involve

a journal of mathematics

Jacobian varieties of Hurwitz curves with automorphism group PSL$(2, q)$

Allison Fischer, Mouchen Liu and Jennifer Paulhus

msp

2016 vol. 9, no. 4

INVOLVE 9:4 (2016)
dx.doi.org/10.2140/involve.2016.9.639

Jacobian varieties of Hurwitz curves with automorphism group PSL(2, q)

Allison Fischer, Mouchen Liu and Jennifer Paulhus

(Communicated by Nigel Boston)

The size of the automorphism group of a compact Riemann surface of genus $g > 1$ is bounded by $84(g-1)$. Curves with automorphism group of size equal to this bound are called Hurwitz curves. In many cases the automorphism group of these curves is the projective special linear group $\mathrm{PSL}(2, q)$. We present a decomposition of the Jacobian varieties for all curves of this type and prove that no such Jacobian variety is simple.

1. Introduction

Let X be a compact Riemann surface of genus g (henceforth called a "curve"), and G its automorphism group with identity element denoted id_G. A result of Wedderburn gives the decomposition of the group ring $\mathbb{Q}G$,

$$\mathbb{Q}G \cong \bigoplus_i M_{n_i}(\Delta_i),$$

where $M_{n_i}(\Delta_i)$ denotes $n_i \times n_i$ matrices with coefficients in a division ring Δ_i. It is possible to decompose the Jacobian variety, JX, of the curve X into abelian varieties, up to isogeny $\sim$, as

$$JX \sim \bigoplus_i (e_i(JX))^{n_i}, \tag{1}$$

where e_i are certain idempotents in $\mathrm{End}(JX) \otimes_{\mathbb{Z}} \mathbb{Q}$. More details about this decomposition may be found in [Paulhus 2008]. It is important to note here that this decomposition may not be the finest possible decomposition. Some of the abelian variety factors $e_i(JX)$ could decompose further.

Decomposable Jacobian varieties have applications to rank and torsion questions in number theory [Howe et al. 2000; Rubin and Silverberg 2001]. In genus 2,

MSC2010: 14H40, 14H37, 20G05.
Keywords: Jacobian varieties, Hurwitz curves, projective special linear group, representation theory.

the elliptic curve factors appearing in these decompositions have interesting arithmetic properties (see [Cardona 2004; Earle 2006; Magaard et al. 2009], among many others).

The dimension, as an abelian variety, of the factor $e_i(J_X)$ in (1) is $\frac{1}{2}\langle\psi_i, \chi\rangle$, where $\langle\psi_i, \chi\rangle$ denotes the inner product of ψ_i, the i-th irreducible $\mathbb{Q}$-character labeled according to the Wedderburn decomposition, with χ, a character we define below called the *Hurwitz character*. To define the character χ, we consider the covering from X to its quotient $Y = X/G$, a curve with genus denoted g_Y. Let $h_1, \dots, h_s \in G$ be the monodromy of this covering. For any subgroup H of G, define the character χ_H to be the trivial character of H induced to G, and 1_G to be the trivial character of G. In this paper H is a cyclic subgroup generated by one element of the monodromy, which we write as $\langle h_i\rangle$. Note that with this notation $\chi_{\langle \mathrm{id}_G\rangle}$ is the character associated to the regular representation. Define the *Hurwitz character* as

$$\chi = 2\cdot 1_G + 2(g_Y - 1)\chi_{\langle \mathrm{id}_G\rangle} + \sum_{j=1}^{s}(\chi_{\langle \mathrm{id}_G\rangle} - \chi_{\langle h_j\rangle}), \tag{2}$$

which is the character of the representation of G on $H^1_{\mathrm{et}}(X, \mathbb{Q}_\ell)$ [Milne 1980, Chapter V, §2]. To determine the dimensions of factors of JX from (1), we must know the automorphism group of X, the irreducible $\mathbb{Q}$-characters for that particular group, and the monodromy of the covering $X \to Y$.

The upper bound on the size of the automorphism group of a curve of genus $g > 1$ is given by $84(g-1)$. Curves whose automorphism groups attain this bound are called *Hurwitz curves* and the groups themselves are called *Hurwitz groups*. Hurwitz groups have a long history in the study of triangle groups, Riemann surfaces, and hyperbolic geometry. See [Conder 1990] for a nice survey of these groups and their significance.

For all Hurwitz curves, the quotient curve Y is the projective line, so $g_Y = 0$. Since the quotient curve has genus 0, the monodromy of the covering is a set of elements $\{h_1, \dots, h_s\}$ in G such that $h_1 \cdots h_s = \mathrm{id}_G$ and the set of all h_i generates G. The monodromy for Hurwitz curves is always of type (2, 3, 7), meaning it consists of an element of order 2, an element of order 3, and an element of order 7, denoted in this paper by h_2, h_3, and h_7, respectively. (Equivalently, a Hurwitz group is a finite, nontrivial quotient of the (2, 3, 7)-triangle group.) For Hurwitz curves, (2) may be simplified to

$$\chi = 2\cdot 1_G + \chi_{\langle \mathrm{id}_G\rangle} - \chi_{\langle h_2\rangle} - \chi_{\langle h_3\rangle} - \chi_{\langle h_7\rangle}. \tag{3}$$

Let $\mathrm{PSL}(2, q)$ denote the projective special linear group with coefficients in the finite field of order q. In this paper we will use (1) to decompose the Jacobian varieties of all Hurwitz curves with automorphism group $\mathrm{PSL}(2, q)$. This decomposition may be found in Theorem 10 and, in particular, in Corollary 9 we prove that the Jacobian variety of these curves is never simple.

While there is an infinite family of Hurwitz curves with automorphism group $\mathrm{PSL}(2, q)$ (as we will see immediately below), there are many Hurwitz curves with other automorphism groups. For example, the alternating group A_n is a Hurwitz group for all $n \geq 168$ as well as for many smaller n [Conder 1990]. It is likely that a similar analysis would yield results about the decomposition of the Jacobians of these families of curves too.

Macbeath determines for which q the group $\mathrm{PSL}(2, q)$ is a Hurwitz group.

Theorem 1 [Macbeath 1969]. *The group* $\mathrm{PSL}(2, q)$ *is a Hurwitz group if and only if*

(i) $q = 7$,

(ii) q *is a prime and congruent to* $\pm 1 \bmod 7$, *or*

(iii) $q = p^3$ *for a prime* $p \equiv \pm 2$ *or* $\pm 3 \bmod 7$.

Note that in both cases (ii) and (iii), we have $q \equiv \pm 1 \bmod 7$. Case (i) occurs for a Hurwitz curve of genus 3, and the Jacobian is known to decompose as $JX \sim E^3$, where E is an elliptic curve [Kuwata 2005]. In case (ii), when $q = 13$ (and $g = 14$), the technique above may be used to show that $JX \sim E^{14}$, again for E some elliptic curve. Case (iii) includes the special case where $q = 8$. This corresponds to a genus 7 curve sometimes called the *Macbeath curve*. It has long been known that $JX \sim E^7$ [Wolfart 2002].

For odd q, $\mathrm{PSL}(2, q)$ has a well understood and relatively straightforward character table. Additionally, the monodromy of the coverings is not hard to find as (3) only requires knowledge of the monodromy *up to conjugation*. It turns out that, as we show below in Proposition 2, for almost all q satisfying Theorem 1, $\mathrm{PSL}(2, q)$ has only one conjugacy class of elements of order 2, one of elements of order 3, and three conjugacy classes of elements of order 7. This then allows us to compute the inner product $\langle \psi_i, \chi \rangle$ in all such examples and prove very general results about the Jacobian decompositions of curves with these groups as automorphism groups. The few exceptional q are either discussed above or at the end of the paper in Section 6.

