Genus 2 curves with $(3, 3)$-split Jacobian and Large Automorphism Group

Tony Shaska

University of California at Irvine, Irvine, CA 92697.
tshaska@math.uci.edu
WWW home page: http://www.math.uci.edu/~tshaska

Abstract. Let $\mathcal{C}$ be a genus 2 curve defined over k, $char(k) = 0$. If $\mathcal{C}$ has a $(3, 3)$-split Jacobian then we show that the automorphism group $Aut(\mathcal{C})$ is isomorphic to one of the following: $\mathbb{Z}_2, V_4, D_8$, or D_{12}. There are exactly six $\mathbb{C}$-isomorphism classes of genus two curves $\mathcal{C}$ with $Aut(\mathcal{C})$ isomorphic to D_8 (resp., D_{12}) and with $(3, 3)$-split Jacobian. We show that exactly four (resp., three) of these classes with group D_8 (resp., D_{12}) have representatives defined over $\mathbb{Q}$. We discuss some of these curves in detail and find their rational points.

1 Introduction

Let $\mathcal{C}$ be a genus 2 curve defined over an algebraically closed field k, of characteristic zero. We denote by $K := k(\mathcal{C})$ its function field and by $Aut(\mathcal{C}) := Aut(K/k)$ the automorphism group of $\mathcal{C}$. Let $\psi : \mathcal{C} \to \mathcal{E}$ be a degree n maximal covering (i.e. does not factor through an isogeny) to an elliptic curve $\mathcal{E}$ defined over k. We say that $\mathcal{C}$ has a *degree n elliptic subcover*. Degree n elliptic subcovers occur in pairs. Let $(\mathcal{E}, \mathcal{E}')$ be such a pair. It is well known that there is an isogeny of degree n^2 between the Jacobian $J_\mathcal{C}$ of $\mathcal{C}$ and the product $\mathcal{E} \times \mathcal{E}'$. We say that $\mathcal{C}$ has **(n,n)-split Jacobian**. The locus of such $\mathcal{C}$ (denoted by $\mathcal{L}_n$) is an algebraic subvariety of the moduli space $\mathcal{M}_2$ of genus two curves. For the equation of $\mathcal{L}_2$ in terms of Igusa invariants, see [18]. Computation of the equation of $\mathcal{L}_3$ was the main focus of [17]. For $n > 3$, equations of $\mathcal{L}_n$ have not yet been computed.

Equivalence classes of degree 2 coverings $\psi : \mathcal{C} \to \mathcal{E}$ are in 1-1 correspondence with conjugacy classes of non-hyperelliptic involutions in $Aut(\mathcal{C})$. In any characteristic different from 2, the automorphism group $Aut(\mathcal{C})$ is isomorphic to one of the following: $\mathbb{Z}_2$, $\mathbb{Z}_{10}$, V_4, D_8, D_{12}, $\mathbb{Z}_3 \rtimes D_8$, $GL_2(3)$, or 2^+S_5; see [18]. Here V_4 is the Klein 4-group, D_8 (resp., D_{12}) denotes the dihedral group of order 8 (resp., 12), and $\mathbb{Z}_2, \mathbb{Z}_{10}$ are cyclic groups of order 2 and 10. For a description of other groups, see [18]. If $Aut(\mathcal{C}) \cong \mathbb{Z}_{10}$ then $\mathcal{C}$ is isomorphic to $Y^2 = X^6 - X$. Thus, if $\mathcal{C}$ has extra automorphisms and it is not isomorphic to $Y^2 = X^6 - X$ then $\mathcal{C} \in \mathcal{L}_2$. We say that a genus 2 curve $\mathcal{C}$ has **large automorphism group** if the order of $Aut(\mathcal{C})$ is bigger then 4.

In section 2, we describe the loci for genus 2 curves with $Aut(\mathcal{C})$ isomorphic to D_8 or D_{12} in terms of Igusa invariants. From these invariants we are able to determine the field of definition of a curve $\mathcal{C}$ with $Aut(\mathcal{C}) \cong D_8$ or D_{12}. Further, we find the equation for this $\mathcal{C}$ and j-invariants of degree 2 elliptic subcovers in terms of i_1, i_2, i_3 (cf. section 2). This determines the fields of definition for these elliptic subcovers.

Let $\mathcal{C}$ be a genus 2 curve with $(3, 3)$-split Jacobian. In section 3 we give a short description of the space $\mathcal{L}_3$. Results described in section 3 follow from [17], even though sometimes nontrivially. We find equations of degree 3 elliptic subcovers in terms of the coefficients of $\mathcal{C}$. In section 4, we show that $Aut(\mathcal{C})$ is one of the following: $\mathbb{Z}_2$, V_4, D_8, or D_{12}. Moreover, we show that there are exactly six $\mathbb{C}$-isomorphism classes of genus two curves $\mathcal{C} \in \mathcal{L}_3$ with automorphism group D_8 (resp., D_{12}). We explicitly find the absolute invariants i_1, i_2, i_3 which determine these classes. For each such class we give the equation of a representative genus 2 curve $\mathcal{C}$. We notice that there are four cases (resp., three) such that the triple of invariants $(i_1, i_2, i_3) \in \mathbb{Q}^3$ when $Aut(C) \cong D_8$ (resp., $Aut(C) \cong D_{12}$). Using results from section 2, we determine that there are exactly four (resp., three) genus 2 curves $\mathcal{C} \in \mathcal{L}_3$ (up to $\bar{\mathbb{Q}}$-isomorphism) with group D_8 (resp., D_{12}) defined over $\mathbb{Q}$ and list their equations in Table 1. We discuss these curves and their degree 2 and 3 elliptic subcovers in more detail in section 5. Our focus is on the cases which have elliptic subcovers defined over $\mathbb{Q}$. In some of these cases we are able to use these elliptic subcovers to find the rational points of the genus 2 curve. This technique has been used before by Flynn and Wetherell [5] for the degree 2 elliptic subcovers.

Curves of genus 2 with degree 2 elliptic subcovers (or with elliptic involutions) were first studied by Legendre and Jacobi. The genus 2 curve with the largest known number of rational points has automorphism group isomorphic to D_{12}; thus it has degree 2 elliptic subcovers. It was found by Keller and Kulesz and it is known to have at least 588 rational points; see [10]. Using degree 2 elliptic subcovers Howe, Leprevost, and Poonen [8] were able to construct a family of genus 2 curves whose Jacobians each have large rational torsion subgroups. Similar techniques probably could be applied using degree 3 elliptic subcovers. Curves of genus 2 with degree 3 elliptic subcovers have already occurred in the work of Clebsch, Hermite, Goursat, Burkhardt, Brioschi, and Bolza in the context of elliptic integrals. For a history of this topic see Krazer [11] (p. 479). For more recent work see Kuhn [12] and [17]. More generally, degree n elliptic subfields of genus 2 fields have been studied by Frey [6], Frey and Kani [7], Kuhn [12], and this author [16].

