Calculs explicites avec les surfaces abéliennes

Lassina Dembélé

École d'été 2021 des jeunes chercheurs et jeunes chercheuses en théorie des nombres (JC2A)

23 - 27 août 2021

1 Introduction

Dans ces notes, nous décrivons quelques méthodes explicites pour calculer avec les surfaces abéliennes. Les approches que nous utilisons sont basées sur les deux outils suivants : La conjecture d'Eichler-Shimura sur les corps totalement réels et les équations explicites pour les surfaces modulaires de Hilbert. Plusieurs de nos exemples sont tirés du papier conjoint de l'auteur de ces notes avec A. Kumar [11].

2 Courbes elliptiques

2.1 Définition des courbes elliptiques

Soit k un corps commutatif. Une *courbe elliptique* E définie sur k, est une cubique non-singulière donnée par une équation de Weierstrass

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

avec $a_1, a_2, a_3, a_4, a_6 \in k$. On peut exprimer la lissité (ou non-singularité) de E en terme de la non-nullité du discriminant Δ_E qui est une polynôme en a_1, a_2, a_3, a_4, a_6. On réfère à [38, Chap. III] pour la définition de Δ_E et autres invariants, tous exprimés en termes des a_i.

Lorsque $\mathrm{car}(k) = 0$, on peut écrire E sous la forme

$$E : \ y^2 = x^3 + ax + b,$$

avec $a, b \in k$. Dans ce cas, $\Delta_E = -16(4a^3 + 27b^2)$ et E est une courbe elliptique $\iff$ $\Delta_E \neq 0$. L'ensemble des points de E est

$$E(\overline{k}) = \{(x, y) \in \overline{k} : y^2 = x^3 + ax + b\} \sqcup \{\infty\},$$

où ∞ est l'unique point à l'infini sur la fermeture projective de E. E admet alors une structure de groupe algébrique dont l'élément neutre est ∞. La beauté et l'attrait des courbes elliptiques en théorie des nombres aussi bien qu'en cryptographie viennent du fait qu'elles possèdent une structure de groupe à la fois simple et sophistiquée définie par la méthode des *cordes et tangentes*, datant de la Grèce ancienne (voir la Figure 1 pour illustration).

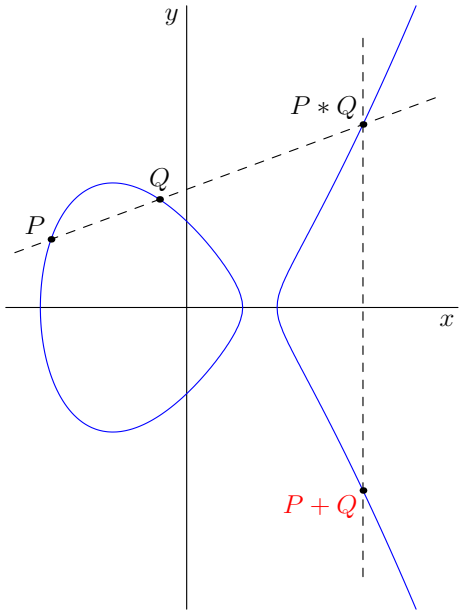


FIGURE 1 – Loi d'addition d'une courbe elliptique

2.2 La L-série d'une courbe elliptique

Soit F un corps de nombres et $\mathcal{O}_F$ l'anneau des entiers de F. Soit E une courbe elliptique définie sur F. Le *conducteur* de E est un idéal entier $\mathfrak{N}$ ayant les mêmes diviseurs premiers que Δ_E. C'est un invariant arithmétique assez délicat dont la définition exacte est au delà de ces notes. Pour en savoir plus, nous référons [38, Chap. VIII]. Pour un idéal premier $\mathfrak{p} \nmid \mathfrak{N}$, soit $\widetilde{E}_\mathfrak{p}$ la réduction de E modulo $\mathfrak{p}$. On voit que c'est une courbe elliptique définie sur $\mathbf{F}_\mathfrak{p} = \mathcal{O}_F/\mathfrak{p}$. On définit la quantité

$$a_\mathfrak{p} := \mathrm{N}\mathfrak{p} + 1 - \#\widetilde{E}_\mathfrak{p}(\mathbf{F}_\mathfrak{p}).$$

Cette définition peut être étendue aux idéaux premiers $\mathfrak{p} \mid \mathfrak{N}$; on obtient alorss $a_\mathfrak{p} \in \{-1, 0, 1\}$ dépendant du type de réduction de E modulo $\mathfrak{p}$. La L-série de E est définie par

$$L(E,s) := \prod_{\mathfrak{p}\mid\mathfrak{N}} \left(1 - a_\mathfrak{p}\mathrm{N}\mathfrak{p}^{-s}\right)^{-1} \prod_{\mathfrak{p}\nmid\mathfrak{N}} \left(1 - a_\mathfrak{p}\mathrm{N}\mathfrak{p}^{-s} + \mathrm{N}\mathfrak{p}^{1-2s}\right)^{-1}.$$

Celle-ci converge pour $\mathrm{Re}(s) > 3/2$. (Voir [38].)

2.3 Uniformisation des courbes elliptiques

Dans cette sous-section, on suppose que $k = \mathbf{C}$.
Un *réseau* $\Lambda \subset \mathbf{C}$ est un sous-ensemble

$$\Lambda := \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 = \{a\omega_1 + b\omega_2 : a, b \in \mathbf{Z}\},$$

où $\omega_1, \omega_2 \in \mathbf{C}$ sont linéairement indépendants sur $\mathbf{R}$. On peut montrer que $\Lambda \subset \mathbf{C}$ est un réseau si et seulement si les deux conditions suivantes sont satisfaites :

— Λ est un sous-groupe de $\mathbf{C}$ isomorphe à $\mathbf{Z} \times \mathbf{Z}$,
— Λ est discret : c'est-à-dire, pour $0 < r < \min\{|\omega_1|, |\omega_2|\}$ et $D(0,r) = \{z \in \mathbf{C} : |z| < r\}$, on a $D(0,r) \cap \Lambda = \{0\}$. Ainsi, pour tout $\omega \in \Lambda$, $\omega + D(0,r) = D(\omega, r)$ et $D(\omega, r) \cap \Lambda = \{\omega\}$.

Soit $\Lambda \subset \mathbf{C}$ un réseau. La *$\wp$-fonction de Weierstrass* $\wp_\Lambda(z)$ attachée à Λ est définie par

$$\wp_\Lambda(z) := \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right). \tag{1}$$

On a le théorème suivant.

Théorème 2.1. *Soient $\Lambda \subset \mathbf{C}$ un réseau et $\wp_\Lambda(z)$ la $\wp$-fonction de Weierstrass associée. Alors, on a*

a) $\wp_\Lambda(z)$ est paire, méromorphe *et a un* pole double *en chaque $\omega \in \Lambda$.*

b) $\wp_\Lambda(z+\omega) = \wp_\Lambda(z)$, pour $z \in \mathbf{C}$ (doublement périodique).

Pour un réseau $\Lambda \subset \mathbf{C}$, on pose

$$E_\Lambda : y^2 = 4x^3 - g_2 x - g_3,$$

avec $g_2 = 60G_4, g_3 = 140G_6$. On peut montrer que $16(g_2^3 - 27g_3^2) \neq 0$, c'est-à-dire que E_Λ est une courbe elliptique.

Théorème 2.2. *Soient $\Lambda \subset \mathbf{C}$ un réseau, $\wp_\Lambda(z)$ la $\wp$-fonction de Weierstrass associée, et E_Λ la courbe ci-dessus. Alors, l'application*

$$\begin{aligned} \phi : \mathbf{C}/\Lambda &\to E_\Lambda(\mathbf{C}) \\ z + \Lambda &\mapsto \begin{cases} (\wp_\Lambda(z), \wp'_\Lambda(z)), & z \notin \Lambda, \\ \infty, & \textit{sinon}, \end{cases} \end{aligned}$$

est une isomorphisme de groupes (de Lie).

Réciproquement, toute courbe elliptique E sur $\mathbf{C}$ s'obtient de cette façon.

En posant $c_4 = 12g_2$ et $c_6 = 216g_3$, on peut réécrire l'équation de la courbe comme

$$y^2 = x^3 - 27c_4 x - 54c_6.$$

2.4 Formes modulaires classiques

On rappelle que le demi-plan supérieur de Poincaré est défini par :

$$\mathfrak{H} := \{\tau \in \mathbf{C} : \mathrm{Im}(\tau) > 0\}.$$

On fixe un entier $N \geq 1$ et on pose

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) : N \mid c \right\}.$$

On pose également $\mathfrak{H}^* = \mathfrak{H} \cup \mathbf{P}^1(\mathbf{Q})$. On rappelle que $\mathrm{GL}_2^+(\mathbf{R})$, le groupe des matrices 2×2 inversibles de déterminant strictement positif, agit sur $\mathfrak{H}$ par

$$\gamma\tau = \frac{a\tau + b}{c\tau + d}, \ \tau \in \mathfrak{H} \text{ et } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbf{R}).$$

Une *forme modulaire de niveau N* et *de poids* 2 est une fonction holomorphe $f : \mathfrak{H} \to \mathbf{C}$ qui satisfait aux conditions suivantes :

(a) $f(\gamma\tau) = (c\tau + d)^2 f(\tau)$, pour tout $\tau \in \mathfrak{H}$ et $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$.

(b) Pour tout $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Q})$, $(c\tau + d)^{-2} f(\gamma\tau)$ admet une expansion de Puiseux

$$(c\tau + d)^{-2} f(\gamma\tau) = a_0 + \sum_{n=1}^{\infty} a_n q^n,$$

où $q = e^{2\pi i \tau}$.

On dit que f est *cuspidale* si $a_0 = 0$ pour tout $\gamma \in \mathrm{SL}_2(\mathbf{Q})$ dans (b). On note $S_2(N)$ l'ensemble des formes cuspidales de niveau N et de poids 2. C'est un $\mathbf{C}$-espace vectoriel de dimension finie g.

Pour tout premier $p \nmid N$, on définit l'*opérateur de Hecke* agissant sur $S_2(N)$ par

$$T_p f(\tau) = f(p\tau) + \frac{1}{p} \sum_{i=0}^{p-1} f\left(\frac{\tau + i}{p}\right).$$

On étend cette définition à tous les entiers $m \geq 1$ tels que $\gcd(m, N) = 1$ comme suit :

— Pour tout premier p et tout entier $s \geq 1$, $T_{p^{s+1}} = T_p T_{p^s} - \delta_p p T_p^{s-1}$, avec $\delta_p = 1$, si $p \parallel N$, et $\delta_p = 0$, si $p^2 \mid N$.

— Pour tous entiers $m, n \geq 1$ tels que $\gcd(m, n) = 1$, $T_{mn} = T_m T_n$.

On définit l'*algèbre de Hecke* $\mathbf{T}$ comme étant la $\mathbf{Z}$-sous-algèbre de $\mathrm{End}(S_2(N))$ engendrée par les T_n avec $\gcd(n, N) = 1$. C'est une algèbre commutative diagonalisable. Elle admet donc une base de vecteurs propres communs. On appelle *forme propre* tout élément $f(\tau) = \sum_{n \geq 1} a_n q^n \in S_2(N)$ qui est un vector propre commun non-nul de $\mathbf{T}$. Dans ce cas, on montre qu'il existe $c \in \mathbf{C}^\times$ tel que

$$T_n f = c a_n f, \text{ pour tout } n \geq 1 \text{ tel que } \gcd(n, N) = 1.$$

On dit alors que f est une forme propre *normalisée* si $c = 1$. Dans ce cas on a

$$T_n f = a_n f, \text{ pour tout } n \geq 1 \text{ tel que } \gcd(n, N) = 1.$$

Remarquons que, pour tous $M \mid N$ et $d \mid N/M$, et $f \in S_2(M)$, la fonction $\tau \mapsto f(d\tau)$ appartient à $S_2(N)$. Cela permet de définir une inclusion $\iota_d : S_2(M) \hookrightarrow S_2(N)$. On appelle *sous-espace ancien de* $S_2(N)$ le sous-espace engendré par les images de tous les ι_d et on le note $S_2(N)^{\mathrm{old}}$. Le complément de $S_2(N)^{\mathrm{old}}$ par rapport au produit scalaire de Petersson est appelé *sous-espace nouveau* ; il est noté $S_2(N)^{\mathrm{new}}$. Donc, on a

$$S_2(N) = S_2(N)^{\mathrm{old}} \oplus \left(S_2(N)^{\mathrm{old}}\right)^{\perp} = S_2(N)^{\mathrm{old}} \oplus S_2(N)^{\mathrm{new}}.$$

Une *forme nouvelle* $f \in S_2(N)$ est une forme propre normalisée qui appartient à $S_2(N)^{\mathrm{new}}$.

