# Tours de courbes de Shimura

Christophe Levrat

M2 Algèbre Appliquée

Université Paris-Saclay,
Université de Versailles Saint-Quentin

*Encadrant*
Matthieu Rambaud

*Professeur référent*
Luca De Feo

Stage effectué à l'INRIA Saclay au sein de l'équipe GRACE du 1er avril au 31 juillet 2018

Mémoire soumis le 18 septembre 2018

# Table des matières

# Introduction

Les courbes modulaires sont connues en théorie des codes depuis les travaux de Gekeler, Ihara et Tsfasman-Vlăduţ-Zink [TVT82], qui ont montré qu'elles permettaient de dépasser la borne de Gilbert-Varshamov. Construire ces codes records de façon explicite nécessite de connaître les équations de ces courbes sur les complexes, puis de les réduire sur les corps finis.

Garcia et Stichtenoth ont été les premiers à découvrir une famille de courbes modulaires (ce fait ayant été prouvé a posteriori par Elkies) avec une formule récursive pour calculer leurs équations. Elkies [Elk97] a ensuite démontré que cette propriété de récursivité est un fait général. En résumé, si $\Gamma_0(N^2) \subset \Gamma_0(N)$ sont deux sous groupes discrets de $\mathsf{PSL}_2(\mathbb{R})$ donnant lieu à des courbes modulaires $\mathcal{X}_0(N^2)$ et $\mathcal{X}_0(N)$, alors la courbe modulaire suivante $\mathcal{X}_0(N^3)$ s'obtient à partir de la donnée du revêtement canonique $f_2 : \mathcal{X}_0(N^2) \to \mathcal{X}_0(N)$ (ainsi que d'involutions, dites d'Atkin-Lehner, $w_1$ et $w_2$ de $\mathcal{X}_0(N)$ et $\mathcal{X}_0(N^2)$) à l'aide du produit fibré suivant :

$$\begin{array}{ccc} \mathcal{X}_0(N^3) & \longrightarrow & \mathcal{X}_0(N^2) \\ \downarrow & & \downarrow{\scriptstyle f_2} \\ \mathcal{X}_0(N^2) & \xrightarrow{w_1 \circ f_2 \circ w_2} & \mathcal{X}_0(N) \end{array}$$

On voit donc qu'un calcul de revêtement permet d'obtenir toute une famille de courbes. Le stage fait suite à la recherche récente sur les calculs de revêtements de courbes modulaires dites *de Shimura*, qui sont en général uniformisées par un groupe $\Gamma$ *cocompact*. Jusqu'à maintenant, les seules méthodes de revêtement détaillées dans la littérature étaient au dessus de courbes de genre 0 (avec notamment l'accent sur les revêtements de Belyi).

La première partie du stage (§2) consistait à calculer un exemple de revêtement de courbe de Shimura de genre supérieur. Il a donc fallu d'abord étudier quelques résultats essentiels de la théorie des courbes algébriques et de leurs revêtements (§1). La base du revêtement est la courbe de genre 1 sur $\mathbb{Q}(\sqrt{2})$ avec le label e3d8D9 dans [Sij13] (qui est remarquable car son corps des modules est égal à $\mathbb{Q}$ mais elle ne descend pas sur $\mathbb{Q}$). La théorie [Voi09c] prédit que le revêtement le plus "petit" est de genre 2, de degré 3 et ramifié exactement au dessus d'un point triple. Il peut exister jusqu'à trois revêtements distincts avec ces propriétés, on souhaite donc tous les calculer.

La deuxième partie du stage (§4) s'inscrit dans l'objectif de recherche consistant à calculer le revêtement de degré 27 et de genre 10 au dessus de la courbe elliptique $\mathcal{X}_0(3)$, identifiée comme 147.c1 dans LMFDB (le revêtement de $\mathbb{P}^1$ de degré 28 par cette dernière ayant fait l'objet de [Elk06]). Des éléments de la théorie des courbes de Shimura nécessaires à la compréhension de cette partie sont présentés en §3. Un objectif plus atteignable est de calculer le quotient de la courbe $\mathcal{X}_0(9)$ cherchée par l'involution d'Atkin-Lehner ; on calcule ce quotient $\mathcal{X}_0(9)^\star$, qui est de genre 2, à partir de la donnée du groupe $\Gamma_0(9)^\star$ qui l'uniformise. On pourra ensuite déterminer $\mathcal{X}_0(9)$ comme revêtement de degré 2 de $\mathcal{X}_0(9)^\star$. Le calcul de $\mathcal{X}_0(9)^\star$ peut en principe se faire à partir de développement de formes modulaires, calculés à l'aide des algorithmes [Voi09b, VW14], la difficulté consistant ensuite à trouver une équation à coefficients *rationnels*, en s'inspirant de [KMSV14].

On décompose enfin la jacobienne de cette courbe (§4.4), dans laquelle la théorie suggère qu'il existe une copie de la courbe elliptique $\mathcal{X}_0(3)$, afin de trouver des points remarquables sur $\mathcal{X}_0(9)^\star$ (notamment la ou les préimages du point à l'origine de $\mathcal{X}_0(3)$).

## Outils informatiques utilisés

### MAGMA

Tous les calculs évoqués ou détaillés dans ce travail ont été réalisés à l'aide de Magma. Magma est un logiciel de calcul formel créé et distribué par le *Computer Algebra Group* de l'université de Sydney. Il permet de travailler avec les structures algébriques usuelles, mais également de définir un grand nombre d'objets plus spécifiques qui apparaissent en géométrie algébrique et théorie des nombres : schémas, corps de nombres, algèbres de quaternions, courbes affines et projectives, courbes elliptiques et hyperelliptiques, variétés jacobiennes... Les calculs ont été effectués sur les versions 2.18-8 (pour le §4) et 2.23-6 (pour le §2) de Magma.

### LMFDB

La plupart des courbes elliptiques citées dans ce document sont identifiées par un label, que l'on peut trouver sur le site `lmfdb.org`. LMFDB est une base de données d'objets provenant de l'arithmétique et de la géométrie : corps globaux et locaux, formes modulaires, fonctions $L$, courbes elliptiques et de genre supérieur...

# 1. Préliminaires sur les courbes algébriques

On fixe pour toute cette partie un corps $k$, de clôture algébrique $\bar{k}$. Étant donnée une courbe algébrique $C$ définie sur $k$, on note $k[C]$ son anneau des coordonnées et $k(C)$ son corps des fonctions. On note $C(k)$ l'ensemble des points de la courbe définis sur $k$, et encore $C := C(\bar{k})$ l'ensemble des points géométriques, ou juste "points". On dit que $C$ est lisse si tous les points de $C(\bar{k})$ sont réguliers. On note $\mathsf{div}\, C$ le groupe des diviseurs de $C$ ; il est muni d'une action de $\mathsf{Gal}(\bar{k}/k)$, et le groupe de ses éléments fixés par cette action est noté $\mathsf{div}_k\, C$. On note $\mathsf{Pic}\, C$ le groupe des classes de diviseurs modulo les diviseurs de fonctions rationnelles, et $\mathsf{Pic}^0\, C$ le groupe des classes de diviseurs de degré 0. Pour un diviseur $D \in \mathsf{div}_k\, C$, on note $\mathscr{L}(D) := \{f \in k(C) \mid \mathsf{div}\, f + D \geqslant 0\}$ son espace de Riemann-Roch, et $\ell(D) := \dim_k \mathscr{L}(D)$. Le genre de $C$ est le maximum des $\deg D - \ell(D) + 1$, où $D \in \mathsf{div}_k\, C$.

## 1.1. Diviseurs canoniques et théorème de Riemann-Roch

### 1.1.1. Formes différentielles et diviseurs canoniques

Le théorème de Riemann-Roch fait intervenir la notion de diviseur canonique, qui est un diviseur associé à une forme différentielle. Nous allons donc d'abord étudier les formes différentielles, puis la façon de leur associer un diviseur. Les propriétés énoncées ici sont démontrées dans [Sil09] §II.4.

**Définition 1.1.1** (Différentielles)**.** Soit $C$ une courbe algébrique définie sur un corps $k$, de corps de fonctions $k(C)$. Le *module des différentielles* de $C$, noté $\Omega_k(C)$, est le $k(C)$-module libre engendré par les symboles $\mathrm{d}x,\ x \in k(C)$, quotienté par les relations suivantes :
- $\mathrm{d}(x+y) = \mathrm{d}x + \mathrm{d}y$ pour $x, y \in k(C)$
- $\mathrm{d}(xy) = x\,\mathrm{d}y + y\,\mathrm{d}x$ pour $x, y \in k(C)$
- $\mathrm{d}a = 0$ pour $a \in k$.

Ces propriétés signifient entre autre que l'application $\mathrm{d} : x \to \mathrm{d}x$ est une dérivation de $k(C)$. De plus, on en déduit que si $f(x_1, ..., x_n) \in k[C]$ alors :

$$\mathrm{d}f = \sum_i \frac{\partial f}{\partial x_i}\,\mathrm{d}x_i.$$

Afin de déterminer le diviseur d'une forme différentielle, il est nécessaire de définir son ordre en un point. La proposition suivante permet de définir cet ordre.

**Proposition 1.1.1.** Soit $P \in C$ et $t$ une uniformisante en $P$. Soit $\omega \in \Omega_k(C)$. Il existe une unique fonction $f \in k(C)$ telle que :

$$\omega = f\,\mathrm{d}t.$$

On note alors $f = \omega/\mathrm{d}t$. L'ordre $\mathsf{ord}_P(\omega/\mathrm{d}t)$ ne dépend que de $P$ et $\omega$.

**Définition 1.1.2.** L'*ordre* d'une différentielle $\omega \in \Omega_k(C)$ en $P \in C$ est l'entier :

$$\operatorname{ord}_P \omega := \operatorname{ord}_P \frac{\omega}{\mathrm{d}t}$$

où $t$ est une uniformisante en $P$.

On peut maintenant définir le diviseur d'une forme différentielle de façon analogue à celui d'une fonction rationnelle.

**Définition 1.1.3.** Soit $\omega \in \Omega_k(C)$. On définit le diviseur de $\omega$ par :

$$\operatorname{div} \omega := \sum_{P \in C} \operatorname{ord}_P \omega \cdot (P).$$

D'après 1.1.1, les formes différentielles sont toutes égales à multiplication par une fonction près. En effet, pour $\omega_1, \omega_2 \in \Omega_k(C)$ et une uniformisante $t$ en un point $P \in C$, on peut écrire $\omega_1 = f_1 \,\mathrm{d}t$ et $\omega_2 = f_2 \,\mathrm{d}t$, donc :

$$\omega_1 = \frac{f_1}{f_2} \omega_2.$$

En particulier, leurs diviseurs sont tous équivalents.

**Définition 1.1.4** (Diviseur canonique)**.** On appelle *diviseur canonique* de $C$ tout diviseur de la forme $\operatorname{div} \omega$, où $\omega \in \Omega_{\bar{k}}(C)$. On appelle *classe canonique* la classe d'un diviseur canonique dans $\operatorname{Pic} C$.

### 1.1.2. Le théorème de Riemann-Roch

Le théorème de Riemann-Roch est un outil puissant concernant la taille des espaces de Riemann-Roch des diviseurs sur une courbe. Une preuve de ce théorème utilisant la dualité de Serre se trouve par exemple dans [Mir95] §VI.3.

**Théorème 1.1.1** (Riemann-Roch)**.** Soit $C$ une courbe algébrique sur $k$ de diviseur canonique $K$ et de genre $g$, et $D \in \operatorname{div}_k C$. Alors :

$$\ell(D) - \ell(K - D) = \deg D + 1 - g.$$

En particulier, $\ell(K) = g$ et $\deg K = 2g - 2$. De plus, si $\deg D > 2g - 2$ alors $K - D$ est de degré strictement négatif, donc $\ell(K - D) = 0$ et on a :

$$\ell(D) = \deg D + 1 - g.$$

Nous nous en servirons à plusieurs reprises, par exemple pour montrer que les courbes de genre 2 sont hyperelliptiques (1.5.1) et admettent une équation d'une certaine forme (1.5.2).

## 1.2. Revêtements et formule de Riemann-Hurwitz

### 1.2.1. Revêtements

L'objet principal d'étude de ce travail est la notion de revêtement de courbes algébriques.

**Définition 1.2.1** (Morphisme fini)**.** Un morphisme $f : X \to Y$ de variétés affines est dit *fini* s'il est dominant et $k[X]$ est un $k[Y]$-module de type fini.
Un morphisme $f : X \to Y$ de variétés projectives est dit fini si tout $y \in Y$ admet un voisinage affine $V$ tel que la restriction $f_{|f^{-1}(V)} : f^{-1}(V) \to V$ est un morphisme fini de variétés affines.

**Définition 1.2.2** (Revêtement)**.** Un morphisme $f : X \to Y$ de variétés algébriques est appelé *revêtement* de degré $d$ si c'est un morphisme fini séparable de degré $d$.

