JACOBIANS WITH COMPLEX MULTIPLICATION

ANGEL CAROCCA, HERBERT LANGE AND RUBÍ E. RODRÍGUEZ

Abstract. We construct and study two series of curves whose Jacobians admit complex multiplication. The curves arise as quotients of Galois coverings of the projective line with Galois group metacyclic groups $G_{q,3}$ of order $3q$ with $q \equiv 1 \mod 3$ an odd prime, and G_m of order 2^{m+1}. The complex multiplications arise as quotients of double coset algebras of the Galois groups of these coverings. We work out the CM-types and show that the Jacobians are simple abelian varieties.

1. Introduction

An abelian variety A over an algebraically closed field is said to have or to admit *complex multiplication* if there is a CM-field K of degree $2\dim(A)$ over $\mathbb{Q}$ such that $K \subset \mathrm{End}_{\mathbb{Q}}(A)$. A smooth projective curve C is said to admit *complex multiplication* if its Jacobian variety does. In these cases one says that A (respectively C) has complex multiplication *by* K. It is known (see [8]) that abelian varieties which admit complex multiplication are $\mathbb{C}$-isomorphic to abelian varieties defined over number fields. Since curves and their Jacobians may be defined over the same field, Jacobians which admit complex multiplication are interesting for algebraic geometers and number theorists.

In this paper we use Galois coverings of the projective line with metacyclic Galois groups, in order to construct and investigate two series of curves with complex multiplication.

For the first series let q be an odd prime and n a positive integer such that $n|q-1$. Consider the group

$$G_{q,n} := \langle a, b \mid a^q = b^n = 1,\ b^{-1}ab = a^k \rangle$$

where $1 < k < q$ is such that $k^n \equiv 1 \mod q$ and $k^m \not\equiv 1 \mod q$ for all $1 \leq m < n$ (that is, the order of k mod q is n). Denote the subgroup generated by b by

$$H = \langle b \rangle.$$

In [4] Ellenberg used Galois coverings Y of the projective line with Galois group $G_{q,n}$, such that the Jacobian of the quotient curve $X = Y/H$ admits a totally real field as an endomorphism algebra. In this note we show that his method can also be applied to construct smooth projective curves admitting complex multiplication. In fact, we show that for every q as above with $n = 3$ there is exactly one Galois covering Y such that $X = Y/H$ has complex multiplication. To be more precise, our first result is the following theorem. To state it, let $\zeta = \zeta_q$ denote a primitive q-th root of unity and let $\mathbb{Q}(\zeta^{(n)})$ denote the unique subfield of index n of the cyclotomic field $\mathbb{Q}(\zeta)$. Clearly $\mathbb{Q}(\zeta^{(n)})$ is a

1991 *Mathematics Subject Classification.* 11G15, 14K22 .

Key words and phrases. Complex Multiplications, Jacobians, Abelian Varieties.

The first and third author were supported by Fondecyt grants 1095165 and 1100767 respectively.

CM-field if and only if n is odd, which we assume in the sequel.

Theorem 1. *Suppose Y is a Galois covering of $\mathbb{P}^1$ with group $G_{q,n}$ with n odd and branch points $p_i \in \mathbb{P}^1$ of ramification index n_i for $i = 1, \dots, r$ over an algebraically closed field $\mathcal{K}$ of characteristic 0.*

(1) *The curve $X = Y/H$ admits complex multiplication by $\mathbb{Q}(\zeta^{(n)})$ if and only if $n = r = 3$ and $\{n_1, n_2, n_3\} = \{q, 3, 3\}$.*
(2) *For every odd prime $q \equiv 1 \mod 3$ and $n = 3$ there is, up to isomorphism, exactly one such curve Y.*

Furthermore, in this case the following results hold.

(3) *The Jacobian JY is isogenous to JX^3.*
(4) *The Jacobian JX is a simple abelian variety, of dimension $\frac{q-1}{6}$.*
(5) *The function field of Y over $\mathcal{K}$ is*

$$\mathcal{K}(Y) = \mathcal{K}(z, y)$$

where $\mathcal{K}(\mathbb{P}^1) = \mathcal{K}(x)$ and z and y satisfy the equations

$$z^3 = \frac{x}{x-2} \quad \text{and} \quad y^q = (z-1)(z-\omega_3)^k (z-\omega_3^2)^{k^2},$$

with ω_3 a primitive third root of unity.

For the second series of curves let $m \geq 3$ and consider the group

$$G_m = \langle a, b \mid a^{2^m} = b^2 = 1, bab = a^d \rangle$$

where $d = 2^{m-1} - 1$ (note that $d^2 \equiv 1 \mod 2^m$).

Let $\xi = \xi_{2^m}$ denote a primitive 2^m-th-root of unity, and observe that $\xi + \xi^d = \xi - \overline{\xi}$ is not real.

Consider the complex irreducible representation V of G_m given by

$$V(a) = \begin{pmatrix} \xi & 0 \\ 0 & \xi^d \end{pmatrix}, \; V(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Its character field $K_V = \mathbb{Q}[\xi + \xi^d]$ is a cyclic CM-field of degree $[K_V : \mathbb{Q}] = 2^{m-2}$.

Theorem 2. *Let $m \geq 3$. Then*

(1) *There exists a Galois covering $Y \to \mathbb{P}^1$ with Galois group G_m, branched at 3 points in $\mathbb{P}^1$ with monodromy a, b and ab.*
(2) *The curve $X = Y/\langle b \rangle$ and the Prym variety P of the covering $Y \to X$ have complex multiplication by K_V.*
(3) *JY is isogenous to JX^2.*
(4) *JX and P are isogenous simple principally polarized abelian varieties, of dimension 2^{m-3}.*
(5) *Y and X are hyperelliptic curves. An equation for Y is*

$$y^2 = x(x^{2^{m-1}} - 1).$$

In the second section we fix the notation and collect some preliminaries on the representations of the groups $G_{q,n}$ and G_m.

Section 3 contains the proof of Theorem 1. To be more precise, in 3.1 we prove parts (1) and (2) of the theorem. In 3.2 we see how the Jacobians of X and Y are related. In fact, JY is isogenous to the third power of JX (part (3)). In particular JY also admits complex multiplication. In 3.3 we apply the theorem of Chevalley-Weil in order to compute the CM-type of JY. This implies part (4) of the theorem. Finally in 3.4 we work out the function field of the curve Y.

In Section 4 we prove Theorem 2. To be more precise, in 4.1 we prove (1), (2) and (3) of Theorem 2. Section 4.2 contains the proof of (4). Moreover, in this section we compute the CM-types of JY and JX. Finally, in 4.3 we give the equations of the curves Y and X. We did not include the equation of X in Theorem 2, because it requires some more notation.

We would like to thank Eduardo Friedman and Wulf-Dieter Geyer for some valuable conversations.

2. Preliminaries

2.1. **Some notation.** For any finite group G we denote by χ_0 the trivial representation of G. If H is any subgroup of G, χ_H will denote the character of the representation of G induced by the trivial representation of H. If H is cyclic generated by $g \in G$, we also write χ_g for $\chi_{\langle g \rangle}$. In particular, if $H = \{1\}$, then $\chi_1 = \chi_{\{1\}}$ is the character of the regular representation of G.

