INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

ProQuest Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600

CURVES OF GENUS TWO COVERING ELLIPTIC CURVES

By

TANUSH SHASKA

A DISSERTATION PRESENTED TO THE GRADUATE SCHOOL
OF THE UNIVERSITY OF FLORIDA IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

UNIVERSITY OF FLORIDA

2001

UMI Number: 3009967

UMI Microform 3009967

Bell & Howell Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

To my parents,

and all the others who suffered the injustices

of the communist regimes, in Albania and elsewhere.

ACKNOWLEDGEMENTS

It is a pleasure to thank my thesis advisor, Helmut Voelklein, for patiently guiding my intellectual development in innumerable ways. In addition, John Thompson, Gerhard Frey and Mike Fried generously shared their ideas in many occasions.

I wish to thank the Department of Mathematics at the University of Florida for providing me with financial support for most of the period that this thesis was written, Karl Strambach and the Department of Mathematics at the University of Erlangen for their financial support and hospitality during the year 2000, and the College of Liberal Arts and Sciences at the University of Florida for the Threadgill Dissertation Fellowship during my final semester.

Finally, I would like to thank my family for their continuous support during my graduate studies.

TABLE OF CONTENTS

Abstract of Dissertation Presented to the Graduate School
of the University of Florida in Partial Fulfillment of the
Requirements for the Degree of Doctor of Philosophy

CURVES OF GENUS TWO COVERING ELLIPTIC CURVES

By

Tanush Shaska

May 2001

Chairman: Dr. Helmut Voelklein
Major Department: Mathematics

Let $\mathcal{L}_n$ be the locus of genus 2 curves that have a degree n maximal covering to an elliptic curve. There are several general results on the spaces $\mathcal{L}_n$ in the literature. In particular Frey and Kani have identified $\mathcal{L}_n$ with a "modular diagonal quotient surface." These general results rely on the Jacobian variety of a genus 2 curve and are therefore not constructive.

In this dissertation, explicit equations for $\mathcal{L}_n$, $n = 2, 3$ and for some interesting subvarieties of $\mathcal{L}_5$ and $\mathcal{L}_7$, are found by using computer algebra systems. This yields more information than the abstract approach. The case $n = 2$ has already been studied by Jacobi and Legendre, and recently by Gaudry, Schost, Geyer and others. Among other things, we find the following new result for $n = 2$: An explicit 1-dimensional family of genus 2 curves each having exactly 2 isomorphic elliptic subcovers of degree 2. This family is parameterized birationally by the j-invariants of these elliptic subcovers.

For $n = 3$ we show that the number of elliptic subfields is generically 2. There are sporadic cases with 4 or 8 elliptic subfields. For a curve $\mathcal{C} \in \mathcal{L}_3$ its automorphism group $Aut(\mathcal{C})$ is one of the following, $\mathbb{Z}_2, V_4, D_4, D_6$. Moreover, there are exactly 6 curves in $\mathcal{L}_3$ with automorphism group D_4 or D_6.

CHAPTER 1
INTRODUCTION

Let $\mathcal{C}$ be a genus 2 curve defined over an algebraically closed field k of $char(k) \neq 2$. Let K be its function field. We study genus 1 subfields of K (which we call elliptic subfields). More precisely, we are interested in the following invariant $\epsilon_n(\mathcal{C}) := \epsilon_n(K)$: The number of orbits of $Aut(K)$ on the set of elliptic subfields of K of degree n. We denote by $\mathcal{L}_n$ the locus of genus 2 fields with $\epsilon_n(K) \geq 1$. We use the classical invariants J_i, $i = 1, 2, 3, 5$ to describe $\mathcal{L}_n$ as a surface in the 3-dimensional moduli space $\mathcal{M}_2$ of genus 2 curves.

In chapter two we determine the automorphism group $Aut(\mathcal{C}) \cong Aut(K)$. This unifies and extends many partial treatments in the literature. The group $Aut(K)$ has exactly one involution whose fixed field has genus 0. The other involutions have fixed field of genus 1, we call them elliptic involutions. Thus, $\epsilon_2(K)$ is the number of conjugacy classes of elliptic involutions. It is shown that $\epsilon_2(K) = 1$ if and only if $\mathcal{C}$ is isomorphic to $Y^2 = X^5 - X$, otherwise $\epsilon_2(K) = 0$ or 2.

In chapters 3-6 we assume that $char(k) = 0$. In chapter three, we parameterize $\mathcal{L}_2$ and compute an equation in terms of the classical invariants. The latter was done by Gaudry and Schost by another method. We determine the j-invariants of elliptic subfields in terms of the classical invariants. In special cases these elliptic subfields are isogenous of degree 2 or 3. These cases are noted in the remarks. We find a 1-dimensional family of genus 2 curves having exactly two isomorphic elliptic subfields of degree 2: this family is parameterized by the j-invariant of these subfields. This leads to a remarkable embedding of the moduli space $\mathcal{M}_1$ of genus one curves into $\mathcal{M}_2$.

In chapter four we collect some results on $c_n(K)$ for arbitrary n. These results are mostly due to Frey and Kani. This leads us to the definition of the Frey-Kani coverings and their ramifications. Let $\varphi_1 : \mathcal{C} \longrightarrow E_1$ be a covering of degree n from a curve $\mathcal{C}$ of genus 2 to the elliptic curve E_1. Denote by $\pi_{\mathcal{C}} : \mathcal{C} \longrightarrow \mathbb{P}^1$ (resp. $\pi_1 : E_1 \longrightarrow \mathbb{P}^1$) the hyperelliptic projection of $\mathcal{C}$ (resp. E_1). There is a degree n covering $\phi_1 : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ such that $\phi_1 \circ \pi_{\mathcal{C}} = \pi_1 \circ \varphi_1$, (cf. chapter 4). This covering $\phi_1 : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ is called the corresponding *Frey-Kani covering* of $\varphi_1 : \mathcal{C} \longrightarrow E_1$. We determine all possible ramifications of the Frey-Kani coverings of degree n. If the cover $\varphi_1 : \mathcal{C} \longrightarrow E_1$ is maximal there is a unique elliptic subcover E_2 of $\mathcal{C}$ such that the corresponding cover $\varphi_2 : \mathcal{C} \longrightarrow E_2$ is maximal and of degree n. The Jacobian of $\mathcal{C}$ is isogenous to $E_1 \times E_2$.

In the remaining chapters we study cases $n = 3, 5$ or 7. We parameterize and determine the equation for the locus $\mathcal{L}_3$. We show that in $\mathcal{L}_3$ we have generically $c_3 = 2$; there are sporadic cases when $c_3 = 4, 8$ and a 1-dimensional family with $c_3 = 1$. The automorphism group of a curve $\mathcal{C}$ in $\mathcal{L}_3$ is one of the following $\mathbb{Z}_2, V_4, D_4, D_6$. In $\mathcal{L}_3$ there are exactly 6 curves $\mathcal{C}$ with automorphism group D_4 and 6 with automorphism group D_6. Their absolute invariants are computed explicitly and displayed in chapter 5. We determine the j-invariants of elliptic subfields. When one of the elliptic subfields is totally ramified we determine the relation between the j-invariants of the elliptic subfields. Cases when $n = 5$ or 7 are discussed briefly in chapter 6. Since the computations are much harder and results very large for display we treat only cases when the Frey-Kani covering has a branch point of ramification index 4. The j-invariants of the elliptic subfield are computed in both cases.

Curves of genus 2 with elliptic subcovers go back to Legendre and Jacobi. Legendre, in his *Théorie des fonctions elliptiques*, gave the first example of a genus 2 curve with degree 2 elliptic subcovers. In a review of Legendre's work, Jacobi (1832) gives a complete description for $n = 2$. The case $n = 3$ was studied during the 19th

century from Hermite, Goursat, Burkhardt, Brioschi, and Bolza. For a history and background of the 19th century work see Krazer [11] (pg. 479). Also Kuhn (1988) gives a brief description of the case $n = 3$. Cases when $n > 3$ are more difficult to handle. Frey and Kani note the difficulty to get explicit examples, see Frey [5] and Frey, Kani [6].