Acknowledgements: The author wants to thank Professor Fried for his continuous support.

2 Genus two curves with extra automorphisms and the moduli space $\mathcal{M}_2$.

Let k be an algebraically closed field of characteristic zero and $\mathcal{C}$ a genus 2 curve defined over k. Then $\mathcal{C}$ can be described as a double cover of $\mathbb{P}^1(k)$ ramified in 6 places $w_1, \dots, w_6$. This sets up a bijection between isomorphism classes of genus 2 curves and unordered distinct 6-tuples $w_1, \dots, w_6 \in \mathbb{P}^1(k)$ modulo automorphisms of $\mathbb{P}^1(k)$. An unordered 6-tuple $\{w_i\}_{i=1}^6$ can be described by a binary sextic (i.e. a homogenous equation $f(X,Z)$ of degree 6). Let $\mathcal{M}_2$ denote the moduli space of genus 2 curves; see [15]. To describe $\mathcal{M}_2$ we need to find polynomial functions of the coefficients of a binary sextic $f(X,Z)$ invariant under linear substitutions in X, Z of determinant one. These invariants were worked out by Clebsch and Bolza in the case of zero characteristic and generalized by Igusa for any characteristic different from 2; see [1], [9].

Consider a binary sextic, i.e. a homogeneous polynomial $f(X,Z)$ in $k[X,Z]$ of degree 6:

$$f(X,Z) = a_6X^6 + a_5X^5Z + \cdots + a_0Z^6.$$

Igusa J-invariants $\{J_{2i}\}$ of $f(X,Z)$ are homogeneous polynomials of degree $2i$ in $k[a_0, \dots, a_6]$, for $i = 1, 2, 3, 5$; see [9], [18] for their definitions. Here J_{10} is simply the discriminant of $f(X,Z)$. It vanishes if and only if the binary sextic has a multiple linear factor. These J_{2i} are invariant under the natural action of $SL_2(k)$ on sextics. Dividing such an invariant by another one of the same degree gives an invariant under $GL_2(k)$ action.

Remark 1. There many sets of $SL_2(k)$ invariants of binary sextics. The J_{2i} invariants that we use were first defined by Igusa [9] and work in all characteristics. One can download a MAPLE package that computes J_{2i} from author's web site. For more information on other sets of invariants the reader can see the *Igusa Invariants* package in MAGMA written by E. Howe.

Two genus 2 fields K (resp., curves) in the standard form $Y^2 = f(X,1)$ are isomorphic if and only if the corresponding sextics are $GL_2(k)$ conjugate. Thus if I is a $GL_2(k)$ invariant (resp., homogeneous $SL_2(k)$ invariant), then the expression $I(K)$ (resp., the condition $I(K) = 0$) is well defined. Thus the $GL_2(k)$ invariants are functions on the moduli space $\mathcal{M}_2$ of genus 2 curves. This $\mathcal{M}_2$ is an affine variety with coordinate ring $k[\mathcal{M}_2] = k[a_0, \dots, a_6, J_{10}^{-1}]^{GL_2(k)}$ which is the subring of degree 0 elements in $k[J_2, \dots, J_{10}, J_{10}^{-1}]$; see Igusa [9]. The *absolute invariants*

$$i_1 := 144\frac{J_4}{J_2^2}, \quad i_2 := -1728\frac{J_2J_4 - 3J_6}{J_2^3}, \quad i_3 := 486\frac{J_{10}}{J_2^5} \tag{1}$$

are even $GL_2(k)$-invariants. Two genus 2 curves with $J_2 \neq 0$ are isomorphic if and only if they have the same absolute invariants. If $J_2 = 0$ then we can define new invariants as in [17]. For the rest of this paper if we say "there is a genus 2 curve $\mathcal{C}$ defined over k" we will mean the k-isomorphism class of $\mathcal{C}$.

One can define $GL_2(k)$ invariants with J_{10} in the denominator which will be defined everywhere. However, this is not efficient in doing computations since the degrees of these rational functions in terms of the coefficients of $\mathcal{C}$ will be multiples of 10 and therefore higher then degrees of i_1, i_2, i_3. For the purposes of this paper defining i_1, i_2, i_3 as above is not a restriction as it will be seen in the proof of Theorem 1. For the proofs of the following two lemmas, see [18].

Lemma 1. *The automorphism group G of a genus 2 curve $\mathcal{C}$ in characteristic $\neq 2$ is isomorphic to $\mathbb{Z}_2$, $\mathbb{Z}_{10}$, V_4, D_8, D_{12}, $\mathbb{Z}_3 \rtimes D_8$, $GL_2(3)$, or 2^+S_5. The case when $G \cong 2^+S_5$ occurs only in characteristic 5. If $G \cong \mathbb{Z}_3 \rtimes D_8$ (resp., $GL_2(3)$) then $\mathcal{C}$ has equation $Y^2 = X^6 - 1$ (resp., $Y^2 = X(X^4 - 1)$). If $G \cong \mathbb{Z}_{10}$ then $\mathcal{C}$ has equation $Y^2 = X^6 - X$.*

Remark 2. For the analogue of the above lemma for $g > 2$ in characteristic zero see [13] where sophisticated methods of computational group theory are used.

For the rest of this paper we assume that $char(k) = 0$.

Lemma 2. *i) The locus $\mathcal{L}_2$ of genus 2 curves $\mathcal{C}$ which have a degree 2 elliptic subcover is a closed subvariety of $\mathcal{M}_2$. The equation of $\mathcal{L}_2$ is given by equation (17) in [18].*

ii) The locus of genus 2 curves $\mathcal{C}$ with $Aut(\mathcal{C}) \cong D_8$ is given by the equation of $\mathcal{L}_2$ and

$$1706 J_4^2 J_2^2 + 2560 J_4^3 + 27 J_4 J_2^4 - 81 J_2^3 J_6 - 14880 J_2 J_4 J_6 + 28800 J_6^2 = 0 \quad (2)$$

iii) The locus of genus 2 curves $\mathcal{C}$ with $Aut(\mathcal{C}) \cong D_{12}$ is

$$\begin{aligned} -J_4 J_2^4 + 12 J_2^3 J_6 - 52 J_4^2 J_2^2 + 80 J_4^3 + 960 J_2 J_4 J_6 - 3600 J_6^2 = 0 \\ 864 J_{10} J_2^5 + 3456000 J_{10} J_4^2 J_2 - 43200 J_{10} J_4 J_2^3 - 2332800000 J_{10}^2 - J_4^2 J_2^6 \\ -768 J_4^4 J_2^2 + 48 J_4^3 J_2^4 + 4096 J_4^5 = 0 \end{aligned} \quad (3)$$

We will refer to the locus of genus 2 curves $\mathcal{C}$ with $Aut(\mathcal{C}) \cong D_{12}$ (resp., $Aut(\mathcal{C}) \cong D_8$) as the D_8-locus (resp., D_{12}-locus).