If V is a representation of G, then V^H denotes the subspace of V fixed by H.

All curves will be smooth, projective and irreducible; for simplicity we assume the curves to be defined over the field of complex numbers. As in [4], the results remain valid over any algebraically closed field of characteristic not dividing the group orders by using l'adic cohomology and Grothendieck's algebraic fundamental group instead of singular cohomology and usual monodromy.

2.2. **Representations of $G_{q,n}$.** Let $G_{q,n}$ denote the group defined in the introduction. As a semidirect product of the subgroup $N = \langle a \rangle$ by the subgroup $H = \langle b \rangle$, it is a metacyclic group of order qn.

Let $\omega = \omega_n$ be a primitive n-th root of unity. The non-isomorphic one-dimensional representations of $G_{q,n}$ are the following:

$$\chi_i(a) = 1 \ ; \ \chi_i(b) = \omega^i \ \text{ for } \ i = 0, \dots n-1.$$

There are exactly

$$s := \frac{q-1}{n}$$

complex irreducible representations V_i of dimension n, defined as follows. If $a^{i_1}, \dots, a^{i_s}$ with $s = \frac{q-1}{n}$ is a set of representatives for the action of H on N defined by the relation $b^{-1}ab = a^k$, the corresponding orbits are $\{a^{i_j}, a^{ki_j}, \dots, a^{k^{n-1}i_j}\}$ for $j = 1, \dots, s$. If $\zeta = \zeta_q$ denotes a primitive q-th root of unity, then for $j = 1, \dots, s$ the representation V_j is given by

$$V_j(a) = \begin{pmatrix} \zeta^{i_j} & 0 & 0 & \cdots & 0 \\ 0 & \zeta^{ki_j} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & \zeta^{k^{n-1}i_j} \end{pmatrix}; \qquad V_j(b) = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

For any $\ell | n$ consider the subgroup $S_\ell = \langle b^{\frac{n}{\ell}} \rangle$ of H of order ℓ. Also, $S_\ell \subset \ker(\chi_i)$ if and only if $n | \frac{n}{\ell} i$, and there are exactly $\frac{n}{\ell}$ such i's. We have

$$\dim V_j^H = 1 \quad \text{and} \quad \dim V_j^{S_\ell} = \frac{n}{\ell}\,,$$

and it is easy to check that

$$\begin{aligned} \chi_N &= \chi_0 + \chi_1 + \cdots + \chi_{n-1}, \\ \chi_H &= \chi_0 + \chi_{V_1} + \chi_{V_2} + \cdots + \chi_{V_s}, \\ \chi_{S_\ell} &= \sum_{\substack{0 \le i < n \\ n | \frac{n}{\ell} i}} \chi_i + \frac{n}{\ell}(\chi_{V_1} + \chi_{V_2} + \cdots + \chi_{V_s}). \end{aligned}$$

We will use the following result, for the proof of which we refer to [1] or [4]. Let G denote a finite group acting on a compact Riemann surface Y with monodromy $g_1, g_2, \ldots, g_u$. Let χ_Y denote the character of the representation $H^1(Y, \mathbb{Q})$. Then

$$\chi_Y = 2\chi_0 + (2g(Y/G) - 2 + u)\chi_{\{1\}} - \sum_{j=1}^{u} \chi_{\langle g_j \rangle}. \tag{2.1}$$

The following proposition appears essentially in [4].

Proposition 2.1. *Suppose the metacyclic group $G_{q,n}$ acts on the compact Riemann surface Y with monodromy $g_1, \ldots, g_r, g_{r+1} \ldots, g_{r+t}$, where g_j has order n_j (dividing n) for $j = 1, \ldots, r$ and order q for $j = r+1 \ldots, u = r+t$ and assume $g(Y/G_{q,n}) = 0$. Then*

$$\chi_Y = (r-2)\sum_{i=1}^{n-1} \chi_i - \sum_{j=1}^{r} \sum_{\substack{0 < i < n \\ n | \frac{n}{n_j} i}} \chi_i + \left(n(r+t-2) - \sum_{j=1}^{r} \frac{n}{n_j} \right) (\chi_{V_1} + \cdots \chi_{V_s}).$$

Proof. First observe that if g_j has order n_j dividing n, then $\langle g_j \rangle$ is conjugate to S_{n_j}, and that if g_j has order q then $\langle g_j \rangle = N$.

Then, from (2.1) and using the formulas above for χ_N, χ_H and χ_{S_ℓ}, we obtain

$$\begin{aligned} \chi_Y \;\; = \;\; & 2\chi_0 + (r+t-2)\left(\chi_0 + \cdots + \chi_{n-1} + n(\chi_{V_1} + \cdots + \chi_{V_s})\right) \\ & - \left(t(\chi_0 + \cdots + \chi_{n-1}) + (\sum_{j=1}^{r} \frac{n}{n_j})(\chi_{V_1} + \cdots + \chi_{V_s}) + \sum_{j=1}^{r} \sum_{\substack{0 \le i < n \\ n | \frac{n}{n_j} i}} \chi_i \right). \end{aligned}$$

This implies the assertion. $\square$

2.3. **Representations of the group G_m.** For $m \geq 3$ let G_m denote the group defined in the introduction. As a semidirect product of the subgroup $N = \langle a \rangle$ by the subgroup $H = \langle b \rangle$, it is a metacyclic group of order 2^{m+1}.

The group G_m has 3 nontrivial representations of degree 1, namely

$$\chi_1 : \ a \mapsto 1, \ b \mapsto -1, \qquad \chi_2 : \ a \mapsto -1, \ b \mapsto 1, \qquad \chi_3 : \ a \mapsto -1, \ b \mapsto -1.$$

Let $\xi = \xi_{2^m}$ denote a primitive 2^m-th root of unity. For $i = 1, \dots, m-1$ consider the representation V_i defined by

$$V_i(a) = \begin{pmatrix} \xi^{2^{i-1}} & 0 \\ 0 & \xi^{2^{i-1}d} \end{pmatrix}, \qquad V_i(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Note that V_1 is the representation V of the introduction. V_i is a complex irreducible representation with Galois character field

$$K_i = \mathbb{Q}[\xi^{2^{i-1}} + \xi^{2^{i-1}d}]$$

with $[K_i : \mathbb{Q}] = 2^{m-1-i}$. Hence, V_i has 2^{m-1-i} non-equivalent complex irreducible Galois-conjugate representations $V_i^1, \dots, V_i^{2^{m-1-i}}$. Since these representations are obviously pairwise non-equivalent, we get in this way

$$2^{m-2} + 2^{m-3} + \dots + 1 = 2^{m-1} - 1$$

complex irreducible representations of degree 2. Now

$$4 \cdot 1^2 + (2^{m-1} - 1) \cdot 2^2 = 2^{m+1} = |\, G_m \,|,$$

which implies that these are all the complex irreducible representations of G_m.

The non-equivalent rational irreducible representations are, apart from $\chi_0, \dots, \chi_3$, the representations W_i, $i = 1, \dots, m-1$, whose complexifications are

$$W_i \otimes_{\mathbb{Q}} \mathbb{C} \simeq \oplus_{j=1}^{2^{m-1-i}} V_i^j \, .$$

Note that W_i is of degree 2^{m-i}.

