Isogenous (non-)hyperelliptic CM Jacobians: Shimura class groups, algorithms, and equations

Jeroen Sijsling (Universität Ulm)

joint work with
Bogdan Dina (Universität Ulm)
and
Sorina Ionica (Université de Picardie Jules Verne)

Obseminar Algebra und Zahlentheorie
Universität Ulm
29 April 2021

Recapitulation

Last time, Bogdan treated:

- The construction of a principally polarized abelian variety $(\mathbb{C}^g/\Phi(\mathfrak{a}), E)$ from a fractional ideal $\mathfrak{a}$ of a CM field K and a CM type Φ of K;

Recapitulation

Last time, Bogdan treated:

- The construction of a principally polarized abelian variety $(\mathbb{C}^g/\Phi(\mathfrak{a}), E)$ from a fractional ideal $\mathfrak{a}$ of a CM field K and a CM type Φ of K;
- The classification of (primitive) CM types Φ and their reflex fields K^r for sextic CM fields K. (Case $g = 3$.)

Recapitulation

Last time, Bogdan treated:

- The construction of a principally polarized abelian variety $(\mathbb{C}^g/\Phi(\mathfrak{a}), E)$ from a fractional ideal $\mathfrak{a}$ of a CM field K and a CM type Φ of K;
- The classification of (primitive) CM types Φ and their reflex fields K^r for sextic CM fields K. (Case $g = 3$.)

Main result

Heuristically, there are only 14 sextic CM fields K in the LMFDB for which there exists both a hyperelliptic and a non-hyperelliptic Jacobian with primitive CM by $\mathbb{Z}_K$.

Goal

Today, our goal is the following:

- Describe algorithms that, given a sextic CM field K, find representatives of the set of PPAVs with primitive CM by $\mathbb{Z}_K$ up to Galois conjugacy.
- Find defining equations for corresponding curves of genus 3 in a special case.

The group $\mathcal{C}_K$

Given a CM field K, let $\mathcal{M}_K$ be the set of isomorphism classes of PPAVs with primitive CM by $\mathbb{Z}_K$.

In order to understand the Galois action of $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ on $\mathcal{M}_K$, we need the following definition.

Definition

The Shimura class group $\mathcal{C}_K$ of K is the abelian group of equivalence classes

$$\mathcal{C}_K = \left\{(\mathfrak{b}, \beta) : \mathfrak{b} \subset K,\ \beta \in (K_0^*)^+ \text{ with } \mathfrak{b}\overline{\mathfrak{b}} = \beta\mathbb{Z}_K\right\} / \sim$$

where $(\mathfrak{b}, \beta) \sim (\mathfrak{b}', \beta')$ if $(\mathfrak{b}', \beta') = (x\mathfrak{b}, x\overline{x}\beta)$ for $x \in K^*$.

The group $\mathcal{C}_K$

Definition

The Shimura class group $\mathcal{C}_K$ of K is the abelian group of equivalence classes

$$\mathcal{C}_K = \left\{(\mathfrak{b}, \beta) : \mathfrak{b} \subset K,\ \beta \in (K_0^*)^+ \text{ with } \mathfrak{b}\overline{\mathfrak{b}} = \beta\mathbb{Z}_K\right\} / \sim$$

where $(\mathfrak{b}, \beta) \sim (\mathfrak{b}', \beta')$ if $(\mathfrak{b}', \beta') = (x\mathfrak{b}, x\overline{x}\beta)$ for $x \in K^*$.

There is an exact sequence

$$1 \to (\mathbb{Z}_{K_0}^*)^+ / N_{K|K_0}(\mathbb{Z}_K^*) \to \mathcal{C}_K \to \mathrm{Cl}(K) \to \mathrm{Cl}^+(K_0).$$

The group C

Definition

We let

$$C = \left\{(\mathfrak{b}, \beta) : \mathfrak{b} \subset \mathbb{Z}_K,\ \beta \in K_0^* \text{ with } \mathfrak{b}\bar{\mathfrak{b}} = \beta\mathbb{Z}_K\right\} / \sim$$

where $(\mathfrak{b}, \beta) \sim (\mathfrak{b}', \beta')$ if $(\mathfrak{b}', \beta') = (x\mathfrak{b}, x\bar{x}\beta)$ for $x \in K^*$.