Ceci correspond à la notion topologique de revêtement ramifié : tous les points de $Y$, sauf un nombre fini, ont $d$ antécédents par le morphisme $f$. Nous appliquerons cette notion à des courbes algébriques lisses, les morphismes non constants considérés seront donc tous surjectifs. La plupart du temps, les courbes seront définies sur une extension de $\mathbb{Q}$, et les morphismes seront donc également séparables.

**Définition 1.2.3** (Indice de ramification)**.** Soit $f : X \to Y$ un revêtement de courbes algébriques. Soit $P \in X$. Notons $t$ une uniformisante de $Y$ en $f(P)$. L'*indice de ramification* de $f$ en $P$ est l'entier :

$$e_f(P) := \mathrm{ord}_P\, f^\star t.$$

Lorsque $e_f(P)$ est divisible par la caractéristique de $k$, on parle de ramification *sauvage* ; sinon, de ramification *modérée*.

Un point $P \in X$ tel que $e_f(P) > 1$ est appelé point de ramification de $f$, et $Q := f(P)$ sera appelé point de branchement de $f$. Un point de branchement est donc un point qui n'a pas autant de préimages par $f$ que le degré de $f$. Plus précisément, on a le résultat suivant :

**Proposition 1.2.1.** Soit $f : X \to Y$ un revêtement de courbes algébriques. Alors pour tout $Q \in Y$, on a :

$$\sum_{P \in f^{-1}(Q)} e_f(P) = \deg f.$$

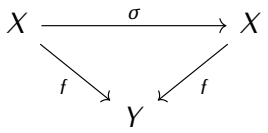
Nous serons amenés par la suite à étudier des compositions de revêtements. La formule suivante permettra alors de déterminer les indices de ramification.

**Proposition 1.2.2.** Soient $f : X \to Y$ et $g : Y \to Z$ des revêtements de courbes algébriques. Alors pour tout $P \in X$ :

$$e_{g\circ f}(P) = e_f(P) \cdot e_g(f(P)).$$

On peut également définir la notion d'automorphisme d'un revêtement : il s'agit intuitivement d'une permutation des feuillets du revêtement.

**Définition 1.2.4** (Automorphisme d'un revêtement)**.** Soit $f : X \to Y$ un revêtement de courbes algébriques. Un *automorphisme* de $f$ est un automorphisme $\sigma$ de $X$ tel que le diagramme suivant soit commutatif :



### 1.2.2. La formule de Riemann-Hurwitz

Le formule de Riemann-Hurwitz s'applique à un revêtement de courbes algébriques, et relie le genre des deux courbes, le degré du revêtement ainsi que les indices des points de ramification. Une démonstration de cette formule se trouve par exemple dans [Sil09] §II.5.

**Théorème 1.2.1** (Riemann-Hurwitz)**.** Soient $C$ et $C'$ deux courbes algébriques définies sur $k$ de genres respectifs $g$ et $g'$. Soit $\phi : C' \to C$ un revêtement de degré $d$ modérément ramifié. Alors :

$$2g' - 2 = d(2g - 2) + \sum_{P \in C} \left( e_\phi(P) - 1 \right).$$

Ce théorème a diverses utilisations selon le contexte. Par exemple, il peut permettre, étant donné un revêtement de courbes, de déterminer le genre de l'une en connaissant celui de l'autre. Nous nous en servirons en 1.4.8 pour déterminer le genre d'une courbe hyperelliptique en fonction du degré d'une équation. De plus, il peut servir à déterminer le nombre de points de ramification d'un revêtement, ce que nous ferons en 2.3.1.

## 1.3. Variétés abéliennes, jacobienne d'une courbe

### 1.3.1. Variétés abéliennes et isogénies

Un groupe algébrique est une variété algébrique qui possède une structure de groupe, où la multiplication et l'inverse sont donnés par des morphismes de variétés. Les variétés abéliennes constituent une classe importante de groupes algébriques, rencontrée fréquemment en géométrie algébrique et théorie des nombres.

**Définition 1.3.1** (Variété abélienne)**.** On appelle *variété abélienne* un groupe algébrique projectif connexe.

L'appellation "variété abélienne" est justifiée par le fait que la loi de groupe de ces variétés est toujours commutative (voir [Mil08] §1). Étant donnée une variété abélienne $A$, nous noterons $0_A$ l'élément neutre de sa loi de groupe.
Les courbes elliptiques fournissent un premier exemple de variétés abéliennes. En effet, ce sont des courbes projectives connexes munies d'une loi de groupe donnée par des formules polynomiales. Comme dans le cas des courbes elliptiques, on peut définir une notion d'isogénie entre variétés abéliennes.

**Définition 1.3.2** (Isogénie)**.** Une *isogénie* entre deux variétés abéliennes $A$ et $B$ est un morphisme de variété algébriques $f : A \to B$ à fibres finies tel que $f(0_A) = 0_B$.

On peut alors montrer que les isogénies sont automatiquement des morphismes surjectifs de groupes. Un exemple très simple d'isogénie est la multiplication par un entier $n$ :

$$[n]_A : P \longmapsto \underbrace{P + \cdots + P}_{n \text{ fois}}.$$

Son noyau, l'ensemble des points de $n$-torsion de $A$, sera noté $A[n]$. Les isogénies duales de courbes elliptiques se généralisent également aux variétés abéliennes.

**Proposition 1.3.1.** Soit $\phi : A \to B$ une isogénie de variétés abéliennes. Alors il existe une isogénie $\psi : B \to A$ de même degré que $\phi$ telle que :

$$\phi \circ \psi = [\deg \phi]_B \quad \text{et} \qquad \psi \circ \phi = [deg\, \phi]_A.$$

### 1.3.2. Jacobienne d'une courbe

Il est connu que les courbes lisses de genre 1 munies d'un point rationnel sont en bijection avec leur groupe de Picard ; c'est ainsi que l'on peut définir une structure de groupe sur la courbe, mais également munir son groupe de Picard d'une structure de variété algébrique. La notion de jacobienne d'une courbe généralise ce dernier phénomène : il s'agit d'une variété abélienne dont le groupe sous-jacent est le groupe de Picard de la courbe.

**Proposition 1.3.2.** Soit $C$ une courbe algébrique lisse sur un corps $k$, munie d'un point $k$-rationnel. Il existe une variété abélienne $J_C$, appelée jacobienne de la courbe $C$, telle que pour toute extension $\ell$ de $k$ :

$$J_C(\ell) = \mathrm{Pic}^0_\ell(C).$$

Soit $C$ une telle courbe munie d'un point $Q \in C(k)$. On définit le morphisme de variétés algébriques

$$\begin{array}{rccc} f_Q : & C & \longrightarrow & J_C \\ & P & \longmapsto & (P) - (Q). \end{array}$$

dont la restriction à $C(k)$ est définie sur $k$ (voir [Mil18] §2). La propriété universelle suivante définit alors le couple $(J_C, f_Q)$.

**Proposition 1.3.3.** Pour toute variété abélienne $A$ et tout morphisme de variétés algébriques $g : C \to A$ tel que $g(Q) = 0_A$, il existe un unique morphisme de variétés abéliennes

$$\phi : J_C \to A$$

tel que le diagramme suivant soit commutatif :

$$\begin{array}{ccc} C & \xrightarrow{g} & A \\ {\scriptstyle f_Q}\downarrow & \nearrow_{\phi} & \\ J_C & & \end{array}$$

Concrètement, la structure de variété sur $\mathrm{Pic}^0(C)$ est construite de la façon suivante (voir [Mil18] §3). Notons $g$ le genre de la courbe $C$. Le groupe symétrique $\mathfrak{S}_g$ agit sur le produit cartésien $C^g$ en permutant les facteurs. La $g$-ième puissance symétrique $C^{(g)}$ de $C$ est alors le quotient $C^g/\mathfrak{S}_g$. Si $P_0 \in C(k)$, on définit la structure de variété sur $\mathrm{Pic}^0_k(C)$ à l'aide du morphisme surjectif ([dP13]) :

$$\begin{array}{rcl} C^{(g)}(k) & \longrightarrow & Pic^0_k(C) \\ (P_1, ..., P_g) & \longmapsto & (P_1) + \cdots + (P_g) - g(P_0). \end{array}$$

En particulier, pour les courbes de genre 2, la loi de groupe de la jacobienne peut être présentée comme une addition de paires de points. De façon semblable aux courbes elliptiques, on peut la définir de façon géométrique : la somme de trois paires de points vaut 0 lorsque les six points concernés sont l'intersection de la courbe avec une cubique (voir [Smi16]).

## 1.4. Courbes hyperelliptiques

### 1.4.1. Quelques résultats essentiels

**Définition 1.4.1** (Courbe hyperelliptique)**.** Une *courbe hyperelliptique* sur un corps $k$ est une courbe lisse $C$ définie sur $k$ munie d'un revêtement double de la droite projective, c'est-à-dire un morphisme séparable : $C \to \mathbb{P}^1$ (défini sur $\bar{k}$) de degré 2.

**Proposition 1.4.1.** Soit $C \xrightarrow{\phi} \mathbb{P}^1$ une courbe hyperelliptique de genre $g$. Alors $\phi$ admet $2g+2$ points de ramification.

*Démonstration.* On applique la formule de Riemann-Hurwitz à $\phi$ :

$$2g - 2 = \deg \phi \cdot (2g(\mathbb{P}^1) - 2) + \sum_{P \in C} (e_\phi(P) - 1)$$

c'est-à-dire, comme $g(\mathbb{P}^1) = 0$ et $\deg \phi = 2$ :

$$\sum_{P \in C} (e_\phi(P) - 1) = 2g + 2$$

Comme $\phi$ est de degré 2, les points de ramification sont d'indice 2, et il y en a donc $2g + 2$. □

**Définition 1.4.2** (Points de Weierstrass)**.** Les $2g+2$ points de ramification de $\phi$ sont appelés *points de Weierstrass* de $C$.

**Proposition 1.4.2.** Soit $C \xrightarrow{\phi} \mathbb{P}^1$ une courbe hyperelliptique. Le revêtement $\phi$ admet un unique automorphisme $\iota : C \to C$.

*Démonstration.* Le revêtement $\phi$ induit une extension de corps $\phi^\star : \bar{k}(\mathbb{P}^1) \to \bar{k}(C)$ de degré 2, on a donc :

$$\#\,\mathsf{Gal}(\bar{k}(C)/\bar{k}(\mathbb{P}^1)) = 2$$

donc $\mathsf{Gal}(\bar{k}(C)/\bar{k}(\mathbb{P}^1)) = \{1, \iota\}$ où $\iota$ est d'ordre 2. Or ce groupe de Galois est exactement l'ensemble des automorphismes de $\bar{k}(C)$ fixant les éléments de $\bar{k}(x)$. L'automorphisme de $C$ correspondant à $\iota$ est donc celui que l'on cherche. □

**Définition 1.4.3** (Involution hyperelliptique)**.** L'automorphisme $\iota$ défini à la proposition précédente est une involution appelée *involution hyperelliptique*.

L'involution hyperelliptique échange donc simplement les deux feuillets du revêtement $\phi : C \to \mathbb{P}^1$.

**Proposition 1.4.3.** $C/\iota$ est de genre 0.

*Démonstration.* D'après la définition de $\iota$, les orbites sous son action sont exactement les paires de points qui ont la même image par le morphisme surjectif $\phi : C \to \mathbb{P}^1$. □

Notons bien que nous n'avons pas demandé que $\phi$ soit défini sur $k$ : ainsi, il n'y a pas nécessairement un isomorphisme défini sur $k$ entre $C/\iota$ et $\mathbb{P}^1$. De même, les équations que nous détaillerons dans la section à venir ne sont définies que sur $\bar{k}$. Nous verrons plus tard dans le cas particulier des courbes de genre 2 une condition suffisante pour obtenir une équation hyperelliptique à coefficients dans $k$.

### 1.4.2. Équations des courbes hyperelliptiques

**Proposition 1.4.4.** Une courbe hyperelliptique sur un corps $k$ admet une équation affine de la forme :

$$y^2 + h(x)y = f(x) \tag{EQ1}$$

où $h, f \in \bar{k}[x]$.

*Démonstration.* Si $\phi : C \to \mathbb{P}^1$ est le revêtement de degré 2 associé à la courbe, il définit une extension $\phi^\star : \bar{k}(\mathbb{P}^1) \to \bar{k}(C)$ de degré 2. Donc $\bar{k}(C)$ est une extension de degré 2 de $\bar{k}(x)$, et $\bar{k}(C) = \bar{k}(x, y)$ où $y$ est de degré 2 sur $\bar{k}(x)$. □

En particulier, le morphisme $\phi$ est donné explicitement par la formule :

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

On dispose également d'une formule simple pour l'involution hyperelliptique :

$$\iota(x, y) = (x, -y - h(x)).$$

En effet, il s'agit évidemment d'une involution, et elle commute à $\phi : (x, y) \to x$.
On peut encore raffiner un peu la forme de l'équation de la courbe, en contrôlant le degré de $h$ par rapport à celui de $f$. Nous donnons ici une condition supplémentaire sur les coefficients de l'équation, qui permettra de s'assurer que la complétion projective de la courbe dans un espace approprié soit régulière.