1.1 Classical Invariants

Recall that every homogeneous polynomial of two variables $f(X, Z)$ over an algebraically closed field k decomposes as

$$f(X, Z) = \prod (X\alpha_i - Z\beta_i)$$

The projective points (β_i, α_i) in $\mathbb{P}^1$ depend only on f and are called roots of f. Let

$$f(X, Z) = a_6X^6 + a_5X^5Z + a_4X^4Z^2 + a_3X^3Z^3 + a_2X^2Z^4 + a_1XZ^5 + a_0Z^6$$

be a nonzero sextic. Classical invariants of $f(X, Z)$ are the following homogeneous polynomials in $k[a_0, \ldots, a_6]$ of degree $2i$, for $i = 1, 2, 3, 5$.

$$\begin{aligned}
J_2 :=& -240a_0a_6 + 40a_1a_5 - 16a_2a_4 + 6a_3^2 \\
J_4 :=& 48a_0a_4^2 + 48a_1^2a_6 + 4a_2^2a_4^2 + 1620a_0^2a_6^2 + 36a_1a_3^2a_5 - 12a_1a_2a_4^2 - 12a_2^2a_3a_5 + 300a_1^2a_4a_6 \\
&+ 300a_0a_3^2a_2 + 324a_0a_5^2a_3^2 - 504a_0a_4a_2a_6 - 180a_0a_4a_3a_5 - 180a_1a_3a_2a_6 + 44a_1a_4a_2a_5 \\
&- 540a_0a_5a_1a_6 - 80a_2^2a_6^2 \\
J_6 :=& -a_2^3a_4^3 - 1600a_0^3a_6^3 + 1600a_0a_4^3a_6^2 - 2240a_0^2a_2^2a_6^2 + 20664a_0^2a_4^2a_6^2 - 198a_0a_4^4a_6 \\
&- 640a_0a_4^2a_2^3a_6^2 - 18600a_0a_4^2a_3^2a_6^2 + 76a_1a_4^3a_2a_4 - 198a_1a_4^3a_3a_5 + 264a_1a_4a_2^2a_6^2 + 330a_1^2a_3^2a_6a_4 \\
&+ 616a_2^3a_5a_1a_6 + 28a_1a_4^2a_2^2a_5 - 640a_1^2a_4^2a_2a_6 + 264a_1^2a_2^2a_4a_5 + 616a_1a_4^3a_0a_5 - 18600a_0^2a_2^2a_6a_4 \\
&+ 59940a_0^2a_5^2a_2^2a_1 + 330a_0a_2^2a_3^2a_4^2 + 8a_2^2a_4^3a_4^2 - 24a_2^2a_4^2a_5 + 60a_2^3a_3^2a_6 - 24a_1a_2^3a_4^3 + 72a_1a_3^4a_5 \\
&+ 60a_0a_4^3a_2^2 - 192a_2^3a_0a_6^2 - 320a_2^4a_4a_6 + 176a_1^2a_2^2a_3^2 + 2250a_1^2a_2a_6^2 - 900a_2^2a_4^2a_6^2 + 2250a_0^2a_2^2a_4^2 \\
&- 900a_0^2a_2^2a_4^2 - 10044a_0^2a_5^2a_3^2 + 162a_0a_6a_4^3 - 24a_2^3a_4^3 - 36a_2^4a_5^2 - 36a_2^2a_4^4 + 76a_2^3a - 119880a_0^2a_6^2 \\
&- 320a_1^2a_4^3 + 484a + 492a_0a_4^2a_2a_4a_5 + 3060a_0^2a_4a_6a_4a_5 - 468a_0a_4a_3^2a_2a_6 - 1860a_1a_4a_0a_3^2a_5 \\
&+ 3472a_0a_4a_2a_5a_1a_6 - 876a_0a_4^2a_1a_6a_5 + 492a_1a_3a_2^2a_4a_6 - 238a_1a_3^2a_2a_4a_5 + 3060a_1a_3a_0a_5^2a_2 \\
&+ 1818a_1a_3^2a_0a_6a_5 - 1860a_1^2a_3a_2a_5a_6 - 876a_1^2a_0a_6a_4a_5 - 3a_5 \\
J_{10} :=& R_X\left(f, \frac{\partial f}{\partial X}\right)
\end{aligned} \tag{1.1}$$

Thus, J_{10} is the resultant with respect to X of f and $\frac{\partial f}{\partial X}$ which is usually called the discriminant of f. It vanishes if and only if the binary sextic has a multiple root. J_{2i}, $i = 1, 2, 3, 5$, are invariant under the natural action of $SL_2(k)$ on sextics. Dividing

such an invariant by another of the same degree gives a rational function. invariant under $GL_2(k)$ action.

Each genus 2 curve $\mathcal{C}$ is isomorphic to

$$Z^4Y^2 = f(X,Z)$$

where $f(X,Z)$ is a binary sextic with $J_{10} \neq 0$. Its function field is of the form $k(X,Y)$ where

$$Y^2 = f(X,1).$$

If I is an $GL_2(k)$ invariant as defined above, then I takes the same values on all sextics $f(X,Z)$ defining $\mathcal{C}$. So $I(\mathcal{C})$ is well defined. We also denote it by $I(K)$. If $J \in k[a_0,\ldots,a_6]$ is a homogeneous $SL_2(k)$ invariant the the condition $J(K) = 0$ is well defined.

Particular $GL_2(k)$ invariants are

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

It is a classical result of Clebsch and Bolza extended by Igusa to positive characteristic that two sextics f and f' are conjugate under $GL_2(k)$ if and only if there is $r \neq 0$ such that

$$J_{2i}(f) = r^{2i}J_{2i}(f'), \quad for \quad i = 1,2,3,5$$

If $J_2 = 0$, then this holds if and only if

$$i_\mu(f) = i_\mu(f'), \quad for \quad \mu = 1,2,3$$

CHAPTER 2
THE AUTOMORPHISM GROUP OF A GENUS TWO FIELD

In this chapter, we determine the automorphism group of a genus 2 curve, see theorem 1.3. This was also treated by Geyer [18] (with proofs only sketched) and Brandt and Stichtenoth [2] (in characteristic 0 only), and Brandt in a more general set-up, (see Brandt [3], unpublished thesis).

2.1 Automorphism Groups of Genus 2 Fields

Let k be an algebraically closed field of characteristic not equal to 2. Let $k(X)$ be the field of rational functions in X. We identify the places of $k(X)$ with the points of $\mathbb{P}^1 = k \cup \{\infty\}$ in the natural way (the place $X = \alpha$ gets identified with the point $\alpha \in \mathbb{P}^1$). Let K a quadratic extension field of $k(X)$ ramified exactly at six places $\alpha_1, \ldots, \alpha_6$ of $k(X)$. The corresponding places of K are called the Weierstrass points K. Let $P := \{\alpha_1, \ldots, \alpha_6\}$. Then $K = k(X, Y)$, where

$$Y^2 = \prod_{\substack{\alpha \in P \\ \alpha \neq \infty}} (X - \alpha) \tag{2.1}$$

Let $G = Aut(K/k)$. It is well known that $k(X)$ is the only genus 0 subfield of degree 2 of K: thus G fixes $k(X)$. Thus, $G_0 := Gal(K/k(X)) = \langle z_0 \rangle$, with $z_0^2 = 1$, is central in G. We call *the reduced automorphism group* of K the group $\bar{G} := G/G_0$. Then, $\bar{G}$ is naturally isomorphic to the subgroup of $Aut(k(X)/k)$ induced by G. We have

$$\Gamma := PGL_2(k) \xrightarrow{\cong} Aut(k(X)/k) \tag{2.2}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\bullet} \longrightarrow \left(X \to \frac{aX + c}{bX + d} \right)$$

The action of Γ on the places of $k(X)$ corresponds under the above identification to the usual action on $\mathbb{P}^1$ by fractional linear transformations: $t \mapsto \frac{at+b}{ct+d}$. If l is prime to $char(k)$ then each element of order l of Γ is conjugate to $\begin{pmatrix} \xi_l & 0 \\ 0 & 1 \end{pmatrix}$, where ξ_l is a primitive l-th root of unity. Each such element has 2 fixed points on $\mathbb{P}^1$ and other orbits are of length l. If $l = char(k)$ then, Γ has exactly one class of elements of order l, represented by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Each such element has exactly one fixed point on $\mathbb{P}^1$.

Further, G permutes $a_1, \ldots, a_6$. This yields an embedding $G \hookrightarrow S_6$.

Lemma 2.1. *Let $\tau \in G$ and $\bar{g}$ its image in G.*

a) Suppose $\bar{g}$ is an involution. Then τ has order 2 if and only if it fixes no Weierstrass points.

b) If $\bar{g}$ has order 4, then τ has order 8.

Proof. a) Suppose g is an involution. By the above we may assume $g(X) = -X$. We may further assume that $1 \in \mathcal{P}$ by replacing X by cX for a suitable $c \in k^*$.

Now assume g fixes no points in $\mathcal{P}$. Thus, $\mathcal{P} = \{1, -1, b, -b, a, -a\}$, where $a, b \in \mathbb{P}^1 \setminus \{0, \infty, \pm 1\}$. Hence

$$Y^2 = (X^2 - 1)(X^2 - a^2)(X^2 - b^2)$$

So we have, $\tau(Y)^2 = Y^2$. Hence $\tau(Y) = \pm Y$, and τ has order 2.

Suppose g fixes 2 points of $\mathcal{P}$. Then, $\mathcal{P} = \{0, \infty, 1, -1, a, -a\}$, where $a \in \mathbb{P}^1 \setminus \{0, \infty, \pm 1\}$. Hence

$$Y^2 = X(X^2 - 1)(X^2 - a^2)$$

So $\tau(Y)^2 = -Y^2$ and $\tau(Y) = \sqrt{-1}\, Y$. Hence, τ has order 4.

b) Each element of $PGL_2(k)$ of order 4 acts on $\mathbb{P}^1$ with two fixed points and all other orbits of length 4. So if $\bar{g}$ has order 4, then it fixes 2 points in $\mathcal{P}$. Thus g^2 has order 4, from lemma 2.1 a). Then, τ has order 8.

□

Because K is the unique degree 2 extension of $k(X)$ ramified exactly at $\alpha_1, \ldots, \alpha_6$, each automorphism of $k(X)$ permuting these 6 places extends to an automorphism of K. Thus, $\bar{G}$ is the stabilizer in $Aut(k(x)/k)$ of the set $\mathcal{P}$. Hence under the isomorphism (2.2), $\bar{G}$ corresponds to the stabilizer $\Gamma_{\mathcal{P}}$ in Γ of the 6-set $\mathcal{P}$. In the following list for each $\Gamma_{\mathcal{P}}$ we display some information on the corresponding genus 2 field, in particular its automorphism group G.