Lemme 2.3. *Soit $f \in S_2(N)$ une forme propre normalisée et $\sigma \in \mathrm{Hom}(K_f, \mathbf{C})$. Alors $f^\sigma(\tau) := \sum_{n=1}^{\infty} a_n^\sigma q^n$ est une forme propre normalisée de niveau N et de poids 2. Si f est une forme nouvelle, alors il en est ainsi pour f^σ.*

Démonstration. Voir [13, Chap. 6]. □

On peut ainsi définir une relation d'équivalence sur l'ensembles des formes propres normalisée par

$$f \sim f' \iff \text{il existe } \sigma \in \mathrm{Aut}(\mathbf{C}) \text{ tel que } f' = f^\sigma.$$

On note $[f]$ la classe de f et on l'appelle l'*orbite de Hecke* de f.

Corollaire 2.4. *Il existe une base de $S_2(N)$ donnée par des formes à coefficients rationnels.*

Démonstration. Voir [13, Chap. 6]. □

2.5 La variété abélienne associée à une forme nouvelle

Soit $X_0(N)$ la courbe modulaire de niveau N. On sait que $X_0(N)$ est une courbe algébrique définie sur $\mathbf{Q}$. Soit $J_0(N)$ la Jacobienne de $X_0(N)$. C'est une courbe de genre g. On peut définir la Jacobienne comme étant

$$J_0(N)(\mathbf{C}) = S_2(N)^\vee / \mathrm{H}_1(X_0(N), \mathbf{Z}),$$

où $\mathrm{H}_1(X_0(N), \mathbf{Z})$ est le groupe d'homologie et $S_2(N)^\vee = \left(\Omega^1_{X_0(N)}\right)^\vee = \mathrm{Hom}(\Omega^1_{X_0(N)}, \mathbf{C})$. On voit alors que $\mathrm{H}_1(X_0(N), \mathbf{Z})$ correspond à un réseau Λ_g de rank $2g$ dans $S_2(N)^\vee$. On a donc

$$J_0(N)(\mathbf{C}) = \mathbf{C}^g / \Lambda_g.$$

Le groupe $\mathrm{H}_1(X_0(N), \mathbf{Z})$ peut être décrit en termes des *symboles modulaires*. Pour obtenir le réseau, on choisit une base $f_1, \ldots, f_g$ de $S_2(N)$ comme dans le Corollaire 2.4 et une base $\delta_1, \ldots \delta_{2g}$ de $\mathrm{H}_1(X_0(N), \mathbf{Z})$. Alors, on a $\Lambda_g = \langle \delta_j, \omega_i \rangle$, avec $\omega_i = 2\pi i f_i(\tau) d\tau$.

Soit $f \in S_2(N)$ une forme propre normalisée, alors il existe un homomorphism d'anneaux $\lambda_f : \mathbf{T} \to \mathbf{C}$ déterminé par le fait que $Tf = \lambda_f(T) f$. Posons

$$I_f := \mathrm{Ann}_{\mathbf{T}}(f) = \{T \in \mathbf{T} : Tf = 0\} = \ker(\lambda_f).$$

Alors on a

$$\mathbf{T}/I_f \simeq \mathcal{O}_f = \mathbf{Z}[\{a_n(f)\}].$$

Let corps $K_f = \mathbf{Q}(\{a_n(f)\})$ est appelé le *corps des coefficients de f*. Il est le corps des fractions de $\mathcal{O}_f$. Si $f \in S_2(N)$ est une forme nouvelle, la *variété abélienne associée à f* est définie par

$$A_f := J_0(N)/I_f J_0(N).$$

Par les travaux de Shimura, on sait que A_f est une variété abélienne de dimension $[K_f : \mathbf{Q}]$ définie sur $\mathbf{Q}$ et que $\mathcal{O}_f \subseteq \mathrm{End}_{\mathbf{Q}}(A_f)$.

Sur $\mathbf{C}$, on peut décrire A_f comme suit. Posons

$$V_f = \mathrm{span}([f]) \subset S_2(N).$$

Par restriction du sous-groupe $\mathrm{H}_1(X_0(N), \mathbf{Z})$ de $S_2(N)^\vee$ aux fonctions de V_f, on obtient un sous-groupe du dual $V_f^\vee$ donné par

$$\Lambda_f = \mathrm{H}_1(X_0(N), \mathbf{Z})|_{V_f}.$$

On peut montrer que

$$A_f(\mathbf{C}) = V_f^\vee / \Lambda_f.$$

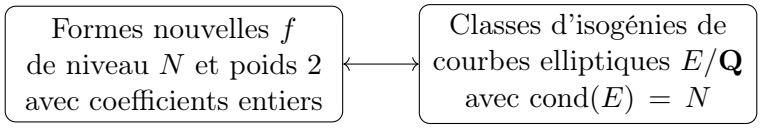
Le réseau Λ_f est le sous-groupe de symboles modulaires attaché à f. On peut le calculer assez facilement, et cela permet de déterminer le réseau des périodes de A_f.

3 Courbes elliptiques sur Q

3.1 Construction d'Eichler-Shimura et modularité des courbes elliptiques

Théorème 3.1. *Il existe une application $f \mapsto E_f$ de l'ensemble des formes nouvelles f de niveau N et de poids 2, à coefficients entiers, à l'ensemble des courbes elliptiques de conducteur N définies sur $\mathbf{Q}$, telle que $L(f,s) = L(E_f,s)$. Cette application induit une bijection sur l'ensemble des classes isogénies.*

Le Théorème 3.1 se résume par le diagramme ci-dessous :



L'application $f \mapsto E_f$ s'appelle la *construction d'Eichler-Shimura pour les courbes elliptiques*. Par le théorème des isogénies de Faltings, deux courbes elliptiques isogènes partagent la même fonction L. Ainsi, dire que l'application ci-dessus induit une bijection revient à dire que chaque classe d'isogénie contient une courbe elliptique E_f de conducteur N provenant d'une forme nouvelle $f \in S_2(N)^{\mathrm{new}}$, à coefficients entiers.

3.2 Exemple : calculs avec les symboles modulaires

```
> SetDefaultRealFieldPrecision(300);
> QQ := Rationals();
> PolsQQ<x> := PolynomialRing(QQ);
> M := CuspForms(73);
> N := Newforms(M);
> f := N[1][1];
> Mf := ModularSymbols(f);
> Mf;
Modular symbols space for Gamma_0(73) of weight 2 and dimension 2 over Rational Field
> Basis(Mf);
[
    {-1/48, 0} + -2*{-1/12, 0} + 2*{-1/18, 0} + -1*{-1/24, 0} + 2*{-1/36, 0},
    {-1/57, 0} + -1*{-1/12, 0} + {-1/29, 0} + {-1/18, 0} + -1*{-1/24, 0} + {-1/36, 0}
]
> Pf := Periods(Mf, 3000);
> tau := Pf[2][1]/Pf[1][1];
> jtau := jInvariant(tau);
> PolsQQ!MinimalPolynomial(jtau, 1);
5329*x - 6128487
> j := Roots(PolsQQ!MinimalPolynomial(jtau, 1))[1][1];
> j;
6128487/5329
> Pf := [ Pf[1][1], Pf[2][1] ];
> EllipticCurveFromPeriods(Pf);
```

```
Elliptic Curve defined by y^2 + x*y = x^3 - x^2 + 4*x - 3 over Rational Field
```

4 Surfaces abéliennes

4.1 Construction d'Eichler-Shimura et modularité

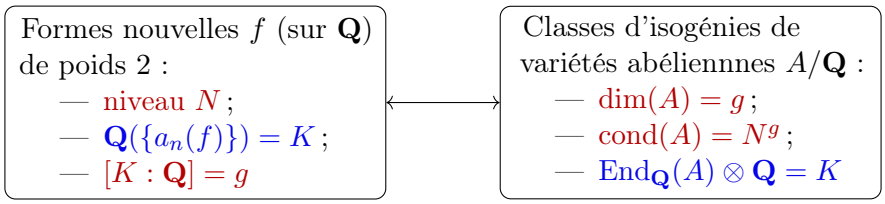
Soit A une variété abélienne de dimension g définie sur $\mathbf{Q}$. On dit que A est de *type* GL_2 s'il existe un corps de nombres K de degré g tel que $\mathrm{End}_{\mathbf{Q}}(A)$ est un ordre dans K, c'est-à-dire tel que $\mathrm{End}_{\mathbf{Q}}(A) \otimes \mathbf{Q} = K$.

Théorème 4.1. *Soit $K/\mathbf{Q}$ un corps totalement réel de degré g. Alors, il existe une application $f \mapsto A_f$ de l'ensemble des formes nouvelles $f \in S_2(N)$, avec $K_f = K$, à l'ensemble des variétés abéliennes de type GL_2 et de conducteur N^g, avec $\mathrm{End}_{\mathbf{Q}}(A) \otimes \mathbf{Q} = K$, telle que*

$$L(A_f, s) = \prod_{\tau \in \mathrm{Hom}(K_f, \overline{\mathbf{Q}})} L(f^\tau, s).$$

Cette application induit une bijection sur l'ensemble des classes d'isogénies.

Comme précédemment, le Théorème 4.1 se résume par le diagramme suivant :



Le Théorème 4.1 généralise clairement le Théorème 3.1. Comme dans le cas des courbes elliptiques, l'application $f \mapsto A_f$ est un théorème connu sous le nom de *construction d'Eichler-Shimura* sur $\mathbf{Q}$. Le fait qu'elle soit une bijection sur les classes d'isogénies est une conséquence de la conjecture de Serre sur $\mathbf{Q}$. Cette dernière est maintenant un théorème grâce aux travaux de Khare et Wintenberger [25].

4.2 Surfaces abéliennes principalement polarisées

En général, il n'est pas facile de calculer la variété abélienne A_f associée à la forme nouvelle f dans le Théorème 4.1. Par contre, lorsque A_f est une surface abélienne principalement polarisée, il existe des méthodes pour calculer sa classe d'isogénie. La méthode que nous allons maintenant décrire, passe par les invariants d'Igusa et utilise la paramétrisation de Rosenhain.

Soit f une forme nouvelle à coefficients dans un corps quadratique réel K_f et A_f la surface abélienne associée à f. On suppose que A_f est principalement polarisée. Soit $\Omega = (\Omega_1 | \Omega_2)$ la matrice des périodes associée à A_f. On peut calculer Ω à partir de V_f et Λ_f. Soit $Z = \Omega_1^{-1}\Omega_2$ la matrice des périodes normalisée de A_f.

Lemme 4.2. *Soit $h \in \mathbf{Q}[x]$ un polynôme de degré 5 ou 6 tel que A_f soit la Jacobienne de la courbe $C : y^2 = h(x)$. Alors les racines de h ne dépendent que de Z.*

Démonstration. Ceci est une autre façon de dire que la classe d'isomorphisme de A_f ne dépend que de Z. On peut exprimer les racines de h en termes des "nullwertes". Voir [24]. □

Lemme 4.3 (Rosenhain). *Soient A une surface abélienne principalement polarisé et Z sa matrice des périodes normalisée de Riemann. Alors, il existe une courbe $C' : y^2 = x(x-1)h'(x)$ telle que $A' = \mathrm{Jac}(C')$ soit isomorphe à A. Le polynôme h' est uniquement déterminé par Z.*

La paramétrisation de Rosenhain permet donc de calculer *a priori* les invariants d'Igusa ou d'Igusa-Clebsch qui déterminent la classe d'isomorphisme de A.