The group C acts on the pairs $(\mathfrak{a}, \xi)$ from Bogdan's talk via

$$(\mathfrak{b}, \beta)(\mathfrak{a}, \xi) = (\mathfrak{b}^{-1}\mathfrak{a}, \beta\xi).$$

Actions

Proposition

Let $c = (\mathfrak{b}, \beta) \in C$, and let $(\mathfrak{b}, \beta)(\mathfrak{a}, \xi) = (\mathfrak{a}', \xi')$. Let Φ' be the CM type of $(\mathfrak{a}', \xi')$. Then $\Phi' = \Phi$ if and only if $c \in \mathcal{C}_K$.

Actions

Given a CM type Φ, we let $\mathcal{M}_K(\Phi) \subset \mathcal{M}_K$ be the subset of PPAV that admit CM of type Φ.

Proposition

The set $\mathcal{M}_K(\Phi)$ is a torsor under $\mathcal{C}_K$.

Galois conjugation

Proposition

Let A be a PPAV that admits the CM type Φ up to equivalence. If $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$, then σA admits CM type $\sigma\Phi$ up to equivalence.

Galois conjugation

Proposition

Let A be a PPAV that admits the CM type Φ up to equivalence. If $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$, then σA admits CM type $\sigma\Phi$ up to equivalence.

Corollary

If $g = 3$, then the Galois action on the components $\mathcal{M}_K(\Phi)$ of $\mathcal{M}_K$ is transitive.

We fix a primitive type Φ for the remainder of the talk, and with it, a component $\mathcal{M}_K(\Phi)$. Recall that $\sigma\Phi = \Phi$ iff $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}|K^r)$.

Galois conjugation

We combine the norm map $N = N_{K^r|\mathbb{Q}} : K^r \to \mathbb{Q}_{>0}$ with the reflex type norm

$$\begin{aligned} N_{\Phi^r} : \mathrm{Cl}(K^r) &\to \mathrm{Cl}(K) \\ [\mathfrak{a}] &\mapsto \mathbb{Z}_{K^r} \cap \prod_{\varphi \in \Phi^r} \varphi(\mathfrak{a})\mathbb{Z}_L, \end{aligned}$$

to get

$$\begin{aligned} \mathcal{N}_{\Phi^r} : \mathrm{Cl}(K^r) &\to \mathcal{C}_K \\ [\mathfrak{a}] &\mapsto (N_{\Phi^r}(\mathfrak{a}), N(\mathfrak{a})). \end{aligned}$$

Galois conjugation

Main Theorem of Complex Multiplication

Let $(A, E) \cong A(\mathfrak{a}, \xi)$ in $\mathcal{M}_K(\Phi)$, and let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}} \mid K^r)$. Suppose that under the Artin map, the element σ corresponds to the class of the ideal $\mathfrak{b}$. Then

$$\sigma(A(\mathfrak{a}, \xi)) \cong A(\mathcal{N}_{\Phi^r}(\mathfrak{b})(\mathfrak{a}, \xi)) \in \mathcal{M}_K(\Phi).$$

To find a small set of representatives up to Galois conjugation it therefore suffices to show that $\mathcal{N}_{\Phi^r}$ has large image.