We begin in Section 2 by reviewing known results about $G = \mathrm{PSL}(2, q)$. In particular, in Section 2.3 we determine the irreducible $\mathbb{Q}$-characters, a key piece in our determination of the dimension of the factors in the Jacobian decompositions. In Section 3 we compute the Hurwitz character χ, and in Section 4 we compute the inner products. Finally we put the pieces together and present the Jacobian decomposition in Section 5.

Using a different set of idempotents in $\mathbb{Q}G$ and the fact that $\mathrm{PSL}(2, q)$ has a *partition* (a set of subsets of G whose pairwise intersection is the identity and whose union is the whole group), Kani and Rosen [1989, Example 2] describe a decomposition of a power of the Jacobian variety of curves with such automorphisms. The factors are themselves Jacobians of quotients of the curve by p-Sylow subgroups or Cartan subgroups of G.

2. Properties of PSL(2, q)

Here we collect the relevant information about the group $G = \mathrm{PSL}(2,q)$. More details may be found in [Karpilovsky 1994] and we follow the notation in that book. For the rest of the paper, assume q is odd, $q > 27$, and q satisfies case (ii) or case (iii) in Theorem 1. All cases not covered by this are discussed above, except for $q = 27$, which we cover in Section 6.

First, the size of $\mathrm{PSL}(2,q)$ is

$$\tfrac{1}{2}q(q+1)(q-1).$$

To describe the character table of $\mathrm{PSL}(2,q)$ we need several special elements of $\mathrm{SL}(2,q)$. Let α be a generator of the group of units of the finite field with q^2 elements, let $\beta = \alpha^{q+1}$, and define b as the element of $\mathrm{SL}(2,q)$ determined by the map $x \to \alpha^{q-1}x$ for $x \in \mathbb{F}_{q^2}$. Additionally define elements of $\mathrm{SL}(2,q)$

$$a = \begin{bmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{bmatrix}, \quad c = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad \text{and} \quad d = \begin{bmatrix} 1 & 0 \\ \beta & 1 \end{bmatrix}.$$

The images of the elements a, b, c, and d in the quotient $\mathrm{PSL}(2,q)$ are denoted as $\bar{a}$, $\bar{b}$, $\bar{c}$, and $\bar{d}$. The element $\bar{a}$ has order $\frac{1}{2}(q-1)$, the element $\bar{b}$ has order $\frac{1}{2}(q+1)$ and the elements $\bar{c}$ and $\bar{d}$ each have order q.

2.1. ***Conjugacy classes.*** To determine the monodromy of the covering, we need to understand the conjugacy classes of elements of orders 2, 3, and 7. The representatives of the conjugacy classes of $\mathrm{PSL}(2,q)$ are $\bar{1}$, $\bar{c}$, $\bar{d}$, $\bar{a}^n$, and $\bar{b}^m$, where $1 \le n, m \le \frac{1}{4}(q-1)$ if $q \equiv 1 \bmod 4$, while $1 \le n \le \frac{1}{4}(q-3)$ and $1 \le m \le \frac{1}{4}(q+1)$ if $q \equiv -1 \bmod 4$. We will write the conjugacy class of an element $h \in G$ as $[h]$.

Conjugacy classes with a representative $\bar{a}^n$ have size $q(q+1)$, and conjugacy classes with a representative $\bar{b}^m$ have size $q(q-1)$, with the exception of the conjugacy class containing elements of order 2 which has order half that size, $\big($or $\frac{1}{2}q(q-1)\big)$ [Karpilovsky 1994]. We will see in the proof of Proposition 2 that the conjugacy class of elements of order 2 is $[\bar{a}^{(q-1)/4}]$ if $q \equiv 1 \bmod 4$ and $[\bar{b}^{(q+1)/4}]$ if $q \equiv -1 \bmod 4$.

It turns out that χ as defined in (3) is 0 outside of the conjugacy classes of elements of orders 1, 2, 3, and 7, as we will see in Section 3. So it will be sufficient to only study these conjugacy classes of $\mathrm{PSL}(2,q)$ since any other conjugacy class will not contribute to our goal of computing the inner product of χ with the irreducible $\mathbb{Q}$-characters. But how many such conjugacy classes are there?

Proposition 2. *If $G = \mathrm{PSL}(2, q)$ for q odd, greater than* 27, *and satisfying case* (ii) *or case* (iii) *in Theorem 1, then G has three distinct conjugacy classes of elements of order* 7, *and one each of elements of orders* 2 *and* 3.

Proof. When q is as in the proposition, since elements of the conjugacy classes represented by $\bar{c}$ and $\bar{d}$ have order q, the elements of order 7 can only lie in conjugacy classes represented by some power of $\bar{a}$ or $\bar{b}$. (For $q = 7$ this need not be true as $\bar{c}$ and $\bar{d}$ both have order $q = 7$.)

Recall for a finite group G, the order of g^k for any $g \in G$ and positive integer k is $o(g^k) = o(g)/\gcd(k, o(g))$. Thus, 7 must divide the order of $\bar{a}$ or the order of $\bar{b}$ but not both, else it divides $\frac{1}{2}(q+1) - \frac{1}{2}(q-1) = 1$. Thus the conjugacy class(es) of order 7 are either represented by some power(s) of $\bar{a}$ or some power(s) of $\bar{b}$.

First consider the case where $q \equiv 1 \mod 4$. Suppose that the conjugacy classes of elements of order 7 are represented by powers of $\bar{a}$ (so $q \equiv 1 \mod 7$). The number of conjugacy classes will be the number of i such that $7 = o(\bar{a})/\gcd(o(\bar{a}), i)$, where $1 \le i \le \frac{1}{4}(q-1)$. Since 7 divides the order of $\bar{a}$, we let $o(\bar{a}) = 7j$ for some positive integer j. Then the number of i such that $7 = 7j/\gcd(7j, i)$ is the number of i that satisfy $\gcd(7j, i) = j$ and $1 \le i \le \frac{7}{2}j$. Since $o(\bar{a}) = \frac{1}{2}(q-1)$ and $q > 13$, there are always three of them: $i = j$ $\bigl(\text{or } \frac{1}{14}(q-1)\bigr)$, $i = 2j$ $\bigl(\text{or } \frac{1}{7}(q-1)\bigr)$, and $i = 3j$ $\bigl(\text{or } \frac{3}{14}(q-1)\bigr)$. Hence the elements of order 7 are in the conjugacy classes represented by $\bar{a}^{(q-1)/14}$, $\bar{a}^{(q-1)/7}$, and $\bar{a}^{3(q-1)/14}$. A similar argument works if these classes are represented by powers of $\bar{b}$ (or $q \equiv -1 \mod 7$). The elements of order 7 are in the conjugacy classes represented by $\bar{b}^{(q+1)/14}$, $\bar{b}^{(q+1)/7}$, and $\bar{b}^{3(q+1)/14}$.