4.3 Exemples : calculs avec les symboles modulaires

Nous allons maintenant illustrer la discussion précédente avec quelques exemples. Pour cela on prend $N = 73$. L'espace $S_2(73)^{\mathrm{new}}$ est de dimension 5 et se décompose trois orbites de Hecke :

$$\begin{aligned}
f &= q + q^2 - q^4 + 2q^5 + 2q^7 - 3q^8 + O(q^9);\\
g &= q - \frac{\sqrt{5}+3}{2}q^2 + \frac{\sqrt{5}-3}{2}q^3 + \frac{3\sqrt{5}+3}{2}q^4\\
&\quad - \frac{\sqrt{5}+3}{2}q^5 + q^6 - 3q^7 - (2\sqrt{5}+3)q^8 + O(q^9);\\
h &= q + \frac{\sqrt{13}+1}{2}q^2 + \frac{-\sqrt{13}+1}{2}q^3 + \frac{\sqrt{13}+3}{2}q^4\\
&\quad - \frac{\sqrt{13}+1}{2}q^5 - 3q^6 - q^7 + 3q^8 + O(q^9).
\end{aligned}$$

Les variétés abéliennes associées à ses formes sont disponibles au `lmfdb.org`. La courbe elliptique associée à f a été décrite plus haut mais elle peut-être aussi calculer avec l'algorithme dans [8]. Maintenant intéressons nous aux surfaces attachées aux formes g et h.

D'abord, on calcule une base une base du groupe d'homologie $H_1(A_g, \mathbf{Z})$ en utilisant les symboles modulaires.

$$\begin{aligned}
\delta_1' &:= \{-1/48, 0\} - \{-1/24, 0\} + \{-1/36, 0\},\\
\delta_2' &:= \{-1/57, 0\} - \{-1/41, 0\} - \{-1/18, 0\} + \{-1/36, 0\},\\
\delta_3' &:= \{-1/62, 0\} - \{-1/52, 0\} + \{-1/18, 0\},\\
\delta_4' &:= \{-1/12, 0\} + \{-1/18, 0\} - \{-1/24, 0\}
\end{aligned}$$

La matrice d'intersection par rapport à cette base est

$$\begin{pmatrix} 0 & 0 & 0 & 2\\ 0 & 0 & 2 & -2\\ 0 & -2 & 0 & 0\\ -2 & 2 & 0 & 0 \end{pmatrix}$$

En calculant la forme alternée de Frobenius, on a

$$\begin{pmatrix} 0 & 0 & 2 & 0\\ 0 & 0 & 0 & 2\\ -2 & 0 & 0 & 0\\ 0 & -2 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0\\ 1 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 2\\ 0 & 0 & 2 & -2\\ 0 & -2 & 0 & 0\\ -2 & 2 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0\\ 1 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0 \end{pmatrix}^t$$

On voit que la variété abélienne A_g a une polarisation principale $(2,2)$. Comme A_g est de dimension 2, elle est donc isogène à la Jacobienne d'une courbe de genre 2. Le change de base

$$\begin{pmatrix}\delta_1\\ \delta_2\\ \delta_3\\ \delta_4\end{pmatrix} = \begin{pmatrix}1 & 1 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}\begin{pmatrix}\delta'_1\\ \delta'_2\\ \delta'_3\\ \delta'_4\end{pmatrix},$$

donne la base symplectique

$$\begin{aligned}
\delta_1 &:= \{-1/48,0\} - \{-1/24,0\} + \{-1/36,0\},\\
\delta_2 &:= \{-1/48,0\} + \{-1/62,0\} - \{-1/52,0\} + \{-1/18,0\} - \{-1/24,0\} + \{-1/36,0\},\\
\delta_3 &:= \{-1/57,0\} - \{-1/41,0\} - \{-1/18,0\} + \{-1/36,0\},\\
\delta_4 &:= \{-1/12,0\} + \{-1/18,0\} - \{-1/24,0\}.
\end{aligned}$$

On calcule une base intégrale de $H^1(A_g, \mathbf{C})$ à partir de l'orbite de Hecke g, on intègre cette base contre celle de $H_1(A_g, \mathbf{Z})$ pour obtenir la matrices des périodes $\Omega := (\Omega_1|\Omega_2)$, avec

$$\begin{aligned}
\Omega_1 &:= \begin{pmatrix}1.41...i & -7.18... + 0.70...i\\ -2.49...i & -4.41... - 1.24...i\end{pmatrix},\\
\Omega_2 &:= \begin{pmatrix}-2.76... + 3.37...i & -5.32...i\\ 1.65... + 0.70...i & -3.90...i\end{pmatrix}.
\end{aligned}$$

En utilisant le Théorème de Torelli, on recouvre la courbe C_g dont la Jacobienne est A_g. Pour cela, on calcule d'abord la matrice des périodes normalisée de Riemann, ensuite on calcule les invariants d'Igusa-Clebsch en utilisant le modèle de Rosenhain. Cela nous permet alors d'obtenir une première courbe hyperelliptique que l'on réduit pour obtenir la courbe

$$C'_g : y^2 = -x^6 - 2x^5 - x^4 - 6x^3 - 2x^2 + 4x - 1,$$

de laquelle on déduit le modèle minimal

$$C_g : y^2 + (x^3 + x^2 + 1)y = x^3 - x$$

dont la Jacobienne a RM par $\mathbf{Z}[\frac{1+\sqrt{5}}{2}]$.

De façon similaire, on obtient le modèle minimal

$$C_h : y^2 + (x^3 + x^2 + 1)y = -x^6 - 3x^5 + 2x^4 + 6x^3 - 10x^2 - 3x + 1$$

associé à la forme h dont la Jacobienne A_h a RM par $\mathbf{Z}[\frac{1+\sqrt{13}}{2}]$.

Dans [24, 22], il est décrit un meilleur algorithme pour calculer les courbes C_g et C_h. Malheureusement, il n'y a pas encore une implémentation connue de cet algorithme.

5 Formes modulaires de Hilbert

On fixe un corps de nombres totalement réel F de degré $d > 1$ et de nombre de classes étroites un. On note $\mathcal{O}_F$ l'anneau des entiers de F et $\mathfrak{d}_F$ sa différente. Pour chaque $i = 1, \ldots, d$, on désigne

ar $a \mapsto a_i$ le i-ième plongement de F dans $\mathbf{R}$, de sorte qu'on a l'identification $F \otimes \mathbf{R} \simeq \mathbf{R}^d$. On désigne par F_+ l'ensemble des éléments totalement positifs de F, c'est-à-dire l'image inverse du cone positif $(\mathbf{R}_+)^d$, et on pose $\mathcal{O}_{F,+} = F_+ \cap \mathcal{O}_F$. On fixe un générateur totalement positif δ de $\mathfrak{d}_F$. On remarque en passant que, puisque le nombre de classes étroites de F est un, tout idéal non-nul de F est engendré par un élément totalement positif.

5.1 Définitions et propriétés de base

On rappelle que le *groupe modulaire de Hilbert* est $\mathrm{SL}_2(\mathcal{O}_F)$, le groupe des matrices 2×2 à coefficients dans $\mathcal{O}_F$ et de déterminant 1. Le demi-plan supérieur de Poincaré est l'ensemble

$$\mathfrak{H} := \{z \in \mathbf{C} : \mathrm{Im}(z) > 0\}.$$

Le groupe $\mathrm{SL}_2(\mathcal{O}_F)$ agit sur $\mathfrak{H}^d$ par les transformations de Mobiüs :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot (z_1, \ldots, z_d) = \left(\frac{a_i z_i + b_i}{c_i z_i + d_i} \right)_{i=1,\ldots,d}.$$

Pour chaque $\gamma \in \mathrm{GL}_2(F)$ et $z \in \mathfrak{H}^d$, nous poserons

$$cz + d = \prod_{i=1}^{d} (c_i z_i + d_i), \text{ où } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_F).$$

On fixe un idéal entier $\mathfrak{N}$ et on pose

$$\Gamma_0(\mathfrak{N}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_F) : c \in \mathfrak{N} \right\}.$$

Définition 5.1. *Une* forme modulaire de Hilbert *de* poids 2 *et de* niveau $\mathfrak{N}$ *est une fonction holomorphe* $f : \mathfrak{H}^d \to \mathbf{C}$ *telle que*

$$f(\gamma z) = (cz + d)^2 f(z) \text{ pour tout } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\mathfrak{N}).$$

On note $M_2(\mathfrak{N})$ l'espace des formes modulaires de Hilbert de poids 2 et de niveau $\mathfrak{N}$.

Soit $f \in M_2(\mathfrak{N})$. Alors f est invariant sous l'action des matrices $\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$ pour $\mu \in \mathcal{O}_F$. Comme une telle matrice agit par $z \mapsto z + \mu$, on voit que f admet une q-expansion

$$f(z) = \sum_{\mu \in \mathcal{O}_F} a_\mu e^{2\pi i \mathrm{Tr}(\frac{\mu z}{\delta})},$$

avec $\mathrm{Tr}(\nu z) = \nu_1 z_1 + \cdots + \nu_d z_d$, pour $\nu \in F$. On a alors le lemme suivant.

Lemme 5.2 (Principe de Goetzky-Koecher)**.** *Soit f une forme modulaire de Hilbert de poids* 2 *et de niveau $\mathfrak{N}$. Alors f admet une q-expansion de la forme*

$$f(z) = a_0 + \sum_{\mu \in \mathcal{O}_{F,+}} a_\mu e^{2\pi i \mathrm{Tr}(\frac{\mu z}{\delta})}.$$

En particulier, f est holomorphe (aux pointes*).*

Démonstration. Ce résultat est une conséquence directe du Théorème des unités de Dirichlet. Voir Bruinier [3] ou Goren [23] pour la preuve. □

Soient $f \in M_2(\mathfrak{N})$ et $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(F)$. On voir alors que $(cz+d)^{-2} f(\gamma z)$ est aussi invariant sous l'action des matrices $\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$ pour $\mu \in \mathcal{O}_F$. Ainsi donc, on a encore une q-expansion

$$(cz+d)^{-2} f(\gamma z) = a_0^\gamma + \sum_{\mu \in \mathcal{O}_{F,+}} a_\mu^\gamma e^{2\pi i \mathrm{Tr}(\frac{\mu z}{\delta})}.$$

Définition 5.3. *Soit f une forme modulaire de Hilbert de poids 2 et de niveau $\mathfrak{N}$. On dit que f est une* forme cuspidale *si $a_0^\gamma = 0$ pour tout $\gamma \in \mathrm{SL}_2(F)$.*

On note $S_2(\mathfrak{N})$ le sous-espace des formes cuspidales de poids 2 et de niveau $\mathfrak{N}$.

Théorème 5.4. *Les espaces $S_2(\mathfrak{N})$ et $M_2(\mathfrak{N})$ sont des espaces vectoriels de dimension* finie *sur* $\mathbf{C}$.

Démonstration. Voir [18]. □

Soient $f \in S_2(\mathfrak{N})$. On voit que f est invariant sous l'action des matrices $\begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_F)$, pour $\epsilon \in \mathcal{O}_F^\times$, qui agissent par $z \mapsto \epsilon^2 z$. Donc, on a

$$a_{\epsilon^2 \mu} = a_\mu \text{ pour tout } \mu \in \mathcal{O}_{F,+} \text{ et } \epsilon \in \mathcal{O}_F^\times.$$

Ainsi, pour tout idéal $\mathfrak{m} \subseteq \mathcal{O}_F$, la quantité $a_\mathfrak{m}(f) = a_\mu$, où μ est un générateur totalement positif de $\mathfrak{m}$, est bien définie et ne dépend que de $\mathfrak{m}$.