First, we fix some notation. By D_N we will denote the dihedral group of order $2N$. V_4 is the Klein 4-group and Q_8 is the quaternion group of order 8. Let $\pi : G \to \bar{G}$ be the canonical map.

Remark 2.2. If a finite subgroup H of Γ with $(|H|, char(k)) = 1$, fixes a point of $\mathbb{P}^1$ then H is cyclic.

Proof. If H fixes a point then H is conjugate to $A := \{\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}^{\bullet} : b \in k^*, a \in k\}$. Thus we may assume that $H \leq A$. Let $B := \{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^{\bullet} : a \in k\}$. Then $H \cap B = 1$. Therefore H embeds into $A/B \cong k^*$. Hence H is cyclic. □

Remark 2.3. The degree 2 central extensions of S_4.

Since $H^2(S_4, C_2) = 1$ (see Stichtenoth [2]) there are exactly 4 non-equivalent central extensions of degree 2 of S_4. We construct them as follows. Let W be the group of 4×4 matrices over $\mathbb{F}_3$ generated by

$$S' = \begin{pmatrix} S & 0 \\ 0 & I \end{pmatrix}, \quad T' = \begin{pmatrix} T & 0 \\ 0 & U \end{pmatrix}$$

where $S, T, U \in GL_2(3)$ and $GL_2(3) = \langle S, T \rangle$ such that $S^3 = 1, T^2 = 1, U^4 = 1$. Then, W is a central extension of S_4 with kernel a Klein 4-group $V_4 = \{1, v_1, v_2, v_3\}$, where

$$v_1 = \begin{pmatrix} I & 0 \\ 0 & -I \end{pmatrix}, \quad v_2 = \begin{pmatrix} -I & 0 \\ 0 & I \end{pmatrix}, \quad v_3 = v_1 v_2.$$

Let $W_i := W(r,s)$, for $i = 1,2,3$. Then W_1, W_2, W_3, and the split extension comprise all the degree 2 central extensions of $S_4 \cong PGL_2(3)$. W_2 has no elements of order 8 and W_3 has only one involution which is the central involution.

1. $\Gamma_{\mathcal{P}}$ *acts transitively on* $\mathcal{P}$

1.a) $\Gamma_{\mathcal{P}} \cong S_3$ in its regular representation on 6 points. Let $\bar{r}$ be an element of order 3 in $\bar{G}$. Let $r \in G$ be the inverse image of order 6 of $\bar{r}$. Each involution $\bar{j}$ of $\bar{G}$ fixes no points of $\mathcal{P}$ hence lifts to an involution j of G. Thus, $G \cong \langle r \rangle \rtimes \langle j \rangle \cong D_6$.

We may assume that the fixed points of $\bar{r}$ are 0 and ∞. Then $\bar{r}(X) = cX$ for $c \in k^*$. We may further assume that $1 \in \mathcal{P}$ by replacing X by cX for a suitable $c \in k^*$. Then, $\mathcal{P} = \{1, \xi_3, \xi_3^2, \lambda, \lambda\xi_3, \lambda\xi_3^2\}$ where ξ_3 is a primitive third root of unity and $\lambda \in \mathbb{P}^1 - \{0, 1, \infty, \xi_3, \xi_3^2\}$. Thus

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

For $\lambda = \pm 1$ this equation becomes $Y^2 = X^6 \pm 1$ and $\Gamma_{\mathcal{P}} \cong D_6$, see below 1.c).

1.b) $\Gamma_{\mathcal{P}} \cong S_4$.

If $char(k) \neq 2,3$ then the stabilizer in S_4 of each point of $\mathbb{P}^1$ is cyclic (see remark 2.2), hence has order 4, 3, or 2. Then the orbit length is 6, 8, or 12. Thus, S_4 has exactly one orbit of length 6 because if an element of Γ of order 4 acts on 6 points, then it fixes 2. Hence $S_3 \leq S_4$ acts transitively on this orbit because point stabilizer $\mathbb{Z}_4 \cap S_3 = \{1\}$.

Let $g \in S_4$ be an element of order 4. Then, g has order 8. So G is not isomorphic to $\mathbb{Z}_2 \times S_4$ or W_2 (see remark 2.3). Since $S_3 \leq S_4$ is transitive, it follows from 1.a) that G has an involution not equal to z_0. Thus, it is not isomorphic to W_3. Then $G \cong W_1$.

An element $\bar{g} \in \Gamma_{\mathcal{P}}$ of order 4 fixes two points in $\mathcal{P}$. So we may assume the two fixed points are 0 and ∞. We may further assume that $1 \in \mathcal{P}$ by replacing X by

cX for a suitable $c \in k^*$. Then, $\mathcal{P} = \{0, \infty, 1, -1, i, -i\}$ and

$$Y^2 = X^5 - X$$

If $char(k) = 3$ then the stabilizer in S_4 of each point of $\mathbb{P}^1$ is either cyclic, or is the normalizer of a 3-cycle. The rest is as above.

1.c) $\Gamma_{\mathcal{P}} \cong D_6$. Then, $G = \langle \bar{r} \rangle \rtimes \langle \bar{j} \rangle$, where $\bar{r}$ is of order 6 and j of order 2. We know that r has one or two fixed points and all other orbits on $\mathbb{P}^1$ have length 6. Hence, r acts as a 6-cycle on $\mathcal{P}$ and $z = r^3$ is an involution which fixes no points in $\mathcal{P}$. Further, j fixes 2 or no points in $\mathcal{P}$. More precisely, j fixes 2 points if and only if zj fixes no points on $\mathcal{P}$. Take $\bar{j}$ to fix 2 points on $\mathcal{P}$.

From lemma 2.1, $\pi^{-1}(\langle \bar{z} \rangle) = \{1, z_0, z_1, z_2\} =: V$, a normal 4-Klein subgroup in G. We denote the lift of order 3 of $\bar{r}^2$ by r. Since $z_0^r = z_0$, then $z_1^r = z_1$. Then, $\pi^{-1}(\langle \bar{r} \rangle) \cong V \rtimes \langle r \rangle$.

Since j fixes 2 points in $\mathcal{P}$, both lifts of $\bar{j}$ in G have order 4; let j be one of them. Then $\langle z_1, r \rangle \cap \langle j \rangle = \{1\}$, because $\mathbb{Z}_6 \cong \langle z_1, r \rangle$ has only one element of order 2 and no element of order 4.

If $z_1^j = z_1$, then $(jz_1)^2 = z_0$. But jz_1 maps to $j\bar{z}$ in G which fixes no points in $\mathcal{P}$, contradictory to lemma 2.1 a). Thus, $z_1^j = z_2$. Then, $\langle V, j \rangle \cong D_4$. Finally, $\langle r \rangle \lhd G$ and $G \cong \mathbb{Z}_3 \rtimes D_4$, where D_4 V acts on $\mathbb{Z}_3$ by inversion.

Since r acts as a 6-cycle on $\mathcal{P}$ then $r(X) = \xi_6 X$ where ξ_6 is a primitive 6-th root of unity. We may further assume that $1 \in \mathcal{P}$ by replacing X by cX for a suitable $c \in k^*$. Then $\mathcal{P} = \{1, \xi_6, \ldots, \xi_6^5\}$ and

$$Y^2 = X^6 - 1$$

1.d) $\Gamma_{\mathcal{P}} \cong S_5$. In this case $char(k) = 5$ and $S_5 \cong PGL_2(5)$ is given in its natural embedding in $PGL_2(k)$. So $\mathcal{P} \sim \mathbb{P}^1(\mathbb{F}_5)$.

Since every element of order 4 in $\Gamma_{\mathcal{P}}$ lifts to elements of order 8 (see lemma 2.1) then G is not the split extension. In the transitive permutation representation of

S_5 on 6 points the transpositions fix none of the 6 points. So they lift to involutions in G, lemma 2.1. Thus, $G \cong 2^+S_5$ (the unique non-split extension where transpositions lift to involutions). Thus we may assume that $P = \{0, 1, 2, 3, 4, \infty\}$. Then,

$$Y^2 = X^5 - X$$

2. Γ_P *acts intransitively on* P

2. a) $\Gamma_P \cong \mathbb{Z}_2$. Let g be the involution in G. If g fixes no points in P, then τ has order 2 (see lemma 2.1) Thus, $G \cong V_4$. We may assume that $1 \in P$ by replacing X by cX for a suitable $c \in k^*$. Then, $P = \{1, a, b, -1, -a, -b\}$ and

$$Y^2 = (X^2 - 1)(X^2 - a^2)(X^2 - b^2)$$

Suppose that g fixes 2 points in P. As in the proof of lemma 2.1, we may assume that $P = \{0, \infty, 1, -1, a, -a\}$ and $\tau(X) = -X$. Then exists $r \in \Gamma_P$, $r(x) = -\frac{1}{x}$, such that $r = g$ which is contradictory to $G \cong \mathbb{Z}_2$. Thus, $G \cong V_4$.

b) $\Gamma_P \cong \mathbb{Z}_5$. Then $G \cong \mathbb{Z}_{10}$. In this case $char\, k = 5$. The element $g \in \Gamma_P$ of order 5 fixes one point in P and $g(X) = \xi_5 X$. We may assume that the fixed point in P is 0 and further $1 \in P$ by replacing X by cX for a suitable $c \in k^*$. Then, $P = \{0, 1, \xi_5, \xi_5^2, \xi_5^3, \xi_5^4\}$ and

$$Y^2 = X^6 - X$$

c) $\Gamma_P \cong V_4$. If $g \in G$ fixes no points of P, then τ is an involution and $G \cong D_4$. If g fixes 2 points in P, then as in 2. a). $P = \{0, \infty, 1, -1, a, -a\}$ and $\tau(X) = -X$. Then, there is $r \in G$, $r(x) = -\frac{1}{x}$, such that r is an involution in G which fixes no points in P. Then again $G \cong D_4$.