**Proposition 1.4.5.** Soit $k$ un corps de caractéristique différente de 2, et $C$ une courbe hyperelliptique sur $k$. Alors il existe $d > 0$, $f_0, ..., f_{2d}, h_0, ..., h_d \in \bar{k}$ tels que $C$ soit isomorphe à la courbe d'équation :

$$y^2 + (h_d x^d + \cdots + h_1 x + h_0)y = f_{2d}x^{2d} + \cdots + f_1 x + f_0. \tag{EQ2}$$

En outre, pour toute équation de cette forme d'une courbe hyperelliptique, l'une des deux conditions suivantes est satisfaite :
• $h_d = 0$ et ($f_{2d} \neq 0$ ou $f_{2d-1} \neq 0$)
• $h_d \neq 0$ et ($f_{2d} \neq -h_d^2/4$ ou $f_{2d-1} \neq h_d h_{d-1}/2$).

*Démonstration.* D'après 1.4.4, $C$ admet une équation affine de la forme $y^2 + h(x)y = f(x)$ avec $h, f \in \bar{k}[x]$. Notons $d = \max(\deg h, \lfloor(\deg f + 1)/2\rfloor)$. Supposons $d$ minimal pour cette propriété. Si $h_d = 0$ alors, d'après la définition de $d$, l'un des coefficients $f_{2d}$ et $f_{2d-1}$ est non nul. Si $h_d \neq 0$, $f_{2d} = -h_d^2/4$ et $f_{2d-1} = h_d h_{d-1}/2$, alors le changement de variable :

$$y' = y + \frac{h_d}{2}x^d$$

annule les termes en $x^d y$, $x^{2d}$ et $x^{2d-1}$, contredisant la minimalité de $d$. □

En effectuant encore le changement de coordonnées $y \mapsto y + h(x)/2$ (toujours lorsque la caractéristique de $k$ est différente de 2), on obtient une équation de la forme :

$$y^2 = f(x). \tag{EQ3}$$

### 1.4.3. Condition suffisante sur une équation affine pour être hyperelliptique

**Espaces projectifs gradués**

Nous verrons que les complétions projectives des courbes données par une équation de la forme EQ1 ou EQ3 ne sont pas toujours lisses dans l'espace projectif usuel, c'est pourquoi nous serons amenés à considérer des espaces projectifs gradués, dans lesquels la complétion de l'équation de forme EQ2 donne une courbe lisse.

De façon intuitive, l'espace projectif gradué $\mathbb{P}_k(a_0, ..., a_n)$ est l'espace projectif $\mathbb{P}^n_k$, où l'on a assigné aux coordonnées $x_0, ..., x_n$ les poids $a_0, .., a_n$, c'est-à-dire que dans l'anneau des coordonnées, les monômes $x_0, ..., x_n$ ont pour degrés respectifs $a_0, ..., a_n$.

**Définition 1.4.4** (Espace projectif gradué)**.** Soient $a_0, ..., a_n \in \mathbb{N}$. L'*espace projectif gradué* $\mathbb{P}_k(a_0, ..., a_n)$ sur un corps $k$ est le quotient de $\mathbb{A}^{n+1}_k$ par l'action de groupe de $k^\times$ :

$$\lambda \cdot (x_0, ..., x_n) := (\lambda^{a_0} x_0, ..., \lambda^{a_n} x_n).$$

De façon similaire aux variétés dans l'espace projectif usuel, on définit les variétés dans l'espace projectif gradué par des polynômes homogènes.

**Définition 1.4.5** (Polynômes homogènes)**.** Le *degré* d'un monôme $x_0^{d_0} \cdots x_n^{d_n} \in k[x_0, ..., x_n]$ relativement aux poids $a_0, ..., a_n$ est $\sum_i a_i d_i$. Un polynôme est dit *homogène* relativement aux poids $a_0, ..., a_n$ si tous ses monômes ont le même degré relativement à $a_0, ..., a_n$.

Une variété dans l'espace projectif gradué $\mathbb{P}_k(a_0, ..., a_n)$ est alors le lieu des zéros d'une famille de polynômes de $k[x_0, ..., x_n]$ homogènes relativement aux poids $a_0, ..., a_n$. Les cartes affines usuelles sont également modifiées : pour les indices $i$ tels que $a_i \neq 1$, la carte $x_i \neq 0$ est encore un quotient de $\mathbb{A}^n$ par une action de groupe ; les détails se trouvent dans [Hos16].

**Équations de courbes dans l'espace projectif gradué**

Expliquons d'abord la nécessité de se placer dans un espace projectif gradué. Prenons l'exemple de la courbe affine d'équation

$$y^2 = x^5 - x.$$

C'est une courbe lisse, mais sa complétion projective dans $\mathbb{P}^2$ d'équation homogène

$$y^2 z^3 = x^5 - x z^4$$

ne l'est pas. En effet, le point à l'infini $(0 : 1 : 0)$ n'est pas régulier. Ce problème, qui ne se présente pas dans le cas des courbes de genre 1 d'équation de Weierstrass $y^2 = x^3 + ax + b$, vient du fait qu'on multiplie $y$ par une grande puissance de $z$. La solution est de se placer dans un espace projectif gradué où on assigne un grand degré à $y$.
Considérons une courbe affine lisse $C$ d'équation de la forme EQ2 vérifiant les conditions de 1.4.5. La complétion projective de cette courbe dans l'espace gradué $\mathbb{P}(1, d, 1)$, que nous noterons encore $C$, a pour équation :

$$y^2 + (h_d x^d + h_{d-1} x^{d-1} z + \cdots + h_0 z^d) y = f_{2d} x^{2d} + f_{2d-1} x^{2d-1} z + \cdots + f_0 z^{2d}. \qquad \text{(EQ4)}$$

Les points à l'infini de cette courbe sont les $(1 : a : 0)$ ; où $a$ vérifie :

$$a^2 + h_d a = f_{2d}.$$

Dans le cas où $f_{2d} = -h_d^2/4$, il y a un seul point à l'infini ; sinon, il y en a 2.
Comme la coordonnée $x$ est de degré 1, on peut se placer dans la carte affine usuelle $x \neq 0$ pour étudier la régularité de ces points.

**Proposition 1.4.6.** Les points à l'infini de la courbe $C$ d'équation EQ4 sont réguliers.

*Démonstration.* Dans la carte affine $x = 1$, la courbe a pour équation :

$$y^2 + (h_d + h_{d-1}z + \cdots + h_0 z^d)y = f_{2d} + f_{2d-1}z + \cdots + f_0 z^{2d}.$$

Le gradient en $(1 : a : 0)$ est

$$(2a + h_d, h_{d-1}a - f_{2d-1}).$$

Si le point était singulier, on aurait donc $2a = -h_d$ et $h_{d-1}a = f_{2d-1}$, soit :

$$f_{2d-1} = -\frac{h_d h_{d-1}}{2}$$

qui est exactement le cas qu'on avait exclu lors de la description de l'équation en 1.4.5. Les points à l'infini sont donc réguliers. □

La courbe $C$ d'équation EQ4 est donc lisse. Elle est munie d'un revêtement $\phi : C \to \mathbb{P}^1$ donné par :

$$\phi(x : y : z) = (x : z).$$

Ce revêtement est de degré 2, $C$ est donc une courbe hyperelliptique. Étudions plus en détail les propriétés de $\phi$.

**Proposition 1.4.7.** Le morphisme $\phi$ a $2d$ points de ramification.

*Démonstration.* Afin de trouver les points de ramification , l'équation qui était de la forme :

$$y^2 + H(x, z)y = F(x, z)$$

peut être ramenée à :

$$\left(y + \frac{H(x, z)}{2}\right)^2 = F(x, z) + \frac{H(x, z)^2}{4}.$$

Les points de ramification sont donc ceux où $F(x, z) + H(x, z)^2/4$ s'annule. Si $f_{2d} \neq -h_d^2/4$ alors le polynôme $F(x, 1) + H(x, 1)^2/4$ est de degré $2d$ et la courbe a 2 point à l'infini ; sinon, il est de degré $2d - 1$, et la courbe a un seul point à l'infini.
• Si $f_{2d} \neq -h_d^2/4$ : il y a $2d$ points de ramification de la forme $(x : y : 1)$, et les points à l'infini $(1 : a : 0)$ n'en sont pas.
• Si $f_{2d} \neq -h_d^2/4$ : il y a $2d - 1$ points de ramification de la forme $(x : y : 1)$, et le point à l'infini $(1 : a : 0)$ est un point de ramification. □

Connaissant le nombre de points de ramification, on peut maintenant déterminer le genre de la courbe $C$ grâce à la formule de Riemann-Hurwitz.

**Proposition 1.4.8.** Le genre de la courbe $C$ est :

$$g(C) = d - 1.$$

*Démonstration.* On considère le morphisme $\phi : C \to \mathbb{P}^1$. Il y a $2d$ points de ramification, tous d'indice de ramification 2 puisque $\phi$ est de degré 2. La formule de Riemann-Hurwitz donne ici

$$2g(C) - 2 = 2 \cdot (2 \times 0 - 2) + 2d$$

et ainsi :

$$g(C) = d - 1.$$

□

## 1.5. Courbes de genre 2

Nous étudierons plus en détail les courbes de genre 2 ; voici quelques résultats importants à leur sujet.

**Proposition 1.5.1.** Les courbes de genre 2 sont hyperelliptiques.

*Démonstration.* Soit $K$ un diviseur canonique sur $C$ : comme $C$ est de genre 2,

$$\ell(K) = g(C) = 2$$

et

$$\deg K = 2g(C) - 2 = 2.$$

Quitte à lui ajouter le diviseur d'une fonction de $\mathscr{L}(K)$, on peut supposer $K$ effectif. Donc $K = (P) + (Q)$ avec $P, Q \in C$. Soit $f : C \to \mathbb{P}^1$ une fonction non constante de $\mathscr{L}(K)$.
Comme $\operatorname{div} f \geqslant -(P) - (Q)$, la fonction $f$ a un pôle simple, un pôle double ou deux pôles simples. Notons $\infty$ le diviseur du point à l'infini $(1 : 0) \in \mathbb{P}^1$.
• Si $f$ a un pôle double ou deux pôles simples alors le diviseur $f^\star(\infty)$ est de degré 2 ; or

$$\deg f^\star(\infty) = \deg f \cdot \deg(\infty) = \deg f$$

donc $\deg f = 2$.
• Si $f$ a un pôle simple : le même raisonnement donne $\deg f = 1$ et $C \simeq \mathbb{P}^1$, ce qui est faux. □

Les résultats de la partie 1.4 nous permettent d'affirmer qu'une courbe de genre 2 définie sur $k$ admet une équation de la forme :

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

avec $h, f \in \bar{k}[x]$. Voici une condition suffisante simple pour qu'elle admette une telle équation à coefficients dans $k$.

**Proposition 1.5.2.** Soit $C$ une courbe de genre $g = 2$ définie sur $k$. Si $C$ a un point $k$-rationnel, alors elle admet une équation de la forme $y^2 + h(x)y = f(x)$ avec $h, f \in k[x]$, $\deg h \geqslant 2$ et $\deg f \geqslant 5$.