Définition 5.5. *Soit f une forme cuspidale de poids 2 et de niveau $\mathfrak{N}$ admettant la q-expansion*

$$f(z) = \sum_{\mu \in \mathcal{O}_{F,+}} a_\mu e^{2\pi i \mathrm{Tr}(\frac{\mu z}{\delta})}.$$

Soit $\mathfrak{m}$ un idéal entier de F. On définit le coefficient de Fourier *de f en $\mathfrak{m}$ par*

$$a_\mathfrak{m}(f) := a_\mu,$$

où $\mathfrak{m} = (\mu)$.

5.2 Produit scalaire de Petersson

Il existe une mesure sur $\mathfrak{H}^d$ donnée par

$$d\mu := \frac{dx_1 dy_1}{y_1^2} \cdots \frac{dx_d dy_d}{y_d^2}.$$

On rappelle que $\mathrm{SL}_2(\mathbf{R})^d$ agit transitivement sur $\mathfrak{H}^d$. Le stabilisateur de $\underline{i} = (\sqrt{-1}, \ldots, \sqrt{-1})$ sous cette action est $\mathrm{SO}(2)^d$. La mesure $d\mu$ est le "pushforward" de la meseur de Haar dg sur $\mathrm{SL}_2(\mathbf{R})^d$ par la bijection $\mathrm{SL}_2(\mathbf{R})^d / \mathrm{SO}(2)^d \simeq \mathfrak{H}^d$. Donc, elle est $\mathrm{SL}_2(\mathbf{R})^d$-invariante. Pour f, $g \in S_2(\mathfrak{N})$, on peut montrer que l'intégrale

$$\int_{\Gamma_0(\mathfrak{N}) \backslash \mathfrak{H}^d} f(z) \overline{g(z)} (y_1 \cdots y_d)^2 d\mu$$

converge (voir [3, 18]).

Définition 5.6. *Soient $f, g \in S_2(\mathfrak{N})$. On définit le* produit scalaire de Petersson *de f et g par*

$$\langle f, g \rangle := \int_{\Gamma_0(\mathfrak{N})\backslash \mathfrak{H}^d} f(z)\overline{g(z)}(y_1 \cdots y_d)^2 d\mu.$$

Le produit scalaire de Petersson sur $S_2(\mathfrak{N})$ est très utile aussi bien d'un point de vue théorique qu'algorithmique.

5.3 Opérateurs de Hecke

Soit f une forme cuspidale de Hilbert de poids 2 et de niveau $\mathfrak{N}$. Soit $\mathfrak{p} \nmid \mathfrak{N}$ un idéal premier de F. On définit la fonction $T_\mathfrak{p} f : \mathfrak{H}^d \to \mathbf{C}$ comme suit. D'abord, on écrit $\mathfrak{p} = (\pi)$, où π est un générateur totalement positif. Ensuite on pose

$$(T_\mathfrak{p} f)(z) = f(\pi z) + \frac{1}{\pi} \sum_{a \in \mathcal{O}_F/\mathfrak{p}} f\left(\frac{z+a}{\pi}\right).$$

Lemme 5.7. *Soit $\mathfrak{p} \nmid \mathfrak{N}$ un idéal premier. Alors, pour tout $f \in S_2(\mathfrak{N})$, $T_\mathfrak{p} f \in S_2(\mathfrak{N})$ et l'application*

$$\begin{aligned} T_\mathfrak{p} : S_2(\mathfrak{N}) &\to S_2(\mathfrak{N}) \\ f &\mapsto T_\mathfrak{p} f \end{aligned}$$

*est un opérateur linéaire. On appelle $T_\mathfrak{p}$ l'*opérateur de Hecke *en $\mathfrak{p}$.*

Démonstration. Exercice. □

On peut étendre la définition des opérateurs de Hecke à tous les idéaux entiers $\mathfrak{n}$ tels que $\gcd(\mathfrak{n}, \mathfrak{N}) = 1$ de la manière suivante :

- Pour tout idéal premier $\mathfrak{p}$ et tout entier $s \geq 1$, $T_{\mathfrak{p}^{s+1}} = T_\mathfrak{p} T_{\mathfrak{p}^s} - \delta_\mathfrak{p} \mathrm{N}\mathfrak{p} T_\mathfrak{p}^{s-1}$, avec $\delta_\mathfrak{p} = 1$ si $\mathfrak{p} \parallel \mathfrak{N}$ et $\delta_\mathfrak{p} = 0$ si $\mathfrak{p}^2 \mid \mathfrak{N}$.
- Pour tous idéaux entiers $\mathfrak{m}, \mathfrak{n}$ tels que $\gcd(\mathfrak{m}, \mathfrak{n}) = 1$, $T_{\mathfrak{mn}} = T_\mathfrak{m} T_\mathfrak{n}$.

On définit l'*algèbre de Hecke* $\mathbf{T}$ comme étant la $\mathbf{Z}$-sous-algèbre de $\mathrm{End}(S_2(\mathfrak{N}))$ engendrée par les $T_\mathfrak{n}$ avec $\gcd(\mathfrak{n}, \mathfrak{N}) = 1$. C'est une algèbre commutative.

Théorème 5.8. *Soient $f, g \in S_2(\mathfrak{N})$ et $\mathfrak{m} \nmid \mathfrak{N}$ un idéal entier. Alors, on a*

$$\langle T_\mathfrak{m} f, g \rangle = \langle f, T_\mathfrak{m} g \rangle.$$

Démonstration. Voir [37, §2]. □

Le Théorème 5.8 implique que les opérateurs de Hecke $T_\mathfrak{m}$, pour $\mathfrak{m} \nmid \mathfrak{N}$, sont normaux.

5.4 Formes propres

Comme $\mathbf{T}$ est une algèbre commutative, que chaque opérateur est normal, et que l'espace $S_2(\mathfrak{N})$ est de dimension finie, on voit que $\mathbf{T}$ admet une base de vecteurs propres communs (voir [37, §2]).

Définition 5.9. *Soit f une forme cuspidale de poids 2 et de niveau $\mathfrak{N}$. On dit que f est une* forme propre *si f est un vector propre common de $\mathbf{T}$ agissant sur $S_2(\mathfrak{N})$.*

Théorème 5.10 (Shimura). *Soit $f \in S_2(\mathfrak{N})$ une forme propre. Alors, on a*

$$T_{\mathfrak{m}} f = a_{\mathfrak{m}}(f) f \text{ pour tout idéal entier } \mathfrak{m} \nmid \mathfrak{N}.$$

Définition 5.11. *Soit f une forme propre de poids 2 et de niveau $\mathfrak{N}$. On dit que f est* normalisée *si $a_{(1)}(f) = 1$.*

Théorème 5.12 (Shimura). *Soit $f \in S_2(\mathfrak{N})$ une forme propre normalisée. Alors, on a :*

(a) Pour tout idéal entier $\mathfrak{m} \nmid \mathfrak{N}$, $a_{\mathfrak{m}}(f)$ est un entier algébrique ;

(b) $K_f := \mathbf{Q}(a_{\mathfrak{m}}(f) : \mathfrak{m} \subseteq \mathcal{O}_F)$ est un corps de nombres totalement réel.

On note $\mathcal{O}_f := \mathbf{Z}[a_{\mathfrak{m}}(f) : \mathfrak{m} \subseteq \mathcal{O}_F]$.

Remarque 5.13. Le fait que K_f soit totalement réel dans l'assertion Théorème 5.12 (b) est due au fait que F a une seule classe restreinte et que la forme est de caractère trivial. En général, K_f est plutôt CM. (Voir [37, §2] pour plus de details.)

5.5 Sous-espaces anciens et nouveaux

Soient $\mathfrak{M}$ un idéal entier tel que $\mathfrak{M} \mid \mathfrak{N}$ et $\mathfrak{D}$ un diviseur de $\mathfrak{N}\mathfrak{M}^{-1}$. On choisit un générateur u totalement positif de $\mathfrak{D}$. Alors, on voit que l'application

$$\begin{aligned} \iota_{\mathfrak{D}} : S_2(\mathfrak{M}) &\to S_2(\mathfrak{N}) \\ f &\mapsto f_u, \end{aligned}$$

où $f_u(z) := f(uz)$, est indépendante du choix de u. De plus, elle est injective. On pose

$$\begin{aligned} S_2(\mathfrak{N})^{\text{old}} &:= \sum_{\substack{\mathfrak{M} \mid \mathfrak{N} \\ \mathfrak{D} \mid \mathfrak{N}\mathfrak{M}^{-1}}} \iota_{\mathfrak{D}}(S_2(\mathfrak{M})); \\ S_2(\mathfrak{N})^{\text{new}} &:= \left(S_2(\mathfrak{N})^{\text{old}} \right)^{\perp}. \end{aligned}$$

On appelle $S_2(\mathfrak{N})^{\text{old}}$ (resp. $S_2(\mathfrak{N})^{\text{new}}$) le *sous-espace ancien* (resp. *sous-espace nouveau*) de $S_2(\mathfrak{N})$. On peut montrer que $S_2(\mathfrak{N})^{\text{old}}$ et $S_k(\mathfrak{N})^{\text{new}}$ sont préservés par l'action de Hecke.

Définition 5.14. *Soit $f \in S_2(\mathfrak{N})$ une forme propre normalisée. On dit que f est une* forme nouvelle *si $f \in S_2(\mathfrak{N})^{\text{new}}$.*

Définition 5.15. *Soit $f \in S_2(\mathfrak{N})$ une forme nouvelle. On définit la L-série de f par*

$$L(f, s) := \sum_{\mathfrak{m} \subseteq \mathcal{O}_F} \frac{a_{\mathfrak{m}}(f)}{\mathrm{N}\mathfrak{m}^s}.$$

Théorème 5.16 (Shimura). *Soit $f \in S_2(\mathfrak{N})$ une forme nouvelle. Alors $L(f, s)$ est une fonction entière, c'est-à-dire qu'elle est holomorphe sur $\mathbf{C}$. De plus $L(f, s)$ admet un* produit eulérien.

Démonstration. Voir [34, 37]. □

Théorème 5.17 (Multipicité un). *Soient $f, g \in S_2(\mathfrak{N})$ des formes propres normalisées telles que*

$$a_{\mathfrak{m}}(f) = a_{\mathfrak{m}}(g) \text{ pour tout } \mathfrak{m} \nmid \mathfrak{N}.$$

Alors, on a $f = g$.

Démonstration. Ce résultat est une conséquence de la relation entre les valeurs propres de Hecke et les coefficients de Fourier, et du fait que f et g sont déterminées par leurs q-expansions. □

La définition des opérateurs de Hecke peut être étendue à tous les idéaux entiers, y compris ceux divisant le niveau $\mathfrak{N}$. Avec ceci, on a le résultat suivant.

Théorème 5.18 (Multipicité un forte). *Soit $f \in S_2(\mathfrak{N})$ une forme nouvelle. Alors, on a*

$$T_{\mathfrak{m}} f = a_{\mathfrak{m}}(f) f \text{ pour tout } \mathfrak{m} \subseteq \mathcal{O}_F.$$

Démonstration. Voir [28]. □

Les Théorèmes 5.17 et 5.18 sont extrêmement utiles. Ils impliquent qu'une forme nouvelle est uniquement déterminée par ses valeurs propres de Hecke (ou coefficients de Fourier). En voici une application immédiate.

