Géométrie et arithmétique explicites des variétés abéliennes et applications à la cryptographie

Thèse de doctorat spécialité Mathématiques rédigée et présentée par

CHRISTOPHE ARENE

pour obtenir le grade de

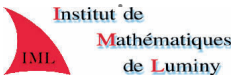
Docteur de l'université de la Méditerrannée, Aix-Marseille 2

Membres du jury

Sylvain DUQUESNE	(Prof. Univ. Rennes 1)	**rapporteur**
Florian HESS	(Prof. Univ. Oldenburg)	**rapporteur**
Pierrick GAUDRY	(DR CNRS – LORIA)	
Laurent IMBERT	(CR CNRS – LIRMM)	
David KOHEL	(Prof. Univ. Aix-Marseille 2)	**directeur**
Gilles LACHAUD	(Prof. Émerite Univ. Aix-Marseille 2)	
Christophe RITZENTHALER	(MC Univ. Aix-Marseille 2)	**codirecteur**

Soutenue publiquement le mardi 27 septembre 2011 à 15h00
à l'Institut de Mathématiques de Luminy

IML - UMR 6206,
Campus de Luminy, Case 907,
13288 Marseille Cedex 9



Remerciements

L'écriture de cette thèse n'aurait pu être envisagée sans l'obtention d'un financement qui, les personnes présentes alors se rappelleront, fut incertaine, longue et douloureuse. Je tiens donc tout naturellement à exprimer ma gratitude envers Jacques Derrien et Hamish Short ainsi que Laurent Regnier, Gilles Lachaud, David Kohel et Christophe Ritzenthaler pour les efforts qu'ils ont fournis m'ayant permis d'obtenir une bourse de thèse. Je remercie également le Fond Axa pour la Recherche d'avoir été mon mécène et de m'avoir laissé la liberté d'action ayant abouti à ce mémoire.

J'ai eu le plaisir de faire partie du projet CHIC, regroupant les équipes de Rennes (IRMAR), Nancy (LORIA) et Marseille (IML) durant ses deux premières années. Ce fut l'occasion de rencontrer des mathématiciens brillants qui se sont révélés être d'une compagnie agréable et joyeuse. Ces rencontres furent mathématiquement fructueuses, notamment lors d'une invitation par l'équipe CARAMEL du Loria dont je remercie les membres pour leur accueil chaleureux. En particulier Pierrrick Gaudry, Emmanuel Thomé, Jérémie Detrey, Pascal Molin, Răzvan Bărbulescu, Nicolas Estibals, et Romain Cosset avec qui j'ai eu l'enthousiasme de travailler. Je remercie également Damien Robert, Luca De Feo, Gaëtan Bisson, Laurent Imbert, Marc Perret, Ben Smith, Alexey Zykin et encore une fois Pierrick Gaudry et Emmanuel Thomé, entre autres, pour leur grande amabilité et les discussions (plus ou moins) mathématiques que nous avons eues lors de nos diverses rencontres.

Je remercie Pierrick Gaudry, Laurent Imbert et Gilles Lachaud d'avoir accepté de faire partie de mon jury, et particulièrement Sylvain Duquesne et Florian Hess pour avoir relu cette thèse avec beaucoup de rigueur et pour les commentaires qui en ont suivi.

Le contexte scientifique de l'IML a été très important pour moi, j'en profite donc pour remercier Gilles Lachaud pour sa direction du laboratoire pendant mon passage, ainsi qu'Aurélia et Corinne pour leur aide administrative et Jean-Bruno pour son attention à nous fournir du matériel informatique de qualité. La présence du CIRM à quelques centaines de mètres du laboratoire a été une source inépuisable d'informations, et je remercie les documentalistes pour leur aide et la gestion de la bibliothèque.

Je suis fier d'avoir été encadré par David Kohel, dont les longues discussions ont été imprégnées de sa grande maîtrise des objets mathématiques et de son intuition dans leur utilisation pratique, et resteront empreintes d'une touche de mystère ; et par Christophe Ritzenthaler qui reste pour moi un exemple de travail, de perspicacité et de sens moral, toujours près à me répéter les (nombreuses) explications que je ne comprenais pas et qui a su me donner du coeur à l'ouvrage. Je suis reconnaissant à tous deux.

Ces trois années de recherche auraient été bien moroses sans les membres de l'équipe ATI qui sont finalement devenus bien plus que des collègues de travail — et grâce à qui je peux rédiger ces lignes confortablement installé dans mon lit :-). Je commence par remercier les

nombreux (actuels et ex) thésards : tout d'abord Tammam, Hamish et le Cracken (que tout le monde reconnaîtra) avec qui j'ai eu le plaisir de partager le bureau 114, Stéphanie, Julia, Virgile, Yih-Dar, Marc et Florian, et parmi les permanents, Yves, Stéphane, François et encore une fois Christophe pour les repas partagés, les soirées organisées et les séjours au ski ! ! Je remercie spécialement Virgile d'avoir été un ami proche depuis plus de deux ans et pour ses imitations qui, je dois bien le dire (car je serai certainement le seul), étaient hilarantes (à part Gollum et le "chanteur" dont je tairai le nom). Je n'oublie pas non plus Milla pour sa jovialité et Cécile qui a fait un rapide mais mémorable passage parmi nous.

Je tiens à remercier les membres du Dojo Makoto que j'ai eu le grand plaisir de connaître ces deux dernières années, notamment Delphine, Melek, Maude, Chloé, Nico, et bien entendu Fabrice, Laurent, Alexandra et André. Pratiquer dans ce Dojo m'a permis de découvrir un art martial fascinant, de me vider la tête quelques heures par semaine et a été aussi une source de nombreux moments de joies (malgré quelques muscles mis à mal, mais cela en valait la peine !).

Je termine enfin en remerciant tous les membres de ma famille qui m'ont soutenu tout au long de mes études. Je remercie également Magali pour avoir été à l'origine de mon engagement dans de si longues études, et Bélénos et Toutatis qui ont, malgré tous leurs miaulement, été très réconfortants.

À mon père.

Table des matières

Introduction générale

En 1976, Diffie et Hellman [DH76] ont posé les bases de la cryptographie asymétrique. Le but est, d'une part, de permettre une communication privée entre deux personnes sur un canal pouvant être espionné, ceci sans échange préalable d'une clé secrète, mais aussi, par exemple, d'authentifier l'origine du message ou de le signer. De tels systèmes sont basés sur l'utilisation de *fonctions à sens unique*, c'est à dire des fonctions faciles à calculer mais difficiles à inverser.

Du point de vue cryptologique, la difficulté d'un problème mathématique est évaluée par la complexité du meilleur algorithme permettant de le résoudre. On distingue trois classes de complexité, par ordre croissant de difficulté, selon que la complexité de l'algorithme est polynomiale, sous-exponentielle ou exponentielle en la taille de l'entrée. En effet, pour avoir un niveau de sécurité satisfaisant, il faudra prendre des entrées de tailles d'autant plus grande que la fonction servant à chiffrer soit facile à inverser.

Divers problèmes mathématiques ont menés à la création de protocoles cryptographiques asymétriques : générer un vecteur de petite norme dans un réseau de grande dimension (NTRU, apparemment résistant à la cryptographie quantique), factoriser de grands entiers (RSA, actuellement largement utilisé), ... Le problème qui nous intéresse est le problème du *logarithme discret*. Celui-ci consiste, étant donnés un groupe G noté multiplicativement, deux éléments $g \in G$ et $m \in \langle g \rangle$, à déterminer un exposant x tel que $m = g^x$. El Gamal proposa en 1985 le premier protocole basé sur ce problème en considérant le groupe multiplicatif d'un corps fini [ElG85]. Miller [Mil86a] et Koblitz [Kob87] introduisirent indépendamment en cryptographie les groupes de points sur certaines variétés algébriques projectives : les *variétés abéliennes*, et notamment sur les courbes elliptiques et les jacobiennes de courbes définies sur un corps fini. De plus, l'existence de couplages sur ces groupes de points a également été source de beaucoup d'applications tant cryptanalytiques (réduction du logarithme discret sur le groupe multiplicatif d'un corps fini) que cryptographiques (cryptographie basée sur l'identité, signature courte).

Depuis plus de trois décennies de recherche, les algorithmes de calcul ont été amélioré et le choix de "bonnes" courbes s'est affiné au gré de diverses attaques. Aujourd'hui, on ne connaît pas, pour les courbes de petit genre, d'attaque plus efficace que l'attaque générique (méthode ρ de Pollard notamment) sur les courbes utilisées, qui est de complexité exponentielle. Ceci rend l'utilisation de courbes de genre 1 ou 2 très attractives. Au contraire, on dispose d'algorithmes sous-exponentiels pour attaquer les autres cryptosystèmes précités.

Mais malgré l'absence d'algorithmes efficaces pour attaquer ces protocoles, les attaques dites *par canaux cachés*, des attaques physiques, doivent être prises en compte, notamment pour sécuriser l'utilisation de systèmes embarqués tels que dans les cartes à puce. En effet, le calcul d'une puissance est basé sur l'idée de l'algorithme d'exponentiation rapide, fait par multiplications et carrés successifs. Or, dans les modèles les plus utilisés, ces deux opérations sont faites par des formules différentes, et la fuite de données telles que la consommation de courant pendant ce processus permet de distinguer ces deux types d'opérations et de retrouver la clé utilisée de manière statistique. Ces attaques, dites passives, peuvent être contournées en ajoutant des opérations superflues limitant les différences de coûts entre une multiplication et une élévation

au carré (algorithme de type double-and-add). Mais des attaques par injection de fautes (par exemple utiliser un laser pour affecter une opération à un moment précis), dites actives, peuvent identifier ces opérations.

Le sujet de cette thèse est l'étude des formules décrivant l'addition de points sur des variétés abéliennes, et plus spécifiquement dans les cas cryptographiquement intéressants, à savoir sur courbes elliptiques ou sur la jacobienne de courbes hyperelliptiques de genre 2. Ces formules dépendent directement de la représentation des points que nous nous donnons, *i.e.* d'un plongement projectif de la variété abélienne. Nous nous intéresserons particulièrement aux formules définies pour tous leurs points $\Bbbk$-rationnels. Cette propriété permet de se prémunir contre les attaques par canaux cachés et est obtenue par la manipulation de concepts mathématiques très intéressants.

Le point de départ de cette étude est un article d'Edwards [Edw07]. Il y étudie une famille de courbes de genre 1. Nous commençons, dans la première partie, par nous concentrer sur ce modèle. Nous étudions les formules d'addition de ses points, notamment la possibilité que celles-ci soient définies pour tous points $\Bbbk$-rationnels, donnons des formules explicite efficaces pour le calcul du couplage de Tate réduit sur celle-ci, et générons des courbes d'Edwards, dédiées au calcul de couplages, de taille respectant les standards cryptographiques.

La second partie de cette thèse prolonge un article de Lange et Ruppert [LR85] et deux articles qui le suivirent, l'un aussi de Lange et Ruppert [LR87], l'autre de Bosma et Lenstra [BL95]. Les auteurs y étudient l'existence d'ensembles *complets* de lois d'addition, d'abord sur une variété abélienne en général, puis plus spécifiquement sur le modèle de Weierstraß des courbes elliptiques. En plus de l'aspect géométrique de la complétude d'ensembles de lois d'addition considérée par les auteurs précités, nous nous penchons également sur l'aspect arithmétique de la complétude d'une loi d'addition. Cette partie comporte trois résultats importants. Concernant l'aspect géométrique, nous démontrons que tout ensemble complet de lois d'addition sur une variété de dimension g contient au moins $g + 1$ lois. Ceci généralise un résultat de Bosma et Lenstra dans le cas du modèle de Weierstraß d'une courbe elliptique. Pour l'aspect arithmétique, nous démontrons l'existence d'une seule loi permettant d'additionner les points $\Bbbk$-rationnels d'une variété abélienne, sous l'hypothèse que le groupe de Galois absolu de $\Bbbk$ soit infini. En particulier nous démontrons que c'est le cas, sur corps finis, pour le modèle de Weierstraß d'une courbe elliptique et pour le plongement usuel dans $\mathbb{P}^{15}$ de la jacobienne d'une courbe de genre 2. Nous donnons pour ce dernier les premières formules explicites d'une loi d'addition $\mathbb{F}_q$-complète, pour q suffisamment grand.

Première partie

Calcul rapide du couplage de Tate réduit sur les courbes d'Edwards tordues

La première partie de cette thèse porte sur une façon efficace de calculer le couplage de Tate réduit sur une courbe d'Edwards tordue. Elle présente d'une part les résultats obtenus durant mon stage de Master [Are08] et d'autre part les travaux qui en ont découlés avec Lange, Naehrig et Ritzenthaler [ALNR10].

Ces travaux ont porté sur l'étude des courbes d'Edwards. Plus précisément, nous avons commencé par déterminer leur lien avec le modèle canonique dans $\mathbb{P}^3$ d'une courbe elliptique, puis nous avons clarifié l'origine de la loi d'addition explicitée par Edwards [Edw07] en la déduisant de formules d'addition des fonctions thêta. Ensuite nous en avons donné une interprétation géométrique. L'utilisation de ce dernier point pour le calcul du couplage de Tate réduit a permis, après plusieurs améliorations, d'obtenir des formules explicites plus efficaces que celles connues dans la plupart des cas pour une courbe elliptique donnée sous forme de Weierstraß.

Les Chapitres 1 et 3 sont des rappels respectivement sur les courbes elliptiques et les couplages. Ils permettent de fixer les notions et notations. Le Chapitre 2 présente les résultats sur les courbes d'Edwards, et plus généralement leurs tordues, tentant de faire apparaître l'évolution des idées sur ce sujet. Nous rappelons dans la première section du Chapitre 4 la méthode de construction de courbes elliptiques basée sur la multiplication complexe (CM), que nous appliquons dans la seconde section de ce chapitre à la construction de courbes d'Edwards *pairing-friendly* dont les paramètres sont de taille cryptographique.

Chapitre 1

Rappels sur les courbes elliptiques

Ce chapitre sert à introduire les notations et résultats de base dont nous nous servirons dans le reste de cette partie. Celui-ci est composé de trois parties, les principaux objets décrits dans la première sont les diviseurs sur une courbe. Dans la seconde nous abordons les courbes elliptiques puis finissons par les fonctions thêta en genre 1, notamment les relations de Riemann les liant.

1.1 Courbes, diviseurs et théorème de Riemann-Roch

Les résultats de cette section peuvent être retrouvés dans [Sil92, Chapter II]. Dans toute cette thèse, le corps de base $\Bbbk$ est supposé parfait. Soit $C/\Bbbk$ une courbe sur un corps $\Bbbk$. Lorsque l'on parle de points sur C on sous-entend points *géométriques*, *i.e.* définis sur $\overline{\Bbbk}$. La courbe C étant définie sur $\Bbbk$, le groupe de Galois absolu $\mathrm{Gal}\left(\overline{\Bbbk}/\Bbbk\right)$ agit sur ses points. Un point $P \in C$ sera dit $\Bbbk$-*rationnel* s'il est fixe sous cette action, *i.e.* $P^\sigma = P$ pour tout $\sigma \in \mathrm{Gal}\left(\overline{\Bbbk}/\Bbbk\right)$. Nous supposons dans toute cette thèse que C possède un point $\Bbbk$-rationnel. Nous définissons $\mathrm{Div}(C)$ le groupe libre engendré par les points de C et appelons *diviseurs* ses éléments. Un diviseur $D \in \mathrm{Div}(C)$ est noté

$$D = \sum_{P \in C} n_P(P),$$

les n_P étant presque tous nuls et faisant attention aux parenthèses autours des points pour distinguer, dans le cas elliptique, un diviseur et la somme des points. On dit qu'un diviseur $D = \sum n_P(P) \in \mathrm{Div}(C)$ est *effectif* si $n_P \geq 0$ pour tout $P \in C$, on note alors $D \geq 0$. On définit une relation d'ordre partielle sur $\mathrm{Div}(C)$ comme suit : soient $D_1, D_2 \in \mathrm{Div}(C)$, on a $D_1 \geq D_2$ si $D_1 - D_2$ est effectif. Le *support* d'un diviseur est l'ensemble des points de poids non nul

$$\mathrm{Supp}(D) := \{P \in C, n_P \neq 0\}.$$

On appelle *degré* d'un diviseur l'entier

$$\deg(D) := \sum_{P \in C} n_P.$$

L'application $\deg : \mathrm{Div}(C) \to \mathbb{Z}$ est un morphisme de groupes et son noyau, le sous-groupe des diviseurs de degré 0, est noté

$$\mathrm{Div}^0(C) := \{D \in \mathrm{Div}(C), \deg(D) = 0\}.$$

L'action de $\mathrm{Gal}\left(\overline{\Bbbk}/\Bbbk\right)$ sur les points de C induit une action sur $\mathrm{Div}(C)$, respectivement $\mathrm{Div}^0(C)$. Les diviseurs fixés par cette action, *i.e.* tels que $D^\sigma = D$ pour tout $\sigma \in \mathrm{Gal}\left(\overline{\Bbbk}/\Bbbk\right)$, sont dits $\Bbbk$-*rationnels* et forment un groupe noté $\mathrm{Div}_\Bbbk(C)$, respectivement $\mathrm{Div}^0_\Bbbk(C)$.

Remarque 1.1.1. *La subtilité entre les notions de rationalité pour un point et un diviseur vient du fait que l'on puisse avoir un diviseur* $\Bbbk$*-rationnel dont aucun point du support ne soit* $\Bbbk$*-rationnel ; l'existence de tels diviseurs sera d'ailleurs centrale dans la seconde partie de cette thèse. Par exemple* $\big((i:1)\big)+\big((-i:1)\big)\in \mathrm{Div}_{\mathbb{R}}\left(\mathbb{P}^1(\mathbb{C})\right)$ *bien que ni* $(i:1)$ *ni* $(-i:1)$ *ne soient* $\mathbb{R}$*-rationnels.*

À une fonction $f\in\overline{\Bbbk}(C)^*$ on associe le diviseur

$$\mathrm{div}(f)=\sum_{P\in C}\mathrm{ord}_P(f)(P)\in\mathrm{Div}(C).$$

Un tel diviseur est dit *principal* et on dénote par $\mathrm{Princ}(C)$ le sous-groupe des diviseurs principaux de C. Deux diviseurs $D_1,D_2\in\mathrm{Div}(C)$ sont dits *linéairement équivalents* si $D_1-D_2\in\mathrm{Princ}(C)$, on le note $D_1\sim D_2$. Le groupe quotient $\mathrm{Pic}(C)=\mathrm{Div}(C)/\mathrm{Princ}(C)$ est appelé le *groupe de Picard* de C. Aussi tout diviseur principal est de degré 0, on définit ainsi

$$\mathrm{Pic}^0(C)=\mathrm{Div}^0(C)\,/\,\mathrm{Princ}(C)$$

appelé la *jacobienne* de C. L'*espace des formes différentielles* sur C, noté Ω_C, est le $\overline{\Bbbk}(C)$-espace vectoriel engendré par les objets df avec $f\in\overline{\Bbbk}(C)$ satisfaisant les propriétés

- Pour tout $f,g\in\overline{\Bbbk}(C)$, $d\,(f+g)=df+dg$,
- Pour tout $f,g\in\overline{\Bbbk}(C)$, $d\,(fg)=f\,dg+g\,df$,
- Pour tout $a\in\overline{\Bbbk}$, $da=0$.

À toute forme différentielle $\omega\in\Omega_C$ on associe le diviseur

$$\mathrm{div}(\omega)=\sum_{P\in C}\mathrm{ord}_P(\omega)(P)\in\mathrm{Div}(C).$$

Si $\omega_1,\omega_2\in\Omega_C$ sont non nulles alors il existe $f\in\overline{\Bbbk}(C)^*$ telle que $\omega_1=f\omega_2$, ainsi

$$\mathrm{div}(\omega_1)\sim\mathrm{div}(\omega_2).$$

Par abus de langage on définit le *diviseur canonique* de C, noté κ_C, comme étant la classe de $\mathrm{div}(\omega)$ dans $\mathrm{Pic}(C)$ pour $\omega\in\Omega_C$. On a

$$\deg(\kappa_C)=2g-2.$$

On dira "un" diviseur canonique en parlant d'un représentant du diviseur canonique.

Définition 1.1.2. *Soient* $C/\Bbbk$ *une courbe lisse et* $D\in\mathrm{Div}(C)$*. L'ensemble de fonctions*

$$L(D)=\left\{f\in\overline{\Bbbk}(C)^*,\mathrm{div}(f)\geq -D\right\}\cup\{0\}$$

est un $\overline{\Bbbk}$*-espace vectoriel de dimension finie notée* $l(D)$*. On l'appelle l'*espace de Riemann-Roch *associé à* D*.*

On déduit de la Proposition 5.1.5 page 55 que si D est un diviseur $\Bbbk$-rationnel sur C alors l'espace $L(D)$ possède une base formée de fonctions dans $\Bbbk(C)$.

Théorème 1.1.3 (Riemann-Roch)**.** *Soient* C *une courbe lisse et* κ_C *un diviseur canonique sur* C*. Il existe un entier* $g\geq 0$*, appelé* genre *de* C*, tel que pour tout diviseur* $D\in\mathrm{Div}(C)$

$$l(D)-l\,(\kappa_C-D)=\deg(D)-g+1.$$

Si $\deg(D)>2g-2$ *alors* $l(D)=\deg(D)-g+1$.

1.2 Courbes elliptiques

Cette section a pour but d'introduire les courbes elliptiques d'une part, l'équation de Weierstraß, la structure de groupe dont elles sont naturellement munies ; et la structure de leur anneau d'endomorphisme d'autre part, qui sera exploitée dans le Chapitre 4 pour la construction de courbes elliptiques par multiplication complexe. Pour une démonstration des résultats suivants, nous renvoyons le lecteur à [Sil92, Chapters III, V] et [CFA+06, Chapter IV].

1.2.1 Équations et invariants

Définition 1.2.1. *Une courbe elliptique sur* $\Bbbk$ *est la donnée d'une courbe projective, lisse, absolument irréductible de genre* 1 *et d'un point* $\Bbbk$*-rationnel noté* O*.*

Soit $E/\Bbbk$ une courbe elliptique. En considérant les espaces de Riemann-Roch $L(nO)$ pour $n = 2, 3, 6$, le théorème de Riemann-Roch affirme qu'il existe $x, y \in \Bbbk(E)$ telles que $\{1, x\}$ soit une base de $L(2O)$, $\{1, x, y\}$ soit une base de $L(3O)$ et $\{1, y, y^2, xy, x, x^2, x^3\}$ soit liée. On en déduit, après normalisation, qu'il existe $a_1, a_2, a_3, a_4, a_6 \in \Bbbk$ tels que

$$y^2 + (a_1x + a_3)\, y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.1}$$

appelée *équation de Weierstraß* de E. Aussi le point $\Bbbk$-rationnel O correspond au point à l'infini $(0 : 1 : 0)$.

Nous n'abordons pas le cas de la caractéristique 2 puisqu'il ne sera pas utile dans notre étude des courbes d'Edwards. Selon que la caractéristique de $\Bbbk$ est 3 ou première avec 6, on applique des transformations linéaires pour obtenir une *équation de Weierstraß réduite* de E. La transformation

$$(x, y) \mapsto \left(x, y + \frac{a_1x + a_3}{2}\right)$$

est un $\Bbbk$-isomorphisme entre la courbe elliptique d'équation (1.1) et celle d'équation

$$y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4},$$

avec $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$ et $b_6 = a_3^2 + 4a_6$.
Si de plus la caractéristique de $\Bbbk$ est différente de 3 on applique à l'équation ci-dessus la transformation

$$(x, y) \mapsto \left(x + \frac{b_2}{12}, y\right),$$

c'est un $\Bbbk$-isomorphisme avec la courbe elliptique d'équation

$$y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864},$$

avec $c_4 = b_2^2 - 24b_4$ et $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$.

Définition 1.2.2. *Soit* $E/\Bbbk$ *une courbe elliptique donnée par une équation de Weierstraß. On définit le* discriminant $\Delta(E)$ *et le* j-invariant $j(E)$ *de l'équation comme suit*

$$\Delta(E) = \frac{c_4^3 - c_6^2}{1728},$$
$$j(E) = \frac{c_4^3}{\Delta(E)}.$$

Le même symbole Δ est utilisé pour le discriminant et pour la diagonale d'une courbe elliptique car cette notation est largement répandue et l'ambiguïté est levée par le contexte.

Remarque 1.2.3. *La division par $\Delta(E)$ dans la définition du j-invariant n'est pas gênante puisque $\Delta(E) = 0$ si et seulement si la courbe définie par l'équation de Weierstraß associée est singulière. Elle ne correspond alors pas à l'équation d'une courbe elliptique.*

Proposition 1.2.4. *Deux courbes elliptiques sous forme de Weierstraß sont isomorphes si et seulement si elles ont le même j-invariant.*

Proposition 1.2.5. *Soit $j \in \Bbbk$, il existe une courbe elliptique E définie sur $\Bbbk(j)$ telle que $j(E) = j$. De plus une telle courbe elliptique est donnée par l'équation de Weierstraß réduite $y^2 = x^3 + a_4x + a_6$ suivante :*

1. *si $j = 0$, $a_4 = 0, a_6 \in \Bbbk(j)^*$,*
2. *si $j = 1728$, $a_4 \in \Bbbk(j)^*, a_6 = 0$,*
3. *si $j \neq 0, 1728$, $-a_4 = a_6 = \frac{27j}{4(j-1728)}$.*

1.2.2 La loi de groupe

On sait depuis Gauss additionner deux points sur une courbe elliptique. Prenant le point O pour élément neutre, si trois points (comptés avec multiplicité) sont alignés alors leur somme est nulle. En particulier l'addition est commutative et le symétrique d'un point affine $P = (x, y)$ est $\overline{P} = (x, -y)$. Cette définition géométrique du morphisme de groupe est simple à énoncer, mais il devient moins commode de chercher à le décrire par des formules. Partant de deux points $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, on obtient les formules décrivant leur addition comme suit : soit $y = \lambda x + \mu$ l'équation de la droite passant par P_1 et P_2. Notons $(x_3, y_3) := (x_1, y_1) + (x_2, y_2)$, on a les équations

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \\ y_3 &= -(\lambda + a_1)x_3 - \nu - a_3. \end{aligned} \tag{1.2}$$

Supposons que le couple (P_1, P_2) n'est pas dans un des ensembles suivants

$$E \times \{O\}, \{O\} \times E, \Delta, \nabla,$$

où $\Delta = \big\{(P, P), P \in E\big\}$ est la diagonale dans $E \times E$ et $\nabla = \big\{(P, -P), P \in E\big\}$ est l'antidiagonale. Les équations (1.2) sont vérifiées avec

$$\begin{aligned} \lambda &= \frac{y_2 - y_1}{x_2 - x_1}, \\ \nu &= \frac{y_1x_2 - y_2x_1}{x_2 - x_1}. \end{aligned}$$

Dans le cas où $P_1 = P_2$ on a, en considérant la tangente en P_1,

$$\begin{aligned} \lambda &= \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \\ \nu &= \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}. \end{aligned}$$

Finalement, si $P_2 = \overline{P_1}$ alors $P_1 + P_2 = O$ et pour tout point $P \in E\big(\overline{\Bbbk}\big)$, $P + O = O + P = P$.

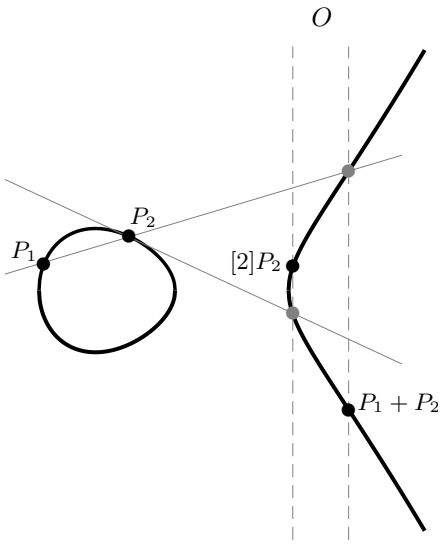


FIGURE 1 – Interprétation géométrique de l'addition sur une courbe elliptique réelle.

La proposition suivante montre qu'il existe un isomorphisme de groupes entre $\mathrm{Pic}^0(E)$ et E.

Proposition 1.2.6. *Soient E une courbe elliptique, $0 \neq D \in \mathrm{Div}^0(E)$. Il existe un unique $P \in E$ tel que $D \sim (P) - (O)$, de plus cette application*

$$\begin{array}{rcl} \mathrm{Pic}^0(E) & \to & E, \\ D & \mapsto & P \end{array}$$

est un isomorphisme de groupes.

Corollaire 1.2.7. *Soient E une courbe elliptique, $D = \sum n_P(P) \in \mathrm{Div}^0(E)$.*

$$D \text{ est principal} \iff \sum [n_P]P = O \text{ sur } E.$$

1.2.3 Isogénies et anneau d'endomorphismes

Définition 1.2.8. *Soient $E_1, E_2/\Bbbk$ deux courbes elliptiques. Une* isogénie $\phi : E_1 \to E_2$ *est un morphisme de courbes elliptiques,* i.e. *un morphisme de courbes (algébriques projectives) et un morphisme de groupe, fini et surjectif.*

E_1 et E_2 sont dites isogènes *s'il existe une isogénie $\phi : E_1 \to E_2$. On note alors $E_1 \sim E_2$.*

On peut se restreindre, seulement dans le cas d'une isogénie entre deux courbes elliptiques, à demander à ce que ϕ soit un morphisme de courbes tel que $\phi(O_{E_1}) = O_{E_2}$ et qui est non constant. Aussi, en tant que morphisme de courbes, ϕ induit un morphisme de corps $\phi^* : \Bbbk(E_2) \to \Bbbk(E_1)$ qui définit son *degré* par $\deg(\phi) = \big[\Bbbk(E_1) : \phi^*\big(\Bbbk(E_2)\big)\big]$.

Définition 1.2.9. *Soient E_1, E_2 deux courbes elliptiques. On définit*

$$\mathrm{Hom}(E_1, E_2) = \left\{ \textit{isogénies } \phi : E_1 \to E_2 \textit{ définies sur } \overline{\Bbbk} \right\},$$

c'est un groupe pour l'addition $\phi + \psi(P) = \phi(P) + \psi(P)$, et, si $E_1 = E_2 = E$, on définit

$$\mathrm{End}(E) := \mathrm{Hom}(E, E),$$

*qui devient un anneau en le munissant de la composition. On l'appelle l'*anneau d'endomorphismes *de E. Les endomorphismes inversibles sont appelés* automorphismes.

Exemple 1.2.10. *Soit $m \in \mathbb{Z}$, $m \neq 0$, la* multiplication par m, *$[m] : E \to E$, est une isogénie. On note $E[m]$ son noyau, ses éléments sont appelés les* points de m-torsion. *Ces points peuvent ne pas être définis sur $\Bbbk$.*

L'anneau d'endomorphismes $\mathrm{End}(E)$ est un anneau intègre de caractéristique 0. En particulier $\mathbb{Z}$ se plonge dans $\mathrm{End}(E)$ par $m \mapsto [m]$. Nous décrivons dans l'exemple suivant un autre endomorphisme particulier en caractéristique positive.

Exemple 1.2.11. *Soient $\Bbbk$ un corps de caractéristique positive p, $E/\Bbbk$ une courbe elliptique et q une puissance de p. On définit $E^{(q)}/\Bbbk$ la courbe associée à l'équation donnée par l'équation de Weierstraß de E dont les coefficients ont été élevés à la puissance q. On définit alors le morphisme*

$$\begin{aligned} \phi_q : E &\to E^{(q)} \\ (x, y) &\mapsto (x^q, y^q)\,. \end{aligned}$$

*On vérifie $\Delta\big(E^{(q)}\big) = \Delta(E)^q$, donc $E^{(q)}$ est bien une courbe elliptique, et $j\left(E^{(q)}\right) = j(E)^q$. Si $\Bbbk = \mathbb{F}_q$ alors $E = E^{(q)}$ et $\phi_q \in \mathrm{End}(E)$ est appelé l'*endomorphisme de Frobenius.

Proposition 1.2.12. *Soit $\phi : E_1 \to E_2$ une isogénie de degré m. Il existe une unique isgénie*

$$\widehat{\phi} : E_2 \to E_1$$

telle que

$$\widehat{\phi} \circ \phi = [m]_{E_1}.$$

En particulier la relation "être isogènes" est une relation d'équivalence. L'isogénie $\widehat{\phi}$ est appelée *isogénie duale* de ϕ. Si $\deg(\phi) = m$ alors $\deg\left(\widehat{\phi}\right) = m$ et $\phi \circ \widehat{\phi} = [m]_{E_2}$.

Cette proposition permet de décrire la structure de m-torsion sur une courbe elliptique.

Corollaire 1.2.13. *Soient $E/\Bbbk$ une courbe elliptique et $m \in \mathbb{Z} \setminus \{0\}$.*

1. $\deg\big([m]\big) = m^2$.
2. *Si* $\mathrm{car}(\Bbbk) = 0$ *ou* $\mathrm{car}(\Bbbk) \nmid m$, *alors*

$$E\,[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

3. *Si* $\mathrm{car}(\Bbbk) = p$, *alors*

$$E\big[p^r\big] \cong \begin{cases} \{0\},\ \forall r \geq 1, \\ \textit{ou} \\ \mathbb{Z}/p^r\mathbb{Z},\ \forall r \geq 1. \end{cases}$$

Définition 1.2.14. *Si le corps $\Bbbk$ est de caractéristique p positive, on dit qu'une courbe elliptique $E/\Bbbk$ est* ordinaire *si $E[p] \cong \mathbb{Z}/p\mathbb{Z}$, elle est dite* supersingulière *sinon.*

Pour terminer cette sous-section nous nous intéressons aux différentes structures d'anneau qui peuvent apparaître pour $\mathrm{End}(E)$.

Proposition 1.2.15. *L'anneau d'endomorphismes d'une courbe elliptique est soit $\mathbb{Z}$, soit un ordre maximal dans un corps quadratique imaginaire, soit un ordre dans une algèbre de quaternions.*

Définition 1.2.16. *Si* $\mathrm{End}(E)$ *contient strictement $\mathbb{Z}$ alors on dit que la courbe elliptique E est à* multiplication complexe.

Une méthode basée sur la multiplication complexe (méthode CM) permet de construire des courbes elliptiques sur corps finis avec un nombre déterminé de points rationnels. Nous reviendrons sur cette méthode dans le Chapitre 4.

1.2.4 Courbes elliptiques sur corps finis

Soit $\Bbbk = \mathbb{F}_q$ un corps fini de caractéristique p. Nous considérons une courbe elliptique $E/\mathbb{F}_q$ et commençons par nous intéresser au nombre de points $\mathbb{F}_q$-rationnels. Le théorème suivant fournit une borne très fine de $|E(\mathbb{F}_q)|$, il repose sur le fait qu'un point $P \in E$ est $\mathbb{F}_q$-rationnel si et seulement si $\phi_q(P) = P$, où ϕ_q est l'endomorphisme de Frobenius sur $E/\mathbb{F}_q$ (cf Exemple 1.2.11).

Théorème 1.2.17 (Hasse-Weil)**.** *Soit $E/\mathbb{F}_q$ une courbe elliptique. On a*

$$\left|q + 1 - |E(\mathbb{F}_q)|\right| \leq 2\sqrt{q}.$$

L'entier $t = q + 1 - |E(\mathbb{F}_q)|$ est la trace de l'endomorphisme de Frobenius. On abrège en l'appelant la *trace* de E.

Nous avons vu dans la section précédente que deux cas peuvent se produire concernant la p-torsion et l'anneau d'endomorphismes de E. Le théorème suivant montre l'analogie qui existe entre ces deux structures.

Théorème 1.2.18. *Soient q une puissance d'un nombre premier p et $E/\mathbb{F}_q$ une courbe elliptique. Les propositions suivantes sont équivalentes.*

1. *E est supersingulière.*
2. *Le sous-groupe de p-torsion est trivial : $E[p] = \{O\}$.*
3. *L'anneau $\mathrm{End}(E)$ est un ordre maximal dans une algèbre de quaternions.*
4. *La trace de l'endomorphisme de Frobenius est divisible par p.*

Remarque 1.2.19. *Toute courbe elliptique définie sur un corps fini est à multiplication complexe.*

On termine cette section en disant quelques mots sur un aspect cryptographique : le compte des opérations pour additionner deux points. Le lecteur peut retrouver une description détaillée des formules explicites des principaux modèles elliptiques en visitant le site [BL].

Les opérations arithmétiques qui interviennent dans le calcul de lois d'addition sont la multiplication, l'inversion, la multiplication par un paramètre de la courbe, l'élévation au carré et l'addition. Le coût en terme de temps de calculs de cette dernière étant négligeable face aux autres nous ne prenons pas en compte le nombre d'additions dans les formules explicites. Aussi le coût d'une inversion étant très supérieur aux autres coûts (la référence est de 100 multiplications pour une inversion sur le site cité ci-dessus), il devient alors très profitable de travailler en coordonnées projectives, ce qui nous laisse trois opérations à considérer.

Notation 1.2.20. *Nous utilisons les notations suivantes*

- $\mathbf{m}$ *: multiplication de deux coordonnées,*
- $\mathbf{s}$ *: élévation au carré d'une coordonnée,*
- $\mathbf{m_\alpha}$ *: multiplication d'une coordonnée par un paramètre α de la courbe.*

Nous considérons les courbes définies par une équations de Weiestraß réduite

$$y^2 = x^3 + a_4 x + a_6 \tag{1.3}$$

sur un corps fini premier $\mathbb{F}_p$, p étant suffisamment grand pour une utilisation cryptographique, a fortiori $p \neq 2, 3$. Il est plus avantageux de représenter les points dans un espace projectif pondéré satisfaisant la relation

$$(X : Y : Z) \sim (\lambda^2 X : \lambda^3 Y : \lambda Z).$$

Le point $(X : Y : Z)$ satisfaisant l'équation

$$Y^2 = X^3 + a_4 X Z^4 + a_6 Z^6$$

représente le point affine $(X/Z^2, Y/Z^3)$ vérifiant (1.3) si $Z \neq 0$, sinon le point $(1 : 1 : 0)$ représente le point à l'infini. On réduit également le nombre d'opérations en se plaçant dans des cas spéciaux, en particuliers les formules explicites dans le cas $a_4 = -3$ [BL, BL07a] nécessitent $11\mathbf{m} + 5\mathbf{s}$ pour une addition et $3\mathbf{m} + 5\mathbf{s}$ pour un doublement.

1.3 Fonctions thêta en genre 1

Commençons par introduire la fonction thêta de Riemann. Les formules rappelées dans cette partie sont tirées du livre de Mumford ([Mum83, Sections I.1-5]). Nous nous sommes restreint aux formules que nous utiliserons dans la Section 2.2. Dans le reste de ce chapitre, τ désigne un nombre complexe fixé dans le demi-plan supérieur $\Im z > 0$.

Définition 1.3.1. *On appelle* fonction thêta *la fonction complexe*

$$\vartheta(z, \tau) = \sum_{n \in \mathbb{Z}} e^{i\pi\left(n^2\tau + 2nz\right)}.$$

La fonction thêta étant holomorphe, elle ne peut pas être doublement périodique sans être constante. En revanche, la proposition suivante montre ce que l'on peut appeler une quasi-périodicité sur le réseau $\{1, \tau\}$.