Now, when $q \equiv -1 \mod 4$, the argument is identical except the bounds on i change to $1 \le i \le \frac{1}{4}(q-3)$ if $q \equiv 1 \mod 7$ and $1 \le i \le \frac{1}{4}(q-1)$ if $q \equiv -1 \mod 7$. The rest of the argument does not change and so there are three conjugacy classes of elements of order 7, again defined as $\bar{a}^{(q-1)/14}$, $\bar{a}^{(q-1)/7}$, and $\bar{a}^{3(q-1)/14}$ if $q \equiv 1 \mod 7$ or $\bar{b}^{(q+1)/14}$, $\bar{b}^{(q+1)/7}$, and $\bar{b}^{3(q+1)/14}$ if $q \equiv -1 \mod 7$.

The cases with orders 2 and 3 follow similarly. When $q \equiv 1 \mod 4$, the elements of order 2 are in the conjugacy class $[\bar{a}^{(q-1)/4}]$; when $q \equiv -1 \mod 4$, the elements of order 2 are in the conjugacy class $[\bar{b}^{(q+1)/4}]$. For elements of order 3, the conjugacy class is $[\bar{a}^{(q-1)/6}]$ if $q \equiv 1 \mod 3$ and $[\bar{b}^{(q+1)/6}]$ if $q \equiv -1 \mod 3$. (If $q = 27$ there are two conjugacy classes of elements of order 3. See Section 6 for this special case.) □

2.2. *Character tables.* Let ε be a primitive $(q-1)$-th root of unity and let δ be a primitive $(q+1)$-th root of unity, where $\varepsilon_{kn} = \varepsilon^{2kn} + \varepsilon^{-2kn}$ and $\delta_{tm} = -(\delta^{2tm} + \delta^{-2tm})$.

When $q \equiv 1 \mod 4$, the character table of $G = \mathrm{PSL}(2, q)$ is given in Table 1 for $1 \le m, n, t \le \frac{1}{4}(q-1)$ and $1 \le k \le \frac{1}{4}(q-5)$ [Karpilovsky 1994, Theorem 8.9].

When $q \equiv -1 \mod 4$, the character table of $G = \mathrm{PSL}(2, q)$ is given in Table 2 for $1 \le n, k, t \le \frac{1}{4}(q-3)$ and $1 \le m \le \frac{1}{4}(q+1)$ [Karpilovsky 1994, Theorem 8.11].

	$[\bar{1}]$	$[\bar{a}^n]$	$[\bar{b}^m]$	$[\bar{c}]$	$[\bar{d}]$
1_G	1	1	1	1	1
λ	q	1	-1	0	0
μ_k	$q+1$	ε_{kn}	0	1	1
θ_t	$q-1$	0	δ_{tm}	-1	-1
χ_1	$\frac{1}{2}(q+1)$	$(-1)^n$	0	$\frac{1}{2}(1+\sqrt{q})$	$\frac{1}{2}(1-\sqrt{q})$
χ_2	$\frac{1}{2}(q+1)$	$(-1)^n$	0	$\frac{1}{2}(1-\sqrt{q})$	$\frac{1}{2}(1+\sqrt{q})$

Table 1. The character table of $G = \mathrm{PSL}(2, q)$ for $q \equiv 1 \bmod 4$.

	$[\bar{1}]$	$[\bar{a}^n]$	$[\bar{b}^m]$	$[\bar{c}]$	$[\bar{d}]$
1_G	1	1	1	1	1
λ	q	1	-1	0	0
μ_k	$q+1$	ε_{kn}	0	1	1
θ_t	$q-1$	0	δ_{tm}	-1	-1
γ_1	$\frac{1}{2}(q-1)$	0	$(-1)^{m+1}$	$\frac{1}{2}(-1+\sqrt{-q})$	$\frac{1}{2}(-1-\sqrt{-q})$
γ_2	$\frac{1}{2}(q-1)$	0	$(-1)^{m+1}$	$\frac{1}{2}(-1-\sqrt{-q})$	$\frac{1}{2}(-1+\sqrt{-q})$

Table 2. The character table of $G = \mathrm{PSL}(2, q)$ for $q \equiv -1 \bmod 4$.

2.3. ***Irreducible $\mathbb{Q}$-characters.*** The character tables above give the irreducible $\mathbb{C}$-characters of $\mathrm{PSL}(2, q)$ but we need $\mathbb{Q}$-characters to compute the dimensions of the factors of the Jacobian decompositions. Since all irreducible $\mathbb{C}$-characters of $\mathrm{PSL}(2, q)$ have Schur index 1 [Janusz 1974], it is sufficient to find the Galois conjugates of all $\mathbb{C}$-characters.

The characters 1_G and λ are already $\mathbb{Q}$-characters, and it is clear that $\chi_1 + \chi_2$ and $\gamma_1 + \gamma_2$ are $\mathbb{Q}$-characters as their noninteger entries are Galois conjugates. This leaves the μ_k and θ_t characters.

Proposition 3. (a) *Let r be a divisor of $\frac{1}{2}(q-1)$ and define the set*

$$M_r = \begin{cases} \{\mu_i \mid 1 \le i \le \frac{1}{4}(q-5) \text{ and } \gcd(i, \frac{1}{2}(q-1)) = r\} & \text{if } q \equiv 1 \bmod 4, \\ \{\mu_i \mid 1 \le i \le \frac{1}{4}(q-3) \text{ and } \gcd(i, \frac{1}{2}(q-1)) = r\} & \text{if } q \equiv -1 \bmod 4. \end{cases}$$

The sum of the characters in each M_r is an irreducible $\mathbb{Q}$-character of $\mathrm{PSL}(2, q)$.

(b) *Let s be a divisor of $\frac{1}{2}(q+1)$ and define the set*

$$\Theta_s = \begin{cases} \{\theta_i \mid 1 \le i \le \frac{1}{4}(q-1) \text{ and } \gcd(i, \frac{1}{2}(q-1)) = s\} & \text{if } q \equiv 1 \bmod 4, \\ \{\theta_i \mid 1 \le i \le \frac{1}{4}(q-3) \text{ and } \gcd(i, \frac{1}{2}(q-1)) = s\} & \text{if } q \equiv -1 \bmod 4. \end{cases}$$

The sum of the characters in each Θ_s is an irreducible $\mathbb{Q}$-character of $\mathrm{PSL}(2, q)$.

	$[\bar{a}]$	$[\bar{a}^2]$	$\cdots$	$[\bar{a}^{(q-1)/4}]$
μ_1	$\rho+\rho^{-1}$	$\rho^2+\rho^{-2}$	$\cdots$	$\rho^{(q-1)/4}+\rho^{-(q-1)/4}$
μ_2	$\rho^2+\rho^{-2}$	$\rho^4+\rho^{-4}$	$\cdots$	$\rho^{(q-1)/2}+\rho^{-(q-1)/2}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\mu_{(q-5)/4}$	$\rho^{(q-5)/4}+\rho^{-(q-5)/4}$	$\rho^{(q-5)/2}+\rho^{-(q-5)/2}$	$\cdots$	$\rho^{(q-5)(q-1)/16}+\rho^{-(q-5)(q-1)/16}$

Table 3. Values of μ_k on conjugacy classes of elements $\bar{a}^n$ when $q \equiv 1 \mod 4$.