Each genus 2 curve $\mathcal{C} \in \mathcal{L}_2$ has a non-hyperelliptic involution $v_0 \in Aut(\mathcal{C})$. There is another non-hyperelliptic involution $v_0' := v_0\, w$, where w is the hyperelliptic involution. Thus, degree 2 elliptic subcovers come in pairs. We denote the pair of degree 2 elliptic subcovers by (E_0, E_0'). If $Aut(\mathcal{C}) \cong D_8$ then $E_0 \cong E_0'$ or E_0 and E_0' are 2-isogenous. If $Aut(\mathcal{C}) \cong D_{12}$, then E_0 and E_0' are isogenous of degree 3. See [18] for details. The parameterizations of the following lemma were pointed out by G. Cardona.

Lemma 3. *Let $\mathcal{C}$ be a genus 2 curve defined over k. Then,*

i) $Aut(\mathcal{C}) \cong D_8$ if and only if $\mathcal{C}$ is isomorphic to

$$Y^2 = X^5 + X^3 + tX \quad (4)$$

for some $t \in k \setminus \{0, \frac{1}{4}, \frac{9}{100}\}$.

ii) $Aut(\mathcal{C}) \cong D_{12}$ if and only if $\mathcal{C}$ is isomorphic to

$$Y^2 = X^6 + X^3 + t \quad (5)$$

for some $t \in k \setminus \{0, \frac{1}{4}, -\frac{1}{50}\}$.

Proof. i) $Aut(\mathcal{C}) \cong D_8$: Then $\mathcal{C}$ is isomorphic to

$$Y^2 = (X^2 - 1)(X^4 - \lambda X^2 + 1)$$

for $\lambda \neq \pm 2$; see [18]. Denote $\tau := \sqrt{-2\frac{\lambda+6}{\lambda-2}}$. The transformation

$$\phi : (X, Y) \to (\frac{\tau x - 1}{\tau x + 1}, \frac{4\tau}{(\tau x + 1)^3} \cdot \frac{(\lambda + 6)^2}{\lambda - 2})$$

gives

$$Y^2 = X^5 + X^3 + tX$$

where $t = \frac{1}{4}(\frac{\lambda-2}{\lambda+6})^2$ and $t \neq 0, \frac{1}{4}$. If $t = \frac{9}{100}$ then $Aut(\mathcal{C})$ has order 24.

Conversely, the absolute invariants i_1, i_2, i_3 of a genus 2 curve $\mathcal{C}$ isomorphic to

$$Y^2 = X^5 + X^3 + tX$$

satisfy the locus as described in Lemma 2, part ii). Thus, $Aut(\mathcal{C}) \cong D_8$.

ii) $Aut(\mathcal{C}) \cong D_{12}$: In [18] it is shown that $\mathcal{C}$ is isomorphic to

$$Y^2 = (X^3 - 1)(X^3 - \lambda)$$

for $\lambda \neq 0, 1$ and $\lambda^2 - 38\lambda + 1 \neq 0$. Then,

$$\phi : (X, Y) \to ((\lambda + 1)^{\frac{1}{3}} X, (\lambda + 1) Y)$$

transforms $\mathcal{C}$ to the curve with equation

$$Y^2 = X^6 + X^3 + t$$

where $t = \frac{\lambda}{(\lambda+1)^2}$ and $t \neq 0, \frac{1}{4}$. If $t = -\frac{1}{50}$ then $Aut(\mathcal{C})$ has order 48.

The absolute invariants i_1, i_2, i_3 of a genus 2 curve $\mathcal{C}$ isomorphic to

$$Y^2 = X^6 + X^3 + t$$

satisfy the locus as described in Lemma 2, part iii). Thus, $Aut(\mathcal{C}) \cong D_{12}$. This completes the proof.

□

The following lemma determines a genus 2 curve for each point in the D_8 or D_{12} locus.

Lemma 4. *Let* $\mathfrak{p} := (J_2, J_4, J_6, J_{10})$ *be a point in* $\mathcal{L}_2$ *such that* $J_2 \neq 0$ *and* (i_1, i_2, i_3) *the corresponding absolute invariants.*

i) If $\mathfrak{p}$ *is in the* D_8*-locus, then the genus two curve* $\mathcal{C}$ *corresponding to* $\mathfrak{p}$ *is given by:*

$$Y^2 = X^5 + X^3 - \frac{3}{4} \cdot \frac{345 i_1^2 + 50 i_1 i_2 - 90 i_2 - 1296 i_1}{2925 i_1^2 + 250 i_1 i_2 - 9450 i_2 - 54000 i_1 + 139968} X.$$

ii) If $\mathfrak{p}$ *is in the* D_{12}*-locus, then the genus two curve* $\mathcal{C}$ *corresponding to* $\mathfrak{p}$ *is given by:*

$$Y^2 = X^6 + X^3 + \frac{1}{4} \cdot \frac{540 i_1^2 + 100 i_1 i_2 - 1728 i_1 + 45 i_2}{2700 i_1^2 + 1000 i_1 i_2 + 204525 i_1 + 40950 i_2 - 708588}.$$

Proof. i) By the previous lemma every genus 2 curve $\mathcal{C}$ with automorphism group D_8 is isomorphic to $Y^2 = X^5 + X^3 + tX$. Since $J_2 \neq 0$ then $t \neq -\frac{3}{20}$ and the absolute invariants are:

$$i_1 = -144\, t\, \frac{(20t-9)}{(20t+3)^2}, \quad i_2 = 3456\, t^2\, \frac{(140t-27)}{(20t+3)^3}, \quad i_3 = 243\, t^3\, \frac{(4t-1)^2}{(20t+3)^5} \tag{6}$$

From the above system we have

$$t = -\frac{3}{4}\, \frac{345 i_1^2 + 50 i_1 i_2 - 90 i_2 - 1296 i_1}{2925 i_1^2 + 250 i_1 i_2 - 9450 i_2 - 54000 i_1 + 139968}.$$

ii) By the previous lemma every genus 2 curve $\mathcal{C}$ with automorphism group D_{12} is isomorphic to $Y^2 = X^6 + X^3 + t$. The absolute invariants are:

$$i_1 = 1296 \frac{t(5t+1)}{(40t-1)^2}, \quad i_2 = -11664 \frac{t(20t^2+26t-1)}{(40t-1)^3}, \quad i_3 = \frac{729}{16}\, \frac{t^2(4t-1)^3}{(40t-1)^5}. \tag{7}$$

From the above system we have

$$t = \frac{1}{4}\, \frac{540 i_1^2 + 100 i_1 i_2 - 1728 i_1 + 45 i_2}{2700 i_1^2 + 1000 i_1 i_2 + 204525 i_1 + 40950 i_2 - 708588}.$$

This completes the proof.