Proposition 1.3.2. *La fonction ϑ est holomorphe sur $\mathbb{C}$, de plus :*

$$\begin{aligned} \vartheta(z+1, \tau) &= \vartheta(z, \tau), \\ \vartheta(z+\tau, \tau) &= e^{-i\pi(\tau+2z)}\vartheta(z, \tau). \end{aligned}$$

Pour mettre en valeurs les propriétés de la fonction thêta sur le réseau $\{1, \tau\}$, on introduit des translatés de cette fonction.

Définition 1.3.3. *Soient $\varepsilon, \varepsilon'$ dans $\{0, 1\}$ et τ un nombre complexe dans le demi-plan supérieur $\Im z > 0$. On appelle* fonction thêta de caractéristique $[\varepsilon, \varepsilon']$ *la fonction*

$$\vartheta_{\varepsilon\,\varepsilon'}(z, \tau) = \sum_{n \in \mathbb{Z}} e^{i\pi\left((n+\varepsilon/2)^2\tau + 2(n+\varepsilon/2)(z+\varepsilon'/2)\right)}.$$

En particulier, on a $\vartheta_{00} = \vartheta$.

Il faut prendre garde aux facteurs $1/2$ apparaissant dans la définition, nous prenons la convention de Mumford avec des caratéristiques entières puisque nous n'utiliserons que les quatres fonctions thêta définies ci-dessus.

Proposition 1.3.4. *On a les formules suivantes :*

$$\begin{array}{ll}
\vartheta_{00}(-z,\tau)=\vartheta_{00}(z,\tau), & \vartheta_{00}(z+1/2,\tau)=\vartheta_{01}(z,\tau),\\
\vartheta_{01}(-z,\tau)=\vartheta_{00}(z,\tau), & \vartheta_{01}(z+1/2,\tau)=\vartheta_{00}(z,\tau),\\
\vartheta_{10}(-z,\tau)=\vartheta_{00}(z,\tau), & \vartheta_{10}(z+1/2,\tau)=\vartheta_{11}(z,\tau),\\
\vartheta_{11}(-z,\tau)=-\vartheta_{00}(z,\tau), & \vartheta_{11}(z+1/2,\tau)=-\vartheta_{10}(z,\tau),
\end{array}$$

$$\begin{array}{l}
\vartheta_{00}(z+\tau/2,\tau)=e^{-i\pi(\tau/4+z)}\,\vartheta_{10}(z,\tau),\\
\vartheta_{01}(z+\tau/2,\tau)=-ie^{-i\pi(\tau/4+z)}\,\vartheta_{11}(z,\tau),\\
\vartheta_{10}(z+\tau/2,\tau)=e^{-i\pi(\tau/4+z)}\,\vartheta_{00}(z,\tau),\\
\vartheta_{11}(z+\tau/2,\tau)=-ie^{-i\pi(\tau/4+z)}\,\vartheta_{01}(z,\tau).
\end{array}$$

Remarque 1.3.5. *Ces formules illustrent les liens entre les différentes fonctions $\vartheta_{\varepsilon\varepsilon'}$. Elles permettent en outre d'obtenir, par des arguments combinatoires, les* formules thêta de Riemann *dont on déduit les* formules d'addition *des fonctions thêta. Il existe une multitude de telles formules, c'est pourquoi nous n'énonçons ci-dessous que celles qui nous seront utiles. Enfin, nous remarquons que ϑ_{11} étant impaire, $\vartheta_{11}(0)=0$ alors que les trois autres fonctions thêta ne s'annulent pas en zéro.*

Pour rendre les formules suivantes plus lisibles et puisqu'il n'y a pas d'ambiguité, nous omettons volontairement τ des arguments des fonction thêta.

Proposition 1.3.6. *Soient z_1, z_2 deux nombres complexes. On a*

$$\begin{array}{l}
\vartheta_{11}(z_1+z_2)\vartheta_{00}(z_1-z_2)\vartheta_{01}(0)\vartheta_{10}(0)=\vartheta_{00}(z_1)\vartheta_{11}(z_1)\vartheta_{01}(z_2)\vartheta_{10}(z_2)+\vartheta_{10}(z_1)\vartheta_{01}(z_1)\vartheta_{00}(z_2)\vartheta_{11}(z_2),\\
\vartheta_{01}(z_1+z_2)\vartheta_{00}(z_1-z_2)\vartheta_{01}(0)\vartheta_{00}(0)=\vartheta_{00}(z_1)\vartheta_{01}(z_1)\vartheta_{00}(z_2)\vartheta_{01}(z_2)+\vartheta_{10}(z_1)\vartheta_{11}(z_1)\vartheta_{10}(z_2)\vartheta_{11}(z_2),\\
\vartheta_{10}(z_1+z_2)\vartheta_{01}(z_1-z_2)\vartheta_{10}(0)\vartheta_{01}(0)=\vartheta_{10}(z_1)\vartheta_{01}(z_1)\vartheta_{10}(z_2)\vartheta_{01}(z_2)-\vartheta_{11}(z_1)\vartheta_{00}(z_1)\vartheta_{11}(z_2)\vartheta_{00}(z_2),\\
\vartheta_{00}(z_1+z_2)\vartheta_{01}(z_1-z_2)\vartheta_{00}(0)\vartheta_{01}(0)=\vartheta_{00}(z_1)\vartheta_{01}(z_1)\vartheta_{00}(z_2)\vartheta_{01}(z_2)-\vartheta_{10}(z_1)\vartheta_{11}(z_1)\vartheta_{10}(z_2)\vartheta_{11}(z_2).
\end{array}$$

Proposition 1.3.7. *On a*

$$\left\{\begin{array}{l}
\vartheta_{00}(0)^2\vartheta_{00}(z)^2=\vartheta_{01}(0)^2\vartheta_{01}(z)^2+\vartheta_{10}(0)^2\vartheta_{10}(z)^2,\\
\vartheta_{00}(0)^2\vartheta_{11}(z)^2=\vartheta_{10}(0)^2\vartheta_{01}(z)^2-\vartheta_{01}(0)^2\vartheta_{10}(z)^2.
\end{array}\right.$$

En prenant $z=0$ dans la première formule ci-dessus (la même opération dans la deuxième ne nous apporte rien), nous obtenons l'*identité de Jacobi* entre les *thêta constantes* :

$$\vartheta_{00}(0)^4=\vartheta_{01}(0)^4+\vartheta_{10}(0)^4.$$

Chapitre 2

Introduction aux courbes d'Edwards

Le but de ce chapitre est d'étudier l'objet qui suit

Définition 2.0.1. *Soient* $\Bbbk$ *un corps de caractéristique différente de* 2 *et* $d \in \Bbbk$ *avec* $d \neq 0, 1$. *On appelle* courbes d'Edwards *les courbes elliptiques définies par l'intersection dans* $\mathbb{P}^3$ *des deux quadriques suivantes*

$$\begin{cases} XY = ZT, \\ X^2 + Y^2 = Z^2 + dT^2. \end{cases} \tag{2.1}$$

Elles possèdent le point $\Bbbk$-rationnel $(0 : 1 : 1 : 0)$, ce sont donc des courbes elliptiques. L'addition de deux points $(X_3, Y_3, T_3, Z_3) = (X_1, Y_1, T_1, Z_1) + (X_2, Y_2, T_2, Z_2)$ est donnée par les équations suivantes

$$\begin{aligned} X_3 &= (X_1Y_2 + X_2Y_1)(Z_1Z_2 - dT_1T_2), \\ Y_3 &= (Y_1Y_2 - X_1X_2)(Z_1Z_2 + dT_1T_2), \\ T_3 &= (X_1Y_2 + X_2Y_1)(Y_1Y_2 - X_1X_2), \\ Z_3 &= (Z_1Z_2 - dT_1T_2)(Z_1Z_2 + dT_1T_2), \end{aligned} \tag{2.2}$$

Le lien avec la définition usuelle des courbes d'Edwards (Définition 2.1.1) apparaîtra à la fin de la Section 2.6. Dans la première section, nous rappelons la définition du modèle d'Edwards dans $\mathbb{P}^2$ et en donnons une paramétrisation par des fonctions thêta, dans le cas complexe, dans la seconde section. Dans les quatre sections suivantes, nous étudions de plus près leur loi d'addition usuelle et en donnons notamment une interprétation géométrique. La dernière section traite d'autres modèles elliptiques ayant une loi d'addition avec des propriétés comparables à celles sur les courbes d'Edwards.

2.1 Le début des courbes d'Edwards

Originellement Edwards a considéré les courbes d'équation

$$x^2 + y^2 = c^2\,(1 + x^2y^2), \qquad c^5 - c \neq 0, \tag{2.3}$$

sur un corps non binaire [Edw07]. Ce sont des quartiques possédant huit $\Bbbk$-automorphismes engendrés par les involutions $(x, y) \mapsto (-x, y)$, $(x, y) \mapsto (x, -y)$ et $(x, y) \mapsto (y, x)$. Elles sont singulières et leurs singularités sont les deux points à l'infini $\Omega_1 = (1 : 0 : 0)$ et $\Omega_2 = (0 : 1 : 0)$, qui sont de multiplicité 2. La désingularisée d'une courbe d'Edwards est donc une courbe elliptique. Son j-invariant s'exprime comme une fraction rationnelle en le paramètre d, toute courbe elliptique est ainsi birationnellement équivalente sur $\overline{\Bbbk}$ à une courbe d'Edwards. Concernant

l'addition de points, on doit clairement se restreindre aux points affines de ce modèle. Edwards démontre algébriquement que l'application

$$\big((x_1,y_1),(x_2,y_2)\big) \mapsto \left(\frac{x_1y_2+x_2y_1}{c\,(1+x_1x_2y_1y_2)}, \frac{y_1y_2-x_1x_2}{c\,(1-x_1x_2y_1y_2)}\right) \tag{2.4}$$

est bien une loi d'addition sur les points affines de ces courbes. Cependant on ne trouve aucune trace de la provenance de ces formules dans la littérature d'alors.

Après quelques changements portant sur le paramètre c, la définition des *courbes d'Edwards* a été arrêtée à la suivante

Définition 2.1.1. *Soit* $\Bbbk$ *un corps de caractéristique différente de* 2. *Les* courbes d'Edwards *sont définies par les équations de la forme*

$$E_{1,d} : x^2+y^2 = 1+d\,x^2y^2, \qquad d \neq 0,1. \tag{2.5}$$

À partir d'ici nous nous référons à cette définition lorsque l'on parle de courbes d'Edwards. La notation $E_{1,d}$ est un cas particulier de la notation que nous utiliserons pour les courbes d'Edwards tordues (voir la Définition 2.4.1 page 28).

On vérifie que l'homothétie de rapport $1/c$ est un isomorphisme de la courbe (2.3) de paramètre c vers $E_{1,d}$ où $d = c^4$. On en déduit que l'application suivante

$$\big((x_1,y_1),(x_2,y_2)\big) \mapsto \left(\frac{x_1y_2+x_2y_1}{1+dx_1x_2y_1y_2}, \frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right) \tag{2.6}$$

permet d'additionner deux points affines lorsqu'elle est définie. Dans la suite nous nous référons, sans mention contraire, à ces formules pour la loi d'addition sur une courbe d'Edwards.

Introduisons quelques points : outre les deux points à l'infini Ω_1, Ω_2, toutes les courbes d'Edwards possèdent quatre points affines $\Bbbk$-rationnels $O := (0,1)$, $O' := (0,-1)$, $T := (1,0)$, $T' := -T = (-1,0)$. Ils forment un sous-groupe cyclique d'ordre 4 de $E_{1,d}(\Bbbk)$ engendré par T. Pour qu'une courbe elliptique puisse être transformée en une courbe d'Edwards elle doit donc posséder un point d'autre 4. La proposition suivante montre que c'est aussi une condition suffisante.

Proposition 2.1.2 ([BBJ+08, Theorem 3.3])**.** *Une courbe elliptique sur* $\Bbbk$ *est birationnellement équivalente sur* $\Bbbk$ *à une courbe d'Edwards si et seulement si elle possède un point* $\Bbbk$*-rationnel d'ordre* 4.

Notons que si (u_4, v_4) est un point $\Bbbk$-rationnel de 4-torsion sur une courbe elliptique alors on associe à celle-ci la courbe d'Edwards de paramètre $d = 1 - 4u_4^3/v_4^2$.

Avant d'aller plus loin, on s'intéresse à la détermination de cette loi d'addition, pour cela nous allons utiliser la paramétrisation des courbes d'équation (2.3) par des quotients de fonctions thêta [Edw07, Section 15].

2.2 Paramétrisation par des fonctions thêta

Notons qu'Edwards choisit délibérément de se passer de la théorie des fonctions thêta et démontre "à la main" la Proposition 2.2.3 ci-après, mais l'utilisation des formules d'addition des fonctions thêta fait apparaître naturellement la loi d'addition (2.4) (Théorème 2.2.4).

Dans cette section nous travaillons dans le corps des nombres complexes $\mathbb{C}$. Pour plus de simplicité dans les notations on se ramène aux courbes initialement étudiées par Edwards en considérant que d est une puissance quatrième : $d = c^4$. On transforme alors $E_{1,d}$ en la courbe définie par $x^2 + y^2 = c^2\left(1 + x^2y^2\right)$ sur lesquelles l'addition est donnée par (2.4) et l'élément neutre est $(0, c)$.

Edwards introduit deux fonctions méromorphes ϕ et ψ comme ci-dessous (Définition 2.2.1) puis démontre en utilisant de l'analyse complexe qu'elles paramètrent la courbe voulue [Edw07, Section 16]. Nous proposons ici de démontrer ce résultat en utilisant les relations algébriques liant les fonctions thêta rappelées en Section 1.3, cela fournira également un moyen de retrouver la loi d'addition (2.4) (voir le Théorème 2.2.4).

Définitions 2.2.1. *Étant fixé un nombre complexe τ dans le demi-plan supérieur, on définit la fonction complexe méromorphe ψ par la formule*

$$\psi(z) = \frac{\displaystyle\sum_{n \text{ impair}} e^{i\pi\left(\frac{n^2}{2}\tau + nz\right)}}{\displaystyle\sum_{n \text{ pair}} e^{i\pi\left(\frac{n^2}{2}\tau + nz\right)}}, \tag{2.7}$$

les indices de sommation étant dans $\mathbb{Z}$.
On définit de plus la fonction complexe méromorphe ϕ par $\phi(z) = \psi(z - 1/2)$.

Proposition 2.2.2. *ϕ et ψ sont le quotient de deux fonctions thêta :*

$$\psi(z) = \frac{\vartheta_{10}(z, 2\tau)}{\vartheta_{00}(z, 2\tau)}, \tag{2.8}$$

$$\phi(z) = -\frac{\vartheta_{11}(z, 2\tau)}{\vartheta_{01}(z, 2\tau)}. \tag{2.9}$$

Démonstration. Développons les sommes intervenant dans la formule (2.7) :

$$\begin{aligned}
\sum_{n \text{ impair}} e^{i\pi\left(\frac{n^2}{2}\tau + nz\right)} &= \sum_{n\in\mathbb{Z}} e^{i\pi\left(\frac{(2n+1)^2}{2}\tau + (2n+1)z\right)} \\
&= \sum_{n\in\mathbb{Z}} e^{i\pi\left((n+1/2)^2 2\tau + 2(n+1/2)z\right)} \\
&= \vartheta_{10}(z, 2\tau). \\
\sum_{n \text{ pair}} e^{i\pi\left(\frac{n^2}{2}\tau + nz\right)} &= \sum_{n\in\mathbb{Z}} e^{i\pi\left(\frac{(2n)^2}{2}\tau + 2nz\right)} \\
&= \sum_{n\in\mathbb{Z}} e^{i\pi\left(2n^2\tau + 2nz\right)} \\
&= \vartheta_{00}(z, 2\tau).
\end{aligned}$$

Ceci démontre la formule (2.8). Par la suite nous ne notons plus l'argument 2τ des fonctions thêta, sauf si nous énonçons une propriété générale. Enfin, on obtient la formule (2.9) en appliquant la Proposition 1.3.4 :

$$\phi(z) = \psi(z - 1/2) = \frac{\vartheta_{10}(z - 1/2)}{\vartheta_{00}(z - 1/2)} = -\frac{\vartheta_{11}(z)}{\vartheta_{01}(z)}.$$

□

Proposition 2.2.3. *Les fonctions ϕ et ψ satisfont l'équation fonctionnelle :*

$$\phi^2+\psi^2=\psi(0)^2\left(1+\phi^2\psi^2\right). \tag{2.10}$$

Démonstration. Pour éclaircir les équations suivantes nous utilisons les notations $x_0=\vartheta_{00}(z)$, $x_1=\vartheta_{01}(z)$, $x_2=\vartheta_{10}(z)$, $x_3=\vartheta_{11}(z)$. D'après la Proposition 1.3.7 page 21 on a

$$\begin{cases} \vartheta_{00}(0)^2\left(\dfrac{x_0}{x_2}\right)^2=\vartheta_{01}(0)^2\left(\dfrac{x_1}{x_2}\right)^2+\vartheta_{10}(0)^2, \\ \vartheta_{00}(0)^2\left(\dfrac{x_3}{x_1}\right)^2=\vartheta_{10}(0)^2-\vartheta_{01}(0)^2\left(\dfrac{x_2}{x_1}\right)^2. \end{cases}$$

Éliminant $\left(\dfrac{x_2}{x_1}\right)^2$ on obtient

$$\vartheta_{00}(0)^4\left(\frac{x_3}{x_1}\right)^2-\vartheta_{00}(0)^2\vartheta_{10}(0)^2\left(\frac{x_2}{x_0}\right)^2\left(\frac{x_3}{x_1}\right)^2=\vartheta_{00}(0)^2\vartheta_{10}(0)^2-\vartheta_{10}(0)^4\left(\frac{x_2}{x_0}\right)^2-\vartheta_{01}(0)^4\left(\frac{x_2}{x_0}\right)^2,$$

ce qui permet de conclure

$$\left(\frac{x_2}{x_0}\right)^2+\left(\frac{x_3}{x_1}\right)^2=\left(\frac{\vartheta_{10}(0)}{\vartheta_{00}(0)}\right)^2\left(1+\left(\frac{x_2}{x_0}\right)^2\left(\frac{x_3}{x_1}\right)^2\right).$$

□

Finalement le théorème suivant fournit la loi d'addition (2.4).

Théorème 2.2.4. *Soient $z_1,z_2\in\mathbb{C}$.*
Notons $(x_1,y_1)=\big(\phi(z_1),\psi(z_1)\big)$ et $(x_2,y_2)=(\phi(z_2),\psi(z_2))$, on a

$$\big(\phi(z_1+z_2),\psi(z_1+z_2)\big)=\left(\frac{x_1y_2+x_2y_1}{\psi(0)\left(1+x_1y_1x_2y_2\right)},\frac{y_1y_2-x_1x_2}{\psi(0)\left(1-x_1x_2y_1y_2\right)}\right).$$

Démonstration. C'est ici que nous utilisons les formules de la Proposition 1.3.6 page 21 :

$$\begin{aligned}
\frac{x_1y_2+x_2y_1}{\psi(0)\left(1+x_1y_1x_2y_2\right)} &= \frac{\vartheta_{00}(0)}{\vartheta_{10}(0)}\,\frac{-\dfrac{\vartheta_{11}(z_1)}{\vartheta_{01}(z_1)}\dfrac{\vartheta_{10}(z_2)}{\vartheta_{00}(z_2)}-\dfrac{\vartheta_{11}(z_2)}{\vartheta_{01}(z_2)}\dfrac{\vartheta_{10}(z_1)}{\vartheta_{00}(z_1)}}{1+\dfrac{\vartheta_{11}(z_1)}{\vartheta_{01}(z_1)}\dfrac{\vartheta_{11}(z_2)}{\vartheta_{01}(z_2)}\dfrac{\vartheta_{10}(z_1)}{\vartheta_{00}(z_1)}\dfrac{\vartheta_{10}(z_2)}{\vartheta_{00}(z_2)}} \\
&= -\frac{\vartheta_{00}(0)}{\vartheta_{10}(0)}\,\frac{\vartheta_{00}(z_1)\vartheta_{11}(z_1)\vartheta_{01}(z_2)\vartheta_{10}(z_2)+\vartheta_{01}(z_1)\vartheta_{10}(z_1)\vartheta_{00}(z_2)\vartheta_{11}(z_2)}{\vartheta_{00}(z_1)\vartheta_{01}(z_1)\vartheta_{00}(z_2)\vartheta_{01}(z_2)+\vartheta_{10}(z_1)\vartheta_{11}(z_1)\vartheta_{10}(z_2)\vartheta_{11}(z_2)} \\
&= -\frac{\vartheta_{00}(0)}{\vartheta_{10}(0)}\,\frac{\vartheta_{11}(z_1+z_2)\vartheta_{00}(z_1-z_2)\vartheta_{01}(0)\vartheta_{10}(0)}{\vartheta_{01}(z_1+z_2)\vartheta_{00}(z_1-z_2)\vartheta_{01}(0)\vartheta_{00}(0)} \\
&= \phi(z_1+z_2).
\end{aligned}$$

De même,

$$\begin{aligned}
\frac{y_1y_2-x_1x_2}{\psi(0)\left(1-x_1x_2y_1y_2\right)} &= \frac{\vartheta_{00}(0)}{\vartheta_{10}(0)}\,\frac{\dfrac{\vartheta_{10}(z_1)}{\vartheta_{00}(z_1)}\dfrac{\vartheta_{10}(z_2)}{\vartheta_{00}(z_2)}-\dfrac{\vartheta_{11}(z_1)}{\vartheta_{01}(z_1)}\dfrac{\vartheta_{11}(z_2)}{\vartheta_{01}(z_2)}}{1-\dfrac{\vartheta_{11}(z_1)}{\vartheta_{01}(z_1)}\dfrac{\vartheta_{11}(z_2)}{\vartheta_{01}(z_2)}\dfrac{\vartheta_{10}(z_1)}{\vartheta_{00}(z_1)}\dfrac{\vartheta_{10}(z_2)}{\vartheta_{00}(z_2)}} \\
&= \frac{\vartheta_{00}(0)}{\vartheta_{10}(0)}\,\frac{\vartheta_{01}(z_1)\vartheta_{10}(z_1)\vartheta_{01}(z_2)\vartheta_{10}(z_2)-\vartheta_{00}(z_1)\vartheta_{11}(z_1)\vartheta_{00}(z_2)\vartheta_{11}(z_2)}{\vartheta_{00}(z_1)\vartheta_{01}(z_1)\vartheta_{00}(z_2)\vartheta_{01}(z_2)-\vartheta_{10}(z_1)\vartheta_{11}(z_1)\vartheta_{10}(z_2)\vartheta_{11}(z_2)} \\
&= \frac{\vartheta_{00}(0)}{\vartheta_{10}(0)}\,\frac{\vartheta_{10}(z_1+z_2)\vartheta_{01}(z_1-z_2)\vartheta_{01}(0)\vartheta_{10}(0)}{\vartheta_{00}(z_1+z_2)\vartheta_{01}(z_1-z_2)\vartheta_{00}(0)\vartheta_{01}(0)} \\
&= \psi(z_1+z_2).
\end{aligned}$$

□

À propos de cette loi d'addition, Edwards écrit [Edw07, Abstract] "Its principal advantage is that it allows the *addition law*, the group law on the elliptic curve, to be stated explicitly". Cette remarque correspond à la notion de *complétude* que nous allons commencer à approcher dans la prochaine section. Faisant état cependant qu'Edwards ne fait pas mention des cas où ces formules ne sont pas définies. Ce sont Bernstein et Lange [BL07a] qui donnèrent le critère de "$\Bbbk$-complétude" de la loi d'addition.

2.3 Le premier cas de complétude arithmétique

L'objet de cette thèse est d'étudier la complétude de lois d'addition sur une variété abélienne, un plongement projectif de celle-ci étant fixé. Mais les courbes d'Edwards ne sont pas des plongements de variétés abéliennes par leurs singularités ! Nous définissons donc dans cette section la $\Bbbk$-complétude (ou complétude arithmétique) de façon intuitive et la définirons plus rigoureusement dans la seconde partie de la thèse.

Définition 2.3.1. *Soit $E_{1,d}/\Bbbk$ une courbe d'Edwards. Sa loi d'addition est dite* $\Bbbk$-complète *si elle est définie pour tous les couples de points $\Bbbk$-rationnels de $E_{1,d}$. Par abus de langage on dira que $E_{1,d}$ est $\Bbbk$-complète.*

On dit qu'une courbe d'Edwards $E_{1,d}/\Bbbk$ est *triviale* si ses points $\Bbbk$-rationnels $E_{1,d}(\Bbbk)$ sont réduits aux quatre points $\{O, T, O', T'\}$, c'est par exemple le cas de $E_{1,4}/\mathbb{F}_5$.

L'addition d'un point affine avec l'un des quatre points O, T, O', T' est toujours définie car les dénominateurs dans la formule (2.6) sont alors tous deux égaux à 1. Si une courbe d'Edwards est triviale alors la loi d'addition sera définie sur ses points $\Bbbk$-rationnels. Dans le cas où il existe un point $\Bbbk$-rationnel $P_1 = (x_1, y_1)$ non trivial, construisons un point $P_2 = (x_2, y_2) \in E_{1,d}(\overline{\Bbbk})$ tel que l'addition ne soit pas définie en (P_1, P_2). Supposons donné un tel point (x_1, y_1) avec $x_1 y_1 \neq 0$, l'addition ne sera pas $\Bbbk$-complète si et seulement si il existe (x_2, y_2) tel que $dx_1x_2y_1y_2 = \pm 1$. Quitte à considérer P_1 ou son symétrique $(-x_1, y_1)$, la non $\Bbbk$-complétude de l'addition est équivalente à l'existence d'un point (x_2, y_2) tel que

$$dx_1x_2y_1y_2 = 1.$$

Supposons que l'addition ne soit pas $\Bbbk$-complète. Alors

$$\begin{aligned}(x_2 + y_2)^2 &= 1 + dx_2^2y_2^2 + 2x_2y_2 \\ &= 1 + \frac{1}{dx_1^2y_1^2} + \frac{2}{dx_1y_1} \\ &= 1 + dx_1^2y_1^2 + 2x_1y_1 \\ &= \frac{(x_1 + y_1)^2}{dx_1^2y_1^2}.\end{aligned}$$

De même on obtient $(x_2 - y_2)^2 = \dfrac{(x_1 - y_1)^2}{dx_1^2y_1^2}$. Finalement le système

$$\begin{cases} x_2 + y_2 = \dfrac{x_1 + y_1}{\sqrt{d}\, x_1y_1}, \\ x_2 - y_2 = \dfrac{x_1 - y_1}{\sqrt{d}\, x_1y_1}, \end{cases}$$

fournit les solutions

$$x_2 = \frac{1}{\sqrt{d}\, x_1},\ y_2 = \frac{1}{\sqrt{d}\, y_1}. \tag{2.11}$$

Lemme 2.3.2. *Soient $P_1 = (x_1, y_1)$ un point non trivial de $E_{1,d}(\Bbbk)$ et $P_2 = (x_2, y_2)$ défini comme ci-dessus en* (2.11)*. On a $P_2 \in E_{1,d}\big(\Bbbk\big(\sqrt{d}\,\big)\big)$ et l'addition* (2.6) *n'est pas définie au point (P_1, P_2).*

Démonstration. Le point P_2 est bien sur la courbe car

$$\begin{aligned} x_2^2 + y_2^2 &= \frac{1}{dx_1^2} + \frac{1}{dy_1^2} \\ &= \frac{x_1^2 + y_1^2}{dx_1^2 y_1^2} \\ &= \frac{1 + dx_1^2 y_1^2}{dx_1^2 y_1^2} \\ &= 1 + d\left(\frac{1}{\sqrt{d}\,x_1}\right)^2 \left(\frac{1}{\sqrt{d}\,y_1}\right)^2 \\ &= 1 + dx_2^2 y_2^2. \end{aligned}$$

Aussi la loi d'addition (2.6) n'est pas définie en (P_1, P_2) car $dx_1x_2y_1y_2 = 1$. □

La discussion ci-dessus se résume en le théorème suivant

Théorème 2.3.3. *Soit $E_{1,d}/\Bbbk$ une courbe d'Edwards. Sa loi d'addition est $\Bbbk$-complète si et seulement si $E_{1,d}$ est triviale ou d n'est pas un carré dans $\Bbbk$.*

La proposition suivante a inspiré la construction d'un modèle en caractéristique 2 analogue au modèle d'Edwards (voir la Section 2.7). Cependant elle tend à donner un rôle trop important aux singularités à l'infini qui ne sont en fait pas nécessaires, comme nous le verrons dans la seconde partie de cette thèse.

Proposition 2.3.4. *Soit $E_{1,d}/\Bbbk$ une courbe d'Edwards. d n'est pas un carré dans $\Bbbk$ si et seulement si Ω_1 et Ω_2 ont chacun un éclatement irrationnel.*

Heuristiquement Bernstein et Lange [BL07a] constatent que sur corps fini plus d'un quart des courbes elliptiques sont birationnellement équivalentes à une courbe d'Edwards $\Bbbk$-complète.

Ahmadi et Granger [AG11] se sont intéressés aux classes d'isogénies des courbes d'Edwards. Pour cela, ils utilisent des 2-isogénies explicites entre la courbe d'Edwards de paramètre d et la courbe de Legendre de même paramètre définie par l'équation affine

$$L_d, d \neq 0, 1 : \qquad y^2 = x(x-1)(x-d),$$

pour utiliser des résultats connus sur ces dernières tels que leurs classes d'isomorphisme ou lorsqu'elles sont supersingulières. Ils retrouvent par exemple que deux courbes d'Edwards $E_{1,d}$ et $E_{1,d'}$ sont isomorphes si et seulement si d' prend l'une des 6 valeurs

$$\left\{ d, \frac{1}{d}, \left(\frac{1 \pm \sqrt[4]{d}}{1 \mp \sqrt[4]{d}}\right)^4, \left(\frac{1 \pm i\sqrt[4]{d}}{1 \mp i\sqrt[4]{d}}\right)^4 \right\},$$

où i est une racine carrée de -1. Ils donnent également le nombre de classes d'isogénies pour des courbes d'Edwards définies sur un corps fini $\mathbb{F}_q$, prouvent que chacune de ces classes contient des courbes d'Edwards ayant un paramètre qui n'est pas un résidu quadratique dans $\mathbb{F}_q$ (qui sont donc $\mathbb{F}_q$-complètes). Plus précisément, pour $|t| \leq 2\sqrt{q}$, si l'on note, $N(t)$ (respectivement

$N_{n2}(t)\big)$ le nombre de paramètres $d \in \mathbb{F}_q$, $d \neq 0, 1$, (non résidus quadratiques dans $\mathbb{F}_q$) tels que la trace du Frobenius sur L_d soit égale à t, alors :

$$N_{n2}(t) = \begin{cases} \min\big(N(t), N(-t)\big), & \text{si } q \equiv 1 \pmod 4, \\ N(t), & \text{si } q \equiv -1 \pmod 4 \text{ et } q+1-t \equiv 4 \pmod 8, \\ N(t)/3, & \text{si } q \equiv -1 \pmod 4 \text{ et } q+1-t \equiv 0 \pmod 8, \end{cases}$$

Indépendamment, Morain montre dans [Mor09, Theorem 17], en utilisant la structure de volcan de 2-isogénies, que si une courbe elliptique a toute sa 2-torsion $\mathbb{F}_q$-rationnelle, alors elle est isogène à une courbe elliptique birationnellement équivalente à une courbe d'Edwards $\mathbb{F}_q$-complète. Ce résultat est explicite dans le sens où il montre que les courbes elliptiques qui nous intéressent sont au pied du volcan.

2.4 Courbes d'Edwards tordues

Bernstein et al remarquent dans [BBJ+08, Section 2] que les courbes d'Edwards ne sont pas stables par twists quadratiques. Ils introduisent leurs tordues :

Définition 2.4.1. *Soit $\Bbbk$ un corps de caractéristique différente de 2. Les* courbes d'Edwards tordues *sont définies, pour $ad(a-d) \neq 0$, par les équations de la forme*

$$E_{a,d} : \qquad a\,x^2 + y^2 = 1 + d\,x^2y^2. \tag{2.12}$$

Les deux points à l'infini $\Omega_1 = (1 : 0 : 0)$ et $\Omega_2 = (0 : 1 : 0)$ ainsi que les deux points rationnels affines $O = (0, 1)$ et $O' = (0, -1)$ sont toujours sur les courbes d'Edwards tordues. Le morphisme

$$E_{a,d} \to E_{1,d/a}, \quad (x, y) \mapsto \big(\sqrt{a}\,x, y\big)$$

induit la loi d'addition

$$\big((x_1, y_1), (x_2, y_2)\big) \mapsto \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}\right) \tag{2.13}$$

définie pour des points affines de $E_{a,d}$.

On voit ainsi d'une part qu'une courbe d'Edwards tordue $E_{a,d}$ est birationnellement équivalente sur $\Bbbk$ à une courbe d'Edwards si et seulement si a est un carré dans $\Bbbk$. D'autre part on peut représenter plus de courbes elliptiques :

Proposition 2.4.2 ([BBJ+08, Theorem 3.2])**.** *Toute courbe d'Edwards tordue est birationnellement équivalente sur $\Bbbk$ à une courbe de Montgomery, et réciproquement.*

Nous verrons dans la Section 2.6 que la désingularisée définie par l'équation (2.12) est l'intersection dans $\mathbb{P}^3$ des quadriques suivantes

$$E_{a,d} : \qquad \begin{cases} XY = ZT, \\ aX^2 + Y^2 = Z^2 + dT^2. \end{cases}$$

On voit que $E_{a,d}$ est isomorphe sur $\Bbbk$ à $E_{d,a}$ en appliquant les permutations $X \leftrightarrow T$, $Y \leftrightarrow Z$. De plus, pour tout $\lambda \in \overline{\Bbbk}^*$, $E_{\lambda a,\lambda d}$ est isomorphe sur $\Bbbk\big(\sqrt{\lambda}\big)$ à $E_{a,d}$.

Il est intéressant de regarder les transformations entre différents modèles elliptiques non isomorphes. Justifions que le modèle de Weierstraß et celui d'Edwards ne sont pas isomorphes par le fait qu'ils sont respectivement définis par les fibrés en droite $\mathcal{L}\big(3(O)\big)$ et $\mathcal{L}\big(3(O) + (O')\big)$ [1].

1. La théorie des fibrés en droite est présentée dans le Chapitre II.5.

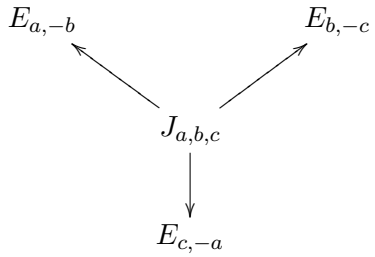
Un autre modèle elliptique est le *modèle de Jacobi*, il est défini par l'intersection dans $\mathbb{P}^3$ des quadriques suivantes, avec $a+b+c=0$:

$$J_{a,b,c}: \quad \begin{cases} aX_0^2 + X_1^2 = X_2^2, \\ bX_0^2 + X_2^2 = X_3^2, \\ cX_0^2 + X_3^2 = X_1^2, \end{cases}$$

De telles courbes elliptiques ont toute leur 2-torsion $\Bbbk$-rationnelle, correspondant aux points tels que $X_0 = 0$. Ce plongement dans $\mathbb{P}^3$ est donc déterminé par $\mathcal{L}\big(4(O)\big)$. On remarque que $J_{a,b,c}$ est isomorphe sur $\Bbbk$ à $J_{c,b,a}$ en appliquant le 3-cycle (X_1, X_3, X_2). De plus, le morphisme

$$\begin{aligned} J_{a,b,c} &\to E_{a,-b} \\ (X_0 : X_1 : X_2 : X_3) &\mapsto (X_0X_3 : X_1X_2 : X_2X_3 : X_0X_1), \end{aligned}$$

est une 2-isogénie entre les deux modèles dans $\mathbb{P}^3$. Ce n'est pas étonnant car toute courbe elliptique sur un corps de caractéristique différente de 2 avec toute la 2-torsion rationnelle est 2-isogène à une courbe d'Edwards tordue [BBJ+08, Theorem 5.1]. On obtient, par composition avec les isomorphismes entre modèles de Jacobi ci-dessus, les 2-isogénies suivantes.



En posant $a = 1$, $b = -d$, $c = d-1$, on obtient des 4-isogénies définies sur $\Bbbk$:

$$E_{1,d} \sim E_{-d,1-d} \sim E_{d-1,-1}.$$

En appliquant les isomorphismes précédents entre courbes d'Edwards tordues, on retrouve que $E_{1,d}$ est 4-isogène aux courbes d'Edwards $E_{1,1-\frac{1}{d}}, E_{1,\frac{1}{1-d}}, E_{1,\frac{d}{d-1}}, E_{1,1-d}$ et isomorphe à $E_{1,\frac{1}{d}}$, la rationalité de ces morphismes dépendant de l'existence dans $\Bbbk$ d'une racine carrée de $-1, d, d-1$ [AG11, Introduction, Theorem 3.2].

2.5 Interprétation géométrique de l'addition

Remarquablement, l'interprétation géométrique de la loi d'addition met du temps à apparaître. Cela vient probablement du fait que l'on ne peut la comprendre en termes d'intersection avec la droite définie par les deux points à additionner à l'instar du cas elliptique sous forme de Weierstraß. En effet, l'intersection entre une quartique et une droite donne un quatrième point. Quand on s'intéresse au degré 2, on a besoin de cinq points pour définir une conique et son intersection avec une courbe d'Edwards tordue donne huit points géométriques comptés avec multiplicité. En prenant Ω_1 et Ω_2, O' et les deux points P_1 et P_2 à additionner pour définir C, la multiplicité des points à l'infini entraîne l'existence d'un unique nouveau point d'intersection. Le théorème suivant montre que ce huitième point d'intersection est le symétrique de $P_1 + P_2$.

Théorème 2.5.1. *Soient P_1, P_2 sur $E_{a,d}$, l_1, l_2, ϕ les équations homogènes respectives par la droite horizontale passant par $P_3 = P_1 + P_2$, la droite verticale passant par O et la conique passant par $P_1, P_2, O', \Omega_1, \Omega_2$. On a la relation suivante*

$$\operatorname{div}\left(\frac{\phi}{l_1 l_2}\right) = (P_1) + (P_2) - (P_3) - (O). \tag{2.14}$$

Démonstration. Notons Q le huitième point d'intersection entre la conique et la courbe d'Edwards tordue $E_{a,d}$. L'intersection entre $E_{a,d}$ et la droite à l'infini $z = 0$ étant donnée par le diviseur $2(\Omega_1) + 2(\Omega_2)$, on obtient les diviseurs principaux suivants

$$\operatorname{div}\left(\frac{l_1}{z}\right) = (Q) + \left(\overline{Q}\right) - 2(\Omega_2), \qquad \operatorname{div}\left(\frac{l_2}{z}\right) = \left(O'\right) + (O) - 2(\Omega_1),$$
$$\operatorname{div}\left(\frac{\phi}{z^2}\right) = \left(O'\right) + (P_1) + (P_2) + (Q) - 2(\Omega_1) - 2(\Omega_2).$$

On a ainsi que la fonction $\dfrac{\phi}{l_1 l_2}$ sur $E_{a,d}$ a pour diviseur $(P_1) + (P_2) - \left(\overline{Q}\right) - (O)$. Finalement, le corollaire 1.2.7 page 17 permet de conclure que $\overline{Q} = P_1 + P_2$. □

Notation 2.5.2. *Soient P_1, P_2 deux points sur $E_{a,d}$. Dans ce chapitre et le suivant, on note C_{P_1,P_2} la conique passant par les points $P_1, P_2, O', \Omega_1, \Omega_2$. La Figure 3 page 31 représente cette interprétation géométrique de l'addition de deux points dans différents cas d'intérêt.*

Remarquons que cette construction est le cas dégénéré de l'interprétation géométrique de l'addition sur la jacobienne d'une quartique non singulière, *i.e.* une courbe non hyperelliptique de genre 3, dûe à Flon, Oyono et Ritzenthaler [FOR08] que nous résumons ici. Soit $C/\Bbbk$ une telle courbe et l^∞ une droite coupant C en quatre points $\Bbbk$-rationnels notés $P_1^\infty, P_2^\infty, P_3^\infty, P_4^\infty$. On pose $D^\infty := P_1^\infty + P_2^\infty + P_3^\infty$ et, pour $D \in \mathrm{Jac}_C$, on définit D^+ le diviseur associé à un antécédent de D par l'application surjective $S^3C \to \mathrm{Jac}_C$, $(P_1, P_2, P_3) \mapsto (P_1) + (P_2) + (P_3) - D^\infty$.