Théorème 5.19. *Soient $f \in S_2(\mathfrak{N})^{\text{new}}$ une forme nouvelle et K_f son corps de coefficients de Fourier. Pour tout plongement $\tau : K_f \hookrightarrow \overline{\mathbf{Q}}$, il existe forme nouvelle $f^\tau \in S_2(\mathfrak{N})$ définie par*

$$a_{\mathfrak{m}}(f^\tau) := \tau(a_{\mathfrak{m}}(f)), \text{ pour tout } \mathfrak{m} \subseteq \mathcal{O}_F.$$

L'ensemble $\{f^\tau : \tau \in \mathrm{Hom}(K_f, \overline{\mathbf{Q}})\}$ est appelé l'orbite de Hecke *de f. On la note par $[f]$.*

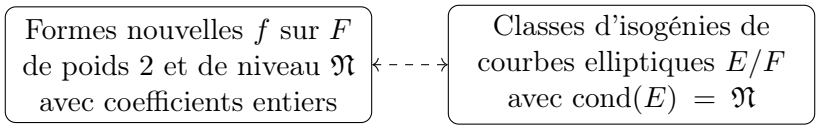
Démonstration. Voir [37, §2]. □

Pour une étude théorique plus approfondie des formes modulaires de Hilbert, nous référons à [3, 12, 18, 23, 37] et aux références qui s'y trouvent. La plupart des méthodes de calculs actuelles de ces formes reposent sur la correspondance d'Eichler-Jacquet-Langlands-Shimizu entre les formes modulaires de Hilbert et les formes modulaires quaternioniques. Pour plus de détails sur cet aspect, nous encourageons le lecteur à consulter [12] et les références qui s'y trouvent. Les exemples que nous présenterons par la suite ont été calculés à l'aide du Hilbert Modular Forms Package dans `Magma` [2] qui utilise les algorithmes présentés dans [12].

5.6 Modularité des courbes elliptiques

Conjecture 5.20. *Il existe une application $f \mapsto E_f$ de l'ensemble des formes nouvelles f sur F de poids 2 et de niveau $\mathfrak{N}$, avec coefficients entiers, à l'ensemble des courbes elliptiques de conducteur $\mathfrak{N}$ définies sur F, telle que $L(f, s) = L(E_f, s)$. Cette application induit une bijection sur l'ensemble des classes d'isogénies.*

La Conjecture 5.20 se résume de façon succincte par le diagramme suivant :



$\mathrm{N}\mathfrak{p}$	$\mathfrak{p}$	$a_{\mathfrak{p}}(f)$
4	2	-3
5	$-2w+1$	-2
9	3	2
11	$-3w+1$	4
11	$-3w+2$	-4
19	$-4w+3$	4
19	$-4w+1$	-4
29	$-w+6$	-2
29	$w+5$	-2
31	$-5w+2$	8
31	$-5w+3$	-1

TABLE 1 – Quelques coefficients de Fourier de la forme nouvelle de poids 2 et de niveau $\mathfrak{N} = (5+2w)$ sur $\mathbf{Q}(\sqrt{5})$.

On voit bien qu'elle généralise le Théorème 3.1. Maintenant, l'application $f \mapsto E_f$ s'appelle la *conjecture d'Eichler-Shimura pour les courbes elliptiques* (sur F). Encore une fois, par le théorème des isogénies de Faltings, deux courbes elliptiques isogènes partagent la même fonction L. Donc, dire que cette application est une bijection sur l'ensemble des classes d'isogénies revient à dire que chaque classe d'isogénie contient une courbe elliptique E_f associée à une forme nouvelle $f \in S_2(\mathfrak{N})^{\mathrm{new}}$, avec coefficients entiers.

Pour $[F : \mathbf{Q}] > 1$, on peut se servir du Hilbert Modular Forms Package implementé par l'auteur et ses collaborateurs Steve Donnelly, Matthew Greenberg and John Voight (voir [12]) pour calculer les formes modulaires de Hilbert sur un corps de nombres totalement réel de degré raisonnable. Nous nous sommes servis de ce logiciel pour calculer les exemples ci-dessous.

Exemple 5.21. Soient $F = \mathbf{Q}(\sqrt{5})$, $w = \frac{1+\sqrt{5}}{2}$ et $\mathfrak{N} = (5+2w)$. Alors $\mathfrak{N}$ est un premier de norme 31, la plus petite norme pour laquelle $S_2(\mathfrak{N}) \neq 0$. Dans ce cas, on a $\dim S_2(\mathfrak{N}) = 1$. Donc, il existe une forme nouvelle $f \in S_2(\mathfrak{N})$ avec coefficients de Fourier dans $\mathbf{Z}$. Nous avons énuméré ces coefficients pour les premiers de petite norme dans la Table 1.

Considérons la courbe elliptique

$$E : \ y^2 + xy + wy = x^3 - (1+w)x^2.$$

Elle est de conducteur $\mathrm{cond}(E) = (5+2w)$. Le Théorème 5.22 ci-dessous nous dit qu'elle est modulaire. Donc, nous savons que

$$L(E, s) = L(f, s).$$

Comme mentionné ci-haut, la Conjecture 5.20 est encore grande ouverte. Mais, grâce aux travaux de Siksek et de ses collaborateurs, nous savons pour toute courbe elliptique E sur un corps quadratique réel F est *moduaire*, c'est-à-dire qu'il existe une forme modulaire de Hilbert f de poids 2 sur F telle que $L(E, s) = L(f, s)$ (voir Freitas-Le Hung-Siksek [19]).

Théorème 5.22 (Freitas-Le Hung-Siksek)**.** *Soient F un corps quadratique réel et E une courbe elliptique définie sur F. Alors, E est modulaire.*

Exemple 5.23. Soit $F = \mathbf{Q}(\sqrt{1997})$, $w := \frac{1+\sqrt{1997}}{2}$. Une recherche dans `Magma` donne six courbes elliptiques de conducteur trivial sur F. Ces courbes se repartissent en trois classes de $\mathrm{Gal}(F/\mathbf{Q})$-conjugaison données par

$$E_1 : y^2 + wxy = x^3 + (w+1)x^2 + (111w + 5401)x + (2406w + 81112);$$
$$E_2 : y^2 + wxy + (w+1)y = x^3 - x^2 + (9370w - 208733)x + (2697263w - 61535794);$$
$$E_3 : y^2 + (w+1)xy + (w+1)y = x^3 - wx^2 + (19636w + 434383)x + (5730650w + 125261893).$$

Par le Théorème 5.22 ces courbes sont modulaires. À l'aide du Hilbert Modular Forms Package dans `Magma`, on vérifie qu'il y a exactement six formes nouvelles de Hilbert de poids 2 et de niveau (1), avec coefficients de Fourier entiers et qu'elles correspondent bien aux courbes trouvées. Cela montre donc que ce sont les seules courbes elliptiques de conducteur trivial sur F.

6 Modularité des variétés abéliennes de type GL_2

Soit A une variété abélienne de dimension g définie sur F. On dit que A est de *type* GL_2 s'il existe un corps de nombres K de degré g tel que $\mathrm{End}_F(A)$ est un ordre dans K, c'est-à-dire tel que $\mathrm{End}_{\mathbf{Q}}(A) \otimes \mathbf{Q} = K$.

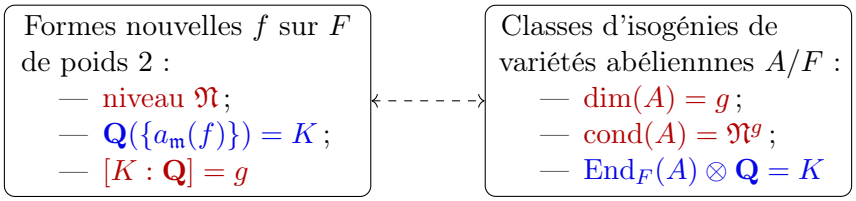
On définie la *L-série* $L(A, s)$ de A en comptant ses points sur les corps finis comme dans le cas des courbes elliptiques.

Conjecture 6.1. *Soient F un corps de nombres totalement réel de nombre de classes étroites et $\mathfrak{N}$ un idéal entier de F. Soit $K/\mathbf{Q}$ un corps de nombres totalement réel de degré g. Alors, il existe une application $f \mapsto A_f$ de l'ensemble des formes nouvelles $f \in S_2(\mathfrak{N})$, avec $K_f = K$, dans l'ensemble des variétés abéliennes de type GL_2 et de conducteur $\mathfrak{N}^g$, avec $\mathrm{End}_F(A) \otimes \mathbf{Q} = K$, telle que*

$$L(A_f, s) = \prod_{\tau \in \mathrm{Hom}(K_f, \overline{\mathbf{Q}})} L(f^\tau, s).$$

L'application induit une bijection sur les classes d'isogénies.

La Conjecture 6.1 se résume par le diagramme suivant :



La Conjecture 6.1 est clairement une généralisation de la Conjecture 5.20. Comme nous avons vu plus haut, ces deux conjectures ne sont rien d'autre que les Théorèmes 3.1 et 4.1 pour $F = \mathbf{Q}$.

Pour $[F : \mathbf{Q}] > 1$, l'application $f \mapsto A_f$ est souvent appelée la *conjecture d'Eichler-Shimura* pour les variétés abéliennes de type GL_2. Les cas connus de cette conjecture exploitent la cohomologie des courbes de Shimura. Ainsi, la conjecture est connue lorsque $[F : \mathbf{Q}]$ est impaire, ou lorsque $\mathfrak{N}$ est divisible exactement par un idéal premier $\mathfrak{p}$ de $\mathcal{O}_F$ [44]. Blasius donne une construction de A_f basée sur les conjectures standards en géométrie arithmétique. Le case le plus simple où la conjecture

$\mathrm{N}\mathfrak{p}$	$\mathfrak{p}$	$a_{\mathfrak{p}}(f)$
4	2	$2e-2$
5	$-2w+1$	$-3e+1$
9	3	$-e-2$
11	$-3w+1$	$-e$
11	$-3w+2$	$4e-2$
19	$-4w+3$	$3e-6$
19	$-4w+1$	$e+1$
29	$-w+6$	$-5e+1$
29	$w+5$	$-2e+6$
31	$-5w+2$	$-2e+8$
31	$-5w+3$	$-5e+1$

TABLE 2 – Quelques coefficients de Fourier de la nouvelle forme f de poids 2 et de niveau $\mathfrak{N} = (7+3w)$ sur $\mathbf{Q}(\sqrt{5})$. (Ici, $e = \frac{1+\sqrt{5}}{2}$.)

d'Eichler-Shimura en encore non connue es lorsque f est une forme nouvelle de poids 2 et de niveau (1) sur un corps quadratique réel. Dans ce cas, on voit que la conjecture d'Eichler-Shimura prédit que A_f devrait être une variété abélienne avec bonne réduction partout.

Remarque 6.2. Dans la Conjecture 6.1, nous devons supposer que K est totalement réel. Cela résulte de l'hypothèse que le nombre de classes restreintes de F est un (voir [37, Proposition 2.8]).

Exemple 6.3. Soient $F = \mathbf{Q}(\sqrt{5})$, $w = \frac{1+\sqrt{5}}{2}$, et $\mathfrak{N} = (7+3w)$. Alors, $\mathfrak{N}$ est un idéal premier de norme 61, c'est la plus petite norme telle que $\dim S_2(\mathfrak{N}) > 1$. L'espace $S_2(\mathfrak{N})$ est de dimension 2, il contient une forme nouvelle f telle que $K_f = \mathbf{Q}(\sqrt{5})$ et $\mathcal{O}_f := \mathbf{Z}[\{a_{\mathfrak{m}}(f)\}] = \mathbf{Z}[\frac{1+\sqrt{5}}{2}]$. Nous avons énuméré quelques valeurs propres de Hecke dans la Table 2.

Maintenant, on considère la courbe hyperelliptique

$$C : y^2 + Q(x)y = P(x)$$

donnée par

$$P(x) := -wx^4 + (w-1)x^3 + (5w+4)x^2 + (6w+4)x + 2w + 1;$$
$$Q(x) := x^3 + (w-1)x^2 + wx + 1.$$

Nous avons obtenue cette courbe en spécialisant la famille D_5 de Brumer de courbes de genre 2 avec RM par $\mathbf{Z}[\frac{1+\sqrt{5}}{2}]$. Le discriminant de C est $\mathrm{disc}(C) = w^{26}(7+3w)^2$. Donc, sa Jacobienne $\mathrm{Jac}(C)$ a RM par $\mathbf{Z}[\frac{1+\sqrt{5}}{2}]$. Dans [12], nous avons montré que $\mathrm{Jac}(C)$ correspond à la forme f, c'est-à-dire que

$$L(\mathrm{Jac}(C), s) = L(f, s)L(f^\tau, s),$$

où τ est l'élément non-trivial de $\mathrm{Gal}(K_f/\mathbf{Q})$.