*Démonstration.* Soit $K$ un diviseur canonique sur $C$. Alors $(P), K \in \operatorname{div}_k C$. D'abord, $\deg(K - 2P) = 0$ donc $k \subseteq \mathscr{L}(K - 2P)$ et d'après le théorème de Riemann-Roch :

$$\ell(2P) = \ell(K - 2P) + 1 \geqslant 2.$$

De plus, pour $n > 2g - 2 = 2$ :

$$\ell(nP) = n + 1 - g = n - 1.$$

Donc $\ell(3P) = 2$, or $\mathscr{L}(3P)$ contient $\mathscr{L}(2P)$ donc $\ell(2P) = 2$. On peut donc écrire $\mathscr{L}(2P) = \langle 1, x\rangle$, où la fonction $x \in k(C)$ a un pôle d'ordre $\leqslant 2$ en $P$. C'est un pôle d'ordre exactement 2 : sinon, $x$ serait dans $\mathscr{L}(P)$ et $x^2$ dans $\mathscr{L}(2P)$, qui est de dimension 2 et contient déjà 1 et $x$, ce qui est absurde. Ainsi, $x^2 \in \mathscr{L}(4P)$, donc $\mathscr{L}(4P) = \langle 1, x, x^2\rangle$ puisque $\ell(4P) = 3$. Par contre, $x^3$ a un pôle d'ordre 6 en $P$ et n'est donc pas dans $\mathscr{L}(5P)$, qui est de dimension 4. Par conséquent, il existe une fonction $y \in k(C)$ indépendante de $1, x, x^2, x^3$ telle que $\mathscr{L}(5P) = \langle 1, x, x^2, y\rangle$. En continuant ce raisonnement, on obtient :
• $\mathscr{L}(6P) = \langle 1, x, x^2, x^3, y\rangle$
• $\mathscr{L}(7P) = \langle 1, x, x^2, x^3, y, xy\rangle$
• $\mathscr{L}(8P) = \langle 1, x, x^2, x^3, x^4, y, xy\rangle$
• $\mathscr{L}(9P) = \langle 1, x, x^2, x^3, x^4, y, xy, x^2y\rangle$
Mais enfin, $\mathscr{L}(10P)$ est de dimension 9 et contient les 10 éléments suivants, entre lesquels il y a donc une relation linéaire :

$$1, x, x^2, x^3, x^4, x^5, y, y^2, xy, x^2y.$$

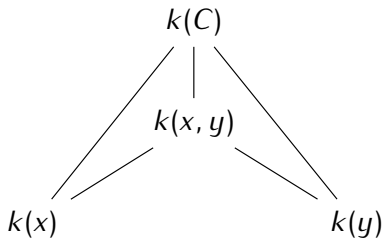
On peut donc définir un morphisme :

$$\begin{array}{ccc} C & \longrightarrow & \mathbb{P}^2 \\ P & \longmapsto & (x : y : 1) \end{array}$$

dont l'image est la courbe $H$ donnée par une équation de la forme :

$$y^2 + a_1xy^2 + a_2xy + a_3y = b_6x^6 + \cdots + b_1x + b_0.$$

Il reste à montrer que ce morphisme est injectif. Le corps des fonctions de la courbe $H$ est exactement $k(x, y)$. Considérons alors les extensions de corps suivantes :




Comme $x$ a un unique pôle d'ordre 2, le morphisme $x : C \to \mathbb{P}^1$ est de degré 2 ; de même, $y$ est de degré 5. Le degré d'extension $[k(C) : k(x, y)]$ doit diviser $[k(C) : k(x)] = 2$ et $[k(C) : k(y)] = 5$, il vaut donc 1 et $k(C) = k(x, y)$. □

# 2. Revêtements de genre 2 de courbes de genre 1

## 2.1. Jacobiennes décomposables

Nous allons maintenant étudier les revêtements de genre 2 de courbes de genre 1. Nous allons montrer que les courbes de genre 2 cherchées sont précisément celles dont la jacobienne est *décomposable*. Fixons pour toute cette section une courbe lisse $C$ de genre 2.

**Définition 2.1.1** (Jacobienne d'une courbe)**.** La *jacobienne* $J_C$ de $C$ est dite $(n, n)-$décomposable s'il y a une isogénie $J_C \to E_1 \times E_2$ de degré $n^2$, où $E_1$ et $E_2$ sont des courbes elliptiques.

**Proposition 2.1.1.** Si la jacobienne $J_C$ de $C$ est décomposable, alors il y a un revêtement $C \to E$ où $E$ est elliptique.

*Démonstration.* La jacobienne $J_C$ est décomposable, il existe donc une isogénie $J_C \to E_1 \times E_2$, où $E_1$ et $E_2$ sont elliptiques. Notons $\alpha : C \to J_C$ une injection de $C$ dans sa jacobienne, et $p_1 : E_1 \times E_2 \to E_1$ la projection sur la première coordonnée. On construit un morphisme non-constant (et donc surjectif) de courbes algébriques $C \to E$ de la façon suivante :

$$C \xrightarrow{\alpha} J_C \longrightarrow E_1 \times E_2 \xrightarrow{p_1} E_1.$$

□

Lorsque la jacobienne de $C$ est décomposable, il y a donc nécessairement un tel revêtement d'une courbe elliptique par $C$. La réciproque de ce résultat nécessite une propriété d'optimalité du revêtement.

**Définition 2.1.2** (Revêtement optimal)**.** Un tel revêtement $\phi : C \to E_1$ est dit *optimal* s'il ne se factorise pas par une isogénie non triviale, c'est-à-dire que s'il y a un diagramme commutatif :

$$\begin{array}{ccc} C & \xrightarrow{\phi} & E_1 \\ \downarrow & \nearrow_{\psi} & \\ E_2 & & \end{array}$$

où $E_2$ est une courbe elliptique et $\psi$ une isogénie, alors $\deg \psi = 1$.

Cela signifie en particulier que les revêtements de degré premier seront toujours optimaux.

**Proposition 2.1.2.** S'il existe une courbe elliptique $E_1$ et un revêtement optimal $C \to E_1$ de degré $n$, alors la jacobienne $J_C$ est $(n, n)-$décomposable.

*Démonstration.* Un revêtement $\phi : C \to E_1$ donne lieu à une isogénie $\phi_\star : J_C \to J_{E_1} \simeq E_1$. Le noyau de cette isogénie est connexe car $f$ est optimal (voir [Ser88] §VI.13) et même une courbe elliptique (voir [Dju17] §1.3) que nous noterons $E_2$, et on obtient une suite exacte de variétés abéliennes :

$$0 \longrightarrow E_2 \xrightarrow{\varphi} J_C \xrightarrow{\phi_\star} E_1 \longrightarrow 0.$$

La suite *duale* suivante est également exacte (voir [Mil08] §11) :

$$0 \longrightarrow E_1 \xrightarrow{\phi^\star} J_C \xrightarrow{\varphi^\vee} E_2 \longrightarrow 0.$$

On construit $g : E_1 \times E_2 \to J_C$ cherchée comme :

$$g := \phi^\star + \varphi.$$

Il s'agit clairement d'un morphisme de groupes algébriques ; il reste à vérifier que son noyau est fini. Calculons-le ! Les éléments du noyau de $g$ sont exactement les couples $(P_1, P_2)$ tels que $\phi^\star P_1 = -\varphi P_2$ ; le noyau est donc isomorphe à l'intersection des images de $\phi^\star$ et de $-\varphi$.

$$\begin{aligned} \ker g &\simeq \operatorname{im}\phi^\star \cap \operatorname{im}\varphi \\ &= \operatorname{im}\phi^\star \cap \ker \phi_\star \\ &= \ker(\phi_\star\phi^\star) \\ &= E[n] \end{aligned}$$

En remplaçant $\operatorname{im}\phi^\star$ par $\ker\varphi^\vee$, le même raisonnement montre que $\ker g \simeq E_2[n]$. □

Voyons un cas très simple dans lequel la jacobienne d'une courbe de genre 2 est décomposable. Nous le rencontrerons dans la pratique en 4.4.

**Proposition 2.1.3.** Si $\sigma$ est une involution non hyperelliptique non triviale de $C$ alors $\iota\sigma$ en est encore une.

*Démonstration.* Il est évident que $\iota\sigma$ est différente de $\iota$. De plus, comme l'involution hyperelliptique commute avec toutes les autres, $\iota\sigma$ est encore d'ordre 2. □

**Proposition 2.1.4.** Si $\sigma$ est une involution non hyperelliptique non triviale de $C$, alors $C/\sigma$ est de genre 1.

*Démonstration.* Le genre de $C/\sigma$ se détermine à l'aide de la formule de Riemann-Hurwitz, appliquée à $\pi : C \to C/\sigma$. Elle donne :

$$6 - 4g(C/\sigma) = \sum_{P \in C/\sigma} e_\pi(P) \geqslant 0$$

donc $g(C/\sigma) = 0$ ou 1. Si c'était 0, $\sigma$ serait l'involution hyperelliptique, ce qui n'est pas le cas. □

En fait, l'existence d'une involution supplémentaire n'est pas seulement suffisante, mais aussi nécessaire pour que la jacobienne de $C$ soit (2,2)-décomposable.

**Proposition 2.1.5.** La jacobienne de $C$ est (2,2)-décomposable si et seulement si $C$ possède une involution non hyperelliptique.

*Démonstration.* Si $C$ possède une telle involution $\sigma$, alors les propositions 2.1.2 et 2.1.4 permettent de conclure, puisqu'alors le revêtement $C \to C/\sigma$ est de degré premier 2 et donc optimal. Si $J_C$ est (2,2)-décomposable, il existe un revêtement $\phi : C \to E$ de degré 2 où $E$ est une courbe elliptique. Le groupe $\mathsf{Gal}(k(C)/\phi^\star k(E))$ est d'ordre 2 : son générateur est une involution de $C$ non hyperelliptique. □

## 2.2. Revêtement de Frey-Kani

On considère un revêtement $k$-rationnel $\psi : C \to E$ de courbes algébriques définies sur $k$, où $C$ est de genre 2 et $E$ de genre 1. Le but de cette section est de montrer que ce revêtement donne lieu à un revêtement $\mathbb{P}^1 \to \mathbb{P}^1$ plus facile à étudier.

Soit $\iota$ l'involution hyperelliptique de $C$, et $\pi_C : C \to C/\langle\iota\rangle \simeq \mathbb{P}^1$. La construction suivante est présentée dans [Kuh88].

**Lemme 2.2.1.** Soit $P_0 \in C$ un point de Weierstrass, et $\alpha : P \mapsto (P) - (P_0)$ un plongement de $C$ dans sa jacobienne $J_C$. Alors l'involution $[-1]$ de $J_C$ rend commutatif le diagramme :

$$\begin{array}{ccc} C & \xrightarrow{\iota} & C \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\alpha} \\ J_C & \xrightarrow{-1} & J_C \end{array}$$

*Démonstration.* Il s'agit de montrer que pour tout $P \in C$, $(\iota(P)) - (P_0) \sim (P_0) - (P)$, c'est-à-dire que le diviseur $(\iota(P)) + (P) - 2(P_0)$ est principal. C'est le cas puisque, comme $P_0$ est un point de Weierstrass :

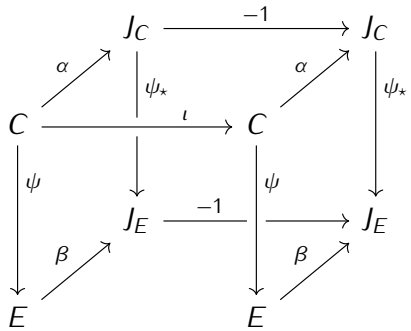
$$\operatorname{div}\left(\frac{\pi_C - \pi_C(P)}{\pi_C - \pi_C(P_0)}\right) = (P) + (\iota(P)) - 2(P_0).$$

□

**Lemme 2.2.2.** Il existe une involution $\nu$ de $E$ telle que le diagramme suivant soit commutatif :

$$\begin{array}{ccc} C & \xrightarrow{\iota} & C \\ \downarrow{\scriptstyle\psi} & & \downarrow{\scriptstyle\psi} \\ E & \xrightarrow{\nu} & E \end{array}$$

*Démonstration.* Reprenons les notations du lemme précédent. $E$ est isomorphe à sa jacobienne via $\beta : Q \mapsto (Q) - (\psi(P_0))$. Alors $\psi$ induit un morphisme $\psi_\star : J_C \to J_E$ sur les jacobiennes qui vérifie $\psi_\star \circ \alpha = \beta \circ \psi$ et $[-1]_{J_E} \circ \psi_\star = \psi_\star \circ [-1]_{J_C}$. On vérifie alors aisément que le diagramme suivant est commutatif :




On peut maintenant définir le revêtement $\nu$ cherché :

$$\nu := \beta^{-1} \circ [-1]_{J_E} \circ \beta.$$

Comme $\beta \circ \psi \circ \iota = [-1]_{J_E} \circ \beta \circ \psi$, on a bien $\nu \circ \psi = \psi \circ \iota$.

□

Ici, on a donc donné à $E$ une structure de courbe elliptique, dont l'élément neutre de la loi de groupe est $\psi(P_0)$.

**Théorème 2.2.1.** Notons $\pi_C : C \to C/\langle\iota\rangle \simeq \mathbb{P}^1$ et $\pi_E : E \to E/\langle\nu\rangle \simeq \mathbb{P}^1$. Le revêtement $\psi$ induit un revêtement $\phi : \mathbb{P}^1 \to \mathbb{P}^1$, appelé revêtement de Frey-Kani [FK89], tel que le diagramme suivant soit commutatif :

$$\begin{array}{ccc} C & \xrightarrow{\psi} & E \\ \downarrow{\scriptstyle \pi_C} & & \downarrow{\scriptstyle \pi_E} \\ \mathbb{P}^1 & \xrightarrow{\phi} & \mathbb{P}^1 \end{array}$$

*Démonstration.* Il s'agit de montrer que $\pi_E \circ \psi$ passe au quotient par $C/\langle\iota\rangle$, ce qui est le cas puisque si $Q = \iota(P)$ alors $\psi(Q) = \nu(\psi(P)) \equiv \psi(P)$ dans $E/\langle\nu\rangle$. □

## 2.3. Un cas particulier détaillé

On étudie ici en détail le cas où le revêtement $\psi : C \to E$ est de degré 3 et ramifié en un seul point $P' \in C$. On suppose de plus que $k$ n'est pas de caractéristique 2 ou 3. De cette façon, les courbes $C$ et $E$ admettent des équations de la forme $y^2 = f(x)$, et il n'y a pas de ramification sauvage : la formule de Riemann-Hurwitz s'applique.