Soient $D_1, D_2 \in \mathrm{Jac}_C(\Bbbk)$, on retrouve $(D_1 + D_2)^+$ comme suit

1. Soit E la cubique passant par les points du support de D_1^+, D_2^+, et $P_1^\infty, P_2^\infty, P_4^\infty$ comptés avec multiplicité. On note D_3 le diviseur résiduel de l'intersection entre C et E.
2. Soit R la conique déterminée par les points du support de D_3 et P_1^∞, P_2^∞. Elle définit un diviseur résiduel sur C qui est égal à $(D_1 + D_2)^+$.

Cette construction est illustrée dans la Figure 2 ci-dessous, où la courbe C et la conique R sont tracées par une ligne pleine et la cubique E est représentée en pointillés.

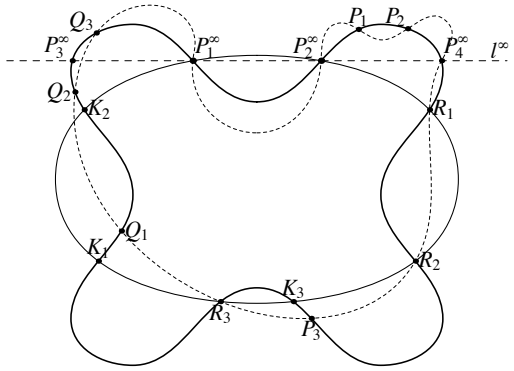
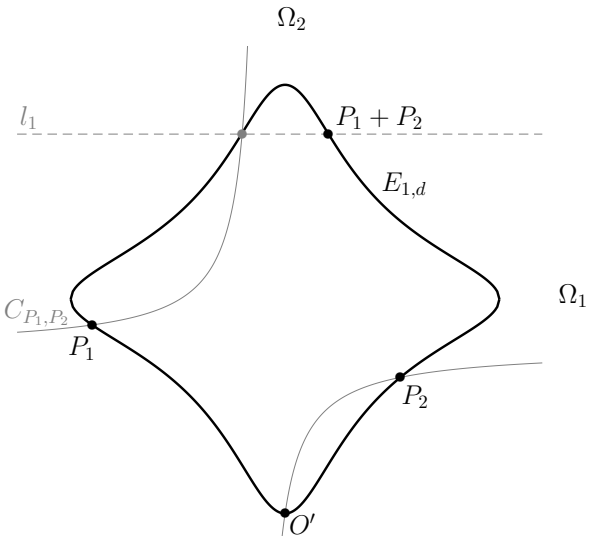


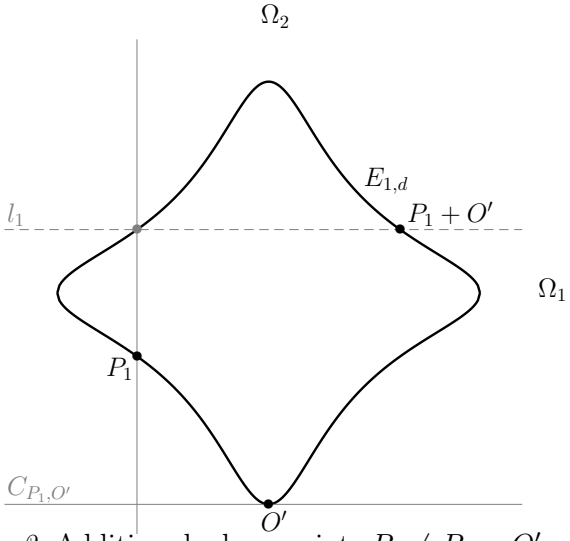
FIGURE 2 – Interprétation de l'addition sur la jacobienne d'une courbe de genre 3 non hyperelliptique.

On retrouve l'interprétation géométrique de l'addition sur les courbes d'Edwards tordues comme une dégénération du cas lisse de la façon suivante : Soient $P_1, P_2 \in E_{a,d} = C$.

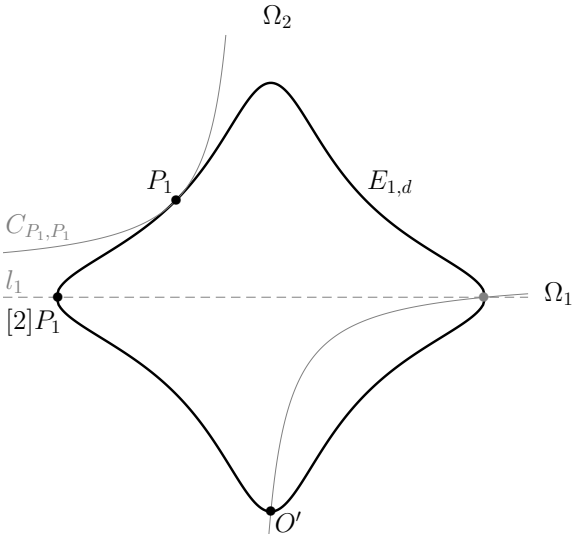
1. On pose $P_1^\infty = P_2^\infty = \Omega_1$ et $P_3^\infty = P_4^\infty = \Omega_2$. Puis on choisit $D_1^+ := (P_1) + (\Omega_1) + (\Omega_2)$, $D_2^+ := (P_2) + (\Omega_1) + (\Omega_2)$.
2. On a alors $D_3 = (P_3) + (O') + (\Omega_2)$, $E = l_\infty \cup C_{P_1,P_2}$ et $R = l_1 \cup l_2$, avec l_1 la droite horizontale passant par P_3 et l_2 la droite verticale passant par O'. Finalement, on a $(D_1 + D_2)^+ = \left(\overline{P_3}\right) + (O) + (\Omega_2)$.



1. Addition de deux points $P_1 \neq P_2$ et $P_1, P_2 \neq O'$.



2. Addition de deux points $P_1 \neq P_2 = O'$.



3. Doublement d'un point P_1.

FIGURE 3 – Divers cas de l'interprétation géométrique de l'addition sur une courbe d'Edwards.

2.6 Nombre d'opérations

Comme dans le cas des courbes sous forme de Weierstraß réduite, on cherche à minimiser le coût du calcul de l'addition de deux points. Commençons par représenter un point $(x, y) \in E_{a,d}$ par le point projectif $(X : Y : Z) \in \mathbb{P}^2\left(\overline{\Bbbk}\right), Z \neq 0$, tel que $x = X/Z, y = Y/Z$ et satisfaisant l'équation

$$\left(aX^2 + Y^2\right) Z^2 = Z^4 + dX^2Y^2.$$

Notons $(X_3 : Y_3 : Z_3)$ l'addition $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$, la loi (2.13) page 28 s'exprime alors par les polynômes bihomogènes suivants

$$\begin{aligned}
X_3 &= Z_1Z_2\left(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2\right)\left(X_1Y_2 + X_2Y_1\right), \\
Y_3 &= Z_1Z_2\left(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2\right)\left(Y_1Y_2 - aX_1X_2\right), \\
Z_3 &= \left(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2\right)\left(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2\right).
\end{aligned}$$

Les formules explicites données dans [BBJ+08] permettent de calculer cette addition pour un coût de $10\mathbf{m} + 1\mathbf{s} + 1\mathbf{m_a} + 1\mathbf{m_d}$. Cependant la manipulation des coordonnées a permis d'améliorer sensiblement ce coût : Bernstein et Lange introduisent les *coordonnées d'Edwards inversées* ([BL07b]) et donnent des formules explicites nécessitant $1\mathbf{m}$ de moins, puis Hisil et al [HWCD08, Section 3] introduisent les *coordonnées d'Edwards étendues* qui permettent encore de réduire le coût de $1\mathbf{s}$. Pour cette dernière représentation on ajoute, pour un point affine (x, y) la coordonnée $t = xy$. Projectivement le point $(X : Y : T : Z), Z \neq 0$, correspond au point affine étendu $(X/Z, Y/Z, T/Z)$ et vérifie $T = XY/Z$.

Notons $(X_3 : Y_3 : T_3 : Z_3) = (X_1 : Y_1 : T_1 : Z_1) + (X_2 : Y_2 : T_2 : Z_2)$, la loi d'addition (2.13) est décrite comme suit

$$\begin{aligned}
X_3 &= (X_1Y_2 + X_2Y_1)(Z_1Z_2 - dT_1T_2), \\
Y_3 &= (Y_1Y_2 - aX_1X_2)(Z_1Z_2 + dT_1T_2), \\
T_3 &= (X_1Y_2 + X_2Y_1)(Y_1Y_2 - aX_1X_2), \\
Z_3 &= (Z_1Z_2 - dT_1T_2)(Z_1Z_2 + dT_1T_2),
\end{aligned} \tag{2.15}$$

pour un coût de $9\mathbf{m} + 1\mathbf{m_a} + 1\mathbf{m_d}$.

Le moment est venu de faire le lien (*i.e.* construire un morphisme birationnel sur $\Bbbk$) entre la définition rigoureuse des courbes d'Edwards donnée dans le préambule (Définition 2.0.1) et les courbes d'Edwards (singulières) que l'on a étudiées jusqu'ici. L'idée est de remarquer que la donnée supplémentaire du produit xy définit un plongement dans $\mathbb{P}^3(\Bbbk)$.

On représente les points $(x, y) \in E_{a,d} \subset \mathbb{A}^1 \times \mathbb{A}^1$ par les points $\big((x : w), (y : z)\big) \in \mathbb{P}^1 \times \mathbb{P}^1$. Ces derniers vérifient l'équation

$$a(xz)^2 + (yw)^2 = (wz)^2 + d(xy)^2.$$

Puis on plonge $\mathbb{P}^1 \times \mathbb{P}^1$ dans $\mathbb{P}^3$ par le plongement de Segre, ce qui amène à considérer les points $(X : Y : T : Z) \in \mathbb{P}^3$ avec $X = xz, Y = yw, T = xy, Z = wz$. Ils vérifient

$$\begin{cases} XY = ZT, \\ aX^2 + Y^2 = Z^2 + dT^2. \end{cases}$$

La courbe ainsi obtenue est une courbe lisse de genre 1. Par construction les formules d'addition (2.15) fournissent la loi d'addition (2.2) sur le modèle d'Edwards plongé dans $\mathbb{P}^3$. Cette dernière est $\Bbbk$-complète dans le cas où d n'est pas un carré et a en est un dans $\Bbbk$.

2.7 La complétude arithmétique dans d'autres modèles elliptiques

Le modèle de Weierstraß n'est pas le seul modèle elliptique auquel les cryptographes se sont intéressés. Aussi la $\Bbbk$-complétude de courbes d'Edwards a mené à la recherche de lois d'addition, ayant cette propriété, sur ces modèles elliptiques, notamment le modèle hessien intéressant pour sa structure de 3-torsion. Soient $a, d \in \Bbbk$, les *courbes hessiennes tordues* $H_{(a,d)}$ sont les courbes d'équation

$$aX^3 + Y^3 + Z^3 = dXYZ, \qquad ad\left(d^3 - 27a\right) \neq 0.$$

Soient $P_1 = (X_1 : Y_1 : Z_1), P_2 = (X_2 : Y_2 : Z_2) \in H_{(a,d)}$ et $(X_3 : Y_3 : Z_3) = P_1 + P_2$. Bernstein, Kohel et Lange [BKL11] démontrent que les deux lois d'addition $\mathfrak{s}_1$ et $\mathfrak{s}_2$ ci-dessous sont $\Bbbk$-complètes si et seulement si a n'est pas un cube dans $\Bbbk$.

$$\mathfrak{s}_1 : \begin{array}{l} X_3 = X_1Y_1Y_2^2 - Z_1^2X_2Z_2, \\ Y_3 = aX_1Z_1X_2^2 - Y_1^2Y_2Z_2, \\ Z_3 = Y_1Z_1Z_2^2 - aX_1^2X_2Y_2. \end{array} \qquad \mathfrak{s}_2 : \begin{array}{l} X_3 = X_1Z_1Z_2^2 - Y_1^2X_2Y_2, \\ Y_3 = Y_1Z_1Y_2^2 - aX_1^2X_2Z_2, \\ Z_3 = aX_1Y_1X_2^2 - Z_1^2Y_2Z_2. \end{array}$$

Un autre modèle récemment introduit en cryptographie est le *modèle de Huff*, ce dernier est défini sur un corps $\Bbbk$ non binaire par les équations

$$aX(Y^2 - Z^2) = bY(X^2 - Z^2), \qquad ab(a^2 - b^2) \neq 0.$$

Bien que l'on ne dispose pas de loi d'addition $\Bbbk$-complète, Joye, Tibouchi et Vergnaud [JTV10, Corollary 1] fournissent une loi d'addition ci-dessous définie pour tout couple de points dans le sous-groupe engendré par un point d'ordre impair. En réutilisant les notations précédentes,

$$\begin{array}{l} X_3 = (X_1Z_2 + X_2Z_1)(Y_1Y_2 + Z_1Z_2)^2(Z_1Z_2 - X_1X_2), \\ Y_3 = (Y_1Z_2 + Y_2Z_1)(X_1X_2 + Z_1Z_2)^2(Z_1Z_2 - Y_1Y_2), \\ Z_3 = \left(Z_1^2Z_2^2 - X_1^2X_2^2\right)\left(Z_1^2Z_2^2 - Y_1^2Y_2^2\right). \end{array}$$

Cette propriété est suffisante pour apporter une protection contre les attaques par canaux cachés puisqu'on ne travaille que dans le sous-groupe engendré par un point d'ordre premier très grand (voir la Section 4.2 pour les différentes tailles conseillées). Cela pourrait mener à la notion de complétude sur un sous-groupe de $E\left(\overline{\Bbbk}\right)$, généralisant la définition de $\Bbbk$-complétude, mais nous ne nous concentrons que sur cette dernière.

Bernstein et al [BLF08] définissent un modèle elliptique en caractéristique 2 pouvant être muni d'une loi d'addition $\Bbbk$-complète. Dans la recherche de telles courbes, les auteurs ont cherché à transporter en caractéristique 2 les propriétés des courbes d'Edwards en se donnant les contraintes suivantes :

- Les degrés en x et y sont inférieurs à 2, ils considèrent donc une courbe d'équation

$$\sum_{i,j=0}^{2} a_{ij}x^iy^j = 0.$$

- La symétrie : $a_{ij} = a_{ji}$.
- De genre 1 : $a_{22} \neq 0$ ou $a_{21} \neq 0$.
- Des points à l'infini singuliers, donc $a_{22} \neq 0$.
- Les deux points à l'infini $(1 : 0 : 0)$ et $(0 : 1 : 0)$ ont un éclatement irrationnel si et seulement si le polynôme $T^2 + a_{21}T + a_{20} \in \Bbbk[T]$ est irréductible. On prend $a_{21} \neq 0$ et on se ramène à $a_{21} = 1$ par la transformation linéaire $(x, y) \mapsto (a_{21}x, a_{21}y)$.

- On veut que le symétrique d'un point (x, y) soit (y, x), dans ce cas pour que la courbe soit ordinaire il faut un point d'ordre 2, on impose alors $a_{00} = 0$ et $a_{11} = 1$ pour avoir les points $(0, 0)$ et $(1, 1)$, mais $a_{10} \neq 0$ sans quoi $(0, 0)$ serait singulier.

Finalement l'équation retenue est la suivante, et cette construction est fructueuse.

Définition 2.7.1. *Soient* $\Bbbk$ *un corps de caractéristique* 2, $d_1, d_2 \in \Bbbk$ *tels que* $d_1(d_2+d_1^2+d_1) \neq 0$. *Les* courbes d'Edwards binaires *sont définies par l'équation affine*

$$E_{B,d_1,d_2} : \qquad d_1(x + y) + d_2(x^2 + y^2) = xy + xy(x + y) + x^2y^2.$$

Proposition 2.7.2. *Soient* $(x_1, y_1), (x_2, y_2)$ *deux points sur une telle courbe. Leur addition* (x_3, y_3) *est donnée par les formules*

$$x_3 = \frac{d_1(x_1 + x_2) + d_2(x_1 + y_1)(x_2 + y_2) + (x_1 + x_1^2)\big(x_2(y_1 + y_2 + 1) + y_1y_2\big)}{d_1 + \big(x_1 + x_1^2\big)(x_2 + y_2)},$$
$$y_3 = \frac{d_1(y_1 + y_2) + d_2(x_1 + y_1)(x_2 + y_2) + (y_1 + y_1^2)\big(y_2(x_1 + x_2 + 1) + x_1x_2\big)}{d_1 + \big(y_1 + y_1^2\big)(x_2 + y_2)}.$$

Si le polynôme $T^2 + T + d_2$ *est irréductible, alors la loi d'addition ci-dessus est* $\Bbbk$*-complète.*

De plus, si $\Bbbk = \mathbb{F}_{2^r}$ avec $r \geq 3$, alors toute courbe elliptique ordinaire définie sur $\Bbbk$ est birationnellement équivalente sur $\Bbbk$ à une courbe d'Edwards binaire [BLF08, Theorem 4.3]. Cependant, le coût d'une addition reste élevé avec dans le plus simple cas ($d_1 = d_2$) $16\mathbf{m} + 1\mathbf{s} + 4\mathbf{m_d}$, mais le coût d'un doublement de $2\mathbf{m} + 5\mathbf{s} + 2\mathbf{m_d}$ est équivalent à ceux trouvés dans la littérature pour les équations de Weierstraß [BLF08, Sections 5, 6].

Diao [Dia10, Section 7.2] retrouve en partie ce modèle en effectuant un changement de coordonnées dans le modèle complexe afin d'obtenir une bonne réduction des équations de $E_{1,d}$ modulo 2. Pour cela il considère un relevé de $E_{1,d}$ sur un corps 2-adique plongé dans $\mathbb{C}$. Il obtient un modèle de courbes elliptiques ordinaires définies par les équations

$$x^2 + y^2 + \frac{1}{c}xy = 1 + x^2y^2, \qquad c \in \Bbbk^*.$$

C'est un cas particulier des courbes d'Edwards binaires précédentes car celles-ci seront isomorphes sur $\overline{\Bbbk}$ si l'on choisit les paramètres tels que $d_1^2 = d_2^2 = c$.

Chapitre 3

Le couplage de Tate réduit

Ce chapitre est dévolu au calcul de couplages sur les courbes d'Edwards. Nous rappelons brièvement dans la première section l'intérêt, en cryptologie, de l'existence de couplages sur des groupes de points d'une courbe elliptique. Dans les deux sections suivantes nous nous concentrons sur le couplage de Tate réduit et l'algorithme de Miller permettant de le calculer. Nous donnons, dans la quatrième section, des formules explicites pour calculer ce couplage sur les courbes d'Edwards tordues en nous basant sur l'interprétation géométrique de l'addition sur celles-ci. Nous terminons en comparant ces résultats avec ceux obtenus sur le modèle de Weierstraß, ces derniers s'avérant moins efficaces dans la plupart des cas. Notons que les formules explicites pour le calcul du couplage de Tate réduit sur le modème de Weierstraß sont également développées dans [ALNR10]. Cependant, nous avons choisi de ne travailler ici que sur les courbes d'Edwards pour ne pas répéter deux fois des raisonnements similaires.

3.1 Apport des couplages en cryptologie

Définition 3.1.1. *Soient G_1, G_2 deux groupes abéliens finis notés additivement et G_3 un groupe cyclique noté multiplicativement. Un* couplage *est une application*

$$e : G_1 \times G_2 \longrightarrow G_3$$

bilinéaire et non-dégénérée.

On utilise ces notations puisque dans les applications nous voulons que les deux premiers groupes G_1, G_2 soient des groupes de points sur une courbe elliptique (voire la jacobienne d'une courbe) tandis que G_3 sera un sous-groupe du groupe multiplicatif d'un corps fini. Les propriétés ci-dessus s'expriment alors ainsi

- *Bilinéarité :* $e(P_1 + P_2, Q) = e(P_1, Q)\, e(P_2, Q)$,
  $e(P, Q_1 + Q_2) = e(P, Q_1)\, e(P, Q_2)$.
- *Non-dégénérescence :* pour tout $0 \neq P \in G_1$ il existe $Q \in G_2$ tel que $e(P, Q) \neq 1$; de même pour tout $Q \in G_2$ il existe $P \in G_1$ tel que $e(P, Q) \neq 1$.

On doit également garder à l'esprit que les couplages que l'on considère doivent être calculables efficacement, sans quoi ils seraient inutilisables. On peut les utiliser pour réduire le problème du logarithme discret sur une courbe elliptique $E/\mathbb{F}_q$ à celui sur le groupe multiplicatif d'une extension de $\mathbb{F}_q$, qui est de complexité sous-exponentielle. Plus précisément, étant donnés un point $P \in E(\mathbb{F}_q)$ d'ordre n_0, on peut, sous des conditions raisonnables, choisir un

point $Q \in E(\overline{\mathbb{F}}_q)$ tel que $e(P,Q)$ soit une racine non triviale $n_0^{\text{ième}}$ de l'unité. On a alors

$$e\big([l]P, Q\big) = e(P,Q)^l.$$

Connaissant $e(P,Q)$, on se ramène ainsi à résoudre le problème du logarithme discret dans le groupe $\mu_{n_0} \subset \overline{\mathbb{F}}_q$. C'est pour cela que les couplages ont été utilisés à leur début dans un but cryptanalytique. Donnons deux exemples de l'utilisation des couplages de Weil et Tate (nous les définissons dans la section suivante) en ce sens. Menezes, Okamoto et Vanstone [MOV93] appliquèrent une telle attaque sur les courbes elliptiques supersingulières en utilisant le couplage de Weil. Puis Frey et Rück [FR94] se basèrent sur le couplage de Tate. On préfère ce dernier puisqu'en pratique il est plus efficace à calculer. Aussi l'utilisation du couplage de Weil requiert que la n_0-torsion soit rationnelle alors que le couplage de Tate nécessite de travailler dans le corps engendré par les racines $n_0^{\text{ième}}$ de l'unité. Cette dernière remarque n'est pas gênante dans le cas des courbes elliptiques utilisées en cryptographie (voir [BK98, Theorem 1]) mais le devient si l'on s'intéresse aux jacobiennes de courbes de genre $g \geq 2$ ([FR94]).

Les premières applications cryptographiques des couplages apparurent seulement au début des années 2000, et non des moindres puisque Boneh et Franklin ([BF01] ou [BF03] pour une version étendue) ont utilisé le couplage de Weil pour concrétiser l'idée de Shamir [Sha85] d'un protocole cryptographique asymétrique dont la clé publique serait l'identité du correspondant, créant le premier cryptosystème basé sur l'identité. Joux (premièrement paru dans [Jou00] puis complété dans [Jou04]) découvrit un protocole d'échange de clé tripartite en une étape généralisant le protocole de Diffie-Hellman à trois correspondants A_1, A_2, A_3. L'idée est de rendre publics une courbe elliptique E et deux points P, Q engendrant sa l-torsion. Chaque participant A_i choisit un entier l_i et calcule $P_i := [l_i]P$ et $Q_i := [l_i]Q$, $i = 1, 2, 3$. Ces points sont échangés et, notant e_l le couplage de Weil sur $E[l] \times E[l]$, chacun calcule et partage le secret

$$e_l(P_{i+1}, Q_{i+2})^{l_i} = e_l(P,Q)^{l_1 l_2 l_3}.$$

Ce protocole peut aussi être adapté au couplage de Tate [Jou04]. Citons également la création de protocoles de signatures courtes (voir [BLS04b] révision de [BLS01]), permettant de diviser leur taille par deux pour un même niveau de sécurité.

3.2 Couplage de Tate

Tate introduisit de façon abstraite un couplage sur une variété abélienne puis Lichtenbaum parvint à obtenir des formules explicites pour ce couplage dans le cas de la jacobienne d'une courbe. Nous nous intéressons à ce dernier que nous appelons *couplage de Tate* mais qui peut également être nommé *couplage de Tate-Lichtenbaum* dans la littérature. Plus particulièrement nous considérons ce couplage dans le cas d'une courbe elliptique (Définiton 3.2.3). Introduisons quelques notations en vue de le définir.

Définition 3.2.1. *Soient C une courbe, $D \in \mathrm{Div}^0(C)$ et $f \in \Bbbk(C)$ ayant des supports disjoints. On définit la quantité*

$$f(D) = \prod_{P \in C} f(P)^{n_P(D)}.$$

Le fait que le diviseur D soit de degré 0 entraîne que $f(D)$ ne dépend que de la classe de D. La fonction f étant fixée, il est ainsi aisé de construire un diviseur $D' \sim D$ dont le support soit disjoint de celui de $\mathrm{div}(f)$.

Dans toute cette section nous considérons une courbe elliptique définie sur un corps fini $E/\mathbb{F}_q$ et un nombre premier r tel que $(r,q) = 1$ et $r \,\big|\, |E(\mathbb{F}_q)|$. Le degré de plongement de $E/\mathbb{F}_q$ relatif à r défini ci-dessous sera noté k dans cette section et les suivantes.

Définition 3.2.2. *Le plus petit entier k tel que*

$$r | q^k - 1$$

est appelé le degré de plongement de E relatif à r.

Soient $P \in E\left(\mathbb{F}_{q^k}\right)[r]$ et $Q \in E\left(\mathbb{F}_{q^k}\right)$, on note f_P une fonction sur E dont le diviseur soit $\mathrm{div}(f_P) = r(P) - r(O)$ et $D_Q \sim (Q) - (O)$ défini sur $\mathbb{F}_{q^k}$ et dont le support soit disjoint de celui de $\mathrm{div}(f_P)$.

Définition 3.2.3. *Le* couplage de Tate *est défini par*

$$\begin{array}{rccl} T_r : & E\left(\mathbb{F}_{q^k}\right)[r] \times E\left(\mathbb{F}_{q^k}\right) / \, rE\left(\mathbb{F}_{q^k}\right) & \longrightarrow & \mathbb{F}_{q^k}^* / \mathbb{F}_{q^k}^{*\,r}, \\ & (P, Q) & \longmapsto & f_P\left(D_Q\right). \end{array}$$

Remarques 3.2.4.

- *$Q \in E\left(\mathbb{F}_{q^k}\right) / \, rE\left(\mathbb{F}_{q^k}\right)$ étant défini à un r-multiple près, $f_P\left(D_Q\right)$ sera définie à la multiplication d'une puissance $r^{ième}$ près.*
- *On ne peut pas toujours utiliser les points de $E\left(\mathbb{F}_{q^k}\right)[r]$ pour représenter les classes de $E\left(\mathbb{F}_{q^k}\right) / \, rE\left(\mathbb{F}_{q^k}\right)$ [BSS05, p186], mais s'il n'y a pas de points d'ordre r^2 définis sur $\mathbb{F}_{q^k}$ alors $E\left(\mathbb{F}_{q^k}\right)[r] \cong E\left(\mathbb{F}_{q^k}\right) / \, rE\left(\mathbb{F}_{q^k}\right)$ [Nae09, p34].*

Comme on travaille sur des corps finis, on peut s'affranchir des puissances $r^{\text{ième}}$ dans la classe de $T_r(P, Q)$ en l'élevant à la puissance $(q^k - 1)/r$. On obtient alors une racine $r^{\text{ième}}$ de l'unité dans $\mathbb{F}_{q^k}^*$. C'est ce que l'on appelle le *couplage de Tate réduit*.

Définition 3.2.5. *Le* couplage de Tate réduit *est l'application*

$$\begin{array}{rccl} e_r : & E\left(\mathbb{F}_{q^k}\right)[r] \times E\left(\mathbb{F}_{q^k}\right) / \, rE\left(\mathbb{F}_{q^k}\right) & \longrightarrow & \mu_r \subseteq \mathbb{F}_{q^k}^*, \\ & (P, Q) & \longmapsto & T_r(P, Q)^{\left(q^k - 1\right)/r}. \end{array}$$

3.3 Fonctions et algorithme de Miller

La difficulté est d'évaluer les fonctions dont le diviseur est $r(P) - r(O)$ alors que l'on ne connaît que leur existence. L'idée de Miller [Mil04] est de les construire par récurrence à l'aide de fonctions auxiliaires appelées *fonctions de Miller*.

Définition 3.3.1. *Soient $m \in \mathbb{Z}$, $P \in E\left(\mathbb{F}_{q^k}[r]\right)$, on appelle* fonction de Miller *toute fonction $f_{m,P} \in \overline{\Bbbk}(E)$ telle que*

$$\mathrm{div}(f_{m,P}) = m\,(P) - ([m]P) - (m-1)\,(O).$$

Remarque 3.3.2. *P étant un point de r-torsion on voit que $f_{r,P}$ est la fonction recherchée.*

Notation 3.3.3. *Ayant fixé un modèle pour E, soient $P_1, P_2 \in E$. On note g_{P_1,P_2} la fonction ayant pour diviseur*

$$\mathrm{div}\left(g_{P_1,P_2}\right) = (P_1) + (P_2) - (P_1 + P_2) - (O).$$

La proposition suivante décrit la construction par récurrence des fonctions de Miller en appliquant les *formules de Miller*. Ces formules sont basées sur l'existence d'une telle fonction g_{P_1,P_2}, nous allons décrire sa construction dans les cas elliptiques et des courbes d'Edwards tordues. Celle-ci est fournie par l'interprétation géométrique du morphisme d'addition.

Proposition 3.3.4. *Soit $P \in E$, on pose $f_{1,P} = 1$ puis pour $m, n \in \mathbb{Z}$*

$$f_{m+n,P} = f_{m,P}\, f_{n,P}\, g_{[m]P,[n]P},$$
$$f_{mn,P} = f_{m,P}^n\, f_{n,[m]P} = f_{n,P}^m\, f_{m,[n]P}.$$

Remarque 3.3.5. *En particulier, partant de la décomposition binaire de r, l'algorithme de Miller ci-dessous n'utilise que les deux formules suivantes*

$$f_{m+1,P} = f_{m,P}\, g_{[m]P,P},$$
$$f_{2m,P} = f_{m,P}^2\, g_{[m]P,[m]P}.$$

Input : $P \in E(\mathbb{F}_q)[r]$, $Q \in E(\mathbb{F}_{q^k})$, $r = (r_l, \ldots, r_0)_2$.
Output : $e_r(P, Q)$.
$R \leftarrow P, f \leftarrow 1$
for $(i \leftarrow l-1, i \geq 0, i--)$ **do**
  $f \leftarrow f^2 \cdot g_{R,R}(Q)$
  $R \leftarrow [2]R$
  } Doublement : $1\mathbf{M} + 1\mathbf{S}$ + coûts de $g_{R,R}(Q)$ et $[2]R$
  if $(r_i = 1)$ **then**
    $f \leftarrow f \cdot g_{R,P}(Q)$
    $R \leftarrow R + P$
    } Addition : $1\mathbf{M}$ + coûts de $g_{R,P}(Q)$ et $R + P$
  end if
end for
$f \leftarrow f^{(q^k-1)/r}$
return f

ALGORITHME 1 – Algorithme de Miller et détail des opérations arithmétiques dans les étapes de doublement et d'addition.

Remarque 3.3.6. *À chaque boucle de l'algorithme on effectue une étape de doublement qui impose une multiplication et une élévation au carré dans l'extension $\mathbb{F}_{q^k}$, respectivement notées* **M** *et* **S**, *et d'autres coûts, dépendant, eux, du modèle choisi, restant à évaluer. Cette étape est éventuellement suivie d'une étape d'addition nécessitant une multiplication* **M** *indépendamment du modèle et des coûts annexes.*

Le but de la section suivante est de déterminer précisément ces derniers coûts dans le cas du modèle d'Edwards. Notons que comme dans la Sous-Section 1.2.4 les minuscules sont réservées aux opérations dans le corps de base $\mathbb{F}_q$.

3.4 Formules explicites pour les couplages sur courbes d'Edwards tordues

Pour appliquer l'algorithme de Miller ci-dessus, il faut évaluer une fonction g_{P_1,P_2} en un point. Le Théorème 2.5.1 montre que pour le modèle d'Edwards l'équation de la fonction g_{P_1,P_2} (Notation 3.3.3) dépend de celle de la conique C_{P_1,P_2}. Cette dernière passant par les deux points à l'infini Ω_1 et Ω_2 et par O', elle est définie par un polynôme homogène de la forme

$$c_{Z^2}(Z^2 + YZ) + c_{XY}XY + c_{XZ}XZ = 0,$$

avec $(c_{Z^2} : c_{XY} : c_{XZ}) \in \mathbb{P}^2(\Bbbk)$.
Soient $(X_3 : Y_3 : Z_3)$ les coordonnées du point $P_1 + P_2$, on exprime la fonction g_{P_1,P_2} de la façon suivante

$$g_{P_1,P_2}(X : Y : Z) = \frac{c_{Z^2}(Z+Y)Z + c_{XY}XY + c_{XZ}XZ}{(Z_3Y - Y_3Z)X}.$$

On applique ici une méthode utilisée dans le cas du modèle de Weierstraß [BLS04a, Section 4]. On construit un point $Q \in E(\mathbb{F}_{q^k})$ en appliquant un twist quadratique sur un point $Q' \in E(\mathbb{F}_{q^{k/2}})$. Pour cela, on se restreint au cas k pair. On considère également $\{1, \alpha\}$ une base de $\mathbb{F}_{q^k}$ vu comme $\mathbb{F}_{q^{k/2}}$ - espace vectoriel et on pose $\delta := \alpha^2 \in \mathbb{F}_{q^{k/2}}$. Soit $Q' = (X_0 : Y_0 : Z_0)$ un point de $E_{a\delta,d\delta}(\mathbb{F}_{q^{k/2}})$, on construit le point $Q = (X_0\alpha : Y_0 : Z_0) \in E_{a,d}(\mathbb{F}_{q^k})$ comme l'image du twist par α de Q'. En plus de garantir que le corps de définition du point Q est $\mathbb{F}_{q^k}$, cela permet de réduire grandement les opérations nécessaire au calcul de couplages comme nous le voyons ci-dessous.

On a dans l'algorithme de Miller, selon que l'étape soit celle d'addition ou de doublement, $(P_1, P_2) = (P, R)$ ou $(P_1, P_2) = (R, R)$. Posons $y_0 := \frac{Y_0}{Z_0}$ et $\eta := \frac{Z_0+Y_0}{X_0\delta}$.

$$\begin{aligned} g_{P_1,P_2}(Q) &= \frac{c_{Z^2}\frac{Z_0+Y_0}{X_0\delta}\alpha + c_{XY}y_0 + c_{XZ}}{Z_3y_0 - Y_3}, \\ &\in (c_{Z^2}\eta\alpha + c_{XY}y_0 + c_{XZ})\,\mathbb{F}^*_{q^{k/2}}. \end{aligned}$$

Remarque 3.4.1. *Les valeurs de η et y_0 étant constantes tout au long de l'algorithme de Miller, elles peuvent être précalculées. De plus elles sont dans $\mathbb{F}_{q^{k/2}}$ et les coefficients c_{Z^2}, c_{XY}, c_{XZ} sont définis sur $\mathbb{F}_q$, et comme on considère $\mathbb{F}_{q^k}$ engendré par $\{1, \alpha\}$ sur $\mathbb{F}_{q^2}$ la multiplication de $c_{Z^2}\eta$ et α n'est pas à calculer. Ainsi, en supposant que les coefficients de la conique soient connus, on peut calculer $g_{R,P}(Q)$ en $k\mathbf{m}$, les calculs de $c_{Z^2}\eta$ et $c_{XY}y_0$ demandant chacun $\frac{k}{2}\mathbf{m}$.*

Il reste donc à déterminer le nombre d'opérations pour calculer les coefficients c_{Z^2}, c_{XY}, c_{XZ} et l'addition, ou le doublement, de points.

Théorème 3.4.2. *Soient $P_1 = (X_1 : Y_1 : Z_1), P_2 = (X_2 : Y_2 : Z_2)$. Les coefficients de la conique C_{P_1,P_2} sont calculés comme suit*

1. *Si $P_1 \neq P_2, P_1 \neq O', P_2 \neq O'$, alors*

$$\begin{aligned} c_{Z^2} &= X_1X_2(Y_1Z_2 - Y_2Z_1), \\ c_{XY} &= Z_1Z_2(X_1Z_2 - X_2Z_1 + X_1Y_2 - X_2Y_1), \\ c_{XZ} &= X_2Y_2Z_1^2 - X_1Y_1Z_2^2 + Y_1Y_2(X_2Z_1 - X_1Z_2). \end{aligned}$$

2. *Si $P_1 \neq P_2 = O'$, alors $c_{Z^2} = -X_1, c_{XY} = Z_1, c_{XZ} = Z_1$.*
3. *Si $P_1 = P_2$, alors*

$$\begin{aligned} c_{Z^2} &= X_1Z_1(Z_1 - Y_1), \\ c_{XY} &= dX_1^2Y_1 - Z_1^3, \\ c_{XZ} &= Z_1(Z_1Y_1 - aX_1^2). \end{aligned}$$

Démonstration. *1.* Si $P_1 \neq P_2$, on obtient les deux équations

$$\begin{cases} c_{Z^2}(Z_1^2 + Y_1Z_1) + c_{XY}X_1Y_1 + c_{XZ}X_1Z_1 = 0, \\ c_{Z^2}(Z_2^2 + Y_2Z_2) + c_{XY}X_2Y_2 + c_{XZ}X_2Z_2 = 0. \end{cases}$$

Ainsi les formules proviennent des solutions

$$c_{Z^2} = \begin{vmatrix} X_1Y_1 & X_1Z_1 \\ X_2Y_2 & X_2Z_2 \end{vmatrix}, \quad c_{XY} = \begin{vmatrix} X_1Z_1 & Z_1^2 + Y_1Z_1 \\ X_2Z_2 & Z_2^2 + Y_2Z_2 \end{vmatrix}, \quad c_{XZ} = \begin{vmatrix} Z_1^2 + Y_1Z_1 & X_1Y_1 \\ Z_2^2 - Y_2Z_2 & X_2Y_2 \end{vmatrix}.$$

2. On se place dans le cas $P_1 \neq P_2 = O'$. La conique C_{P_1,P_2} est l'union des droites d'équation $Y + Z = 0$ et $Z_1X - X_1Z = 0$, d'où les coefficients du théorème.