Some lemmata

Lemma

Let K be a sextic CM field with Galois group $C_2^3 \rtimes C_3$ or $C_2^3 \rtimes S_3$, and let Φ be a CM type of K. Then for all $\mathfrak{a} \subset K$ we have

$$N_{\Phi^r}(N_\Phi(\mathfrak{a})) = N_{K|\mathbb{Q}}(\mathfrak{a})^2(\mathfrak{a}\overline{\mathfrak{a}}^{-1})^2.$$

Some lemmata

Lemma

Let K be a sextic CM field with Galois group $C_2^3 \rtimes C_3$ or $C_2^3 \rtimes S_3$, and let Φ be a CM type of K. Then for all $\mathfrak{a} \subset K$ we have

$$N_{\Phi^r}(N_\Phi(\mathfrak{a})) = N_{K|\mathbb{Q}}(\mathfrak{a})^2(\mathfrak{a}\overline{\mathfrak{a}}^{-1})^2.$$

We translate the element of the group algebra:

$$H+n_1H+n_2H+n_1n_2H+\sigma H+n_1\sigma H+n_2\sigma H+n_1n_2\sigma H+\sigma^2 H+n_1\sigma^2 H+n_2\sigma^2 H+n_1n_2\sigma^2 H$$

$$=H+H+H+H+\sigma H+\sigma\rho H+\sigma H+\sigma\rho H+\sigma^2 H+\sigma^2 H+\sigma^2\rho H+\sigma^2\rho H$$

$$=4H+2\sigma H+2\sigma^2 H+2\sigma\rho H+2\sigma^2\rho H$$

$$=(2H+2\sigma H+2\sigma^2 H+2\rho H+2\sigma\rho H+2\sigma^2\rho H)+(2H-2\rho H).$$

Some lemmata

Proposition

Let K be a sextic CM field with Galois group $C_2^3 \rtimes C_3$ or $C_2^3 \rtimes S_3$, and let Φ be a CM type of K.

If $[\mathfrak{b}] \in \mathrm{Cl}(K)$ satisfies $\mathfrak{b}\overline{\mathfrak{b}} = \beta\mathbb{Z}_K$ for $\beta \in K_0^*$, then $[\mathfrak{b}^4]$ is in the image of the reflex type norm $N_{\Phi^r} : \mathrm{Cl}(K^r) \to \mathrm{Cl}(K)$.

Some lemmata

Similarly:

Proposition

Let K be a sextic CM field with Galois group isomorphic to C_6 or D_6, and let Φ be a primitive CM type of K.

If $[\mathfrak{b}] \in \mathrm{Cl}(K)$ satisfies $\mathfrak{b}\overline{\mathfrak{b}} = \beta\mathbb{Z}_K$ for $\beta \in K_0^*$, then $[\mathfrak{b}^2]$ is in the image of the reflex type norm $N_{\Phi^r} : \mathrm{Cl}(K^r) \to \mathrm{Cl}(K)$.

Large image result

Theorem

Fix $A(\mathfrak{a}_0, \xi_0)$ in $\mathcal{M}_K(\Phi)$, and let

- $G_2 = \ker(N_{K|K_0}) \subset \mathrm{Cl}(K)$;
- $B =$ set of representatives of quotient $Q = G_2/eG_2$, where $e = 2$ if $\mathrm{Gal}(K) \in \{C_6, D_6\}$ and where $e = 4$ if $\mathrm{Gal}(K) \in \left\{C_2^3 \rtimes C_3, C_2^3 \rtimes S_3\right\}$.
- $V =$ set of representatives of quotient $(\mathbb{Z}_{K_0}^*)^+/N_{K|K_0}(\mathbb{Z}_K^*)$.

Let $A(\mathfrak{a}, \xi)$ in $\mathcal{M}_K(\Phi)$ be given. Then the Galois orbit of $A(\mathfrak{a}, \xi)$ under $G^r = \mathrm{Gal}(\overline{\mathbb{Q}}|K^r)$ contains $A(\mathfrak{b}\mathfrak{a}_0, v\beta^{-1}\xi_0)$, where $\mathfrak{b} \in B$, where $\beta \in K_0$ generates $\mathfrak{b}\overline{\mathfrak{b}}$, and where $v \in V$.

