatifs quelconques.

— $|\cdot|_p$ et ord_p la norme et la valuation p-adique ;

— $\mathbb{Q}_p$ le corps des nombres p-adique et $\mathbb{Z}_p$ son anneau de valuation ;

— $W(\mathbb{F}_q)$ l'anneau des vecteurs de Witt sur $\mathbb{F}_q$;

— $\mathbb{Q}_q$ l'extension non-ramifiée (à isomorphisme près) de $\mathbb{Q}_p$ et $\mathbb{Z}_q$ son anneau de valuation ;

— La p-ième puissance du Frobenius σ et $\hat{\sigma} = \sigma^{-1}$ sur le corps résiduel $\mathbb{F}_q$;

— Σ et $\hat{\Sigma}$ sont les rélévés de σ et $\hat{\sigma}$ dans le groupe de Galois $\mathrm{Gal}(\mathbb{Q}_q/\mathbb{Q}_p)$;

— $\mathbb{Z}_q^{ur}$ l'extension non-ramifiée maximale de $\mathbb{Z}_q$;

— π et $\hat{\pi}$ sont respectivement le p-isogénie du Frobenius et son dual le "petit" Verschiebung ; Π et $\hat{\Pi}$ sont respectivement leur relevé sur $\mathbb{Z}_q$;

— $\tilde{\mathcal{A}}$ le rélévé d'une variété $\mathcal{A}$;

— $\mathcal{A}[n]$ le groupe de n-torsion d'une variété $\mathcal{A}$;

— Φ_p le système de polynômes modulaires de niveau p ;

— Ψ_p polynôme de p-division sur une courbe elliptique ;

— $\tilde{x}$ le relevé d'un élément x de $\mathbb{F}_q$;

— DF la matrice Jacobienne du système polynômial F ;

— HF la matrice Hessienne de F ;

— $\mathrm{SNF}(S)$ la Forme Normale de Smith d'un système polynomial S ;

— $\mathcal{M}_g$ le schéma de module des courbes de genre g ;

— $\mathfrak{A}_g$ l'espace de module de Siegel en dimension g ;
— $\mathfrak{H}_g$ le demi-espace de Siegel en dimension g ;
— $\mathbb{A}^k$ l'espace affine de dimension k ;
— Γ_g le groupe simplectique en dimension g ;
— $\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}$ la fonction trace sur l'extension $\mathbb{Q}_q/\mathbb{Q}_p$;
— $N_{\mathbb{Q}_q/\mathbb{Q}_p}$ la fonction norme sur l'extension $\mathbb{Q}_q/\mathbb{Q}_p$;

INTRODUCTION

INTRODUCTION

Dans un monde hyper-connecté et dominé par les échanges d'informations, l'importance de sécuriser ces flux devient très evidente pour le commun des humains. Au-cours de leurs évolutions ces protocoles ont utilisé et utilisent des outils mathématiques diverses, certains plus simples et d'autres très sofistiqués. La Cryptographie Asymétrique est la branche de la cryptographie qui fournit des protocoles d'échange de clés à distance. Elle utilise depuis plusieurs décennies des protocoles comme RSA basé sur la difficulté de la factorisation des entiers naturels et d'autre comme le protocole Diffie-Helmann qui utilise des problèmes comme le Logarithme Discret sur les corps finis. Le dévéloppement des outils et techniques de *Gros Calculs* imposèrent l'exploration d'autres bases mathématiques pour la réalisation des protocoles cryptographiques.

Les améliorations des Schémas cryptographiques et l'évolution de la Cryptographie à Clés Publiques ont influencé jusqu'à nos jours, l'orientations des Recherches sur Variétés Abéliennes surtout en Géométrie Algébrique et en Théorie des Nombres. Ces résultats sont d'autant plus importants en Théorie Algorithmique des Nombres.
Les Variétés Abéliennes sont devenues des outils mathématiques plus populaires depuis leur introduction progréssive dans la Cryptographie à Clés Publiques à partir 1985 par N. Koblitz [63] et V. Miller [80]. En effet en Dimension 1, la Théorie sur les Courbes Elliptiques fournissait les outils nécéssaires à la réalisation d'un Échange de Clés basé sur le Problème du Logarithme Discret (DLP). Par comparaison aux groupes des unités de corps finis, les algorithmes de résolution du Problème du Logarithme Discret sur les courbes elliptiques avaient des complexités plus intéréssantes pour la Cryptographie [37, 63, 80].

En plus de servir de groupe pour la réalisation des crystosystèmes utilisés actuellement sur le marché industriel de sécurité des informations, les variétés abéliennes à travers leur espace de module sont de potentielles candidates pour la standarisation de cryptosystème postquantique. En effet l'algorithme quantique de Shor résoud en temps polynomial le Problème du Logarithme Discret sur les groupes abéliens. Dès lors, l'espace de module des variétés abéliennes est devenu une alternative très intéressante en cryptographie postquantique. En effet il est montré par des auteurs comme Couveignes que cet espace est un excellent générateur de *graphes de Schreier* pour la réalisation d'un protocol "*Diffie-Hellman*". Dans les meilleurs cas (cas supersingulier) ces graphes sont de *Ramanujan* (aller à [20, 22, 30] pour plus de details).
Et très récemment des cryptosystèmes postquantiques sont élaborés sur les espaces de modules de variétés abéliennes en dimension 1 (et superieures) avec des propriétés très intéréssantes pour la sécurité des informations [54].

Le but de cette thèse est de réaliser des algorithmes de calcul de rélèvés canonique sur l'espace de module des surfaces abéliennes ordinaires en utilisant des invariants absolus adaptés et utiliser ces rélévés pour calculer en petites caractéristiques des formes modulaires vectorielles et le polynôme caractéristique des courbes ordinaires de genre 2*, qui sont des éléments éssentiels en Théorie des Nombres, en Cryptographie et en Théorie de Codes Correcteurs d'Erreurs.*

Pendant plusieurs siècles les recherches sur les Variétés Abéliennes nourrissent nos connaissances sur certaines vieilles conjectures notament en Théorie des Nombres et Géométrie Algébrique et plus récemment en Géométrie Arithmétique. On peut entre autre citer le *Dernier Théorème de Fermat* et *l'Hypothèse de Riemann*. Les résultats sur l'étude des variétés abéliennes sont aussi des outils essentiels dans les recherches sur *les Systèmes Dynamiques*. Dès lors des contributions majeures fûrent apportées à leurs études sur plusieurs angles par plusieurs chercheurs comme Riemann, Weierstrass, Frobenius, Poincaré, Picard etc...Il faut attendre André Weil dans les années 1940 pour voir les formalismes actuels sur les variétés abéliennes en language de la Géométrie Algébrique.

0.0.1 *Variétés Abéliennes*

Une variété abélienne sur un corps $\Bbbk$ parfait est un groupe algébrique lisse sur $\Bbbk$ complet et connexe. Dès lors, on montre qu'elles sont projectives et que leur loi de groupe est définie par des fonctions régulières. Une manière simple de construire de telles classes d'objets est de considérer les Jacobiennes de courbes sur $\Bbbk$. Soit $\mathcal{C}$ une courbe algébrique sur $\Bbbk$ de genre g, on appelle Jacobienne $\mathrm{Jac}(\mathcal{C})$ de $\mathcal{C}$ l'ensemble des g-uplets de points de $\mathcal{C}$ représentant des classes d'équivalences de points géométriques de $\mathcal{C}$ appelés *diviseurs* sur $\mathcal{C}$. Alors le nombre g est la dimension de la variété abélienne $\mathrm{Jac}(\mathcal{C})$.
De plus lorsque l'on considère $\mathcal{C}$ hyperelliptique c'est-à-dire que $\mathcal{C}$ peut être définie dans $\mathrm{Spec}(\Bbbk[x,y])$ par une équation (appelée *modèle hyperelliptique de* $\mathcal{C}$) de la forme:

$$y^2 + h(x)y = f(x)$$

avec $f \in \Bbbk[x]$ de degré $2g+1$ ou $2g+2$. À partir de la représentation de Mumford et de la réduction de Cantor on décrit chaque élément de la Jacobienne $\mathrm{Jac}(\mathcal{C})$ par un unique diviseur (appelé *forme normale de Cantor*) de la forme:

$$\sum_{i=1}^{d} (P_i - P_\infty)$$

$$\text{avec } \; d \leq g \;\; P_i \in \mathcal{C}(\bar{\Bbbk}), \; P_i \neq P_j, \; P_\infty \text{ pour tous } 1 \leq i,j \leq d.$$

On peut aussi repésenter les diviseurs sous forme normale de Cantor par des couples (u,v), où u est un polynôme unitaire de degré d et v un polynôme tel que $\deg(v) < \deg(u)$ et $u \mid (f - v^2)$. Ces représentations ont permit l'élaboration d'algorithmes d'addition dans le groupe $\mathrm{Jac}(\mathcal{C})$ (aller à [9, 64] pour plus de détails).

Une isogénie (séparable) entre deux variétés abéliennes est un morphisme (séparable) surjectif et de noyau fini. Un morphisme de variétés abéliennes est à la fois un morphisme de variétés et un morphisme de groupes. Le cardinal du noyau de l'isogénie (séparable) entre deux variétés abéliennes est appelé son degré, alors ces variétés seront dites *p-isogènes* lorsque ce cardinal est nombre premier p.
Lorsque nous considerons $\mathbb{C}$ comme corps de base, une variété abélienne complexe est un tore complexe muni d'un plongement dans un espace projective associé à l'existence d'un morphisme appelé *polarisation*. Dans le cas où la polarisation est un isomorphisme on dit que la variété abélienne est principalement polarisée. Le théorème d'Abel-Jacobi [3, thm 11.1.3] établit que toute Jacobienne $\mathrm{Jac}(\mathcal{C})$ de courbe hyperelliptique sur $\mathbb{C}$ de genre g est canoniquement isomorphe à une variété abélienne principalement polarisée $\mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$

de dimension g où $\Omega \in \mathfrak{H}_g = \left\{\Omega \in M_g(\mathbb{C}),\ {}^t\Omega = \Omega,\ Im(\Omega) > 0\right\}$; on appelle Ω matrice de période de la courbe et $\mathfrak{H}_g$ l'espace de Siegel. En dimension inférieure ou égale à 2 et dans le cas où la polarisation est indécomposable, la réciproque de cette assertion est vraie [3, cor 11.8.2].
On définit *l'espace modulaire de Siegel des variétés principalement polaisées* par $\mathrm{Sp}_{2g}(\mathbb{Z})\backslash\mathfrak{H}_g$, elle fournit en dimensions ≤ 2 des outils de tests pour les varétés p-isogènes. En effet on utilise un paramétrage à partir de polynômes de l'espace des variétés abéliennes p-isogènes appelés *polynômes modulaires*. Et sur ces espaces, les variétés abéliennes sont *représentées à isomorphisme près* par des *invariants* qui sont fournis par des *formes modulaires*.
Cette notion a pris une grande importance du point de vue algorithmique lorsque qu'elle fût utilisée pour améliorer les algorithmes de comptage de points de variétés et aussi pour transférer le Problème de Logarithme Discret d'une variété abélienne à une autre où il est plus simple à résoudre.

0.0.2 *Espace de Module des Courbes de Genre* 2

La Théorie des Invariants joue un rôle fondamental dans l'étude des variétés abéliennes depuis le 19$^{\text{ième}}$ siècle. Cependant elle connait une renaissance à partir d'importantes utilisations motivées par des applications algorithmiques en cryptographie, robotique, théorie des codes correcteurs d'erreurs etc...
En considerant les *actions linéaires* de certains groupes classiques comme $GL_2(\bar{\Bbbk})$ sur les formes binaires comme dans la *Théorie des Invariants Algébrique d'Hilbert*, Clebsh [16] établit une étude des invariants et covariants associés aux équations de courbes de genre 2 en caractéristiques différentes de 2. En utilisant une opération appelée "*Ueberschiebung*" Clebsh donna une évaluation des *invariants algébriques* $A,\ B,\ C,\ D$ qui forment une base de l'anneau gradué des invariants pairs des courbes genre 2 en caractéristiques différentes de 2 et 3. Ces invariants suffisent alors à la caractérisation des classes d'isomorphismes pour ces caractéristiques. Lorsque $y^2 = f(x)$ (avec $\deg f = 6$) est le modèle hyperelliptique réduit d'une courbe de genre 2 en caractéristiques différentes de 2, J.S. Igusa définit des invariants en fonctions des racines de f. Ces derniers invariants notés $I_2,\ I_4,\ I_6$, et I_{10} sont équivalents à ceux de Clebsh lorsque la caractéristique différente de $2, 3$ et 5 d'où leur nom: *invariants d'Igusa-Clebsh* [51, 52]. En caractéristique 3 ils sont bien définis mais ne permettent pas une classification des courbes de genre 2.
D'une autre part sur $\mathbb{C}$, les actions de $\mathrm{Sp}_4(\mathbb{Z})$ sur l'espace $\mathfrak{H}_2$ des matrices de périodes de surfaces abéliennes complexes conduisent à la définition des *invariants absolus* qui sont des formes modulaires de degré zéro appelées *fonctions modulaires*. Plus généralement sous certaines conditions les principes de Koecher permettent d'établir une équivalence entre les covariants (rationnels en fonction des coéfficients des courbes) et les forme modulaires méromorphes de même poids (pour plus de détails voir [98, §3.2]).
Enfin en caractéristique 2 nous avons la construction d'Artin-Schreier d'une courbe de genre 2 que J.S. Igusa [51, §2] utilisa pour étendre les *invariants algébriques* I_{2i}'s aux *invariants arithmétiques* J_{2i}'s lesquels ont une bonne reduction en toute caractéristique. En utilisant à la fois l'action du groupe d'Artin-Schreier et le groupe projectif linéaire PGL_2, G. Cardona et autres ont introduit des classes d'invariants spécifiant les mêmes classes d'isomorphisme pour les courbes de genre 2 [33].

En général l'espace de module des courbes de genre 2: $\mathcal{M}_2$ (consideré au sens "coarse" ou au sens "stack") est de dimension 3. En caractéristique différente de 2 son corps de fonctions est engendré par les invariants absolus d'Igusa j_1, j_2 et j_3 ou par équivalence birationelle ceux de Streng ou autres... À partir d'un triplet de ces invariants l'algorithme de J.F. Mestre construit un model hyperelliptique d'une courbe $\mathcal{C}$ de genre 2 dont les invariants correspondent au triplet, mais cette construction n'admet pas une bonne réduction pour les caractéristiques inférieures ou égales à 5.
Sur $\mathbb{C}$, les classes d'isomorphismes des variétés Jacobiennes génériques de courbes de genre 2 sont données par des triplets de fonctions modulaires (j_1, j_2, j_3) (les invariants d'Igusa). Lorsque p est un nombre premier, les polynômes modulaires encodent les surfaces abéliennes (p, p)-isogènes en fonction des invariants d'Igusa. Plus précisement un model birationel de l'espace de module (en coarse) $\mathfrak{A}_2(p) = \mathfrak{H}_2/\Gamma^0(p)$ est donné par $\mathbb{C}(\mathfrak{A}_2(p)) = \mathbb{C}(j_1, j_2, j_3, j_{1,p}, j_{2,p}, j_{3,p})$ où $j_{i,p} = j_i(\tau/p)$. Alors les polynômes modulaires de niveau p sont définis comme suite: $\phi_{1,p}(X)$ est le polynôme minimal de $j_{1,p}$ sur $K = \mathbb{C}(\mathfrak{A}_2) = \mathbb{C}(j_1, j_2, j_3)$, et $j_{2,p} = \phi_{2,p}(j_{1,p})$, $j_{3,p} = \phi_{3,p}(j_{1,p})$ pour $\phi_{2,p}(X)$ et $\phi_{3,p}(X)$ polynôme unitaire dans $\mathbb{C}(j_1, j_2, j_3)[X]$ de degré inférieurs à $\deg(\phi_{1,p}(X))$. Lorsque x parcours les racines de $\phi_{1,p}(X)$ sur $\mathbb{C}$, alors $(x, \phi_{2,p}(x), \phi_{3,p}(x))$ sont les j-invariants absolus des surfaces abéliennes principallement polarisées (p, p)-isogènes à celle définie par les invariants (j_1, j_2, j_3) . Ainsi le lieu schématique des p-polynômes modulaires en dimension 2:

$$\begin{cases} \phi_{1,p}(X_1, X_2, X_3, Y_1) = 0, \\ Y_2 = \phi_{2,p}(X_1, X_2, X_3, Y_1) \\ Y_3 = \phi_{3,p}(X_1, X_2, X_3, Y_1) \end{cases}$$

décrit un modèle birationnel de $\mathfrak{A}_2(p)$.
Le calcul de ces polynômes a été initié par R. Dupont dans sa thèse de Doctorat [28]. Des améliorations fûrent proposées par d'autres auteurs comme dans [7] et plus recemment ces calculs ont été étendus à d'autre invariants [78]. Et les invariants théta $\mathfrak{b}_1$, $\mathfrak{b}_2$ et $\mathfrak{b}_3$ qui sont des fonctions modulaires pour le sous groupe $\Gamma(2, 4)$ fournissent les polynômes plus petits en taille, mais tous ces différents polynômes pour $\mathfrak{A}_2$ deviennent vite impraticables après $p = 5$ car leurs degrés en fonctions de ces invariants et leurs coefficients grandissent très rapidement.
Cependant des alternatives se présentent sur l'espace modulaire de Hilbert défini par $\mathrm{SL}_2(\mathcal{O}_K)\backslash\mathfrak{H}_1^2$. Lorsque l'on considère un ordre quadratique réel maximal de discriminant Δ_K, alors $\mathrm{SL}_2(\mathcal{O}_K)\backslash\mathfrak{H}_1^2$ décrit les classes d'isomorphismes des surfaces abéliennes principalement polarisées avec multiplication réelle par $\mathcal{O}_K$. De plus le plongement de Hilbert de $\mathfrak{H}_1^2$ dans $\mathfrak{H}_2$ fournit des coordonnées rationnelles des *surfaces Humbert* (images de ces plongements) en fonction des invariants de Gundlach ou sur un recouvrement des surfaces de Humbert en fonction des invariants théta. Lorsque le discriminant $\Delta_K = 2$, 3 ou 5 ce paramétrage permet de calculer les β-polynômes modulaires (pour $\beta = \ell$ un premier et pour β un élément totalement positif de norme ℓ) [79]. Ces polynômes sont très pratiques jusqu'à des premiers inférieurs à 100 (voir https://members.loria.fr/EMilio/modular-polynomials/).

0.0.3 *Relèvement Canonique des Variétés Ordinaires*

La Théorie du *Relèvement des variétés abéliennes* a pris depuis la deuxième moitié du 20$^{\text{ième}}$ siècle une considération très importante en Géométrie Algébrique. Ces interêts sont très souvent motivés par les nombreuses propriétés qu'offrent les différents espaces de module

sur $\mathbb{Z}_p$. Et plus particulièrement l'une des approches pour définir la cohomologie de Weil sur une variété $\mathcal{A}$ définie sur un corps $\Bbbk$ de caractéristique p est de le réléver sur l'anneau des vecteurs de Witt $W(\Bbbk)$(en caractéristique nulle) puis prendre la cohomologie de De Rham de la variété rélévée se réduisant bien sur $\mathcal{A}$ modulo p. Dans le cas *ordinaires* ce rélévé est unique et donné par le *relèvement canonique*. Et par le *Théorème de Serre-Tate* la théorie de déformation d'une variété abélienne $\mathcal{A}$ et celle de ses sous-groupes $\mathcal{A}[p^\infty]$ sont équivalentes (aller à [55] pour une dissertation détaillée). En outre comme montre les P. Norman et F. Oort [15, 90] la théorie de la déformation $\mathcal{A}[p^\infty]$ donne assez d'informations sur l'espace de module des variétés abéliennes.

Ainsi pour toute variété abélienne ordinaire $\mathcal{A}/\mathbb{F}_q$ (avec $q = p^n$), il existe une variété abélienne unique $\tilde{\mathcal{A}}$ sur $\mathbb{Z}_q$ telle que la réduction modulo p de $\tilde{\mathcal{A}}$ est $\mathcal{A}$ et $\mathrm{End}(\tilde{\mathcal{A}}) \cong \mathrm{End}(\mathcal{A})$ (comme anneaux).
En dimension 1, lorsque l'on désigne par j le j-invariant de $\tilde{E}$ pour une courbe elliptique ordinaire E sur $\mathbb{F}_q$, on a l'équation modulaire: $\Phi_p(j, j^\Sigma) = 0$, où Φ_p est le polynôme modulaire de niveau p et Σ est le représentant dans $\mathrm{Gal}\,(\mathbb{Q}_{p^n}/\mathbb{Q}_p)$ du petit Frobenius σ. À partir de $\Phi_p(X, Y) \equiv (X^p - Y)(X - Y^p) \mod p$ on montre les rélations suivantes appelées *conditions de Kronecker*:

$$\begin{cases} \dfrac{\partial \Phi_p}{\partial X}(j, j^\sigma) \equiv 0 \mod p \\ \dfrac{\partial \Phi_p}{\partial Y}(j, j^\sigma) \not\equiv 0 \mod p \end{cases}$$

Alors en partant de $j \mod p$, un algorithme de Newton permet de determiner j à une précision N. C'est le cas de l'algorithme de T.Satoh [99] qui utilise cette propriété pour reléver un cycle de courbes conjuguées:

$$E \xrightarrow{\pi} E^\sigma \longrightarrow \cdots \xrightarrow{\pi} E^{\sigma^{n-1}} \xrightarrow{\pi} E^{\sigma^n} \simeq E$$

T.Satoh introduisit aussi une méthode de relèvement du noyau du petit Verschiebung comme un facteur h du polynôme de p-division Ψ_p bien qu'on ait $\Psi_p \equiv h^p \mod p$ et $ord_p \Psi_p'(x) = 1$ pour $(x, y) \in \tilde{E}[p] \cap \tilde{E}(\mathbb{Z}_q^{ur}) \neq \{\mathcal{O}\}$ [99, Lemma 3.7.]. Alors l'action du petit Verschiebung est déduite après le calcul du Verschiebung normalisé par l'algorithme de Vélu. Par suite en considérant les bornes de Hasse, on a assez de précision dans le produit des coefficients des isogénies du cycles des E^i (qui est équivalent à un calcul de norme dans $\mathbb{Q}_q/\mathbb{Q}_p$ d'un coefficient) pour rétrouver la trace t du Frobenius et $\#E(\mathbb{F}_q) = 1 + q - t$.
Cet algorithme de Satoh qui tournait avec une complexité en temps $\tilde{O}(n^3)$ et en espace mémoire de $O(n^3)$ (à p fixé) , connût très vite des améliorations majeurs. Par exemple Harley utilisa les conditions de Kronecker pour construire une équation:

$$e^\sigma + Ae + B = 0 \quad \text{avec} \quad A \equiv 0 \mod p$$

appelée "*équation d'Artin-Schreier*" pour sa ressemblance avec celle-ci. À partir de cette équation on arrive à réléver les invariants d'un couple de courbes elliptiques conjuguées et ainsi évaluer les valeurs propres du petit Frobenius [35]. Cette approche connaît plusieurs améliorations autant sur la partie rélevement que la partie de calcul de norme et les meilleures de ces méthodes ont une complexité quadratique en temps et en espace [35, 108].
Par suite, les algorithmes utilisant le relèvement canonique seront classés dans une classe sous le nom de *méthodes p-adiques*. Dans cette classe on distingue aussi une sous classe

de méthodes pour les quelles le rélèvement de la courbe ordinaire est quelconque . Ces méthodes p-adiques ont été développé par Kedlaya and al. [56]. Elles utilisent les groupes de *cohomologie de Monsky-Washnitzer (et Dwork)* et leurs complexités en p est linéaire (un des avantages du rélevement quelconque) cependant celle en n augmente en cubique.
Dans l'ensemble, les méthodes p-adiques proposent les algorithmes de comptages les plus pratiques en petites caractéristiques sur les courbes elliptiques. Ces propriétés sont une grande motivation pour leur généralisation en dimensions supérieures.
Ainsi J.F. Mestre proposa très tôt une méthode généralisant la méthode "AGM" à partir des *formules de duplication de Riemann* pour les courbes hyperelliptiques ordinaires en caractéristique 2 [75]. F. Vercauteren et J. Denef prosèrent ensuite une extension de la méthode de Kedlaya en caractéristique 2 et par suite sur les courbes de classe C_{ab} qui admettent une équation de la forme $y^a + \sum_{a-1}^{i=1} f_i(x)y^i + f_0(x) = 0$, où $\deg(f_0) = b$ et tel que $a \deg f_i + b_i < ab$ pour $i = 1, \cdots, a-1$ [24, 25]. Après des améliorations ces algorithmes déterminent le nombre de points d'une courbe sur un corps fini $\mathbb{F}_{p^n}$ avec une complexité de $\tilde{O}(g^5 n^3)$. Une comparaison plus détaillée suit le chapitre 8.
Plus récemment R. Carlz et D. Lubicz décrivirent dans [13] une méthode de relèvement d'une variété ordinaire basée sur le calcul des invariants arithmétiques des relevés canonique à partir de systèmes de coordonnées fournies par les thêta constantes. Cette méthode donne une complexité quasi-quadratique en n mais très couteuse en p.
Il existe d'autres avantages du relèvement canonique autre que le calcul du polynôme caractéristique. En effet sur les courbes elliptiques l'approche de Satoh consiste au relèvement de la fonction modulaire j-invariants. En genre 2 en plus de pouvoir reléver les j-invariants modulaires, lorsque l'on sait réléver l'équation d'une courbe, nous pourrions reléver toutes fonctions modulaires vectorielles à partir des covariants associés et en utilisant les principes de Koecher [98, § 2.2].
Nous proposons dans nos travaux ci-résumé une généralisation de l'approche Satoh du relèvement canonique d'une surface abélienne ordinaire. Cette méthode travaille directement avec les invariants et un système d'équations fourni par les polynômes modulaires en dimension 2. Nous proposons aussi des algrithmes de complexité quadratique en n, pour le relèvement de fonctions modulaires vectorielles et l'evaluation du polynôme caractéristique associés à une courbe ordinaire de genre 2.
Ce qui est très pratique en terme de complexité en n comparer aux autres méthodes p-adiques basées sur un relèvement quelconque (approche de Kedlaya et al.). La méthode de relèvement proposée par R.Carlz et D. Lubicz dans [13] nécessite de prendre une extension de corps et les fonctions thêta ne sont pas rationnelles en général, même si elle reste pratique du point de vue asymptotique, le calcul des courbes à partir de relevés de fonctions thêta se complique rapidement en fonction de p. Alors que nos algorithmes calculent le polynôme caractéristique avec le même coût en p que le calcul de la p-torsion de la courbe sur $\mathbb{F}_q$.

Lorsque une surface abélienne $\mathcal{A}$ n'est pas absolument simple, il est isomorphe à un produit de deux courbes elliptiques: $\mathcal{A} = E_1 \times E_2$ et relever $\mathcal{A}$ revient à relever les deux courbes elliptiques. Alors on considère que $\mathcal{A}$ principalement polarisée et absolument simple sur un corps $\mathbb{k}$. Relever canoniquement $\mathcal{A}$ peut signifier différentes choses: relever des invariants modulaires, des formes modulaires, ou encore la courbe de genre 2 associée. Nous allons utiliser des polynômes modulaires en fonction des invariants spécifiques et nous traitons diffèremment pour plusieurs raisons qui seront citer plus loin, les cas *caractéristiques paires et impaires*.
En effet les espaces modules pour certains invariants absolus comme ceux de Streng cités

précédemment ne couvrent pas les caractéristiques 2 ou 3, alors les polynômes modulaires issus n'ont pas *bonne réduction* pour ces caractéristiques. Une alternative en caractéristique 2 est d'utiliser les fonctions thêta (de niveau 2 et 4) comme on peut les définir pour les variétés abéliennes ordinaires [11, 13, 95]. Alors les polynômes modulaires en fonctions thêta sont extraites des *formules de duplication* [74, 75], une généralisation de l'AGM pour calculer le relèvement canonique puis faire du *comptage de points* [66]. Cependant ces méthodes exigent de prendre des extensions puisque les fonctions thêta ne sont pas modulaires de niveau $\Gamma(2,4)$ ou $\Gamma(4,8)$, donc elles ne sont pas rationnelles en général. Bien que ceci ne soit pas nécéssairement un problème pour les applications en comptage de points (pour un point de vue asymptotique). Les relèvements canoniques de courbes à partir de fonctions thêta sont définis sur des extensions de $\mathbb{Z}_q$ alors on sera obligé d'appliquer une descente de Galois délicate tout en contrôlant la précision p-adique pour retourner sur $\mathbb{Z}_q$. En outre l'extension est facile à manœuvrer seulement lorsqu'on travaille sur les corps finis. Notre méthode peut être adapter aux corps de fonctions de caractéristique 2, et dans ce cas nous voudrions réellement utiliser des invariants modulaire de niveau 1.
Plus précisement notre objectif est de:
• Premièrement définir des invariants absolus ayant bonne réduction pour des espaces de modules non couvert par les invariants connus avant. Et reussir à calculer des polynômes modulaires avec de bonnne réduction pour ces invariants.
• Deuxièment étendre l'approche de Satoh au genre 2 c'est-à-dire agir sur les invariants pour construire les relèvements canoniques des surfaces abéliennes ordinaires.
• Et enfin utiliser le relèvement canonique pour des applications comme: le calcul du polynôme caractéristique et les formes modulaires vectorielles sur $\mathbb{F}_q$.
• Nous proposons des méthodes éfficientes pour chaque étape afin de rendre nos algorithmes plus pratiques.

0.0.4 *Résultats*

Dans les deux premiers chapitres de ce document nous introduisons des algorithmes de Newton " bien adaptés " au relèvement de la p-torsion des variétés abéliennes principalement polarisées en général. En dimension 1, l'étape dominante du relèvement canonique utilisant la forme classique du Théorème de Lubin-Serre-Tate réside dans l'évaluation Φ_p à la précision N sur $\mathbb{Z}_q$ pour un coût de $\tilde{O}(p^2 N \log q) = \tilde{O}(p^2 N n)$. À la fin du deuxième chapitre nous avons établi un résultat (le théorème 2.6.2) équivalent au Théorème de Lubin-Serre-Tate pour le relèvement canonique des courbes elliptiques ordinaires. Et par la suite nous avons le résultat suivant :

Théorème 2.6.10: Pour toute courbe elliptique $E/\mathbb{F}_q$ on calcule le relèvement canonique $\tilde{E}/\mathbb{Z}_q$ et la trace du Frobenius à la précision p-adique N en temps $\tilde{O}(n.N.p)$.
En particulier, pour le comptage où $N = O(n)$, on détermine χ_π avec $\tilde{O}(pn^2)$ opérations.

Une courbe de genre 2 en général admet en toute caractéristique, une équation birationnellement équivalent à:

$$XY^2 + (1 + aX + bX^2)Y + X^2(c + dX + X^2) = 0$$

appelée sa *forme normale* ; et ceci est équivalente à la connaissance du quintuplet d'invariants arithmetique d'Igusa $(J_2, J_4, J_6, J_8, J_{10})$ avec $J_2J_6 - J_4^2 - 4J_8 = 0$ [51, §3]. En caractéristique 2, une forme normale de courbe de genre 2 se réduit sur l'une des trois équations :

$$Y^2 - Y = \begin{cases} \alpha X + \beta X^{-1} + \gamma(X-1)^{-1}, & (1,1,1) \\ X^3 + \alpha X + \beta X^{-1}, & (3,1) \\ X^5 + \alpha X^3, & (5) \end{cases}$$

Selon le nombre et degré de ramification des points de Weierstrass [51, §2]. Cette classification est donnée aussi par le rang de la p-torsion étale sur la Jacobienne. Alors le type $(1,1,1)$ correspond aux Jacobiennes de courbes ordinaires, le type $(3,1)$ correspond aux Jacobiennes de p-rang 1, et le type (5) aux Jacobiennes supersingulaires (ou courbes). En outre, J. Igusa [51, §7] montre que la variété arithmétique $\mathcal{M}_2$ de l'espace des courbes de genre 2 est engendré sur $\mathbb{Z}$ par dix invariants (définis en fonctions de J_{2i}'s), notés γ_i par Goren-Lauter [41]. Lorsque $\mathrm{char}(\Bbbk) = 2$, les invariants arithmétiques absolus $\mathfrak{a}_1 = J_4/J_2^2$, $\mathfrak{a}_2 = J_8/J_2^4$ et $\mathfrak{a}_3 = J_{10}/J_2^5$ définissent sur $\mathcal{M}_2 \otimes \Bbbk$ l'ouvert $\mathcal{M}_2[J_2^{-1}] \otimes \Bbbk$ des courbes birationnellement équivalent au type $(1,1,1)$. Le triplet $(0, J_8^3/J_6^4, J_{10}^3/J_6^5)$ définit sur ensemble de $\mathcal{M}_2[J_6^{-1}] \otimes \Bbbk$ des courbes birationnellement équivalent au type $(3,1)$. Et le type (5) excepté un point (donné par $J_2 = J_4 = J_6 = J_8 = 0$) , est contenu dans $\mathcal{M}_2[J_8^{-1}] \otimes \Bbbk$ est défini à partir du triplet d'invariants $(0, 0, J_{10}^4/J_8^5)$. Alors nous utilisons les dix invariants absolus γ_i's pour démontrer l'un des résultats fondamentaux de cette thèse:

Théorème 4.3.2: Les triplets d'invariants $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$, $(\mathfrak{d}_1, \mathfrak{d}_2, \mathfrak{d}_3)$, $(\mathfrak{u}_1, \mathfrak{u}_2, \mathfrak{u}_3)$ *et* $(\mathfrak{w}_1, \mathfrak{w}_2, \mathfrak{w}_3)$ *induisent un isomorphisme de* $\mathcal{M}_2[J_2^{-1}]$, $\mathcal{M}_2[J_4^{-1}]$ *et* $\mathcal{M}_2[J_6^{-1}]$ *vers l'ouvert standard de* $\mathbb{A}^3$ *défini par* $\mathfrak{a}_3^{-1}$, $\mathfrak{d}_3^{-1}$, $\mathfrak{u}_3^{-1}$ *respectivement, sur* $\mathbb{Z}$, $\mathbb{Z}[1/2]$ *et* $\mathbb{Z}$ *respectivement.*
Le dernier système d'invariants défini un récouvrement fini de $\mathcal{M}_2[J_8^{-1}]$ *vers l'ouvert standard* $\mathbb{A}^3[\mathfrak{w}_3^{-1}]$ *sur* $\mathbb{Z}$. *En caractéristique* 2, *ce dernier triplet defini un morphisme radiciel du lieu des points singuliers (*$J_2 = J_6 = 0$*) vers* $\mathbb{A}^1_{\Bbbk} \setminus \{0\}$.

Alors à partir des triplets de bonne réduction du théorème 4.3.2, l'algorithme 6 dans le chapitre 5 et la section 5.2 (une variante des algorithmes de Dupont et de Milio) nous permettent de calculer des polynômes modulaires avec bonne réduction décrivant les surfaces abéliennes principalement polarisées $(2,2)$-isogènes, avec J_2 non nul modulo 2 et $(3,3)$-isogènes, avec J_4 non nul modulo 3. Les polynômes modulaires calculés au-paravant dans [28, 78] n'avaient pas ces propriétés de bonne réduction en caractéristique 2 (et caractéristique 3 sur l'espace de Siegel).

Comme dans l'approche originale de Satoh, il existe une propriété généralisant les conditions de Kronecker sur l'espace de module des variétés abéliennes ordinaires de dimension g. Nous proposons une preuve génerale sur l'espace de module fin $\mathfrak{A}^{(0)}_{g,\Gamma_0(p)}$ dans le chapitre 6, la section 6.2 et la proposition 6.2.1.

Proposition 6.2.1: Pour tout point géométrique $(\Pi : A_{/\Bbbk} \longrightarrow A^{\Pi}_{/\Bbbk}, \lambda_A)$ du lieu $\mathfrak{A}^0_{g,\Gamma_0(p)}$ des points ordinaires de $\mathfrak{A}_{g,\Gamma_0(p)}$, la fonction vectorielle $\mathfrak{S}$ satisfait les conditions:

1. $\dfrac{\partial \mathfrak{S}}{\partial X}(\hat{\Pi}, \Pi)$ s'annule modulo p,
2. $\dfrac{\partial \mathfrak{S}}{\partial Y}(\hat{\Pi}, \Pi)$ est inversible modulo p.

En particulier pour tout point J du sous schéma du module grossier $\mathcal{M}_g$ décrit par le système Φ_p de polynômes modulaires de niveau p on a:

$$\begin{cases} \dfrac{\partial \Phi_p}{\partial X}(J, J^{\Sigma}) \equiv 0 \mod p \\ \dfrac{\partial \Phi_p}{\partial Y}(J, J^{\Sigma}) \not\equiv 0 \mod p \end{cases}$$

Ainsi sur les espaces de module de Siegel (la section 7.1) et de Hilbert (la section 7.4), nous proposons des extensions de l'algorithme de Harley en dimension 2 pour calculer le relevés des invariants qui satisfont les conditions de Kronecker par rapport aux polynômes modulaires utilisés.

Comme en genre 1 avec l'algorithme de Satoh, nous travaillons directement sur les invariants modulaires de niveau 1, avec l'avantage de rester sur le corps de définition afin d'optimiser la complexité des calculs. Et différement des autres méthodes p-adiques en genre 2, notre approche fournit des méthodes de relèvement canonique de l'équation de la courbe.

Des applications: Ces relèvements des courbes permettent le calcul de covariants, par suite des formes modulaires (vectorielles) sur ces courbes, et ceci est utilisé dans le calcul des polynômes de classe [12]. Nos méthodes de relèvement peuvent être utiliser dans les calculs de polynôme de classe comme indiqué dans [39], sans passer par les invariants de Rosenhain (qui peuvent avoir des valuations négatives).
En dimension 2, le relevé de la p-torsion est donnée par la proposition 7.2.2 (dans la section 7.1) qui est une extension en dimension 2 du [99, Lemma 3.7.] de Satoh. Ainsi nous avons les théorèmes suivants dans le chapitre 8:

Théorème:8.2.3 Pour toute courbe hyperelliptique ordinaire $\mathcal{C}$ de genre 2 sur $\mathbb{F}_{2^n}$ dont les invariants $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ satisfont les conditions de Kronecker. Notre algorithme (dans le chapitre 8 et la section 8.2.2) détermine $\#\operatorname{Jac}(\mathcal{C})(\mathbb{F}_{2^n})$ (ou le polynôme caractéristique du Frobenius) en $\tilde{O}(n^2)$ opérations, à partir du polynôme en fonction des $\mathfrak{a}_1$, $\mathfrak{a}_2$ et $\mathfrak{a}_3$.

Théorème: 8.2.5 En caractéristique impaire notre méthode dans le chapitre 8 et la section 8.2.3 calcule $\#\operatorname{Jac}(\mathcal{C})(\mathbb{F}_q)$ pour une courbe $\mathcal{C}$ de genre 2 vérifiant les conditions de Kronecker en $\tilde{O}(n^2)$.

En utilisant nos méthodes d'évaluation directe du Verschiebung on a:

Théorème: 8.2.7 Par la méthode d'évaluation du Verschiebung on calcule le polynôme caractéristique d'une courbe ordinaire de genre 2 en utilisant au plus $O(M(p^4)\log(p)\log(n).n^2)$ opérations binaires.

Ces différents résultats sont résumés en quatre manuscrits:

1. **A. Maïga and D. Robert**: *Computing the 2-adic canonical lift of genus 2 curves*.In: Giri, D., Raymond Choo, KK., Ponnusamy, S., Meng, W., Akleylek, S., Prasad Maity, S. (eds) Proceedings of the Seventh International Conference on Mathematics and Computing . Advances in Intelligent Systems and Computing, vol 1412. Springer, Singapore. March.2022 https://doi.org/10.1007/978-981-16-6890-6_48
2. **A. Maïga and D. Robert**: *Computing the canonical lift of genus 2 curves in odd characteristic*. Dec.2020.http://www.normalesup.org/~robert/pro/publications/articles/canonical_lift_g2.pdf. Submitted to: Springer Journals Editorial Office The Ramanujan Journal.

3. **A. Maïga and D. Robert**: *Towards computing canonical lifts of ordinary elliptic curves in medium characteristic*. https://hal.inria.fr/INRIA/hal-03702658v1
4. **A. Maïga and D. Robert and D. Sow**: *Towards computing canonical lifts of ordinary abelian surfaces in medium characteristic*. Preprint

En perpective nous prévoyons des méthodes pour améliorer la complexité en p dans le calcul de relevé canonique de surfaces abéliennes ordinaires :
• La première serait d'étendre aux courbes de genre 2 nos méthodes introduites dans le troisième manuscrit et abordées à la fin du chapitre 2. Ces méthodes calculent le relevé canonique d'une courbe ordinaire de genre 2 sans utiliser respectivement les polynômes modulaires et le polynôme de division.
• La deuxième serait d'y associer une évaluation le Verschiebung directement en utilisant l'approche d'Elkies du calcul d'isogenie qui fournit une meilleure complexité en p, en effet cela pourrait être une alternative à l'evaluation de la p-torsion coûte $O(M(p^4)\log(p))$ opérations en $\mathbb{F}_p$.

0.0.5 *Plan de la Thèse*

Nous organisons le résumé de ces travaux de thèse: de parties en chapitres et de chapitres en sections. de la manière suivante :
• La partie i concerne le chapitre 1 et le chapitre 2. Dans le premier nous rappellons les constructions de l'anneau des entiers p-adiques $\mathbb{Z}_q$ favorables aux calculs de Frobenius rapides (choix du polynôme de Teichmüller) utilisées très souvent dans les exemples. Nous introduisons aussi dans ce chapitre une extension des méthodes de Hensel aux cas où $\mathrm{ord}_p(f'(x)) > 0$ (pour les cas univariés et multivariés). Le chapitre 2 est un rappel détaillé des méthodes p-adiques utilisant le rélèvement canonique: algorithmes de Satoh [99] et de Harley [35] dont nous proposons plus loin des extensions en dimension 2. Et aussi une amélioration considérable de la complexité de ces dites méthodes.
• Dans la partie ii et le chapitre 3, nous abordons les variétés abéliennes principalement polarisées complexes (comme une généralisation des courbes elliptiques complexes). Une arithmétique plus pratique (l'usage des fonctions thêta) sur ces variétés est abordé. Nous étudions ensuite les espaces de module des surfaces abéliennes principalement polarisées complexes dans le sens de Siegle $\mathrm{SL}_4(\mathbb{Z})\backslash\mathfrak{H}_2$ et aussi dans le sens de Hilbert $\mathrm{SL}_2(\mathcal{O}_K)\backslash\mathfrak{H}_1^2$ avec l'objectif de pouvoir utiliser des variantes des algorithmes d'évaluation de polynômes modulaires. Dans la partie ii et le chapitre 4 nous parcourons les structures de $\mathcal{M}_2 \otimes \Bbbk$ en utilisant la *Théorie des Invariants Arithmétiques* d'Igusa et nous introduisons des invariants arithmétiques absolus avec bonne réduction sur $\mathbb{Z}$ ou sur $\mathbb{Z}_{(2)}$. À la fin de ce chapitre nous étudions les différentes contructions de courbes de genre 2 et les conversions entre elles (en effet, dans les applications certaines formes sont plus avantageuses que d'autres). Le dernier chapitre 5 de cette partie concerne le calcul de polynômes modulaires en fonction des nouveaux invariants $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ et $(\mathfrak{u}_1, \mathfrak{u}_2, \mathfrak{u}_3)$ et quelques détails sur les polynômes modulaires de Siegel et de Hibert.
• Dans la partie iii, le premier chapitre (6) concerne un bref rappel des résultats fondamentaux sur la *Théorie du Relèvement Canonique* comme le *Théorème de Serre-Tate* [55] et la théorie de réduction de l'espace des schémas de module de Siegel de genre 2 avec une structure de niveau $\Gamma_0(p)$ [15, 90]. En utilisant ces résulats nous proposons une preuve générale des conditions de Kronecker. Le chapitre 7 concernent respectivement le relèvement canonique sur l'espace de Siegel et sur l'espace de Hilbert. Tout le chapitre 8 concerne des applications

du relèvement canonique: du calcul de formes modulaires vectorielles associées aux courbes de genre 2, au calcul du polynôme caractéristique d'une courbe de genre 2. Et à la fin, nous faisons une conclusion détaillée sur les résultats et leur impact sur d'autres domaines comme la cryptographie et nous proposons des perpectives pour des améliorations de complexité de certains algorithmes.

Première partie

PRÉLIMINAIRES

1

EXTENSION NON-RAMIFIÉE DU CORPS DES NOMBRES P-ADIQUES

On considère le corps des nombres rationels $\mathbb{Q}$ muni de la valuation ord_p définie par :

$$\begin{aligned}
&\mathrm{ord}_p(0) = \infty;\\
&\mathrm{ord}_p(a) = \max\{m,\ a \equiv 0 \mod p^m\} \quad pour \quad tout \quad a \in \mathbb{Z};\\
&\mathrm{ord}_p(\frac{a}{b}) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b) \quad pour \quad tout \quad b \in \mathbb{Z}^*.
\end{aligned}$$

Proposition 1.0.1. *Alors l'application de $|\cdot|_p$ définie sur $\mathbb{Q}$ par :*

$$|x|_p = \begin{cases} 0 & si \quad x = 0, \\ \dfrac{1}{p^{\mathrm{ord}_p x}} & sinon \end{cases}$$

est une norme non-Archimedienne sur $\mathbb{Q}$ c'est à dire que $|x+y|_p \leq \max(|x|_p,\ |y|_p)$.

Démonstration. En effet, l'homogénité se déduit de la propriété $\mathrm{ord}_p(xy) = \mathrm{ord}_p\, x + \mathrm{ord}_p\, y$. De plus $\mathrm{ord}_p(x+y) \geq min(\mathrm{ord}_p\, x,\ \mathrm{ord}_p\, y)$, alors

$$|x+y|_p = p^{-\,\mathrm{ord}_p(x+y)} \leq \max(|x|_p,\ |y|_p)$$

qui implique à la fois l'inégalité triangulaire et que $|\cdot|_p$ est non-Archimedienne sur $\mathbb{Q}$. Cette dernière propriété donne à $|\cdot|_p$ une très grande importance en Analyse. □

En remplaçant $1/p$ par tout $\rho \in [0,\ 1]$ dans la définition nous obtenons des normes équivalentes (c'est à dire les mêmes suites de Cauchy). Et le Théorème d'Ostrowski établit que toute norme nontriviale sur $\mathbb{Q}$ est soit équivalente à la norme usuelle $|\cdot|$ ou soit équivalente à une norme du type $|\cdot|_p$ pour un premier p.
L'une des constructions du corps des nombres reéls $\mathbb{R}$ à partir de celui des nombres rationels $\mathbb{Q}$ est d'abord de considerer les suites de Cauchy de l'espace métrique $(\mathbb{Q}, |\cdot|)$ avec la rélation d'équivalence : $\{a_j\} \sim \{b_j\}$ si $|a_j - b_j| \to 0$ quand $j \to \infty$. Ainsi $\mathbb{R}$ est défini comme l'ensemble des classes d'équivalence des suites de Cauchy sur $(\mathbb{Q}, |\cdot|)$. Et on y définit une addition et une multiplication qui confèrent à $\mathbb{R}$ une structure de corps.
On considère au début la même construction que précédemment, avec cette fois-ci la norme $|\cdot|_p$.
Soit $\mathbb{Q}_p$ l'ensemble des classes d'équivalence des suite de Cauchy de $(\mathbb{Q}, |\cdot|_p)$ par la rélation d'équivalence $\sim$. Alors nous avons $\mathbb{Q} \subset \mathbb{Q}_p$ car les suites constantes sont de Cauchy et représentent chacune une classe d'équivalence et la classe de $\{0\}$ sera notée 0. La norme $|\cdot|_p$ s'étend aux classes d'équivalence par la définition suivante : Soit $a \in \mathbb{Q}_p$, $|a|_p = lim_{i\to\infty}|a_i|_p$ pour un représentant $\{a_i\}$ de a . Grâce à la propriété que $|\cdot|_p$ est non-Archimedienne cette limite existe pour toute suite de Cauchy.
Par la suite on peut définir l'addition et la multiplication de deux classes d'équivalence a et b par $a+b$ et $a.b$ les classes d'équivalence des suites de Cauchy $a_i + b_i$ et $a_i.b_i$ où $\{a_i\}$ et $\{b_i\}$

sont respectivement des représentants quelconques des classes a et b.
L'inverse d'une classe non nulle a se définit par $\{1/a_i\}$ pour un représentants $\{a_i\}$ dont tous les termes sont non nuls. Pour cela il est facile de rémarquer qu'une suite de Cauchy $\{a_i\}$ dont un terme $a_j = 0$ est équivalente à la suite $\{a'_i\}$ avec $a'_j = p^j$. Ainsi les autres propriétés ($-a$ et $a(b+c)$) héritent celles des termes et on obtient que $\mathbb{Q}_p$ est un corps contenant $\mathbb{Q}$.
En considerant une suite de Cauchy $\{a_j\}$ sur $\mathbb{Q}_p$ où la suite de Cauchy représentant chaque classe $\{a_j\}$ est $\{a_{ji}\}$. Pour chaque j nous avons $|a_{ji} - a_{ji'}|_p < p^{-j}$ quand $i, i' \geq N_j$, alors la classe d'équivalence de $\{a_{jN_j}\}$ est la limite de $\{a_j\}$. Ainsi $(\mathbb{Q}_p, |\cdot|_p)$ est complet .

Théorème 1.0.2. *Le sous-ensemble de $\mathbb{Q}_p$ défini par :*

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p / \ |x|_p \leq 1\} = \{x \in \mathbb{Q}_p / \ ord_p x \geq 0\}$$

est un anneau local d'idéal maximal $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p / \ ord_p x > 0\}$, et chaque $a \in \mathbb{Z}_p$ peut s'écrire de manière unique $\{a_i\}$ avec : $0 \leq a_i < p^i$ et $a_i \equiv a_{i+1} \mod p^i$ pour $i = 1, 2, 3, ...$

Démonstration. Voir [62, chap 3]. □

Les éléments de $\mathbb{Z}_p$ sont appelés les *entiers p-adiques*, nous avons $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p / \ |x|_p = 1\}$ et le corps résiduel $\mathbb{Z}_p / p\mathbb{Z}_p$ est isomorphe à $\mathbb{F}_p$ le corps premier à p éléments.
Nous parlons maintenant d'un résultat très important sur $\mathbb{Z}_p$, qui permet de réduire sous certaines conditions la résolution d'une équation sur $\mathbb{Z}_p$ à sa réduite modulo p qui est beaucoup plus facile.

Théorème 1.0.3. *(Lemme de Hensel). Soient $f(x) \in \mathbb{Z}_p[x]$ et $a \in \mathbb{Z}_p$ tels que $f(a) \equiv 0 \mod p$ et $f'(a) \not\equiv 0 \mod p$ où f' est la dérivé de f. Alors il existe un unique $\tilde{a}$ dans $\mathbb{Z}_p$ tel que :*

$$f(\tilde{a}) = 0 \quad et \quad \tilde{a} \equiv a \mod p$$

Démonstration. Aller à [62, chap 1, thm 3]. □

Alors nous avons pour toute erreur r telle que : $\tilde{a} - a = p^k r$, r est solution sur $\mathbb{F}_p$ de l'équation:

$$f(a) + p^k r . f'(a) = 0 \mod p^{2k}$$

c'est-à-dire encore que

$$\frac{f(a)}{f'(a)} + p^k r . 1 = 0 \mod p^{2k}$$

Alors sur une boule de centre a et de rayon p^k, les deux fonctions f et $\frac{1}{f'(a)}.f$ coïncident et la même erreur r corrige a pour les deux fonctions. Il existe encore d'autres approximations de la fonction f sur la même boule. Nous allons voir dans la section 1.2 que certaines de ces approximations permettent d'élargir l'hypothèse de Hensel.

1.1 REPRÉSENTATION DE TEICHMULLER

Pour ce qui suit nous nous intéressons aux extensions algébriques du corps des nombres p-adiques c'est à dire des corps $\mathbb{K}$ dont tout élément α est solution d'un polynôme sur $\mathbb{Q}_p$.

Lorsque $\mathbb{K}$ est de dimension finie sur $\mathbb{Q}_p$ alors l'extension $\mathbb{K}/\mathbb{Q}_p$ est séparable (car $char(\mathbb{Q}_p) = 0$) et $\mathbb{K} = \mathbb{Q}_p(\alpha)$. Ainsi $\mathbb{K}$ est isomorphe à $\mathbb{Q}_p[X]/M(X)$ où M est un polynôme

irréductible sur $\mathbb{Q}_p$ avec $M(\alpha) = 0$ et $deg(M) = [\mathbb{K} : \mathbb{Q}_p]$. Alors on peut définir $N_{\mathbb{K}/\mathbb{Q}_p}(\alpha) := \alpha_1\alpha_2\cdots\alpha_n$, où les α_i sont les conjugués de $\alpha = \alpha_1$ sur $\mathbb{Q}_p$.
Dans ce cas il existe une seule norme sur $\mathbb{K}$ définie par $|\alpha|_{\mathbb{K}} := |N_{\mathbb{K}/\mathbb{Q}_p}(\alpha)|_p^{1/deg(M)}$ se réduisant sur la norme $|\cdot|_p$ de $\mathbb{Q}_p$. Nous noterons $|\cdot|_{\mathbb{K}}$ aussi par $|\cdot|_p$ et $ord_p(\alpha) := -log_p(|\alpha|_p)$.
Soient $\mathcal{R} = \{x \in \mathbb{K} / |x|_p \leq 1\}$ l'anneau des entiers de $\mathbb{K}$ et $\mathcal{M}$ son idéal maximal, alors nous avons le diagramme suivant :

$$\begin{array}{ccc} \mathbb{Z}_p & \xrightarrow{\psi} & \mathcal{R} \\ \downarrow{\scriptstyle \text{mod } p} & & \downarrow{\scriptstyle \text{mod } p} \\ \mathbb{F}_p & \longrightarrow & \mathcal{R}/\mathcal{M} \end{array}$$

Où mod p est la projection naturelle $\mathbb{Z}_p$ sur $\mathbb{F}_p$,
ψ est l'inclusion naturelle de $\mathbb{Z}_p$ dans $\mathcal{R}$.

Proposition 1.1.1. *Soient $e = ord_p(\psi(p))$ et $n = [\mathcal{R}/\mathcal{M} : \mathbb{F}_p]$ alors $[\mathbb{K} : \mathbb{Q}_p] = e.n$.*

Démonstration. Aller à [62, chap 3]. □

e est appelé l'indice de ramification de $\mathbb{K}$ et n le degré de ramification de $\mathbb{K}$.
Lorsque $e = 1$, l'extension $\mathbb{K}/\mathbb{Q}_p$ est dite non-ramifiée de degré n et est notée $\mathbb{Q}_q$, son anneau de valuation $\mathbb{Z}_q$ pour $q = p^n$.

Proposition 1.1.2. *$\mathbb{Q}_q$ est une extension Galoisienne de $\mathbb{Q}_p$, unique à isomorphisme près et $\text{Gal}(\mathbb{Q}_q/\mathbb{Q}_p)$ est un groupe cyclique engendré par Σ se réduisant sur l'automorphism de Frobenius $\sigma : x \mapsto x^p$.*

Démonstration. Aller à [62, chap 3] et [17] □

L'union de toutes les extensions non-ramifiées finies de $\mathbb{Q}_p$ est appelée l'Extension Non-Ramifiée Maximale de $\mathbb{Q}_p$. Elle sera notée par ${\mathbb{Q}_p}^{ur}$ et son anneau des entiers par $\mathbb{Z}_p^{ur}$ dont l'idéal maximal est $p\mathbb{Z}_p^{ur}$ tel que :

$$\mathbb{Z}_p^{ur} := \{x \in {\mathbb{Q}_p}^{ur} / |x|_p \leq 1\} \quad et \quad p\mathbb{Z}_p^{ur} := \{x \in {\mathbb{Q}_p}^{ur} / |x|_p < 1\}$$

Chaque élément x de $\overline{\mathbb{F}}_p$ admet un unique "*représentant de Teichmüller*" $\tilde{x} \in \mathbb{Z}_p^{ur}$ lequel est une racine de l'unité et son image $\tilde{x} \mod p = x$ dans $\mathbb{Z}_p^{ur}/p\mathbb{Z}_p^{ur} \simeq \overline{\mathbb{F}}_p$.

Anneau de Vecteurs de Witt

Soit $\Bbbk$ un corps de caractéristique $p > 0$ on definit l'anneau $W_{n+1}(\Bbbk)$ de vecteurs de Witt comme l'ensemble des éléments $(\alpha_0, \cdots, \alpha_n) \in \Bbbk^{n+1}$ muni des opérations $+, \cdot$ définies de manière suivante:

$$(x_0, \cdots, x_n) + (y_0, \cdots, y_n) = (s_0, \cdots, s_n)$$
$$(x_0, \cdots, x_n) \cdot (y_0, \cdots, y_n) = (m_0, \cdots, m_n)$$

tel que pour tout $i = 0, \cdots, n$ on a s_i, m_i sont des polynômes de $\mathbb{Z}[x_0, \cdots, x_n, y_0, \cdots, y_n]$ définis par les propriétés suivantes:

1. $s_0 = x_0 + y_0$, et $m_0 = x_0 y_0$,
2. On définit $\phi(z_0, \cdots, z_i) = z_0^{p^i} + pz_1^{p^{i-1}} + \cdots + p^i z_i$ pour $i = 1, \cdots, n$.
3. Pour $i = 1, \cdots, n$, les s_i et m_i sont donnés par :

$$\phi_i(s_0, \cdots, s_i) = \phi_i(x_0, \cdots, x_i) + \phi_i(y_0, \cdots, y_i),$$

$$\phi_i(m_0, \cdots, m_i) = \phi_i(x_0, \cdots, x_i) + \phi_i(y_0, \cdots, y_i).$$

Alors nous avons les propriétés suivantes:
• L'idéal $pW_{n+1}(\Bbbk)$ de l'anneau $W_{n+1}(\Bbbk)$ est nilpotent de degré n tel que :

$$W_{n+1}(\Bbbk)/pW_{n+1}(\Bbbk) \simeq \Bbbk$$

• Lorsque corps $\Bbbk$ est une extension finie de $\mathbb{Z}/p\mathbb{Z}$, alors l'anneau défini par

$$W(\Bbbk) = \lim_{n\to\infty} W_{n+1}(\Bbbk)$$

est une extension finie de $\mathbb{Z}_p$ isomorphe à $\mathbb{Z}_p^{ur}$.

Ainsi $\mathbb{Z}_p^{ur}$ est appelé "*anneau des vecteurs de Witt*" ou encore le "*Lift de* $\overline{\mathbb{F}}_p$ *en caractéristique zéro*".
Les méthodes de relèvement canoniques de courbes elliptiques ordinaires avec le polynôme modulaire s'appuient sur l'unicité du lift de l'isogénie Frobenius (qui ne se ramifie pas sur $\mathbb{Z}_q$) . Pour cela ces méthodes utilisent des représentations de $\mathbb{Q}_q$ dans lesquels l'automorphisme Frobenius Σ se calcule le plus simplement possible. Ce choix permet aussi un calcul de norme $N_{\mathbb{Q}_q/\mathbb{Q}_p}$ très rapide .
Soient $q = p^n$ et $\mathbb{F}_q$ donné par $\mathbb{F}_p[X]/m(X)$ avec $m(X)$ un polynôme irréductible unitaire sur $\mathbb{F}_p$. Une manière naturelle de choisir le relevé $M(X)$ de $m(X)$ est de prendre : $M \in \mathbb{Z}_p[X]$ avec $M(X)|X^q - X$ et $M(X) \equiv m(X) \mod p$. Cela preserve la structure Galoisienne aussi simple que possible et nous prendrons $M(X)$ comme *relevé de Teichmuller* de $m(X)$.
Alors on pourra travailler à la précision k en effectuant les opérations dans $(\mathbb{Z}/p^k\mathbb{Z})[X]/M(X)$. Et dans ces conditions la complexité d'une opération élémentaire sur $(\mathbb{Z}/p^k\mathbb{Z})[X]/M(X)$ requiert par exemple $\tilde{O}(nklogp)$ avec la méthode de Kronecker-Schönhage [35].

1.2 RELÈVEMENT DES SOLUTIONS D'UN SYSTÈME DE DIMENSION ZÉRO

Dans ce qui suit, nous exposons des résultats répris dans le deuxième article (Introduction: la section 0.0.4), sur des extensions aux conditions de Hensel. Ces résultats fournissent des algorithmes de relèvement des éléments de $\mathbb{F}_q$ en lesquels la Jacobienne du système n'est pas inversible modulo p avec un contrôle fin des pertes de précision.

1.2.1 *Relèvement des Solutions d'un Polynôme Univarié*

Lorsque f est un polynôme sur $\mathbb{Z}_q$ et $x \in \mathbb{F}_q$ tel que $ord_p(f'(x)) = 0$ alors le *Lemme de Hensel* donne à la fois l'existence et l'unicité du relevé $\tilde{x}$ de x sur $\mathbb{Z}_q$. Cependant comme nous allons le voir dans les chapitres 2 et 7.1 nous rencontrons des situations où $ord_p(f'(x)) > 0$. Par exemple lorsque $p \geq 3$ et $\tilde{E} : y^2 = x^3 + \tilde{A}x + \tilde{B}$ on a $ker(\hat{\Sigma}) = \tilde{E}[p] \cap \tilde{E}(\mathbb{Z}_q^{ur})$ où $\mathbb{Z}_q^{ur}$ est

l'anneau de valuation de l'extension non-ramifiée ${\mathbb{Q}_q}^{ur}$ de $\mathbb{Q}_q$ [99, Theorem 3.1]. Et pour tout $P \in \tilde{E}(\mathbb{Z}_q^{ur}) - \{\mathcal{O}\}$ le [99, Lemma 3.7.] établit que :

$$\operatorname{ord}_p\left(\Psi'_p(x_P)\right) = 1 \quad \text{où} \quad \Psi'_p = \frac{\partial \Psi_p}{\partial x}$$

Bien que l'unicité du relevé soit établie par le relèvement canonique, cependant l'algorithme standard de Hensel n'est pas pratique pour calculer le rélévé de x_P à partir de $\mathbb{F}_q$, car la valuation de la dérivée en x_P fait perdre de la précision dans les calculs. Cependant, comme $\Psi_p(x) \equiv H(x)^p \mod p$, nous avons $\operatorname{ord}_p \Psi_p(x_P) \geq 2$ pour tout $P \in E[p]$ alors les méthodes détaillées ci-dessous permettent de calculer sans pertes de précisions le relevé $x_{\tilde{P}}$ de x_P.
Pour ce qui suit on pose: $f^{<n>} = n!.f^{(n)}$ pour tout $f = \sum a_i.X^i \in \mathbb{Z}_q[a_i, X]$.

Lemme 1.2.1. *Soient p un nombre premier, f un polynôme sur $\in \mathbb{Z}_q$ et $x \in \mathbb{Z}_q$ tels que $ord_p f(x) = k$ et $\operatorname{ord}_p f'(x) = e$ avec $e < k$. Alors pour toute solution r de l'équation*

$$f(x) + f^{<1>}(x)p^{(k-e)}r + \cdots + f^{<i-1>}(x)p^{(i-1)(k-e)}r^{i-1} \equiv 0 \mod p^{i(k-e)} \tag{1.1}$$

$$\text{où} \quad i = \lceil (k+1)/(k-e) \rceil$$

$x + p^{(k-e)}r$ est une solution de f à la précision $p^{i(k-e)}$.

Démonstration. On suppose que $\operatorname{ord}_p f(x) = k$ et $\operatorname{ord}_p f'(x) = e$ avec $e < k$. Le dévéloppement de Taylor de f est donné par:

$$f(x+\Delta) = f(x) + f'(x).\Delta + f''(x) \cdot \Delta^2 + \cdots + f^{<i-1>}(x)\Delta^{i-1} + \Delta^i \cdot Q(x)$$

où $Q(x)$ est dans $\mathbb{Z}_q$.
On pose $\operatorname{ord}_p(\Delta) = m$, nous voulons déterminer l'erreur r à la précision au moins p et il est avantageux de résoudre avec le degré le plus grand possible en r. Nécéssairement $f(x)$ et $f'(x).\Delta$ doivent être à la même précision, alors $m = k - e$. Par conséquent nous pouvons résoudre l'équation (en fonction de r) à la précision $p^{i(k-e)}$ telle que: $i(k-e) \geq k+1$; par exemple pour $i = \lceil (k+1)/(k-e) \rceil$.

$$f(x) + f^{<1>}(x)p^{(k-e)}r + \cdots + f^{<i-1>}(x)p^{(i-1)(k-e)}r^{i-1} \equiv 0 \mod p^{i(k-e)}$$

□

• Dans le cas où $k > 2e$ c'est-à-dire encore $2(k-e) > k$, l'équation (1.1) détermine une unique solution modulo $p^{2(k-e)}$ (avec $i = 1$) qui converge vers un unique relevé sans pertes de précision sur x. Ainsi pour toute solution x modulo p, la condition $\operatorname{ord}_p f(x) > 2 \operatorname{ord}_p f'(x)$ assure l'existence et l'unicité à la fois à partir de la précision $p^{2(k-e)}$ du relevé sur $\mathbb{Z}_q$. En plus

$$\begin{aligned} f'(x + p^{(k-e)}r) = f'(x) + f''(x)p^{(k-e)}r + \cdots \\ + f^{<i>}(x)p^{i(k-e)}r^i + p^{(i+1)(k-e)}(\cdots) \end{aligned}$$

ce qui implique $\operatorname{ord}_p f'(x + p^{(k-e)}r) = e$ car $e < k - e$.

• Lorsque $k \leq 2e$ la résolution de l'équation (1.1) dépend des valuations des $f^{<j>}(x)$ pour $2 \leq j \leq i(k-e)$. Alors l'équation (1.1) pourrait avoir une solution sur une extension $\mathbb{Z}_q$ ou ne pas avoir de solutions du tout. Par exemple:

— S'il existe seulement un $j \in \{2,\ i(k-e)\}$ tel que $\mathrm{ord}_p\, p^{j(k-e)} f^{<j>}(x)$ est inférieure à k alors r n'existe pas. Dans ce cas *x n'admet pas de relevés sur $\mathbb{Z}_q$*.

— Si $\mathrm{ord}_p\, p^{j(k-e)} f^{<j>}(x)$ est supérieure ou égal à $i(k-e)$ pour tout $j \in \{2,\ i(k-e)\}$, alors dans ce cas *chaque solution de l'équation définit un relevé de x sur $\mathbb{Z}_q$*.

Exemple 1.2.2. Soit p un nombre premier impair et E une courbe elliptique sur $\mathbb{F}_q$, nous rappellons que pour $P(x_0, y_0) \in E[p]$, $\mathrm{ord}_p\, \Psi_p(x_0) > 1$, $\mathrm{ord}_p\, \Psi'_p(x_0) = 1$, et nous avons aussi $\mathrm{ord}_p\, \Psi''_p(x_0) \geq 1$ car $\Psi_p = h^p \mod p$.
Alors nous avons $\mathrm{ord}_p\, \Psi_p(x_0) \geq 2.\mathrm{ord}_p(\Psi'_p(x))$ et en utilisant le lemme 1.2.1 on peut déterminer l'unique rélévé de x_0 sur $\mathbb{Z}_q$.
Par exemple lorsque $\mathrm{ord}_p\, \Psi_p(x_0) = 2$, nous avons $k = 2$ et $e = 1$ alors dans le lemme 1.2.1, l'équation (1.1) devient:

$$\Psi_p(x_0) + \Psi'_p(x_0).p.r \equiv 0 \mod p^3 \quad \text{comme} \quad \mathrm{ord}_p\, \Psi''_p(x_0) \geq 1.$$

Ce qui correspond à un seul relevé modulo p^3.
Pour $k \geq 3$, alors on est dans le cas $2(k-e) > k$ et on peut résoudre l'équation du lemme 1.2.1 modulo $p^{2(k-e)}$ comme dans le cas de l'algorithme de Newton standard.

$$\Psi_p(x) + \Psi'_p(x).p^{(k-e)}.r \equiv 0 \mod p^{2(k-e)}.$$

Nous rappelons que T. Satoh a introduit dans [99, Lemme 2.1] une variante de l'algorithme de Hensel qui calcule le rélévé du polynôme h définissant le noyau du Verschiebung sur $\mathbb{Z}_q$. En petites caractéristiques, et avec n assez grand, la méthode précédente (le lemme 1.2.1) devient plus rapide puisque Satoh utilise à chaque étape l'algorithme d'Euclide étendu pour calculer l'erreur r.

Lorsque nous sommes dans le cas $\mathrm{ord}_p\, f(x) \leq e$ on peut appliquer la méthode suivante pour obtenir une précision suffisante correspondant au lemme 1.2.1. La stratégie est simple mais elle n'assure aucune convergence pour une solution, le but est d'atteindre la condition de convergence précédente (décrite dans le lemme 1.2.1). Pour déterminer l'erreur r nous pouvons continuer le calcul jusqu'à $f^{<j>}(x)$ telle que $\mathrm{ord}_p(f^{<j>}(x)p^{j\alpha}) = \mathrm{ord}_p\, f(x)$ et $\alpha \in \mathbb{N}$. Nous supposons qu'une racine $\tilde{x} \in \mathbb{Z}_q$ de f existe et que nous connaissons $x = \tilde{x} \mod p$.

Lemme 1.2.3. *Lorsque $\mathrm{ord}_p\, f(x) = k$ et $\mathrm{ord}_p\, f'(x) = e$ tels que $1 \leq k \leq e$. Soit j le plus petit entier non nul (s'il existe) tel que $\mathrm{ord}_p(f^{<j>}(x)) + j \leq k$. Alors pour toute solution r de l'équation:*

$$f(x) + f^{<1>}(x).p^{\alpha}.r + \cdots + f^{<j>}(x).p^{j\alpha} r^j \equiv 0 \mod p^{(j+1)\alpha} \tag{1.2}$$

$$\text{où} \quad \alpha = \lfloor \frac{k - \mathrm{ord}_p(f^{<j>}(x))}{j} \rfloor;$$

$x + p^{\alpha} r$ est une solution de f à la précision $p^{(j+1)\alpha}$.
De plus si $\mathrm{ord}_p(f^{<j>}(x)) \leq \alpha$ alors $\mathrm{ord}_p\, f'(x + p^{\alpha} r) < (j+1)\alpha$ (condition d'application du lemme 1.2.1).

On peut évidemment remarquer qu'un tel j est inférieur ou égal à $(\deg f + 1)$.
La situation $\mathrm{ord}_p(f^{<j>}(x)p^{j\alpha}) < k$ dans le lemme 1.2.3 se produit surtout quand à ce stade x n'est pas à une bonne précision en tant que approximation d'un possible relevé $\tilde{x}$. Et à cette précision, f a de nombreuses racines mais elles ne sont pas toutes des réductions du rélévé inconnu $\tilde{x}$.

Démonstration. Dans le dévéloppement de Taylor de l'équation (1.2), nous avons assez de précision pour diviser par $\mathrm{ord}_p(f^{<j>}(x)p^{j\alpha})$ et nous obtenons modulo p^α une équation:

$$a_j r^j + \cdots a_1 r + a_0 = 0 \quad \text{avec} \quad a_i \in \mathbb{Z}_q.$$

les possibles solutions modulo p^α de cette dernière équation, sont les erreurs pour les précisions suivantes. On peut les calculer en utilisant les bases de Grœbner.
Pour une racine r de l'équation précédente, nous avons:

$$f(x + p^\alpha r) = 0 \mod p^{(j+1)\alpha}.$$

De plus si $\mathrm{ord}_p(f^{<j>}(x)) \leq \alpha$, alors la rélation:

$$f'(x + p^\alpha r) = f'(x) + f^{<2>}(x).p^\alpha r + \cdots + f^{<j>}(x).p^{(j-1)\alpha} r^{j-1} + p^{j\alpha}(\cdots)$$

implique que:

$$\mathrm{ord}_p f'(x + p^\alpha r) = \mathrm{ord}(f^{<j>}(x)) + (j-1)\alpha$$
$$\text{car seule } \mathrm{ord}_p(p^{j\alpha} f^{<j>}(x)) \leq k \text{ alors } f'(x + p^\alpha r) < (j+1)\alpha$$

□

Interprétation:

Nous voulons expliquer d'autre part le lien entre les méthodes précédentes et l'algorithme standard de Hensel (qui est utilisé habituellement lorsque $\mathrm{ord}_p f'(x) = 0$).
Dans les deux situations étudiées précédemment (le lemme 1.2.1 et le lemme 1.2.3) le calcul de l'erreur marche comme dans le cas de la méthode standard de Hensel, sur une fonction équivalente à f dans un voisinage de l'approximation x.
Par conséquent, dans le cas où un relevé de $\tilde{x}$ existe (comme dans le cas du noyau du Verschiebung pour le relèvement canonique) il est possible d'extraire une approximation de la fonction f qui satisfait les conditions standard de Hensel. Par exemple:

— Dans le cas où $\mathrm{ord}_p f(x) > 2 \cdot \mathrm{ord}_p f'(x)$ la fonction locale définie dans un voisinage de x (la boule de centre x et rayon p^{k-e}) est donnée par: $g = p^{-e} f$ ainsi nous avons la condition de Hensel standard: $\mathrm{ord}_p g(x) = k - e$ et $\mathrm{ord}_p g'(x) = 0$.

— Pour le lemme 1.2.3 la situation est un peu plus complexe puisqu'il est possible d'avoir plus d'une solutions à partir de l'équation de l'erreur (l'équation (1.2)) et chaque solution définit une approximation de la fonction f dans une boule de centre x et de rayon p^α. L'objectif principal étant d'atteindre les conditions d'application du lemme 1.2.1, alors l'erreur correspondante peut être calculée en utilisant les fonctions d'approximation de f définies par:
Pour simplifier nous allons supposer $\mathrm{ord}_p f^{<j>}(x) = 0$, alors la condition $\mathrm{ord}_p f^{<j>}(x) + j\alpha = k$ détermine α sachant que celui-ci est nécéssairement ≥ 1.

$$g = p^{-j\alpha}\left(b_0 f + b_1 f^{<1>} + \cdots + b_{j-1} f^{<j-1>}\right) \quad \text{avec} \quad \mathrm{ord}_p b_{j-1} = 0.$$

Par suite la fonction déduite g satisfait la condition: $\mathrm{ord}_p g'(x) = 0$ (en utilisant la définition de j et le fait que $\mathrm{ord}_p f^{<j>}(x) = 0$). En particulier les évaluations en x de ces fonctions d'approximation sont données par une factorisation en facteurs premiers sur $\mathbb{Z}_q$ (en fonction de r) de l'équation "2.5" à la précision p^α (la condition de Newton). Par suite pour chaque " branche de Taylor " (définie par une solution r de l'équation "2.5") l'étape suivante converge vers un unique rélévé sur $\mathbb{Z}_q$ de x.

Nombre de relevés à partir d'une racine sur $\mathbb{F}_q$:

En résumé, à partir des lemmes 1.2.1 et 1.2.3 nous pouvons déduire que: pour $f \in \mathbb{Z}_q[X]$ et x une approximation d'une racine de f sur $\mathbb{Z}_q$ telle que $\mathrm{ord}_p f(x) = k$ et $\mathrm{ord}_p f'(x) = e$.

— Si $k > 2e$ alors seulement une racine de f sur $\mathbb{Z}_q$ se réduit sur x modulo p^k.

— Autrement le nombre des racines de f sur $\mathbb{Z}_q$ se réduisant modulo p^k sur x peut être plus d'une racine.

Les méthodes détaillées précédemment permettent sous certaines conditions de calculer le rélévé canonique d'une racine d'un polynôme dans $\mathbb{Z}_q[X]$ sans perte de précision. Dans l'exemple 1.2.2 on explique le calcule d'un point de torsion p d'un rélévé canonique d'une courbe elliptique ordinaire. Ensuite, nous voulons généraliser ces méthodes au cas d'un système polynomial multivarié de dimension zéro dans l'objectif de pouvoir calculer le rélévé de la p-torsion sur une variété abélienne ordinaire.

1.2.2 *Relèvement de Solutions dans un Système Polynomial multivarié*

Lorsque F est une fonction vectorielle multivariée associée à un système polynomial de dimension zéro défini par: $F(x_1, \cdots, x_k) = 0$ sur $\mathbb{Z}_q$ et on note par DF la matrice Jacobienne du système.
Nous supposons que $\tilde{X}$ une racine de F sur $\mathbb{Z}_q$ existe et que nous connaissons une approximation X (à précision inconnue) telle que $\mathrm{ord}_p F(X) = k$, $\mathrm{ord}_p \det(DF(X)) = e$ et $\tilde{X} = X \mod p$. Généralement les composantes de X peuvent être à des précisions différentes (comparées aux composantes de $\tilde{X}$). Par conséquent, nous devons d'abord connaître la précision de chaque composante de X. Et en séparant les erreurs dans les composantes, nous pourrions utiliser la méthode (le lemme 1.2.1 ou le lemme 1.2.3) correspondant à chaque "erreur-équation".
Soit S la Forme Normale de Smith (SNF) sur $\mathbb{Z}_q$ de la matrice Jacobienne $DF(X)$ de F en X telle que $DF(X) = M \cdot S \cdot N$ avec M et N inversibles sur $\mathbb{Z}_q$. Alors nous avons $DG(X) = M^{-1} \cdot DF(X) \cdot N^{-1} = S$ et $G(X) = M^{-1} \cdot F(XN^{-1})$ avec $DG(X)$ sous la forme

$$DG(X) = \mathrm{diag}(p^{e_1}, p^{e_2}, ..., p^{e_n}) \quad \text{où} \quad e = e_1 + \cdots + e_n.$$

Proposition 1.2.4. *Lorsque l'on suppose que chaque composante X_i de X est à la précision p^{k_i}. Alors on peut déterminer avec les mêmes complexités que l'algorithme de Hensel standard les approximations des possibles $\tilde{X}$ à la précision $N > k_i$ en utilisant:*

— *la méthode proposée dans le lemme 1.2.1 si chaque $k_i > e_i$;*

— *sinon en utilisant celle proposée dans le lemme 1.2.3.*

Démonstration. L'information sur les valuations données par le calcul de SNF est nécéssaire à defaut d'un résultat connu (comme dans les sections 7.1 et 7.2 et la proposition 7.2.2) sur la matrice Jacobienne.
Comme le changement de bases n'affectent pas les erreurs que nous voulons déterminer, on part directement du système sous la forme G définie comme précédemment. Ainsi l'algorithme de Newton en fonction X fonctionnera de façon similaire au cas univarié (des lemmes précédents). Lorsque nous avons $\mathrm{ord}_p G_i(X_i) = k_i$ avec $k_i > e_i$ pour tout i, alors les possibles rélévés sur $\mathbb{Z}_q$ de X (à la précision $N > \max(k_i)$) peuvent être déterminer en

utilisant sur G la méthode proposée dans le lemme 1.2.1.
Dans le cas contraire, certaines équations ont besoin d'informations supplémentaires, alors globalement on calcule les autres dérivées successives comme suggérer dans le lemme 1.2.3. Ainsi on détermine les approximations de relevés correspondant au lemme 1.2.1 pour les étapes suivantes.
À partir des équations données par le dévéloppement de Taylor de F en $(X + Rp^k)$, un calcul de bases de Grœbner lexicographique modulo p^N permet de déterminer l'erreur R pour l'étape suivante. □

Il est nécéssaire à chaque étape d'évaluer à la bonne précision sur sa chaque composante afin d'éviter des pertes de précision.

1.2.3 *Amélioration par Évaluation Directe du Sytème*

Cependant lorsque que l'on travaille sur certaines charactéristiques p un peu plus grand: *En une précision k, évaluer directement un système en des valeurs est de complexités plus légères que de déterminer le système global.*
On considère un système polynomial à plusieurs variables S défini sur $\mathbb{Z}_q$ par une rélation:

$$\mathcal{R}(F, X)$$

où F est une fonction qu'on peut évaluer rapidement à une précision k en une valeur X. Lorsque un élément P satisfait sur $\mathbb{Z}_q$ la rélation $\mathcal{R}(F, X)$; cela signifie que l'évaluation de F en P s'annulle: $F(P) = 0$. Alors la méthode de Newton suivante permet de calculer le relevé de P modulo p à une précision N en remplaçant les calculs de dérivées par des évaluations directes de F.
Supposons que nous connaissons P à précision k et nous sommes dans le cas d'un Newton où intervient seulement la Jacobienne J (exemple le lemme 1.2.1: lorsque on a $k > 2e$ où $e = \mathrm{ord}_p J(P)$) alors on peut déterminer P à la précision $2k - e$, en évaluant F en r déformations spécifiques et distinctes $P + R_i.p^k$ avec $i \in \{1, 2, \cdots r\}$ où r est le nombres de composantes de la variable X. À partir du développement de Taylor de F on a :

$$J(P).R_i = \frac{1}{p^k}\left[F(P + R_i.p^k) - F(P)\right] \mod p^{2k}$$

En posant R_i égal au i-ième vecteur colonne de la base canonique de $\mathbb{R}^r$. Alors modulo p^k, la i-ième colonne de la matrice Jacobienne J en P est donnée par :

$$C_i = \frac{F(P + R_i.p^k) - F(P)}{p^k}$$

Dans les cas où l'on a besoin de la Héssienne en plus de la Jacobienne pour réaliser un algorithme de Newton (comme c'est détaillé dans les exemples $k \leq 2e$, dans les sous-sections plus haut) nous pouvons prendre d'autres déformations pour déterminer la matrice Héssienne. Ainsi procéder comme dans l'exemple suivant : On suppose que $F(X, Y) = 0$ est un système d'équation à deux variables et P une solution de ce système à précision k que l'on veut relever par une évaluation éfficace de F en P. On pose $R_1 = (1, 0)$, $R_2 = (0, 1)$ et $R_5 = (1, 1)$, alors $P_1 = P + R_1 p^k$, $P_2 = P + R_2 p^k$, $P_3 = P - R_1 p^k$, $P_4 = P - R_2 p^k$ et $P_5 = P + R_5 p^k$.

$$J_X = \frac{F(P_1) - F(P_3)}{2p^k} \quad \text{et} \quad J_Y = \frac{F(P_2) - F(P_4)}{2p^k}$$

$$H_X = \frac{F(P_1) - J_X}{p^{2k}}, \qquad H_Y = \frac{F(P_2) - J_Y}{p^{2k}} \quad \text{et}$$
$$H_{XY} = \frac{F(P_5) - F(P) - J_X - J_Y - H_X - H_Y}{p^{2k}}$$

Alors H_X est la première colonne de la matrice Héssienne $H(P,P)$ modulo p^k (représentant les coefficients en ∂X^2), H_{XY} est sa seconde colonne (en $\partial X \partial Y$) et H_Y est sa troisième colonne (en ∂Y^2).

En dimension supérieure notre méthode semble plus pratique qu'une possible généralisation de la méthode de Satoh, pour calculer le rélévé de la p-torsion d'une variété abélienne ordinaire. En effet à partir de la dimension 2, le polynôme de division présente une taille et structure un peu plus complexes nécéssitant des opérations très coûteuses.

1.3 CALCUL DE NORME SUR UNE EXTENSION NON-RAMIFIÉE DE $\mathbb{Q}_p$

Dans cette partie nous faisons un bref rappel sur deux des algorithmes de calcul rapide de norme $N_{\mathbb{Q}_q/\mathbb{Q}_p}$. Ces algorithmes présentent de grands interêts dans la mésure où elles remplacent l'évaluation par tous les conjugués succéssifs Σ^i du Frobenius Σ dans le calcul des valeurs propres de l'endomorphisme Frobenius $x \mapsto x^q$.
Par définition nous avons :

$$N_{\mathbb{Q}_q/\mathbb{Q}_p}(x) = \prod_{i=0}^{n-1} \Sigma^i(x)$$

1.3.1 *Méthode Analytique*

Satoh, Skjernaa et Taguchi ont proposé dans [100] un algorithme de calcul $N_{\mathbb{Q}_q/\mathbb{Q}_p}(x)$ basé sur une méthode analytique.
On considère $ord_p(x-1) > 1/(p-1)$, alors :

$$N_{\mathbb{Q}_q/\mathbb{Q}_p}(x) = \exp\left(\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p} \log(x)\right)$$

Dans le cas où l'on a pas $ord_p(x-1) > 1/(p-1)$. Soit $\dot{x} \in \mathbb{Z}_q$ le relevé de Teichmüller de $\pi(x) \in \mathbb{F}_q$, alors on a : $ord_p(\dot{x}^{-1}x - 1) > 1/(p-1)$ pour $p \geq 3$. Pour $p = 2$ on peut prendre le carré de $\dot{x}^{-1}x \mod 2^{N+1}$. Et on a :

$$N_{\mathbb{Q}_q/\mathbb{Q}_p}(x) = N_{\mathbb{Q}_q/\mathbb{Q}_p}(\dot{x}) N_{\mathbb{Q}_q/\mathbb{Q}_p}(\dot{x}^{-1}x)$$

Par suite on considère que x vérifie $ord_p(x-1) > 1/(p-1)$, les méthodes suivantes rendent performents les calculs de $log(x)$ et $exp(x)$ sur $\mathbb{Z}_q$.
Si l'on pose $x = \sum_{i=1}^{n-1} a_i X^i$, cela implique : $\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(x) = \sum_{i=1}^{n-1} a_i \mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(X^i)$.
$\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(X^i)$ sont des valeurs précalculées en utilisant la méthode dite de Newton :

$$\begin{aligned}
\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(X) &\equiv -M_{n-1} (mod p^N),\\
\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(X^2) &\equiv -\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(X) M_{n-1} - 2M_{n-2} (mod p^N),\\
&\vdots\\
\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(X^i) &\equiv -\sum_{j=1}^{i-1} \mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_p}(X^{i-j}) M_{n-j} - iM_{n-i} (mod p^N)
\end{aligned}$$

avec $M = \sum_{i=1}^{n} M_i X^i$ et pour une précision N fixée.
Soit $x \in \mathbb{Z}_q$ le logarithme et l'exponentielle p-adique de x sont définis par :

$$log(x) = \sum_{k=1}^{\infty} (-1)^{k-1} \frac{(x-1)^k}{k} \quad et \quad exp(x) = \sum_{k=1}^{\infty} \frac{x^k}{k!}$$

log converge pour $ord_p(x-1) > 0$ et exp converge for $ord_p(x) > 1/(p-1)$.
Pour $x \in \mathbb{Z}_q$ avec $ord_p(x-1) \geq 1$ il est prouvé que $ord_p(x^{p^k} - 1) > k$ pour $k \in \mathbb{N}$ et :

$$log(x) \equiv p^{-k} \left(log(x^{p^k}) \mod p^{N+k} \right) \mod p^N$$

Ainsi $log(a^{p^k}) \mod p^{N+k}$ se calcule plus facilement dans $\mathbb{Z}_q / p^{N+k}\mathbb{Z}_q$.
Pour le cas de $exp(x)$ on part d'une majoration de la valuation $ord_p(i!)$ donnée par : $ord_p(i!) \leq (i-1)/(p-1)$. Cela implique

$$exp(x) \equiv \sum_{1 \leq i < \beta} \frac{x^i}{i!} \mod p^N \quad et \quad \beta = \frac{(p-1)N - 1}{(p-1) ord_p(x) - 1}$$

.

1.3.2 *Méthode du Résultant*

Dans une autre approche de calcul rapide de la norme, Harley a proposé [45] un algorithme qui est asymptotiquement parmi les meilleurs. Sa méthode utilise un calcul de résultant, elle-même calculée avec une variante de l'algorithme de calcul rapide du pgcd de Mœnck [83].