Let $\tau \in \Gamma_P$ be an involution which fixes no points in P. Take the fixed points of this involution to be 0 and ∞. Then $\tau(X) = cX$ for $c \in k^*$. As above, we may assume $1 \in P$. Then $P = \{1, -1, a, b, -a, -b\}$. There is exactly one element $\bar{r} \in \Gamma_P \cong V_4$ which fixes two points in P, namely $\bar{r}(X) = \frac{1}{X}$. Then, $b = \frac{1}{a}$ and

$$Y^2 = (X^2 - 1)(X^4 - \lambda X^2 + 1), \quad where \quad \lambda = a^2 + \frac{1}{a^2}$$

Remark 2.4. The two orbits of S_3 length 3 give a 6-set $\mathcal{P} \subset \mathbb{P}^1$ fixed by S_3. The full stabilizer of this $\mathcal{P}$ is D_6. So S_3 does not occur in the intransitive case.

Combining all cases together we have the following theorem.

Theorem 2.5. *Let G be the automorphism group of a genus 2 function field over k, where $k = \bar{k}$, and $\mathrm{char}(k) = 2$. Then, G is isomorphic to one of the following: $\mathbb{Z}_2$, $\mathbb{Z}_{10}$, V_4, D_4, D_6, $\mathbb{Z}_3 \triangleleft D_4$, W_4, or the group 2^+S_5 of order 240. The center of G is of order 2, generated by the hyperelliptic involution, unless G is isomorphic to V_4 or $\mathbb{Z}_{10}$.*

CHAPTER 3
GENUS 2 FIELDS WITH DEGREE 2 ELLIPTIC SUBFIELDS

3.1 Introduction

In this chapter we study genus 2 function fields with elliptic subfields of degree 2. The locus $\mathcal{L}_2$ of these fields is a 2-dimensional subvariety of the moduli space $\mathcal{M}_2$ of genus 2 fields. We use a birational parameterization of $\mathcal{L}_2$ by affine 2-space to study the relation between the j-invariants of the degree 2 elliptic subfields. This extends work of Geyer, Gaudry, Schost, Stichtenoth and others. We find a 1-dimensional family of genus 2 curves having exactly two isomorphic elliptic subfields of degree 2; this family is parameterized by the j-invariant of these subfields. This leads to a remarkable embedding of the moduli space $\mathcal{M}_1$ of genus one curves into $\mathcal{M}_2$.

Let $\mathcal{C}$ be a genus 2 curve defined over k, $k = \bar{k}$, $char(k) = 0$ and K its function field. Jacobi [14] gives a general form of genus 2 curves with degree 2 elliptic subcovers:

$$Y^2 = X^6 - s_1 X^4 + s_2 X^2 - 1$$

and a description of $\mathcal{L}_2$ in terms of the cross ratios of the roots $\alpha_1, \ldots, \alpha_6$ of the sextic:

$$\frac{\alpha_3 - \alpha_1}{\alpha_3 - \alpha_2} : \frac{\alpha_4 - \alpha_1}{\alpha_4 - \alpha_2} = \frac{\alpha_5 - \alpha_1}{\alpha_5 - \alpha_2} : \frac{\alpha_6 - \alpha_1}{\alpha_6 - \alpha_2}$$

Thus, $\mathcal{L}_2$ is parameterized by the pair $(s_1, s_2) \in k^2$. We note that this parameterization of $\mathcal{L}_2$ factors through a ramified Galois covering

$$k^2 \longrightarrow k^2$$

$$(s_1, s_2) \to (u, v)$$

where $u = s_1 s_2$ and $v = s_1^3 + s_2^3$. This induces a birational parameterization of $\mathcal{L}_2$ by the pairs (u, v). All our computations use these coordinates (u, v). We use this to compute an equation for $\mathcal{L}_2$ in terms of the classical invariants. In section 4 and 5 we give a general relation between the j-invariants of degree 2 elliptic subfields of K. This improves [17], where each isomorphism type of G is treated separately. We determine conditions when degree 2 elliptic subfields of K are 2 or 3-isogenous.

3.2 Genus 2 Curves with Elliptic Involutions

The notation is as in previous chapter.

Definition 3.1. An **elliptic involution** of K is an involution in G which is different from z_0 (the hyperelliptic involution). Thus the elliptic involutions of G are in 1-1 correspondence with the elliptic subfields of K of degree 2 (by the Riemann-Hurwitz formula).

If z_1 is an elliptic involution and z_0 the hyperelliptic one, then $z_2 := z_0 z_1$ is another elliptic involution. So the elliptic involutions come naturally in pairs. This pairs also the elliptic subfields of K of degree 2. Two such subfields E_1 and E_2 are paired if and only if $E_1 \cap k(X) = E_2 \cap k(X)$. E_1 and E_2 are G-conjugate unless $G \cong D_6$ or $G \cong V_4$ (This can be checked from Theorem 2.5).

Theorem 3.2. *Let K be a genus 2 field and $\epsilon_2(K)$ the number of $Aut(K)$-classes of elliptic subfields of K of degree 2. Suppose $\epsilon_2(K) \geq 1$. Then the classical invariants of K satisfy the equation.*

$$
\begin{aligned}
&-J_2^7 J_4^1 + 8748 J_{10} J_2^4 J_6^2 507384000 J_{10}^2 J_4^2 J_2 - 19245600 J_{10}^2 J_4 J_2^3 - 592272 J_{10} J_4^4 J_2^1 + 77436 J_{10} J_4^3 J_2^4 - 78 J_2^5 J_4^5 \\
&-81 J_2^7 J_6^2 - 3499200 J_{10} J_2 J_6^2 + 4743360 J_{10} J_4^1 J_2 J_6 - 870912 J_{10} J_4^2 J_2^3 J_6 + 3090960 J_{10} J_4 J_2^2 J_6^2 - 5832 J_{10} J_2^5 J_4 J_6 \\
&+1332 J_2^4 J_4^1 J_6 - 125971200000 J_{10}^3 + 384 J_4^6 J_6 + 41472 J_{10} J_4^6 + 159 J_4^6 J_2^1 - 236196 J_{10}^2 J_2^5 - 80 J_4^7 J_2 - 54 J_2^5 J_4^2 J_6^2 \\
&-47952 J_2 J_4 J_6^4 + 1049760000 J_{10}^2 J_2^2 J_6 - 1728 J_4^5 J_2^2 J_6 + 6048 J_4^4 J_2 J_6^2 - 9331200 J_{10} J_4^2 J_6^2 + 108 J_2^4 J_4 J_6^3 \\
&+12 J_2^5 J_4^3 J_6 + 29376 J_2^3 J_4^4 J_6^2 - 8910 J_2^3 J_4^3 J_6^3 - 209952000 J_{10}^2 J_4 J_6 + 31104 J_6^5 - 6912 J_4^3 J_6^5 4 + 972 J_{10} J_2^6 J_4^2 = 0
\end{aligned}
\tag{3.1}
$$

Further, $\epsilon_2(K) = 2$ unless $K = k(X, Y)$ with

$$Y^2 = X^5 - X$$

in which case $e_2(K) = 1$.

Since $e_2(K)$ is the number of conjugacy classes of elliptic involutions in G the claim about $e_2(K)$ follows from theorem 2.5.

Lemma 3.3. *Suppose* z_1 *is an elliptic involution of* K. *Let* $z_2 = z_1 z_0$, *where* z_0 *is the hyperelliptic involution. Let* E_i *be the fixed field of* z_i *for* $i = 1, 2$. *Then* $K = k(X, Y)$ *where*

$$Y^2 = X^6 - s_1 X^4 + s_2 X^2 - 1 \tag{3.2}$$

and $27 - 18 s_1 s_2 - s_1^2 s_2^2 + 4 s_1^3 + 4 s_2^3 \neq 0$. *Further* E_1 *and* E_2 *are the subfields* $k(X^2, Y)$ *and* $k(X^2, YX)$.

Proof. Recall that $z_0(X) = X, z_0(Y) = -Y$. We choose the coordinate X such that $z_1(X) = -X$. By lemma 2.1 the involution z_1 fixes no points of $\mathcal{P}$, hence $\mathcal{P} = \{\pm\alpha, \pm\beta, \pm\gamma\}$, where $\alpha, \beta, \gamma \in k \setminus \{0\}$. Let

$$a := \alpha^2, \quad b := \beta^2, \quad c := \gamma^2$$

Then from 2.1 we have $K = k(X, Y)$ with

$$Y^2 = (X^2 - a)(X^2 - b)(X^2 - c)$$

We may further replace X by λX, for a suitable λ, to get $abc = 1$. Then

$$Y^2 = X^6 - s_1 X^4 + s_2 X^2 - 1$$

where $s_1 = a + b + c$ and $s_2 = ab + ac + bc$. Since the roots $\alpha_1, \ldots, \alpha_6$ are distinct then $27 - 18 s_1 s_2 - s_1^2 s_2^2 + 4 s_1^3 + 4 s_2^3 \neq 0$. The elements X^2 and XY are fixed by z_2. This implies the claim.