One checks that

$$\chi_N = \chi_0 + \chi_1,$$

$$\chi_H = \chi_0 + \chi_2 + \sum_{i=1}^{m-1} \chi_{W_i},$$

$$\chi_{\langle ab \rangle} = \chi_0 + \chi_3 + \sum_{i=2}^{m-1} \chi_{W_i}.$$

Using this, we immediately obtain from (2.1),

Proposition 2.2. *Let $Y \to \mathbb{P}^1$ denote a Galois covering with Galois group G_m, $m \geq 3$, ramified over 3 points of $\mathbb{P}^1$ with monodromy a, b and $(ab)^{-1}$. Then*

$$\chi_Y = \chi_{W_1}.$$

3. Curves with Galois group $G_{q,n}$

3.1. **Curves with complex multiplication by $\mathbb{Q}(\zeta_q^{(n)})$.** Let $Y \to \mathbb{P}^1$ be a Galois covering with group $G_{q,n}$ over an algebraically closed field $\mathcal{K}$ of characteristic 0. Consider the curve

$$X := Y/H$$

where H denotes the subgroup generated by b. In this section we use Proposition 2.1 in order to determine those Galois coverings Y for which the curve X admits complex multiplication.

Recall that a *CM-field* K of degree $2g$ is a totally complex quadratic extension of a totally real field of rank g over $\mathbb{Q}$.

The main result of this section is the following Proposition. As in the introduction let $\mathbb{Q}(\zeta_q^{(n)})$ denote the unique subfield of index n of the cyclotomic field $\mathbb{Q}(\zeta_q)$. It is a CM-field if and only if n is odd, which we assume in the sequel.

Proposition 3.1. *Suppose Y is a Galois covering of $\mathbb{P}^1$ with group $G_{q,n}$ and branch points $p_i \in \mathbb{P}^1$ of ramification index n_j dividing n for $i = 1, \dots, r$ and equal to q for $j = r+1, \dots, r+t$.*

Then the curve $X = Y/H$ has complex multiplication by $\mathbb{Q}(\zeta_q^{(n)})$ if and only if $n = r + t = 3$ and $\{n_1, n_2, n_3\} = \{3, 3, q\}$.

Proof. According to the Hurwitz formula, the genus of X is

$$g(X) = \frac{q-1}{2}\left(r + t - 2 - \sum_{j=1}^{r} \frac{1}{n_j}\right).$$

If the curve X has complex multiplication by $\mathbb{Q}(\zeta_q^{(n)})$ then $[\mathbb{Q}(\zeta_q^{(n)}) : \mathbb{Q}] = 2\dim(JX)$. This is the case if and only if

$$\frac{q-1}{n} = 2\,\frac{q-1}{2}\left(r + t - 2 - \sum_{j=1}^{r} \frac{1}{n_j}\right)$$

which is equivalent to

$$\sum_{j=1}^{r} \frac{n}{n_j} = n(r + t - 2) - 1. \tag{3.1}$$

This implies $t \le 2$.

If $t = 2$, then (3.1) says $\sum_{j=1}^{r} \dfrac{n}{n_j} = nr - 1$, a contradiction, since $\dfrac{n}{n_j}$ is either 1 or ≥ 3.

If $t = 0$, then (3.1) says $\sum_{j=1}^{r} \dfrac{n}{n_j} = n(r-2) - 1$. Since n is odd, $n_j \ge 3$, which implies $\dfrac{nr}{3} \ge nr - 2n - 1$ and thus $r \le 3 + \dfrac{3}{2n}$. This gives $r = 2$ or 3. In both cases (3.1) cannot be satisfied. For $r = 2$ the right hand side would be negative and for $r = 3$ the even number $n - 1$ is not the sum of 3 genuine divisors of n.

Hence $t = 1$, in which case (3.1) says $\sum_{j=1}^{r} \frac{n}{n_j} = n(r-1) - 1$. By the same argument as above, this implies $\frac{nr}{3} \geq nr - n - 1$, which gives $\frac{2}{3}r \leq 1 + \frac{1}{n}$. Since $n \geq 3$, this implies $r \leq \frac{3}{2}(1 + \frac{1}{3}) = 2$ and thus $r = 2$. But then (3.1) says

$$\frac{n}{n_1} + \frac{n}{n_2} = n - 1$$

whose only odd solution is $n = n_1 = n_2 = 3$.

Hence we have shown that the curve $X = Y/H$ has complex multiplication by $\mathbb{Q}(\zeta_q^{(n)})$ only if $n = r + t = 3$ and $\{n_1, n_2, n_3\} = \{3, 3, q\}$.

Certainly there exists a Galois covering of this type, with branch points p_1, p_2, p_3 in $\mathbb{P}^1$ and stabilizers $G_{p_1} = \langle a \rangle$, $G_{p_2} = \langle b \rangle$ and $G_{p_3} = \langle ab \rangle$, since $ab(ab)^{-1} = 1$.

We will now finish the proof by showing that under the assumptions $\mathbb{Q}(\zeta_q^{(3)})$ is contained in $\mathrm{End}_{\mathbb{Q}}(JX)$.

Let W be the rational irreducible representation of $G_{q,3}$ whose complexification is the direct sum of all the irreducible complex representations V_j of dimension 3.

Note that Proposition 2.1 in our case says $\chi_Y = \chi_W$. This, together with [5, p. 202, Corollaire], implies that there is an isomorphism of $\mathbb{Q}[G]$-modules

$$H^1(Y, \mathbb{Q}) \simeq W$$

and an isomorphism of $\mathbb{Q}[H\backslash G/H]$-modules

$$H^1(X, \mathbb{Q}) \simeq H^1(Y, \mathbb{Q})^H \simeq (W^H)^{\oplus m} \tag{3.2}$$

with $m = n(r + t - 2) - \sum_{j=1}^{r} \frac{n}{n_j} = 3(2 + 1 - 2) - \sum_{j=1}^{2} 1 = 1.$

Moreover, (3.2) implies that the canonical homomorphism $\mathbb{Q}[H\backslash G/H] \to \mathrm{End}_{\mathbb{Q}}(JX)$ induces a homomorphism $\rho : \mathbb{Q}[H\backslash G/H] \to \mathrm{End}(H^1(X, \mathbb{Q})) = \mathrm{End}(W^H)$, and the image of ρ is isomorphic to the image of $\mathbb{Q}[H\backslash G/H]$ in $\mathrm{End}_{\mathbb{Q}}(JX)$.

Now the image of $\mathbb{Q}[G]$ in $\mathrm{End}(W)$ is isomorphic to the 3×3-matrix algebra over $\mathbb{Q}(\zeta_q^{(3)})$, and the fact that $\dim V_1^H = 1$ implies that $\mathbb{Q}[H\backslash G/H] \cong \mathbb{Q} \oplus \mathbb{Q}(\zeta_q^{(3)})$ (see [2, Theorem 4.4] and [4]).