Proof. We prove (a) below. The argument for (b) is almost identical. Since the only nonrational values of the μ_k characters are their values on the $[\bar{a}^n]$, we only need to consider the values on these conjugacy classes. For simplicity of notation, we define ρ to be ε^2, so ρ is a primitive $\frac{1}{2}(q-1)$-th root of unity. Then the values of the μ_k on the conjugacy classes $[\bar{a}^n]$ in the case where $q \equiv 1 \mod 4$ are given in Table 3. $\big($For $q \equiv -1 \mod 4$, replace $\frac{1}{4}(q-5)$ in the last row with $\frac{1}{4}(q-3)$ and change the exponent in the last column from $\frac{1}{4}(q-1)$ to $\frac{1}{4}(q-3)$.$\big)$

Fix a particular μ_k with $\gcd\big(k, \frac{1}{2}(q-1)\big) = r$. The Galois orbit is completely determined by $\mu_k([\bar{a}])$ since the values of μ_k on the conjugacy classes with representative powers of $\bar{a}$ are sums of powers of the summand of $\mu_k([\bar{a}])$ (as seen in Table 3). So it is enough to find the Galois conjugates of $\mu_k([\bar{a}])$. Now $\mu_k([\bar{a}]) = \rho^k + \rho^{-k}$, where ρ^k is a primitive $\frac{1}{2r}(q-1)$-th root of unity. The Galois conjugates of this will be sums of the other primitive $\frac{1}{2r}(q-1)$-th roots of unity. By a simple order argument, we determine that ρ^i is a primitive $\big(\frac{1}{2}(q-1)/\gcd\big(i, \frac{1}{2}(q-1)\big)\big)$-th root of unity. So the other primitive $\frac{1}{2r}(q-1)$-th roots of unity appear for exactly those μ_i such that $\gcd\big(i, \frac{1}{2}(q-1)\big) = r$. So the irreducible $\mathbb{Q}$-character associated with μ_k will be the sum of μ_k with the other characters μ_i such that $\gcd\big(i, \frac{1}{2}(q-1)\big) = \gcd\big(k, \frac{1}{2}(q-1)\big) = r$. □

Example. We demonstrate the previous proposition with an example. Consider $q=29\equiv 1 \mod 4$. Here $\frac{1}{2}(q-1)=14$, $\frac{1}{2}(q+1)=15$, $\frac{1}{4}(q-5)=6$, and $\frac{1}{4}(q-1)=7$ and so there are 6 μ_k characters and 7 θ_t characters. The only divisors of $\frac{1}{2}(q-1)$ less than 6 are 1 and 2. From Proposition 3(a) we have two distinct sets

$$M_1 = \{\mu_i \mid \gcd(i, 14) = 1\} = \{\mu_1, \mu_3, \mu_5\},$$

$$M_2 = \{\mu_i \mid \gcd(i, 14) = 2\} = \{\mu_2, \mu_4, \mu_6\}.$$

The divisors of $\frac{1}{2}(q+1)$ less than 7 are 1, 3, and 5, so from Proposition 3(b) there are three distinct sets

$$\Theta_1 = \{\theta_i \mid \gcd(i, 15) = 1\} = \{\theta_1, \theta_2, \theta_4, \theta_7\},$$

$$\Theta_3 = \{\theta_i \mid \gcd(i, 15) = 3\} = \{\theta_3, \theta_6\},$$

$$\Theta_5 = \{\theta_i \mid \gcd(i, 15) = 5\} = \{\theta_5\}.$$

Therefore when $q = 29$, there are two irreducible $\mathbb{Q}$-characters of degree $q+1$ ($\mu_1+\mu_3+\mu_5$ and $\mu_2+\mu_4+\mu_6$) and three irreducible $\mathbb{Q}$-characters of degree $q-1$ ($\theta_1+\theta_2+\theta_4+\theta_7$, $\theta_3+\theta_6$, and θ_5).

We also need the values of the irreducible $\mathbb{Q}$-characters from Proposition 3 for the inner product computation of the dimensions of the factors in (1). In the rest of the paper, for any character μ_k, we denote by r the $\gcd\bigl(k, \frac{1}{2}(q-1)\bigr)$, and for any character θ_t, we denote by s the $\gcd\bigl(t, \frac{1}{2}(q+1)\bigr)$. Thus M_r from Proposition 3(a) will contain the character μ_k and Θ_s from Proposition 3(b) will contain θ_t. The value of the characters in Proposition 3 will be the value of μ_k (or θ_t) times the number of irreducible $\mathbb{C}$-characters in the set M_r (or Θ_s). The size of M_r is half the number of i such that $\gcd\bigl(i, \frac{1}{2}(q-1)\bigr) = r$, or half the number of i such that $\gcd\bigl(i, \frac{1}{2r}(q-1)\bigr) = 1$. This is $\frac{1}{2}\phi\bigl(\frac{1}{2r}(q-1)\bigr)$, where $\phi(x)$ is the Euler phi function. Similarly, the size of Θ_s is equal to $\frac{1}{2}\phi\bigl(\frac{1}{2s}(q+1)\bigr)$. Additionally for our computations, we will only need the values of the characters on conjugacy classes of orders 1, 2, 3, and 7, as it turns out that the Hurwitz character χ is 0 outside these conjugacy classes. This means the inner product we use to compute the dimension of the factors of the Jacobian will not be impacted by the values outside of these conjugacy classes. Again, see Section 3 and (5).

Determining the value of each μ_k or θ_t on the relevant conjugacy classes boils down to whether elements of that order are powers of $\bar{a}$ or $\bar{b}$. The next three propositions give the values of these characters on conjugacy classes of elements of orders 2, 3, and 7, respectively.

Proposition 4. *Consider the conjugacy class of elements of order* 2 *in* $\mathrm{PSL}(2, q)$ *for q satisfying the conditions in Proposition 2.*

(a) *When* $q \equiv 1 \bmod 4$, *the irreducible $\mathbb{Q}$-characters from Proposition 3*(a) *evaluate to* $(-1)^k\phi\bigl(\frac{1}{2r}(q-1)\bigr)$, *while the irreducible $\mathbb{Q}$-characters from Proposition 3*(b) *evaluate to* 0.

(b) *When* $q \equiv -1 \bmod 4$, *the irreducible $\mathbb{Q}$-characters from Proposition 3*(a) *evaluate to* 0, *while the irreducible $\mathbb{Q}$-characters from Proposition 3*(b) *evaluate to* $(-1)^{t+1}\phi\bigl(\frac{1}{2s}(q+1)\bigr)$.

Proof. (a) As we saw in the proof of Proposition 2, the conjugacy class of elements of order 2 is represented by a power of either $\bar{a}$ or $\bar{b}$, depending on whether $q \equiv \pm 1 \bmod 4$. In the first case, it is $[\bar{a}^{(q-1)/4}]$. Consider the value of one μ_k on this conjugacy class:

$$\varepsilon_{k(q-1)/4} = \varepsilon^{k(q-1)/2} + \varepsilon^{-k(q-1)/2}.$$

Since ε is a primitive $(q-1)$-th root of unity, $\varepsilon^{(q-1)/2}$ is a primitive second root of unity, i.e., -1. Thus $\varepsilon_{k(q-1)/4} = (-1)^k + (-1)^{-k}$. When k is odd, this value is -2, and when k is even, this value is 2. Combining this value with the number of characters in the set M_r yields the value of

$$(-1)^k \phi\left(\frac{q-1}{2r}\right).$$

The $\mathbb{Q}$-characters which are sums of the characters in Θ_s (as in Proposition 3(b)) are 0 on this class in this case. From the character table for this case, it is clear that each θ_t has a value of 0 on any conjugacy class of the form $[\bar{a}^n]$ and hence the sum of such characters also has a value of 0.