Lorsque $x = \sum_{i=1}^{n-1} a_i X^i \in \mathbb{Z}_q$ alors on définit le polynôme $A(X) = \sum_{i=1}^{n-1} a_i X^i \in \mathbb{Z}_p[X]$. Alors nous aurons :

$$N_{\mathbb{Q}_q/\mathbb{Q}_p}(x) = \prod_{i=1}^{n-1} A\left(\Sigma^i(\theta)\right) = Res\left(M(X), A(X)\right)$$

où $\alpha \in \mathbb{Z}_q$ est une racine de M.

1.3.3 *Base Normale Gaussienne*

Nous avons précédement résumé quelques méthodes rapides de calcul de norme sur $\mathbb{Z}_q$ dans le cas où le polynôme irréductible *était de Teichmuller*. Cependant lorsque le corps $\mathbb{F}_{p^n}$ admet une *base normale Gaussienne* c'est-à dire une base de la forme $\{\lambda\alpha / \ \lambda \ parcourant \ \mathrm{Gal}\left(\mathbb{F}_q/\mathbb{F}_p\right)\}$ pour un $\alpha \in \mathbb{F}_q$ donné par:

$$\alpha = \sum_{i=0}^{t-1} \gamma^{\tau^i}$$

où τ est une racine t-ième primitive de l'unité dans un corps $\mathbb{Z}/(Nt+1)\mathbb{Z}$ avec $(Nt+1) \neq p$ et γ une racine $(Nt+1)$-ième primitive de l'unité sur une extension de $\mathbb{F}_q$.
α est appelé période gaussienne de (N,t). Et engendre une base normale pour $\mathbb{F}_{q^N}/\mathbb{F}_q$ si et seulement si $(Nt/e, N) = 1$ avec e l'ordre de q modulo $(Nt+1)$.
Par exemple il existe 26 valeurs pour un nombre premier N entre 160 et 600 ayant une base normale Gaussienne de type 2 ou 4 sur l'extension $\mathbb{F}_{2^N}/\mathbb{F}_2$ [60].

Comme tout relèvement d'une base de $\mathbb{F}_q/\mathbb{F}_p$ est une base de $\mathbb{Q}_q/\mathbb{Q}_p$, par suite nous allons considérer le même générateur α pour la base normale de l'extension $\mathbb{Q}_q(\alpha)/\mathbb{Q}_q$. Ainsi pour Σ désignant le Frobenius de $\mathrm{Gal}\left(\mathbb{Q}_q(\alpha)/\mathbb{Q}_q\right)$ on a $\Sigma(\gamma) = \gamma^q$ car $\gamma^{Nt+1} = 1$ et $q^{Nt} \equiv 1 \mod Nt+1$.

Exemple 1.3.1. On part de $\mathbb{F}_p$ comme de corps base avec $t = 1$ et $\gamma = \alpha \in \mathbb{Q}_{p^N}$ un élément normal ; $\pi(\alpha)$ est un élément normal générateur de la base normale Gaussienne sur $\mathbb{F}_p$.

$$\mathfrak{B} = \left\{\alpha, \sigma(\alpha), \cdots, \sigma^{N-1}(\alpha)\right\} = \left\{\alpha, \alpha^2, \cdots, \alpha^N\right\}$$

Pour la multiplication dans $\mathbb{Z}_{p^N} := \mathbb{Z}_p[X]/m(X)$ où $m(X) \in \mathbb{Z}_p[X]$ est le polynôme minimal de α, la méthode introduite par H.Y.Kim et autre dans [60] consiste à transporter $\mathbb{Z}_{p^N}$ vers l'anneau $\mathbb{Z}_p[X]/(X^{N+1}-1)$ via l'application:

$$\sum_{i=0}^{N-1} a_i X^i \longmapsto \sum_{i=0}^{N-1} a_i X^i + 0X^N.$$

Alors pour tous $A, B \in \mathbb{Z}_p[X]/F(X) \in \mathbb{Z}_p[X]/F(X)$:

$$A \cdot B \equiv \left(A \cdot B \mod X^{N+1}-1\right) \mod F(X)$$

Alors pour tout $A(X) = a_0 + a_1X + \cdots + a_NX^N \in \mathbb{Z}_p[X]/(X^{N+1}-1)$, le Frobenius de $A(\alpha)$ est donné:

$$\Sigma\left(\sum_{i=0}^{N} a_i\alpha^i\right) = \sum_{i=0}^{N} a_i\alpha^{pi} = a_0 + \sum_{j=1}^{N} a_{j/p}\alpha^j \quad avec \quad j/p \in (\mathbb{Z}/(N+1)\mathbb{Z})^*.$$

et pour tout $k \in \mathbb{Z}$

$$\Sigma^k\left(\sum_{i=0}^{N} a_i\alpha^i\right) = a_0 + \sum_{j=1}^{N} a_{j/p^k}\alpha^j, \quad avec \quad j/p^k \in (\mathbb{Z}/(N+1)\mathbb{Z})^*.$$

Ainsi le calcul de $\Sigma^k(A)$ se fait par simple permutation sur $(\mathbb{Z}/(N+1)\mathbb{Z})^*$.
Par suite on en déduit un calcul de norme rapide sur $\mathbb{Q}_{p^N}/\mathbb{Q}_p$ modulo p^M. Soit $N = \sum_{i=0}^{r} n_i 2^i$ la décomposition binaire de N.
On pose:
$[n_0, n_1, \ldots, n_j] = \sum_{i=0}^{j} n_i 2^i$, $M_i = \left(\sigma^{2^{i-1}} M_{i-1}\right) M_{i-1}$ et $M_0 = A$
alors

$$\begin{aligned} N_{\mathbb{Q}_{p^N}/\mathbb{Q}_p}(A) =& A\left(A^{\sigma}\right)\ldots A\left(A^{\sigma^{N-1}}\right) \\ =& M_{r-1}\prod_{i=0}^{r-2}\left(\sigma^{N-[n_0,n_1,\ldots,n_i]_2} M_i\right)^{n_i} \end{aligned}$$

En général lorsque le corps de base admet une base normale Gausienne de type t H.Y.Kim et autres introduisirent un algorithme du type "*diviser pour règner*" permettant de calculer $N_{\mathbb{Q}_{p^N}/\mathbb{Q}_p}(A)$ à partir de la formule précédente et à une précision m avec une complexité en temps de $O(\log(n)(mn)^\mu)$ et de $O(nm)$ en espace.

2

RELÈVEMENT CANONIQUE DE COURBES ELLIPTIQUES ORDINAIRES

2.1 COURBES ELLIPTIQUES

Au debut de ce chapitre, nous rappellons quelques résultats sur les courbes elliptiques définies sur un corps quelconque $\mathbb{k}$ et ensuite les résultats sur celles définies sur $\mathbb{C}$ en utilisant les reférences suivants: [65, 78, 82, 105, 106]. Après nous détaillons les différentes améliorations de la méthode de Satoh pour le calcul du polynôme caractéristique.
La dernière partie du chapitre concerne nos nouveaux résultats portant sur les algorithmes (la section 2.6.3) de calcul du polynôme caractéristique en une complexité au plus linéaire en p. Ces algorithmes constituent une amélioration considérable de la complexité en p dans la méthode de Satoh.

Une courbe elliptique sur un corps $\mathbb{k}$ est une courbe projective lisse de genre 1 sur $\mathbb{k}$ avec un point donné O sur $\mathbb{k}$.
À partir du *théorème de Riemann-Roch* on montre qu'il existe des fonctions x, y dans le corps de fonctions $\mathbb{k}(E)$ de E, appelées fonctions de coordonnées de Weierstrass n'ayant pas de pôles en dehors de O et telles que:

$$ord_O(x) = -2, \quad ord_O(y) = -3 \quad et \quad \frac{y^2}{x^3}(O) = 1.$$

Les points de la courbe elliptique sont alors solutions d'une équation homogène de $\mathbb{P}^2(\overline{\mathbb{k}})$:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\,,\ a_i \in \mathbb{k}$$

Ainsi les coordonnées affines x et y sont liées par l'equation affine :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\,,\ a_i \in \mathbb{k}$$

Avec $x = X/Z$ et $y = Y/Z$ et le discriminant

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \quad \text{non nul.}$$

où

$$b_2 = a_1^2 + 4a_2,\ b_4 = a_1a_3 + 2a_4,\ b_6 = a_3^2 + 4a_6,$$
$$b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2.$$

Alors on appelle j-invariant de la courbe elliptique E:

$$j(E) = (b_2^2 - 24b_4)^3/\Delta.$$

Exemple 2.1.1. Pour une courbe elliptique E définie sur $\mathbb{k}$, à partir de changement de variables linéaires sur x et y l'equation de E se réduit comme suite:

— Lorsque $char(\Bbbk) = 2$, et $E : y^2 + xy = x^3 + a$ alors $\Delta = -a - 432a^2$ et $j(E) = \dfrac{-1}{\Delta}$,

— Lorsque $char(\Bbbk) = 3$, et $E : y^2 = x^3 + ax^2 + b$ alors $j(E) = \dfrac{-256a^6}{4a^3b + 27b^2}$,

— Lorsque $char(\Bbbk) \neq, 2, 3$, et $E : y^2 = x^3 + ax + b$ alors $\Delta = -16(4a^3 + 27b^2)$ et $j(E) = -\dfrac{342(a^3)}{\Delta}$.

D'autre part une courbe elliptique peut être munie d'une structure de groupe abélien dont l'élément neutre est O. Comme toute courbe elliptique est définie par une cubique, par le théorème de Bézout, une droite de $\mathbb{P}^2(\overline{\Bbbk})$ intersecte la courbe en exactement 3 points (en comptant avec multiplicités). La loi de groupe est une conséquence de la colinéarité entre ces trois points: *leur somme est nulle*. Alors la somme de 2 points est le symétrique du troisième par l'involution hyperelliptique. Et tout ceci s'interprete algébriquement par les coordonnées de ces points.
Par exemple lorsque l'on considère que la caractéristique du corps $\Bbbk$ est différente de 2 ou 3 et $y^2 = x^3 + ax + b$ une équation de la courbe elliptique E. Soit $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$ deux points de $E - \{O\}$, alors: Si $x_1 = x_2$ et $y_1 = -y_2$ alors $P_1 + P_2 = O$, sinon

$$on \quad pose \quad : \lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & si \quad P_1 \neq P_2 \\ \dfrac{3x_1^2 + a}{2y_1} & sinon \end{cases} \quad \text{alors} \quad \begin{cases} x_3 = & \lambda^2 - x_1 - x_2, \\ y_3 = & -\lambda x_3 - y_1 + \lambda x_1. \end{cases}$$

et $P_1 + P_2 = P_3$.

Points de n-Torsion et Polynômes de n-Division

Soit $E/\Bbbk$ une courbe elliptique, pour un point P sur E on note par $[m]P = P + ... + P$ (m-facteurs) pour tout $m \in \mathbb{Z}$. Alors le sous-groupe $E[m] = \{P \in E(\overline{\Bbbk})/mP = O\}$ de E est appelé le sous-groupe de m-torsion.

— Lorsque $char(\Bbbk) = p$ et $E[p^r] = O$ pour un $r \in \mathbb{N}_{>0}$, la courbe elliptique $E/\Bbbk$ est dite *supersingulière*, et dans ce cas $j(E) \in \mathbb{F}_{p^2}$.

— Et une courbe elliptique non-supersingulière est appelée ordinaire.

Lorsque $char(\Bbbk) \neq 2, 3$ et ne divide pas $m \geq 3$ alors on a : $E : y^2 = x^3 + Ax + B$ ainsi,

$$[m](x, y) = \left(\frac{\phi_m(x)}{\psi_m^2(x)}, \frac{\omega_m(x, y)}{\psi_m^3(x, y)} \right)$$

$$\text{où} \quad \phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1} \quad et \quad \omega_m = (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)/(4y).$$

ψ_m est appelé polynôme de n-torsion (ou polynôme de n-division) et est associé à l'équation de la courbe. Un point $P = (x, y)$ sur E est un point de m-torsion si et seulement si ses coordonnées constituent une solution de ψ_m.

Exemple 2.1.2. Soit $E : y^2 = x^3 + Ax + B$ une courbe elliptique les polynômes de n-division associés à E sont des polynômes dans $\mathbb{Z}[A, B, x, y]$ définies par :

$$\psi_1 = 1, \quad \psi_2 = 2y, \quad \psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,$$
$$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$$

et par suite on montre que :

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad pour \quad m \geq 2$$
$$et \quad \psi_{2m} = (2y)^{-1}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \quad pour \quad m \geq 3.$$

Morphismes entre Courbes Elliptiques

Les courbes elliptiques étant des variétés projectives lisses de dimension 1 et de genre 1, les applications rationnelles entres elles sont des *morphismes* de courbes algébriques.
Soit $\phi : E_1 \longrightarrow E_2$ un morphisme de courbe elliptiques alors il est soit constant ou soit surjectif. Et on définit son *tiré en arrière* ("pullback") par:

$$\phi^* : \overline{\Bbbk}(E_2) \longrightarrow \overline{\Bbbk}(E_1), \qquad \phi^* f = f \circ \phi$$

et son degré par $\deg \phi = 0$ si ϕ est constant sinon

$$\deg \phi = [\overline{\Bbbk}(E_1) : \phi^* \overline{\Bbbk}(E_2)].$$

Ainsi on dit que ϕ est séparable, inséparable, ou purement inséparable si l'extension de corps $\overline{\Bbbk}(E_1)/\phi^*\overline{\Bbbk}(E_2)$ a la propriété correspondante et on note par $\deg_s \phi$ et $\deg_i \phi$ respectivement le degré separabilité et d'inseparabilité de l'extension. Et lorsque $\Bbbk$ est un corps fini de $q = p^n$ éléments, ϕ se factorise en :

$$\phi : E_1 \xrightarrow{\pi_q} E_1^{\pi_q} \xrightarrow{\phi_s} E_2$$

où π_q est le q-ième puissance Frobenius et le morphisme ϕ_s est séparable.

D'autre part une courbe elliptique E étant une courbe algébrique projective de genre 1, on note par $Pic(E) = Div(E)/Prin(E)$ le *groupe des classes de diviseurs* aussi appelé le *Groupe de Picard*. Alors il existe un isomorphisme entre E et $\mathrm{Pic}_0(E) = \mathrm{Div}_0(E)/\mathrm{Prin}(E)$ sa variété Jacobienne, définie par $P \in E \longmapsto \text{classe}[(P) - (O)] \in \mathrm{Pic}_0(E)$. Et on a la suite exacte suivante :

$$1 \longrightarrow \overline{\Bbbk}^* \longrightarrow \overline{\Bbbk}(E)^* \xrightarrow{\text{div}} \mathrm{Div}_0(E) \longrightarrow \mathrm{Pic}_0(E) \longrightarrow 0$$

Isogénies

Une isogénie ϕ est un morphisme non trivial entre courbes elliptiques qui est aussi un homorphisme de groupe. Soit $\phi : E_1 \longrightarrow E_2$ une isogénie de courbes elliptiques. Lorsque $\phi(E_1) \neq \{0\}$ on dit que E_1 et E_2 sont isogènes et on note par $\mathrm{Hom}\,(E_1, E_2)$ le $\mathbb{Z}$-module formé par le morphisme 0 et les isogénies de E_1 vers E_2 sur $\overline{\Bbbk}$. L'ensemble $\mathrm{End}(E_1) = \mathrm{Hom}\,(E_1, E_1)$ muni $+$ et de la loi composition des applications est un anneau.

Proposition 2.1.3. *Soit $\phi : E_1 \longrightarrow E_2$ une isogénie de courbes elliptiques:*

- *si ϕ est séparable alors on a $\#\ker(\phi) = \deg(\phi)$, sinon on a $\#\ker(\phi) = \deg_s(\phi)$.*
- *si ϕ est une ℓ-isogénie (isogénie séparable de degré ℓ), elle admet une unique isogénie duale $\hat{\phi} : E_2 \longrightarrow E_1$ telle que $\phi \circ \hat{\phi} = [\ell]$ sur E_2 et $\hat{\phi} \circ \phi = [\ell]$ sur E_1. Sous ces conditions $\phi(E_1[\ell]) = \mathrm{Ker}\,\hat{\phi}$.*
- *Pour tout premier $\ell \neq char(k)$, on a $E_1[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ et les $\ell + 1$ sous-groupes cycliques de $E[\ell]$ sont les noyaux de ℓ-isogenies.*

Démonstration. Aller à [65, 105]. □

Soit E une courbe elliptique dont l'équation de Weierstrass est $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. On appelle *invariant différentiel* de E, noté ω l'élément de Ω_E (le $\overline{\Bbbk}(E)$-espace vectoriel des formes différentielles) défini par :

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x + 2a_2x + a_4 - a_1y}$$

Ainsi pour tout point Q de E le tiré en arrière de ω le long de la translation par Q est ω lui-même. Et de manière générale lorsque $\phi : E_1 \longrightarrow E_2$ est une isogénie entre courbes elliptiques et ϕ_x et ϕ_y les applications coordonnées de ϕ, on a:

$$\phi^*\omega_2 = \alpha(\phi_x, \phi_y)d\phi_x \quad avec \quad \omega_2 = \alpha dx \in \Omega_{E_2}.$$

Alors on montre que $\phi^*(\omega_2) = c \cdot \omega_1$ pour une constante $c \in \overline{\Bbbk}$. Et pour $c = 1$, l'isogénie ϕ est dite *normalisée*.

Isomorphismes

Soient deux courbes elliptiques

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
$$\text{et} \quad E' : y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6$$

sur $\Bbbk$, on dira que E et E' sont isomorphes lorsque l'on peut obtenir l'équation de Weierstrass de l'une en appliquant à celle de l'autre une application de la forme:

$$(x, y) \longmapsto (u^2x + r,\ u^2y + su^2x + t) \quad \text{avec} \quad u, r, s, t \in \Bbbk \quad \text{et} \quad u \neq 0.$$

Ce qui implique :

$$ua_1 = a'_1 + 2s, \quad u^2a_2 = a'_2 - sa'_1 + 3r - s^2, \quad u^3a_3 = a'_3 + ra'_1 + 2t,$$
$$u^4a_4 = a'_4 - sa'_3 + 2ra'_2 - (t + rs)a'_1 + 3r^2 - 2st$$
$$u^6a_6 = a'_6 + ra'_4 + r^2a'_2 + r^3 - ta'_3 - t^2 - rta'_1$$

Par conséquent on a:

$$u^{12}\Delta = \Delta', \quad j(E) = j(E') \quad \text{et} \quad u^{-1}\omega = \omega'.$$

Ainsi deux courbes elliptiques isomorphes sur $\Bbbk$ ont le même j-invariant. On montre dans [105] que la réciproque est vraie sur $\overline{\Bbbk}$. Et pour tout $j_0 \in \overline{\Bbbk}$ il existe une courbe elliptique définie sur $\Bbbk(j_0)$ dont j_0 est le j-invariant.

2.2 ESPACE DE MODULE

Soit Λ un réseau complexe, c'est à dire un sous groupe complexe discret admettant une $\mathbb{R}$-base.

$$\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} \quad avec \quad \frac{\omega_1}{\omega_2} \notin \mathbb{R}$$

On associe au réseau Λ, la fonction $\wp$ de Weierstrass définie par :

$$\wp(z) = \frac{1}{z^2} + \sum_{w \in \Lambda - \{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

— $\wp$ est une fonction elliptique pour Λ c'est à dire elle est méromorphe sur $\mathbb{C} \cup \{\infty\}$ et $\wp(z+w) = \wp(z)$ pour tout $z \in \mathbb{C}$ et $w \in \Lambda$.

— de plus elle vérifie l'équation differentielle :

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3, \quad pour \quad tout \quad z \notin \Lambda$$

où $g_2(\Lambda) = 60E_4(\Lambda)$, $g_3(\Lambda) = 140E_6(\Lambda)$ et $E_{2k}(\Lambda) = \sum_{w\in\Lambda-\{0\}} w^{-2k}$ la série d'Eisenstein de poids $2k$.

D'autre part l'équation $y^2 = 4x^3 - g_2x - g_3$ définit une courbe elliptique sur $\mathbb{C}$. Et nous avons le théorème suivant.

Théorème 2.2.1. *L'application :*

$$\begin{aligned} \mathbb{C}/\Lambda &\to E \subset \mathbb{P}^2(\mathbb{C}) \\ 0 &\mapsto [0:1:0] \\ z &\mapsto [\wp_\Lambda(z) : \wp'_\Lambda(z) : 1] \end{aligned}$$

est un isomorphisme de Surfaces de Riemann et aussi un morphisme de groupes.

Démonstration. Aller à [106, Corollaire 4.3]. □

Réciproquement lorsque l'on considère une courbe elliptique E sur $\mathbb{C}$ avec x et y comme coordonnées de Weierstrass. Alors

$$\omega_1 = \int_\alpha dx/y \quad \text{et} \quad \omega_2 = \int_\beta dx/y \quad \text{tels que } \alpha \text{ et } \beta \text{ sont des lacets sur } E/\mathbb{C}$$

sont $\mathbb{R}$-linéairement indépendants et définissent un réseau Λ. Et l'application :

$$\begin{aligned} E/\mathbb{C} &\longrightarrow \mathbb{C}/\Lambda \\ P &\longmapsto \int_{\mathcal{O}}^{P} dx/y \mod \Lambda \end{aligned}$$

est l'inverse de l'isomorphisme de Surfaces de Riemann du Théorème 2.2.1 (aller à [106, Proposition 5.2]).

Ainsi deux courbes elliptiques $\mathbb{C}/\Lambda_1$ et $\mathbb{C}/\Lambda_2$ sont isomorphes si seulement si les réseaux Λ_1 et Λ_2 sont homothétiques i.e $\Lambda_1 = \alpha\Lambda_2$ avec $\alpha \in \mathbb{C}^*$. Comme tout réseau est homothétique à un réseau de base $[1, \tau]$ avec $\mathcal{I}m(\tau) > 0$. On en déduit que sur le *demi-plan de Pointcaré* $\mathcal{H}_1 = \{z \in \mathbb{C};\ \mathcal{I}m(z) > 0\}$ chaque point τ représente (à isomorphisme près) une courbe elliptique.

D'autre part le groupe modulaire $\Gamma_1 = \{\gamma \in M_2(\mathbb{Z});\ det(\gamma) = 1\}$ agit sur $\mathcal{H}_1$ par $\begin{pmatrix} a & b \\ c & d \end{pmatrix}.\tau = \dfrac{a\tau + b}{c\tau + d}$ pour $\tau \in \mathcal{H}_1$.

Polynômes Modulaires

Définition 2.2.2. Soit Γ un sous groupe de Γ_1 d'indice fini. Une forme Γ-modulaire de poids k est une function $f : \mathcal{H} \longrightarrow \mathbb{C}$ holomorphe sur $\mathcal{H}_1^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$ et modulaire sur Γ de poids k c'est à dire :

$$f(\gamma.\tau) = (c\tau + d)^k f(\tau)$$

pour $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ et $\tau \in \mathcal{H}_1$.

Une fonction Γ-modulaire peut être vu comme quotient de deux formes modulaires de même poids.

Exemple 2.2.3. La fonction Γ_1-modulaire appelée *fonction j-invariant* définie par $j(\tau) = 1728\frac{(60E_4(\tau))^3}{\Delta(\tau)}$. Elle est holomorphe sur $\mathcal{H}_1$ avec des coéfficients de Fourier entiers.

$$\begin{aligned} j(\tau) &= q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 \\ &+ 20245856256q^4 + 333202640600q^5 + 4252023300096q^6 + \cdots \end{aligned}$$

Théorème 2.2.4. *Le corps des fonctions Γ_1-modulaires notée $\mathbb{C}_{\Gamma_1}$ est égal $\mathbb{C}(j)$ tel que $j(\mathcal{H}_1) = \mathbb{C}$.*

Démonstration. Aller à [101, Théorème 2.5.1] . □

Corollaire 2.2.5. *$j(\tau) = j(\tau') \iff \tau$ et τ' sont homothétiques.*

Soit p un nombre premier, on définit la matrice $R = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ et la fonction $j_p(\tau) := j(R.\tau)$, alors j_p est une fonction modulaire sur $\Gamma^0(p) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1,\ b \equiv 0 \mod p \right\}$.
Nous avons $\mathbb{C}_{\Gamma^0(p)} = \mathbb{C}(j, j_p)$ et le polynôme minimal de j_p noté $\Phi_r(X, j)$ est élément de $\mathbb{Z}[X, j]$.
Les représentants des classes à droite de $\Gamma_1/\Gamma^0(p)$ sont: $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ et les T^i où $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ et $i = 1, ...p-1$.

Les actions de ces derniers sur $\tau \in \mathcal{H}_1$ donnent $p\tau$ et $\frac{\tau+i}{p}$ modulo Γ_1 qui sont homothétiques au réseaux définissant les tores p-isogènes à $\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$.
En effet les fonctions holomorphes entre tores, qui envoient 0 sur 0 définies par:

$$\begin{array}{ccccc} \mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}) & \longrightarrow & \mathbb{C}/(\mathbb{Z}+\frac{\tau+i}{p}\mathbb{Z}) & & \\ z & \longmapsto & z & & \end{array} \quad et$$

$$\begin{array}{ccccc} \mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}) & \longrightarrow & \mathbb{C}/(\mathbb{Z}+p\tau\mathbb{Z}) \\ z & \longmapsto & z \end{array}$$

sont les p-isogenies partant de $\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$.

Définition 2.2.6. Le polynôme modulaire classique de niveau p en $j(\tau)$, noté $\Phi_p(X, j(\tau))$ est le polynôme dont les racines sont les j-invariants de toutes les courbes elliptiques p-isogènes à la courbe de $j(\tau)$.

$$\Phi_p(X, j(\tau)) := \prod_{i=1}^{p+1}(X - j_p(R_i \cdot \tau)) \quad \text{avec} \quad R_i \quad \text{parcourant} \quad \{S, T^i,\ i = 1, ...p-1\}$$

Exemple 2.2.7.

$$\begin{aligned} \Phi_3(X,\ Y) = {} & X^4 - X^3Y^3 + 2232X^3Y^2 - 1069956X^3Y + 36864000X^3 \\ & + 2232X^2Y^3 + 2587918086X^2Y^2 + 8900222976000X^2Y \\ & + 452984832000000X^2 - 1069956XY^3 + 8900222976000XY^2 \\ & - 770845966336000000XY + 1855425871872000000000X + Y^4 \\ & + 36864000Y^3 + 452984832000000Y^2 \\ & + 1855425871872000000000Y. \end{aligned}$$

2.3 ANNEAU DES ENDOMORPHISMES D'UNE COURBE ELLIPTIQUE

Soit E une courbe elliptique définie sur un corps $\Bbbk$. L'anneau des endomorphismes de E avec la multiplication par 0 muni de l'addition et de la composition des applications est un anneau noté $\mathrm{End}(E)$.
Les endomorphismes de multiplication par des entiers s'identifient à $\mathbb{Z}$ alors $\mathbb{Z} \subset \mathrm{End}(E)$. De plus lorsque le corps $\Bbbk$ est $\mathbb{F}_q$ nous avons : $\mathbb{Z}[\pi_q] \subset \mathrm{End}(E)$ où π_q est l'endomorphisme de Frobenius.

Théorème 2.3.1. *Soit E une courbe elliptique définie sur le corps $\Bbbk$, alors l'anneau $\mathrm{End}(E)$ est isomorphe :*

- *soit à $\mathbb{Z}$;*
- *soit à un ordre dans un corps quadratique imaginaire $\mathbb{Q}(\sqrt{-D})$ avec $D > 0$, si E est ordinaire ;*
- *soit à un ordre maximal dans un corps de quaternion ramifié $p = char(\Bbbk)$ et à ∞, si E est supersingulière.*

Démonstration. Aller à [65]. □

Dans le cas où la courbe elliptique E est définie sur $\mathbb{F}_q$, l'automorphisme de Frobenius π_q vérifie l'équation quadratique:

$$X^2 - tX + q = 0$$

où t est appelé la trace de π_q et vérifie la rélation $|t| \leq 2\sqrt{q}$ appelée les bornes de Hasse.

Théorème 2.3.2. *Soient E une courbe elliptique ordinaire sur $\mathbb{F}_q$ et $D_{\pi_q} = t^2 - 4q < 0$ alors :*

- $\#E(\Bbbk) = q + 1 - t$,
- $\mathbb{Z}[\pi_q] \subset End(E) \subset \mathcal{O}_{\mathbb{K}}$ *où* $\mathbb{K} = \mathbb{Q}[\sqrt{D_{\pi_q}}]$.

2.4 CALCUL D'ISOGÉNIES

Selon les entrées les algorithmes de calcul d'isogénies peuvent se classifier en deux grands groupes. Les premiers initiés par vélu [115] donnent à partir d'une courbe elliptique E et un sous-groupe H de E une forme explicite de l'isogenie $E \longrightarrow E/H$. Et à partir de deux courbes elliptiques E et E' et un entier $\ell > 0$, Stark [110] introduisit une approche de calcul de l'isogénie $E \longrightarrow E'$ de degré ℓ.

2.4.1 *Approche de Vélu*

Lorsque $E/\Bbbk$ est une courbe elliptique et H est un sous-groupe fini de $E(\overline{\Bbbk})$, les formules de Vélu [115] donnent une forme explicite de l'isogénie normalisée $\phi : E \longrightarrow E/H$ en fonction des points de H et aussi une équation de la courbe elliptique E/H.
Ainsi pour tout $P \in E$:

$$x_{\phi(P)} = x_P + \sum_{Q \in H^*} (x_{P+Q} - x_Q) \quad et \quad y_{\phi(P)} = y_P + \sum_{Q \in H^*} (y_{P+Q} - y_Q)\,.$$

En considerant les améliorations apportées par D. Kohel [65] on arrive aux mêmes résultats lorsque $\ker \phi$ est représenté par un polynôme.

Exemple 2.4.1. Lorsque $char(\mathbb{k}) > 3$ et une courbe elliptique E sur $\mathbb{k}$ est donnée: $E : y^2 = f(x) = x^3 + a_4x + a_6$.
Soit h le polynôme définissant le noyau H de l'isogénie séparable et normalisée ϕ de degré ℓ de domaine E.
Posons:

$$Q(x) = \gcd\left(f(x), h(x)\right)$$

$$\begin{aligned} D(x) &= h(x)^2/Q(x) \\ &= x^{\ell-1} - d_1x^{\ell-2} + d_2x^{\ell-3} - d_3x^{\ell-4} + \cdots \end{aligned}$$

Alors pour tout point $P(x, y)$ de E nous avons:

$$\phi(x, y) = (\alpha(x), y\alpha(x))$$

$$\text{où} \quad \alpha(x) = \ell x - d_1x - (3x^2 + a_4).\frac{D'(x)}{D(x)} - 2f(x).\left(\frac{D'(x)}{D(x)}\right)'.$$

Et E/H est donné par l'équation suivante:

$$y^2 = x^3 + (a_4 - 5v)x + (a_6 - 7w)$$

$$\text{où} \quad v = a_4(\ell - 1) + 3(d_1^2 - 2d_2) \quad \text{et}$$

$$w = 3a_4d_1 + 2a_6(\ell - 1) + 5(d_1^3 - 3d_1d_2 + 3d_3).$$

2.4.2 *Approche de Stark-Elkies*

Lorsque E et E' sont des courbes elliptiques ℓ-isogènes sur $\mathbb{k}$ (par $\phi : E \to E'$) avec $char(\mathbb{k}) \neq \ell$. On considère que E et E' sont données respectivement par les équations $y^2 = x^3 + ax + b$ et $y^2 = x^3 + a'x + b'$ et aussi $\phi(x, y) = (\phi_x, cy\phi_y)$ où c est la constante de *normalisation*.
Alors en utilisant l'action de ϕ sur les espaces tangents et le fait que ϕ_x et $cy\phi_y$ vérifient l'équation de E' on a:

$$\begin{cases} \dfrac{\phi_x' dx}{y\phi_y} = c\dfrac{dx}{y} \\ c^2\left(x^3 + ax + b\right)\phi_y^2 = \phi_x^3 + a'\phi_x + b' \end{cases}$$

où c est la constante de *normalisation* et les fractions rationnelles ϕ_x et ϕ_y sont telles que $\phi_x = \dfrac{N(x)}{D(x)}$ et $\phi_y = \left(\dfrac{N(x)}{D(x)}\right)'$.

L'idée principale de la méthode de Elkies [32] est de calculer une expansion de la fraction rationnelle N/D à l'infini pour recouvrir la somme des racines de D.En partant de la même approche que l'algorithme d'Elkies [32] on pose le changement de variable suivant:

$$S(x) = \sqrt{\frac{D(1/x^2)}{N(1/x^2)}} \quad \Leftrightarrow \quad \frac{N(x)}{D(x)} = \frac{1}{S(1/\sqrt{x})^2};$$

Alors la deuxième equation différentielle devient

$$c^2(bx^6 + ax^4 + 1)S'(x)^2 = 1 + a'S(x)^4 + b'S(x)^6$$

Pour plus de simplicité, on peut supposer que ℓ est impair. Le noyau de l'isogénie ϕ noté H, comme ϕ est separable soit:

$$h(x) = x^d - p_1 x^{d-1} + \cdots$$

l'unique polynôme dont les racines sont les abscisses des $d = \frac{\ell-1}{2}$ paires de points de $H - \{O\}$. Ce qui suit résume les améliorations apportées dans [5]. On pose:

$$S = xT(x^2) \quad et \quad U(x) = \frac{1}{T(x)^2} \in 1 + x^2\Bbbk[[x]]$$

$$tel\ que \quad \frac{N(x)}{D(x)} = xU\left(\frac{1}{x}\right).$$

Alors l'algorithme suivant calcule $\dfrac{N(x)}{D(x)}$ en $O(M(\ell))$ opérations.

1. Calculer $C(x) = c^2(bx^6 + ax^4 + 1)^{-1} \mod x^{8d+4} \in \Bbbk[[x]]$;
2. Calculer $S(x) \mod x^{8d+5}$ et déduire $T(x) \mod x^{4d+2}$;
3. Calculer $U(x) = 1/T^2(x) \mod x^{4d+2}$,
4. Reconstruire la fraction rationnelle $U(x)$;
5. Retourner $N(x)/D(x) = xU(1/x)$.

2.5 GÉNÉRALITÉS SUR LES MÉTHODES p-ADIQUES

Dans cette section nous faisons une reconstitution technique du Relèvement Canonique de Courbes Elliptiques Ordinaires definies sur $\mathbb{F}_q$, tout en faisant ressortir les propriétés à partir desquelles nous proposons une généralisation en dimension 2. Chaque algorithme utilise tous le Théorème suivant de Lubin, Serre et Tate permettant de relever canoniquement une courbe elliptique à partir de son j-invariant lorsque ce dernier satisfait une condition dite de *Kronecker*.

Théorème 2.5.1. *(Lubin-Serre-Tate) Soit E une courbe elliptique ordinaire sur $\mathbb{F}_q$, alors il existe une unique courbe elliptique à isomorphisme près $\tilde{E}$ sur $\mathbb{Z}_q$ telle que :*

— *E est la réduite de $\tilde{E}$ modulo p ,*

— *$End(\tilde{E}) \cong End(E)$.*

$\tilde{E}$ est appelée le relèvement canonique de E et elle est uniquement caractérisée par le relèvement de l'isogénie Frobenius π en Π, alors l'équation:

$$\Phi_p(j(\tilde{E}), j(\tilde{E})^{\Sigma})) = 0$$

$$\begin{array}{ccc} \tilde{E} & \xrightarrow{\Pi} & \tilde{E}^{\Sigma} \\ \Big\downarrow{\scriptstyle \bmod p} & & \Big\downarrow{\scriptstyle \bmod p} \\ E & \xrightarrow{\pi} & E^{\sigma} \end{array}$$

De plus le polynôme modulaire Φ_p se réduit à :

$$\Phi_p(X,Y) \equiv (X^p - Y)(X - Y^p) \mod p$$

Soit $j \notin \mathbb{F}_{p^2}$ nous avons les rélations suivantes appelées *conditions de Kronecker*:

$$\begin{cases} \dfrac{\partial \Phi_p}{\partial X}(j, j^\sigma) \equiv & j^p - j^p \equiv 0 \mod p \\ \dfrac{\partial \Phi_p}{\partial Y}(j, j^\sigma) \equiv & j^{p^2} - j \not\equiv 0 \mod p \end{cases}$$

Si l'on pose $X = j$: alors $Y = j^p$ est une solution de multipicité 1 de l'équation $\Phi_p(j, Y) \equiv 0 \mod p$ c'est à dire que le Frobenius σ est de multiplicité 1.
D'autre part si l'on pose $Y = j^p$, $\Phi_p(X, j^p) \equiv (X - j)^p (X - j^{p^2}) \mod p$. Alors $X = j$ est de multiplicité p dans l'équation $\Phi_p(j, Y) \equiv 0 \mod p$, c'est à dire que le Verschiebung $\hat{\sigma}$ est de multiplicité p.
En effet nous avons sur $\mathbb{Z}_q$ deux points de $\tilde{E}[\mathbb{Z}_q]$ se réduisant sur $\bar{P}$ et 0 respectivement. Alors les p noyaux $\langle P + kQ \rangle$ avec $0 \leq k < p$ réduit sur $\bar{P}$ et le dernier $\langle Q \rangle$ se réduit sur $\langle 0 \rangle$. Ainsi en utilisant les conditions de Kronecker on peut construire une variante de l'algorithme de Hensel permettant de calculer le j-invariant des deux courbes p-isogènes $\tilde{E}$ et $\tilde{E}^\Sigma$.

Ainsi dans [99] T. Satoh a calculé les relevés des j-invariants d'un cycle de n courbes conjuguées E^{σ^i} avec $i = 1, \cdots n$ de E en utilisant les conditions de Kronecker. Comme le Frobenius est inséparable, le cycle est construit dans le sens du Verschiebung qui possède un noyau étale sur $\mathbb{Z}_q$.
On pose $E_{n-i} = E^{\sigma^i}$ et π_i est l'isogénie entre E_{i+1} et E_i définie par $(x, y) \mapsto (x^p, y^p)$. Alors on obtient le Verschiebung (le dual de l'endomorphisme Frobenius) par :

$$\hat{\pi}_q = \hat{\pi}_{n-1} \hat{\pi}_{n-2} \cdots \hat{\pi}_0$$

Comme les courbes E_i sont ordinaires on note par $\tilde{E}_i$ les relevés canoniques respectives des E_i et par $\hat{\Sigma}_i$ les relevés canoniques respectives des $\hat{\sigma}_i$.

$$\begin{array}{ccccccccc} \tilde{E}_0 & \xrightarrow{\hat{\Pi}_0} & \tilde{E}_1 & \xrightarrow{\hat{\Pi}_1} & \cdots & \xrightarrow{\hat{\Pi}_{n-2}} & \tilde{E}_{n-1} & \xrightarrow{\hat{\Pi}_{n-1}} & \tilde{E}_n \\ \mod p \downarrow & & \downarrow & & & & \downarrow & & \downarrow \mod p \\ E_0 & \xrightarrow{\hat{\pi}_0} & E_1 & \xrightarrow{\hat{\pi}_1} & \cdots & \xrightarrow{\hat{\pi}_{n-2}} & E_{n-1} & \xrightarrow{\hat{\pi}_{n-1}} & E_n \end{array}$$

FIGURE 2.1 – Le cycle de courbes elliptiques p-isogènes

Soit $\Theta : \mathbb{Z}_q \longrightarrow \mathbb{Z}_q$ l'application définie par :

$$\Theta(x_0, x_1, \cdots, x_{n-1}) = \big(\Phi_p(x_0, x_1), \Phi_p(x_1, x_2), \cdots \Phi_p(x_{n-1}, x_0)\big)$$

dont le determinant de la matrice Jacobienne est noté : $(D\Theta)(x_0, x_1, \cdots, x_{n-1})$ Nous avons :

$$\Theta\left(j(E_0), j(E_1), \cdots, j(E_{n-1})\right) = (0, 0, \cdots, 0) \quad et$$
$$(D\Theta)(j(E_0), j(E_1), \cdots, j(E_{n-1}) = \frac{\partial \Phi_p}{\partial X}(E_0, E_1) \cdots \frac{\partial \Phi_p}{\partial X}(E_{n-1}, E_0)$$

Où par les conditions de Kronecker tous les $\frac{\partial \Phi_p}{\partial X}(E_{i+1}, E_i) = \frac{\partial \Phi_p}{\partial Y}(j(E_i), j(E_i)^p)$ sont non nuls modulo p.
Alors un algorithme à la Hensel permet de determiner le n-uplets de j-invariants $(j(\tilde{E}_0), j(\tilde{E}_1), \cdots, j(\tilde{E}_{n-1})$ à la précision N avec une complexité en espace de $O(N^3)$.
En utilisant le même cycle des n courbes conjuguées Vercauteren introduisit dans [117] une méthode qui coûtait moins en espace de calculs soit $O(N^2)$. Cette méthode était basée sur la propriété suivante :
Pour tout $x \in \mathbb{Z}_q$ avec $x \equiv x_0 \mod p$ il existe un unique $y \in \mathbb{Z}_q$ tel que $y \equiv y_0 \mod p$ et $\Phi_p(x, y) = 0$ (Kronecker). Alors si on part d'un x à précision N, on obtient un unique y à précision $N+1$ tel que $y \equiv y_0 \mod p^{N+1}$.
Ainsi partant d'un j-invariant $j(E_{N-1}) \mod p$, avec la propriété précédente permet d'augmenter la précision et atteindre $j(E_0)$ à la précision N après N itérations.
L'objectif final étant d'évaluer le Verschiebung sur l'espace tangent, avec les algorithmes de " calcul de norme " rapides, relever canoniquement un seul j-invariant devenait plus avantageux. En effet si l'on note par γ l'information donnée par l'action de $\hat{\pi}_q$ sur la forme différentielle $\frac{dx}{y}$. Alors γ se décompose sur $\mathbb{Q}_q$ en γ_i pour chaque $\hat{\pi}_i$ et par conjugaison on obtiendrait $\gamma = \gamma_0^{\Sigma_q}$ c'est à dire $\gamma = N_{\mathbb{Q}_q/\mathbb{Q}_p}(\gamma_0)$.
Par la suite nous détaillons l'algorithme de Harley dont la complexité asymptotique est parmi les meilleures puisque le temps de calcul est quasi-linéaire en la taille.

2.5.1 *L'Algorithme de Harley*

On suppose toujours que nous sommes dans un cas où le calcul du Frobenius Σ est éfficient.
Soit $\tilde{j} = j + p^k e$ une approximation de $\tilde{j}$ à la précision k pour une erreur $e \in \mathbb{Z}_q$ que nous voulons déterminer. Le dévéloppement de Taylor de $\Phi_p(\tilde{j}, \tilde{j}^\sigma) = 0$ en $j + p^k e$ nous donne :

$$0 = \Phi_p(j + p^k e, j^\sigma + p^k e^\sigma)$$

$$0 = \Phi_p(j, j^\sigma) + p^k e \frac{\partial \Phi_p}{\partial X}(j, j^\sigma) + p^k e^\sigma \frac{\partial \Phi_p}{\partial Y}(j, j^\sigma) + p^{2k}(...),$$

où le facteur derrière p^{2k} est dans $\mathbb{Z}_q$. Alors $\Phi_p(j, j^\sigma)$ a une valuation au moins égale k et on peut l'écrire comme $p^k u$ avec $u \in \mathbb{Z}_q$. En simplifiant l'expréssion par p^k on obtient l'équation en e suivante :

$$u + e \frac{\partial \Phi_p}{\partial X}(j, j^\sigma) + e^\sigma \frac{\partial \Phi_p}{\partial Y}(j, j^\sigma) \equiv 0 \mod p^k.$$

En considérant $j \notin \mathbb{F}_{p^2}$, les rélations Kronecker impliquent que :

$$\frac{\partial \Phi_p}{\partial X}(j, j^\sigma) \equiv 0 \mod p \quad et \quad \frac{\partial \Phi_p}{\partial Y}(j, j^\sigma) \not\equiv 0 \mod p$$

Alors l'erreur e est solution sur $\mathbb{Z}_q$ d'une équation de la forme :

$$e^\sigma + Ae + B = 0.$$

où $A \equiv 0 \mod p$. Cette équation a été appelée *équation d'Artin-Schreier* à cause de sa ressemblance avec les équations de la même forme mais irréductibles. Cependant dans la présente situation la condition congruence $A \equiv 0 \mod p$ assure l'unicité de la solution. La

racine p-ième de B est l'unique solution de l'équation modulo p. Si l'on pose à son tour $e = x + p^k\alpha$ avec $\alpha \in \mathbb{Z}_q$, alors l'erreur α est solution d'une équation du type Artin-Schreier ainsi de manière récurssive on aboutit à un algorithme de type Newton 1 pour résoudre l'équation $e^\sigma + Ae + B = 0$ dans $\mathbb{Z}_q$.

Entrée: $a, b \in \mathbb{Z}_q$ avec $a \equiv 0 \mod p$ et une précision N.
Sortie: e tel que $e^p + ae + b \equiv 0 \mod p^N$.

1. Si $N = 1$ Retourner $-\sqrt[p]{b} \mod p$.
2. $X \leftarrow ArtinSchreier(a, b, N/2)$.
3. Relever arbitrairement X à la précision p^N.
4. $b' \leftarrow (X^\sigma + aX + b)/p^{N/2}$.
5. $e \leftarrow ArtinSchreier(a, b', N/2)$.
6. Retourner $X + p^{N/2}e$.

Algorithm 1 – Résolution d'une "équation d'Artin-Schreier " avec $A = 0 \mod p$

2.5.2 *Réconstitution de l'Équation de Weierstrass*

L'équation de Weierstrass sous sa forme simple possède au plus deux paramètres ayant une rélation arithmétique réductible modulo p avec le j-invariant. Alors avec un algorithme de type Hensel et un relevé $\tilde{j}$ de j à une précision N, on peut calculer le relevé d'une équation de Weierstrass à la précision N.
Par exemple en caractéristique 3, soit $E : y^2 = x^3 + a_2x^2 + a_6$ l'équation sur $\mathbb{F}_{3^n}$. Comme $j = \dfrac{-256a_2^6}{4a_2^3a_6 + 27a_6^2}$, on considère $\tilde{a}_2 = a_2$ et $f(X) = (\tilde{j}(a_2^3X + 27X^2/4) + 64a_2^6)$ alors $f(a_6) \equiv 0 \mod 3$ et $f'(a_6) \not\equiv 0 \mod 3$. Un algorithme de Hensel sur f permet de construire une équation de $\tilde{E}$ se réduisant sur $E : y^2 = x^3 + a_2x^2 + a_6$.
D'autre part en caractéristique ≥ 5 Skjernaa [108] suggérait de considérer simplement $a_6 = 3\alpha$ et $a_4 = 2\alpha$ avec

$$\alpha = \frac{j(E)}{1728 - j(E)}$$

Et $\tilde{j}$ donne une équation de $\tilde{E}$. Cette éfficiente méthode utilise simplement une inversion sur $\mathbb{Z}_q$ à partir de $\tilde{j}$.

2.5.3 *Relèvement du Verschiebung*

Soit E une courbe elliptique dont le j-invariant satisfait les conditions de Kronecker sur $\mathbb{F}_q$. Le noyau du Verschiebung $\widehat{\sigma}$ est un sous groupe d'ordre p de $E[p]$ donné par le facteur unitaire h du polynôme de p-division Ψ_p et h défini par :

$$h(x) = \prod_{P \in \ker \hat{\pi} \setminus \{\mathcal{O}\}} (x - x(P))$$

Soit $\tilde{E}$ le relèvement canonique de E, relever $End(E)$ revient à relever $\ker(\sigma_q)$ et cela revient à relever h sur $\mathbb{Z}_q$.

Lemme 2.5.2. *(Satoh)*
On considère $p \geq 3$, alors $ker(\hat{I}I) = \tilde{E}[p] \cap \tilde{E}(\mathbb{Z}_q^{ur})$ avec $\mathbb{Z}_q^{ur}$ l'anneau de valuation de l'extension maximale non ramifiée ${\mathbb{Q}_q}^{ur}$ de $\mathbb{Q}_q$.

Soit H le relevé de h sur $\mathbb{Z}_q$, alors H est un facteur unitaire de degré $(p-1)/2$ de Ψ_p et $H(x) = h(x) \mod p$ est sans facteur carré. De plus $\Psi_p(x) \equiv H(x)^p \mod p$ c'est à dire que modulo p, les facteurs $H(x)$ et $\Psi_p(x)/H(x)$ ne sont pas premiers .

Proposition 2.5.3. *(Lemme de Satoh)*
On considère $p \geq 5$ et $\tilde{E} : y^2 = x^3 + \tilde{A}x + \tilde{B}$ tel que $\tilde{E}[p] \cap \tilde{E}(\mathbb{Z}_q^{ur}) \neq \{\mathcal{O}\}$. Alors pour tout $P \in \tilde{E}(\mathbb{Z}_q^{ur}) - \{\mathcal{O}\}$,

$$\operatorname{ord}_p\left(\Psi'_p(x_P)\right) = 1$$

où $\Psi'_p = \dfrac{\partial \Psi_p}{\partial x}$.

Démonstration. Aller à Lemme 3.7. dans [99]. □

En général soit $P = p_m X^m + p_{m-1}X^{m-1} + ... + p_1 X + p_0$ un polynôme sur $\mathbb{Z}_q$ et α un élément non ramifié de $\mathbb{Q}_q$ tel que $P(\alpha) \neq 0$ et $\operatorname{ord}_p(\alpha) = 0$. Si p-valuation des coefficients p_k de P sont tous différents cela implique que $\operatorname{ord}(\alpha)$ n'est pas "*une valeur exptionnelle*" [1] et $\operatorname{ord}(P(\alpha))$ est fini. Alors d'après [14, Pages: 2-5] nous avons :

$$\operatorname{ord}_p(P(\alpha)) = \min_k \left(\operatorname{ord}_p(p_k) + k \operatorname{ord}_p(\alpha)\right)$$

alors

$$\operatorname{ord}_p(P(\alpha)) = \min_k \left(\operatorname{ord}_p(p_k)\right).$$

Proposition 2.5.4. *Lorsque p est un premier impaire et Ψ_p est le polynôme de p-division d'une courbe elliptique sur $\mathbb{Z}_q$ alors :*

$$ord_p(\Psi'_p) = 1.$$

Démonstration. En considerant p un premier impaire et $P(x_0, y_0) \in E[p] \cap E(Z_q^{ur})$, le résultat précédent sur Ψ'_p et x_0 donne $\left(ord_p(\Psi'_p)\right) = ord_p\left(\Psi'_p(x_0)\right)$. Alors la proposition 2.5.3 s'applique et nous avons : $ord_p(\Psi'_p) = 1$. □

Le lemme de Hensel originel ne pouvant s'appliquer dans les cas précédents, T. Satoh introduisit dans [99] une méthode de relèvement de Hensel déterminant le rélévé du facteur d'un polynôme.

Proposition 2.5.5. *Considerons p impair, $u \in \mathbb{N}$ et $G(x) \in \mathbb{Z}_q[x]$ tels que $t = \operatorname{ord}_p(G'(x))$. Soit $h(x) \in \mathbb{Z}_q[x]$ un polynôme unitaire tel que :*

- *modulo p, $h(x)$ est séparable et premier avec $p^{-t}G'(x)$,*
- *et nous connaissons $G(x) \equiv q(x)h(x) \mod p^{u+t}$,*

Alors le polynôme :

$$H(x) = h(x) + \left(\frac{G(x)}{G'(x)} h'(x) \mod h(x)\right)$$

est le lift de $h(x)$ à la précision p^{2u} et $G(x) \equiv Q(x)H(x) \mod p^v$ où $v = 2u + \min(t, u)$

L'algorithme 2.5.1 construit H en $O((\deg h + \deg G)^2)$ opérations arithmétiques sur $\mathbb{Z}_q$ à la précision p^{2n}.

Démonstration. Aller à [99]. □

Entrée: Des polynômes G, h satisfaisant les conditions 2.5.5 et un entier N comme précision.
Sortie: Le lift de H à la précision N.

1. $t = ord_p(G'(x))$;
2. **Si** $N = 1$ **Retourner** $h(x)$;
3. **Sinon** $k = N/2$;
   a. $H(x)$=LiftPolynôme(G, H, k) ;
   b. **Retourner** $H(x) + \dfrac{G(x)H'(x)}{G'(x)} \mod H(x)$;

Algorithm 2.5.1 LiftPolynôme : Méthode de Satoh de Relèvement du polynôme de p-torsion

---

En utilisant l'algorithme 2.5.1 de Satoh on peut donc relever h en H sur $\mathbb{Z}_q$. L'algorithme 2.5.1 construit H avec $O((\deg h + \deg G)^2)$ opérations arithmétiques sur $\mathbb{Z}_q$ à la précision p^{2n}.
D'autre part nous avons proposé une méthode dans le chapitre 1, la section 1.2 et le lemme 1.2.1, pour réléver directement les abscisses des points de torsion de E. Cette nouvelle méthode est généralisable aux systèmes d'équations comme l'illustre les exemples 1.2.2 de la section 1.2.

2.6 COMPTAGE DE POINTS RATIONNELS SUR LES COURBES ELLIPTIQUES ORDINAIRES

On considère E une courbe elliptique dont $\tilde{E}$ est le relevé canonique sur $\mathbb{Z}_q$. Le polynôme caractéristique de E noté χ est le polynôme reciproque du polynôme minimal du Frobenius définie sur $\mathbb{Z}$ par :

$$\chi(X) = X^2 - tX + q$$

où t est la trace du Frobenius. Nous avons $\chi(1) = \#E(\mathbb{F}_q)$ avec t vérifiant la condition : $|t| \leq 2\sqrt{q}$ appelée *bornes de Hasse*.
Soit γ la valeur propre inversible du Frobenius σ alors nous avons :

$$t = \gamma + \frac{q}{\gamma}$$

Pour toute forme modulaire ϑ_k de poids k définie sur $\mathcal{H}_1$ nous pouvons déterminer γ par :

$$\gamma_0^k = \frac{\vartheta_k(E^\Sigma)}{\vartheta_k(E)} \quad et \quad \gamma = N_{\mathbb{Q}_q/\mathbb{Q}_p}(\gamma_0)$$

2.6.1 *Méthode d'Évaluation par l'Algorithme de Vélu*

Nous avons le diagramme suivant de décomposition de l'isogénie $\hat{I}I$ le relevé de $\hat{\pi}$ où π est définie par $(x, y) \in E \mapsto (x^p, y^p) \in E^\sigma$. Où ν est l'isogénie normalizée déterminée par les Formules de Vélu's et λ est l'isomorphisme entre $\tilde{E}/ker(\hat{I}I)$ et $\tilde{E}^{\hat{\Sigma}}$. Comme ν est normalizé son action est trivial sur l'espace tangent et on a seulement besoin de l'action de l'isomorphisme λ pour avoir celle de l'isogénie $\hat{I}I$.

1. c'est-à-dire qu'il ne coïncide pas avec les pentes négatives des arêtes du polygone de Newton de P

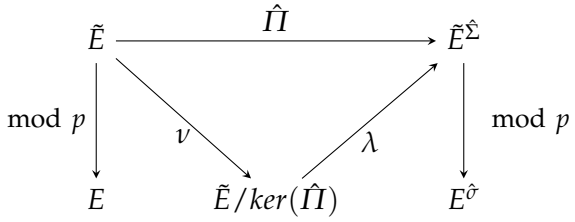


FIGURE 2.2 – Décomposition du Verschiebung $\hat{II}$

Soit $\tilde{E}$ définie par $y^2 = x^3 + \tilde{A}x + \tilde{B}$, Satoh montre dans [99] que les Formules de Vélu déterminant l'équation de $\tilde{E}/ker(\hat{II})$ sont simplement donnée par :

$$\begin{aligned} A' &= (6-5p)\tilde{A} - 30(h_1^2 - 2h_2), \\ B' &= (15-14p)\tilde{B} - 70(-h_1^3 + 3h_1h_2 - 3h_3) + 42\tilde{A}h_1 \end{aligned}$$

Où h_i est le coefficient de $x^{(p-1)/2-i}$ dans le polynôme $H(x)$ et $h_i = 0$ pour $(p-1)/2 - i < 0$. Nous voudrions maintenant calculer le coefficient γ_0 de l'isomorphisme λ entre les courbes elliptiques d'équations $\tilde{E}/ker(\hat{II}) : y^2 = x^3 + A'x + B'$ et $\tilde{E}^{\hat{II}} : y^2 = x^3 + A''x + B''$. Sachant que B'/A' et B''/A'' sont des formes modulaires de poids 2, alors :

$$\gamma_0^2 = \frac{B''/A''}{B'/A'}$$

Et d'autre part la bonne racine de cette expréssion est le coéfficient de x^{p-1} dans le polynôme $(x^3 + Ax + B)^{(p-1)/2} \in \mathbb{F}_q[x]$ [107] et nous avons : $\gamma = N_{\mathbb{Q}_q/\mathbb{Q}_p}(\gamma_0)$.

Remarque 2.6.1. Nous allons conclure cette partie par une comparaison sur quelques variantes de la méthode originale de Satoh. Leurs points communs résident essentiellement sur l'utilisation du théorème de Lubin Serre et Tate 2.5.1 en des courbes elliptiques vérifiant les conditions de Kronecker 2.5 et ensuite la factorisation du dual de l'isogénie $\hat{II}$ en utilisant les Formules de Vélu. Cependant l'idée originale de relever le cycle des n courbes conjuguées était assez coûteuse en complexité. Sachant qu'il fallait relever la courbe à une précision $k > \frac{n}{2} + log_p(4)$, cette méthode marchait avec $O(n^3 \log n \log\log n)$ opérations binaires et $O(n^3)$ en espace pour p fixé. Les variantes les plus performentes en complexité utilisent un relèvement de seulement deux courbes $\hat{\pi}$-isogènes jusqu'à cette précision, ce qui coûte $\tilde{O}(n^2)$, puis effectuer un calcul de norme rapide du coéfficient γ_0, ce qui peut se faire dans les meilleurs cas avec la même complexité.

2.6.2 *Méthodes d'Elkies Améliorées*

Différentiation d'Elkies

Soient E et E' deux courbes elliptiques sur $\mathbb{C}$, $\phi : E \longrightarrow E'$ une isogénie de courbes elliptiques et Φ_ℓ le polynôme modulaire classique de niveau $\ell = \deg\phi$.

$$\phi : E \xrightarrow{\sim} \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}) \longrightarrow \mathbb{C}/(\mathbb{Z} + \tfrac{\tau}{\ell}\mathbb{Z}) \xrightarrow{\sim} E'$$

Alors on a:

$$\begin{cases} \frac{dj}{d\tau}(\tau)\frac{\partial\Phi_\ell}{\partial X}(j(\tau), j(\tau/\ell)) + \frac{1}{\ell}\frac{dj}{d\tau}(\tau/\ell)\frac{\partial\Phi_\ell}{\partial Y}(j(\tau), j(\tau/\ell)) = 0 \\ \qquad et \quad \frac{dj}{d\tau} = \lambda j\frac{E_6}{E_4} \quad avec \quad \lambda \in \mathbb{C}^*. \end{cases}$$

Où E_{2k} est la série d'Eisenstein de poids $2k$.
La première équation est une conséquence de $\Phi_\ell(j(\tau), j(\tau/\ell)) = 0$ et la seconde est la derivée $\frac{dj}{d\tau}$ mise en fonction des coefficients a et b de E à partir des modules E_6 et E_4.
Lorsque l'on remplace les dérivées partielles $\frac{dj}{d\tau}(\tau)$ et $\frac{dj}{d\tau}(\tau/\ell)$ par leurs valeurs en fonction des coefficients de E et E', on peut extraire le coefficient de normalisation γ_0.
Cette méthode de calcul du coefficient de normalisation γ_0 de ϕ permet un algorithme de calcul de la trace du Frobenius à partir de relevé canonique d'une courbe elliptique $E/\mathbb{F}_q$.
Le nouveau algorithme est une combinaison utilisant le relèvement canonique pour obtenir le couple $(\tilde{E}, \tilde{E}^\Sigma)$, et l'algorithme d'Elkies [32] pour evaluer directement le coefficient de normalisation γ_0 de l'isogénie π. Par la suite un calcul de norme rapide donne $\gamma = N_{\mathbb{Q}_q/\mathbb{Q}_p}(\gamma_0)$.
Et nous avons l'algorithme suivant 2.6.1.

Entrée: $q = p^n$, une courbe elliptique E sur $\mathbb{F}_q$ et précision $N \sim n$.
Sortie: La trace t de l'isogénie π_q.

1. Calculer $\tilde{j}$ en utilisant $\Phi_p(j, j^\sigma) = 0$;
2. Calculer les équations de $\tilde{E}$ et $\tilde{E}^\Sigma$;
3. Calculer γ_0 en utilisant la méthode de Différentiation d'Elkies;
4. Calculer $\gamma = N_{\mathbb{Q}_q/\mathbb{Q}_p}(\gamma_0)$;
5. Retourner $t = \gamma + \frac{q}{\gamma}$.

Algorithm 2.6.1

2.6.3 *Relèvement Canonique sans Polynôme Modulaire*

Dans cette sous-section nous supposons p un nombre premier impaire. Le cas $p = 2$ est bien traité par J.Mestre en utilisant la méthode de l'AGM (en anglais "Arithmetic-Geometric-Means") [35] pour calculer les courbes elliptiques 2-isogènes conjuguées par le p^{th}-Frobenius. Cette méthode dite de l'AGM n'utilise pas de polynôme modulaire.

L'objectif de cette partie est de diminuer considérablement le coût du relèvement canonique afin de rendre ces algorithmes plus pratiques que possible en dimension 1. *Ces nouveaux résultats détaillés ci-dessous portent sur les algorithmes de calcul du polynôme caractéristique d'une courbe elliptique ordinaire en une complexité au plus linéaire en p. Les idées sont reprises de la troisième publication (Introduction la section 0.0.4).*

En effet, pour les méthodes utilisant les polynômes modulaires, la complexité totale est de $\tilde{O}(p^3 + p^2nN)$ pour un relèvement à la précision N (dans le cas du comptage de points rationnels $N = O(n)$). Ces polynômes modulaires sont de tailles $\tilde{O}(p^3)$ en les invariants et

leurs hauteurs logarithmiques sont $h(\Phi_p) \leq 6p \log p + 18p$ (aller à [8]). Puisqu'on les utilise qu'avec un seuil de précision connu, par évaluation directe de ces polynômes on pourrait réduire la dépendance en p jusqu'à $\tilde{O}(p^2 nN)$ dans le cas du comptage de points [97, § 6.6].

Correspondance Modulaire par la Méthode de Décomposition du Verschiebung

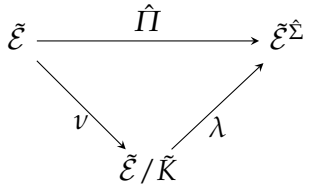
En utilisant le diagramme de décomposition du Verschiebung (la section 2.5.1), on arrive à un résultat équivalent au théorème de Serre-Tate (la section 2.5.1 et le théorème 2.5.1) .

Théorème 2.6.2. *Soit E une courbe elliptique ordinaire sur $\mathbb{F}_q$, alors $\tilde{E}$ est l'unique courbe elliptique (à isomorphisme près) vérifiant:*

- *E est la réduite modulo p de $\tilde{E}$,*
- *la partie étale de $E[p]$ est la réduction modulo p du noyau $\ker \nu$ et*
- $j(\tilde{E}^{\nu}) = j(\tilde{E})^{\hat{\Sigma}}$

Démonstration. Comme $\tilde{E}$ est bien définie par les assertions du théorème de Serre-Tate la section 2.5.1 et le théorème 2.5.1, alors l'isogénie Frobenius π et son dual se relèvent caniquement sur $\mathbb{Z}_q$. Ainsi $\tilde{E}$ vérifie les trois propriétés du théorème 2.6.2.
Réciproquement, lorsque $\mathcal{E}$ est une courbe elliptique sur $\mathbb{Z}_q$ vérifiant les trois propriétés du théorème 2.6.2, alors modulo p on a $j(\mathcal{E}) = j(E)$ et le noyau du Verschiebung de $\mathcal{E}$ se réduit à $E[p]_{\text{ét}}$ ce qui implique que $\mathrm{End}(\mathcal{E}) \simeq \mathrm{End}(E)$ et par suite $\mathcal{E} \simeq \tilde{E}$. □

Le théorème précédent (le théorème 2.6.2) établit l'unicité (à isomorphisme près) du diagramme de décomposition du Verschiebung pour toute courbe elliptique ordinaire E de $\mathbb{F}_q$ à $\mathbb{Z}_q$.



Ainsi, les propriétés suivantes sont équivalentes:

- $j(E^{\nu}) = j(E^{\hat{\Sigma}})$;
- $\mathrm{End}(E) \cong \mathrm{End}(\bar{E})$ et $\Phi_p(j(E), j(E)^{\hat{\Sigma}})) = 0$ où $\bar{E}$ est la réduite modulo p de E.

Les propriétés du théorème 2.6.2 fournissent une méthode de relèvement du j-invariant d'une courbe elliptique ordinaire E définie sur $\mathbb{F}_q$ basée sur les formules de Vélu à la place du polynôme modulaire. Nous détaillons ci-dessous un exemple à partir des formules de Vélu standard.

Méthodes du Diagramme de Décomposition du Verschiebung

Au départ, on pourra de façon plus pratique calculer H_p sur $\mathbb{F}_q$ en interpolant sur $O(p)$ points l'équation $\hat{\pi}(\pi(P)) = [p].P$ pour en extraire H_p dans le dénominateur de la fraction rationnelle coordonnée de $\hat{\pi}$.

Supposons que à une précision k nous ayons $E : y^2 = x^3 + Ax + B$ et $P(x_p, y_p) \in E[p] - \{\mathcal{O}\}$.
Soit (e, r) le couple d'erreurs tel que: $x_{\tilde{P}} - x_P = e.p^k$ et $y_{\tilde{P}} - y_P = r.p^k$, alors nous pouvons obtenir un relèvement de l'équation à partir des coefficients A et $B + \theta.p^k$. Ainsi les trois erreurs e, r et θ forment l'unique solution du système d'équations suivant:

$$\begin{cases} \tilde{P} \in \tilde{E}, \\ \Psi_p(x_{\tilde{P}}) = 0, \\ j(\tilde{E}^v) = j(\tilde{E})^{\hat{\Sigma}} \end{cases}$$

D'après la section 2.5.1 et le théorème 2.5.1 la Jacobienne de système est inversible sur $\mathbb{Z}_q$. Ainsi, de la première équation nous avons:

$$r = \frac{1}{2y_P}\left[(x_P^3 + A.x_P + B - y_P^2)/p^k + (3.e.x_P^2 + A.e + \beta)\right].$$

Et à partir de la second équation, on pourra extraire $p.e$ de

$$\Psi_p\left(x_p + e.p^k, A, B + \beta.p^k\right) = 0$$

(car d'après le lemme 2.5.2 de Satoh $\Psi'_p(x_p + e.p^k)$ est de p-valuation 1).
On considère A_v et B_v les coefficients de l'équation de la courbe p-isogène E^v (par le petit Frobenius) donnés par les formules de Vélu sur les entrées $(A, B + \beta.p^k, P_{e,r})$ à la précision $2k$ où $P_{e,r} = (x_P + e.p^k,\ y_P + r.p^k)$. Alors l'égalité entre les j-invariants des courbes isomorphiques E^v et $E^{\hat{\Sigma}}$ détermine la troisième équation:

$$A_v^3.(B^{\hat{\Sigma}})^2 - (A^{\hat{\Sigma}})^3.B_v^2 = 0$$

Par suite, en considerant les valeurs de r et celle de $p.e$ dans cette dernière équation on aboutit à une équation en β de la forme :

$$\beta^{\Sigma} + a.\beta + b = 0 \quad \text{avec} \quad a = 0 \mod p$$

que l'on peut résoudre avec la méthode (la section 2.5.1 et l'algorithme 1) ainsi obtenir: β, e et r.

N.B: *Cette méthode s'étend bien au calcul de relevé canonique des courbes elliptiques ordinaires dont les j-invariants appartiennent à* $\mathbb{F}_{p^2}\backslash\{0, 1728\}$.
De manière pratique lorsque $\mathcal{S}_E$ exprime les données comprenant les coefficients de l'équation et le j-invariant d'une courbe ordinaire, alors l'équation dont l'unique solution est $\tilde{E}$ est donnée par:

$$A.\mathcal{S}_E^{\Sigma} + B.\mathcal{S}_E + C = 0$$

$$\text{avec} \quad A \neq 0 \mod p \quad \text{and} \quad B = 0 \mod p$$

Comme $A \neq 0 \mod p$ et le système est séparable, on pourra toujours se focaliser sur une ligne pour obtenir une forme d'Artin-Schreier.
Et cela est une conséquence du résultat 6.2.1 dans le chapitre 6 et la section 6.2. En effet comme nous allons le voir dans le chapitre 6 les conditions de Kronecker en général n'ont pas de restriction sur les points ordinaires de l'espace de module fin.

Entrée: Une équation $y^2 = x^3 + A.x + B$ de la courbe $E/\mathbb{F}_{p^n}$ et un entier $N = 0(n)$ comme précision.
Sortie: Une équation $y^2 = x^3 + \tilde{A}.x + \tilde{B}$ de la courbe $\tilde{E}$ à la précision N.

1. $k = 1$;
2. Tant que $k \leq N/2 + 1$;
   a. On pose $r = \frac{1}{2y_P}\left[(x_P^3 + A.x_P + B - y_P^2)/p^k + (3.e.x_P^2 + A.e + \beta)\right]$;
   b. Extraire $p.e$ de l'équation $\Psi_p\left(x_P + e.p^k, A, B + \beta.p^k\right) = 0$
   c. À partir de l'équation $A_v^3.(B^{\hat{\Sigma}})^2 - (A^{\hat{\Sigma}})^3.B_v^2 = 0$ calculer $\beta^{\Sigma} + a.\beta + b = 0$.
   d. En utilisant l'algorithme 1, calculer les erreurs β puis e, r .
   e. $B = B + \beta.p^k$, $x_P = x_P + e.p^k$, $y_P = y_P + r.p^k$ et $k = 2k$;
3. Retourner A, B et P ;

Algorithm 2 – Relèvement Canonique sans Polynôme Modulaire

Remarque 2.6.3. Remarquons qu'un point de p-torsion P différent du point à l'infini est défini de manière équivalente par le système:

$$\begin{cases} f(x,y) & = 0 \\ \Psi_p(x) & = 0 \end{cases} \quad \text{or} \quad \begin{cases} f(x,y) = 0 \\ g(x,y) = 0 \end{cases}$$

où $g(x,y)$ est une des équations de $[k+1]P = -[k]P$. La Jacobienne de ce système est donnée par:

$$\begin{pmatrix} \frac{\partial f}{\partial x}(x,y) & \frac{\partial f}{\partial y}(x,y) \\ \Psi_p'(x) & 0 \end{pmatrix}$$

Comme $p \neq 2$, nous avons $\frac{\partial f}{\partial y}(P)$ non nul modulo p. Alors d'après le lemme de Satoh (la proposition 2.5.3), la valuation du déterminant de la Jacobienne de ce système en P est 1. En considerant le second système équivalent, la forme de la Jacobienne devient :

$$\begin{pmatrix} * & * \\ 0 & p \end{pmatrix}$$

En considérant le développement de Taylor sur le système on déduit que lors du relèvement, les coordonnées du point P sont en rétard d'une précision sur les coefficients de l'équation de la courbe de $\tilde{E}$. Plus explicitement lorsque le point $P = \tilde{P} \mod p^k$ vérifie l'équation de la courbe de $\tilde{E}$ avec une précision N c'est-à-dire $f(P) = 0 \mod p^N$; nous n'aurons besoin que de $P \mod p^{k-1}$ pour atteindre la même précision N sur les équations de la p-torsion.
Ainsi dans la troisième équation nous perdrons souvent[2] *une précision sur les formules de Vélu pour le calcul du Verschiebung.*

Exemple 2.6.4. :

2. Cette perte commencera après les compensations de précisions apportées par les coefficients d'homogénisation dans l'équation.

Soit E une courbe elliptique ordinaire sur $\mathbb{F}_5[T]/m(T)$ avec $m(T) = T^{10} + 3T^6 + 3T^5 + T^2 + 2T + 4$ donnée par l'équation :

$y^2 = x^3 + a_4x + a_6$ où : $a_4 = T + 3$ et $a_6 = -(T^9 + 2T^8 + 2T^6 + T^3 + 4T^2 + 2)$
tels que le j-invariant de E est $j = 2T + 3$;

Le polynôme de Teichmuller M de m à la précision 13 est

$$\begin{aligned} M =& T^{10} + 759170540T^9 + 11870001351T^8 + 435927860T^7 + 1154383168T^6 + 1177330303T^5 \\ &+ 512301245T^4 + 661739075T^3 + 46449971T^2 + 1140095647T + 1220703124 \end{aligned}$$

l'algorithme 2 calcule le relèvement des coefficients a_4, a_6, du j-invariant j et de la p-torsion de $\tilde{E}$ à la précision N.
On obtient pour $N = 2$:

$$\begin{aligned} e_1 &= T^7 + 3T^6 + 3T^5 + T^4 + 4T^3 + 2T^2 + 2; \\ r_1 &= T^9 + 4T^8 + 4T^7 + T^6 + 2T^5 + 2T^4 + 4T^3 + 4T^2 + T + 3; \\ \beta_1 &= 4T^9 + T^8 + 4T^7 + T^5 + T^4 + T^3 + 3T^2 + 4T + 3; \end{aligned}$$

Alors à la precision 2

$$\tilde{J} = 5T^8 + 20T^7 + 5T^6 + 10T^5 + 15T^4 + 15T^3 + 12T + 18;$$

On obtient pour $N = 4$:

$$\begin{aligned} r_2 &= 5T^9 + 19T^8 + 18T^7 + 5T^6 + 2T^5 + 24T^4 + 17T^3 + 2T^2 + 17T + 24; \\ e_2 &= 15T^9 + 2T^8 + 10T^7 + 22T^6 + 19T^5 + T^4 + 20T^3 + T^2 + 11T + 23; \\ \beta_2 &= 19T^9 + 18T^8 + 8T^7 + 22T^6 + 2T^5 + 21T^4 + 20T^3 + 18T^2 + 21T + 16; \end{aligned}$$

Alors à la precision 4

$$\tilde{J} = 100T^9 + 30T^8 + 145T^7 + 405T^6 + 260T^5 + 40T^4 + 140T^3 + 125T^2 + 137T + 143;$$

On obtient pour $N = 8$:

$$\begin{aligned} e_4 &= 44T^9 + 42T^8 + 97T^7 + 11T^6 + 105T^5 + 15T^4 + 121T^3 + 39T^2 + 52T + 45; \\ r_4 &= 500T^9 + 149T^8 + 368T^7 + 279T^6 + 105T^5 + 390T^4 + 429T^3 + 258T^2 + 240T + 263 \\ \beta_4 &= 200T^9 + 606T^8 + 300T^7 + 349T^6 + 599T^5 + 529T^4 + 304T^3 + 342T^2 + 333T + 366; \end{aligned}$$

Alors on a:

$$\begin{aligned} \tilde{J} = & 337600T^9 + 353780T^8 + 317020T^7 + 61030T^6 + 39635T^5 + \\ & 665T^4 + 378890T^3 + 152000T^2 + 199512T + 19518. \end{aligned}$$

Lorsque ϕ est une isogénie séparable de degré ℓ et d est le degré minimal tel que le polynôme de ℓ-division Ψ_ℓ admet toutes ses racines sur l'extension algébrique $\mathbb{K}/\Bbbk$ de degré d. Alors les formules d'isogénies de Kohel ont une complexité de $O(\ell.M(d))$ opérations sur $\Bbbk$ où $M(d)$ est le coût de la multiplication dans l'extension $\mathbb{K}/\Bbbk$. Les mêmes formules coûteront $O(\ell)$ opérations lorsque l'isogénie ϕ est définie sur $\Bbbk$. Mieux encore, le recent algorithme (développé dans [2]) peut calculer une isogénie définie sur $\Bbbk$ avec $O(\sqrt{p})$ opérations. Ainsi, les méthodes basées sur le théorème 2.6.2 offrent une complexité en p plus pratique que les autres méthodes connues.

Théorème 2.6.5. *Lorsque $p \geq 3$ et E une courbe elliptique ordinaire sur $\mathbb{F}_{p^n}$, alors l'algorithme 2 calcule relèvement canonique $\tilde{E}$ (en relevant l'équation de E) à la précision N, avec un coût au plus $\widetilde{O}(pn^2 + p^{0.5}.d.n.N)$ opérations, où $N = O(n)$.*

Démonstration. Le degré de décomposition de Ψ_p sur $\mathbb{F}_{p^n}$ est noté d et $d \leq (p-1)$. Le calcul du polynôme de p-division coûte $\widetilde{O}(p^2.N)$ opérations à la précision N et ses racines sont obtenues modulo p avec $\widetilde{O}(p.n^2)$ opérations (d'après [97, § 6.6]). D'un autre côté les formules de Vélu (pour l'évaluation du Verschiebung normalisé) coûtent au plus $O(p)$ et à la précision N l'évaluation de l'équation d'Artin-Schreier l'algorithme 1 est quasi-linéaire en temps (d'après [35, § 5.3]). Alors la complexité globale du relèvement canonique de E est au plus $\widetilde{O}(pn^2 + p^{0.5}.d.n.N)$ opérations lorsque le calcul du Verschiebung se fait en $O(\sqrt{p})$ opérations binaires. □

Amélioration par Évaluation Directe du Verschiebung

La méthode précédente est un algorithme de Newton basé sur un système polynomial défini au départ avec un point de p-torsion modulo p. Cependant lorsque que le polynôme du noyau n'a pas ses racines sur $\mathbb{F}_q$, on pourra compenser le calcul d'une extension de $\mathbb{F}_q$ avec une méthode combinant: une idée introduite par D. Robert dans son HDR [97, § 6] avec un algorithme de calcul d'isogénie éfficace comme les formules de Kohel l'exemple 2.4.1 ; ci-dessous nous proposons un algorithme basé sur ces idées.
Lorsque que l'on considère l'algorithme de calcul du Verschiebung sur $\mathbb{Z}_q$ comme une fonction $F(X)$ sur $\mathbb{Z}_q$ à une variable X sur l'espace de modules des courbes elliptiques ordinaires modulo p. À partir du développement de Taylor et les conditions de Kronecker (à la section 2.5.1) on a:

$$F(X+\Delta) = F(X) + F'(X).\Delta \mod p^{2k}$$

où $F'(X)$ est la dérivée de F en fonction de X.
D'autre part, on sait des résultats précédents que le calcul du Verschiebung à une précision k provoque une perte de précision dans le second membres de l'égalité, ainsi on a:

$$F(J + e.p^k) = A + B.e.p^{k-1} \mod p^{2k-1}$$

Ainsi lorsque nous partons d'une courbe elliptique ordinaire relevée canoniquement à une précision k et d'un algorithme de calcul du Verschiebung, nous pouvons déterminer canoniquement le prochain j-invariant (c'est-à-dire $A + B.e.p^{k-1}$) à partir d'une évaluation directe du nombre dérivée $F'(J)$ en J à la précision k. On obtient $F'(J)$ en procédant comme dans le chapitre 1 et la section 1.2.3 : On calcule deux déformations $F(J + e_1.p^k)$ et $F(J + e_2.p^k)$ quelconque de $F(J)$ où J est le j-invariant E à la précision k, alors le système suivant détermine A et B:

$$\begin{cases} F(J + e_1.p^k) = & A + B.e_1.p^{k-1} \mod p^{2k-1} \\ F(J + e_2.p^k) = & A + B.e_2.p^{k-1} \mod p^{2k-1} \end{cases}$$

On pourra prendre $e_1 = 0$ pour simplifier les calculs.
D'un autre côté, le théorème 2.6.2 établit que:

$$j(\tilde{E}^{\nu}) = j(\tilde{E})^{\hat{\Sigma}}$$

Cela implique que, modulo p^{2k-1} l'erreur correcte e correspondant à l'approximation de $\tilde{J}$ à la précision $2k-1$ vérifie la relation :

$$A + B.e.p^{k-1} = J^{\hat{\Sigma}} + e^{\hat{\Sigma}}.p^k$$

En appliquant le Frobenius Σ, on obtient :

$$A^{\Sigma} + B^{\Sigma}.e^{\Sigma}.p^{k-1} = J + e.p^{k}$$

Comme $A = F(J) \mod p^{2k-1}$, alors on a: $\mathrm{ord}_{\mathrm{p}}\,(A^{\Sigma} - J) = k - 1$ et par suite on obtient :

$$B^{\Sigma}e^{\Sigma} + a.e + b = 0 \mod p^{k}$$

où $a = -p$ et $b = \dfrac{A^{\Sigma} - J}{p^{k-1}}$.

Comme $\mathrm{ord}_{\mathrm{p}}\, b = 0$, on en déduit que $\mathrm{ord}_{p}\, B^{\Sigma} = 0$. Alors on pourra diviser l'équation précédente par B^{Σ} et obtenir une forme "d'Artin-Schreier" dont la solution est donnée par l'algorithme 1 (la section 2.5.1).

Remarque 2.6.6. On remarque que les étapes détaillées ci-dessus ne peuvent commencer à la précision $k = 1$. Heureusement la p-torsion $h(X)$ ainsi que la relation $j(E^{\nu}) = j(E)^{\hat{\Sigma}}$ sont à la bonne précision c'est-à-dire 1. Les seuls éléments du système qui sont donc à relever (à la précision 2) sont les coefficients de l'équation de la courbe (cela détermine le j-invariant aussi à la précision 2). L'existence et l'unicité de ce relèvement (à isomorphisme-près) sont garanties par la p-torsion $h(X)$ plus précisément par l'équation:

$$\Psi_p(\tilde{E}) = 0 \mod h(X) \quad \text{à la précision 2}$$

Lorsque nous utilisons la nouvelle approche dite par évaluation directe du Verschiebung basée sur le théorème 2.6.2:

Corollaire 2.6.7. *Le relèvement canonique de toute courbe elliptique ordinaire $E/\mathbb{F}_q$ avec $j(E) \neq 0, 1728$ se fait en $\tilde{O}(p.n^2 + n.N.D(p))$, où $D(p)$ est la complexité des formules de Kohel pour le calcul du Verschiebung à la précision N (ces formules n'ont pas besoin de prendre des extensions). Lorsque d est le degré de l'extension de $\mathbb{F}_q$ sur laquelle se trouvent les racines du polynôme Ψ_p, la méthode utilise seulement $\tilde{O}(p.n^2 + p^{0.5}.n.d.N)$ opérations, où le meilleur cas correspondrait à $d = 1$ où $O(p^{0.5})$ est la complexité de la méthode [2].*

Exemple 2.6.8. :

Soit E une courbe elliptique ordinaire sur $\mathbb{F}_5[T]/m(T)$ avec $m(T) = T^{10} + 3T^6 + 3T^5 + T^2 + 2T + 4$ donnée par l'équation :

$y^2 = x^3 + a_4x + a_6$ où : $a_4 = T^7 + T^5 + T$ et $a_6 = T^9 + T^3$
tels que le j-invariant de E est $j = 3T^9 + 4T^8 + 4T^7 + T^6 + T^5 + 2T^4 + T^3 + 4T + 2$;

Le polynôme de p-division et le noyau du Verschiebung sont donnés par:

$$\begin{aligned}\Psi_p &= (2T^7 + 2T^5 + 2T)x^{10} + (4T^9 + 4T^8 + 3T^7 + 4T^6 + 2T^5 + T^4 \\ &\quad + T^3 + 4T^2 + 4T + 4)x^5 + (4T^9 + 3T^8 + 2T^7 + T^5 + T^4 + 2T^3 + 2T^2 + 2T);\\ h_p &= x^2 + (T^9 + T^8 + 2T^3 + 4T^2 + 3T + 1)x + (3T^9 + T^7 + T^6 + 2T^5 + T^3 + 2T^2 + 4T + 3);\end{aligned}$$

exemple 2.1 – Calcul du Relevé Canonique par Évaluation Directe du Verschiebung

Le même polynôme de Teichmuller M de l'exemple 2.6.4 reste valide.
En utilisant la remarque 2.6.6, on obtient à la précision 2:
$[A4, A6] = [T^7 + T^5 + T,\ T^9 + 10T^8 + 20T^7 + 10T^6 + 5T^5 + 10T^4 + 6T^3 + 20T^2 + 15T + 20]$
$H_p = x^2 + (21T^9 + 21T^8 + 5T^5 + 5T^4 + 17T^3 + 24T^2 + 8T + 1)x + (8T^9 + 16T^7 + 6T^6 + 22T^5 + 15T^4 + 16T^3 + 2T^2 + 19T + 3)$
En utilisant la méthode la section 2.6.3 on obtient une forme d'Artin-Schreier:

$$e^{\Sigma} + a.e + b = 0 \mod p^2$$

$a = 5T^9 + 5T^7 + 5T^6 + 10T^5 + 20T^4 + 5T^3 + 20$,
$b = 21T^9 + 15T^8 + 2T^7 + 2T^6 + 14T^4 + 24T^3 + 17T^2 + 10T + 23$
Par suite à partir de l'algorithme 7, on obtient le relèvement canonique du j-invariant j de $\tilde{E}$ à la précision $3 = 2(2) - 1$.

$$298T^9 + 164T^8 + 184T^7 + 241T^6 + 516T^5 + 577T^4 + 371T^3 + 425T^2 + 594T + 482$$

Relèvement Canonique par Relèvement de la p-Torsion Étale

On remarque que dans la relation de la proposition 2.5.5 de Satoh:

$$\tilde{H}_p = H_p + e \quad \text{avec} \quad e = \frac{\tilde{\Psi}_p.H'_p}{\tilde{\Psi}'_p} \mod H_p$$

pour le relèvement de la p-torsion H_p de la précision k à la précision $2k+1$ encode les informations entre l'équation de la courbe $\tilde{E}$ et sa p-torsion H_p à la précision $2k$ comme dans le système défini dans la section 2.6.3. Alors on arrive à corriger tous les éléments à partir d'une troisième équation donnée par la relation $j(E^v) = j(E)^{\tilde{\Sigma}}$ en tenant compte du retard de precision sur H_p. Ainsi dans la relation $j(E^v) = j(E)^{\tilde{\Sigma}}$ on peut calculer le relevé $\tilde{E}$ en corrigeant son coefficient $\tilde{a}_6$ avec une faible dépendance en p.
D'autre part, à une précision N on peut évaluer Ψ_p (associée à la courbe $\tilde{E}/\mathbb{Z}_q$) modulo H_p en temps $\tilde{0}(\alpha.N.\log q.\log p) = \tilde{0}(\alpha.N.n)$ où $\alpha = \deg H_p$. Alors nous avons le lemme suivant:

Lemme 2.6.9. *À partir de $\tilde{H}_p$ à la précision k et un relèvement quelconque H^*_p de $\tilde{H}_p$ à la précision $2k+1$, le relevé $\tilde{H}_p$ à la précision $2k$ associé à $\tilde{E}$ est donné par:*

$$\tilde{H}_p = H^*_p + e \quad \textit{avec} \quad e = \frac{\Psi_p.H^{*\prime}_p}{\Psi'_p} \mod H^*_p.$$

Démonstration. La formule de Newton associée à ce relèvement est la suivante: prendre un relevé arbitraire H^*_p , soit $a = \Psi_p \mod H^*_p$ et $b = \Psi_p \mod (H^*_p + p)$. Alors la dérivée associée à cette méthode de Newton est donnée par: $c = (b-a)/p^k$, et nous avons l'équation suivante $a + cp^kQ = 0 \mod (H^*_p, p^{2k})$. Comme l'équation reste valide à la précision k, elle ne dépend pas du choix de H^*_p. Alors le relevé $\tilde{H}_p$ associé à $\tilde{E}$ est: $\tilde{H}_p = H^*_p + p^kQ$. □

D'où le résultat suivant:

Théorème 2.6.10. *Pour toute courbe elliptique $E/\mathbb{F}_q$, en utilisant la méthode (la section 2.6.3) on calcule le relèvement canonique $\tilde{E}/\mathbb{Z}_q$ et la trace du Frobenius à la précision p-adique N en temps $\tilde{O}(n.N.p)$.*
En particulier, pour le comptage où $N = O(n)$, on détermine χ_{π_q} avec $\tilde{O}(pn^2)$ opérations.