Hence the image of $\mathbb{Q}[H\backslash G/H]$ in $\mathrm{End}(W^H)$ is isomorphic to $\mathbb{Q}(\zeta_q^{(3)})$ and therefore

$$\mathbb{Q}(\zeta_q^{(3)}) \subset \mathrm{End}_{\mathbb{Q}}(JX).$$

□

We have thus proven the following result.

Corollary 3.2. *Let Y be a Galois covering of $\mathbb{P}^1$ with group $G := G_{q,3}$. Then $X = Y/H$ has complex multiplication by $\mathbb{Q}(\zeta_q^{(3)})$ if and only if $Y \to \mathbb{P}^1$ is isomorphic to the G-covering with branch points p_1, p_2, p_3 in $\mathbb{P}^1$ and stabilizers $G_{p_1} = \langle a \rangle$, $G_{p_2} = \langle b \rangle$ and $G_{p_3} = \langle ab \rangle$.*

Remark 3.3. For each q there exists a unique curve Y satisfying the conclusions in the Corollary; hence for every q there is only one such curve X, as was observed already by Lefschetz in [6, p. 463].

3.2. **The Jacobians JY and JX.** Let q be an odd prime with $q \equiv 1 \mod 3$ and denote

$$G := G_{q,3} = < a, b \mid a^q = b^3 = 1,\ b^{-1}ab = a^k >$$

where $k^3 \equiv 1 \mod q,\ 1 < k < q$. Let Y and X denote the curves of Corollary 3.2. In this section we want to see how the Jacobians JY and JX are related.

First, the Hurwitz formula gives

$$g(Y) = \frac{q-1}{2} \quad \text{and} \quad g(X) = \frac{q-1}{6}. \tag{3.3}$$

In particular $g(Y) = 3g(X)$. The following proposition is more precise.

Proposition 3.4. *The Jacobian of Y is isogenous to the third power of the Jacobian of X:*

$$JY \sim JX^3.$$

In particular JY admits complex multiplication by $\mathbb{Q}(\zeta_q)$.

Proof. There are exactly 2 nontrivial rational irreducible representations of G, namely W_1, whose complexification is $\chi_1 \oplus \chi_2$, and W_2, whose complexification is $V_1 \oplus \cdots \oplus V_s$, with χ_i and V_j as defined in Section 2. Correspondingly, according to [2, Proposition 5.2], there are abelian subvarieties B_1 and B_2 of JY, uniquely determined up to isogeny, such that

$$JY \sim B_1^{\frac{\dim \chi_1}{m_1}} \times B_2^{\frac{\dim V_1}{m_2}}$$

and

$$JX \sim B_1^{\frac{\dim \chi_1^H}{m_1}} \times B_2^{\frac{\dim V_1^H}{m_2}},$$

where m_i is the Schur index of the corresponding representation. Hence $m_1 = m_2 = 1$. Since $\dim V_1 = 3$ and $\dim V_1^H = 1$, it suffices to show for the first assertion that $\dim B_1 = 0$. This is a consequence of [7, Theorem 5.12], which in our case says

$$\dim B_1 = [K_{\chi_1} : \mathbb{Q}](-\dim \chi_1 + \frac{1}{2}\sum_{j=1}^{3}(\dim \chi_1 - \dim \chi_1^{G_j})),$$

where K_{χ_1} denotes the field generated by the values of the character χ_1 over $\mathbb{Q}$, $G_1 = \langle a \rangle$, $G_2 = \langle b \rangle$, and $G_3 = \langle ab \rangle$. Hence we get

$$\dim B_1 = 2(-1 + \frac{1}{2}(1 - 1 + 1 - 0 + 1 - 0)) = 0\,,$$

which completes the proof of the first assertion. According to Corollary 3.2, JX admits complex multiplication by $\mathbb{Q}(\zeta_q^{(3)})$. The last assertion follows from the first and the fact that $\mathbb{Q}(\zeta_q)$ is a degree-three CM-extension of $\mathbb{Q}(\zeta_q^{(3)})$. $\square$

Remark 3.5. The Prym variety P of the threefold covering $Y \to X$ is defined as the connected component containing 0 of the kernel of the norm map $JY \to JX$. Since JY is isogenous to the product $JX \times P$, we deduce from Corollary 3.2 and Proposition 3.4 that

$$P \sim JX^2.$$

In particular, P admits complex multiplication by a CM-extension of degree 2 of $\mathbb{Q}(\zeta_q^{(3)})$.

3.3. **The CM-types of JY and JX.** Recall that a CM-field K of degree $2g$ admits g pairs of complex conjugate embeddings into the field of complex numbers. A *CM-type* of K is by definition the choice of a set of representatives of these pairs; that is, a set of g pairwise non-isomorphic embeddings $K \hookrightarrow \mathbb{C}$.

The Jacobian JC of a curve C admits complex multiplication by a CM-field K, if and only if $H^1(C,\mathbb{Q})$ is a K-vector space of dimension 1. In this case the Hodge decomposition

$$H^1(C,\mathbb{C}) = H^0(C,\omega_C) \oplus \overline{H^0(C,\omega_C)}$$

induces a CM-type on the field K. It is called the *CM-type* of the Jacobian JC. In this section we compute the CM-types of the Jacobians JY and JX of Section 4.

We need some elementary preliminaries. The congruence

$$k^3 \equiv 1 \mod q$$

admits exactly 2 integer solutions with $2 \le k \le q-2$. If k is one such solution, $q-1-k$ is the other one.

For any integer n let $[n]$ denote the uniquely determined integer with

$$0 \le [n] \le q-1 \ \text{ and } \ [n] \equiv n \mod q$$

and for any integer ℓ, $1 \le \ell \le q-1$ consider the set

$$O_\ell := \{\ell, [k\ell], [k^2\ell]\}.$$

Lemma 3.6. *Let k be an integer with $2 \le k \le \frac{q-1}{2}$ and $k^3 \equiv 1 \mod q$. Then*
(1)

$$1 + k + [k^2] = q;$$

(2) *For any ℓ, $1 \le \ell \le q-1$,*

$$\ell + [k\ell] + [k^2\ell] = \begin{cases} q & \textit{if 2 of the numbers in } O_\ell \textit{ are smaller than } \frac{q-1}{2}, \\ 2q & \textit{otherwise.} \end{cases}$$

Proof. (1): We have $1 + k + [k^2] \equiv 0 \mod q$. On the other hand, $1 < 1 + k + [k^2] \le 1 + \frac{q-1}{2} + q - 1 = \frac{3}{2}q - \frac{1}{2}$. This implies the assertion.
(2): We have $\ell + k\ell + k^2\ell = \ell(1+k+k^2) \equiv 0 \mod q$. Hence q divides $\ell + [k\ell] + [k^2\ell]$. On the other hand, $1 \le \ell + [k\ell] + [k^2\ell] < 3q$. This implies

$$\ell + [k\ell] + [k^2\ell] = q \ \text{ or } \ 2q.$$

Suppose 2 of the 3 numbers are less than $\frac{q-1}{2}$. Then $\ell + [k\ell] + [k^2\ell] < 2\frac{q-1}{2} + q - 1 < 2q$ and hence $\ell + [k\ell] + [k^2\ell] = q$.