### 2.3.1. Ramification

Notons $P := \psi(P')$, $Q := \pi_C(P)$ et $f := \phi \circ \pi_C = \pi_E \circ \psi$. On sait que $\pi_E$ est ramifié en 4 points, et $\pi_C$ en 6 points. Le revêtement de Frey-Kani $\phi$ est de degré 3 puisque $f = \pi_E \circ \psi$ est de degré 6. On appellera encore points de branchement d'un revêtement les images de ses points de ramification.

$$\begin{array}{ccc} C & \xrightarrow{\psi} & E \\ \downarrow{\scriptstyle \pi_C} & \searrow^{f} & \downarrow{\scriptstyle \pi_E} \\ \mathbb{P}^1 & \xrightarrow{\phi} & \mathbb{P}^1 \end{array}$$

**Détermination de $e_\phi(Q)$.** Comme $e_\psi(P') = 3$, $e_f(P)$ est un multiple de 3. Étant donné que $\deg(\pi_C) = 2$, $e_{\pi_C}(P')$ est strictement inférieur et donc premier à 3, et la seule possibilité est que $e_\phi(Q) = 3$.

**Autres points de ramification de $\phi$.** D'après la formule de Riemann-Hurwitz, comme le revêtement $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ est de degré 3 :

$$\sum_{x \in \mathbb{P}^1} (e_\phi(x) - 1) = 4.$$

Étant donné que $e_\phi(\pi_C(P')) = 3$ et que $f = \pi_E \circ \phi$ a un seul point de ramification d'indice un multiple de 3 (car $\psi$ en a un et $\pi_E$ n'en a pas), $\phi$ a donc deux autres points de ramification d'indice 2.

**$P'$ est-il un point de ramification de $\pi_C$ ?** On applique la formule de Riemann-Hurwitz à $f : C \to \mathbb{P}^1$ qui est de degré 6 :

$$\sum_{x \in C} (e_f(x) - 1) = 14$$

Montrons que $P'$ est ramifié par $\pi_C$. Supposons que $e_{\pi_C}(P') = 1$. Alors $C$ a 6 points de Weierstrass distincts de $P$. Notons $\lambda$ le nombre de points de Weierstrass dont l'image dans $\mathbb{P}^1$ est un point de ramification de $\phi$. La fonction $f$ a donc un point de ramification d'indice 3, $\lambda$ points de ramification d'indice 4 et $(6 - \lambda) + (4 - 2\lambda)$ points de ramification d'indice 2 (les points de Weierstrass restants, et les antécédents des points de ramification de $\phi$). Ainsi, on obtient :

$$\sum_{x \in C} (e_f(x) - 1) = 2 + 3\lambda + (6 - \lambda) + (4 - 2\lambda) = 12.$$

Ce résultat est absurde, on en déduit donc que $e_{\pi_C}(P') = 2$. Par conséquent,

$$e_f(P') = e_{\pi_C}(P') \cdot e_\phi(Q) = 6.$$

Or $e_f(P') = 3e_{\pi_E}(P)$, donc $P$ est l'un des points de ramification de $\pi_E$.

**Les points de branchement de $\pi_C$ ne sont pas des points de ramification de $\phi$.** Étant donné que $f = \pi_E \circ \psi$ et que le seul point de branchement de $\psi$ est un point de ramification de $\pi_E$, on sait que $f$ a exactement 10 points de ramification : $P'$, et les $3 \times 3 = 9$ antécédents des trois autres points de ramification de $\pi_E$.

Ces points sont $P'$, les 5 autres points de Weierstrass de $C$ et les antécédents des points de ramification de $\phi$, qui doivent donc être au nombre de 4. Ainsi, les points de ramification de $\phi$ ne sont pas images par $\pi_C$ des points de Weierstrass.

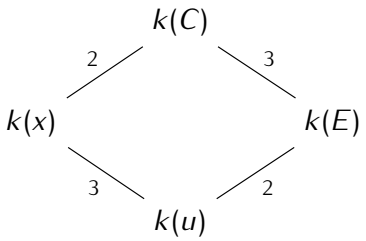
**Images par $f$ des points de Weierstrass de $C$.** La courbe $C$ a 5 points de Weierstrass autres que $P'$. Leurs images ne sont pas des points de ramification de $\phi$. Cependant, comme ils sont des points de ramification de $f$, leurs images par $f$ sont parmi les 4 points de branchement de $\pi_E$.

### 2.3.2. Équations de $E$ et $C$

Cette section détaille et corrige certains des arguments donnés dans [Sha04] et [Sha05]. Supposons que dans un système de coordonnées approprié, $E$ soit donnée par une équation de la forme :

$$v^2 = u(u - q_1)(u - q_2) \qquad \text{avec } q_1 q_2, q_1 + q_2 \in k$$

Alors $\pi_E$ est la fonction coordonnée $u$, et ses points de branchement sont $0, q_1, q_2, \infty$. Le revêtement $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ induit une extension de corps de fonctions $k(x)/k(u)$ de degré 3. On a donc le diagramme d'extensions de corps suivant :



On sait que $\phi$ est de degré 3. On peut, par souci de simplicité, choisir (modulo un automorphisme de $\mathbb{P}^1$) que $\phi(\infty) = \infty$, et que $q_1$ et $q_2$ soient les deux autres points de branchement de $\phi$. Alors $u$ est un polynôme de degré 3 en $x$ ; notons-le encore $\phi(x)$. On peut donc supposer (via multiplication de $U$ par un scalaire) que $u = x^3 + ax^2 + bx + c$, et en remplaçant $x$ par $x + \frac{a}{3}$ on obtient :

$$u = x^3 + bx + c$$

Contrairement à ce qui est affirmé dans [Sha04], on ne peut pas se passer de $b$ ici. Le polynôme $x^3 + bx + c$ est à racines simples puisque 0 n'est pas un point de branchement de $\phi$.

**Équation de $C$.** On commence par chercher les points de $\phi^{-1}\{q_1, q_2\}$. Ce sont exactement les racines du résultant :

$$R(x) := \mathrm{Res}_z \left( \frac{\phi(x) - \phi(z)}{x - z}, \phi'(z). \right)$$

En effet, les racines de ce polynôme sont les $x \in \mathbb{P}^1 \backslash \{\infty\}$ dont l'image par $\phi$ a une préimage par $\phi$ racine de $\phi'$, c'est-à-dire les $x$ dont l'image est un point de branchement de $\phi$. Un calcul avec Magma donne :

$$R(x) = (3x^2 + b)(3x^2 + 4b)$$

où les racines de $3x^2 + b = \phi'(x)$ correspondent aux préimages doubles de $\phi$, et les racines de $3x^2 + 4b$ aux préimages simples.

Dans un système de coordonnées approprié, la courbe $C$ admet une équation de la forme $y^2 = h(x)$, où $h$ est un polynôme de degré 5 en $x$, et $\pi_C(x, y) = x$. On a vu plus haut que les points de ramification de $\pi_C$ autres que $P'$ ont pour image par $\pi_C$ les préimages simples de $0, q_1, q_2$. Les préimages de 0 sont les racines de $x^3 + bx + c$, et les préimages simples de $q_1$ et $q_2$ sont les racines de $3x^2 + 4b$. On a donc une équation de $C$ :

$$y^2 = (x^3 + bx + c)(3x^2 + 4b).$$

**Équation de $E$.** La courbe $E$ admet une équation de la forme :

$$v^2 = u(u - q_1)(u - q_2)$$

où $u, v \in k(C)$ sont données par le revêtement $\psi : C \to E$ :

$$(u, v) = \psi(x, y).$$

Afin de trouver $v(x, y)$, on détermine en quels points la fonction $v$ s'annule. Les zéros de $v$ sont les points de ramification de $\pi_E$ autres que $P$, ils proviennent donc de points de ramification d'ordre 2 de $f$. Ceux-ci sont :

- les points de Weierstrass de $C$ autres que $P'$ : ce sont les zéros de $y$,
- les points dont les images par $\pi_C$ sont des préimages doubles de $q_1, q_2$ : ce sont les zéros de $3x^2 + b$.

On obtient donc :

$$v = y(3x^2 + b)$$

et afin d'obtenir l'équation de $E$, on calcule :

$$\begin{aligned} v^2 &= y^2(3x^2+b)^2 \\ &= (x^3+bx+c)(3x^2+4b)(3x^2+b)^2 \\ &= u(27u^2 - 54cu + 4b^3 + 27b^2). \end{aligned}$$

Pour avoir un polynôme unitaire en $u$, on remplace $u$ par $3u$ et on obtient :

$$v^2 = u(u^2 - 6cu + 4b^3/3 + 9c^2)$$

et le revêtement est alors :

$$\begin{aligned} \psi(x,y) &= (u,v) \\ &= \Big((3(x^3+bx+c), y(3x^2+b)\Big). \end{aligned}$$

## 2.4. Étude d'un exemple concret

Appliquons ce raisonnement à un cas concret. On s'intéresse à la courbe elliptique $E$ labellisée e3d8D9 dans [Sij13], définie sur $\mathbb{Q}(\sqrt{2})$ par l'équation :

$$v^2 = u^3 + (-4 - 2\sqrt{2})u^2 + (-231 - 154\sqrt{2})u + (-1520 - 1064\sqrt{2})$$

dont l'équation de Weierstrass donnée par MAGMA est :

$$v^2 = u^3 + (-309744 - 206496\sqrt{2})u + (-95420160 - 66794112\sqrt{2}).$$

On effectue maintenant le changement de variable $u \mapsto u + z$, où $z$ vérifie

$$z^3 + (-309744 - 206496\sqrt{2})z + (95420160 + 66794112\sqrt{2}) = 0.$$

Ce polynôme a trois racines, dont une dans $\mathbb{Q}(\sqrt{2})$ : $-528 - 264\sqrt{2}$, et deux dans une extension quadratique de $\mathbb{Q}(\sqrt{2})$. Ces racines donnent lieu à des revêtements différents, que nous allons étudier séparément.

**Avec $z = -528 - 264\sqrt{2}$.** On se ramène, par le changement de variable $u \mapsto u + z$, à la forme souhaitée :

$$v^2 = u(u^2 - 6cu + 4b^3/3 + 9c^2)$$

avec $c = z/2$ et $b^3 = 916 + 1944\sqrt{2}$.
Malheureusement, $916 + 1944\sqrt{2}$ n'est pas un cube dans $\mathbb{Q}(\sqrt{2})$. La courbe $C$ trouvée avec la méthode précédente est donc définie sur l'extension cubique $\mathbb{Q}(\sqrt{2}, b)$ de $\mathbb{Q}(\sqrt{2})$, par l'équation :

$$y^2 = 3x^5 + 7bx^3 + (-792 - 396\sqrt{2})x^2 + 4b^2x + (-1056 - 528\sqrt{2})b$$

et le revêtement $\psi : C \to E$ est donné par :

$$\psi(x,y) = \Big(3[x^3 + bx + (-264 - 132\sqrt{2})], y(3x^2+b)\Big).$$

**Avec les autres racines.** On effectue maintenant le changement de variable $u \mapsto u + z$ où $z$ est l'un des deux nombres complexes conjugués vérifiant :

$$z^2 + (528 + 264\sqrt{2})z + 108432 + 72288\sqrt{2} = 0.$$

On travaille donc sur le corps de nombres de degré 4 : $\mathbb{Q}(\sqrt{2}, z)$. On obtient encore une équation de la forme :

$$v^2 = u(u^2 - 6cu + 4b^3/3 + 9c^2)$$

avec $c = z/2$ et $b^3 = [(-594 - 297\sqrt{2})z - 293301 - 195534\sqrt{2}]/2$.
Encore une fois, $b^3$ n'est pas un cube dans $\mathbb{Q}(\sqrt{2}, z)$, on va donc travailler sur le corps de nombres de degré 12 : $\mathbb{Q}(\sqrt{2}, z, b)$. La courbe $C$ trouvée avec la méthode précédente est définie sur ce corps par l'équation :

$$y^2 = 3x^5 + 7bx^3 - \frac{3}{2}zx^2 + 4b^2x + 2zb$$

et le revêtement $\psi : C \to E$ est donné par :

$$\psi(x, y) = \left(3(x^3 + bx + z/2), y(3x^2 + b)\right).$$

# 3. Algèbres de quaternions et courbes de Shimura

## 3.1. Algèbres de quaternions

Nous verrons que les courbes de Shimura sont définies par un groupe qui provient d'un ordre dans une algèbre de quaternions sur un corps de nombres. Nous allons donc présenter d'abord les algèbres de quaternions, puis leurs ordres, et enfin les groupes de transformations qui en résultent. Les démonstrations des propriétés énoncées ici se trouvent dans [Voi18] §2,3,10 et [AB04] §1. Les termes français sont ceux employés dans [Vig95]. Fixons pour toute cette partie un corps $K$ de caractéristique différente de 2.