Entrée: E une courbe elliptique sur $\mathbb{F}_q$ avec $q = p^n$, $n \in \mathbb{N}$.
Sortie: Le relèvement canonique de E à la précision N.

1. Calculer H_p sur $\mathbb{F}_q$ en utilisant une interpolation rapide $\hat{\pi}(\pi(P))$ alors $\Psi_p = H_p^p$;
2. Calculer $\tilde{a}_6$ de $\tilde{E}$ à la précision 2 à partir de l'équation $\tilde{\Psi}_p \mod H_p = 0$ à la précision 2 ;
3. Calculer $\tilde{H}_p \mod p^{2+1}$.
4. $k = 2$
5. while $k < \lceil N/2 \rceil$;
   a. Calculer à la précision $2(k+1)$, $\tilde{\Psi}_p \mod \tilde{H}_p$ à la précision $2k$ à partir de deux approximations de $\tilde{E} \mod p^{k+1}$;
   b. Calculer $\tilde{H}_p \mod p^{2k+1}$ à partir des formules de Satoh (la proposition 2.5.5).
   c. Déterminer le coefficient $\tilde{a}_6$ de $\tilde{E} \mod p^{2k+1}$ dans la relation $j(\tilde{E}^\nu) = j(\tilde{E})^{\hat{\Sigma}}$;
   d. $k = 2k$;
6. Retourner $\tilde{E}(\tilde{a}_6)$ à la précision N (l'autre coefficient étant relevé au hazard).

Algorithm 3 – Calcul du Relevé Canonique à partir du Relèvement du p-torsion étale

En resumé, le théorème 2.6.2 constitue une bonne alternative pour améliorer la dépendance en p dans les algorithmes utilisant le relèvement canonique. Et le résultat du théorème 2.6.10 présente un coût plus pratique pour le calcul du polynôme caractéristique χ d'une courbe elliptique ordinaire. En effet l'approche de Kedlaya (relèvement quelconque utilisant la cohomologie Monsky-Washnitzer) présente aussi une bonne dépendance en p (linéaire) ; cependant elle réconstitue χ avec une complexité en temps (et en espace) de $O(n^{3+\varepsilon})$. Cette dependance en p fût amélioré par Havey [46] en $\tilde{O}(\sqrt{p}n^{5/2}m + n^4 m \log p)$ au prix de coût élevé en n.

Ce qui complète l'étude de nos améliorations des algorithmes de relèvement canonique en dimension 1.
Cependant du genre $g = 1$ au genre superieur (par exemple $g = 2$), certaines de ces astuces peuvent devenir moins agréables en terme de complexité des opérations.

Deuxième partie

DIMENSION SUPERIEURE

3

VARIÉTÉS ABÉLIENNES

Dans la section 2.2 du chapitre 2 nous avons abordé les courbes elliptiques sur $\mathbb{C}$ comme étant des tores complexes de dimension 1 ($\mathbb{C}/\Lambda$ avec Λ un réseau sur $\mathbb{C}$) sur lesquels existe un plongement naturel dans l'espace projectif $\mathbb{P}^2$ défini par :

$$z \mapsto [\wp_\Lambda(z) : \wp'_\Lambda(z) : 1] \quad et \quad 0 \mapsto [0 : 1 : 0]$$

On dit que les courbes elliptiques complexes sont des variétés abéliennnes de dimension 1. En général nous avons la définition suivante.

Définition 3.0.1. Une variété abélienne complexe est un groupe de Lie complexe $\mathcal{A}$ connexe admettant un plongement dans un espace projectif.

Un tel groupe de Lie est nécéssairement compact et si nous notons par V son espace tangent en 0 et $\phi_v : \mathbb{C} \longrightarrow \mathcal{A}$ l'unique homomorphisme différentiable telque : $\phi_v(0) = 0$ et $d\phi_v(1) = v$. Alors l'application exponentielle $\exp : V \longrightarrow \mathcal{A}$ définie pour tout v par : $\phi_v(1)$, est surjective et son noyau $\ker(\exp) = \Lambda$ est un réseau dans l'espace vectoriel V [81]. Ainsi $\mathcal{A}$ est isomorphisme au tore V/Λ.
Nous abordons ce chapitre par une étude descriptive des tores complexes ensuite nous allons nous focaliser sur ceux admettant un plongement dans un espace projectif .

3.1 TORES COMPLEXES

Soit V un espace vectoriel complexe de dimension g et Λ un réseau dans V c'est à dire un sous groupe discret de rang $2g$ de V. Alors on appelle tore de dimension g, le quotient $X = V/\Lambda$ de l'action de Λ sur V, c'est un groupe de Lie complexe de dimension g.
Pour caractériser un tore $X = V/\Lambda$ on peut se convenir sur une base de $e_1, ..., e_g$ de V et $\lambda_1, ..., \lambda_{2g}$ du réseau Λ. Lorsqu'on écrit les λ_i dans la base $e_1, ..., e_g$ on obtient la matrice $\Pi \in M(g \times 2g, \mathbb{C})$ définie par :

$$\Pi = \begin{pmatrix} \lambda_{11} & \cdots & \lambda_{1,2g} \\ \vdots & & \vdots \\ \lambda_{g1} & \cdots & \lambda_{g,2g} \end{pmatrix} \quad avec \quad \lambda_i = \sum_{j=1}^{g} \lambda_{ji} e_j$$

appelée *matrice de période de* X. Cette matrice caractérise le tore X même si elle dépend du choix des bases de V et de Λ. La proposition suivante caractérise les matrices de ce type qui déterminent un tore.

Proposition 3.1.1. *$\Pi \in M(g \times 2g, \mathbb{C})$ est une matrice de période d'un tore complexe si et seulement si la matrice $P = \begin{pmatrix} \Pi \\ \overline{\Pi} \end{pmatrix} \in M_{2g}(\mathbb{C})$ est inversible, avec $\overline{\Pi}$ matrice conjuguée de Π.*

Démonstration. Aller à [3, § 1.1]. □

3.1.0.1 *Homomorphismes*

Soient $X_1 = V_1/\Lambda_1$ et $X_2 = V_2/\Lambda_2$ des tores complexes de dimensions respectives g_1 et g_2. Une application analytique de X_1 vers X_2 est la composée d'un morphisme (de groupes de Lie) et d'une translation.
Tout morphisme $f : X_1 \longrightarrow X_2$ se déduit de manière unique d'une application $\mathbb{C}-$linéaire $F : V_1 \longrightarrow V_2$ telle que : $F(\Lambda_1) \subset \Lambda_2$.
L'ensemble des morphismes entre les tores X_1 et X_2 forment un groupe abélien noté $\mathrm{Hom}(X_1, X_2)$. Par suite on obtient deux morphismes de groupes injectifs notés ρ_a et ρ_r définis par :

$$\rho_a : \mathrm{Hom}(X_1, X_2) \longrightarrow \mathrm{Hom}_{\mathbb{C}}(V_1, V_2), \quad \rho_a(f) = F\,;$$
$$\rho_r : \mathrm{Hom}(X_1, X_2) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\Lambda_1, \Lambda_2), \quad \rho_r(f) = F_{\Lambda_1}$$

où F_{Λ_1} la restriction de F à Λ_1 est $\mathbb{Z}-$linéaire . Le morphisme ρ_a est appelé la *représentation analytique* de $\mathrm{Hom}(X_1, X_2)$ et ρ_r est appelé sa *représentation rationnelle*. On notera par

$$\mathrm{Hom}_{\mathbb{Q}}(X_1, X_2) := \mathrm{Hom}(X_1, X_2) \otimes_{\mathbb{Z}} \mathbb{Q}$$

Proposition 3.1.2. $\mathrm{Hom}(X_1, X_2) \simeq \mathbb{Z}^m$ *pour un certain* $m \leq 4g_1g_2$.

Démonstration. Voir [3, Proposition 1.2.2.]. Le morphisme F_{Λ_1} détermine totalement F et f et d'autre part nous avons $\mathrm{Hom}_{\mathbb{Z}}(X_1, X_2) \simeq \mathbb{Z}^m$. Alors on conclut avec l'injectivité de ρ_r. □

On considère Π_1 et Π_2 les matrices de période respectives des tores X_1 et X_2 selon des bases choisies de (V_1, Λ_1) et de (V_2, Λ_2). Soit $f : X_1 \longrightarrow X_2$ un morphisme, on note respectivement par $A \in M(g_2 \times g_1, \mathbb{C})$ et $R \in M(2g_2 \times 2g_1, \mathbb{Z})$ les matrices des morphismes ρ_a et ρ_r. Alors de la condition $\rho_a(f)(\Lambda_1) \subset \Lambda_2$ nous avons :

$$A\Pi_1 = \Pi_2 R.$$

Et réciproquement toutes matrices $A \in M(g_2 \times g_1, \mathbb{C})$ et $R \in M(2g_2 \times 2g_1, \mathbb{Z})$ satisfaisant cette condition définissent un morphisme de X_1 vers X_2.
Lorsque $f \in \mathrm{End}\, X$, on a la rélation :

$$\begin{pmatrix} A & 0 \\ 0 & \overline{A} \end{pmatrix} \begin{pmatrix} \Pi \\ \overline{\Pi} \end{pmatrix} = \begin{pmatrix} \Pi \\ \overline{\Pi} \end{pmatrix} R$$

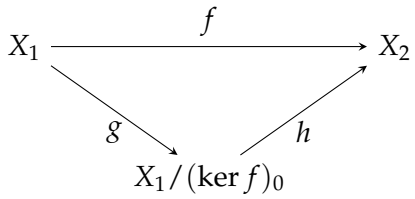
Sachant que la matrice $\begin{pmatrix} \Pi \\ \overline{\Pi} \end{pmatrix}$ est inversible on peut déterminer A à partir de R et vise-versa.

Proposition 3.1.3. *Soit* $f : X_1 \to X_2$ *un morphisme de tores complexes, alors :*

- $\mathrm{Im}\, f$ *est un sous tore de* X_2 *;*
- $\ker f$ *est un sous groupe fermé de* X_1 *et sa composante connexe contenant* 0 *notée* $(\ker f)_0$ *est un sous tore* X_1 *d'indice fini dans* $\ker f$.

Démonstration. Voir [3]. En effet $\mathrm{Im}\, f = F(V_1)/F(V_1) \cap \Lambda_2$ et $F(V_1) \cap \Lambda_2$ est un sous groupe discret de $F(V_1)$ engendré par $F(V_1)$ comme un $\mathbb{R}-$espace vectoriel.
D'autre part $\ker f$ étant compact ; la composante connexe $F^{-1}(\Lambda_2)_0$ de $F^{-1}(\Lambda_2)$ contenant 0 est un sous espace de V_1 et $(\ker f)_0 = F^{-1}(\Lambda_2)_0/(F^{-1}(\Lambda_2)_0 \cap \Lambda_1)$ est compact avec $F^{-1}(\Lambda_2)_0 \cap \Lambda_1$ est un réseau dans $F^{-1}(\Lambda_2)_0$. □

Nous allons nous intéresser maintenant à une classe d'homomorphismes de tores complexes appelés *isogénies*. Par définition une isogénie de tore complexe de X_1 vers X_2 est un morphisme surjective de $X_1 \to X_2$ ayant un noyau fini et le cardinal de son noyau est appelé son *degré*. Le degré de l'isogénie est aussi égal à $[\Lambda_2 : \rho_r(f)(\Lambda_1)]$. De plus si f est un endomorphisme on a $\Lambda_1 = \Lambda_2$ et $\deg f = \deg \rho_r(f)$.
D'autre part un morphisme $X_1 \to X_2$ est une isogénie si et seulement si il est surjectif et $\dim X_1 = \dim X_2$.
Si $K \subset X_1$ est un sous groupe fini, le quotient X_1/K est un tore complexe et la projection naturelle $X_1 \to X_1/K$ est une isogénie. Et réciproquement à isomorphisme près toute isogénie est de cette forme.
Tout morphisme surjectif $f : X_1 \to X_2$ de tore complexe se décompose canoniquement suivant le diagramme de *factorisation de Stein* ci-dessous :



Où g est un morphisme surjectif de noyau $(\ker f)_0$ et h une isogénie.
L'application analytique $F = \rho_a(f)$ est un isomorphisme si seulement si f est une isogénie. Dans ce cas, à isomorphisme près, on peut prendre $F = \mathrm{id}$ alors $\Lambda_1 \subset \Lambda_2$ et f dévient l'application canonique $V_1/\Lambda_1 \to V_2/\Lambda_2$. Par consequent il y a une bijection entre les isogénies partant de X_1 et les sous groupes de X_1.
Pour tout entier n on note par n_{X_1} l'endomorphisme de X_1, $x \mapsto nx$. Si $n \neq 0$ on appelle *groupe des points de n-torsion* et note $X_1[n]$ le noyau de n_{X_1}. On a

$$X_1[n] = \frac{1}{n}\Lambda_1/\Lambda_1 \simeq \Lambda_1/n\Lambda_1 \simeq (\mathbb{Z}/n\mathbb{Z})^{2g_1}.$$

Par conséquent $\mathrm{Hom}(X_1, X_2)$ est un groupe abélien sans torsion et on peut le considérer comme un sous groupe de $\mathrm{Hom}_{\mathbb{Q}}(X_1, X_2)$. On y étend aussi la notion de degré par la propriété de composition :

$$\deg fg = \deg f . \deg g \quad \forall f, g \in \mathrm{Hom}_{\mathbb{Q}}(X_1, X_2).$$

Par suite on définit *l'exposant* $e = e(f)$ d'une isogénie f comme étant le plus petit entier positif n pour lequel $nx = 0$, $\forall x \in \ker f$.

Proposition 3.1.4. *Pour tout isogénie $f : X_1 \to X_2$ d'exposant e il existe une isogénie $g : X_2 \to X_1$, unique (à isomorphisme près) telle que $gf = e_{X_1}$ et $fg = e_{X_2}$. Et g est appelé isogénie contragrédiente de f.*

Démonstration. Voir [3, Proposition 1.2.6.]. Comme $\ker f \subset \ker e_{X_1} = X_1[e]$, on prend $g : X_1 \to X_2$ comme l'unique facteur tel que $gf = e_{X_1}$. Pour tout $y \in \ker g$ on a $x \in \ker e_{X_1}$ avec $f(x) = y$ et $ey = f(ex) = 0$ alors $\ker g \subset X_2[e]$. Et le reste du résultat suit. □

On en déduit que "*l'existense d'une isogènie*" définie une rélation d'équivalence sur l'ensemble des tores complexes. Nous dirons alors que les tores en rélation sont *isogènes*. Et un élément de $\mathrm{End}\, X$ est une isogénie si et seulement si, il est inversible dans $\mathrm{End}_{\mathbb{Q}} X$.

3.1.0.2 *Formes de Riemann sur un Tore*

On rapelle qu'une forme Hermitienne H sur un l'espace vectoriel V est une application $V \times V \to \mathbb{C}$, $\mathbb{C}$-linéaire en la prémière variable et vérifiant $H(x,y) = \overline{H(y,x)}$ pour tout $x, y \in V$.

Définition 3.1.5. Une forme de Riemann sur un tore complexe $X = V/\Lambda$ est une forme Hermitiennne sur V telle que $\operatorname{Im} H(\Lambda, \Lambda) \subset \mathbb{Z}$.

Exemple 3.1.6. Soit $\Omega \in M_g(\mathbb{C})$ qui est symétrique et $\operatorname{Im}\Omega > 0$, alors $H(x,y) = {}^t x.(\operatorname{Im}\Omega)^{-1}.\overline{y}$ est une forme de Riemann définie et positive sur $\mathbb{C}^g(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$.

Remarque 3.1.7. Les correspondances suivantes :

$$E(x,y) = \operatorname{Im} H(x,y) \quad et \quad H(x,y) = E(ix,y) + iE(x,y).$$

définissent une bijection entre les formes hermitiennes H sur V et les formes alternées réelles E sur V telles que $E(ix,iy) = E(x,y)$ pour tout $x, y \in V$ [3, Lemme 2.1.7]. En effet, lorsque que nous avons E on a:

$$H(x,y) = E(ix,y) + iE(x,y) = E(iy,x) - iE(y,x) = \overline{H(y,x)}$$

Et réciproquement à partir H, la forme $E = \operatorname{Im} H$ est alternée et on a:

$$E(ix,iy) = \operatorname{Im} H(ix,iy) = \operatorname{Im} H(x,y) = E(x,y).$$

De plus, on dira que E est une forme symplectique si E est non dégénérée.

3.1.0.3 *Dual d'un Tore Complexe*

Soit $\hat{V} = \operatorname{Hom}_{\bar{\mathbb{C}}}(V, \mathbb{C})$ l'ensemble des formes antilinéaires de V vers $\mathbb{C}$. L'ensemble

$$\hat{\Lambda} = \{l \in \hat{V} : \operatorname{Im}(l(\Lambda)) \subset \mathbb{Z}\}$$

est un réseau dans $\hat{V}$ et on appelle *tore complexe dual* $\hat{X}$ de X le tore complexe de dimension g défini par : $\hat{V}/\hat{\Lambda}$. Soit $f : X_1 \to X_2$ un morphisme de représentation analytique F. L'application $F^* : \widehat{V}_2 \to \widehat{V}_1$ qui associe à toute forme antilinéaire $l_2 \in \widehat{V}_2$ la forme antilinéaire $l_2 \circ F \in \widehat{V}_1$ induit un morphisme $\widehat{f} : \widehat{X}_2 \to \widehat{X}_1$ puisque $F^*\widehat{\Lambda}_2 \subseteq \widehat{\Lambda}_1$.
De plus nous avons :

— $\widehat{\mathrm{id}}_X = \mathrm{id}_{\widehat{X}}$ et $\widehat{\widehat{f}} = f$.

— Et si $g : X_2 \to X_3$ est un morphisme de tore complexe, alors

$$\widehat{gf} = \widehat{f}\widehat{g}.$$

Proposition 3.1.8. *Soit $f : X_1 \to X_2$ est une isogénie de tores complexes, alors l'application duale $\widehat{f} : \widehat{X}_2 \to \widehat{X}_1$ est une isogénie dont le noyau est isomorphe à* $\operatorname{Hom}(\ker f, \mathbb{C}_1)$ *et nous avons* $\deg \widehat{f} = \deg f$.

Démonstration. Aller à [3]. □

3.1.1 *Fibrés en Droites et Facteur d'Automorphie*

Une variété abélienne étant (à isomorphisme près) un tore de dimension g, cependant à part le cas de la dimension 1 un tore de dimension g n'est pas forcement une variété abélienne.
Soient $X = V/\Lambda$ un tore et $f : X \to \mathbb{C}$ fonction analytique définie sur tout X. Alors f est de la forme $f : V \longrightarrow \mathbb{C}$ et invariant par Λ. On considère une classe de ses fonctions définies par :

$$f(v + \lambda) = a(v, \lambda) f(v). \tag{3.1}$$

où a est une fonction donnée de $V \times \Lambda \to \mathbb{C}^*$ vérifiant la condition d'associativité $a(x, \lambda_1 + \lambda_2) = a(x, \lambda_1) a(x + \lambda_1, \lambda_2)$. On appelle la fonction a un *facteur d'automorphie*. Par la suite le théorème d'Appell-Humbert caractérise les facteurs d'automorphie pour lesquels les fonctions $f_1, \cdots, f_{n+1}$ de cette classe définissent une application $v \in V \mapsto (f_1(v), \cdots, f_{n+1}(v)) \in \mathbb{P}^n_{\mathbb{C}}$ se factorisant en une application rationnelle $X \to \mathbb{P}^n_{\mathbb{C}}$.
On peut voir f comme une application $V \to V \times \mathbb{C}$, $v \to (v, f(v))$ une section de la projection canonique $V \times \mathbb{C} \to V$. Alors Λ agit aussi sur $V \times \mathbb{C}$ par : $\lambda.(v, \alpha) \mapsto (v + \lambda, a(v, \lambda)\alpha)$ et nous avons le diagramme commutatif suivant :

$$\begin{array}{ccc} V \times \mathbb{C} & \longrightarrow & (V \times \mathbb{C})/a(\Lambda) \\ \downarrow & & \downarrow p \\ V & \xrightarrow{v} & X = V/\Lambda \end{array}$$

Où p est la projection canonique induite par la projection $V \times \mathbb{C} \to V$. Comme Λ est un groupe discret agissant proprement et librement sur V alors il existe toujours des sections (analytiques) locales pour a. On appelle l'espace géometrique $\mathcal{L} = (V \times \mathbb{C})/a(\Lambda)$ un fibré en droite sur X dont l'ensemble des sections (locales) forme un faisceau qui détermine entièrement $\mathcal{L}$.

3.1.2 *Théorème d'Appell-Humbert*

Les facteurs d'automorphie caractérisent explicitement les fibrés en droite sur les tores complexes. Nous résumons dans cette partie quelques propriétés sur ces facteurs d'automorphie pour plus de détails le lecteur peut se réferer à [96].
On note Pic X le groupe des fibrés en droite sur X et Pic $X \simeq H^1(X, \mathcal{O}_X^*)$. Pour un fibré en droites analytique $\mathcal{L}$ sur X on note par $\tilde{\mathcal{L}} = v^*\mathcal{L}$ l'image réciproque de $\mathcal{L}$ sur V. Soit $\mathcal{O}_V$ le fibré des fonctions analytiques sur V et $\mathcal{O}_V^*$ celui des fonctions analytiques inversibles, alors nous avons la suite exacte suivante:

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathcal{O}_V \xrightarrow{exp} \mathcal{O}_V^* \longrightarrow 0$$

On en déduit que $H^p(V, \mathcal{O}_V^*) = 0$ pour $p > 0$.
Il est prouvé dans [96] que $H^1(X, \mathcal{O}_X^*) \simeq H^1(\Lambda, \Gamma(\mathcal{O}_X^*))$. Si $\mathcal{F}$ est un fibré en droites sur X alors le facteur d'automorphie associé à $\mathcal{F}$ sera noté $a_{\mathcal{F}}$ un cocycle représentant $\mathcal{F}$. Les sections globales de $\mathcal{F}$ sont exactement les fonctions analytiques $\vartheta : V \to \mathbb{C}$ telles que : pour tout $\lambda \in \Lambda$ et $v \in V$,

$$\vartheta(v + \lambda) = a_{\mathcal{F}}(v, \lambda)\vartheta(v).$$

De la suite exacte suivante :

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathcal{O}_X \xrightarrow{exp} \mathcal{O}_X^* \longrightarrow 0$$

On déduit un morphisme de connexion $c_1 : H^1(X, \mathcal{O}_X^*) \to H^2(X, \mathbb{Z})$. Si $\mathcal{L}$ est un fibré en droites sur X, le facteur d'automorphie associé à $\mathcal{L}$ peut être écrit sous la forme $a_{\mathcal{L}} = exp(2\pi i g)$ et sa classe de Chern notée $c_1(\mathcal{L})$ correspond sur Λ à la forme alternée $E_{\mathcal{L}} : (\lambda_1, \lambda_2) \mapsto g(\lambda_2, v + \lambda_1) + g(\lambda_1, v) - g(\lambda_1, v + \lambda_2) - g(\lambda_2, v)$ pour v quelconque dans V. Si $Alt^n(V, \mathbb{C})$ désigne le groupe des $\mathbb{R}$-formes alternées sur $\mathbb{C}$ alors l'extension réelle $E_{\mathcal{L}} \in Alt^2_{\mathbb{R}}(V, \mathbb{C})$ satisfait $E(ix, iy) = E(x, y)$ pour tout $x, y \in V$. Réciproquement, l'image de la classe de Chern c_1 correspond exactement aux formes alternées $E \in Alt^2_{\mathbb{R}}(V, \mathbb{C})$ telles que $E(\Lambda, \Lambda) \subset \mathbb{Z}$ et $E(ix, iy) = E(x, y)$ pour tout $x, y \in V$. Le lemme 3.1.7 montre qu'on peut voir $E_{\mathcal{L}}$ comme une forme hermitienne sur V.
On appelle *groupe de Néron-Severi* de X noté $NS(X)$, le noyau de $\gamma : H^2(X, \mathbb{Z}) \to H^2(X, \mathcal{O}_X)$. C'est l'ensemble des classes de Chern des éléments de $\operatorname{Pic} X$, alors on désigne par $\operatorname{Pic}_0 X$ le noyau de $c_1 : \operatorname{Pic} X \to H^2(X, \mathbb{Z})$.
Soit $\mathcal{L} \in \operatorname{Pic} X$ dont E et H sont respectivement sa forme de Chern et sa forme Hermitienne associées. Soit $\mathbb{C}_1^* = \{z \in \mathbb{C}, |z| = 1\}$ et $\chi : \Lambda \to \mathbb{C}_1^*$ un semi-caractère sur Λ pour E, c'est à dire $\chi(\lambda_1 + \lambda_2) = \chi(\lambda_1)\chi(\lambda_2)\exp(i\pi E(\lambda_1, \lambda_2))$ si $\lambda_1, \lambda_2 \in \Lambda$. Le théorème suivant montre qu'il existe toujours un facteur d'automorphie de la forme $a_{\mathcal{L}}(\lambda, v) = \chi(\lambda)exp(\pi H(v, \lambda) + \frac{\pi}{2}H(\lambda, \lambda))$ pour $\mathcal{L}$. Réciproquement, si H est une forme hermitienne telle que $\operatorname{Im} H(\Lambda, \Lambda) \subset \mathbb{Z}$ et χ est un semi-caractère pour H (c'est à dire pour $\operatorname{Im} H$), alors $a(\lambda, v) = \chi(\lambda)exp(\pi H(v, \lambda) + \frac{\pi}{2}H(\lambda, \lambda))$ est un facteur d'automorphie. Par suite on notera $L(H, \chi)$ le fibré en droites associé au facteur d'automorphie $a(\lambda, v)$.

Théorème 3.1.9. *(Appell-Humbert). L'ensemble des (H, χ) où H est une forme hermitienne telle que $\operatorname{Im} H(\Lambda, \Lambda) \subset \mathbb{Z}$ et χ est un semi-caractère pour H forme un groupe via :*

$$(H_1, \chi_1).(H_2, \chi_2) = (H_1 + H_2, \chi_1\chi_2)$$

De plus ce groupe est isomorphe à $\operatorname{Pic} X$ via l'application $(H, \chi) \mapsto L(H, \chi)$, rendant le diagramme suivant commutatif :

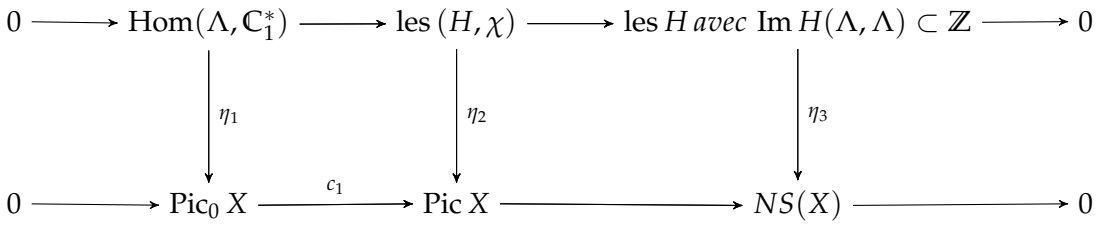


FIGURE 3.1 – Diagramme d'Appell-Humbert

Démonstration. Aller à [3, § 2.2] et [96, § 2.3]. □

Si $\mathcal{L} = L(H, \chi)$ est un fibré en droites sur X. on notera $L(H, \chi)^n = L(nH, \chi^n)$ et pour tout $v \in V$ on a :

$$t_v^* L(H, \chi) = L(H, \chi exp(\operatorname{Im} H(v, \cdot)))$$

On dira que $\mathcal{L}$ est symétrique (resp. antisymétrique) si $[-1]^*\mathcal{L} \simeq \mathcal{L}$ (resp. si $[-1]^*\mathcal{L} \simeq \mathcal{L}^{-1}$). De manière équivalente $\mathcal{L}$ est symétrique (resp. antisymétrique) si $[n]^*\mathcal{L} \simeq \mathcal{L}^{n^2}$ (resp. $[n]^*\mathcal{L} \simeq \mathcal{L}^n$), pour tout $n \in \mathbb{Z}$.
De plus si $f : X_1 \to X_2$ une isogénie de tores complexes, soit H_2 une forme hermitienne sur V_2 de semi-caractère associé χ_2 alors on a :

$$f^* L_2(H_2, \chi_2) = L_1(\rho_a(f)^* H_2,\, \rho_r(f)^* \chi_2).$$

Remarque 3.1.10. Si $\mathcal{L} = L(H, \chi) \in \operatorname{Pic} X$, alors le Théorème 2.3.3 de [3] montre qu'il existe un morphisme :

$$\phi_{\mathcal{L}} : X \to \widehat{X}, \quad x \mapsto t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$$

dont la représentation analytique est $\phi_H : V \to \widehat{V}, \quad v \mapsto H(v, \cdot)$.
$\phi_{\mathcal{L}}$ ne dépend de la classe de Chern de $\mathcal{L}$. Réciproquement une application $f : X \to \widehat{X}$ est de la forme $\phi_{\mathcal{L}}$ pour un fibré en droites $\mathcal{L}$ sur X si seulement si l'application :

$$H : V \times V \to \mathbb{C}, \quad (v, w) \mapsto \rho_a(f)(v)(w)$$

est hermitienne, et H est alors le type de $\mathcal{L}$ [3].

3.1.3 *Polarisation sur un Tore*

D'après la définition 3.0.1, un tore complexe $X = V/\Lambda$ est une variété abélienne si elle admet un plongement dans un espace projectif. Un facteur d'automorphie (ou son fibré) sur X définit un morphisme $X \to \mathbb{P}_{\mathbb{C}}^{\deg \mathcal{L}}$. On dit que ce fibré est *très ample* lorsque ce morphisme est un plongement. Réciproquement tout plongement de ce genre provient d'un fibré très ample.
On dit qu'un fibré $\mathcal{L}$ est *ample* s'il existe un n suffisamment grand pour que $\mathcal{L}^n$ soit très ample.

Proposition 3.1.11. *$L(H, \chi)$ est ample si et seulement si H est définie et positif (c'est à dire E non dégénérée).*

Démonstration. Aller à [3, Théorème 4.5.1]. □

Remarque 3.1.12. Soit $f : X_1 \to X_2$ une isogénie de tores complexes, si $\mathcal{L}_2$ un fibré très ample sur X_2, alors $f^*\mathcal{L}_2$ est un fibré très ample sur X_1. De plus on peut trouver une rélation explicite entre les coordonnées projectives de X_2 associées à $\mathcal{L}_2$ et celles de X_1 associées à $f^*\mathcal{L}_2$ [96, Lemme 2.4.2], c'est à dire que l'on peut expliciter l'isogénie f par rapport à ces systèmes de coordonnées.

Une variété abélienne polarisée est un couple $(X, \mathcal{L})$ où X est une variété abélienne complexe et $\mathcal{L}$ un fibré ample sur X. Dans ce cas si $\mathcal{L} = (H, \chi)$, H est une forme hermitienne définie positive, alors le morphisme $\phi_{\mathcal{L}}$ est une isogénie et on dit que c'est la *polarisation* associée à $\mathcal{L}$. Le noyau noté $K(\mathcal{L})$ de $\phi_{\mathcal{L}}$ est l'ensemble des x dans X tels que $t_x^*\mathcal{L} \simeq \mathcal{L}$.

Proposition 3.1.13. *Soit $f : X_1 \to X_2$ une isogénie de variétés abéliennes, et $\mathcal{L}_1 = (H_1, \chi_1)$ un fibré en droites sur X_1. Alors il existe un fibré $\mathcal{L}_2 \in \operatorname{Pic} X_2$ tel que $\mathcal{L}_1 = f^*\mathcal{L}_2$ si et seulement si le noyau de f est un sous-groupe isotrope pour $E_1 = \operatorname{Im} H_1$ de $K(\mathcal{L}_1)$. Et le lien entre les deux polarisations est donné par le diagramme commutatif suivant :*

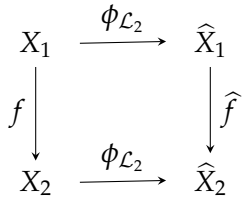


FIGURE 3.2 – Transport de polarisation entre variétés isogènes.

Démonstration. Aller à [96, Proposition 2.4.7.]. □

En particulier, $\#K(\mathcal{L}_1) = (\deg f)^2.\#K(\mathcal{L}_2)$, et par suite nous avons le corollaire suivant.

Corollaire 3.1.14. *Soit $\mathcal{M}$ un fibré en droites sur une variété abélienne X. Alors il existe un fibré en droites sur X tel que $\mathcal{M} = \mathcal{L}^n$ si seulement si $X[n] \subset K(\mathcal{M})$.*

Démonstration. Aller à [96, Corollaire 2.4.8.].
Si l'on suppose $\mathcal{M} = \mathcal{L}^n$, $\Lambda(\mathcal{M}) = \frac{1}{n}\Lambda(\mathcal{L})$ et donc $X[n] \subset K(\mathcal{M})$. Réciproquement la proposition précédente 3.1.13 donne l'existence d'un fibré $\mathcal{M}'$ tel que $\mathcal{M}^n = [n]^*\mathcal{M}'$. On déduit de la symétrie de $\mathcal{M}'$ et de la divisibilité de $\mathrm{Pic}_0 X$ que $\mathcal{L} = M' \otimes \mathcal{N}^{-1}$ tel que $\mathcal{M}'^n \otimes \mathcal{M}^{-1} \simeq \mathcal{N}^n$ satisfait $\mathcal{M} = \mathcal{L}^n$. □

3.1.4 *Espace Modulaire*

Soit $(X, \mathcal{L})$ une variété abélienne polarisée, notée souvent (X, H).
On appelle *base simplectique* de $E = \mathrm{Im}\, H$ une base $\alpha_1, \cdots, \alpha_g, \beta_1, \cdots, \beta_g$ de Λ telle que :

$$E(\alpha_i, \alpha_j) = E(\beta_i, \beta_j) = 0 \quad et \quad E(\alpha_i, \beta_j) = \delta_{i,j} d_i$$

où d_i sont des entiers positifs avec $d_i | d_{i+1}$ et $\delta_{i,j}$ est le symbole de Kronecker.
On appelle *Pfaffien* de E le produit $Pf(E) = d_1 \cdots d_g$. Si on pose $D = diag(d_1, \cdots, d_g)$ alors la matrice de E dans cette base est $\begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix}$. Et la matrice de période de X selon cette base et la base $e_1 = \beta_1, \cdots, e_g = \beta_g$ de V est

$$\Pi = (\Omega', \mathrm{Id})$$

On appelle le *type* de la polarisation $\mathcal{L}$, le g-uplets $(d_1, \cdots, d_g)$ (souvent par abus nous dirons "de type D"). Le produit $Pf(E)$ correspond au *degré* de la polarisation. La polarisation est dite *principale* si le type est $(1, \cdots, 1)$ ce qui est équivalent à dire que son degré est égal à 1.
De plus on montre que la matrice de H est $(\mathrm{Im}\, \Omega)^{-1}$ où $\Omega' = \Omega D$, alors Ω est symétrique et $\mathrm{Im}\, \Omega$ définie positive.
D'autre part si $\Omega \in \mathfrak{H}_g$ où :

$$\mathfrak{H}_g = \left\{ \Omega \in M_g(\mathbb{C}),\ {}^t(\Omega) = \Omega,\ Im(\Omega) > 0 \right\}$$

appelé le *demi-espace de Siegel* alors on montre que $\mathrm{Im}\, \Omega$ est une polarisation pour la variété abélienne $X_\Omega = \mathbb{C}^g / (\Omega D \mathbb{Z} + \mathbb{Z})$ associée à un fibré canonique $\mathcal{L}_0$ symétrique de caractéristique 0.

Soit $\mathcal{J}_D = \begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix}$ alors $Sp_{2g}^D(\mathcal{R}) = \left\{M \in M_{2g}(\mathcal{R}) : M\mathcal{J}_D\,{}^tM = \mathcal{J}_D\right\}$, pour un anneau commutatif $\mathcal{R}$ est un groupe. On notera $Sp_{2g}(\mathcal{R}) = Sp_{2g}^{\mathrm{Id}_g}(\mathcal{R})$. On appelle groupe symplectique de type D, le groupe $\Gamma_D = Sp_{2g}^D(\mathbb{Z})$. Il agit sur $\mathfrak{H}_g$ par : pour tout $\Omega \in \mathfrak{H}_g$ et $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_D$

$$\gamma\Omega = (\Omega Dc + d)^{-1}(\Omega Da + b)D^{-1}$$

Alors les deux tores X_Ω et $X_{\gamma\Omega}$ sont isomorphes en tant que variétés abéliennes polarisées de types D, la représentation rationnelle (resp. analytique) de cet isomorphisme est donnée par γ^{-1} (resp. $(c\Omega D + d)^{-1}$). Réciproquement deux variétés abéliennes polarisées $(X_{\Omega_1}, H_{\Omega_1})$ et $(X_{\Omega_2}, H_{\Omega_2})$ de types D sont isomorphes si et seulement si Ω_1 et Ω_2 sont dans la même orbite par Γ_D [3]Proposition 8.1.3. On note par $\mathfrak{A}_D = \mathfrak{H}_g/\Gamma_D$ l'espace modulaire des variétés abéliennes polarisées de type D.
En prenant pour base de V, $e_1 = \beta_1/d_1, \cdots, e_g = \beta_g/d_g$, on peut rafiner l'action de Γ_D. D'abord la matrice de période de X s'écrira : $\Pi = (\Omega_0, D)$ avec $\Omega_0 = D\Omega D$ et celle de H sera $(\operatorname{Im}\Omega_0)^{-1}$ pour la nouvelle base.
On part d'un isomorphisme σ_D de $Sp_{2g}^D(\mathbb{Q})$ sur $Sp_{2g}(\mathbb{Q})$ donnée par :

$$\gamma_D \mapsto \begin{pmatrix} \mathrm{Id}_g & 0 \\ 0 & D \end{pmatrix}^{-1} \gamma \begin{pmatrix} \mathrm{Id}_g & 0 \\ 0 & D \end{pmatrix}$$

γ_D induit un isomorphisme de $Sp_{2g}^D(\mathbb{Z})$ sur $\Gamma_D^0 = \left\{\gamma \in Sp_{2g}(\mathbb{Q}) : {}^t\gamma\Lambda_D \subset \Lambda_D\right\}$ où $\Lambda_D = \begin{pmatrix} \mathbb{Z}^g \\ D\mathbb{Z}^g \end{pmatrix}$. Ce qui conduit à une action de Γ_D^0 sur $\mathfrak{H}_g$ définie par :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\Omega = (\Omega c + d)^{-1}(\Omega a + b)$$

Et $\mathfrak{A}_D$ est isomorphe à $\mathfrak{H}_g/\Gamma_D^0$.

3.1.5 *Endomorphismes*

Soit $X = V/\Lambda$ une variété abélienne de dimension g sur laquelle on considère une polarisation $\mathcal{L}$. Cette polarisation induit une isogénie $\phi_\mathcal{L} : X \to \widehat{X}$ de degré d. Par suite la proposition 3.1.4 donne l'existence d'une isogénie $\psi_\mathcal{L}$ de degré d aussi telle que $\psi_\mathcal{L} \circ \phi_\mathcal{L} = d_X$ et $\phi_\mathcal{L} \circ \psi_\mathcal{L} = d_{\widehat{X}}$. D'où $\phi_\mathcal{L}$ admet dans $\mathrm{Hom}_\mathbb{Q}(\widehat{X}, X)$ un inverse $\phi_\mathcal{L}^{-1} = \frac{1}{d}\psi_\mathcal{L}$. Par conséquent tout $f \in \mathrm{End}_\mathbb{Q}(X)$ s'écrit sous la forme rh avec $h \in \mathrm{End}(X)$ et $r \in \mathbb{Q}$. On aura ainsi $\widehat{f} = r\widehat{h} \in \mathrm{End}_\mathbb{Q}(\widehat{X})$.
On considère l'application :

$$' : \mathrm{End}_\mathbb{Q}(X) \to \mathrm{End}_\mathbb{Q}(X), \quad f' = \phi_\mathcal{L}^{-1}\widehat{f}\phi_\mathcal{L}$$

À partir de $\widehat{gf} = \widehat{f}\widehat{g}$, $\widehat{\widehat{f}} = f$ et $\widehat{\phi_\mathcal{L}} = \phi_\mathcal{L}$ nous avons pour tout $f, g \in \mathrm{End}_\mathbb{Q}(X)$ et $r, s \in \mathbb{Q}$:

$$(rf + sg)' = rf' + sg'$$

$$(fg)' = g'f' \quad et \quad f'' = f$$

Alors l'application $'$ est une involution sur $\mathrm{End}_{\mathbb{Q}}(X)$, appelé *involution de Rosati* associée à la polarisation $\mathcal{L}$. Et le résultat suivant montre que $'$ est un *opérateur adjoint* à la forme hermitienne H et à la forme alternée E.

Proposition 3.1.15. *Soit $f \in \mathrm{End}_{\mathbb{Q}}(X)$.*

— $E(\rho_r(f)(\lambda), \nu) = E(\lambda, \rho_r(f')(\nu))$ *pour tout* $\lambda, \nu \in \Lambda$.

— $H(\rho_a(f)(v), w) = H(v, \rho_a(f')(w))$ *pour tout* $v, w \in V$.

Démonstration. Voir [3, Proposition 5.1.1.]. □

Soit $f \in \mathrm{End}_{\mathbb{Q}}(X)$, on note par P_f^r le polynôme caractéristique $\det(x\,\mathrm{Id}_\Lambda - \rho_r(f))$ de $\rho_r(f)$ son degré est $2g$ et on note par $Tr_r(f)$ l'opposé du coefficient de degré $(2g-1)$ appelé *trace rationnelle de f*. Alors l'application $(f, g) \mapsto Tr_r(f'g)$ est une forme bilinéaire symétrique, définie et positive sur le $\mathbb{Q}$-espace vectoriel $\mathrm{End}_{\mathbb{Q}}(X)$ [3, Pages: 117-118].. Et il en découle que le groupe des automorphismes d'une variété abélienne polarisée $(X, \mathcal{L})$ est fini et pour $f \in \mathrm{Aut}(X)$, $n \geq 3$ un entier, $f_{|X_n} = \mathrm{id}_{X_n}$ implique $f = \mathrm{id}_X$. Alors pour $n \geq 3$ on a :

$$Aut(X, \mathcal{L}) \hookrightarrow Aut_{\mathbb{Z}/n\mathbb{Z}}(X[n]) = GL_{2g}(\mathbb{Z}/n\mathbb{Z})$$

On dit que $f \in \mathrm{End}_{\mathbb{Q}}(X)$ est symétrique suivant la polarisation $\mathcal{L}$ si $f' = f$ et on note $\mathrm{End}^s_{\mathbb{Q}}(X)$ (resp. $\mathrm{End}^s(X)$) le sous ensemble de $\mathrm{End}_{\mathbb{Q}}(X)$ (resp. $\mathrm{End}(X)$) des éléments symétriques. Alors $\mathrm{End}^s_{\mathbb{Q}}(X)$ est $\mathbb{Q}$-espace vectoriel et $\mathrm{End}^s(X)$ est un groupe additif tel que: $\mathrm{End}^s_{\mathbb{Q}}(X) \simeq \mathrm{End}^s(X) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Proposition 3.1.16. *Soit $\mathcal{L}_0$ une polarisation sur X, alors l'application*

$$\phi : NS_{\mathbb{Q}}(X) \longrightarrow \mathrm{End}^s_{\mathbb{Q}}(X), \quad \mathcal{L} \mapsto \phi_{\mathcal{L}_0}^{-1}\phi_{\mathcal{L}}$$

est un isomorphisme de $\mathbb{Q}$-espace vectoriel, qui se réduit en un isomorphisme de groupes entre $NS(X)$ et $\mathrm{End}^s(X)$ lorsque $\mathcal{L}_0$ est principale.

Démonstration. Aller à [3, Proposition 5.2.1.]. □

On dit d'une variété abélienne qu'elle est *simple* lorsqu'elle ne contient que 0 et X comme sous variétés abéliennes.
Et pour toute variété abélienne X le théorème de *Réductibilité Complète de Poincarré* donne l'existence d'une isogénie : $X \to X_1^{n_1} \times \cdots \times X_r^{n_r}$, avec X_i des variétés abéliennes simples non isogènes entre elles et déterminées (avec les exposants) à isogénie et permutation près [3]. Il en découle que pour une variété abélienne simple $(X, \mathcal{L})$ de dimension g, $\mathrm{End}_{\mathbb{Q}}(X)$ est un corps gauche de dimension finie sur $\mathbb{Q}$ muni de l'involution de Rosati $'$ par rapport à $\mathcal{L}$.

Proposition 3.1.17. *Soient K le centre de $\mathrm{End}_{\mathbb{Q}}(X)$ et K_0 le sous-corps de K invariant par l'involution $'$. On note*

$$[F : K] = d^2, \quad [K : \mathbb{Q}] = e, \quad [K_0 : \mathbb{Q}] = e_0, \quad et \quad rg(NS(X)) = \varrho.$$

Alors le tableau 3.1 suit .

Démonstration. Aller à [3, Proposition 5.5.7.]. □

Le couple $(\mathrm{End}_{\mathbb{Q}}, ')$ est dit du *premier type* si $K = K_0$, sinon il est dit du *second type*.

$\mathrm{End}_{\mathbb{Q}}(X)$	d	e_0	ϱ	$restriction$
Corps de nombre totalement réel	1	e	e	$e\|g$
Algèbre de quaternions totalement indéfinie	2	e	$3e$	$2e\|g$
Algèbre de quaternions totalement définie	2	e	e	$2e\|g$
$(\mathrm{End}_{\mathbb{Q}}{}')$ du second	d	$\frac{e}{2}$	e_0d^2	$e_0d^2\|g$

TABLE 3.1 – Tableau de l'anneau $\mathrm{End}_{\mathbb{Q}}(X)$ des variétés abéliennes simples [3, § 5.5]

3.2 VARIÉTÉS ABÉLIENNES PRINCIPALEMENT POLARISÉES

Dans cette section nous introduisons les fonctions thêtas, qui définissent un plongement projectif associé à un fibré très ample. Puis nous étudions les liens entre courbes hyperelliptiques de genre g et variétés abéliennes principalement polarisées.
Soit $(X, \mathcal{L})$ une abélienne polarisée de type D. Soit $\Lambda = \Lambda_1 \oplus \Lambda_2$ une décomposition symplectique du réseau de X, et $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$ celle de $K(\mathcal{L})$ associée. Alors il existe une base $(\theta_i)_{i\in K_2(\mathcal{L})}$ des fonctions thêta de $\mathcal{L}$. Et cela peut se ramener à l'étude des fonctions thêta pour le fibré symétrique $\mathcal{L}_0$ de caractéristique 0 induit par la décomposition symplectique de Λ (pour plus de détails se référer à [3, § 3.2] ou à [96, § 2.6]).
La forme hermitienne H étant symétrique sur V_2, on note par B l'extension bilinéaire $H_{|V_2}$ à $V \times V$. Alors on définit le *facteur d'automorphie classique* $a^c_{\mathcal{L}}$ par :

$$(\lambda, v) \mapsto \chi(\lambda)\exp[\pi(H-B)(v,\lambda) + \tfrac{\pi}{2}(H-B)(\lambda,\lambda)]$$

Ainsi une fonction f satisfaisant l'équation fonctionnelle : $f(z+\lambda) = a^c_{\mathcal{L}}(\lambda, v)f(z)$ avec le facteur d'automorphie classique $a^c_{\mathcal{L}}$, est appelée *fonction thêta classique* pour $\mathcal{L}$. Soit $\Lambda_1 = \Omega\mathbb{Z}^g$, $\Lambda_2 = \mathbb{Z}^g$ et $\Lambda = \Lambda_1 \oplus \Lambda_2$ telle que $\Omega D^{-1} \in \mathfrak{H}_g$. Alors la fonction thêta classique f vérifie les conditions :

$$f(z+m) = f(z)$$
$$f(z+\Omega m) = f(z)\exp\left[-\pi i\, {}^t m \cdot (D\Omega) \cdot m - 2\pi i\, {}^t z \cdot D \cdot m\right]$$

Cette fonction étant $\mathbb{Z}$-périodique, son dévéloppement de Fourier lui offre plus de flexibilité .
On appelle *fonctions thêta de niveau D*, les fonctions $\left(\theta\begin{bmatrix}0\\ b\end{bmatrix}(\cdot, \Omega D^{-1})\right)_{b\in D^{-1}\mathbb{Z}^g/\mathbb{Z}^g}$ et elles forment une base des fonctions thêta classiques [88, Page: 124].

3.2.1 *Fonctions Thêta Classiques*

Soit $(X_\Omega = \mathbb{C}^g/\Lambda, H)$ une variété abélienne principalement polarisée avec $\Omega \in \mathfrak{H}_g$ tel que $\Lambda = \Omega\mathbb{Z}^g \oplus \mathbb{Z}^g$. Soit $a, b \in \mathbb{Q}^g$, on appelle fonction thêta de caractéristique (a, b) la fonction sur $\mathbb{C}^g$ définie par :

$$\theta\begin{bmatrix}a\\ b\end{bmatrix}(z,\Omega) = \sum_{n\in\mathbb{Z}^g} \exp[i\pi\, {}^t(n+a)\Omega(n+a) + 2i\pi\, {}^t(n+a)(z+b)]$$

On notera $\theta = \theta\begin{bmatrix}0\\ 0\end{bmatrix}$. Les fonctions thêta classiques sont holomorphes et vérifient pour tout $m, n \in \mathbb{Z}^g$, l'équation :

$$\theta\begin{bmatrix}a\\ b\end{bmatrix}(z+\Omega m+n,\Omega) = \exp[2\pi i({}^t a.n - {}^t b.m) - \pi i({}^t m\Omega m + 2\, {}^t mz)]\theta\begin{bmatrix}a\\ b\end{bmatrix}(z,\Omega)$$

De plus on montre :

$$\theta[{}^{a}_{b}](z+\Omega m+n,\Omega)=\theta(z+\Omega a+b,\Omega)\cdot\exp\left[\pi i\,{}^{t}a\Omega a+2\pi i\,{}^{t}a(z+b)\right]$$

$$\theta[{}^{a+n}_{b+m}](z,\Omega)=\theta[{}^{a}_{b}](z,\Omega)\cdot\exp\left(2\pi i\,{}^{t}a.m\right)$$

Le groupe symplectique Γ_g agit sur les paramètres des fonctions thêta selon la proposition suivante :

Proposition 3.2.1. *(Équation Fonctionnelle). Soient $\gamma=\left(\begin{smallmatrix}A & B\\ C & D\end{smallmatrix}\right)\in\Gamma_g$, et e' (reps. e'') est le vecteur formé par les coefficients de la diagonale de $\frac{1}{2}\,{}^{t}AC$ (resp. $\frac{1}{2}\,{}^{t}DB$). Alors pour tous $a,b\in\mathbb{Q}^g$, $z\in\mathbb{C}^g$ et $\Omega\in\mathfrak{H}_g$, on a :*

$$\begin{aligned}\theta\left[{}^{a}_{b}\right](\gamma z,\gamma\Omega)=&\zeta_\gamma\sqrt{\det(C\Omega+D)}\exp\left(i\pi\,{}^{t}z(C\Omega+D)^{-1}Cz\right)\\&\cdot\theta\left[{}^{t}\gamma\left({}^{a}_{b}\right)+\left({}^{e'}_{e''}\right)\right](z,\Omega)\exp\left(-2i\pi\,{}^{t}({}^{t}Aa+{}^{t}Cb+e')e''\right)\\&\cdot\exp(-i\pi\,{}^{t}aA\,{}^{t}Ba)\exp(-i\pi\,{}^{t}bC\,{}^{t}Db)\exp(-2i\pi\,{}^{t}aB\,{}^{t}Cb)\quad,\end{aligned}$$

où ζ_γ est une racine huitième de l'unité qui ne depend que de γ.

Démonstration. Une démonstration se trouve dans [18, Propriété 3.1.24.] . □

Remarque 3.2.2. Pour ce qui va suivre, nous n'évaluerons que des quotients de puissances paires des fonctions thêta, alors nous n'aurons pas besoin de la racine huitième de l'unité et la racine carré (qui sont indépendantes de la caractéristique).

Proposition 3.2.3. *Soient $\Omega\in\mathfrak{H}_g$ et $X=\mathbb{C}^g/\Omega\mathbb{Z}^g\oplus\mathbb{Z}^g$ une variété abélienne principalement polarisée. Alors les ensembles de fonctions :*

- $\left(\theta[{}^{a}_{0}](nz,n\Omega)\right)_{a\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}$;
- $\left(\theta[{}^{0}_{b}](z,\Omega/n)\right)_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}$;
- *Si $n=k^2$,* $\left(\theta[{}^{a}_{b}](nz,\Omega)\right)_{a,b\in\frac{1}{k}\mathbb{Z}^g/\mathbb{Z}^g}$

forment une base de l'espace vectoriel R_n^Ω des fonctions thêta classiques de niveau n et $\dim R_n^\Omega=n^g$.

Démonstration. Aller à [88]. □

Soient $\mathcal{L}$ le fibré principal de caractéristique 0 associée Ω et $n\in\mathbb{N}$. On considère la base de fonctions thêta classiques de niveau n (associées à $\mathcal{L}$) donnée par :

$$\left(\theta[{}^{0}_{b}](z,\Omega/n)\right)_{b\in\frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}$$

On suppose que $3|n$. Soient la fonction $a_\Omega:\mathbb{R}^g\times\mathbb{R}^g\to\mathbb{C}^g$ définie par $(x,y)\mapsto\Omega x+y$ et la forme symplectique A canonique sur $\mathbb{R}^{2g}$ définie par $A(x,y)={}^{t}x_1y_2-{}^{t}y_1x_2$. On considère $L\subset\mathbb{Z}^{2g}$ un réseau d'indice s, et $L^\perp$ son orthogonal par rapport à la forme A. Soit $a_i,b_i\in L^\perp$ avec $1\leq i\leq s$ parcourant un système représentative de $L^\perp/\mathbb{Z}^{2g}$ on définit pour $m\in\mathbb{N}^*$, la fonction :

$$\begin{aligned}\phi_L:\mathbb{C}^g/a_\Omega(\frac{1}{m}L)&\longrightarrow\mathbb{P}^{s-1}_{\mathbb{C}}\\z&\longmapsto\left(\theta[{}^{a_i}_{b_i}](mz,\Omega)\right)_{a_i,b_i\in L^\perp/\mathbb{Z}^{2g}}\end{aligned}$$

Théorème 3.2.4. *(Lefschetz)*

— *ϕ_L est une application rationnelle de $X' = \mathbb{C}^g/a_\Omega(\frac{1}{m}L)$ dans l'espace projectif $\mathbb{P}^{s-1}_{\mathbb{C}}$.*

— *Si de plus $L \subseteq rL^\perp$ pour un certain $r \in \mathbb{N}$*

  — *$r = 2$ implique l'ensemble des points de X qui annulent toutes les fonctions thêta $\theta\left[\begin{smallmatrix}a_i\\ b_i\end{smallmatrix}\right](m\cdot, \Omega)$ est vide.*

  — *$r \geq 3$ implique ϕ_L est un plongement et son image est une sous-variété algébrique de $\mathbb{P}^{s-1}$.*

Démonstration. Aller à [88, Théorème 1.3]. □

Pour $m = 1$, $L = n\mathbb{Z}^g + \mathbb{Z}^g$, on a $a_{\Omega/n}(L) = \Omega\mathbb{Z}^g + \mathbb{Z}^g$. Lorsque $n \geq 3$ on retrouve le plongement défini par la base :

$$\left(\theta\left[\begin{smallmatrix}0\\ b\end{smallmatrix}\right](z, \Omega/n)\right)_{b \in \frac{1}{n}\mathbb{Z}^g/\mathbb{Z}^g}$$

Dans le cas où $n = 2$ et la variété X est simple, alors les fonctions thêta de niveau 2 ne permettent qu'un plongement projective de $(\mathbb{C}^g/\Lambda)/\pm 1$.

3.2.2 *Liens avec les Jacobiennes de Courbes: Application d'Abel-Jacobi*

Dans cette partie nous abordons une constructions de variétés abéliennes principalement polarisées à partir de courbes hyperelliptiques.
Nous commençons d'abord par quelques détailles sur une courbe hyperelliptique.

Définition 3.2.5. Une courbe lisse $\mathcal{C}/\Bbbk$ de genre $g \geq 1$ est appelée *courbe hyperelliptique* si son corps de fonction $\Bbbk(\mathcal{C})$ est une extension séparable de degré 2 du corps de fonction rationnel $\Bbbk(x)$ pour une fonction x, d'un point de vue géométrique cela signifie que $\mathcal{C}$ admet sur $\Bbbk$ un morphisme φ de degré 2 sur $\mathbb{P}^1$.

Si on pose $\Bbbk(\mathcal{C}) = \Bbbk(x, y)$ pour un entier $y \in \Bbbk(\mathcal{C})$ alors il existe des polynômes h et f dans $\Bbbk[x]$ tel que l'équation de la courbe $\mathcal{C}$ soit donnée par :

$$y^2 + h(x)y = f(x).$$

Où $2g + 1 \leq \deg f \leq 2g + 2$ et $\deg h \geq g + 1$ sans singularités. La preuve découle du théorème de Riemann-Roch.
Ainsi φ est définie par $\varphi(x, y) = x$ et l'involution hyperelliptique ι est définie par :

$$\iota : \mathcal{C} \to \mathcal{C}, \quad \iota(x, y) = (x, -y - h(x))$$

les points fixes de ι sont appeés les points de Weierstrass de $\mathcal{C}$ et ils correspondent exactement aux points de ramification de φ.
Pour $g > 1$ le corps de fonctions de $\Bbbk(\mathcal{C})$ est unique ; ainsi les courbes elliptiques se distinguent des autres courbes hyperelliptiques.

Remarque 3.2.6. — Quand $\deg f$ est impair on dit que la courbe a un modèle imaginaire (cela signifie qu'elle admet un unique point à l'infini) ; sinon on dit qu'elle a un modèle réel.

— Lorsque la caractéristique du corps $\mathbb{k}$, $char(\mathbb{k})$ est différente de 2, alors par le changement de variable $y \mapsto y - h(x)/2$, l'équation hyperelliptique se réduit à $\mathcal{C} : y^2 = f(x)$, où $f \in \mathbb{k}[x]$ est un polynôme séparable de degré $2g+1$ ou $2g+2$. Alors un changement de variable comme par exemple $(x, y) \mapsto \left(\frac{\alpha x}{x-\alpha}, \frac{y}{(x-\alpha)^3}\right)$ permet de passer du cas degré $2g+2$ au cas degré $2g+1$ en envoyant le point d'abscisse α à l'infini.

Une courbe hyperelliptique $\mathcal{C}$ sous la forme $y^2 = f(x)$ est lisse sur $\overline{\mathbb{k}}$ sauf en son point à l'infini $(0:1:0)$ pour les cas où $\deg f \geq 4$.
Pour la suite les courbes sous le model $y^2 = f(x)$ seront considerées désingularisées. Et lorsque nous disons que la courbe a deux points à l'infini, cela signifie que l'arbre de désingularisation de l'unique point à l'infini possède deux feuilles.
En général nous avons les résultas suivants concernant les courbes lisses.

Définition 3.2.7. Pour une courbe lisse $\mathcal{C}$ sur un corps parfait $\mathbb{k}$; on appelle diviseur de $\mathcal{C}$ tout élément de $\mathrm{Div}_{\overline{\mathbb{k}}}(\mathcal{C})$, le groupe libre engendré par les points de $\mathcal{C}(\overline{\mathbb{k}})$.

Le groupe de Galois $\mathrm{Gal}(\overline{\mathbb{k}}/\mathbb{k})$ agit sur $\mathrm{Div}_{\overline{\mathbb{k}}}(\mathcal{C})$ par :

$$\sigma\left(\sum_{P\in\mathcal{C}(\overline{\mathbb{k}})} n_P P\right) = \sum_{P\in\mathcal{C}(\overline{\mathbb{k}})} n_P \sigma(P) \quad pour \quad \sigma \in \mathrm{Gal}(\overline{\mathbb{k}}/\mathbb{k}).$$

Et les éléments stables sous cette action sont appelés diviseurs sur $\mathbb{k}$, on note par $\mathrm{Div}_{\mathbb{k}}(\mathcal{C})$ l'ensemble des diviseurs sur $\mathbb{k}$. Par exemple toute fonction rationnelle définie un diviseur noté $div(f)$ par : $div(f) = \sum_{P\in\mathcal{C}(\overline{\mathbb{k}})} ord_P(f)P$ on l'appelle *diviseur principal* de $\mathcal{C}$.
On définit le morphisme de groupe appelé *degré* noté deg de $\mathrm{Div}_{\mathbb{k}}(\mathcal{C})$ dans $\mathbb{Z}$ par : $\sum_{P\in\mathcal{C}(\overline{\mathbb{k}})} n_P P \mapsto \sum_{P\in\mathcal{C}(\overline{\mathbb{k}})} n_P$. Et son noyau noté $\mathrm{Div}^0_{\mathbb{k}}(\mathcal{C})$ contient $\mathrm{PDiv}_{\mathbb{k}}(\mathcal{C})$ le groupe des diviseurs principaux de $\mathcal{C}$ car une fonction rationnelle possède le même nombre fini de zéros que de pôles.
Alors on appelle *groupe de Picard de degré zéro*, le groupe quotient

$$\mathrm{Pic}^0_{\mathbb{k}}(\mathcal{C}) = \mathrm{Div}^0_{\mathbb{k}}(\mathcal{C}) / \mathrm{PDiv}_{\mathbb{k}}(\mathcal{C})$$

Pour des raisons que nous allions voir par la suite, l'on préfère $\mathrm{Pic}^0_{\overline{\mathbb{k}}}(\mathcal{C})$ à $\mathrm{Pic}^0_{\mathbb{k}}(\mathcal{C})$. Et plus généralement lorsque la courbe possède un point rationnel alors :

$$\mathrm{Pic}^0_{\overline{\mathbb{k}}}(\mathcal{C})^{\mathrm{Gal}(\overline{\mathbb{k}}/\mathbb{k})} = \mathrm{Pic}^0_{\mathbb{k}}(\mathcal{C})$$

Soit $\mathcal{C}$ une courbe hyperelliptique de genre g sur $\mathbb{C}$, alors il existe $a_i \in \mathbb{C}$ avec $i \in \{1, \cdots, 2g+1\}$ tous distincts telle que l'équation de $\mathcal{C}$ se réduise à :

$$y^2 = \prod_{i=1}^{2g+1} (x - a_i) \quad et \quad a_{2g+2} = \infty \in \mathbb{P}^1(\mathbb{C})$$

La courbe $\mathcal{C}$ étant une surface de Riemann compacte, on peut construire le premier groupe d'homologie $H_1(\mathcal{C}, \mathbb{Z})$ de $\mathcal{C}$ en traçant des chemins disjoints γ_n de $\mathbb{P}^1(\mathbb{C})$ d'origine a_{2n-1} et d'extrémité a_{2n} comme l'indiquent la figure ci-dessous : Où $A_1, \cdot, A_g, B_1, \cdots, B_g$ est une base de $H_1(\mathcal{C}, \mathbb{Z})$. Pour plus de détailles sur la construction voir [18].
L'espace vectoriel $\mathcal{C}^1$ des 1-formes différentielles est donné par :

$$\mathcal{C}^1 = \left\{ \frac{P(x)dx}{y},\ P \in \mathbb{C}[X]\, et\, \deg P \leq (g-1) \right\}$$

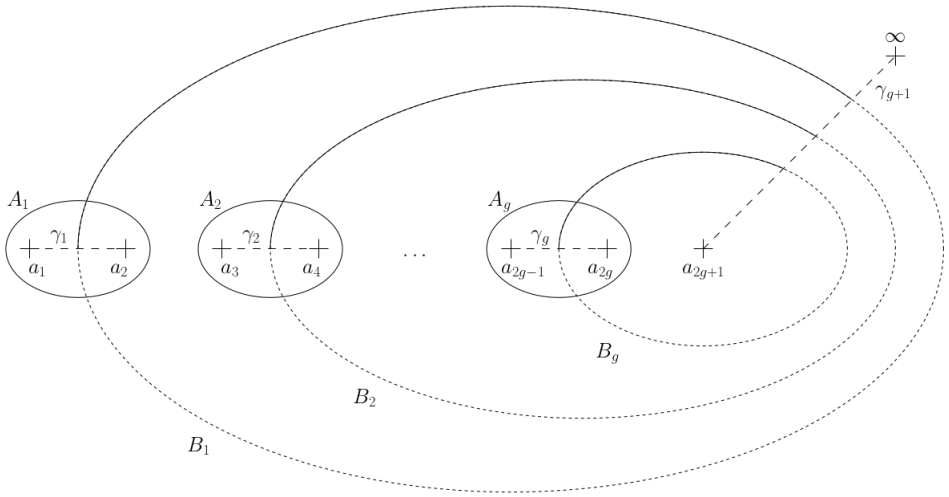


FIGURE 3.3 – Projection des lacets sur $\mathbb{P}^1(\mathbb{C})$.

On note par $(\omega_i)_{1\leq i\leq g}$ une base normalisée de $\mathcal{C}^1$, alors on a :

$$\int_{A_i} \omega_j = \delta_{i,j}.$$

Ainsi la matrice de périodes associée à une courbe hyperelliptique $\mathcal{C}$ est définie par (Ω, Id) telle que :

$$\Omega_{ij} = \int_{B_i} \omega_j$$

On montre que la matrice Ω appartienne à $\mathfrak{H}_g$ le demi-espace de Siegel [88, cor.2.2].
De plus si on note par ω le g-uplet $(\omega_i)_{1\leq i\leq g}$, alors la correspondance $\varpi : P \mapsto \int_{P_\infty}^{P} \omega \mod \Lambda_\Omega$ définit une application de $\mathcal{C} \to \mathbb{C}^g/\Lambda_\Omega$ ne dependant pas du chemin de P_∞ à P sur $\mathcal{C}$. L'application ϖ peut s'étendre à $\mathrm{Div}\,\mathcal{C}$ par linéarité sur les diviseurs:

$$\varpi\left(\sum_{P\in\mathcal{C}} n_P P\right) = \left(\sum_{P\in\mathcal{C}} n_P \varpi(P)\right) \mod \Lambda_\Omega$$

Théorème 3.2.8. *(Abel-Jacobi). L'application ϖ d'Abel-Jacobi est un isomorphisme entre la jacobienne algébrique $Jac(\mathcal{C})$ et la jacobienne analytique $\mathbb{C}^g/\Lambda_\Omega$.*

Démonstration. Aller à [3, Théorème 11.1.3]. □

Ce qui montre que $\mathrm{Pic}_0(\mathcal{C})$ admet une structure de variété abélienne principalement polarisée. La réciproque n'est pas vrai en général. En effet Schottky a montré qu'en dimension 4, il existe des variétés abéliennes non Jacobienne de courbes [103]. Cependant nous avons le théorème suivant :

Théorème 3.2.9. *Une variété abélienne principalement polarisée et simple de dimension $g \leq 3$ est la Jacobienne d'une courbe lisse de genre g.*

D'autre part toute courbe lisse de genre $g \leq 2$ est hyperelliptique.

Démonstration. Aller à [3, Corollaire 11.8.2]. □

3.3 SURFACES ABÉLIENNES PRINCIPALEMENT POLARISÉES

Nous consacrons cette partie aux résultats liés à l'espace modulaire des surfaces abéliennes principalement polarisées. Comme pour les courbes elliptiques dans le Chapitre 2 nous voulons travailler génériquement sur l'espace modulaire. Nous avons vu que ces surfaces sont isomorphes aux Jacobiennes de courbes hyperelliptiques de genre 2 et qu'elles sont représentées par des matrices des périodes dans $\mathfrak{H}_2$.

3.3.1 *Espace Modulaire de Siegel*

Nous commençons par une description du domaine fondamental dans $\mathfrak{H}_2$ sous l'action espace modulaire de Seigel Γ_2.
En général pour tout entier $g \geq 2$ le groupe symplectique noté Γ_g désigne

$$Sp_{2g}(\mathbb{Z}) = \{\gamma \in M_{2g}(\mathbb{Z}) : \gamma \mathcal{I}_g {}^t\gamma = \mathcal{I}_g\} \quad avec \quad \mathcal{I}_g = \begin{pmatrix} 0 & \mathrm{Id}_g \\ -\mathrm{Id}_g & 0 \end{pmatrix}$$

Une matrice $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ appartient à Γ_g si et seulement si :

$$ {}^tAC = {}^tCA \quad {}^tBD = {}^tDB \quad {}^tDA - {}^tBC = \mathrm{Id}_g\,.$$

ou encore si et seulement si

$$A\,{}^tB = B\,{}^tA \quad D\,{}^tC = C\,{}^tB \quad A\,{}^tD - B\,{}^tC = \mathrm{Id}_g\,.$$

Le groupe Γ_g est engendré par la matrice $\mathcal{I}_g$ et les $\dfrac{g(g+1)}{2}$ matrices de la forme :

$$\mathfrak{M}_{i,j} = \begin{pmatrix} \mathrm{Id}_g & \mathfrak{m}_{i,j} \\ 0 & -\mathrm{Id}_g \end{pmatrix},$$

où $\mathfrak{m}_{i,j}$ désigne la matrice de $M_g(\mathbb{Z})$ dont tous les coefficients sont nuls sauf les coefficients (i,j) et (j,i) qui valent 1 [61].
Nous allons alors noter par : $\mathfrak{M}_1 = \mathfrak{M}_{1,1}$, $\mathfrak{M}_1 = \mathfrak{M}_{1,2}$ et $\mathfrak{M}_3 = \mathfrak{M}_{2,2}$ les générateurs de Γ_2.
On définit quelques sous groupes de Γ_g dont on utilisera pour simplifier l'action de Γ_2 sur $\mathfrak{H}_2$.

$$\Gamma_g(N) := \left\{\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_g : A \equiv D \equiv \mathrm{Id}_g \mod N \, et \, B \equiv C \equiv 0 \mod N\right\},$$

$$\Gamma_g(N, 2N) := \left\{\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_g(N) : {}^t(AC)_0 \equiv {}^t(DB)_0 \equiv 0 \mod 2N\right\},$$

$$\Gamma_{g,0}(N) := \left\{\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_g : C \equiv 0 \mod N\right\},$$

$$et \quad \Gamma_g^0(N) := \left\{\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_g : B \equiv 0 \mod N\right\}.$$

3.3.1.1 *Domaine Fondamental*

Nous avons vu que Γ_g agit sur $\mathfrak{H}_g$ par :

$$\gamma\Omega = (A\Omega + B)(C\Omega + D)^{-1} \quad for \quad \gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_g$$

Définition 3.3.1. Nous dirons qu'une matrice rélle symétrique M est *réduite au sens de Minkowski* si pour tout vecteur $n = (n_1, \cdots, n_g) \in \mathbb{Z}^g$ avec $\text{pgcd}(n_1, \cdots, n) = 1$, ${}^t n M {}^t n \geq M_{ii}\, \forall i \in \{1, \cdots, g\}$ et $M_{i,i+1} \geq 0\, \forall i \in \{1, \cdots, g-1\}$

Alors il existe un domaine fondamental de l'action de $\Gamma_g/(\pm \text{Id}_{2g})$ sur $\mathfrak{H}_g$ noté $\mathcal{F}_g$ et dont les éléments Ω sont définis par les trois propriétés suivantes:

— $|\text{Re}\,\Omega_{ij}| \leq \frac{1}{2}$ pour tous $i, j \in \{1, \cdots, g\}$;

— la matrice $\text{Im}(\Omega)$ est réduite au sens de Minkowski;

— pour tout $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_g$, $|\det(C\Omega + D)| \geq 1$.

Ainsi pour tout $\Omega \in \mathcal{H}_g$, il existe $\gamma \in \Gamma_g/(\pm \text{Id}_{2g})$ tel que $\gamma\Omega \in \mathcal{F}_g$, de plus γ est unique si $\gamma\Omega$ est un point intérieur de $\mathfrak{H}_g$ [61].
D'autre part pour $g = 2$ il existe 19 matrices $\mathfrak{N}_i$, $i \in \{1, \cdots, 19\}$ de Γ_g qu'il suffit d'utiliser pour le test de la troisième propriété de caractérisation du domaine fondamental [42].

$$\mathfrak{N}_1 = \left(\begin{smallmatrix} 0 & -\text{Id}_2 \\ \text{Id} & 0 \end{smallmatrix}\right), \mathfrak{N}_2 = \left(\begin{smallmatrix} 0 & -\text{Id}_2 \\ \text{Id}_2 & \mathfrak{m}_{1,1} \end{smallmatrix}\right), \mathfrak{N}_3 = \left(\begin{smallmatrix} 0 & -\text{Id}_2 \\ \text{Id}_2 & -\mathfrak{m}_{1,1} \end{smallmatrix}\right),$$

$$\mathfrak{N}_4 = \left(\begin{smallmatrix} 0 & -\text{Id}_2 \\ \text{Id}_2 & \mathfrak{m}_{2,2} \end{smallmatrix}\right), \mathfrak{N}_5 = \left(\begin{smallmatrix} 0 & -\text{Id}_2 \\ \text{Id} & -\mathfrak{m}_{2,2} \end{smallmatrix}\right), \mathfrak{N}_6 = \left(\begin{smallmatrix} 0 & -\text{Id}_2 \\ \text{Id}_2 & \text{Id}_2 \end{smallmatrix}\right),$$

$$\mathfrak{N}_7 = \left(\begin{smallmatrix} 0 & -\text{Id}_2 \\ \text{Id}_2 & -\text{Id}_2 \end{smallmatrix}\right), \mathfrak{N}_8 = \left(\begin{smallmatrix} 0 & -\text{Id}_2 \\ \text{Id}_2 & \mathfrak{m}_{2,2}-\mathfrak{m}_{1,1} \end{smallmatrix}\right), \mathfrak{N}_9 = \left(\begin{smallmatrix} 0 & -\text{Id}_2 \\ \text{Id} & \mathfrak{m}_{1,1}-2,2 \end{smallmatrix}\right),$$

$$\mathfrak{N}_{10} = \left(\begin{smallmatrix} 0 & -\text{Id}_2 \\ \text{Id}_2 & \mathfrak{m}_{1,2} \end{smallmatrix}\right), \mathfrak{N}_{11} = \left(\begin{smallmatrix} 0 & -\text{Id}_2 \\ \text{Id}_2 & -\mathfrak{m}_{1,2} \end{smallmatrix}\right), \mathfrak{N}_{12} = \left(\begin{smallmatrix} 0 & -\text{Id}_2 \\ \text{Id}_2 & \mathfrak{m}_{1,1}+\mathfrak{m}_{1,2} \end{smallmatrix}\right),$$

$$\mathfrak{N}_{13} = \left(\begin{smallmatrix} 0 & -\text{Id}_2 \\ \text{Id} & -\mathfrak{m}_{1,1}-\mathfrak{m}_{1,2} \end{smallmatrix}\right), \mathfrak{N}_{14} = \left(\begin{smallmatrix} 0 & -\text{Id}_2 \\ \text{Id}_2 & \mathfrak{m}_{1,2}+\mathfrak{m}_{2,2} \end{smallmatrix}\right), \mathfrak{N}_{15} = \left(\begin{smallmatrix} 0 & -\text{Id}_2 \\ \text{Id}_2 & -\mathfrak{m}_{1,2}-\mathfrak{m}_{2,2} \end{smallmatrix}\right),$$

$$\mathfrak{N}_{16} = \left(\begin{smallmatrix} \text{Id}_2 & -\text{Id}_2 \\ \mathfrak{m}_{1,1} & \mathfrak{m}_{2,2} \end{smallmatrix}\right), \mathfrak{N}_{17} = \left(\begin{smallmatrix} \text{Id}_2 & -\text{Id}_2 \\ \mathfrak{m}_{2,2} & \mathfrak{m}_{1,1} \end{smallmatrix}\right), \mathfrak{N}_{18} = \left(\begin{smallmatrix} \text{Id}_2 & 0 \\ \text{Id}_2 & -\mathfrak{m}_{1,2} \end{smallmatrix}\right) \text{Id}_2,$$

$$\mathfrak{N}_{19} = \left(\begin{smallmatrix} -\text{Id}_2 & 0 \\ \text{Id}_2 & -\mathfrak{m}_{1,2} \end{smallmatrix}\right) -\mathfrak{m}_{1,1}-\mathfrak{m}_{1,2}.$$

Il en découle un algorithme 4 permettant de réduire au sens de Minkowski une matrice symétrique réelle et un autre algorithme 5 permettant de réduire une matrice de $\mathfrak{H}_2$ sur $\mathcal{F}_2$. D'autre part on montre que pour tout $\Omega = \left(\begin{smallmatrix} \Omega_1 & \Omega_2 \\ \Omega_2 & \Omega_3 \end{smallmatrix}\right) \in \mathcal{F}_2 : \text{Im}(\Omega_1) \geq \frac{\sqrt{3}}{2}$ et toutes les valeurs propres de $\text{Im}\,\Omega$ sont supérieures ou égales $\frac{\sqrt{3}}{2}$.

Entrée: $\gamma = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ réelle définie positive.
Sortie: U entière et unimodulaire telle que $U\gamma\,{}^tU$ est réduite au sens de Minkowski.

1. $U = \mathrm{Id}_2$, $V = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ et $W = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$;
2. **si** $2|c| \leq |a|$ **alors**
   a. **si** $|a| \leq |b|$ **alors**
      i. **si** $|c| \leq 0$ **alors** $\gamma = V\gamma V$ et $U = VU$;
      ii. **sinon retourner** U ;
   b. **sinon si** $|c| \leq 0$ **alors** $\gamma = W\gamma W$ et $U = WU$;
3. $q = \lfloor c/a \rceil$;
4. $\gamma = \left(\begin{smallmatrix} 1 & 0 \\ -q & 1 \end{smallmatrix}\right) \gamma \left(\begin{smallmatrix} 1 & -q \\ 0 & 1 \end{smallmatrix}\right)$;
5. $U = \left(\begin{smallmatrix} 1 & 0 \\ -q & 1 \end{smallmatrix}\right) U$;
6. **retourner à étape** 2.

Algorithm 4 – Réduction de Minkowski

Entrée: $\Omega \in \mathfrak{H}_2$;
Sortie: Un couple $(\gamma, \Omega') \in \Gamma_2 \times \mathcal{F}_2$ tel que $\Omega' = \gamma\Omega$.

1. $\gamma = I_4$; $\Omega' = \Omega$;
2. $U = \mathrm{Minkowski}(\mathrm{Im}(\Omega'))$;
3. $\gamma = \left(\begin{smallmatrix} U & 0 \\ 0 & {}^tU^{-1} \end{smallmatrix}\right) \gamma$;
4. $\Omega' = U\Omega'\,{}^tU$;
5. **pour** $j = 1$ **à** 3 **faire** :
   a. $a = -\lfloor \mathrm{Re}\,\Omega'_j \rceil$;
   b. $\Omega' = M_j^a \Omega'$;
   c. $\gamma = M_j^a \gamma$;
6. **retourner** (γ, Ω') ;
7. **pour** $j = 1$ à 19 **faire** :
   a. **si** $|\det(C_j\Omega' + D_j)| < 1$ **alors** :
      i. $i = 1$;
      ii. $\Omega' = \mathfrak{N}_j\Omega'$;
      iii. $\gamma = \mathfrak{N}_j\gamma$;
8. **retourner à l'étape** 2 ;

Algorithm 5 – Réduction sur $\mathcal{F}_2$

3.3.1.2 *Formes et Fonctions Modulaires*

On appelle *thêta constante*, la fonction sur $\mathfrak{H}_g$ correspondant à l'evaluation d'une fonction thêta en $z = 0$. Pour ce qui va suivre nous allons utiliser les thêta constantes en caractéristique $1/2$ c'est à dire que nous prenons $\theta_{a,b}(\Omega) := \theta \begin{bmatrix} a/2 \\ b/2 \end{bmatrix} (0, \Omega)$ pour $a, b \in \{0,1\}^g$.

Proposition 3.3.2. *(Formules de duplication). Pour tous $a, b \in \{0,1\}^g$ et $\Omega \in \mathfrak{H}_g$:*

$$\theta_{a,b}(2\Omega) = \frac{1}{2^g} \sum_{b_1+b_2 \equiv b \mod 2} (-1)^{{}^t a b_1} \theta_{0,b_1}(\Omega)\theta_{0,b_2}(\Omega)$$

$$\theta_{a,b}\left(\frac{\Omega}{2}\right) = \frac{1}{2^g} \sum_{a_1+a_2 \equiv a \mod 2} (-1)^{{}^t a_1 b} \theta_{a_1,0}(\Omega)\theta_{a_2,0}(\Omega)$$

Démonstration. Aller à [28]. □

D'autre part nous avons que :

$$\theta \begin{bmatrix} a+n \\ b+m \end{bmatrix} (z, \Omega) = \exp(2i\pi\, {}^t a m)\theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \Omega) \quad et \quad \theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \Omega) = \theta \begin{bmatrix} -a \\ -b \end{bmatrix} (z, \Omega)$$

ce qui implique: $\theta_{a,b}(\Omega) = \exp(2i\pi\, {}^t ab)\theta_{a,b}(\Omega)$.
Nous dirons que la thêta constante $\theta_{a,b}(\Omega)$ est *paire*, lorsque ${}^t ab \equiv 0 \mod 2$, sinon nous dirons que la thêta constante est *impaire*. Et on remarque que dans le cas impaire, la fonction thêta est nécéssairement nulle. On montre que sur les 4^g thêta constantes : $2^{g-1}(2^g + 1)$ sont paires et $2^{g-1}(2^g - 1)$ sont impaires.

Définition 3.3.3. Soit Γ un sous-groupe d'indice fini de Γ_g (avec $g > 1$), une *forme modulaire de poids k* pour Γ est une fonction holomorphe f définie sur $\mathfrak{H}_g$ telle que $f(\gamma\Omega) = \det(C\Omega + D)^k f(\Omega)$ pour tous $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma$ et $\Omega \in \mathfrak{H}_g$.

Pour $g = 1$ on ajoute la condition "*d'holomorphie aux pointes*" dont la condition correspondante est vérifiée lorsque $g > 1$ d'après le principe de Koecher [61, § 4].

Exemple 3.3.4. Pour N pair et $a_1, a_2, b_1, b_2 \in \frac{1}{N}\mathbb{Z}^g$, les fonctions sur $\mathfrak{H}_g$ définies par:

$$\theta \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} (0, \Omega)\theta \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} (0, \Omega)$$

sont modulaires de poids 1 pour $\Gamma_g\left(N^2, 2N^2\right)$.

Définition 3.3.5. Soit Γ un sous-groupe d'indice fini de Γ_g, on appelle fonction Γ-modulaire sur $\mathfrak{H}_g$, toute fonction définie par le quotient de deux formes Γ-modulaires de même poids.

Exemple 3.3.6. Pour tous $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_g(2,4)$, et $a, b \in \{0,1\}^g$ et $\Omega \in \mathfrak{H}_g$ on montre que :

$$\theta^2_{a,b}(\gamma\Omega) = \zeta^2_\gamma \det(C\Omega + D)\theta^2_{a,b}(\Omega).$$

Alors les quotients des carrés des $\theta_{a,b}$ pairs sont des fonctions modulaires pour $\Gamma_g(2,4)$.

3.3.1.3 *Invariants Modulaires pour* Γ_2

Nous introduisons dans cette partie, les invariants modulaires qui sont l'analogue du j-invariant en dimension 1 et le corps des fonctions modulaires. Afin de simplifier les notations, nous utiliserons les numérotations de R.Dupont [28] sur les thêta constantes en genre 2 de 0 à 15. Pour tous $a = \binom{a_0}{a_1}$, $b = \binom{b_0}{b_1} \in \{0, 1\}^2$ on pose :

$$\theta_{b_0+2b_1+4a_0+8a_1}(\Omega) := \theta_{a,b}(\Omega)$$

Ils sont au nombre de 16, dont 6 identiquement nulles (car impaires) et les 10 autres sont les θ_i avec $i \in \mathcal{P}_2 = \{0, 1, 2, 3, 4, 6, 8, 9, 12, 15\}$.
Alors la proposition suivante établit des rélations polynomiales entre les six derniers thêta constantes et les quatres premiers.