3. Supposons $P_1 = P_2 = O'$, alors C_{P_1,P_2} a pour équation $X(Y+Z) = 0$ car elle est de multiplicité 3 en O'. Les coefficients $c_{Z^2} = 0, c_{XY} = 1, c_{XZ} = 1$ sont bien donnés par les formules annoncées. Supposons $P_1 = P_2 \neq O'$, utilisons les coordonnées affines $x_1 = X_1/Z_1, y_1 = Y_1/Z_1$. Les vecteurs tangents en P_1 sont colinéaires si et seulement si

$$\begin{vmatrix} dx_1^2 y_1 - y_1 & -c_{Z^2} - c_{XY} x_1 \\ ax_1 - dx_1 y_1^2 & c_{XY} y_1 + c_{XZ} \end{vmatrix} = 0.$$

On cherche donc les solutions du système linéaire

$$\begin{cases} c_{Z^2}(1 + y_1) + c_{XY} x_1 y_1 + c_{XZ} x_1 = 0, \\ c_{Z^2} x_1 (a - dy_1^2) + c_{XY}(x_1^2(a - dy_1^2) + y_1^2(dx_1^2 - 1)) + c_{XZ} y_1 (dx_1^2 - 1) = 0. \end{cases}$$

égales, à une constante multiplicative près, à

$$\begin{aligned} c_{Z^2} &= x_1(dx_1^2 y_1^2 - ax_1^2) \\ &= x_1(y_1 + 1)(y_1 - 1), \\ c_{XY} &= ax_1^2 - dx_1^2 y_1^2 - (1 + y_1) y_1 (dx_1^2 - 1) \\ &= (1 + y_1)(1 - dx_1^2 y_1), \\ c_{XZ} &= (ax_1^2 - y_1^2)(1 + y_1) - y_1(1 - y_1^2) \\ &= (ax_1^2 - y_1)(1 + y_1). \end{aligned}$$

Le point O' étant écarté, on simplifie par $-(y_1 + 1)$ et les formules sont obtenues par homogénéisation. □

3.4.1 L'étape d'addition

Le cas 1. du Théorème 3.4.2 fournit les coefficients de la conique sachant que les deux points sont distincts. En effet on peut supposer qu'aucun des points considérés n'est le point O' car pour une utilisation cryptographique nous utilisons des points dans un sous-groupe de $E_{a,d}(\mathbb{F}_p)$ de cardinal premier et grand (voir Chapitre 4), donc ne contenant aucun des quatre points triviaux de $E_{a,d}$ autre que O. Aussi considérons que les points P_1, P_2 sont donnés en coordonnées d'Edwards étendues, *i.e.* $P_i = (X_i : Y_i : T_i : Z_i)$ avec $T_i = X_i Y_i / Z_i$, et on utilise la redondance de la coordonnée T_i pour réexprimer ces coefficients :

$$\begin{aligned} c_{Z^2} &= X_1 X_2 (Y_1 Z_2 - Y_2 Z_1) \\ &= Z_1 Z_2 (T_1 X_2 - X_1 T_2), \\ c_{XY} &= Z_1 Z_2 (X_1 Z_2 - X_2 Z_1 + X_1 Y_2 - X_2 Y_1), \\ c_{XZ} &= X_2 Y_2 Z_1^2 - X_1 Y_1 Z_2^2 + Y_1 Y_2 (X_2 Z_1 - X_1 Z_2) \\ &= Z_1 Z_2 (Z_1 T_2 - T_1 Z_2 + Y_1 T_2 - T_1 Y_2). \end{aligned}$$

Ainsi on calcule les coefficients de la conique et les coordonnées étendues du point $P_1 + P_2$ pour un coût de $14\mathbf{m} + 1\mathbf{m_a}$ en suivant les formules explicites ci-dessous.

$$\begin{gathered} A = X_1 X_2, \quad B = Y_1 Y_2, \quad C = Z_1 T_2, \quad D + T_1 Z_2, \quad E + D + C, \\ F = (X_1 - Y_1)(X_2 + Y_2) - A + B, \quad G = aA + B, \quad H = D - C, \quad I = T_1 T_2, \\ c_{Z^2} = (T_1 - X_1)(T_2 + X_2) + A - I, \quad c_{XY} = X_1 Z_2 - X_2 Z_1 + F, \\ c_{XZ} = (Y_1 - T_1)(Y_2 + T_2) - B - H + I, \end{gathered}$$

$$X_3 = EF, \quad Y_3 = GH, \quad T_3 = EH, \quad Z_3 = FG.$$

Une étape d'addition dans l'algorithme de Miller sera donc effectuée pour un coût total de $1\mathbf{M} + (k+14)\mathbf{m} + 1\mathbf{m_a}$. De plus, si le point P_2 satisfait $Z_2 = 1$ alors ce coût se réduit à $1\mathbf{M} + (k+12)\mathbf{m} + 1\mathbf{m_a}$.

3.4.2 L'étape de doublement

Pour ce qui est de l'étape de doublement dans l'algorithme de Miller, plus fréquente que celle d'addition, on applique la même étude que précédemment. D'une part on multiplie les formules du Théorème 3.4.2 cas 3. par $-2Y_1/Z_1$ pour obtenir des formules plus efficaces, cela fournit les premières égalités ci-dessous. Ceci est possible car les coefficients de la conique sont définis projectivement et $Y_1 Z_1 \neq 0$ puisque $P_1 \neq T, T'$. D'autre part, si cela permet de réduire les calculs préliminaires, on utilise les coordonnées d'Edwards étendues pour obtenir les secondes formules ci-dessous.

$$\begin{aligned} c_{Z^2} &= X_1(2Y_1^2 - 2Y_1Z_1) \\ &= 2Y_1Z_1(T_1 - X_1), \\ c_{XY} &= Z_1\big(2(Z_1^2 - aX_1^2 - Y_1^2) + 2Y_1Z_1\big), \\ c_{XZ} &= Y_1(2aX_1^2 - 2Y_1Z_1) \\ &= 2Z_1(aX_1T_1 - Y_1^2). \end{aligned}$$

Bien évidemment on simplifie le facteur Z_1 apparaissant dans chacune de ces dernières formules. Les formules explicites suivantes permettent de calculer $P_3 = (X_3 : Y_3 : Z_3 : T_3)$ et $(c_{Z^2} : c_{XY} : c_{xz})$ pour un coût de $6\mathbf{m} + 5\mathbf{s} + 2\mathbf{m_a}$.

$$A = X_1^2, \quad B = Y_1^2, \quad C = Z_1^2, \quad D = (X_1 + Y_1)^2, \quad E = (Y_1 + Z_1)^2,$$

$$F = D - (A + B), \quad G = E - (B + C), \quad H = aA, \quad I = B + H, \quad J = C - I, \quad K = J + C,$$

$$c_{Z^2} = 2Y_1(T_1 - X_1), \quad c_{XY} = 2J + G, \quad c_{XZ} = 2(aX_1T_1 - B),$$

$$X_3 = FK, \quad Y_3 = I(B - H), \quad Z_3 = IK, \quad T_3 = F(B - H).$$

Ainsi une étape de doublement requiert $1\mathbf{M} + 1\mathbf{S} + (k+6)\mathbf{m} + 5\mathbf{s} + 2\mathbf{m_a}$.

3.5 Comparaison avec le modèle de Weierstraß

Dans cette section nous comparons les coûts évalués dans la précédente section avec ceux des principaux modèles présents alors dans la littérature. Notamment nous comparons nos résultats avec ceux de Chatterjee et al. [CSB05] qui utilisent des coordonnées jacobiennes et ceux de Ionica et Joux [IJ08] qui concernent les courbes d'Edwards. Ces différents coûts sont récapitulés dans le tableau 1. On note DBL le coût pour une étape de doublement, puis on distingue deux types d'étapes d'addition : l'addition mixte, notée mADD, si l'un des deux points est donné en coordonnées affines, *i.e.* $Z_2 = 1$, et l'addition générale, notée ADD, si les deux points sont donnés en coordonnées projectives. Les coordonnées jacobiennes, respectivement projectives, pour le modèle de Weierstraß sont indiquées par $\mathcal{J}$, respectivement $\mathcal{P}$, tandis que $\mathcal{E}$ correspond au modèle d'Edwards et $\mathcal{E}^e$ représente l'utilisation des coordonnées d'Edwards étendues. Les résultats présentées dans les sections précédentes sont référencés par [ALNR10]. Les coûts d'une étape d'addition ayant en commun $1\mathbf{M} + k\mathbf{m}$ quelque soit le modèle, ces opérations ont été déduites dans le tableau 1. De même pour le coût de $1\mathbf{M}+1\mathbf{S}+k\mathbf{m}$ dans les étapes de doublement.

L'utilisation des formules explicites sur le modèle d'Edwards permet non seulement de réduire les coûts pré-existant pour ce modèle, mais également ne sont pas plus élevés que ceux existant en coordonnées jacobiennes.

Modèle	DBL	mADD	ADD
$\mathcal{J}$ [IJ08, CSB05]	$1\mathbf{m} + 11\mathbf{s} + 1\mathbf{m_{a_4}}$	$9\mathbf{m} + 3\mathbf{s}$	–
$\mathcal{J}, a_4 = -3$ [CSB05]	$7\mathbf{m} + 4\mathbf{s}$	$9\mathbf{m} + 3\mathbf{s}$	–
$\mathcal{J}, a_4 = 0$ [CN05, CSB05]	$6\mathbf{m} + 5\mathbf{s}$	$9\mathbf{m} + 3\mathbf{s}$	–
$\mathcal{P}, a_4 = 0, a_6 = b^2$ [CHB$^+$09]	$3\mathbf{m} + 5\mathbf{s}$	$10\mathbf{m} + 2\mathbf{s} + 1\mathbf{m_b}$	$13\mathbf{m} + 2\mathbf{s} + 1\mathbf{m_b}$
$\mathcal{E}$ [IJ08]	$8\mathbf{m} + 4\mathbf{s} + 1\mathbf{m_d}$	$14\mathbf{m} + 4\mathbf{s} + 1\mathbf{m_d}$	–
$\mathcal{E}^e$ [ALNR10]	$6\mathbf{m} + 5\mathbf{s} + 1\mathbf{m_a}$	$12\mathbf{m} + 1\mathbf{m_a}$	$14\mathbf{m} + 1\mathbf{m_a}$

TABLEAU 1 – Comparatif de coûts des différentes étapes dans l'algorithme de Miller.

Les courbes supersingulières avec $a_4 = 0$ et a_6 un carré utilisés dans [CHB$^+$09] sont très spéciales : si $p \equiv 1 \pmod 3$ elles ont un degré de plongement $k = 2$, et si $p \equiv 2 \pmod 3$ on peut utiliser de telles courbes pour trois classes d'isomorphismes. L'étape de doublement est bien plus rapide que dans tous les autres cas mais l'addition mixte et l'addition générale sont plus lentes.

Ces comparaisons dépendent de la proportionnalité des coûts $\mathbf{m} - \mathbf{s}$ et de la taille des paramètres. Pour ce dernier point, notons que a_4 et a peuvent être choisis suffisamment petits pour que le coût de leur multiplication soit négligeable (on a vu à la fin de la Section 2.3 que l'on peut se ramener, par 2-isogénies, à une courbe d'Edwards $\mathbb{F}_q$-complète), on peut donc supposer $\mathbf{m_{a_4}} = \mathbf{m_a} = 0$. Pour l'étape de doublement nos formules ont le même coût que le plus bas pour le modèle de Weierstraß pour les courbes BN, et ont l'avantage de couvrir plus de courbes. Considérant l'étape d'addition notre coût est compétitif avec les autres modèles si le coût d'une élévation au carré $\mathbf{s}$ est très proche de celui d'une multiplication $\mathbf{m}$, et légèrement plus faible sinon.

Remarque 3.5.1. *Lubicz et Robert [LR10] présentent une nouvelle façon de calculer les couplages de Weil et de Tate en utilisant des coordonnées provenant des formules d'addition des fonctions thêta. Ses particularités sont qu'elle ne fait pas appel à l'algorithme de Miller et permet de calculer ces couplages sur toute variété abélienne, pas seulement des jacobiennes. En genre 1 et 2, cet algorithme apparaît compétitif avec l'algorithme de Miller, mais l'utilisation des courbes d'Edwards dans ce dernier semble apporter un léger avantage à la méthode classique en genre 1. Cependant la nature des deux algorithmes étant différente, il est difficile de les comparer de façon systématique. Notamment l'algorithme de Miller effectue à chaque boucle une étape de doublement suivie éventuellement d'une d'addition tandis que l'algorithme de Lubicz et Robert effectue toujours une étape de doublement et deux d'addition (voir [Rob10, Sous-Section 5.4.1]).*

Chapitre 4

Génération de courbes d'Edwards pour le calcul de couplages

Dans ce chapitre nous souhaitons appliquer la méthode de multiplication complexe (méthode CM) de construction de courbes elliptiques pour chercher des courbes d'Edwards ayant les propriétés adaptées au calcul de couplages en cryptologie. Dans la première section, nous rappelons rapidement les idées directrices de la méthode CM, puis dans la seconde section, nous détaillons la construction de courbes d'Edwards dédiées aux couplages.

4.1 Brefs rappels sur la construction par multiplication complexe

Commençons par rappeler qu'une courbe elliptique est dite à multiplication complexe si son anneau d'endomorphismes contient strictement $\mathbb{Z}$ et que toute courbe elliptique sur corps fini est à multiplication complexe (Remarque 1.2.19). Cependant nous ne nous intéressons qu'à la construction de courbes elliptiques ordinaires. En effet Menezes, Okamoto et Vanstone [MOV93] montrent que les degrés de plongement des courbes elliptiques supersingulières sont majorés par 2 sur un corps fini premier et par 6 sur un corps fini quelconque. Afin de faciliter l'arithmétique dans le corps de base on se limite à un degré de plongement supérieur à 6. Les courbes supersingulières sur un corps fini de grande caractéristique sont donc à proscrire. Notons cependant que la programmation dans un contexte cryptographique de courbes supersingulières définies sur une extension de $\mathbb{F}_3$ de grand degré sur FPGA apporte de meilleures performances que l'utilisation de courbes BN [CDF+11]. Néanmoins, seules les courbes supersingulières ayant un degré de plongement égal à 6 seraient intéressantes et leur utilisation resterait limitée aux petits niveaux sécurité (les deux premières entrées du Tableau 2 page 47).

Le résultat central de la théorie est dû à Deuring (Lifting Theorem [Lan87, Chapter 13]). Soit $\mathcal{O}$ un ordre dans un corps quadratique imaginaire. On peut vulgariser ce résultat en disant qu'une courbe elliptique $\overline{E}/\mathbb{F}_p$ ayant multiplication complexe par $\mathcal{O}$ est la réduction d'une courbe elliptique $E/\mathbb{C}$ ayant multiplication complexe par $\mathcal{O}$.

La méthode CM a été introduite en cryptologie par Atkin et Morain [AM93] dans le but de vérifier la primalité d'entiers. Elle est basée sur la théorie du corps de classe pour laquelle nous renvoyons le lecteur à [Sil94, Chapter II]. Dans cette section, nous voyons comment construire des courbes elliptiques sur $\mathbb{C}$ ayant un anneau d'endomorphismes prédéterminé, puis expliquons comment la réduction du polynôme de classes de Hilbert permet de construire des courbes elliptiques ayant le nombre de points voulu sur corps finis.

Les rappels suivants concernant les courbes elliptiques complexes sont tirés de [Sil92, Section VI.5]. Toute courbe elliptique $E/\mathbb{C}$ peut être représentée comme un tore complexe (et réciproquement), *i.e.* il existe un réseau $\Lambda \subset \mathbb{C}$ et un isomorphisme analytique tels que $\mathbb{C}/\Lambda \simeq E(\mathbb{C})$. L'anneau d'endomorphismes de E peut être décrit par

$$\mathrm{End}(E) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}.$$

De plus E est à multiplication complexe si et seulement si $\mathrm{End}(E) \otimes \mathbb{Q}$ est isomorphe à un corps quadratique imaginaire et $\mathrm{End}(E)$ est isomorphe à un ordre dans ce corps. Dans la suite nous notons $\mathbb{K}$ un corps quadratique imaginaire. Nous considérons les cas où $\mathrm{End}(E) = \mathcal{O}_\mathbb{K}$ est l'anneau des entiers de $\mathbb{K}$, et notons

$$\mathrm{Ell}(\mathcal{O}_\mathbb{K}) = \{\text{classes d'isomorphismes de } E/\mathbb{C} : \mathrm{End}(E) \simeq \mathcal{O}_\mathbb{K}\}.$$

Cet ensemble est en bijection avec l'ensemble des classes de réseaux complexes ayant multiplication complexe par $\mathcal{O}_\mathbb{K}$ modulo la relation d'homothétie. En suivant [Sil94, Section II.1], si $\mathfrak{a}$ est un idéal fractionnaire de $\mathbb{K}$ (voir [Lan94, Section I.6] pour des rappels concernant les idéaux fractionnaires et les anneaux de Dedekind) alors $\mathfrak{a} \subset \mathbb{C}$ est un réseau et la courbe elliptique associée a multiplication complexe par $\mathcal{O}_\mathbb{K}$. On note $\mathrm{Cl}(\mathcal{O}_\mathbb{K})$ le groupe de classes de $\mathcal{O}_\mathbb{K}$ et $h_\mathbb{K}$ son cardinal, on a alors

$$\#\,\mathrm{Ell}(\mathcal{O}_\mathbb{K}) = h_\mathbb{K}.$$

Le théorème suivant donne le lien étroit entre les j-invariants de ces différentes classes. Il amène à définir l'outil central dans la méthode CM : le *polynôme de classes de Hilbert* (voir la définition 4.1.2).

Théorème 4.1.1 ([Sil94, Theorem II.4.3.(c), Theorem II.6.1])**.** *Soient $\mathbb{K}$ un corps quadratique imaginaire et $j_1, \ldots, j_{h_\mathbb{K}}$ les j-invariants de courbes elliptiques représentant les classes de $\mathrm{Ell}(\mathcal{O}_\mathbb{K})$. L'ensemble $\{j_1, \ldots, j_{h_\mathbb{K}}\}$ forme une classe de conjugaison pour l'action de $\mathrm{Gal}\left(\overline{\mathbb{K}}/\mathbb{K}\right)$ et sont des entiers algébriques.*

Définition 4.1.2. *Soient $\mathbb{K}$ un corps quadratique et j l'un des j-invariants énoncés dans le Théorème 4.1.1. On note $H_\mathbb{K}(X)$ le polynôme minimal de j. On a $H_\mathbb{K}(X) \in \mathbb{Z}[X]$ et*

$$H_\mathbb{K}(X) = \prod_{i=1}^{h_\mathbb{K}} (X - j_i)\,.$$

Il est appelé le polynôme de classes de Hilbert.

Enfin nous allons voir comment une courbe elliptique sur $\mathbb{C}$ se réduit en une courbe elliptique sur un corps fini premier $\mathbb{F}_p$ dont on sait le nombre de points $\mathbb{F}_p$-rationnels, et comment en trouver l'équation. On commence par introduire le discriminant de $\mathbb{K}$, les constantes pouvant légèrement différer d'un auteur à l'autre, on choisit d'utiliser la définition de [AM93] suivante

Définition 4.1.3. *Soit $\mathbb{K}$ un corps quadratique imaginaire. Son* discriminant *est l'entier positif $D \equiv 3 \pmod 4$, $D \equiv 4, 8 \pmod{16}$, non divisible par un facteur carré impair et tel que $\mathbb{K} = \mathbb{Q}(\sqrt{-D})$ et $\mathcal{O}_\mathbb{K} = \mathbb{Z}[\omega]$ avec*

$$w = \begin{cases} \dfrac{\sqrt{-D}}{2} & \text{si } D \equiv 0 \pmod 4, \\ \dfrac{1+\sqrt{-D}}{2} & \text{sinon.} \end{cases}$$

Théorème 4.1.4 ([Lan87, Chapter 13, Theorem 12]). *Soient $\mathbb{K}$ un corps quadratique imaginaire, $E/\mathbb{C}$ une courbe elliptique ayant multiplication complexe par $\mathcal{O}_\mathbb{K}$ et $p \nmid \Delta(E)$ un nombre premier. L'idéal (p) se décompose complètement dans $\mathcal{O}_\mathbb{K}$ en $(p) = \mathfrak{P}\mathfrak{P}'$ avec $\mathfrak{P}, \mathfrak{P}'$ idéaux premiers si et seulement si la réduction de E modulo $\mathfrak{P}$, notée $\overline{E}$, est une courbe elliptique ordinaire sur $\mathbb{F}_p$. Dans ce cas,* $\mathrm{End}(E) \simeq \mathrm{End}(\overline{E})$.

Théorème 4.1.5 ([AM93, Theorem 3.1, Theorem 3.2]). *Soient $\mathbb{K}$ un corps quadratique imaginaire, $E/\mathbb{C}$ une courbe elliptique ayant multiplication complexe par $\mathcal{O}_\mathbb{K}$ et p un nombre premier. Les conditions suivantes sont équivalentes.*

1. $\exists\ \pi \in \mathcal{O}_\mathbb{K} : p = \pi\overline{\pi}$.
2. *(p) se décompose totalement dans $\mathcal{O}_{\mathbb{K}(j(E))}$.*
3. *Le polynôme $H_\mathbb{K}(X) \pmod p$ n'a que des racines simples dans $\mathbb{F}_p$.*

Si p satisfait la condition 1. ci-dessus, on dit alors que p est une *norme* dans $\mathbb{K}$. Il satisfait l'*équation aux normes*

$$4p = \mathrm{Tr}(\pi)^2 + Dv^2, \tag{4.1}$$

où $\mathrm{Tr}(\pi) = \pi + \overline{\pi} \in \mathbb{Z}$ est la *trace* de π et $v \in \mathbb{Z}$.

L'élément π représente alors l'endomorphisme de Frobenius de $\overline{E}/\mathbb{F}_p$, on a ainsi

$$\left|\overline{E}(\mathbb{F}_p)\right| = p + 1 - \mathrm{Tr}(\pi).$$

Supposons donc donnés un corps quadratique $\mathbb{K}$, le polynôme $H_\mathbb{K}(X)$, p un nombre premier satisfaisant la condition 1. du Théorème 4.1.5 et posons $n = p + 1 - (\pi + \overline{\pi})$. On considère une courbe elliptique dont le j-invariant est une racine de $H_\mathbb{K}(X) \pmod p$ (voir Proposition 1.2.5) et on sait alors qu'elle ou une tordue quadratique aura n points $\mathbb{F}_p$-rationnels, puisque le j-invariant décrit la classe d'isomorphisme sur $\overline{\mathbb{F}_p}$ d'une courbe elliptique. On peut choisir laquelle des deux a le bon nombre de points en vérifiant que $[n]$ appliqué à un point arbitraire est l'élément neutre. Mais le simple fait de chercher à générer un point aléatoire fait appel au calcul d'un symbole de Jacobi et du calcul d'une racine carrée. Aussi Rubin et Silverberg [RS10] donnent des algorithmes simples retournant le signe de la trace de $\overline{E}/\mathbb{F}_p$ d'après des congruences modulo 4 des solutions de l'équation (4.1). En dépit de leur simplicité, ces algorithmes proviennent de résultats profonds des mêmes auteurs [RS09] sur le calcul du caractère de Hecke, pour $\mathbb{K}$ fixé, de E qui détermine le Frobenius de $\overline{E}$.

Nous terminons cette section en citant des papiers récents traitant du calcul des polynômes de classe de Hilbert. Notons qu'un nombre suffisant a été précalculé [CFA+06, Remark 18.1] permettant de générer les courbes souhaitées. Remarquons aussi que les polynôme de classe de Hilbert nous ont été bien commodes pour illustrer les bases théoriques de la méthodes CM, mais qu'en pratique on peut privilégier l'utilisation des polynômes de Weber associés à d'autres invariants de classe [AM93, Subsections 7.2, 8.6].

On dispose de trois méthodes pour calculer des polynômes de classe de Hilbert $H_\mathbb{K}(X)$, une faisant appel à de l'analyse complexe [Eng09], un algorithme p-adique [Brö08] et une basée sur le théorème des restes chinois (CRT) [BBEL08]. Mais ces polynômes sont riches en informations, et cela se ressent dans la taille de leurs coefficients. Cette dernière est en $O(|D|^{1+\epsilon})$, où D est le discriminant de $\mathbb{K}$. Ceci rend leur manipulation seulement envisageable pour de petits discriminants, *i.e.* $|D| \leq 10^{10}$ en considérant des polynômes de classe ayant de plus petits coefficients, l'espace mémoire disponible étant mis en défaut. Les méthodes citées ci-dessus sont considérées comme optimales dans le sens où leur complexité est également en $O(|D|^{1+\epsilon})$.

Se fixant les paramètres D et p, Sutherland [Sut11] améliore la méthode CRT avec un algorithme de même complexité en temps de calculs mais nécessitant un espace mémoire en

$O(|D|^{1/2+\epsilon}\log(p))$ (sous l'hypothèse de Riemann généralisée), en retournant directement une racine de $H_{\mathbb{K}}(X) \pmod p$, évitant le calcul des polynômes de classe en entier suivi d'une réduction modulo p. Ceci permet de construire des courbes elliptiques ayant multiplication complexe par $\mathbb{K}$ de discriminant vérifiant $|D| \geq 10^{16}$ et p de taille cryptographique [ES10, Sut10].

4.2 Constructions spécifiques et exemples

L'adjectif anglais "pairing-friendly" est très commode pour exprimer qu'une courbe est bien adaptée au calcul de couplages (nous allons voir ci-dessous que l'efficacité de tels calculs est généralement mauvaise pour les courbes elliptiques), mais la langue de Shakespeare est bien plus modelable que celle de Molière et je ne connais pas d'adjectif français équivalent. Il m'arrivera donc d'utiliser l'anglicisme "pairing-friendly" signifiant "bien adaptée au calcul de couplages" pour améliorer la clarté de la rédaction.

Nous allons considérer des courbes elliptiques $E/\mathbb{F}_q$ dans le but de construire des courbes d'Edwards. En particulier, $E(\mathbb{F}_q)$ doit posséder un sous-groupe d'ordre 4, *i.e.* $\left|E(\mathbb{F}_q)\right|$ est divisible par 4. Dans cette section, nous notons

$$n = \left|E(\mathbb{F}_q)\right| = 4hr,$$

où r est le plus grand entier premier divisant $\left|E(\mathbb{F}_q)\right|$. $4h$ est appelé le *cofacteur* de $E/\mathbb{F}_q$.

Dans une optique cryptographique de l'utilisation des courbes d'Edwards, nous souhaitons proposer des courbes répondant aux critères de sécurité actuellement en vigueur (voir le Tableau 2 ci-dessous).

La construction de ces courbes est basée sur des méthodes pré-existantes que l'on trouvera regroupées pour l'essentiel dans [FST06]. Celles-ci font appel à la méthode CM de construction de courbes elliptiques brièvement rappelée dans la Section 4.1 précédente.

Pour une courbe elliptique $E/\mathbb{F}_q$, être *pairing-friendly* est plutôt vague. On a besoin d'un sous-groupe de points $\mathbb{F}_q$-rationnels d'ordre premier r suffisamment grand pour éviter les attaques génériques, et d'un degré de plongement k relatif à r petit afin d'apporter une arithmétique dans $\mathbb{F}_{q^k}^*$ efficace (voir la Remarque 3.3.6 page 38). Cependant, ce dernier ne doit pas être trop petit afin d'éviter l'attaque de l'index dans $\mathbb{F}_{q^k}^*$. Ces notions de grandeur sont subjectives, et Freeman et al [FST06] proposent les bornes

$$\begin{aligned} &r \geq \sqrt{q}, \\ &k \leq \log_2(r)/8. \end{aligned} \tag{4.2}$$

Notons que cette définition inclut les courbes elliptiques ayant un degré de plongement k pas assez grand pour se prémunir d'une attaque de type MOV (Section 3.1). On cherchera donc à construire des courbes elliptiques ayant un degré de plongement k équilibré, *i.e.* offrant une sécurité contre l'attaque du calcul de l'index dans $\mathbb{F}_{q^k}^*$ équivalente à une attaque du DLP sur $E(\mathbb{F}_q)$.

Les courbes elliptiques pairing-friendly sont rares. Balasubramanian et Koblitz [BK98] ont montré que pour la plupart des courbes elliptiques $E/\mathbb{F}_q$ avec $r \sim q$ on a $k \sim q$. Les calculs sont alors infaisables dans l'extension $\mathbb{F}_{q^k}$. Nous avons donc besoin de constructions spécifiques pour les courbes elliptiques en vue de calculs de couplages. L'idée conductrice est de fixer le degré de plongement k et de déterminer des polynômes $q(x), t(x), r(x) \in \mathbb{Q}[x]$ à valeurs entières (sur $\mathbb{Z}$) tels que si $q(x_0)$ est une puissance d'un nombre premier pour un certain entier x_0, alors il existe une courbe elliptique $E/\mathbb{F}_{q(x_0)}$ de trace $t(x_0)$ et un sous-groupe de $E\left(\mathbb{F}_{q(x_0)}\right)$ d'ordre $r(x_0)$ (non

nécessairement premier) de degré de plongement relatif à $r(x_0)$ égal à k (indépendant de x_0). Le degré de plongement est fixé en imposant la condition

$$r(x) \big| \Phi_k\big(t(x)-1\big),$$

où Φ_k est le $k^{\text{ième}}$ polynôme cyclotomique car on souhaite que q soit d'ordre k dans $\mathbb{F}_r$([FST06, Proposition 2.4]). Un avantage à la donnée de tels polynômes est de conserver un degré de liberté sur la taille du paramètre r.

Définition 4.2.1. *Soient $E/\mathbb{F}_q$ une courbe elliptique et r divisant $|E(\mathbb{F}_q)|$. On appelle* valeur-ρ *de E (par rapport à r) la quantité*

$$\rho(E) = \frac{\log(q)}{\log(r)}.$$

Dans notre cas on ne s'intéresse qu'au cas où r est le plus grand facteur premier de n, donc la valeur-ρ sera toujours prise par rapport à r. Notons que les courbes elliptiques que nous considérons ont une valeur-ρ comprise entre 1 et 2. Une valeur-ρ proche de 1 est le meilleur cas car correspond à un petit cofacteur par les bornes de Hasse-Weil, et $\rho \leq 2$ dans les constructions de [FST06] grâce à la borne (4.2) sur r.

Dans le but de simplifier l'arithmétique dans le corps de base $\mathbb{F}_q$, les courbes elliptiques à usage cryptographique sont considérées sur de grandes extensions de $\mathbb{F}_2$ ou bien sur un corps premier de grande caractéristique $\mathbb{F}_p$. La définition du modèle d'Edwards que nous avons étudié excluant le cas de la caractéristique 2, nous allons générer des courbes sur des corps premiers $\mathbb{F}_p$. Nous supposons donc dans la suite que $q = p$ est un nombre premier.

Comme nous l'avons vu deux types d'attaques doivent être prises en compte pour estimer la sécurité inhérente à un courbe elliptique $E/\mathbb{F}_p$. Pour cela nous allons choisir p et k de telle sorte que les difficultés du DLP sur la courbe d'Edwards engendrée et dans le corps fini $\mathbb{F}_{p^k}^*$ soient équilibrées. Nous reprenons les niveaux de sécurité recommandés par ECRYPT [Sma10, p.32] et donnons les tailles binaires du plus grand entier premier r divisant $\big|E(\mathbb{F}_p)\big|$ et de p^k dans le tableau 2 pour un niveau de sécurité équivalent. La référence est la taille des clés secrètes utilisées dans AES.

Sécurité (bits)	80	96	112	128	160	256
$\log_2(r)$	160	192	224	256	320	512
$\log_2\left(p^k\right)$	1248	1776	2432	3248	4800	15424
$\rho \cdot k$	7.80	9.25	10.86	12.67	15	30.13

TABLEAU 2 – Tailles optimales de n, p et $\rho \cdot k$ pour différents niveaux de sécurité standards.

Nous fournissons ci-dessous un exemple détaillé de courbe d'Edwards pairing-friendly pour chacun des niveaux de sécurité annoncé dans le tableau 2. Galbraith, McKee et Valença fournissent toutes les familles quadratiques, *i.e.* dont le polynôme $q(x)$ est quadratique, de courbes elliptiques ayant un cofacteur divisible par 2,3,4,5, un degré de plongement égal à 3,4,6 [GMV07, Theorem 1]. Ils généralisent le travail de Miyaji, Nakabayashi et Takano [MNT01] qui ont donné les familles explicites de polynômes $(q(x), t(x))$ générant des courbes elliptiques d'ordre premier pour ces mêmes degrés de plongement. Les deux premiers sont tirés de [GMV07, Table 6]. Il est remarquable que parmi les cinq familles quadratiques données la majorité des courbes que nous avons construites proviennent de la famille paramétrée par les polynômes

$$\begin{aligned} q(x) &= 208x^2 + 30x + 1, \\ t(x) &= -26x - 2. \end{aligned}$$

Ce fait était déjà annoncé dans [GMV07] et les deux premiers exemples ci-dessous proviennent de cette famille. Raisonnons donc avec ces polynômes. Faisant varier le discriminant D, nous cherchons à résoudre l'équation (4.1). Comme remarqué dans [MNT01], on se ramène à résoudre une équation de Pell, ici de la forme

$$u^2 - 39Dv^2 = 4$$

avec $u = 39x + 11$. Celle-ci est une norme dans le corps quadratique réel $K = \mathbb{Q}\big(\sqrt{39D}\big)$. Si elle possède une solution (u_0, v_0) on les construit toutes en multipliant $u_0 + \sqrt{39D}\, v_0$ par une puissance d'une unité fondamentale de K. On en déduit une valeur x_0 pour laquelle on teste la primalité de $q(x_0)$. On sait alors qu'il existe une courbe elliptique ayant multiplication complexe par $\mathbb{Q}\big(\sqrt{-D}\big)$ définie sur $\mathbb{F}_{q(x_0)}$ et d'ordre $q(x_0) + 1 - t(x_0)$ divisible par 4. Pour une utilisation cryptographique, on ne considère que les entiers x_0 tels que la taille de $p = q(x_0)$ corresponde à l'un des deux premiers niveaux de sécurité dans le Tableau 2 avec $k = 6$. Il ne reste alors plus qu'à conserver les courbes dont l'ordre ait un facteur premier r de taille voulue puis d'appliquer des 2-isogénies jusqu'à faire apparaître un point rationnel d'ordre 4. Pour nos exemples nous nous sommes limités à $D < 20000$.

Pour les autres exemples, les constructions sont tirées de [FST06] où les auteurs fixent également le discriminant D. On choisit un degré de plongement k et une construction correspondante. On fait alors varier x pour que $q(x)$ soit un nombre premier de taille souhaitée et $q(x)+1-t(x)$ soit divisible par 4. Notons par exemple que pour la construction utilisée dans les Exemples iii. et iv. ci-dessous, on se restreint à $x \equiv 1 \pmod 4$ pour que l'ordre de la courbe soit divisible par 4.

Pour chaque exemple nous donnons la sécurité de la courbe contre les attaques génériques et contre le calcul de l'index.

i. Niveau de sécurité de 80 bits (générique : 82 bits, calcul de l'index : 79 bits)
$k = 6, \rho = 1.22$ (voir [GMV07, Table 6]) :
$D = 4 \cdot 7230, \lceil \log_2(r) \rceil = 165, \lceil \log_2(h) \rceil = 34, \lceil \log_2(p) \rceil = 201, \lceil \log_2\left(p^k\right) \rceil = 1206.$

$$\begin{aligned}
p &= 20516136637681296060935834328758873984153019622274901875088 01,\\
r &= 44812545413308579913957438201331385434743442366277,\\
h &= 7 \cdot 733 \cdot 2230663,\\
d &= 11006613094214930568367451593188892082109313804594175789766 26.
\end{aligned}$$

ii. Niveau de sécurité de 96 bits (générique : 95 bits, calcul de l'index : 93 bits)
$k = 6, \rho = 1.48$ (voir [GMV07, Table 6]) :
$D = 4 \cdot 4630, \lceil \log_2(r) \rceil = 191, \lceil \log_2(h) \rceil = 90, \lceil \log_2(p) \rceil = 283, \lceil \log_2\left(p^k\right) \rceil = 1698.$

$$\begin{aligned}
p &= 12076422473257620999622772924220230535655104285600826357856070179619031510615886361601,\\
r &= 24988862358874094149482890202204768877072632109398454858 39,\\
h &= 11161 \cdot 19068349 \cdot 5676957216676051,\\
d &= 27639154268991893588450593507273815049468152861899724386810826363999840671659115908 84.
\end{aligned}$$

iii. Niveau de sécurité de 112 bits (générique : 112 bits, calcul de l'index : 117 bits)
$k = 8, \rho = 1.50$ (voir [FST06, Example 6.10]) :
$D = 4, \lceil \log_2(r) \rceil = 224, \lceil \log_2(h) \rceil = 111, \lceil \log_2(p) \rceil = 337, \lceil \log_2\left(p^k\right) \rceil = 2696.$

$$p = 233773665369910566926038390015691888142454746929295686689625913289090$$
$$94370357234875602877887448160428 9,$$
$$r = 22985796260053765810955211899935144604417092746113717429138553265289,$$
$$h = 315669989 \cdot 558193107149 \cdot 14429732414341,$$
$$d = 21373841441636012883551957246343228553489584548232523879997636200280 7$$
$$96159999984855664083615810471203 2.$$

iv. Niveau de sécurité de 128 bits (générique : 133 bits, calcul de l'index : 127 bits)
$k = 8, \rho = 1.50$ (voir [FST06, Example 6.10]) :
$D = 4, \lceil \log_2(r) \rceil = 267, \lceil \log_2(h) \rceil = 133, \lceil \log_2(p) \rceil = 401, \lceil \log_2\left(p^k\right) \rceil = 3208.$

$$p = 5106500003052745062671102775396566649855857676935384847563820321458 49$$
$$74495354436071209268470508469629312810691036880709,$$
$$r = 8337030425086788445100704671763896482549397437850042633596560118040562$$
$$641504433,$$
$$h = 5 \cdot 17 \cdot 1229 \cdot 3181 \cdot 46080531647786897856138922773 41,$$
$$d = 2553250001526372531335551387698283324927928838467692423781910160729248$$
$$72476772180356046342352542348146564053455184403 55.$$

v. Niveau de sécurité de 160 bits (générique : 164 bits, calcul de l'index : 154 bits)
$k = 10, \rho = 1.49$ (voir [FST06, Example 6.5]) :
$D = 4, \lceil \log_2(r) \rceil = 328, \lceil \log_2(h) \rceil = 160, \lceil \log_2(p) \rceil = 490, \lceil \log_2\left(p^k\right) \rceil = 4900.$

$$p = 3196670719340789713156777469647383628127137039140603444123206048687086$$
$$138966651733275252543330209754427990875101879841425427646115157594515$$
$$629491249,$$
$$r = 5468127044386521901760484736383627796884230617944997563119259455454621$$
$$52449512232744941959488864241,$$
$$h = 2^4 \cdot 70199^4 \cdot 7831391^4,$$
$$d = 3668389580328868388573603941665358577475569348526211751641207343461016$$
$$28194129743602008259319768868802620569094456792293200142806009932471922$$
$$115210.$$

vi. Niveau de sécurité de 256 bits (générique : 259 bits, calcul de l'index : 259 bits)
$k = 22, \rho = 1.39$ (voir [FST06, Construction 6.6]) :
$D = 12, \lceil \log_2(r) \rceil = 519, \lceil \log_2(h) \rceil = 204, \lceil \log_2(p) \rceil = 724, \lceil \log_2\left(p^k\right) \rceil = 15928.$

$$p = 7932439078365382251019196635819537709137655806628495942035746368745188368582705551601449209838272803868154339121902148247413729605337155986911218807161824591404393677677719266617711394358641504491185166978529065469512 3,$$

$$r = 9621311878085603778985691952625727109889848694647550025094596661780692626283672821912529731051013737049538186606705506586597903896379176063425017329234863 69,$$

$$h = 3^5 \cdot 7 \cdot 13^2 \cdot 19^2 \cdot 37^2 \cdot 6421^2 \cdot 7219 \cdot 3498559^2 \cdot 22526869^2 \cdot 78478074679,$$

$$d = 2644146275479397808108398267273953832599874449813525607535828770863200746806506337805719203736155180325092008523328642164130413289498650166667597282180194560972046877108310481765609201687961490116024544394578625639951 8.$$

Deuxième partie

Étude géométrique et arithmétique de la notion de complétude pour une loi d'addition sur une variété abélienne

Rappelons qu'une *variété abélienne* A sur un corps parfait $\mathbb{k}$ est un groupe algébrique qui est également une variété projective. La loi de groupe étant donnée par un morphisme $\mu : A \times A \to A$, elle est localement décrite, après avoir fixé un plongement projectif de A, par des polynômes bihomogènes. Ces derniers constituent ce que l'on appelle une *loi d'addition* (voir la Définition 6.1.2 pour une définition rigoureuse).