Exemple 6.4. Dans les Exemples 5.21 et 6.3, les variétés abéliennes sont des Jacobiennes de courbes de Shimura. En effet, comme nous avons expliqué plus tôt, la théorie des courbes de Shimura est la

seule méthode qui permet de prouver les cas connus de la Conjecture 6.1. Cependant, cette approche ne marche pas pour l'Exemple 5.23 ou le prochain.

Soient $F = \mathbf{Q}(\sqrt{353})$ et $w := \frac{1+\sqrt{353}}{2}$. Considérons la courbe $C : y^2 + Q(x)y = P(x)$ donnée par

$$\begin{aligned} P(x) := &-(15w+149)x^6 - (1119w+9948)x^5 - (36545w+325090)x^4 \\ &- (636332w+5659370)x^3 - (6227174w+55387985)x^2 \\ &- (32480001w+288869715)x - 70532813w - 627353458; \\ Q(x) := &(w+1)x^3 + x^2 + wx + w + 1. \end{aligned}$$

Notons par ${}^\sigma C$ la conjuguée galoisienne de C ; A et ${}^\sigma A$ les Jacobiennes de C et ${}^\sigma C$ respectivement. Le discriminant de la courbe C est $\mathrm{disc}(C) = -\epsilon^4$, où ϵ est l'unité fondamental de F. Donc, C, ${}^\sigma C$ et les surfaces A, ${}^\sigma A$ ont bonne réduction partout. A et ${}^\sigma A$ ont multiplication réelle par $\mathbf{Z}[\frac{1+\sqrt{5}}{2}]$. On peut montrer que A et ${}^\sigma A$ sont modulaires en utilisant les travaux de Khare-Thorne. Mais, il n'y pas de méthode connue qui permet de construire directement la surface correspondant à la forme f. Nous avons trouvé les surfaces A et ${}^\sigma A$ en cherchant pour les surfaces abéliennes de petite hauteur sachant que l'on connaît leur corps de 2-torsion (donnée par la connaissance des formes f et ${}^\sigma f$).

7 Surfaces abéliennes avec bonne réduction partout

7.1 Surfaces modulaires de Hilbert

Soit K un corps quadratic réel de discriminant D'. La surface modulaire de Hilbert $Y_-(D')$ est la compactification de l'espace de modules (grossier) qui paramétrise les surface abéliennes principalement polarisées avec multiplication réelle par l'anneau des entiers $\mathcal{O}_K$ de K, c'est-à-dire l'ensemble des paires (A, ι), où $\iota : \mathcal{O}_K \to \mathrm{End}_{\overline{\mathbf{Q}}}(A)$ est un homomorphisme. Les surfaces $Y_-(D')$ ont des modèles sur $\mathbf{Z}$, avec bonne réduction en dehors des premiers divisant D'.

Elkies et Kumar [16] ont déterminé des models birationnels explicites sur $\mathbf{Q}$ pour ces surfaces modulaires de Hilbert pour tous les discriminants fondamentaux $D' \leq 100$. Ils décrivent une telle surface $Y_-(D')$ comme un revêtement double de $\mathbf{P}^2$ donné par une équation de la forme $z^2 = f(r, s)$, où r, s sont des paramètres sur $\mathbf{P}^2$. Ils donnent également une application birationnelle $\mathcal{A}_2 \dashrightarrow \mathcal{M}_2$, où $\mathcal{M}_2$ est l'espace de modules des courbes de genre 2. Cette application est donnée par l'expression des invariants d'Igusa-Clebsch du point image point comme fonctions rationnelles de r et s.

7.2 La stratégie

Pour produire des surfaces abéliennes avec bonne réduction partout, nous combinons la Conjecture 6.1 avec les équations explicites dans [16]. Pour trouver de telles surfaces A, on choisit deux corps quadratics réels F et K tels que F soit de classe de nombres étroites un, et on procède comme suit :

(a) Trouver une forme nouvelle de Hilbert de poids 2 et de niveau (1) sur F, avec corps de coefficients $K_f = K$ de discriminant D'.

(b) Trouver un point F-rationnel A_x sur la surface $Y_-(D')$ tel que la fonction L de la surface abélienne associée A_x match les premiers facteurs d'Euler de f, à une tordue près.

(c) Calculer la bonne tordue quadratique A de la surface A_x, c'est-à-dire de la courbe de genre 2 correspondante.

(d) Vérifier que la surface abélienne A a bonne réduction partout.

(e) Montrer que nous avons bien l'égalité des fonctions L, c'est-à-dire que A est modulaire.

7.3 Méthode 1 : Recherche de points sur les surfaces modulaires de Hilbert

Nous illustrons cette méthode avec l'exemple suivant. Le plus petit discriminant pour lequel nous avons une surface abélienne avec bonne réduction partout est $D = 53$. La surface abélienne A_f a multiplication réelle par $\mathbf{Z}[\sqrt{2}]$, l'anneau des entiers du corps $\mathbf{Q}(\sqrt{2})$.

$\mathrm{N}\mathfrak{p}$	$\mathfrak{p}$	$a_{\mathfrak{p}}(f)$	$s_{\mathfrak{p}}(f)$	$t_{\mathfrak{p}}(f)$
4	2	$e+1$	2	7
7	$-w-2$	$-e-2$	-4	16
7	$-w+3$	$-e-2$	-4	16
9	3	$-3e+1$	2	1
11	$w-2$	$3e$	0	4
11	$w+1$	$3e$	0	4
13	$w-1$	$-2e+1$	2	19
13	$-w$	$-2e+1$	2	19
17	$-w-5$	-3	-6	43
17	$w-6$	-3	-6	43
25	5	$2e+4$	8	58
29	$-w-6$	$3e-3$	-6	49
29	$w-7$	$3e-3$	-6	49

TABLE 3 – Quelques valeurs propres de Hecke de la forme nouvelle de poids 2 et de niveau (1) sur $\mathbf{Q}(\sqrt{53})$. Ici, on a $e = \sqrt{2}$.

Une équation de la surface modulaire de Hilbert $Y_-(8)$ est donnée dans [16]. C'est un revêtement double de $\mathbf{P}^2_{r,s}$ donné par

$$z^2 = 2(16rs^2 + 32r^2s - 40rs - s + 16r^3 + 24r^2 + 12r + 2).$$

Dans ce cas, on sait que $Y_-(8)$ est une surface *rationnelle* sur $\mathbf{Q}$. Par conséquent, les points rationnels sont denses. En particulier, il y a une abondance de points de petite hauteur. Pour un tel point, les invariants d'Igusa-Clebsch $(I_2 : I_4 : I_6 : I_{10}) \in \mathbf{P}^2_{(1:2:3:5)}$ sont donnés par

$$\left(-\frac{24B_1}{A_1}, -12A, \frac{96AB_1 - 36A_1B}{A_1}, -4A_1B_2\right),$$

avec

$$\begin{aligned} A_1 &= 2rs^2, \\ A &= -(9rs + 4r^2 + 4r + 1)/3, \\ B_1 &= (rs^2(3s + 8r - 2))/3, \\ B &= -(54r^2s + 81rs - 16r^3 - 24r^2 - 12r - 2)/27, \\ B_2 &= r^2. \end{aligned}$$

Rappelons nous que nous espérons trouver un point de $Y_-(8)$ sur $F = \mathbf{Q}(\sqrt{53})$, correspondant à une surface abélienne principalement polarisée A qui match la forme nouvelle de Hilbert f. La fonction L de la surface A s'obtient en comptant les points sur les corps résiduels $\mathbf{F}_\mathfrak{p} = \mathcal{O}_F/\mathfrak{p}$, avec $\mathfrak{p}$ parcourant l'ensemble des idéaux premiers de F. De l'autre côté, la fonction L de la surface conjecturale A_f attachée à f s'écrit comme

$$L(A_f, s) = L(f, s)L(f^\tau, s) = \prod_\mathfrak{p} \frac{1}{Q_\mathfrak{p}(\mathrm{N}(\mathfrak{p})^{-s})},$$

où

$$\begin{aligned} Q_\mathfrak{p}(T) &:= (T^2 - a_\mathfrak{p}(f)T + \mathrm{N}(\mathfrak{p}))(T^2 - a_\mathfrak{p}(f)^\tau T + \mathrm{N}(\mathfrak{p})) \\ &= T^4 - s_\mathfrak{p}(f)T^3 + t_\mathfrak{p}(f)T^2 - \mathrm{N}(\mathfrak{p})s_\mathfrak{p}(f)T + \mathrm{N}(\mathfrak{p})^2. \end{aligned}$$

Nous voudrions que les facteurs locaux de ces deux fonctions L soient égaux.

D'abord, nous commençons par calculer l'ensemble des points F-rationnels de hauteur $\leq B$ sur la surface $Y_-(8)$, pour une borne B fixée. Ensuite, pour chaque point (r, s) de cette liste, nous essayons de construire la courbe C de genre 2 dont la Jacobienne $\mathrm{Jac}(C)$ correspond à (r, s), et nous vérifions que le polynôme caractéristique de Frobenius sur le groupe de cohomologie étale de degré 1 est le même que le polynôme $Q_\mathfrak{p}(T)$ donnant le facteur d'Euler de la surface A_f attachée à la forme f. Si notre point candidate (r, s) passe ce test, disons pour tous les premiers de F de norme plus petite que 100, en lesquels $A = \mathrm{Jac}(C)$ a bonne réduction, nous pouvons être raisonnablement confiants que nous avons trouvé la bonne courbe. Dans ce cas, nous cherchons alors à prouver que A correspond à f. (Nous avons passé sous silence plusieurs aspects subtiles de ce processus. Pour plus de détails, nous référons à [11].)

Dans l'exemple en mains, une recherche de points de hauteur ≤ 200 sur $Y_-(8)$ utilisant l'agorithme de Doyle-Krumm [14] (implementé dans `Sage`) donne les paramètres

$$r = -\frac{24 + 10w}{11^2}, \ s = \frac{136 - 24w}{11^2},$$

et les invariants d'Igusa-Clebsch

$$\begin{aligned} I_2 &= 208 + 88w, \\ I_4 &= -1660 - 588w, \\ I_6 &= -428792 - 135456w, \\ I_{10} &= 643072 + 204800w. \end{aligned}$$

En utilisant l'algorithme de Mestre [27], implementé dans `Magma`, nous obtenons une courbe avec les invariants ci-dessus. Nous réduisons ensuite cette courbe en utilisant l'algorithme de Bouyer-Streng [1] implementé dans `Sage` [30]. Cela nous permet d'obtenir la courbe

$$\begin{aligned} C' : y^2 = &(-6w + 25)x^6 + (-60w + 246)x^5 + (-242w + 1017)x^4 \\ &+ (-534w + 2160)x^3 + (-626w + 2688)x^2 \\ &+ (-440w + 1724)x - 127w + 567. \end{aligned}$$

Par une seconde réduction de la courbe C', nous obtenons le résultat suivant.

Théorème 7.1. *Soit* $C : y^2 + Q(x)y = P(x)$ *la courbe sur* $F = \mathbf{Q}(\sqrt{53})$ *donnée par*

$$\begin{aligned} P &:= -4x^6 + (w-17)x^5 + (12w-27)x^4 + (5w-122)x^3 + (45w-25)x^2 \\ &\quad + (-9w-137)x + 14w + 9, \\ Q &:= wx^3 + wx^2 + w + 1. \end{aligned}$$

Alors, on a

(a) Le discriminant de la courbe C *est* $\Delta_C = -\epsilon^7$. *Donc,* C *a bonne réduction partout.*

(b) La surface $A := \mathrm{Jac}(C)$ *a multiplication réelle* $\mathbf{Z}[\sqrt{2}]$. *Elle est modulaire et correspond à l'unique orbite de Hecke* $[f]$ *dans* $S_2(1)$.