Large image result

Theorem

Fix $A(\mathfrak{a}_0, \xi_0)$ in $\mathcal{M}_K(\Phi)$, and let

- $G_2 = \ker(N_{K|K_0}) \subset \mathrm{Cl}(K)$;
- $B =$ set of representatives of quotient $Q = G_2/eG_2$, where $e = 2$ if $\mathrm{Gal}(K) \in \{C_6, D_6\}$ and where $e = 4$ if $\mathrm{Gal}(K) \in \left\{C_2^3 \rtimes C_3, C_2^3 \rtimes S_3\right\}$.
- $V =$ set of representatives of quotient $(\mathbb{Z}_{K_0}^*)^+/N_{K|K_0}(\mathbb{Z}_K^*)$.

Let $A(\mathfrak{a}, \xi)$ in $\mathcal{M}_K(\Phi)$ be given. Then the Galois orbit of $A(\mathfrak{a}, \xi)$ under $G^r = \mathrm{Gal}(\overline{\mathbb{Q}}|K^r)$ contains $A(\mathfrak{b}\mathfrak{a}_0, v\beta^{-1}\xi_0)$, where $\mathfrak{b} \in B$, where $\beta \in K_0$ generates $\mathfrak{b}\overline{\mathfrak{b}}$, and where $v \in V$.

Use

$$1 \to (\mathbb{Z}_{K_0}^*)^+/N_{K|K_0}(\mathbb{Z}_K^*) \to \mathcal{C}_K \to \mathrm{Cl}(K) \to \mathrm{Cl}^+(K_0).$$

Nuts and bolts

- Finding a pair $(\mathfrak{a}_0, \xi_0)$;

Nuts and bolts

- Finding a pair $(\mathfrak{a}_0, \xi_0)$;
- Minimizing the representatives in B and V;
- Computing theta-null values (Labrande).

An example

We consider the CM field K defined by $x^6 + 10x^4 + 21x^2 + 4$. There are two Galois orbits of length 4, one of them hyperelliptic and the other non-hyperelliptic.

Fiddling around with Mestre's reconstruction algorithms shows that a corresponding hyperelliptic curve X can be found over the subfield over the quartic subfield L of the reflex field that is defined by the polynomial $x^4 - 5x^2 - 2x + 1$.

Equation for X

We have

$$\begin{aligned} X: \quad y^2 = {} & x^8+(-28r^3-4r^2+132r+84)x^7 \\ & +(-600r^3-160r^2+2920r+2044)x^6 \\ & +(-3532r^3-940r^2+17224r+11944)x^5 \\ & +(9040r^3+2890r^2-44860r-31460)x^4 \\ & +(167536r^3+49480r^2-824532r-576212)x^3 \\ & +(-226976r^3-64932r^2+1113648r+776872)x^2 \\ & +(-244204r^3-69572r^2+1197716r+835300)x \\ & +(319956r^3+94725r^2-1575062r-1100801) \end{aligned}$$

where r is a zero of $x^4 - 5x^2 - 2x + 1$.

How to recover the plane quartic curve

Fact

There is a plane quartic curve Y whose Jacobian is isogenous to that of X by an isogeny of degree 2.

Over $\mathbb{C}$, we can recover a Weber model of Y from theta-null values of a corresponding period matrix.

How to recover the plane quartic curve

Fact

There is a plane quartic curve Y whose Jacobian is isogenous to that of X by an isogeny of degree 2.

Over $\mathbb{C}$, we can recover a Weber model of Y from theta-null values of a corresponding period matrix.