Nous nous limitons, pour les aspects effectifs, aux courbes elliptiques et aux surfaces abéliennes, mais ce n'est pas une véritable restriction. En effet, le problème du logarithme discret sur les variétés abéliennes de dimension supérieure devient plus faible. Pour le genre 3 nous renvoyons à [DT08] pour le cas non hyperelliptique et à [Smi09] pour le cas hyperelliptique.

Suite à l'étude, dans la première partie, de la loi d'addition usuelle sur les courbes d'Edwards, on souhaiterait comprendre plus précisément l'origine de sa complétude arithmétique (lorsque le paramètre de la courbe n'est pas un carré) et comprendre s'il existe un critère aidant à la construction d'une loi effective. Nous répondons à cette première question dans l'article [AKR11]. Kohel apporte des précisions en genre 1 sur la seconde ([Koh11] ou la Sous-Section 6.2.3 page 72) et on trouve des informations, plus limitées, en genre 2 [AC11].

Cette partie reprend les résultats présentés dans les articles [AKR11] et [AC11], le premier correspondant essentiellement au Chapitre 6 et le second au Chapitre 7. Le Chapitre 6 comporte deux résultats importants : Étant donnée une variété abélienne $A/\mathbb{k}$, le premier est que, quels que soient la variété abélienne et le plongement projectif considérés, il n'existe pas de loi d'addition (géométriquement) complète, *i.e.* définie sur $(A \times A)\big(\overline{\mathbb{k}}\big)$; le second est qu'il existe un plongement projectif pour lequel il existe une loi d'addition $\mathbb{k}$-complète, *i.e.* définie sur $(A \times A)(\mathbb{k})$, pourvu que l'on puisse prendre des extensions séparables de degré suffisamment grand sur $\mathbb{k}$. La complétude de lois d'addition sur des modèles elliptiques ayant déjà été bien étudiée, nous nous intéressons dans le Chapitre 7, aux surfaces abéliennes et plus spécifiquement à leur plongement projectif dans $\mathbb{P}^{15}$. Nous montrons l'existence d'un ensemble complet de lois d'addition de cardinalité minimale et apportons les premières formules explicites d'une loi d'addition $\mathbb{k}$-complète sur une surface abélienne définie sur un corps fini non binaire. Mais nous verrons que bien que la complétude arithmétique de cette loi d'addition soit une réussite, elle en est malheureusement d'autant moins efficace. Le Chapitre 5 introduit les notions et les résultats préliminaires éclairant l'étude de ces deux derniers chapitres, notamment les résultats de Lange et Ruppert [LR85] apportant le socle sur lesquels ces travaux sont construits.

Chapitre 5

Rappels sur les variétés abéliennes

Nous introduisons ici la théorie des fibrés en droites – *i.e.* une fibration sur une variété algébrique dont les fibres sont des droites (vectorielles) – sur une variété algébrique lisse et quelques résultats sur les variétés abéliennes dans le but de les appliquer dans les chapitres suivants. Nous expliquons notamment le lien entre diviseurs (de Cartier) et fibrés en droites dans la première section. Il existe également une équivalence avec les faisceaux inversibles [Har77, Section II.6], mais nous avons choisi de ne pas les utiliser ici. Nous donnons ensuite les rappels qui nous serons nécessaires dans la suite sur les variétés abéliennes.

5.1 Diviseurs et fibrés en droites

Les rappels de cette section sont tirés de [HS00, Sections A.2, A.3], [Sha94a, Section III.1], [Sha94b, Section VI.1]. Sans mention contraire, les variétés algébriques considérées sont définies sur un corps $\Bbbk$ algébriquement clos.

5.1.1 Diviseurs, systèmes linéaires complets

Définition 5.1.1. *Soit X une variété algébrique irréductible et lisse*[1]*. On généralise la définition de diviseur sur une courbe vue au début de la Section 1.1, en définissant un* diviseur (de Weil) *comme une somme formelle entière de sous-variétés fermées de X irréductibles et de codimension un. On le note*

$$D = \sum n_i V_i.$$

Le *support* d'un diviseur de Weil est l'ensemble des sous-variétés V_i attachées à un entier non nul. Il est dit *effectif* si les entiers n_i sont positifs. Il reste à définir les diviseurs principaux sur X, *i.e.* les diviseurs de fonctions. Soient V une sous-variété irréductible de X de codimension un et $f \in \Bbbk(X)^*$. Il existe un ouvert affine U sur lequel f soit régulière et V définie par une équation g. On définit alors $\mathrm{ord}_V(f)$ le plus grand entier a tel que $f = g^a h$, h régulière sur U. On définit ainsi le diviseur *principal*

$$\mathrm{div}(f) := \sum \mathrm{ord}_V(f) V,$$

la somme parcourant toutes les sous-variétés irréductibles de X de codimension un.

Une autre façon de définir un diviseur – *diviseur de Cartier* – est par la donnée de couples $(U_i, f_i)_{i \in I}$, les ouverts U_i formant un recouvrement de X et les fonctions f_i non identiquement

1. Cette théorie peut aussi être développée si X est supposée non lisse, mais ce cas ne se présentera pas dans notre étude et cela facilite l'introduction d'objets tels que les diviseurs de Weil principaux et la correspondance entre diviseurs de Weil et diviseurs de Cartier.

nulles vérifiant la condition de compatibilité suivante : f_i/f_j et f_j/f_i sont régulières sur $U_i \cap U_j$. Deux familles $(U_i, f_i)_{i\in I}$ et $(V_j, g_j)_{j\in J}$ décrivent le même diviseur si, pour tout i, j, f_i/g_j est régulière sur $U_i \cap V_j$. La somme de deux diviseurs de Cartier $(U_i, f_i)_{i\in I}$ et $(U_j, g_j)_{j\in J}$ est définie par $(U_i \cap U_j, f_i g_j)_{(i,j)\in I\times J}$. Le *support* d'un tel diviseur est l'ensemble des zéros et des pôles des fonctions f_i. Il est dit *effectif* s'il peut être défini par (U_i, f_i) avec f_i régulière sur U_i. Enfin, les diviseurs de Cartier *principaux* sont ceux de la forme (X, f) pour $f \in \Bbbk(X)^*$.

On relie les diviseurs de Weil et de Cartier comme suit. Soient V une sous-variété de X irréductible et de codimension un et D un diviseur de Cartier décrit par $(U_i, f_i)_{i\in I}$. On considère un ouvert U_{i_0} tel que $U_{i_0} \cap V \neq 0$. On définit $\mathrm{ord}_V(D) := \mathrm{ord}_V(f_{i_0})$ indépendamment du choix du couple (U_{i_0}, f_{i_0}). On associe alors à D le diviseur de Weil $\sum \mathrm{ord}_V(D)V$. Cette application envoie les diviseurs de Cartier principaux (respectivement effectifs) sur les diviseurs de Weil principaux (respectivement effectifs). De plus, X étant lisse, c'est un isomorphisme de groupes.

On définit, comme dans le cas des courbes lisses (Définition 1.1.2 page 14) l'*espace de Riemann-Roch* associé à un diviseur D de X

$$L(D) := \{f \in \Bbbk(X)^*,\ \mathrm{div}(f) + D \geq 0\} \cup \{0\}.$$

C'est un $\Bbbk$-espace vectoriel de dimension finie notée $l(D)$.

Définition 5.1.2. *Étant donné un diviseur D, un* système linéaire *est un ensemble de diviseurs effectifs linéairement équivalents à D. L'ensemble de tous ces diviseurs est appelé le* système linéaire complet *de D, on le note $|D|$.*

Ce dernier est paramétré par $\mathbb{P}\big(L(D)\big) \cong \mathbb{P}^{l(D)-1}$ grâce à l'application

$$\begin{aligned}\mathbb{P}\big(L(D)\big) &\to |D| \\ \bar{f} &\mapsto D + \mathrm{div}(f),\end{aligned}$$

où $\bar{f}$ désigne la classe de f modulo $\Bbbk^*$. Soit $f_1, \ldots, f_{l(D)}$ une base de $L(D)$, on définit le morphisme

$$\begin{aligned}\varphi_{L(D)} : X &\to \mathbb{P}^{l(D)-1} \\ x &\mapsto \big(f_1(x) : \cdots : f_{l(D)}(x)\big).\end{aligned}$$

Il est bien défini modulo les automorphismes de $\mathbb{P}^{l(D)-1}$ et en dehors des pôles des fonctions f_i et de leurs zéros communs. D'où la définition suivante

Définition 5.1.3. *Les* points de base *de $|D|$ sont les points dans l'intersection des supports des diviseurs dans $|D|$. Si cette intersection est vide, on dit que $|D|$ est* sans point de base.

On s'intéresse aux diviseurs dont l'espace de Riemann-Roch associé a suffisamment de fonctions pour définir un plongement projectif de X.

Définition 5.1.4. *Un diviseur D est dit* très ample *si le morphisme $\varphi_{L(D)}$ précédent est un plongement. Il est dit* ample *si l'un de ses multiples (positifs) est très ample.*

Nous ne donnons les définitions ci-dessus pour des diviseurs et énoncerons les résultats associés dans le cas des fibrés en droite à la fin de la prochaine sous-section.

Le dernier résultat cette sous-section justifie que l'on se place sur un corps algébriquement clos dans ces rappels et que tout se passe bien pour les questions concernant les diviseurs lorsque $\Bbbk$ n'est pas algébriquement clos. On en déduit que, si D est un diviseur $\Bbbk$-rationnel, alors il existe une base de $L(D)$ de fonctions définies sur $\Bbbk$.

Proposition 5.1.5. *Soient $\Bbbk$ un corps parfait, $X/\Bbbk$ une variété projective et D un diviseur $\Bbbk$-rationnel sur X. Notons $L_\Bbbk(D) := \big\{f \in \Bbbk(X)^* \ ; \ D + \mathrm{div}(f) \geq 0\big\} \cup \{0\}$. On a*

$$L_\Bbbk(D) \otimes_\Bbbk \overline{\Bbbk} = L(D).$$

De plus, si D est un diviseur principal, il existe une fonction $f \in \Bbbk(X)$ telle que $D = \mathrm{div}(f)$.

Dans la prochaine sous-section nous définissons les fibrés en droites et donnons un aperçu du lien diviseurs $\leftrightarrow$ fibrés en droites.

5.1.2 Fibrés en droites

Soit X une variété algébrique. On appelle *famille de droites vectorielles* sur X la donnée d'un morphisme de variétés algébriques $\pi : \mathcal{L} \to X$ tel que, pour tout $x \in X$, les fibres $\mathcal{L}_x := \pi^{-1}(x)$ sont des droites vectorielles sur $\Bbbk$. Un morphisme entre deux telles familles $p_1 : \mathcal{L}_1 \to X$ et $p_2 : \mathcal{L}_2 \to X$ est un morphisme $f : \mathcal{L}_1 \to \mathcal{L}_2$ compatible avec les morphismes p_1 et p_2. Une famille de droites vectorielles est dite *triviale* si elle est isomorphe à la famille $\pi_1 : X \times \mathbb{A}^1 \to X$ avec π_1 la projection canonique.

Définition 5.1.6. *Soit $X/\Bbbk$ une variété algébrique. On appelle* fibré en droites $\pi : \mathcal{L} \to X$, *abrégé à la simple donnée de $\mathcal{L}$, une famille de droites vectorielles telle que pour tout $x \in X$ il existe un voisinage U de x sur lequel la restriction $\mathcal{L}|_U$ est triviale.*

On dit alors que l'isomorphisme

$$\varphi_U : \mathcal{L}|_U \to U \times \mathbb{A}^1$$

est une *trivialisation* du fibré en droites. Si on dispose de trivialisations (U_i, φ_i), on définit les *fonctions de transition* $g_{i,j} : U_i \cap U_j \to \mathrm{GL}_1\big(\mathcal{O}_X(U_i \cap U_j)\big)$ telles que le morphisme

$$\varphi_i \circ \varphi_j^{-1} : U_i \cap U_j \times \mathbb{A}^1 \to U_i \cap U_j \times \mathbb{A}^1$$

vérifie $\varphi_i \circ \varphi_j^{-1}(x, v) = \big(x, g_{i,j}(x)v\big)$. Celles-ci vérifient

$$g_{i,i} = \mathrm{Id}_{U_i}, \qquad g_{i,j}g_{j,k} = g_{i,k} \text{ sur } U_i \cap U_j \cap U_k. \tag{5.1}$$

Réciproquement, la donnée de fonctions $g_{i,j} : U_i \cap U_j \to \mathrm{GL}_1\big(\mathcal{O}_X(U_i \cap U_j)\big)$ vérifiant (5.1) permettent de construire un fibré en droites par recollement. Ceci est un moyen de construire les nouveaux fibrés suivants. On définit le *dual* de $\mathcal{L}$, noté $\mathcal{L}^*$, le fibré en droites dont les fibres sont les espaces vectoriels duaux des fibres de $\mathcal{L}$. De même, on définit le *produit tensoriel* de deux fibrés en droites $\mathcal{L}_1$ et $\mathcal{L}_2$, noté $\mathcal{L}_1 \otimes \mathcal{L}_2$, dont les fibres sont les produits tensoriels de leurs fibres respectives. Aussi, étant donné un morphisme de variétés algébriques $\phi : Y \to X$, on appelle *pullback* du fibré en droites $\pi : \mathcal{L} \to X$, le fibré en droites défini par le produit fibré

$$\phi^*\mathcal{L} := \mathcal{L} \times_X Y = \big\{(y, v) \in Y \times \mathcal{L} \ ; \ \phi(y) = \pi(v)\big\}.$$

Définition 5.1.7. *Une* section globale *d'un fibré en droites $\pi : \mathcal{L} \to X$ est un morphisme $s : X \to \mathcal{L}$ tel que*

$$\pi \circ s = \mathrm{Id}_X\,.$$

L'ensemble des sections globales est noté $H^0(X, \mathcal{L})$.

La structure d'espace vectoriel des fibres $\mathcal{L}_x$ permet de définir l'addition de deux sections globales et la multiplication d'une section globale par un élément de $\mathcal{O}_X(X)$, faisant de $H^0(X,\mathcal{L})$ un module sur l'algèbre $\mathcal{O}_X(X)$.

Finalement, nous terminons cette section en reliant diviseurs de Cartier et fibrés en droites. À partir d'un diviseur de Cartier $D = (U_i, f_i)_{i\in I}$, on construit un fibré en droites sur X en recollant les fibrés triviaux $U_i \times \mathbb{A}^1 \to U_i$ par les isomorphismes

$$\begin{aligned} U_i \cap U_j \times \mathbb{A}^1 &\to U_i \cap U_j \times \mathbb{A}^1 \\ (x,\alpha) &\mapsto \big(x, \alpha(f_i/f_j)(x)\big), \end{aligned}$$

nous le notons $\mathcal{L}(D)$.

On a une bijection entre les sections globales de $\mathcal{L}(D)$ et les fonctions de $L(D)$ par la relation

$$\big\{ \operatorname{div}(s) \ ; \ s \in H^0\big(X, \mathcal{L}(D)\big), s \neq 0\big\} = |D|. \tag{5.2}$$

Proposition 5.1.8. *L'application $D \mapsto \mathcal{L}(D)$ induit un isomorphisme de groupes entre le groupe des classes de diviseurs de Cartier sur X et le groupe des classes d'isomorphisme de fibrés en droites sur X.*

En particulier, on a

$$\mathcal{L}\big(D + D'\big) = \mathcal{L}(D) \otimes \mathcal{L}\big(D'\big), \qquad \mathcal{L}(-D) = \mathcal{L}(D)^* = \mathcal{L}(D)^{-1},$$

et pour tout morphisme $\phi : X \to Y$,

$$\mathcal{L}\big(\phi^*(D)\big) = \phi^*\big(\mathcal{L}(D)\big).$$

En utilisant cette correspondance nous parlerons de fibrés en droite *sans point de base, amples,* ou *très amples*. Enfin, nous avons les résultats classiques suivants.

Proposition 5.1.9. *Soit $\phi : X \to Y$ un morphisme de variétés projectives. Si $\mathcal{L}$ est un fibré en droites sur Y sans point de base, alors $\phi^*\mathcal{L}$ est sans point de base.*

Théorème 5.1.10. *Soit A une variété abélienne et $\mathcal{L}$ un fibré en droites sur A. Si $\mathcal{L}$ est ample alors $\mathcal{L}^2$ est sans point de base et $\mathcal{L}^n$ est très ample pour $n \geq 3$.*

5.2 Cas des variétés abéliennes

Cette section a pour objectif de démontrer le Lemme 5.2.18 auquel nous nous référerons dans les prochains chapitres. Nous profitons de ces rappels pour introduire des résultats techniques de Lange et Ruppert permettant d'alléger la preuve de ce lemme. Ces résultats auxiliaires sont signalés par la dénomination "Application".

Dans la suite, nous désignerons par A une variété abélienne. Deux parties composent la première sous-section sur le groupe de Picard d'une variété abélienne, on commence par donner les premières propriétés des fibrés en droites, puis on considère la notion de polarisation. La seconde sous-section sert à énoncer le théorème de Riemann-Roch et démontrer le lemme dû à Lange et Ruppert. Ces rappels sont tirés de [Mum85, Chapter III] et [Mil86b].

Donnons ici une notation que nous utiliserons abondamment dans les prochains chapitres.

Notation 5.2.1. *Soient A une variété abélienne, $\mathcal{L}$ un fibré en droites sur A. On note μ le morphisme (de variétés projectives) de groupe sur A, $\pi_1, \pi_2 : A \times A \to A$ les projections canoniques et, pour $m, n \geq 2$, on définit $\mathcal{M}_{m,n}$ le fibré en droites sur $A \times A$ suivant*

$$\mathcal{M}_{m,n} := \mu^*\mathcal{L}^{-1} \otimes \pi_1^*\mathcal{L}^m \otimes \pi_2^*\mathcal{L}^n.$$

Plus spécifiquement, nous notons $\mathcal{M}$ le fibré en droites $\mathcal{M}_{2,2}$.

5.2.1 Groupe de Picard

La rigidité des fibrés en droites apparaît bien dans le théorème suivant, source de nombreux résultats.

Théorème 5.2.2 (Théorème du cube)**.** *Soient X, Y, Z trois variétés complètes, x_0, y_0, z_0 un de leurs points respectifs, et $\mathcal{L}$ un fibré en droites sur $X \times Y \times Z$. Si les restrictions de $\mathcal{L}$ à $X \times Y \times \{z_0\}$, $X \times \{y_0\} \times Z$ et $\{x_0\} \times Y \times Z$ sont triviales alors $\mathcal{L}$ est trivial.*

Désormais A désigne une variété abélienne. Pour $x \in A$, on définit la translation par x le morphisme $t_x : A \to A$, $y \mapsto y + x$.

Définition 5.2.3. *Le* groupe de Picard *de A, noté* $\mathrm{Pic}(A)$*, est le groupe des fibrés en droites sur A, à isomorphisme près, et* $\mathrm{Pic}^0(A)$ *le sous-groupe formé par les classes d'isomorphisme des fibrés en droite $\mathcal{L}$ tels que l'une des deux conditions équivalentes suivantes est vérifiée :*

1. $\forall x \in A,\ t_x^* \mathcal{L} \cong \mathcal{L}$.
2. *On a, sur $A \times A$, $\mu^* \mathcal{L} \cong \pi_1^* \mathcal{L} \otimes \pi_2^* \mathcal{L}$.*

L'équivalence dans cette définition provient du principe de la balançoire (seesaw principle).

Corollaire 5.2.4 (Théorème du carré)**.** *Pour tout $\mathcal{L} \in \mathrm{Pic}(A)$ et pour tout $x, y \in A$, on a*

$$t_{x+y}^* \mathcal{L} \otimes \mathcal{L} \cong t_x^* \mathcal{L} \otimes t_y^* \mathcal{L}.$$

En particulier $t_x^* \mathcal{L} \otimes \mathcal{L}^{-1} \in \mathrm{Pic}^0(A)$. On définit alors l'homomorphisme

$$\begin{aligned} \phi_{\mathcal{L}} \ : \ A &\to \mathrm{Pic}^0(A) \\ x &\mapsto t_x^* \mathcal{L} \otimes \mathcal{L}^{-1}. \end{aligned}$$

Il ne dépend que de la classe de $\mathcal{L}$ modulo $\mathrm{Pic}^0(A)$. On note $K(\mathcal{L})$ son noyau, *i.e.*

$$K(\mathcal{L}) = \big\{ x \in A \ ; \ t_x^* \mathcal{L} \cong \mathcal{L} \big\}.$$

Application 5.2.5. *Soit $\mathcal{L}$ un fibré en droites ample sur A et Δ la diagonale de $A \times A$. On a (voir Notation 5.2.1 page 56)*

$$\Delta \subseteq K(\mathcal{M}).$$

En effet, soit $x \in A$,

$$\begin{aligned} t_{(x,x)}^* \mathcal{M} \otimes \mathcal{M}^{-1} &\cong \mu^* t_{[2]x}^* \mathcal{L}^{-1} \otimes \pi_1^* t_x^* \mathcal{L}^2 \otimes \pi_2^* t_x^* \mathcal{L}^2 \otimes \mu^* \mathcal{L} \otimes \pi_1^* \mathcal{L}^{-2} \otimes \pi_2^* \mathcal{L}^{-2}. \\ &\cong \mu^* \big(t_x^* \mathcal{L}^{-2} \otimes \mathcal{L}^2 \big) \otimes \pi_1^* \big(t_x^* \mathcal{L}^2 \otimes \mathcal{L}^{-2} \big) \otimes \pi_2^* \big(t_x^* \mathcal{L}^2 \otimes \mathcal{L}^{-2} \big), \end{aligned}$$

car par le théorème du carré on a $t_{[2]x}^* \mathcal{L}^{-1} \otimes \mathcal{L} \cong \big(t_x^* \mathcal{L}^{-1} \big)^2 \otimes \mathcal{L}^2$. Or on a vu précédemment que $t_x^* \mathcal{L}^{-2} \otimes \mathcal{L}^2 \in \mathrm{Pic}^0(A)$. Donc par la propriété 2. de la Définition 5.2.3, on a que $t_{(x,x)}^* \mathcal{M} \otimes \mathcal{M}^{-1}$ est trivial sur $A \times A$.

On peut mettre une structure de schéma en groupe sur $K(\mathcal{L})$ (voir [Mum85, Section 13]). Nous utiliserons cela dans la démonstration du Lemme 5.2.18 en considérant la dimension de $K(\mathcal{L})$. On note $K(\mathcal{L})_0$ la composante connexe neutre de $K(\mathcal{L})$ et dit qu'un fibré en droites $\mathcal{L}$ sur A est *non dégénéré* si $K(\mathcal{L})$ est un sous-groupe fini de A. La proposition suivante fournit un critère d'amplitude dépendant de la dimension de $K(\mathcal{L})$.

Proposition 5.2.6. *Soit $\mathcal{L} \in \mathrm{Pic}(A)$ tel que $H^0(A, \mathcal{L}) \neq 0$. Alors $\mathcal{L}$ est ample si et seulement si il est non dégénéré.*

Définition 5.2.7. *Un fibré en droites $\mathcal{L} = \mathcal{L}(D)$ sur A est dit* symétrique *si $\mathcal{L} \cong [-1]^*\mathcal{L}$, ou de façon équivalente $D \sim [-1]^*D$.*

On donne une autre conséquence du théorème du cube sous forme de corollaire.

Corollaire 5.2.8. *Soient $\mathcal{L}$ un fibré en droites sur A et $n \in \mathbb{Z}$. On a*

$$[n]^*\mathcal{L} \cong \mathcal{L}^{\frac{n^2+n}{2}} \otimes [-1]^*\mathcal{L}^{\frac{n^2-n}{2}}.$$

Application 5.2.9. *On peut voir qu'un fibré en droites ample $\mathcal{L}$ est symétrique si et seulement si $\mathcal{M}|_\Delta$ est trivial. En effet, soit $d : A \to A \times A$, $x \to (x, x)$, on a*

$$\begin{aligned}\mathcal{M}|_\Delta &\cong d^*\mathcal{M} \\ &\cong [2]^*\mathcal{L}^{-1} \otimes \mathcal{L}^2 \otimes \mathcal{L}^2 \\ &\cong \mathcal{L}^{-3} \otimes [-1]^*\mathcal{L}^{-1} \otimes \mathcal{L}^4 \\ &\cong \mathcal{L} \otimes [-1]^*\mathcal{L}^{-1}.\end{aligned}$$

Il existe une structure de variété abélienne sur le groupe $\mathrm{Pic}^0(A)$. Celle-ci provient de l'existence, que nous supposons, d'une variété abélienne $\widehat{A}$ et d'un fibré en droite P sur $A \times \widehat{A}$ tels que, pour tout $\alpha \in \widehat{A}$, $P\big|_{A\times\{\alpha\}}$ représente un point de $\mathrm{Pic}^0(A)$ et $P\Big|_{\{0\}\times\widehat{A}}$ soit trivial. La variété abélienne $\widehat{A}$ est appelée la *duale* de A et P, uniquement déterminé à isomorphisme près, est appelé le *fibré de Poincaré*.

Une *isogénie* entre deux variétés abéliennes A et B est un morphisme $f : A \to B$ surjectif et de noyau fini. Son *degré* est son degré en tant que morphisme de variétés algébriques, il est égal à la cardinalité de son noyau lorsque celui-ci est premier avec la caractéristique de $\Bbbk$.

Une *polarisation* λ sur une variété abélienne A est une isogénie $\lambda : A \to \widehat{A}$ telle que $\lambda = \phi_{\mathcal{L}}$ pour un certain fibré en droites ample $\mathcal{L}$. Le *degré* de λ est son degré en tant qu'isogénie. Une *variété abélienne polarisée* est la donnée d'un couple (A, λ). Si λ est de degré un, on parle ce *variété abélienne principalement polarisée*.

On définit ci-dessous l'équivalence algébrique qui formalise la notion de "déformation algébrique" d'un fibré en droites. Celle-ci est importante car elle conserve la polarisation de A.

Définition 5.2.10. *Deux fibrés en droites $\mathcal{L}, \mathcal{L}' \in \mathrm{Pic}(A)$ sont dits* algébriquement équivalents *s'il existe une variété connexe $T/\Bbbk$ et un fibré en droites $\mathcal{N}$ sur $A \times T$ tels que, pour certains $t_0, t_1 \in T$, $\mathcal{N}|_{A\times\{t_0\}} \cong \mathcal{L}$ et $\mathcal{N}|_{A\times\{t_1\}} \cong \mathcal{L}'$.*

Un fibré en droites $\mathcal{L}$ est dans $\mathrm{Pic}^0(A)$ si et seulement si il est algébriquement équivalent au fibré en droites trivial. La condition nécessaire provient de l'existence de la variété abélienne duale. La condition nécessaire est une conséquence du théorème du cube (voir [Mum85, Section II.8 Property (vi)]).

Lemme 5.2.11. *Soient $\mathcal{L}$ et $\mathcal{L}'$ deux fibrés en droites amples sur A. Ils sont algébriquement équivalents si et seulement si $\mathcal{L}' \cong t_x^*\mathcal{L}$ pour un certain $x \in A$.*

Démonstration. Le fibré en droites $\mathcal{L}$ est algébriquement équivalent à $\mathcal{L}'$ si et seulement si $\mathcal{L}^{-1} \otimes \mathcal{L}' \approx 0$, *i.e.* $\mathcal{L}^{-1} \otimes \mathcal{L}' \in \mathrm{Pic}^0(A)$. Comme $\mathcal{L}$ est ample, $\phi_{\mathcal{L}} : A \to \mathrm{Pic}^0(A)$ est surjective, donc il existe $x \in A$ tel que $\mathcal{L}^{-1} \otimes \mathcal{L}' \cong t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$, d'où $\mathcal{L}' \cong t_x^*\mathcal{L}$. □

En particulier, la polarisation associée à une variété abélienne polarisée est invariante par équivalence algébrique.

Lemme 5.2.12 ([Lan83b, Proposition 2 p.92]). *Soient $n \in \mathbb{Z}$ et $\mathcal{L} \in \mathrm{Pic}(A)$ ample. On a*

$$[n]^*\mathcal{L} \approx \mathcal{L}^{n^2}.$$

Lemme 5.2.13. *Soit (A, λ) une variété abélienne polarisée. Il existe un fibré en droites symétrique qui induit la polarisation λ sur A.*

Démonstration. Notons $\mathcal{L}'$ un fibré en droites ample associé à la polarisation λ. D'après le Lemme 5.2.11, il suffit de construire un fibré en droites $\mathcal{L}$ symétrique et algébriquement équivalent à $\mathcal{L}'$. Comme $\mathcal{L}'$ est algébriquement équivalent à $[-1]^*\mathcal{L}'$ (Lemme 5.2.12), il existe $x \in A$ tel que

$$t_x^*\,\mathcal{L}' \cong [-1]^*\mathcal{L}'.$$

Soient $y \in A$ tel que $2y = x$ et $\mathcal{L} := t_y^*\mathcal{L}'$. Alors $\mathcal{L}$ est algébriquement équivalent à $\mathcal{L}'$ et on a

$$\mathcal{L} = t_y^*\,\mathcal{L}' = t_{-y}^*\,t_x^*\,\mathcal{L}' \cong t_{-y}^*\,[-1]^*\mathcal{L}' = [-1]^*\mathcal{L}.$$

D'où la symétrie de $\mathcal{L}$. □

5.2.2 Cohomologie des fibrés en droites

Je donne ci-dessous des théorèmes généraux de cohomologie des fibrés en droite pour pouvoir m'y référer mais ne présente leurs démonstrations techniques.

On définit la *caractéristique d'Euler* d'un fibré en droites $\mathcal{L}$ sur A par la quantité

$$\chi(\mathcal{L}) := \sum (-1)^i h^i(A, \mathcal{L}).$$

Théorème 5.2.14 (Théorème de Riemann-Roch). *Soient A une variété abélienne de dimension g. Pour tout fibré en droites $\mathcal{L} = \mathcal{L}(D)$, on a*

$$\chi(\mathcal{L}) = \frac{\left(D^g\right)}{g!},$$

où $\left(D^g\right)$ désigne la $g^{ième}$ auto-intersection du diviseur D.

Définition 5.2.15. *Si $\mathcal{L}$ est un fibré en droites non dégénéré sur A, il existe un unique entier $i_{\mathcal{L}} \geq 0$, appelé* indice de $\mathcal{L}$, *tel que*

$$H^{i_{\mathcal{L}}}(A, \mathcal{L}) \neq 0.$$

Dans le cas où $\mathcal{L}$ est ample on a $i_{\mathcal{L}} = 0$, en particulier $\chi(\mathcal{L}) = h^0(A, \mathcal{L})$.

Citons deux théorèmes auquel nous nous référerons dans la démonstration du lemme ci-après.

Théorème 5.2.16 ([Kem70, Theorem 1 p.95]). *Soient A une variété abélienne et $\mathcal{L}$ un fibré en droites sur A. On note $K(\mathcal{L})_0$ la composante connexe neutre de $K(\mathcal{L})$ et $p : A \to A/K(\mathcal{L})_0$ la projection canonique.*

1. *Si la restriction de $\mathcal{L}$ à $K(\mathcal{L})_0$ est non triviale, alors $H^i(A, \mathcal{L}) = 0$ pour tout i.*
2. *Sinon il existe un fibré en droites $\widetilde{\mathcal{N}}$ sur $A/K(\mathcal{L})_0$ tel que $\mathcal{L} \cong p^*\widetilde{\mathcal{N}}$ et, si l'on note i_0 l'indice de $\widetilde{N}$,*

$$H^i(A, \mathcal{L}) \cong H^{i_0}\left(A, \widetilde{\mathcal{N}}\right) \otimes H^{i-i_0}\left(K(\mathcal{L})_0, \mathcal{O}_{K(\mathcal{L})_0}\right), \text{ pour tout } i.$$

Théorème 5.2.17 ([Mum85, p.155], [Kem70, Theorem 2 p.98]). *Soient A une variété abélienne de dimension g, $\mathcal{M}$ et $\mathcal{N}$ deux fibrés en droites respectivement non dégénéré et ample sur A. Le polynôme P défini par $P(x) = \chi\left(\mathcal{M} \otimes \mathcal{N}^x\right)$ a g racines, toutes réelles, et l'indice de $\mathcal{M}$ est égal au nombre de racines strictement positives de P comptées avec multiplicité.*

De plus, si l'on ne suppose pas $\mathcal{M}$ non dégénéré, alors $\dim K(\mathcal{M})$ *est la multiplicité de P en* 0.

On donne la démonstration du lemme suivant qui sera central dans le prochain chapitre.

Lemme 5.2.18 ([LR85])**.** *Soient A une variété abélienne et $\mathcal{L}$ un fibré en droites sur A ample et sans point de base. On note $\delta : A \times A$, $(x, y) \mapsto x - y$. Rappelons $\mathcal{M}_{m,n} := \mu^*\mathcal{L}^{-1} \otimes \pi_1^*\mathcal{L}^m \otimes \pi_2^*\mathcal{L}^n$ pour $m, n \geq 2$ (Notation 5.2.1).*

1. *Supposons $m = n = 2$.*
   - *i. Si $\mathcal{L}$ est symétrique alors $|\mathcal{M}|$ est sans point de base et $\mathcal{M} \cong \delta^*\mathcal{L}$. De plus $h^0(A \times A, \mathcal{M}) = h^0(A, \mathcal{L})$.*
   - *ii. Sinon $H^0(A \times A, \mathcal{M}) = 0$.*
2. *Supposons $(m, n) \neq (2, 2)$. Dans ce cas, $h^0(A \times A, \mathcal{M}_{m,n}) = h^0(A, \mathcal{L})^2\,(mn - m - n)^g$.*

Démonstration. Soit $\mathcal{N} := \pi_1^*\mathcal{L} \otimes \pi_2^*\mathcal{L}$ un fibré en droites ample sur $A \times A$. Lange et Ruppert démontrent l'égalité

$$P(x) := \chi(A \times A, \mathcal{M}_{m,n} \otimes \mathcal{N}^x) = h^0(A, \mathcal{L})^2\big(x^2 + (m + n - 2)x + mn - m - n\big)^g$$

et, par le Théorème 5.2.17, la dimension de $K(\mathcal{M}_{m,n})$ est la multiplicité en 0 de $P(x)$. Comme $mn - m - n = (m - 1)(n - 1) - 1$ et m, n sont des entiers plus grands que 2, on a

$$\dim K(\mathcal{M}_{m,n}) = \begin{cases} g, & \text{si } m = n = 2, \\ 0, & \text{sinon.} \end{cases} \tag{5.3}$$

1i. Supposons $\mathcal{L}$ symétrique et commençons par expliciter l'isomorphisme entre $\mathcal{M}$ et $\delta^*\mathcal{L}$. Lange et Ruppert considèrent le diagramme commutatif suivant dont les deux lignes sont des suites exactes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \{0\} \times A & \longrightarrow & A \times A & \xrightarrow{\pi_1} & A \times \{0\} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle (\mu,\pi_2)} & \nearrow{\scriptstyle \delta} & \downarrow & & \\ 0 & \longrightarrow & A & \xrightarrow{d} & A \times A & \xrightarrow{p} & A \times A/\Delta & \longrightarrow & 0 \end{array}$$

où $p : A \times A \to A \times A/\Delta$ est la projection canonique. D'après le cas *2.* du Théorème 5.2.16, il existe un fibré en droites $\widetilde{\mathcal{N}}$ sur $A \times A/\Delta$ tel que $\mathcal{M} = p^*\widetilde{\mathcal{N}}$. En effet, l'Application 5.2.5 page 57 et l'équation (5.3) ci-dessus montrent que l'on a $K(\mathcal{M})_0 = \Delta$. En remontant dans le diagramme, on a l'existence d'un fibré en droites $\mathcal{N}$ sur $A \times \{0\}$ tel que $(\mu, \pi_2)^*\mathcal{M} \cong \pi_1^*\mathcal{N}$. On a alors $\mathcal{N} = \mathcal{L}$. En effet, en identifiant A et $A \times \{0\}$ et en notant $i_1 : A \times \{0\} \to A \times A$ l'injection canonique,

$$\begin{aligned} \mathcal{N} &= i_1^*\pi_1^*\mathcal{N} \\ &= i_1^*(\mu, \pi_2)^*\mathcal{M} \\ &= \big(\mu \circ (\mu, \pi_2) \circ i_1\big)^*\mathcal{L}^{-1} \otimes \big(\pi_1 \circ (\mu, \pi_2) \circ i_1\big)^*\mathcal{L}^2 \otimes \big(\pi_2 \circ (\mu, \pi_2) \circ i_1\big)^*\mathcal{L}^2 \\ &= \mathcal{L}^{-1} \otimes \mathcal{L}^2 \\ &= \mathcal{L}. \end{aligned}$$

On retrouve ainsi $\mathcal{M} \cong \delta^*\mathcal{L}$ dont on déduit que $\mathcal{M}$ est sans point de base (voir la Proposition 5.1.9). Il reste à expliquer l'égalité $h^0(A \times A, \mathcal{M}) = h^0(A, \mathcal{L})$. On a démontré dans l'Application 5.2.9 que la restriction de $\mathcal{M}$ à $K(\mathcal{M})_0$ est triviale. Comme $\mathcal{L}$ est ample son indice est nul et, selon le cas *2.* du Théorème 5.2.16, on a $H^0(A \times A, \mathcal{M}) \cong H^0(A, \mathcal{L})$.

1ii. On a démontré dans les Applications 5.2.5 et 5.2.9 que si $\mathcal{L}$ n'est pas symétrique alors la restriction de $\mathcal{M}$ à la composante connexe de $K(\mathcal{M})$ est non triviale. Or, d'après le cas *1.*

du Théorème 5.2.16, cela entraîne que les espaces $H^i(A \times A, \mathcal{M})$ sont nuls pour tout i. En particulier, il n'y a pas de sections globales sur $\mathcal{M}$.