□

Note: If $J_2 = 0$ then there is exactly one isomorphism class of genus 2 curves with automorphism group D_8 (resp., D_{12}) given by $Y^2 = X^5 + X^3 - \frac{3}{20}X$ (resp., $Y^2 = X^6 + X^3 - \frac{1}{40}$).

Remark 3. If the invariants $i_1, i_2, i_3 \in \mathbb{Q}$ then from the lemma above there is a $\mathcal{C}$ corresponding to these invariants defined over $\mathbb{Q}$. If a genus 2 curve does not have extra automorphisms (i.e. $Aut(\mathcal{C}) \cong \mathbb{Z}_2$), then an algorithm of Mestre determines if the curve is defined over $\mathbb{Q}$.

If the order of the automorphism group $Aut(C)$ is divisible by 4, then $\mathcal{C}$ has degree 2 elliptic subcovers. These elliptic subcovers are determined explicitly in [18]. Do these elliptic subcovers of $\mathcal{C}$ have the same field of definition as $\mathcal{C}$? In general the answer is negative. The following lemma determines the field of definition of these elliptic subcovers when $Aut(\mathcal{C})$ is isomorphic to D_8 or D_{12}.

Lemma 5. *Let $\mathcal{C}$ be a genus 2 curve defined over k, $char(k) = 0$.*

i) If $\mathcal{C}$ has equation

$$Y^2 = X^5 + X^3 + tX,$$

where $t \in k \setminus \{\frac{1}{4}, \frac{9}{100}\}$, then its degree 2 elliptic subfields have j-invariants given by

$$j^2 - 128 \frac{2000t^2 + 1440t + 27}{(4t-1)^2} j + 4096 \frac{(100t-9)^3}{(4t-1)^3} = 0.$$

ii) If $\mathcal{C}$ has equation

$$Y^2 = X^6 + X^3 + t,$$

where $t \in k \setminus \{\frac{1}{4}, -\frac{1}{50}\}$*, then its degree 2 elliptic subfields have* j*-invariants given by*

$$j^2 - 13824\, t\, \frac{500t^2 + 965t + 27}{(4t-1)^3} j + 47775744\, t\, \frac{(25t-4)^3}{(4t-1)^4} = 0.$$

Proof. The proof is elementary and follows from [18]. □

3 Curves of genus 2 with degree 3 elliptic subcovers

In this section we will give a brief description of the spaces $\mathcal{L}_2$ and $\mathcal{L}_3$. In the case $J_2 \neq 0$ we take these spaces as equations in terms of i_1, i_2, i_3, otherwise as homogeneous equations in terms of J_2, J_4, J_6, J_{10}. By a point $\mathfrak{p} \in \mathcal{L}_3$ we will mean a tuple (J_2, J_4, J_6, J_{10}) which satisfies the equation of $\mathcal{L}_3$. When it is clear that $J_2 \neq 0$ then $\mathfrak{p} \in \mathcal{L}_3$ would mean a triple $(i_1, i_2, i_3) \in \mathcal{L}_3$. As before k is an algebraically closed field of characteristic zero.

Definition 1. *A* **non-degenerate pair** *(resp.,* **degenerate pair***) is a pair* $(\mathcal{C}, \mathcal{E})$ *such that* $\mathcal{C}$ *is a genus 2 curve with a degree 3 elliptic subcover* $\mathcal{E}$ *where* $\psi : \mathcal{C} \to \mathcal{E}$ *is ramified in two (resp., one) places. Two such pairs* $(\mathcal{C}, \mathcal{E})$ *and* $(\mathcal{C}', \mathcal{E}')$ *are called isomorphic if there is a* k*-isomorphism* $\mathcal{C} \to \mathcal{C}'$ *mapping* $\mathcal{E} \to \mathcal{E}'$*.*

If $(\mathcal{C}, \mathcal{E})$ is a non-degenerate pair, then $\mathcal{C}$ can be parameterized as follows

$$Y^2 = (\mathfrak{v}^2 X^3 + \mathfrak{u}\mathfrak{v} X^2 + \mathfrak{v} X + 1)\,(4\mathfrak{v}^2 X^3 + \mathfrak{v}^2 X^2 + 2\mathfrak{v} X + 1), \tag{8}$$

where $\mathfrak{u}, \mathfrak{v} \in k$ and the discriminant

$$\Delta = -16\, \mathfrak{v}^{17}\,(\mathfrak{v} - 27)\,(27\mathfrak{v} + 4\mathfrak{v}^2 - \mathfrak{u}^2\mathfrak{v} + 4\mathfrak{u}^3 - 18\mathfrak{u}\mathfrak{v})^3$$

of the sextic is nonzero. We let $R := (27\mathfrak{v} + 4\mathfrak{v}^2 - \mathfrak{u}^2\mathfrak{v} + 4\mathfrak{u}^3 - 18\mathfrak{u}\mathfrak{v}) \neq 0$. For $4\mathfrak{u} - \mathfrak{v} - 9 \neq 0$ the degree 3 coverings are given by $\phi_1(X, Y) \to (U_1, V_1)$ and $\phi_2(X, Y) \to (U_2, V_2)$ where

$$\begin{aligned} U_1 &= \frac{\mathfrak{v} X^2}{\mathfrak{v}^2 X^3 + \mathfrak{u}\mathfrak{v} X^2 + \mathfrak{v} X + 1}, \quad U_2 = \frac{(\mathfrak{v} X + 3)^2\, (\mathfrak{v}(4\mathfrak{u} - \mathfrak{v} - 9)X + 3\mathfrak{u} - \mathfrak{v})}{\mathfrak{v}\,(4\mathfrak{u} - \mathfrak{v} - 9)(4\mathfrak{v}^2 X^3 + \mathfrak{v}^2 X^2 + 2\mathfrak{v} X + 1)}, \\ V_1 &= Y\, \frac{\mathfrak{v}^2 X^3 - \mathfrak{v} X - 2}{\mathfrak{v}^2 X^3 + \mathfrak{u}\mathfrak{v} X^2 + \mathfrak{v} X + 1}, \\ V_2 &= (27 - \mathfrak{v})^{\frac{3}{2}}\, Y \frac{\mathfrak{v}^2(\mathfrak{v} - 4\mathfrak{u} + 8)X^3 + \mathfrak{v}(\mathfrak{v} - 4\mathfrak{u})X^2 - \mathfrak{v} X + 1}{(4\mathfrak{v}^2 X^3 + \mathfrak{v}^2 X^2 + 2\mathfrak{v} X + 1)^2} \end{aligned} \tag{9}$$

and the elliptic curves have equations:

$$\begin{aligned} \mathcal{E} :\quad & V_1^2 = R\, U_1^3 - (12\mathfrak{u}^2 - 2\mathfrak{u}\mathfrak{v} - 18\mathfrak{v})U_1^2 + (12\mathfrak{u} - \mathfrak{v})U_1 - 4 \\ \mathcal{E}' :\quad & V_2^2 = c_3 U_2^3 + c_2 U_2^2 + c_1 U_2 + c_0 \end{aligned} \tag{10}$$

where

$$\begin{aligned} c_0 &= -(9\mathfrak{u} - 2\mathfrak{v} - 27)^3 \\ c_1 &= (4\mathfrak{u} - \mathfrak{v} - 9)\,(729\mathfrak{u}^2 + 54\mathfrak{u}^2\mathfrak{v} - 972\mathfrak{u}\mathfrak{v} - 18\mathfrak{u}\mathfrak{v}^2 + 189\mathfrak{v}^2 + 729\mathfrak{v} + \mathfrak{v}^3) \\ c_2 &= -\mathfrak{v}\,(4\mathfrak{u} - \mathfrak{v} - 9)^2\,(54\mathfrak{u} + \mathfrak{u}\mathfrak{v} - 27\mathfrak{v}) \\ c_3 &= \mathfrak{v}^2\,(4\mathfrak{u} - \mathfrak{v} - 9)^3 \end{aligned} \tag{11}$$