In the remaining case at least one of the numbers is $> \frac{q-1}{2}$, implying $\ell + [k\ell] + [k^2\ell] > 1 + 2\frac{q-1}{2} = q$ which completes the proof. $\square$

The following lemma gives a criterion for the set O_ℓ to contain two elements less than $\frac{q-1}{2}$.

Lemma 3.7. *For any integer ℓ; $1 \leq \ell \leq q-1$ consider the real number*

$$\beta_\ell := \sin\left(\frac{2\pi\ell}{q}\right) + \sin\left(\frac{2\pi k\ell}{q}\right) + \sin\left(\frac{2\pi k^2\ell}{q}\right).$$

Then the set O_ℓ contains two elements less than $\frac{q-1}{2}$ if and only if $\beta_\ell > 0$.

Proof. Suppose O_ℓ contains two elements less than $\frac{q-1}{2}$. Without loss of generality we may assume that they are ℓ and $[k\ell]$. Since $1+k+k^2 \equiv 0 \mod q$, we have

$$\begin{aligned}
\sin\left(\frac{2\pi[k^2\ell]}{q}\right) &= \sin\left(\frac{2\pi[-(1+k)\ell]}{q}\right) = -\sin\left(\frac{2\pi[(1+k)\ell]}{q}\right) \\
&= -\left[\sin\left(\frac{2\pi\ell}{q}\right)\cos\left(\frac{2\pi[k\ell]}{q}\right) + \cos\left(\frac{2\pi\ell}{q}\right)\sin\left(\frac{2\pi[k\ell]}{q}\right)\right].
\end{aligned}$$

Hence

$$\begin{aligned}
\beta_\ell &= \sin\left(\frac{2\pi\ell}{q}\right) + \sin\left(\frac{2\pi[k\ell]}{q}\right) + \sin\left(\frac{2\pi[k^2\ell]}{q}\right) \\
&= \sin\left(\frac{2\pi\ell}{q}\right)\left[1-\cos\left(\frac{2\pi[k\ell]}{q}\right)\right] + \sin\left(\frac{2\pi[k\ell]}{q}\right)\left[1-\cos\left(\frac{2\pi\ell}{q}\right)\right]
\end{aligned}$$

is positive, because both ℓ and $[k\ell]$ are positive and smaller than $\frac{q-1}{2}$.

The "only if" part of the assertion follows from the fact that the elements of $O_{q-\ell}$ are the negatives mod q of the numbers of O_ℓ, and therefore $\beta_{q-\ell} = -\beta_\ell$. This completes the proof. □

Let the notation be as in Section 2 with $n = 3$. In particular $\{a^{i_1}, \dots, a^{i_s}\}$ ($s = \frac{q-1}{3}$) denotes a set of representatives for the action of the group $H = \langle b \rangle$ on the group $N = \langle a \rangle$. The corresponding orbits are $\{a^{i_j}, a^{ki_j}, a^{k^2 i_j}\}$ for $j = 1, \dots, s$. Now with $\{a^{i_j}, a^{ki_j}, a^{k^2 i_j}\}$ also $\{a^{q-i_j}, a^{k(q-i_j)}, a^{k^2(q-i_j)}\}$ is an orbit, disjoint from it. Hence we can enumerate the orbits in the following way: The orbits of N under the adjoint action of the group H are exactly

$$\{a^{i_\nu}, a^{ki_\nu}, a^{k^2 i_\nu}\}_{\nu=1}^{\frac{s}{2}} \quad \text{and} \quad \{a^{q-i_\nu}, a^{k(q-i_\nu)}, a^{k^2(q-i_\nu)}\}_{\nu=1}^{\frac{s}{2}}, \tag{3.4}$$

where 2 of the numbers $i_\nu, [ki_\nu], [k^2 i_\nu]$ are less than $\frac{q-1}{2}$ (and thus 2 of the numbers $q - i_\nu, [k(q-i_\nu)], [k^2(q-i_\nu)]$ are $\geq \frac{q-1}{2}$).

If V_j denotes the complex irreducible representations as in Section 2 for $j = 1, \dots, s$, then we have

Proposition 3.8.

$$H^0(Y, \omega_Y) = \bigoplus_{\nu=1}^{\frac{s}{2}} V_\nu\,.$$

Proof. Since $3\dfrac{s}{2} = \dfrac{q-1}{2} = g(Y)$, it suffices to show that every V_ν with $1 \le \nu \le \frac{s}{2}$ occurs exactly once in the representation $H^0(Y, \omega_Y)$ of G.

According to the Theorem of Chevalley-Weil (see [3]), the representation V_ν occurs exactly

$$N = -\deg V_\nu + \sum_{\mu=1}^{3} \sum_{\alpha=0}^{n_\mu - 1} N_{\mu,\alpha} \left\langle -\frac{\alpha}{n_\mu} \right\rangle \tag{3.5}$$

times in the representation $H^0(Y, \omega_Y)$, where

- μ runs through the branch points of the covering $Y \to \mathbb{P}^1$,
- n_μ is the order of the μ-th branch point,
- $N_{\mu,\alpha}$ denotes the multiplicity of the eigenvalue $e^{\frac{2\pi i \alpha}{n_\mu}}$ in the matrix $V_\nu(g_\mu)$, where g_μ is any nontrivial element of G stabilizing a point in the fiber of μ, and
- $\langle r \rangle := r - \lfloor r \rfloor$ denotes the fractional part of the real number r.

Hence we have $n_1 = q,\ n_2 = n_3 = 3$ and thus

$$\begin{aligned} N &= -3 + \left\langle -\frac{i_\nu}{q} \right\rangle + \left\langle -\frac{[ki_\nu]}{q} \right\rangle + \left\langle -\frac{[k^2 i_\nu]}{q} \right\rangle + 2\left\langle -\frac{1}{3} \right\rangle + 2\left\langle -\frac{2}{3} \right\rangle \\ &= -1 + \frac{q - i_\nu}{q} + \frac{q - [ki_\nu]}{q} + \frac{q - [k^2 i_\nu]}{q} \\ &= 1, \end{aligned}$$

where the last equation follows from Lemma 3.6 (2), since by assumption, 2 of the numbers $q - i_\nu, q - [ki_\nu], q - [k^2 i_\nu]$ are $\ge \frac{q-1}{2}$. □

Corollary 3.9. *Let Y and X denote the curves of Section 3, and denote $\zeta = \zeta_q = e^{\frac{2\pi i}{q}}$. Let $\{a^{i_\nu}, a^{ki_\nu}, a^{k^2 i_\nu}\}_{\nu=1}^{\frac{s}{2}}$ be the first half of the orbits in (3.4). Then*
(1) The CM-type of JY is given by the following $g(Y) = \dfrac{3s}{2}$ embeddings φ_j of $\mathbb{Q}(\zeta)$ into $\mathbb{C}$: $\varphi_j(\zeta) = \zeta^j$ for j in $\{i_1, k\,i_1, k^2\,i_1, \ldots, i_{\frac{s}{2}}, k\,i_{\frac{s}{2}}, k^2\,i_{\frac{s}{2}}\}$.
(2) Denoting $\alpha_\nu := \zeta^{i_\nu} + \zeta^{ki_\nu} + \zeta^{k^2 i_\nu}$ for $\nu = 1, \ldots, \frac{s}{2}$, the CM-type of JX is given by the following $g(X) = \dfrac{s}{2}$ embeddings ψ_ν of $\mathbb{Q}(\alpha_1)$ into $\mathbb{C}$: $\psi_\nu(\alpha_1) = \alpha_\nu$.