Proposition 3.3.7. *Pour tout* $\Omega \in \mathfrak{H}_2$, *si l'on pose* $(a, b, c, d) = \left(\theta_j^2(\Omega)_{j\in\{0,1,2,3\}}\right)$, *alors :*

$$\begin{aligned}
&(x - \theta_4^4(\Omega))(x - \theta_6^4(\Omega)) = x^2 + (b^2 + d^2 - a^2 - c^2)x + (ac - bd)^2,\\
&(x - \theta_8^4(\Omega))(x - \theta_9^4(\Omega)) = x^2 + (c^2 + d^2 - a^2 - b^2)x + (ab - cd)^2,\\
\textit{et}\quad &(x - \theta_{12}^4(\Omega))(x - \theta_{15}^4(\Omega)) = x^2 + (b^2 + c^2 - a^2 - d^2)x + (ad - bc)^2.
\end{aligned}$$

Démonstration. Aller à [28]. □

On considère les applications h_j avec $j \in \{4, 6, 10, 12, 16\}$ de vers $\mathbb{C}$ définies :

$$h_4 = \sum_{i\in\mathcal{P}} \theta_i^8, \quad h_6 = \sum_{60\,tuples\,(i,j,k)\in\mathcal{P}^3} (\theta_i\theta_j\theta_k)^4, \qquad h_{10} = \prod_{i\in\mathcal{P}} \theta_i^2,$$

$$\begin{aligned}
h_{12} =&(\theta_0\theta_1\theta_2\theta_4\theta_8\theta_{15})^4 + (\theta_0\theta_1\theta_2\theta_6\theta_9\theta_{12})^4 + (\theta_0\theta_1\theta_3\theta_4\theta_9\theta_{15})^4\\
&+ (\theta_0\theta_1\theta_3\theta_6\theta_8\theta_{12})^4 + (\theta_0\theta_1\theta_4\theta_6\theta_{12}\theta_{15})^4 + (\theta_0\theta_2\theta_3\theta_4\theta_9\theta_{12})^4\\
&+ (\theta_0\theta_2\theta_3\theta_6\theta_8\theta_{15})^4 + (\theta_0\theta_2\theta_8\theta_9\theta_{12}\theta_{15})^4 + (\theta_0\theta_3\theta_4\theta_6\theta_8\theta_9)^4\\
&+ (\theta_1\theta_2\theta_3\theta_4\theta_8\theta_{12})^4 + (\theta_1\theta_2\theta_3\theta_6\theta_9\theta_15)^4 + (\theta_1\theta_2\theta_4\theta_6\theta_8\theta_9)^4\\
&+ (\theta_1\theta_3\theta_8\theta_9\theta_{12}\theta_{15})^4 + (\theta_2\theta_3\theta_4\theta_6\theta_{12}\theta_{15})^4 + (\theta_4\theta_6\theta_8\theta_9\theta_{12}\theta_{15})^4 \quad ,
\end{aligned}$$

$$\begin{aligned}
h_{16} =& \left(\theta_3^8 + \theta_6^8 + \theta_9^8 + \theta_{12}^8\right)(\theta_0\theta_1\theta_2\theta_4\theta_8\theta_{15})^4 + \left(\theta_3^8 + \theta_4^8 + \theta_8^8 + \theta_{15}^8\right)(\theta_0\theta_1\theta_2\theta_6\theta_9\theta_{12})^4\\
&+ \left(\theta_2^8 + \theta_6^8 + \theta_8^8 + \theta_{12}^8\right)(\theta_0\theta_1\theta_3\theta_4\theta_9\theta_{15})^4 + \left(\theta_2^8 + \theta_4^8 + \theta_9^8 + \theta_{15}^8\right)(\theta_0\theta_1\theta_3\theta_6\theta_8\theta_{12})^4\\
&+ \left(\theta_2^8 + \theta_3^8 + \theta_8^8 + \theta_9^8\right)(\theta_0\theta_1\theta_4\theta_6\theta_{12}\theta_{15})^4 + \left(\theta_1^8 + \theta_6^8 + \theta_8^8 + \theta_{15}^8\right)(\theta_0\theta_2\theta_3\theta_4\theta_9\theta_{12})^4\\
&+ \left(\theta_1^8 + \theta_4^8 + \theta_9^8 + \theta_{12}^8\right)(\theta_0\theta_2\theta_3\theta_6\theta_8\theta_{15})^4 + \left(\theta_1^8 + \theta_3^8 + \theta_4^8 + \theta_6^8\right)(\theta_0\theta_2\theta_8\theta_9\theta_{12}\theta_{15})^4\\
&+ \left(\theta_1^8 + \theta_2^8 + \theta_{12}^8 + \theta_{15}^8\right)(\theta_0\theta_3\theta_4\theta_6\theta_8\theta_9)^4 + \left(\theta_0^8 + \theta_6^8 + \theta_9^8 + \theta_{15}^8\right)(\theta_1\theta_2\theta_3\theta_4\theta_8\theta_{12})^4\\
&+ \left(\theta_0^8 + \theta_4^8 + \theta_8^8 + \theta_{12}^8\right)(\theta_1\theta_2\theta_3\theta_6\theta_9\theta_{15})^4 + \left(\theta_0^8 + \theta_3^8 + \theta_{12}^8 + \theta_{15}^8\right)(\theta_1\theta_2\theta_4\theta_6\theta_8\theta_9)^4\\
&+ \left(\theta_0^8 + \theta_2^8 + \theta_4^8 + \theta_6^8\right)(\theta_1\theta_3\theta_8\theta_9\theta_{12}\theta_{15})^4 + \left(\theta_0^8 + \theta_1^8 + \theta_8^8 + \theta_9^8\right)(\theta_2\theta_3\theta_4\theta_6\theta_{12}\theta_{15})^4\\
&+ \left(\theta_0^8 + \theta_1^8 + \theta_2^8 + \theta_3^8\right)(\theta_4\theta_6\theta_8\theta_9\theta_{12}\theta_{15})^4.
\end{aligned}$$

$$\text{Et on a la relation:} \quad 3h_{16} = h_{12}h_4 - 2h_6h_{10}$$

On montre que des formules de transformation des thêta constantes sous l'action de Γ_2 peuvent se réduire à :

$$\theta_j^2(\gamma\Omega) = i^{\kappa(\gamma)+\nu(\gamma,j)} \det(C\Omega + D)\theta^2_{\xi(\gamma,j)}(\Omega), \quad \forall\Omega \in \mathfrak{H}_2 \quad et \quad j \in [0, 15].$$

tel que $\kappa(\gamma) \in [0,3]$, $\nu(\gamma,\cdot) : [0,15] \to [0,3]$ et $\xi(\gamma,\cdot)$ une permutation de $[0,15]$ existent pour tout $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_2$.
Ainsi des calculs explicites dans [28] montrent que pour $j \in \{4,12,10,16\}$, h_j est invariante sous l'action de $\mathfrak{M}_1$, $\mathfrak{M}_2$, et $\mathfrak{M}_3$ et pour tout $\Omega \in \mathfrak{H}_2$:

$$h_j(\mathrm{Id}_4\,\Omega) = \det(\Omega)^j h_j(\Omega)$$

Alors les h_j avec $j \in \{4,12,10,16\}$ sont des formes modulaires de Siegel de poids j pour $\Gamma_2 = \langle \mathrm{Id}_4, \mathfrak{M}_1, \mathfrak{M}_2, \mathfrak{M}_3 \rangle$.

Définition 3.3.8. On appelle *invariants d'Igusa ou encore j-invariants en dimension* 2, les fonctions modulaires j_1, j_2 et j_3 pour Γ_2 définies par :

$$j_1 = \frac{h_{12}^5}{h_{10}^6}, \quad j_2 = \frac{h_4 h_{12}^3}{h_{10}^4}, \quad j_3 = \frac{h_{16} h_{12}^2}{h_{10}^4}$$

Ces fonctions ont été introduites par J.Igusa [53] . D'autre part, on appelle série d'Eisentein de poids $k \geq 4$, la série ψ_k donnée par:

$$\psi_k(\Omega) = \sum_{\gamma \in \Gamma_2} \det(C\Omega + D)^{-k}$$

et on définit par suite, les *formes modulaires paraboliques* χ_{10}, χ_{12}, avec des expréssions en fonction des ψ_k avec $k \in \{4,6,10,12\}$.

$$\chi_{10} = -2^{-12}3^{-5}5^{-2}7^{-1}153^{-1}43867(\psi_4\psi_6 - \psi_{10})$$

$$\chi_{12} = 2^{-13}3^{-7}5^{-3}7^{-2}337^{-1}131 \cdot 593(3^2 7^2 \psi_4^3 + 2 \cdot 5^3 \psi_6^2 - 691\psi_{12})$$

c'est-à-dire que ces formes modulaires peuvent s'exprimer sous la forme d'une série de Fourier: $\sum_{t>0} a(t) \exp(2i\pi \operatorname{Tr} t\Omega)$ où t parcourt l'ensemble des matrices semi-entières positives. De plus, nous avons:

$$h_4 = 2^2\psi_4, \quad h_6 = 2^2\psi_6, \quad h_{10} = -2^{14}\chi_{10} \quad \text{and} \quad h_{12} = 2^{17}3\chi_{12}.$$

Sur $\mathbb{C}$ et en dimension 2, l'anneau gradué des formes modulaires de Siegel de poids paires est engendré par les quatre formes modulaires ψ_4 ,ψ_6 , χ_{10} , χ_{12} [52].

Par suite nous pouvons introduire les fonctions modulaires très pratiques (appelées souvent aussi *j-invariants*) que l'on doit à Streng [113, Chapter 2, § 2.1] par:

$$\mathfrak{j}_1 = -2^{-10}\frac{\psi_4\psi_6}{\chi_{10}}, \quad \mathfrak{j}_2 = 2^{-7}\cdot 3\frac{\psi_4^2\chi_{12}}{\chi_{10}^2}, \quad \mathfrak{j}_3 = 2^{-18}\frac{\psi_4}{\chi_{10}^2}.$$

Ces invariants sont birationnellement équivalents au j-invariants (j_1, j_2, j_3) d'Igusa [53] avec certains avantages algorithmiques de fournir des dénominateurs de tailles plus petites (par exemples pour les polynômes de classses). De plus nous allons remarquer dans le chapitre 4 et la section 4.6 que ces invariants ont des rélations très simples et très "appréciées" avec des invariants absolus (j_1, j_2, j_3) abordés dans le chapitre 4 et la section 4.3.

Nous pouvons ainsi énoncer le résultat fondamental suivant: *deux surfaces abéliennes principalement polarisées sont isomorphes si et seulement si leurs représentants sur $\mathcal{F}_2$ prennent les mêmes valeurs pour le triplet $(\mathfrak{j}_1, \mathfrak{j}_2, \mathfrak{j}_3)$ ou de manière équivalente pour le triplet (j_1, j_2, j_3)* (aller à [28, 53] pour plus détails sur la démonstration). Et il s'en suit le résultat suivant :

Théorème 3.3.9. *Le corps des fonctions modulaires de Siegel en dimension 2 est* $\mathbb{C}(j_1, j_2, j_3) = \mathbb{C}(j_1, j_2, j_3)$*, on le note* $\mathbb{C}_{\Gamma_2}$.

Démonstration. Aller à [52]. □

Généralement, de manière générique, les valeurs (j_1, j_2, j_3) (ou (j_1, j_2, j_3)) sur un corps $\mathbb{k}$ (pour $\mathrm{char}(\mathbb{k}) \neq 2$) spécifient de manière unique une classe d'isomorphisme de surfaces abéliennes principalement polarisée sur $\mathbb{k}$. Cette correspondance échoue cependant en les points singuliers et aux pôles de l'application rationnelle $\mathfrak{A}_2 \longrightarrow \mathbb{A}^3$. Les invariants Igusa ne sont pas définis sur les produits de courbes elliptiques (c'est-à-dire pour $\chi_{10} = 0$) et ne représentent pas une classe d'isomorphisme unique lorsque $\psi_4 = 0$. Et en effet pour $\psi_4 = 0$ tous les éléments du triplet s'annulent, on pourra utiliser d'autres invariants birationnels pour caractériser les classes d'isomorphimes, des exemples de triplets de ce genre sont fournis par le théorème 4.3.2 (le chapitre 4 et la section 4.3) en utilisant leurs fonctions modulaires associées.

3.3.2 *Invariants avec les thêta constantes*

On considère le sous groupe $\Gamma_2(2,4)$ de Γ_2, c'est un sous groupe normal d'indice 11520. Soit $\Omega \in \mathcal{F}_2$, on reprend les considérations de la proposition 3.3.7 en supposant qu'aucune thêta constante paire ne s'annule en Ω. Alors les huits possibles 10-uplets de theta constante paires qui satisfont le système d'équations 3.3.7 sont définis par :

$$\left\{ \left(\theta_j^2 \left(\Omega + \left(\begin{smallmatrix} 2a & b \\ b & 2c \end{smallmatrix} \right) \right) \right)_{j \in \mathcal{P}_2} \; : \; (a,b,c) \in \{0,1\}^3 \right\}$$

Il en découle la proposition suivante :

Proposition 3.3.10. *Pour tout* $\Omega, \Omega' \in \mathfrak{H}_2$ *tels que :*

$$\left[\theta_0^2(\Omega) : \theta_1^2(\Omega) : \theta_2^2(\Omega) : \theta_3^2(\Omega)\right] = \left[\theta_0^2(\Omega') : \theta_1^2(\Omega') : \theta_2^2(\Omega') : \theta_3^2(\Omega')\right],$$

il existe $\gamma \in \Gamma_2(2,4)$ *tel que* $\Omega' = \gamma\Omega$.

Démonstration. Aller à [28] □

Et l'exemple 3.3.6 nous dit que pour tout $i \in \mathcal{P}_2$ et $j = 1, 2, 3$ les fonctions définies par :

$$\mathfrak{c}_i(\Omega) := \frac{\theta_i^2(\Omega)}{\theta_0^2(\Omega)} \quad et \quad \mathfrak{b}_j(\Omega) := \frac{\theta_i(\Omega/2)}{\theta_0(\Omega/2)}$$

sont $\Gamma_2(2,4)$-modulaires. À partir des formules de duplication 3.3.2 on montre que l'on peut passer des $\mathfrak{c}_i$ aux $\mathfrak{b}_j$ et inversement. Par suite nous avons le résultat suivant :

$$\begin{aligned}
\mathfrak{b}_1 &= (\mathfrak{c}_1 + \mathfrak{c}_9)(1 + \mathfrak{c}_4 + \mathfrak{c}_8 + \mathfrak{c}_{12})^{-1}, \\
\mathfrak{b}_2 &= (\mathfrak{c}_2 + \mathfrak{c}_6)(1 + \mathfrak{c}_4 + \mathfrak{c}_8 + \mathfrak{c}_{12})^{-1}, \\
\mathfrak{b}_3 &= (\mathfrak{c}_3 + \mathfrak{c}_{15})(1 + \mathfrak{c}_4 + \mathfrak{c}_8 + \mathfrak{c}_{12})^{-1}.
\end{aligned}$$

Théorème 3.3.11. *Le corps des fonctions modulaires invariantes par* $\Gamma_2(2,4)$ *est* $\mathbb{C}(\mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3) = \mathbb{C}(\mathfrak{c}_1, \cdots, \mathfrak{c}_{15})$.

Démonstration. Aller à [72, 78] □

3.4 ESPACE MODULAIRE DE HILBERT

Dans cette partie nous définissons l'espace modulaire de Hilbert. Cet espace à l'avantage de produire des polynômes modulaires plus petits. Et des polynômes modulaires de Hilbert ont été évalués par E.Milio dans [78] (en fonctions de invariants de Gundlach et aussi en fonctions des invariants thêta). Nous faisons dans cette section un rappel sur la structure de l'espace de module d'Hilbert en se referant aussi sur les travaux de [44, 47-50].

3.4.1 *Surfaces de Humbert*

Soit $\Omega = \left(\begin{smallmatrix} \Omega_1 & \Omega_2 \\ \Omega_2 & \Omega_3 \end{smallmatrix}\right) \in \mathfrak{H}_2$ et $a, b, c, d, e \in \mathbb{Z}$. Une équation de la forme:

$$a\Omega_1 + b\Omega_2 + c\Omega_3 + d(\Omega_2^2 - \Omega_1\Omega_3) + e = 0$$

est appelée *relation singulière* de *discriminant* $\Delta = b^2 - 4ac - 4de$. Et si de plus pgcd $(a, b, c, d, e) = 1$ on dira que la relation singulière est *primitive*.
Lorsque $\Omega \in \mathfrak{H}_2$ vérifie ces propriétés alors on montre que toute sa classe d'équivalence modulo Γ_2 les vérifient. Et d'après le *Lemme d'Humbert*[48, 49], il existe un $\gamma \in \Gamma_2$ tel que élément $\Omega' = \gamma\Omega = \left(\begin{smallmatrix} \Omega'_1 & \Omega'_2 \\ \Omega'_2 & \Omega'_3 \end{smallmatrix}\right)$ dans cette classe vérifiant la relation normalisée de la forme:

$$\Omega'_1 + \ell\Omega'_2 - \Omega'_3 = 0$$

où k et ℓ sont déterminés uniquement par $\Delta = 4k + \ell$ et $\ell \in \{0, 1\}$.
Pour tout $\Omega \in \mathfrak{H}_2$ satisfaisant une relation singulière de discriminant Δ, des algorithmes dans [4, 78] permettent de déterminer un $\gamma \in \Gamma_2$ comme dans le Lemme d'Humbert.
Soit $\Delta \equiv 0, 1 \mod 4$ *et* $\Delta > 0$, *on appelle surface de Humbert* H_Δ *de discriminant* Δ *l'ensemble formé par les* $\Omega \in \mathfrak{H}_2/\Gamma_2$ *qui satisfont une relation primitive singulière de discriminant* Δ.

Proposition 3.4.1. *Soient* $\mathcal{A}_\Omega$ *la surface abélienne principalement polarisée associée à* $\Omega \in \mathfrak{H}_2$ *et* $\Delta \neq \Delta'$ *deux discriminants qui ne sont pas des carrés, alors:*

- $\mathcal{A}_\Omega$ *est simple si et seulement si* $\Omega \notin \bigcup_{m>0} H_{m^2}$;
- *Si* $\Omega \in H_\Delta$, *alors* $\mathrm{End}\,(\mathcal{A}_\Omega) \otimes \mathbb{Q}$ *contient* $\mathbb{Q}(\sqrt{\Delta})$;
- *Si* $\Omega \in H_\Delta \cap H_{\Delta'}$, *alors soit* $\mathcal{A}_\Omega$ *est simple et* $\mathrm{End}\,(\mathcal{A}_\Omega) \otimes \mathbb{Q}$ *est une algèbre de quaternions totalement indéfinie sur* $\mathbb{Q}$, *ou* $\mathcal{A}_\Omega$ *est isogène à* $E \times E$, *où* E *est une courbe elliptique.*

Soit D un entier sans facteur carré et $K = \mathbb{Q}(\sqrt{D})$ un corps quadratique réel de discriminant Δ (égal à D si $D \equiv 1 \mod 4$ sinon $4D$, son anneau des entiers est $\mathcal{O}_K = \mathbb{Z} + \omega\mathbb{Z}$; (où $\omega = \frac{1+\sqrt{D}}{2}$ si $D \equiv 1 \mod 4$ sinon $\omega = \sqrt{D}$).
Pour tout $\lambda \in K$ et pour $z = (z_1, z_2) \in \mathfrak{H}_1^2$ avec $\mathfrak{H}_1 = \{z \in \mathbb{C} : \mathrm{Im}\, z > 0\}$, on définit sur $\mathfrak{H}_1^2$:

$$\lambda z = (\lambda z_1, \overline{\lambda} z_2), \quad N(z) = z_1 z_2 \quad et \quad \mathrm{Tr}(z) = z_1 + z_2$$

et une involution v telle que : $(z_1, z_2) \mapsto (z_2, z_1)$.
Le groupe $\mathrm{SL}_2(\mathcal{O}_K)$ agit par la gauche sur $\mathfrak{H}_1^2$ par :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot (z_1, z_2) = \left(\frac{az_1 + b}{cz_1 + d}, \frac{\overline{a} z_2 + \overline{b}}{\overline{c} z_2 + \overline{d}} \right)$$

On appelle *surface modulaire de Hilbert*, l'espace quotient $\mathrm{SL}_2(\mathcal{O}_{\mathbb{K}}) \backslash \mathfrak{H}_1^2$ lequel décrit les surfaces abéliennes principalement polarisées $\mathcal{A}$ avec multiplication réelle par l'ordre maximal $\mathcal{O}_{\mathbb{K}}$

dont un plongément est donné par $\mu : \mathcal{O}_{\mathbb{K}} \longrightarrow \mathrm{End}(\mathcal{A})$. Une fonction holomorphique f sur $\mathfrak{H}_1^2$ est appelée une formes modulaires de Hilbert de poids k pour le sous groupe Γ de $\mathrm{SL}_2(\mathcal{O}_{\mathbb{K}})$, si il vérifie pour tout $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ et $\tau = (\tau_1, \tau_2) \in \mathfrak{H}_1^2$ la condition $f(\gamma\tau) = N(c\tau + d)^k f(\tau)$; et une fonction modulaire de Hilbert est le quotient de deux formes modulaires de Hilbert de même poids. Une forme ou une fonction modulaire f est dite symétrique si elle vérifie $f(v(z)) = f(z)$.

Exemple 3.4.2. Soit (e_1, e_2) une $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$, on définit les séries d'Eisenstein de poids pair $k \geq 2$ par :

$$G_k(z) = 1 + \sum_{t=a+b\bar{e}\in\mathcal{O}_K^+} b_k(t) q_1^a q_2^b \quad avec \quad b_k(t) = \kappa_k \sum_{t\mathcal{O}_K \subset \mu\mathcal{O}_K} |\mathcal{O}_K/\mu\mathcal{O}_K|^{k-1}$$

et $\kappa_k = \zeta_K(k)^{-1}(2\pi)^{2k}((k-1)!)^{-2}\Delta_K^{1/2-k}$. Où on a:

$$q_1 = \exp(2i\pi(e_1 t_1 + \overline{e_1} t_2)) \quad \text{et} \quad q_2 = \exp(2i\pi(e_2 t_1 + \overline{e_2} t_2))$$

Ces séries d'Eisenstein sont des formes modulaires symétriques pour $\mathrm{SL}_2(\mathcal{O}_K)$ avec des coefficients dans $\mathbb{Q}$.

Soit $\dot{\Gamma}(1) = \mathrm{SL}_2(\mathcal{O}_{\mathbb{K}} \otimes \partial_{\mathbb{K}})$ où

$$\mathrm{SL}_2(\mathcal{O}_{\mathbb{K}} \otimes \partial_{\mathbb{K}}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{K}) : \ a, b \in \mathcal{O}_{\mathbb{K}}, \ b \in \frac{1}{\sqrt{\Delta_{\mathbb{K}}}}\mathcal{O}_{\mathbb{K}} \text{ et } c \in \sqrt{\Delta_{\mathbb{K}}}\mathcal{O}_{\mathbb{K}} \right\}.$$

Soient $z = (z_1, z_2) \in \mathfrak{H}_1^2$, $x \in \mathbb{K}$ et $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{K})$ alors on admet les notations suivantes: $z^* = \left(\begin{smallmatrix} z_1 & 0 \\ 0 & z_2 \end{smallmatrix}\right)$, $x^* = \left(\begin{smallmatrix} x & 0 \\ 0 & \bar{x} \end{smallmatrix}\right)$ et $\gamma^* = \left(\begin{smallmatrix} a^* & b^* \\ c^* & d^* \end{smallmatrix}\right)$.
Lorsqu'une $\mathbb{Z}$-base (e_1, e_2) de $\mathcal{O}_{\mathbb{K}}$ fixée l'on définit les applications :

$$\begin{array}{rccc} \phi_{e_1,e_2}: & \mathfrak{H}_1^2 & \longrightarrow & \mathfrak{H}_2 \\ & z & \longmapsto & {}^tRz^*R \end{array} \quad \text{et} \quad \begin{array}{rccc} \phi_{e_1,e_2}: & \mathrm{SL}_2(\mathbb{K}) & \longrightarrow & \mathrm{Sp}_4(\mathbb{Q}) \\ & \gamma & \longmapsto & S\gamma^*S^{-1} \end{array}$$

où $R = \left(\begin{smallmatrix} e_1 & e_2 \\ \bar{e}_1 & \bar{e}_2 \end{smallmatrix}\right)$ et $S = \left(\begin{smallmatrix} {}^tR & 0 \\ 0 & R^{-1} \end{smallmatrix}\right)$. Et ces applications satisfont:

- $\phi_{e_1,e_2}^{-1}(\Gamma_2) = \dot{\Gamma}(1)$ et $\phi_{e_1,e_2}(v(z)) = \gamma \cdot \phi_{e_1,e_2}(z)$ pour un certain $\gamma \in \Gamma_2$.
- $\phi_{e_1,e_2}(\gamma \cdot z) = \phi_{e_1,e_2}(\gamma) \cdot \phi_{e_1,e_2}(z)$, $\forall \gamma \in \dot{\Gamma}(1)$ et $z \in \mathfrak{H}_1^2$.
- Pour une autre $\mathbb{Z}$-base (f_1, f_2) de $\mathcal{O}_{\mathbb{K}}$ il existe $\gamma \in \Gamma_2$ tel que: $\phi_{e_1,e_2}(z) = \gamma \cdot \phi_{e_1,e_2}(z)$.

La fonction: ϕ_{e_1,e_2} définie sur $\mathfrak{H}_1^2$ et $\mathrm{SL}_2(\mathbb{K})$ envoie $\mathfrak{H}_1^2$ et $\left(\dot{\Gamma}(1) \cup \dot{\Gamma}(1)_v\right) \backslash \mathfrak{H}_1^2$ vers la surface de Humbert de discrimant $\Delta_{\mathbb{K}}$. L'espace analytique quotient $\left(\dot{\Gamma}(1) \cup \dot{\Gamma}(1)_v\right) \backslash \mathfrak{H}_1^2$ est appelé une surface modulaire symmétrique de Hilbert. Il est birationnellement équivalent à la surface de Humbert.
Ces résultats sont illustrés sur le diagramme commutatif suivant: où η est une application rationnelle de degré 2 et ρ est une application génériquement de degré 1 sur la surface de Humbert $H_{\Delta_{\mathbb{K}}}$ (pour plus de détails sur cette construction aller à [79, § 2]). Une composante irréductible de $H_{\Delta_{\mathbb{K}}}^{\Gamma} = \eta^{-1}(H_{\Delta_{\mathbb{K}}})$ dans $\Gamma\backslash\mathfrak{H}_2$ est appelé une composante de la surface de Humbert.
En particulier lorsque $\mathbb{C}(\Gamma) = \mathbb{C}(i_1, \cdots, i_k)$ pour le sous groupe modulaire Γ tel que les restrictions des fonctions modulaires i_j n'admettent pas de pôles en les points génériques des composantes $H_{\Delta_{\mathbb{K}}}^{\mathcal{G}}$ (où $\mathcal{G} = \phi_{1,\omega}^{-1}(\Gamma)$). Alors les $\rho^* i_j$ engendrent le corps de fonctions $\mathbb{C}_{\mathcal{G}}$ des fonctions modulaires de Hilbert. Par suite, ces tirés-en-arrières ("pullbacks") engendrent les fonctions modulaires symétriques de Hilbert pour $\dot{\Gamma} = \mathcal{G} \cap \dot{\Gamma}(1)$ ou ils engendrent tout

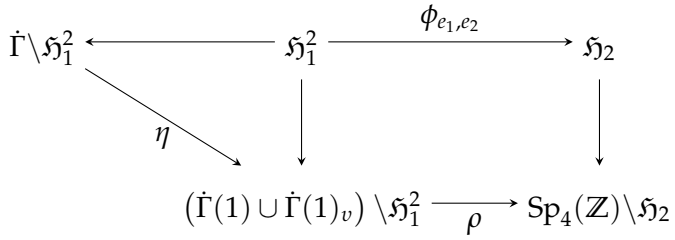


FIGURE 3.4 – Diagramme de description de composantes de surface de Humbert

le corps de fonctions $\mathbb{C}_{\dot{\Gamma}}$ des fonctions modulaires de Hilbert pour $\dot{\Gamma}$ [79, Prop 2.15.]. Donc le tiré-en-arrière par le plongément de Hilbert permet d'exprimer les j_i (en utilisant $\phi_{1,\omega}^* j_i$) comme invariants sur une surface modulaire symétrique de Hilbert. De façon similaire, $\dot{b}_k = \phi^* b_k$ et $\dot{t}_k = \phi^* t_k$ pour $k = 1,2,3$ sont les générateurs pour le corps de fonctions modulaires de Hilbert invariants par $\dot{\Gamma}(2)$ respectivement par $\dot{\Gamma}(2,4)$ si $D \equiv 1 \mod 4$ et par $\dot{\Gamma}(2)\cup\dot{\Gamma}(2)_v$ respectivement par $\dot{\Gamma}(2,4)\cup\dot{\Gamma}(2,4)_v$ si $D \equiv 2,3 \mod 4$ où:

$$\dot{\Gamma}(2) = \phi_{1,\omega}^{-1}(\Gamma(2)) \cap \mathrm{SL}_2(\mathcal{O}_{\mathbb{K}} \otimes \partial_{\mathbb{K}}) \quad \text{et}$$

$$\dot{\Gamma}(2,4) = \phi_{1,\omega}^{-1}(\Gamma(2,4)) \cap \mathrm{SL}_2(\mathcal{O}_{\mathbb{K}} \otimes \partial_{\mathbb{K}}).$$

Comme $\mathbb{C}_{\Gamma_2} = \mathbb{C}(j_1, j_2, j_3)$ et les tirés en arrière des invariants d'Igusa peuvent être exprimés en terme des invariants de Gundlach comme l'indique le théorème 3.4.4.
Ainsi toute fonction modulaire symétrique de Hilbert peut être ainsi exprimée en terme des invariants de Gundlach. Et pour les D où l'on n'a pas d'invariants de Gundlach on peut prendre les fonctions algébriquement dépendantes $\phi^* j_k$ pour $k = 1,2,3$ comme invariants sur la surface modulaire symétrique de Hilbert.

Par exemple pour le cas $\Gamma = \Gamma_2(2,4)$ le nombre de composantes de la surface de Humbert est:

$$\begin{cases} 10 & si \quad D \equiv 1 \mod 8, \\ 6 & si \quad D \equiv 5 \mod 8, \\ 60 & si \quad D \equiv 2,3 \mod 4 \end{cases}$$

Et pour $D = 2,3,5$, les composantes de ces surfaces de Humbert sont données par les équations suivantes:

$$b_1 - \frac{1}{2}(b_2 + b_3^2) = 0,$$

$$-b_1^4 - b_2^4 - 4b_3^2 - 2b_1^2 b_2^2 + 4b_1 b_2 + 4b_1 b_2 b_3^2 = 0,$$

$$-\frac{1}{2}\left(\sum_i b_i^4 + \sum_i \sum_{j\neq i} (b_i b_j)^4\right) + b_1 b_2 b_3 \left(1 + \sum_i b_i^4 - b_1 b_2 b_3\right) = 0.$$

La surface modulaire de Hilbert $\mathrm{SL}_2(\mathcal{O}_{\mathbb{K}})\backslash\mathfrak{H}_1^2$ est rationnelle seulement pour $D = 2, 3, 5, 6, 7, 13, 17, 21, 33$ (d'après [47]). Et les deux générateurs de la surface modulaire symétrique de Hilbert pour les cas $D = 2$ et 5 sont définis comme suite .
• Pour $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, on pose :

$$H_4 = \frac{11(G_2^2 - G_4)}{2^{-6}.3^{-2}} \quad et \quad H_6 = \frac{-5\cdot 7^2 \cdot G_2^3}{2^8 \cdot 3^3 \cdot 13} + \frac{11 \cdot 59 G_2 G_4}{2^8 3^2 5 \cdot 13} - \frac{19^2 \cdot G_6}{2^7 \cdot 3^3 \cdot 5 \cdot 13}$$

• Pour $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, on pose :

$$H_6 = \frac{67(G_2^3 - G_6)}{2^5 3^3 5^2}, \quad H_{12} = 2^{-2}(H_6^2 - G_2 H_{10}) \quad et$$
$$H_{10} = 2^{-10}3^{-5}5^{-5}7^{-1}(412751G_{10} - 5 \cdot 67 \cdot 2293 G_2^2 G_6 + 2^2 3 \cdot 7 \cdot 4231 G_2^5)$$

Théorème 3.4.3. *Le corps des fonctions modulaires de Hilbert pour $\mathrm{SL}_2(\mathcal{O}_\mathbb{K})$ sont des fonctions rationnelles en $\mathfrak{I}_1$ et $\mathfrak{I}_2$ appelés invariants de Gundlach pour $\mathbb{K}$.*

• *Lorsque $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ on a $\mathfrak{I}_1 = \dfrac{G_2^2}{H_4}$ et $\mathfrak{I}_2 = \dfrac{G_2 H_6}{H_4^2}$.*

• *Lorsque $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ on a $\mathfrak{I}_1 = \dfrac{G_2^5}{H_{10}}$ et $\mathfrak{I}_2 = \dfrac{G_2^2 H_6}{H_{10}}$.*

Démonstration. Aller à [44]. □

3.4.2 *De Hilbert à Siegel*

On considère $\mathbb{K} = \mathbb{Q}(\sqrt{D})$, alors on a $\partial_\mathbb{K} = \sqrt{\Delta_\mathbb{K}}\mathcal{O}$ et $\partial_\mathbb{K}^{-1} = \dfrac{1}{\Delta_\mathbb{K}}\mathcal{O}_\mathbb{K}$.

Une base plus pratique est donnée par $e_1 = 1$ et $e_2 = \epsilon$. Dans ce cas, on a que pour tout $z \in \mathfrak{H}_1^2$, l'image $\phi_{1,\epsilon}(z) = \left(\begin{smallmatrix} \Omega_1 & \Omega_2 \\ \Omega_2 & \Omega_3 \end{smallmatrix}\right) \in \mathfrak{H}_2$ vérifie :

$$\frac{D-1}{4}\Omega_1 + \Omega_2 - \Omega_3 = 0 \quad si \quad D \equiv 1 \mod 4,$$
$$D\Omega_1 - \Omega_3 = 0 \quad si \quad D \equiv 2,3 \mod 4.$$

Si de plus ϵ est une unité de norme -1, il existe des bijections $\phi_0 : z \mapsto \dfrac{\epsilon}{\sqrt{\Delta_K}}z$ et $\phi_0 : \gamma \mapsto \alpha\gamma\alpha^{-1}$ de $\mathrm{SL}_2(\mathcal{O}_\mathbb{K})$ sur $\mathrm{SL}_2(\mathcal{O}_\mathbb{K} \otimes \partial_\mathbb{K}^{-1})$ avec $\alpha = diag(1, \sqrt{\Delta_\mathbb{K}}/\epsilon)$ telles que lorsque l'on définit $\phi_\epsilon = \phi_1 \circ \phi_0$ avec $\phi_1 = \phi_{1,\bar{\epsilon}}$; alors une forme modulaire symétrique de Hilbert peut être définie comme le tiré en arrière par ϕ_ϵ d'une forme modulaire de Siegel pour Γ_2 de poids k [78, Proposition 5.1.10]. En utilisant cette approche on montre le théorème suivant exprimant en fonction des invariants de Gunlach les tirés en arrière par ϕ_ϵ des invariants d'Igusa dans les cas $D = 2$ et $D = 5$.

Théorème 3.4.4. *(De Hilbert à Siegel).*

• *Lorsque $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, on a :*

$$\phi_\epsilon^* j_1 = 8\mathfrak{I}_1 \left(3\mathfrak{I}_2^2/\mathfrak{I}_1 - 2\right)^5 ;$$
$$\phi_\epsilon^* j_2 = 2^{-1}\mathfrak{I}_1 \left(3\mathfrak{I}_2^2/\mathfrak{I}_1 - 2\right)^3 ;$$
$$\phi_\epsilon^* j_3 = 2^{-3}\mathfrak{I}_1 \left(3\mathfrak{I}_2^2/\mathfrak{I}_1 - 2\right)^2 \left(4\mathfrak{I}_2^2/\mathfrak{I}_1 + 2^5 3^2 \mathfrak{I}_2/\mathfrak{I}_1 - 3\right).$$

• *Lorsque $\mathbb{K} = \mathbb{Q}(\sqrt{5})$, on a :*

$$\phi_\epsilon^* j_1 = 8\mathfrak{I}_1^3/\mathfrak{I}_2 \left(1 + 12/\mathfrak{I}_2 + 12\mathfrak{I}_2/\mathfrak{I}_1\right)^5 ;$$
$$\phi_\epsilon^* j_2 = 2\mathfrak{I}_1^2/\mathfrak{I}_2 \left(\mathfrak{I}_1 + 144\right)\left(1 + 12/\mathfrak{I}_2 + 12\mathfrak{I}_2\mathfrak{I}_1\right)^3 ;$$
$$\phi_\epsilon^* j_3 = 8^{-1}\left(1 + 12/\mathfrak{I}_2 + 12\mathfrak{I}_2\mathfrak{I}_1\right)^2 \cdot \left(\mathfrak{I}_1^3/\mathfrak{I}_2 + 16\mathfrak{I}_1^2\right.$$
$$\left. + 16\mathfrak{I}_1^3/\mathfrak{I}_2^2 + 2304\mathfrak{I}_1^2/\mathfrak{I}_2^2 + 408\mathfrak{I}_1^2/\mathfrak{I}_2 + 2880\mathfrak{I}_1\right).$$

Démonstration. Elle consiste à calculer en fonction des invariants de Gunlach les tirés en arrière par ϕ_ϵ des formes modulaires ψ_4, ψ_6, χ_{10} et χ_{12} en utilisant la Proposition 5.1.10 [78]. Pour plus de détails aller à [93]. □

4

ESPACES DE MODULE DES COURBES DE GENRE 2

Dans le chapitre 3 nous avons vu que sur $\mathbb{C}$ les Jacobiennes de courbes de genre 2 étaient exactement des surfaces abéliennes principalement polarisées que l'on pouvait générer à isomophisme près, à partir d'éléments de $\mathcal{F}_2$. Et d'une manière plus précise, les valeurs prises par les triplets d'invariants d'Igusa (ou de Streng) correspondent aux classes d'isomorphismes et mieux encore nous pouvons retrouver ces classes avec les invariants thêta .
Dans cette partie nous allons revoir les différents types d'invariants définis pour les courbes de genre 2 sur un corps quelconque.
Et cela a été le cas d'abord pour les courbes elliptiques où par exemple, on définit à équivalence près le j-invariant à partir de l'équation de la courbe par :

$$j = 1728a_4^3/4\Delta \quad avec \quad \Delta = -16(4a_4^3 + 27a_6^2),$$

pour une courbe elliptique d'équation: $y^2 = x^3 + ax + b$ sur un corps $\Bbbk$ de caractéristique $char(\Bbbk) \neq 2, 3$. Alors deux courbes elliptiques isomorphes E et E' ont le même j-invariant, et réciproquement si $j(E) = j(E')$, les courbes E et E' sont isomorphes sur $\Bbbk$. Ainsi l'espace modulaire des courbes elliptiques sur $\Bbbk$ est dimension 1.

L'objectif principal de ce chapitre est l'introduction de nouveaux invariants (la section 4.3) absolus pour les courbes de genre 2, ayant bonne réduction en toutes caractéristiques pour permettre de calculer le relevé canonique en petites caractéristiques sur l'espace de Siegle. Certaines des idées ci-dessous sont reprises de la publication [71].

4.1 INVARIANT D'UNE FORME SEXTIQUE

Soit un corps $\Bbbk$ de clôture algebrique $\overline{\Bbbk}$, une courbe de genre 2 $\mathcal{C}$ sur $\Bbbk$ admet un model affine $\mathcal{C} : y^2 + h(x)y = f(x)$ sur $\Bbbk[x, y]$, où $\deg(h) = 2$, f est unitaire de degré 5 ou 6. En effet la courbe $\mathcal{C}$ est complètement définie par son corps de fonction $\Bbbk(\mathcal{C})$. Et dans le cas où $\mathcal{C}$ est lisse, elle est une normalisation d'un model birationel de $\Bbbk(\mathcal{C})$. Alors comme dans le chapitre 3 et la section 3.2.2, $\Bbbk(\mathcal{C})$ est décrit en utilisant la *Théorie de Kummer* en caractéristique différente 2 ou en utilisant la *Théorie d'Artin-Schreier* en caractéristique 2.

Lorsque la caractéristique de $\Bbbk$ est $char(\Bbbk) \neq 2$, nous pouvons associer à un modèle hyperelliptique $y^2 = f(x)$, une forme sextique définie par :

$$F(x_1, x_2) = x_2^6 f(x_1/x_2)$$

et F aura la forme suivante:

$$F(x_1, x_2) = a_0x_1^6 + a_1x_1^5x_2 + ... + a_5x_1x_2^5 + a_6x_2^6$$

Selon la *Théorie des Invariants Algébriques de Hilbert* [76], un *covariant* est un polynôme $C \in \Bbbk[a_0, ..., a_6, x_1, x_2]$ en les coefficients de la forme générique du sextique, telque tout changement de variable

$$(x_1, x_2) \longrightarrow (\alpha x_1 + \beta x_2, \gamma x_1 + \delta x_2)$$

associé à la matrice $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in GL_2(\bar{\mathbb{k}})$, change C par une puissance fixée du $\det(M)$, c'est-à-dire

$$C(a'_0, ..., a'_6, \alpha x_1 + \beta x_2, \gamma x_1 + \delta x_2) = \det(M)^k C(a_0, ..., a_6, x_1, x_2)$$

où les a'_i avec $i \in \{0, \cdots 6\}$ sont les coefficients après changement.

Définition 4.1.1. Lorsque C est un covariant alors :

— C est homogène en x_1 et x_2 avec un degré total appelé *l'ordre de C* ;

— C est aussi homogène en a_i avec un degré total appelé *le degré de C* ;

— et k est appelé *l'indice de C*.

Alors nous avons la propriété suivante [76] :

$$2k = 6(\textit{degre de } C) - (\textit{ordre de } C)$$

Les covariants de covariants de $\mathcal{C}$ sont des covariants de $\mathcal{C}$. Et l'algèbre des covariants est de type fini [16].
Soit G le sous-groupe de $\mathrm{GL}_2(\mathbb{k})$ qui transforme une forme sextique F en uF, $u \in \mathbb{k}^*$, alors G contient les homothéties. Et le groupe des $\mathbb{k}$-automorphismes de F: $Aut_{\mathbb{k}}(F)$ est l'image de G dans $\mathrm{PGL}_2(\mathbb{k})$. [76].

Définition 4.1.2. Un invariant I d'une forme sextique F est un covariant d'ordre 0. On note par $I(\mathcal{C})$ ou $I(F)$ la valeur de I associée à la forme sextique F ou à la courbe de genre 2 $\mathcal{C}$.

Deux formes sextiques F et F' sont linéairement équivalentes (classification) si et seulement si il existe $r \in \bar{\mathbb{k}}^*$ tel que pour tout invariant I, on a $I(F) = r^d I(F')$, où d est le degré de I. Alors le fait qu'un invariant s'annule sur certaines courbes, dépend de la classe d'isomorphisme de la courbe.
Soient f et g deux formes binaires de degré n et m. Pour calculer les covariants d'une forme sextique, Clebsch introduisit une opération appelée *Ueberschiebung* définie par :

$$(fg)_k = \frac{(m-k)!(n-k)!}{m!n!} \left(\frac{\partial f}{\partial x}\frac{\partial g}{\partial y} - \frac{\partial f}{\partial y}\frac{\partial g}{\partial x} \right)^k$$

où dans le calcul binomial $\left(\frac{\partial f}{\partial x}\right)^r \left(\frac{\partial f}{\partial y}\right)^s$ signifie $\frac{\partial^{r+s} f}{\partial x^r \partial y^s}$. Et quand $f = g$ on prefère noter $(ff')_k$ à la place de $(ff)_k$.

Proposition 4.1.3.
— *$(fg)_k$ est un covariant de f et g d'ordre $m + n - 2k$ où $m = \deg(f)$ et $n = \deg(g)$.*

— *En particular si g et h sont deux formes binaires de f d'ordre m et n , de degré r et s alors $(gh)_k$ est un covariant de f d'ordre $m + n - k$ et de degré $r + s$.*

— *Tout covariant de f peut être déterminer en utilisant le* Ueberschiebung *(appliqué de manière itérée à f).*

Démonstration. Aller à [16, 76]. □

Exemple 4.1.4. Soit f une forme sextique, par le *Ueberschiebung* nous avons les covariants suivant :

covariants	*ordre*	deg
$i = (ff')_4$	4	2
$\Delta = (ii')_2$	4	4
$y_1 = (fi)_4$	2	3
$y_2 = (iy_1)_2$	2	5
$y_3 = (iy_2)_2$	2	7
$A = (ff')_6$	0	2
$B = (ii')_4$	0	4
$C = (i\Delta)_4$	0	6
$D = (y_3y_1)_2$	0	10
$R = -(y_1y_2)(y_2y_3)(y_3y_1)$	0	15

L'algèbre des invariants est engéndré par A, B, C, D et R [16]. D'autre part R^2 admet une expression polynomiale en les quatres générateurs de degrés pairs. Alors la condition d'équivalence linéaire des formes sextiques se réduit aux quatres invariants A, B, C, D appelés *invariants de Clebsh*.
En considérant le modèle hyperelliptique des courbes de genre 2 $\mathcal{C}$: $y^2 = f(x) = u_0x^6 + u_1x^5 + ... + u_5x + u_6$ et $\alpha_1, \cdots, \alpha_6$ des racines distinctes de f : on note par (ij) la différence $(\alpha_{\sigma(i)} - \alpha_{\sigma(j)})$. Alors J. Igusa a montré [51] que les expréssions:

$$I_2 = u_0^2 \sum_{15} (12)^2(34)^2(56)^2 \ ,$$

$$I_4 = u_0^4 \sum_{10} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2 \ ,$$

$$I_6 = u_0^6 \sum_{60} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2 \ ,$$

$$I_{10} = u_0^{10} \prod_{i<j} (\alpha_i - \alpha_j)^2$$

telles que une racine α_i apparaît dans chaque expréssion m fois égal au degré de u_0, sont des invariants homogènes (à coefficients entiers) de degré m. L'invariant I_{10} est le discriminant de la forme sextique associée. Il est possible de calculer ces nouveaux invariants en fonction de ceux de Clebsh et vis-versa, par les rélations suivantes:

$$\begin{aligned}
I_2 &= -120A \ , \\
I_4 &= -720A^2 + 6750B \ , \\
I_6 &= 8640A^3 - 108000AB + 202500C \ , \\
I_{10} &= -62208A^5 + 972000A^3B + 1620000A^2C - 3037500AB^2 - \\
&\quad 6075000BC - 4556250D.
\end{aligned}$$

Ainsi on appelle les I_{2i} avec $\{1, 2, 3, 5\}$ les *invariants d'Igusa-Clebsh*. Et Igusa montra qu'à tout quadruplet (A, B, C, D) correspond une forme sextique admettant A, B, C, D comme invariants . En caractéristique nulle la connaissance du quadruplet (A, B, C, D) (par équivalence celle des I_{2i}) dans l'espace projectif gradué correspond exactement à celle des courbes de

genre 2 dans l'espace de module ("coarse") $\mathcal{M}_2$.
Cependant, ces invariants n'ont pas une bonne réduction pour certaines caractéristiques. En effet, les invariants de Clebsh (A, B, C, D) ont une mauvaise réduction en caractéristique 2, 3, 5. Et les réductions en caractéristiques 2 et 3 des invariants d'Igusa-Clebsh même si elle sont définies ne permettent pas une classification des courbes de genre 2 pour ces caractéristiques.

4.2 INVARIANTS ARITHMÉTIQUES

Dans le sens d'étendre la classification fournie par les invariants I_{2i} au caractéristique 2 et 3, Igusa procède par exprimer les invariants I_{2i} avec $i \in \{1, 2, 3, 5\}$ comme polynômes sur $\mathbb{Z}$ en les coefficients a, b, c, d de la *forme normale universelle* associé à une courbe de genre 2 en caractŕistique quelconque.

4.2.1 *Forme Normale Universelle*

Dans cette partie nous nous intéressons aux résultats d'Igusa [51, § 2] sur la construction d'une *forme normale* associée à une courbe hyperelliptique de genre 2.
Lorsque $\mathcal{C}$ est une courbe hyperelliptique de genre 2, P un point de Weierstrass de $\mathcal{C}$ et Q un point n'étant pas de Weierstrass. Alors d'après la construction d'Igusa [51, § 2], pour P et Q fixé et en utilisant que des transformations projectives on peut toujours déterminer un modèle non-homogène de $\mathcal{C}$ sous la forme

$$XY^2 + (1 + aX + bX^2)Y + X^2(c + dX + X^2) = 0 \tag{4.1}$$

de manière unique (par transformation près de la forme $(a, b, c, d) \longrightarrow (\zeta a,\ \zeta^2 b,\ \zeta^3 b,\ \zeta^4 b)$ avec $\zeta^5 = 1$.) Et réciproquement, si une courbe définie par une telle équation n'admet des singularités qu'en $(0, 1, 0)$ alors son model lisse est une courbe hyperelliptique d'équation :

$$Y^2 + (1 + aX + bX^2)Y = -X^3(c + dX + X^2)$$

Et l'équation (4.1) est appélée *forme normale universelle* de la courbe hyperelliptique $\mathcal{C}$ de genre 2.
Lorsque la caractéristique est différente de 2, une telle équation peut donner une forme de Rosenhain. En effet pour x différent de 0 et ∞, les deux racines de l'équation en Y:

$$xY^2 + (1 + ax + bx^2)Y + x^2(c + dx + x^2) = 0$$

détermine un membre d'un système canonique de $\mathcal{C}$ autre que $2P$ et $Q + Q'$ (qui correspondent respectivement à $x = 0$ et $x = \infty$). Alors les autres points de Weierstrass (définissant des Y doubles) sont les solutions de l'équation:

$$(1 + aX + bX^2)^2 - 4X^3(c + dX + X^2) = 0$$

Ainsi nous obtenons les points de Weierstrass d'une forme de Rosenhain:

$$X(X - 1)(X - \mathfrak{r}_1)(X - \mathfrak{r}_2)(X - \mathfrak{r}_3) = 0$$

En caractéristique 2, le résultat correspond à la construction d'Artin-Schreier d'une courbe de genre 2: $y^2 - y = R(x)$, où R est une fonction rationelle en x avec diviseurs de pôle. Les classes d'isomorphismes de ces courbes sont en bijection avec les orbites des $R(x)$ sous

la double action par le goupe d'Artin-Schreier $AS(\Bbbk(x))$ et le groupe projective linéaire $\mathrm{PGL}_2(\Bbbk)$. Pour plus de détails sur ces actions de groupes se referer à [33, 51]. Il en découle l'existence de trois types de ramifications pour les points de Weierstrass $(1,1,1)$, $(3,1)$, (5) et une courbe correspondant à un de ces types est birationnellement équivalente à une courbe plane affine définie par:

$$Y^2 - Y = \begin{cases} \alpha X + \beta X^{-1} + \gamma(X-1)^{-1}, \quad \alpha\beta\gamma \neq 0 & (1,1,1) \\ X^3 + \alpha X + \beta X^{-1}, \quad \beta \neq 0 & (3,1) \\ X^5 + \alpha X^3, & (5) \end{cases}$$

En effet en partant de la forme normale non réduite définie précédente, les points de Weierstrass de $\mathcal{C}$ autre que P (s'il en existe) correspondent aux solutions $1 + aX + bX^2 = 0$. Ainsi les cas $ab \neq 0$ correspondent à trois points de Weierstrass c'est-à-dire le type $(1,1,1)$. Le cas $a = 0$ ou-bien $b = 0$, nous avons un seul point de Weierstrass différent de P et le type est $(3,1)$. Dans le dernier cas $a = b = 0$, correspondant au type (5), tous les points de Weierstrass se réduisent sur P.

4.2.2 *Invariants Arithmétiques*

En dimension 1, on considère la fonction j-invariant j. Selon la théorie des invariants de Deuring [26]: $\mathbb{Z}[j]$ est l'anneau des fonctions continues préservant la caractéristique et ne dependant que des classes birationnelles, définies sur l'ensemble des courbes elliptiques à valeur dans le domaine arithmétique universel.
Alors Igusa définit un *invariant intégral* comme une fonction continue préservant la caractéristique définie sur l'espace des formes sextiques à valeur dans le domaine arithmétique universel qui ne dépendent que des orbites. Et ceux qui ne dépendent que des classes birationnelles des courbes hyperelliptiques de genre 2 sont appelés des *invariants absolus*. En terminologie moderne, un invariant intégral est une section global du champ ("stack") algébrique quotienté par cette action, autrement dit une section de l'espace de module fine $\mathcal{M}_2$ ("stack") et aussi de son espace de module (en "coarse").
En genre 2, les invariants intégrals forment un anneau intègre gradué sur $\mathbb{Z}$. Cet anneau tensorisé avec $\mathbb{Q}$ sur $\mathbb{Z}$ est l'anneau intègre gradué des invariants rationnels. Et les $I_{2i}(\mathcal{C})$ sont les valeurs prises par les invariants intègrals homogènes I_{2i} de degré $2i$ sur la sextique assocée à $\mathcal{C}$. Un *invariant arithmétique* est définit comme un invariant rationnel sur $\mathbb{Z}$ en les coefficients a, b, c, d d'une forme normale.
Par exemple :

$$J_2 = 2^{-3} I_2, \quad J_4 = 2^{-5}3^{-1}(4J_2^2 - I_4),$$
$$J_6 = 2^{-6}3^{-2}(8J_2^3 - 160 J_2 J_4 - I_6),$$
$$J_8 = 2^{-2}(J_2 J_6 - J_4^2), \quad J_{10} = 2^{-12} I_{10}.$$

sont des invariants arithmétiques associés à la courbe d'équation

$$XY^2 + (1 + aX + bX^2)Y + X^2(c + dX + X^2) = 0$$

introduits par Igusa dans [51, p. 621]. Les J_{2i} se réduisent bien en toute caractéristique et on a bien $J_{10} \neq 0$ car il encode la propriété que $\mathcal{C}$ est lisse. Et lorsque la caracteéristique n'est pas 2, I_{10} correspond au discriminant de $\mathcal{C}$, donc inversible sur $\mathcal{M}_2$, car ces courbes sont lisses sur leur base. Les J_{2i} comme polynômes en fonction des a, b, c, d est une quantité ne

dépendant que de la classe birationnelle des courbes de genre 2. En caractéristique différent de 2, c'est une conséquence de la propriété d'invariance des I_{2i} et en caractéristique 2, c'est une conséquence des rélations explicites entre les formes normales réduites l'équation (4.1) et les J_{2i} (détaillées plus loin les équations (4.7) à (4.9)).
Et réciproquement Igusa montre dans [51] qu'en toute caractéristique, à tout quintuplet $(J_2, J_4, J_6, J_8, J_{10})$ avec $J_{10} \neq 0$ correspond une forme normale d'invariant arithmétiques J_2, J_4, J_6, J_8 et J_{10} (souvent sur des extensions de corps) [51, § 3, § 5]. Lorsque la caractéristique n'est pas 2, cette construction peut se faire algorithmiquement en utilisant la méthode de Igusa-Clebsh [76] et en caractéristique 2 on pourra utiliser les relations la section 4.3.2. En utilisant la relation $J_2J_6 - J_4^2 - 4J_8 = 0$, on peut se restreindre au quadruplet (J_2, J_4, J_6, J_{10}) en caractéristique différente 2. Cependant en caractéristique 2, le rôle de l'invariant J_8 est crucial pour décrire les classes d'isomorphismes.

On considère le localisé par les puissances de J_{10}, de l'anneau gradué engendré par les invariants J_{2i} $i = 1, 2, 3, 4, 5$. On désigne par $\mathcal{R}$ l'anneau intègre formé par ses éléments homogènes de degré zéro.
Alors d'après [51, § 7] l'anneau $\mathcal{R}$ est engendré sur $\mathbb{Z}$ par les éléments de la forme $J_2^{e_1}J_4^{e_2}J_6^{e_3}J_8^{e_4}J_{10}^{-e_5}$ avec e_i des entiers naturels satisfaisant $e_1 + 2e_2 + 3e_3 + 4e_4 = 5e_5$. Et si y_1, y_2, y_3 et y_4 sont des variables indépendantes avec $4y_4 = y_1y_3 - y_2^2$, alors la correspondance :

$$J_2^{e_1}J_4^{e_2}J_6^{e_3}J_8^{e_4}J_{10}^{-e_5} \longmapsto y_1^{e_1}y_2^{e_2}y_3^{e_3}y_4^{e_4}$$

de $\mathcal{R}$ vers $\mathbb{Z}[y_1, y_2, y_3, y_4]$ définit un isomorphisme entre $\mathcal{R}$ et les éléments de $\mathbb{Z}[y_1, y_2, y_3, y_4]$ invariant par la transformation $y^i \longmapsto \zeta_5^i y_i$ pour $i = 1, 2, 3, 4$, où ζ_5 est une racine cinquième de l'unité.
En considérant la condition $J_2J_6 - J_4^2 - 4J_8 = 0$ on arrive à montrer que le monoïde des puissances e_i est engendré par dix éléments, reduit à huit en caractéristique différente de 2. Alors $\mathcal{R}$ est engendré par dix éléments suivants appelés γ_i dans [41]:

$$\gamma_1 = J_2^5/J_{10}, \quad \gamma_2 = J_2^3J_4/J_{10}, \quad \gamma_3 = J_2^2J_6/J_{10}, \quad \gamma_4 = J_2J_8/J_{10},$$
$$\gamma_5 = J_2J_6/J_{10}, \quad \gamma_6 = J_4J_8^2/J_{10}^2, \quad \gamma_7 = J_6^2J_8/J_{10}^2, \quad \gamma_8 = J_6^5/J_{10}^3,$$
$$\gamma_9 = J_6J_8^3/J_{10}^3, \quad \gamma_{10} = J_8^5/J_{10}^4.$$

On considère que, μ_5 le groupe des racines cinquième de l'unité, alors en résumé nous avons le résultat suivant.

Théorème 4.2.1. *l'espace de module $\mathcal{M}_2$ des courbes de genre 2 est isomorphe à*

$$\mathrm{Proj}\left(\mathbb{Z}[J_2, J_4, J_6, J_8, J_{10}]\right)_{(J_{10})} = \mathrm{Spec}\left(\mathbb{Z}[y_1, y_2, y_3, y_4]^{\mu_5}\right) = \mathrm{Spec}\left(\mathbb{Z}[\gamma_1, \ldots, \gamma_{10}]\right)$$

(avec une graduation pondérée sur Proj*). Et la variété $\mathcal{M}_2$ peut être vue comme une sous-variété de l'espace affine sur $\mathbb{Z}$ de dimension dix et pas moins.*

En caractéritique 2, l'espace tangent de la variété $\mathcal{M}_2 \otimes \Bbbk$ au point singulier ($J_2 = J_6 = J_8 = 0$) est de dimension 10.

Démonstration. Aller à [51, Théorème 2 et Théorème 6]. □

Corollaire 4.2.2. *Nous notons par $\gamma_i(\mathcal{C})$ l'evaluation de γ_i sur le model de représentation de $\mathcal{C}$.*

— *Ainsi pour une courbe $\mathcal{C}$ définie sur un corps de nombre $\mathbb{K}$, $\mathcal{C}$ a une bonne réduction pour un premier $\mathfrak{p}$ de $\mathbb{K}$ si et seulement si :*

$$ord_{\mathfrak{p}}\left(\gamma_i(\mathcal{C})\right) \geq 0, \quad i = 1, \cdots, 10.$$

— *Et pour $\mathcal{C}_1$ et $\mathcal{C}_2$ des courbes sur $\overline{\mathbb{k}}$, alors :*

$$\begin{aligned} \mathcal{C}_1 \simeq \mathcal{C}_2 \iff & \quad (\gamma_1(\mathcal{C}_1), \cdots, \gamma(\mathcal{C}_1)) = (\gamma_1(\mathcal{C}_2), \cdots, \gamma(\mathcal{C}_2)) \\ \iff & \quad (J_2(\mathcal{C}_1) : J_4(\mathcal{C}_1) : J_6(\mathcal{C}_1) : J_8(\mathcal{C}_1) : J_{10}(\mathcal{C}_1)) = \\ & \quad (J_2(\mathcal{C}_2) : J_4(\mathcal{C}_2) : J_6(\mathcal{C}_2) : J_8(\mathcal{C}_2) : J_{10}(\mathcal{C}_2)) \end{aligned}$$

(avec graduations pondérées).

4.3 CLASSES D'ISOMORPHISMES ET INVARIANTS ABSOLUS

On dit qu'un triplet d'invariants (i_1, i_2, i_3) constitue un triplet d'invariants absolus pour $\mathcal{M}_2$ s'il engendre le corps de fonctions $\mathbb{k}(\mathcal{M}_2 \otimes \mathbb{k})$. De manière équivalente, un tel triplet d'invariants définit un morphisme birationnel $\mathcal{M}_2 \otimes \mathbb{k} \to \mathbb{A}^3_{\mathbb{k}}$, ainsi il définit des coordonnées sur un ouvert U de $\mathcal{M}_2 \otimes \mathbb{k}$. Les invariants absolus sont de degré nul (sous forme de quotients d'invariants de même degré). Nous dirons que le triplet d'invariants (i_1, i_2, i_3) est bien défini en $\mathcal{C}$ si son évaluation en $\mathcal{C}$ correspond à un point géométrique de U. C'est une propriété plus forte que celle de: i_j n'ayant juste pas de pôles à $\mathcal{C}$, on voudrait aussi que la classe birationnale de $\mathcal{C}$ puisse être récupérée à partir de $(i_1(\mathcal{C}), i_2(\mathcal{C}), i_3(\mathcal{C}))$, ou de manière équivalente par le théorème 4.2.1, que $(J_2(\mathcal{C}) : J_4(\mathcal{C}) : J_6(\mathcal{C}) : J_8(\mathcal{C}) : J_{10}(\mathcal{C}))$ peut être réconstitué.
Par exemple un système standard d'invariants utilisé pour le calcul des polynômes de classe ou de polynômes modulaires était

$$\left(I_2^5 / I_{10}, I_2^3 I_4 / I_{10}, I_2^2 I_6 / I_{10}\right)$$

et le U correspondant est $I_2 \neq 0$.

Pour décrire les espaces $\mathcal{M}_2 \otimes \mathbb{k}$, nous avons besoin de système d'invariants. Nous dirons qu'un tel système d'invariants $\{i, i', i'' \dots\}$ est récouvrement complet si ces invariants définissent des coordonnées sur une stratification de $\mathcal{M}_2 \otimes \mathbb{k}$. D'une manière spécifique, on utilise un système d'invariants absolus i sur un U_0 ouvert, puis un autre ensemble d'invariants i' sur un U_1 ouvert de $\mathcal{M}_2 \otimes \mathbb{k} \setminus U_0$, et ainsi de suite. Dans ce cas i_1 n'a pas besoin d'être un invariant absolu puisque nous avons seulement besoin qu'il soit défini sur un sous-schéma localement fermé plutôt que sur un sous-schéma ouvert. Et on aura seulement besoin qu'il induise un isomorphisme de U_1 vers un ouvert de $\mathbb{A}^{m_1}_{\mathbb{k}}$. Par exemple en caractéristique 2 on allège cette dernière condition à un morphisme universellement injectif sur U_1.

On dit qu'un système de recouvrement complet d'invariants est optimal s'il induit une bijection $\mathcal{M}_2 \otimes \mathbb{k} \longmapsto \mathbb{A}^3_{\mathbb{k}}$ (il faudrait remarquer, que puisque le système est défini sur une stratification, l'application n'est pas un morphisme).

4.3.1 *En Caractéristique Différente de* 2

On peut utiliser les invariants arithmétiques J_{2i} pour définir des invariants absolus comme dans [10, § 1], d'où des coordonnées sur l'espace des modules. Sachant que l'invariant J_{10} définit le discriminant de la courbe, donc n'est pas nul, on obtient que:

— La classe des courbes de genre 2 avec un J_2 non nul, est un ensemble ouvert de $\mathcal{M}_2$ sur lequel nous avons comme coordonnées le triplet des invariants absolus:

$$\left(J_2^5/J_{10}, J_2^3J_4/J_{10}, J_2^2J_6/J_{10}\right).$$

— Les courbes de genre 2 qui s'annulent en J_2 avec un J_4 non nul, est un sous-espace de $\mathcal{M}_2$ où les coordonnées peuvent être définies par:

$$\left(0, J_4^5/J_{10}^2, J_4J_6/J_{10}\right).$$

— Les autres courbes se trouvent dans un ensemble avec des coordonnées définies par:

$$\left(0, 0, J_6^5/J_{10}^3\right).$$

Il en découle que l'ensemble des points de $\mathcal{M}_2 \otimes \mathbb{k}$ est en bijection avec l'ensemble des triplets définis précédemment, donc en bijection avec $\mathbb{A}^3_{\mathbb{k}}$. En d'autres termes, ces invariants (k_1, k_2, k_3) sur la stratification définis précédemment sont optimaux.

Remarque 4.3.1. Réciproquement, nous pouvons récouvrir les J_{2i} projectifs à partir de n'importe quel triplet $(k_1, k_2, k_3) \in \mathbb{A}^3_{\mathbb{k}}$ (un point de $\mathcal{M}_2 \otimes \mathbb{k}$) en utilisant le chemin suivant de [10, Lemme 1]:

$$(J_2, J_4, J_6, J_{10}) = \begin{cases} (k_1, k_1k_2, k_1^2k_3, k_1^4), & \text{si} \quad k_1 \neq 0, \\ (0, k_2, k_2k_3, k_2^2), & \text{sinon-si if} \quad k_1 = 0,\ k_2 \neq 0, \\ (0, 0, k_3^2, k_3^3), & \text{autrement.} \end{cases}$$

4.3.2 *En Caractéristique* 2

Nous rappelons que toute courbe hyperelliptique du genre 2 est birationnellement équivalente à l'un des trois types suivants selon le nombre et le degré des points de Weierstrass ramifiés:

$$Y^2 - Y = \begin{cases} \alpha X + \beta X^{-1} + \gamma(X-1)^{-1}, & (1,1,1) \\ X^3 + \alpha X + \beta X^{-1}, & (3,1) \\ X^5 + \alpha X^3, & (5) \end{cases}$$

Lorsque $\mathbb{k}$ a q éléments, le nombre $\overline{\mathbb{k}}$-classes d'isomorphisme des courbes projectives lisses du genre 2 défini sur $\mathbb{k}$ est donné dans le tableau suivant selon le type ([33, Théorème 20]): On considère la forme normale associée à une courbe de genre 2 en caractéristique 2.

Type	Nombre
$(1,1,1)$	$q^3 - q^2$
$(3,1)$	$q^2 - q$
(5)	q

TABLE 4.1 – Nombre de classes d'isomorphisme selon le type sur $\mathbb{F}_{2^n}$.

$$XY^2 + (1 + aX + bX^2)Y + X^2(c + dX + X^2) = 0.$$

• Si ab est différent de 0, nous obtenons trois points Weierstrass (comme expliquer plus haut): le point à l'infini et deux autres points donnés par l'équation: $1 + aX + bX^2 = 0$. Cela correspond au type $(1,1,1)$. On peut mettre l'équation sous la forme: $y^2 - y = R(x)$ en la multipliant par $X(1 + aX + bX^2)^{-2}$ puis en remplaçant Y par $X(1 + aX + bX^2)^{-1}Y$. Après un changement de variable dans [51, § 3] (un peu technique), comprenant une action $Y \mapsto Y + B(X)$ du groupe d'Artin-Schreier et une action linéaire sur X, on peut obtenir:

$$\alpha = ab^{-3}, \tag{4.2}$$

$$\beta = a^{-3}b\xi^{-2}\left(c + \xi^{-2} + a(c\xi + d + \xi^{-1})^{1/2}\right), \tag{4.3}$$

$$\gamma = a^{-3}b\eta^{-2}\left(c + \eta^{-2} + a(c\eta + d + \eta^{-1})^{1/2}\right) \tag{4.4}$$

tel que $\xi + \eta = a$, $\eta\xi = b$;
• Mais si a ou b est différent de zéro et $ab = 0$, cela correspond au type $(3,1)$; et si $a \neq 0$ et $b = 0$, on peut transformer:

$$XY^2 + (1 + aX + bX^2)Y + X^2(c + dX + X^2) = 0$$

en

$$Y^2 - Y = X^3 + \alpha X + \beta X^{-1}$$

où

$$\alpha = a^{5/3}\left(a^{-3}c + (a^{-5} + a^{-4}d)^{1/2}\right), \tag{4.5}$$

$$\beta = a^{-5/3}\left(a^{-5} + a^{-3}c + (a^{-5} + a^{-4}d + a^{-3}c)^{1/2}\right). \tag{4.6}$$

Si $b \neq 0$ et $a = 0$, nous obtenons α, β en termes de b, c, d via une expréssion plus compliquée pour laquelle nous nous référons à Igusa [51, § 3].
• Le type (5) correspond à $a = b = 0$ et la forme normale associée $XY^2 + Y + X^2(c + dX + X^2) = 0$ peut être transformée en $Y^2 - Y = X^5 + \alpha X^3$ avec $\alpha = c$.

Nous désignons par $\mathcal{M}_2[J_2^{-1}] \otimes \Bbbk$ l'ouvert de dans $\mathcal{M}_2 \otimes \Bbbk$ constitué des courbes birationales équivalentes aux courbes de type $(1,1,1)$. Il est caractérisé par la non-annulation de J_2 modulo 2, et peut être défini à l'aide des trois invariants arithmétiques absolus suivants:

$$\mathfrak{a}_1 = J_4/J_2^2, \quad \mathfrak{a}_2 = J_8/J_2^4 \text{ et } \mathfrak{a}_3 = J_{10}/J_2^5.$$

En outre on peut récouvrir ces invariants à partir des coefficients de la forme normale en utilisant la rélation suivante [51, § 3]:

$$\begin{cases} \alpha^2 + \beta^2 + \gamma^2 &= J_4/J_2^2, \\ \alpha^2\beta^2\gamma^2 &= J_{10}/J_2^5, \\ \alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2 &= J_8/J_2^4 + (J_4/J_2^2)^3 + (J_4/J_2^2)^4 \end{cases} \tag{4.7}$$

Alors on remarque que les invariants birationnels $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3$ sont totalement définis en fonction des trois invariants symétriques standards: $\alpha + \beta + \gamma$, $\alpha\beta + \beta\gamma + \gamma\alpha$, $\alpha\beta\gamma$, ces derniers sont également utilisés par Cardona et al. dans [33, § 2] pour définir des invariants: bien qu'ils soient ramifiés sur les invariants symétriques. Dès lors il y a des avantages très importants à travailler avec le système de trois invariants $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3$: puisqu'ils proviennent de fonctions modulaires sur $\mathbb{C}$ et sont en fait définis sur $\mathbb{Z}$. Par contre, les invariants symétriques

ne peuvent être relevés en formes modulaires (sans caractères) en caractéristique 0. Plus précisément, il est démontré dans le théorème 4.3.2 que ces invariants décrivent $\mathcal{M}_2[J_2^{-1}]$ sur $\mathbb{Z}$. En particulier, sur $\mathbb{Z}_2$ ces invariants décrivent l'ensemble ouvert $\mathcal{M}_2[J_2^{-1}]$ de $\mathcal{M}_2$ qui se réduit à $\mathcal{M}_2[J_2^{-1}] \otimes \Bbbk$ modulo 2, c'est-à-dire des courbes avec une bonne réduction modulo 2, et dont la réduction est de type $(1,1,1)$.

Le type $(3,1)$ est caractérisé par $J_2 = 0$ et la non-annulation de J_6 sur $\Bbbk$, cela correspond à un sous-schéma fermé de $\mathcal{M}_2[J_6^{-1}] \otimes \Bbbk$, d'où un sous-schéma localement fermé dans $\mathcal{M}_2 \otimes \Bbbk$, de courbes birationnellement équivalentes à ce type. Les coordonnées de ce sous-schéma sont définies à l'aide du triplet d'invariants absolus suivant: $(0,\ J_8J_{10}/J_6^3,\ J_{10}^3/J_6^5)$. En outre à partir de la section 4.3.2, on retrouve ce triplet en utilisant les rélations suivntes:

$$\begin{cases} \alpha^6 &= J_8^{3/4}/J_6^1, \\ \beta^6 &= J_{10}^3/J_6^5, \\ \alpha^2\beta^2 &= J_8^{1/4}J_{10}/J_6^2. \end{cases} \tag{4.8}$$

Et les invariants birationnels sont donnés par: $\alpha^3, \alpha\beta$ dans [51, §2].

Le type (5) est caractérisé par $J_2 = J_6 = 0$. Le sous-ensemble fermé correspondant de $\mathcal{M}_2 \otimes \Bbbk$, peut être défini en utilisant le triplet d'invariants $(0,0,J_8^5/J_{10}^4)$. Et nous avons la rélation suivante:

$$\left\{ \alpha^{10} = J_8^{5/4}/J_{10}. \right. \tag{4.9}$$

Et α^5 est un invariant birationnel d'aprés [51, § 2].

Nous déduisons de cette discussion, que les systèmes d'invariants:

$(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3) = (J_4/J_2^2, J_8/J_2^4, J_{10}/J_2^5)$ lorsque $J_2 \neq 0$,
$(0,\ J_8J_{10}/J_6^3,\ J_{10}^3/J_6^5)$ lorsque $J_2 = 0, J_6 \neq 0$,
et $(0,0,J_8^5/J_{10}^4)$

induisent une bijection entre l'ensemble des points de $\mathcal{M}_2 \otimes \Bbbk$ et $\mathbb{A}^3_{\Bbbk}$, sont donc optimaux. En effet les formules ci-dessus montre comment récouvrir les α, β, γ à partir de ces invariants. Un inconvénient par rapport aux invariants optimaux définis ci-dessus en caractéristique différente de 2 est qu'ils ne partagent pas de dénominateur commun. Il sérait intéressant de combiner les deux versions pour avoir des invariants optimaux valables à la fois pour toute caractéristique.

4.3.3 *Invariants Absolus pour toute Caractéristique*

Un système standard d'invariants utilisé pour le calcul des polynômes de classe ou modulaires était ceux d'Igusa $\left(I_2^5/I_{10},\ I_2^3I_4/I_{10},\ I_2^2I_6/I_{10}\right)$ introduits plus haut. Pour réduire la taille de ces polynômes, Streng a introduit dans [113] les invariants absolus I_4I_6'/I_{10}, $I_2I_4^2/I_{10}$, I_4^5/I_{10}^2 où $I_6' = 1/2(I_2I_4 - 3I_6)$ pour un ouver U donné par $I_4 \neq 0$. Ces choix d'invariants correspondent à une belle caractérisation par des formes modulaires définies en termes de constantes thêta (aller à la section 4.6 pour plus détails).

Cependant ces invariants ne se réduisent pas bien modulo 2 et modulo 3. Même si leurs réductions existent, ils ne définissent pas des invariants absolus sur $\mathcal{M}_2 \otimes \Bbbk$ pour ces caractéristiques. Et nous avons à partir de [51, Theorem 4] que:

— Si $\mathrm{char}(\Bbbk) \neq 2$, la variété $\mathcal{M}_2 \otimes \Bbbk$ admet un et un seul point singulier, ce qui correspond à $J_2 = J_6 = J_8 = 0$.

— Si $\mathrm{char}(\Bbbk) = 2$, le lieu des points singuliers de $\mathcal{M}_2 \otimes \Bbbk$ est une courbe rationnelle correspondant à $J_2 = J_6 = 0$ autrement dit les courbes de type (5) n'ayant qu'un seul point Weierstrass.

Nous allons par suite introduire un système de trois invariants pour chacun des trois ouverts: $\mathcal{M}_2[J_2^{-1}]$, $\mathcal{M}_2[J_4^{-1}]$, $\mathcal{M}_2[J_6^{-1}]$, $\mathcal{M}_2[J_8^{-1}]$ dans $\mathcal{M}_2$ sur $\mathbb{Z}$. Ces ouverts se réduisent bien en toute caractéristique sur un recouvrement de $\mathcal{M}_2 \otimes \Bbbk$, excepter pour la seule courbe $\mathcal{C}_0$ définie par: $J_2 = J_4 = J_6 = J_8 = 0$. Une équation de cette courbe est donnée par $\mathcal{C}_0 : \ y^2 + y = x^5$ sur $\mathbb{Q}$, qui a potentiellement une bonne réduction partout [92, Exemple 1], et elle se réduit modulo 2 sur la courbe de type (5) avec $\alpha = 0$.

Les trois ouverts $\mathcal{M}_2[J_2^{-1}]$, $\mathcal{M}_2[J_4^{-1}]$, $\mathcal{M}_2[J_6^{-1}]$ sont suffisants pour recouvrir $\mathcal{M}_2 \otimes \Bbbk$ en caractéristique différente de 2, moins le seul point non lisse $\mathcal{C}_0$ défini précédemment. En caractéristique 2, le premier ouvert correspond aux courbes de type $(1,1,1)$, et le troisième ouvert contient les courbes de type $(3,1)$. Nous ne pouvons espérer que les trois invariants sur le dernier ouvert puisse définir un isomorphisme avec un ouvert de $\mathbb{A}^3$ (car $\mathcal{M}_2[J_8^{-1}]$ contient les points singuliers).

En résumé, on peut remarquer que nos choix de récouvrement et d'invariants absolus est particulièrement bien adapté à la réduction d'une courbe en $\mathcal{M}_2 \otimes \mathbb{Z}_{(2)}$ (et respectivement en $\mathcal{M}_2 \otimes \mathbb{Z}_{(3)}$). D'où, en particulier en caractéristique deux (respectivement trois) et zéro, et encore plus précisément pour représenter les relevés sur $\mathbb{Z}_q$ des courbes de genre 2 définies sur $\mathbb{F}_q$, avec $q = 2^n$ (et respectivement $q = 3^n$). Ces situations ne peuvent être couvertes par les invariants habituels comme ceux d'Igusa et ceux de Streng. Alors nous utiliserons plus bas les invariants pour construire des algorithmes de calculs de relevés pour les courbes de genre 2 ordinaires en caractéristique 2 et 3.

Théorème 4.3.2. *Nous pouvons associer à chacun des récouvrements affines définis précédement, un système de trois invariants comme suite:*

— $\mathfrak{a}_1 = J_4/J_2^2$, $\mathfrak{a}_2 = J_8/J_2^4$ *et* $\mathfrak{a}_3 = J_{10}/J_2^5$ *pour* $\mathcal{M}_2[J_2^{-1}]$,

— $\mathfrak{d}_1 = J_2^2/J_4$, $\mathfrak{d}_2 = J_6^2/J_4^3$ *et* $\mathfrak{d}_3 = J_{10}^2/J_4^5$ *pour* $\mathcal{M}_2[J_4^{-1}]$,

— $\mathfrak{u}_1 = J_4^3/J_6^2$, $\mathfrak{u}_2 = J_8J_{10}/J_6^3$, *et* $\mathfrak{u}_3 = J_{10}^3/J_6^5$ *pour* $\mathcal{M}_2[J_6^{-1}]$,

— $\mathfrak{w}_1 = J_2^4/J_8$, $\mathfrak{w}_2 = J_6^4/J_8^3$, *et* $\mathfrak{w}_3 = J_{10}^4/J_8^5$ *pour* $\mathcal{M}_2[J_8^{-1}]$.

tels que ces invariants induisent un isomorphisme de $\mathcal{M}_2[J_2^{-1}]$, $\mathcal{M}_2[J_4^{-1}]$ et $\mathcal{M}_2[J_6^{-1}]$ avec l'ouvert standard de $\mathbb{A}^3$ défini par $\mathfrak{a}_3^{-1}$, $\mathfrak{d}_3^{-1}$, $\mathfrak{u}_3^{-1}$ respectivement, sur $\mathbb{Z}$, $\mathbb{Z}[1/2]$ et $\mathbb{Z}$ respectivement.

Le dernier système d'invariants défini un récouvrement de $\mathcal{M}_2[J_8^{-1}]$ vers l'ouvert standard $\mathbb{A}^3[\mathfrak{w}_3^{-1}]$ sur $\mathbb{Z}$. Et en caractéristique 2, ils se restreignent sur l'ensemble des points singuliers $J_2 = J_6 = 0$ vers un morphisme radiciel avec image $\mathbb{A}^1_{\Bbbk} \setminus \{0\}$.

Démonstration. La bonne réduction des invariants J_{2i} implique celle de ces invariants. Il nous reste à démontrer que ces invariants définissent des coordonnées locales autrement dit qu'ils décrivent localement l'espace $\mathbb{Z}[\mathcal{M}_2]$. D'après les résultats de la section 4.2.2, il suffit de prouver que nous pouvons réconstituer tous les γ_i.

Nous allons procéder par calcul direct:

• Pour l'ouvert $\mathcal{M}_2[J_2^{-1}]$, nous exprimons les invariants γ_i en fonction de $\mathfrak{a}_1$, $\mathfrak{a}_2$ et $\mathfrak{a}_3$.

$$\gamma_1 = \frac{1}{\mathfrak{a}_3}, \quad \gamma_2 = \frac{\mathfrak{a}_1}{\mathfrak{a}_3}, \quad \gamma_3 = \frac{\mathfrak{a}_1^2}{\mathfrak{a}_3} + 4\frac{\mathfrak{a}_2}{\mathfrak{a}_3}, \quad \gamma_4 = \frac{\mathfrak{a}_2}{\mathfrak{a}_3}, \quad \gamma_5 = \frac{\mathfrak{a}_1^3}{\mathfrak{c}} + 4\frac{\mathfrak{a}_1\mathfrak{a}_2}{\mathfrak{a}_3},$$

$$\gamma_6 = \frac{\mathfrak{a}_1\mathfrak{a}_2^2}{\mathfrak{a}_3^2}, \quad \gamma_7 = \frac{\mathfrak{a}_1^4\mathfrak{a}_2}{\mathfrak{a}_3^2} + 8\frac{\mathfrak{a}_1^2\mathfrak{a}_2^2}{\mathfrak{a}_3^2} + 16\frac{\mathfrak{a}_2^3}{\mathfrak{a}_3^2},$$

$$\gamma_8 = \frac{1}{\mathfrak{a}_3^3}\left(\mathfrak{a}_1^{10} + 20\mathfrak{a}_1^8\mathfrak{a}_2 + 160\mathfrak{a}_1^6\mathfrak{a}_2^2 + 640\mathfrak{a}_1^4\mathfrak{a}_2^3 + 1280\mathfrak{a}_1^2\mathfrak{a}_2^4 + 1024\mathfrak{a}_2^5\right),$$

$$\gamma_9 = \frac{1}{\mathfrak{a}_3^3}\left(\mathfrak{a}_1^2\mathfrak{a}_2^3 + 4\mathfrak{a}_2^4\right), \quad \gamma_{10} = \frac{\mathfrak{a}_2^5}{\mathfrak{a}_3^4}.$$

Cette conversion a un sens sur $\mathbb{Z}$. Alors

$$\mathcal{M}_2[J_2^{-1}] = \mathrm{Spec}\left(\mathbb{Z}[\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3][\mathfrak{a}_3^{-1}]\right)$$

et $\mathcal{M}_2[J_2^{-1}]$ est un sous espace de $\mathcal{M}_2$ de dimension trois sur $\mathbb{Z}$.

• Sur $\mathbb{Z}[1/2]$, les invariants γ_i sont exprimés en fonction de $\mathfrak{d}_1$, $\mathfrak{d}_2$ et $\mathfrak{d}_3$ sur $\mathcal{M}_2[J_4^{-1}]$ comme suite:

$$\gamma_1 = \frac{\mathfrak{d}_1^5}{\mathfrak{d}_3}, \quad \gamma_2 = \frac{\mathfrak{d}_1^3}{\mathfrak{d}_3}, \quad \gamma_3 = \frac{\mathfrak{d}_1^2 s}{\mathfrak{d}_3}, \quad \gamma_4 = \frac{\mathfrak{d}_1^2\mathfrak{d}_2}{4\mathfrak{d}_3} - \frac{\mathfrak{d}_1}{4\mathfrak{d}_3}, \quad \gamma_5 = \frac{\mathfrak{d}_2}{\mathfrak{d}_3},$$

$$\gamma_6 = \frac{1}{16\mathfrak{d}_3^2}\left(\mathfrak{d}_1^2\mathfrak{d}_2^2 - 2\mathfrak{d}_1\mathfrak{d}_2 + 1\right), \quad \gamma_7 = \frac{1}{4\mathfrak{d}_3^2}\left(\mathfrak{d}_1\mathfrak{d}_2^3 - \mathfrak{d}_2^2\right), \quad \gamma_8 = \frac{\mathfrak{d}_2^5}{\mathfrak{d}_3^3},$$

$$\gamma_9 = \frac{1}{64\mathfrak{d}_3^3}\left(\mathfrak{d}_1^3\mathfrak{d}_2^4 - 3\mathfrak{d}_1^2\mathfrak{d}_2^3 + 3\mathfrak{d}_1\mathfrak{d}_2^2 - \mathfrak{d}_2\right),$$

$$\gamma_{10} = \frac{1}{1024\mathfrak{d}_3^4}\left(\mathfrak{d}_1^5\mathfrak{d}_2^5 - 5\mathfrak{d}_1^4\mathfrak{d}_2^4 + 10\mathfrak{d}_1^3\mathfrak{d}_2^3 - 10\mathfrak{d}_1^2\mathfrak{d}_2^2 + 5\mathfrak{d}_1\mathfrak{d}_2 - \mathfrak{d}_3^4\right).$$

• Pour le cas de $\mathcal{M}_2[J_6^{-1}]$, nous pouvons exprimer les γ_i en fonction de u_1, u_2 et u_3. Cette conversion a aussi sens sur $\mathbb{Z}$ et la sous-variété $\mathcal{M}_2[J_6^{-1}]$ de $\mathcal{M}_2$ est de dimension trois sur $\mathbb{Z}$.

$$\gamma_1 = \frac{1}{u_3^6}(u_3^5u_1^{10} + 20u_3^4u_2u_1^8 + 160u_3^3u_2^2u_1^6 + 640u_3^2u_2^3u_1^4 + 1280u_3u_2^4u_1^2 + 1024u_2^5),$$

$$\gamma_2 = \frac{1}{u_3^4}(u_3^3u_1^7 + 12u_3^2u_2u_1^5 + 48u_3u_2^2u_1^3 + 64u_2^3u_1),$$

$$\gamma_3 = \frac{1}{u_3^3}(u_3^2u_1^4 + 8u_3u_2u_1^2 + 16u_2^2), \quad \gamma_4 = \frac{1}{u_3^3}(u_3u_2u_1^2 + 4u_2^2),$$

$$\gamma_5 = \frac{u_1}{u_3}, \quad \gamma_6 = \frac{u_1u_2^2}{u_3^4}, \quad \gamma_7 = \frac{u_2}{u_3^3}, \quad \gamma_8 = \frac{1}{u_3^3}, \quad \gamma_9 = \frac{u_2^3}{u_3^6}, \quad \gamma_{10} = \frac{u_2^5}{u_3^9}.$$

• Pour le cas de $\mathcal{M}_2[J_8^{-1}]$, alors on arrive à exprimer les carrés des γ_i en fonction de $\mathfrak{w}_1$, $\mathfrak{w}_2$ et $\mathfrak{w}_3$.

$$\gamma_1^2 = \frac{\mathfrak{w}_1^{10}}{\mathfrak{w}_3^2}, \quad \gamma_2^2 = \frac{1}{\mathfrak{w}_3^2}\left(\mathfrak{w}_1^7\mathfrak{w}_2 - 4\mathfrak{w}_1^6\right), \quad \gamma_3^2 = \frac{\mathfrak{w}_1^4\mathfrak{w}_2^2}{\mathfrak{w}_3^2}, \quad \gamma_4^2 = \frac{\mathfrak{w}_1^2}{\mathfrak{w}_3^2},$$

$$\gamma_5^2 = \frac{1}{\mathfrak{w}_3^2}\left(\mathfrak{w}_1\mathfrak{w}_2^3 - 4\mathfrak{w}_2^2\right), \quad \gamma_6^2 = \frac{1}{\mathfrak{w}_3^4}\left(\mathfrak{w}_1\mathfrak{w}_2 - 4\right), \quad \gamma_7^2 = \frac{\mathfrak{w}_2^4}{\mathfrak{w}_3^4},$$

$$\gamma_8^2 = \frac{\mathfrak{w}_2^{10}}{\mathfrak{w}_3^6}, \quad \gamma_9^2 = \frac{\mathfrak{w}_2^2}{\mathfrak{w}_3^6}, \quad \gamma_{10}^2 = \frac{1}{\mathfrak{w}_3^8}.$$

Comme on peut le remarquer, nous ne pouvons faire mieux en caractéristique 2, puisque $\mathcal{M}_2[J_8^{-1}] \otimes \mathbb{k}$ contiennent le lieu $J_2 = J_6 = 0$ des points singuliers de l'ensemble des courbes de type (5). Si nous nous focalisons sur ce domaine en caractéristique 2, nous obtenons que $\mathfrak{w}_3 = \alpha^{-40}$. Comme α^5 est un invariant birationel sur ce lieu, on voit que les coordonnées $\mathfrak{w}_3$ induisent un récouvrement totalement ramifiée de degré 8 sur les courbes de type (5), excepter comme d'habitude, la courbe $\mathcal{C}_0 : \ y^2 - y = x^5$. □

4.4 CONSTRUCTION DE COURBES DE GENRE 2 À PARTIR D'INVARIANTS

4.4.1 *En Caractéristique* 2

À partir des invariants arithmétiques J_2 J_4, J_6, J_8 et J_{10} ou des triplets qu'ils définissent selon chaque type, nous pouvons déterminer une équation de la courbe en utilisant les rélations 4.7 et celles de la section 4.3.2 entre les coefficients des formes normales réduites et les triplets d'invariants absolus. Ainsi on arrive à construire une forme normale (ou un model hyperelliptique $y^2 + (1 + ax + bx^2)y = -x^3(c + dx + x^2)$) à partir des invariants J_{2i}. Réciproquement les rélations 4.7 offrent un passage d'une équation sous forme normale aux invariants absolus.