The above facts can be deduced from Lemma 1 of [17]. The case $4\mathfrak{u} - \mathfrak{v} - 9 = 0$ is treated separately in [17]. There is an automorphism $\beta \in Gal_{k(\mathfrak{u},\mathfrak{v})/k(i_1,i_2,i_3)}$ given by

$$\begin{aligned} \beta(\mathfrak{u}) &= \frac{(\mathfrak{v}-3\mathfrak{u})(324\mathfrak{u}^2+15\mathfrak{u}^2\mathfrak{v}-378\mathfrak{u}\mathfrak{v}-4\mathfrak{u}\mathfrak{v}^2+243\mathfrak{v}+72\mathfrak{v}^2)}{(\mathfrak{v}-27)(4\mathfrak{u}^3+27\mathfrak{v}-18\mathfrak{u}\mathfrak{v}-\mathfrak{u}^2\mathfrak{v}+4\mathfrak{v}^2)} \\ \beta(\mathfrak{v}) &= -\frac{4(\mathfrak{v}-3\mathfrak{u})^3}{4\mathfrak{u}^3+27\mathfrak{v}-18\mathfrak{u}\mathfrak{v}-\mathfrak{u}^2\mathfrak{v}+4\mathfrak{v}^2} \end{aligned} \tag{12}$$

which permutes the j-invariants of $\mathcal{E}$ and $\mathcal{E}'$. The map

$$\theta : (\mathfrak{u}, \mathfrak{v}) \to (i_1, i_2, i_3)$$

defined when $J_2 \neq 0$ and $\Delta \neq 0$ has degree 2. Denote by J_θ the Jacobian matrix of θ. Then $det(J_\theta) = 0$ consist of the (non-singular) curve $\mathfrak{X}$ given by

$$\mathfrak{X}: \quad 8\mathfrak{v}^3 + 27\mathfrak{v}^2 - 54\mathfrak{u}\mathfrak{v}^2 - \mathfrak{u}^2\mathfrak{v}^2 + 108\mathfrak{u}^2\mathfrak{v} + 4\mathfrak{u}^3\mathfrak{v} - 108\mathfrak{u}^3 = 0 \tag{13}$$

and 6 isolated $(\mathfrak{u}, \mathfrak{v})$ solutions. These solutions correspond to the following values for (i_1, i_2, i_3):

$$(-\frac{8019}{20}, -\frac{1240029}{200}, -\frac{531441}{100000}), \ (\frac{729}{2116}, \frac{1240029}{97336}, \frac{531441}{13181630464}), \ (81, -\frac{5103}{25}, -\frac{729}{12500}) \tag{14}$$

We denote the image of $\mathfrak{X}$ in the $\mathcal{L}_3$ locus by $\mathfrak{Y}$. The map θ restricted to $\mathfrak{X}$ is unirational. The curve $\mathfrak{Y}$ can be computed as an affine curve in terms of i_1, i_2. For each point $\mathfrak{p} \in \mathfrak{Y}$ the degree 3 elliptic subcovers are isomorphic. If $\mathfrak{p}$ is an ordinary point in $\mathfrak{Y}$ and $\mathfrak{p} \neq \mathfrak{p}_6$ (cf. Table 1) then the corresponding curve $\mathcal{C}_\mathfrak{p}$ has automorphism group V_4.

If $(\mathcal{C}, \mathcal{E})$ is a degenerate pair then $\mathcal{C}$ can be parameterized as follows

$$Y^2 = (3X^2 + 4)(X^3 + X + c)$$

for some c such that $c^2 \neq -\frac{4}{27}$; see [17]. We define $\mathfrak{w} := c^2$. The map

$$\mathfrak{w} \to (i_1, i_2, i_3)$$

is injective as was shown in [17].

Definition 2. *Let $\mathfrak{p}$ be a point in $\mathcal{L}_3$. We say $\mathfrak{p}$ is a* **generic point** *in $\mathcal{L}_3$ if the corresponding $(\mathcal{C}_\mathfrak{p}, \mathcal{E})$ is a non-degenerate pair. We define*

$$e_3(\mathfrak{p}) := \begin{cases} |\theta^{-1}(\mathfrak{p})|, & if\ \mathfrak{p}\ is\ a\ generic\ point \\ 1 & otherwise \end{cases}$$

In [17] it is shown that the pairs $(\mathfrak{u}, \mathfrak{v})$ with $\Delta(\mathfrak{u}, \mathfrak{v}) \neq 0$ bijectively parameterize the isomorphism classes of non-degenerate pairs $(\mathcal{C}, \mathcal{E})$. Those $\mathfrak{w}$ with $\mathfrak{w} \neq -\frac{4}{27}$ bijectively parameterize the isomorphism classes of degenerate pairs $(\mathcal{C}, \mathcal{E})$. Thus, the number $e_3(\mathfrak{p})$ is the number of isomorphism classes of such pairs $(\mathcal{C}, \mathcal{E})$. In [17] it is shown that $e_3(\mathfrak{p}) = 0, 1, 2$, or 4. The following lemma describes the locus $\mathcal{L}_3$. For details see [17].

Lemma 6. *The locus $\mathcal{L}_3$ of genus 2 curves with degree 3 elliptic subcovers is the closed subvariety of $\mathcal{M}_2$ defined by the equation*

$$C_8 J_{10}^8 + \cdots + C_1 J_{10} + C_0 = 0 \qquad (15)$$

where coefficients $C_0, \ldots, C_8 \in k[J_2, J_6, J_{10}]$ are displayed in [17].

As noted above, with the assumption $J_2 \neq 0$ equation (15) can be written in terms of i_1, i_2, i_3.

4 Automorphism groups of genus 2 curves with degree 3 elliptic subcovers

Let $\mathcal{C} \in \mathcal{L}_3$ be a genus 2 curve defined over an algebraically closed field k, $char(k) = 0$. The following theorem determines the automorphism group of $\mathcal{C}$.