□

We need to determine to what extent the normalization in the above proof determines the coordinate X. The condition $z_1(X) = -X$ determines the coordinate

X up to a coordinate change by some $\gamma \in \Gamma$ centralizing z_1. Such γ satisfies $\gamma(X) = mX$ or $\gamma(X) = \frac{m}{X}$, $m \in k \setminus \{0\}$. The additional condition $abc = 1$ forces $1 = \gamma(a)\gamma(b)\gamma(c) = m^3$, hence $m^3 = 1$. So X is determined up to a coordinate change by the subgroup $H \cong D_6$ of Γ generated by $\tau_1 : X \to \xi_6 X$, $\tau_2 : X \to \frac{1}{X}$, where ξ_6 is a primitive 6-th root of unity. Let $\xi_3 := \xi_6^2$. The coordinate change by τ_1 replaces s_1 by $\xi_3 s_2$ and s_2 by $\xi_3^2 s_2$. The coordinate change by τ_2 switches s_1 and s_2. Invariants of this H-action are:

$$u := s_1 s_2$$

$$v := s_1^3 + s_2^3$$

Classical invariants of the field K given by lemma 3.3 are:

$$\begin{aligned} J_2 &= 240 - 16u \\ J_4 &= 18v + 4u^2 - 1620 - 504u \\ J_6 &= -206616u - 96v - 424u^2 - 24u^3 + 160uv + 119880 \\ J_{10} &= 64(27 - 18u - u^2 + 4v)^2 \end{aligned} \tag{3.3}$$

For $J_2 = 0$ the absolute invariants are

$$\begin{aligned} i_1 &:= \frac{3^2(u^2 - 126u + 12v + 405)}{2^2(15 + u)^2} \\ i_2 &:= \frac{3^4(u^3 - 729u^2 + 4131u - 36uv - 1404v - 3645)}{2^3(15 + u)^3} \\ i_3 &:= \frac{3^5(u^2 + 18u - 4v - 27)^2}{2^{13}(15 + u)^5} \end{aligned} \tag{3.4}$$

We can eliminate u and v and get the following equation of $\mathcal{L}_2$.

$$\begin{aligned} &-27i_1^6 + 9i_1^7 + 161243136i_3i_1^3 - 12441600i_3i_2^3 + 2i_2^5 + 10749542 4i_3i_1^2i_2 + 54i_1^3i_2^2 \\ &-52254720i_3i_1i_2^2 - 47278080i_3i_1^3i_2 - 8294400i_3i_1^2i_2^2 - 945959731 2000i_3^2i_1^2 - 18i_1^4i_2^2 \\ &-2407347121029 12i_3^2 - 111451255603200i_3^2i_1 - 20639121408000i_3^2i_2 - 5524070 4i_3i_1^4 \\ &+2i_1^6i_2 - 4i_1^4i_2^3 + 331776i_3i_1^5 - 27i_2^4 - 28665446400 00i_3^2i_1i_2 + 161243136i_3i_2^2 + 9i_1i_2^4 \\ &-26418075402240000i_3^3 = 0 \end{aligned} \tag{3.5}$$

This equation was found by Gaudry and Schost in [17], where they don't cancel the common divisor 3486784401. To get rid of the condition $J_2 \neq 0$ we multiply by J_2^5 to get the "projective" equation (3.1) of $\mathcal{L}_2$. This holds indeed for all $K \in \mathcal{L}_2$, as can be checked by substituting from (3.3). This completes the proof of theorem 3.2.

The following proposition determines the group G in terms of u and v.

Proposition 3.4. *Let $\mathcal{C}$ be a genus 2 curve such that $G := Aut(\mathcal{C})$ has an elliptic involution and $J_2 \neq 0$. Then,*

a) $G \cong \mathbb{Z}_3 \rtimes D_4$ if and only if $(u, v) = (0, 0)$ or $(u, v) = (225, 6750)$.

b) $G \cong W_1$ if and only if $u = 25$ and $v = -250$.

c) $G \cong D_6$ if and only if $4v - u^2 + 110u - 1125 = 0$, for $u \neq 9, 70 + 30\sqrt{5}, 25$. Moreover, the classical invariants satisfy the equations,

$$\begin{aligned} -J_4J_2^4 + 12J_2^3J_6 - 52J_4^2J_2^2 + 80J_4^3 + 960J_2J_4J_6 - 3600J_6^2 = 0 \\ 864J_{10}J_2^5 + 3456000J_{10}J_4^2J_2 - 43200J_{10}J_4J_2^3 - 2332800000J_{10}^2 - J_4^2J_2^6 \\ -768J_4^4J_2^2 + 48J_4^3J_2^4 + 4096J_4^5 = 0 \end{aligned} \tag{3.6}$$

d) $G \cong D_4$ if and only if $v^2 - 4u^3 = 0$, for $u \neq 1, 9, 0, 25, 225$. Cases $u = 0, 225$ and $u = 25$ are reduced to cases a) and b) respectively. Moreover, the classical invariants satisfy (3.1) and the following equation,

$$1706J_4^2J_2^2 - 2560J_4^3 + 27J_4J_2^4 - 81J_2^3J_6 - 14880J_2J_4J_6 + 28800J_6^2 = 0 \tag{3.7}$$

Proof. a) If $G \cong \mathbb{Z}_3 \rtimes D_4$ then $\mathcal{C}$ is isomorphic to $Y^2 = X^6 - 1$ (see theorem 4.3). Thus,

$$\begin{aligned} i_1 &= \frac{3^2(u^2 - 126u + 12v + 405)}{2^2(15 + u)^2} = \frac{81}{20} \\ i_2 &= \frac{3^3(u^3 - 729u^2 + 4131u - 36uv - 1404v - 3645)}{2^3(15 + u)^3} = -\frac{729}{200} \\ i_3 &= \frac{3^5(u^2 + 18u - 4v - 27)^2}{2^{15}(15 + u)^5} = \frac{729}{25600000} \end{aligned} \tag{3.8}$$

The only solutions of the system are $(u, v) = (0, 0)$ and $(u, v) = (225, 6750)$. They correspond to the same genus 2 curve, namely $Y^2 = X^6 - 1$.

b) If $G \cong W_1$ then $\mathcal{C}$ is isomorphic to

$$Y^2 = X^5 - X$$

(see theorem 4.3). Then, $\mathcal{C}$ is isomorphic to

$$Y^2 = X^6 + 5X^4 - 5X^2 - 1$$

(by the linear fractional transformation $X \to \frac{X+\sqrt{5}}{X-\sqrt{5}}$). Then, $s_1 = s_2 = -5$ and $u = 25$, $v = -250$. These are the unique values for u and v since the system

$$\begin{aligned} i_1 &= \frac{3^2(u^2 - 126u + 12v + 405)}{2^2(15+u)^2} = -\frac{36}{5} \\ i_2 &= \frac{3^3(u^3 + 729u^2 + 4131u - 36uv - 1404v - 3645)}{2^3(15+u)^3} = -\frac{1512}{25} \\ i_3 &= \frac{3^5(u^2 + 18u - 4v - 27)^2}{2^{13}(15+u)^5} = \frac{243}{200000} \end{aligned} \tag{3.9}$$

has a unique solution $(u, v) = (25, -250)$.

Conversely, every genus 2 curve with $(u, v) = (25, -250)$ is isomorphic to

$$Y^2 = X^6 + 5X^4 - 5X^2 - 1$$

so $G \cong W_1$.

(c) If $G \cong D_6$ then $\mathcal{C}$ is isomorphic to

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

for $\lambda \neq 0, 1$, and $\lambda^2 - 38\lambda + 1 \neq 0$ (see theorem 4.3). Then the system,

$$\begin{aligned} i_1 &= \frac{3^2(u^2 - 126u + 12v + 405)}{2^2(15+u)^2} = 1296\frac{\lambda(\lambda^2 + 7\lambda + 1)}{(\lambda^2 - 38\lambda + 1)^2} \\ i_2 &= \frac{3^3(u^3 + 729u^2 + 4131u - 36uv - 1404v - 3645)}{2^3(15+u)^3} = -11664\frac{\lambda(\lambda^4 - 22\lambda^3 - 66\lambda^2 - 22\lambda + 1)}{(\lambda^2 - 38\lambda + 1)^3} \\ i_3 &= \frac{3^5(u^2 + 18u - 4v - 27)^2}{2^{13}(15+u)^5} = \frac{729}{16}\frac{\lambda^2(\lambda - 1)^6}{(\lambda^2 - 38\lambda + 1)^5} \end{aligned} \tag{3.10}$$

has solutions,

$$u = 9\,\frac{\lambda^2 - 98\lambda + 1}{(\lambda - 1)^2}, \quad v = 54\frac{\lambda^4 + 364\lambda^3 + 2726\lambda^2 + 364\lambda + 1}{(\lambda - 1)^4}$$

Eliminating λ from the above expressions we have

$$1125 - 110u - u^2 - 4v = 0 \tag{3.11}$$

From the above equation the values $u = 9, 70 + 30\sqrt{5}$ make $J_{10} = 0$, so we exclude them. Note that, for $(u, v) = (25, -250)$ this is case b), so $u = 25$ is also excluded.