4.4.2 *Algorithme de Mestre*

Lorsque la caractéristique est différente de 2, pour construire une courbe à partir des invariants coordonnés de $\mathcal{M}_2(\Bbbk)$, J-F.Mestre propose dans [76] la méthode suivante dans le cas générique ($\mathrm{Aut}\,(\mathcal{C}) \simeq C_2$):
Soit $\mathcal{C} : y^2 = f(x)$ une courbe de genre 2 définie sur $\overline{\Bbbk}$ avec des invariants absolus sur $\Bbbk$ et $\mathrm{Aut}\,(\mathcal{C}) \simeq C_2$. On suppose $char\Bbbk \neq 2, 3, 5$ et on note F la sextique associée à f. On définit les invariants et covariants suivants où i et R les sont déjà dans le tableau 4.1.4:

$$Y_1 = (F, i)_4\,, \quad Y_2 = (i, Y_1)_2\,, \quad Y_3 = (i, Y_2)_2\,,$$

$$X_1 = (Y_2, Y_3)_1\,, \quad X_2 = (Y_3, Y_1)_1\,, \quad X_3 = (Y_1, Y_2)_1\,,$$

$$A_{ij} = (Y_1, Y_2)_2\,, \quad a_{ijk} = (F, Y_i)_2(F, Y_j)_2(F, Y_k)_2\,.$$

Ces covariants satisfont les relations suivantes :

$$\sum_{i,j=1}^{3} A_{ij}X_iX_j = 0\,, \quad \sum_{i,j,k=1}^{3} a_{ijk}X_iX_jX_k = R^3F\,,$$

Ce sont des polynômes en les variables x_1 et x_2 de la sextique F.
On considère aussi la conique L et la cubique M définies par :

$$L\ :\ \sum_{i,j=1}^{3} A_{ij}Y_iY_j\,, \quad M\ :\ \sum_{i,j,k=1}^{3} a_{ijk}Y_iY_jY_k\,.$$

Les coefficients A_{ij} et a_{ijk} sont des invariants de degré pairs alors ils admettent des expréssions polynômiales en les J_{2i}. Ainsi nous obtenons les coefficients des équations sur $\Bbbk$ de L et M en les J_{2i} (ou en les invariants j_i d'Igusa).
Si $L(\Bbbk)$ est non vide alors il existe une courbe $\mathcal{C}$ de genre 2 définie sur $\Bbbk$ dont les invariants déterminent les coefficients A_{ij} et a_{ijk} de L et de M.
Dans ce cas à partir d'un point $P \in L(\Bbbk)$ on peut paramétrer l'équation de L ce qui correspond au $\Bbbk$-isomorphisme de $\mathbb{P}^1$ dans L donné par :

$$(x_1, x_2) \mapsto (L_1(x_1, x_2),\ L_2(x_1, x_2),\ L_3(x_1, x_2))$$

On détermine une forme sextique de $\mathcal{C}$ sur $\Bbbk$ en mettant les équations L_i dans M.
Cette contruction marche bien en toute caractéristique differente de 2, 3 et 5 à cause de l'apparition de leurs multiples dans les dénominateurs des A_{ij} et a_{ijk}. On peut toute fois

corriger le problème en caractéristique 3 en multipliant par des entiers, les covariants et invariants pour avoir des coefficients entiers. Malheureusement cette méthode ne marche pas en caractérsitique 5, la conique obtenue est dégénérée [67].

Cependant, en caractéristique différente de 2, on peut toujours construire une forme de Rosenhain d'une courbe $\mathcal{C}$ de genre 2 à partir d'un triplet d'invariants (i_1, i_2, i_3) défini par exemple par le théorème 4.3.2. En effet les bijections définies soit par les invariants $\mathfrak{a}_i$ (ou soit $\mathfrak{d}_i$, $\mathfrak{u}_i$ et $\mathfrak{w}_i$) de ce théorème permettent de définir la solution unique correspondant à l'équation de la courbe $\mathcal{C}$. On peut calculer cette solution à partir d'un système polynômial en fonction des λ, ν et μ tel que $\mathcal{C} : y^2 = x(x-1)(x-\lambda)(x-\nu)(x-\mu)$ et les polynômes du système sont donnés par les $J_{2i}(\mathcal{C})$ et les valeurs (i_1, i_2, i_3) du triplet d'invariants.
Une autre approche est de déterminer la forme normale birationnellement équivalente à une forme de Rosenhain

$$\mathcal{C} : y^2 = (x-1)(x-2)(x-\lambda)(x-\nu)(x-\mu)$$

Alors on aura à déterminer les coefficients c et d sachant que $a = -3/2$ et $b = 1/2$ avec

$$\mathcal{C} : y^2 + (1 + ax + bx^2)y = -(1/4)x^3(c + dx + x^2)$$

Et par suite on arrive à déterminer c et d en utilisant les $J_{2i}(\mathcal{C})$ et les valeurs (i_1, i_2, i_3) du triplet d'invariants comme équations d'un système dont une solution complète les coefficients de la forme normale de $\mathcal{C}$. On peut ainsi couvrir les cas des caractéristiques 3 et 5.

4.4.3 *Courbes de Genre 2 et Invariants Thêta*

Soit $\mathcal{C}$ la courbe de genre 2 sur $\mathbb{C}$. Alors $\mathcal{C}$ est isomorphe via une transformation linéaire fractionnaire à une courbe de la forme :

$$y^2 = x(x-1)(x-\lambda)(x-\nu)(x-\mu)$$

et les λ, ν et μ sont appelés *invariants de Rosenhain de* $\mathcal{C}$. *Ces invariants sont des fonctions modulaires pour* $\Gamma_2(2)$.

$$\lambda = \frac{\theta_0^2\theta_1^2}{\theta_3^2\theta_2^2}, \qquad \mu = \frac{\theta_1^2\theta_{12}^2}{\theta_2^2\theta_{15}^2} \quad et \quad \nu = \frac{\theta_0^2\theta_{12}^2}{\theta_3^2\theta_{15}^2}.$$

D'autre part, les formules de Thomae [114] établissent des rélations entre les racines $\{0, 1, \lambda, \mu, \nu\}$ et les puissances quatrièmes des thêta constantes de niveau $(2, 2)$ de la matrice de période Ω associée à $\mathcal{C}$. Partant des racines $\{0, 1, \lambda, \mu, \nu\}$ dans cet ordre nous avons :

$$\left(\frac{\Theta_4}{\Theta_0}\right)^4 = \frac{\mu}{\lambda\nu} \qquad \left(\frac{\Theta_8}{\Theta_0}\right)^4 = \frac{\mu(\nu-1)(\lambda-\mu)}{\nu(\mu-1)(\lambda-\nu)}$$
$$\left(\frac{\Theta_1}{\Theta_0}\right)^4 = \frac{\mu(\nu-1)(\lambda-1)}{\lambda\nu(\mu-1)} \qquad \left(\frac{\Theta_2}{\Theta_0}\right)^4 = \frac{\mu(\lambda-1)(\nu-\mu)}{\lambda(\mu-1)(\nu-\lambda)}$$

Il en découle que *le corps des fonctions* $\Gamma_2(2)$*-modulaires est engendré par les invariants de Rosenhain.*
Lorsque l'on travaille sur $\mathbb{C}$ on peut déterminer les racines carrés des $\mathfrak{c}_i^2 = \theta_i^4(\Omega)/\theta_0^4(\Omega)$ avec $i \in \mathcal{P}_2$, en procédant par intégration numérique à faible précision. L'algorithme 4.4.1 dont les

Entrée: $(\alpha_1, \cdots, \alpha_6) \in \mathbb{C}^6$ où $\mathcal{C} : y^2 = (x-\alpha_1).\cdots.(x-\alpha_6)$.
Sortie: $(\mathfrak{c}_i(\Omega))_{i\in\mathcal{P}_2}$ à précision N, où $\Omega \in \mathcal{F}_2$ décrit (par équivalence) Jac $\mathcal{C}$.

1. Calculer la matrice Ω' associée à C (par intégration numérique à faible précision) sur la même base du groupe d'homologie que les formules de Thomae ;
2. Calculer $(\gamma, \Omega) \in \Gamma_2 \times \mathcal{F}_2$ tels que $\Omega = \gamma\Omega'$ avec l'algorithme 5 ;
3. Calculer les $\mathfrak{c}_i^2(\Omega')$ par les formules de Thomae à précision N ;
4. En déduire les $\mathfrak{c}_i^2(\Omega) = \mathfrak{c}_i^2(\gamma\Omega')$ par l'équation fonctionnelle ;
5. Calculer les $\mathfrak{c}_i(\Omega)$ à faible précision à partir de Ω et les thêta constantes comme séries de Fourier ;
6. En déduire les bonnes racines carrés $\mathfrak{c}_i(\Omega)$ à précision N en utilisant leurs approximations.

Algorithm 4.4.1 Évaluation des $\mathfrak{c}_i$ associés à une courbe de genre 2

---

détailles se trouvent dans [28] en est un exemple. Et l'avantage de cet algorithme est qu'elle tourne avec un nombre constant d'opérations à la précision N.
Cependant sur un corps fini, on détermine les thêta constantes de niveau n associées à une variété isomorphe à la Jacobienne de $\mathcal{C}$ [68]. Ces isomorphismes sont donnés par l'action de Γ_2 sur $\mathbb{C}^2 \times \mathfrak{H}_2$ définies par: pour $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ et $z \in \mathbb{C}^2$;

$$(z, \Omega) \mapsto (\gamma.z, \gamma.\Omega) = \left({}^t(C\Omega + D)^{-1}z,\ (A\Omega + B)(C\Omega + D)^{-1}\right)$$

On considère les sous groupes :

$$\Gamma_2'(n) = \{\gamma \in \Gamma_2,\ \gamma \equiv \pm \mathrm{Id}_4 \mod n\}$$

$$et \quad \Gamma_2'(n, 2n) = \left\{ \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_2,\ diag({}^tAC) \equiv diag({}^tBD) \equiv 0 \mod 2n \right\}.$$

Alors on montre que le sous groupe $\Gamma_2'(n)$ est celui des isomorphismes qui fixent les puissances $2n$-ième des thêta constantes de niveau (n, n) (modulo une constante) ; $\Gamma_2'(n, 2n)$ les puissances n-ième et $\Gamma_2'(n^2, 2n^2)$ les thêta constantes de niveau (n, n). Pour chaque thêta constante non nulle, il existe une matrice $\gamma \in \Gamma_2'(2, 4)$ changeant son signe et laissant fixe les autres thêta constantes de telle sorte que, chaque choix de racines carrés correspond à une variété isomorphe. Alors on peut faire un choix arbitraire des racines carrés sur les : $\left(\frac{\Theta_1}{\Theta_0}\right)^4$, $\left(\frac{\Theta_2}{\Theta_0}\right)^4$, $\left(\frac{\Theta_4}{\Theta_0}\right)^4$ et $\left(\frac{\Theta_8}{\Theta_0}\right)^4$. Les autres carrés des thêta constantes de niveau $(2, 2)$ sont :

$$\Theta_6^2 = \frac{1}{\nu}\frac{\Theta_0^2\Theta_2^2}{\Theta_4^2}, \qquad \Theta_{12}^2 = \frac{1}{\lambda}\frac{\Theta_0^2\Theta_8^2}{\Theta_4^2}, \qquad \Theta_3^2 = (\nu - 1)\frac{\Theta_4^2\Theta_6^2}{\Theta_1^2},$$

$$\Theta_9^2 = (\lambda - 1)\frac{\Theta_4^2\Theta_{12}^2}{\Theta_1^2} \quad et \quad \Theta_6^2 = \frac{\Theta_0^2\Theta_3^2 - \Theta_1^2\Theta_2^2}{\Theta_{12}^2}.$$

Jacobiennes Décomposables

Pour ce qui concerne le cas non générique, nous avons le théorème suivant.

Théorème 4.4.1. *Soit $\mathcal{C}$ une courbe de genre 2 admettant une involution non triviale. Alors il existe au plus deux courbes elliptiques quotient de degré 2 de sa Jacobienne à isomorphisme près. C'est-à-dire il existe une $(2, 2)$-isogénie entre* Jac$(\mathcal{C})$ *et le produit de ces deux courbes elliptiques.*

Dans ce cas on trouve dans [34] des formules algébriques réliant les modules de $\mathcal{C}$ au j-invariant des courbes elliptiques dont la Jacobienne de $\mathcal{C}$ est le produit.

4.5 CONVERSIONS FORME NORMALE ET MODÈLE HYPERELLIPTIQUE

4.5.1 *D'une Forme Normale à un Modèle Hyperelliptique*

Lorsque l'on part d'une forme normale associée à une courbe $\mathcal{C}$ de genre 2

$$XY^2 + (1 + aX + bX^2)Y + X^2(c + dX + X^2) = 0,$$

on peut se ramener sur un modèle hyperelliptique en fixant x différent de 0 et de ∞, alors de manière équivalente on a:

$$X^2Y^2 + (1 + aX + bX^2)XY + X^3(c + dX + X^2) = 0$$

alors en appliquant le changement $Y \longmapsto Y/X$ on obtient une équation:

$$Y^2 + h(X)Y = f(X) \quad \text{où} \quad h(X) = 1 + aX + bX^2 \quad \text{et} \quad f(X) = -X^3(c + dX + X^2)$$

Lorsque l'on considère deux courbes de genre 2: $\mathcal{C}_1$ et $\mathcal{C}_2$ données sur $\Bbbk$ respectivement par:

$$XY^2 + (1 + aX + bX^2)Y + X^2(c + dX + X^2) = 0$$

et

$$XY^2 + (1 + a'X + b'X^2)Y + X^2(c' + d'X + X^2) = 0$$

D'autre part, lorsque l'on considère leurs modèles hyperelliptiques sur $\Bbbk$ données respectivement par les équations :

$$y^2 + h_1(x)y = f_1(x) \quad et \quad y^2 + h_2(x)y = f_2(x).$$

Les deux courbes sont isomorphes sur $\Bbbk$ si et seulement si l'on pouvait passer d'une équation à l'autre à l'aide de la transformation définie par:

$$(x, y) \mapsto (u^2x + b, u^5y' + a_2x^2 + \cdots + a_1x + a_0)$$

avec $(a_2, \cdots, a_1, a_0, b, u) \in \Bbbk^4 \times \Bbbk$.
En caractéristique différente de 2, on pourra choisir un point de Weierstrass P et un non-point de Weierstrass Q tel que $Q + Q'$ appartient au système canonique sur chaque courbe. Lorsque ce choix est fixé, correspondant respectivement à $x = \infty$ et $x = 0$. Par conséquent, les cinq points de Weierstrass manquants correspondent aux valeurs de x auxquelles les équations quadratiques ci-dessus en Y ont des racines doubles, c'est-à-dire aux racines des équations:

$$(1 + aX + bX^2)^2 - 4X^3(c + dX + X^2) = 0$$

et

$$(1 + a'X + b'X^2)^2 - 4X^3(c' + d'X + X^2) = 0$$

Alors dans ce cas $\mathcal{C}_1$ et $\mathcal{C}_2$ seront isomorphes sur $\overline{\Bbbk}$ si et seulement si les six racines de ces équations (tous deux considérés comme des équations sextiques non homogènes,) sont projectivement équivalentes. Ce qui équivaut à l'existence d'une racine cinquième de l'unité ξ tel que un coefficients (a', b', c', d') correspondent aux coefficients de la forme $(\xi a, \xi^2 b, \xi^3 c, \xi^4 d)$.

4.5.2 *D'un Modèle Hyperelliptique à une Forme Normale*

Soit $\mathcal{C}$ une courbe de genre 2 sur un corps $\Bbbk$. On veut calculer à partir de son modèle hyperelliptique une équation normale de $\mathcal{C}$ c'est-à-dire les coefficients (a, b, c, d) tels que $\mathcal{C}$ soit défini sur $\Bbbk$ par:

$$XY^2 + (1 + aX + bX^2)Y + X^2(c + dX + X^2) = 0$$

Nous allons nous référer à [51, Pages 6-8] pour la conversion entre les modèles hyperelliptiques et les modèles d'Artin-Shreier.

Si la caractéristique de $\Bbbk$ *est* 2

On rappelle qu'en caractéristique 2, il existe une relation entre le modèle hyperelliptique et les coefficients (a, b, c, d) provenant des invariants J_{2i} via les fonctions symétriques sur α, β, γ (selon le type d'Artin-Shreier), que l'on peut expliciter comme suite.
Soit $y^2 + h(x)y = f(x)$ un model hyperelliptique de $\mathcal{C}$ sur $\Bbbk$. On calcule d'abord certains J_{2i} associés à $\mathcal{C}$ selon le besoin:
• Si $J_2 \neq 0$ alors $\mathcal{C}$ est ordinaire ce qui correspond au type $(1, 1, 1)$;
• Si $J_2 = 0$ et $J_6 \neq 0$ alors $\mathcal{C}$ est de p-rang 1 ce qui correspond au type $(3, 1)$;
• Pour les autres cas, $\mathcal{C}$ est de p-rang 2 et le model hyperelliptique correspondant se réduit en $y^2 + y = x^5 + a_3x^3$ ce qui correspond au type (5).
Pour cette classe de courbes, on a $(a, b, c, d) = (0, 0, a_3, 0)$ comme les coefficients d'une forme normale de $\mathcal{C}$ over $\Bbbk$.
Pour les deux premières classes, la stratégie est la même. Nous mettons en évidence un isomorphisme en considérant les points de Weierstrass non triviaux pour les deux modèles de $\mathcal{C}$. Dans le modèle hyperelliptique, elles correspondent aux solutions de l'équation $h(x) = 0$, et à un changement de variables près sur x nous pouvons les prendre non nulles.
•Par exemple, lorsque $J_2 \neq 0$, nous avons deux points de Weierstrass non triviaux avec les abscisses ξ et η, alors nous pouvons prendre: $b = 1/(\eta\xi)$ et $a = b(\xi + \eta)$. Pour calculer c et d on peut toujours utiliser les rélations 4.3.2 et 4.7 dans la section 4.2.
• Lorsque $J_2 = 0$ avec $J_6 \neq 0$ la courbe $\mathcal{C}$ admet un unique point de Weierstrass non trivial d'abscisse x_0. Alors on pourra prendre $a = 1/x_0$ et $b = 0$. Par suite on détermine c et d en utilisant les rélations 4.3.2 et 4.8 dans la section 4.2.

Si la caractéristique de $\Bbbk$ *est différente de* 2

Soit $y^2 = u \cdot (x - \alpha_1) \cdots (x - \alpha_5)$ le modèle hyperelliptique associée à $\mathcal{C}$ sur $\overline{\Bbbk}$, et supposons que tous les α_i sont différents de 0 et 1. D'après [51, Pages 6-8], il existe sur $\overline{\Bbbk}$ des a, b, c et d tels que les α_i soient solutions de l'équation:

$$(1 + aX + bX^2)^2 - 4X^3(c + dX + X^2) = 0.$$

En évaluant en les α_i, cela induit un système d'équation en les a, b, c et d (comme variables) ce qui est alors facile à résoudre.

Cependant nous pouvons aussi reconstituer la forme normale à partir d'un modèle hyperelliptique directement, sans calcul de point de Weierstrass.
Nous avons d'une part la décomposition suivante:

$$\begin{aligned} y^2 &= (1+ax+bx^2)^2 - 4x^3(c+dx+x^2) \\ &= -4x^5 + (b^2-4d)x^4 + (2ab-4c)x^3 + (a^2+2b)x^2 + 2ax + 1 \end{aligned}$$

tels que les paramètres a, b, c et d ont respectivement les poids 1, 2, 3 et 4.
Et d'autre part, en partant du model suivant associé à une courbe de genre 2:

$$y^2 = a_5x^5 + \cdots + a_1x + a_0 \quad \text{avec} \quad a_0, a_5 \quad \text{non nuls.}$$

En appliquant succéssivement les transformations: $y \longmapsto \sqrt{a_0}y$ et $x \longmapsto -\sqrt[5]{\frac{4a_0}{a_5}}.x$ à:

$$y^2 = a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

nous avons

$$y^2 = -4x^5 + \frac{a_4}{a_0}\left(\frac{4a_0}{a_5}\right)^{4/5}x^4 - \frac{a_3}{a_0}\left(\frac{4a_0}{a_5}\right)^{3/5}x^3 + \frac{a_2}{a_0}\left(\frac{4a_0}{a_5}\right)^{2/5}x^2 - \frac{a_1}{a_0}\left(\frac{4a_0}{a_5}\right)^{1/5}x + 1$$

Posons $\zeta = \sqrt[5]{\frac{4a_0}{a_5}}$, alors le quadruplet (a,b,c,d) est défini par:

$$a = -\frac{a_1}{2a_0}\zeta, \quad b = \left(\frac{a_2}{2a_0} - \frac{a_1^2}{8a_0^2}\right)\zeta^2,$$

$$c = \left(\frac{a_3}{4a_0} + \frac{a_1^3}{32a_0^3} - \frac{a_2a_1}{8a_0^2}\right)\zeta^3, \quad d = \left[\frac{1}{4}\left(\frac{a_2}{2a_0} - \frac{a_1^2}{8a_0^2}\right)^2 - \frac{a_4}{4a_0}\right]\zeta^4.$$

Comme pour le modèle hyperelliptique qui n'est pas lisse à l'infini, le modèle normal n'est pas lisse au point $(0:1:0)$. Par le même procédé dévéloppé dans la sous section précédente, le modèle normal est obtenu en réduisant un point de Weierstrass P et un non point de Weierstrass Q ensemble. Une fois que P et Q sont fixés, le modèle normal est unique sous l'action des transformations de la forme $(a',b',c',d') \longmapsto (a'\xi, b'\xi^2, c'\xi^3, d'\xi^4)$ tel que ξ est une racine cinquième de l'unité.

4.6 FORMES MODULAIRES VECTORIELLES ET COVARIANTS

Dans cette section nous discutons des interprétations algébriques de Katz des formes modulaires en tant que sections des représentations du fibré vectoriel de Hodge.
L'espace de modules grossier sur $\mathbb{Z}$ des courbes hyperelliptiques $\mathcal{M}_2$, admet un plongément (via le morphisme de Torelli) dans l'espace de modules grossier $\mathfrak{A}_2$ des schémas abéliens de dimension relative 2.

En général, lorsque l'on considère une représentation de dimension finie $\rho : \mathrm{GL}_2(\mathbb{C}) \to \mathrm{GL}(V)$, une forme modulaire (vectorielle) de Siegel de poids ρ est une fonction holomorphique $f : \mathfrak{H}_2 \to V$ satisfaisant: $f(\gamma\Omega) = \rho(C\Omega + D)f(\Omega)$ pour tout $\Omega \in \mathfrak{H}_2$ et $\gamma \in \Gamma_2$. Par conséquent une forme modulaire de Siegel f définie en la section 3.3 et la section 3.3.1 correspond ici au cas où V est de dimension 1 et on dit que f est de *valeur-scalaire*, dans

le cas contraire on dit que f de *valeur-vectorielle*. Comme toute représentation irréductible de $GL_1(\mathbb{C})$ est de dimension 1, seules les formes modulaires de Siegel à valeur scalaire se produisent dans le genre 1.
On note généralement $\det^k$ (avec $k \in \mathbb{Z}$) la représentation unidimensionnelle (pour $V = C$) où l'action d'une matrice $m \in \mathrm{GL}_2(\mathbb{C})$ est la multiplication par $\det(m)^k$. Alors pour toutes formes modulaires de Siegel f et g de poids respectifs $\det^k$ et $\det^l$, leur produit fg sera de poids $\det^{k+l}$. En dimension 2, il est montré que les représentations irréductibles sont exactement de la forme: $\det^k \mathrm{Sym}^n$ pour $k \in \mathbb{Z}$ et $n \in \mathbb{N}$. Sym^n est le n-ième puissance symétrique des représentations de $\mathrm{GL}_2(\mathbb{C})$ sur $\mathbb{C}^2$ donné sur $\mathbb{C}_n[x]$ (des polynômes de degré au plus n) par la relation:

$$\mathrm{Sym}^k(m)P(x) = (bx+d)^k P\left(\frac{ax+c}{bx+d}\right) \quad \text{pour tous}$$

$m = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{C})$ et $P \in \mathbb{C}[X]$ avec $\deg(P) \leq k$.

Par suite, lorsque f n'admet pas de pôle en $\Omega \in \mathfrak{H}_2$, pour toute surface abélienne complexe principalement polarisée $\mathcal{A}$ isomorphe à $\mathcal{A}_\Omega = \mathbb{C}^2/(\mathbb{Z}^2 + \Omega\mathbb{Z}^2)$ avec une base $\omega \in \Omega^1(\mathcal{A})$ on définit la quantité suivante:

$$f(\mathcal{A}, \omega) := \rho({}^t(m^{-1}))f(\Omega)$$

où $m \in \mathrm{GL}_2(\mathbb{C})$ est la matrice de changement de bases entre ω et la base canonique sur les formes différentielles $(2\pi i dz_1, 2\pi i dz_2)$ sur $\mathcal{A}_\Omega$. Et la matrice m dépend uniquement de $\mathcal{A}$, ω et Ω nous renvoyons à [98, §2.2] pour plus de détails sur cette construction.
Puisque le paramètre $(\mathcal{A}, \omega)$ est bien défini sur tout corps quelconque $\Bbbk$, lorsque f est définie sur un certain $\mathbb{Z}[1/N]$ (comme le montre ses coefficients de Fourier) avec $\mathrm{char}(k) \nmid N$, alors la quantité $f(\mathcal{A}, \omega)$ aura bien un sens sur $\Bbbk$.
D'autre part, lorsque $\mathcal{A}$ n'est pas un produit de courbes elliptiques on a :

$$\omega = m\eta^*(\omega(\Omega))$$

où η est un isomorphisme entre $\mathcal{A}$ et la surface complexe $\mathcal{A}_\Omega$ avec $\Omega \in \mathfrak{H}_2$ dont une base des différentielles $\omega(\Omega)$. Alors on obtient une courbe hyperelliptique sur $\mathbb{C}$ d'équation:

$$\mathcal{C}(\Omega) : \ y^2 = a_6(\Omega)x^6 + \cdots + a_1(\Omega)x + a_0(\Omega)$$

où les q-expansions des coefficients $a_i(\Omega)$ sont données par [98, Corollaire 3.9] (listés avec des degrés totaux inférieurs à 1.)
En particulier les équations d'une courbe hyperelliptique $\mathcal{C}$ de genre 2 fournissent des paires $(\mathcal{A}, \omega)$ tel que $\omega(\mathcal{C}) = (dx/y, xdx/y)$ soit une base de $\Omega^1(\mathrm{Jac}(\mathcal{C}))$ des formes différentielles sur la surface principallement polarisée $\mathrm{Jac}\,(\mathcal{C})$. Par conséquent à toute forme modulaire on pourra associer un covariant sur $\mathcal{C}$ en utilisant l'application définie par :

$$\mathrm{Cot}(f) : \mathcal{C} \mapsto f(\mathrm{Jac}\,(\mathcal{C}), \omega(\mathcal{C})),$$

à partir de laquelle on pourra exprimer $\mathrm{Cot}(f)$ en fonction des coefficients la courbe. Et l'on connait des méthodes de détermination de $\mathrm{Cot}(f)$ à partir de la q-expansion de f (aller à [98, § 3.3] pour plus détails). En d'autres termes, on peut regarder une forme modulaire comme une section d'une représentation de poids ρ du fibré vectoriel de Hodge sur $\mathfrak{A}_2$, et le tiré-en-arrière ("pullback" en anglais) du morphisme de Torelli $\mathcal{M}_2 \to \mathfrak{A}_2$ induit une section

de la représentation de poids ρ du fibré vectoriel de Hodge sur $\mathcal{M}_2$.
Par conséquent, étant donné f une fonction modulaire de Siegel de poids ρ, $\mathrm{Cot}(f)$ est un covariant fractionnaire (rationnelle en terme des coefficients de la courbe) de poids ρ.
À noter que $\mathrm{Cot}(f)$ est un covariant polynomial si et seulement si f n'admet pas de pôles au diviseur à l'infini dans $\overline{\mathfrak{A}_2}$ (une compactification toroïdale de $\mathfrak{A}_2$).
En particulier, si f est une forme modulaire, $\mathrm{Cot}(f)$ est un covariant polynomial selon le principe de Koecher.
Réciproquement, si F est un covariant fractionnaire, la fonction méromorphe $\Omega \mapsto F(\mathcal{C}(\Omega))$ est une forme modulaire de Siegel méromorphe bien définie f (du même poids) associé à F ; puisque $\mathcal{C}(\Omega)$ est exactement de poids $det^{-2}\,\mathrm{Sym}^6$. Et dans le cas où F est un polynôme, alors f est une forme modulaire s'il n'admet pas de pôles en Ω tel que $\chi_{10}(\Omega) = 0$.

En résumé, les représentations irréductibles sont de la forme $\det^k \mathrm{Sym}^n$ avec $k \in \mathbb{Z}$ et $n \in \mathbb{N}$. Lorsque l'on considère les paramètres: $m \in \mathrm{GL}_2(\Bbbk)$ et $u \in \Bbbk^*$ des isomorphismes entres les modèles $y^2 = f(x)$ de courbes hyperelliptiques alors en posant $u = \det(m)$, les transformations entre les équations sont données par $\det^2 \mathrm{Sym}^6$ et les bases de différentielles sont déterminées à une action près de la matrice m^{-t}. Dès lors les bases de $\Omega^1(\mathrm{Jac}\,(\mathcal{C})))$ sont déterminées à une transformation près donnée par ces changements de variables. Ainsi les équations hyperelliptiques représentent toutes les paires $(\mathcal{A}, \omega)$ où $\mathcal{A}$ n'est pas un produit de deux courbes elliptiques.
Par suite les covariants d'ordre n et de degré k selon la Théorie des Invariants de Hilbert abordée dans la section 4.1 correspondent aux covariants polynômials de poids $\det^{(k-n/2)} \mathrm{Sym}^n$.

Exemple 4.6.1. En particulier, les covariants polynômes J_{2i} ont l'interprétation suivante en terme de formes modulaires (nous utilisons ici les formes paraboliques standards χ_{10}, χ_{12} plutôt que celles normalisées de [98]):

$$\begin{aligned} -3\mathrm{Cot}(\chi_{12}/\chi_{10}) &= J_2, \\ 4\mathrm{Cot}(\psi_4) &= I_4, \\ 4\mathrm{Cot}(\psi_6) &= \frac{1}{2}(I_2 I_4 - 3I_6) = I_6', \\ -2^2\mathrm{Cot}(\chi_{10}) &= J_{10}. \end{aligned}$$

Alors on pourra exprimer les j-invariants $\mathfrak{j}_i$ définis dans le chapitre 3 et la section 3.3.1.3 en terme de quotients de covariants de même poids comme suite:

$$\begin{aligned} \mathrm{Cot}(\mathfrak{j}_1) &= \frac{1}{256 J_{10}} \left(J_2^5 - 60 J_4 J_2^3 + 216 J_6 J_2^2 + 864 J_4^2 J_2 - 5184 J_6 J_4 \right), \\ \mathrm{Cot}(\mathfrak{j}_2) &= \frac{1}{32 J_{10}} \left(J_2^5 - 48 J_4 J_2^3 + 576 J_4^2 J_2 \right), \\ \mathrm{Cot}(\mathfrak{j}_3) &= \frac{1}{16384 J_{10}^2} \Big(J_2^{10} - 120 J_4 J_2^8 + 5760 J_4^2 J_2^6 - 138240 J_4^3 J_2^4 + \\ &\qquad 1658880 J_4^4 J_2^2 - 7962624 J_4^5 \Big). \end{aligned}$$

5

CALCUL DE POLYNÔMES MODULAIRES EN DIMENSION DEUX

Dans ce chapitre nous abordons une généralisation des polynômes modulaires permettant une caractérisation des points (p, p)-isogènes sur l'espace de module des surfaces abéliennes principalement polarisés . Ces polynômes modulaires ont été évalués pour la première fois en fonction des invariants d'Igusa par Régit Dupont dans sa thèse de Doctorat [28]. Son algorithme fut ensuite étendu à d'autres invariants par d'autres auteurs.
Nous faisons une présentation générale des polynômes modulaires en dimension 2 ainsi que les principes d'évaluation utilisés en vue de les adapter à des évaluations en fonction des nouveaux invariants (le chapitre 4 et la section 4.3), ayant une bonne réduction en toute caractéristique. À la fin nous allons plus nous interesser aux améliorations proposées par Enea Milio [78].

5.1 MATRICE DE $\mathfrak{H}_2$ ASSOCIÉE À UNE COURBE HYPERELLIPTIQUE DE GENRE 2

5.1.1 *Évaluation des Thêta Constantes*

Dans la proposition suivante nous résumons quelques valeurs connues des theta constantes sur le domaine fondamental $\mathcal{F}_2$.

Proposition 5.1.1. *Soit $\Omega \in \mathcal{F}_2$:*

— *La plus petite valeur propre de* $\operatorname{Im}\Omega$ *notée $\lambda(\Omega)$ est telle que:*

$$\lambda(\Omega) \geq \frac{\sqrt{3}}{4}.$$

— *Pour tout $j \in \{0,1,2,3\}$, $|\theta_j(\Omega) - 1| \leq 0.405$.*
Et cela reste vrai pour tout $\alpha\Omega$ avec $\alpha > 1$.

— *Pour tous $j \in \{4,6\}$ et $k \in \{8,9\}$ avec $E = |2\exp(i\pi\Omega_1/2)|$ on a:*

$$\left|\frac{\theta_j(\Omega)}{2\exp(i\pi\Omega_1/4)} - 1\right| \leq |E| \quad et \quad \left|\frac{\theta_k(\Omega)}{2\exp(i\pi\Omega_3/4)} - 1\right| \leq |E|.$$

Démonstration. Aller à [28, Pages: 138-145] □

Par conséquent on montrent que :
• La fonction θ_{12} ne s'annule pas sur $\mathcal{F}_2$.
• θ_{15} est la seule thêta constante paire pouvant sannuler sur $\mathcal{F}_2$. Et il en découle le résultat suivant.

Proposition 5.1.2. *Soit $\Omega \in \mathfrak{H}_2$ et Ω' son représentant dans le domaine fondamental $\mathcal{F}_2$. Alors soit la matrice Ω' est diagonale auquel cas exactement une des thêtas constantes paire s'annule en Ω et avec aussi $\theta_{15}(\Omega') = 0$, soit Ω' n'est pas diagonale et dans ce cas aucune des thêtas constantes ne s'annule en Ω (ni en Ω' par l'équation fonctionnelle).*

5.1.2 *Applications de la Moyenne de Borchardt*

Cette partie s'intéresse en premier lieu au problème d'évaluation rapide avec une précision N d'une matrice de Riemann associée à une courbe hyperelliptique $\mathcal{C}$ de genre $g \geq 1$ donnée sous son model

$$\mathcal{C} : y^2 = \prod_{i=1}^{2g+2} (x - e_i).$$

Elle se refère sur une approche de Dupont [28] dont la complexité est $O(\mathcal{M}(N).\log N)$.

Suites de Borchardt

On considère toujours g un entier fixé ≥ 1 et on pose $\mathcal{I}_g = (\mathbb{Z}/2\mathbb{Z})^g$.
Soit $(a_v)_{v\in\mathcal{I}_g} \in \mathbb{C}^{2^g}$, on dit qu'un 2^g-uplet $(a'_v)_{v\in\mathcal{I}_g}$ est un itéré de Borchardt de $(a_v)_{v\in\mathcal{I}_g}$ s'il existe $(\alpha_v)_{v\in\mathcal{I}_g} \in \mathbb{C}^{2^g}$ tel que, pour tout $v \in \mathcal{I}_g$:

$$\alpha_v^2 = a_v \quad et \quad b_v = \frac{1}{2^g} \sum_{v_1+v_2=v} \alpha_{v_1}\alpha_{v_2}.$$

Où le 2^g-uplet (α_v) est le *choix de racines* correspondant à cette itération de Borchardt. Ce choix sera dit *bon* si pour tous $v_2, v_2 \in \mathcal{I}_g$ on a :

$$|\alpha_{v_1} - \alpha_{v_2}| < |\alpha_{v_1} - \alpha_{v_2}|.$$

Sinon le choix de racines sera dit *mauvais*.
Les choix $(\alpha_v)_{v\in\mathcal{I}_g}$ et $(-\alpha_v)_{v\in\mathcal{I}_g}$ conduisent au même itéré, ainsi on a au plus 2^{g-1} itéré possibles.
On appelle suite de Borchardt toute suite $(a_v^{(n)})_{v\in\mathcal{I}_g}$ tel que pour tout $n \in \mathbb{N}$, $(a_v^{(n+1)})_{v\in\mathcal{I}_g}$ est itéré de Borchardt de $(a_v^{(n)})_{v\in\mathcal{I}_g}$.
Lorsque $g = 1$ ces suites correspondent aux suites AGM.
Soit $(a_v^{(n)})_{v\in\mathcal{I}_g}$ une suite de Borchardt avec $(\alpha_v^{(n)})_{v\in\mathcal{I}_g}$ une suite de choix de racines associée. Alors il existe un unique $A \in \mathbb{C}$ tel que, pour tout $v \in \mathcal{I}_g$: la suite $(a_v^{(n)})$ tend vers A. De plus, $A = 0$ si et seulement si la suite $(\alpha_v^{(n)})$ contient une infinité de mauvais choix de racines [3, Théorème 7.1]. Alors le nombre A est appelé *moyenne de Borchardt* associée à la suite de Borchardt $(a_v^{(n)})_{v\in\mathcal{I}_g}$.
Et on a que A vérifie les propriétés suivantes pour un n fixé :

$$|A| \leq \max_{v\in\mathcal{I}_g} |a_v^{(n)}|, \qquad \mathrm{Re}(A) \geq \min_{v\in\mathcal{I}_g} \left(\mathrm{Re}\,(a_v^{(n)})\right)$$

$$et \qquad \min_{v\in\mathcal{I}_g} \left(\arg(a_v^{(n)})\right) \leq \arg(A) \leq \max_{v\in\mathcal{I}_g} \left(\arg(a_v^{(n)})\right).$$

avec $\mathrm{Im}\left(\alpha_v^{(n)}/\alpha_0^{(n)}\right) > 0$ en cas d'égalité.

Et pour la suite nous allons plus nous intéresser à la suite de Borchardt suivante :

Soit $(z_v)_{v\in\mathcal{I}_g\setminus\{0\}} \in \mathbb{C}^{2^g-1}$, on considère la suite de Borchardt $(a_v^{(n)})_{v\in\mathcal{I}_g}, n \in \mathbb{N}$ définie par $a_0^{(0)} = 1$, $a_v^{(0)} = z_v$ pour $v \in \mathcal{I}_g\setminus\{0\}$ et tel que l'on ait les formules de récurrence suivantes sur n :

$$a_0^{(n+1)} = \frac{1}{2^g} \sum_{v\in\mathcal{I}_g} a_v^{(n))} \quad et \quad a_0^{(n+1)} = \sum_{v_1+v_2=v} \alpha_{v_1}^{(n))}\alpha_{v_1}^{(n))}$$

Entrée: $(z_v)_{v\in\mathcal{I}_g\setminus\{0\}} \in \mathbb{C}^{2^g-1}$ tels que $\mathrm{Re}\,(z_v) > 0$, $\forall v$ et un entier N.

Sortie: A tel que $\left|\dfrac{A}{B_g\left((z_v)\right)} - 1\right| \leq 2^{-N}$.

1. $B = B\left(N+1, (z_v)\right)$; $\quad a_0 = 1$;
2. **Pour** $v \in \mathcal{I}_g\setminus\{0\}$ **Faire**;
   a. $a_v = z_v$;
3. **Pour** $n = 1$ **à** B **Faire**;
   a. **Pour** $v \in \mathcal{I}_g$ **Faire**
      i. $r_v = \sqrt{a_v}$ avec $\mathrm{Re}\,(r_v) > 0$;
      ii. $b_v = 0$;
   b. **Pour** $v \in \mathcal{I}_g$ **Faire**
      i. $b_0 = b_0 + a_v$
      ii. **Pour** $v \in \mathcal{I}_g$ **Faire** $\quad b_v = b_v + r_{v_1} r_{v+v_1}$;
   c. **Pour** $v \in \mathcal{I}_g$ **Faire**
      i. $a_v = b_v/2^g$;
4. **Retourner** a_0;

Algorithm 5.1.1 Evaluation de la Moyenne de Borchardt

---

où $\alpha_0^{(n)}$ est une racine carré quelconque de $a_0^{(n)}$ telle que pour tout $v \neq 0$, $\alpha_v^{(n)} = 0$ si $\alpha_0^{(n)} = 0$ ou si $a_v^{(n)} = 0$ et sinon c'est une racine carré de $a_v^{(n)}$ telle que : $\quad |\alpha_0^{(n)} - \alpha_v^{(n)}| \leq |\alpha_0^{(n)} + \alpha_v^{(n)}|$. On note par $B_g\left((z_v)_{v\in\mathcal{I}_g\setminus\{0\}}\right)$ la limite d'une telle suite.

Dans le cas où $g \leq 2$, la valeur de $B_g\left((z_v)_{v\in\mathcal{I}_g\setminus\{0\}}\right)$ ne dépend que de l'ensemble $\{z_v\}_{v\in\mathcal{I}_g\setminus\{0\}}$, ce qui n'est pas le cas pour $g > 2$.

Lorsque nous considérons $\mathrm{Re}\,(z_v) > 0$ pour tout $v \in \mathcal{I}_g\setminus\{0\}$; l'algorithme suivant la section 5.1.2 calcule $A = B_g\left((z_v)_{v\in\mathcal{I}_g\setminus\{0\}}\right)$ en prennant $a^{(B(N,(z_v)))}$ comme approximation de A avec une précision relative de N bits [28]. Où $B(N,(z_v))$ est définie par :

$$B(N,(z_v)) = \left\lceil \frac{\log\left(1-\frac{1}{2^g}\right)}{\log\frac{m_0}{7\Delta_0}} \right\rceil + N + 1 + \left\lceil \log\frac{M_0}{7m_0} \right\rceil$$

En utilisant la moyenne de Borchardt on déduit que pour tout $\Omega \in \mathfrak{H}_2$, la suite de Borchardt définie pour tout $n \in \mathbb{N}$ par :

$$(a_n, b_n, c_n, d_n) = \left(\frac{\theta_j^2(2^n\Omega)}{\theta_0^2(\Omega)}\right)_{j\in\{0,1,2,3\}}$$

converge vers $\dfrac{1}{\theta_0^2(\Omega)}$. Et dont tout choix de racines est bon lorsque $\Omega \in \mathcal{F}_2$. [78, Lemme 2.6.13] et [28, Proposition 9.1]. Ainsi il en découle que pour tout $\Omega \in \mathcal{F}_2$ on a :

$$B_2\left(\mathfrak{c}_1(\Omega),\, \mathfrak{c}_2(\Omega),\, \mathfrak{c}_3(\Omega)\right) = \frac{1}{\theta^2(\Omega)}. \tag{5.1}$$

Ce qui permet de determiner les carrés des thêta constantes à partir des $\mathfrak{c}_j$ et de la relation $\theta_j^2(\Omega) = \mathfrak{c}_j(\Omega)\theta_0^2(\Omega)$. Par suite on peut extraire la matrice Ω en utilisant le résultat suivant .

Proposition 5.1.3. *Pour tous $\Omega \in \mathcal{F}_2$ et $\gamma \in \{(\mathfrak{IM}_1)^2, (\mathfrak{IM}_2)^2, (\mathfrak{IM}_3)^2\}$,*

$$B_2\left(\mathfrak{c}_1(\gamma\Omega), \mathfrak{c}_2(\gamma\Omega), \mathfrak{c}_3(\gamma\Omega)\right) = \frac{1}{\theta^2(\gamma\Omega)}$$

Démonstration. Voir [58, Lemme 4.2.]. □

Ce qui permet d'étendre le domaine de *bon choix des racines* dans l'utilisation du résultat précédent 5.1.
Lorsque l'on pose : $\Omega = \left(\begin{smallmatrix} \Omega_1 & \Omega_2 \\ \Omega_2 & \Omega 3 \end{smallmatrix}\right) \in \mathfrak{H}_2$, on en déduit que :

$$\Omega_1 = i.\left[\theta_4^2(\Omega) B_2\left(\frac{\theta_0^2(\Omega)}{\theta_4^2(\Omega)}, \frac{\theta_0^2(\Omega)}{\theta_4^2(\Omega)}, \frac{\theta_0^2(\Omega)}{\theta_4^2(\Omega)}\right)\right]^{-1},$$

$$\Omega_3 = i.\left[\theta_8^2(\Omega) B_2\left(\frac{\theta_9^2(\Omega)}{\theta_8^2(\Omega)}, \frac{\theta_0^2(\Omega)}{\theta_8^2(\Omega)}, \frac{\theta_1^2(\Omega)}{\theta_8^2(\Omega)}\right)\right]^{-1},$$

$$\Omega_2^2 - \Omega_1\Omega_3 = \left[\theta_4^2(\Omega) B_2\left(\frac{\theta_0^2(\Omega)}{\theta_4^2(\Omega)}, \frac{\theta_0^2(\Omega)}{\theta_4^2(\Omega)}, \frac{\theta_0^2(\Omega)}{\theta_4^2(\Omega)}\right)\right]^{-1}.$$

Alors pour $\Omega \in \mathcal{F}_2$ on a $\operatorname{Im}\Omega_2 > 0$ ce qui permet de determiner la bonne racine carré de Ω_2^2. D'autres variantes de cet algorithmes n'utilisant pas le résultat 5.1.3 sont décrites dans [28, Pages 200-201].

5.2 POLYNÔMES MODULAIRES DE SIEGEL

Cette section introduit les polynômes modulaires de Siegel et décrit le principe de calcul de ces polynômes en dimension 2 pour des systèmes d'invariants quelconques en se réferant à [28, 78]. Ces résultats seront utilisés pour caractériser les *conditions de Kronecker* sur l'espace de Siegel (la section 7.1 et la section 7.1.1) . Et une variante de l'algorithme décrit s'étend aux calculs de polynômes modulaires en fonction des invariants introduits dans le chapitre 4, la section 4.2 et le théorème 4.3.2.

5.2.1 *Polynômes Modulaires pour $\Gamma_0(p)$*

On considère un entier premier p. On définit le groupe modulaire $\Gamma_0(p)$ par :

$$\Gamma_0(p) := \left\{\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_2;\ C \equiv 0 \mod p\right\}.$$

Alors on montre [28], que $[\Gamma_2 : \Gamma_0(p)] = p^3 + p^2 + p + 1$; et que l'ensemble de représentants pour les classes de Γ_2 sous l'action (à droite) de $\Gamma_0(p)$ est défini par :

$$\begin{aligned}\mathcal{C}_p = &\left\{T_1(a,b,c),\ (a,b,c) \in [0,\ p-1]^3\right\} \cup \left\{T_3(a),\ a \in [0,\ p-1]\right\} \\ &\cup \left\{T_2(a,b,c),\ (a,b,c) \in [0,\ p-1]^3 \text{ et } ac \equiv b^2\, mod p\right\} \cup \{T_4\}\end{aligned}$$

Où pour tout $a, b, c \in \{0, \cdots, p-1\}$ on a :

$$T_1(a,b,c) = \begin{pmatrix} I_2 & 0 \\ \begin{smallmatrix} a & b \\ b & c \end{smallmatrix} & I_2 \end{pmatrix}, \quad T_2(a,b,c) = \begin{pmatrix} 0 & -I_2 \\ I_2 & \begin{smallmatrix} a & b \\ b & c \end{smallmatrix} \end{pmatrix}$$

$$T_3(a) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & a \\ -a & 1 & 0 & 0 \end{pmatrix}, \quad T_4 = \begin{pmatrix} -1 & -1 & 1 & -1 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \end{pmatrix}$$

Soit f une fonction modulaire sur Γ_2 et $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_2$, on définit la matrice γ_p et les fonctions f^γ, f_p et f_p^γ de $\mathcal{H}_2 \longleftarrow \mathbb{C}$ par :

$$f^\gamma(\Omega) = f(\gamma\Omega), \quad f_p(\Omega) = f(p\Omega),$$

$$f_p^\gamma(\Omega) = f(p\gamma\Omega) \quad et \quad \gamma_p := \left(\begin{smallmatrix} A & pB \\ C/p & D \end{smallmatrix}\right)$$

Proposition 5.2.1. *Les trois fonctions* $\mathrm{j}_{l,p} := (\mathrm{j}_l)_p$ *sont des invariants modulaires pour* $\Gamma_0(p)$. *Et* $\mathbb{C}_{\Gamma_0(p)}$ *est égal à* $\mathbb{C}_{\Gamma_2}\left(\mathrm{j}_{l,p}\right)$ *pour* $l = 1, 2, 3$.

Démonstration. Pour tout $\gamma \in \Gamma_0(p)$, on a $p\gamma\Omega = \gamma_p(p\Omega)$ et $\gamma_p \in \Gamma_2$. Alors $\mathrm{j}_{l,p}(\gamma\Omega) = \mathrm{j}_l(\gamma_p(p\Omega)) = j_l(p\Omega) = \mathrm{j}_{l,p}(\Omega)$.
On utilise le résultat qui dit qu'il existe une surjection entre $\Gamma_2 = Sp_4(\mathbb{Z})$ *et* $Sp_4(\mathbb{Z}/N\mathbb{Z})$ *pour tout* N *entier* [78, Lemme 4.2.4].
Comme $\mathbb{C}_{\Gamma_0(p)}$ est une extension de $\mathbb{C}_{\Gamma_2}$ de degré $[\Gamma_2 : \Gamma_0(p)]$, alors suffit de montrer qu'à l fixé, les fonctions $\mathrm{j}_{l,p}^\gamma$ pour $\gamma \in \Gamma_2/\Gamma_0(p)$ sont distinctes. Sinon si deux de ces fonctions sont égales cela implique que le stabilisateur $S \subset \Gamma_2$ de $\mathrm{j}_{l,p}$ est égal à Γ_2 [78, Proposition 4.2.5], ce qui est absurde. □

Les matrices de périodes des variétés abéliennes principalement polarisées p-isogènes à une variété Ω donnée sont les $p\gamma\Omega$ pour $\gamma \in \mathcal{C}_p$ (par [6, Théorème 3.2]). Et les fonctions $\mathrm{j}_{l,p}$ ont des pôles en les matrices de période Ω des variétés p-isogènes à un produit de courbes elliptiques.

Le polynôme modulaire de niveau p modular pour j_1 est le polynôme minimal de $\mathrm{j}_{1,p}$ sur le corps $\mathbb{C}(\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3)$, et

$$\phi_{1,p}(X) = \prod_{\gamma \in \mathcal{C}_p} (X - \mathrm{j}_{1,p}^\gamma).$$

Comme $\mathrm{j}_{2,p}$ et $\mathrm{j}_{3,p}$ sont dans $\mathbb{C}_{\Gamma_2}(\mathrm{j}_{1,p}) = \mathbb{C}_{\Gamma_2}[\mathrm{j}_{1,p}]$ d'après la proposition précédente 5.2.1 alors $\mathrm{j}_{2,p} = \phi_{2,p}(\mathrm{j}_{1,p})$ et $\mathrm{j}_{3,p} = \phi_{3,p}(\mathrm{j}_{1,p})$ où $\phi_{2,p}(X)$ et $\phi_{2,p}(X)$ des polynômes unitaires dans $\mathbb{C}(\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3)[X]$ de degré strictement inferieur à $deg(\phi_{1,p}(X))$. Et pour $l = 2, 3$,

$$\phi_{l,p}(X) = \frac{\psi_{l,p}(X)}{\phi'_{1,p}(X)} \quad avec \quad \psi_{l,p}(X) = \sum_{\gamma \in \mathcal{C}_p} \mathrm{j}_{l,p}^\gamma \prod_{\gamma' \in \mathcal{C}_p \setminus \{\gamma\}} (X - \mathrm{j}_{1,p}^{\gamma'}).$$

Ces polynômes modulaires $\phi_{1,p}(X)$, $\psi_{2,p}(X)$ et $\psi_{3,p}(X)$ sont tous des éléments de $\mathbb{Q}(\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3)[X]$ [6, Théorème 2.5]. Et on les appelle les *p-polynômes modulaires pour* j_1, j_2 *et* j_3.
L'évaluation de $(\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3)$ en $\Omega \in \mathfrak{H}_2$ envoie les polynômes $\phi_{1,p}(X)$, $\phi_{2,p}(X)$ et $\phi_{3,p}(X)$ sur des polynômes dans $\mathbb{C}[X]$. Et si x est une solution sur $\mathbb{C}$ de $\phi_{1,p}(X)$, alors $(x, \phi_{2,p}(x), \phi_{3,p}(x))$ sont les j-invariants absolus des surfaces abéliennes principalement polarisées (p, p)-isogènes à la surface Ω.

Plus généralement lorsque Γ est un sous groupe de congruence Γ_2, c'est-à-dire pour un certain entier N on a :

$$\Gamma_2(N) = \{M \in \Gamma_2 \,:\, M \equiv I_4 \mod N\} \subset \Gamma.$$

Alors pour un premier p ne divisant pas N, $\mathcal{C}_p$ désignera l'ensemble des représentants des classes de $\Gamma/(\Gamma \cap \Gamma_0(p))$.
Soient f_1, f_2 et f_3 les trois fonctions modulaires génératrices du corps de fonctions $\mathbb{C}_\Gamma$. Alors les p-polynômes modulaires pour f_1, f_2 et f_3 sont $l = 2, 3$:

$$\phi_{1,p}(X) = \prod_{\gamma \in \mathcal{C}_p} (X - f_{1,p}^{\gamma}), \quad et \quad \psi_{l,p}(X) = \sum_{\gamma \in \mathcal{C}_p} f_{l,p}^{\gamma} \prod_{\gamma' \in \mathcal{C}_p \setminus \{\gamma\}} (X - f_{1,p}^{\gamma'}).$$

5.2.2 *Evaluations*

Pour l'évaluation des polynômes modulaires la plupart des auteurs utilisent des algorithmes d'interpolation des polynômes et des fractions rationnelles multivariées. Pour ce qui suit, nous utilisons une variante de l'algorithme d'Enea Milio [78] qui généralise celui de Dupont [28] dont nous rappellons les principes de fonctionnement .
On suppose que nous avions un algorithme qui envoie une approximation flottante de la valeur $F(x_1, \cdots, x_m)$ pour tout $(x_1, \cdots, x_m) \in \mathbb{C}^m$. Et F est une fraction rationnelle multivariée de $\mathbb{C}[X]$ que l'on veut calculer .
Soit $A(X), B(X) \in \mathbb{Z}[X]$ tel que $F(X) = \dfrac{A(X)}{B(X)}$ avec $\deg A(X) = d_X^A$ et $\deg B(X) = d_X^B$. On pose $n = d_X^A + d_X^B + 1$, si on connaît au préalable les degrés d_X^A et d_X^B et si l'on dispose de $(n+1)$ valeurs x_i de F alors on peut déterminer les coefficients $(A_0, \cdots, A_{d_X^A}, B_0, \cdots, B_{d_X^B}) \in \mathbb{Z}^{n+1}$ tels que :

$$\begin{pmatrix} 1 & x_1 & \cdots & x_1^{d_X^A} & -F(x_1) & -F(x_1)x_1 & \cdots & -F(x_1)x_1^{d_X^B} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \cdots & x_n^{d_X^A} & -F(x_n) & -F(x_n)x_n & \cdots & -F(x_n)x_n^{d_X^B} \end{pmatrix} \cdot \begin{pmatrix} A_0 \\ \vdots \\ A_{d_X^A} \\ B_0 \\ \vdots \\ B_{d_X^B} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Alors on obtient une solution F (de l'équation $A(X) - B(X)F(X) = 0$) définie à une constante (multiplicative) près.
En pratique, on peut déterminer les degrés d_X^A et d_X^B en déterminant la plus petite valeur de m telle que l'espace des solutions du système associé à $A(X) - B(X)F(X) = 0$. Une base de l'espace des solutions permettra alors de déterminer les valeurs de d_X^A et d_X^B, ainsi qu'une solution $(A_0, \cdots, A_{d_X^A}, B_0, \cdots, B_{d_X^B}) \in \mathbb{Z}^{n+1}$.
Cette méthode est n'est pas difficile à implémenter mais elle a une mauvaise complexité.
Lorsque $\deg A < k$ et $\deg B \leq m - k$, on part de l'interpolation de polynômes univariés $y_i = F(x_i)$ pour un $(x_1, \cdots, x_n) \in \mathbb{C}^m$. On obtient des polynômes $r(X)$ et $t(X)$ tels que $r_i(x_i) = t(x_i)F(x_i)$ pour tout i. Et par le théorème des restes Chinois, on extrait $r \equiv tf \mod g$, où $g = \prod_{i=1}^{m} (X - x_i)$. Ensuite on utilise l'algorithme d'Euclide étendu sur g et f. De plus il est possible de ne calculer qu'une ligne de cet algorithme pour interpoler la fraction F.
Ce qui produit un algorithme de complexité $O(\mathcal{M}_N(n)\log(n))$ où $\mathcal{M}_N(n)$ est la complexité de la multiplication de deux polynômes de degrés inférieurs ou égaux à n avec des coefficients de N bits. Alors on aura seulement n nombres d'évaluations. Cependant cette méthode présente quelques subtilités pour son fonctionnement optimal, pour plus de détails nous

renvoyons le lecteur à la [78, Section 4.1].

Le sous groupe modulaire $\Gamma_2(2,4)$ de Γ_2 est normal d'indice 11520 et de niveau 4 et on a $\mathbb{C}_{\Gamma_2(2,4)} = \mathbb{C}(\mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3) = \mathbb{C}(\mathfrak{c}_1, \cdots, \mathfrak{c}_{15})$ d'après le chapitre 3, la section 3.3.1 et le théorème 3.3.11.
Lorsque $p > 2$, les classes d'équivalence $\Gamma(2,4)/(\Gamma_0(p) \cap \Gamma(2,4))$ sont bijections avec celles de $\Gamma_2/\Gamma_0(p)$, ainsi $\mathbb{C}_{\Gamma_0(p)\cap\Gamma(2,4)}$ est égal à $\mathbb{C}_{\Gamma(2,4)}(\mathfrak{b}_{i,p})$ pour tout $i = 1, 2, 3$ [78, Pages: 120-122].
Pour déterminer Ω à partir de $(\mathfrak{b}_1(\Omega), \mathfrak{b}_2(\Omega), \mathfrak{b}_3(\Omega))$, on peut utiliser les formules de duplication pour les $\left(\mathfrak{c}_j(\Omega)\right)_{j\in\mathcal{P}_2}$ et extraire les invariants d'Igusa correspondant à Ω. Pour atteindre le bon Ω modulo l'action de $\Gamma_2(2,4)$, une méthode détaillée dans [78, Pages: 122, 124] permet de précalculer l'action sur les thêta constantes (permutations et constantes) de l'ensemble des représentants de $\Gamma_2/\Gamma_2(2,4)$ en utilisant l'équation fonctionnelle qui donne :

$$\theta_k^2\left(\gamma\Omega'\right) = \zeta_\gamma^2 \det(\cdots) i^{\epsilon(\gamma,k)} \theta_l^2\left(\Omega'\right) \quad avec \quad \epsilon(\gamma,k) \in \{0,1,2,3\}.$$

On dira ici que l'action de γ envoie l'indice k vers l'indice l. Cela peut conduire à un ensemble $\mathcal{A}$ des $\mathfrak{c}_i(\Omega) = \mathfrak{c}_i(\gamma\Omega')$ et celui $\mathcal{B}$ des dix $\mathfrak{c}_i(\Omega')$ et en comparant A et B on déduit de l'action le représentant γ correspondant, ce qui nous permet d'avoir $\gamma\Omega' = \Omega$. On peut aussi avoir le cas où il existe $c \in \mathcal{P}_2$ qui s'envoie sur 0 et un $d \in \mathcal{P}_2$ tel que 0 s'envoie sur d et

$$\mathfrak{c}_c\left(\gamma\Omega'\right) = i^{\epsilon(\gamma,c)-\epsilon(\gamma,0)} \mathfrak{c}_d\left(\Omega'\right)^{-1}.$$

En multipliant l'ensemble $\mathcal{A}$ par $\mathfrak{c}_d\left(\Omega'\right)^{-1}$ et en comparant ce nouvel ensemble avec $\mathcal{B}$ on peut aussi déduire l'action de γ.

Par suite lorsque l'on considère f_1, f_2 et f_3 les trois invariants générateurs du corps de fonctions modulaires $\mathbb{C}_\Gamma$.
À partir de $(f_1(\Omega), f_2(\Omega), f_3(\Omega))$ et un premier p ne divisant pas le niveau de Γ, l'algorithme de la section 5.2 et l'algorithme 6 calcule le polynôme $\phi_{1,p}(X)$ en $O(\mathcal{M}(n_p)\log n_p)$ où $n_p = p^3 + p^2 + p + 1$ est le degré de $\phi_{1,p}(X)$. Ensuite en utilisant des interpolations rapides on évalue les polynômes modulaires $\psi_{2,p}(X)$ et $\psi_{3,p}(X)$ avec la même complexité.
De manière pratique on suppose que rélations modulaires $F(f_i, \mathfrak{j}_i)$ sont connues (ou comme alternative on pourra prendre les rélations modulaires $F(f_i, \mathfrak{b}_i)$). Lors des premières étapes de l'algorithme, ces rélations fournissent des conversions entre les valeurs $f_i(\Omega)$ et les j-invariants $\mathfrak{j}_i$ (ou avec les invariants de Rosenhain). De même on pourra récupérer les valeurs de $f_{i,p}^\gamma(\Omega)$ à partir de celles de $\mathfrak{j}_{i,p}^\gamma(\Omega)$ en utilisant des algorithmes de Newton combinés avec des calculs à faibles précision pour leurs initialisations.
Lorsque l'on note par $n_p = p^3 + p^2 + p + 1$ le degré de $\phi_{1,p}(X)$, l'algorithme 6 évalue $\phi_{1,p}(X)$ en $O(\mathcal{M}(n_p)\log n_p)$ opérations.
On peut améliorer le coût de cacul de ces polynômes en les évaluant à une précision fixée au besoin au-lieu de les déterminer complètement. Aussi en les évaluant pour un triplet $(f_1(\Omega), f_2(\Omega), f_3(\Omega))$ donné, donc pour obtenir des équations polynômiales seulement en fonction d'un triplet (comme variables). Cette approche est celle utilisée par J.Kieffer dans [59]. Ainsi sous certaines conditions heuristiques, pour un triplet $(\mathfrak{j}_1, \mathfrak{j}_2, \mathfrak{j}_3) \in \mathbb{Q}^3$ de hauteur $O(1)$ où les dénominateurs des polynômes ne s'annulent pas, son algorithme calcule les équations modulaires en $(\mathfrak{j}_1, \mathfrak{j}_2, \mathfrak{j}_3)$ avec un coût de $\tilde{O}(p^6)$ opérations binaires.

Entrée: $(f_1(\Omega), f_2(\Omega), f_3(\Omega))$ tel que $\mathbb{C}_\Gamma = \mathbb{C}(f_1(\Omega), f_2(\Omega), f_3(\Omega))$, un premier p ne divisant pas le niveau de Γ, $\mathcal{C}_p$ des classes représentatives dans $\Gamma/(\Gamma \cap \Gamma_0(p))$ et un pré-calcul des actions des classes représentatives dans Γ_2/Γ, une précision $N \in \mathbb{N}$.

Sortie: $\phi_{1,p}(X, f_1(\Omega), f_2(\Omega), f_3(\Omega))$ et $\psi_{l,p}(X, f_1(\Omega), f_2(\Omega), f_3(\Omega))$ à précision N pour $l = 2, 3$.

1. Récupérer les j-invariants $\mathfrak{j}_i(\Omega)$ ou les invariants de Rosenhain à partir $f_i(\Omega)$;
2. À partir de ces invariants construire une courbe hyperelliptique $Y^2 = f(X)$ à précision N ;
3. Réconstituer les dix $\mathfrak{c}_i(\Omega)$ à précision N en utilisant les formules de Thomae et avec une intégration numérique pour le choix de racines ;
4. Renverser les fonctions pour récupérer Ω' à précision N en utilisant [28] ;
5. Déterminer Ω et $\gamma \in \Gamma_2/\Gamma$ tel que $\Omega = \gamma\Omega'$ (en comparant $f_i(\Omega)$ et $f_i(\Omega')$) ;
6. Calculer à précision N les $\mathfrak{b}^\gamma_{i,p}(\Omega)$ pour $\gamma \in \mathcal{C}_p$ en utilisant [28] et les $\mathfrak{j}^\gamma_{i,p}(\Omega)$ correspondants ;
7. Calculer à précision N les $f^\gamma_{i,p}(\Omega)$ pour $\gamma \in \mathcal{C}_p$;
8. Calculer $\phi_{1,p}(X, f_1(\Omega), f_2(\Omega), f_3(\Omega))$ et $\psi_{l,p}(X, f_1(\Omega), f_2(\Omega), f_3(\Omega))$ à précision N en utilisant un arbre de sous-produit ;
9. Calculer $\phi_{1,p}, \psi_{l,p}$ à précision N pour $l = 2, 3$ en utilisant une interpolation de fonctions rationnelles [77] ;

Algorithm 6 – Évaluation de Polynômes Modulaires en dimension 2

5.2.3 *Exemples avec les Invariants de Streng et des Invariants Thêta*

La méthode détaillée dans la section 5.2 a permis à Regit Dupont d'évaluer les polynômes modulaires pour $p = 2$ en fonction des invariants d'Igusa [28]. Suivant une idée de Streng [113] d'introduire les invariants $(\mathfrak{j}_1, \mathfrak{j}_2, \mathfrak{j}_3)$ dans le but de réduire la taille des dénominateurs des polynômes de classe, E.Milio [78] a évalué des polynômes modulaires pour $p = 2$ puis $p = 3$ en les invariants $(\mathfrak{j}_1, \mathfrak{j}_2, \mathfrak{j}_3)$. Les invariants de Streng fourniraient donc des polynômes plus petits en termes de degrés, précision et espace mémoire.

On note $\mathcal{L}_p$ *le lieu de toutes les surfaces abéliennes principalement polarisées qui sont p-isogènes à un produit de courbes elliptiques.* C'est une sous-variété de $\mathfrak{H}_2/\Gamma_2$ de dimension 2 caractérisée par une équation $L_p = 0$ pour un polynôme L_p de $\mathbb{Q}[\mathfrak{j}_1, \mathfrak{j}_2, \mathfrak{j}_3]$. On montre que L_p divise les dénominateurs des coefficients de $\phi_{1,p}(X)$, $\psi_{1,p}(X)$ et $\psi_{2,p}(X)$.

Soit $\Delta \equiv 0, 1 \mod 4$ et $\Delta > 0$, la *surface de Humbert* H_Δ *de discriminant* Δ *est la surface irreductible surface des matrices de périodes equivalentes aux* $\Omega = \left(\begin{smallmatrix} \Omega_1 & \Omega_2 \\ \Omega_2 & \Omega_3 \end{smallmatrix}\right) \in \Gamma_2 \backslash \mathcal{H}_2$ *vérifiant* $k\Omega_1 + \ell\Omega_2 - \Omega_3 = 0$ *tels que* k *et* ℓ *sont determinés de manière unique par* $\Delta = 4k + \ell$ *et* $\ell \in \{0, 1\}$. *Alors la surface de Humbert surface* H_{m^2} *(pour* $m \in \mathbb{N}$*) est l'espace de moduli pour les classes d'isomorphismes des surfaces abéliennes principalement polarisées et isogène à un produit de courbes elliptiques via une isogenie de degré* m^2. (Aller à [43].)
Pour tout discriminant Δ, il existe un polynôme irréductible $L_\Delta(j_1, j_2, j_3)$ dont l'ensemble des zéros est la surface de Humbert de discriminant Δ. Ainsi $L_{p^2}(j_1, j_2, j_3)$ divise les dénominateurs des polynômes modulaires définis avec les invariants d'Igusa avec une puissance pouvant se déduire du degré de la surface de Humbert de discriminant p^2 [78]. Plus particulièrement, le dénominateur commun exact $D_p(\Omega)$ de l'équation modulaire évaluée en un Ω est donné par [59, Proposition 3.3.].

Nous allons pas nous intéresser éssentiellement aux valeurs exactes des degrés (en les invariants) des polynômes modulaires correspondants par contre leurs formes de définition seront considerès lors de leurs utilisations dans les chapitres suivants.
Dans un soucis de pouvoir utiliser les (p,p)-polynômes modulaires en toute caractéristique p et avec une bonne réduction, nous aurons besoin d'évaluer des polynômes modulaires en les invariants définis par le théorème 4.3.2 dans le chapitre 4 et la section 4.2.
En effet nous ne disposions pas de polynômes avec bonne reduction en caractéristique 2 parmi ceux déjà évalués (qui sont en fonctions d'invariants n'ayant pas bonne réduction modulo 2).
D'autre part en toute caractéristique (plus particulièrement pour $p \leq 5$), nous voulons calculer des rélévés de covariants fractionnaires. Alors en caractéristique 3 aussi, il nous faudrait utiliser des polynômes modulaires en fonctions d'invariants ayant bonne réduction modulo 3.

5.2.4 *Polynômes Modulaires avec les Invariants* $\mathfrak{a}_1$, $\mathfrak{a}_2$, $\mathfrak{a}_3$

Les conversions d'un modèle hyperelliptique standard: $y^2 + h(x) = f(x)$ vers la forme normale associées à une courbe hyperelliptique sont expliquées dans le chapitre 4 et la section 4.5. Et réciproquement les points de Weierstrass sont donnés par l'équation: $(1 + aX + bX^2)^2 - 4X^3(c + dX + X^2) = 0$ (en caractéristique différent de 2) ce qui permet de récouvrir le model hyperelliptique standard de la courbe associé d'une forme normale. Alors on pourra réconstituer les invariants I_2, I_4, I_6, I_{10} en fonction des coefficients a, b, c, d d'une forme normale, puis reconstituer les invariants $J_2, J_4, J_6, J_8, J_{10}$ comme fonctions rationnelles en les coefficients a, b, c, d. Comme la forme normale et ses covariants (en fonctions des a, b, c, d) se réduisent bien modulo tout p, alors les fonctions rationnelles définies par J_{2i} étant des covariants en les a, b, c, d ont une bonne réduction modulo tout p.

À partir des J_i's, qui sont des covariants de poids, on peut déterminer les 10 invariants γ_i. Et inversement, les γ_i's permettent de réconstituer les covariants tel que $J_{10} = 1$, ainsi J_6 est obtenu (à une racine 5-ième de l'unité près) à partir de γ_8. Ce qui permet de retrouver les J_2, J_4, J_8. La bonne racine pour J_6 peut être déterminer en utilisant γ_7 et γ_9. Ensuite nous pouvons rétrograduer par J_{10} pour obtenir un point projectif pondéré rationnel.

Cependant, l'utilisation de γ_i n'est pas pratique lors de la définition de polynômes modulaires. En effet, nous aimerions décrire l'espace des modules $\mathcal{M}_2$ en utilisant seulement trois invariants (au moins birationnellement). De plus, par le résultat [51, Theorem 5], on sait qu'un point générique de la variété des modules $\mathcal{M}_2 \otimes \Bbbk$ génère une extension purement transcendantale de dimension trois. Et en corollaire, nous obtenons que $\mathcal{M}_2 \otimes \Bbbk$ est birationnel à $\mathbb{A}^3_{\Bbbk}$. Ainsi nous pourrions utiliser les triplets avec bonne réduction définis dans le chapitre 4, la section 4.2 et le théorème 4.3.2.

Par exemple en caractéristique 2 on peut toujours passer d'un model hyperelliptique standard vers l'une des formes normales réduites définies par des types $(1,1,1)$, $(3,1)$ et (5) (et vice-versa) en utilisant la Théorie d'Artin-Schreier (aller à le chapitre 4, la section 4.3 et la section 4.3.2). On peut aussi exprimer les J_i's en termes de fonctions symétriques α, β, γ, et réciproquement en utilisant le chapitre 4, la section 4.2 et les équations (4.7) à (4.9). De plus les réductions (en les types) des formes normales se font intégralement dans les classes définies par les rangs respectifs 2, 1 et 0, en particulier les courbes ordinaires sont

birationnellement équivalentes à un type $(1,1,1)$; donc leurs classes d'isomorphismes sont entièrement définies par les invariants $\mathfrak{a}_1$, $\mathfrak{a}_2$, $\mathfrak{a}_3$.

Par les méthodes détaillées dans les sections 5.1 et 5.2, E.Milio a évalué les polynômes modulaires pour les niveaux 2, 3, 5 etc ... pour plusieurs systèmes d'invariants. Cependant, ses polynômes modulaires de niveau 2 utilisant les invariants modulaires j_i ont une mauvaise réduction en caractéristique 2 et 3. Nous avons plutôt utilisé l'algorithme 6 pour calculer les polynômes modulaires pour les invariants $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ qui réduisent bien en toute caractéristique et plus particulièrement en caractéristique 2 ce système d'invariants suffit pour décrire les classes d'isomorphisme sur les espaces des courbes ordinaires de genre 2. Ainsi de tels polynômes décrivent les jacobiennes $(2,2)$-isogènes dans $\mathcal{M}_2[J_2^{-1}]$. Cet ouvert est bien adapté aux courbes de type $(1,1,1)$ dans la caractéristique 2 par des rélations décrites dans le chapitre 4.

— Puisque les invariants $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ et les invariants (j_1, j_2, j_3) sont birationnellement équivalents, nous aurions pu calculer les polynômes modulaires pour $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ en utilisant un changement de variable dans les polynômes modulaires de (j_1, j_2, j_3). En pratique, ce changement de variable impliquait une fonction rationnelle, cela coûtait trop cher de le faire directement et au risque de voir apparaitre dans les polynômes des facteurs parasites qui pourraient affecter sa réduction. Nous aurions pu le calculer en utilisant l'évaluation/interpolation, mais il était plus facile de simplement réutiliser l'algorithme 6.

— Le dénominateur commun de (j_1, j_2, j_3) est χ_{10}, qui s'annule sur le lieu du produit des courbes elliptiques. Le lieu $\mathcal{L}_p$ des surfaces principalement abéliennes polarisées qui sont (p,p)-isogènes à un produit de courbes elliptiques, est une sous-variété algébrique de dimension 2 de l'espace des modules $\Gamma_2\backslash\mathfrak{H}_2$ et peut être décrit par une équation $L_p = 0$. Et le polynôme L_p divise les dénominateurs des coefficients de $\phi_{1,p}(X, f_1(\Omega), f_2(\Omega), f_3(\Omega))$, $\psi_{1,p}(X, f_1(\Omega), f_2(\Omega), f_3(\Omega))$ et $\psi_{2,p}(X, f_1(\Omega), f_2(\Omega), f_3(\Omega))$. En utilisant $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$, le dénominateur des polynômes modulaires contiennent le lieu des Jacobiennes (p,p)-isogènes aux surfaces abéliennes $\mathcal{A}$ avec $J_2(\mathcal{A}) = 0$. Il serait intéressant d'avoir une interprétation modulaire de ce lieu, similaire à la description de $\mathcal{L}_p$ ci-dessus. Par suite on notera par $\mathcal{D}_p$ le lieu des dénominateurs des polynômes modulaires $\Phi_{1,p}, \Psi_{1,p}, \Psi_{2,p}$.

— Nous n'avons appliqué l'algorithme 6 qu'aux invariants birationnels de niveau 1. Il serait intéressant de trouver de bons invariants comme par exemple des niveaux plus élevés qui donneraient des polynômes plus petits.

5.2.5 *Exemples avec les Invariants* u_1, u_2, u_3

Sur l'espace modulaire de Siegel, nous disposons de polynômes modulaires de niveau 3 en fonction des invariants d'Igusa et ceux de Streng. Puisqu'ils ont une mauvaise réduction en caractéristique 3, nous proposons d'utiliser les triplets d'invariants définis sur les espaces $\mathcal{M}_2[J_2^{-1}] \otimes \Bbbk$, $\mathcal{M}_2[J_4^{-1}] \otimes \Bbbk$ et $\mathcal{M}_2[J_6^{-1}] \otimes \Bbbk$. En effet nous avons par exemple:

$$\gamma_2 = j_2^5/(192j_3^2) - j_2^3/(12j_3), \text{ et } \gamma_3 = 2j_2^2j_1/(27j_3) + j_2^5/(3456j_3^2) - j_2^3/(72j_3)$$

dont l'expression en fonction des Invariants algébriques de Streng ont une mauvaise réduction en caractéristique 3.
Cependant nous avons à partir du théorème 4.3.2 dans le chapitre 4 et la section 4.2 que

: lorsque $char(\Bbbk) \neq 2$, la variété $\mathcal{M}_2 \otimes \Bbbk$ admet un unique point singulier, défini par la condition $J_2 = J_6 = J_8 = 0$. En considerant la rélation $J_2J_6 = 4J_8 + J_4^2$, ainsi pour les points non-singuliers soit nous avons ($J_4 \neq 0$) ou soit (au moins un des invariants J_2 ou J_6 ne s'annullent pas). Alors les trois espaces $\mathcal{M}_2[J_2^{-1}]$, $\mathcal{M}_2[J_4^{-1}]$ et $\mathcal{M}_2[J_6^{-1}]$ (définis dans le théorème 4.3.2 au le chapitre 4 et la section 4.2) suffisent pour décrire les points non-singuliers (en particulier les courbes ordinaires) sur $\mathcal{M}_2 \otimes \Bbbk$.
Les triplets $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$, $(\mathfrak{d}_1, \mathfrak{d}_2, \mathfrak{d}_3)$ et $(\mathfrak{u}_1, \mathfrak{u}_2, \mathfrak{u}_3)$ d'invariants induisent un isomorphisme de $\mathcal{M}_2[J_2^{-1}]$, $\mathcal{M}_2[J_4^{-1}]$ et $\mathcal{M}_2[J_6^{-1}]$ respectivement avec les ouverts standards de $\mathbb{A}^3$ définis par $\mathfrak{a}_3^{-1}$, $\mathfrak{d}_3^{-1}$, $\mathfrak{u}_3^{-1}$ sur $\mathbb{Z}[1/2]$.
Dès lors comme dans le cas du calcul de polynômes modulaires avec bonne réduction en caractéristique 2, nous pouvons utiliser les triplets d'invariants sur les espaces $\mathcal{M}_2[J_2^{-1}]$, $\mathcal{M}_2[J_4^{-1}]$ et $\mathcal{M}_2[J_6^{-1}]$ et l'algorithme 6 pour évaluer des polynômes modulaires qui restent pratiques en caractéristque 3.

5.2.6 *Polynômes Modulaires de Hilbert*

Dans cette section nous faisons une introduction sur les polynômes modulaires pour l'espace modulaire de Hilbert et nous allons nous intéresser à leurs propriétés en vue de les utiliser pour le relèvement canoniques de surfaces abéliennes dont l'anneau d'endomorphisme a une multiplication réelle par $\mathcal{O}_K$ où $K = \mathbb{Q}(\sqrt{D})$ pour $D = 2$ ou 5. Certains de ces polynômes ont été évalués par E.Milio [78].
Les méthodes de calcul restent des améliorations des méthodes précédentes pour l'espace modulaire de Siegel.
Nous n'avons pas évaluer concretement de nouveaux polynômes dans le cas Hilbert. Nous allons parcourir les cas classiques avec les invariants de Gundlach pour $D = 2$ ou 5 et les cas faisant récourt aux invariants thêta.

Soit $\mathbb{K} = \mathbb{Q}(\sqrt{D})$ un corps quadratique réel de discriminant $\Delta_{\mathbb{K}}$ et d'anneau des entiers $\mathcal{O}_{\mathbb{K}}$. Nous avons $\mathcal{O}_{\mathbb{K}} = \mathbb{Z} + \omega\mathbb{Z}$ où $\omega = \frac{1+\sqrt{D}}{2}$ si $D \equiv 1 \mod 4$ sinon $\omega = \sqrt{D}$.
Nous avons parcouru les sections 3.3 et 3.4, quelques rappels sur l'espace de module de Hilbert $\mathrm{SL}_2(\mathcal{O}_{\mathbb{K}})\backslash\mathfrak{H}_1^2$ lequel décrit les surfaces abéliennes principalement polarisées $\mathcal{A}$ avec multiplication réelle par l'ordre maximale $\mathcal{O}_{\mathbb{K}}$, et dont un plongement dans $\mathrm{End}(\mathcal{A})$ est explicitement donné par μ.

• Lorsque $\beta = \ell$ est un nombre premier. Les sous groupes isotropiques maximaux pour le couplage de Weil qui restent stables sous l'action de la multiplication réelle par $\mathcal{O}_{\mathbb{K}}$ sont décrits par $\mathcal{O}_{\mathbb{K}}e_i$ (sous l'action près $\dot{\Gamma}^0(\ell)\backslash \mathrm{SL}_2(\mathcal{O}_{\mathbb{K}} \otimes \partial_{\mathbb{K}})$ sur la base (e_1, e_2)). Alors le nombre de classe de sous groupes stables par multiplication réelle (ℓ-isogénies) est donné par le cardinal de $\mathrm{SL}_2(\ell\mathcal{O}_{\mathbb{K}}\backslash\mathcal{O}_{\mathbb{K}})$:
– Si ℓ est inerte dans $\mathcal{O}_K$, on a $\ell\mathcal{O}_{\mathbb{K}}\backslash\mathcal{O}_{\mathbb{K}} \simeq \mathbb{F}_{\ell^2}$ et le nombre de ℓ-isogénies est $\ell^2 + 1$, ;
– Si ℓ se décompose (split) dans $\mathcal{O}_K$, on a $\ell\mathcal{O}_{\mathbb{K}}\backslash\mathcal{O}_{\mathbb{K}} \simeq \mathbb{F}_\ell^2$ et le nombre de ℓ-isogénies $(\ell + 1)^2$;
– Si ℓ est ramifié dans $\mathcal{O}_K$, on a $\ell\mathcal{O}_{\mathbb{K}}\backslash\mathcal{O}_{\mathbb{K}} \simeq \mathbb{F}_\ell[X]/X^2$ et le nombre de ℓ-isogénies $\ell^2 + \ell$.
(aller [79, Prop 4.3] pour plus de détails).

• D'autre part lorsque $\beta \in \mathcal{O}_{\mathbb{K}}$ est totallement positive de norme ℓ. Dans ce cas soit ℓ ramifie dans $\mathcal{O}_{\mathbb{K}}$ et il existe un seul type d'isogénies cycliques de degré ℓ: les β-isogénies,

ou soit ℓ se décompose (splits) en $\ell = \beta\overline{\beta}$ et $\mathcal{A}[\ell] = \mathcal{A}[\beta] \otimes \mathcal{A}[\beta]$, il existe alors dans ce cas, deux types d'isogenies cycliques : les β-isogénies et les $\overline{\beta}$-isogénies.
Soit

$$\dot{\Gamma}^0(\beta) = \left\{ \begin{pmatrix} a & b/\sqrt{\Delta_{\mathbb{K}}} \\ c\sqrt{\Delta_{\mathbb{K}}} & d \end{pmatrix} \in \dot{\Gamma} \ : \ b \in \beta\mathcal{O}_{\mathbb{K}} \right\} \text{ et}$$

$$\dot{\Gamma}^0(\beta) = \left\{ \begin{pmatrix} a & b/\sqrt{\Delta_{\mathbb{K}}} \\ c\sqrt{\Delta_{\mathbb{K}}} & d \end{pmatrix} \in \dot{\Gamma} \ : \ (a-1), (d-1), b, c \in \beta\mathcal{O}_{\mathbb{K}} \right\}.$$

Alors le recouvrement de Hilbert $\dot{\Gamma}^0(\beta)\backslash\mathfrak{H}_1^2$ décrit les surfaces abéliennes principalement polarisées β-isogènes avec multiplication par $\mathcal{O}_{\mathbb{K}}$, ou de manière équivalente $\dot{\Gamma}^0(\beta)\backslash\mathfrak{H}_1^2$ décrit les paires $(\mathcal{A}, K)$ où $\mathcal{A}$ admet multiplication réelle par $\mathcal{O}_{\mathbb{K}}$ et $K \subset \mathcal{A}[\beta]$ est un noyau isotropique maximal pour le β-couplage de Weil et stable par $\mathcal{O}_{\mathbb{K}}$.

Soient $\mathfrak{i}_1, \mathfrak{i}_2$ et $\mathfrak{i}_3$ les générateurs du corps de fonction de l'espace de module de Hilbert $\mathbb{C}_{\mathcal{G}}$ (avec $\mathcal{G} = \dot{\Gamma}$ ou $\dot{\Gamma} \cup \dot{\Gamma}_v$) et soit $\mathfrak{j}$ une fonction modulaire de Hilbert invariant par $\dot{\Gamma} \cap \dot{\Gamma}^0(\beta)$ mais pas par $\dot{\Gamma}$. Alors lorsque $\mathfrak{j}$ est symétrique $\mathbb{C}(\mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3, \mathfrak{j}) = \mathbb{C}_{(\dot{\Gamma}\cap\dot{\Gamma}^0(\beta))\rtimes\langle v\rangle}$ sinon $\mathbb{C}(\mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3, \mathfrak{j}) = \mathbb{C}_{\dot{\Gamma}\cap\dot{\Gamma}^0(\beta)}$ (d'après [79, Prop 4.11]).

Ainsi on considère $\mathfrak{i}_{k,\beta}$, $\mathfrak{i}_{k,\beta}^{\gamma}$ et $\mathfrak{i}_{k,\beta}^{v}$ les fonctions de $\mathfrak{H}_1^2$ vers $\mathbb{C}$ définies par:

$$\mathfrak{i}_{k,\beta}(z) = \mathfrak{i}_k\left(\frac{1}{\beta}z\right) \quad \mathfrak{i}_{k,\beta}^{\gamma}(z) = \mathfrak{i}_k\left(\frac{1}{\beta}\gamma z\right) \text{ et } \mathfrak{i}_{k,\beta}^{v}(z) = \mathfrak{i}_k\left(\frac{1}{\beta}vz\right)$$

pour $k = 1,\ 2,\ 3$ et pour tout $\gamma \in \dot{\Gamma} \cup \dot{\Gamma}_v$. D'autre part pour tout $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \dot{\Gamma}^0(\beta)$ on note par $\gamma_\beta = \left(\begin{smallmatrix} a & b/\beta \\ c\beta & d \end{smallmatrix}\right) \in \dot{\Gamma}$, et nous avons $\gamma_\beta\left(\frac{1}{\beta}z\right) = \frac{1}{\beta}\gamma z$. Alors en utilisant ces définitions on aboutit aux propriétés suivantes:

$$\mathfrak{i}_{k,\beta}^{\gamma}(z) = \mathfrak{i}_k^{\gamma_\beta}\left(\frac{1}{\beta}z\right), \quad \mathfrak{i}_{k,\beta}^{v}(z) = \mathfrak{i}_k^{v}\left(\frac{1}{\overline{\beta}}z\right) \text{ et } \mathfrak{i}_{k,\beta}^{\gamma v}(z) = \mathfrak{i}_k^{v\bar{\gamma}\bar{\beta}}\left(\frac{1}{\overline{\beta}}z\right)$$

En considerant $\dot{\Gamma}_\beta = \{\gamma \in \dot{\Gamma}(1) \mid \gamma_\beta \in \dot{\Gamma}\}$ pour tout $\dot{\Gamma}$ un sous groupe $\dot{\Gamma}(1)$, alors pour toute fonction $\mathfrak{i}$ modulaire pour $\dot{\Gamma}$, $\mathfrak{i}_\beta$ modulaire pour $\dot{\Gamma}_\beta$. De plus dans le cas où $\mathfrak{i}$ est symétrique et $\bar{\beta} = \beta$ son correspondant $\mathfrak{i}_\beta$ est symétrique aussi. Et si on a $\dot{\Gamma} \cap \dot{\Gamma}^0(\beta) = \dot{\Gamma} \cap \dot{\Gamma}_\beta$ on peut définir la correspondance modulaire $H_{\dot{\Gamma}\cap\dot{\Gamma}^0(\beta)}$ vers
$H_{\dot{\Gamma}} \times H_{\dot{\Gamma}}$, $z \mapsto ((\mathfrak{i}_1(z), \mathfrak{i}_2(z), \mathfrak{i}_3(z)), (\mathfrak{i}_1(z/\beta), \mathfrak{i}_2(z/\beta), \mathfrak{i}_3(z/\beta))$ tels que $\mathfrak{i}_1$, $\mathfrak{i}_2$ et $\mathfrak{i}_3$ engendrent $\mathbb{C}_{\dot{\Gamma}}$.