Theorem 1. *Let $\mathcal{C}$ be a genus two curve which has a degree 3 elliptic subcover. Then the automorphism group of $\mathcal{C}$ is one of the following: $\mathbb{Z}_2, V_4$, D_8, or D_{12}. Moreover, there are exactly six curves $\mathcal{C} \in \mathcal{L}_3$ with automorphism group D_8 and six curves $\mathcal{C} \in \mathcal{L}_3$ with automorphism group D_{12}.*

Proof. We denote by $G := Aut(\mathcal{C})$. None of the curves $Y^2 = X^6 - X$, $Y^2 = X^6 - 1$, $Y^2 = X^5 - X$ have degree 3 elliptic subcovers since their J_2, J_4, J_6, J_{10} invariants don't satisfy equation (15). From Lemma 1 we have the following cases:

i) If $G \cong D_8$, then $\mathcal{C}$ is isomorphic to

$$Y^2 = X^5 + X^3 + t\,X$$

as in Lemma 3. Igusa invariants are:

$$J_2 = 40t + 6,\ J_4 = 4t(9 - 20t),\ J_6 = 8t(22t + 9 - 40t^2),\ J_{10} = 16t^3(4t - 1)^2.$$

Substituting into the equation (15) we have the following equation:

$$(196t - 81)^4 (49t - 12)(5t - 1)^4 (700t + 81)^4 (490000\,t^2 - 136200\,t + 2401)^2 = 0 \qquad (16)$$

For

$$t = \frac{81}{196}, \frac{12}{49}, \frac{1}{5}, -\frac{81}{700}$$

the triple (i_1, i_2, i_3) has the following values respectively:

$$(\frac{729}{2116}, \frac{1240029}{97336}, \frac{531441}{13181630464}), \quad (\frac{4288}{1849}, \frac{243712}{79507}, \frac{64}{1323075987}),$$

$$(\frac{144}{49}, \frac{3456}{8575}, \frac{243}{52521875}), \quad (-\frac{8019}{20}, -\frac{1240029}{200}, -\frac{531441}{10000})$$

If

$$490000\,t^2 - 136200\,t + 2401 = 0$$

then we have two distinct triples (i_1, i_2, i_3) which are in $\mathbb{Q}(\sqrt{2})$. Thus, there are exactly 6 genus 2 curves $\mathcal{C} \in \mathcal{L}_3$ with automorphism group D_8 and only four of them have rational invariants.

ii) If $G \cong D_{12}$ then $\mathcal{C}$ is isomorphic to a genus 2 curve in the form

$$Y^2 = X^6 + X^3 + t$$

as in Lemma 3. Then, $J_2 = -6(40t - 1)$ and

$$J_4 = 324t(5t+1), \; J_6 = -162t(740t^2 + 62t - 1), \; J_{10} = -729t^2(4t-1)$$

Then the equation of $\mathcal{L}_3$ becomes:

$$(25t-4)\,(11t+4)^3\,(20t-1)^6\,(111320000t^3 - 60075600t^2 + 13037748t + 15625)^3 = 0 \quad (17)$$

For

$$t = \frac{4}{25}, -\frac{4}{11}, \frac{1}{20}$$

the corresponding values for (i_1, i_2, i_3) are respectively:

$$(\frac{64}{5}, \frac{1088}{25}, \frac{1}{84375}), \quad (\frac{576}{361}, \frac{60480}{6859}, \frac{243}{2476099}), \quad (81, -\frac{5103}{25}, -\frac{729}{12500})$$

If

$$111320000t^3 - 60075600t^2 + 13037748t + 15625 = 0$$

then there are three distinct triples (i_1, i_2, i_3) none of which is rational. Hence, there are exactly 6 classes of genus 2 curves $\mathcal{C} \in \mathcal{L}_3$ with $Aut(\mathcal{C}) \cong D_{12}$ of which three have rational invariants.

iii) $G \cong V_4$. There is a 1-dimensional family of genus 2 curves with a degree 3 elliptic subcover and automorphism group V_4 given by $\mathfrak{Y}$.

iv) Generically genus 2 curves $\mathcal{C}$ have $Aut(\mathcal{C}) \cong \mathbb{Z}_2$. For example, every point $\mathfrak{p} \in \mathcal{L}_3 \backslash \mathcal{L}_2$ correspond to a class of genus 2 curves with degree 3 elliptic subcovers and automorphism group isomorphic to $\mathbb{Z}_2$. This completes the proof.

□

The theorem determines that there are exactly 12 genus 2 curves $\mathcal{C} \in \mathcal{L}_3$ with automorphism group D_8 or D_{12}. Only seven of them have rational invariants. From Lemma 4, we have the following:

Corollary 1. *There are exactly four (resp., three) genus 2 curves $\mathcal{C}$ defined over $\mathbb{Q}$ (up to $\bar{\mathbb{Q}}$-isomorphism) with a degree 3 elliptic subcover which have automorphism group D_8 (resp., D_{12}). They are listed in Table 1.*

Remark 4. All points $\mathfrak{p}$ in Table 1 are in the locus $det(J_\theta) = 0$. We have already seen cases $\mathfrak{p}_1, \mathfrak{p}_4$, and $\mathfrak{p}_7$ as the exceptional points of $det(J_\theta) = 0$; see equation (14). The class $\mathfrak{p}_3$ is a singular point of order 2 of $\mathfrak{Y}$, $\mathfrak{p}_2$ is the only point which belong to the degenerate case, and $\mathfrak{p}_6$ is the only ordinary point in $\mathfrak{Y}$ such that the order of $Aut(\mathfrak{p})$ is greater then 4.

	$\mathcal{C}$	$\mathfrak{p} = (i_1, i_2, i_3)$	$e_3(\mathfrak{p})$	$Aut(\mathcal{C})$
$\mathfrak{p}_1$	$196X^5 + 196X^3 + 81X$	$i_1 = \frac{729}{2116}, i_2 = \frac{1240029}{97336}, i_3 = \frac{531441}{13181630464}$	2	D_8
$\mathfrak{p}_2$	$49X^5 + 49X^3 + 12X$	$i_1 = \frac{4288}{1849}, i_2 = \frac{243712}{79507}, i_3 = \frac{64}{1323075987}$	1	D_8
$\mathfrak{p}_3$	$5X^5 + 5X^3 + X$	$i_1 = \frac{144}{49}, i_2 = \frac{3456}{8575}, i_3 = \frac{243}{52521875}$	2	D_8
$\mathfrak{p}_4$	$700X^5 + 700X^3 - 81X$	$i_1 = -\frac{8019}{20}, i_2 = -\frac{1240029}{200}, i_3 = -\frac{531441}{10000}$	2	D_8
$\mathfrak{p}_5$	$25X^6 + 25X^3 + 4$	$i_1 = \frac{64}{5}, i_2 = -\frac{1088}{25}, i_3 = -\frac{1}{84375}$	1	D_{12}
$\mathfrak{p}_6$	$11X^6 + 11X^3 - 4$	$i_1 = \frac{576}{361}, i_2 = \frac{60480}{6859}, i_3 = \frac{243}{2476099}$	1	D_{12}
$\mathfrak{p}_7$	$20X^6 + 20X^3 + 1$	$i_1 = 81, i_2 = -\frac{5103}{25}, i_3 = -\frac{729}{12500}$	2	D_{12}