Proof. (1) is a direct consequence of Propositions 3.4 and 3.8, and the definition of the representations V_ν in Section 2.

According to Corollary 3.2 the Jacobian JX has complex multiplication by $\mathbb{Q}(\zeta^{(3)})$. Hence (2) follows from Theorem 3.8 and the fact that

$$\mathbb{Q}(\zeta^{(3)}) = \mathbb{Q}(\alpha_1) = \mathbb{Q}(\zeta + \zeta^k + \zeta^{k^2})$$

is the only subfield of $\mathbb{Q}(\zeta)$ of index 3. □

Proposition 3.10. *The Jacobian JX is a simple abelian variety, of dimension $\frac{q-1}{6}$.*

This proves part (4) of Theorem 1 in the Introduction.

Proof. Let Φ denote the CM-type of JX, i.e. of the field $\mathbb{Q}(\zeta^{(3)})$ as given in Corollary 3.9 (2). With $\alpha = \zeta + \zeta^k + \zeta^{k^2}$ as above and $\mu := \alpha - \overline{\alpha}$ we have

- $K_0 = \mathbb{Q}(\alpha + \overline{\alpha})$ is totally real;
- $\eta := -\mu^2 = 4\beta_1$ is a totally positive element of K_0 (by Lemma 3.7);
- The elements of Φ are exactly the embeddings $\varphi : \mathbb{Q}(\mu) \hookrightarrow \mathbb{C}$ for which the imaginary part of $\varphi(\mu)$ is positive (according to Lemma 3.7).

We have to show that Φ is a primitive CM-type. For this we apply the criterion [8, Prop.27] of Shimura-Taniyama which says the following: Φ is primitive if and only if the following two conditions are satisfied:
(i) $K_0(\mu) = \mathbb{Q}(\mu)$;
(ii) for any conjugate α' of α over $\mathbb{Q}$, other than α itself, $\frac{\alpha'}{\alpha}$ is not totally positive.

The first condition holds trivially, since both fields are equal to $\mathbb{Q}(\zeta^{(3)}) = \mathbb{Q}(\alpha)$. As for the second condition: for any conjugate μ' of μ over $\mathbb{Q}$ different from μ, $\frac{\mu'}{\mu}$ is not totally positive, because $\frac{\mu'}{\mu}$ runs over $\frac{\beta_\ell}{\beta_1}$. □

3.4. **The function field $\mathcal{K}(Y)$.** In this section we use Kummer theory in order to prove part (5) of Theorem 1 in the Introduction.

Let Y be the Galois covering of $\mathbb{P}^1$ of Corollary 3.2, with Galois group $G_{q,3}$ ramified over the points p_1, p_2 and p_3 of $\mathbb{P}^1$ in affine coordinates. The subgroup $N = \langle a \rangle$ is normal of index 3 in $G_{q,3}$, and gives a factorization of the covering $Y \to \mathbb{P}^1$ into cyclic coverings $Y \to Z := Y/N$ of degree q and $Z \to \mathbb{P}^1$ of degree 3. The last covering is ramified over p_2 and p_3. Hence, according to the Hurwitz formula,

$$g(Z) = 0.$$

We choose an affine coordinate x of $\mathbb{P}^1$ in such a way that $p_1 = 1, p_2 = 0$ and $p_3 = 2$. Then the covering $Z \to \mathbb{P}^1$ is given by the equation

$$z^3 = \frac{x}{x-2}$$

and the function field of $Z = \mathbb{P}^1$ is $\mathcal{K}(z)$.

Proposition 3.11. *Let ω_3 denote a primitive third root of unity, and choose $1 < k < q$ such that $k^3 \equiv 1 \mod q$. A (singular) model of the curve Y is given by the equation*

$$y^q = (z-1)(z-\omega_3)^k(z-\omega_3^2)^{k^2}.$$

With these notations, automorphisms σ and τ of the curve Y of corresponding orders q and 3, are given by

$$\sigma : \ z \mapsto z, \quad y \mapsto \zeta_q y\,, \quad \textit{and}$$

$$\tau : \ z \mapsto \omega_3 z, \quad y \mapsto \frac{\omega_3^{m'}}{(z-\omega_3^2)^m} y^k$$

where m and m' are given by $k^3 = mq + 1$ and $k^2 + k + 1 = m'q$.

An immediate consequence of the proposition is statement (5) of Theorem 1 in the Introduction.

Proof. The covering $Y \to Z$ is ramified exactly over the points $1, \omega$ and ω^2 of $Z = \mathbb{P}^1$. According to Kummer theory the covering $Y \to Z$ is given by the affine equation

$$y^q = (z-1)(z-\omega_3)^k(z-\omega_3^2)^{k^2}, \tag{3.6}$$

with k as in the statement of the proposition.

The automorphism $\tau : Z \to Z$ given by $z \mapsto \omega_3 z$ extends to the automorphism of Y as defined in the proposition since, denoting the right hand side of (3.6) by $F = F(z)$, we have

$$\tau(F) = \omega_3^{1+k+k^2}(z-\omega_3^2)(z-1)^k(z-\omega_3)^{k^2} = \frac{\omega_3^{1+k+k^2}}{(z-\omega_3^2)^{mq}}F^k = \left(\frac{\omega_3^{m'}}{(z-\omega_3^2)^m}y^k\right)^q.$$

If σ denotes the automorphism of Y given above, then it is clear that $Y \to \mathbb{P}^1$ is a Galois covering with Galois group $<\sigma, \tau> = G_{q,3}$. □

4. Curves with Galois group G_m

4.1. **Complex multiplication of the curves.** Let $Y \to \mathbb{P}^1$ denote a Galois covering with Galois group

$$G_m = \langle a, b \mid a^{2^m} = b^2 = 1, bab = a^d\rangle$$

for $m \geq 3$ and where $d = 2^{m-1} - 1$, branched over 3 points in $\mathbb{P}^1$ with monodromy a, b and $(ab)^{-1}$. Notice that such a covering exists, since $ab(ab)^{-1} = 1$. In fact, for any $m \geq 3$ there is exactly one such curve up to isomorphism. From Proposition 2.2 we find the genus of Y,

$$g(Y) = 2^{m-2}.$$

Consider the curve

$$X := Y/H$$

where H denotes the subgroup generated by b. We want to show that X admits complex multiplication.

As in Section 2.3 let $\xi = \xi_{2^m}$ denote a primitive 2^m-th root of unity. The complex representation $V = V_1$ has character field $K_V = \mathbb{Q}(\xi + \xi^d)$, and its Schur index is equal to 1. The field K_V is of CM-type and degree $[K_V : \mathbb{Q}] = 2^{m-2}$.