Démonstration. La surface A a un point de 7-torsion sur F. Cela implique que la représentation galoisienne résiduelle modulo 7 est réductible. Pour montrer que A est modulaire, on peut alors utiliser les résultats de Skinner-Wiles [40]. Voir [11] pour plus de détails. □

7.4 Méthode 2 : Décomposition de variétiés abéliennes

On peut utiliser cette méthode lorsque la forme nouvelle f est un changement de base, c'est-à-dire que lorsque les coefficients de Fourier de f satisfont à la relation

$$a_{\mathfrak{p}}(f) = a_{\sigma(\mathfrak{p})}(f) \text{ pour tout premier } \mathfrak{p},$$

où $\mathrm{Gal}(F/\mathbf{Q}) = \langle\sigma\rangle$. Dans ce cas, f est le changement de base d'une nouvelle forme classique $g \in S_2(\Gamma_1(D))$. Comme le niveau de f est (1), la forme $g \in S_2(\Gamma_1(D), \chi_D)^{\mathrm{new}}$ par [26, Prop. 2, p.263], où χ_D est le caractère fondamental du corps quadratique $F = \mathbf{Q}(\sqrt{D})$. Le corps des coefficients L_g de g est un corps quartique de type CM qui contient K_f. L'élément non-trivial de $\mathrm{Gal}(L_g/K_f)$, que nous notons $(x \mapsto \bar{x}, x \in L_g)$, étend la conjugaison complexe. La variété abélienne B_g attachée à la forme g est une 4-variété telle que $\mathrm{End}_{\mathbf{Q}}(B_g) \otimes \mathbf{Q} \simeq L_g$.

Soit w_D l'involution d'Atkin-Lehner sur $S_2(\Gamma_1(D), \chi_D)^{\mathrm{new}}$. Elle induit, à son tour, une involution sur B_g que nous notons également w_D. Shimura [34, § 7.7] montre alors les choses suivantes :

(a) w_D est définie sur F et $w_D^\sigma = -w_D$;

(b) $w_D \cdot [x] = [\bar{x}] \cdot w_D$, où $[x]$ est l'endomorphisme induit par $x \in L_g$ sur B_g.

(c) La surface abélienne $A_f := (1+w_D)B_g$ est définie sur F et est isogène à sa conjuguée galoisienne donnée par $A_f^\sigma := (1-w_D)B_g$. De plus, on a l'isogénie

$$B_g \otimes_{\mathbf{Q}} F \sim A_f \times A_f^\sigma.$$

Pour que la décomposition algébrique ci-dessus nous soit utile, il faudrait que nous puissions en donnée une interprétation analytique qui va nous permettre de calculer A_f à partir de l'uniformsation complexe de B_g. Pour ce faire, nous supposons que A_f et A_f^σ sont principalement polarisables.

Pour décrire notre approche, rappelons que, par [6, Theorems 6.2.4 and 6.2.6], il existe des formes nouvelles $g_1, g_2 \in S_2(\Gamma_1(D), \chi_D)^{\mathrm{new}}$ telles que $\{g_1, \overline{g}_1, g_2, \overline{g}_2\}$ soit une base de $\mathrm{span}([g])$ et que

$$w_D(g_1) = \bar{\lambda}_D(g_1)\bar{g}_1,\ w_D(g_2) = \bar{\lambda}_D(g_2)\bar{g}_2,$$

où $a_D(g)$ est la valeur propre de Hecke de g en D et $\lambda_D(g) = \frac{a_D(g)}{\sqrt{D}}$, la pseudo-valeur propre w_D. La matrice de w_D dans la base $\{g_1, \bar{g}_1, g_2, \bar{g}_2\}$ est donnée par

$$W_D := \begin{bmatrix} 0 & \lambda_D(g_1) & 0 & 0 \\ \bar{\lambda}_D(g_1) & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda_D(g_2) \\ 0 & 0 & \bar{\lambda}_D(g_2) & 0 \end{bmatrix}$$

De ceci, il découle alors que $W_D^\sigma = -W_D$. On obtient ainsi le lemme suivant.

Lemme 7.2. *L'ensemble des formes $h_i^\pm := \frac{1}{2}(g_i \pm w_D(g_i))$, $i = 1, 2$, donnent des bases pour les sous-espaces propres ± 1 de W_D agissant sur* $\mathrm{span}([g])$. *On obtient ainsi une décomposition de l'espace des 1-formes différentielles $H^0(B_g \otimes_{\mathbf{Q}} F, \Omega^1_{B_g \otimes_{\mathbf{Q}} F/F})$ sous l'action de* $\mathrm{Gal}(F/\mathbf{Q})$.

Démonstration. C'est une simple adaptation de [7, Lemma 5.6.2]. □

Rappelons que, puisque $H_1(B_g, \mathbf{Z})$ est un module de Hecke de rang 4 sur $\mathbf{Z}$, les sous-espaces propres $H_1(B_g, \mathbf{Z})^\pm$ de w_D sont aussi des modules de Hecke de rang 2 sur $\mathbf{Z}$ chacun.

Lemme 7.3. *Soient $\Lambda_g^\pm$ les réseaux des périodes obtenus en integrant les formes du Lemme 7.2 contre $H_1(B_g, \mathbf{Z})^\pm$ et $\Lambda_g = \Lambda_g^+ \oplus \Lambda_g^-$. Alors, il existe une 4-variété abélienne B'_g définie sur $\mathbf{Q}$ et une isogénie $\phi : B'_g \to B_g$, dont le degré est une puissance de, telle que $B'_g(\mathbf{C}) = \mathbf{C}^4/\Lambda_g$. De plus, $B'_g = \mathrm{Res}_{F/\mathbf{Q}}(A_f)$ où A_f est une surface abélienne définie sur F.*

Démonstration. Voir [11]. □

En remplaçant au besoin B_g par B'_g, le Lemme 7.3 permet d'écrire

$$H_1(B_g, \mathbf{Z}) = H_1(B_g, \mathbf{Z})^+ \oplus H_1(B_g, \mathbf{Z})^- = H_1(A_f, \mathbf{Z}) \oplus H_1(A_f^\sigma, \mathbf{Z}).$$

Ce qui donne la décomposition de la matrice des périodes de B_g

$$\Omega_{B_g} = \Omega_{A_f} \times \Omega_{A_f^\sigma} = (\Omega_1 \,|\, \Omega_2) \times (\Omega_1^\sigma \,|\, \Omega_2^\sigma).$$

Pourvu que la restriction de l'accouplement intersection à $H_1(A_f, \mathbf{Z})$ et $H_1(A_f^\sigma, \mathbf{Z})$ induise des polarisations principales, nous pouvons calculer les surfaces A_f et A_f^σ comme les Jacobiennes de courbes C_f et C_f^σ (définies sur F).

Nous illustrons maintenant cette discussion avec un exemple provenant du discriminant $D = 73$. La surface abélienne A_f a multiplication réelle par $\mathbf{Z}[\frac{1+\sqrt{5}}{2}]$.

Une base symplectique de $H_1(B_g, \mathbf{Z})$ est donnée par les symboles modulaires [41]

$$\begin{aligned}
\gamma_1 &:= 2\{-1/57, 0\} - \{-1/62, 0\} - \{-1/52, 0\} + 2\{-1/29, 0\} + \{-1/18, 0\}, \\
\gamma_2 &= -\{-1/62, 0\} + 2\{-1/41, 0\} - \{-1/52, 0\} + 2\{-1/12, 0\} + 2\{-1/29, 0\} \\
&\quad + \{-1/18, 0\} - \{-1/36, 0\}, \\
\gamma_3 &:= \{-1/57, 0\} - \{-1/41, 0\} - \{-1/18, 0\} + \{-1/36, 0\}, \\
\gamma_4 &:= -\{-1/57, 0\} + \{-1/62, 0\} - \{-1/41, 0\} + \{-1/52, 0\} - \{-1/12, 0\} \\
&\quad - 2\{-1/29, 0\} - \{-1/18, 0\} + \{-1/24, 0\}, \\
\gamma'_1 &:= \{-1/57, 0\} + \{-1/41, 0\} + \{-1/18, 0\} - \{-1/36, 0\}, \\
\gamma'_2 &:= \{-1/57, 0\} + \{-1/62, 0\} + \{-1/41, 0\} - \{-1/52, 0\} - \{-1/12, 0\} \\
&\quad - \{-1/18, 0\} + \{-1/24, 0\}, \\
\gamma'_3 &:= -\{-1/62, 0\} + \{-1/52, 0\} + \{-1/18, 0\}, \\
\gamma'_4 &:= \{-1/62, 0\} - \{-1/52, 0\} - \{-1/18, 0\} + \{-1/36, 0\}.
\end{aligned}$$

Nous avons choisi cette base de telle sorte que $\{\gamma_1,\gamma_2,\gamma_3,\gamma_4\}$ et $\{\gamma_1',\gamma_2',\gamma_3',\gamma_4'\}$ soient des bases intégrales de $H_1(B_g,\mathbf{Z})^+$ et de $H_1(B_g,\mathbf{Z})^-$. En calculant la matrice G d'intersection dans cette base, on voit que B_g est principalement polarisée. On obtient également que $H_1(B_g,\mathbf{Z})^+$ et $H_1(B_g,\mathbf{Z})^-$ ont la même polarisation de type $(2,2)$, ce qui signifie que A_f et A_f^σ sont principalement polarisées. En intégrant les bases de formes différentielles $\{h_1^+,h_2^+\}$ et $\{h_1^-,h_2^-\}$ du Lemma 7.2 contres les bases de Darboux $\{\gamma_1,\gamma_2,\gamma_3,\gamma_4\}$ et $\{\gamma_1',\gamma_2',\gamma_3',\gamma_4'\}$, on obtient les matrices des périodes de Riemann Ω_{A_f} and $\Omega_{A_f^\sigma}$, où

$$\Omega_{B_g}=\Omega_{A_f}\times\Omega_{A_f^\sigma}=(\Omega_1\,|\,\Omega_2)\times(\Omega_1^\sigma\,|\,\Omega_2^\sigma),$$

avec

$$\begin{aligned}
\Omega_1&:=\begin{pmatrix}101.3400...-7.5977...i & -2.6423...-2.6129...i\\ 23.9220...-47.3790...i & 11.1930...-4.6090...i\end{pmatrix}\\
\Omega_2&:=\begin{pmatrix}38.7080...-12.2930...i & -6.9177...+1.6149...i\\ -62.6300...+19.8910...i & -4.27540...+0.9980...i\end{pmatrix}\\
\Omega_1^\sigma&:=\begin{pmatrix}0.5369...-3.7425...i & 3.6304...-3.4371...i\\ 0.8688...-6.0555...i & -2.2437...+2.1243...i\end{pmatrix}\\
\Omega_2^\sigma&:=\begin{pmatrix}-1.4059...+2.3130...i & -1.3867...-5.5613...i\\ -1.4059...-2.3130...i & -1.3867...+5.5613...i\end{pmatrix}
\end{aligned}$$

Cela nous donne les matrices des périodes normalisées

$$\begin{aligned}
Z&:=\begin{pmatrix}-0.5010...+0.2910...i & 0.4370...-0.0125...i\\ 0.4370...-0.0126...i & 0.4138...+0.1802...i\end{pmatrix}\\
Z^\sigma&:=\begin{pmatrix}-0.2257...+0.8002...i & 0.5463...-0.3208...i\\ 0.5464...-0.3208...i & -0.6793...+0.4794...i\end{pmatrix}
\end{aligned}$$

On calcule alors les invariants d'Igusa-Clebsch I_2,I_4,I_6 et I_{10} avec 200 décimales de précision en utilisant Z et Z^σ, et on les identifie comme des éléments de F (en utilisant le Lemme 7.3). Dans l'espace projectif pondéré, $\mathbf{P}^2_{(1:2:3:5)}$, cela nous donne le point

$$\begin{aligned}
&(I_2:I_4:I_6:I_{10})=\\
&\left(1,\frac{-3080592b+36303121}{3750827536},\frac{-72429788520b+811909152327}{229715681614784},\frac{680871365928b-5817295179641}{6731436750404224780408}\right),
\end{aligned}$$

où $b=\sqrt{73}$. En utilisant l'alogrithme de Mestre [27], on obtient une courbe avec les invariants ci-dessus. La réduction de cette courbe avec l'algorithme de Bouyer-Streng [1] donne la courbe

$$\begin{aligned}
C':\ y^2=&(4w-19)x^6+(12w-56)x^5+(12w-74)x^4+(16w-10)x^3+(-12w-63)x^2\\
&+(12w+46)x-4w-15.
\end{aligned}$$

On obtient alors le modèle minimal global dans le théorème suivant.