(b) When $q \equiv -1 \mod 4$, the conjugacy class is represented by $\bar{b}^{(q+1)/4}$ and so the $\mathbb{Q}$-characters in Proposition 3(a) are 0 on that class since each μ_k evaluates to 0. A similar argument as for $q \equiv 1 \mod 4$ gives that θ_t will be 2 when t is odd and -2 when t is even. Then the irreducible $\mathbb{Q}$-characters in Proposition 3(b) evaluate to this value multiplied by the size of Θ_s. This gives

$$(-1)^{t+1} \phi\left(\frac{q+1}{2s}\right). \qquad \square$$

Proposition 5. *Consider the conjugacy class of elements of order* 3 *in* PSL(2, q) *for q satisfying the conditions in Proposition 2.*

(a) *When $q \equiv 1 \mod 3$ the irreducible $\mathbb{Q}$-characters in Proposition 3*(a) *evaluate to*

$$\begin{cases} \phi\left(\frac{1}{2r}(q-1)\right) & \text{if } k \equiv 0 \mod 3, \\ -\frac{1}{2}\phi\left(\frac{1}{2r}(q-1)\right) & \text{otherwise,} \end{cases}$$

while the irreducible $\mathbb{Q}$-characters from Proposition 3(b) *evaluate to* 0.

(b) *When $q \equiv -1 \mod 3$, the characters described in Proposition 3*(a) *evaluate to* 0, *while the irreducible $\mathbb{Q}$-characters in Proposition 3*(b) *evaluate to*

$$\begin{cases} -\phi\left(\frac{1}{2s}(q+1)\right) & \text{if } t \equiv 0 \mod 3, \\ \frac{1}{2}\phi\left(\frac{1}{2s}(q+1)\right) & \text{otherwise.} \end{cases}$$

Proof. As was discussed in the proof of Proposition 2, the conjugacy class of elements of order 3 is represented by $\bar{a}^{(q-1)/6}$ or $\bar{b}^{(q+1)/6}$.

(a) Consider the value of μ_k:

$$\varepsilon_{k(q-1)/6} = \varepsilon^{k(q-1)/3} + \varepsilon^{-k(q-1)/3}.$$

Since ε is a primitive $(q-1)$-th root of unity, $\varepsilon^{(q-1)/3}$ is a third root of unity, which we call ω. Thus, $\varepsilon_{k(q-1)/4} = \omega^k + \omega^{-k}$. When $3 \mid k$, this is 2 and when $3 \nmid k$, this is $\varepsilon_{k(q-1)/4} = \omega + \omega^2 = -1$. This value, together with the size of M_r gives the value of the irreducible $\mathbb{Q}$-characters in Proposition 3(a) on elements of order 3. Since each θ_t evaluates to 0 on the conjugacy classes represented by powers of $\bar{a}$, the irreducible $\mathbb{Q}$-characters from Proposition 3(b) also evaluate to 0.

(b) A similar argument may be used when $q \equiv -1 \mod 3$ (or the elements of order 3 are in the conjugacy class represented by $\bar{b}^{(q+1)/6}$). $\square$

Proposition 6. *Consider the conjugacy classes of elements of order* 7 *in* PSL(2, q) *for q satisfying the conditions in Proposition 2.*

(a) *When* $q \equiv 1 \mod 7$, *the characters in Proposition 3*(b) *evaluate to* 0, *while the irreducible* $\mathbb{Q}$*-characters from Proposition 3*(a) *evaluate to*

$$\begin{cases} \phi\left(\frac{1}{2r}(q-1)\right) & \textit{if } k \equiv 0 \mod 7, \\ -\frac{1}{2}\phi\left(\frac{1}{2r}(q-1)\right) & \textit{otherwise}. \end{cases}$$

(b) *When* $q \equiv -1 \mod 7$, *the irreducible* $\mathbb{Q}$*-characters in Proposition 3*(a) *evaluate to* 0, *while the irreducible* $\mathbb{Q}$*-characters from Proposition 3*(b) *evaluate to*

$$\begin{cases} -\phi\left(\frac{1}{2s}(q+1)\right) & \textit{if } t \equiv 0 \mod 7, \\ \frac{1}{2}\phi\left(\frac{1}{2s}(q+1)\right) & \textit{otherwise}. \end{cases}$$

Proof. From the proof of Proposition 2 we know that the three conjugacy classes of order 7 are represented by $\bar{a}^{(q-1)/14}$, $\bar{a}^{(q-1)/7}$, and $\bar{a}^{3(q-1)/14}$ or $\bar{b}^{(q+1)/14}$, $\bar{b}^{(q+1)/7}$, and $\bar{b}^{3(q+1)/14}$.

(a) If $q \equiv 1 \mod 7$ (equivalently the conjugacy classes of elements of order 7 are represented by powers of $\bar{a}$) then μ_k evaluates to $\zeta^k + \zeta^{-k}$ on these conjugacy classes, where ζ is a primitive 7th root of unity. If $7 \mid k$, then $\zeta^k + \zeta^{-k}$ is 2 and if $7 \nmid k$, then $\zeta^k + \zeta^{-k}$ is -1. Combining this with the size of the set M_r or Θ_s gives the result.

(b) A similar argument follows for $q \equiv -1 \mod 7$ except we are considering conjugacy classes represented by powers of $\bar{b}$. $\square$

3. Computation of the Hurwitz character

Recall from (3) that in order to compute χ, we need to determine $\chi_{\langle \mathrm{id}_G \rangle}$, $\chi_{\langle h_2 \rangle}$, $\chi_{\langle h_3 \rangle}$, and $\chi_{\langle h_7 \rangle}$. Let H be a subgroup of G. By the definition of χ_H, the induced character of the trivial character of H is

$$\chi_H(g) = \frac{1}{H} \sum_{x \in G} \chi^o(xgx^{-1}), \quad \text{where } \chi^o(g) = \begin{cases} 1 & \text{if } g \in H, \\ 0 & \text{if } g \notin H. \end{cases}$$

Note that $\chi_{\langle \mathrm{id}_G \rangle}$ is just the regular representation

$$\chi_{\langle \mathrm{id}_G \rangle}(g) = \begin{cases} |G| & \text{if } g = \mathrm{id}_G, \\ 0 & \text{if } g \neq \mathrm{id}_G. \end{cases}$$

To compute the remaining three characters, we need several facts from Section 2.1 and a lemma, which is an immediate consequence of the orbit-stabilizer theorem considering the group action of conjugation.

Lemma 7. *Let G be a group and $g, h \in G$ with g not the identity. The number of $x \in G$ such that $xgx^{-1} = h$ is the size of the centralizer of h if $g \in [h]$ and 0 otherwise.*

Consider $\chi_{\langle h_2 \rangle}$. We know

$$\chi_{\langle h_2 \rangle}(g) = \frac{1}{2} \sum_{x \in G} \chi^o(xgx^{-1}). \tag{4}$$