2. D'après la Formule (5.3), on a que, dans le cas $(m,n) \neq (2,2)$, $\mathcal{M}_{m,n}$ est non dégénéré et $H^i(A \times A, \mathcal{M}_{m,n}) \neq 0$ seulement pour i égal au nombre de racines positives de P. Sans perte de généralité, supposons $m \leq n$. Le discriminant de P est $(n-m)^2+4$, ses racines sont $x_\pm = \dfrac{2-m-n \pm \sqrt{(n-m)^2+4}}{2}$. Or

$$2x_- \leq 2x_+ \leq 2-m-n-\sqrt{(n-m+2)^2} = -2n < 0.$$

Ainsi $H^0(A \times A, \mathcal{M}_{m,n}) \neq 0$, et plus précisément

$$h^0(A \times A, \mathcal{M}_{m,n}) = \chi(A \times A, \mathcal{M}_{m,n}) = P(0) = h^0(A, \mathcal{L})^2 (mn-m-n)^g.$$

□

Remarque 5.2.19. *L'isomorphisme $\mathcal{M} \cong \delta^*\mathcal{L}$ est défini sur $\Bbbk$. Ceci sera utilisé dans la Section 6.2 pour identifier les diviseurs de leurs sections globales respectives.*

5.3 Rappels sur la jacobienne d'une courbe de genre 2

5.3.1 Coordonnées de Mumford

On s'intéresse maintenant aux *jacobiennes de courbes hyperelliptiques de grenre* 2. Celles-ci sont munies d'une structure de variétés abéliennes. Rappelons que nous avons introduit dans la Section 1.1 de la première partie la jacobienne d'une courbe comme étant le groupe des diviseurs sur la courbe de degré 0 quotienté par le sous-groupe des diviseurs principaux. Pour ces rappels nous renvoyons à [CFA+06, Chapter 14] et [Mum75a, Lectures III and IV].

Soit C une courbe de genre $g \geq 2$. elle est dite *hyperelliptique* s'il existe un morphisme séparable $\overline{\pi} : C \to \mathbb{P}^1$ de degré 2 défini sur $\overline{\Bbbk}$. Lorsque C est de genre pair, en particulier 2, il existe alors un morphisme $\pi : C \to \mathbb{P}^1$ défini sur $\Bbbk$ [Mes91]. Les points de ramification de π sont appelés les *points de Weierstraß* de C. On définit l'*involution hyperelliptique* sur C comme l'application définie sur $\Bbbk$ qui a un point associe le second point (compté avec multiplicité), noté $\overline{P}$, ayant la même image par π. On suppose maintenant que la courbe C est de genre 2.

Proposition 5.3.1. *Une courbe hyperelliptique $C/\Bbbk$ de genre* 2 *est donnée par une équation affine non singulière, appelée* équation de Weierstraß*, de la forme*

$$y^2 + h(x)y = f(x), \tag{5.4}$$

avec $h(x), f(x) \in \Bbbk[x]$, $\deg(h) \leq g$ et f de degré 5 *ou* 6.

Dans le cas où la caractéristique de $\Bbbk$ est différente de 2, on peut se ramener à $h(x) = 0$ en complétant le carré dans le membre de gauche. Si la courbe C possède un point de Weierstraß $\Bbbk$-rationnel, alors on peut supposer $\deg(f) = 5$, ce point correspondant au point à l'infini, $\infty = (0:1:0)$, de C.

Supposons que l'on dispose d'un diviseur $\Bbbk$-rationnel P_∞ de degré 1 tel que $2P_\infty \sim \kappa_C$ (voir la Section I.1.1). Celui-ci va nous permettre de définir le plongement de puissance symétriques de C dans sa jacobienne. Il vérifie $(P) + \left(\overline{P}\right) \sim 2P_\infty \sim \kappa_C$.

Voyons comment représenter les points de Jac_C, *i.e.* les classes des diviseurs de degré 0. Pour $k \geq 1$, on considère l'application

$$C^k \to \mathrm{Jac}_C$$
$$\big(P_1, \ldots, P_k\big) \mapsto \sum_{i=1}^{k} (P_i) - kP_\infty.$$

On note S^kC le quotient de C^k par le groupe de permutations $\mathfrak{S}_k$, appelé la $k^{ième}$ *puissance symétrique de* C, et on défini l'application induite

$$\phi^{(k)} : S^kC \to \mathrm{Jac}_C\,.$$

On note W^k son image. Cette application est surjective pour $k \geq 2$ et, pour $k = 1$, W^1 est un diviseur de Jac_C appelé *diviseur thêta*. On le note aussi Θ. C'est un diviseur ample, symétrique et qui induit une polarisation principale sur Jac_C. Nous verrons dans la prochaine sous-section une autre caractérisation de ce diviseur en termes de fonctions thêta.

Notation 5.3.2. *Pour tout $x \in \mathrm{Jac}_C\big(\overline{\Bbbk}\big)$, on note $\Theta_x := \Theta + x$ le translaté du diviseur Θ par x.*

Remarquons que tout point de $x \in \mathrm{Jac}_C$ peut être écrit comme un diviseur de la forme $(P) - (Q)$, avec $P, Q \in C\big(\overline{\Bbbk}\big)$. En effet, $\phi^{(2)}$ étant surjective, il existe P_0, Q_0 deux points de C tels que $x = (P_0) + (Q_0) - 2P_\infty$. Mais $2P_\infty \sim (Q_0) + \big(\overline{Q_0}\big)$, donc $(P_0) + (Q_0) \sim (P_0) - \big(\overline{Q_0}\big)$.

Proposition 5.3.3 ([Mum75a, p.275])**.** *Soient C une courbe de genre 2 et $x \in \mathrm{Jac}_C\big(\overline{\Bbbk}\big)$ de la forme $x = (P) - (Q)$. On a*

$$\Theta \cap \Theta_x = \big\{(P) - P_\infty, \big(\overline{Q}\big) - P_\infty\big\}.$$

On suppose désormais que l'on dispose d'un point de Weierstraß $\Bbbk$-rationnel sur C. L'involution hyperelliptique fixe le point à l'infini et à un point $P = (x, y)$ associe $\overline{P} = \big(x, -y - h(x)\big)$, que l'on ne confond pas avec le symétrique du point P (dans le cas elliptique) qui n'a plus de sens ici. On pose alors $P_\infty = (\infty)$.

On a vu que l'application $\phi^{(2)}$ est surjective et plus précisément on a que tout diviseur sur C est linéairement équivalent à un unique diviseur

$$\sum_{i=1}^{r} (P_i) - r(\infty),$$

où $P_i \neq \overline{P_j}$ pour tout $i \neq j$, $P_i \neq \infty$ pour tout i, et $r \leq 2$. Les diviseurs de cette forme sont appelés *diviseurs réduits*.

Proposition 5.3.4 (Représentation de Mumford)**.** *Soit D un diviseur réduit de la forme*

$$D = \sum_{i=1}^{r} (P_i) - r(\infty),$$

avec $P_i = (x_i, y_i)$. Il est représenté de façon unique par deux polynômes $u(x), v(x) \in \Bbbk[x]$ avec $\deg(v) < \deg(u) \leq$ tels que

$$u(x) = \prod (x - x_i),$$
$$u \,\big|\, v^2 + vh - f.$$

Le point ∞ est représenté par le couple $(1, 0)$.

L'algorithme de Cantor ci-dessous permet de calculer de façon efficace la somme de deux classes de diviseurs.

Input : Une courbe hyperelliptique sous forme de Weierstraß et deux classes $\mathrm{Cl}(D_1), \mathrm{Cl}(D_2)$ données par leurs coordonnées de Mumford $(u_1, v_1), (u_2, v_2)$.

output : Coordonnées de Mumford de $\mathrm{Cl}(D_1 + D_2)$.

$d_1 \leftarrow \mathrm{pgcd}(u_1, u_2)$, $d \leftarrow \mathrm{pgcd}(d_1, v_1 + v_2 + h)$

$\left[d_1 = e_1 u_1 + e_2 u_2,\ d = c_1 d_1 + c_2(v_1 + v_2 + h)\right]$

$u \leftarrow \dfrac{u_1 u_2}{d^2}$, $v \leftarrow \dfrac{c_1 e_1 u_1 v_2 + c_1 e_2 u_2 v_1 + c_2(v_1 v_1 + f)}{d} \mod u$

while $\deg(u) > 2$ **do**

$u \leftarrow \dfrac{f - vh - v^2}{u}$, $v \leftarrow (-h - v) \mod u$

end do

return (u, v)

ALGORITHME 2 – Algorithme de Cantor.

L'utilisation de la représentation de Mumford et de l'algorithme de Cantor fournissent des coûts intéressants pour le calcul de l'addition de deux points, par exemple $47\mathbf{m} + 4\mathbf{s}$ pour une addition générique (voir [Lan05]).

Les coordonnées de Mumford rendent explicite l'isomorphisme entre Jac_C et le groupe de classe des idéaux de C. Ce dernier est plus avantageux pour des calculs pratiques, notamment grâce à l'algorithme de Cantor. Nous allons voir dans la prochaine sous-section une autre représentation des points de Jac_C en la plongeant dans $\mathbb{P}^{15}$ et résumer la construction d'un isomorphisme entre ces deux représentations.

5.3.2 Fonctions thêta en genre 2

Nous nous plaçons ici sur $\mathbb{C}$ pour pouvoir manipuler plus aisément les fonctions thêta pour une variété principalement polarisée (A, λ). Les résultats de cette sous-section étant de nature algébrique, nous pourrons les utiliser sur corps finis (voir la Remarque 5.3.8). En effet, ces fonctions peuvent être naturellement interprétées en termes de sections globales de puissances du fibré définissant la polarisation principale λ. Concernant la théorie classique des fonctions thêta, nous renvoyons à [Mum83, Mum84]. Soit Ω un élément dans le demi-espace de Siegel :

$$\left\{\Omega \in \mathrm{Mat}_{2\times 2}(\mathbb{C}),\ {}^t\Omega = \Omega,\ \Im(\Omega) > 0\right\}.$$

Comme dans la Section I.1.3, on commence par définir la fonction thêta de Riemann

$$\vartheta(z, \Omega) = \sum_{n \in \mathbb{Z}^2} \exp\left(i\pi\, {}^t n \Omega n + 2i\pi\, {}^t n z\right), z \in \mathbb{C}^2.$$

Pour tout $a, b \in \mathbb{Q}^2$, la fonction thêta avec caractéristique a, b est définie par

$$\begin{aligned}\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \Omega) &= \sum_{n \in \mathbb{Z}^2} \exp\left(i\pi\, {}^t(n + a)\Omega(n + a) + 2i\pi\, {}^t(n + a)(z + b)\right) \\ &= \exp\left(i\pi\, {}^t a \Omega a + 2i\pi\, {}^t a(z + b)\right) \vartheta(z + \Omega a + b, \Omega). \end{aligned} \tag{5.5}$$

Les caractéristiques sont considérées modulo $\mathbb{Z}^2$ puisque pour tout $\alpha, \beta \in \mathbb{Z}^2$ on a

$$\vartheta \left[\begin{smallmatrix} a+\alpha \\ b+\beta \end{smallmatrix} \right] (z, \Omega) = \exp(2i\pi\, {}^t a\beta) \vartheta \left[\begin{smallmatrix} a \\ b \end{smallmatrix} \right] (z, \Omega)\,.$$

Dans la suite nous allons considérer des fonctions thêta de niveau 4, *i.e.* les fonctions thêta dont les caractéristiques sont dans $\frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2$.

Un résultat classique de Lefschetz établit que les fonctions thêta de niveau 4 donnent un plongement de $\mathbb{C}^2/\Omega\mathbb{Z}^2 + \mathbb{Z}^2$ dans $\mathbb{P}^{15}(\mathbb{C})$ [Mum85, p.29]. Il existe un élément $\mathcal{K}$ de Jac_C, appelé *constante de Riemann*, tel que le diviseur induit sur le tore complexe $\mathbb{C}^2/\Omega\mathbb{Z}^2 + \mathbb{Z}^2$ par la fonction thêta de Riemann soit $\Theta_{\mathcal{K}}$ le translaté du diviseur Θ, introduit dans la Sous-Section 5.3.1, par le point $\mathcal{K}$. La formule (5.5) montre que les diviseurs associés aux fonctions thêta de niveau 4 sont les translatés du diviseur $\Theta_{\mathcal{K}}$ par un point de 2-torsion.

Dans la suite, nous ferons souvent références aux fonctions thêta de niveau 4, il est donc nécessaire d'adopter une notation plus simple pour ces fonctions.

Notation 5.3.5 ([Gau07, Section 7.1])**.** *On numérote les fonctions thêta de niveau* 4 *comme suit :*

$$\begin{aligned}
\vartheta_1(z) &= \vartheta \left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(0\ 0) \end{smallmatrix} \right] (z, \Omega)\,, & \vartheta_2(z) &= \vartheta \left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(\frac{1}{2}\ \frac{1}{2}) \end{smallmatrix} \right] (z, \Omega)\,,\\
\vartheta_3(z) &= \vartheta \left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(\frac{1}{2}\ 0) \end{smallmatrix} \right] (z, \Omega)\,, & \vartheta_4(z) &= \vartheta \left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(0\ \frac{1}{2}) \end{smallmatrix} \right] (z, \Omega)\,,\\
\vartheta_5(z) &= \vartheta \left[\begin{smallmatrix} {}^t(\frac{1}{2}\ 0) \\ {}^t(0\ 0) \end{smallmatrix} \right] (z, \Omega)\,, & \vartheta_6(z) &= \vartheta \left[\begin{smallmatrix} {}^t(\frac{1}{2}\ 0) \\ {}^t(0\ \frac{1}{2}) \end{smallmatrix} \right] (z, \Omega)\,,\\
\vartheta_7(z) &= \vartheta \left[\begin{smallmatrix} {}^t(0\ \frac{1}{2}) \\ {}^t(0\ 0) \end{smallmatrix} \right] (z, \Omega)\,, & \vartheta_8(z) &= \vartheta \left[\begin{smallmatrix} {}^t(\frac{1}{2}\ \frac{1}{2}) \\ {}^t(0\ 0) \end{smallmatrix} \right] (z, \Omega)\,,\\
\vartheta_9(z) &= \vartheta \left[\begin{smallmatrix} {}^t(0\ \frac{1}{2}) \\ {}^t(\frac{1}{2}\ 0) \end{smallmatrix} \right] (z, \Omega)\,, & \vartheta_{10}(z) &= \vartheta \left[\begin{smallmatrix} {}^t(\frac{1}{2}\ \frac{1}{2}) \\ {}^t(\frac{1}{2}\ \frac{1}{2}) \end{smallmatrix} \right] (z, \Omega)\,,\\
\vartheta_{11}(z) &= \vartheta \left[\begin{smallmatrix} {}^t(0\ \frac{1}{2}) \\ {}^t(0\ \frac{1}{2}) \end{smallmatrix} \right] (z, \Omega)\,, & \vartheta_{12}(z) &= \vartheta \left[\begin{smallmatrix} {}^t(0\ \frac{1}{2}) \\ {}^t(\frac{1}{2}\ \frac{1}{2}) \end{smallmatrix} \right] (z, \Omega)\,,\\
\vartheta_{13}(z) &= \vartheta \left[\begin{smallmatrix} {}^t(\frac{1}{2}\ 0) \\ {}^t(\frac{1}{2}\ 0) \end{smallmatrix} \right] (z, \Omega)\,, & \vartheta_{14}(z) &= \vartheta \left[\begin{smallmatrix} {}^t(\frac{1}{2}\ \frac{1}{2}) \\ {}^t(\frac{1}{2}\ 0) \end{smallmatrix} \right] (z, \Omega)\,,\\
\vartheta_{15}(z) &= \vartheta \left[\begin{smallmatrix} {}^t(\frac{1}{2}\ 0) \\ {}^t(\frac{1}{2}\ \frac{1}{2}) \end{smallmatrix} \right] (z, \Omega)\,, & \vartheta_{16}(z) &= \vartheta \left[\begin{smallmatrix} {}^t(\frac{1}{2}\ \frac{1}{2}) \\ {}^t(0\ \frac{1}{2}) \end{smallmatrix} \right] (z, \Omega)\,.
\end{aligned}$$

Remarquons que les dix premières fonctions thêta sont les paires tandis que les six dernières sont les impaires. Pour $i = 1, \ldots, 10$, on note ϑ_i la thêta constante $\vartheta_i(0)$.

Rappelons que C est une courbe de genre 2. On lui associe sa matrice des périodes Ω qui est un élément du demi-espace de Siegel. L'application d'Abel-Jacobi est un isomorphisme analytique entre Jac_C et $\mathbb{C}^2/\Omega\mathbb{Z}^2+\mathbb{Z}^2$. On souhaite en donner une description algébrique pour une utilisation pratique. On commence pour cela par calculer les thêta constantes.

Les formules de Thomae [Tho70] relient les puissances $4^{\text{ième}}$ des thêta constantes aux paramètres de C (voir aussi [Mum84, Section III.8]). À isomorphisme près, on peut retrouver les thêta constantes en choisissant les racines avec soins (voir [CR11]). Supposons que la courbe C soit donnée sous forme de Rosenhain :

$$C : \qquad y^2 = f(x) = x(x-1)(x-\lambda)(x-\mu)(x-\nu).$$

Le choix d'un ordre sur les racines du polynôme f donne les relations suivantes :

$$\left(\frac{\vartheta_5}{\vartheta_1}\right)^4 = \frac{\mu}{\lambda\nu}, \qquad \left(\frac{\vartheta_7}{\vartheta_1}\right)^4 = \frac{\mu\,(\nu-1)\,(\lambda-\mu)}{\nu\,(\mu-1)\,(\lambda-\nu)},$$
$$\left(\frac{\vartheta_3}{\vartheta_1}\right)^4 = \frac{\mu\,(\nu-1)\,(\lambda-1)}{\lambda\nu\,(\mu-1)}, \qquad \left(\frac{\vartheta_4}{\vartheta_1}\right)^4 = \frac{\mu\,(\lambda-1)\,(\nu-\mu)}{\lambda\,(\mu-1)\,(\nu-\lambda)}.$$

Les carrés des autres thêta constantes de niveau 4 sont donnés par les formules suivantes :

$$\vartheta_6^2 = \frac{1}{\nu}\frac{\vartheta_1^2\vartheta_4^2}{\vartheta_5^2}, \qquad \vartheta_8^2 = \frac{1}{\lambda}\frac{\vartheta_1^2\vartheta_7^2}{\vartheta_5^2},$$
$$\vartheta_2^2 = (\nu-1)\,\frac{\vartheta_5^2\vartheta_6^2}{\vartheta_3^2}, \qquad \vartheta_9^2 = (\lambda-1)\,\frac{\vartheta_5^2\vartheta_8^2}{\vartheta_3^2},$$
$$\vartheta_{10}^2 = \frac{\vartheta_1^2\vartheta_2^2 - \vartheta_3^2\vartheta_4^2}{\vartheta_8^2}.$$

On peut prendre arbitrairement des racines carrées pour chaque thêta constante.

On peut ensuite expliciter algébriquement un isomorphisme entre Jac_C et l'image dans $\mathbb{P}^{15}(\mathbb{C})$ du plongement donné par les fonctions thêta de niveau 4. Ces formules peuvent être trouvées dans [CR11] pour le cas du genre 2 (et dans [Cos11] pour le cas général).

Soient $\{a_1, \ldots, a_5\}$ les racines ordonnées de f et

$$\eta_1 := {}^t\left[\tfrac{1}{2}, 0; 0, 0\right], \qquad \eta_2 := {}^t\left[\tfrac{1}{2}, 0; \tfrac{1}{2}, 0\right], \qquad \eta_3 := {}^t\left[0, \tfrac{1}{2}; \tfrac{1}{2}, 0\right],$$
$$\eta_4 := {}^t\left[0, \tfrac{1}{2}; \tfrac{1}{2}, \tfrac{1}{2}\right], \qquad \eta_5 := {}^t\left[0, 0; \tfrac{1}{2}, \tfrac{1}{2}\right], \qquad \eta_\infty := {}^t\left[0, 0; 0, 0\right].$$

Pour un sous-ensemble $S \subset \{1, \ldots, 5, \infty\}$, on pose

$$\eta_S := \sum_{i \in S} \eta_i.$$

Ceci vient du fait que si l'on définit η'_S et η''_S les premières et secondes parties de η_S et que l'on note A_i les points de Weierstraß de coordonnées affines $(a_i, 0)$, $i = 1, \ldots, 5$, et $A_\infty = \infty$ le point à l'infini de C, alors le diviseur $\sum_{i\in S}(A_i) - \#S(\infty)$ a pour image $\Omega\eta'_S + \eta''_S$ par l'application d'Abel-Jacobi. En particulier, si l'on note $\mathcal{U}$ l'ensemble $\{1, 3, 5\}$, alors $\mathcal{K}$ correspond au point $\Omega\eta'_{\mathcal{U}} + \eta''_{\mathcal{U}}$ et le diviseur Θ est le diviseur de la fonction thêta $\vartheta[\eta_{\mathcal{U}}] = \vartheta_{16}$ ([Cos11])

Notation 5.3.6. *Les fonctions thêta de niveau 4 peuvent être écrites comme $\vartheta\left[\eta_{\mathcal{U}\circ V}\right]$ avec V un sous-ensemble de $\{1, \ldots, 5\}$ de cardinalité impaire et $\circ$ la différence symétrique de deux ensembles. Pour de tels ensembles, van Wamelen [vW98] définit la fonction $t_V(z) := f_V\vartheta\left[\eta_{\mathcal{U}\circ V}\right](z)$ où f_V est une constante définie comme suit, $f_V := \vartheta\left[0\right]/\vartheta\left[\eta_{\mathcal{U}\circ V}\right]$ pour les fonctions paires (*i.e. *$\#V = 3$*) sinon*

$$f_1 = \frac{-1}{\sqrt{a_2 - a_1}}\frac{\vartheta_1\vartheta_5\vartheta_6\vartheta_8}{\vartheta_2\vartheta_3\vartheta_9\vartheta_{10}}, \qquad f_2 = \frac{-1}{\sqrt{a_2 - a_1}}\frac{\vartheta_5\vartheta_6\vartheta_8}{\vartheta_4\vartheta_7\vartheta_{10}},$$
$$f_3 = \frac{-1}{\sqrt{a_2 - a_1}}\frac{\vartheta_1\vartheta_6}{\vartheta_2\vartheta_4}, \qquad f_4 = \frac{1}{\sqrt{a_2 - a_1}}\frac{\vartheta_5}{\vartheta_3},$$
$$f_5 = \frac{-1}{\sqrt{a_2 - a_1}}\frac{\vartheta_1\vartheta_8}{\vartheta_7\vartheta_9}, \qquad f_\emptyset = f_{\{1,2,3,4,5\}} = \frac{-1}{\sqrt{a_2 - a_1}^3}\frac{\vartheta_5^2\vartheta_6^2\vartheta_8^2}{\vartheta_2\vartheta_3\vartheta_4\vartheta_7\vartheta_9\vartheta_{10}}.$$

Le théorème suivant réunit plusieurs résultats de van Wamelen [vW98]. Il introduit les quantités servant à obtenir des équations algébriques permettant de retrouver des quotients des fonctions thêta.

Théorème 5.3.7. *Soit $D = (P_1) + (P_2) - 2(\infty)$ un diviseur n'appartenant pas au diviseur Θ et soit $z \in \mathbb{C}^2/(\Omega\mathbb{Z}^2 + \mathbb{Z}^2)$ le vecteur correspondant. Notons (x_i, y_i) les coodonnées des points P_i, $i = 1, 2$. On note (u, v) les polynômes de Mumford de D. Pour k, l, m trois éléments distincts de $\{1, \ldots, 5\}$, on a*

$$u(a_k) = \frac{t_k^2(z)}{t_\emptyset^2(z)}, \qquad v(a_k) = \frac{Y_{k,m} - Y_{k,l}}{a_l - a_m},$$

$$Y_{l,m} := \frac{y_1(x_2 - a_l)(x_2 - a_m) - y_2(x_1 - a_l)(x_1 - a_m)}{x_2 - x_1} = c_{1,2}\frac{t_l(z)t_m(z)t_{\{l,m\}}(z)}{t_\emptyset^3(z)},$$

$$Y := y_1 y_2 = \prod_{l=1}^{5} \frac{t_l(z)}{t_\emptyset(z)},$$

où $c_{1,2}$ est un signe ± 1.

En particulier, on obtient des formules pour tous les quotients $\vartheta_i(z)^2/\vartheta_{16}(z)^2$, $0 \leq i \leq 15$, en évaluant u aux racines de f. Pour trouver les fonctions thêta de niveau 4, on utilise finalement les formules de doublement [Gau07] :

$$4\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](2z)\,\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]\vartheta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right]^2 = \sum_{\alpha,\beta \in \frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2} \exp\left(-4i\pi\, {}^t a\beta\right)\vartheta\left[\begin{smallmatrix} a+\alpha \\ b+\beta \end{smallmatrix}\right](z)^2\,\vartheta\left[\begin{smallmatrix} \alpha \\ \beta \end{smallmatrix}\right](z)^2,$$

$$4\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](2z)\,\vartheta\left[\begin{smallmatrix} a \\ 0 \end{smallmatrix}\right]\vartheta\left[\begin{smallmatrix} 0 \\ b \end{smallmatrix}\right]\vartheta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right] = \sum_{\alpha,\beta \in \frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2} \exp\left(-4i\pi\, {}^t a\beta\right)\vartheta\left[\begin{smallmatrix} a+\alpha \\ b+\beta \end{smallmatrix}\right](z)\,\vartheta\left[\begin{smallmatrix} a+\alpha \\ \beta \end{smallmatrix}\right](z)\,\vartheta\left[\begin{smallmatrix} \alpha \\ b+\beta \end{smallmatrix}\right](z)\,\vartheta\left[\begin{smallmatrix} \alpha \\ \beta \end{smallmatrix}\right](z).$$

La première formule permet de retrouver les fonctions thêta paires et la seconde les impaires. Les produits dans le second membre peuvent être exprimés en termes des constantes f_A et des fonctions $Y_{l,m}$, Y et $u(a_i)$. Comme nous aurons besoin de diviser par $u(a_i)$, on suppose que le support du diviseur ne contient pas de point de Weierstraß affine. Par exemple, la seconde formule fournit

$$\begin{aligned}
\vartheta_{16}(2z)\vartheta_1\vartheta_4\vartheta_8 &= \vartheta_1(z)\vartheta_4(z)\vartheta_8(z)\vartheta_{16}(z) - \vartheta_9(z)\vartheta_{12}(z)\vartheta_{13}(z)\vartheta_{15}(z) \\
&\quad + \vartheta_5(z)\vartheta_6(z)\vartheta_7(z)\vartheta_{11}(z) - \vartheta_2(z)\vartheta_3(z)\vartheta_{10}(z)\vartheta_{14}(z), \\
&= \frac{t_{2,4}(z)t_{2,3}(z)t_{3,4}(z)t_\emptyset(z)}{f_{2,4}f_{2,3}f_{3,4}f_\emptyset} + \frac{t_{1,5}(z)t_2(z)t_4(z)t_3(z)}{f_{1,5}f_2f_4f_3} \\
&\quad + \frac{t_{3,5}(z)t_{4,5}(z)t_{2,5}(z)t_1(z)}{f_{3,5}f_{4,5}f_{2,5}f_1} + \frac{t_{1,3}(z)t_{1,4}(z)t_{1,2}(z)t_5(z)}{f_{1,3}f_{1,4}f_{1,2}f_5}, \\
\frac{\vartheta_{16}(2z)\vartheta_1\vartheta_4\vartheta_8}{t_\emptyset^4(z)} &= \frac{Y_{2,4}Y_{2,3}Y_{3,4}}{u(a_2)u(a_3)u(a_4)}\frac{1}{f_{2,4}f_{2,3}f_{3,4}f_\emptyset} + \frac{Y_{1,5}Y}{u(a_1)u(a_5)}\frac{1}{f_{1,5}f_2f_3f_4} \\
&\quad + \frac{Y_{2,5}Y_{3,5}Y_{4,5}Y}{u(a_2)u(a_3)u(a_4)u(a_5)^2}\frac{1}{f_{2,5}f_{3,5}f_{4,5}f_1} \\
&\quad + \frac{Y_{1,2}Y_{1,3}Y_{1,4}Y}{u(a_1)^2u(a_2)u(a_3)u(a_4)}\frac{1}{f_{1,2}f_{1,3}f_{1,4}f_5}.
\end{aligned}$$

Remarque 5.3.8. *Il est important de garder à l'esprit que, bien que le travail présenté dans cette sous-section soit basé sur $\mathbb{C}$, ces résultats s'appliquent à d'autres corps (de caractéristique différente de 2). Pour les justifier dans le cas qui nous intéresse ici, à savoir sur des surfaces abéliennes définies sur un corps fini, nous pouvons faire appel au principe de Lefschetz puis réduire les résultats sur corps finis. Autrement, dans le cas général, on peut utiliser la théorie algébrique des fonctions thêta développée par Mumford [Mum66, Mum67a, Mum67b].*

Chapitre 6

Complétude de lois d'addition

6.1 Complétude géométrique et ensembles de lois d'addition

Nous allons appliquer les notions introduites dans la précédente section à l'étude de lois d'addition sur une variété abélienne $A/\Bbbk$ plongée dans un espace projectif $\mathbb{P}^r$ pour un certain $r > 1$. Dans la suite de cette partie nous notons $\iota : A \hookrightarrow \mathbb{P}^r$ ce plongement et $\mathcal{L}$ le fibré en droites associé à ce plongement. Pour $\{x_0, \ldots, x_r\}$ une base des fonctions coordonnées dans $\mathbb{P}^r$ nous avons besoin pouvoir décrire les sections globales de $\mathcal{L}$ sur A par des polynômes homogènes en les x_i, *i.e.* ι soit *projectivement normal.*

Définition 6.1.1. *Le plongement $\iota : A \hookrightarrow \mathbb{P}^r$ est dit* projectivement normal *si pour tout $i \geq 1$ la restriction*

$$H^0\big(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(i)\big) \to H^0\big(A, \mathcal{L}^i\big)$$

est surjective.

Dans la suite nous ne considérons que des plongements projectivement normaux. Remarquons que ceci est vrai dans les cas dans les utilisations pratiques des variétés abéliennes. En effet, pour $\mathcal{L} = \mathcal{L}_0^{n_0}$ avec $\mathcal{L}_0$ un fibré en droites ample et $n_0 \geq 3$, le plongement associé est projectivement normal [BL04, Theorem 7.3.1] ou [Sek77].

Définition 6.1.2. *Soient $m, n \geq 2$ deux entiers. Une* loi d'addition *de bidegré (m, n) est un $r+1$-uplet*

$$\mathfrak{p} = (p_0, \ldots, p_r)$$

de polynômes bihomogènes de bidegré (m, n) tel que, sur un ouvert non vide de $A \times A$, le morphisme

$$(x, y) \mapsto \big(p_0(x, y) : \cdots : p_r(x, y)\big)$$

décrit le morphisme de groupe $\mu : A \times A \to A$.

Etant donnée une loi d'addition, l'ensemble de points de $A \times A$ annulant les polynômes p_i est appelé l'*ensemble exceptionnel*. On définit, quelque soit le bidegré, la *loi d'addition nulle* $(0, \ldots, 0)$, son ensemble exceptionnel est $(A \times A)\big(\overline{k}\big)$.

Définition 6.1.3. *Un ensemble de lois d'addition est dit* $\Bbbk$-complet *si pour tout point $\Bbbk$-rationnel $(x, y) \in A \times A$ il existe une loi d'addition dans cet ensemble définie sur un ouvert contenant (x, y). Si cette propriété est vraie sur la clôture algébrique de $\Bbbk$, on parle alors d'ensemble* complet. *Dans le cas d'un singleton $\{\mathfrak{p}\}$ on dit que la loi d'addition $\mathfrak{p}$ est* $\Bbbk$-complète, *respectivement* complète.

Rappelons la Notation 5.2.1 page 56. Soient $m, n \geq 2$ et $\pi_1, \pi_2 : A \times A \to A$ les projections sur le premier, respectivement le second, facteur. Le fibré en droites $\mathcal{M}_{m,n}$ sur $A \times A$ est

$$\mathcal{M}_{m,n} := \mu^*\mathcal{L}^{-1} \otimes \pi_1^*\mathcal{L}^m \otimes \pi_2^*\mathcal{L}^n.$$

Lange et Ruppert interprètent les lois d'addition de bidegré (m, n) en termes de sections globales sur $A \times A$ de $\mathcal{M}_{m,n}$.

Proposition 6.1.4 ([LR85, Lemma 2.1])**.** *Il existe une loi d'addition, respectivement un ensemble complet de lois d'addition, de bidegré (m, n) sur $A \hookrightarrow \mathbb{P}^r$ si et seulement si*

$$H^0(A \times A, \mathcal{M}_{m,n}) \neq 0,$$

respectivement le système linéaire complet $\left|\mathcal{M}_{m,n}\right|$ est sans point de base.

Explicitons le lien entre sections globales de $\mathcal{M}_{m,n}$ et lois d'addition mis en évidence. Soit $0 \neq w \in H^0(A \times A, \mathcal{M}_{m,n})$ une section globale. Pour $0 \leq j \leq r$, soit $t_j := \iota^* X_j$, formant une base de $H^0(A, \mathcal{L})$, où X_j sont les fonctions coordonnées de $\mathbb{P}^r$. On a

$$H^0(A \times A, \mu^*\mathcal{L}) = \mu^* H^0(A, \mathcal{L}),$$

donc $s_j := \mu^* t_j$ est une base de $H^0(A \times A, \mu^*\mathcal{L})$. Pour tout j et $(x, y) \in A \times A$, on a

$$s_j(x, y) = t_j \circ \mu(x, y) = X_j(\iota \circ \mu(x, y)).$$

Ensuite $w \otimes s_j \in H^0(A \times A, \pi_1^*\mathcal{L}^m \otimes \pi_2^*\mathcal{L}^n)$. Le plongement ι étant projectivement normal, on a

$$\pi_1^*\mathcal{L}^m \otimes \pi_2^*\mathcal{L}^n = (\iota \times \iota)^*\big(\mathcal{O}_{\mathbb{P}^r}(m) \otimes \mathcal{O}_{\mathbb{P}^r}(n)\big),$$

ce qui montre l'existence de polynômes bihomogènes p_j de bidegré (m, n) tels que pour tout (x, y),

$$(w \otimes s_j)(x, y) = p_j\big(\iota(x), \iota(y)\big).$$

Ainsi, sur l'ouvert $A \times A \setminus (w)_0$, avec $(w)_0$ le lieu des zéros de la section w, on obtient

$$\begin{aligned}\big(p_0(\iota(x), \iota(y)) : \ldots : p_r(\iota(x), \iota(y))\big) &= \big((w \otimes s_0)(x, y) : \ldots : (w \otimes s_r)(x, y)\big), \\ &= \big(s_0(x, y) : \ldots : s_r(x, y)\big), \\ &= \big(X_0(\iota \circ \mu(x, y)) : \ldots : X_r(\iota \circ \mu(x, y))\big).\end{aligned}$$

Les polynômes définissant une loi d'addition étant considérés modulo l'idéal homogène de A, on obtient un isomorphisme de $\Bbbk$-espaces vectoriels

$$\left\{ \begin{array}{c} \text{lois d'addition de bidegré } (m, n) \\ \text{sur } A \text{ relativement à } \iota \end{array} \right\} \cong H^0(A \times A, \mathcal{M}_{m,n}).$$

Puis en quotientant par l'action naturelle de $\Bbbk^*$ on obtient la bijection suivante

$$\left\{ \begin{array}{c} \text{lois d'addition de bidegré } (m, n) \text{ non nulles} \\ \text{sur } A \text{ relativement à } \iota \end{array} \right\} \Big/ \begin{array}{ccc} \Bbbk^* & \leftrightarrow & |\mathcal{M}_{m,n}| \\ \overline{\mathfrak{p}} & \mapsto & \operatorname{div}(w), \end{array} \tag{6.1}$$

où w est une section globale non nulle de $H^0(A \times A, \mathcal{M}_{m,n})$ telle que la loi d'addition $\mathfrak{p}$ soit définie en dehors de $\operatorname{div}(w)$.

L'étude des lois d'addition mène à considérer des sections sur un fibré en droites sur $A \times A$. On souhaiterait désormais avoir une description simple de telles sections. Le Lemme 5.2.18 page 60 montre que dans la cas biquadratique, *i.e.* $m = n = 2$, si $\mathcal{L}$ est symétrique, le fibré en droites $\mathcal{M}$ est le pullback par δ de $\mathcal{L}$ et qu'il existe un ensemble complet de lois d'addition, tandis que dans le cas contraire il n'existe aucune loi d'addition biquadratique. Si $(m, n) \neq (2, 2)$, on ne connaît pas de description de $\mathcal{M}$ en fonction de $\mathcal{L}$.

Outre l'existence de lois d'addition biquadratiques, le symétrie de $\mathcal{L}$ entraîne que l'inversion $[-1] : A \to A$ est décrite par des polynômes linéaires définis sur $\Bbbk$.

Lemme 6.1.5. *Soit $A/\Bbbk$ une variété abélienne plongée dans un espace projectif $\mathbb{P}^r$ par fibré en droites $\mathcal{L}$ très ample. Si $\mathcal{L}$ est symétrique alors le morphisme d'inversion $[-1] : A \to A$ est induit par un automorphisme de $\mathbb{P}^r$. De plus, si $\mathrm{car}(\Bbbk) \neq 2$, on peut choisir des coordonnées telles que $[-1]$ agisse comme la multiplication par ± 1 sur chaque coordonnée.*

Démonstration. La première partie de l'énoncé est une autre expression de la symétrie de $\mathcal{L}$. Soient (t_i) une base de $H^0(A, \mathcal{L})$ et

$$M := \mathrm{Mat}_{(t_i)}\big([-1]\big).$$

Comme $[-1]$ est induit par une involution de $\mathbb{P}^r$, il existe $\epsilon \in \Bbbk$ tel que

$$M^2 - \epsilon \,\mathrm{Id} = 0. \tag{6.2}$$

Soit O l'élément neutre de A de coordonnées $(a_0 : \cdots : a_r)$ dans $\mathbb{P}^r$ induites par (t_i). Le vecteur $(a_0, \ldots, a_r)$ est un vecteur propre de M de valeur propre un certain $\epsilon_0 \in \Bbbk$. On a ainsi $\epsilon = \epsilon_0^2$ et, si $\mathrm{car}(\Bbbk) \neq 2$, la factorisation de l'équation (6.2) montre que la matrice M peut être diagonalisée sur $\Bbbk$ et a pour valeurs propres $\pm\epsilon_0$, d'où la conclusion. □

Concernant la cardinalité d'un ensemble complet de lois d'addition, Lange et Ruppert [LR87] consacrent un article à l'étude du cas elliptique dans lequel ils construisent un ensemble complet de trois lois d'addition biquadratiques, puis Bosma et Lenstra [BL95] vont plus loin en démontrant, toujours dans le cas elliptique, qu'il suffit de deux lois d'addition pour obtenir un ensemble complet et que ces lois doivent nécessairement être biquadratiques pour que ce minimum soit atteint. Ils apportent aussi un exemple d'un tel ensemble complet. Nous présentons ci-dessous une généralisation de ce résultat.