Then $v = \frac{1}{4}(u^2 - 110u + 1125)$ and i_1, i_2, i_3 are

$$\begin{aligned} i_1 &= 9\,\frac{(u-9)(u-105)}{(15+u)^2} \\ i_2 &= -27\,\frac{(u-9)(u^2-162u-5535)}{(15+u)^3} \\ i_3 &= 486\,\frac{(u-9)^2}{(15+u)^2} \end{aligned} \tag{3.12}$$

The classical invariants satisfy

$$\begin{aligned} -J_4J_2^4 + 12J_2^3J_6 - 52J_4^2J_2^2 + 80J_4^3 + 960J_2J_4J_6 - 3600J_6^2 = 0 \\ 864J_{10}J_2^3 - 3456000J_{10}J_4^2J_2 - 43200J_{10}J_4J_2^3 - 2332800000J_{10}^2 - J_4^2J_2^6 \\ -768J_4^4J_2^2 - 48J_4^3J_2^4 - 4096J_4^5 = 0 \end{aligned} \tag{3.13}$$

c) If $G \cong D_4$, then C is isomorphic to

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

for $\lambda \neq \pm 2$ (see theorem 4.3). Then the system

$$\begin{aligned} i_1 &= \frac{3^2(u^2 - 126u + 12v + 405)}{2^2(15+u)^2} = \frac{9}{4}\,\frac{(\lambda^2 + 32\lambda + 76)(\lambda - 2)^2}{(\lambda^2 + 2\lambda + 16)^2} \\ i_2 &= \frac{3^3(u^3 - 729u^2 - 4131u - 36uv - 1404v - 3645)}{2^3(15+u)^3} = \frac{27}{8}\,\frac{(\lambda^2 - 58\lambda - 104)(\lambda - 2)^4}{(\lambda^2 + 2\lambda + 16)^3} \\ i_3 &= \frac{3^5(u^2 - 18u - 4v - 27)^2}{2^{13}(15+u)^5} = \frac{243}{8192}\,\frac{(\lambda - 2)^6(\lambda - 2)^2}{(\lambda^2 + 2\lambda + 16)^5} \end{aligned} \tag{3.14}$$

has the following solutions,

$$u = \frac{(\lambda - 14)^2}{(\lambda + 2)^2}, \quad v = -2\frac{(\lambda - 14)^3}{(\lambda + 2)^3}$$

Eliminating λ from the above equations we get

$$v^2 - 4u^3 = 0$$

If $u = 0, 25, 225$ this case reduces to one of the previous cases. For $u = 1, 9$ we have $J_{10} = 0$ so we have to exclude these values also. The classical invariants must also satisfy the equation

$$1706J_4^2J_2^2 + 2560J_4^3 + 27J_4J_2^4 - 81J_2^3J_6 - 14880J_2J_4J_6 + 28800J_6^2 = 0 \tag{3.15}$$

□

Proposition 3.5. *The mapping*

$$A : (u, v) \longrightarrow (i_1, i_2, i_3)$$

gives a birational parameterization of $\mathcal{L}_2$. *The fibers of* A *of cardinality* > 1 *correspond to those curves* $\mathcal{C}$ *with* $|Aut(\mathcal{C})| > 4$.

Proof. We denote $A(u, v) = \mathcal{C}_{(u,v)} = (i_1, i_2, i_3)$ and $A(u', v') = \mathcal{C}_{(u',v')} = (i'_1, i'_2, i'_3)$. The solution set of the system

$$\begin{cases} i_1 = i'_1 \\ i_2 = i'_2 \\ i_3 = i'_3 \end{cases} \tag{3.16}$$

is $(u, v) = (u', v')$ or $(v^2 - 4u^3)(4v - u^2 + 110u - 1125) = 0$. Thus, if $(u, v) \neq (u', v')$ then $(v^2 - 4u^3)(4v - u^2 + 110u - 1125) = 0$. So $Aut(\mathcal{C})$ is isomorphic to one of W_1, $\mathbb{Z} \times D_1$, D_1 or D_2. Therefore, $|Aut(\mathcal{C})| > 4$. If $(v^2 - 4u^3)(4v - u^2 + 110u - 1125) \neq 0$ then $(u, v) = (u', v')$ and A is injective.

□

3.3 j-invariants of Elliptic Subcovers

Let j_1 and j_2 denote the j-invariants of the elliptic curves E_1 and E_2 from lemma 3.3. Then, j_1 and j_2 are,

$$\begin{aligned} j_1 &= -256\frac{(s_1^2 - 3s_2)^3}{(4s_1^3 + 27 - 18s_1s_2 - s_1^2s_2^2 + 4s_2^3)} \\ j_2 &= -256\frac{(s_2^2 - 3s_1)^3}{(4s_1^3 + 27 - 18s_1s_2 - s_1^2s_2^2 + 4s_2^3)} \end{aligned} \tag{3.17}$$

Lemma 3.6. *The invariants* j_1 *and* j_2 *and are roots of the quadratic*

$$j^2 + 256\frac{(2u^3 - 54u^2 + 9uv - v^2 + 27v)}{(u^2 + 18u - 4v - 27)}j + 65536\frac{(u^2 + 9u - 3v)}{(u^2 + 18u - 4v - 27)^2} = 0 \tag{3.18}$$

Proof. From equations (3.17) and $c = s_1^3 + s_2^3$, $a = s_1 s_2$ we eliminate s_1 and s_2 and get

$$\begin{aligned} a(a^2+18a-4c-27)^2 j_1^2 + 256(2a^3-54a^2+9ac-c^2+27c)(a^2+18a-4c-27)j_1 \\ +65536(a^2+9a-3c)) = 0 \\ a(a^2+18a-4c-27)^2 j_2^2 + 256(2a^3-54a^2+9ac-c^2+27c)(a^2+18a-4c-27)j_2 \\ +65536(a^2+9a-3c)) = 0 \end{aligned} \tag{3.19}$$

Thus j_1 and j_2 are roots of the same quadratic equation. Since $(a^2+18a-4c-27) = J_{10} = 0$ we can divide by it and write the equation as

$$a\left(j^2 + 256\frac{(2a^3-54a^2+9ac-c^2+27c)}{(a^2+18a-4c-27)}j + 65536\frac{(a^2+9a-3c)}{(a^2+18a-4c-27)^2}\right) = 0 \tag{3.20}$$

If $a = 0$, then $s_1 = 0$ or $s_2 = 0$ and $c = s_1^3$ or $c = s_2^3$. The j-invariants of E_1 and E_2 are

$$j_1 = -256\frac{c^2}{4c-27}, \qquad j_2 = 6912\frac{c}{4c-27}$$

and they satisfy equation (3.18). If $a \neq 0$ then we divide by a and get equation (3.18).

□

3.3.1 Isomorphic Elliptic Subfields

The elliptic curves E_1 and E_2 are isomorphic when equation (3.18) has a double root. The discriminant of the quadratic is zero for

$$(c^2 - 4a^3)(c - 9a - 27) = 0$$

Remark 3.7. From lemma 3.3, $c^2 = 4a^3$ if and only if $Aut(\mathcal{C}) \cong D_4$. So for $\mathcal{C}$ such that $Aut(\mathcal{C}) \cong D_4$, E_1 is isomorphic to E_2. It is easily checked that z_1 and $z_2 = z_0 z_1$ are conjugate when $G \cong D_4$. So they fix isomorphic subfields.

If $c = 9(a-3)$ then the locus of these curves is given by,

$$\begin{aligned} 4i_1^3 - 9i_1^4 + 73728i_1^2 i_3 - 150994944 i_3^2 = 0 \\ 289i_1^3 - 729i_1^2 + 54 i_1 i_2 - i_2^2 = 0 \end{aligned} \tag{3.21}$$

For $(u,v) = (\frac{9}{4}, -\frac{27}{4})$ the curve has $Aut(\mathcal{C}) \cong D_4$ and for $(u,v) = (137, 1206)$ it has $Aut(\mathcal{C}) \cong D_6$. All other curves with $v = 9(u-3)$ belong to the general case, so $Aut(\mathcal{C}) \cong V_4$. The j-invariants of elliptic curves are $j_1 = j_2 = 256(9-u)$. Thus, these genus 2 curves are parameterized by the j-invariant of the elliptic subcover.

Remark 3.8. This embeds the moduli space $\mathcal{M}_1$ into $\mathcal{M}_2$ in a functorial way.

3.4 Isogenous Degree 2 Elliptic Subfields

In this section we study pairs of degree 2 elliptic subfields of K which are 2 or 3-isogenous. We denote by $\Phi_n(x,y)$ the n-th modular polynomial (see Blake et al. [1] for the formal definitions. Two elliptic curves with j-invariants j_1 and j_2 are n-isogenous if and only if $\Phi_n(j_1, j_2) = 0$.

3.4.1 3-Isogeny.