Proposition 4.1. *The curve X has complex multiplication by K_V. In particular,*

$$g(X) = 2^{m-3}.$$

Proof. As in Section 2.3, let W_1 denote the rational irreducible representation whose complexification is $\oplus_{j=1}^{2^{m-2}} V_1^j$. According to [5, p.202, Corollaire] and Proposition 2.2 above, there is an isomorphism of $\mathbb{Q}[H\backslash G/H]$-modules

$$H^1(X, \mathbb{Q}) \simeq W_1^H. \tag{4.1}$$

Since $\dim V_1^H = 1$, this implies $\dim W_1^H = 2^{m-2}$ and thus $g(X) = 2^{m-3}$. Moreover (4.1) implies that the canonical map $\mathbb{Q}[H\backslash G/H] \to \mathrm{End}_{\mathbb{Q}}(JX)$ induces a homomorphism

$$p : \mathbb{Q}[H\backslash G/H] \to \mathrm{End}(W_1^H).$$

whose image is isomorphic to the image of $\mathbb{Q}[H\backslash G/H]$ in $\mathrm{End}_{\mathbb{Q}}(JX)$. Now the image of $\mathbb{Q}[G]$ in $\mathrm{End}(W_1)$ is isomorphic to the 2×2-matrix algebra over K_V, and $\mathbb{Q}[H\backslash G/H]$ is isomorphic to $\mathbb{Q} \oplus K_V$ (since $\dim V^H = 1$).

Hence the image of $\mathbb{Q}[H\backslash G/H]$ in $\mathrm{End}(W_1^H)$ is isomorphic to K_V, which means that the curve X admits complex multiplication by K_V. □

This proves (2) of Theorem 2 of the Introduction. Part (4) of Theorem 2 is proven by the following proposition.

Proposition 4.2. *The Jacobian of Y is isogenous to the second power of the Jacobian of X:*

$$JY \sim JX^2.$$

In particular JY admits complex multiplication by the cyclotomic field $\mathbb{Q}(\xi_{2^m})$.

Proof. We already know from Proposition 2.2 that there is only one nontrivial isogeny factor of JY: it is associated to the representation W_1. Using [2, Proposition 5.2] this means that there is an abelian subvariety B_1 of JY such that

$$JY \sim B_1^2,$$

using that $\dim V_1 = 2$ and the Schur index of V_1 is 1. Since $\dim V_1^H = 1$ we get moreover from [2] that

$$JX \sim B_1.$$

The two isogenies together imply the first assertion. Since JX admits complex multiplication by a CM-subfield of index 2 in $\mathbb{Q}(\xi_{2^m})$, $JY \sim JX^2$ admits complex multiplication by $\mathbb{Q}(\xi_{2^m})$. □

The projection map $\pi_b : Y \to X$ is a double covering ramified at two points. Hence its Prym variety $P = \ker(JY \to JX)_0$ is a principally polarized abelian variety, of dimension equal to $g(X) = 2^{m-3}$.

Corollary 4.3. *The Prym variety of the covering $\pi_b : Y \to X$ has complex multiplication by K_V.*

Proof. This follows immediately from Propositions 4.1 and 4.2, and the fact that JY is isogenous to the product $JX \times P$. □

4.2. **The CM-types of JY and JX.** In order to determine the CM-types of JY and JX, recall that, according to Proposition 2.2, the representation $H^1(Y, \mathbb{Q})$ of G_m is just the rational irreducible representation W_1. Moreover, the complexification of W_1 is the direct sum of the $[K_V : \mathbb{Q}] = 2^{m-2}$ Galois conjugate representations V_1^j of the complex irreducible representation V_1. For every positive integer i consider the complex irreducible representation U_i defined by

$$U_i(a) = \begin{pmatrix} \xi^{2i-1} & 0 \\ 0 & \xi^{(2i-1)d} \end{pmatrix}, \qquad U_i(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

and denote

$$U_i' := U_{2^{m-2}+i}.$$

Lemma 4.4. *The complex irreducible representations V_1^j, $j = 1, \dots, 2^{m-2}$ are given by the representations $U_1, \dots, U_{2^{m-3}}$ and $U_1', \dots, U_{2^{m-3}}'$. The representation U_i' is the complex conjugate of U_i for $i = 1, \dots, 2^{m-3}$.*

Proof. First note that U_1 coincides with the representation V_1 and every U_i is Galois conjugate to U_1. Moreover clearly $U_1, \dots, U_{2^{m-3}}$ are pairwise non-isomorphic. Hence it suffices to show that U_i' is the complex conjugate of U_i. But this follows from the congruences

$$2^{m-1} + 2i - 1 \equiv -(2i-1)d \mod 2^m \text{ and } (2^{m-1} + 2i - 1)d \equiv -(2i-1) \mod 2^m.$$

□

Proposition 4.5.

$$H^0(Y, \omega_Y) = \oplus_{i=1}^{2^{m-3}} U_i.$$

Proof. Since $2 \cdot 2^{m-3} = g(Y)$, it follows from Lemma 4.4 that it suffices to show that every U_i with $1 \le i \le 2^{m-3}$ occurs exactly once in the representation $H^0(Y, \omega_Y)$ of G_m. Again this is a consequence of the Theorem of Chevalley-Weil; that is, equation (3.5).

Here $Y \to \mathbb{P}^1$ is branched over 3 points in $\mathbb{P}^1$ with $n_1 = 2^m$, $n_2 = 2$ and $n_3 = 4$, and we have for the representation U_i, $1 \le i \le 2^{m-3}$,

$$\begin{aligned} N &= -2 + \left\langle -\frac{(2i-1)}{2^m} \right\rangle + \left\langle -\frac{(2i-1)d}{2^m} \right\rangle + \left\langle -\frac{1}{2} \right\rangle + \left\langle -\frac{1}{4} \right\rangle + \left\langle -\frac{3}{4} \right\rangle \\ &= -2 + \frac{2^m - 2i + 1}{2^m} + \frac{2^{m-1} + 2i - 1}{2^m} + \frac{1}{2} + \frac{3}{4} + \frac{1}{4} \\ &= 1. \end{aligned}$$

□

As a consequence we get

Corollary 4.6. *Let $\xi = e^{\frac{2\pi i}{2^m}}$. Then we have*
(1): *The CM-type of JY is given by $\{\xi^{2i-1}, \mid i = 1, \dots, 2^{m-2}\}$;*
(2): *The CM-type of JX is given by $\{\xi^{2i-1} + \xi^{(2i-1)d} \mid i = 1, \dots, 2^{m-3}\}$.*

Proof. According to Proposition 4.5 the CM-type of JY is $\{\xi^{2i-1}, \ \xi^{(2i-1)d} \mid i = 1, \dots, 2^{m-3}\}$. This implies (1), since $\xi^{(2i-1)d} \equiv 2^{m-1} - 2i + 1 \mod 2^m$ for $i = 1, \dots, 2^{m-3}$. (2) is an immediate consequence of (1), since the CM-field of X is the fixed field of the involution $\xi \mapsto \xi^d$. □

Proposition 4.7. *The Jacobian JX and the Prym variety P of the covering $Y \to X$ are simple abelian varieties of dimension 2^{m-3}.*

This proves part (4) of Theorem 2 of the introduction.

Proof. It suffices to show that the field $K_V = \mathbb{Q}(\xi + \xi^d)$ does not admit a proper CM-subfield, since then every CM-type of it is primitive, and in particular JX is a simple abelian variety.