Table 1. Rational points $\mathfrak{p} \in \mathcal{L}_3$ with $|Aut(\mathfrak{p})| > 4$

5 Computing elliptic subcovers

Next we will consider all points $\mathfrak{p}$ in Table 1 and compute j-invariants of their degree 2 and 3 elliptic subcovers. To compute j-invariants of degree 2 elliptic subcovers we use lemma 5 and the values of t from the proof of theorem 1. We recall that for $\mathfrak{p}_1, \dots, \mathfrak{p}_4$ there are four degree 2 elliptic subcovers which are two and two isomorphic. We list the j-invariant of each isomorphic class. They are 2-isogenous as mentioned before. For $\mathfrak{p}_5, \mathfrak{p}_6, \mathfrak{p}_7$ there are two degree 2 elliptic subcovers which are 3-isogenous to each other. To compute degree 3 elliptic subcovers for each $\mathfrak{p}$ we find the pairs $(\mathfrak{u}, \mathfrak{v})$ in the fiber $\theta^{-1}(\mathfrak{p})$ and then use equations (9). We focus on cases which have elliptic subcovers defined over $\mathbb{Q}$. There are techniques for computing rational points of genus two curves which have degree 2 subcovers defined over $\mathbb{Q}$ as in Flynn and Wetherell [5]. Sometimes the degree 3 elliptic subcovers are defined over $\mathbb{Q}$ even though the degree 2 elliptic subcovers are not; see Examples 2 and 6. These degree 3 subcovers help determine rational points of genus 2 curves as illustrated in examples 2, 4, 5, and 6.

Example 1. $\mathfrak{p} = \mathfrak{p}_1$: The j-invariants of degree 3 elliptic subcovers are $j = j' = 66^3$. A genus 2 curve $\mathcal{C}$ corresponding to $\mathfrak{p}$ is

$$\mathcal{C}: \ Y^2 = X^6 + 3X^4 - 6X^2 - 8.$$

Claim: The equation above has no rational affine solutions.

Indeed, two of the degree 2 elliptic subcovers (isomorphic to each other) have equations

$$\mathcal{E}_1: \ Y^2 = x^3 + 3x^2 - 6x - 8$$
$$\mathcal{E}_2: \ Y^2 = -8x^3 - 6x^2 + 3x + 1$$

where $x = X^2$ (i.e. $\phi : \mathcal{C} \to \mathcal{E}_1$ of degree 2 such that $\phi(X, Y) = (X^2, Y)$). The elliptic curve $\mathcal{E}_1$ has rank 0. Thus, the rational points of $\mathcal{C}$ are the preimages of the torsion points of $\mathcal{E}_1$. The torsion group of $\mathcal{E}_1$ has order 4 and is given by

$$Tor(\mathcal{E}_1) = \{\infty, (-1, 0), (2, 0), (-4, 0)\}$$

None of the preimages is rational. Thus, $\mathcal{C}$ has no rational points except the point at infinity.

Example 2. $\mathfrak{p} = \mathfrak{p}_2$: The j-invariants of the degree 2 elliptic subcovers are

$$76771008 \pm 44330496\sqrt{3}.$$

The point $\mathfrak{p}_2$ belongs to the degenerate locus with $\mathfrak{w} = 0$. Thus, the equation of the genus 2 curve $\mathcal{C}$ corresponding to $\mathfrak{p}$ is

$$\mathcal{C}: \quad Y^2 = (3\,X^2 + 4)\,(X^3 + X).$$

Indeed, this curve has both pairs $(\mathcal{C}, \mathcal{E})$ and $(\mathcal{C}, \mathcal{E}')$ as degenerate pairs. It is the only such genus 2 curve defined over $\mathbb{Q}$. This fact was noted in [12] and [16]. Both authors failed to identify the automorphism group. The degree 3 coverings are

$$(U_1, V_1) = (X^3 + X, Y(3X^2 + 1)), \quad (U_2, V_2) = (\frac{X^3}{3X^2 + 4}, Y X^2\, [\frac{X^2 + 4}{(3X^2 + 4)^2}]^2)$$

and the elliptic curves have equations:

$$\mathcal{E}: \; V_1^2 = 27U_1^3 + 4U_1, \quad \textit{and} \quad \mathcal{E}': \; V_2^2 = U_2^3 + U_2.$$

$\mathcal{E}$ and $\mathcal{E}'$ are isomorphic with j-invariant 1728. They have rank 0 and rational torsion group of order 2, $Tor(\mathcal{E}) = \{\infty, (0, 0)\}$. Thus, the only rational points of $\mathcal{C}$ are in the fibers $\phi_1^{-1}(0)$ and $\phi_2^{-1}(\infty)$. Hence, $\mathcal{C}(\mathbb{Q}) = \{(0, 0), \infty\}$.

Example 3. $\mathfrak{p} = \mathfrak{p}_3$: All degree 2 and 3 elliptic subcovers are defined over $\mathbb{Q}(\sqrt{5})$.

Example 4. $\mathfrak{p} = \mathfrak{p}_4$: The degree 2 elliptic subcovers have j-invariants

$$\frac{1728000}{2809} \pm \frac{17496000}{2809}\sqrt{I}$$

where $I^2 = -1$. Thus, we can't recover any information from the degree 2 subcovers. One corresponding value for $(\mathfrak{u}, \mathfrak{v})$ is $(\frac{25}{2}, \frac{250}{9})$. Then $\mathcal{C}$ is

$$\mathcal{C}: \quad 3^8 \cdot Y^2 = (100X + 9)(2500X^2 + 400X + 9)\,(25X + 9)(2500X^2 + 225X + 9).$$

The degree 3 elliptic subcovers have equations

$$\begin{aligned} \mathcal{E}: \quad & V_1^2 = -\frac{1}{81}(10U_1 - 3)(8575U_1^2 - 2940U_1 + 108) \\ \mathcal{E}': \quad & V_2^2 = -\frac{686}{59049}\,(1700U_2 - 441)(1445000U_2^2 - 696150U_2 + 83853) \end{aligned} \tag{18}$$

where U_1, V_1, U_2, V_2 are given by formulas in (9).