### 3.1.1. Définitions de base

Historiquement, les algèbres de quaternions sont une généralisation des quaternions de Hamilton : une $\mathbb{R}$-algèbre $\mathbb{H}$ de dimension 4 engendrée comme espace vectoriel par les éléments $1, i, j, k$ tels que

$$i^2 = j^2 = k^2 = ijk = -1.$$

**Définition 3.1.1** (Algèbre de quaternions)**.** Une *algèbre de quaternions* sur $K$ est une $K$-algèbre de dimension 4 munie d'une $K$-base $\{1, i, j, k\}$ où

$$i^2 = a,\ j^2 = b,\ k = ij = -ji$$

avec $a, b \in K^\times$. L'algèbre de quaternions définie par ces éléments $a, b \in K^\times$ sera notée :

$$\left(\frac{a, b}{K}\right).$$

Avec cette notation, les quaternions de Hamilton sont définis par :

$$\mathbb{H} = \left(\frac{-1, -1}{\mathbb{R}}\right).$$

Pour une extension de corps $K \subset L$ et des éléments $a, b \in K^\times$, on a :

$$\left(\frac{a, b}{K}\right) \otimes_K L = \left(\frac{a, b}{L}\right).$$

Un exemple fondamental d'algèbre de quaternions sur $K$ est l'algèbre $M_2(K)$ des matrices $2 \times 2$ à coefficients dans $K$. D'ailleurs, toute $K$-algèbre de quaternions est soit un corps non commutatif, soit isomorphe à $M_2(K)$ ([AB04] §1.1). A l'image des nombres complexes, les algèbres de quaternions sont munies d'une conjugaison, et on peut définir la norme et la trace réduites d'un élément. Pour les définitions suivantes, on fixe une algèbre de quaternions $B$ sur $K$, de base $\{1, i, j, k\}$.

**Définition 3.1.2** (Conjugaison)**.** La *conjugaison* est l'application $\overline{\ } : B \to B$ définie par :

$$\overline{t + xi + yj + zk} = t - (xi + yj + zk)$$

pour tous $t, x, y, z \in K$.

**Proposition 3.1.1.** La conjugaison est l'unique involution $K-$linéaire de $B$ vérifiant les propriétés suivantes pour tous $\alpha, \gamma \in B$ :
- $\overline{1} = 1$
- $\overline{\alpha\gamma} = \overline{\gamma\alpha}$
- $\alpha + \overline{\alpha} \in K$ et $\alpha\overline{\alpha} = \overline{\alpha}\alpha \in K$.

**Définition 3.1.3** (Trace réduite)**.** La *trace réduite* d'un élément $\alpha \in B$ est :

$$\mathrm{trd}(\alpha) = \alpha + \overline{\alpha} \in K.$$

**Proposition 3.1.2.** La trace réduite est $K$-linéaire et vérifie pour tous $\alpha, \gamma \in B$ :

$$\mathrm{trd}(\alpha\gamma) = \mathrm{trd}(\gamma\alpha).$$

**Définition 3.1.4** (Norme réduite)**.** La *norme réduite* d'un élément $\alpha \in B$ est :

$$\mathrm{nrd}(\alpha) = \alpha\overline{\alpha} \in K.$$

**Proposition 3.1.3.** La norme réduite est multiplicative, et les inversibles de $B$ sont exactement les éléments de norme réduite non nulle.

**Définition 3.1.5.** Soit $L$ une extension de $K$. On dit que $L$ *déploie* (en anglais, *split*) $B$ s'il y a un isomorphisme de $K$-algèbres :

$$L \otimes_K B \simeq M_2(L).$$

On définira à partir des quaternions des groupes de transformation du demi-plan supérieur. Dans ce but, on construit donc des matrices à partir de quaternions.

**Exemple 3.1.1.** On dispose d'un morphisme injectif de $k$-algèbres :

$$\sigma : \left(\frac{a, b}{k}\right) \longrightarrow M_2(k(\sqrt{a}))$$

défini par :

$$\sigma(i) = \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix} \quad \text{et} \quad \sigma(j) = \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}.$$

Dans le cas où $a = 1$, $\sigma$ est un isomorphisme de $K$-algèbres.

### 3.1.2. Ramification et discriminant

On considère à partir de maintenant un corps de nombres $K$ d'anneau des entiers $R$.

**Définition 3.1.6** (Ramification)**.** Soit $v$ une place de $K$, et $K_v$ le complété de $K$ en $v$. On dit que $B$ est *déployée* en $v$ si $B_v := B \otimes_K K_v$ est isomorphe à $M_2(K_v)$, et *ramifiée* sinon. Pour un idéal premier $\mathfrak{p}$ de $R$ de place $v_\mathfrak{p}$, on dit que $B$ est *ramifiée* en $\mathfrak{p}$ si elle est ramifiée en $v_\mathfrak{p}$.

L'ensemble $\mathrm{Ram}\, B$ des places en lesquelles $B$ est ramifiée est fini ([Voi18] §14.5), ce qui permet la définition suivante.

**Définition 3.1.7** (Discriminant)**.** Le *discriminant* $\mathcal{D}_B$ de $B$ est l'idéal de $R$ défini par :

$$\mathcal{D}_B := \prod_{\mathfrak{p} \in \mathrm{Ram}\, B} \mathfrak{p}.$$

### 3.1.3. Ordres

**Définition 3.1.8** (Ordres)**.** Soit $B$ une algèbre de quaternions sur $K$. Un $R$-*ordre* de $B$ est un sous-anneau $\mathcal{O}$ de $B$ qui est en même temps un réseau complet, c'est-à-dire un $R$-module libre tel qu'il y ait un isomorphisme de $K$-espaces vectoriels :

$$K \otimes_R \mathcal{O} \simeq B.$$

Nous serons intéressés par des ordres particuliers appelés ordres d'Eichler.

**Définition 3.1.9** (Ordre d'Eichler)**.** Un $R$-ordre est dit *maximal* s'il n'est inclus strictement dans aucun autre $R$-ordre de $B$. Un *ordre d'Eichler* est l'intersection de deux ordres maximaux.

Afin de construire un groupe de matrices à partir d'un ordre $\mathcal{O}$, nous allons considérer le groupe de ses unités de norme réduite 1 :

$$\mathcal{O}^1 := \{\gamma \in \mathcal{O} \mid \mathrm{nrd}\,\gamma = 1\}.$$

Pour tout idéal premier $\mathfrak{p}$ de $R$, on notera $R_\mathfrak{p}$ la complétion de $R$ correspondante et

$$\mathcal{O}_\mathfrak{p} := \mathcal{O} \otimes_R R_\mathfrak{p}$$

qui est un $R_\mathfrak{p}$-ordre de $B_\mathfrak{p} = B \otimes_K K_\mathfrak{p}$.

**Proposition 3.1.4.** Un sous-anneau $\mathcal{O}$ de $B$ est un ordre d'Eichler si et seulement si $\mathcal{O}_\mathfrak{p}$ est un ordre d'Eichler pour tout idéal premier $\mathfrak{p}$ de $R$.

Un ordre d'Eichler particulier de $M_2(K_\mathfrak{p})$ est :

$$\mathcal{O}_{\mathfrak{p},n} := \begin{pmatrix} R_\mathfrak{p} & R_\mathfrak{p} \\ \mathfrak{p}^n R_\mathfrak{p} & R_\mathfrak{p} \end{pmatrix}.$$

**Définition 3.1.10** (Niveau)**.** Soit $\mathcal{O}$ un ordre d'Eichler de $B$, et $\mathcal{N} = \prod_\mathfrak{p} \mathfrak{p}^{e_\mathfrak{p}}$ un idéal de $R$. On dit que $\mathcal{O}$ est *de niveau* $\mathcal{N}$ si $\mathcal{O}_\mathfrak{p}$ est conjugué à $\mathcal{O}_{\mathfrak{p},e_\mathfrak{p}}$ pour les idéaux premiers $\mathfrak{p}$ divisant $\mathcal{N}$, et maximal pour les autres.

## 3.2. Les courbes de Shimura $\mathcal{X}_0(\mathcal{N})$

On suppose désormais que le corps de nombres $K$ est *totalement réel* (c'est-à-dire que tous ses plongements dans $\mathbb{C}$ ont une image incluse dans $\mathbb{R}$) de degré $n$, et une algèbre de quaternions $B$ sur $K$ déployée en une seule des places réelles de $K$. Il y a donc un isomorphisme :

$$B \otimes_\mathbb{Q} \mathbb{R} \simeq M_2(\mathbb{R}) \times \mathbb{H}^{n-1}$$

et on dispose d'une injection $i : B \to M_2(\mathbb{R})$. On définit, comme pour les courbes modulaires classiques, des groupes $\Gamma(N)$ et $\Gamma_0(N)$, qui agissent sur le demi-plan de Poincaré $\mathcal{H}$.

**Définition 3.2.1.** Soit $\mathcal{N}$ un idéal de $R$ premier au discriminant de $B$, et $\mathcal{O}$ un ordre d'Eichler de $B$ de niveau $\mathcal{N}$. On définit le groupe :

$$\Gamma(1) := i(\mathcal{O}^1)/\{\pm 1\} \subseteq \mathrm{PSL}_2(\mathbb{R})$$

ainsi que son sous-groupe

$$\Gamma_0(\mathcal{N}) := \{\gamma \in \Gamma(1) \mid \gamma \text{ est triangulaire supérieure modulo } \mathcal{N}\}.$$

Notons que $\Gamma_0(\mathcal{N})$ dépend de $B$ et de l'ordre $\mathcal{O}$ de niveau $\mathcal{N}$ choisi. Nous pouvons maintenant définir les courbes de Shimura que nous étudierons par la suite.

**Définition 3.2.2** (Courbes de Shimura)**.** On note $\mathcal{X}(1)$ et $\mathcal{X}_0(\mathcal{N})$ les quotients respectifs $\Gamma(1)\backslash\mathcal{H}$ et $\Gamma_0(\mathcal{N})\backslash\mathcal{H}$.

Une propriété très importante des courbes de Shimura est la suivante ; elle les distingue des courbes modulaires ordinaires, pour lesquelles il faut passer de $\mathcal{H}$ à $\mathcal{H}^\star = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ pour obtenir une courbe compacte.

**Proposition 3.2.1.** Le quotient $\mathcal{X}_0(\mathcal{N})$ est une surface de Riemann compacte.

**Exemple 3.2.1.** La courbe elliptique étudiée en 2.4 est une courbe de Shimura. Plus précisément, c'est la courbe $\mathcal{X}_0(\mathfrak{p}_2)$ associée à un ordre d'Eichler d'une algèbre de quaternions sur $\mathbb{Q}(\sqrt{2})$, de niveau un idéal $\mathfrak{p}_2 \subset \mathbb{Z}[\sqrt{2}]$ au-dessus de $(2)$.

**Courbes de Shimura sur $\mathbb{Q}$**

Lorsque $K = \mathbb{Q}$, on dispose de résultats précis sur les courbes de Shimura. Le discriminant et le niveau d'un ordre d'Eichler de $B$ sont des idéaux de $\mathbb{Z}$, donc engendrés par des entiers $D$ et $N$. On peut par exemple calculer explicitement le degré de $\mathcal{X}_0(N)$ degré en fonction de $N$ et $D$([Cla03] §0.3.1).

**Proposition 3.2.2.** Le genre de la courbe $\mathcal{X}_0(N)$ est donné par la formule :

$$g = 1 + \frac{1}{12}\prod_{p|D}(p-1)\prod_{q|N}(q+1) - \frac{1}{4}\prod_{p|D}\left(1+\frac{1}{p}\right)\prod_{q|N}\left(1-\frac{1}{q}\right) - \frac{1}{3}\prod_{p|D}\left(1+\frac{3}{p}\right)\prod_{q|N}\left(1-\frac{3}{q}\right).$$

**Interprétation modulaire :** De façon similaire aux courbes modulaires usuelles, les courbes de Shimura sont les espaces de modules de variétés abéliennes. Plus précisément, la courbe $\mathcal{X}_0(N)$ correspond à un triplet $(A, i, H)$ où $A$ est une surface abélienne principalement polarisée, $i$ est une injection d'anneaux $\mathcal{O} \hookrightarrow \mathrm{End}\, A$ où $\mathcal{O}$ est un $\mathbb{Z}$-ordre maximal de $B$, et $H$ est un sous-groupe isomorphe à $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ de $A[N]$, monogène en tant que $\mathcal{O}$-module (voir [Cla03] §0.3.2).

### 3.2.1. Points CM

Conservons les notations de la partie précédente ; soit $B$ une algèbre de quaternions munie d'une injection $i : B \hookrightarrow M_2(\mathbb{R})$. Considérons une extension quadratique *totalement imaginaire* $L$ de $K$, d'anneau des entiers $\mathbb{Z}_L$. Soient $\mathcal{O}$ un ordre de $B$ et $\Theta$ un ordre du corps de nombres $L$.

**Proposition 3.2.3.** S'il y a un plongement $\phi : L \hookrightarrow B$, alors toutes les transformations $\gamma \in i(\phi(L^\star))\backslash\{\mathrm{id}\}$ ont un seul et même point fixe.

*Démonstration.* La preuve repose sur le fait que deux transformations $\gamma, \delta \in \mathrm{GL}_2(\mathbb{R})$ ont les mêmes points fixes précisément lorsque $\delta = \alpha\gamma + \beta\,\mathrm{id}$ avec $(\alpha, \beta) \in \mathbb{R}^\star \times \mathbb{R}$ (voir [AB04]§6.1). □

Concrètement, un tel plongement $\phi : L \hookrightarrow B$ est défini par un élément $\mu \in \mathcal{O}$ tel que $\mathbb{Z}_L = R[\mu]$ (voir [Voi09a]).