For each $g \in G$, we must determine the number of $x \in G$ such that $xgx^{-1} = \mathrm{id}_G$ or h_2, since $\langle h_2 \rangle = \{\mathrm{id}_G, h_2\}$. The case of $xgx^{-1} = \mathrm{id}_G$ follows from the fact that, for any group G and $g \in G$ not the identity, there is no $x \in G$ so that $xgx^{-1} = \mathrm{id}_G$. Thus the number of $x \in G$ such that $xgx^{-1} = \mathrm{id}_G$ or h_2 is the size of G when g is the identity and 0 otherwise. For $\chi_{\langle h_2 \rangle}(g)$ when $g \neq \mathrm{id}_G$, if $g \notin [h_2]$ then this number is 0, else we must determine the number of $x \in G$ so that $xgx^{-1} = h_2$. By Lemma 7, this is the size of the centralizer of h_2. Recall that under the action of conjugation, orbits are conjugacy classes. By the orbit-stabilizer theorem, $|C_G(h_2)| = |G|/|[h_2]|$. For h_2 of order 2, we have $|[h_2]| = \frac{1}{2}q(q+1)$ when $q \equiv 1 \mod 4$, and $|[h_2]| = \frac{1}{2}q(q-1)$ when $q \equiv -1 \mod 4$, hence $|C_G(h_2)| = q-1$ if $q \equiv 1 \mod 4$ and $|C_G(h_2)| = q+1$ if $q \equiv -1 \mod 4$. Plugging these values into (4) gives

$$\chi_{\langle h_2 \rangle}(g) = \begin{cases} \frac{1}{2}|G| & \text{if } g = \mathrm{id}_G, \\ \frac{1}{2}(q-1) & \text{if } g \in [h_2] \text{ and } q \equiv 1 \mod 4, \\ \frac{1}{2}(q+1) & \text{if } g \in [h_2] \text{ and } q \equiv -1 \mod 4, \\ 0 & \text{otherwise.} \end{cases}$$

Now, we calculate $\chi_{\langle h_3 \rangle}$. As before, for each $g \in G$, we need to find the number of $x \in G$ so that $xgx^{-1} \in \langle h_3 \rangle = \{1, h_3, h_3^2\}$, and the formula in this case is

$$\chi_{\langle h_3 \rangle}(g) = \frac{1}{3} \sum_{x \in G} \chi^o(xgx^{-1}).$$

When $g = \mathrm{id}_G$, we have $\chi_{\langle h_3 \rangle}(\mathrm{id}_G) = \frac{1}{3}|G|$. Else by Lemma 7 and the fact that $h_3^2 \in [h_3]$, we have $\chi_{\langle h_3 \rangle}(g) = \frac{2}{3}|C_G(h_3)|$ if $g \in [h_3]$ and 0 otherwise. From Section 2.1 we know $|[h_3]| = q(q-1)$ if $3 \mid \frac{1}{2}(q+1)$ and $|[h_3]| = q(q+1)$ if $3 \mid \frac{1}{2}(q-1)$. Then $|C_G(h_3)| = \frac{1}{2}(q+1)$ if $3 \mid \frac{1}{2}(q+1)$ and $|C_G(h_3)| = \frac{1}{2}(q-1)$ if $3 \mid \frac{1}{2}(q-1)$, and

$$\chi_{\langle h_3 \rangle}(g) = \begin{cases} \frac{1}{3}|G| & \text{if } g = \mathrm{id}_G, \\ \frac{1}{3}(q-1) & \text{if } g \in [h_3] \text{ and } q \equiv 1 \mod 3, \\ \frac{1}{3}(q+1) & \text{if } g \in [h_3] \text{ and } q \equiv 2 \mod 3, \\ 0 & \text{otherwise.} \end{cases}$$

q mod 84	Value for elements of order 1	2	3	7
± 1	$\frac{1}{42}\lvert G\rvert$	$-\frac{1}{2}(q \mp 1)$	$-\frac{1}{3}(q \mp 1)$	$-\frac{1}{7}(q \mp 1)$
± 13	$\frac{1}{42}\lvert G\rvert$	$-\frac{1}{2}(q \mp 1)$	$-\frac{1}{3}(q \mp 1)$	$-\frac{1}{7}(q \pm 1)$
± 29	$\frac{1}{42}\lvert G\rvert$	$-\frac{1}{2}(q \mp 1)$	$-\frac{1}{3}(q \pm 1)$	$-\frac{1}{7}(q \mp 1)$
± 43	$\frac{1}{42}\lvert G\rvert$	$-\frac{1}{2}(q \pm 1)$	$-\frac{1}{3}(q \mp 1)$	$-\frac{1}{7}(q \mp 1)$

Table 4. Values of χ' on conjugacy classes of elements of orders 1, 2, 3, and 7.

For $\chi_{\langle h_7\rangle}$, as with the proof of the other characters, $\chi_{\langle h_7\rangle}(\mathrm{id}_G) = \frac{1}{7}|G|$. To compute the value on other elements, observe that for any g of order 7, we know that g and g^{-1} are in the same conjugacy class [Karpilovsky 1994, Corollary 8.3] but g, g^2, and g^3 are all in distinct conjugacy classes. Combining Lemma 7 with this information gives us that $\chi_{\langle h_7\rangle}(g) = \frac{2}{7}|C_G(h_7)|$, and we know the sizes of the conjugacy classes by Section 2.1. Putting all this information together, the value of $\chi_{\langle h_7\rangle}(g)$ is

$$\chi_{\langle h_7\rangle}(g) = \begin{cases} \frac{1}{7}|G| & \text{if } g = \mathrm{id}_G, \\ \frac{1}{7}(q-1) & \text{if } g \in [h_7] \text{ and } q \equiv 1 \bmod 7, \\ \frac{1}{7}(q+1) & \text{if } g \in [h_7] \text{ and } q \equiv -1 \bmod 7, \\ 0 & \text{otherwise.} \end{cases}$$

Note that the values of χ are invariant under the three conjugacy classes of elements of order 7. This means we do not have to find in which conjugacy class of elements of order 7 the monodromy exists in order to compute (3) (i.e., we do not have to explicitly find h_7, we can just use the formula above for any element of order 7).

We will use χ to calculate inner products with irreducible $\mathbb{Q}$-characters to find the dimensions of the factors in the Jacobian variety decomposition. To simplify later calculations, we rewrite χ as $\chi = 2\cdot 1_G + \chi'$, where $\chi' = \chi_{\langle 1_G\rangle} - \chi_{\langle h_2\rangle} - \chi_{\langle h_3\rangle} - \chi_{\langle h_7\rangle}$. Then, the inner product of an irreducible $\mathbb{Q}$-character ψ_i and χ will be $\langle \psi_i, \chi\rangle = 2\langle \psi_i, 1_G\rangle + \langle \psi_i, \chi'\rangle$. But since ψ_i and 1_G are orthogonal when $\psi_i \neq 1_G$, we have that $\langle \psi_i, \chi\rangle$ is simply $\langle \psi_i, \chi'\rangle$ in all cases except for the trivial character.

Table 4 gives the values of χ' on the conjugacy classes of elements of orders 1, 2, 3, and 7, computed by combining all the data in this section. Additionally, $\chi'(g) = 0$ if g is not in one of these conjugacy classes.