Théorème 7.4. *Soit* $C : y^2 + Q(x)y = P(x)$ *la courbe sur* $F = \mathbf{Q}(\sqrt{73})$ *donnée par*

$$\begin{aligned} P &:= (w-5)x^6 + (3w-14)x^5 + (3w-19)x^4 + (4w-3)x^3 + (-3w-16)x^2 + (3w+11)x \\ &\quad + (-w-4); \\ Q &:= x^3 + x + 1. \end{aligned}$$

Alors, on a

(a) Le discriminant de la courbe est $\Delta_C = -\epsilon^2$. *Donc,* C *a bonne réduction partout.*

(b) La surface $A := \mathrm{Jac}(C)$ *a multiplication réelle par* $\mathbf{Z}[\frac{1+\sqrt{5}}{2}]$. *Elle est modulaire et correspond à l'unique orbite de Hecke* $[f]$ *dans* $S_2(1)$.

Démonstration. La seule différence avec l'exemple précédent est la preuve de la modularité. Ici, on remarque que le premier 3 est inerte dans $\mathcal{O}_f = \mathbf{Z}[\frac{1+\sqrt{5}}{2}]$. On montre alors que la surface A est modulaire en combinant les arguments dans [17] et [20, 21]. □

Contrairement aux exemples des Théorèmes 7.1 et 7.4, il peut y avoir des courbes dont les Jacobiennes ont bonne réduction partout même si cela n'est pas le case pour les courbes elles-mêmes. Dans notre dernier exemple, nous décrivons un tel exemple sur le corps $F = \mathbf{Q}(\sqrt{929})$, où le corps des coefficients de la forme est $\mathbf{Q}(\sqrt{13})$.

$\mathrm{N}\mathfrak{p}$	$\mathfrak{p}$	$a_{\mathfrak{p}}(f)$	$s_{\mathfrak{p}}(f)$	$t_{\mathfrak{p}}(f)$
2	$561w - 8830$	$-e + 1$	1	1
2	$561w + 8269$	e	1	1
5	$-4w - 59$	$-e + 1$	1	7
5	$4w - 63$	e	1	7
9	3	3	6	27
11	$-8342w + 131301$	$2e - 3$	-4	13
11	$8342w + 122959$	$-2e - 1$	-4	13
19	$-50w - 737$	$e - 2$	-3	37
19	$50w - 787$	$-e - 1$	-3	37
23	$-42832w + 674165$	$4e - 4$	-4	-2
23	$42832w + 631333$	$-4e$	-4	-2
29	$-2w + 31$	$-2e + 6$	10	70
29	$2w + 29$	$2e + 4$	10	70

TABLE 4 – Quelques coefficients de Fourier d'une forme nouvelle non changement de base de poids 2 et de niveau (1) sur $\mathbf{Q}(\sqrt{929})$. Ici, $e = (1 + \sqrt{13})/2$.

Théorème 7.5. *Soit* $C : y^2 + Q(x)y = P(x)$ *la courbe sur* F *donnée par*

$$\begin{aligned} P(x) &:= 23x^6 + (90w - 45)x^5 + 33601x^4 + (28707w - 14354)x^3 + 3192149x^2 \\ &\quad + (811953w - 405977)x + 19904990, \\ Q(x) &:= x^3 + x + 1. \end{aligned}$$

Alors, on a

(a) Le discriminant $\Delta_C = 3^{22}$, donc C a mauvaise réduction en (3).
(b) La surface $A := \mathrm{Jac}(C)$ a bonne réduction partout. Elle est modulaire et correspond à la forme nouvelle f donnée dans la Table 4.

Démonstration. Pour prover la modularité, on utilise [20, 21, Theorem 1.1 in Erratum]. Voir [11] pour plus de détails. □

Références

[1] F. Bouyer and M. Streng, *Examples of CM curves of genus two defined over the reflex field*, preprint, http://arxiv.org/pdf/1307.0486.pdf.

[2] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265.

[3] J. H. Bruinier, *Hilbert modular forms and their applications*, The 1-2-3 of modular forms, 105–179, Universitext, Springer, Berlin, 2008.

[4] A. Brumer, *The rank of $J_0(N)$*, Columbia University Number Theory Seminar (New York, 1992). Astérisque No. **228** (1995), 3, 41–68.

[5] W. Casselman, *On abelian varieties with many endomorphisms and a conjecture of Shimura's*, Invent. Math. **12** (1971), 225–236.

[6] J.-M. Couveignes and B. Edixhoven (eds.), *Computational aspects of modular forms and Galois representations. How one can compute in polynomial time the value of Ramanujan's tau at a prime*, Annals of Mathematics Studies **176**, Princeton University Press, Princeton, NJ, 2011.

[7] J. E. Cremona, *Modular symbols for $\Gamma_1(N)$ and elliptic curves with everywhere good reduction*, Math. Proc. Cambridge Philos. Soc. **111** (1992), no. 2, 199–218.

[8] J. E. Cremona, *Algorithms for modular elliptic curves*, second edition, Cambridge University Press, Cambridge, 1997, available at http://homepages.warwick.ac.uk/staff/J.E.Cremona//book/.

[9] L. Dembélé, *Explicit computations of Hilbert modular forms on $\mathbf{Q}(\sqrt{5})$*, Experiment. Math. **14** (2005), no. 4, 457–466.

[10] L. Dembélé and Steve Donnelly, *Computing Hilbert modular forms over fields with nontrivial class group*, Algorithmic number theory (Banff, 2008), Lecture Notes in Comput. Sci., vol. **5011**, Springer, Berlin, 2008, 371–386.

[11] , L. Dembélé and A. Kumar, *Examples of abelian surfaces with everywhere good reduction*, Math. Ann. **364** (2016), no. 3-4, 1365–1392.

[12] L. Dembélé and J. Voight, *Explicit methods for Hilbert modular forms*, Elliptic curves, Hilbert modular forms and Galois deformations, Birkhauser, Basel, 2013, 135–198.

[13] F. Diamond and J. Shurman, *A first course in modular forms.* Graduate Texts in Mathematics, **228**. Springer-Verlag, New York, 2005. xvi+436 pp.

[14] J. R. Doyle and D. Krumm, *Computing algebraic numbers of bounded height*, Math. Comp. (to appear), http://arxiv.org/pdf/1111.4963.pdf.

[15] N. D. Elkies, *Elliptic curves of unit discriminant over real quadratic number fields*, database available at http://math.harvard.edu/~elkies/rqfu.

[16] N. D. Elkies and A. Kumar, *K3 surfaces and equations for Hilbert modular surfaces*, Algebra Number Theory **8** (2014), no. 10, 2297–2411.

[17] J. S. Ellenberg, *Serre's conjecture over* $\mathbf{F}_9$, Ann. of Math. (2) **161** (2005), no. 3, 1111–1142.

[18] E. Freitag, *Hilbert modular forms*, Springer-Verlag, Berlin, 1990.

[19] N. Freitas, B. V. Le Hung, and S. Siksek, *Elliptic curves over real quadratic fields are modular*, Invent. Math. **201** (2015), no. 1, 159–206.

[20] T. Gee, *A modularity lifting theorem for weight two Hilbert modular forms*, Math. Res. Lett. **13** (2006), no. 5-6, 805–811.

[21] T. Gee, *Erratum–a modularity lifting theorem for weight two Hilbert modular forms*, Math. Res. Lett. **16** (2009), no. 1, 57–58.

[22] E. González-Jiménez, J. González and J. Guàrdia, *Computations on modular Jacobian surfaces*, Algorithmic number theory (Sydney, 2002), 189–197, Lecture Notes in Comput. Sci., **2369**, Springer, Berlin, 2002.

[23] E. Z. Goren, *Lectures on Hilbert modular varieties and modular forms*. With the assistance of Marc-Hubert Nicole. CRM Monograph Series, **14**. American Mathematical Society, Providence, RI, 2002. x+270 pp.

[24] J. Guàrdia, *Jacobian nullwerte and algebraic equations*, J. Algebra **253** (2002), no. 1, 112–132.

[25] C. Khare and J.-P. Wintenberger, *On Serre's conjecture for* 2*-dimensional mod* p *representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Ann. of Math. (2) **169** (2009), no. 1, 229–253.

[26] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. **76** (1984), no. 2, 179–330.

[27] J.-F. Mestre, *Construction de courbes de genre* 2 *à partir de leurs modules*, Effective methods in algebraic geometry (Castiglioncello, 1990), 313–334, Progr. Math. **94**, Birkhäuser Boston, Boston, MA, 1991.

[28] T. Miyake, *On automorphic forms on* GL_2 *and Hecke operators*, Ann. of Math. (2) **94** (1971), 174–189.

[29] R. Pinch, *Elliptic curves with everywhere good reduction*, preprint, http://www.chalcedon.demon.co.uk/rgep/publish.html#04.

[30] W. Stein et al., *Sage Mathematics Software* (Version 5.0), The Sage Development Team, 2012, http://www.sagemath.org.

[31] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

[32] J.-P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230.

[33] B. Setzer, *Elliptic curves with good reduction everywhere over quadratic fields and having rational* j*-invariant*, Illinois J. Math. **25** (1981) no. 2, 233–245.

[34] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, reprint of the 1971 original, Publications of the Mathematical Society of Japan **11**. Kanô Memorial Lectures no. 1, Princeton University Press, Princeton, NJ, 1994.

[35] G. Shimura, *Class fields over real quadratic fields and Hecke operators*, Ann. of Math. (2) **95** (1972), 130–190.

[36] G. Shimura, *On the factors of the jacobian variety of a modular function field*, J. Math. Soc. Japan **25** (1973), 523–544.

[37] G. Shimura, *The special values of the zeta functions associated with Hilbert modular forms*, Duke Math. J. **45** (1978), no. 3, 637–679.

[38] J. .H. Silverman, *The arithmetic of elliptic curves.* Second edition. Graduate Texts in Mathematics, **106**. Springer, Dordrecht, 2009. xx+513 pp.

[39] N. P. Smart, *S-unit equations, binary forms and curves of genus* 2, Proc. London Math. Soc. (3) **75** (1997), no. 2, 271–307.

[40] C. M. Skinner and A. J. Wiles, *Residually reducible representations and modular forms*, Inst. Hautes Études Sci. Publ. Math. **89** (1999), 5–126.

[41] W. Stein, *Modular forms, a computational approach*, with an appendix by Paul E. Gunnells, Graduate Studies in Mathematics, **79**. American Mathematical Society, Providence, RI, 2007. xvi+268 pp.

[42] R. J. Stroeker, *Reduction of elliptic curves over imaginary quadratic number fields*, Pacific J. Math. **108** (1983), no. 2, 451–463.

[43] G. van der Geer, *Hilbert Modular Surfaces*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), **16**. Springer-Verlag, Berlin, 1988.

[44] S. Zhang, *Heights of Heegner points on Shimura curves*, Ann. of Math. (2) **153** (2001), no. 1, 27–147.

[45] A. Wiles, *Modular elliptic curves and Fermat's last theorem.* Ann. of Math. (2) **141** (1995), no. 3, 443–551.