Par suite lorsque $\mathbb{C}(\dot{\Gamma}(1)) = \mathbb{C}(\mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3)$, les β-polynômes modulaires pour les invariants $\mathfrak{i}_k$ décrivent le lieu des points modulaires

$$((\mathfrak{i}_1(z), \mathfrak{i}_2(z), \mathfrak{i}_3(z)), (\mathfrak{i}_1(z/\beta), \mathfrak{i}_2(z/\beta), \mathfrak{i}_3(z/\beta))$$

pour $z \in \mathfrak{H}_1^2$. Alors si $z \in \dot{\Gamma}(1)\backslash\mathfrak{H}_1^2$, pour $\gamma \in \dot{\Gamma}^0(\beta)\backslash\dot{\Gamma}(1)$: $\frac{1}{\beta}\gamma \cdot z$ et $\frac{1}{\overline{\beta}}\gamma \cdot z$ décrivent respectivement les variétés β-isogènes et celles $\bar{\beta}$-isogènes.

Définition 5.2.2. *Les polynômes $\phi_\beta(X, \mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3)$ et $\psi_{k,\beta}(X, \mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3)$ pour $k = 2,\ 3$ définis comme suite*

$$\phi_\beta(X, \mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3) = \prod_{\gamma \in C_\beta} \left(X - \mathfrak{i}_{1,\beta}^{\gamma}\right) \quad \text{et}$$

$$\psi_{k,\beta}(X, \mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3) = \sum_{\gamma \in C_\beta} \mathfrak{i}_{2,\beta}^{\gamma} \frac{\Phi_\beta(X, \mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3)}{(X - \mathfrak{i}_{1,\beta}^{\gamma})}$$

sont appelés les β-polynômes modulaires pour les invariants $\mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3$. Où dans le cas:
- **non symétrique** : $\mathcal{C}_\beta$ est l'ensemble des classes représentatives de $\dot{\Gamma} \cap \dot{\Gamma}^0(\beta)\backslash\dot{\Gamma}$ et $\dot{\Gamma}$ est un sous groupe de congruence tel que $\dot{\Gamma}(2,4) \subset \dot{\Gamma} \subset \mathrm{SL}_2(\mathcal{O}_{\mathbb{K}} \otimes \partial_{\mathbb{K}})$.
- **et symétrique**: $\mathcal{G} = \dot{\Gamma} \cup \dot{\Gamma}_v$, et lorsque $\bar{\beta} = \beta$, $\mathcal{C}_\beta$ est l'ensemble des classes représentatives de $\dot{\Gamma} \cap \dot{\Gamma}^0(\beta))\backslash\dot{\Gamma}$, sinon on prend $\mathcal{C}_\beta$ l'ensemble des classes représentatives de $(\mathcal{G} \cap \dot{\Gamma}^0(\beta))\backslash\mathcal{G}$
.

Ainsi à partir $J_1 = (\mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3)$, un point β-isogènes $J_2 = (a_1, a_2, a_3)$ sur l'espace de module de Hilbert modular (eventuellement dans le cas symmétrique) est caractérisé par les équations suivantes: $\phi_\beta(J_1, a_1) = 0$, $a_2\phi'_\beta(J_1, a_1) = \psi_{\beta,k}(J_1, a_1)$ et $a_3\phi'_\beta(J_1, a_1) = \psi_{\beta,k}(J_1, a_1)$.

Remarque 5.2.3. Pour plus d'informations sur les degrés des polynômes de Hilbert et selon les cas aller à [79], ce que nous allons remarquer ce qu'ils sont tous inférieurs ou égals à $\ell^2 + 1$. Et cela rend ces polynômes beaucoup plus pratiques comparer à ceux de Siegel pour le même degré. On peut aussi noter que: Dans le cas où ℓ se décompose (splits) en $\ell = \beta\bar{\beta}$ (i.e β admet ℓ comme norme) et $\dot{\Gamma}$ non symétrique, lorsque $v \in \mathcal{G}$, avec $\mathcal{G} = \dot{\Gamma} \rtimes \langle v \rangle$, alors comme $\dot{\Gamma}$ est stable sous l'action de la conjugaison sur les réels, l'action de v peut être expliciter comme suite sur les polynômes modulaires :

$$\phi_\ell(X, \mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3) = \prod_{\gamma \in C_\beta} \left(X - \mathfrak{i}_{1,\beta}^{\gamma}\right)\left(X - \mathfrak{i}_{1,\bar{\beta}}^{\gamma v}\right) = \prod_{\gamma \in C_\beta} \left(X - \mathfrak{i}_{1,\beta}^{\gamma}\right)\left(X - \mathfrak{i}_{1,\bar{\beta}}^{\gamma}\right)$$

$$\psi_\ell(X, \mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3) = \sum_{\gamma \in C_\beta} \mathfrak{i}_{2,\beta}^{\gamma} \frac{\Phi_\ell(X, \mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3)}{(X - \mathfrak{i}_{1,\beta}^{\gamma})} + \sum_{\gamma \in C_\beta} \mathfrak{i}_{2,\bar{\beta}}^{\gamma} \frac{\phi_\ell(X, \mathfrak{i}_1, \mathfrak{i}_2, \mathfrak{i}_3)}{(X - \mathfrak{i}_{1,\bar{\beta}}^{\gamma})}.$$

où C_β est l'ensemble des classes représentatives de $\dot{\Gamma} \cap \dot{\Gamma}(\beta)\backslash\dot{\Gamma}$.

5.2.6.1 *Exemples de Polynômes de Hilbert avec les Invariants de Gundlach*

Soit ℓ un nombre premier tel que $\ell = \beta\overline{\beta}$ avec des facteurs totalement positifs. On note $\overline{\Gamma} = \mathrm{SL}_2(\mathcal{O}_K)$; pour un $z \in \mathfrak{H}_1^2/\overline{\Gamma}$, les variétés β-isogènes et $\overline{\beta}$-isogènes sont respectivement définies par $\dfrac{1}{\beta}\gamma z$ et $\dfrac{1}{\overline{\beta}}\gamma z$ pour $\gamma \in \overline{\Gamma}$.
On considère les matrices:

$$S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \quad et \quad T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$$

et le sous-groupe de $\overline{\Gamma}$, $\overline{\Gamma}^0(\beta) = \left\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \overline{\Gamma} : \beta | b\right\}$ d'indice $\ell + 1$.
Alors on montre que l'ensemble des matrices:

$$C_\beta = \left\{S, T^i \,/\, i \in \{0, \cdots, \ell - 1\}\right\}$$

est un ensemble de représentants des classes d'équivalence de $\overline{\Gamma}/\overline{\Gamma}^0(\beta)$.
Alors on montre que le corps $\mathbb{C}_{\overline{\Gamma}^0(\beta)}/\mathbb{C}_{\overline{\Gamma}\cup\overline{\Gamma}_v}$ est une extension algébrique de degré $2[\overline{\Gamma} : \overline{\Gamma}^0(\beta)] = 2(\ell + 1)$ [78, Lemme 5.3.6.].

On définit les fonctions $\mathfrak{J}_{i,\beta}$ et $\mathfrak{J}_{i\beta}^{\gamma}$ de $\mathfrak{H}_1^2 \longrightarrow \mathbb{C}$: par

$$\mathfrak{J}_{i,\beta}(z) = \mathfrak{J}_i\left(\frac{1}{\beta}z\right) \quad et \quad \mathfrak{J}_{i,\beta}^{\gamma}(z) = \mathfrak{J}_i\left(\frac{1}{\beta}\gamma z\right)$$

pour $i = 1, 2$ et pour tout $\gamma \in \overline{\Gamma} \cup \overline{\Gamma}_v$. Ces fonctions ne sont pas en général symétriques.
Pour tous $\gamma \in \overline{\Gamma}^0(\beta)$ et $\gamma_\beta = \begin{pmatrix} a & b/\beta \\ c\beta & d \end{pmatrix} \in \overline{\Gamma}$ on a $\gamma_\beta \left(\frac{1}{\beta} z\right) = \frac{1}{\beta}\gamma z$. Par suite on montre que:

$$\mathfrak{J}^{\gamma}_{i,\beta}(z) := \mathfrak{J}_i\left(\frac{1}{\beta}\gamma z\right) = \mathfrak{J}_{i,\beta}(z).$$

Ainsi le corps des fonctions $\overline{\Gamma}^0(\beta)$-moduaires de Hilbert est

$$\mathbb{C}_{\overline{\Gamma}^0(\beta)} = \mathbb{C}\left(\mathfrak{J}_{i,\beta}, \mathfrak{J}_1, \mathfrak{J}_2\right) \quad \textit{pour} \quad i = 1, 2.$$

et le polynôme minimal de $\mathfrak{J}_{1,\beta}$ sur $\mathbb{C}_{\overline{\Gamma}\cup\overline{\Gamma}_v}$ sera noté $\Phi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2)$.
Pour ce qui suit, on considère ϵ l'unité fondamentale et ϵ' une unité totalement positive de $\mathcal{O}_K$ tel que cette dernière soit une puissance paire de ϵ. Alors $\mathfrak{J}_i(\epsilon' z) = \mathfrak{J}_i(z)$ et ainsi toute β-isogénie sera aussi une $\epsilon'\beta$-isogénie.
Pour $\ell = \beta\overline{\beta}$ avec $\beta \in \mathcal{O}_K^+$, on appelle β-polynômes modulaires, les polynômes définis par:
• Si ℓ est ramifié,

$$\phi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2) = \prod_{\gamma \in C_\beta} \left(X - \mathfrak{J}^{\gamma}_{1,\beta}\right) \quad et \quad \Psi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2) = \sum_{\gamma \in C_\beta} \mathfrak{J}^{\gamma}_{2,\beta} \frac{\Phi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2)}{(X - \mathfrak{J}^{\gamma}_{1,\beta})}$$

• Si ℓ se décompose,

$$\phi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2) = \prod_{\gamma \in C_\beta} \left(X - \mathfrak{J}^{\gamma}_{1,\beta}\right)\left(X - \mathfrak{J}^{\gamma}_{1,\overline{\beta}}\right) \quad et$$

$$\psi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2) = \sum_{\gamma \in C_\beta} \mathfrak{J}^{\gamma}_{2,\beta} \frac{\Phi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2)}{(X - \mathfrak{J}^{\gamma}_{1,\beta})} + \sum_{\gamma \in C_\beta} \mathfrak{J}^{\gamma}_{2,\overline{\beta}} \frac{\phi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2)}{(X - \mathfrak{J}^{\gamma}_{1,\overline{\beta}})}$$

On montre que les polynômes modulaires $\phi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2)$ et $\psi_\ell(X, \mathfrak{J}_1, \mathfrak{J}_2)$ sont des éléments $\mathbb{Q}(\mathfrak{J}_1, \mathfrak{J}_2)[X]$ et dépendent seulement de ℓ. (Aller à [78, Pages 152-153])

Proposition 5.2.4. *Les dénominateurs des polynômes modulaires ϕ_ℓ et ψ_ℓ sont divisibles:*

- *dans le cas $D = 5$ par un polynôme L_ℓ dans $\mathbb{Q}[\mathfrak{J}_1, \mathfrak{J}_2]$ paramétrant le lieu $\mathcal{L}_\ell$ des surfaces abéliennes principalement polarisées ayant multiplication réelle par $\mathcal{O}_K$ qui sont β-isogènes (ou $\overline{\beta}$-isogènes dans le cas décomposé) à un produit de courbes elliptiques.*
- *dans le cas $D = 2$ par un polynôme L'_ℓ dans $\mathbb{Q}[\mathfrak{J}_1, \mathfrak{J}_2]$ paramétrant $\mathcal{L}'_\ell$ le sous-ensemble de $\mathcal{L}_\ell$ défini par les pôles des invariants $\mathfrak{J}_1$ et $\mathfrak{J}_2$ c'est-à-dire les z telles que $H_4\left(\frac{1}{\beta}\gamma z\right) = 0$ (ou $H_4\left(\frac{1}{\overline{\beta}}\gamma z\right) = 0$ dans le cas décomposé), pour un certain $\gamma \in C_\beta$.*

Démonstration. (En utilisant le [78, Théorème 5.3.9. et Théorème 5.3.10.]). □

5.2.6.2 *Exemples de Polynômes de Hilbert avec les Invariants Thêta*

Dans cette section nous introduisons les β-polynômes modulaires proposés par E.Milio [78] pour obtenir des polynômes plus petits que ceux définis avec les invariants de Gundlach. En utilisant les tirés en arrière $\dot{\mathfrak{b}}_i = \phi^* \mathfrak{b}_i$ respectivement ou $\dot{\mathfrak{r}}_i = \phi^* \mathfrak{r}_i$ pour $i = 1, 2, 3$ des thêta constantes ou des invariants de Rosenhain comme invariants (la section 3.4.1 et la section 3.3), pour tout D sans facteur carré on arrive a construire des polynômes modulaires pour tout premier $\ell = \beta\overline{\beta}$ différent de 2. Cependant les sous-groupes utilisés sont différents selon D et les facteurs choisis de ℓ. Pour les detailles qui suivent nous nous focalisons sur le cas des

invariants thêta utilisant le groupe $\dot{\Gamma}(2,4)$; ces résultats peuvent être adapter au cas avec les invariants de Rosenhain en prennant le groupe $\dot{\Gamma}(2)$ à la place de $\dot{\Gamma}(2,4)$.
On considère les mêmes notations données à la section 3.4.1 et la section 3.3: $\dot{\Gamma} = \mathrm{SL}\left(\mathcal{O}_K \otimes \partial_K^{-1}\right)$ et $\mathfrak{H}_1^2/(\dot{\Gamma} \cap \dot{\Gamma}_v)$ est la *surface modulaire symétrique de Hilbert*. Les $\dot{\mathfrak{b}}_i$ sont des fonctions modulaires pour le sous-groupe $\dot{\Gamma}(2,4)$ et on montre que son sous-groupe $\dot{\Gamma}(2,4) \cap \dot{\Gamma}^0(\beta)$ est d'indice $(\ell+1)$. En effet pour tout $\gamma \in \dot{\Gamma}/\dot{\Gamma}^0(\beta)$, il existe un $\gamma' \in \dot{\Gamma}^0(\beta)$ tel que $\gamma'\gamma \in \dot{\Gamma}(2,4)$ [78, Lemme 5.3.11.].
On définit pour $i = 1,2,3$, les fonctions $\dot{\mathfrak{b}}_{i,\beta}$ et $\dot{\mathfrak{b}}_{i,\beta}^{\gamma}$ de $\mathfrak{H}_1^2 \longrightarrow \mathbb{C}$ telles que pour tous $\beta \in \mathcal{O}_K^+$ et $\gamma \in \dot{\Gamma} \cap \dot{\Gamma}_v$:

$$\dot{\mathfrak{b}}_{i,\beta}(z) = \dot{\mathfrak{b}}_i\left(\frac{1}{\beta}z\right) \quad et \quad \dot{\mathfrak{b}}_{i,\beta}^{\gamma}(z) = \dot{\mathfrak{b}}_i\left(\frac{1}{\beta}\gamma z\right)$$

Par des calculs directs, on montre que les fonctions $\dot{\mathfrak{b}}_i$ pour $i = 1,2,3$ sont modulaires pour le sous-groupe $\dot{\Gamma}(2,4) \cap \dot{\Gamma}^0(\beta)$ de $\dot{\Gamma}(2,4)$ lorsque:
• $D \equiv 1 \mod 4$;
• $D \equiv 2 \mod 4$ et $\beta = a + b\omega$ avec b pair (c'est à dire encore $\ell \equiv 1 \mod 4$) où $\mathcal{O}_K = \mathbb{Z} + \omega\mathbb{Z}$;
• $D \equiv 3 \mod 4$ et $\beta = a + b\omega$ avec b pair.
Ainsi pour ces cas le corps des fonctions modulaires de Hilbert invariantes par le sous-groupe $\dot{\Gamma}(2,4) \cap \dot{\Gamma}^0(\beta)$ est: $\mathbb{C}\left(\dot{\mathfrak{b}}_{i,\beta}, \dot{\mathfrak{b}}_1, \dot{\mathfrak{b}}_2, \dot{\mathfrak{b}}_3\right)$.

Pour le calcul des polynômes modulaires une différence considérable réside entre les cas $D \equiv 1 \mod 4$ et $D \equiv 2,3 \mod 4$. Dans le premier cas, l'application

$$\mathfrak{H}_1^2/\dot{\Gamma}(2,4) \longrightarrow \mathfrak{H}_2/\Gamma$$

est injective alors que dans le second, c'est bien l'application

$$\mathfrak{H}_1^2/\left(\dot{\Gamma}(2,4) \cup \dot{\Gamma}(2,4)_v\right) \longrightarrow \mathfrak{H}_2/\Gamma$$

qui est injective.
Ainsi pour $\ell = \beta\overline{\beta}$ avec $\beta \in \mathcal{O}_K^+$ et C_β un système de représentation des classes de $\dot{\Gamma}(2,4)/\dot{\Gamma}(2,4) \cap \dot{\Gamma}^0(\beta)$, on appelle β-polynômes modulaires pour K, les polynômes définis par:
• Si $D \equiv 1 \mod 4$,

$$\phi_\beta(X, \dot{\mathfrak{b}}_1, \dot{\mathfrak{b}}_2, \dot{\mathfrak{b}}_3) = \prod_{\gamma \in C_\beta}\left(X - \dot{\mathfrak{b}}_{1,\beta}^{\gamma}\right) \quad et$$

$$\psi_{k,\beta}(X, \dot{\mathfrak{b}}_1, \dot{\mathfrak{b}}_2, \dot{\mathfrak{b}}_3) = \sum_{\gamma \in C_\beta} \dot{\mathfrak{b}}_{k,\beta}^{\gamma} \frac{\phi_\beta(X, \dot{\mathfrak{b}}_1, \dot{\mathfrak{b}}_2, \dot{\mathfrak{b}}_3)}{X - \dot{\mathfrak{b}}_{1,\beta}^{\gamma}} \quad pour \quad k = 2,3.$$

• Si $D \equiv 2,3 \mod 4$ et $\beta = a + b\omega$ avec b pair, alors

$$\phi_\beta(X, \dot{\mathfrak{b}}_1, \dot{\mathfrak{b}}_2, \dot{\mathfrak{b}}_3) = \prod_{\gamma \in C_\beta}\left(X - \dot{\mathfrak{b}}_{1,\beta}^{\gamma}\right)\left(X - \dot{\mathfrak{b}}_{1,\beta}^{\gamma v}\right) \quad et$$

$$\psi_{k,\beta}(X, \dot{\mathfrak{b}}_1, \dot{\mathfrak{b}}_2, \dot{\mathfrak{b}}_3) = \sum_{\gamma \in C_\beta} \dot{\mathfrak{b}}_{k,\beta}^{\gamma} \frac{\phi_\beta(X, \dot{\mathfrak{b}}_1, \dot{\mathfrak{b}}_2, \dot{\mathfrak{b}}_3)}{X - \dot{\mathfrak{b}}_{1,\beta}^{\gamma}} + \sum_{\gamma \in C_\beta} \dot{\mathfrak{b}}_{k,\beta}^{\gamma v} \frac{\phi_\beta(X, \dot{\mathfrak{b}}_1, \dot{\mathfrak{b}}_2, \dot{\mathfrak{b}}_3)}{X - \dot{\mathfrak{b}}_{1,\beta}^{\gamma v}}$$

pour $k = 2,3$.

Lorsque $\mathcal{L}_\beta$ désigne le lieu des surfaces abéliennes principalement polarisées modulo $\dot{\Gamma}(2,4)$ ayant multiplication réelle par $\mathcal{O}_K$ telles que z, ou $\sigma(z)$ (dans le cas $D \equiv 2,3 \mod 4$) est β-isogène à z' avec $\phi(z')$ 2-isogène à un produit de courbes elliptiques par $\phi(z') \longrightarrow \phi(z')/2$ où $\theta_0(\phi(z')/2) = 0$.
Alors on montre par les mêmes arguments que dans le cas classique que tout polynôme L_β décrivant l'espace $\mathcal{L}_\beta$ est un facteur communs aux dénominateurs des polynômes modulaires ϕ_β et $\psi_{k,\beta}$.

Remarque 5.2.5.

— Lorsque l'on considère un autre couple $(\beta', \overline{\beta'})$ de $\mathcal{O}_K^+$ tel que $\beta'\overline{\beta'} = \ell$ et que : $\beta' = \epsilon^{2n}\beta$ pour ϵ une unité fondamentale de norme 1 ou -1. Alors cela implique que pour tout $z \in \mathfrak{H}_1^2$:

$$\dot{\mathfrak{b}}_{i,\beta'}(z) = \dot{\mathfrak{b}}_i\left(\left(\begin{smallmatrix}\epsilon^n & 0\\ 0 & \epsilon^{-n}\end{smallmatrix}\right)\frac{1}{\beta}z\right) \quad \textit{pour} \quad i = 1,2,3.$$

Ainsi on peut en déduire les β'-polynômes modulaires.

— Lorsque l'on connaît les β-polynômes modulaires ϕ_β et $\psi_{k,\beta}$ pour $k = 2,3$ alors à partir des propriétés suivantes :
$(\dot{\mathfrak{b}}_1^v, \dot{\mathfrak{b}}_2^v, \dot{\mathfrak{b}}_3^v) = (\dot{\mathfrak{b}}_1, \dot{\mathfrak{b}}_2, \dot{\mathfrak{b}}_3)$ pour tout $D \equiv 2,3 \mod 4$,
$(\dot{\mathfrak{b}}_1^v, \dot{\mathfrak{b}}_2^v, \dot{\mathfrak{b}}_3^v) = (\dot{\mathfrak{b}}_3, \dot{\mathfrak{b}}_2, \dot{\mathfrak{b}}_1)$ pour tout $D \equiv 1 \mod 4$
définies par l'action de σ sur $\mathcal{H}_1^2$, on déduit les $\overline{\beta}$-polynômes modulaires $\phi_{\overline{\beta}}$ et $\psi_{k,\overline{\beta}}$.

Troisième partie

RELÈVEMENT CANONIQUE DE SURFACES ABÉLIENNES

6

GÉNÉRALITÉ SUR LE RELÈVENEMENT CANONIQUE

En resumé nous avons parcouru des résultats fondamentaux sur le schéma $\mathfrak{A}_g$ des variétés abéliennes complexes et plus particulièrement sur le schéma $\mathfrak{A}_2$ dont le corps de fonctions est donné par $\mathbb{C}(j_1, j_2, j_3)$. D'une autre part un résultat très important d'Igusa [51] montre que $\mathcal{M}_2$ est un schéma non lisse sur $\mathbb{Z}$ (le chapitre 4 et la section 4.2) sur lequel nous avons construit des invariants absolus ayant une bonne réduction en toute caractéristique.

L'objectif de cette section est d'aboutir à une généralisation des *conditions de Kronecker* utilisées en dimension 1 à partir du polynôme modulaire le chapitre 2 et la section 2.5.1. En effet la proposition 6.2.1(Conditions de Kronecker en Dimension g) qui suit est l'un de nos résultats fondamentaux fournissant les bases algorithmiques d'un calcul éfficace du relevé canonique en fonction du genre g et de la caractéristique moyenne p.

6.1 THÉORÈME DE SERRE-TATE

Dans cette section nous nous focalisons sur un important résultat de J.P.Serre et J.Tate [69, 104], établissant l'équivalence entre la théorie de la déformation des schémas abéliens et celle associée à leurs groupes p-divisibles.
Nous ne proposons pas une démonstration de ce résultat et nous allons nous referer sur les démonstrations de Drinfeld dans l'article de Katz [55].
Notre objectif serait d'établir une forme plus générale des *conditions de Kronecker*. Et pour ce qui suit nous admettons les notations et définitions suivantes.
On considère que $p > 0$ est un nombre premier et R est un anneau admettant un idéal nilpotent I tel que $R_0 := R/I$. On pose $S_0 = Spec(R_0)$ et $S = Spec(R)$ de telle sorte que $S_0 \hookrightarrow S$ soit un éppaississement infinitésimal.

Groupes p-Divisibles

Lorsque R est un anneau Noétherien localement complet.
Un système inductif $(G(n))_{n\in\mathbb{N}}$ de schéma de groupes sur R est un *groupe p-divisible* de hauteur h: si $G(n)$ est fini d'ordre p^{nh} et pour tout $n \geq 1$, la suite suivante est exacte,

$$1 \longrightarrow G(n) \longrightarrow G(n+1) \xrightarrow{p^n} G(n+1)$$

Ainsi $G(n)$ est identifié comme le groupe de p^n-torsion de $G(n+1)$ et pour cette raison on note très souvent $G(n)$ par $G[p^n]$ et le groupe p-divisible par G.
Nous pouvons aussi noter la définition proposée par Grothendieck où G est un faisceau abélien sur un site de *fppf* (fidèlement plate de présentation finie) telle que :

$$G = \varinjlim G[p^n]$$

avec $[p] : G \longrightarrow G$ est un épimorphisme de gerbes abéliennes et $G[p^n]$ est le noyau donné sur un point de $[p^n] : G(T) \longrightarrow G(T)$.
Alors on montre que pour tout groupe commutative algébrique G/S de type fini tel que

$[p] : G \to G$ est localement libre de rang p^h, $G[p^\infty] := (G[p^n])$ est un groupe p-divisible de hauteur h. Et plus partculièrement pour un schéma abélien A/S de dimension g, $A[p^\infty]$ est un groupe p-divisible de hauteur $2g$. Soit $S_0 \hookrightarrow S$ un appaississement infinitésimal avec p localement nilpotent sur S. Alors on désignera par $\mathsf{AbVar}(S)$ la catégorie des schémas abéliens sur S et par $\mathcal{D}(S_0)$ la catégorie des triplets (A_0, G, i) où A_0/S_0 est un schéma abélien, G/S est un groupe p-divisible et i un isomorphisme $A_0[p^\infty] \xrightarrow{\sim} G \otimes_S S_0$.

Théorème 6.1.1. *(Théorème de Serre-Tate)*
Le foncteur :

$$\begin{array}{rccc} \Phi : & \mathsf{AbVar}(S) & \longrightarrow & \mathcal{D}(S_0) \\ & A & \longmapsto & (A \otimes S_0, A[p^\infty], i) \end{array}$$

est une équivalence de catégories.

Démonstration. Aller à [55]. □

Corollaire 6.1.2. *(Applications)*

- *Soient A_0/S_0 un schéma abélien et G/S un groupe p-divisible tel qu'il existe un isomorphisme $i_0 : A_0[p^\infty] \xrightarrow{\sim} G_0$ de groupes p-divisible. Alors par le* Théorème de Serre-Tate *(A_0, i_0) admet un relèvement (A, i) où A est un schéma abélien et un isomorphisme $i : A[p^\infty] \xrightarrow{\sim} G$ de groupes p-divisible.*
- *Soient A/S, B/S des schémas abéliens et $f_0 \in \mathrm{Hom}_{S_0}(A_0, B_0)$ alors par le* Théorème de Serre-Tate, *f_0 admet un relèvement $f \in \mathrm{Hom}_S(A, B)$ si et seulement si $f_{0,p} \in \mathrm{Hom}(A[p^\infty], B[p^\infty])$ admet sur $\mathrm{Hom}(A[p^\infty], B[p^\infty])$ un relèvement. Et ces relèvements lorsqu'ils existent sont uniques.*

Démonstration. Voir [27, § 1.]. □

Le *Théorème de Serre-Tate* trouve plusieurs extension avec l'utilisation des Théories de Modules de Dieudonné: *contravariant, covariant et crystalline* pour s'élargir sur d'autres angles.

6.2 CONDITIONS DE KRONECKER

Dans l'objectif, d'une démonstration générale aux *conditions de Kronecker* rencontrés dans le chapitre 2 et la section 2.5.1, nous introduisons au debut de cette section la notion de champ algébrique ("stack"), qui est une généralisation du concept de schéma, au même sens que le concept de schèma est une généralisation du concept de variété projective. Nous utiliserons comme reférences, des travaux de D.Mumford [87] , de Normann-Oort [90], de Tomás L. Gómez [40] et plus principalement nous allons nous focaliser sur les travaux [15] de Ching-Li Chai et P.Norman.
$\mathfrak{A}_g$ et $\mathcal{M}_g$ ne sont pas des espaces de modules fins, dû au fait que des points sur $\mathfrak{A}_g$ et $\mathcal{M}_2$ ont des automorphismes supplémentaires. L'idée serait d'obtenir des " espace de module fin " à la place de $\mathfrak{A}_g$ et $\mathcal{M}_g$. Alors, on procède par adjonction de structure supplémentaire (structures de niveau p par exemple) pour « tuer l'effet » des automorphismes (suivant des idées qui remontent à Grothendieck et Giraud, et développées par Deligne, Mumford et Artin) en remplaçant le foncteur $F : (\mathrm{Sch}) \to (\mathrm{Ens})$ par un autre foncteur F' muni d'un morphisme $\phi : F' \to F$ (oubli de la structure supplémentaire) de telle sorte que F' soit un espace algébrique . Alors on dira qu'un faisceau d'ensembles sur Sch est représentable par

un schéma M s'il est isomorphe au foncteur des points $\mathrm{Hom}_S(-, M)$ (où M est un schéma sur S). Ce qui n'est pas le cas de $\mathfrak{A}_g$ et $\mathcal{M}_g$.
Dans le cas du module grossier « coarse » M, le schéma M est coreprésenté par un foncteur F tel que pour tout corps algébriquement clos $\mathbb{k}$ on a la bijection:

$$\phi(\mathbb{k}) : F(\mathrm{Spec}\,\mathbb{k}) \longrightarrow \mathrm{Hom}_S(\mathrm{Spec}\,\mathbb{k}, M)$$

Par exemple dans le cas du morphisme $\mathrm{Ell} \to \mathbb{A}^1$.
Un préfaisceau dans les groupoïdes (également appelé quasi-foncteur) est un 2-foncteur F contravariant de (Sch/S) à (groupoïdes). Pour chaque schéma B nous avons un groupoïde $F(B)$ et pour chaque morphisme $f : B' \to B$ nous avons une transformation naturelle des foncteurs $F(f)$ qui est notée f^* (définie par un pullback dans nos exemples). *Alors on peut définir un champ « stack » comme un faisceau de groupoïdes, c'est-à-dire un 2-functor (préfaisceau) qui satisfait les axiomes du faisceau à savoir les principes de: "recollement de morphismes", "mono-préfaisceau" et "recollement d'objets"* [40, Definition 2.10]. Ce qui implique: qu'un champs admettant un objet avec un automorphisme autre que l'identité, ne peut être représenté par un schéma. Un champ $\mathcal{X}$ est dit représentable par un espace algébrique (resp. schéma) s'il existe un espace algébrique (resp. schéma) X tel que le champ associé à X est isomorphe à $\mathcal{X}$.
Alors nous allons définir un *champ algébrique* selon Deligne-Mumford. Cette définition est semblable à celle généralement donnée à un espace algébrique (dans le contexte correspondant aux espaces) .
Lorsque l'on considère la catégorie (Sch/S) des S-schémas muni de la topologie étale, un champ F est appelé un champ algébrique (Deligne-Mumford) si : le morphisme diagonale $\Delta F : F \to F \times_S F$ est représentable, quasi-compact et separé ; de plus il existe un schéma U (appelé atlas) avec un morphisme étale surjectif $u : U \to F$.
Soit $\mathfrak{A}_{g,\Gamma_0(p)}$ le champ algébrique paramétrant les variétés abéliennes principalement polarisées avec une structure de niveau p.
Pour tout schéma S, $\mathfrak{A}_{g,\Gamma_0(p)}(S)$ est la catégorie des isogénies.

$$\begin{array}{ccc} A_1 & \xrightarrow{\ \phi\ } & A_2 \\ & \swarrow & \\ & S & \end{array}$$

des schémas abéliens principalement polarisés $(A_{i/S},\ \lambda_{A_i})$, $i = 1, 2$ tels que la polarisation $\phi^*(\lambda_{A_2})$ définie par $\hat{\phi} \circ \lambda_{A_2} \circ \phi$ coïncide avec $p \cdot \lambda_{A_1}$. En particulier $\mathfrak{A}_{2,\Gamma_0(p)}$ est régulier excepter en un nombre fini de points. Ces points isolés singuliers correspondent aux isogénies $\phi : A_1 \longrightarrow A_2$ de $\mathfrak{A}_{2,\Gamma_0(p)} \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p$ où les trois composantes irréductibles de $\mathfrak{A}_{2,\Gamma_0(p)}$ s'intersectent [15]. Par exemple en caractéristique 2, ces trois composantes sont respectivement définies sur la variété $\mathcal{M}_2 \otimes \mathbb{k}$ par les trois premiers triplets du 4.3.2 dans le chapitre 4 et la section 4.3.Cependant on remarquera que dans ce cas-ci la topologie est fine (dans le cas de $\mathcal{M}_2$ elle est grossière) .
Dans ce qui suit, notre objectif est de trouver une démonstration aux *conditions de Kronecker* sur le lieu des points ordinaires de l'espace de module de Siegel de $\mathfrak{A}_{g,\Gamma_0(p)}$ muni d'une structure de niveau $\Gamma_0(p)$. Le module $\mathfrak{A}_{g,\Gamma_0(p)}$ a été étudié en profondeur par P.Norman et

Ching-Li Chai comme schéma sur Spec $\mathbb{Z}_p$ (pour plus de détails, voir [15]). Et en général, on montre d'après la théorie de déformation de variétés abéliennes ordinaires [55], que son lieu des points ordinaires noté $\mathfrak{A}^0_{g,\Gamma_0(p)}$ est lisse sur Spec $\mathbb{Z}_p$.

On considère pour la suite que le corps $\Bbbk$ est algébriquement clos et de caractéristique $p > 0$. Pour une variété abélienne ordinaire $A_{/\Bbbk}$, le module de Tate et son dual sont donnés par:

$$T_pA(\Bbbk) = \varprojlim A[p^n](\Bbbk), \quad T_p\hat{A}(\Bbbk) = \varprojlim \hat{A}[p^n](\Bbbk)$$

D'après le résultat [15, Theorem Pages:12-13] le Théorème de Serre-Tate implique que pour tout point géométrique $(\phi : A_{/\Bbbk} \longrightarrow B_{/\Bbbk}, \lambda_A, \lambda_B)$ du lieu $\mathfrak{A}^0_{g,\Gamma_0(p)}$ avec $\phi^*(\lambda_B) = p \cdot \lambda_A$. Alors ϕ induit deux applications $\mathbb{Z}_p$-linéaires l'une $F : V = T_pA(\Bbbk) \longrightarrow W = T_pB(\Bbbk)$ et l'autre $T : W \longrightarrow V$ (à partir de son dual $\hat{\phi}$) telles que $T \circ F = p \cdot \mathrm{id}_V$ et $F \circ T = p \cdot \mathrm{id}_W$ et le foncteur contravariant $\mathfrak{M}$ de Dieudonné est canoniquement donné par:

$$R \longmapsto \left\{ \begin{array}{c} \text{couplages symétriques} \\ \langle\ ,\ \rangle_V : V \otimes_{\mathbb{Z}_p} V \to 1 + m_R \\ \langle\ ,\ \rangle_W : W \otimes_{\mathbb{Z}_p} W \to 1 + m_R \\ \text{telles que} \\ \langle u, T(w)\rangle_V = \langle F(v), w\rangle_W,\ \forall v \in V, w \in W \end{array} \right\}$$

où R parcourt les anneaux artiniens locaux dont le corps résiduel est $\Bbbk$.
Lorsque l'on désigne respectivement par $(v_1, \cdots, v_g)$ et $(w_1, \cdots, w_g)$ les $\mathbb{Z}_p$-bases de V et de W le résultat précédent peut être interpréter en terme de rélations linéaires algébriques de la manière suivantes:

$$\{F(v_i) = w_i \ \text{ et } \ F(v_{a+j}) = p \cdot w_{a+j}\} \quad \text{et}$$
$$\{T(w_i) = p \cdot v_i \ \text{ et } \ T(w_{a+j}) = v_{a+j}\}$$
$$\text{pour } 1 \leq i \leq a,\ 1 \leq j \leq g$$
$$\text{où} \quad p^a = \#\left(V/T(W)\right)$$

En utilisant les conditions de couplages symétriques sur ces rélations précédentes on obtient:

$$\left\{ \begin{array}{ll} \langle v_i, pv_j\rangle_V = \langle w_i, w_j\rangle_W & \text{pour} \quad 1 \leq i, j \leq a \\ \langle v_\mu, pv_i\rangle_V = \langle pw_\mu, w_i\rangle_W & \text{pour} \quad 1 \leq i \leq a,\ a+1 \leq \mu \leq g \\ \langle v_i, v_\mu\rangle_V = \langle w_i, w_\mu\rangle_W, & \text{pour} \quad 1 \leq i \leq a,\ a+1 \leq \mu \leq g \\ \langle v_\mu, v_\nu\rangle_V = \langle w_\mu, w_\nu\rangle_W, & \text{pour} \quad a+1 \leq \mu, \nu \leq g \end{array} \right.$$

En résumé chaque module artinien local du [15, Theorem Pages:12-13] définit un couplage symétrique tel que en un point géométrique $(\phi : A_{/\Bbbk} \longrightarrow B_{/\Bbbk}, \lambda_A, \lambda_B)$ du lieu $\mathfrak{A}^0_{g,\Gamma_0(p)}$ de l'espace de module de Siegel $\mathfrak{A}^0_{g,\Gamma_0(p)}$, le système $\mathfrak{S} = 0$ dont les équations sont défines par les g^2 fonctions suivantes:

$$\mathfrak{S} = \left\{ \begin{array}{ll} \langle v_i, pv_j\rangle_V - \langle w_i, w_j\rangle_W & \text{pour} \quad 1 \leq i, j \leq a \\ \langle v_j, pv_i\rangle_V - \langle pw_j, w_i\rangle_W & \text{pour} \quad 1 \leq i \leq a,\ a+1 \leq j \leq g \\ \langle v_i, v_j\rangle_V - \langle w_i, w_j\rangle_W, & \text{pour} \quad 1 \leq i \leq a,\ a+1 \leq j \leq g \\ \langle v_i, v_j\rangle_V - \langle w_i, w_j\rangle_W, & \text{pour} \quad a+1 \leq i, j \leq g \end{array} \right.$$

satisfait la condition:

$$\mathfrak{S}(\hat{\phi}, \phi) = 0$$

En utilisant les propriétés de symétrie des formes bilinéaires $\langle\ ,\ \rangle_V$ et $\langle\ ,\ \rangle_W$ on peut définir le système $\mathfrak{S} = 0$ de manière plus simple en ne considerant que les équations contenant les valeurs:

$$\langle v_i, v_j\rangle_V \quad 1 \leq i \leq j \leq a, \qquad \langle w_\nu, w_\mu\rangle_W, \quad 1 \leq \nu \leq \mu \leq g$$
$$\langle v_i, v_\mu\rangle_V \left(= \langle w_i, w_\mu\rangle_W\right), \qquad 1 \leq i \leq a,\ a+1 \leq \mu \leq g$$

D'autre part, le schéma $\mathfrak{A}^0_{g,\Gamma_0(p)}$ des points ordinaires de $\mathfrak{A}_{g,\Gamma_0(p)}$ est lisse sur $\mathrm{Spec}(\mathbb{Z}_p)$ de dimension $g\dfrac{(g+1)}{2}$ [15, Theorem 3.3, Page: 13].

Par suite nous pouvons considérer la fonction vectorielle $\mathfrak{S}$ avec seulement les $g\dfrac{(g+1)}{2}$ fonctions définies précédemment.

Proposition 6.2.1. *(Conditions de Kronecker)*
Pour tout point géométrique $(\Pi : A_{/\Bbbk} \longrightarrow A^{\Pi}_{/\Bbbk}, \lambda_A)$ du lieu $\mathfrak{A}^0_{g,\Gamma_0(p)}$ des points ordinaires de $\mathfrak{A}_{g,\Gamma_0(p)}$, la fonction vectorielle $\mathfrak{S}$ satisfait les conditions:

1. $\dfrac{\partial\mathfrak{S}}{\partial X}(\hat{\Pi}, \Pi)$ *s'annule modulo p,*
2. $\dfrac{\partial\mathfrak{S}}{\partial Y}(\hat{\Pi}, \Pi)$ *est inversible modulo p.*

Démonstration. Lorsque nous sommes en dimension $g = 1$, soit V et W représentant respectivement les modules de Tate associés à A et A^σ du point géométrique $(\Pi : A_{/\Bbbk} \longrightarrow A^{\Pi}_{/\Bbbk}, \lambda_A, \lambda_{A^{\Pi}_{/\Bbbk}})$. Alors sur $\mathbb{Z}_p$ nous avons: $V = \langle v\rangle$ et $W = \langle w\rangle$. En considérant les notations ci-dessus, on note par T l'application linéaire induite par le Verschiebung à partir de $A^{\Pi}_{/\Bbbk}$, alors $\#\left(V/T(W)\right) = p$ et $a = 1$. Dans ce cas, le système $\mathfrak{S} = 0$ admet une seule équation définie par la valeur:

$$\mathfrak{S} = \langle v, T(w)\rangle_V - \langle F(v), w\rangle_W$$

Lorsque l'on considère le couplage $\langle v, v\rangle = X$ et $\langle w, w\rangle = Y$, nous obtenons:

$$\mathfrak{S} = \langle v, p.v\rangle - \langle w, w\rangle = X^p - Y$$

Alors :

- $\dfrac{\partial\mathfrak{S}}{\partial X}(\hat{\Pi}, \Pi) = pX^{p-1}$ s'annule modulo p ;
- $\dfrac{\partial\mathfrak{S}}{\partial Y}(\hat{\Pi}, \Pi) = -1$ est inversible modulo p, en effet le vecteur $(\hat{\Pi}, \Pi)$ représente un point du schéma lisse $\mathfrak{A}^0_{g,\Gamma_0(p)}$ de dimension 1 sur $\mathbb{Z}_p$.

Dans le cas de la dimension g nous avons $\#\left(V/T(W)\right) = p^g$ c'est-à-dire $a = g$.
Les fonctions constituant la fonction vectorielle $\mathfrak{S}$ sont toutes de la forme:

$$X^p_{ij} - Y_{ij} \quad \text{pour} \quad 1 \leq i \leq j \leq g$$

Alors, posons $X = \{X_{ij}\}$ et $Y = \{Y_{ij}\}$ tels que $X_{ij} = \langle v_i, v_j\rangle$ et $Y_{ij} = \langle w_i, w_j\rangle$ pour $1 \leq i \leq j \leq g$ on obtient:

- $\frac{\partial \mathfrak{S}}{\partial X}(\hat{\Pi}, \Pi)$ s'annule modulo p ; car les composantes de cette matrice sont les pX_{ij}^{p-1}.
- $\frac{\partial \mathfrak{S}}{\partial Y}(\hat{\Pi}, \Pi) = -\mathrm{Id}_m$ est inversible modulo p, en effet $(\hat{\Pi}, \Pi)$ représentent un point du schéma lisse $\mathfrak{A}^0_{g,\Gamma_0(p)}$ de dimension $m = g\frac{(g+1)}{2}$ sur $\mathbb{Z}_p$.

□

Remarque 6.2.2. Pour les chapitres qui vont suivre, nous allons travailler sur l'espace de module grossier $\widehat{\mathfrak{A}}_g$ paramétré par des polynômes modulaires de Siegel ou de Hilbert plutôt que sur l'espace de module fin $\mathfrak{A}_{g,\Gamma_0(p)}$. Une différence considérable entre la structure canonique de "stack" de $\mathfrak{A}_{g,\Gamma_0(p)}$ et la structure "coarse" de $\widehat{\mathfrak{A}}_g$ est que certains points de $\mathfrak{A}^0_{g,\Gamma_0(p)}$ ne sont pas lisses sur le schéma $\widehat{\mathfrak{A}}_g$. En effet ces points représentent des surfaces abéliennes ayant des automorphismes supplémentaires. C'est-à-dire par exemple des points sur $\mathcal{M}_2$ tels que $\mathrm{Aut}(\mathcal{C}) \not\simeq C_2$ ou des points $j = 0,\ 1728$ sur la courbe modulaire en dimension 1. Le lieu des points lisses de $\mathfrak{A}_g$ est birationnellement équivalente au schéma décrit par l'équation modulaire. Lorsque $g = 1$, à partir des opérations de "blowups" on pourait rendre ce schéma modulaire lisse en les points ordinaires (avec automorphismes triviaux) de $\mathfrak{A}_g$, pour en faire un espace de module grossier. Ce qui pourra bien étendre le domaine de réalisation des conditions de Kronecker en dimension 1 en les points $j \in \mathbb{F}_{p^2}$ de $\mathfrak{A}_{1,\Gamma_0(p)}$ sauf pour $j = 0,\ 1728$ (dans le chapitre 2 et la section 2.5.1, le domaine de réalisation des conditions de Kronecker était $j \notin \mathbb{F}_{p^2}$). Cependant les blowups ne sont suffisant pour lissifier que sur une courbe, ie $g = 1$ d'après [92].

En résumé les conditions Kronecker fournissent une généralisation de la méthode de calcul du rélévé canonique de Satoh aux variétés abéliennes ordinaires.
D'autre part on pourait se demander qu'en est-il des variétés abéliennes non-ordinaires ?
Dans [85] Mumford avait établi un programme pour répondre à cette question. Son approche réposait sur le fait que le point générique de chaque composante de l'espace de module grossier $\widehat{\mathfrak{A}}_g$ correspond à une variété abélienne ordinaire. Alors on pourra réléver chaque composante à partir de son point générique. Et cela était suffisant car on sait comment réléver chaque point générique par les méthodes de relèvement canonique.
Cependant c'est à partir des travaux de F.Oort et P.Norman [90] que l'on retrouve les caractéristiques du relèvement d'une variété abélienne d'un corps $\Bbbk$ sur anneau intègre R de caractéristique zéro.

6.3 RÉDUCTION STABLE DES COURBES DE GENRE 2

Soit $\mathcal{C}$ une courbe lisse sur $\mathbb{Q}_q$, géométriquement connexe de genre $g \geq 1$. D'après un théorème de Deligne et Mumford , il existe une extension finie de K de $\mathbb{Q}_q$, telle que la courbe $\mathcal{C}_s = \mathcal{C} \times_R \overline{\mathbb{F}_q(s)}$ est une courbe stable sur $\overline{\mathbb{F}_q}$ ne dépendant pas du choix de s ni de K. Lorsque nous sommes en dimension 1 si $\mathrm{j}_E \in \mathbb{Z}_q$ est le j-invariant d'une courbe elliptique E, alors E_s est lisse sur $\mathbb{F}_q$, si $\mathrm{j} \notin \mathbb{Z}_q$, alors $\mathcal{C}_s$ est une courbe rationnelle avec un seul point double ordinaire.
Ainsi un modèle stable d'une courbe $\mathcal{C}$ sur R est une courbe stable sur R à fibre générique isomorphe $\mathcal{C} \times_K Frac(R)$ [92].

Lorsque $g = 2$ et que la courbe $\mathcal{C}$ admet comme équation hyperelliptique:

$$y^2 + h(x)y = f(x), \quad \textit{avec} \quad h, f \in \Bbbk[x] \quad \textit{et} \quad \deg h \leq 2, \deg f \leq 5 \textit{ or } 6$$

Si la caractéristique de $\Bbbk \neq 2$ nous pouvons réduire l'equation précédente à $y^2 = a_0x^5 + \cdots + a_5$ et l'on peut définir J_{2i} en fonction de $(a_0, \cdots, a_5)$:

$$\begin{aligned}
J_2 &= 5a_0a_4 - 2a_1a_3 + 2^{-2}3a_2^2;\\
J_4 &= -2^{-3}(5^2a_0^2a_3a_5 - 3\cdot 5a_0^2a_4^2 - 3\cdot 5a_0a_1a_2a_5 + 7a_0a_1a_3a_4 +\\
&\quad 2^{-1}a_0a_2^2a_4 - a_0a_2a_3^2 + 2^2a_1a_5 - a_1^2a_2a_4 - a_1^2a_3^2 + a_1a_2^2a_3 - 2^{-4}3a_2^4);\\
J_6 &= -2^{-4}(2^{-1}5^3a_0^3a_2a_5^2 - 5^2a_0a_3a_4a_5 + 5a_0^3a_4^3 - 5^2a_0^2a_1^2a_5^2 -\\
&\quad 2\cdot 5a_0^2a_1a_2a_4a_5 + 2\cdot 5a_0^2a_1a_3^2a_5 - a_0^2a_1a_3a_4^2 - 2^{-2}5a_0^2a_2^2a_3a_5 -\\
&\quad 2^{-2}11a_0^2a_2^2a_4^2 + 2^{-1}7a_0^2a_2a_3^2a_4 - a_0^2a_3^4 + 2\cdot 3a_0a_1^3a_4a_5 - 3a_0a_1^2a_2a_3a_5\\
&\quad + 2^{-1}7a_0a_1^2a_2a_4^2 - 2a_0a_1^2a_3^2a_4 + 2^{-2}3a_0a_1a_2^3a_5 - 2^{-2}7a_0a_1a_2^2a_3a_4 +\\
&\quad a_0a_1a_2a_3^3 + 2^{-4}7a_0a_2^4a_4 - 2^{-2}a_0a_2^3a_3^2 - a_1^4a_4^2 + a_1^3a_2a_3a_4 -\\
&\quad 2^{-2}a_1^2a_2^3a_4 - 2^{-2}a_1^2a_2^2a_3^2 + 2^{-3}a_1a_2^4a_3 - 2^{-6}a_2^6).
\end{aligned}$$

Et d'autre part $J_8 = 2^{-2}(J_2J_6 - J_4^2)$ et J_{10} est défini par le discrimant D.
Lorsque la caractéristique de $\Bbbk = 2$, les invariants J_{2i} correspondant sont alors les reductions modulo 2 de ceux obtenus sur $\mathbb{Z}_q$ en utilisant la forme $y^2 = \tilde{h}^2 + 4\tilde{f}$ où $\tilde{h}$ et $\tilde{f}$ sont les relévés de h et f sur $\mathbb{Z}_q$.

Soient K une extension finie de $\mathbb{Q}_q$, R la clôture intégrale de $\mathbb{Z}_q$ dans K. On dira que $\mathcal{C}$ est *à réduction stable sur K* si elle admet un modèle stable sur une localisation R' de R en un idéal maximal dont la fibre spéciale géométrique est notée $\mathcal{C}_s$ sur R'. Cette courbe sur $\overline{\mathbb{F}_q}$ ne dépend pas du choix de R', ni de celui de sa localisation.
Soit J_{2i} avec $1 \leq i \leq 5$, les invariants associés à une équation

$$y^2 + h(x)y = f(x)$$

Théorème 6.3.1. *Alors on a:*

- *la courbe $\mathcal{C}_s$ est lisse si et seulement si: $J_{2i}^5 J_{10}^{-i} \in \mathbb{Z}_q$ pour tout $i = 1, \cdots, 5$;*
- *$\mathcal{C}_s$ est irréductible avec un seul point double si et seulement si: $J_{2i}^6 I_{12}^{-i} \in \mathbb{Z}_q$ pour tout $i = 1, \cdots, 5$ et $J_{10}^6 I_{12}^{-5} \in p\mathbb{Z}_q$*
- *$\mathcal{C}_s$ est totalement dégénérée si et seulement si*

$$I_{12}I_4^{-3} \in p\mathbb{Z}_q, \quad J_{10}^2 I_4^{-5} \in p\mathbb{Z}_q, \quad J_{10}I_{2e}I_4^{-3e} \in p\mathbb{Z}_q.$$

où $e = 4$ si $p = 2$, $e = 3$ si $p = 3$ sinon $e = 1$.

Démonstration. Le premier point du théorème est une conséquence directe du [51, Théorème 6].
Les deux autres sont des cas particuliers du [92, Théorème 1]. On peut les démontrer selon le même procédé que dans [92, Théorème 1]. En vérifiant directement par calculs sur un ouvert affine de $\mathcal{C}$ dense dans toutes les fibres pour les cas $p \neq 2$ et $\mathcal{C}_s$ n'est pas réunion de deux courbes elliptiques d'invariant modulaire nul. Sinon pour les autres cas [92] utilisent la continuité sur l'espace de module $\overline{\mathcal{M}} \times \mathbb{Z}_q$. □

Exemple 6.3.2. Nous donnons par suite les exemples suivants (aller à [92] pour plus détails) comme des applications aux propriétés citées précédemment .

— Soit $\mathcal{C}$ la courbe sur $\mathbb{Q}$ définie par l'équation: $y^2 + y = x^5$. On vérifie que $J_{2i} = 0$ pour tout $i \neq 5$ et $J_{10} = 5^5$. On en déduit que $\mathcal{C}$ a bonne réduction partout.

— Soit $\mathcal{C}$ la courbe sur $\mathbb{Q}$ définie par l'équation: $y^2 = x^5 + x$. On vérifie que:

$$J_2 = 5, \quad J_4 = 2^{-3}15, \quad I_4 = -2^2.5, \quad J_6 = -2^{-4}5,$$

$$J_8 = -2^{-8}325, \quad J_{10} = 2^{-4}, \quad I_{12} = -2 \cdot 25.$$

D'après le théorème précédent la courbe $\mathcal{C}$ a bonne réduction en toute place différente de 2, sa réduction stable $\mathcal{C}_s$ est la réunion de deux courbes elliptiques d'invariant modulaire nul.

7

CALCUL DE RELEVÉ CANONIQUE EN DIMENSION 2

Dans ce chapitre nous proposons une extension de la methode de Satoh en genre 2. Ce résumé détaille un peu plus nos nouveaux résultats exposés dans les deux premiers papiers ([70, 71]).

7.1 AVEC L'ESPACE MODULAIRE DE SIEGEL

7.1.1 *Conditions de Kronecker sur l'Espace de Siegel*

Dans cette section abordons une propriété très importante des polynômes modulaires sur $\mathbb{Z}_q$. On part d'une variété abélienne $\mathcal{A}$ définie sur $\mathbb{Z}_q$, et l'on se propose d'étudier les différentes types de réductions des (p^3+p^2+p+1) noyaux de $\mathcal{A}$.

Réduction des (p^3+p^2+p+1) Isogénies

On considère les points P, Q, R et S avec: P et Q étales, R et S ramifiés et tels que R est le dual de P et S le dual de Q pour le Couplage de Weil. Un noyau isotropique K de l'isogénie de degré p partant de $\mathcal{A}$ a trois possibilités de réduction sur $\overline{\mathcal{A}}$:

- *Dans un premier cas* : $K = \langle R, S\rangle$, alors il se réduit entièrement sur $\langle 0\rangle$ et cela correspond au noyau du relèvement du Frobenius.
- *Dans second cas* : K se réduit modulo p à un groupe cyclique d'ordre p. Comme modulo p nous avons $(p+1)$ groupes cycliques d'ordre p sous les formes: $\langle \overline{P} + b\overline{Q}\rangle$ and $\langle \bar{Q}\rangle$ avec $0 \leq b < p-1$. Supposons que K réduit sur $\langle \overline{P}\rangle$, alors K est sous la forme $\langle P + aR + bS, cR + dS\rangle$. En utilisant les conditions de linéarité et d'isotropie nous obtenons $K = \langle P + aR, S\rangle$. Cela correspond à p choix pour chaque groupe cyclique d'ordre p modulo p. Et nous avons $(p+1)p$ noyaux relevés.
- *Et dans le troisième cas*, K se réduit sur $\langle \overline{P}, \overline{Q}\rangle$ alors il est sous la forme $\langle P + aR + bS, Q + cR + dS\rangle$. En appliquant les conditions de linéarité et d'isotropie sur ces bases l'on obtient $b = c$. Cela correspond à p^3 noyaux.

Ce qui complète la réduction des p^3+p^2+p+1 isogénies correspondant aux solutions du système défini sur $\mathbb{Z}_q$ par les polynômes $\phi_{1,p}$, $\psi_{1,p}$ et $\psi_{1,p}$.
On considère les polynômes modulaires $\phi_{1,p}$, $\psi_{1,p}$ et $\psi_{1,p}$ en fonction d'un système d'invariants absolus (f_1, f_2, f_3). Soient $U = (x_1, x_2, x_3)$ avec $x_1 = f_1(\Omega_{\mathcal{A}})$, $x_2 = f_2(\Omega_{\mathcal{A}})$, $x_3 = f_3(\Omega_{\mathcal{A}})$ les invariants absolus de la variété $\mathcal{A}$ et $V = (u, v, w)$ les invariants absolus d'une variété p-isogène à $\mathcal{A}$. Alors on définit les polynômes suivants :

$$\Phi_{1,p} = Num(\phi_{1,p})(u, x_1, x_2, x_3)$$
$$\Psi_{2,p} = (\psi_{2,p} - v) \cdot Den(\psi_{2,p})(x_1, x_2, x_3, u, v)$$
$$\Psi_{3,p} = (\psi_{3,p} - w) \cdot Den(\psi_{3,p})(x_1, x_2, x_3, u, w)$$

avec $Num(\dots)$ et $Den(\dots)$ les numérateurs et les dénominateurs des polynômes correspondant. Sachant que $\phi_{1,p}$, $\psi_{2,p}$ et $\psi_{3,p}$ sont les polynômes donnés par la section 5.2 et l'algorithme 6.

Ainsi la matrice colonne dont les composantes sont les $\Phi_{1,p}$, $\Psi_{2,p}$ et $\Psi_{3,p}$ sera notée Φ_p. Alors on a:

$$\frac{\partial \Phi_p}{\partial V} = \begin{pmatrix} \Phi'_{1,p} & 0 & 0 \\ 0 & -\Phi'_{1,p}.Den(\psi_{2,p}) & 0 \\ 0 & 0 & -\Phi'_{1,p}.Den(\psi_{3,p}) \end{pmatrix}$$

$$\frac{\partial \Phi_p}{\partial U} = \begin{pmatrix} \frac{\partial \Phi_{1,p}}{\partial x_1} & \frac{\partial \Phi_{1,p}}{\partial x_2} & \frac{\partial \Phi_{1,p}}{\partial x_3} \\ \frac{\partial \Phi_{2,p}}{\partial x_1} & \frac{\partial \Phi_{2,p}}{\partial x_2} & \frac{\partial \Phi_{2,p}}{\partial x_3} \\ \frac{\partial \Phi_{3,p}}{\partial x_1} & \frac{\partial \Phi_{3,p}}{\partial x_2} & \frac{\partial \Phi_{3,p}}{\partial x_3} \end{pmatrix}$$

Proposition 7.1.1. *(Condition de Kronecker) Soit $J = (a, b, c)$ un triplet d'invariant absolus d'une surface abélienne $\mathcal{A}$ sur $\mathbb{F}_q$. Si $a \notin \mathbb{F}_p$ et $J \notin \mathcal{L}_p$ alors :*

i) $\dfrac{\partial \Phi_p}{\partial V}(J, J^\sigma)$ *est inversible sur* $\mathbb{Z}_q$*;*

ii) $\dfrac{\partial \Phi_p}{\partial U}(J, J^\sigma) \equiv 0 \mod p$.

Démonstration. D'après la proposition 6.2.1 dans le chapitre 6 et la section 6.2 le Frobenius réalise les conditions de Kronecker sur le lieu des points ordinaires du champ algébrique $\mathfrak{A}_{g,\Gamma_0(p)}$. Cette proposition est une adaptation à partir des équations modulaires sur le schéma $\mathfrak{A}_2(p)$.

i) Nous avons :

$$\det\left(\frac{\partial \Phi_p}{\partial V}\right) = \Phi'_{1,p} \cdot \mathrm{Den}(\psi_{2,p}) \cdot \mathrm{Den}(\psi_{3,p}) \quad avec \quad \Phi'_{1,p} = \frac{\partial \Phi_{1,p}}{\partial u}$$

où $\Phi'_{1,p}$, $\mathrm{Den}(\psi_{2,p})$ et $\mathrm{Den}(\psi_{3,p})$ dépendent seulement des variables x_1, x_2, x_3 et u. Et on sait des définitions le chapitre 5 et la section 5.2.1 que les dénominateurs $\mathrm{Den}(\psi_{2,p})$ et $\mathrm{Den}(\psi_{3,p})$ ont deux facteurs: l'un est une puissance de $\Phi'_{1,p}$ et l'autre est un multiple de L_p. Pour $J \notin \mathcal{L}_p$, si $J \in \mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p$ alors $\hat{\sigma}(J) = \sigma(J) = J$. Comme modulo p le Verschiebung $\hat{\sigma}$ a une multiplicité de p^3 alors :

$$\Phi'_{1,p}((a, b, c), a^p) \equiv 0 \mod p \text{ c'est-à-dire } \frac{\partial \Phi_p}{\partial V}(J, J^\sigma) \notin \mathbb{Z}_q^\times.$$

Lorsque l'on considère l'un des invariants, supposons $a \notin \mathbb{F}_p$ avec $J \notin \mathcal{L}_p$. D'après la section 7.1.1, l'isogénie Frobenius σ admet un relevé unique sur $\mathbb{Z}_q$ et de multiplicité 1 modulo p dans le polynôme $\phi_{1,p}(x_1, x_2, x_3, X)$. D'un autre côté le seul p^2-endomorphisme sur $\mathcal{A}$ est $[p]$, les autres isogénies différentes du Verschiebung ont des co-domaines différents, alors en les composant avec leur dual correspondant on obtiendra un non trivial p^2-endomorphisme, alors:

$$\Phi'_{1,p}((a, b, c), a^p) \not\equiv 0 \mod p$$

Comme $J \notin \mathcal{L}_p$, nous avons aussi: $\mathrm{Den}(\psi_{2,p})(a, b, c)$ et $\mathrm{Den}(\psi_{3,p})(a, b, c)$ non nuls modulo p. Par conséquent

$$\frac{\partial \Phi_p}{\partial V}(J, J^\sigma) \in \mathbb{Z}_q^\times.$$

ii) L'assertion $\dfrac{\partial \Phi_p}{\partial U}(J, J^\sigma) \equiv 0 \mod p$ signifie que chaque dérivée partielle respectivement en x_1, x_2 et x_3 des polynômes $\Phi_{1,p}(x_1, x_2, x_3, u)$, $\Phi_{2,p}(x_1, x_2, x_3, u, v)$ et $\Phi_{3,p}(x_1, x_2, x_3, u, w)$ se réduit à 0 modulo p lorsque évaluée en $(a, b, c) \notin \mathcal{L}_p$.
On considère en premier le polynôme $\Phi_{1,p} = \phi_{1,p} \cdot Den(\phi_{1,p})$, où la réduction modulo p du polynôme modulaire $\phi_{1,p}$ est

$$\phi_{1,p}(x_1, x_2, x_3, u) = \prod_{\gamma \in \mathcal{C}_p} (u - f_{1,p}^{\gamma})$$

où les $f_{1,p}^{\gamma}$ sont en fonction des variables x_1, x_2 et x_3.
D'après la section 7.1.1, p^3 fonctions $f_{1,p}^{\gamma}$ représentent les relevés du Verschiebung . Ces p^3 fonctions se réduisent en une seule fonction modulo p en les variables x_1, x_2 et x_3. Alors on obtient:

$$\frac{\partial \Phi_{1,p}}{\partial x_k}(a, b, c, a^p) \equiv 0 \mod p \quad pour \quad k = 1, 2, 3.$$

Alors chaque dérivée partielle en x_1, x_2 et x_3 des polynômes $\Phi_{1,p}$ devient 0 modulo p en (J, J^p).

Pour $\Phi_{2,p}(x_1, x_2, x_3, u, v)$ et $\Phi_{3,p}(x_1, x_2, x_3, u, w)$ la procédure reste la même.

$$\begin{aligned}
\Phi_{2,p} &= \big(\psi_{2,p} - v\big) \cdot Den(\psi_{2,p}) \\
\frac{\partial \Phi_{2,p}}{\partial x_k} &= Den(\psi_{2,p}) \cdot \frac{\partial \psi_{2,p}}{\partial x_k} + \big(\psi_{2,p} - v\big) \cdot \frac{\partial Den(\psi_{2,p})}{\partial x_k} \quad pour \quad k = 1,\ 2,\ 3 \\
\psi_{2,p}(x_1, x_2, x_3, u) &= \sum_{\gamma \in \mathcal{C}_p} f_{2,p}^{\gamma} \cdot \prod_{\gamma' \in \mathcal{C}_p \setminus \{\gamma\}} (u - f_{1,p}^{\gamma'})
\end{aligned}$$

où comme dans le cas précédent, les $f_{1,p}^{\gamma}$ sont en fonction des variables x_1, x_2 et x_3 telles que p^3 parmi elles se réduisent en une seule fonction modulo p .
Soit $(a, b, c) \notin \mathcal{L}_p$, comme :

$$\begin{cases}
\psi_{2,p}(a, b, c, a^p) \equiv b^p \mod p & et \\
\dfrac{\partial \psi_{2,p}}{\partial x_k}(a, b, c, a^p) \equiv 0 \mod p \quad pour \quad k = 1,\ 2,\ 3
\end{cases}$$

Alors pour $l = 2$ ou 3 nous avons : $\dfrac{\partial \Phi_{l,p}}{\partial x_k}(a, b, c, a^p, b^p) \equiv 0 \mod p$ pour $k = 1,\ 2,\ 3$
Ainsi nous pouvons conclure que $\dfrac{\partial \Phi}{\partial U}(J, J^\sigma) \equiv 0 \mod p$. □

Définition 7.1.2. On dira d'un systme d'invariants qu'il vérifie les conditions de Kronecker si la matrice Φ_p définie par les polynômes modulaires correspondant vérifie les propriétés i) et ii) de la section 7.1.1 et la proposition 7.1.1.

7.2 RELÈVEMENT CANONIQUE EN CARACTÉRISTIQUE IMPAIRE AVEC L'ESPACE DE SIEGEL

Cette section est une application algorithmique du Théorème de Serre-Tate (le chapitre 6 et la section 6.1). Nous utilisons les polyômes modulaires pour calculer les invariants absolus du rélévé canonique d'une surface abélienne principalement polarisée.

7.2.1 *L'Algorithme de Harley en Dimension 2*

Cette section utilise principalement la section 7.1.1 et la proposition 7.1.1, alors nous utiliserons les mêmes notations. Le Frobenius induit une isogénie, vérifiant les conditions de Kronecker avec les polynômes modulaires, comme en dimension 1 nous allons construire un algorithme de Newton avec cette propriété.

On suppose que l'on peut calculer éfficacement le Frobenius σ de $\mathbb{Q}_q$ et que l'on connaît $X \in \mathbb{Z}_q^3$ une approximation de $\tilde{J}$ à précision p^k c'est-à-dire $\tilde{J} - X = p^k e$ pour une erreur e un vecteur de $\mathbb{Z}_q^3$ que nous voudrions déterminer. En utilisant l'equation modulaire et l'expansion de Taylor sur Φ_p, on obtient:

$$0 = \Phi_p(X + p^k e, X^\sigma + p^k e^\sigma)$$

$$0 = \Phi_p(X, X^\sigma) + p^k e \frac{\partial \Phi_p}{\partial U}(X, X^\sigma) + p^k e^\sigma \frac{\partial \Phi_p}{\partial V}(X, X^\sigma) + p^{2k}(\cdots)$$

où le facteur $(\cdots)$ est un élément de $\mathbb{Z}_q$. Alors $\Phi_p(X, X^\sigma)$ a une valuation au moins k (soit sous la forme $p^k.u$) et en divisant toute l'expression par p^k on obtient l'equation suivante en e:

$$u + e \frac{\partial \Phi_p}{\partial U}(X, X^\sigma) + e^\sigma \frac{\partial \Phi_p}{\partial V}(X, X^\sigma) \equiv 0 \mod p^k.$$

Sachant que:

$$\frac{\partial \Phi_p}{\partial V}(X, X^\sigma) \in \mathbb{Z}_q^\times \quad et \quad \frac{\partial \Phi_p}{\partial U}(X, X^\sigma) \equiv 0 \mod p.$$

d'après la section 7.1.1 et la proposition 7.1.1, l'erreur e est déterminée alors par une forme matricielle de l'algorithme 1 dans le chapitre 2 et la section 2.5

Théorème 7.2.1. *Soit $J = (a, b, c)$ le triplet d'invariants absolus d'une surface abélienne principalement polarisée $\mathcal{A}$ sur $\mathbb{F}_q$. Lorsque J vérifie les conditions de Kronecker (la section 7.1.1 et la proposition 7.1.1) alors l'algorithme 7 détermine le relévé $\tilde{J}$ sur $\mathbb{Z}_q$ des invariants absolus de J en $O(n^2 \log p)$ opérations où $q = p^n$.*

Démonstration. En utilisant les conditions de Kronecker de la section 7.1.1 et la proposition 7.1.1 on construit un algorithme de Harley matriciel de complexité $O(n^2 \log p)$.
On considère que $\phi_{1,p}$ est le polynôme minimal (le chapitre 5, la section 5.2 et la section 5.2.1) pour l'élement du triplet qui est toujours hors de $\mathbb{F}_p$. □

7.2.2 *Relèvement du Verschiebung*

On se propose de calculer le relèvement du Verschiebung sur $\mathbb{Z}_q$ en utilisant l'algorithme suivant de relèvement de la p-torsion d'une variété abélienne sur $\mathbb{Z}_q$.
Comme il existe des formules complètes pour de conversion entre coordonnées Mumford et Thêta, pour plus de convenance on peut travailler sur la surface de Kummer.
Ainsi un algorithme de calcul d'isogénies à la Vélu comme celui proposé par D. Robert et R. Cosset pourra ensuite évaluer le Verschiebung relevé sur $\mathbb{Z}_q$.

Soit $\mathcal{A}$ une variété abélienne de dimension g sur $\mathbb{Z}_q$ et $\mathcal{K}$ sa variété Kummer associée. On notera par $\mathfrak{M}_p$ la matrice Jacobienne du système polynômial définissant par la p-torsion point sur $\mathcal{A}$ ou $\mathcal{K}$.

Entrée: J, et la précision N.
Sortie: $\tilde{J}$ le relevé de J à précision N.

1. **Si** $N = 1$ **Retourner** J à précision p ;
2. **Sinon** $N' = N/2$;
3. J =Harley@Siegel(J, N') ;
   a. $G = \frac{\partial \Phi}{\partial U}(J, J^\sigma)$; $H = \frac{\partial \Phi}{\partial V}(J, J^\sigma)$; $Q = \Phi(J, J^\sigma)$;
   b. $a = G.H^{-1}$, $b = Q.H^{-1}$;
   c. e =ArtinSchreier(a, b, N') ;
   d. **Retourner** $J = J + p^k e$ à la précision p^{2k} ;

Algorithm 7 – Pour calculer le relevé des invariants sur l'espace de Siegel de dimension 2.

Par exemple un point $P = (x_1, \cdots, x_m)$ sur $\mathcal{A}$ est un point de p-torsion si seulement si $[k+1].P = -[k]P$ (avec $p = 2k+1$) .
En dimension 1, lorsque $p \neq 2$: d'après la section 2.5.1 et la remarque 2.6.3, la Jacobienne $\mathfrak{M}_p$ est de la forme:

$$\begin{pmatrix} * & * \\ 0 & p \end{pmatrix}$$

ce qui implique que dans l'algorithme de Newton, par exemple lorsque x_p est à une précision k alors y_p est à la précision $k-1$.
La proposition suivante généralise cette propriété équivalente au lemme de Satoh sur les courbes elliptiques (le chapitre 2, la section 2.5 et la proposition 2.5.3) à un système polynomial définissant la p-torsion sur une variété abélienne de dimension g.

Proposition 7.2.2. *Soit $\mathcal{A}$ une variété abélienne de dimension g sur $\mathbb{Z}_q$, en tout point P de $\mathcal{A}$ il existe une base de l'espace tangent à $\mathcal{A}$ pour laquelle, la matrice $\mathfrak{M}_p$ est égale à p fois la matrice identité .*

Démonstration. D'après [86] , il existe un isomorphisme naturel

$$\Omega_0 \otimes_{\mathbb{k}} O_{\mathcal{A}} \simeq \Omega^1_{\mathcal{A}}$$

où Ω_0 est le dual de l'espace tangent en 0 à $\mathcal{A}$ et $\Omega^1_{\mathcal{A}}$ est le faisceau des 1-formes regulières sur $\mathcal{A}$.
Comme la différentielle de l'application "Addition" n'est autre que l'addition des composantes. Ainsi on considère l'application "Multiplication" $[p] : \mathcal{A} \longrightarrow \mathcal{A}$, sa Jacobienne est alors sous la forme

$$\mathfrak{M}_p = diag(p, \cdots, p) = p \cdot \mathrm{Id}_g .$$

□

Corollaire 7.2.3. *Soit $\mathcal{A}$ une variété abélienne définie par un système polynômial $(f_1, \cdots f_n)$ sur l'espace affine $\mathbb{A}^n$. En tout point $P \in \mathcal{A}[p]$ il existe une base telle que :*

$$\begin{pmatrix} Jac(f_1, \cdots f_n) \\ \mathfrak{M}_p \end{pmatrix} = \begin{pmatrix} * & * \\ 0 & p.\mathrm{Id}_g \end{pmatrix}$$

Ainsi son déterminant a une p-valuation g et son inverse est de p-valuation -1 .

Démonstration. Comme pour tout point P de $\mathcal{A}[p]$ le rang de $Jac(f_1, \cdots, f_n)$ est $(n-g)$. Alors en appliquant la proposition 7.2.2 on obtient le résultat. □

Théorème 7.2.4. *(Relèvement de la p-Torsion) Soit $\mathcal{A}$ une variété abélienne ordinaire sur $\mathbb{F}_q$, alors on peut déterminer le relèvement canonique de tout point de p-torsion de $\mathcal{A}/\mathbb{F}_q$ sur $\mathbb{Z}_q$ en $O(n^2 \log p)$ opérations au plus.*

Démonstration. Soit F la fonction vectorielle définissant le système polynômial p-torsion sur $\mathcal{A}$, d'après le corollaire précedent 7.2.3 la Forme Normale de Smith de $(DF(P))$ est de la forme:

$$\begin{pmatrix} * & * \\ 0 & p.I_g \end{pmatrix}$$

selon un changement de base $M \cdot S \cdot N = DF(P)$.
En considérant le chapitre 1, la section 1.2 et la proposition 1.2.4 la méthode de Newton sur F en X marche comme dans le cas univarié pour chaque composante de X.
Ainsi pour tout $P = \tilde{P} \mod p$: $ord_p F_i(P_i) = 1$ et $ord_p F_i'(P_i) = 0$ pour les $(n-g)$ premiers polynômes. Et pour les g autres polynômes on a: $ord_p F_i(P_i) = 1$ et $ord_p F_i'(P_i) = 1$.
D'après le chapitre 1, la section 1.2 et le lemme 1.2.1 pour gagner plus de précisions dans les g dernières équations, l'on doit résoudre des équations :

$$F_i(P_i) + p.DF(P_i).R_i + p^2/2.{}^tR_i.HF(P_i).R_i = 0 \mod p^3$$

Comme le relevé de X est unique d'après [99], alors chaque équation quadratique prècédente détermine un unique R_i sur $\mathbb{Z}_q$.
Les étapes suivantes des Newtons univariés correspondront aux cas (le chapitre 1, la section 1.2 et la proposition 1.2.4) c'est-à-dire le cas $ord_p(F_i(P_i)) > 2.ord_p F_i'(P_i)$. Et par suite on détermine l'unique relevé de la p-torsion en $O(n^2 \log p)$. □

Exemple 7.2.5. (Dimension 1)
On considère la courbe elliptique définie sur $\mathbb{F}_3[t]/(t^5+2t+1)$ par :

$$E : y^2 = x^3 + (t^2-t)x^2 + t^3 - t^2 + 1$$

Le polynôme de Teichmuller de t^5+2t+1 à la précision 3^{16} est :

$$M = t^5 + 40187187t^4 + 22623057t^3 + 28433298t^2 + 42740657t + 1$$

Par l'algorithme de Harley, le relevé du j-invariant à la précision 3^{16} est:

$$\tilde{j} = 4184705t^4 + 21892713t^3 + 36017948t^2 + 23621781t + 31000250$$

La courbe relévée est $\tilde{E} : y^2 = x^3 + Ax^2 + B$, où : $A = t^2+1$, $B = 35012730t^4 + 19700410t^3 + 13577987t^2 + 12290190t + 25369066$.
Un point $P = (x, y)$ est dans $\tilde{E}[p]$ si et seulement si $[2].P = -P$ et comme les points $[2].P$ et P sont sur la même droite alors:

$$\tilde{P} \in \tilde{E}[p] \Leftrightarrow F(x, y) = 0.$$

$$avec \quad F(x,y) = \begin{pmatrix} -x^3 - Ax^2 + (y^2 - B) \\ 9/4x^4 + 3Ax^3 + A^2x^2 - 3y^2x - Ay^2 \end{pmatrix}.$$

On a $P = (2t^4 + 2t^3 + 2t^2 + 1,\ 1) \in E[3]$ et en utilisant l'algorithme 7.2.4, on obtient:

$$\begin{aligned}\tilde{P} = (&555542t^4 + 15403853t^3 + 5231684t^2 + 29534907t + 30143767,\\ &11152449t^4 + 34597530t^3 + 41418387t^2 + 1833597t + 31531297).\end{aligned}$$

Exemple 7.2.6. (Dimension 2)
On considère la courbe de genre 2 définie sur $\mathbb{F}_3[T]/T^{10} + 2T^6 + 2T^5 + 2T^4 + T + 2$:

$$\begin{aligned}\mathcal{C} : y^2 = {} & x^5 + (2T^8 + T^2 + T)x^4 + (T^8 + T^7 + T^6 + T^5 + T^3 + 2T + 2)x^3\\ & + (T^9 + 2T^8 + T^6 + T^5 + T^4 + 2T^3 + 2)x^2\\ & + (2T^9 + T^8 + 2T^7 + T^6 + T^5 + 2T^4 + 2T^2 + 1)x\end{aligned}$$

On note ses invariants thêta absolus de niveau 2 par $J = (a, b, c)$ avec:

$$\begin{aligned}a =& 2T^9 + 2T^6 + 2T^5 + 2T^4 + T^3 + T^2 + T,\\ b =& 2T^9 + T^8 + 2T^7 + T^6 + T^5 + 2T^4 + 2T^2,\\ c =& 2T^9 + 2T^6 + T^4 + 2T^3 + 2T + 2\end{aligned}$$

Alors une équation projective de la surface de Kummer $\mathcal{K}$ est donnée par :

$$(x^4 + y^4 + z^4 + t^4) + 2Exyzt - F(x^2t^2 + y^2z^2) - G(x^2z^2 + y^2t^2) - H(x^2y^2 + z^2t^2) = 0$$

où F, H et G sont en fonction de a, b et c (aller à l'appendice a et l'appendice a.1).
Et la 3-torsion sur $\mathbb{F}_3[T]/T^{10} + 2T^6 + 2T^5 + 2T^4 + T + 2$ est définie par le système polynômial donné par $2P = P$. On obtient en plus du thêta-nul point les points affines :

$$\begin{aligned}tors0 = {} & [T^7 + T^6 + T^4 + 2T^2 + 2T, 2T^9 + T^8 + T^7 + 2T^4 + 2T^3 + T^2 + 2,\\ & 2T^8 + T^7 + T^6 + T^4 + 2];\\ tors1 = {} & [2T^9 + 2T^8 + 2T^7 + T^6 + 2T^5 + T^2 + T + 1, 2T^9 + T^8 + T^7 + T^6\\ & + T^5 + T^4 + 2T^3 + T^2 + 2T, T^9 + 2T^8 + 2T^5 + 2T^4 + 2T^3 + 2T + 1];\\ tors2 = {} & [T^9 + 2T^8 + T^7 + 2T^6 + T^4 + 2T^3 + 2T^2 + 1, 2T^9 + 2T^7 + 2T^5 + T^4\\ & + 2T^3 + T^2 + T + 2, T^9 + 2T^8 + 2T^7 + T^6 + 2T^4 + 2T^3 + T^2 + 2T + 2];\\ tors3 = {} & [2T^9 + 2T^6 + T^4 + 2T^3 + 2T, T^9 + 2T^7 + T^5 + 2T^3,\\ & 2T^9 + T^8 + 2T^6 + T^4 + 2T^3 + 2T^2 + T + 1]\end{aligned}$$

Comme J satisfait les conditions de Kronecker, on utilise l'algorithme 7 avec les polynômes modulaires en thêta.
Après la phase de relèvement canonique, on obtient à la précision 3^{20}:

$$\begin{aligned}M = {} & T^{10} + 2549079126T^9 + 1424896413T^8 + 387776124T^7 + 1501830083T^6\\ & + 2399043737T^5 + 1835343671T^4 + 3327249759T^3 + 1052748765T^2\\ & + 1815623119T + 3486784400\end{aligned}$$

exemple 7.1 – Relèvement canonique de la p-torsion d'une variété abélienne ordinaire.

$$\begin{aligned}\tilde{a} =&1632442511T^9 + 3184765518T^8 + 3476194941T^7 + 3108882704T^6\\ &+ 2423383142T^5 + 1764926933T^4 + 1098986671T^3 + 2957646787T^2\\ &+ 1669307941T + 2686192050,\\ \tilde{b} =&1855464665T^9 + 458606629T^8 + 1644296153T^7 + 2202845860T^6\\ &+ 2959176835T^5 + 2200438487T^4 + 1716586968T^3 + 1038290165T^2\\ &+ 133634418T + 2980506843,\\ \tilde{c} =&3067405283T^9 + 2017143027T^8 + 1539671400T^7 + 2805617504T^6\\ &+ 754015086T^5 + 1269571459T^4 + 2964123128T^3 + 609859068T^2\\ &+ 3096552740T + 605100932,\end{aligned}$$

En utilisant l'algorithme 7.2.4 sur le système polynômial définie par $2P = P$, on obtient le relevé de chaque point de 3-torsion comme par exemple celui de $tors0$ donne :

$$\begin{aligned}\tilde{tors}0 = [&783079641T^9 + 2124478056T^8 + 836911573T^7 + 2573975062T^6\\ &+ 902190282T^5 + 366817813T^4 + 3020511501T^3 + 3106437113T^2\\ &+ 1881969155T + 838267932, 1475631209T^9 + 1062021913T^8\\ &+ 1843928959T^7 + 795907434T^6 + 2521901733T^5 + 1698902771T^4\\ &+ 2534696996T^3 + 3155556349T^2 + 3023958660T + 1433503754,\\ &2400942648T^9 + 833485184T^8 + 2017122688T^7 + 265798210T^6\\ &+ 371555682T^5 + 828437455T^4 + 3052717911T^3 + 3041519346T^2\\ &+ 2288895138T + 3190509602].\end{aligned}$$

7.3 RELÈVENEMENT CANONIQUE EN CARACTÉRISTIQUE 2 OU 3

Dans cette section nous introduisons une méthode de calcul de relevé canonique d'une courbe $\mathcal{C}$ de genre 2 en carctéristique 2. La partie de cette méthode concernant le calcul des invariants du relevé canonique $\tilde{\mathcal{C}}$ pourra facilement s'adapter aux caractéristiques 3 à partir de polynômes modulaires en les invariants fournis par les trois composantes de $\mathcal{M}_2 \otimes \mathbb{Z}_3$. Les autres parties sont spécifiques au relèvement canonique des courbes de genre 2 en caractéristique paire.
Nous allons utiliser les polyômes modulaires pour calculer le relevé les invariants absolus correspondant comme dans la section 7.2, et après nous expliquons comment calculer le relevé d'une équation de la courbe $\mathcal{C}$. Ensuite nous introduisons des méthodes de calcul du relevé 2-adique de l'isogénie du Frobenius. Mais il faudrait bien distinguer les cas où le relevé est canonique (type $(1,1,1)$) des cas où le relevé n'est pas unique (les autres types).

7.3.1 *Relèvement des Invariants*

Nous avions vu dans le chapitre 4 et la section 4.3 que la réduction modulo 2 des courbes de genre 2 sur $\mathbb{Z}_q$ suit la classification birationnelle donnée par les types $(1,1,1)$, $(3,1)$ et (5). On peut directement remarquer que des courbes de types différents ne sont pas isogènes par le Frobenius, alors le relevé de l'isogénies Frobenius réliera des courbes 2-isogènes de même type sur $\mathbb{Z}_q$. Les courbes de genre 2 ordinaires sont celles qui sont birationnellement équivalentes au type $(1,1,1)$ c'est-à-dire encore celles qui sont de p-rang 2. En effet les autres types sont de p-rang 0 et 1 (correspondant au nombre de points de Weierstrass triviaux)

donc non ordinaires.
Par suite les polynômes modulaires en les invariants $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ (le chapitre 5 et la section 5.2.4) décrivent sur $\mathcal{M}_2 \otimes \mathbb{Z}_2$ les relevés canoniques des courbes ordinaires 2-isogènes sur $\mathbb{F}_q$ (avec $q = 2^n$).

Alors on considère que $\mathcal{A} = \mathrm{Jac}(\mathcal{C})$ est ordinaire ou de manière équivalente que C est de type $(1,1,1)$. Comme pour le cas de la caractéristique impaire on se propose de calculer le relevé $\tilde{J} = (\tilde{\mathfrak{a}_1}, \tilde{\mathfrak{a}_2}, \tilde{\mathfrak{a}_3})$ de $J = (\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ en utilisant la même approche que précedement pour la caractéristique impaire c'est-à-dire en utilisant la relation modulaire entre J et J^σ.

Soit $U = (x, y, z)$ le triplet de variables (dans les polynômes modulaires) représentant les invariants absolus dans $\mathcal{M}_2[J_2^{-1}]$ et respectivement $V = (u, v, w)$ représentant les invariants absolus $(2,2)$-isogènes à U.

Corollaire 7.3.1. *Lorsque $p = 2$ et $\mathcal{A}$ est une surface abélienne sur $\mathbb{F}_q$ telle que $J_2(\mathcal{A})J_{10}(\mathcal{A}) \neq 0$. Alors $\mathcal{A}$ est ordinaire, et est la Jacobienne d'une courbe $\mathcal{C}$ de type $(1,1,1)$. Si $J = (\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ est le triplet d'invariants absolus de $\mathcal{A}$ dans $\mathcal{M}_2[J_2^{-1}]$ sur $\mathbb{F}_{2^n}$ avec $n > 2$, alors :*
i) $\dfrac{\partial \Phi_p}{\partial V}(J, J^\sigma)$ *est inversible ;*
ii) $\dfrac{\partial \Phi_p}{\partial U}(J, J^\sigma) \equiv 0 \mod p$.