Théorème 6.1.6. *Soit A une variété abélienne de dimension g plongée dans un espace projectif $\mathbb{P}^r$ par $\mathcal{L}$ très ample et symétrique. Tout ensemble complet de lois d'addition sur A est de cardinalité au moins $g + 1$.*

Démonstration. Soit S un ensemble complet de lois d'addition sur A de bidegré (m, n), $\nabla = \ker(\mu) \subset A \times A$ et O l'élément neutre de A de coordonnées projectives $(a_0 : \cdots : a_r)$. D'après le Lemme 6.1.5, l'isomorphisme

$$[1] \times [-1] : A \to \nabla$$

est linéaire, ainsi $\big([1] \times [-1]\big)^* S$ est un ensemble de morphismes rationnels constants $A \to \{O\}$ décrits par des polynômes homogènes de degré $m+n$. Il existe donc un ensemble I, de cardinalité majorée par $\#S$, de tels polynômes tel que

$$\big([1] \times [-1]\big)^* S = \big\{\big(a_0\, q(x_0, \ldots, x_r), \ldots, a_r\, q(x_0, \ldots, x_r)\big),\ q \in I\big\}.$$

Comme S est un ensemble complet de lois d'addition, la sous-variété $V(I) \cap A$ est vide. Or, on a

$$\dim\big(V(I) \cap A\big) \geq \dim(A) - \#I \geq g - \#S.$$

□

On peut également donner une borne supérieure à la cardinalité d'un tel ensemble dans le cas biquadratique. Si A est une variété abélienne principalement polarisée, nous avons montré dans le Lemme 5.2.13 qu'il existe un fibré en droites ample et symétrique $\mathcal{L}$ induisant cette polarisation. On déduit du Lemme 5.2.18 qu'il existe, pour le plongement défini par $\mathcal{L}^3$, un ensemble complet de lois d'addition biquadratiques de cardinalité $h^0(A, \mathcal{L}^3) = 3^g$ par le théorème de Riemann-Roch (Théorème 5.2.14).

6.2 Complétude arithmétique et lois d'addition

6.2.1 Le cas général

Soit $\mathcal{L}$ un fibré en droites symétrique et très ample, défini par un diviseur D effectif et $\Bbbk$-rationnel sur $A/\Bbbk$, et associé à un plongement projectivement normal. Considérons v une section de $H^0(A, \mathcal{L})$ dont le lieu des zéros est $(v)_0 = D$ et $w = \delta^* v$. D'après le Lemme 5.2.18, w est une section de $H^0(A \times A, \mathcal{M})$ et une loi d'addition biquadratique est définie sur le complémentaire de $(w)_0 = \delta^* D$. Ainsi il est suffisant (et nécessaire) que D soit sans point $\Bbbk$-rationnels pour que cette loi d'addition soit $\Bbbk$-complète.

Théorème 6.2.1. *Soient $A/\Bbbk$ une variété abélienne avec $\Bbbk$ ayant un groupe de Galois absolu infini. On se donne un plongement $\iota_0 : A \hookrightarrow \mathbb{P}^{r_0}$ pour $r_0 > 1$ tel qu'il existe une extension $K/\Bbbk$ de degré $d > r_0$. Il existe un plongement $\iota : A \hookrightarrow \mathbb{P}^r, r = (2d)^g(r_0 + 1) - 1$ et une loi d'addition biquadratique $\Bbbk$-complète associée à ce plongement.*

Démonstration. Soit $\alpha_0 \in K$ n'appartenant pas à une sous-exetnsion propre de K et notons $\alpha_0, \ldots, \alpha_{d-1}$ ses conjugués dans K. Pour $i = 0, \ldots, d-1$, soient H_i les hyperplans de $\mathbb{P}^{r_0}$ suivants

$$H_i : X_0 + \alpha_i X + \cdots + \alpha_i^{r_0} X^{r_0} = 0.$$

Comme on a choisi $d > r_0$, les éléments $1, \alpha_i, \ldots, \alpha_i^{r_0}$ sont $\Bbbk$-linéairement indépendants pour tout i, donc $H_i(\Bbbk)$ est vide. Considérant le diviseur $\Bbbk$-rationnel $\sum H_i$, on définit les diviseurs $D_0 := \iota^*(\sum H_i)$ et $D := D_0 + [-1]^* D_0$ sur A. Alors, le diviseur D est symétrique, effectif, $\Bbbk$-rationnel et sans point $\Bbbk$-rationnels. Soit $\mathcal{L}_0$ le fibré en droites associé à ι_0. Le fibré en droites $\mathcal{L} := \mathcal{L}(D)$ est isomorphe à $\mathcal{L}_0^{2d}$, ainsi est très ample et le plongement associé $A \hookrightarrow \mathbb{P}^r$, pour un certain r, est projectivement normal. Les propriétés du diviseur D montrent qu'il existe une loi d'addition biquadratique $\Bbbk$-complète et, d'après le théorème de Riemann-Roch, on a $r = (2d)^g(r_0 + 1) - 1$. □

6.2.2 Exemple du genre 1

Soit $E/\Bbbk$ une courbe elliptique. Désormais on se restreint au cas $\Bbbk = \mathbb{F}_q$ et on note σ l'automorphisme de Frobenius de $\overline{\Bbbk}/\Bbbk$. Nous nous intéressons au cas où E est donnée par une équation de Weierstraß.

Lemme 6.2.2. *Si $q \geq 5$, il existe un point $P_0 \in E(\overline{\Bbbk})$ dont l'orbite est donnée par trois points distincts dont la somme est O.*

Démonstration. Soit $N : E\left(\mathbb{F}_{q^3}\right) \to E\left(\mathbb{F}_q\right)$ le morphisme de groupes défini par

$$P \mapsto P + P^\sigma + P^{\sigma^2}.$$

On cherche un point $P_0 \in \ker(N) \setminus E\left(\mathbb{F}_q\right)$, on souhaite donc avoir

$$\left|\ker(N)\right| > \left|\ker(N) \cap E\left(\mathbb{F}_q\right)\right|.$$

L'intersection $\ker(N) \cap E(\mathbb{F}_q)$ est le groupe de points de E de 3-torsion $\mathbb{F}_q$-rationnels, donc le second membre de l'équation ci-dessus divise 9. De plus, pour tout $q \geq 5$, on a

$$\big|\ker(N)\big| \geq \frac{\big|E\left(\mathbb{F}_{q^3}\right)\big|}{\big|E\left(\mathbb{F}_q\right)\big|} \geq \frac{q^3+1-2\sqrt{q^3}}{q+1+2\sqrt{q}} > 9,$$

d'où l'existence du point P_0. □

Remarque 6.2.3. *La condition $q \geq 5$ est optimale, en effet, pour $q = 2, 3, 4$, il existe une courbe elliptique $E/\mathbb{F}_q$ telle que $\big|\ker(N)\big| = \big|\ker(N) \cap E(\mathbb{F}_q)\big|$.*

Théorème 6.2.4. *Soient $\Bbbk = \mathbb{F}_q, q \geq 5$, et $E/\Bbbk$ une courbe elliptique. Il existe une loi d'addition biquadratique $\Bbbk$-complète sur $E \subset \mathbb{P}^2$ donnée sous forme de Weierstraß.*

Démonstration. Soit $P_0 \in E(\overline{\Bbbk})$ un point fourni par le Lemme 6.2.2 et $D \in \mathrm{Div}_{\Bbbk}(E)$ le diviseur

$$D := \big(P_0\big) + \big(P_0^{\sigma}\big) + \big(P_0^{\sigma^2}\big).$$

C'est un diviseur $\Bbbk$-rationnel sans point $\Bbbk$-rationnels et, puisque $D \sim 3(O) \sim [-1]^* D$, le fibré en droites $\mathcal{L}(D)$ est symétrique, très ample, et le plongement associé est projectivement équivalent au modèle de Weierstraß de E. □

Remarque 6.2.5. *On peut s'intéresser au cas où le corps de base n'est pas un corps fini. Si $\Bbbk$ est un corps global, ou plus généralement un corps hilbertien (voir [Lan83a, Chapter 9]), on montre qu'un point P_0 comme dans le Lemme 6.2.2 existe. En effet, supposons que E est définie par une cubique $y^2 + a(x)y = f(x)$, sur un corps $\Bbbk$ hilbertien. Il esiste $y_0 \in \Bbbk$ tel que $y_0^2 + a(x)y_0 - f(x)$ est irréductible. On prend alors $P_0 := (x_0, y_0)$ avec x_0 une racine de $y_0^2 + a(x)y_0 - f(x)$ dans $\overline{\Bbbk}$.*

Exemple 6.2.6. *Pour $\mathrm{car}(\Bbbk) \neq 2, 3$, soit $E/\Bbbk$ une courbe elliptique donnée sous forme de Weiesrtraß réduite $Y^2Z = X^3 + aXz^2 + bZ^3$, $a, b \in \Bbbk$. Supposons que $E/\Bbbk$ n'a pas de points $\Bbbk$-rationnels d'ordre 2,* i.e. *$x^3 + ax + b$ est irréductible sur $\Bbbk$. Une loi d'addition biquadratique $\Bbbk$-complète est donnée par*

$$\begin{aligned}\big(\,&(X_1Y_2+Y_1X_2)(Y_1Y_2-6bZ_1Z_2) - a\,(Y_1Z_2+Z_1Y_2)(2X_1X_2-aZ_1Z_2)\\ &\quad - X_1Z_2(aX_1Y_2+3bY_1Z_2) - Z_1X_2(aY_1X_2+3bZ_1Y_2),\\ &Y_1^2Y_2^2 + a\,X_1X_2(3X_1X_2-2aZ_1Z_2) - a^2\,(X_1Z_2+Z_1X_2)^2\\ &\quad + 3b\,(X_1Z_2+Z_1X_2)(3X_1X_2-aZ_1Z_2) - (a^3+9b^2)Z_1^2Z_2^2,\\ &Y_1Y_2(Y_1Z_2+Z_1Y_2) + (3X_1X_2+2aZ_1Z_2)(X_1Y_2+Y_1X_2)\\ &\quad + (aX_1+3bZ_1)Y_1Z_2^2 + Z_1^2(aX_2+3bZ_2)Y_2\,\big),\end{aligned} \tag{6.3}$$

Cette loi provient de la loi d'addition $\big(X_3^{(2)}, Y_3^{(2)}, Z_3^{(2)}\big)$ de Bosma et Lenstra [BL95, pp.237-238] dans le cas particulier $(a_1, a_2, a_3, a_4, a_6) = (0, 0, 0, a, b)$. En effet, l'ensemble exceptionnel de cette loi, qui est un diviseur de $E \times E$, est $\delta^*\{Y = 0\} = \nabla_{P_1} + \nabla_{P_2} + \nabla_{P_3}$, où pour $P \in E(\overline{\Bbbk})$, on note $\nabla_P := \nabla + (P, O)$ le translaté par (P, O) de l'antidiagonale et P_1, P_2, P_3 sont les points d'ordre 2 de E.

Remarquons que l'exemple ci-dessus permet en fait de construire toutes les lois d'addition biquadratiques $\Bbbk$-complètes sur le modèle de Weiestraß d'une courbe elliptique. On a en effet la proposition suivante, valide pour tout corps de base $\Bbbk$.

Proposition 6.2.7. *Soit $E/\Bbbk : y^2+a(x)y = f(x)$ une courbe elliptique donnée par une équation de Weierstraß générale. Les conditions suivantes sont équivalentes.*

1. *Il existe une loi d'addition biquadratique $\Bbbk$-complète sur $E/\Bbbk$.*
2. *Il existe une droite $\Bbbk$-rationnelle d'équation affine $y = b(x), \deg(b) = 1$, qui intersecte E en trois points distincts non $\Bbbk$-rationnels.*
3. *Il existe un polynôme $b(x) \in \Bbbk[x]$ de degré 1 tel que $f(x)-b(x)\big(a(x)+b(x)\big)$ est irréductible.*

Démonstration. Supposons 1. vraie. Le diviseur exceptionnel associé à cette loi d'addition est de la forme $\delta^*(D)$ avec D un diviseur effectif de degré 3 sur E et vérifiant $D \sim 3(O)$ (voir [Koh11]). Alors la droite passant par les trois points dans le support de D est une droite satisfaisant 2. En effet ces trois points ne sont pas $\Bbbk$-rationnels, et soit $ax + by = c$ une équation affine de cette droite, alors l'irrationalité des points d'intersection avec E entraîne $b \neq 0$, d'où la condition 2.

Maintenant supposons 2. On applique l'isomorphisme suivant

$$\begin{array}{rcl} \phi : E & \to & E' \\ (x : y : z) & \mapsto & \big(x : y - b_h(x,z) : z\big) \end{array}$$

défini sur $E\big(\overline{\Bbbk}\big)$, où E' est la courbe elliptique d'équation

$$E'/\Bbbk : y^2 + \big(a(x) + 2b(x)\big)y = f(x) - b(x)\big(a(x) + b(x)\big)$$

et $b_h(x,z)$ est le polynôme homogène associé à $b(x)$. Pour $i = 1, 2, 3$, soient $P_i = (x_i : y_i : 1)$ les trois points annoncés en condition 2. Leur corps de définition est une extension $K/\Bbbk$ de degré 3, en particulier chaque coordonnée x_i vit dans K et non un sous-corps propre. De plus, l'image des points P_i par ϕ sont les points $(x_i : 0 : 1) \in E'(K)$. Donc les x_i sont les trois racines du polynôme $f(x) - b(x)\big(a(x) + b(x)\big)$, qui est donc irréductible sur $\Bbbk$. On obtient ainsi 3.

Finalement supposons 3. Bosma et Lenstra [BL95] fournissent une loi d'addition biquadratique associée à la section y (voir les commentaires de l'Exemple 6.2.6), que nous notons $\mathfrak{p}'$, sur la courbe elliptique E' définie précédemment. Alors on construit la loi d'addition $\mathfrak{p}$ sur E telle que le diagramme suivant soit commutatif.

$$\begin{array}{ccc} E' \times E' & \xrightarrow{\mathfrak{p}'} & E' \\ {\scriptstyle \phi\times\phi}\uparrow & & \downarrow{\scriptstyle \phi^{-1}} \\ E \times E & \xrightarrow[\mathfrak{p}]{} & E \end{array}$$

La loi d'addition $\mathfrak{p}$ est $\Bbbk$-complète car $\mathfrak{p}'$ l'est et les morphismes ϕ et ϕ^{-1} sont définis par une seule famille de polynômes sur $E'(k)$. Elle est aussi biquadratique parce que ϕ et ϕ^{-1} sont des transformations linéaires. □

6.2.3 Mise à profit de la torsion

Nous donnons ici quelques résultats et notions dûs à Kohel [Koh11, Section 7]. Soit G un sous-groupe de torsion fini. Un diviseur D_0 est dit G-invariant si pour tout $P \in G$, $t_P^* D_0 = D_0$.

Lemme 6.2.8. *Soit $\mathcal{L} = \mathcal{L}(D)$, D effectif et G un sous-groupe de torsion fini. Si D est G-invariant alors G agit sur A par automorphismes de $\mathbb{P}^r$.*

Démonstration. Soit $P \in G$, l'égalité $t_P^* D = D$ entraîne que t_P^* induit un automorphisme linéaire de $H^0(A, \mathcal{L})$. Le plongement $\iota : A \hookrightarrow \mathbb{P}^r$ étant supposé projectivement normal, la surjection $H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(1)) \to H^0(A, \mathcal{L})$, t_P est décrit par des polynômes linéaires. □

Soit G_2 le noyau du morphisme de groupes $G \times G \times G \to G$, $(R, S, T) \mapsto R + S + T$. Soient $m, n \geq 2$, le lemme précédent nous montre que G_2 agit linéairement sur les lois d'addition de bidegré (m, n) comme suit :

$$\forall (P, Q) \in A \times A, \qquad (R, S, T) \cdot \mathfrak{p}\ (P, Q) := \mathfrak{p}(P + R, Q + S) + T.$$

Définition 6.2.9. *Une loi d'addition $\mathfrak{p}$ est dite G_2-complète si l'ensemble*

$$\left\{(R, S, T) \cdot \mathfrak{p}\ ;\ (R, S, T) \in G_2\right\}$$

est un ensemble complet de lois d'addition.

Kohel [Koh11, Section 8] utilise la $\Bbbk$-rationalité de sous-groupes de 3, 4 ou 5-torsion de divers modèles elliptiques pour construire des bases de l'espaces des lois d'addition biquadratiques. Nous construirons, au Chapitre 7 dans le cas du plongement usuel dans $\mathbb{P}^{15}$ de la jacobienne d'une courbe C de genre 2, une base de l'espace des lois d'addition biquadratiques engendrée par chacun de ses éléments par l'action de G_2 pour G le groupe des points de 2-torsion de Jac_C.

Chapitre 7

Le cas du genre 2

Comme pour le cas du genre 1 présenté dans les Sous-Sections 6.2.2, nous voulons construire une loi d'addition pour un plongement projectif usuel de la jacobienne d'une courbe de genre 2 définie sur un corps fini. Nous avons donné les rappels relatifs à l'arithmétique sur les courbes hyperelliptiques de genre 2 dans les Sections 5.3.1 et 5.3.2.

7.1 Existence

Soit C une courbe de genre 2 définie sur un corps fini $\Bbbk = \mathbb{F}_q$ et $P \mapsto \overline{P}$ son involution hyperelliptique. Par [TV91, Proposition 2.3.21], C possède un diviseur $\Bbbk$-rationnel de degré 1 noté P_∞ et tel que $2P_\infty \sim \kappa_C$. Nous renvoyons à la Sous-Section 5.3.1 pour les rappels sur la construction de la jacobienne de C.

Suivant la démonstration du Théorème 6.2.4 page 71, on utilise l'existence d'un point P_0 ayant une orbite galoisienne particulière pour la construction du diviseur $D \in \mathrm{Div}_{\Bbbk}(\mathrm{Jac}_C)$ souhaité (voir Sous-Section 6.2.1).

Lemme 7.1.1. *Si $q \geq 7$, il existe un point $P_0 \in C\big(\overline{\Bbbk}\big)$ dont l'orbite galoisienne a cardinalité 4 et tel que $P_0^{\sigma^2} = \overline{P_0}$.*

Démonstration. Soit $\pi : C \to \mathbb{P}^1$ le quotient par l'involution hyperelliptique. On cherche un point $P_0 \in C\big(\mathbb{F}_{q^4}\big) \setminus C\big(\mathbb{F}_{q^2}\big)$ tel que $\pi(P_0) \in \mathbb{P}^1(\mathbb{F}_{q^2})$. On remarque qu'un tel point n'existe pas si et seulement si $\pi\big(C(\mathbb{F}_{q^2})\big) = \mathbb{P}^1\big(\mathbb{F}_{q^2}\big)$. Cette dernière condition est équivalente à

$$\big|C\big(\mathbb{F}_{q^2}\big)\big| = 2(q^2+1) - e_2,$$

où e_2 est le nombre de points de Weierstraß dans $C\big(\mathbb{F}_{q^2}\big)$. Pour $q \geq 7$, la borne de Weil

$$\big|C\big(\mathbb{F}_{q^2}\big)\big| \leq q^2 + 4q + 1$$

contredit cette égalité, d'où l'existence du point P_0. □

Remarque 7.1.2. *Comme pour le genre 1, la condition $q \geq 7$ est optimale car pour $q = 2, 3, 4, 5$ il existe des contre-exemples. Dans le cas $q = 5$, la preuve est mise en défaut seulement lorsque tous les points de Weierstraß sont $\mathbb{F}_{q^2}$-rationnels ($e_2 = 6$).*

On peut désormais énoncer notre principal résultat pour le genre 2.

Théorème 7.1.3. *Soit C une courbe de genre 2 définie sur $\Bbbk = \mathbb{F}_q, q \geq 7$. Il existe une loi d'addition biquadratique $\Bbbk$-complète pour le plongement $\mathrm{Jac}_C \hookrightarrow \mathbb{P}^{15}$ associé à $\mathcal{L}(4\Theta)$.*

Démonstration. Soit $P_0 \in C$ un point tel que dans le Lemme 7.1.1 précédent. On définit les quatre points de Jac_C suivants

$$\begin{aligned} \alpha_0 &:= \big(P_0\big) + \big(P_0^\sigma\big) - \kappa_C, \quad \alpha_1 := \big(P_0^\sigma\big) + \big(\overline{P_0}\big) - \kappa_C, \\ \alpha_2 &:= \big(\overline{P_0}\big) + \big(\overline{P_0}^\sigma\big) - \kappa_C, \quad \alpha_3 := \big(\overline{P_0}^\sigma\big) + \big(P_0\big) - \kappa_C. \end{aligned}$$

Remarquons que, pour $i = 0, \ldots, 3$, on a $\alpha_i = \alpha_0^{\sigma^i}$ et $\sum \alpha_i = 0$. Aussi, d'après la Proposition 5.3.3, on obtient

$$\begin{aligned} \Theta_{\alpha_0} \cap \Theta_{\alpha_1} &= \Big(\Theta \cap \Theta_{(\overline{P_0})-(P_0)}\Big) + \alpha_0 = \big\{\big(\overline{P_0}\big) - P_\infty + \alpha_0\big\}, \\ \Theta_{\alpha_0} \cap \Theta_{\alpha_3} &= \Big(\Theta \cap \Theta_{(\overline{P_0}^\sigma)-(P_0^\sigma)}\Big) + \alpha_0 = \big\{\big(\overline{P_0}^\sigma\big) - P_\infty + \alpha_0\big\}. \end{aligned} \tag{7.1}$$

Définissons le diviseur $D := \sum \Theta_{\alpha_i}$ sur Jac_C, vérifions qu'il satisfait toutes les propriétés cherchées. Il est par construction ample, symétrique, $\Bbbk$-rationnel et linéairement équivalent à 4Θ. L'action du groupe de Galois sur les composantes Θ_{α_i} étant transitive, tout point $\Bbbk$-rationnel est dans leur intersection. Ainsi D n'a pas de points $\Bbbk$-rationnels par (7.1). □

On peut étendre ce résultat quand le corps de définition est un corps de nombres en adaptant l'idée utilisée dans la Remarque 6.2.5 en construisant un point P_0 ayant la même propriété que dans le Lemme 7.1.1. Cependant on se limite aux courbes C définies par une équation de la forme $y^2 = f(x)$ avec $\deg(f) = 5$ et $P_\infty = (\infty)$. Dans le cas général, un tel diviseur P_∞ peut ne plus exister.

Remarque 7.1.4. *La construction du diviseur D dans la preuve du Théorème 7.1.3 fait intervenir des points α_i de $W^2 = W^g$. En général, pour C une courbe de genre g, de tels diviseurs sont nécessaires pour généraliser une telle construction. En effet, d'après [FK80, Proposition III.11.16 case b. p.146] on a*

$$\bigcap_{a \in W^r + b} \Theta_{-a} \neq \emptyset,$$

pour tout $0 \leq r \leq g-1$ et $b \in \mathrm{Jac}_C$.

7.2 Construction

Nous voulons utiliser les morphismes décrits dans la Sous-Section 5.3.2, pour cela nous supposons désormais que q est impair et que C est donnée sous forme de Rosenhain. Comme dans cette sous-section nous utilisons une notation complexe et décrivons le plongement ι à l'aide des fonctions thêta de niveau 4, mais ces résultats restent vrais sur $\mathbb{F}_q$ (voir la Remarque 5.3.8).

7.2.1 Une base de l'espace des lois d'addition biquadratiques

Les formules d'addition de Riemann sont largement connues et répandues dans la littérature. Nous appliquons les formules générales données par Baily [Bai62, Section 2.2, Formulae (9)] pour obtenir les formules suivantes pour les fonctions thêta de niveau 4.

Proposition 7.2.1 (Formules d'addition de Riemann). *Soient $a_k, b_l \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$, $k,l = 1,\dots,4$ tels que*

$$-a_1 + a_2 + a_3 + a_4 = 2a, \qquad -b_1 + b_2 + b_3 + b_4 = 2b,$$

avec $a, b \in \frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2$, alors pour tout z_1, $z_2 \in \mathbb{C}^2$ on a

$$4\,\vartheta\left[\begin{smallmatrix} a_1 \\ b_1 \end{smallmatrix}\right](z_1+z_2)\,\vartheta\left[\begin{smallmatrix} a_2 \\ b_2 \end{smallmatrix}\right](z_1-z_2)\,\vartheta\left[\begin{smallmatrix} a_3 \\ b_3 \end{smallmatrix}\right](0)\,\vartheta\left[\begin{smallmatrix} a_4 \\ b_4 \end{smallmatrix}\right](0) = \sum_{\alpha,\beta\in\frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2} \vartheta\left[\begin{smallmatrix} a_1+a+\alpha \\ b_1+b+\beta \end{smallmatrix}\right](z_2)\,\vartheta\left[\begin{smallmatrix} a_2-a+\alpha \\ b_2-b+\beta \end{smallmatrix}\right](z_2)\,\vartheta\left[\begin{smallmatrix} a_3-a+\alpha \\ b_3-b+\beta \end{smallmatrix}\right](z_1)\,\vartheta\left[\begin{smallmatrix} a_4-a+\alpha \\ b_4-b+\beta \end{smallmatrix}\right](z_1).$$

Pour tout $a_1, a_2, b_1, b_2 \in \frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2$, il existe $a_3, a_4, b_3, b_4 \in \frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2$ vérifiant la condition de la proposition et tels que la constante $\vartheta\left[\begin{smallmatrix} a_3 \\ b_3 \end{smallmatrix}\right](0)\,\vartheta\left[\begin{smallmatrix} a_4 \\ b_4 \end{smallmatrix}\right](0)$ soit non nulle. On revient maintenant aux notations 5.3.5.

Remarque 7.2.2. *Le plongement $\mathrm{Jac}_C \hookrightarrow \mathbb{P}^{15}$ est associé au fibré en droites $\mathcal{L} = \mathcal{L}(4\Theta)$. On considère maintenant les fonctions ϑ_i comme sections globales de ce fibré en droites. Aussi, pour éviter de surcharger les notations, nous notons de la même façon les points de Jac_C et leur image dans $\mathbb{P}^{15}$.*

Remarque 7.2.3. *Les formules ci-dessus expriment, pour $i,j = 1,\dots,16$, le produit $\vartheta_i(z_1+z_2)\vartheta_j(z_1-z_2)$ comme un polynôme biquadratique bihomogène en les fonctions thêta de niveau 4 $\{\vartheta_1(z_1),\dots,\vartheta_{16}(z_1)\}$ et $\{\vartheta_1(z_2),\dots,\vartheta_{16}(z_2)\}$. On remarque également qu'ils sont définis sur le corps de définition des thêta constantes, que l'on note $\mathbb{K}$. Comme nous voulons que le morphisme δ soit $\Bbbk$-rationnel (voir la Section 6.2), nous supposons que les thêta constantes sont $\Bbbk$-rationnelles. Ce n'est pas en contradiction avec la construction d'une loi d'addition $\Bbbk$-complète car toute loi d'addition $\mathbb{K}$-complète sera en particulier $\Bbbk$-complète. On suppose donc dans la suite que $\mathbb{K} = \Bbbk$.*

Cela signifie qu'en fixant l'indice j, si z_1, z_2 sont tels que $\vartheta_j(z_1-z_2) \neq 0$, alors il existe un polynôme biquadratique bihomogène $p_{i,j}$ tel que

$$\vartheta_i(z_1+z_2)\vartheta_j(z_1-z_2) = p_{i,j}\big((\vartheta_1(z_1),\dots,\vartheta_{16}(z_1)),(\vartheta_1(z_2),\dots,\vartheta_{16}(z_2))\big). \tag{7.2}$$

Notation 7.2.4. *Ceci nous permet de construire une loi d'addition*

$$\mathfrak{p}_j := (p_{1,j},\dots,p_{16,j})$$

définie en dehors de l'ensemble exceptionnel $\delta^*(\vartheta_j)_0$.

Soient $x_k = \big(\vartheta_1(z_k) : \cdots : \vartheta_{16}(z_k)\big) \in \iota\left(\mathrm{Jac}_C\right), k = 1,2$, deux points tels que $x_1 - x_2 \notin (\vartheta_j)_0$ $\big($ou de façon équivalente satisfaisant $\vartheta_j(z_1-z_2) \neq 0\big)$. On a

$$\begin{aligned}\iota\circ\mu\,(x_1,x_2) &= \big(\vartheta_1(z_1+z_2) : \cdots : \vartheta_{16}(z_1+z_2)\big)\\ &= \big(\vartheta_j(z_1-z_2)\vartheta_1(z_1+z_2) : \cdots : \vartheta_j(z_1-z_2)\vartheta_{16}(z_1+z_2)\big)\\ &= \mathfrak{p}_j(x_1,x_2).\end{aligned}$$

Il est clair que l'ensemble $\{\mathfrak{p}_1,\dots,\mathfrak{p}_{16}\}$ est complet puisque les fonctions thêta de niveau 4 induisent un plongement projectif de la variété, donc n'ont pas de zéro commun. Plus qu'un ensemble complet, la proposition suivante montre qu'elles forment une base de l'espace des lois d'addition biquadratiques.

Proposition 7.2.5. *L'ensemble* $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_{16}\}$ *est une base de l'espace des lois d'addition biquadratiques sur* $\mathrm{Jac}_C \hookrightarrow \mathbb{P}^{15}$.

Démonstration. On a $\dim_{\Bbbk}\big(\mathcal{L}(4\Theta)\big) = 16$, donc par le Lemme 5.2.18 page 60, le $\Bbbk$-espace vectoriel des lois d'addition biquadratiques sur Jac_C est de dimension 16. Ainsi, il suffit de montrer que la famille $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_{16}\}$ est libre. Démontrons-le par l'absurde en supposant qu'il existe une relation linéaire non triviale

$$\sum \lambda_j \mathfrak{p}_j = 0. \tag{7.3}$$

Notons O_J l'élément neutre de Jac_C. Alors pour tout $x = \big(\vartheta_1(z) : \cdots : \vartheta_{16}(z)\big) \in \mathrm{Jac}_C$, la relation $\sum \lambda_j \mathfrak{p}_j(x, O_J) = 0$ implique

$$\sum \lambda_j p_{i,j}(x, O_J) = 0, \qquad \text{pour tout } i = 1, \ldots, 16.$$

De plus il existe un certain k_0 tel que $\vartheta_{k_0}(z) \neq 0$, donc

$$0 = \sum \lambda_j p_{k_0,j}(x, O_J) = \sum \lambda_j \vartheta_{k_0}(z+0)\vartheta_j(z-0) = \vartheta_{k_0}(z) \sum \lambda_j \vartheta_j(z).$$

La dépendance en k_0 étant éliminée, on obtient finalement la relation linéaire non triviale

$$\sum \lambda_j \vartheta_j = 0,$$

qui est contradictoire car la famille $\{\vartheta_j, j = 1, \ldots, 16\}$ est une base de l'espace des fonctions thêta de niveau 4. Ainsi l'existence de l'équation (7.3) est fausse, et $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_{16}\}$ une famille libre. □

On termine cette sous-section en donnant un dernier résultat sur la complétude géométrique. Le théorème suivant nous dit que l'on peut en extraire un ensemble complet de cardinalité minimale (voir le Théorème 6.1.6).

Théorème 7.2.6. *Il existe un ensemble complet de trois lois d'addition sur* $\mathrm{Jac}_C \hookrightarrow \mathbb{P}^{15}$.

Démonstration. On choisit deux lois d'addition $\mathfrak{p}_i, \mathfrak{p}_j$ dans $\{\mathfrak{p}_{11}, \ldots, \mathfrak{p}_{16}\}$, le diviseur des thêta fonctions auxquelles elles sont associées sont des translatés du diviseur Θ par certains $(A_i) - (\infty)$ et $(A_j) - (\infty)$ avec $i \neq j \in \{1, \ldots, 5, \infty\}$. L'intersection de ces deux diviseurs est réduite aux deux points de 2-torsion $\big\{0, (A_i) - (A_j)\big\}$ (Proposition 5.3.3). Mais chaque image dans $\mathbb{P}^{15}$ d'un point de 2-torsion de Jac_C a six coordonnées nulles, donc il existe une fonction thêta ϑ_k dont le diviseur ne contient pas ces deux points. Ainsi l'ensemble $\{\mathfrak{p}_i, \mathfrak{p}_j, \mathfrak{p}_k\}$ est complet. □

7.2.2 Principe de la construction

À partir d'ici et sans mention contraire nous supposons que $\Bbbk = \mathbb{F}_q$. Nous voulons maintenant construire la loi d'addition annoncée dans le Théorème 7.1.3 page 75. Notons $\mathfrak{p}$ cette loi d'addition biquadratique $\Bbbk$-complète dont l'ensemble exceptionnel est $\delta^* D$ avec $D \in \mathrm{Div}_{\Bbbk}(\mathrm{Jac}_C)$ et $D = \sum \Theta_{\alpha_i} \sim 4\Theta$ pour certains points α_i. Notre but est de construire une solution projective $(\lambda_1 : \cdots : \lambda_{16})$ de la relation

$$\mathfrak{p} = \sum \lambda_j \mathfrak{p}_j \tag{7.4}$$

en utilisant une méthode d'interpolation. Pour cela, soit $x \in D$. Comme on veut que $\mathfrak{p}$ ne soit pas définie sur $\delta^* D$, elle ne doit pas l'être, en particulier, au point (x, O_J). On cherche donc des solutions au système linéaire

$$0 = \sum \lambda_j \mathfrak{p}_j(x, O_J).$$

En choisissant aléatoirement le point $x \in D$, on s'attend à obtenir un système linéaire de rang 15. Remarquons que la solution est projective parce qu'une loi d'addition est définie par son ensemble exceptionnel à la multiplication par un scalaire près.

Remarque 7.2.7. *Soit $\mathfrak{p}$ une loi d'addition. Il est intéressant de voir que la commutativité de μ n'implique pas nécessairement la symétrie $\mathfrak{p}(x,y) = \mathfrak{p}(y,x)$ puisqu'il se peut que $\mathfrak{p}$ soit définie au point (x,y) sans l'être en son symétrique. Dans le cas biquadratique, cela vient du fait que, si l'ensemble exceptionnel de $\mathfrak{p}$ est $\delta^* D$, $x - y \in D$ n'implique pas $y - x \in D$. On voit même directement que $\mathfrak{p}$ est symétrique si et seulement si $D = [-1]^* D$.*

Le théorème suivant permet de limiter le calcul des coefficients λ_j de l'équation (7.4) aux dix premiers. Cette propriété vient de l'égalité $D = [-1]^* D$ plus forte que la propriété de symétrie demandée par la théorie. Rappelons que les lois d'addition $\mathfrak{p}_j$ admettent $\delta^*(\vartheta_j)_0$ comme ensemble exceptionnel (Notation 7.2.4).

Théorème 7.2.8. *Supposons $\Bbbk = \mathbb{F}_q$, avec $q \geq 7$ et $(2,q) = 1$. Soit $\mathfrak{p}$ la loi d'addition introduite ci-dessus et $\mathfrak{p} = \sum \lambda_j \mathfrak{p}_j$ la décomposition de $\mathfrak{p}$ dans la base $\{\mathfrak{p}_j\}$. On a*

$$\lambda_{11} = \cdots = \lambda_{16} = 0.$$

Démonstration. Nous allons utiliser le fait que, par construction, pour tout $x \in D$ on a $-x \in D$. Ceci entraîne que

$$\forall x \in D, \qquad \mathfrak{p}(x, O_J) = \mathfrak{p}(O_J, x) = 0. \tag{7.5}$$

Par parité des fonctions thêta ϑ_j, on réexprime le second membre

$$\mathfrak{p}(O_J, x) = \sum \lambda_j \mathfrak{p}_j(O_J, x) = \sum_{j=1}^{10} \lambda_j \mathfrak{p}_j(x, O_J) - \sum_{j=11}^{16} \lambda_j \mathfrak{p}_j(x, O_J).$$

Les formules (7.5) nous amènent ainsi à considérer les deux équations suivantes

$$\forall x \in D, \qquad \sum_{j=1}^{10} \lambda_j \mathfrak{p}_j(x, O_J) = 0, \text{ et } \sum_{j=11}^{16} \lambda_j \mathfrak{p}_j(x, O_J) = 0. \tag{7.6}$$

Définissons les deux lois d'addition biquadratiques apparaissant ici

$$\mathfrak{q}_1 := \sum_{j=1}^{10} \lambda_j \mathfrak{p}_j, \qquad \mathfrak{q}_2 := \sum_{j=11}^{16} \lambda_j \mathfrak{p}_j,$$

et notons D_1, D_2 les diviseurs sur Jac_C décrivant leurs ensembles exceptionnels respectifs. Nous voulons montrer que $\mathfrak{q}_2$ est nulle. D'après la bijection (6.1), ils vérifient, pour $k = 1, 2$, soit $D_k \sim 4\Theta$ soit $\mathfrak{q}_k = 0$. Les formules (7.6) impliquent $D \leq D_k$, d'où, soit $D_k = D$ soit $\mathfrak{q}_k = 0$. Mais on remarque que $\mathfrak{q}_2(O_J, O_J) = 0$ car les thêta constantes de chacune des coordonnées de $\mathfrak{q}_2(O_J, O_J)$ est nulle $\big($voir les formules (7.2)$\big)$. Or le point (O_J, O_J) est un point $\Bbbk$-rationnel de $\mathrm{Jac}_C \times \mathrm{Jac}_C$ qui n'appartient pas à D par construction. Ainsi $\mathfrak{q}_2$ est nulle. □

Remarque 7.2.9. *Nous n'avons pas obtenu plus d'informations sur les coefficients λ_j en utilisant les équations $\mathfrak{p}(-x, O_J) = \mathfrak{p}(O_J, -x) = 0$ pour $x \in D$.*

Enfin, remarquons que les coordonnées de Mumford des points sur le diviseur $D = \sum \Theta_{\alpha_i}$ sont facilement générées. En effet, ils sont de la forme $x = (P) - (\infty) + \alpha_i$ avec $P \in C\big(\overline{\Bbbk}\big)$. De plus on connaît, par construction, les coordonnées de Mumford (u_i, v_i) de α_i. On choisit alors aléatoirement $x_P \in \overline{\Bbbk}$ et calcule y_P tel que $y_P^2 = f(x_P)$. Ainsi $(x - x_P, y_P)$ sont les coordonnées de Mumford du point $(P) - (\infty)$ et on utilise l'algorithme de Cantor pour calculer les coordonnées de Mumford de x. À partir des coordonnées de Mumford du point x, on calcule ses coordonnées thêta en utilisant les morphismes présentés dans la Sous-Section 5.3.2. Ceci ne peut pas être fait de façon simple en utilisant directement les coordonnées thêta.

7.2.3 Formules explicites

AVIsogenies est un package Magma développé pour travailler sur les variétés abéliennes, en particulier les surfaces abéliennes, en utilisant les fonctions thêta. Nous avons écrit, avec Cosset, des fonctions calculant les coefficients λ_j étant donnée une courbe de genre 2 sous forme de Rosenhain. Le code fait maintenant partie de AVIsogenies.