The modular 3-polynomial is given below

$$\begin{aligned}\Phi_3 = {} & x^4 - x^3y^3 + y^4 + 2232xy(x+y) - 1069956xy(x+y) + 36864000(x^3+y^3) + \\ & 2587918086x^2y^2 - 8900222976000xy(x+y) + 452984832000000(x^2+y^2) - \\ & 770845966336000000xy - 1855425871872000000000(x+y)\end{aligned} \tag{3.22}$$

Suppose E_1 and E_2 are 3-isogenous. Then from equation (3.18) and $\Phi_3(j_1, j_2) = 0$ we eliminate j_1 and j_2. Then,

$$(4v - u^2 + 110u - 1125) \cdot g_1(u,v) \cdot g_2(u,v) = 0 \tag{3.23}$$

where g_1 and g_2 are

$$\begin{aligned}g_1 = {} & -27008u^6 + 256u^7 - 2432u^5v + v^4 + 7296u^3v^2 - 6692v^3u - 1755067500u \\ & + 2419308v^3 - 34553439u^4 + 127753092vu^2 + 16274844vu^3 - 1720730u^2v^2 \\ & - 1941120u^5 + 381631500v + 1018668150u^2 - 116158860u^3 + 52621974v^2 \\ & + 387712u^4v - 48396366vu - 33416676v^2u + 922640625\end{aligned} \tag{3.24}$$

$$
\begin{aligned}
g_2 = {} & 291350448u^6 - v^4u^2 - 998848u^6v - 3456u^7v + 4749840u^4v^2 + 17032u^5v^2 \\
& + 4v^5 + 80368u^8 + 256u^9 + 6848224u^7 - 10535040v^3u^2 - 35872v^3u^3 + 26478v^4u \\
& - 77908736u^7v - 9516699v^4 - 307234984u^3v^2 - 41958374v^3u - 8264367360v^3 \\
& + 275029032960u^4 + 28808773632vu^2 - 234299554560vu^3 + 5455334016u^2v^2 \\
& - 11278242816v + 8255648563 2u^2 - 1087375933440u^3 - 121230950 40v^2 \\
& - 11278242816vu + 3503554560v^2u + 534101990 4u^5 - 245461248 0u^4v
\end{aligned}
\tag{3.25}
$$

Thus, there is a isogeny of degree 3 between E_1 and E_2 if and only if u and v satisfy equation (3.23). The vanishing of the first factor is equivalent to $G \cong D_6$. So, if $Aut(C) \cong D_6$ then E_1 and E_2 are isogenous of degree 3. This was also noted by Gaudry and Schost [17].

3.4.2 2-Isogeny

Below we give the modular 2-polynomial.

$$
\begin{aligned}
\Phi_2 = {} & x^3 - x^2y^2 + y^3 + 1488xy(x + y) + 40773375xy - 162000(x^2 - y^2) + \\
& 87480000000(x + y) - 157464000000000
\end{aligned}
\tag{3.26}
$$

Suppose E_1 and E_2 are isogenous of degree 2. Substituting j_1 and j_2 in Φ_2 we get

$$
f_1(u, v) \cdot f_2(u, v) = 0 \tag{3.27}
$$

where f_1 and f_2 are

$$
\begin{aligned}
f_1 = {} & -16v^3 - 81216v^2 - 892296v - 2460375 + 3312uv^2 + 707616vu + 3805380u + \\
& 18360vu^2 - 1296162u^2 - 1744u^3v - 140076u^3 + 801u^4 + 256u^5
\end{aligned}
\tag{3.28}
$$

$$
\begin{aligned}
f_2 = {} & 4096u^7 + 256016u^6 - 45824u^5v + 4736016u^5 - 2126736vu^4 + 23158143u^4 \\
& - 25451712u^3v - 119745540u^3 + 5291136v^2u^2 - 48166488vu^2 - 2390500350u^2 \\
& - 179712uv^3 + 35831808uv^2 + 1113270480vu + 9300217500u - 4036608v^3 \\
& - 1791153000v - 8303765625 - 1024v^4 + 163840u^3v^2 - 122250384v^2 + 256u^2v^3
\end{aligned}
\tag{3.29}
$$

3.4.3 Other Isogenies between Elliptic Subfields

If $G \cong D_4$, then z_1 and z_2 are in the same conjugacy class. There are again two conjugacy classes of elliptic involutions in G. Thus, there are two degree 2 elliptic subfields (up to isomorphism) of K. One of them is determined by double root j of

the equation (3.18), for $v^2 - 4u^3 = 0$. Next, we determine the j-invariant j' of the other degree 2 elliptic subfield and see how it is related to j.

If $v^2 - 4u^3 = 0$ then $\bar{G} \cong V_4$ and $\mathcal{P} = \{\pm 1, \pm\sqrt{a}, \pm\sqrt{b}\}$. Then, $s_1 = a + \frac{1}{a} + 1 = s_2$. Involutions of $\mathcal{C}$ are $\tau_1 : X \to -X$, $\tau_2 : X \to \frac{1}{X}$, $\tau_3 : X \to -\frac{1}{X}$. Since τ_1 and τ_3 fix no points of $\mathcal{P}$ the they lift to involutions in G. They each determine a pair of isomorphic elliptic subfields. The j-invariant of elliptic subfield fixed by τ_1 is the double root of equation (3.18), namely

$$j = -256\frac{v^3}{v+1}$$

To find the j-invariant of the elliptic subfields fixed by τ_3 we look at the degree 2 covering $\phi : \mathbb{P}^1 \to \mathbb{P}^1$, such that $\phi(\pm 1) = 0$, $\phi(a) = \phi(-\frac{1}{a}) = 1$, $\phi(-a) = \phi(\frac{1}{a}) = -1$, and $\phi(0) = \phi(\infty) = \infty$. This covering is, $\phi(X) = \frac{a-1}{a+1}\frac{X^2+1}{X}$. The branch points of ϕ are $q_i = \pm\frac{2\sqrt{a}}{a-1}$. From lemma 3.3 the elliptic subfields E_1' and E_2' have 2-torsion points $\{0, 1, -1, q_i\}$. The j-invariants of E_1' and E_2' are

$$j' = -16\frac{(v-15)^3}{(v+1)^2}$$

Then $\Phi_2(j, j') = 0$, so E_1 and E_1' are isogenous of degree 2. Thus, τ_1 and τ_3 determine degree 2 elliptic subfields which are 2-isogenous (see also Geyer [18]).

CHAPTER 4
CURVES OF GENUS TWO WITH SPLIT JACOBIANS

Let C be a curve of genus 2 and $\varphi_1 : C \longrightarrow E_1$ a map of degree n, from C to an elliptic curve E_1, both curves defined over a field k of characteristic 0. This map induces a degree n map $\phi_1 : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ which we call a Frey-Kani covering. We determine all possible ramifications for ϕ_1. If $\varphi_1 : C \longrightarrow E_1$ is maximal then there exists a maximal map $\varphi_2 : C \longrightarrow E_2$, of degree n, to some elliptic curve E_2 such that there is an isogeny of degree n^2 from the Jacobian J_C to $E_1 \times E_2$. We say that J_C is (n,n)-decomposable.

Curves of genus 2 with non-simple Jacobians are of much interest. Their Jacobians have large torsion subgroups, e.g. Howe, Leprévost, and Poonen have found a family of genus 2 curve with 128 rational points in its Jacobian (see [9]). For other applications of genus 2 curves with (n,n)-decomposable Jacobians (see Frey [5]). In this chapter, we discuss genus 2 curves C whose function fields have maximal elliptic subfields. Let $\varphi : C \to E$ be a maximal cover (cf. section 4) of odd degree n. The moduli space parameterizing these covers is a surface, more precisely the product of modular curves $X(n) \times X(n)/\Delta$ (see Kani [10]). When $\varphi : C \to E$ is degenerate (cf. section 2), this moduli space is a curve. In sections 2 and 3 we define a Frey-Kani covering and determine all their possible ramifications.

4.1 Frey-Kani Covers

Let C and E be curves of genus 2 and 1, respectively. Both are smooth, projective curves defined over k, $char(k) = 0$. Let $\varphi : C \longrightarrow E$ be a covering of degree n. From the Riemann-Hurwitz formula, $\sum_{P \in C} (\epsilon_\varphi(P) - 1) = 2$ where

$e_v(P)$ is the ramification index of points $P \in C$, under v. Thus, we have two points of ramification index 2 or one point of ramification index 3. The two points of ramification index 2 can be in the same fiber or in different fibers. Therefore, we have the following cases of the covering v:

Case I. There are $P_1, P_2 \in C$, such that $e_v(P_1) = e_v(P_2) = 2$, $v(P_1) \neq v(P_2)$, and $\forall P \in C \setminus \{P_1, P_2\}$, $e_v(P) = 1$.

Case II. There are $P_1, P_2 \in C$, such that $e_v(P_1) = e_v(P_2) = 2$, $v(P_1) = v(P_2)$, and $\forall P \in C \setminus \{P_1, P_2\}$, $e_v(P) = 1$.

Case III. There is $P_1 \in C$ such that $e_v(P_1) = 3$, and $\forall P \in C \setminus \{P_1\}$, $e_v(P) = 1$.

In case I (resp. II, III) the cover v has 2 (resp. 1) branch points in E.

Denote the hyperelliptic involution of C by w. We choose $\mathcal{O}$ in E such that w restricted to E is the hyperelliptic involution on E (see [6] or [12]). We denote the restriction of w on E by v, $v(P) = -P$. Thus, $v \circ w = v \circ v$. E[2] denotes the group of 2-torsion points of the elliptic curve E, which are the points fixed by v. The proof of the following two lemmas is straightforward and will be omitted.

Lemma 4.1. *a) If $Q \in E$, then $\forall P \in v^{-1}(Q)$, $w(P) \in v^{-1}(-Q)$.*

b) For all $P \in C$, $e_v(P) = e_v(w(P))$.