Démonstration. Les relations sont bien vérifiées par les points ordinaires ($J_2 J_{10} \neq 0$.) du lieu géométrique défini par l'équation modulaire (sur $\mathcal{M}_2[J_2^{-1}]$) d'après le chapitre 6 et la section 6.2. Ces rélations proviennent aussi d'un changement de variables birationnel qui induit une transformation inversible différentiable (sur le domaine ouvert de définition). Ces relations sont donc vérifiées pour tout triplet $J = (f_1, f_2, f_3)$ bien défini sur le lieu $J_2 J_{10} \neq 0$. □

Remarque 7.3.2. J est bien défini en $\mathcal{A}$ exactement lorsque $J_2(\mathcal{A})J_{10}(\mathcal{A}) \neq 0$, donc dans ce cas J est automatiquement bien défini en $\mathcal{A}^\sigma$, comme $J(\mathcal{A}^\sigma) = J(\mathcal{A})^\sigma$. Il reste à retirer les points singuliers de l'équation modulaire qui semblent contenir le lieu du dénominateur $\mathcal{D}_p$. Mais nous pouvons toutefois éliminer le dénominateur et se ramener à une équation modulaire sur $\mathcal{A}$ et $\mathcal{A}^\sigma$ puisque J est bien défini en les deux points. Plus précisement, on pourra interpréter le dénominateur comme une forme modulaire pour éliminer les facteurs parasites selon ([79] et [59]).

Comme les polynômes modulaires satisfont les conditions de Kronecker nous pouvons utiliser la méthode de Harley introduit précédement dans la section 7.2, pour obtenir le résultat suivant:

Corollaire 7.3.3. *Lorsque $J = (\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ désigne les invariants absolus d'une surface abélienne vérifiant les conditions de Kronecker le corollaire 7.3.1. Alors l'algorithme 7 dans la section 7.2 calcule (en doublant de précisions) les invariants absolus du relèvement canonique $\tilde{\mathcal{A}}$ sur $\mathbb{Z}_q$.*

Démonstration. En combinant le corollaire 7.3.1 et une adaptation de la méthode de Harley dans la section 7.2. □

7.3.2 *Relèvement 2-Adique d'une Courbe de genre 2*

Nous avons vu précédemment que les conditions de Kronecker fournissent des algorithmes de calcul des invariants du relevé d'une courbe de genre 2 ordinaire. Dans cette partie, on

se propose de déterminer une équation $\tilde{f}(x,y)$ d'une courbe $\tilde{\mathcal{C}}$ de genre 2 dont on connaît les invariants sur $\mathbb{Z}_q$ et une equation $\mathcal{C} : f(x,y) = 0$ modulo 2 de sa réduite de genre 2. On pourra utiliser la même approche (avec des invariants adaptés) pour les caractéristiques non couvertes par l'algorithme de construction de Mestre (mauvaise réduction par exemple de la conique en caractéristique 2).

En considerant les conversions entre la forme normale et le modèle hyperelliptique d'une courbe de genre 2 dans le chapitre 4 et la section 4.5, nous allons nous restreindre au cas d'une forme normale.
Soit $q = 2^n$ et $\mathcal{C}$ une courbe de genre 2 sur $\mathbb{F}_q$ par une équation de sa forme normale:

$$\mathcal{C} : XY^2 + (1 + aX + bX^2)Y + X^2(c + dX + X^2) = 0.$$

Soit $(\tilde{f}_1, \tilde{f}_2, \tilde{f}_3)$ les invariants de $\tilde{\mathcal{C}}$ sur $\mathbb{Z}_q$ (définis par le chapitre 4, la section 4.3 et le théorème 4.3.2), où dans le cas ordinaire ce sont les invariants $(\tilde{\mathfrak{a}_1}, \tilde{\mathfrak{a}_2}, \tilde{\mathfrak{a}_3})$ donnés par l'algorithme 7 avec $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ vérifiant les conditions de Kronecker.
Les invariants J_{2i} admettent des expréssions en fonction des coefficients a, b, c et d, alors on peut aussi exprimer les invariants birationnels (f_1, f_2, f_3) comme fonctions rationnelles en les (a, b, c, d). Ces rélations fournissent un système d'équations (pour $(\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d})$), sur lequel on peut appliquer un relèvement de Newton à partir d'une solution (a, b, c, d) modulo 2 (puisque l'expréssion globale a une bonne réduction).
En particulier, comme le modèle $\tilde{\mathcal{C}}$ a une bonne réduction modulo 2, la réduction w d'une base des formes différentielles $\tilde{w}$ est bien définie. En comparant w avec une base fixée $w_{\mathcal{C}}$ de $\mathcal{C}$, nous obtenons que $w = Mw_{\mathcal{C}}$ pour une certaine matrice M dans $\mathrm{GL}_2(\mathbb{F}_q)$. Relever M en $\tilde{M} \in \mathrm{GL}_2(\mathbb{Z}_q)$, et en posant $\tilde{w}_{\tilde{\mathcal{C}}} = \tilde{M}^{-1}\tilde{w}$, nous pouvons relever $w_{\mathcal{C}}$. En application, soit g une forme modulaire vectorielle (avec une bonne réduction modulo 2), alors $g(\mathcal{C}, \tilde{w}_{\tilde{\mathcal{C}}})$ est un rélévé de $g(\mathcal{C}, w_{\mathcal{C}})$. Nous abordons cette application du relèvement plus en détails dans le chapitre 8.

Relèvement sur $\mathbb{Z}_q$ d'une courbe de type $(1,1,1)$

Pour ce qui suit nous détaillons les différentes étapes du relèvement sur $\mathbb{Z}_q$ d'une courbe de type $(1,1,1)$ ce qui couvre couvre les cas ordinaires (à travers les transformations birationnelles du chapitre 4 et la section 4.3). Ainsi modulo 2, les invariants absolus $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ peuvent être déterminer à partir des coefficients a, b, c, and d directement par les rélations la section 4.3 et la section 4.3.2.
Par suite, les coefficients $\tilde{a}$, $\tilde{b}$, $\tilde{c}$, et $\tilde{d}$ de la forme normale du relevé canonique $\tilde{\mathcal{C}}$ se réduisant sur $\mathcal{C}$ satisfait le system d'equations suivant fourni par les J_{2i} et les relevés $(\tilde{\mathfrak{a}_1}, \tilde{\mathfrak{a}_2}, \tilde{\mathfrak{a}_3})$ (que l'on sait calculer à partir de $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$):

$$\begin{cases} \tilde{J}_4 - \tilde{J}_2^2\tilde{\mathfrak{a}_1} &= 0, \\ \tilde{J}_8 - \tilde{J}_2^4\tilde{\mathfrak{a}_2} &= 0, \\ \tilde{J}_{10} - \tilde{J}_2^5\tilde{\mathfrak{a}_3} &= 0 \end{cases} \tag{7.1}$$

où les J_{2i} sont en fonction des variables a, b, c et d obtenues en utilisant par exemple le modèle hyperelliptique donné par:

$$y^2 + h(x)y = f(x) \quad \text{où} \quad h(x) = 1 + ax + bx^2 \text{ et } f(x) = -x^3(c + dx + x^2).$$

Alors on a le résultat suivant:

Lemme 7.3.4. *Sur $\mathbb{Z}_q$ l'intersection des trois surfaces de l'équation (7.1) est non-singulière en les (a,b,c,d) satisfaisant les conditions de Kronecker, plus précisément non singulière à toute précision > 1. Ces équations se ramifient modulo 2.*

Démonstration. Pour toute courbe $\mathcal{C}$ de genre 2, deux caractérisations de $\mathcal{C}$ se réduisent bien modulo 2: sa forme normale en les (a,b,c,d) et l'évaluation des J_{2i} en $\mathcal{C}$. Le système d'équations 7.1 est construit en exprimant les J_{2i} en fonction of (a,b,c,d) ([51, Pages 10-12]). Sur $\mathbb{Z}_q$ et lorsque J_2 est non nul modulo 2 (c'est-à-dire $ab \not\equiv 0 \mod 2$), le système 7.1 définit un point non-singulier dans $\mathcal{M}_2[J_2^{-1}]$ (représentant les classes d'équivalence birationnelle de $\tilde{C}$).[51, Théorem 4]. De plus modulo 2, nous avons la factorisation suivante:

$$\begin{cases} J_4 = & J_2^2(\alpha^2+\beta^2+\gamma^2), \\ J_8 = & J_2^4(\alpha^2\beta^2+\alpha^2\gamma^2+\beta^2\gamma^2-\mathfrak{g}^3-\mathfrak{g}^4), \\ J_{10} = & J_2^5(\alpha^2\beta^2\gamma^2). \end{cases}$$
$$\text{avec } J_2 \equiv a^2b^2 \text{ et } \mathfrak{g} = \alpha^2+\beta^2+\gamma^2.$$

où α, β et γ sont en fonction de (a,b,c,d) à travers les relations le chapitre 4 et la section 4.3.2. On peut normaliser ces nouvelles équations du 7.1 par des puissances paires de ab. Ainsi sur un modèle affine (fixant un paramètre pour avoir trois variables) les dérivées partielles en a et b du système 7.1 s'annulent. Alors le déterminant de la matrice Jacobienne du système s'annule aussi. À remarquer que la factorisation ci-dessus est seulement valable modulo 2. D'autre part à la précision 2 lorsqu'un paramètre (par exemple a) est fixé, le déterminant de la matrice Jacobienne du système 7.1 est donné par:

$$\begin{aligned} 2a^{12}\Big[&a^{10}+(b^3+db)a^9+(cb^2+b)a^8+(d^2b^5+c^2b)a^7+ \\ &(cb^3+b^2)a^6+(\mathfrak{a}_3b^{15}+c^2b^7+b^5)a^5+\mathfrak{a}_3b^{18}a^4+ \\ &(\mathfrak{a}_3db^{19}+c^4b^5)a^3+(\mathfrak{a}_3cb^{20}+\mathfrak{a}_3b^{19})a^2+ \\ &(\mathfrak{a}_3c^2b^{19}+c^2b^9+b^7)a+(\mathfrak{a}_3cb^{21}+\mathfrak{a}_3b^{20})\Big]. \end{aligned}$$

Alors l'annulation modulo 4 de cette quantité implique celle de la quantité entre paranthèses modulo 2. Cette dernière annulation implique que modulo 2: $\mathfrak{a}_3$ est le quotient de:

$$\begin{aligned} &-a^{10}+(-b^3-db)a^9+(-cb^2-b)a^8+(-d^2b^5-c^2b)a^7+ \\ &(-cb^3-b^2)a^6+(-c^2b^7-b^5)a^5-c^4b^5a^3+(-c^2b^9-b^7)a \end{aligned}$$

par

$$b^{15}a^5+b^{18}a^4+db^{19}a^3+(cb^{20}+b^{19})a^2+c^2b^{19}a+(cb^{21}+b^{20})$$

ce qui n'est pas égal modulo 2 à la valeur de $\mathfrak{a}_3 = J_{10}/J_2^5$ (donné par [51, Pages:11-12]). Alors génériquement le facteur ne s'annule pas modulo 2.
Ainsi le déterminant du système est seulement de 2-valuation 1. □

Remarque 7.3.5. Comme le déterminant de la Jacobienne du système 7.1 est de valuation 2-adique 1 sur $\mathcal{M}_2[J_2^{-1}]$, alors la forme SNF de la Jacobienne est connue (une seule équation est à la précision 2). Ainsi par le Théorème de Serre-Tate on a l'existence du rélévé canonique et la méthode du chapitre 6, la section 1.2 et la proposition 1.2.4 calcule les coefficients $(\tilde{a},\tilde{b},\tilde{c},\tilde{d})$.

Pour ce qui suit on se propose d'étendre la méthode précédente au relèvement (quelconque) des équations de courbes de rang 0 et 1. Plusieurs classes d'isomorphismes de courbe sur $\mathbb{Z}_q$ se réduisent sur ces classes de courbes modulo 2, pour rendre les systèmes d'équations lisses sur $\mathbb{Z}_q$ on pourra choisir une classe d'isomorphisme représentant un point lisse de la composante sur $\mathbb{Z}_q$.
Alors on supposera que l'on connaît ce point sur $\mathbb{Z}_q$ de bonne réduction définis respectivement sur $\mathcal{M}_2[J_6^{-1}]$ avec $J_2 \equiv 0 \mod 2$ et $\mathcal{M}_2[J_8^{-1}]$ avec $J_2 = J_4 = 0$ modulo 2 (se réduisant sur nos triplets).

Dans le cas des courbes de type $(3,1)$

Les courbes de type $(3,1)$ sont définies par (a,b,c,d) avec ($a = 0$ et $b \neq 0$) ou ($a \neq 0$ et $b = 0$). On peut alors utiliser le système polynômial suivant pour relever les coefficients $(\tilde{a},\tilde{b},\tilde{c},\tilde{d})$ correspondant à la forme normale d'une courbe sur $\mathbb{Z}_q$ dont les invariants sont $(\tilde{u_1}, \tilde{u_2}, \tilde{u_3})$ où $\tilde{u_1} = 0$ modulo 2:

$$\begin{cases} J_4^3 - J_6^2\tilde{u_1} & = 0 \\ J_8J_{10} - J_6^3\tilde{u_2} & = 0 \\ J_{10}^3 - J_6^5\tilde{u_3} & = 0 \end{cases} \tag{7.2}$$

Comme nous sommes dans un cas où $J_6 \neq 0$ le système 7.2 définit un point lisse de $\mathcal{M}_2 \otimes \mathbb{Z}_q$ (d'après [51, Theorem 4]). Cependant modulo 2 le même système est équivalent à:

$$\begin{cases} \alpha^6 & = & \tilde{u_2} \\ \beta^6 & = & \tilde{u_3} \end{cases}$$

où α et β sont en fonction de (a,b,c,d) par les relations (le chapitre 4 et l'équation (4.8)). On en conclut que le déterminant de la Jacobienne s'annule modulo 2.
Alors sur $\mathbb{Z}_q$ l'intersection des trois surfaces du système 7.2 est non singulière en (a,b,c,d) et elle se ramifie en ce point seulement modulo 2.

Dans le Cas du Type (5)

Ce type dépend seulement de c sur $\mathbb{F}_q$ et sur $\mathbb{Z}_q$ le quadruplet de coefficients $(\tilde{a},\tilde{b},\tilde{c},\tilde{d})$ est solution du système polynômial défini par:

$$\begin{cases} J_2^4 - J_8\tilde{w_1} & = & 0 \\ J_6^4 - J_8^3\tilde{w_2} & = & 0 \\ J_{10}^4 - J_8^5\tilde{w_3} & = & 0 \end{cases} \tag{7.3}$$

où on a: $w_1 = w_2 = 0$ modulo 2. Sur $\mathbb{Z}_q$ l'intersection des trois surfaces de 7.3 n'est pas forcement non singulière en $(\tilde{a},\tilde{b},\tilde{c},\tilde{d})$. Mais nous pouvons toutefois choisir parmi les différents relevés un point lisse de $\mathcal{M}_2 \otimes \mathbb{Z}_q$ ($\tilde{w_1}$ et $\tilde{w_2}$ non tous nuls) se réduisant sur (w_1, w_2, w_3). Cependant le système se ramifie en ce point modulo 2, on peut toute fois minimiser la valuation du déterminant de la matrice Jacobienne en prenant la plus petite valuation possible pour le produit $\tilde{w_1}\tilde{w_2}$ (valuation 2-adique 1.).
Le même système est équivalent modulo 2 à:

$$\begin{cases} \alpha^4 - \tilde{w} = 0 \end{cases}$$

où α et β sont en fonction de c et d avec a et b un fixé et l'autre nul (par les relations le chapitre 4 et l'équation (4.9)). Alors dans des conditions favorables, le déterminant de la Jacobienne du système en $(\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d})$ peut être de valuation 2-adique 1.

Remarque 7.3.6. Les systèmes polynômiaux 7.2 et 7.2 sont tous lisses sur $\mathbb{Z}_q$ en les solutions $(\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d})$ pour certains triplets. La meilleure situation étant celle où le déterminant de la Jacobienne de ces systèmes en ces points est de valuation 2-adique très petite (même si elle est supérieure ou égale à 2), alors les méthodes de relèvement détaillées dans le chapitre 6, la section 1.2 et la proposition 1.2.4 calculent plus rapidement le quadruplet $(\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d})$. À remarquer que dans ces deux derniers cas le relèvement n'est pas canonique.

7.3.3 *Réduction des Points de Weierstrass*

On considère que l'on connaît les coefficients relévés $\tilde{a}$, $\tilde{b}$, $\tilde{c}$ et $\tilde{d}$ de la courbe $\tilde{\mathcal{C}}$ le relévée canonique de $\mathcal{C}$. Alors l'équation de $\mathcal{C}$ se relève (canoniquement lorsque $J_2 \not\equiv 0 \mod p$) en :

$$Y^2 + (1 + \tilde{a}X + \tilde{b}X^2)Y = -X^3(\tilde{c} + \tilde{d}X + X^2)$$

Un point P de coordonnées affine $(x_P, y_P) \in \mathbb{Z}_q \times \mathbb{Z}_q$ est un point de Weierstrass de $\tilde{\mathcal{C}}$ si et seulement si pour $H(x) = 1 + \tilde{a}x + \tilde{b}x^2$ et $F(x) = x^3(\tilde{c} + \tilde{d}x + x^2)$, nous avons :

$$2y_P + H(x_P) = 0, \quad et \quad y_P^2 + H(x_P)y + F(x_P) = 0$$

Alors les cinq points de Weierstrass de $\tilde{\mathcal{C}}$ se réduisent comme suite :

Dans le cas du type $(1, 1, 1)$

Nous avons deux points Weierstrass se réduisant sur P et deux autres se réduisant sur Q tels que x_P et x_Q sont les solutions modulo 2 de l'équation :

$$1 + ax + bx^2 = 0$$

Et le cinquième point se réduise sur le point à l'infini.

Dans le cas du type $(3, 1)$

Ce cas est caractérisé par ($a = 0$ et $b \neq 0$) ou ($a \neq 0$ et $b = 0$) et l'on peut remarquer que deux points Weierstrass se réduisent sur un unique point dont l'abscisse est la solution de l'équation $1 + ax = 0$ respectivement $1 + bx^2 = 0$ selon le cas ($a = 0$ et $b \neq 0$) respectivement ($a \neq 0$ et $b = 0$). Et les trois autres points se réduisent tous sur le point à l'infini.

Dans le cas du type (5)

Dans ce cas tous les points de Weierstrass de $\tilde{\mathcal{C}}$ se réduisent modulo 2 sur le point à l'infini.

7.3.4 *Réduction de l'Isogénie du Frobenius*

Pour l'étude de la réduction de l'isogénie Frobénius, nous considérons celle du calcul des $(2, 2)$-isogénies par l'algorithme de Richelot [94]. Alors nous allons nous referer aux notations de B.Smith [109]. pour caractériser les noyaux des isogénies Frobenius et Verschiebung. Soient G_1, G_2 et G_3 des polynômes de degré au plus 2 dans $\mathbb{k}[x]$ on note par: $[G_2, G_3] =$

$G_2'G_3 - G_2G_3'$ et $\det(G1, G2, G3)$ le déterminant de la matrice dont les coefficients (ij) sont les j-ième coefficient de G_i.
On note par $\Pi(G_1, G_2, G_3)$ une décomposition (sans facteurs carrés en polynômes de degré 2 au plus) du polynôme $f(x)$ de degré 5 ou 6 du model hyperelliptique $y^2 = f(x)$ d'une courbe de genre 2.
Alors l'opérateur de Richelot $\mathcal{R}$ est défini par :

$$\mathcal{R}(G_1, G_2, G_3) := (\delta[G_2, G_3], \delta[G_3, G_1], \delta[G_1, G_2]),$$

où

$$\det(G_1, G_2, G_3) \neq 0 \quad et \quad \delta = (\det(G_1, G_2, G_3))^{-1}.$$

Soit $(H_1, H_2, H_3) = \mathcal{R}(G_1, G_2, G_3)$ alors :

- $\Pi(H_1, H_2, H_3)$ est un polynôme sans facteurs carrés de degré 5 ou 6.
- $\mathcal{R}(k_1G_1, k_2G_2, k_3G_3) = (k_1^{-1}H_1, k_2^{-1}H_2, k_3^{-1}H_3)$ pour des k_i non nuls sur le corps de base ;
- $\mathcal{R}(G_2, G_3, G_1) = (H_2, H_3, H_1)$ et $\mathcal{R}(G_3, G_1, G_2) = (H_3, H_1, H_2)$;
- $\mathcal{R}(H_1, H_2, H_3) = (G_1, G_2, G_3)$.

Lorsque $\det(G_1, G_2, G_3) \neq 0$, nous appelerons cette décomposition: *décomposition quadratique lisse* en considerant que le polynôme de degré 1 (éventuellement) est quadratique avec une racine à l'infini. Ainsi les décompositions quadratiques lisses forment une partition en paires des points de Weierstrass de $\mathcal{C}$ c'est-à-dire une caractérisation des $(2,2)$-sous groupes de $(\mathrm{Jac}\,\mathcal{C})[2]$.

Lemme 7.3.7. *Soit $\mathcal{C} : y^2 = f_{\mathcal{C}}(x)$ une courbe de genre 2. Pour chaque décomposition quadratique lisse $G = (G_1, G_2, G_3)$ de $f_{\mathcal{C}}$, on définit la courbe $\mathcal{C}_G$ par l'équation $y^2 = f_{\mathcal{C}_G} := \Pi(\mathcal{R}(G))$. Alors les variétés Jacobiennes* $\mathrm{Jac}\,\mathcal{C}$ *et* $\mathrm{Jac}\,\mathcal{C}_G$ *sont $(2,2)$-isogènes par l'isogénie de noyau engendré par les diviseurs définis par $G_1(x)$, $G_2(x)$ et $G_3(x)$.*

Démonstration. En utilisant ensemble la Proposition 8.2.3. et le Théorem 8.4.11. dans [109]. □

Remarque 7.3.8. Lorsque $\det(G_1, G_2, G_3) = 0$ on dira que la décomposition quadratique est singulière et dans ce cas la variété Jacobienne $\mathrm{Jac}\,\mathcal{C}$ est $(2,2)$-isogène à un produit de courbes elliptiques.

Proposition 7.3.9. *(Réduction du Frobenius)*

- *Dans le cas du type $(1,1,1)$: la courbe de genre 2 conjuguée $\tilde{\mathcal{C}}^{\Sigma}$ sur $\mathbb{Z}_q$ of $\tilde{\mathcal{C}}$ est définie par l'équation: $y^2 = \Pi\mathcal{R}(G_1, G_2, G_3)$, où : $G_1(u) = (u - x_1)(u - x_2)$ et $G_2(u) = (u - x_3)(u - x_4)$ tels que $x_1 = x_2 \mod 2$ et $x_3 = x_4 \mod 2$ sont les solutions de l'équation : $1 + ax + bx^2 = 0$.*
- *Le type $(3,1)$ concerne les courbes de p-rang 1, pour ces cas le Frobenius admet 3 relevés.*
- *Et le type (5) concerne les courbes de p-rang 0, pour ces courbes: toutes les isogénies se réduisent sur le Frobenius.*

Démonstration. En utilisant la section 7.3 et le lemme 7.3.7 et les propriétés de réduction du noyau des isogénies de la section 7.1.1 nous avons que les décompositions quadratiques lisses G de l'équation de $\tilde{\mathcal{C}}$ correspondant aux calculs du Frobenius sont celles dont les diviseurs se réduisent sur des diviseurs principaux de $\mathrm{Jac}\,C$.

• *Dans le cas du type* $(1,1,1)$: Posons $G_1(x) = (x-x_1)(x-x_2)$ et $G_2(x) = (x-x_3)(x-x_4)$ où $x_1 = x_2 \mod 2$ et $x_3 = x_4 \mod 2$ sont les solutions de l'équation : $1 + ax + bx^2 = 0$. Les diviseurs définis sont $\tilde{D}_1 = P_1 + P_2 - 2\infty$ et $\tilde{D}_1 = P_3 + P_4 - 2\infty$ et ceux-ci se réduisent modulo 2 sur les diviseurs principaux $\mathrm{div}(x - x_1)$ et $\mathrm{div}(x - x_3)$. Et le diviseur défini par G_3 se réduise sur 0. Alors $\mathcal{R}(G_1, G_2, G_3)$ correspond au calcul du Frobenius par l'algorithme de Richelot.
• *Dans le cas du type* $(3,1)$: Soit x_0 l'unique solution de l'équation $1 + ax = 0$ or $1 + bx^2 = 0$ (selon le cas voir plus haut 7.3.3). On dénote par $\tilde{x}_0$ et $\tilde{x}_0'$ les deux relevés de x_0. Alors les décompositions quadratiques lisses correspondant au calcul du Frobenius sont donnés par:

$$G_1(x) = (x - \tilde{x}_0)(x - \tilde{x}_0'), \quad G_2(x) = (x - \alpha_1)(x - \alpha_2)$$

$$\text{et} \quad G_3(x) = (x - \alpha_3)(x - \alpha_4)$$

où les α_i se réduisent tous en l'infini. Le diviseur de $G_1(x)$ se réduit sur $\mathrm{div}(x - x_0)$ et les autres sur 0. L'isogénie associée à G en utilisant l'algorithme de Richelot se réduise sur le Frobenius. D'après les propriétés des correspondances de Richelot, on en déduit 3 relevés pour le Frobenius.
• *Dans le cas du type* (5): Pour toute décomposition quadratique lisse G de l'équation $\tilde{\mathcal{C}}$ le diviseur défini par $G_i(x)$ pour $i \in \{1,2,3\}$ se réduit sur 0. □

Remarque 7.3.10. On considère,

$$\Sigma : \mathrm{Jac}\,\mathcal{C} \longrightarrow \mathrm{Jac}\,\mathcal{C}^{\Sigma} \quad \text{et} \quad \widehat{\Sigma} : \mathrm{Jac}\,\mathcal{C}^{\Sigma} \longrightarrow \mathrm{Jac}\,\mathcal{C}$$

Lorsque G définit le noyau de l'isogénie du Frobenius Σ, alors $\mathcal{R}(G)$ définit le noyau de l'isogénie du Verschiebung sur $\widehat{\Sigma}$.
En appliquant cette propriété sur $\mathrm{Jac}\,\mathcal{C}^{\Sigma^{-1}}$, cela permet d'identifier le noyau du Verschiebung $\widehat{\Sigma} : \mathrm{Jac}\,\mathcal{C}^{\Sigma} \longrightarrow \mathrm{Jac}\,\mathcal{C}^{\Sigma^{-1}}$ parmi ceux de ses huit-ramifications.

7.4 RELÈVEMENT CANONIQUE AVEC L'ESPACE MODULAIRE DE HILBERT

Dans ce chapitre nous détaillons l'utilisation des polynômes modulaires de Hilbert dans le relèvenement canonique de surfaces abéliennnes ayant multiplication réelle par $\mathcal{O}_K$ où $K = \mathbb{Q}(\sqrt{D})$ pour $D = 2$ ou 5. Ils paramétrent les isogénies cycliques plutôt que les isogénies de noyaux totalement isotropes maximaux permettant ainsi de réduire le degré d'un endomorphisme.

7.4.1 *Conditions de Kronecker sur l'Espace de Hilbert*

On considère les polynômes modulaires de Hilbert définis à la section 5.2.6 et le chapitre 5 selon le cas classique en fonction des invariants de Gundlach et le cas des invariants en fonction des tirés en arrière des invariants d'Igusa ou des thêtas.
Lorsque $z \in \mathfrak{H}_1^2$, en partant des invariants $(\mathfrak{J}_1(z), \mathfrak{J}_2(z))$ ou de tirés en arrière d'invariants, pour calculer les invariants correspondants des variétés β-isogènes certaines situations sont similaires à celles des calculs avec de invariants en Siegel 7.1 alors que d'autres situations utilisent des invariants intermédiaires.

Situations Directes

On considère $q = \ell^n$ et $\ell = \beta\overline{\beta}$ avec $\beta \in \mathcal{O}_K^+$ et C_β un système de représentation des classes de $\dot{\Gamma}(2,4)/\dot{\Gamma}(2,4) \cap \dot{\Gamma}^0(\beta)$ respectivement de $\overline{\Gamma}/\overline{\Gamma}^0(\beta)$. Alors:
• Pour ℓ est ramifié dans le cas des polynômes avec les invariants de Gundlach.
• Et $D \equiv 1 \mod 4$ dans le cas des polynômes avec les invariants d'Igusa ou des thêtas.

Polynômes avec des Invariants Intermédiaires

Cette situation regroupe les cas suivants :
• lorsque ℓ se décompose pour les polynômes avec les invariants de Gundlach ;
• ou lorsque $D \equiv 2,3 \mod 4$ et $\beta = a + b\omega$ avec b pair, pour les polynômes en fonctions des tirés en arrière d'invariants.

Soit J représentant les invariants Gundlach (ou les tirés en arrière d'invariants) correspondant aux situations décrites ci-dessus ; et Φ_p est la matrice colonne dont les coefficients sont les β-polynômes modulaires.
Le corollaire suivant donne une forme simple des conditions de Kronecker correspondant aux situations décrites.

Corollaire 7.4.1. *Lorsque* $J \notin \mathcal{L}_\ell \cap (\mathbb{F}_p)^2$ *(ou* $J \notin \mathcal{L}_\beta \cap (\mathbb{F}_p)^3$ *):*
i) $\dfrac{\partial \Phi_p}{\partial V}(J, J^\sigma)$ *est inversible sur* $\mathbb{Z}_q$ *;*
ii) $\dfrac{\partial \Phi_p}{\partial U}(J, J^\sigma) \equiv 0 \mod p$.

Démonstration. Cela est une conséquence du chapitre 6 et la section 6.2 sur les conditions de Kronecker. Ainsi on peut appliquer la même approche detaillée dans la preuve de la proposition 7.1.1 (les sections 7.1 et 7.2). □

7.4.2 *Relèvement des Invariants*

Dans les premères situations le revlèvement des invariants vérifiant les conditions de Kronecker peut se faire de manière identique à celui des invariants dans le cas de l'espace de Siegel. Alors pour ce qui suit nous résumons les détails du relèvement des invariants paramétrés par les polynômes modulaires cycliques avec des invariants intermédiares 7.4.1.
Soit J le vecteur formé par les invariants (qui peuvent être des invariants de Gundlach ou des tirés en arrière des thêta constantes) spécifiant un point $\mathcal{A}$ sur l'Espace de Hilbert sur $\mathbb{F}_q$ avec $q = p^n$, $n > 1$.
Supposons que, p se décompose sous la forme $p = \beta\bar{\beta}$ et que nous sommes dans le cas où les polynômes modulaires utilisent des invariants intermédiaires définis par l'action de v:

$$\phi_p(X, J) = \prod_{\gamma \in C_\beta} \left(X - J_{1,\beta}^\gamma\right)\left(X - J_{1,\overline{\beta}}^\gamma\right)$$

Ainsi Φ_p la fonction vectorielle formée par les polynômes modulaires ϕ_p, $\psi_{k,p}$, vérifie la condition:

$$\begin{cases} \Phi_p(J, Y) = 0 \\ \Phi_p(Y, J^\sigma) = 0 \end{cases}$$

où Y représente l'invariant intermédiaire correspondant à l'évaluation du polynôme modulaire au couple (J, J^σ).
Alors connaissant J et J^σ, on peut résoudre le système précédemment en Y défini sur $\mathbb{F}_q$, et le lemme suivant garanti l'unicité de sa solution.

Lemme 7.4.2. *Soit $J \notin \mathcal{L}_\beta$ l'invariant définissant un point sur l'espace modulaire de Hilbert tel que une au moins des composantes de J est en dehors de $\mathbb{F}_p$ et ϕ_β le polynôme minimal de la fonction modulaire associaciée à cette composante, alors:*

- $\dfrac{\partial \Phi_p}{\partial V}(J, Y) \not\equiv 0 \mod p, \quad \dfrac{\partial \Phi_p}{\partial V}(Y, J^\Sigma) \not\equiv 0 \mod p;$
- *Et* $\dfrac{\partial \Phi_p}{\partial U}(Y, J^\Sigma) \equiv 0 \mod p.$

Démonstration. • Selon la propriété de réduction des noyaux d'isogénies: le Frobenius admet un unique rélévé Σ: se réduisant modulo p sur le noyau $\langle 0 \rangle$ alors Y est unique c'est-à-dire qu'on ne peut avoir qu'une seule isogénie g entre Y et J^Σ.
Supposons que l'on ait deux isogénies f_1 et f_2 entre J et Y, alors l'unicité de Σ et de g impliquent que $\mathrm{Im}(f_2 - f_1) \subset \ker(g)$. Comme $\ker(g)$ est un schéma affine fini, on aurait $f_2 - f_1$ constant, par la suite nul. Alors on a $f_1 = f_2$. Comme les deux isogénies respectives (entre J et Y) et (entre Y et J^Σ) sont de multiplicité 1 modulo p, alors les dérivées partielles:

$$\frac{\partial \Phi_p}{\partial V}(J, Y) \quad \text{et} \quad \frac{\partial \Phi_p}{\partial V}(Y, J^\sigma)$$

ne s'annulent pas modulo p (comme dans le cas i) de la section 7.1.1 et la proposition 7.1.1).

• D'un autre côté, comme $J^\Sigma \equiv J^p \mod p$ la même méthode détaillée en ii) la section 7.1.1 et la proposition 7.1.1, basée sur les multiplicités du Verschiebung dans la réduction modulo p des polynômes $\Phi_p(X, J^p)$, montre que $\dfrac{\partial \Phi_p}{\partial U}(Y, J^\sigma) \equiv 0 \mod p$. □

Par suite, on suppose que l'on connaît une approximation de X et T respectivement de J et Y à précision p^k, alors on pose $\tilde{J} - X = p^k e$ et $\tilde{Y} - T = p^k r$ où $e, r \in \mathbb{Z}_q$ sont les erreurs que nous voudrions déterminer en utilisant Φ_p.
Comme $J^\Sigma = X^\Sigma + p^k e^\Sigma$, en utilisant le dévéloppement de Taylor de $\Phi(X + p^k e, T + p^k r) = 0$ et $\Phi(T + p^k r, X^\Sigma + p^k e^\Sigma) = 0$ on obtient:

$$\begin{cases} 0 = & \Phi_p(X, T) + p^k \dfrac{\partial \Phi_p}{\partial U}(X, T) \cdot e + p^k \dfrac{\partial \Phi_p}{\partial V}(X, T) \cdot r + p^{2k}(\cdots) \\ 0 = & \Phi_p(T, X^\Sigma) + p^k \dfrac{\partial \Phi_p}{\partial U}(T, X^\Sigma) \cdot r + p^k \dfrac{\partial \Phi_p}{\partial V}(T, X^\Sigma) \cdot e^\Sigma + p^{2k}(\cdots) \end{cases}$$

où les facteurs $(\cdots)$ derrière p^{2k} sont dans $\mathbb{Z}_q$.
Alors en divisant toutes les équations du système par p^k, on obtient modulo p^k:

$$\begin{cases} 0 = & \dfrac{\Phi_p(X, T)}{p^k} + \dfrac{\partial \Phi_p}{\partial U}(X, T) \cdot e + \dfrac{\partial \Phi_p}{\partial V}(X, T) \cdot r \\ 0 = & \dfrac{\Phi_p(T, X^\Sigma)}{p^k} + \dfrac{\partial \Phi_p}{\partial U}(T, X^\Sigma) \cdot r + \dfrac{\partial \Phi_p}{\partial V}(T, X^\Sigma) \cdot e^\Sigma \end{cases}$$

À partir des conditions de Kronecker (le lemme 7.4.2): $\dfrac{\partial \Phi_p}{\partial V}(X, T)$ et $\dfrac{\partial \Phi_p}{\partial V}(T, X^\Sigma)$ sont inversibles, alors on a:

$$r = -\left[\frac{\partial \Phi_p}{\partial V}(X, T)\right]^{-1} \left(\frac{\Phi_p(X, T)}{p^k} + \frac{\partial \Phi_p}{\partial U}(X, T) \cdot e\right),$$

Par conséquent la résolution du système se réduit à celle d'une équation "d'*Artin-Schreier equation*" de la forme:

$$e^{\Sigma} + Ae + B = 0$$

où on a:

$$A = -\left[\frac{\partial \Phi_p}{\partial V}(T, X^{\Sigma})\right]^{-1} . \frac{\partial \Phi_p}{\partial U}(T, X^{\Sigma}). \left[\frac{\partial \Phi_p}{\partial V}(X, T)\right]^{-1} . \frac{\partial \Phi_p}{\partial U}(X, T),$$

$$B = \left[\frac{\partial \Phi_p}{\partial V}(T, X^{\Sigma})\right]^{-1} \left(\frac{\Phi_p(T, X^{\Sigma})}{p^k} - \frac{\partial \Phi_p}{\partial U}(T, X^{\Sigma}). \frac{\partial \Phi_p}{\partial V}(X, T)^{-1}. \frac{\Phi_p(X, T)}{p^k}\right).$$

Comme les conditions de Kronecker (le lemme 7.4.2) implique:

$$\frac{\partial \Phi_p}{\partial U}(T, X^{\Sigma}) \equiv 0 \mod p \text{ alors } A \equiv 0 \mod p.$$

Ainsi on obtient l'erreur e pour corriger l'approximation J (à la précision p^{2k}) en utilisant l'algorithme d'*Artin-Schreier* dans [35, § 5.3]. Alors nous avons le résultat suivant:

Théorème 7.4.3. *Lorsque $J \in \mathbb{F}_q$ (les invariants de Gundlach ou les tirés-en-arrière d'invariants thêta) représentant un point $\mathcal{A}$ sur l'espace de Hilbert tel que J satisfait les conditions de Kronecker pour les polynômes modulaires de Hilbert. Alors la variante de l'algorithme de Harley (l'algorithme 8) calcule le rélévé $\tilde{J}$ en $O(n^2)$ opérations avec $n = \mathrm{ord}_p\, q$.*

Entrée: J des invariants représentant $\mathcal{A}$, Y la solution du système sur $\mathbb{F}_q$ et une précision N.
Sortie: $\tilde{J}$ à la précision N.

1. **Si** $N = 1$ **Retourner** J et Y à la précision p;
2. **Sinon** $N' = N/2$;
3. J =Harley@Hilbert(J, Y N');
   a. $A = -\left[\frac{\partial \Phi_p}{\partial V}(T, X^{\Sigma})\right]^{-1} . \frac{\partial \Phi_p}{\partial U}(T, X^{\Sigma}). \left[\frac{\partial \Phi_p}{\partial V}(X, T)\right]^{-1} . \frac{\partial \Phi_p}{\partial U}(X, T)$;
   b. $B = \left[\frac{\partial \Phi_p}{\partial V}(T, X^{\Sigma})\right]^{-1} \left(\frac{\Phi_p(T, X^{\Sigma})}{p^k} - \frac{\partial \Phi_p}{\partial U}(T, X^{\Sigma}). \frac{\partial \Phi_p}{\partial V}(X, T)^{-1}. \frac{\Phi_p(X, T)}{p^k}\right)$;
   c. e =ArtinSchreier(A, B, N');
   d. $r = -\left[\frac{\partial \Phi_p}{\partial V}(X, T)\right]^{-1} \left(\frac{\Phi_p(X, T)}{p^k} + \frac{\partial \Phi_p}{\partial U}(X, T) \cdot e\right)$,
   e. $J = J + p^k e$ et $Y = Y + p^k r$ à la précision p^{2k};
4. **Returner** J et Y;

Algorithm 8 – Algorithme de Harley sur l'espace de module de Hilbert.

Démonstration. En utilisant les conditions de Kronecker le lemme 7.4.2 et la méthode de résolution "*d'Artin-Schreier*" équation détaillée dans le chapitre 2 et la section 2.5.1, alors la méthode détaillée dans cette section permet de récouvrir (avec la même complexité $O(n^2)$ que la méthode d'Artin-Schreier) l'erreur correcte pour toute précision à partir de $J \in \mathbb{F}_q$. □

7.4.3 *Exemples de Relèvement avec les Polynômes de Hilbert*

Dans ces exemples de calculs de relèvements des invariants thêta nous utilisons des polynômes déjà calculés par E.Milio dans sa thèse de doctorat [78, 79].

Relèvement des Invariants Thêta pour $\mathbb{Q}(\sqrt{2})$ *en Caractéristique* 5

Dans ce cas le morphisme du 5-ième Frobenius est inerte sur $\mathbb{Q}(\sqrt{2})$.
On considère le corps $\mathbb{F}_5[X]/m$ où: $m = X^7 + 3X + 3$ et $\mathfrak{b}_2 = X$, $\mathfrak{b}_3 = 3$ et $\mathfrak{b}_1 = 3X^2 + 2$ les invariants de thêta d'une surface abélienne $\mathcal{A}$ sur $\mathbb{F}_5[X]/m$.
On pose $J = [\mathfrak{b}_2, \mathfrak{b}_3]$ que nous voulons réléver sur $\mathbb{Z}_q$ avec $q = 5^7$ car on a $\mathfrak{b}_1 = (\mathfrak{b}_2 + \mathfrak{b}_3^2)/2$.
À une précision de 5^{16}, on obtient comme polynôme de Teichmuller:

$$\begin{aligned} M =& X^7 + 26941848975X^6 + 2901765225X^5 + 136053272250X^4 \\ &+ 78296802910X^3 + 119068596420X^2 + 117632782643X \\ &+ 49925501068; \end{aligned}$$

Alors l'algorithme 7 dans les sections 7.1 et 7.2 nous donne:

$$\begin{aligned} \tilde{J} = [&138519127940X^6 + 82646512005X^5 + 66125929130X^4 \\ &+ 13577818665X^3 + 100249545506X^2 + 112840384440X \\ &+ 14980687290, 98963138605X^6 + 21368067695X^5 \\ &+ 52557804060X^4 + 151876542585X^3 + 135343131255X^2 \\ &+ 81220969846X + 12795578393]. \end{aligned}$$

exemple 7.2 – Relèvement des Invariants Thêta pour $\mathbb{Q}(\sqrt{2})$ en Caractéristique 5.

Relèvement des Invariants Thêta pour $\mathbb{Q}(\sqrt{2})$ en Caractéristique 7

Dans ce cas le morphisme du 7-ième Frobenius se décompose sur $\mathbb{Q}(\sqrt{2})$.
On considère le corps $\mathbb{F}_7[X]/m$ où $m = X^{10} + X^6 + X^5 + 4X^4 + X^3 + 2X^2 + 3X + 3$ avec J le vecteur des invariants thêta $\mathfrak{b}_1$ et $\mathfrak{b}_2$ de la surface abélienne $\mathcal{A}$ que nous voulons réléver sur $\mathbb{Z}_{7^{10}}$.

$$\begin{aligned} J = [&X^9 + 6X^8 + 2X^7 + 3X^6 + 4X^5 + 6X^2 + X + 6, \\ &X^9 + 6X^8 + 3X^7 + 6X^6 + 5X^5 + 5X^4 + 3X^3 + 4X^2 + X + 3] \end{aligned}$$

À partir du polynôme cyclique on calcul sur $\mathbb{F}_{7^{10}}$ les invariants thêta intermédiaires. Sachant que c'est une solution J_{int} du système

$$\begin{cases} \Phi_p(J, Y) = 0, \\ \Phi_p(Y, J^7) = 0. \end{cases}$$

n'appartenant pas à l'ensemble $\mathcal{L}_\ell \cap (\mathbb{F}_7)^2$.

$$\begin{aligned} J_{int} = [&6X^9 + 2X^8 + 2X^7 + 5X^6 + 5X^4 + 4X^3 + 6X^2 + X + 3, \\ &4X^9 + 2X^8 + 2X^7 + 5X^6 + 6X^4 + 5X^2 + 6X]. \end{aligned}$$

$$\begin{aligned} M = &X^{10} + 389747593107578334251496972X^9 + 180939175172265627977707274X^8 + \\ &820639109166877804289290966X^7 + 131887355846932099924702249X^6 + \\ &121266091566247143956159224X^5 + 461264446170929852035132727X^4 + \\ &601063599941632172000280143X^3 + 359625048065291962433680566X^2 + \\ &892555097284609263309066 18X + 870862203657907303192001683; \end{aligned}$$

Alors l'algorithme 8 dans la section 7.4.2 et la section 7.4 nous donne:

$$\begin{aligned} \tilde{J} = [&1297410835054183574161395 1X^9 + 736285665317500307261954120X^8 + \\ &252704946594161462853025058X^7 + 344881913903677978390848512X^6 + \\ &440061182663717000160228556X^5 + 546567818309614051963074062X^4 + \\ &759971315137437890804466261X^3 + 395505353352671247298116146X^2 + \\ &893378103178005334695930377X + 910636861101123617203813454, \\ &784623245580678440883298857X^9 + 100808707222360157135274574 7X^8 + \\ &234947087489147532452529460X^7 + 432888814352820281132739362X^6 + \\ &567604469139263798493214213X^5 + 628919076485468412446677362X^4 + \\ &350269558955349671468018737X^3 + 770808683780643181938377831X^2 + \\ &274337567861932071403143462X + 957385751029172560819264250]. \end{aligned}$$

exemple 7.3 – Relèvement des Invariants Thêta pour $\mathbb{Q}(\sqrt{2})$ en Caractéristique 7.

8

APPLICATIONS

Dans ce chapitre, nous utilisons le calcul de relevé canonique d'une part pour relever des formes modulaires et d'autre part pour calculer le polynôme caractéristique d'une courbe de genre 2 (comme une extension en genre 2, de la méthode de Satoh). Ces nouveaux algorithmes fournissent des complexités très pratiques ; les idées et certains exemples sont repris des papiers ([70, 71]).

8.1 RELÈVEMENT DE FORMES MODULAIRES

Dans cette section, nous allons nous intéresser dans un premier temps aux méthodes de calcul de formes modulaires vectorielles pour les courbes de genre 2 définie sur $\mathbb{F}_q$ (sur les relevés canoniques). Et en deuxième temps l'opération inverse aussi est abordée à savoir les méthodes de calculs de covariants frationnaires associés aux rélévées canoniques des courbes de genre 2. Et très rapidement on se rend compte que les deux opérations sont associées aux calculs des équations de relevés canoniques sur $\mathbb{Z}_q$.
Lorsqu'on part d'une courbe $\mathcal{C} : f(x, y) = 0$ de genre 2, l'équation $\tilde{f}(x, y) = 0$ du relevé canonique $\tilde{\mathcal{C}}$ dont nous avons besoin, doit nécéssairement vérifier:

$$\tilde{f}(x, y) = f(x, y) \mod p.$$

Dans le chapitre 4 et la section 4.6 nous avons vu que l'action de $\mathrm{GL}_2(\mathbb{C})$ a une représentation scalaire $\det^k$ sur $V = \mathbb{C}$ et une représentation irréductible correspondant à $\det^k \mathrm{Sym}^n$ pour tous k et $n \in \mathbb{N}$. Ainsi $\det^k$ désigne le poids des formes modulaires scalaires de Siegel. Par exemple les formes modulaires de Siegel ψ_4, ψ_6, ψ_{10} et ψ_{12} de poids respectives $\det^k$ avec $k = 4, 6, 10, 12$ engendrent l'anneau gradué des formes modulaires scalaires de poids paires en dimension 2.
Le relèvement des covariants fractionnaires associés à une courbe de genre 2 fournirait des représentations très pratiques: par exemple à partir des triplets définis dans le chapitre 4, la section 4.3 et le théorème 4.3.2 on pourrait travailler sur certaines classes d'isomorphismes comme celles parcourant la composantes $\mathfrak{A}_2$ définies par $\psi_4 = 0$.
Lorsque f est une forme modulaire, $\mathrm{Cot}(f)$ est un covariant polynomial selon le principe de Koecher. Réciproquement, si F est un covariant fractionnaire, la fonction $f : \Omega \mapsto F(\mathcal{C}(\Omega))$ est une forme modulaire de Siegel méromorphe du même poids associé à F.
Ces deux fonctions sont définies dans le chapitre 4 et la section 4.6 pour plus de détails sur leurs propriétés se referer à [98]. Et d'autre part la fonction cot s'étend aux fonctions modulaires de Hilbert.
Lorsque $\mathcal{A}$ représente la variété Jacobienne munie d'un plongement $\mu : \mathcal{O}_{\mathbb{K}} \hookrightarrow \mathrm{End}^s(\mathcal{A})$ et ω une base des différentielles sur $\mathcal{A}$. Soient $\eta : \mathcal{A} \longrightarrow \mathcal{A}(t)$ pour $t \in \mathfrak{H}_1^2$ un isomorphisme et $m \in \mathrm{GL}_2(\mathbb{C})$ une matrice de changement de base telle que: $\omega = m\eta^*\omega(t)$. Lorsque le triplet $(\mathcal{A}, \mu, \omega)$ est normalisé (c'est-à-dire m est diagonale), pour toute fonction modulaire de Hilbert de poids (k_1, k_2) c'est-à-dire toute fonction méromorphique $f : \mathfrak{H}_2 \to \mathbb{C}$ vérifiant:

$$f(\gamma z) = (cz_1 + d)^{k_1}(\bar{c}z_2 + \bar{d})^{k_2} f(z) \ , \ \forall \gamma \in \mathrm{SL}_2(\mathcal{O}_{\mathbb{K}} \otimes \partial_{\mathbb{K}}) \text{ et } z \in \mathfrak{H}_1^2;$$

la quantité $f(\mathcal{A}, \mu, \omega)$ est donné par:

$$f(\mathcal{A}, \mu, \omega) := m_1^{-k_1} m_2^{-k_2} f(t) \quad \text{où} \quad m = \text{diag}(m_1, m_2).$$

Alors $f(\mathcal{A}, \omega)$ est bien-défini lorsque $(\mathcal{A}, \omega)$ a ses endomorphismes réels diagonals c'est-à-dire lorsque pour tout $\alpha \in \text{End}^s(\mathcal{A})$, α^* est diagonal dans la base ω. Par conséquent, sur un autre corps $\mathbb{F}$, pour identifier une courbe Hilbert-normalisée on fixe un morphisme : $\mathcal{O}_{\mathbb{K}} \longrightarrow \mathbb{F}$ (c'est-à-dire on fixe dans $\mathbb{F}$ une valeur de $\sqrt{\Delta}$), alors on pourra utiliser les mêmes caractérisations que $f(\mathcal{A}, \omega)$ données dans le chapitre 4 et la section 4.6. Ainsi la quantité $f(\mathcal{A}, \mu, \omega)$ est bien-définie sur $\mathbb{F}$.

Exemple 8.1.1. Reconstitution de l'équation de $\tilde{\mathcal{C}}$ à partir de l'Espace de Siegel.

En caractéristique $p \leq 5$ **:** Dans ces différents cas, l'algorithme de J.F.Mestre a une mauvaise réduction modulo p (par exemple la réduite de la conique définie dans l'algorithme n'est pas définie modulo p). Ainsi dans la section 7.1 et la section 7.3.2, on utilise un système polynomial avec des invariants définis dans le chapitre 4, la section 4.3 et le théorème 4.3.2 pour calculer les équations d'une forme normale du rélévé canonique d'une courbe ordinaire de genre 2. Nous pouvons étendre cette méthode sur les autres composantes de $\mathcal{M}_2 \otimes \mathbb{k}$ (définies dans le chapitre 4, la section 4.3 et le théorème 4.3.2) pour les caractéristiques 3 et 5.

Par exemple lorsque l'on travaille sur la composante $\mathcal{M}_2[J_4^{-1}]$ de $\mathcal{M}_2$ en caractéristique 3, on peut exprimer les invariants $(\mathfrak{d}_1, \mathfrak{d}_2, \mathfrak{d}_3)$ en fonction des coefficients a, b, c, et d de la forme normale de la courbe $\mathcal{C}$ associée. On peut alors écrire: $y^2 + (1 + ax + bx^2)y = -x^3(c + dx + x^2)$ un modèle hyperelliptique de $\mathcal{C}$. Les coefficients $\tilde{a}$, $\tilde{b}$, $\tilde{c}$ et $\tilde{d}$ de la forme normale du rélévé $\tilde{\mathcal{C}}$ se réduisant sur $\mathcal{C}$ satisfont le système d'équations en les variables a, b, c et d:

$$\begin{cases} J_2^2 - J_4 \tilde{\mathfrak{d}_1} & = 0, \\ J_6^2 - J_4^3 \tilde{\mathfrak{d}_2} & = 0, \\ J_{10}^2 - J_4^5 \tilde{\mathfrak{d}_3} & = 0 \end{cases}$$

où le triplet $(\tilde{\mathfrak{d}_1}, \tilde{\mathfrak{d}_2}, \tilde{\mathfrak{d}_3})$ est le relevé du triplet $(\mathfrak{d}_1, \mathfrak{d}_2, \mathfrak{d}_3)$ définissant la courbe $\mathcal{C}$ que l'on calcule rapidemment avec la méthode de la section 7.1 et la section 7.3.2 lorsque $(\mathfrak{d}_1, \mathfrak{d}_2, \mathfrak{d}_3)$ satisfait les conditions de Kronecker.

En caractéristique $p > 5$ **:** Dans ce cas la conique de Mestre a une bonne réduction. On peut relever le model hyperelliptique $y^2 = f(x)$ d'une courbe $\mathcal{C}$ de genre 2 connaissant les invariants du relevé canonique $\tilde{\mathcal{C}}$ comme suit:

• On construit d'abord la cubique $\mathcal{M}$ et la conique $\mathcal{L}$ correspondant à $\mathcal{C}$ sur $\mathbb{Z}_q$ en utilisant $\tilde{J}$.

• Comme $\mathcal{M}$ et $\mathcal{L}$ ont une bonne réduction, nous pouvons extraire modulo p un point de paramétrage P sur $\mathcal{M} \mod p$ correspondant à la construction de l'équation $y^2 = f(x)$.

• Alors on calcule le rélévé $\tilde{P}$ de P en utilisation $\mathcal{M}$ et par la méthode de Mestre on réconstitue l'équation $y^2 = \tilde{f}(x)$ de la courbe $\tilde{\mathcal{C}}$.

8.2 CALCUL DU POLYNÔME CARACTÉRISTIQUE

L'une des applications les plus répandues du relèvement canonique est bien le calcul des valeurs propres du morphisme de Frobenius pour ensuite retrouver son polynôme caractéristique $\chi \in \mathbb{Z}[t]$ (ou sa fonction zêta) pour une courbe hyperelliptique de genre g.

LES CONJONCTURES DE WEIL

Soit $\mathcal{C}$ une courbe algébrique projective lisse de genre g définie sur $\mathbb{F}_q$ avec $q = p^n$. On appelle *fonction Zêta* de $\mathcal{C}$ sur $\mathbb{F}_q$ la fonction définie par

$$Z(t) = exp\left(\sum_{k\geq 1} N_k \cdot \frac{t^k}{k}\right)$$

où N_k désigne le cardinal de $\mathcal{C}(\mathbb{F}_{q^k})$.
Alors nous avons les résultats suivants connu auparavant sous le nom de *Conjuctures de Weil*:
• $Z(t)$ est une fraction rationnelle et plus précisement

$$Z(t) = \frac{L(t)}{(1-t)(1-qt)}$$

où $L(t) = a_0 + a_1 t + \cdots + a_{2g}t^{2g}$ est un polynôme dont les coefficients sont des entiers vérifiants

$$a_0 = 1, \quad a_{2g} = q^g \quad et \quad a_{2g-i} = q^{g-1}a_i \quad pour \quad 0 \leq i \leq g.$$

• Lorsque l'on considère $L(t) = \prod_{i=1}^{2g}(1-\alpha_i t)$, l'hypothèse de Riemann implique $|\alpha_i| = \sqrt{q}$ ce qui donne pour les coefficients de $L(t)$, la borne

$$|a_i| \leq \binom{2g}{i} q^{i/2}$$

En organisant les racines de la manière $\alpha_i\alpha_{i+g} = q$ pour $i = 0, \cdots, g$ on a:

$$\log Z(t) = \sum_{i=1}^{2g} \log(1-\alpha_i t) - \log(1-t) - \log(1-qt)$$

Comme $\log(1-st) = -\sum_{i=1}^{\infty} \frac{(st)^k}{k}$, on peut conclure que

$$N_k = q^k + 1 - \sum_{i=1}^{2g} \alpha_i^k \quad pour \quad k \in \mathbb{N}^*.$$

Une preuve de la rationnalité de $Z(t)$ dans le cas générale a été proposée par Dwork [29]. Celle de l'hypothèse de Riemann est l'œuvre de Deligne [23].
On notera aussi le Frobenius sur $\operatorname{Jac} C$ par π_q et un point P de $\operatorname{Jac} C$ est $\mathbb{F}_q$-rationnel si et seulement si $\pi_q(P) = P$ c'est-à-dire :

$$\operatorname{Ker}(\pi_q - \mathrm{id}) = \operatorname{Jac} C(\mathbb{F}_q)$$

L'application $(\pi_q - \mathrm{id})$ étant séparable cela implique que

$$|\operatorname{Jac} C(\mathbb{F}_q)| = \deg(\pi_q - \mathrm{id})$$

On montre aussi que: $|\operatorname{Jac} C(\mathbb{F}_q)| = \chi(1)$ et que $L(t) = t^{2g}\chi(1/t)$.
Et pour le cas du genre 1 la connaissance de $\chi(1)$ est équivalente à celle de $Z(t)$.
Le calcul de la fonction Zêta $Z(t)$ d'une courbe $\mathcal{C}$ contient d'importantes propriétés géométriques sur C et $\operatorname{Jac} C$.
Lorsque $L(t) = c_0 + \cdots + c_{2g}t^{2g}$ le p-rang de $\operatorname{Jac} C$ est égal au plus grand i pour lequel c_i

est non nul modulo p [111]. Et Jac C est isogène sur $\overline{\mathbb{F}_q}$ à un produit de courbes elliptiques supersingulières si et seulement si $p^{nk/2}$ divise c_k pour tout $1 \leq k \leq g$ avec $q = p^n$ [112].
D'autre part le calcul du polynôme caractéristique χ (ou de $\chi(1)$) intervient en théorie des codes correcteurs d'erreurs, pour un genre fixé il indique la qualité du code crée à partir de celle-ci. En cryptographie, l'ordre du groupe des points de la jacobienne est un paramètre de sécurité . Ces calculs constituent aussi des outils essentiels pour bon nombres de mathématiciens.

Il existe deux classes de méthodes qui déterminent rapidement la fonction $Z(t)$ ou le polynôme caractéristique $\chi(t)$.
• Les premiers constituent la classes des *méthodes ℓ-adiques* initiées par R.Schoof [102] sur les courbes elliptiques. Il fut ensuite étendu aux variétés abéliennes d'une part par Pila [91], Adleman et Huang [1] et d'autre part par B. Edixhoven [31] tout en gardant la même approche.
On considère que $\mathcal{A}$ est une variété abélienne de dimension g sur $\mathbb{F}_q$ de polynôme caractéristique de l'endomorphisme du Frobenius $\chi(t)$.
Pour tout premier $\ell \neq p$ le groupe de $\mathcal{A}[\ell]$ torsion étant un $\mathbb{F}_\ell$-espace vectoriel de dimension de $2g$ sur lequel π_q agit de manière $\mathbb{F}_\ell$-linéaire, le polynôme caractéristique de cet endomorphisme est $\chi \mod \ell$.
Alors ces algorithmes consistent à:
− Calculer $\chi \mod \ell$ en utilisant l'action de $\mathcal{A}[\ell]$.
− On répète cette opération pour différents ℓ en considerant les bornes des coefficients de $\chi(t)$.
− Reconstruire $\chi(t)$ en utilisant le théorème des restes chinois.
Les différences entre l'algorithme de Schoof et ses améliorations résident surtout dans leur manière de calculer $\chi \mod \ell$. Et pour les courbes elliptiques les plus rapides de ces algorithmes (comme les améliorations de SEA [5, 32]) peuvent calculer $\chi \mod \ell$ en $\tilde{O}\left((\ell + \log q)\ell \log q\right)$ pour une évaluation de χ en $\tilde{O}\left((\log q)^4\right)$.
L'une des difficultés associée à la généralisation des méthodes ℓ-adiques au genre supérieur vient de la difficulté à manipuler $\mathcal{A}[\ell]$ même s'il existe souvent des possibilités à travailler que dans un sous-espace de dimension inférieure. En effet, $\mathcal{A}[\ell]$ contient ℓ^{2g} points ce qui revient à considérer un objet de taille $\ell^{2g} \log q$. Et aussi le calcul effectif de l'image par σ_q des points de $\mathcal{A}[\ell]$ qui se fait en $O\left(\ell^{2g}(\log q)^2\right)$ opérations. Alors l'algorithme schématique de Schoof pourrait au mieux tourner avec une complexité de $\tilde{O}(g^{1+2g}(\log q)^{2g+3})$ (voir [35]). Cependent en pratique l'algorithme de Schoof en genre 2 n'est pas aussi performant que l'on pourrait l'espérer à cause du coût de la caractérisation de l'ideal I_ℓ de $\mathcal{A}[\ell]$ [38]. Ainsi les meilleures implantations ont des complexités totales d'environ $\tilde{O}(\log q^8)$.

• L'autre classe d'algorithmes regroupent ceux utilisant les méthodes dites *p-adiques* qui débutèrent avec l'utilisation par T. Satoh [99] du relèvement canonique pour évaluer la trace du Frobenius d'une courbe elliptique ordinaire. Cette approche fut améliorer par bon nombre d'auteurs selon les manières de calcul du relévé de la courbe ou de l'évaluation de l'action l'endomorphisme du Frobenius π_q (voir dans le chapitre 2 et la section 2.6.1). Toujours sur les courbes elliptiques ordinaires, lorsque la caractéristique est 2 et en considérant que le relevé canonique admet $y^2 = x(x - a^2)(x - b^2)$ équation sur $\mathbb{Z}_q$, alors nous avons une courbe 2-isogène d'équation $y^2 = x(x - a'^2)(x - b'^2)$ avec $a' = \dfrac{a+b}{2}$ et $b' = \sqrt{ab}$. Cette construction par la *moyenne arithmético-géométrique* permet de calculer une suite de courbes reliées par le

Frobenius tout en gagnant de précisions à chaque étape.
Cette méthode dite de *l'AGM* introduite J-F. Mestre bien qu'étant schématiquement différente de l'approche de Satoh (n'utilisant pas de polynômes modulaires), est bien la prémière méthode à connaître une généralisation en dimension supérieure .
Mestre utilisa les relations entre l'AGM et les formules de duplication de Riemann pour les fonctions Thêta analytiques [73]. Une meilleure amélioration de cette approche est donnée par R. Carlz et D. Lubicz dans [13] en utilisant les invariants artithmétiques des relévés canoniques à partir d'un système de coordonnés produit par les thêta nuls points associés à une variété abélienne munie de thêta structure de niveau $2^v p$ pour $p > 2$. En partant des formules de Thomae et des relations de Riemann on peut évaluer l'action du relévé Σ du Frobenius σ sur le tore formel de Serre-Tate [13]. L'algorithme de Carlz et Lubicz a une complexité asymptotique en temps de $O\left(n^{2+o(1)}\right)$ et en espace de $O(n^2)$. On peut souligner que cette méthode nécéssite de prendre des extensions et que l'utilisations des mêmes formules en fonction de p devient rapidement très péniblible.
Une autre méthode p basée sur le calcul de l'action du relévé de l'endomorphisme du Frobenius sur le groupe de cohomologie de Monsky-Washnitzer a été developpée par Kedlaya et autres [57, 116].
Soit $\mathcal{C} : f(x,y) = 0$ une courbe hyperelliptique de genre g sur $\mathbb{F}_q$. La particularité de l'algorithme de Kedlaya est que le relèvement utilisé est quelconque et on prend la complétion faible ("dague") du relevé par les séries convergentes $A^\dagger = \mathbb{Q}_q\langle\langle x,y\rangle\rangle / \tilde{f}(x,y)$ pour définir le relevé Σ du Frobenius. Les seuls groupes de cohomologie de Monsky-Washnitzer associée à $A^\dagger$ sont $H^0(A^\dagger)$ et $H^1(A^\dagger)$. Alors en utilisant le *théorème du point fixe de Lefschetz* $H^0(A^\dagger)$ et $H^1(A^\dagger)$ on a:

$$\#\mathcal{C}/\mathbb{F}_q = Tr\left((q\Sigma_*^{-1})^k | H^0(A^\dagger)\right) - Tr\left((q\Sigma_*^{-1})^k | H^1(A^\dagger)\right)$$

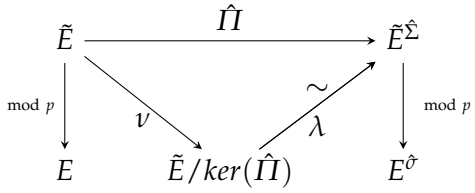
où Σ_* est l'action induite par Σ sur l'espace cohomologique.
L'algorithme de Kedlaya [57] reconstitue la fonction Zêta de $\mathcal{C}$ avec une complexité en temps de $O(g^{4+\epsilon}n^{3+\epsilon})$ et en espace de $O(g^{4+\epsilon}n^{3+\epsilon})$. Les améliorations par des auteurs comme Vercauteren qui proposa un model en caractéristique 2 [25] et Harvey [46] n'ont pas réduit la complexité en n.

Nous proposons dans ce chapitre des algorithmes de calcul du polynôme caractéristique basés sur le relèvement canonique de la variété Jacobienne.
Pour ce qui suit nous partirons des conditions de Kronecker sur les systèmes d'invariants pour calculer le relèvé et selon les approches de calculs d'isogénie on déduit des algorithmes éfficaces de calcul des valeurs propres du Frobenius.

8.2.1 *En Utilisant le Relèvement de la p-Torsion*

Par l'action galoisienne de Σ, il est facile de voir que la matrice changement de base entre la base différentielle canonique de $\tilde{\mathcal{C}}^{\hat{\Sigma}^n}$ et $\tilde{\mathcal{C}}^{\hat{\Sigma}^{n+1}}$ est donné par $\Sigma^{-n}M$. Donc si on considère $\hat{\Sigma}_q$ le relevé du grand Verschiebung $\hat{\sigma_q}$, le dual du Frobenius σ_q, on obtient que la matrice du grand Verschiebung agissant sur les différentielles de $\tilde{\mathcal{C}}$ est $M_q = N_{\mathbb{Q}_q/\mathbb{Q}_p}(M)$. Cette matrice est diagonale, avec pour valeurs propres λ_1, λ_2, les racines inversibles du polynôme caractéristique χ_π. Les deux autres racines sont q/λ_1, q/λ_2.

Alternativement, plutôt que de calculer directement M, nous utilisons le schéma de l'algorithme de Satoh dans la section 2.6.1 et le chapitre 2 qui consiste à relevé canoniquement la variété abélienne et sa p-torsion.



Ensuite par un calcul d'isogénie déduire l'action de l'isogénie Frobenius Σ. Nous pouvons calculer $I_k(\tilde{\mathcal{C}}^{\hat{\Sigma}})/I_k(\tilde{\mathcal{C}}^{\nu})$ pour obtenir $\det M^k$ où I_k est n'importe quel covariant de degré k.

Calcul d'Isogénies: Approche de Vélu

Soit f une isogénie de degré ℓ entre les variétés abéliennes $\mathcal{A}$ et $\mathcal{B}$ de dimension g . Soit K un sous-groupe isotropique maximal de la ℓ-torsion $\mathcal{A}[\ell]$ et $Z(n)$ désigne $\mathbb{Z}^g/n\mathbb{Z}^g$.

$$\begin{aligned} f : \mathcal{A} = \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g) &\longrightarrow \mathcal{B} = \mathbb{C}^g/(\ell\Omega\mathbb{Z}^g + \mathbb{Z}^g) \\ z &\longmapsto \ell.z \end{aligned}$$

On peut toujours choisir une base symplectique de $\mathcal{A}$ pour laquelle K est isomorphe à $\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$. Dans ce cas lorsque $\Omega \in \mathfrak{H}_g$ est la matrice de période de $\mathcal{A}$ on peut calculer K à partir des thêta constantes

$$\theta_b^{\mathcal{A}} := \Theta \begin{bmatrix} 0 \\ \frac{b}{n} \end{bmatrix} \left(\cdot\, , \frac{\Omega}{n} \right) \quad et \quad \theta_b^{\mathcal{B}} := \Theta \begin{bmatrix} 0 \\ \frac{b}{n} \end{bmatrix} \left(\cdot\, , \frac{\ell\Omega}{n} \right)$$

et un point générique de $\mathcal{A}$. On pourra consulter [19] pour plus de détails sur ce calcul .
Nous considérons le cas où l'on part de la connaissance de $\mathcal{A}$ et d'une base de K et nous voulons déterminer les thêta constantes de la surface abélienne $\mathcal{B} = \mathcal{A}/K$.
On note par $(\tilde{e}_1, \cdots, \tilde{e}_g)$ la base canonique de $\frac{1}{\ell}\mathbb{Z}^g$ se réduisant sur la base de coordonnées $(e_1, \cdots, e_g)$ de K.
Alors le théorème suivant détermine les thêta constantes de $\mathcal{B}$ à partir $(\theta_k^{\mathcal{A}}(\tilde{e}_i))_{k\in Z(n)}$ avec des facteurs projectifs inconnus près λ_i pour $i = 1, \cdots, g$.

Théorème 8.2.1. *Soit F une matrice de rang r telle que ${}^tFF = \ell.Id_r$. Soit $X \in (\mathbb{C}^g)^r$ et $Y = \ell.XF^{-1}$. Soit $i \in (Z(n))^r$ et $j = iF^{-1}$. Alors nous avons :*

$$\theta_{i_1}^{\mathcal{B}}(Y_1)\cdots\theta_{i_r}^{\mathcal{B}}(Y_r) = \sum_{\substack{t_1,\cdots,t_r \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g \\ (t_1,\cdots,t_r)F = 0}} \theta_{j_1}^{\mathcal{A}}(X_1 + t_1)\cdots\theta_{j_r}^{\mathcal{A}}(X_r + t_r) \tag{8.1}$$

De plus, pour $k \in Z(n)$ et $j = (k, 0\cdots 0)F^{-1}$:

$$\theta_k^{\mathcal{B}}(0)\theta_0^{\mathcal{B}}(0)\cdots\theta_0^{\mathcal{B}}(0) = \sum_{\substack{t_1,\cdots,t_r \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g \\ (t_1,\cdots,t_r)F = 0}} \theta_{j_1}^{\mathcal{A}}(t_1)\cdots\theta_{j_r}^{\mathcal{A}}(t_r) \tag{8.2}$$

Démonstration. Aller à [19]. □

Dans le cas où $\theta_0^{\mathcal{B}}(0) = 0$, on utilise la première équation avec $i_2 = \cdots = i_r$ correspondant aux coordonnées non nulles. Alors on aura les monômes de la somme avec des facteurs projectifs inconnus. D'après le [19, Lemme 4.2.] les monômes

$$\theta_{j_1}^{\mathcal{A}}(t_1) \cdots \theta_{j_r}^{\mathcal{A}}(t_r)$$

sont invariants sous l'action des transformations T de $\mathbb{C}[\lambda_i, \lambda_{i,j}]$ agissant sur les générateurs par une racine ℓ-ième de l'unité. Par suite, on montre que ces monômes dépendent uniquement des λ_i^ℓ, $\lambda_{i,j}^\ell$ qui sont connus. Les $\left(\theta_k^{\mathcal{B}}(0)\right)_{k \in Z(n)}$ sont donc déterminés projectivement en prenant une racine ℓ-ième des λ_i^ℓ, $\lambda_{i,j}^\ell$ avant d'appliquer l'équation 8.2.

Dans le cas où $\ell = a^2 + b^2$, on peut prendre $F = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ et $r = 2$.
Cependant on peut toujours mettre ℓ sous la forme

$$\ell = a^2 + b^2 + c^2 + d^2$$

et ainsi prendre la matrice de multiplication par $a + b_i + c_j + d_k$ dans une algèbre de quaternions sur $\mathbb{R}$, avec $r = 4$.

Entrée: Une surface abélienne $\mathcal{A}$ et la base $\{e_1, e_2\}$ en coordonnées thêta du sous-groupe isotropique maximal $K \subset \mathcal{A}[\ell]$.
Sortie: Les thêta constantes de surface abélienne $\mathcal{B} = \mathcal{A}/K$.

1. Prendre une matrice F sur $\mathbb{Z}$ de rang r telle que ${}^tFF = \ell\,\mathrm{Id}$;
2. Calculer $e_1 + e_2$ dans $\mathcal{A}$;
3. Écrire $\tilde{e}_1$, $\tilde{e}_2$ et $\tilde{e}_1 + \tilde{e}_2$ en coordonnées thêta avec des facteurs projectifs inconnus λ_1, λ_2 et $\lambda_{1,2}$ utilisés comme indeterminés.
4. En utilisant l'addition différentielle calculer les coordonnées affines de tous les points de K dans $\mathbb{C}[\lambda_1, \lambda_2, \lambda_{1,2}]$.
5. À partir des coordonnées affines de $\frac{\ell-1}{2}\tilde{e}_1$ et $\frac{\ell}{2}\tilde{e}_2$, reconstituer les relations $\lambda_1^\ell = \alpha_1$, $\lambda_2^\ell = \alpha_2$ et $\lambda_{1,2}^\ell = \alpha_{1,2}$.
6. Pour $k \in Z(n)$ et $j = (k, 0, \ldots, 0)F^{-1}$ et calculer dans $\mathbb{C}[\lambda_1, \lambda_2, \lambda_{1,2}]/\{\lambda_1^\ell = \alpha_1,\ \lambda_2^\ell = \alpha_2,\ \lambda_{1,2}^\ell = \alpha_{1,2}\}$

$$\theta_k^{\mathcal{B}}(0)\theta_0^{\mathcal{B}}(0) \cdots \theta_0^{\mathcal{B}}(0) = \sum_{\substack{t_1, \cdots, t_r \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g \\ (t_1, \cdots, t_r)F = 0}} \theta_{j_1}^{\mathcal{A}}(t_1) \cdots \theta_{j_r}^{\mathcal{A}}(t_r)$$

Algorithm 9 – Algorithme de Vélu en coordonnée thêta

Lorsque l'on part d'une courbe de genre 2 et un sous-groupe isotropique maximal de $\mathrm{Jac}(\mathcal{C})[\ell]$. Des conversions entre coordonnées Mumford et Thêta au niveau des éléments de base de K suivies d'une application de l'algorithme 9 permettent d'aboutir à une courbe $\mathcal{C}'$ dont la variété Jacobienne est $\mathrm{Jac}(\mathcal{C})/K$.

Exemple 8.2.2. (Cas $g = 2$) À partir des entrées $\{e_1, e_2\}$ une base en coordonnées thêta d'un sous-groupe isotropique maximal $K \subset \mathcal{A}[\ell]$, l'algorithme 9 retourne $\theta_k^{\mathcal{B}}(0) \times C_0$, où

$C_0 = \theta_0^{\mathcal{B}}(0)$ si $\ell \equiv 1 \mod 4$ et $C_0 = \theta_0^{\mathcal{B}}(0)^3$ si $\ell \equiv 3 \mod 4$.
Notons ce résultat par (a, b, c, d) alors nous avons:

— Pour $\ell \equiv 3 \mod 4$:

$$a = \theta_0^{\mathcal{B}}(0) \cdot C_0, \cdots, d = \theta_3^{\mathcal{B}}(0) \cdot C_0$$

où $a = \theta_k^{\mathcal{B}}(0)^4$ c'est-à-dire $C_0 = \theta_k^{\mathcal{B}}(0)^3$. À partir des formules la section 3.3.1.3 et la section 3.3 on a h_4' avec un facteur C_0^8 et Comme $C_0^8 = a^6$, on en déduit $h_4 = h_4'/a^6$ et en utilisant la même méthode $h_{10} = h_{10}'/a^{15}$.

— Pour le cas $\ell \equiv 3 \mod 4$ on a:

$$a = \theta_0^{\mathcal{B}}(0) \cdot C_0, \cdots, d = \theta_3^{\mathcal{B}}(0) \cdot C_0$$

où $C_0 = \theta_0^{\mathcal{B}}(0)$. Alors $h_4 = h_4'/a^4$ et $h_{10} = h_{10}'/a^{10}$.

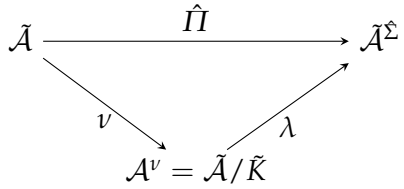
8.2.2 *En Caractéristique Deux: Description et Complexité de l'Algorithme*

Soient $\mathcal{C}$ une courbe hyperelliptique ordinaire de genre 2 sur $\mathbb{F}_{2^n}$ et $\mathcal{A}$ sa variété jacobienne. L'endomorphisme de Frobenius se décompose comme suit:

$$\mathcal{A} \xrightarrow{\pi} \mathcal{A}^{\sigma} \longrightarrow \cdots \longrightarrow \mathcal{A}^{\sigma^{n-1}} \xrightarrow{\pi} \mathcal{A}^{\sigma^n} \simeq \mathcal{A}$$

Algorithm 10 – Calcul du polynôme caractéristique sur une courbe de genre 2 par relèvement canonique 2-adique

Lorsque Π de $\tilde{\mathcal{A}}$ vers $\tilde{\mathcal{A}}^{\Sigma}$ est le rélévé du morphisme de Frobenius π de $\mathcal{A}$ vers $\mathcal{A}^{\sigma}$. Alors $\hat{\Pi}$ se décompose comme suit:



où ν est l'isogénie normalisée et λ est un isomorphisme entre $\tilde{\mathcal{A}}/\tilde{K}$ et $\tilde{\mathcal{A}}^{\hat{\Sigma}}$. Comme ν est normalizée son action est triviale alors l'action du "petit" Verchiebung $\hat{\Sigma}$ se réduit à celle de l'isomorphisme λ.

Calcul du Polynôme Caractéristique du Frobenius

On considère que la courbe hyperelliptique $\mathcal{C}$ est donnée sur $\mathbb{F}_q$ (avec $q = 2^n$) par une équation : $y^2 + h(x)y = f(x)$ où $h(x) = 1 + ax + bx^2$ et $f(x) = x^3(c + dx + x^2)$.

Initialisation

Soit $\mathcal{C}$ une courbe hyperelliptique de genre 2 sur un corps fini $\mathbb{F}_q$ (avec $q = 2^n$) donnée par son équation : $y^2 + h(x)y = f(x)$ où $h(x) = 1 + ax + bx^2$ et $f(x) = x^3(c + dx + x^2)$. À partir des relations 4.7 on peut calculer les invariants correspondants $J = (\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ modulo 2.

Relèvement des Invariants

Par l'action galoisienne de Σ, il est facile de voir que le cas ordinaire correspond au type $(1,1,1)$. L'algorithme 7 de Harley dans les sections 7.1 et 7.2 calcule $\tilde{J}$ en utilisant les polynômes modulaires en fonction de $\mathfrak{a}_1$, $\mathfrak{a}_2$ et $\mathfrak{a}_3$. Ce calcul peut se faire en $\tilde{O}(Nn)$ opérations binaires, où N est la précision p-adique.

Relèvement de la Courbe et du Verschiebung

On peut utiliser la section 7.1 et la section 7.3.2 pour relever la courbe C en calculant $(\tilde{a},\tilde{b},\tilde{c},\tilde{d})$ via une itération de Newton, cela coûte $\tilde{O}(N)$.
Comme Frobenius se décompose en $\pi\cdot\pi^2\cdots\pi^{n-1}$, le produit $\lambda_1\lambda_2$ de ses valeurs propres inversibles est donné par :

$$(\lambda_1\lambda_2)^{2k} = N_{\mathbb{Q}_q/\mathbb{Q}_p}\left(\frac{I_{2k}(\tilde{\mathcal{C}}^{\hat{\Sigma}})}{I_{2k}(\tilde{\mathcal{C}}^{\nu})}\right)$$

La courbe 2-isogène $\tilde{\mathcal{C}}^{\nu}$ (dont la variété Jacobienne est $\tilde{\mathcal{A}}/\tilde{K}$) est donnée par l'algorithme de Richelot (les sections 7.1 et 7.3 et le lemme 7.3.7). La décomposition quadratique lisse (G_1,G_2,G_3) correspondant à une équation de $\tilde{\mathcal{A}}/\tilde{K}$ peut être calculer en testant à faible précision les huits décompositions formées par: $G_1 = P_1P_3$, $G_2 = P_2P_4$ et P_5 telles que ($P_1 \equiv P_2 \mod 2$ et $P_3 \equiv P_4 \mod 2$).
D'autre part lorsque l'on suppose que $\mathcal{R}(G_1,G_2,G_3)$ définit le noyau du Verschiebung sur la courbe $\mathcal{C}_0$ dans le cas où

$$\Pi : \mathcal{C}^{\hat{\Sigma}} \longrightarrow \mathcal{C}_0 \simeq \mathcal{C}$$

$\mathcal{R}(G_1,G_2,G_3)$ est donné par la remarque 7.3.10 dans les sections 7.1 et 7.3. Alors on peut calculer l'image de $\mathcal{R}(G_1,G_2,G_3)$ sur $\mathcal{C}$ en utilisant les méthodes de conversion détaillées dans le chapitre 4 et la section 4.5.

Soit χ le polynôme caractéristique de $\mathcal{C}$, alors $\#\operatorname{Jac}C(\mathbb{F}_q) = \chi(1)$ et il satisfait les inégalités suivantes appelées *bornes de Hasse-Weil* :

$$\lceil(\sqrt{q}-1)^2\rceil \leq \chi(1) \leq \lfloor(\sqrt{q}+1)^2\rfloor.$$

On considère le polynôme P_{sym} de degré 2 sur $\mathbb{Z}$ dont les racines sont $\lambda_1\overline{\lambda}_1+\lambda_2\overline{\lambda}_2$ et $\lambda_1\lambda_2+\overline{\lambda}_1\overline{\lambda}_2$ appelé *polynôme symétrique de* $\mathcal{C}$. Ce polynôme détermine λ_1^2 et λ_2^2 par les relations suivantes démontrées dans [95]: $(\lambda_1\lambda_2)(\lambda_1\overline{\lambda}_2) = \lambda_1^2 q$ sachant que $\lambda_1\lambda_2$ est la racine de valuation n de $x^2-(\lambda_1\lambda_2+\overline{\lambda_1\lambda_2})x+q^2$.
Et si de plus χ est irréductible, λ_1 est une racine du polynôme $\chi(t)$ si $-\lambda_1$ est une racine de $\chi(-t)$. Ainsi λ_1 détermine χ.