It is well known that the Galois group of the extension $\mathbb{Q}(\xi)|\mathbb{Q}$ is

$$\langle \sigma \rangle \times \langle \tau \rangle,$$

with $\langle \sigma \rangle$ is cyclic of order 2^{m-2} generated by $\sigma : \xi \mapsto \xi^5$, and τ is the involution $\tau : \xi \mapsto \xi^d$. Therefore the Galois group of $K_V|\mathbb{Q}$, which is the fixed field of τ, is $\langle \sigma \rangle \simeq \mathbb{Z}/2^{m-2}\mathbb{Z}$. Its only element of order 2 is $\sigma^{2^{m-3}}$, which must be complex conjugation in K_V. Since every nontrivial subgroup of $\langle \sigma \rangle$ contains $\sigma^{2^{m-3}}$, this implies that every proper subfield of K_V is real. □

4.3. **Equations.** Let the notation be as in the previous subsections. Here we want to give equations for the curves Y and X.

First note that the center $Z = Z(G_m) = \langle a^{2^{m-1}} \rangle$ of the group G_m is of order two; furthermore,

$$|Z\backslash G_m/\langle a\rangle| = 2, \quad |Z\backslash G_m/\langle b\rangle| = 2^{m-1}, \quad |Z\backslash G_m/\langle ab\rangle| = 2^{m-1}.$$

According to [7], for any subgroup H of G acting on a curve Y with monodromy $g_1, \dots, g_t$, the genus of the quotient Y/H is given by

$$g_{Y/H} = [G:H](g_{Y/G} - 1) + 1 + \frac{1}{2} \sum_{j=1}^{t} \left([G:H] - |H\backslash G/\langle g_j\rangle|\right) .$$

We obtain that in our case $g(Y/Z) = 0$, and therefore Y is hyperelliptic.

We may choose coordinates in such a way that an affine equation for Y is

$$y^2 = x(x^{2^{m-1}} - 1),$$

and if $\xi = \xi_{2^m}$, then the automorphisms a and b of the curve Y are given by

$$a(x,y) = (\xi^2\, x,\ \xi\, y) \quad ; \quad b(x,y) = \left(\frac{1}{\xi^2\, x},\ \ -i\, \xi^d\, \frac{y}{x^{2(m-2)+1}}\right) .$$

Note that

$$a^{2^{m-1}}(x,y) = (x,-y) =: j(x,y),$$

where j denotes the hyperelliptic involution of Y,

Also, b and j generate a Klein group, with the following associated diagram of covers.

$$\begin{tikzcd}
 & Y \arrow[dl, "\pi_j"'] \arrow[d, "\pi_b"'] \arrow[dr, "\pi_{bj}"] & \\
Y/\langle j\rangle = \mathbb{P}^1 \arrow[dr] & Y/\langle b\rangle = X \arrow[d] & Y/\langle b\,j\rangle \arrow[dl] \\
 & \mathbb{P}^1 &
\end{tikzcd}$$

$\pi_j : Y \to \mathbb{P}^1$ is the hyperelliptic covering ramified over $\{0, \infty, \xi^i_{2^{m-1}} : 0 \le i \le 2^{m-1} - 1\}$, π_b ramifies at the two fixed points $P_i = (\xi^d, y)$ with $y^2 = -2\xi^d$ of b, and π_{bj} ramifies at the two fixed points $(-\xi^d, y)$ with $y^2 = 2\xi^d$ of bj.

Since X is then hyperelliptic and ramifies over $\pi_b(P_1)$, $\pi_b(P_2)$, and the images under π_b of the Weierstrass points of Y, we may consider $f : \mathbb{P}^1 \to \mathbb{P}^1$ of degree two and invariant under $x \to \frac{1}{\xi^2\, x}$ such as

$$f(x) = \frac{\xi\,(\xi\, x + 1)^2}{\xi^2\, x^2 + 1}$$

and adequate $g(x,y)$ so that $\pi_b(x,y) = (f(x), g(x,y))(= (u,v))$, and we obtain

$$X = Y/\langle b\rangle : v^2 = u(u - \xi) \prod_{k=0}^{2^{m-2}-1} (u - f(\xi^{2k})).$$

Remark 4.8. In the case $m = 4$ we obtain the curve of genus two

$$X = Y/\langle b\rangle : v^2 = u^6 - 5\xi_{16}u^5 + 2\xi_{16}^2 u^4 + 14\xi_{16}^3 u^3 - 11\xi_{16}^4 u^2 - \xi_{16}^5 u$$

whose Jacobian has complex multiplication by $\mathbb{Q}(\xi_{16} + \xi_{16}^7) = \mathbb{Q}(\sqrt{-2+\sqrt{2}})$.

Thus we generalize an example given in [9], where it is given by the equation

$$y^2 = -x^5 + 3x^4 + 2x^3 - 6x^2 - 3x + 1$$

The curves are isomorphic, because they have the same Igusa invariants
$i_1 := I_2^5/I_{10} = 1836660096 = 2^7 \cdot 3^{15}$,
$i_2 := I_2^3 \cdot I_4/I_{10} = 28343520 = 2^5 \cdot 3^{11} \cdot 5$, and
$i_3 := I_2^2 \cdot I_6/I_{10} = 9762768 = 2^4 \cdot 3^9 \cdot 31$.

References

[1] S. Broughton: *The homology and higher representations of the automorphism group of a Riemman surface*. Trans. AMS, 300 (1987), 153-158.

[2] A. Carocca, R. E. Rodríguez: *Jacobians with group actions and rational idempotents*. J. Alg. 306 (2006), 322-343.

[3] C. Chevalley, A. Weil: *Über das Verhalten der Integrale erster Gattung bei Automorphisman des Funktionenkörpers*. Hamb. Abh. 10 (1934), 358-361.

[4] J.S. Ellenberg: *Endomorphism Algebras of Jacobians*. Adv. in Math. 162 (2001), 243-271.

[5] A. Grothendieck: *Sur quelques points d'algèbre homologique*. Tohoku Math. J. 9 (1957), 119-221.

[6] S. Leschetz: *On certain numerical invariants of algebraic varieties with application to abelian varieties (cont.)* Trans. Amer. Math. Soc. 22 (1921), no. 4, 407–482.

[7] A.M. Rojas: *Group actions on Jacobian varieties*. Rev. Mat. Iber. 23 (2007), 397-420.

[8] G. Shimura, Y. Taniyama: *Complex Multiplication of Abelian Varieties*. Math. Soc. Japan (1961).

[9] P van Wamelen: *Examples of genus two CM curves defined over the rationals*. Math. Comp. 68 (1999), 307-320.

A. Carocca, Facultad de Matemáticas, Pontificia Universidad Católica de Chile, Casilla 306-22, Santiago, Chile
E-mail address: acarocca@mat.puc.cl

H. Lange, Mathematisches Institut, Universität Erlangen-Nürnberg, Germany
E-mail address: lange@mi.uni-erlangen.de

R. E. Rodríguez, Facultad de Matemáticas, Pontificia Universidad Católica de Chile, Casilla 306-22, Santiago, Chile
E-mail address: rubi@mat.puc.cl