4. Inner product computations

Our next goal is to use our computation of χ' in Section 3 and the irreducible $\mathbb{Q}$-characters in Section 2.3 to compute the inner products $\langle \psi_i, \chi'\rangle$. Consider

$\langle \psi_i, \chi' \rangle$, where ψ_i is an irreducible $\mathbb{Q}$-character of $\mathrm{PSL}(2, q)$. The formula for the inner product is

$$\langle \psi_i, \chi' \rangle = \frac{1}{|G|} \sum_{g \in G} \psi_i(g) \chi'(g^{-1}).$$

Since g and g^{-1} are in the same conjugacy class and χ' is 0 for all elements that are not of order 1, 2, 3, or 7, we have the formula

$$\langle \psi_i, \chi' \rangle = \frac{1}{|G|} \big(\psi_i(\mathrm{id}_G) \chi'(\mathrm{id}_G) + |[h_2]| \psi_i(h_2) \chi'(h_2) \\ + |[h_3]| \psi_i(h_3) \chi'(h_3) + 3|[h_7]| \psi_i(h_7) \chi'(h_7) \big).$$

In Section 3 we saw that

$$|[h_2]|\, \chi'(h_2) = -\tfrac{1}{2}|G|, \quad |[h_3]|\, \chi'(h_3) = -\tfrac{2}{3}|G|, \quad 3|[h_7]|\, \chi'(h_7) = -\tfrac{6}{7}|G|.$$

The formula for the inner product reduces to

$$\langle \psi_i, \chi' \rangle = \tfrac{1}{42} \psi_i(\mathrm{id}_G) - \tfrac{1}{2} \psi_i(h_2) - \tfrac{2}{3} \psi_i(h_3) - \tfrac{6}{7} \psi_i(h_7). \tag{5}$$

Since the values of the irreducible $\mathbb{Q}$-characters are based on whether the conjugacy classes of elements of orders 2, 3 and 7 are represented by $\bar{a}$ or $\bar{b}$ (which depends on the residue of q modulo 3, 4, or 7), the values of these characters, and the subsequent inner products, will depend on what q is modulo $3 \cdot 4 \cdot 7 = 84$.

4.1. ***Trivial character.*** Recall that χ is the Hurwitz character, and $\chi = 2 \cdot 1_G + \chi'$.

Proposition 8. $\langle 1_G, \chi \rangle = 0.$

Proof. By the calculation of χ, we have that $\langle 1_G, \chi \rangle = 2\langle 1_G, 1_G \rangle + \langle 1_G, \chi' \rangle$ and $\langle 1_G, 1_G \rangle = 1$. Consider $\langle 1_G, \chi' \rangle$. We use (5) to get

$$\langle 1_G, \chi' \rangle = \tfrac{1}{42} \cdot 1_G(1) - \tfrac{1}{2} \cdot 1_G(h_2) - \tfrac{2}{3} \cdot 1_G(h_3) - \tfrac{6}{7} \cdot 1_G(h_7) = \tfrac{1}{42} - \tfrac{1}{2} - \tfrac{2}{3} - \tfrac{6}{7} = -2.$$

Thus, $\langle 1_G, \chi' \rangle = 2 - 2 = 0$. □

All other irreducible $\mathbb{Q}$-characters of $\mathrm{PSL}(2, q)$ have degree greater than 1. Hence by (1), where the n_i correspond to the degree of the i-th irreducible $\mathbb{Q}$-character, the decomposition of JX must have more than one factor.

Corollary 9. *No Hurwitz curve with automorphism group* $\mathrm{PSL}(2, q)$ *has a simple Jacobian variety.*

4.2. ***Character of degree q.*** Recall λ is the character of degree q. We again apply (5). Since the value of λ is either 1 or -1 depending on whether the element is in a conjugacy class represented by powers of $\bar{a}$ or $\bar{b}$, we get that $\langle \lambda, \chi' \rangle = \frac{1}{42}(q - u)$, where u is given in Table 5 and the positive u-values correspond to positive q mod 84 values and the same holds for the negative values.

$q \mod 84$	Value of u
± 1	± 85
± 13	± 13
± 29	± 29
± 43	± 43

Table 5. Values for u in $\langle \lambda, \chi' \rangle$.

4.3. ***Characters of degree*** $\frac{1}{2}(q \pm 1)$**.** For $q \equiv 1 \mod 4$, this irreducible $\mathbb{Q}$-character is $\chi_1 + \chi_2$ and evaluates to $q+1$ on the identity, $2(-1)^n$ on the conjugacy classes $[\bar{a}^n]$, and 0 on the conjugacy classes $[\bar{b}^m]$. Furthermore, the conjugacy class of elements of order 2 will always be in the set of conjugacy classes $[\bar{a}^n]$. We use (5) again, which becomes

$$\langle \chi_1 + \chi_2, \chi' \rangle = \frac{q+1}{42} - \frac{(\chi_1+\chi_2)(h_2)}{2} - \frac{2(\chi_1+\chi_2)(h_3)}{3} - \frac{6(\chi_1+\chi_2)(h_7)}{7}.$$

Determining these values depends on whether $q \equiv \pm 1 \mod 3$ and whether $q \equiv \pm 1 \mod 7$ (as we have discussed above, this distinguishes the cases where the elements of orders 3 and 7 are in conjugacy classes represented by powers of $\bar{a}$ or $\bar{b}$). But additionally we need to determine if n is even or odd to determine the sign of $\chi_1 + \chi_2$. Recall n is given by $\frac{1}{6}(q-1)$ for elements of order 3 and $\frac{1}{14}(q-1)$ for elements of order 7. This requires us to consider values modulo $3 \cdot 4 \cdot 7 \cdot 2 = 168$.

Similar arguments will give us the values for $\gamma_1 + \gamma_2$ when $q \equiv -1 \mod 4$. In all cases, the inner product is given by $\frac{1}{42}(q - v)$, where v is given in Table 6. In the table, the positive values of $q \mod 168$ correspond to the positive v-values and the same holds for the negative values.

4.4. ***Characters of degree*** $q \pm 1$**.** The computations for the inner products of χ' with sums of μ_k or θ_t are similar. We recall the values of these $\mathbb{Q}$-characters

$q \mod 168$	Values of v
± 1	± 169
± 13	± 13
± 29	± 29
± 41	± 41
± 43	± 43
± 85	± 85
± 97	± 97
± 113	± 113

Table 6. Values for v in $\langle \chi_1 + \chi_2, \chi' \rangle$ or $\langle \gamma_1 + \gamma_2, \chi' \rangle$.

	$q \equiv 1 \mod 4$	$q \equiv -1 \mod 4$
μ_k	$z+(f-1)\cdot 84$	$z-f\cdot 84$
θ_t	$z+f\cdot 84$	$z-(f-1)\cdot 84$

Table 7. Values of w for the inner products of χ' with characters of degree $q\pm 1$.

on the conjugacy classes of orders 1, 2, 3, and 7 from Section 2.3. The values depend on whether the conjugacy classes are powers of $\bar{a}$ or $\bar{b}$. To describe the value in all cases, we define two additional values. For $r = \gcd\bigl(k, \frac{1}{2}(q-1)\bigr)$ and $s = \gcd\bigl(t, \frac{1}{2}(q+1)\bigr)$, define f to be the number of 2, 3, and 7 which divide r (or s). Also define z to be the least residue of q modulo 84. Then the inner product with irreducible $\mathbb{Q}$-characters from Proposition 3(a) is

$$\frac{1}{2}\phi\left(\frac{q-1}{2r}\right)\frac{q-w}{42},$$

and the inner product with irreducible $\mathbb{Q}$-characters from Proposition 3(b) is

$$\frac{1}{2}\phi\left(\frac{q+1}{2s}\right)\frac{q-w}{42},$$

where w is given in Table 7.