Théorème 8.2.3. *Soit $\mathcal{C}$ une courbe hyperelliptique de genre 2 sur $\mathbb{F}_{2^n}$ dont les invariants $(\mathfrak{a}_1,\mathfrak{a}_2,\mathfrak{a}_3)$ vérifient les conditions de Kronecker, la méthode précédente calcule le polynôme caractéristique de $\mathcal{C}$ en $\tilde{O}(n^2)$ opérations à partir des polynômes modulaire en fonction des invariants $(\mathfrak{a}_1,\mathfrak{a}_2,\mathfrak{a}_3)$.*

Exemple 8.2.4. On considère que la courbe hyperelliptique $\mathcal{C}$ est donnée sur $\mathbb{F}_2[T]/m$ avec $m = T^{15} + T^5 + T^4 + T^2 + 1$, d'équation: $y^2 + h(x)y = f(x)$ où $h(x) = 1 + ax + bx^2$ et $f(x) = -x^3(c + dx + x^2)$ avec

$$\begin{aligned}
a &= T^{14} + T^{13} + T^{12} + T^{11} + T^9 + T^7 + T^5 + T^2 + T + 1,\\
b &= T^{14} + T^{13} + T^{12} + T^{10} + T^8 + T^7 + T^5 + T^4 + T^3,\\
c &= T^{14} + T^{13} + T^{10} + T^9 + T^4,\\
d &= T^{14} + T^{13} + T^{12} + T^{11} + T^9 + T^7 + T^5 + T^2 + T;
\end{aligned}$$

Cette équation est déduite de la *forme normale* de $\mathcal{C}$. Comme le cas ordinaire correspond au type $(1, 1, 1)$, en utilisant les relations du chapitre 4 et l'équation (4.7) on détermine le triplet d'invariants absolus J (en fonction des J_{2i}) correspondant au quadruplet (a, b, c, d).
Lorsque le tripet J vérifie les conditions de Kronecker, l'algorithme 7 de la section 7.2 (avec les polynômes modulaires en les invariants $\mathfrak{a}_1$, $\mathfrak{a}_2$ et $\mathfrak{a}_3$) calcule le relevé canonique sur $\mathbb{Z}_q$ du triplet J en $\tilde{O}(n^2)$ opérations.

$$\begin{aligned}
J =&[T^{13} + T^{11} + T^{10} + T^9 + T^8 + T^7 + T,\\
&T^{13} + T^{11} + T^{10} + T^9 + T^8 + T^7 + T,\\
&T^{14} + T^{13} + T^{11} + T^8 + T^3 + T^2 + T + 1];
\end{aligned}$$

$$\begin{aligned}
\tilde{J} =&[1347494003227200485 0T^{14} + 1675455958925491888 9T^{13} + 8152007378073597672T^{12}\\
&+ 1457277227702969699 5T^{11} + 9119476433797133587T^{10}\\
&+ 4240523924640418307T^9 + 6042690066170973759T^8 + 2446801185468953757T^7\\
&+ 1087907538620788510 2T^6 + 1654302220256170853 4T^5\\
&+ 1045739466450125619 0T^4 + 1008439897351563314T^3\\
&+ 1277064341038377540 8T^2 + 1244230292145767455 7T + 7907936886510960452,\\
&9391731769952962454T^{14} + 5272471816093258695T^{13} + 4694061109440793682T^{12}\\
&+ 1160444082877628509T^{11} + 1154044959289323749 7T^{10}\\
&+ 365295094271749 27T^9 + 4466186733562397311T^8 + 7829903155290047333T^7\\
&+ 1126719654227167343 4T^6 + 1725364635072082314 4T^5 + 6033296500969149134T^4\\
&+ 1747175715973801683 2T^3 + 1021665186136268416T^2 + 1274938999479729051T\\
&+ 17738635541368473904, \quad 1503125542744790693 9T^{14} + 1803878149847925939 5T^{13}\\
&+ 6632965468075882578T^{12} + 1095872262651110682 3T^{11} + 1497048209743982539 6T^{10}\\
&+ 1614075882084456448 8T^9 + 5066524261002336475T^8 + 1560812209382283130 2T^7\\
&+ 6346841391962884778T^6 + 2569207608253317670T^5 + 1756029517692926987 6T^4\\
&+ 772991990626853181T^3 + 1821164183470181092 5T^2 + 3154110753804246243T\\
&+ 10813538131737859899];
\end{aligned}$$

exemple 8.1 – Calcul du polynôme caractéristique sur une courbe de genre 2 par relèvement canonique 2-adique

$$\tilde{a} = a$$

$$\begin{aligned}\tilde{b} =& 55254945626000335T^{14} + 249530347970461244 1T^{13} + 757413555352357894 5T^{12} \\ &+ 176578220105449243 26T^{11} + 183038384555709264 87T^{10} + 869158959289702925 8T^{9} \\ &+ 158809767565081787 63T^{8} + 813754286633853312 3T^{7} + 175151524336232578 0T^{6} \\ &+ 151739178074680238 81T^{5} + 135359909534820066 67T^{4} + 132491914043064223 97T^{3} \\ &+ 152662947156309725 70T^{2} + 112463990606272372 30T + 2818864660668733758,\end{aligned}$$

$$\begin{aligned}\tilde{c} =& 116807728077425268 15T^{14} + 846219643943943 2885T^{13} + 408262115261685367 8T^{12} \\ &+ 344936560847742272 6T^{11} + 804483815412982645 3T^{10} + 127675015062228947 97T^{9} \\ &+ 121565127428705967 62T^{8} + 979805979708415142 4T^{7} + 890940578050211020 T^{6} \\ &+ 130639666450877477 02T^{5} + 166595930419144894 61T^{4} + 183508552613723366 48T^{3} \\ &+ 111248379778397055 8T^{2} + 175608237758594027 82T + 432993616092037345 4,\end{aligned}$$

$$\begin{aligned}\tilde{d} =& 742177288907997284 1T^{14} + 971316989620410821 3T^{13} + 673800514063671056 9T^{12} \\ &+ 175994730006150862 51T^{11} + 116986867146123978 12T^{10} + 767326170560642074 5T^{9} \\ &+ 146371760294285124 28T^{8} + 158682491659148410 89T^{7} + 112557544131821156 4T^{6} \\ &+ 177147986470507591 91T^{5} + 164199332261112449 0T^{4} + 913618315192094656 T^{3} \\ &+ 179538563815376766 97T^{2} + 460448019521240874 3T + 1202716416589165592.\end{aligned}$$

La phase de relèvement détermine la décomposition quadratique lisse de $\mathcal{C}$.

$$\begin{aligned}P1 =& (x + (-27499397306669T^{14} - 104108864093772T^{13} - 72190469780601T^{12} - \\ &1154343335976 85T^{11} - 1306827911756 86T^{10} + 714853447378 19T^{9} + 938104230808 62T^{8} - \\ &7917330676995 4T^{7} - 1274187818186 74T^{6} + 1682104959938 1T^{5} - 6558961424695 5T^{4} + \\ &7025157230866 3T^{3} - 8083568316366 8T^{2} - 1088255398341 1T - 140522863371668));\end{aligned}$$

$$\begin{aligned}P2 =& (x + (319313741718 63T^{14} - 865130992252 24T^{13} - 934576724260 45T^{12} + \\ &1021506717081 27T^{11} - 653055008985 74T^{10} + 111042151260 415T^{9} - 111164785066 26T^{8} - \\ &1145696693067 74T^{7} - 505170444149 22T^{6} + 353431025442 49T^{5} + 682845398698 9T^{4} + \\ &1784352633336 7T^{3} - 967928823712 72T^{2} + 134680560484 65T + 161612642911 60));\end{aligned}$$

$$\begin{aligned}P3 =& (x + (370584000799 07T^{14} - 908947982708 13T^{13} + 136899047104 414T^{12} + \\ &1239808218830 20T^{11} + 637869834059 63T^{10} - 555221757922 15T^{9} - 471674055976 72T^{8} - \\ &6623272830920 6T^{7} - 139226707950 72T^{6} + 1148988549624 28T^{5} + 2381598218863 3T^{4} + \\ &1984581831269 4T^{3} - 886129398470 82T^{2} - 935985228430 36T + 5485452129117 3));\end{aligned}$$

$$\begin{aligned}P4 =& (x + (958767490964 63T^{14} - 462827695475 53T^{13} + 960999014073 66T^{12} - \\ &1084408685227 16T^{11} - 1088848785097 69T^{10} - 2810526573899 5T^{9} - 1348199900784 16T^{8} + \\ &3649346718435 4T^{7} + 3461052013165 6T^{6} + 5866413448212 T^{5} - 4058826766749 1T^{4} - \\ &6851127822454 6T^{3} + 4462676572616 6T^{2} + 2692664208515 6T - \\ &1923535442414 3));\end{aligned}$$

$$P_5 = -(4x + (-549386473001740T^{14} + 185416724591973T^{13} - 268754553342494T^{12} - 9010553886254T^{11} - 160744857714336T^{10} - 395596840372744T^9 + 395006886970112T^8 - 233101947780155T^7 - 495392036247522T^6 + 436026043845296T^5 + 301035644984107T^4 - 156583924329429T^3 - 241580812300751T^2 + 255254170629438T + 354634709659596));$$

Nous avons $P_1 = P_2 \mod 2$ et $P_3 = P_4 \mod 2$ avec $\tilde{\mathcal{C}} : y^2 = P_1P_2P_3P_4P_5$.
À partir de la méthode des tests ou celle utilisant le calcul d'isomorphisme on détermine l'équation $\tilde{\mathcal{C}}^\nu$:

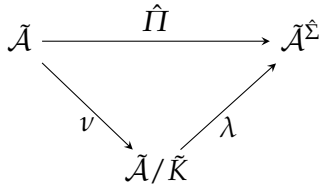
$$G1 = P_1P_3, \quad G_2 = P_4P_5, \quad G_3 = P_2 \quad et \quad nous \quad avons \quad \tilde{\mathcal{C}}^\nu : y^2 = \Pi\mathcal{R}(G_1, G_2, G_3).$$

Après le calcul du produit $\lambda_1\lambda_2$ des valeurs propres inversibles, le polynôme caractéristique réconstitué est :

$$\chi(X) = \left(X^2 + 2482103 \cdot 2^{16}X + 157 \cdot 2^{30}\right)\left(X^2 - 81333551261 \cdot 2X + 129494369717\right)$$

8.2.3 *En Caractéristique Impaire: Description de l'Algorithme*

Soient $\mathcal{C}$ une courbe de genre 2 définie sur $\mathbb{F}_q$, on note $\mathcal{A}$ et $\mathcal{K}$ la variété Jacobienne et sa surface de Kummer.
Soit Π de $\tilde{\mathcal{A}}$ vers $\tilde{\mathcal{A}}^\Sigma$ le relevé du morphisme de Frobenius π entre $\mathcal{A}$ et $\mathcal{A}^\sigma$. Alors son isogénie duale $\hat{\Pi}$ se décompose comme suit :



où ν est l'isogénie normalisée et λ est un isomorphisme entre $\tilde{\mathcal{A}}/\tilde{K}$ et $\tilde{\mathcal{A}}^{\hat{\Sigma}}$.
Lorsque ϑ_k est une forme modulaire de poids k; $\Omega \in \mathcal{H}_g$ et $\gamma \in \Gamma_g$. Alors

$$\vartheta_k(\gamma \cdot \Omega) = Det^k(C\Omega + D) \cdot \vartheta_k(\Omega) \quad avec \quad \gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right).$$

D'autre part si on note par f^* le tiré en arrière ("pull-back") sur l'espace tangent de l'isomorphisme défini par :

$$f : \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g) \longrightarrow \mathbb{C}^g/(\gamma \cdot \Omega\mathbb{Z}^g + \mathbb{Z}^g)$$

Alors $\vartheta_k(\gamma \cdot \Omega) = Det^k(M_f) \cdot \vartheta_k(\Omega)$, où M_f est la matrice de f^*.
Soient $\lambda_1, \cdots, \lambda_g$ les valeurs propres inversibles du morphisme de Frobenius Π de $\tilde{\mathcal{A}}$ sur $\mathbb{Z}_q$. Alors le produit $\lambda_1 \cdots \lambda_g$ est un élément de l'anneau $\mathbb{Z}_q$ et :

$$(\lambda_1 \cdots \lambda_g)^k = N_{\mathbb{Q}_q/\mathbb{Q}_p}\left(\frac{\vartheta_k(\Omega^{\hat{\Sigma}})}{\vartheta_k(\Omega)}\right) \tag{8.3}$$

Pour ce qui suit nous décrivons une extension en dimension 2 de la méthode de Satoh (le chapitre 2 et la section 2.6.1). Pour simplifier les calculs nous travaillons directement en coordonnées thêta sur la variété Kummer $\mathcal{K}$ associée à la courbe hyperelliptique $\mathcal{C}$ de genre 2 définie sur $\mathbb{F}_q$ avec $p > 2$. On pourra toutefois utiliser les formules de conversion entre les coordonnées Mumford et les coordonnées Thêta à l'appendice a.1.

Algorithm 11 – Calcul du polynôme caractéristique sur une courbe de genre 2 par relèvement canonique: cas impair

Initialisation et Calculs sur $\mathbb{F}_q$

On suppose que J est le vecteur des invariants thêta de $\mathcal{K}$ vérifiant les conditions de Kronecker la section 7.1, la section 7.1.1 et la proposition 7.1.1 correspondant aux polynômes modulaire $\Phi_{1,p}$, $\Psi_{2,p}$ et $\Psi_{3,p}$ par exemple.
Le calcul des points de p-torsion sur $\mathbb{F}_q$ peut se faire de deux manières. À partir des coordonnées Mumford suivi d'une conversion vers les coordonnées thêta, cela peut se faire par la méthode de composition modulaire [38].

Autrement on peut directement résoudre le système polynômial affine $(F) : [k+1].P = -[k]P$ (avec $p = 2k+1$) définissant la p-torsion sur la variété Kummer $\mathcal{K}$ les sections 7.1 et 7.2 et la proposition 7.2.2, en utilisant les formules de pseudo-addition de l'appendice a et l'appendice a.2.

Phase de Relèvement

Comme J vérifie les conditions Kronecker dans la section 7.1, la section 7.1.1 et la proposition 7.1.1 correspondant au vecteur Φ des polynômes modulaires, l'algorithme 7, les sections 7.1 et 7.2 détermine $\tilde{J}$. Alors on peut réconstituer l'équation de la surface Kummer de $\tilde{\mathcal{A}}^{\Sigma}$ et $\tilde{\mathcal{A}}$ et aussi le système $\tilde{F}$ en fonction des thêta invariants relevés l'appendice a et l'appendice a.2 à une précision définie.
En utilisant le théorème 7.2.4 et la section 7.1 on détermine une approximation du relevé de chaque $P \in \mathcal{K}[p]$. Lors de la première étape du relèvement on peut faire un petit calcul de base de Gröbner sur : :

$$F(P) + p.DF(P).R + p^2/2.{}^tR.HF(P).R = 0 \mod p^3$$

pour avoir P à la bonne précision. Ce système a seulement trois polynômes de degré 2 chacun.

Calcul du Produit $\lambda_1\lambda_2$ *des Valeurs Propres*

D'une part nous avons le résultat:

$$(\lambda_1\lambda_2)^2 = N_{\mathbb{Q}_q/\mathbb{Q}_p}\left(\frac{\theta_k(\mathcal{K}^{\hat{\Sigma}})}{\theta_k(\mathcal{K}/\ker\Sigma)}\right)$$

D'autre part en utilisant l'algorithme 9 et l'exemple 8.2.2 de la section 8.2.1 et le chapitre 8 on détermine $\theta_k(\mathcal{K}/\ker\Sigma)$ par suite le produit $\lambda_1\lambda_2$.

Reconstitution du polynôme Caractéristique

On pourra utiliser l'algorithme LLL pour séparer les facteurs du produit $\lambda_1\lambda_2$. Cette méthode est plus générale en caractéristique et en genre. Elle consiste à réduire avec un algorithme LLL un réseau dont une base est définie par les racines $\lambda_i + q^g/\lambda_i$ et les coéfficients

du polynôme P_{sym} sont les composantes d'un vecteur de norme minimale de ce réseau [13]. Cependant J.F Mestre dans [75] propose une méthode pour déterminer directement (en genre 2) $\#\operatorname{Jac} C(\mathbb{F}_q)$ et $\#C(\mathbb{F}_q)$ à partir de la connaissance $u = \lambda_1\lambda_2$. En effet $(\lambda_1 + \bar{\lambda}_1)$ et $(\lambda_2 + \bar{\lambda}_2)$ sont les racines du polynôme quadratique: $X^2 - bX + a$ où: la somme des racines $b \equiv u \mod q$ et leur produit a satisfait la relation $a^2 \equiv (\lambda + 2)u \mod q$ avec $\lambda = (b - u)/q$, $|b| \leq 4q$ et $|a| \leq 4\sqrt{q}$. Et

$$\begin{aligned} \#\operatorname{Jac} C(\mathbb{F}_q) &= \prod_{i=1}^{2}(1 - \lambda_i)(1 - \bar{\lambda}_i) \\ \#\mathcal{C}(\mathbb{F}_q) &= q + 1 - (\lambda_1 + \bar{\lambda}_1) - (\lambda_2 + \bar{\lambda}_2). \end{aligned}$$

8.2.4 *Analyses de Complexités*

Lorsque nous sommes à une précision d'ordre n, l'evaluation d'un polynôme modulaire en les invariants peut se faire en $O(p^4.\log(p).n^2)$ opérations avec les polynômes modulaires de Hilbert et en $O(p^{15}.\log(p).n^2)$ opérations en utilisant ceux de Siegel. Alors nous supposons que l'on travaille en petite caractéristique.

Théorème 8.2.5. *Soit $\mathcal{C}$ une courbe hyperelliptique de genre 2 sur $\mathbb{F}_q$ de caractéristique $p > 2$ dont les invariants satisfont les conditions de Kronecker de la section 6.2 et le chapitre 6 (selon le type d'invariants). Par la méthode précédemment détaillée on peut calculer $\#JacC(\mathbb{F}_q)$ en une complexité $\tilde{O}(n^2)$ opérations binaires.*

En effet on arrive à ce résultat en considérant les complexités des étapes de calculs précédents .

Calcul de la p-torsion sur $\mathbb{F}_q$

Par la méthode de composition modulaire proposée par P. Gaudry et É. Schost [38] en coordonnées Mumford le calcul de la p-torsion peut se faire avec une complexité en temps d'au plus $O(pM(p^4) + p^{\omega+3})$ où ω est tel que la multiplication de deux matrices de tailles n se fait en $O(n^\omega)$ opérations. Et la complexité en espace est $O(p^5)$ éléments de $\mathbb{F}_p$.
Par la méthode de composition par la loi de groupe, le calcul de la p-torsion coûte $O(M(p^4)\log(p))$ en temps sur $\mathbb{F}_p$, avec utilisation en espace mémoire $O(p^4)$ éléments de $\mathbb{F}_p$.

Phase de relèvement

Lorsque nous utilisons les polynômes modulaires de Hilbert les calculs les plus coûteux résident dans l'évaluation des polynômes en les invariants qui coûte $O(p^4n^2)$ opérations car l'algorithme de Artin-Schreier ne coûterait que $O(n^2 \log p)$. Ainsi l'algorithme 8 de la section 7.4.2 et la section 7.4 calcule le relevé des invariants en $O(p^4.n^2)$.
Cependant dans le cas des polynômes modulaires de Siegel le correspondant algorithme 7 de les sections 7.1 et 7.2 coûte $O(p^{15}n^2)$.
En ce qui concerne le relèvement de la p-torsion, le coût total est $O(\log n)$ fois le coût de la division entre deux éléments de $\mathbb{Z}_q$ à une précision $\Theta(n)$. Le calcul de base de Gröebner pour la bonne précision de départ ne concerne que trois polynômes de degré 2 à trois variables à la précision p^2, qui est négligeable.

Calcul du Produit $\lambda_1\lambda_2$ et $\#JacC(\mathbb{F}_q)$

Le calcul des thêta constantes de la surface abélienne $\mathcal{B} = \mathcal{A}/\mathcal{K}$ à partir de l'algorithme 9 et de la p-torsion relévé se fait en $O(p^r)$ opérations (dans notre cas $r = 2$). En utilisant la méthode des résultants (le chapitre 1 et la section 1.3), la norme

$$N_{\mathbb{Q}_q/\mathbb{Q}_p}\left(\frac{\theta_k(\mathcal{K}^{\hat{\Sigma}})}{\theta_k(\mathcal{K}/\ker\Sigma)}\right)$$

se calcule en $O(n^\mu logn)$ où $\mu = 1+\epsilon$ (pour n grand) et $\mu = log_2(3)$ en utilisant l'algorithme de multiplication FFT respectivement l'algorithme de Karatsuba [17] . Alors la méthode de Mestre calcule $\#JacC(\mathbb{F}_q)$ à partir du produit $\lambda_1\lambda_2$ en un temps de $O(n^\mu \log p)$, soit le coût du calcul d'un carré sur $\mathbb{F}_q$. Et la réconstitution du polynôme P_{sym} à partir des racines $\lambda_1\overline{\lambda}_1 + \lambda_2\overline{\lambda}_2$ et $\lambda_1\lambda_2 + \overline{\lambda}_1\overline{\lambda}_2$ se fait en $O(n^{\mu+1})$ soit le coût de la multiplication de deux entiers.

Exemple 8.2.6. On considère les mêmes données de l'exemple 7.2.6 et les sections 7.1 et 7.2.

$$\mathcal{C} : y^2 = x^5 + (2T^8 + T^2 + T)x^4 + (T^8 + T^7 + T^6 + T^5 + T^3 + 2T + 2)x^3 +$$

$$(T^9 + 2T^8 + T^6 + T^5 + T^4 + 2T^3 + 2)x^2 + (2T^9 + T^8 + 2T^7 + T^6 + T^5 + 2T^4 + 2T^2 + 1)x$$

est une courbe de genre 2 sur $\mathbb{F}_3[T]/m$ avec $m = T^{10} + 2T^6 + 2T^5 + 2T^4 + T + 2$ dont les invariants thêta de niveau 2 sont:

$$a = 2T^9 + 2T^6 + 2T^5 + 2T^4 + T^3 + T^2 + T, \quad b = 2T^9 + T^8 + 2T^7 + T^6 + T^5 + 2T^4 + 2T^2,$$

$$c = 2T^9 + 2T^6 + T^4 + 2T^3 + 2T + 2$$

Ainsi après la phase des relèvements on obtient à une précision 3^{20}:

$$\begin{aligned} M =& T^{10} + 2549079126T^9 + 1424896413T^8 + 387776124T^7 + 1501830083T^6 + 2399043737T^5 \\ &+ 1835343671T^4 + 3327249759T^3 + 1052748765T^2 + 1815623119T + 3486784400 \end{aligned}$$

$$\begin{aligned} \tilde{a} =& 1632442511T^9 + 3184765518T^8 + 3476194941T^7 + 3108882704T^6 + 2423383142T^5 \\ &+ 1764926933T^4 + 1098986671T^3 + 2957646787T^2 + 1669307941T + 2686192050, \end{aligned}$$

$$\begin{aligned} \tilde{b} =& 1855464665T^9 + 458606629T^8 + 1644296153T^7 + 2202845860T^6 + 2959176835T^5 \\ &+ 2200438487T^4 + 1716586968T^3 + 1038290165T^2 + 133634418T + 2980506843, \end{aligned}$$

$$\begin{aligned} \tilde{c} =& 3067405283T^9 + 2017143027T^8 + 1539671400T^7 + 2805617504T^6 + 754015086T^5 \\ &+ 1269571459T^4 + 2964123128T^3 + 609859068T^2 + 3096552740T + 605100932, \end{aligned}$$

exemple 8.2 – Calcul du polynôme caractéristique sur une courbe de genre 2 par relèvement canonique de la Kummer

Et le rélévé des 4 points de 3-torsion comme indiquer dans l'exemple 7.2.6 et les sections 7.1 et 7.2. À partir de l'algorithme 9 dans http://avisogenies.gforge.inria.fr on obtient les invariants thêta de la variété abélienne p-isogène.

$$\begin{aligned}
&[1665426634T^9 + 2291786881T^8 + 319244275T^7 + 908965652T^6 + 373529527T^5 \\
&+ 3459234302T^4 + 637296308T^3 + 1615339023T^2 + 71993550T + 2412291147, \\
&1375693855T^9 + 1781159471T^8 + 2975497017T^7 + 2625983267T^6 + 3456313825T^5 \\
&+ 258917388T^4 + 169437654T^3 + 2862222480T^2 + 3191428894T + 828753903, \\
&933603536T^9 + 1711410927T^8 + 130528953T^7 + 3466168598T^6 + 1834982298T^5 \\
&+ 1734316195T^4 + 2194380317T^3 + 1333319670T^2 + 2564003393T + 1123362129, \\
&899185444T^9 + 2638232402T^8 + 1147310541T^7 + 2100019531T^6 + 2732363852T^5 \\
&+ 2339070819T^4 + 1863357600T^3 + 2399257487T^2 + 1456953946T + 2821097391]
\end{aligned}$$

$$u = \lambda_1\lambda_2 = 2255204904638089156$$

Alors le polynôme caractéristique de $\mathcal{C}$ à une précision 3^{20} est:

$$\chi(X) = X^4 - 404X^3 + 158902X^2 - 404 \cdot 3^{10}X$$

8.2.5 *Méthode de Relèvement par Évaluation du Verschiebung*

Cette méthode est une extension en dimension 2 de la méthode du chapitre 2 et la section 2.6.3. Elle réduit considérablement la dépendance en p dans les calculs de relevé canonique utilisant les polynômes de Siegel dont les tailles sont en $O(p^{15}n^2)$. Cependant lorsque l'on utilise les polynômes de Hilbert nous avons vu plus haut (la section 8.2.4), que le coût de l'évaluation de ces polynômes est dominé par le calcul de la p-torsion sur $\mathbb{F}_q$ qui se fait en temps $O(M(p^4) + p^{\omega+3})$ et en espace de $O(p^4)$ à partir de la méthode de composition par la loi de groupe [38] en coordonnées Mumford (où $O(n^\omega)$ est le coût de la multiplication de deux matrices de tailles n). En utilisant les algorithmes Cosset-Robert [19] ou Couveignes-Ezomé [21] pour le calcul du Verschiebung à la précision N on excède pas ce coût d'évaluation de la p-torsion. D'autre part en utilisant la méthode de relèvement de la p-torsion à une précision N par évaluation directe (le chapitre 1 et la section 1.2) combinée avec les formules d'addition (de la partie iv) on ne fait pas plus pire. Par la suite nous avons le résultat suivant:

Théorème 8.2.7. *Par la méthode d'évaluation du Verschiebung on calcule le polynôme caractéristique d'une courbe ordinaire de genre* 2 *après* $O(M(p^4)\log(p)\log(n).n^2)$ *opérations binaires.*

8.3 CONCLUSION

En ce qui concerne la dimension 1, à partir d'une interprétation équivalente du Théorème de Lubin-Serre-Tate (le chapitre 2, la section 2.5.1 et le théorème 2.6.2) nous avons développé des méthodes de relèvement canonique plus pratiques que les méthodes connues auparavant. Les plus performantes de nos méthodes de calcul ont un coût en temps $\tilde{O}(n.N.p)$. Ces performances sont aussi les fruits de méthodes de Newton dévéloppées dans le chapitre 1 et la section 1.2 ; lesquelles méthodes s'appliquent directement dans le calcul du relèvement de la p-torsion d'une variété abélienne en général.

Dans le cas de la dimension 2, nous avons utilisé des triplets d'invariants absolus de courbes de genre 2 sur $\mathbb{Z}_q$ ayant bonne réduction en toute caractéristique et en particulier en caractéristique 2 sur les différents types $(1,1,1)$, $(3,1)$ et (5). Ce qui est utile pour définir une équation modulaire sur l'espace de module des courbes ordinaires de genre 2 ayant une bonne réduction en toute caractéristique .
D'autre part nous avons proposé une démonstration aux *Conditions de Kronecker* sur $\mathfrak{A}_{g,\Gamma_0(p)}$, le champ algébrique des variétés abéliennes polarisées de dimension g muni d'une structure de niveau p. Une interprétation algorithmique de ces propriétés à travers les polynômes modulaires permet de construire des algorithmes de calcul du relevé canonique d'une les variétés ordinaires. Ainsi pour $g = 2$, en utilisant des invariants « bien » adaptés, nous avons proposé une extension de l'algorithme de Harley sur les espaces de module de Siegel et de Hilbert avec une complexité au plus en $\tilde{O}(n^2)$ pour $n \sim \log q$. Cependant lorsque l'on travaille sur l'espace de Siegel, la complexité en p de ces algorithmes de relèvement est entièrement couverte par l'évaluation des polynômes modulaires utilisés.
Néanmoins les polynômes de Hilbert sont encore plus pratiques, la complexité de leurs évaluations permettent de faire des tests jusqu'à $p < 100$.
Les p-torsions des variétés abéliennes ordinaires sont étales en partie. En utilisant la forme de leurs matrices sur l'espace tangent nous avons donné un algorithme permettant de les relever sur $\mathbb{Z}_q$. Une variante de cet algorithme permet aussi de relever l'equation d'une courbe hyperelliptique à partir de ses invariants.

Cette étude algorithmique basée sur le *Théorème de Serre-Tate* permet de déterminer le polynôme caractéristique et de calculer les rélévés des formes modulaires vectorielles d'une courbe hyperelliptique .
Ainsi pour les courbes de genre 2 sur $\mathbb{F}_{p^n}$ nous avons proposé des algorithmes de calcul de polynômes caractéristiques en utilisant des calculs d'isogénies à partir du relevé de la p-torsion. Cette approche fût bien-avant introduite en dimension 1 par Satoh [99]. Elle admet une complexité quasi-quadratique en n, "bien-meilleure" comparée aux autres méthodes de calcul de polynôme caractéristique d'une courbe ordinaire de genre 2.
Pour améliorer la complexité en p, notre première alternative a été l'utlisation de polynômes de Hilbert avec lesquels le polynôme caractéristique est déterminé après $O(M(p^4)\log(p)\log(n).n^2)$ opérations. Et le coût $O(M(p^4)\log(p))$ vient de l'évaluation de la p-torsion sur $\mathbb{F}_q$ pour le calcul d'isogénie. La deuxième alternative repose sur le relèvement par évaluation directe du

Verschiebung dont l'étape la plus coûteuse reste le calcul de la p-torsion en $O(M(p^4)\log(p))$. Alors en perspective nous pouvons aborder ce futur projet de réduction de complexité sous plusieurs angles.

8.4 PERSPECTIVES

Pour la suite nous projettons de suivre les idées suivantes pour améliorer par exemple la complexité en p dans le calcul du polynôme caractéristique.

AMÉLIORATION ET EXTENSION DE NOS MÉTHODES DE RELÈVEMENT CANONIQUE AUX VARIÉTÉS ORDINAIRES DE DIMENSION $g > 1$

Comme dans le cas de la dimension 1, pour une bonne réduction de la complexité en p dans le relèvement canonique nous projetons d'utiliser l'approche du chapitre 2, la section 2.6.3 et le théorème 2.6.10 appelée « Calcul du Relevé Canonique par Évaluation du Verschiebung » combinée à des méthodes plus rapides de calcul de la p-torsion sur $\mathbb{F}_q$. Cette méthode présente beaucoup d'avantages en considérant les raisons suivantes:

1. La taille des polynômes modulaires en Dimension superieure à 1 explose très rapidement en fonction de p, g et n.
2. Par contre d'un autre côté on dispose d'algorithmes de Calcul d'Isogénies très pratiques.

Comme dans nos études dans le chapitre 2 et la section 2.6.3 nous espérons atteindre des perfermences considérables.

MÉTHODE DE DIFFÉRENTIATION D'ELKIES POUR L'ÉVALUATION DU VERSCHIEBUNG

Cette approche même si elle utilise le relèvement canonique de la variété abélienne, se dispense du relèvement de la p-torsion. En effet à partir des versions plus améliorées de la méthode de Stark, on peut évaluer directement l'action du petit Verschiebung sur les relevés canoniques des variétés conjuguées $\mathrm{Jac}\,\tilde{\mathcal{C}}$ et $\mathrm{Jac}\,\tilde{\mathcal{C}}^{\sigma}$.
Cette approche d'évaluation de l'action d'une isogénies connaît tout récemment une généralisation à travers les travaux de Damien Robert et autres [97, 98]. Comme l'évaluation de la p-torsion coûte au moins $O(M(p^4)\log(p))$ opérations en $\mathbb{F}_p$, ainsi en évitant le relèvement de la p-torsion et en évaluant le Verschiebung par cette approche permettrait d'obtenir une meilleure complexité en temps et espace mémoire.

CALCUL DE RELEVÉ D'UNE VARIÉTÉ NON ORDINAIRE

Historiquement les idées de calculs de relevés étaient motivées par la détermination du polynôme caractéristique d'une variété abélienne ordinaire sur $\mathbb{F}_q$ pour des applications cryptograpiques en ECC et HECC. Actuellement les intérêts post-quantiques en ECC et HECC portés sur les variétés non-ordinaires constituent une grande motivation pour le calcul de relevés des variétés non ordinaires. Ces possibles relevés n'étant pas canoniques, leur étude devient plus intéressant. Une approche de P. Norman et F. Oort [90] (suivant une idée de Mumford) détermine les relevés de variétés non ordinaires à partir du relèvement canonique de variétés ordinaires.

BIBLIOGRAPHIE

[1] L. Adleman et J. M.-D. Huang. « Counting points on curves and abelian varieties over finite fields ». In : *Symbolic Comput* 32 (2001), p. 171-189 (cf. p. 146).

[2] D. Bernstein, L. DeFeo, A. Leroux et B. Smith. « Faster computation of isogenies of large prime degree ». In : (2020). URL : arXiv:2003.10118 (cf. p. 45, 47).

[3] C. Birkenhake et H. Lange. *Complex abelian varieties*. Second. T. 302. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Berlin : Springer-Verlag, 2004, p. xii+635. ISBN : 3-540-20488-1 (cf. p. 3, 4, 51-54, 56, 57, 59-61, 65, 99).

[4] C. Birkenhake et H. Wilhelm. « Humbert surfaces and the Kummer plane ». In : *Transactions of the American Mathematical society* 355(5) :1819–1841 (2003) (cf. p. 73).

[5] A. Bostan, F. Morain, B. Salvy et É. Schost. « Fast algorithms for computing isogenies between elliptic curves ». In : *Math. Comp.<inria-00091441>* 73.263 (2008), p. 1755-1778 (cf. p. 34, 146).

[6] R. Bröker et K. Lauter. « Modular polynomials for genus 2 ». In : *LMS Journal of Computation and Mathematics*, 1.12 (2009), p. 326-339 (cf. p. 102).

[7] R. Bröker et K. Lauter. « Modular polynomials for genus 2 ». In : *LMS J. Comput. Math.* 12 (2009), p. 326-339. ISSN : 1461-1570. arXiv : 0804.1565 (cf. p. 5).

[8] R. Bröker et A.V. Sutherland. « An explicit height bound for the classical modular polynomial ». In : *The Ramanujan Journal* (2009), p. 1-21 (cf. p. 42).

[9] D.G. Cantor. « Computing in the Jacobian of a hyperelliptic curve ». In : *Mathematics of Computation* 48.177 (1987), p. 95-101 (cf. p. 3, 169, 170).

[10] G. Cardona et J. Quer. « Field of moduli and field of definition for curves of genus 2 ». In : *Computational aspects of algebraic curves*. World Scientific, 2005, p. 71-83 (cf. p. 84, 85).

[11] R. Carls. « Generalized AGM sequences and approximation of canonical lifts ». Thèse de doct. Avr. 2003. URL : http://www.math.leidenuniv.nl/carls (cf. p. 8).

[12] R. Carls, D. Kohel et D. Lubicz. « Higher-dimensional 3-adic CM construction ». In : *J. Algebra* 319.3 (2008), p. 971-1006. ISSN : 0021-8693. DOI : 10.1016/j.jalgebra.2007.11.016 (cf. p. 10).

[13] R. Carls et D. Lubicz. « A p-adic quasi-quadratic time and quadratic space point counting algorithm ». In : *International Mathematics Research Notices* (2008) (cf. p. 7, 8, 147, 156).

[14] B. Casselman. « Newton polygons ». In : () (cf. p. 38).

[15] C.L. Chai et P. Norman. « Bad Reduction of the Siegel Moduli Scheme of Genus Two with $\Gamma_0(p)$-Level Structure ». In : *American Journal of Mathematics* 112.06 (déc. 1990), p. 1003-1071. URL : http://www.jstor.org/stable/2374734 (cf. p. 6, 11, 116-119).

[16] A. Clebsh. « Theorie der Binärien Algebraischen Formen ». In : *Verlag von B. G.* (1872) (cf. p. 4, 79, 80).

[17] Henri COHEN, Gerhard FREY, Roberto AVANZI, Christophe DOCHE, Tanja LANGE, Kim NGUYEN et Frederik VERCAUTEREN, éd. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006, p. xxxiv+808. ISBN : 978-1-58488-518-4 ; 1-58488-518-1 (cf. p. 16, 157).

[18] R. COSSET. « Application des fonctions thêta à la cryptographie sur courbes hyperelliptiques ». Thèse de doct. 2011 (cf. p. 62, 64, 177, 178).

[19] R. COSSET et D. ROBERT. « Computing (ℓ, ℓ)-Isogenies in Polynomial Time on Jacobian of Genus 2 Curves ». In : *American Mathematical Society* (2010), S 0025-5718(XX)0000-0 (cf. p. 148, 149, 158, 176, 177).

[20] C. COSTELLO et B. SMITH. « The supersingular isogeny problem in genus 2 and beyond ». In : *Springer, Cham* 12100 (2020), p. 151-168. URL : https://doi.org/10.1007/978-3-030-44223-1_9 (cf. p. 2).

[21] J-M. COUVEIGNES et T. EZOME. « Computing functions on Jacobians and their quotients ». In : (2014). arXiv : 1409.0481 (cf. p. 158).

[22] L. DE FEO, D. JAO et J. PLÛT. « Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies ». In : *J. Mathematical Cryptology* 8.3 (2014), p. 209-247 (cf. p. 2).

[23] P. DELIGNE. « La conjecture de Weil. I. » In : *Math* 43 (1974), p. 273-307 (cf. p. 145).

[24] J. DENEF et F. VERCAUTEREN. « An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2 ». In : *J. of Cryptology* 19 (2006), p. 1-25 (cf. p. 7).

[25] J. DENEF et F. VERCAUTEREN. « Counting points on C ab curves using Monsky-Washnitzer cohomology ». In : *Finite Fields and Their Applications* 12 (2006), p. 78-102 (cf. p. 7, 147).

[26] Max DEURING. *Die Klassenkörper der komplexen Multiplikation*. T. 2. Teubner Stuttgart, 1958 (cf. p. 82).

[27] G. DOSPINESCU. « Lifting abelian scheme : theorem of Serre-Tate and Grothendieck ». In : (). URL : http://perso.ens-lyon.fr/gabriel.dospinescu/Serre-Tate.pdf (cf. p. 116).

[28] R. DUPONT. « Moyenne arithmetico-geometrique, suites de Borchardt et applications ». Thèse de doct. 2006 (cf. p. 5, 9, 69-72, 92, 98-101, 103, 105).

[29] B. DWORK. « On the rationlity of the zeta function of an algebraic variety ». In : *American Journal of Math* 82 (1960), p. 631-648 (cf. p. 145).

[30] Flynn E.V. et Yan Bo TI. « Genus Two Isogeny Cryptography ». In : *Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019, Chongqing, China, May 8-10* 11505 of Lecture Notes in Computer Science (2019), p. 286-306 (cf. p. 2).

[31] B. EDIXHOVEN. « On the computation of the coefficients of a modular form ». In : *In Algorithmic Number Theory Symposium VII* (2006), number 4076 in LNCS, pages 30–39 (cf. p. 146).

[32] N.D. ELKIES. « Elliptic and modular curves over finite fields and related computational issues ». In : *American Mathematical Society, International Press* 7 of AMS/IP Studies in Advanced Mathematics (1998). Sous la dir. de Computational Perspectives on Number Theory : Proceedings of a Conference in Honor of A. O. L. ATKIN, p. 21-76 (cf. p. 33, 41, 146).

[33] C. GABRIEL, E. NART et J. PUJOLÀS. « Curves of genus two over fields of even characteristic ». In : () (cf. p. 4, 82, 85, 86).

[34] P. GAUDRY. « Algorithmique des courbes hyperelliptiques et applications à la cryptologie ». Thèse de doct. École Polytechnique, déc. 2000 (cf. p. 93, 169, 170).

[35] P. GAUDRY. « Algorithmes de comptage de points d'une courbe définie sur un corps fini ». 2004. URL : http://www.loria.fr/~gaudry/publis/pano.pdf (cf. p. 6, 11, 17, 41, 46, 140, 146).

[36] P. GAUDRY. « Fast genus 2 arithmetic based on Theta functions ». In : *Journal of Mathematical Cryptology* 1.3 (2007), p. 243-265 (cf. p. 171, 178).

[37] P. GAUDRY. « Algorithmique des courbes algébriques pour la cryptologie ». HDR. Oct. 2008. URL : http://www.loria.fr/~gaudry/publis/hdr.pdf (cf. p. 2).

[38] P. GAUDRY et É. SCHOST. « Genus 2 point counting over prime fields ». In : *Journal of Symbolic Computation* (2012), 47 (4), pp.368-400. (Cf. p. 146, 155, 156, 158).

[39] Pierrick GAUDRY, Thomas HOUTMANN, David KOHEL, Christophe RITZENTHALER et Annegret WENG. « The 2-adic CM method for genus 2 curves with application to cryptography ». In : *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2006, p. 114-129 (cf. p. 10).

[40] L. GÓMEZ TOMÁS. « Algebraic stacks ». In : (déc. 1999). URL : arXiv:math/9911199 (cf. p. 116, 117).

[41] E.Z. GOREN et K.E. LAUTER. « Genus 2 curves with complex multiplication ». In : *International Mathematics Research Notices* 2012.5 (2012), p. 1068-1142 (cf. p. 9, 83).

[42] E. GOTTSCHLING. « Explizite Bestimmung der Randflächen des Fundamentalbereiches der Modulgruppe zweiten Grades ». In : *Annals of Mathematics* 138 (1959), p. 103-124 (cf. p. 67).

[43] D. GRUENEWALD. « Explicit algorithms for Humbert surfaces ». Thèse de doct. University of Sydney, 2008 (cf. p. 105).

[44] K.B. GUNDLACH. « Die Bestimmung der Funktionen zur Hilbertschen Modulgruppe des Zahlkörpers $\mathbb{Q}\sqrt{5}$ ». In : *Math. Ann.* 152 (1963), p. 226-256 (cf. p. 73, 76).

[45] R. HARLEY. « Asymptotically optimal p-adic point-counting, e-mail to NMBRTHRY list, December ». In : () (cf. p. 24).

[46] D. HARVEY. « Kedlaya's algorithm in larger characteristic ». In : *International Mathematics Research Notices* (2007), 29 pages (cf. p. 49, 147).

[47] F. HIRZEBRUCH et D. ZAGIER. « Classification of Hilbert modular surfaces ». In : *Cambridge University Press*. W. L. Jr Baily et T. Shioda 116 (1977), p. 43-78 (cf. p. 73, 75).

[48] G. HUMBERT. « Sur les fonctions abéliennes singulières i. » In : *Journal de Mathématiques Pures et Appliquées* V :233–350 (1899) (cf. p. 73).

[49] G. HUMBERT. « Sur les fonctions abéliennes singulières ii. » In : *Journal de Mathématiques Pures et Appliquées* VI :279–386 (1900) (cf. p. 73).

[50] G. HUMBERT. « Sur les fonctions abéliennes singulières iii. » In : *Journal de Mathématiques Pures et Appliquées* VII :97–124 (1901) (cf. p. 73).

[51] J-I. IGUSA. « Arithmetic Variety of Moduli for Genus Two ». In : *Annals of Mathematics* Vol.72, No.3 (1960), p. 612-649 (cf. p. 4, 9, 80-83, 86, 87, 94, 106, 115, 121, 133, 134).

[52] J.I. IGUSA. « On Siegel modular forms of genus 2 ». In : *Johns Hopkins University Press* (1962), 84(1) (cf. p. 4, 71, 72).

[53] J.I IGUSA. *Theta functions*. Die Grundlehren der mathematischen Wissenschaften, Band 194. New York : Springer-Verlag, 1972, p. x+232 (cf. p. 71).

[54] D. JAO et L. DE FEO. « Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies ». In : *PQCrypto'11 Proceedings* (2011), p. 19-34 (cf. p. 2).

[55] N. KATZ. « Serre-Tate Local Moduli ». In : (). URL : https://pdfs.semanticscholar.org/0c5c/37ff064e634eec9d239c4d1a3da3052d3aec.pdf (cf. p. 6, 11, 115, 116, 118).

[56] K.S. KEDLAYA. « Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology ». In : *Preprint* (2001). arXiv : math/0105031 (cf. p. 7).

[57] K.S. KEDLAYA. « Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology ». In : *J. Ramanujan Math. Soc.* 4.16 (2001), p. 323-338 (cf. p. 147).

[58] J. KIEFFER. « Evaluating modular polynomials in genus 2 ». In : (oct. 2020). URL : arXiv:2010.1009v1[math.NT]20Oct2020 (cf. p. 101).

[59] Jean KIEFFER. « Degree and height estimates for modular equations on PEL Shimura varieties ». In : (2020). arXiv : 2001.04138 [math.AG] (cf. p. 104, 105, 131).

[60] Hae Young KIM, Jung Youl PARK, Jung Hee CHEON, Je Hong PARK, Jae Heon KIM et Sang Geun HAHN. « Fast Elliptic Curve Point Counting Using Gaussian Normal Basis ». In : *Algorithmic Number Theory, 5th International Symposium* 116 (July 2002). Sous la dir. de Claus FIEKER et David R. KOHEL, p. 292-307 (cf. p. 24, 25).

[61] H. KLINGEN. « Introductory lectures on Siegel modular forms ». In : *Cambridge studies in advanced mathematics* 20 (1990) (cf. p. 66, 67, 69).

[62] N. KOBLITZ. *p-adic Numbers, p-adic Analysis and Zeta-Functions*. T. Second Edition. Graduate Texts in Mathematics. Springer-Verlag, 1984. ISBN : 0-387-96017-1 (cf. p. 15, 16).

[63] N. KOBLITZ. « Elliptic curves cryptosystems ». In : *Mathematics of Computation* 177.48 (1987). Sous la dir. de JSTOR 2007884, p. 203-209. DOI : 10.2307/2007884 (cf. p. 2).

[64] N. KOBLITZ. « Hyperelliptic cryptosystems ». In : *Journal of cryptology* 1.3 (1989), p. 139-150 (cf. p. 3, 170).

[65] D. KOHEL. « Endomorphism rings of elliptic curves over finite fields ». Thèse de doct. 1996 (cf. p. 26, 28, 32).

[66] R. LERCIER et D. LUBICZ. « A quasi-quadratic time algorithm for hyperelliptic curve point counting ». In : *Ramanujan J.* 12.3 (2006), p. 399-423 (cf. p. 8).

[67] R. LERCIER et C. RITZENTHALER. « Hyperelliptic curves and their invariants : Geometric, arithmetic and algorithmic aspects ». In : *Journal of Algebra* 372 (2012), p. 595-636. URL : http://dx.doi.org/10.1016/j.algebra.2012.07.054 (cf. p. 91).

[68] D. LUBICZ et D. ROBERT. « Arithmetic on Abelian and Kummer Varieties ». In : (2012) (cf. p. 92, 174, 175).

[69] J. LUBIN, J.P. SERRE et J. TATE. « Elliptic curves and formal groups ». In : *Lecture notes prepared in connection with the seminars held at the Summer Institute on Algebraic Geometry, Whitney Estate, Woods Hole, Massachusetts* (1964) (cf. p. 115).

[70] A. MAIGA et D. ROBERT. « Computing the canonical lift of genus 2 curves in odd characteristic ». In : (2020). URL : http://www.normalesup.org/~robert/pro/publications/articles/canonical_lift_g2.pdf (cf. p. 123, 143).

[71] A. MAÏGA et D. ROBERT. « Computing the 2-Adic Canonical Lift of Genus 2 Curves ». In : *Proceedings of the Seventh International Conference on Mathematics and Computing*. Sous la dir. de Debasis GIRI, Kim-Kwang RAYMOND CHOO, Saminathan PONNUSAMY, Weizhi MENG, Sedat AKLEYLEK et Santi PRASAD MAITY. Singapore : Springer Singapore, 2022, p. 637-672. ISBN : 978-981-16-6890-6 (cf. p. 78, 123, 143).

[72] R. MANNI. « Modular varieties with level 2 theta structure ». In : *American Journal of Mathematics* 116 (1994), p. 1489-1511 (cf. p. 72).

[73] J-F. MESTRE. « Algorithmes pour compter des points de courbes en petite caractéristique et en petit genre ». In : *Rédigé par David Lubicz, Seminaire de Rennes* () (cf. p. 147).

[74] J.-F. MESTRE. *Lettre à Gaudry et Harley*. 2001. URL : http://www.math.jussieu.fr/mestre (cf. p. 8).

[75] J.-F. MESTRE. *Notes of a talk given at the Cryptography Seminar Rennes*. 2002. URL : http://www.math.univ-rennes1.fr/crypto/2001-02/mestre.ps (cf. p. 7, 8, 156).

[76] J.F. MESTRE. « Construction de Courbes de Genre 2 à partir de leurs Modules ». In : *In Effective Methods in Algebraic Geometry (Castiglioncello, 1990)* (1991), p. 313-334 (cf. p. 78, 79, 83, 90).

[77] E. MILIO. « A quasi-linear algorithm for computing modular polynomials in dimension 2 ». In : *arXiv preprint arXiv :1411.0409* (2014) (cf. p. 105).

[78] E. MILIO. « Calcul de polynômes modulaires en dimension 2 ». Thèse de doct. Déc. 2015. URL : https://members.loria.fr/EMilio (cf. p. 5, 9, 26, 72, 73, 76, 77, 98, 100-105, 108, 110-112, 140).

[79] E. MILIO et Robert D. « Modular polynomials on Hilbert surfaces ». In : *Journal of Number Theory* 216 (2020), p. 403-459. ISSN : 0022-314X. URL : http://www.sciencedirect.com/science/article/pii/S0022314X20301402 (cf. p. 5, 74, 75, 108-110, 131, 140).

[80] V.S. MILLER. « Use of elliptic curves in cryptography ». In : *In Advances in Cryptology - CRYPTO '85 Proceedings* 218 de Lecture Notes in Computer Science (1986). Sous la dir. de Springer Berlin HEIDELBERG, p. 417-426 (cf. p. 2).

[81] J.S. MILNE. *Abelian varieties*. 1991. URL : http://www.jmilne.org/math/CourseNotes/av.html (cf. p. 51).

[82] J.S. MILNE. *Algebraic Geometry (v6.01)*. 2015. URL : http://www.jmilne.org/math/ (cf. p. 26).

[83] R.T. MOENCK. « Fast computation of GCDs, Proceedings of the 5th Annual ACM Sym ». In : () (cf. p. 24).

[84] D. MUMFORD. « On the equations defining abelian varieties. I ». In : *Invent. Math.* 1 (1966), p. 287-354 (cf. p. 175).

[85] D. MUMFORD. « Bi-extensions of formal groups ». In : *Algebraic geometry, Bombay Colloquium 1968* (1968), p. 307-322 (cf. p. 120).

[86] D. MUMFORD. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Bombay : Published for the Tata Institute of Fundamental Research, 1970, p. viii+242 (cf. p. 127).

[87] D. MUMFORD. « The Structure of The Moduli Spaces of Curves and Abelian Varieties ». In : *Congrès Internal. Math.* (1970), p. 457-465 (cf. p. 116).

[88] D. MUMFORD. *Tata lectures on theta I*. T. 28. Progress in Mathematics. With the assistance of C. Musili, M. Nori, E. Previato and M. Stillman. Boston, MA : Birkhäuser Boston Inc., 1983, p. xiii+235. ISBN : 3-7643-3109-7 (cf. p. 61-63, 65).

[89] D. MUMFORD. *Tata lectures on theta II*. T. 43. Progress in Mathematics. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura. Boston, MA : Birkhäuser Boston Inc., 1984, p. xiv+272. ISBN : 0-8176-3110-0 (cf. p. 172, 176, 177).

[90] P. NORMAN et F. OORT. « Moduli of Abelian Varieties ». In : *Annals of Mathematics* 112.02 (sept. 1980), p. 413-439. URL : https://www.jstor.org/stable/1971152 (cf. p. 6, 11, 116, 120, 160).

[91] J. PILA. « Frobenius maps of abelian varieties and finding roots of unity in finite fields ». In : *Math. Comp.* 192.55 (1990), p. 745-763 (cf. p. 146).

[92] Liu QING. « Courbes Stables de genre 2 et leur schéma de modules ». In : *Mathematische Annalen Springer-Verlag, 295, 201-222* (1993) (cf. p. 88, 120-122).

[93] H.L. RESNIKOFF. « On the Graded Ring of Hilbert Modular Forms Associated with $\mathbb{Q}(\sqrt{5})$ ». In : *Math. Ann.* 208 (1974), p. 161-170 (cf. p. 77).

[94] F. RICHELOT. « Essai sur une méthode générale pour déterminer la valeur des intégrales ultra-elliptiques, fondée sur des transformations remarquables de ces transcendantes ». In : *C. R. Acad. Sci. Paris* 2 (1836), p. 622-627 (cf. p. 135).

[95] C. RITZENTHALER. « Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis ». Thèse de doct. Université Denis Diderot Paris VII, juin 2003 (cf. p. 8, 151).

[96] D. ROBERT. « Fonctions thêta et applications à la cryptographie ». Thèse de doct. 2010. URL : https://tel.archives-ouvertes.fr/tel-00528942 (cf. p. 55-58, 61).

[97] D. ROBERT. « Efficient algorithms for abelian varieties and their moduli spaces ». In : (mars 2021). Habilitation à diriger les recherches. URL : http://www.normalesup.org/~robert/pro/publications/academic/hdr.pdf (cf. p. 42, 46, 160).

[98] D. ROBERT, A. PAGE et J. KIEFFER. « Computing isogenies from modular equations between Jacobians of genus 2 curves ». In : () (cf. p. 4, 7, 96, 97, 143, 160).

[99] T. SATOH. « The canonical lift of an ordinary elliptic curve over a finite field and its point counting ». In : *J. Ramanujan Math. Soc* (2000), 15 :247-270 (cf. p. 6, 10, 11, 18, 19, 35, 38, 40, 128, 146, 159).

[100] T. SATOH, B. SKJERNAA et Y. TAGUCHI. « Fast computation of canonical lifts of elliptic curves and its application to point counting ». In : (2003), p. 89-101 (cf. p. 23).

[101] R. SCHERTZ. « Complex multiplication ». In : *Cambridge University Press*. New mathematical monographs 15 (2010) (cf. p. 31).

[102] R. SCHOOF. « Elliptic curves over finite fields and the computation of square roots mod p ». In : *Mathematics of computation* 44.170 (1985), p. 483-494 (cf. p. 146).

[103] F. SCHOTTKY. « Zur Theorie der Abel schen Functionen vor vier Variablen ». In : *Journal fur die Reine und Angewandte Mathematik* 102 (1888), p. 304-352 (cf. p. 65).

[104] J.P. SERRE et J. TATE. « Good Reduction of Abelian Varieties ». In : *The Annals of Mathematics*. Second Series 88 (1968), p. 492-517 (cf. p. 115).

[105] J.H. SILVERMAN. *The arithmetic of elliptic curves*. T. 106. Graduate Texts in Mathematics. Corrected reprint of the 1986 original. New York : Springer-Verlag, 1986, p. xii+400. ISBN : 0-387-96203-4 (cf. p. 26, 28, 29).

[106] J.H. SILVERMAN. *Advanced topics in the arithmetic of elliptic curves*. T. 151. Graduate Texts in Mathematics. New York : Springer-Verlag, 1994, p. xiv+525. ISBN : 0-387-94328-5 (cf. p. 26, 30).

[107] J.H. SILVERMAN, G. CORNELL et M. ARTIN. *Arithmetic geometry*. Springer, 1986 (cf. p. 40).

[108] B. SKJERNAA. « Satoh's algorithm in characteristic 2 ». In : *Math. Comp. 72(241)* (2003), 477-487(electronic) (cf. p. 6, 37).

[109] B. SMITH. « Explicit Endomorphisms and Correspondences ». Thèse de doct. Déc. 2005 (cf. p. 135, 136).

[110] H.M. STARK. « Class-numbers of complex quadratic fields ». In : *Springer Verlag*, 1973 *Proceedings International Summer School University of Antwerp, RUCA, July* 17-*Agust* 3 320 of Lecture Notes in Mathematics.263 (1972). Sous la dir. de Modular functions of one variable I, p. 155-174 (cf. p. 32).

[111] H. STICHTENOTH. « Die Hasse-Witt-Invariante eines Kongruenzfunktio-nenkörpers ». In : 33.4 (1980), p. 357-360 (cf. p. 146).

[112] H. STICHTENOTH et C.P. XING. « On the structure of the divisor class group of a class of curves over finite fields ». In : *Arch. Math.(Basel)* 65.2 (1995), p. 141-150 (cf. p. 146).

[113] M. STRENG. « Complex multiplication of abelian surfaces ». Thèse de doct. Leiden,marco.streng@gmail.com, 2010. ISBN : -13/EAN : 978-90-5335-291-5 (cf. p. 71, 87, 105).

[114] J. THOMAE. « Beitrag zur Bestimmung von $\theta(0,0,...,0)$ durch die Klassen-moduln algebraischer Funktionen ». In : *Journal für die Reine und Angewandte Mathematik* (1870) (cf. p. 91).

[115] J. VÉLU. « Isogénies entre courbes elliptiques ». In : *Compte Rendu Académie Sciences Paris Série A-B* 273 (1971), A238-A241 (cf. p. 32).

[116] F. VERCAUTEREN. « Computing zeta functions of curves over finite fields ». In : *PhD thesis, Katholieke Universiteit Leuven* (2003) (cf. p. 147).

[117] F. VERCAUTEREN, B. PRENEEL et J. VANDEWALLE. « A memory efficient version of Satoh's algorithm ». In : *Springer-Verlag* 2045 (2001). Sous la dir. d'Advances in CRYPTOLOGY – EUROCRYPT 2001, p. 1-13 (cf. p. 36).

[118] P. WAMELEN. « Equations for the Jacobian of a hyperelliptic curve ». In : *AMS* 350.8 (août 1999), p. 3083-3106 (cf. p. 176).

Quatrième partie

ANNEXE

a

ANNEXE

Dans l'annexe nous rappellons quelques méthodes algorithmiques utilisées dans les exemples tests.

A.1 ARITHMÉTIQUE SUR LA JACOBIENNE

On considère la courbe hyperelliptique $\mathcal{C}$ de genre g sous un modèle imaginaire techniquement plus agréable. Soit $\mathcal{C} : y^2 + h(x)y = f(x)$ (avec $\deg f = 2g+1$ et $\deg h \leq g$), alors toute classe de $\mathrm{Jac}(\mathcal{C})$ contient un unique diviseur D défini par :

$$D = P_1 + \cdots + P_r - r\infty$$

pour $P_1, \cdots, P_r \in \mathcal{C}$ ne dépendant que de la classe, tels que :

— $P_i \neq \infty$ et $P_i \neq \iota(P_j)$ pour $i \neq j$

— et $r \leq g$.

Un tel diviseur D est dit *réduit* et si on n'a pas la condition $r \leq g$, il est dit *semi-réduit* et alors il n'est pas unique. Voir [34] pour plus de détails. On peut remarquer que le diviseur $P + \iota(P) - 2\infty = div(x - x_P)$ étant principal n'affecte pas la classe ; de même 2 fois un point de ramification.
Soit $D = P_1 + \cdots + P_r - r\infty$ un diviseur sous forme réduite (ou semi-réduite). Alors D peut être représenté de manière unique par deux polynômes $u(x)$ et $v(x)$ définis par :

$$u(x) = \prod_{i=1}^{r} (x - x_{P_i}) \quad et \quad v(x_{P_i}) = y_{P_i},\ pour\, i = 1, \cdots, r.$$

et $v(x)$ est l'unique polynôme avec $\deg v < r$ tel que $u(x)$ divise $v^2(x) + v(x)h(x) - f(x)$.
$u(x)$ représente les abcisses des P_i et on pourra déterminer $v(x)$ par interpolation. Et le couple ($u(x)$,$v(x)$) est appelé *représentation de Mumford* et noté

$$D = \langle u(x), v(x) \rangle.$$

L'entier r est appelé le *poids de* D et D est dit *premier* si le polynôme u est irréductible.
Et nous avons l'algorithme a.1.1 de réduction d'un diviseur semi-réduit, qui procède par des ajouts de diviseurs principaux : Dans cet algorithme proposé par Cantor [9], une itération de la boucle fait baisser le poids r de 2 ou de 1 pour la dernière.
Chaque classe de diviseur dans $\mathrm{Jac}(\mathcal{C})$ étant représentée par un unique diviseur réduit, la représentation de Mumford permet d'expliciter l'addition d'éléments de $\mathrm{Jac}(\mathcal{C})$.

A.1.1 *Algorithme de Cantor*

Nous décrivons dans cette partie un algorithme permettant de déterminer la représentation de Mumford de la somme de deux diviseurs réduit et donnés sous forme de Mumford.
Pour un point P de la courbe, on a $div(x - x_P) = P + \iota(P) - 2\infty$ ce qui implique que

Entrée: Diviseur $D = \langle u(x), v(x) \rangle$ semi-réduit ;
Sortie: Diviseur réduit $D' \sim D$;

1. Tant que $\deg u(x) > g$, faire :
   a. $u = \left(f - hv - v^2\right) / u$;
   b. $v = (-h - v) \mod u$;
2. Retourner $D' = \langle u(x), v(x) \rangle$;

Algorithm a.1.1 Réduction de Mumford

Entrée: Diviseurs $D_1 = \langle u_1(x), v_1(x) \rangle$ $D_2 = \langle u_2(x), v_2(x) \rangle$ semi-réduits ;
Sortie: Diviseur réduit $D_3 \sim D_1 + D_2$;

1. Caluler s_1, s_2, s_3 par pcgd étendus tel que:

$$d = pgcd\,(u_1, u_2, v_1 + v_2 + h) = s_1 u_1 + s_2 u_2 + s_3(v_1 + v_2 + h)$$

2. $u_3 = u_1 u_2 / d^2$;
3. $v_3 = d^{-1} \cdot (s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)) \mod u_3$;
4. Retourner $D_3 = \langle u_3(x), v_3(x) \rangle$;

Algorithm a.1.2 Addition de Cantor

---

l'opposé du diviseur $D = P - \infty$ est $-D = \iota(P) - \infty$ c'est-à-dire $D = \langle (x - x_P), y_P \rangle$ et $-D = \langle (x - x_P), -y_P - h(x) \rangle$ car $y_{\iota(P)} = y_P - h(x_P)$. Et le cas général en découle, l'opposé dans $\mathrm{Jac}(\mathcal{C})$ de tout diviseur $D = \langle u(x), v(x) \rangle$ réduit (ou semi-réduit) est donné par :

$$-D = \langle u(x),\ -v(x) - h(x) \mod u(x) \rangle.$$

L'Algorithme d'addition suivant a.1.2 a été proposé par Cantor dans [9] et son équivalent en caractéristique 2 est décrit dans [64].

Les deux algorithmes a.1.1 et a.1.2 permettent la composition de diviseurs réduits.

A.1.2 *Amélioration et Complexité*

Si on note par $M(n)$ le nombre d'opérations dans le corps de base nécessaires pour multiplier deux polynômes de degré au plus n. En considérant une situation plus agréable de composition de Cantor de deux diviseurs réduits et en considérant que l'on peut calculer éfficacement le pgcd de deux polynômes, on peut additionner deux diviseurs réduits avec l'algorithme a.1.2 en $O\,(M(g) \log g)$ opérations dans $\Bbbk$ [34]. Alors que la réduction d'un diviseur de poids au plus $2g$ se fait en $O\,(gM(g))$ opérations dans $\Bbbk$. Bien que dans le cas $g = 2$ ces algorithmes sont parmi les plus efficaces, il est possible de les dérouler selon le poids des diviseurs en entrée et aux différents branchements possibles dans les algorithmes de calcul pgcd (Voir [34] pour plus de détails).

A.2 ARITHMÉTIQUE SUR LA KUMMER

La Jacobienne $\operatorname{Jac} C$ d'une courbe hyperelliptique $\mathcal{C}$ de genre 2 sur $\mathbb{C}$ étant une surface abélienne principalement polarisée et simple, le théorème 3.2.4 dans le chapitre 3 établit que les fonctions thêta de niveau 2 ne permettent qu'un plongement projectif de $(\operatorname{Jac} C) / \pm 1$. Et à partir de la théorie des fonctions thêta Chudnovsky introduisirent des formules éfficientes pour l'Arithmétique sur la variété de Kummer $(\operatorname{Jac} C) / \pm 1$. Cependant en dimension 2 les formules avec les fonctions thêta sont d'abord valables sur $\mathbb{C}$; pour les adaptations sur un corps quelconque certaines conditions doivent être remplies.
Nous nous reférons sur [36] pour décrire dans cette partie certains résultats dont nous utilisons dans l'exemple 7.2.6. Et dans cette partie la caractéristique du corps $\Bbbk$ est différente de 2.
Soit $\Omega \in \mathfrak{H}_2$, la surface de Kummer associée à Ω est le lieu des images par l'application ϕ de $\mathbb{C}^2$ sur $\mathbb{P}^3(\mathbb{C})$ définie par :

$$z \mapsto (\vartheta_1(2z), \vartheta_2(2z), \vartheta_3(2z), \vartheta_4(2z)) \quad \textit{avec}$$

$$\vartheta_1(z) = \theta_0(z, \Omega),\ \ \vartheta_2(z) = \theta_3(z, \omega),\ \ \vartheta_3(z) = \theta_1(z, \Omega),\ \ \vartheta_4(z) = \theta_2(z, \omega).$$

Cet ordre correspond aux notations utilisées par Gaudry dans [36] sur lequel nous allons nous referer dans cette partie.
Les quatres fonctions $\vartheta_i(\cdot)$ avec $i \in \{0, 1, 2, 3\}$ ne s'annulent pas en même temps. De plus comme ces fonctions thêta sont paires, la fonction ϕ est paire et elle envoie deux points opposés sur une même image sur la surface de Kummer (variété projective de dimension 2) que nous notons par $\mathcal{K}$. Nous notons aussi par Θ la fonction thêta associée à 2Ω. Comme les Θ et ϑ sont duals alors nous avons les évaluations suivantes :

$$\Theta_1(z) = \theta_0(z, 2\Omega), \quad \Theta_2(z) = \Theta_{12}(z, 2\omega),$$

$$\Theta_3(z) = \theta_8(z, 2\Omega), \quad \Theta_4(z) = \Theta_4(z, 2\omega).$$

À partir des formules de duplication 3.3.2 et les thêta constantes ϑ_i et Θ_i, on peut toutefois déterminer sur $\mathcal{K}$, $\phi(2z)$ ne connaissant que $\phi(z)$. D'un autre côté: il est impossible de savoir si l'image ϕ provient de $-z$ ou-bien de z. Ainsi on ne peut distinguer $\phi(z - z')$ de $\phi(z + z')$ sur $\mathcal{K}$.

A.2.1 *Equation d'une surface de Kummer*

Pour $\Omega \in \mathfrak{H}_2$, alors $a = \vartheta_1$, $b = \vartheta_2$, $c = \vartheta_3$ et $d = \vartheta_4$ désignent les quatres thêta constantes fondamentales associées à Ω et A, B, C et D ceux associés 2Ω de la variété $(2, 2)$-isogène.
En utilisant les formules de duplication 3.3.2 nous avons :

$$4A^2 = (a^2 + b^2 + c^2 + d^2), \quad 4B^2 = (a^2 + b^2 - c^2 - d^2),$$
$$4C^2 = (a^2 - b^2 + c^2 - d^2), \quad 4D^2 = (a^2 - b^2 - c^2 + d^2),$$

Pour tout $z \in \mathbb{C}^2$ nous notons les fonctions thêta fondamentales en z par :

$$x = \vartheta_1(z), \qquad y = \vartheta_2(z), \qquad z = \vartheta_3(z), \qquad t = \vartheta_4(z).$$

Le quadruplet (x, y, z, t) correspond aux coordonnées projectives associées à un point de la surface de Kummer.

• *Lorsque abcd est non nul et les six autres thêta constantes paires déduites sont aussi non nulles* que nous appellons *condition 1*.
Et les quadruplets vérifiant cette condition définissent bien une matrice de $\mathfrak{H}_2$ en laquelle nous avons: $(a,b,c,d) = (\theta_0, \theta_3, \theta_1, \theta_2)$.
Alors une équation projective de $\mathcal{K}$ peut être construite en combinant des identités de Frobenius [89, Chap: IIIa]. Et une équation projective de $\mathcal{K}$ est définie par:

$$(x^4+y^4+z^4+t^4)+2Exyzt-F(x^2t^2+y^2z^2)-G(x^2z^2+y^2t^2)-H(x^2y^2+z^2t^2)=0$$

$$\begin{aligned}
E &= 256abcdA^2B^2C^2D^2/((a^2d^2-b^2c^2)(a^2c^2-b^2d^2)(a^2b^2-c^2d^2));\\
F &= (a^4-b^4-c^4+d^4)/(a^2d^2-b^2c^2);\\
G &= (a^4-b^4+c^4-d^4)/(a^2c^2-b^2d^2);\\
H &= (a^4+b^4-c^4-d^4)/(a^2b^2-c^2d^2);
\end{aligned}$$

Les dénominateurs apparaissants dans les nombres E, F, G et H sont produits de thêta constantes paires. Les valeurs de Ω pour lesquelles les thêta constantes paires s'annulent correspondent aux variétés abéliennes isomorphes à un produit de courbes elliptiques.
Les formules définies sont tous homogènes alors l'égalité projective est suffisante.

A.2.2 *Formules de Pseudo-Addition*

Pour tous z et z' dans $\mathbb{C}^2$ les formules d'addition donnent les résultats:

$$\begin{aligned}
\vartheta_1(z+z')\vartheta_1(z-z') &= \Theta_1(2z)\Theta_1(2z')+\Theta_2(2z)\Theta(2z')\\
&\quad+\Theta_3(2z)\Theta_3(2z')+\Theta_4(2z)\Theta_4(2z'),\\
\vdots \qquad &= \qquad \vdots\\
\vartheta_4(z+z')\vartheta_4(z-z') &= \Theta_1(2z)\Theta_1(2z')-\Theta_2(2z)\Theta(2z')\\
&\quad-\Theta_3(2z)\Theta_3(2z')+\Theta_4(2z)\Theta_4(2z'),
\end{aligned}$$

et

$$\begin{aligned}
4\Theta_1(z+z')\Theta_1(z-z') &= \vartheta_1(z)\vartheta_1(z')+\vartheta_2(z)\vartheta_2(z')+\vartheta_3(z)\vartheta_3(z')+\vartheta_4(z)\vartheta_4(z'),\\
\vdots \qquad &= \qquad \vdots,\\
4\Theta_4(z+z')\Theta_4(z-z') &= \vartheta_1(z)\vartheta_1(z')-\vartheta_2(z)\vartheta_2(z')-\vartheta_3(z)\vartheta_3(z')+\vartheta_4(z)\vartheta_4(z').
\end{aligned}$$

D'autre part :
• *Lorsque A^2, B^2, C^2, D^2 étant en fonction des a^2, b^2, c^2, d^2 sont tels que abcd est non nul et aussi le produit $ABCD$*, alors nous désignons cela par *condition 2*. Ainsi nous pouvons calculer les valeurs suivantes pour les formules de la pseudo-addition :

$$\begin{aligned}
&y_0 = a/b, \quad z_0 = a/c, \quad t_0 = a/d,\\
&Y_0 = A^2/B^2, \quad Z_0 = A^2/C^2, \quad T_0 = A^2/D^2.
\end{aligned}$$

Et cet algorithme peut s'étendre au produit scalaire par un entier $n > 1$ comme suit: Pour $P \in \mathcal{K}$ et $m > 1$, connaissant mP et $(m+1)P$, on détermine $(2m+1)$ avec "PseudoAdd" ensuite $(2m)$ et $(2m+2)$ avec "PseudoDouble". Et en partant d'une décomposition binaire de n l'algorithme a.2.3 calcule éfficacement nP.

Entrée: $P = (x, y, z, t) \in \mathcal{K}$;
Sortie: $2P = (x_2, y_2, z_2, t_2) \in \mathcal{K}$;

1. $x_1 = (x^2 + y^2 + z^2 + t^2)^2$;
2. $y_1 = Y_0(x^2 + y^2 - z^2 - t^2)^2$;
3. $z_1 = Z_0(x^2 - y^2 + z^2 - t^2)^2$;
4. $t_1 = T_0(x^2 - y^2 - z^2 + t^2)^2$;
5. $x_2 = x_1 + y_1 + z_1 + t_1$;
6. $y_2 = y_0(x_1 + y_1 - z_1 - t_1)$;
7. $z_2 = z_0(x_1 - y_1 + z_1 - t_1)$;
8. $t_2 = t_0(x_1 - y_1 - z_1 + t_1)$;
9. Return (x_2, y_2, z_2, t_2)

Algorithm a.2.1 PseudoDouble

Entrée: $P = (x, y, z, t)$ et $Q = (x_2, y_2, z_2, t_2)$ dans $\mathcal{K}$ et $R = (\underline{x}, \underline{y}, \underline{z}, \underline{t})$ égal $P + Q$ ou-bien $P - Q$, avec $\underline{xyzt} \neq 0$
Sortie: $(X, Y, Z, T) \in \mathcal{K}$ l'autre composition differente de R.

1. $x_3 = (x_2^2 + y_2^2 + z_2^2 + t_2^2)(x^2 + y^2 + z^2 + t^2)$;
2. $y_3 = Y_0(x_2^2 + y_2^2 - z_2^2 - t_2^2)(x^2 + y^2 - z^2 - t^2)$;
3. $z_3 = Z_0(x_2^2 - y_2^2 + z_2^2 - t_2^2)(x^2 - y^2 + z^2 - t^2)$;
4. $t_3 = T_0(x_2^2 - y_2^2 - z_2^2 + t_2^2)(x^2 - y^2 - z^2 + t^2)$;
5. $X = (x_3 + y_3 + z_3 + t_3)/\underline{x}$;
6. $Y = (x_3 + y_3 - z_3 - t_3)/\underline{y}$;
7. $Z = (x_3 - y_3 + z_3 - t_3)/\underline{z}$;
8. $T = (x_3 - y_3 - z_3 + t_3)/\underline{t}$;
9. Return (X, Y, Z, T);

Algorithm a.2.2 PseudoAdd

Entrée: $P = (x, y, z, t) \in \mathcal{K}$ avec $xyzt \neq 0$ et $n > 1$ un entier ;
Sortie: $nP = (x_2, y_2, z_2, t_2) \in \mathcal{K}$;

1. Si $n = 2$, Retourner PseudoDouble(P) ;
2. $n_0 n_1 \cdots n_k$ étant la décomposition binaire de n, avec n_0 le bit dominant ;
3. $P_m = P$, P_d =PseudoDouble(P) ;
4. Pour $i = 1$ allant à k Faire ;
   a. Q = PseudoAdd(P_d,P_m,P) ;
   b. Si $n_i = 1$ Alors,
      i. P_d =PseudoDouble(P_d) ;
      ii. $P_m = Q$;
   c. Sinon ,
      i. P_m =PseudoDouble(P_m) ;
      ii. $P_d = Q$;
5. Retourner P_m .

Algorithm a.2.3 PseudoAdd n-fois

Remarque a.2.1. L'algorithme PseudoAdd a.2.2 ne marche pas si R admet une coordonnée nulle. Même si cette condition reste valable pour la multiplication scalaire, cela présente un problème majeur pour cette approche. Alors une méthode plus générale est l'addition utilisant les formules différentielles de Riemann. Bien que cette dernière est moins bonne en terme de complexité.

A.2.3 *Addition Différentielle*

Soient $Z(n) = \mathbb{Z}^g / n\mathbb{Z}^g$ et μ_n le groupe des n-racines de l'unité dans $\mathbb{C}^*$, alors le dual de Cartier $\widehat{Z}(n) = \oplus_{i=1}^{g} \mu_n$. En utilisant les formules de duplication et les rélations de Riemann D. Lubicz et D. Robert ont perfectionné la Pseudo-Addition dans [68]. Dans cette partie nous allons nous referer sur leurs résultats.

Théorème a.2.2. *(Relations de Riemann). Soient $z_1, z_2, z_3, z_4, z \in \mathbb{C}^g$ avec $2z = z_1 + z_2 + z_3 + z_4$ et $z'_1 = z - z_1$, $z'_2 = z - z_2$, $z'_3 = z - z_3$ et $z'_4 = z - z_4$. Alors pour tout charactère $\chi \in \widehat{Z}(2)$ et tous $i, j, k, l, m \in Z(n)$ tels que $i + j + k + l = 2m$, si $i' = m - i$, $j' = m - j$, $k' = m - k$ et $l' = m - l$, nous avons :*

$$\left(\sum_{t \in Z(2)} \chi(t)\theta_{i+t}(z_1)\theta_{j+t}(z_2)\right) \cdot \left(\sum_{t \in Z(2)} \chi(t)\theta_{k+t}(z_3)\theta_{l+t}(z_4)\right) =$$
$$\left(\sum_{t \in Z(2)} \chi(t)\theta_{i'+t}(z'_1)\theta_{j'+t}(z'_2)\right) \cdot \left(\sum_{t \in Z(2)} \chi(t)\theta_{k'+t}(z'_3)\theta_{l'+t}(z'_4)\right)$$

En particulier, nous avons les formules d'addition :

$$\left(\sum_{t\in Z(2)}\chi(t)\theta_{i+t}(z_1+z_2)\theta_{j+t}(z_1-z_2)\right)\cdot\left(\sum_{t\in Z(2)}\chi(t)\theta_{k+t}(0)\theta_{l+t}(0)\right)=$$
$$\left(\sum_{t\in Z(2)}\chi(t)\theta_{-i'+t}(z_2)\theta_{j'+t}(z_2)\right)\cdot\left(\sum_{t\in Z(2)}\chi(t)\theta_{k'+t}(z_1)\theta_{l'+t}(z_1)\right)$$

Démonstration. Voir [84] pour l'approche analytique ou [68] pour l'approche algébrique. □

On en déduit les formules d'addition explicites suivantes pour les surfaces abéliennes . Soit $(a_i)_{i\in Z(2)}$ un quadruplet de thêta constantes de niveau 2 associé à la Kummer $\mathcal{K}$. Pour tous $x=(x_i)_{i\in Z(2)}$ et $y=(y_i)_{i\in Z(2)}$ on pose $X=x+y$ et $Y=x-y$. Alors les coordonnées de $2W_{ij}=X_iY_j+X_jY_i$ sont donnés par les rélations suivantes:

$$\begin{aligned}
2(X_{10}Y_{00}+X_{00}Y_{10}) &= z_{10}^{00}+z_{10}^{01};\\
2(X_{11}Y_{01}+X_{01}Y_{11}) &= z_{10}^{00}+z_{10}^{01};\\
2(X_{01}Y_{00}+X_{00}Y_{01}) &= z_{01}^{00}+z_{01}^{10};\\
2(X_{11}Y_{10}+X_{10}Y_{11}) &= z_{01}^{00}+z_{01}^{10};\\
2(X_{11}Y_{00}+X_{00}Y_{11}) &= z_{11}^{00}+z_{11}^{11};\\
2(X_{01}Y_{10}+X_{10}Y_{01}) &= z_{10}^{00}+z_{11}^{11};
\end{aligned}$$

où pour $i\in Z(2)$, $\chi\in\widehat{Z}(2)$ on a :

$$z_i^{\chi}=(\sum_{t\in Z(2)}\chi(t)x_{i+t}x_t)(\sum_{t\in Z(2)}\chi(t)y_{i+t}y_t)/(\sum_{t\in Z(2)}\chi(t)a_{i+t}a_t)$$

et $\sum_t\chi(t)a_{i+t}a_t$ n'est autre que la thêta constante $\theta\left[\begin{smallmatrix}\chi/2\\ i/2\end{smallmatrix}\right](0,\Omega)^2$. De plus lorsqu'on ajoute à ces relations les formules d'addition :

$$\begin{aligned}
4X_{00}Y_{00} &= z_{00}^{00}+z_{00}^{01}+z_{00}^{10}+z_{00}^{11};\\
\vdots \quad &= \quad \vdots\\
4X_{11}Y_{11} &= z_{00}^{00}-z_{00}^{01}-z_{00}^{10}+z_{00}^{11};
\end{aligned}$$

on détermine les coordonnées projectives de X dans $\mathcal{K}$. Pour plus de simplicité on peut supposer $a_0=1$ et $A_{00}^{00}=1$.

Remarque a.2.3. Lorsque l'on représente par M le coût d'une multiplication sur le corps de base $\mathbb{k}$, par S celui d'un calcul de carré . Comme nous travaillons avec des coordonnées projectives, l'inversion coûtera quelque multiplications. Ainsi

— Le coût d'une pseudo-addition avec les algorithmes a.2.2 est de $7M+12S+9M_0$.

— Alors la réconstitution des coordonnées de $X_iY_j+X_jY_i$ dans la méthode de l'addition différentielle coûte $10M+20S+9M_0$.

A.3 CONVERSIONS ENTRE FONCTIONS THÊTA ET POLY NÔMES DE MUMFORD

Dans cette partie, nous nous intéressons aux liens entres les coordonnées Mumford d'un diviseurs $D=\langle u,v\rangle$ de la Jacobienne d'une courbe et les coordonnées thêta de son image z

par l'application d'Abel-Jacobi.
Les formules de Thomae permettent d'obtenir les puissances quatrième des thêta constantes en dimension g à partir de l'équation d'une courbe hyperelliptique de genre g. Elles dépendent d'un choix de la base du groupe d'homologie. Des méthodes introduites par Mumford [89] et Van Wamelen [118] déterminent des formules de changement de coordonnées entre (u, v) et des thêta constantes de niveau 4; et ensuite entre (u, v^2) et des thêta constantes de niveau 2 définissant la variété Kummer. Dans cette partie nous nous réferons aux améliorations techniques proposées par R. Cosset dans [19] où l'étude concerne le genre quelconque.
Lorsque $\mathfrak{H}_g^{(2)}$ désigne l'ensemble des paires $(\mathcal{C}, \sigma)$ modulo isomorphismes de courbes, où $\mathcal{C}$ est une courbe hyperelliptique et $\sigma : \{1, \cdots, 2g+2\} \longleftarrow E$ une bijection, avec $E = \{a_1, \cdots, a_{2g+1}\}$ l'ensemble des points de ramification $\pi : \mathcal{C} \longleftarrow \mathbb{P}^1$. On montre que :
$\mathfrak{H}_g^{(2)} \simeq \{$ séquences de points distincts $P_1, \cdots, P_{2g+2}$ de $\mathbb{P}^1\}$ modulo l'équivalence projective $\mathrm{PGL}_2(\mathbb{C})$.
En normalisant et en posant $a_1 = 0$ et $a_2 = 1$, on obtient :
$\mathfrak{H}_g^{(2)} \simeq \{$ sous-ensemble ouvert de $\mathbb{C}^{2g-1}$ de points $(a_3, \cdots, a_{2g+1})$ tel que $a_i \neq a_j$ et $a_i \neq 0, 1$ $\}$.
Alors l'anneau des coordonnées affine de $\mathfrak{H}_g^{(2)}$ est engendré par les fonctions

$$\left(\frac{\theta_{a,b}}{\theta_{0,0}}\right)^{\pm 4}$$

On considère la courbe hyperelliptique sous un modèle imaginiare techniquement plus agréable.

Pour ce qui suit $g = 2$ et pour une simplification des formules, nous admettons les notations suivantes : $\mathcal{C} : y^2 = f(x)$ avec $\deg f = 5$ et $a_1, \cdots, a_5$ les racines de f. On pose :

$$\eta_1 = [(1/2, 0); (0, 0)] \quad \eta_2 = [(1/2, 0); (1/2, 0)] \quad \eta_3 = [(0, 1/2); (1/2, 0)]$$

$$\eta_4 = [(0, 1/2); (1/2, 1/2)] \quad \eta_5 = [(0, 0); (1/2, 1/2)] \quad \eta_\infty = [(0, 0); (0, 0)].$$

Pour $S \subset \{1, \cdots, 5, \infty\}$, on pose : $\eta_S = \sum_{i \in S} \eta_i$, tel que $\Omega\eta'_S + \eta''_S$ est l'image par l'application d'Abel-Jacobi du diviseur $\sum_{i \in S} a_i - \#S(\infty)$. Par suite toute fonction thêta est de la forme $\theta[\eta_{U \circ A}]$ avec $U = \{1, 3, 5\}$ et A un sous-ensemble d'ordre impaire de $\{1, \cdots, 5\}$. Le symbole $\circ$ désigne l'opération de la différence symétrique de deux ensembles.
On definit les fonctions t_A selon Wamelen [118] par :

$$t_A(z) = f_A \cdot \theta[\eta_{U \circ A}]$$

où f_A sont des constantes définies par : $f_A = \theta[0]/\theta[\eta_{U \circ A}]$ pour les fonctions paires autrement par :

$$f_1 = \delta\frac{\theta_0\theta_4\theta_6\theta_{12}}{\theta_1\theta_3\theta_9\theta_{15}}, \quad f_2 = \delta\frac{\theta_4\theta_6\theta_{12}}{\theta_2\theta_8\theta_{15}}, \quad f_3 = \delta\frac{\theta_0\theta_6}{\theta_2\theta_3}, \quad f_4 = \delta\frac{\theta_4}{\theta_1}$$

$$f_5 = \delta\frac{\theta_0\theta_{12}}{\theta_8\theta_9}, \quad f_{\{1,2,3,4,5\}} = f_\emptyset = \delta^3\frac{\theta_4^2\theta_6^2\theta_{12}^2}{\theta_1\theta_2\theta_3\theta_8\theta_9\theta_{15}} \quad avec \quad \delta = \frac{-1}{\sqrt{a_2 - a_1}}.$$

De même pour A de cardinale pair, les fonctions t_{A^c} et f_{A^c} (où A^c est le complémentaire de A dans $\{1, \cdots, 5\}$) seront notées par t_A et f_A.

A.3.1 *De Thêta Constantes aux Coordonnées de Mumford*

Soit $\mathcal{C}$ une courbe de genre 2 d'équation $y^2 = f(x)$ avec $(a_i)_{i\in\{1,\cdots,6\}}$ un ordre choisi sur les racines de f et soit $D \in \mathrm{Jac}\,(C)$ n'est pas un diviseur thêta. Le Théorème [89, Théorème 5.3] de Mumford établit que les coefficients des polynômes de Mumford (u, v) de D sont fonctions méromorphes sur $\mathbb{C}^2/(\Omega\mathbb{Z}^2 + \mathbb{Z}^2)$.
Ainsi Van Wamelen montra qu'avec les fonctions t_A nous avons pour toute racine a_i avec $i \in \{1, \cdots, 6\}$ de f et pour tous l, m deux entiers distincts de $\{1, \cdots, 5\} - \{k\}$:

$$u(a_i) = \frac{t_k^2(z)}{t_\emptyset^2(z)}, \quad v(a_i) = \frac{Y_{k,m} - Y_{k,l}}{a_l - a_m}, \quad et \quad Y_{l,m} := \pm\frac{t_l(z)t_m(z)t_{l,m}(z)}{t_\emptyset^3(z)}$$

Pour la détermination du signe des $Y_{l,m}$ on peut utiliser l'approche de R. Cosset dans [18, Section 5.1.4]. La fonction Y_S a un pôle d'ordre exactement $s + 1$ en les diviseurs thêta sinon elle est regulière ailleure.

Ainsi dans le cas où l'on utilise des fonctions thêta de niveau $n = 2$ ou 4, on peut déterminer les coordonnées de Mumford (u, v) de D par interpollation de Langrange sachant que :

$$u(a_1) = (a_2 - a_1)^2 \frac{\theta_0^2\theta_2^2\theta_8^2}{\theta_4^2\theta_6^2\theta_{12}^2}\frac{\theta_{10}(z)^2}{\theta_{14}(z)^2},$$

$$u(a_2) = (a_2 - a_1)^2 \frac{\theta_1^2\theta_3^2\theta_9^2}{\theta_4^2\theta_6^2\theta_{12}^2}\frac{\theta_{11}(z)^2}{\theta_{14}(z)^2}$$

$$v(a_1) = \frac{1}{a_3 - a_2}\left(Y_{1,2} - Y_{1,3}\right), \quad v(a_2) = \frac{1}{a_3 - a_1}\left(Y_{1,2} - Y_{2,3}\right).$$

Où l'on peut trouver dans [19] un calcul donnant :

$$Y_{1,2} = c_{1,2}\sqrt[7]{a_2 - a_1}\,\frac{\theta_0^3\theta_1^2\theta_2^2\theta_3^2\theta_8^2\theta_9^2}{\theta_4^4\theta_6^4\theta_{12}^4}\frac{\theta_{10}(z)\theta_{11}(z)\theta_{15}(z)}{\theta_{14}(z)^3},$$

$$Y_{1,3} = c_{1,2}\sqrt[7]{a_2 - a_1}\,\frac{\theta_0^3\theta_1^2\theta_2^2\theta_8^2\theta_9^2\theta_{15}^2}{\theta_4^5\theta_6^4\theta_{12}^5}\frac{\theta_3(z)\theta_7(z)\theta_{10}(z)}{\theta_{14}(z)^3},$$

$$Y_{2,3} = c_{1,2}\sqrt[7]{a_2 - a_1}\,\frac{\theta_0^3\theta_1^2\theta_3^2\theta_8^2\theta_9^2\theta_{15}^2}{\theta_4^5\theta_6^4\theta_{12}^5}\frac{\theta_2(z)\theta_7(z)\theta_{11}(z)}{\theta_{14}(z)^3}.$$

Pour raison de simplification, on peut calculer les calculs les produits de fonctions thêta en utilisant les fonctions thêta de niveau 4.[19].
Dans le cas utilisant les thêta de niveau 2, on peut améliorer les calculs des produits de $Y_{1,2}$, $Y_{1,3}$ et $Y_{2,3}$ en utilsant les formules de l'équation de la Kummer a.2.1.
Lorsque D est un diviseur thêta alors il vérifie :

$$\deg(u) \leq 1 \iff t_\emptyset(z) = 0 \iff \theta_{14}(z) = 0.$$

et dans le cas où il s'écrit $[DiviseurTheta] + (a_k - \infty)$, on a :

$$u(a_k) = 0 \iff t_k(z) = 0 \iff \theta[\eta_{U\circ\{k\}}](z) = 0.$$

A.3.2 *Des Coordonnées de Mumford aux Thêta Constantes*

En conservant les mêmes notations, nous partons du diviseur D en coordonnées Mumford (u, v) (ou (u, v^2) pour la surface de Kummer) et nous voulons déterminer les fonctions thêta de niveau $n = 2$ ou 4 (à un facteur constant près) correspondant aux coordonnées projectives de l'image z de D par l'application d'Abel-Jacobi.
Dans le cas $n = 2$, les termes $Y_{i,j}^2$ peuvent être exprimer algébriquement en fonction des polynômes u et v^2 en inversant les formules du problème inverse. En évaluant u en les racines de f, l'on obtient:

$$Y_{l,m}(D)^2 = \frac{(y_1(x_2 - a_l)(x_2 - a_m) - y_2(x_1 - a_l)(x_1 - a_m))^2}{(x_2 - x_1)^2}$$

Et par suite les formules pour les $\dfrac{\theta_i(z)^2}{\theta_{14}(z)^2}$ pour $i \in \{0, \cdots, 15\}$.
Dans le cas $n = 4$, les fonctions thêta de niveau 4 sont de la forme $\theta[\eta_{U\circ A}](2z)$ avec $\#A \leq 2$. Pour les calculer P. Gaudry [36] et R. Cosset [18] proposent les formules de dédoublement suivantes :

$$4\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](2z)\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]\theta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right]^2 = \sum_{\alpha\beta\in Z(2)} \exp\left(-4i\pi^t a\beta\right)\theta\left[\begin{smallmatrix} a+\alpha \\ b+\beta \end{smallmatrix}\right](z)^2\theta\left[\begin{smallmatrix} \alpha \\ \beta \end{smallmatrix}\right](z)^2$$

$$4\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](2z)\theta\left[\begin{smallmatrix} a \\ 0 \end{smallmatrix}\right]\theta\left[\begin{smallmatrix} 0 \\ b \end{smallmatrix}\right]\theta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right]^2 = \sum_{\alpha\beta\in Z(2)} \exp\left(-4i\pi^t a\beta\right)\theta\left[\begin{smallmatrix} a+\alpha \\ b+\beta \end{smallmatrix}\right](z)\theta\left[\begin{smallmatrix} a+\alpha \\ \beta \end{smallmatrix}\right]\theta\left[\begin{smallmatrix} \alpha \\ b+\beta \end{smallmatrix}\right](z)\theta\left[\begin{smallmatrix} \alpha \\ \beta \end{smallmatrix}\right].$$

La première pour les paires et la seconde pour les impaires.
Par suite pour un diviseur générique $D = \langle u, v\rangle$ on arrive à exprimer les termes de droite de ces formules en fonction de $Y_{l,m}$, Y et $u(a_i)$.