Let

$$a_{11} = i\frac{\vartheta_{33}\vartheta_5}{\vartheta_{40}\vartheta_{12}}, \quad a_{12} = i\frac{\vartheta_{21}\vartheta_{49}}{\vartheta_{28}\vartheta_{56}}, \quad a_{13} = i\frac{\vartheta_7\vartheta_{35}}{\vartheta_{14}\vartheta_{42}},$$
$$a_{21} = i\frac{\vartheta_5\vartheta_{54}}{\vartheta_{27}\vartheta_{40}}, \quad a_{22} = i\frac{\vartheta_{49}\vartheta_2}{\vartheta_{47}\vartheta_{28}}, \quad a_{23} = i\frac{\vartheta_{35}\vartheta_{16}}{\vartheta_{61}\vartheta_{14}},$$
$$a_{31} = -\frac{\vartheta_{54}\vartheta_{33}}{\vartheta_{12}\vartheta_{27}}, \quad a_{32} = \frac{\vartheta_2\vartheta_{21}}{\vartheta_{56}\vartheta_{47}}, \quad a_{33} = \frac{\vartheta_{16}\vartheta_7}{\vartheta_{42}\vartheta_{61}}.$$

How to recover the plane quartic curve

Fact

There is a plane quartic curve Y whose Jacobian is isogenous to that of X by an isogeny of degree 2.

Over $\mathbb{C}$, we can recover a Weber model of Y from theta-null values of a corresponding period matrix.

Then

$$Y : (x_1u_1 + x_2u_2 - x_3u_3)^2 - 4x_1u_1x_2u_2 = 0$$

where

$$\begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ \frac{1}{a_{11}} & \frac{1}{a_{12}} & \frac{1}{a_{13}} \\ \frac{1}{a_{21}} & \frac{1}{a_{22}} & \frac{1}{a_{23}} \end{bmatrix}^{-1} \cdot \begin{bmatrix} 1 & 1 & 1 \\ a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}.$$

How to recover the plane quartic curve

Fact

Over $\mathbb{C}$, we can recover a Weber model of Y from theta-null values.

Let $P_X \in M_{3,6}(\mathbb{C})$ be the period matrix of X with respect to $(dx/y, xdx/y, x^2dx/y)$. Let P_Y be the period matrix of Y with respect to $(xdx(\partial F/\partial y)^{-1}, ydx(\partial F/\partial y)^{-1}, dx(\partial F/\partial y)^{-1})$.

Proposition

There exist matrices $T \in M_{3,3}(\mathbb{C})$ and $R \in M_{6,6}(\mathbb{Z})$ such that R has determinant 2 and

$$TP_Y = P_X R.$$

Moreover, the pair (T, R) is uniquely determined up to a minus sign.

How to recover the plane quartic curve

Proposition

Let F be the Weber model with period matrix P_Y, and let F_0 be a multiple of $F \cdot T$ that is normalized in such a way that one of its coefficients is in L. Then

$$Y_0 : F_0(x, y, z) = 0$$

is a model of Y over L.

Equation for Y

We get

$$\begin{aligned} Y_0 : \quad & (14106r^3-150652r^2+185086r+292255)x^4+(-171112r^3+44200r^2+916008r+93360)x^3y \\ & +(-120788r^3+49032r^2+382244r+300708)x^3z+(467744r^3-209864r^2-2160704r+183416)x^2y^2 \\ & +(-72248r^3+64768r^2+347488r-362984)x^2yz+(5720r^3-12378r^2-15628r+50692)x^2z^2 \\ & +(-512608r^3+349824r^2+2423616r-580448)xy^3+(202192r^3-151024r^2-1180320r+403568)xy^2z \\ & +(6512r^3-11272r^2+178120r-71336)xyz^2+(-11832r^3+12268r^2-844r+1376)xz^3 \\ & +(263424r^3-176880r^2-1159232r+335040)y^4+(-201216r^3+100448r^2+856096r-249632)y^3z \\ & +(62112r^3+1984r^2-226512r+71624)y^2z^2+(-12520r^3-13112r^2+27736r-5360)yz^3 \\ & +(1526r^3+2411r^2-658r+197)z^4 = 0. \end{aligned}$$

where r is a zero of $x^4 - 5x^2 - 2x + 1$.