**Définition 3.2.3** (Plongement optimal)**.** Soit $\phi : L \hookrightarrow B$. On dit que $\phi$ est un plongement de $\Theta$ dans $\mathcal{O}$ si $\phi(\Theta) \subseteq \mathcal{O}$. Le plongement est alors dit *optimal* si $\phi(L) \cap \mathcal{O} = \phi(\Theta)$.

**Définition 3.2.4** (Point CM)**.** Soit $\mathcal{O}$ est un ordre d'Eichler de niveau $\mathcal{N}$, et $\mathcal{X}_0(\mathcal{N})$ la courbe de Shimura définie par $\mathcal{O}$. Un point $z \in \mathcal{X}_0(\mathcal{N})$ est appelé *point CM* par $\Theta$ si c'est le point fixe d'une transformation $\gamma \in i(\phi(F^\star))\backslash\{\mathrm{id}\}$, où $\phi$ est un plongement optimal de $\Theta$ dans $\mathcal{O}$.

### 3.2.2. Involutions d'Atkin-Lehner

Considérons une algèbre de quaternions $B$ de discriminant $\mathcal{D}$ déployée en une seule place du corps de nombres $K$ totalement réel, et le groupe de transformations $\Gamma_0(\mathcal{N})$ provenant d'un ordre $\mathcal{O}$ de niveau $\mathcal{N}$. Notons $B^+$ le groupe des éléments de $B$ de norme réduite totalement positive (c'est-à-dire que son image par tous les plongements de $K$ est strictement positive). Fixons $i : B \hookrightarrow M_2(\mathbb{R})$.

**Définition 3.2.5** (Groupe d'Atkin-Lehner)**.** Soit $N_\mathcal{O}$ le normalisateur de $\mathcal{O}$ dans $B^+/K^\star$ : l'ensemble des $\alpha \in B^+/K^\star$ tels que $\alpha\mathcal{O} = \mathcal{O}\alpha$. Notons $W = i(N_\mathcal{O})$ : c'est un sous-groupe de $\mathrm{PSL}_2(\mathbb{R})$ appelé *groupe d'Atkin-Lehner*. Ses éléments sont appelés *involutions d'Atkin-Lehner*.

**Dans notre cas :** Concrètement, nous considérerons par la suite un corps de nombres $K$ dont le groupe de classes restreint, c'est-à-dire la quotient du groupe des idéaux fractionnaires par les idéaux fractionnaires de la forme $\alpha R$ avec $\alpha \in K$ totalement positif, est trivial. De plus, la courbe que nous étudierons sera une courbe $\mathcal{X}_0(\ell^i)$ avec $\ell$ premier. Dans ce cas, le normalisateur est engendré par un seul élément d'ordre 2, et $W \simeq \mathbb{Z}/2\mathbb{Z}$. Nous noterons $\mathcal{X}_0(\ell^i)^\star$ le quotient de $\mathcal{X}_0(\ell^i)$ par cette involution non triviale.

**Interprétation modulaire lorsque $K = \mathbb{Q}$ :** Rappelons que la courbe $\mathcal{X}_0(N)$ paramétrise des triplets $(A, i, H)$ où $i : \mathcal{O} \hookrightarrow \mathrm{End}\, A$ est une injection d'anneaux. Le quotient $\mathcal{X}_0(N)/W$ de $\mathcal{X}_0(N)$ par les involutions d'Atkin-Lehner paramétrise quant à lui les couples $(A, H)$ où $A$ est une surface abélienne à *multiplication quaternionique* par un ordre maximal $\mathcal{O}$ de $B$ (c'est-à-dire qu'il existe une injection $i : \mathcal{O} \hookrightarrow \mathrm{End}\, A$ non fixée ici), et $H$ un sous-groupe isomorphe à $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ de $A[N]$, monogène en tant que $\mathcal{O}$-module (voir [Cla03] S 0.3.2).

# 4. Travail en vue de la construction d'une tour

## 4.1. Construction récursive d'une tour de courbes

Fixons à nouveau un corps de nombres totalement réel $K$ d'anneau des entiers $R$, une $K$-algèbre de quaternions $B$ ramifiée en toutes les places réelles sauf une, etun ordre d'Eichler $\mathcal{O}$ de $B$ de niveau $\ell$, où $\ell$ est un idéal premier de $K$ engendré par un élément $l \in R$.
Elkies présente dans [Elk97] une construction de tours de courbes modulaires, qui s'applique également aux courbes de Shimura. Le but est de construire une tour :

$$\cdots \longrightarrow \mathcal{X}_0(\ell^4) \longrightarrow \mathcal{X}_0(\ell^3) \longrightarrow \mathcal{X}_0(\ell^2) \longrightarrow \mathcal{X}_0(\ell) \longrightarrow \mathcal{X}_0(1)$$

de façon récursive à partir de la connaissance des premiers étages. Cette tour provient de l'inclusion des groupes :

$$\cdots \subset \Gamma_0(\ell^4) \subset \Gamma_0(\ell^3) \subset \Gamma_0(\ell^2) \subset \Gamma_0(\ell) \subset \Gamma_0(1)$$

Il y a donc pour tout $n \geqslant 1$ une projection $\pi_n : \mathcal{X}_0(\ell^n) \to \mathcal{X}_0(\ell^{n-1})$ qui est de degré $[\Gamma_0(\ell^{n-1}) : \Gamma_0(\ell^n)] = \mathrm{nrd}(l)$. Chacune des courbes $\mathcal{X}_0(\ell^n)$ a une involution d'Atkin-Lehner $w_n$. La construction de la tour se base sur la proposition suivante, prouvée dans [Duc13] §5.

**Proposition 4.1.1.** Pour $n \geqslant 1$, le diagramme suivant est commutatif.

$$\begin{array}{ccc} \mathcal{X}_0(\ell^{n+2}) & \xrightarrow{w_{n+1}\circ\pi_{n+2}\circ w_{n+2}} & \mathcal{X}_0(\ell^{n+1}) \\ \downarrow{\scriptstyle \pi_{n+2}} & & \downarrow{\scriptstyle \pi_{n+1}} \\ \mathcal{X}_0(\ell^{n+1}) & \xrightarrow{w_n\circ\pi_{n+1}\circ w_{n+1}} & \mathcal{X}_0(\ell^n) \end{array}$$

De plus, il vérifie la propriété universelle du produit fibré, on a donc :

$$\mathcal{X}_0(\ell^{n+2}) \simeq \mathcal{X}_0(\ell^{n+1}) \times_{\mathcal{X}_0(\ell^n)} \mathcal{X}_0(\ell^{n+1}).$$

Pour construire toute la tour, il suffit donc de connaître les courbes $\mathcal{X}_0(\ell)$ et $\mathcal{X}_0(\ell^2)$, leurs involutions d'Atkin-Lehner $w_1$ et $w_2$, ainsi que le revêtement $\pi_2 : \mathcal{X}_0(\ell^2) \to \mathcal{X}_0(\ell)$.

## 4.2. Reconnaissance de nombres algébriques

Comme les méthodes présentées par la suite reposent sur des calculs numériques approchés, nous aurons besoin d'identifier des nombres rationnels, voire algébriques, à partir de leur développement décimal. Voici deux méthodes qui permettent d'atteindre cet objectif.

### 4.2.1. Pour des nombres quadratiques : les fractions continues

Pour reconnaître un nombre dans un corps quadratique imaginaire $\mathbb{Q}(\sqrt{-D})$ fixé, on peut utiliser le développement en fractions continues. Notons

$$\tilde{x} := \tilde{a} + i\tilde{b}$$

un développement décimal tronqué du nombre à reconnaître. Il suffit alors d'identifier, à l'aide de la méthode des fractions continues implémentée en Magma par la fonction BestApproximation, les développements décimaux de $\tilde{a}$ et $\tilde{b}/\sqrt{D}$ comme des nombres rationnels $a$ et $b$ pour obtenir la forme exacte

$$x = a + b\sqrt{-D}.$$

### 4.2.2. Dans le cas général : LLL

Si l'on cherche à identifier un nombre algébrique $x$ d'un degré algébrique $d$ fixé, on peut essayer d'en obtenir un polynôme annulateur par approximation numérique. L'idée est la suivante : si on dispose d'une relation approchée

$$n(a_0 + a_1\tilde{x} + \cdots + a_d\tilde{x}^d) \approx 0$$

où $n, a_i \in \mathbb{Z}$ et $n \gg a_i$, alors $a_0 + a_1\tilde{x} + \cdots + a_d\tilde{x}^d$ est numériquement très petit, et on espère que $a_0 + a_1x + \cdots + a_dx^d = 0$.

Afin d'obtenir une telle relation, on utilise l'algorithme de réduction de réseaux LLL (Lenstra-Lenstra-Lovász, voir [LLL82]). Concrètement, on applique l'algorithme à la famille des lignes de la matrice suivante, en choisissant $n$ assez grand pour que les coefficients de la matrice soient entiers :

$$\begin{bmatrix} 1 & & & & n & 0 \\ & 1 & & & n\,\mathrm{Re}(\tilde{x}) & n\,\mathrm{Im}(\tilde{x}) \\ & & 1 & & n\,\mathrm{Re}(\tilde{x}^2) & n\,\mathrm{Im}(\tilde{x}^2) \\ & & & \ddots & \vdots & \vdots \\ & & & 1 & n\,\mathrm{Re}(\tilde{x}^d) & n\,\mathrm{Im}(\tilde{x}^d) \end{bmatrix}$$

et on obtient une combinaison linéaire à coefficients entiers $a_0, \ldots, a_d$ des lignes de la matrice, approximant un vecteur de longueur minimale du réseau engendré par celles-ci. Ceci signifie en particulier que les deux éléments du vecteur obtenu sont proches de 0 ; ce sont les parties réelle et imaginaire de $a_0 + a_1x + \cdots + a_dx^d$.

Cette méthode est déjà présente dans les versions récentes de Magma par le biais de la fonction MinimalPolynomial. Cependant, si l'on sait déjà dans quel corps de nombres le nombre cherché est censé se trouver, on peut raffiner cette méthode. En effet, si le corps de nombres est $\mathbb{Q}(s)$ où $s$ est de degré $d+1$ sur $\mathbb{Q}$ et a pour développement décimal tronqué $\tilde{s}$, on peut appliquer LLL à la matrice :

$$\begin{bmatrix} 1 & & & & n & 0 \\ & 1 & & & n\,\mathrm{Re}(\tilde{x}) & n\,\mathrm{Im}(\tilde{x}) \\ & & 1 & & n\,\mathrm{Re}(\tilde{s}) & n\,\mathrm{Im}(\tilde{s}) \\ & & & \ddots & \vdots & \vdots \\ & & & 1 & n\,\mathrm{Re}(\tilde{s}^d) & n\,\mathrm{Im}(\tilde{s}^d) \end{bmatrix}$$

afin d'obtenir une relation :

$$n\left(a\tilde{x} + a_0 + a_1\tilde{s} + \cdots + a_d\tilde{s}^d\right) \approx 0$$

avec $a, a_i \in \mathbb{Z}$, et de pouvoir en déduire une relation :

$$x = -\frac{1}{a}\left(a_0 + a_1 s + \cdots + a_d s^d\right) \in \mathbb{Q}(s).$$

## 4.3. Calcul d'équations de courbes à l'aide de séries entières

Ce travail est le début de la construction des premiers étages d'une tour de courbes de Shimura. Les courbes concernées proviennent d'une algèbre de quaternions $B$ sur le corps de nombres $\mathbb{Q}(\alpha)$ où $\alpha^3 - \alpha^2 - 2\alpha + 1 = 0$. L'algèbre de quaternions est la suivante :

$$B = \left(\frac{-1, -\alpha^2 + \alpha + 1}{\mathbb{Q}(\alpha)}\right).$$

La tour qui nous intéresse est la tour :

$$\cdots \longrightarrow \mathcal{X}_0(3^4) \longrightarrow \mathcal{X}_0(3^3) \longrightarrow \mathcal{X}_0(3^2) \longrightarrow \mathcal{X}_0(3) \longrightarrow \mathcal{X}_0(1)$$

de courbes provenant d'ordres d'Eichler de niveaux $3^n$. En particulier, nous étudierons $\mathcal{X}_0(3)$ et le quotient de $\mathcal{X}_0(9)$ par son involution d'Atkin-Lehner, que nous noterons $\mathcal{X}_0(9)^\star$.