Example. Continuing from the example in Section 2.3, let $q = 29$, so z also is 29. When $r = 1$ (or $s = 1$ or 5) then $f = 0$ and when $r = 2$ (or $s = 3$) we have $f = 1$. In this case (since $q = z$) if $f = 1$, then the value of the inner product on the corresponding irreducible $\mathbb{Q}$-character which is the sum of characters in M_r ($r = 2$) will be 0 and if $f = 0$, the value on the inner product of the corresponding irreducible $\mathbb{Q}$-character which is the sum of characters in Θ_s ($s = 1$ or 5) will also be 0. This just leaves two nonzero values to compute ($r = 1$ and $s = 3$),

$$\langle \mu_1 + \mu_3 + \mu_5, \chi' \rangle = \tfrac{1}{2}\phi\bigl(\tfrac{28}{2}\bigr)\cdot\bigl(\tfrac{29+55}{42}\bigr) = \tfrac{6}{2}\cdot 2 = 6$$

and

$$\langle \theta_3 + \theta_6, \chi' \rangle = \tfrac{1}{2}\phi\bigl(\tfrac{30}{6}\bigr)\cdot\bigl(\tfrac{29+55}{42}\bigr) = \tfrac{4}{2}\cdot 2 = 4.$$

5. Decomposition of Jacobian varieties

As described in the introduction, Jacobian varieties may be factored into the direct product of abelian varieties as in (1). The dimension of the factors is half of the inner product computed in Section 4. Collecting the information in the previous section we get the following result.

Theorem 10. *Let X be a Hurwitz curve with full automorphism group* $\mathrm{PSL}(2, q)$, *where q is odd and $q > 27$. Let u, v, and w be as given in Tables 5, 6, and 7, respectively.*

When $q \equiv 1 \bmod 4$, the Jacobian variety of X is isogenous to

$$A^q \oplus B^{(q+1)/2} \oplus \prod_{\substack{r \mid (q-1)/2 \\ r<(q-5)/4}} C_r^{q+1} \oplus \prod_{\substack{s \mid (q+1)/2 \\ s<(q-1)/4}} D_s^{q-1},$$

and when $q \equiv -1 \bmod 4$, the Jacobian variety of X is isogenous to

$$A^q \oplus B^{(q-1)/2} \oplus \prod_{\substack{r \mid (q-1)/2 \\ r<(q-3)/4}} C_r^{q+1} \oplus \prod_{\substack{s \mid (q+1)/2 \\ s<(q-3)/4}} D_s^{q-1},$$

where the factors in the decomposition are abelian varieties and

- *A has dimension $\frac{1}{84}(q-u)$,*
- *B has dimension $\frac{1}{84}(q-v)$,*
- *each C_r has dimension $\frac{1}{168}\phi\big(\frac{1}{2r}(q-1)\big) \cdot (q-w)$,*
- *and each D_s has dimension $\frac{1}{168}\phi\big(\frac{1}{2s}(q+1)\big) \cdot (q-w)$.*

As mentioned in the introduction, the decomposition technique does not guarantee that the factors are indecomposable. Also, when determining w, note that the product indexed by r corresponds to inner products of characters which are sums of μ_k characters, and the product indexed by s corresponds to inner products of characters which are sums of the θ_t characters.

6. Special case

In the special case when $q = 27 = 3^3$, there are still three conjugacy classes of elements of order 7 and one of elements of order 2; however, there are now two conjugacy classes of elements of order 3. When we apply the decomposition technique to this special case we find

$$JX \sim E_1^{13} \times A_3^{26} \times E_2^{27},$$

where the E_i are elliptic curves and A_3 is a dimension-3 abelian variety. These factors correspond to nonzero inner products of χ with the character $\gamma_1 + \gamma_2$, a sum of θ_t, and λ, respectively.

Acknowledgments

The authors thank Grinnell College for providing generous summer funding through the Mentored Advanced Project program. They also thank the anonymous referee for suggestions which improve the exposition and clarity of the paper.

References

[Cardona 2004] G. Cardona, "$\mathbb{Q}$-curves and abelian varieties of GL_2-type from dihedral genus 2 curves", pp. 45–52 in *Modular curves and abelian varieties*, edited by J. Cremona et al., Progr. Math. **224**, Birkhäuser, Basel, 2004. MR 2058641 Zbl 1080.11045

[Conder 1990] M. Conder, "Hurwitz groups: a brief survey", *Bull. Amer. Math. Soc.* (*N.S.*) **23**:2 (1990), 359–370. MR 1041434 Zbl 0716.20015

[Earle 2006] C. J. Earle, "The genus two Jacobians that are isomorphic to a product of elliptic curves", pp. 27–36 in *The geometry of Riemann surfaces and abelian varieties*, edited by J. M. Muñoz Porras et al., Contemp. Math. **397**, Amer. Math. Soc., Providence, RI, 2006. MR 2217995 Zbl 1099.14017

[Howe et al. 2000] E. W. Howe, F. Leprévost, and B. Poonen, "Large torsion subgroups of split Jacobians of curves of genus two or three", *Forum Math.* **12**:3 (2000), 315–364. MR 1748483 Zbl 0983.11037

[Janusz 1974] G. J. Janusz, "Simple components of $Q[\mathrm{SL}(2,\ q)]$", *Comm. Algebra* **1** (1974), 1–22. MR 0344323 Zbl 0281.20003

[Kani and Rosen 1989] E. Kani and M. Rosen, "Idempotent relations and factors of Jacobians", *Math. Ann.* **284**:2 (1989), 307–327. MR 1000113 Zbl 0652.14011

[Karpilovsky 1994] G. Karpilovsky, *Group representations*, vol. 3, North-Holland Mathematics Studies **180**, North-Holland Publishing Co., Amsterdam, 1994. MR 1280715 Zbl 0804.20001

[Kuwata 2005] M. Kuwata, "Quadratic twists of an elliptic curve and maps from a hyperelliptic curve", *Math. J. Okayama Univ.* **47** (2005), 85–97. MR 2198864 Zbl 1161.11353

[Macbeath 1969] A. M. Macbeath, "Generators of the linear fractional groups", pp. 14–32 in *Number Theory* (Houston, Tex., 1967), vol. XII, Proc. Sympos. Pure Math., Amer. Math. Soc., Providence, R.I., 1969. MR 0262379 Zbl 0192.35703

[Magaard et al. 2009] K. Magaard, T. Shaska, and H. Völklein, "Genus 2 curves that admit a degree 5 map to an elliptic curve", *Forum Math.* **21**:3 (2009), 547–566. MR 2526800 Zbl 1174.14025

[Milne 1980] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series **33**, Princeton University Press, 1980. MR 559531 Zbl 0433.14012

[Paulhus 2008] J. Paulhus, "Decomposing Jacobians of curves with extra automorphisms", *Acta Arith.* **132**:3 (2008), 231–244. MR 2403651 Zbl 1142.14017

[Rubin and Silverberg 2001] K. Rubin and A. Silverberg, "Rank frequencies for quadratic twists of elliptic curves", *Experiment. Math.* **10**:4 (2001), 559–569. MR 1881757 Zbl 1035.11025

[Wolfart 2002] J. Wolfart, "Regular dessins, endomorphisms of Jacobians, and transcendence", pp. 107–120 in *A panorama of number theory or the view from Baker's garden* (Zürich, 1999), edited by G. Wüstholz, Cambridge Univ. Press, 2002. MR 1975447 Zbl 1042.14016

Received: 2015-02-05 Revised: 2015-07-08 Accepted: 2015-07-20

fischera@grinnell.edu *Department of Mathematics and Statistics, Grinnell College, Grinnell, IA 50112, United States*

liumouch@grinnell.edu *Department of Mathematics and Statistics, Grinnell College, Grinnell, IA 50112, United States*

paulhusj@grinnell.edu *Department of Mathematics and Statistics, Grinnell College, Grinnell, IA 50112, United States*

mathematical sciences publishers msp

involve

msp.org/involve

INVOLVE YOUR STUDENTS IN RESEARCH

Involve showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2016 is US $160/year for the electronic version, and $215/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2016 vol. 9 no. 4

1944-4176(2016)9:4;1-1