Exemple 7.2.10. *Considérons la courbe*

$$C : \quad y^2 = f(x) = x^5 + 5782x^4 + 2517x^3 + 2312x^2 + 9402x$$

définie sur le corps fini $\mathbb{F}_{10007}$. *Les thêta constantes associées sont*

$$\begin{array}{llll} \vartheta_1 = 1, & \vartheta_2 = 5242, & \vartheta_3 = 7727, & \vartheta_4 = 678, \\ \vartheta_5 = 3926, & \vartheta_6 = 7092, & \vartheta_7 = 5628, & \vartheta_8 = 7556, \\ \vartheta_9 = 3666, & \vartheta_{10} = 904. & & \end{array}$$

Soient

$$K = \mathbb{F}_{10007}[X] \,/\, \left(X^2 + 1\right) \simeq \mathbb{F}_{10007^2}$$

et $x_0 = 8310 + 2164\sqrt{-1}$. *Le point* $P_0 = \left(x_0, \sqrt{f(x_0)}\right)$ *est un point de* $C\left(\mathbb{F}_{10007^4}\right) \setminus C\left(\mathbb{F}_{10007^2}\right)$. *On trouve les coefficients* λ_j *non nuls suivants*

$$\begin{array}{llll} \lambda_1 = 1, & \lambda_2 = 6924, & \lambda_3 = 1940, & \lambda_4 = 9380, \\ \lambda_5 = 5155, & \lambda_6 = 1278, & \lambda_7 = 7239, & \lambda_8 = 1761, \\ \lambda_9 = 6859, & \lambda_{10} = 5891. & & \end{array}$$

Ces calculs ont pris moins d'une minute. Pour les plus sceptiques, il est possible de vérifier que la loi d'addition ainsi construite est $\mathbb{F}_{10007}$*-complète par un calcul exhaustif. Remarquons qu'il est suffisant de vérifier que l'on a bien* $\mathfrak{p}(x, O_J)$ *pour tout* $x \in \mathrm{Jac}_C\left(\mathbb{F}_{10007}\right)$. *Cette vérification prit une semaine sur une machine de bureau usuelle.*

Concernant l'efficacité de ces lois d'addition, on imagine aisément que ce n'est pas leur plus grande qualité en voyant ci-dessous la loi $\mathfrak{p}_1$. Le calcul de celle-ci coûte $240\mathbf{m} + 16\mathbf{s} + 16\mathbf{m}_\vartheta$, où $\mathbf{m}_\vartheta$ représente la multiplication, dans chaque coordonnée, par un coefficient ne dépendant que des thêta constantes et qui peut être précalculé. On ne prend pas en compte le coût des additions ou des changements de signe. Le calcul de la loi d'addition $\mathfrak{p} = \sum \lambda_j \mathfrak{p}_j$ demande le calcul des dix lois d'addition $\mathfrak{p}_1, \ldots, \mathfrak{p}_{10}$ qui coûterait a priori dix fois le coût de $\mathfrak{p}_1$. Mais en utilisant des propriétés de symétrie des ces lois d'addition on peut se ramener à un coût de "seulement"

$$736\mathbf{m} + 32\mathbf{s} + 160\mathbf{m}_\vartheta.$$

Les lois d'addition $\mathfrak{p}_i$ venant des relations de Riemann (Proposition 7.2.1), elles ont une forme particulière. En effet, on remarque que les polynômes $p_{i,j}, i \neq j$, sont le produit d'une constante avec un polynôme à coefficients dans $\{\pm 1\}$ constitué de huit monômes. De même, les monômes de $p_{i,i}$, $i = 1, \ldots, 10$ sont $\pm X_i^2 Y_i^2$. Nous donnons la loi $\mathfrak{p}_1$ dans l'Exemple 7.2.12 ci-dessous pour éclaircir les propos de ce paragraphe ; nous ne présentons pas les autres lois, celles-ci ayant un aspect combinatoire identique. Les coefficients λ_j étant précalculés, on calcule directement $\lambda_j \mathfrak{p}_j$, de telle sorte que l'on ait un coût de $160\mathbf{m}_\vartheta$. Détaillons maintenant le calcul des monômes. Étant donnés deux points $x = \left(X_1 : \cdots : X_{16}\right)$ et $y = \left(Y_1 : \cdots : Y_{16}\right)$ on commence par calculer tous les produits $X_i X_j$ et $Y_i Y_j$, ceci coûte $240\mathbf{m} + 32\mathbf{s}$, puis les produits $X_i X_j Y_i Y_j$ en $256\mathbf{m}$. Ces monômes biquadratiques sont exactement ceux intervenant dans les dix premiers polynômes des lois d'addition $\mathfrak{p}_j, 1 \leq j \leq 10$ (voir l'Exemple 7.2.12 ci-dessous), donc le calcul des

polynômes $p_{i,j}$ ne requiert pas d'autres opérations (mises à part les additions et changements de signe). Pour les polynômes restants $p_{i,j}$ avec $11 \leq i \leq 16$ et $1 \leq j \leq 10$, remarquons la symétrie $\mathfrak{p}_j(x,y) = \mathfrak{p}_j(y,x)$ permettant de calculer chacun d'eux en $4\mathbf{m}$ en utilisant la relation

$$X_{i_0}X_{j_0}Y_{k_0}Y_{l_0} + X_{k_0}X_{l_0}Y_{i_0}Y_{j_0} = \\ \big(X_{i_0}X_{j_0} + X_{k_0}X_{l_0}\big)\big(Y_{i_0}Y_{j_0} + Y_{k_0}Y_{l_0}\big) - X_{i_0}X_{j_0}Y_{i_0}Y_{j_0} - X_{k_0}X_{l_0}Y_{k_0}Y_{l_0}.$$

D'où un coût total de $736\mathbf{m} + 32\mathbf{s} + 160\mathbf{m}_\vartheta$.

Remarque 7.2.11. *Par analogie avec les lois d'addition construites par Kohel [Koh11, Section 8], on remarque que, pour $G = \mathrm{Jac}_C[2]$, toute loi d'addition de $\{\mathfrak{p}_i\}_{1\leq i\leq 16}$ est G_2-complète (voir la Sous-Section 6.2.3) et que, parallèlement, ces lois d'addition sont relativement plus efficaces en comparaison avec d'autres lois d'addition que l'on obtiendrait par combinaisons linéaires.*

Exemple 7.2.12. *Soient $x = \big(X_1 : \cdots : X_{16}\big), y = \big(Y_1 : \cdots : Y_{16}\big) \in \mathrm{Jac}_C \subset \mathbb{P}^{15}$. Nous donnons ci-dessous les polynômes biquadratiques définissant $\mathfrak{p}_1(x,y)$.*

$$p_{1,1} = \sum_{i=1}^{16} X_i^2 Y_i^2,$$
$$p_{2,1} = \frac{2\vartheta_1}{\vartheta_2}\big(X_1X_2Y_1Y_2 + X_3X_4Y_3Y_4 + X_5X_{15}Y_5Y_{15} + X_6X_{13}Y_6Y_{13} + X_7X_{12}Y_7Y_{12} + X_8X_{10}Y_8Y_{10} + X_9X_{11}Y_9Y_{11} + X_{14}X_{16}Y_{14}Y_{16}\big),$$
$$p_{3,1} = \frac{2\vartheta_1}{\vartheta_3}\big(X_1X_3Y_1Y_3 + X_2X_4Y_2Y_4 + X_5X_{13}Y_5Y_{13} + X_6X_{15}Y_6Y_{15} + X_7X_9Y_7Y_9 + X_{11}X_{12}Y_{11}Y_{12} + X_8X_{14}Y_8Y_{14} + X_{10}X_{16}Y_{10}Y_{16}\big),$$
$$p_{4,1} = \frac{2\vartheta_1}{\vartheta_4}\big(X_1X_4Y_1Y_4 + X_2X_3Y_2Y_3 + X_5X_6Y_5Y_6 + X_7X_{11}Y_7Y_{11} + X_8X_{16}Y_8Y_{16} + X_{10}X_{14}Y_{10}Y_{14} + X_9X_{12}Y_9Y_{12} + X_{13}X_{15}Y_{13}Y_{15}\big),$$
$$p_{5,1} = \frac{2\vartheta_1}{\vartheta_5}\big(X_1X_5Y_1Y_5 - X_2X_{15}Y_2Y_{15} - X_3X_{13}Y_3Y_{13} + X_4X_6Y_4Y_6 + X_7X_8Y_7Y_8 - X_{10}X_{12}Y_{10}Y_{12} - X_9X_{14}Y_9Y_{14} + X_{11}X_{16}Y_{11}Y_{16}\big),$$
$$p_{6,1} = \frac{2\vartheta_1}{\vartheta_6}\big(X_1X_6Y_1Y_6 - X_2X_{13}Y_2Y_{13} - X_3X_{15}Y_3Y_{15} + X_4X_5Y_4Y_5 + X_7X_{16}Y_7Y_{16} + X_8X_{11}Y_8Y_{11} - X_9X_{10}Y_9Y_{10} - X_{12}X_{14}Y_{12}Y_{14}\big),$$
$$p_{7,1} = \frac{2\vartheta_1}{\vartheta_7}\big(X_1X_7Y_1Y_7 - X_2X_{12}Y_2Y_{12} + X_3X_9Y_3Y_9 - X_4X_{11}Y_4Y_{11} + X_5X_8Y_5Y_8 - X_{10}X_{15}Y_{10}Y_{15} - X_6X_{16}Y_6Y_{16} + X_{13}X_{14}Y_{13}Y_{14}\big),$$
$$p_{8,1} = \frac{2\vartheta_1}{\vartheta_8}\big(X_1X_8Y_1Y_8 + X_2X_{10}Y_2Y_{10} - X_3X_{14}Y_3Y_{14} - X_4X_{16}Y_4Y_{16} + X_5X_7Y_5Y_7 - X_6X_{11}Y_6Y_{11} - X_9X_{13}Y_9Y_{13} + X_{12}X_{15}Y_{12}Y_{15}\big),$$
$$p_{9,1} = \frac{2\vartheta_1}{\vartheta_9}\big(X_1X_9Y_1Y_9 - X_2X_{11}Y_2Y_{11} + X_3X_7Y_3Y_7 - X_4X_{12}Y_4Y_{12} + X_5X_{14}Y_5Y_{14} - X_6X_{10}Y_6Y_{10} + X_8X_{13}Y_8Y_{13} - X_{15}X_{16}Y_{15}Y_{16}\big),$$
$$p_{10,1} = \frac{2\vartheta_1}{\vartheta_{10}}\big(X_1X_{10}Y_1Y_{10} + X_2X_8Y_2Y_8 - X_3X_{16}Y_3Y_{16} - X_4X_{14}Y_4Y_{14} + X_5X_{12}Y_5Y_{12} - X_6X_9Y_6Y_9 + X_7X_{15}Y_7Y_{15} - X_{11}X_{13}Y_{11}Y_{13}\big),$$
$$p_{11,1} = \frac{2\vartheta_1^2}{\vartheta_8\vartheta_6}\big(X_1X_{11}Y_6Y_8 + X_2X_9Y_{10}Y_{13} + X_3X_{12}Y_{14}Y_{15} + X_4X_7Y_5Y_{16} + X_5X_{16}Y_4Y_7 + X_6X_8Y_1Y_{11} + X_{10}X_{13}Y_2Y_9 + X_{14}X_{15}Y_3Y_{12}\big),$$
$$p_{12,1} = \frac{2\vartheta_1^2}{\vartheta_7\vartheta_2}\big(X_1X_{12}Y_2Y_7 + X_2X_7Y_1Y_{12} + X_3X_{11}Y_4Y_9 + X_4X_9Y_3Y_{11} + X_5X_{10}Y_8Y_{15} + X_6X_{14}Y_{13}Y_{16} + X_8X_{15}Y_5Y_{10} + X_{13}X_{16}Y_6Y_{14}\big),$$
$$p_{13,1} = \frac{2\vartheta_1^2}{\vartheta_6\vartheta_2}\big(X_1X_{13}Y_2Y_6 + X_2X_6Y_1Y_{13} + X_3X_5Y_4Y_{15} + X_4X_{15}Y_3Y_5 - X_7X_{14}Y_{12}Y_{16} - X_8X_9Y_{10}Y_{11} - X_{10}X_{11}Y_8Y_9 - X_{12}X_{16}Y_7Y_{14}\big),$$
$$p_{14,1} = \frac{2\vartheta_1^2}{\vartheta_5\vartheta_9}\big(X_1X_{14}Y_5Y_9 - X_2X_{16}Y_{11}Y_{15} + X_3X_8Y_7Y_{13} - X_4X_{10}Y_6Y_{12} + X_5X_9Y_1Y_{14} - X_6X_{12}Y_4Y_{10} + X_7X_{13}Y_8Y_3 - X_{11}X_{15}Y_2Y_{16}\big),$$
$$p_{15,1} = \frac{2\vartheta_1^2}{\vartheta_5\vartheta_2}\big(X_1X_{15}Y_2Y_5 + X_2X_5Y_1Y_{15} + X_3X_6Y_4Y_{13} + X_4X_{13}Y_3Y_6 + X_7X_{10}Y_8Y_{12} + X_8X_{12}Y_7Y_{10} + X_9X_{16}Y_{11}Y_{14} + X_{11}X_{14}Y_9Y_{16}\big),$$
$$p_{16,1} = \frac{2\vartheta_1^2}{\vartheta_3\vartheta_{10}}\big(X_1X_{16}Y_3Y_{10} - X_2X_{14}Y_4Y_8 + X_3X_{10}Y_1Y_{16} - X_4X_8Y_2Y_{14} - X_5X_{11}Y_{12}Y_{13} + X_6X_7Y_9Y_{15} + X_9X_{15}Y_6Y_7 - X_{12}X_{13}Y_5Y_{11}\big).$$

Bibliographie

[AC11] Christophe Arene and Romain Cosset. Construction of a k-complete addition on an abelian surface over a non binary finite field. *Proceedings of AGCT'12 and Geocrypt'2*, 2011.

[AG11] Omran Ahmadi and Robert Granger. On isogeny classes of Edwards curves over finite fields. *ArXiv e-prints*, March 2011.

[AKR11] Christophe Arene, David Kohel, and Christophe Ritzenthaler. Complete addition laws on abelian varieties. *Submitted to LMS Journal of Computation and Mathematics*, 2011.

[ALNR10] Christophe Arene, Tanja Lange, Michael Naehrig, and Christophe Ritzenthaler. Faster computation of the Tate pairing. *To appear in Journal of Number Theory, Special Issue : Elliptic Curve Cryptography*, 2010.

[AM93] Arthur O. L. Atkin and François Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203) :29–68, 1993.

[Are08] Christophe Arene. Étude d'un nouveau modèle pour les courbes elliptiques. Master's thesis, Institut de Mathématiques de Luminy, Université de la Méditerranée, Marseille, 2008.

[Bai62] Walter L. Baily, Jr. On the theory of θ-functions, the moduli of abelian varieties, and the moduli of curves. *Ann. of Math. (2)*, 75 :342–381, 1962.

[BBEL08] Juliana Belding, Reinier Bröker, Andreas Enge, and Kristin Lauter. Computing Hilbert class polynomials. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 282–295. Springer, Berlin, 2008.

[BBJ+08] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted Edwards curves. In *Africacrypt*, pages 389–405, 2008. http ://cr.yp.to/papers.html#twisted.

[BF01] Dan Boneh and Matthew Franklin. Identity-based encryption from the Weil pairing. In *Advances in cryptology—CRYPTO 2001 (Santa Barbara, CA)*, volume 2139 of *Lecture Notes in Comput. Sci.*, pages 213–229. Springer, Berlin, 2001.

[BF03] Dan Boneh and Matthew Franklin. Identity-based encryption from the Weil pairing. *SIAM J. Comput.*, 32(3) :586–615, 2003.

[BK98] Ramachandran Balasubramanian and Neal Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. *J. Cryptology*, 11(2) :141–145, 1998.

[BKL11] Daniel J. Bernstein, David Kohel, and Tanja Lange, 2011. preprint.

[BL] Daniel J. Bernstein and Tanja Lange. *Explicit-Formulas Database.* http ://www.hyperelliptic.org/EFD/.

[BL95] Wieb Bosma and Hendrik W. jr. Lenstra. Complete systems of two addition laws for elliptic curves. *J. Number Theory*, 53(2) :229–240, 1995.

[BL04] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004.

[BL07a] Daniel J. Bernstein and Tanja Lange. Faster addition and doubling on elliptic curves. In *Advances in cryptology—ASIACRYPT 2007*, volume 4833 of *Lecture Notes in Comput. Sci.*, pages 29–50. Springer, Berlin, 2007.

[BL07b] Daniel J. Bernstein and Tanja Lange. Inverted Edwards coordinates. Boztaş, Serdar (ed.) et al., Applied algebra, algebraic algorithms and error-correcting codes. 17th international symposium, AAECC-17, Bangalore, India, December 16–20, 2007. Proceedings. Berlin : Springer. Lecture Notes in Computer Science 4851, 20-27 (2007), 2007.

[BLF08] Daniel J. Bernstein, Tanja Lange, and Reza R. Farashahi. Binary Edwards curves. In *CHES '08 : Proceeding sof the 10th international workshop on Cryptographic Hardware and Embedded Systems*, pages 244–265, Berlin, Heidelberg, 2008. Springer-Verlag.

[BLS01] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the Weil pairing. In *Advances in cryptology—ASIACRYPT 2001 (Gold Coast)*, volume 2248 of *Lecture Notes in Comput. Sci.*, pages 514–532. Springer, Berlin, 2001.

[BLS04a] Paulo S.L.M. Barreto, Ben Lynn, and Michael Scott. Efficient implementation of pairing-based cryptosystems. *J. Cryptology*, 17 :321–334, 2004.

[BLS04b] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the Weil pairing. *J. Cryptology*, 17(4) :297–319, 2004.

[Brö08] Reinier Bröker. A p-adic algorithm to compute the Hilbert class polynomial. *Math. Comp.*, 77(264) :2417–2435, 2008.

[BSS05] Ian F. (ed.) Blake, Gadiel (ed.) Seroussi, and Nigel P. (ed.) Smart. *Advances in Elliptic Curve Cryptography*. London Mathematical Society Lecture Note Series 317. Cambridge : Cambridge University Press. xvi, 281 p., 2005.

[CDF+11] R. Cheung, S. Duquesne, J. Fan, N. Guillermin, I. Verbauwhede, and G. Yao. FPGA implementation of pairings using residue number system and lazy reduction, 2011. In *CHES, Lecture Notes in Computer Science*, **6917**, pages 421–441.

[CFA+06] Henri Cohen, Gerhard Frey, Robero M. Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Discrete Mathematics and its Applications. Boca Raton, FL : Chapman & Hall/CRC. xxxiv, 808 p., 2006.

[CHB+09] Craig Costello, Huseyin Hisil, Colin Boyd, Juan Gonzalez Nieto, and Kenneth Koon-Ho Wong. Faster pairings on special Weierstrass curves. Shacham, Hovav (ed.) et al., Pairing-based cryptography – Pairing 2009. Third international conference Palo Alto, CA, USA, August 12–14, 2009. Proceedings. Berlin : Springer. Lecture Notes in Computer Science 5671, 89-101 (2009), 2009.

[CN05] Zhaohui Cheng and Manos Nistazakis. Implementing pairing-based cryptosystems. 3rd International Workshop on Wireless Security Technologies IWWST-2005, 2005.

[Cos11] Romain Cosset. *Applications des fonctions thêta à la cryptographie sur courbes hyperelliptiques*. PhD thesis, Université Henri-Poincarré, Nancy 1, France, 2011.

[CR11] Romain Cosset and Damien Robert. Computing (ℓ, ℓ)-isogenies in polynomial time on Jacobians of genus 2 curves. Cryptology ePrint Archive, Report 2011/143, 2011. `http://eprint.iacr.org/2011/143`.

[CSB05] Sanjit Chatterjee, Palash Sarkar, and Rana Barua. Efficient computation of Tate pairing in projective coordinate over general characteristic fields. In *Information security and cryptology—ICISC 2004*, volume 3506 of *Lecture Notes in Comput. Sci.*, pages 168–181. Springer, Berlin, 2005.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, IT-22(6) :644–654, 1976.

[Dia10] Oumar Diao. *Quelques aspects de l'arithmétique des courbes hyperelliptiques de genre* 2. PhD thesis, Université de Rennes 1, France, 2010.

[DT08] Claus Diem and Emmanuel Thomé. Index calculus in class groups of non-hyperelliptic curves of genus three. *J. Cryptology*, 21(4) :593–611, 2008.

[Edw07] Harold M. Edwards. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, 44 :393–422, 2007. http ://www.ams.org/bull/2007-44-03/S0273-0979-07-01153-6/home.html.

[ElG85] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Advances in cryptology (Santa Barbara, Calif., 1984)*, volume 196 of *Lecture Notes in Comput. Sci.*, pages 10–18. Springer, Berlin, 1985.

[Eng09] Andreas Enge. The complexity of class polynomial computation via floating point approximations. *Math. Comp.*, 78(266) :1089–1107, 2009.

[ES10] Andreas Enge and Andrew V. Sutherland. Class invariants by the CRT method. Hanrot, Guillaume (ed.) et al., Algorithmic number theory. 9th international symposium, ANTS-IX, Nancy, France, July 19–23, 2010. Proceedings. Berlin : Springer. Lecture Notes in Computer Science 6197, 142-156 (2010), 2010.

[FK80] Hershel Farkas and Irwin Kra. *Riemann Surfaces*, volume 71 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1980.

[FOR08] Stéphane Flon, Roger Oyono, and Christophe Ritzenthaler. Fast addition on non-hyperelliptic genus 3 curves. In *Algebraic geometry and its applications*, volume 5 of *Ser. Number Theory Appl.*, pages 1–28. World Sci. Publ., Hackensack, NJ, 2008.

[FR94] Gerhard Frey and Hans-Georg Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, 62(206) :865–874, 1994.

[FST06] David Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. Cryptology ePrint Archive, Report 2006/372, 2006. update 2008, `http://eprint.iacr.org/`.

[Gau07] Pierrick Gaudry. Fast genus 2 arithmetic based on theta functions. *J. Math. Cryptol.*, 1(3) :243–265, 2007.

[GH94] P. Griffiths and J. Harris. *Principles of algebraic geometry*. Wiley Classics Library. John Wiley & Sons Inc., New York, 1994. Reprint of the 1978 original.

[GMV07] Steven D. Galbraith, James F. McKee, and P. C. Valença. Ordinary abelian varieties having small embedding degree. *Finite Fields Appl.*, 13(4) :800–814, 2007.

[Har77] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[HS00] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[HWCD08] Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson. Twisted Edwards curves revisited. In *Advances in cryptology—ASIACRYPT 2008*, volume 5350 of *Lecture Notes in Comput. Sci.*, pages 326–343. Springer, Berlin, 2008.

[IJ08] Sorina Ionica and Antoine Joux. Another approach to pairing computation in Edwards coordinates. In *Progress in cryptology—INDOCRYPT 2008*, volume 5365 of *Lecture Notes in Comput. Sci.*, pages 400–413. Springer, Berlin, 2008.

[Jou00] Antoine Joux. A one round protocol for tripartite Diffie-Hellman. In *Algorithmic number theory (Leiden, 2000)*, volume 1838 of *Lecture Notes in Comput. Sci.*, pages 385–393. Springer, Berlin, 2000.

[Jou04] Antoine Joux. A one round protocol for tripartite Diffie-Hellman. *J. Cryptology*, 17(4) :263–276, 2004.

[JTV10] Marc Joye, Mehdi Tibouchi, and Damien Vergnaud. Huff's model for elliptic curves. Hanrot, Guillaume (ed.) et al., Algorithmic number theory. 9th international symposium, ANTS-IX, Nancy, France, July 19–23, 2010. Proceedings. Berlin : Springer. Lecture Notes in Computer Science 6197, 234-250 (2010), 2010.

[Kem70] George R. Kempf. Appendix of [Mum70], pp. 95–100, 1970.

[Kob87] Neal Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177) :203–209, 1987.

[Koh11] David Kohel. Addition law structure of elliptic curves. *Journal of Number Theory*, 2011.

[Lan83a] S. Lang. *Fundamentals of Diophantine geometry*. Springer-Verlag, New York, 1983.

[Lan83b] Serge Lang. *Abelian varieties*. Springer-Verlag, New York, 1983. Reprint of the 1959 original.

[Lan87] Serge Lang. *Elliptic Functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.

[Lan94] Serge Lang. *Algebraic Number Theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[Lan05] Tanja Lange. Formulae for arithmetic on genus 2 hyperelliptic curves. *Appl. Algebra Engrg. Comm. Comput.*, 15(5) :295–328, 2005.

[LR85] Herbert Lange and Wolfgang Ruppert. Complete systems of addition laws on abelian varieties. *Invent. Math.*, 79 :603–610, 1985.

[LR87] Herbert Lange and Wolfgang Ruppert. Addition laws on elliptic curves in arbitrary characteristics. *J. Algebra*, 107(1) :106–116, 1987.

[LR10] David Lubicz and Damien Robert. Efficient pairing computation with theta functions. Hanrot, Guillaume (ed.) et al., Algorithmic number theory. 9th international symposium, ANTS-IX, Nancy, France, July 19–23, 2010. Proceedings. Berlin : Springer. Lecture Notes in Computer Science 6197, 251-269 (2010), 2010.

[Mes91] Jean-François Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry*, volume 94 of *Prog. Math.*, pages 313–334, Boston, 1991. Birkäuser.

[Mil86a] Victor S. Miller. Use of elliptic curves in cryptography. In *Advances in cryptology—CRYPTO '85 (Santa Barbara, Calif., 1985)*, volume 218 of *Lecture Notes in Comput. Sci.*, pages 417–426. Springer, Berlin, 1986.

[Mil86b] James S. Milne. Abelian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 103–150. Springer, New York, 1986.

[Mil04] Victor S. Miller. The Weil pairing, and its efficient calculation. *Journal of Cryptology*, 17 :235–261, 2004.

[MNT01] Atsuko Miyaji, Masaki Nakabayashi, and Shunzou Takano. New explicit conditions of elliptic curve traces for FR-reduction. IEICE Trans. Fundamentals, E84 A (2001), pp. 1234–1243, 2001.

[Mor09] François Morain. Edwards curves and CM curves, 2009. http ://hal.inria.fr/inria-00375427/PDF/edwards.pdf.

[MOV93] Alfred J. Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inform. Theory*, 39(5) :1639–1646, 1993.

[Mum66] David Mumford. On the equations defining abelian varieties. I. *Invent. Math.*, 1 :287–354, 1966.

[Mum67a] David Mumford. On the equations defining abelian varieties. II. *Invent. Math.*, 3 :75–135, 1967.

[Mum67b] David Mumford. On the equations defining abelian varieties. III. *Invent. Math.*, 3 :215–244, 1967.

[Mum70] David Mumford. Varieties defined by quadratic equations. In *Questions on Algebraic Varieties (C.I.M.E., III Ciclo, Varenna, 1969)*, pages 29–100. Edizioni Cremonese, Rome, 1970.

[Mum75a] David Mumford. *Curves and their Jacobians*. The University of Michigan Press, Ann Arbor, Mich., 1975. Appendix of [Mum75b], pp. 225–291.

[Mum75b] David Mumford. The red book of varieties and schemes, 1975.

[Mum83] David Mumford. *Tata lectures on theta. I*, volume 28 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 1983. With the assistance of C. Musili, M. Nori, E. Previato and M. Stillman.

[Mum84] David Mumford. *Tata lectures on theta. II*, volume 43 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 1984. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura.

[Mum85] David Mumford. *Abelian varieties*. Studies in Mathematics, 5. Tata Institute of Fundamental Research, Bombay. Oxford etc. : Oxford University Press. XII, 279 p., 1985. With appendices by C. P. Ramanujam and Yuri Manin. 2nd ed. Reprint.

[Nae09] Michael Naehrig. *Constructive and Computational Aspects of Cryptographic Pairings*. PhD thesis, Technische Universiteit Eindhoven, 2009.

[Rob10] Damien Robert. *Theta Functions and Cryptographic Applications*. PhD thesis, Université Henri Poincaré, Nancy 1, 2010.

[RS09] Karl Rubin and Alice Silverberg. Point counting on reductions of CM elliptic curves. *J. Number Theory*, 129(12) :2903–2923, 2009.

[RS10] Karl Rubin and Alice Silverberg. Choosing the correct elliptic curve in the CM method. *Math. Comp.*, 79(269) :545–561, 2010.

[Sek77] Tsutomu Sekiguchi. On projective normality of Abelian varieties. II. *J. Math. Soc. Japan*, 29(4) :709–727, 1977.

[Sha85] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Advances in cryptology (Santa Barbara, Calif., 1984)*, volume 196 of *Lecture Notes in Comput. Sci.*, pages 47–53. Springer, Berlin, 1985.

[Sha94a] Igor R. Shafarevich. *Basic algebraic geometry 1.* Springer-Verlag, Berlin, second edition, 1994. Varieties in projective space, Translated from the 1988 Russian edition and with notes by Miles Reid.

[Sha94b] Igor R. Shafarevich. *Basic algebraic geometry 2.* Springer-Verlag, Berlin, second edition, 1994. Schemes and complex manifolds, Translated from the 1988 Russian edition by Miles Reid.

[Sil92] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[Sil94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sma10] Nigel Smart. ECRYPT II Yearly report on algorithms and keysizes (2009-2010). ECRYPT II - European Network of Excellence in Cryptology II, ICT-2007-216676, published as deliverable D.SPA.13, 2010. http ://www.ecrypt.eu.org/documents/D.SPA.13.pdf.

[Smi09] Benjamin Smith. Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves. *J. Cryptology*, 22(4) :505–529, 2009.

[Sut10] Andrew V. Sutherland. Accelerating the CM method. arXiv :1009.1082v1, 2010.

[Sut11] Andrew V. Sutherland. Computing Hilbert class polynomials with the Chinese remainder theorem. *Math. Comp.*, 80(273) :501–538, 2011.

[Tho70] J. Thomae. Beitrag zur Bestimmung von $\vartheta\,(0, 0, \ldots 0)$ durch die Klassbmodulb agebraischer Functionnen. *CRELLE*, 70 :201–222, 1870.

[TV91] M.A. Tsfasman and S.G. Vlăduţ. *Algebraic-geometric codes. Transl. from the Russian.* Mathematics and Its Applications, Soviet Series, 58. Dordrecht etc. : Kluwer Academic Publishers. xxiv, 667 p. , 1991.

[vW98] Paul van Wamelen. Equations for the Jacobian of a hyperelliptic curve. *Trans. Am. Math. Soc.*, 350(8) :3083–3106, 1998.

Notations

$\Bbbk$, corps parfait, 13
$\overline{\Bbbk}$, clôture algébrique de $\Bbbk$, 13
$\mathrm{Gal}\left(\overline{\Bbbk}/\Bbbk\right)$, groupe de Galois absolu, 13
$\mathrm{Div}(C)$, groupe des diviseurs sur C, 13
$\mathrm{Supp}(D)$, support d'un diviseur D, 13
$\deg(D)$, degré d'un diviseur, 13
$\mathrm{Div}^0(C)$, groupe des diviseurs de degré 0 sur C, 13
$\mathrm{Div}_\Bbbk(C)$, groupe des diviseurs $\Bbbk$-rationnels sur C, 13
$\mathrm{Div}^0_\Bbbk(C)$, groupe des diviseurs $\Bbbk$-rationnels de degré 0 sur C, 13
$\mathrm{div}(f)$, diviseur associé à la fonction f, 14
$\mathrm{Princ}(C)$, groupe des diviseurs principaux, 14
$\sim$, relation d'équivalence linéaire sur $\mathrm{Div}(C)$, 14
$\mathrm{Pic}(C)$, groupe de Picard de C, 14
$\mathrm{Pic}^0(C)$, jacobienne de C, 14
κ_C, diviseur canonique de C, 14
$L(D)$, espace de Riemann-Roch, 14
$l(D)$, dimension de $L(D)$, 14
g, genre d'une courbe, 14
E, courbe elliptique, 15
O, élément neutre d'une courbe elliptique, 15
$\Delta(E)$, discriminant d'une courbe elliptique, 15
$j(E)$, j-invariant d'une courbe elliptique, 15
$\overline{P}$, symétrique du point P, 16
Δ, diagonale, 16
∇, antidiagonale, 16
$\sim$, relation d'isogénie (courbes elliptiques), 17
$\mathrm{End}(E)$, anneau d'endomorphismes de E, 17
$[m]$, multiplication par m, 18
$E[m]$, sous-groupe de m-torsion, 18
$\mathbb{F}_q$, corps fini à q éléments, 18
$\widehat{\phi}$, isogénie duale de ϕ, 18
t, trace de l'endomorphisme de Frobenius, 19
$\mathbf{m}$, multiplication dans le corps de base, 19
$\mathbf{s}$, élévation au carré dans le corps de base, 19
$\mathbf{m_\alpha}$, multiplication par un paramètre α, 19
ϑ, fonction thêta de Riemann, 20
$\vartheta_{\varepsilon\,\varepsilon'}$, fonctions thêta avec caractéristique, 20
$E_{1,d}$, courbe d'Edwards, 23
$E_{a,d}$, courbe d'Edwards tordue, 28
$J_{a,b,c}$, modèle de Jacobi, 29
C_{P_1,P_2}, conique passant par $P_1, P_2, O', \Omega_1, \Omega_2$, 30
E_{B,d_1,d_2}, courbe d'Edwards binaire, 34
k, degré de plongement, 36
$\mathbf{M}$, 38
$\mathbf{S}$, 38
$\mathbb{K}$, corps quadratique imaginaire, 44
$\mathcal{O}_\mathbb{K}$, anneau des entiers du corps $\mathbb{K}$, 44
$\mathrm{Ell}(\mathcal{O}_\mathbb{K})$, ensemble des classes d'isomorphisme des courbes elliptiques ayant multiplication complexe par $\mathcal{O}_\mathbb{K}$, 44
$H_\mathbb{K}(X)$, polynôme de classes de Hilbert, 44
D, discriminant, 44
ρ, valeur-ρ, 47
A, variété abélienne, 52
μ, morphisme de groupe, 52
$L(D)$, espace de Riemann-Roch, 54
$l(D)$, dimension de $L(D)$, 54
$|D|$, système linéaire complet, 54
$\varphi_{L(D)} : X \to \mathbb{P}^{l(D)-1}$, 54
$g_{i,j}$, fonctions de transition, 55
$H^0(X, \mathcal{L})$, 55
$\mathcal{M}_{m,n}$, 56
$\mathcal{M}$, 56
t_x, translation par x, 57
$\mathrm{Pic}(A)$, groupe de Picard, 57
$\mathrm{Pic}^0(A)$, 57
$\phi_\mathcal{L} : A \to \mathrm{Pic}^0(A)$, 57
$K(\mathcal{L})$, noyau de $\phi_\mathcal{L}$, 57
$K(\mathcal{L})_0$, composante connexe neutre de $K(\mathcal{L})$, 57
λ, polarisation, 58
$\chi(\mathcal{L})$, caractéristique d'Euler, 59
g, dimension de A, 59
$i_\mathcal{L}$, indice de $\mathcal{L}$, 59
δ, morphisme de différence, 60
$\overline{\ }$, involution hyperelliptique, 61
C, courbe de genre 2, 61
$\infty = (0:1:0)$, 61
P_∞, diviseur $\Bbbk$-rationnel de degré 1 sur C, 61
S^kC, $k^{\text{ième}}$ puissance symétrique de C, 62
$\phi^{(k)} : S^kC \to \mathrm{Jac}_C$, 62
ϑ, fonction thêta de Riemann, 63
$\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$, fonction thêta avec caractéristique, 63
$\mathcal{K}$, constante de Riemann, 64
Ω, matrice des périodes de C, 64
η_S, 65
$A_i = (a_i, 0)$, points de Weierstraß de C, 65
$\mathcal{U} = \{1, 3, 5\}$, 65
$\circ$, différence symétrique, 65
ι, plongement projectif de A, 67
$\mathfrak{p}_j$, lois d'addition, 76
O_J, élément neutre de Jac_C, 77

Index

Résumé

Les principaux objets étudiés dans cette thèse sont les équations décrivant le morphisme de groupe sur une variété abélienne, plongée dans un espace projectif, et leurs applications en cryptographie. Notons g sa dimension et $\Bbbk$ son corps de définition. Ce mémoire est composé de deux parties. La première porte sur l'étude des courbes d'Edwards, un modèle pour les courbes elliptiques possédant un sous-groupe de points $\Bbbk$-rationnels cyclique d'ordre 4, connues en cryptographie pour l'efficacité de leur loi d'addition et la possibilité qu'elle soit définie pour toute paire de points $\Bbbk$-rationnels (loi d'addition $\Bbbk$-complète). Nous en donnons une interprétation géométrique et en déduisons des formules explicites pour le calcul du couplage de Tate réduit sur courbes d'Edwards tordues, dont l'efficacité rivalise avec les modèles elliptiques couramment utilisés. Cette partie se conclut par la génération, spécifique au calcul de couplages, de courbes d'Edwards dont les tailles correspondent aux standards cryptographiques actuellement en vigueur. Dans la seconde partie nous nous intéressons à la notion de complétude introduite ci-dessus. Cette propriété est cryptographiquement importante car elle permet d'éviter des attaques physiques, comme les attaques par canaux cachés, sur des cryptosystèmes basés sur les courbes elliptiques ou hyperelliptiques. Un précédent travail de Lange et Ruppert, basé sur la cohomologie des fibrés en droite, permet une approche théorique des lois d'addition. Nous présentons trois résultats importants : tout d'abord nous généralisons un résultat de Bosma et Lenstra en démontrant que le morphisme de groupe ne peut être décrit par strictement moins de $g+1$ lois d'addition sur la clôture algébrique de $\Bbbk$. Ensuite nous démontrons que si le groupe de Galois absolu de $\Bbbk$ est infini, alors toute variété abélienne peut être plongée dans un espace projectif de manière à ce qu'il existe une loi d'addition $\Bbbk$-complète. De plus, l'utilisation des variétés abéliennes nous limitant à celles de dimension un ou deux, nous démontrons qu'une telle loi existe pour leur plongement projectif usuel. Finalement, nous développons un algorithme, basé sur la théorie des fonctions thêta, calculant celle-ci dans $\mathbb{P}^{15}$ sur la jacobienne d'une courbe de genre deux donnée par sa forme de Rosenhain. Il est désormais intégré au package AVIsogenies de Magma.

Mots clés

Courbes d'Edwards tordues, courbe elliptique, loi d'addition $\Bbbk$-complète, couplage de Tate réduit, formules explicites, fibré en droite, plongement projectif, jacobienne d'une courbe de genre 2, fonctions thêta, thêta constantes.

Abstract

The main objects we study in this PhD thesis are the equations describing the group morphism on an abelian variety, embedded in a projective space, and their applications in cryptograhy. We denote by g its dimension and $\Bbbk$ its field of definition. This thesis is built in two parts. The first one is concerned by the study of Edwards curves, a model for elliptic curves having a cyclic subgroup of $\Bbbk$-rational points of order 4, known in cryptography for the efficiency of their addition law and the fact that it can be defined for any couple of $\Bbbk$-rational points ($\Bbbk$-complete addition law). We give the corresponding geometric interpretation and deduce explicit formulae to calculate the reduced Tate pairing on twisted Edwards curves, whose efficiency compete with currently used elliptic models. The part ends with the generation, specific to pairing computation, of Edwards curves with today's cryptographic standard sizes. In the second part, we are interested in the notion of completeness introduced above. This property is cryptographically significant, indeed it permits to avoid physical attacks as side channel attacks, on elliptic – or hyperelliptic – curves cryptosystems. A preceeding work of Lange and Ruppert, based on cohomology of line bundles, brings a theoretic approach of addition laws. We present three important results: first of all we generalize a result of Bosma and Lenstra by proving that the group morphism can not be described by less than $g+1$ addition laws on the algebraic closure of $\Bbbk$. Next, we prove that if the absolute Galois group of $\Bbbk$ is infinite, then any abelian variety can be projectively embedded together with a $\Bbbk$-complete addition law. Moreover, a cryptographic use of abelian varieties restricting us to the dimension one and two cases, we prove that such a law exists for their classical projective embedding. Finally, we develop an algorithm, based on the theory of theta functions, computing this addition law in $\mathbb{P}^{15}$ on the Jacobian of a genus two curve given in Rosenhain form. It is now included in AVIsogenies, a Magma package.

Keywords

Twisted Edwards curves, elliptic curve, $\Bbbk$-complete addition law, reduced Tate pairing, explicite formulae, line bundle, projective embedding, Jacobian of a genus 2 curve, theta functions, theta constants.