### 4.3.1. Développements en série entière

Galbraith [Gal96] a été le premier à systématiser le calcul d'équations lisses pour les courbes modulaires classiques. Pour obtenir leurs équations, la méthode utilisée par Galbraith consiste à calculer numériquement des développements de formes différentielles holomorphes sur $X_0(N)$, qui s'identifient aux formes modulaires de poids 2 pour le groupe modulaire classique $\Gamma_0(N)$ (voir [DJ04, §1.1]). La théorie générale prédit notamment que les développements au voisinage du point à l'infini de $\mathcal{H}^\star$ (en puissances de $q = e^{2i\pi z}$), ont des coefficients *rationnels*. Une fois ces coefficients identifiés, on peut alors chercher des relations algébriques à coefficients rationnels entre ces formes différentielles et leurs dérivées. Dans ce travail on s'intéresse aux courbes admettant une équation hyperelliptique [Gal96, §4], laissant de côté le cas des plongements projectifs [Gal96, §3].

L'étude des courbes de Shimura est plus compliquée que celle des courbes modulaires classiques car elles n'ont pas de point privilégié – comme pouvait l'être le point à l'infini de $\mathcal{H}^\star$ – où les développements de formes modulaires seraient à coup sûr rationnels. La théorie de Shimura prédit toutefois que les points CM de $\mathcal{X}_0(N)$ sont à coordonnées dans des *petits corps de nombres imaginaires* et admettent des développements de formes modulaires à coefficients *algébriques* [VW14, th 2.5].

### 4.3.2. Équation de la courbe $\mathcal{X}_0(9)^\star$

On utilise la méthode du développement en série entière de formes différentielles. La dimension de l'espace des formes différentielles sur $\mathcal{X}_0(9)^\star$ a pour dimension le genre de la courbe, qui vaut 2. Il est connu (voir [Gal96] §4.1) que les bases de cet espace sont données par :

$$f = \frac{\mathrm{d}x}{y} \qquad \text{et} \qquad g = \frac{x\mathrm{d}x}{y}$$

où $x, y$ engendrent l'anneau des coordonnées de $\mathcal{X}_0(9)^\star$. On calcule donc d'abord une base $(f, g)$ de cet espace (sous forme de séries entières tronquées à un certain degré) grâce à la fonction PowerSeriesBasis implémentée en Magma par Voight et Willis [VW14]. On calcule ensuite $x = f/g$ et $y = x'/g$, puis on détermine une relation linéaire entre les séries entières tronquées $1, y^2, x, x^2, ..., x^6$, en calculant le noyau d'une matrice contenant leurs coefficients, afin d'obtenir une équation de la forme $y^2 = a_6x^6 + ... + a_1x + a_0$ pour la courbe. On obtient ainsi l'équation suivante pour $\mathcal{X}_0(9)^\star$ :

$$y^2 = x^6 + 84x^5 + 4876x^4 + 163296x^3 + \frac{8726544}{7}x^2 - 20500672x + \frac{10355021120}{49}$$

A l'aide de la fonction ReducedMinimalWeierstrassModel de Magma, on obtient l'équation simplifiée suivante de la courbe :

$$y^2 = 5x^6 + 26x^5 + 47x^4 + 40x^3 + 47x^2 + 26x + 5.$$

## 4.4. Décomposition de la jacobienne de $\mathcal{X}_0(9)^\star$

Une équation plus simple de la courbe est :

$$y^2 = 5x^6 + 26x^5 + 47x^4 + 40x^3 + 47x^2 + 26x + 5.$$

Elle dispose de deux involutions non hyperelliptiques, $\sigma_1$ et $\sigma_2 = \iota\sigma_1$ où

$$\sigma_1(x : y : z) = (z^3 : yz^6 : xz^2).$$

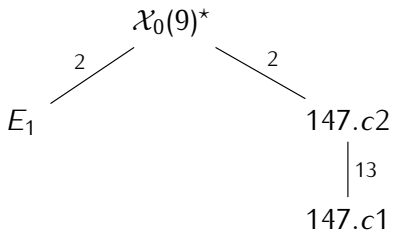
Notons $E_1 := \mathcal{X}_0(9)^\star/\sigma_1$ et $E_2 := \mathcal{X}_0(9)^\star/\sigma_2$ les quotients de $\mathcal{X}_0(9)^\star$ par ces involutions. Elles sont définies sur $\mathbb{Q}$ par les équations suivantes :

| | | |
|---|---|---|
| $E_1$ | $\mid$ | $y^2 = x^3 + 571536$ |
| $E_2$ | $\mid$ | $y^2 = x^3 - 148176x + 23856336$ (c'est la courbe 147.c2 de LMFDB) |

Par conséquent, la jacobienne de la courbe $C$ est (2,2)-décomposable, et il y a une isogénie de degré 4 :

$$J(\mathcal{X}_0(9)^\star) \longrightarrow E_1 \times E_2$$

de noyau $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. On vérifie ensuite avec Magma qu'il existe une isogénie de degré 13 entre les courbes 147.c2 et 147.c1. En résumé, la situation est donc la suivante.



Cette situation illustre bien la notion de revêtement optimal rencontrée en 2.1. Le revêtement de degré 26 $\mathcal{X}_0(9)^\star \to 147.c1$ n'est pas optimal puisqu'il se factorise par le revêtement non trivial $\mathcal{X}_0(9)^\star \to 147.c2$. Ce dernier est optimal car de degré premier.

## 4.5. Détermination des points CM

Comme annoncé en 3.2.1, les points CM sont les points fixes de transformations définies par des éléments d'extensions quadratiques totalement imaginaires de $K$. On choisit donc une extension $L$ de $K$ d'anneau des entiers $\mathbb{Z}_L$, puis un élément $\mu$ tel que $R[\mu] = \mathbb{Z}_L$. Puis on cherche les points fixes de l'image de $\mu$ dans $\Gamma_0(N)$ ; concrètement, avec Magma, on calcule :

FixedPoints(Gamma !mu,UpperHalfPlane()).

Ceci renvoie une liste de valeurs numériques approchées (à une précision fixée au préalable) de points fixes ; comme ils sont algébriques, il faut ensuite en reconnaître un polynôme minimal ou une expression exacte par les procédés décrits en 4.2.

# Conclusion

## Revêtements de courbes elliptiques

Le premier objectif était d'étudier les revêtements de genre 2 d'une courbe elliptique $E$ définie sur $\mathbb{Q}(\sqrt{2})$, ramifiés uniquement au-dessus d'un point de la courbe $E$. Dans ce but, nous avons étudié le revêtement $\mathbb{P}^1 \to \mathbb{P}^1$ qu'il induit (2.2), puis calculé sur un exemple les 3 revêtements possibles (2.4).

## Tours de courbes

Le travail mené est le début de la construction d'une tour de courbes :

$$\cdots \longrightarrow \mathcal{X}_0(3^4) \longrightarrow \mathcal{X}_0(3^3) \longrightarrow \mathcal{X}_0(3^2) \longrightarrow \mathcal{X}_0(3) \longrightarrow \mathcal{X}_0(1)$$

comme exposé en 4.1.

### Ce qui a été fait

On essaie de construire en premier lieu le revêtement $\mathcal{X}_0(9)^\star \to \mathcal{X}_0(3)$, où $\mathcal{X}_0(9)^\star$ est un quotient de degré 2 de $\mathcal{X}_0(9)$. Le premier objectif était d'obtenir une équation de la courbe $\mathcal{X}_0(9)^\star$ à l'aide de développements en série entière de formes modulaires sur la courbe comme décrit en 4.3.1. Après simplification avec Magma, l'équation de cette courbe est :

$$y^2 = 5x^6 + 26x^5 + 47x^4 + 40x^3 + 47x^2 + 26x + 5.$$

Comme on sait qu'il y a un revêtement $\mathcal{X}_0(9)^\star \to \mathcal{X}_0(3)$, la théorie exposée en 2.1 montre que la courbe $\mathcal{X}_0(3)$ est un facteur de la jacobienne de $\mathcal{X}_0(9)^\star$. Nous avons donc décomposé cette jacobienne en 4.4.

### Ce qu'il reste à faire

La construction de l'étage suivant de la tour nécessite de déterminer une équation de $\mathcal{X}_0(9)$ et du revêtement $\mathcal{X}_0(9)^\star \to \mathcal{X}_0(9)$. Pour cela, il faudra en premier lieu déterminer les points CM (4.5) dont nous n'avons pas pour l'instant réussi à trouver une expression exacte ou un polynôme minimal. La suite de la construction se fera de façon récursive à l'aide du produit fibré décrit en 4.1.

# Bibliographie


[AB04] M. Alsina and P. Bayer. *Quaternion orders, quadratic forms, and Shimura curves*. American Mathematical Society, 2004.

[BJS+16] A.R. Booker, J.Sijsling, A.V. Sutherland, J. Voight, and D.Yasaki. A database of genus 2 curves over the rational numbers. *LMS Journal of Computation and Mathematics*, 2016.

[Cla03] P. Clark. *Rational Points on Atkin-Lehner Quotients of Shimura Curves*. PhD thesis, Harvard University, 2003.

[CMSV17] E. Costa, N. Mascot, J. Sijsling, and J. Voight. Rigorous computation of the endomorphism ring of a Jacobian. `https://arxiv.org/abs/1705.09248`, 2017.

[Col13] The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2013.

[DJ04] F. Diamond and J.Shurman. A first course in modular forms. *Springer*, 2004.

[Dju17] M. Djukanovic. *Split jacobians and lower bounds on heights*. PhD thesis, Leiden University, 2017.

[dP13] G. di Piazza. Arithmetic on jacobians of algebraic curves. Master's thesis, Université de Bordeaux, 2013.

[Duc13] V. Ducet. *Construction of curves with many rational points over finite fields*. PhD thesis, Aix-Marseille Université, 2013.

[Elk97] N.D. Elkies. Explicit modular towers. *Proceedings of the Thirty-fifth annual Allerton conference on communication, control and computing*, 1997.

[Elk98] N.D. Elkies. Shimura curve computations. *Algorithmic Number Theory Symposium Proceedings*, 1998.

[Elk06] N.D. Elkies. Shimura curves arising from the (2,3,7) triangle group. *Algorithmic Number Theory Symposium Proceedings*, 2006.

[FK89] G. Frey and E. Kani. *Arithmetic Algebraic geometry*, chapter Curves of genus 2 covering elliptic curves and an arithmetical application. Springer, 1989.

[Gal96] S.D. Galbraith. *Equations For Modular Curves*. PhD thesis, University of Oxford, 1996.

[Gal12] S.D. Galbraith. *Mathematics of public key cryptography*, chapter Hyperelliptic Curves. Cambridge University Press, 2012.

[Hos16] T. Hosgood. An introduction to varieties in weighted projective space. https ://arxiv.org/pdf/1604.02441.pdf, 2016.

[KMSV14] M. Klug, M. Musty, S. Schiavone, and J. Voight. Numerical computation of three-point covers of the projective line. *LMS Journal of Computation and Mathematics*, 2014.

[Kuh88] R.M. Kuhn. Curves of genus 2 with split jacobian. *Transactions of the American Mathematical Society*, 307 :41–49, 1988.

[LLL82] A.K. Lenstra, H.W. Lenstra, and L. Lovasz. Factoring polynomials with rational coefficients. *Mathematische Annalen*, pages 513–534, 1982.

[Mil08] J. Milne. Abelian varieties. https ://www.jmilne.org/math/CourseNotes/AV.pdf, 2008.

[Mil18] J. Milne. Jacobian varieties. https ://www.jmilne.org/math/xnotes/JVs.pdf, 2018.

[Mir95] R. Miranda. *Algebraic Curves and Riemann surfaces*. American Mathematical Society, 1995.

[Ser88] J.-P. Serre. *Algebraic groups and class fields*. Springer, 1988.

[Sha04] T. Shaska. Genus 2 fields with degree 3 subfields. *Forum Mathematicum*, 16 :263–280, 2004.

[Sha05] T. Shaska. Genus two curves covering elliptic curves : a computational approach. *Lecture Notes in Computation*, 13 :151–195, 2005.

[Sij13] J. Sijsling. Canonical models of arithmetic $(1; e)$-curves. *Mathematische Zeitschrift*, 2013.

[Sil09] J. Silverman. *The arithmetic of elliptic curves*. Springer, 2009.

[Smi16] B. Smith. Genus 2 curves for cryptography : progress and problems. http ://www.lorentzcenter.nl/lc/web/2016/834/presentations/Smith, 2016.

[TVT82] M.A. Tsfasman, S.G. Vlăduţ, and T.Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Mathematische Nachrichten*, (109) :21–28, 1982.

[Vig95] M.-F. Vignéras. *Arithmétique des algèbres de quaternions*. Springer, 1995.

[Voi09a] J. Voight. Computing cm points on shimura curves arising from cocompact arithmetic triangle groups. *Algorithmic Number Theory Symposium Proceedings*, 2009.

[Voi09b] J. Voight. Computing fundamental domains for Fuchsian groups. *Journal de Théorie des Nombres de Bordeaux*, 2009.

[Voi09c] J. Voight. Shimura curves of genus at most two. *Mathematics of Computation*, 2009.

[Voi18] J. Voight. Quaternion algebras. https ://math.dartmouth.edu/ jvoight/quatbook.pdf, 2018.

[VW14] J. Voight and J. Willis. *Computations with Modular Forms*, chapter Computing Power Series Expansions of Modular Forms. Springer International Publishing, 2014.