Example 5. $\mathfrak{p} = \mathfrak{p}_5$: The degree 2 j-invariants are $j_1 = 0$ and $j_2 = -1228800$ and the degree 3 j-invariants as shown below are $j = j' = 0$. Let $\mathcal{C}$ be the genus 2 curve with equation

$$\mathcal{C}: \quad Y^2 = (X^3+1)(4X^3+1)$$

corresponding to $\mathfrak{p}$. The case is treated separately in [17]. The degree 3 elliptic subcovers have equations

$$\mathcal{E}: \ V_1^2 = -27U_1^3 + 4, \quad \mathcal{E}': \ V_2^2 = -16(27U_2^3 - 1)$$

where

$$(U_1, V_1) = (\frac{X^2}{X^3+1}, Y\frac{X^3-2}{(X+1)^2}), \quad (U_2, V_2) = (\frac{X}{4X^3+1}, Y\frac{8X^3-1}{(4X^3+1)^2}).$$

The rank of both $\mathcal{E}$ and $\mathcal{E}'$ is zero. Thus, the rational points of $\mathcal{C}$ are the preimages of the rational torsion points of $\mathcal{E}$ and $\mathcal{E}'$. The torsion points of $\mathcal{E}$ are $Tor(\mathcal{E}) = \{\infty, (0,2), (0,-2)\}$. Then $\phi_1^{-1}(0) = \{0, \infty\}$ and $\phi_1^{-1}(\infty) = \{-1, \frac{1}{2} \pm \frac{\sqrt{-3}}{2}\}$. Thus,

$$\mathcal{C}(\mathbb{Q}) = \{(0,1), (0,-1), (-1,0)\}$$

Example 6. $\mathfrak{p} = \mathfrak{p}_6$: This point is in $\mathfrak{Y}$ and it is not a singular point of $\mathfrak{Y}$. It has isomorphic degree 3 elliptic subcovers; see [17]. The corresponding $(\mathfrak{u}, \mathfrak{v})$ pair is $(\mathfrak{u}, \mathfrak{v}) = (20, 16)$ and $e_3(\mathfrak{p}) = 1$. Then the genus 2 curve has equation:

$$\mathcal{C}: \quad Y^2 = (256X^3 + 320X^2 + 16X + 1)\,(1024X^3 + 256X^2 + 32X + 1)$$

The degree 3 elliptic subcovers have j-invariants $j = j' = -32768$ and equations

$$\begin{aligned} \mathcal{E}: &\quad V_1^2 = 4(-5324U_1^3 + 968U_1^2 - 56U_1^2 + 1) \\ \mathcal{E}': &\quad V_2^2 = 11^3(-32000\,U_2^3 + 35200\,U_2^2 - 12320\,U_2 + 11^3) \end{aligned} \tag{19}$$

where U_1, V_1, U_2, V_2 are given by formulas in (9).

Both elliptic curves have trivial torsion but rank $r = 1$. One can try to adapt more sophisticated techniques in this case as Flynn and Wetherell have done for the degree 2 subcovers. This is the only genus 2 curve (up to $\mathbb{C}$-isomorphism) with automorphism group D_{12} and isomorphic degree 2 elliptic subcovers. Indeed all the degree 2 and 3 elliptic subcovers are $\mathbb{C}$-isomorphic with j-invariants $j = -32768$. The degree 2 elliptic subcovers also have rank 1 which does not provide any quick information about rational points of $\mathcal{C}$.

Example 7. $\mathfrak{p} = \mathfrak{p}_7$: All the degree 2 and 3 elliptic subcovers are defined over $\mathbb{Q}(\sqrt{5})$.

Throughout this paper we have made use of several computer algebra packages as Apecs, Maple, and GAP. The interested reader can check [18] and [17] for more details on loci $\mathcal{L}_2$ and $\mathcal{L}_3$. The equations for these spaces, j-invariants of elliptic subcovers of the degree 2 and 3, and other computational aspects of genus 2 curves can be downloaded from author's web site.

References

1. O. Bolza, On binary sextics with linear transformations into themselves. *Amer. J. Math.* **10**, 47-70.
2. J. W. S. Cassels and E. V. Flynn, Prolegomena to a Middlebrow Arithmetic of Curves of Genus Two, LMS, 230, 1996.
3. A. Clebsch, Theorie der Binären Algebraischen Formen, Verlag von B.G. Teubner, Leipzig, (1872).
4. T. Ekedahl and J. P. Serre, Exemples de courbes algébriques á jacobienne complétement décomposable. *C. R. Acad. Sci. Paris Sr. I Math.*, 317 (1993), no. 5, 509–513.
5. E. V. Flynn and J. Wetherell, Finding rational points on bielliptic genus 2 curves, *Manuscripta Math.* 100, 519-533 (1999).
6. G. Frey, On elliptic curves with isomorphic torsion structures and corresponding curves of genus 2. *Elliptic curves, modular forms, and Fermat's last theorem (Hong Kong, 1993)*, 79-98, Ser. Number Theory, I, *Internat. Press, Cambridge, MA*, (1995).
7. G. Frey and E. Kani, Curves of genus 2 covering elliptic curves and an arithmetic application. *Arithmetic algebraic geometry (Texel, 1989)*, 153-176, *Progr. Math.*, 89, *Birkhäuser Boston, Boston, MA, (1991).*
8. E. Howe, F. Leprévost, and B. Poonen, Large torsion subgroups of split Jacobians of curves of genus two or three. *Forum. Math*, **12** (2000), no. 3, 315-364.
9. J. Igusa, Arithmetic Variety of Moduli for genus 2. *Ann. of Math.* (2), 72, 612-649, (1960).
10. W. Keller, L. Kulesz, Courbes algbriques de genre 2 et 3 possdant de nombreux points rationnels. C. R. Acad. Sci. Paris Sr. I Math. 321 (1995), no. 11, 1469–1472.
11. A. Krazer, Lehrbuch der Thetafunctionen, Chelsea, New York, (1970).
12. M. R. Kuhn, Curves of genus 2 with split Jacobian. *Trans. Amer. Math. Soc* **307** (1988), 41-49
13. K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein, The locus of curves with prescribed automorphism group, *RIMS Kyoto Technical Report Series*, Communications in Arithmetic Fundamental Groups and Galois Theory, 2001, edited by H. Nakamura.
14. P. Mestre, Construction de courbes de genre 2 á partir de leurs modules. In T. Mora and C. Traverso, editors, *Effective methods in algebraic geometry*, volume 94. *Prog. Math.* , 313-334. Birkhäuser, 1991. Proc. Congress in Livorno, Italy, April 17-21, (1990).
15. D. Mumford, The Red Book of Varieties and Schemes, Springer, 1999.
16. T. Shaska, Genus 2 curves with (n,n)-decomposable Jacobians, *Jour. Symb. Comp.*, Vol 31, **no. 5**, pg. 603-617, 2001.
17. T. Shaska, Genus 2 fields with degree 3 elliptic subfields, (submited for publication).
18. T. Shaska and H. Völklein, Elliptic Subfields and automorphisms of genus 2 function fields. *Proceeding of the Conference on Algebra and Algebraic Geometry with Applications: The celebration of the seventieth birthday of Professor S.S. Abhyankar*, Springer-Verlag, 2001.