Proof. a) Take $Q \in E$ and $v(P) = Q$. Then, $v \circ v(Q) = v(Q)$. Thus, $(v \circ w)(P) = -Q$.

b) Since $v \circ w = v \circ v$, then $e_{v \circ w}(P) = e_{v \circ v}(P)$ for all $P \in C$. Thus $e_w(P) \cdot e_v(w(P)) = e_v(P) \cdot e_v(v(P))$. So $e_v(w(P)) = e_v(P)$.

□

Let W be the set of points in C fixed by w. Every curve of genus 2 is given, up to isomorphism, by a binary sextic, so there are 6 points fixed by the hyperelliptic

involution w, namely the Weierstrass points of C. The following lemma determines the distribution of the Weierstrass points in fibers of 2-torsion points.

Lemma 4.2. *1.* $v(W) \subset E[2]$

2. If n is an odd number then

i) $v(W) = E[2]$

ii) If $Q \in E[2]$ *then* $\#(v^{-1}(Q) \cap W) = 1 \mod (2)$

3. If n is an even number then for all $Q \in E[2]$, $\#(v^{-1}(Q) \cap W) = 0 \mod (2)$

Proof. For every P such that $w(P) = P$ we have $(v \circ w)(P) = v(P)$. So $(v \circ v)(P) = v(P)$, therefore $v(P) \in E[2]$.

To prove part 2. i) we take $Q \in E[2]$. From previous lemma, w permutes every two points in the fiber of Q. Because n is odd, it has to be a point fixed by w in $v^{-1}(Q)$. So $Q \in v(W)$.

There are 6 Weierstrass points in C. In each fiber of points in $E[2]$ there is at least one point fixed by w. But n is odd, so in one fiber w fixes 3 points. Thus, $\#(v^{-1}(Q) \cap W) = 1 \mod (2)$.

Assume now that n is even. The hyperelliptic involution w permutes every two points in the fiber of Q, for $Q \in E[2]$. So if w fixes any point, it has to fix a even number of them. Thus, we have an even number of Weirstrass points in each fiber of points from $E[2]$.

□

Let $\pi_C : C \longrightarrow \mathbb{P}^1$ and $\pi_E : E \longrightarrow \mathbb{P}^1$ be the natural degree 2 projections. The hyperelliptic involution permutes the points in the fibers of π_C and π_E. The ramified points of π_C, π_E are respectively points in W and $E[2]$ and their ramification index is 2. There is $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ such that the diagram commutes (see Frey [6] or Kuhn [12]).

$$\begin{array}{ccc} C & \xrightarrow{\pi_C} & \mathbb{P}^1 \\ \psi \downarrow & & \downarrow \phi \\ E & \xrightarrow{\pi_E} & \mathbb{P}^1 \end{array}$$

The covering $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ will be called the corresponding **Frey-Kani covering** of $\psi : C \longrightarrow E$. It has first appeared in [6] and [5]. The term, Frey-Kani covering, has first been used by Fried in [7].

4.2 Ramification of Frey-Kani Coverings

In this section we will determine the ramification of Frey-Kani coverings $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$. First we fix some notation. For a given branch point we will denote the ramification of points in its fiber as follows. Any point P of ramification index m is denoted by (m). If there are k such points then we write $(m)^k$. We omit writing symbols for unramified points, in other words $(1)^k$ will not be written. Ramification data between two branch points will be separated by commas. We denote by $\pi_E^{-1}(E[2]) = \{q_1, \ldots, q_4\}$ and $\pi_C^{-1}(W) = \{w_1, \ldots, w_6\}$.

4.2.1 The Case When n is Odd

The following theorem classifies the ramification types for the Frey-Kani coverings $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ when the degree n is odd.

Theorem 4.3. *Let $\psi : C \longrightarrow E$ be a covering of odd degree n and $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ be the Frey-Kani covering induced by ψ. This induces a partitioning of the set of 6 Weierstrass points of C into two sets $W^{(1)} = W^{(1)}(C, E)$ and $W^{(2)} = W^{(2)}(C, E)$, each of cardinality 3 such that $|\phi(W^{(1)})| = 1$ and $|\phi(W^{(2)})| = 3$. Then the ramification structure of ϕ is as follows.*

Case I: *(the generic case)*

$$\left((2)^{\frac{n-1}{2}}, (2)^{\frac{n-1}{2}}, (2)^{\frac{n-1}{2}}, (2)^{\frac{n-1}{2}}, (2)^1\right)$$

Or the following degenerate cases:

Case II: *(the 4-cycle case and the dihedral case)*

$$i)\ \left((2)^{\frac{n-1}{2}},(2)^{\frac{n-1}{2}},(2)^{\frac{n-1}{2}},(4)^1(2)^{\frac{n-7}{2}}\right)$$

$$ii)\ \left((2)^{\frac{n-1}{2}},(2)^{\frac{n-1}{2}},(2)^{\frac{n-1}{2}},(2)^{\frac{n-1}{2}}\right)$$

$$iii)\ \left((2)^{\frac{n-1}{2}},(2)^{\frac{n-1}{2}},(4)^1(2)^{\frac{n-5}{2}},(2)^{\frac{n-1}{2}}\right)$$

Case III: *the 3-cycle case*

$$\left((2)^{\frac{n-1}{2}},(2)^{\frac{n-1}{2}},(2)^{\frac{n-1}{2}},(3)^1(2)^{\frac{n-3}{2}}\right)$$

$$ii)\ \left((2)^{\frac{n-3}{2}},(2)^{\frac{n-3}{2}},(3)^1(2)^{\frac{n-3}{2}},(2)^{\frac{n-3}{2}}\right)$$

Proof. From lemma 4.2 we can assume that $\phi(w_i) = q_i$ for $i \in \{1,2,3\}$ and $\phi(w_4) = \phi(w_5) = \phi(w_6) = q_4$. Next we consider the three cases for the ramification of $\psi : C \longrightarrow E$ and see what ramifications they induce on $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$.

Suppose that $P \in \psi^{-1}(E[2]) \setminus W$ and $e_\psi(P) = 1$. Then $e_\psi(P) \cdot e_{\pi_E}(\psi(P)) = e_{\pi_C}(P) \cdot e_\phi(\pi_C(P)) = 2$, so $e_\phi(\pi_C(P)) = 2$.

Case I: There are P_1 and P_2 in C such that $e_\psi(P_1) = e_\psi(P_2) = 2$ and $\psi(P_1) \neq \psi(P_2)$. By lemma 4.1, $e_\psi(w(P_1)) = 2$. So $w(P_1) = P_1$ or $w(P_1) = P_2$.

Suppose that $w(P_1) = P_1$, so $P_1 \in W$. If $\pi_C(P_1) = w_i$ for $i \in \{1,2,3\}$, say $\pi_C(P_1) = w_1$, then $e_{\pi_E \circ \psi}(P_1) = e_{\pi_E}(\psi(P_1)) = 4$, which implies that $e_\phi(w_1) = 2$. All other points in the fiber of $\pi_E \circ \psi(P_1) =: q_1$ have ramification index 2 under ϕ. So ϕ has even degree, which is a contradiction. If $\pi_C(P_1) = w_i$ for $i \in \{4,5,6\}$, say $\pi_C(P_1) = w_4$, then in the fiber of q_4 are: w_4 of ramification index 2, w_5 and w_6 unramified, and all other points have ramification index 2. So $\#(\phi^{-1}(q_4)) = 2 + 1 + 1 + 2k$, is even. Thus $P_1, P_2 \in W$. Then $P_1, P_2 \in \psi^{-1}(E[2])$, otherwise they would be in the same fiber.

Thus $P_2 = w(P_1) \in C \setminus \psi^{-1}(E[2])$ and $\psi(P_1) = -\psi(P_2)$. Let $\pi_E \circ \psi(P_1) = \pi_E \circ \psi(P_2) = q_5$ and $\pi_C(P_1) = \pi_C(P_2) = S$. So $e_\psi(P_1) \cdot e_{\pi_E}(\psi(P_1)) = e_{\pi_C}(P_1) \cdot e_\phi(\pi_C(P_1))$. Thus, $e_\phi(\pi_C(P_1)) = e_\phi(S) = 2$. All other points in $\phi^{-1}(q_5)$ are unramified.

For $P \in W$, $e_{\pi_E}(P) = 2$. Thus $e_\phi(\pi_C(P)) = 1$. All $w_1, \ldots, w_6$ are unramified and other points in $\phi^{-1}(E[2])$ are of ramification index 2. By the Riemann - Hurwitz formula, ϕ is unramified everywhere else.

Thus, there are $\frac{n-1}{2}$ points of ramification index 2 in the fibers $\phi^{-1}(q_1)$, $\phi^{-1}(q_2)$, $\phi^{-1}(q_3)$, $\frac{n-3}{2}$ points of ramification index 2 in $\phi^{-1}(q_4)$, and one point of index 2 in $\phi^{-1}(q_5)$.

Case II: In this case, there are distinct P_1 and P_2 in C such that $e_\pi(P_1) = e_\pi(P_2) = 2$ and $w(P_1) = w(P_2)$. Then $P_2 = w(P_1)$ or $w(P_i) = P_i$, for $i = 1, 2$.

Let P_1 and P_2 be in the fiber which has three Weierstrass points.

i) Suppose that w permutes P_1 and P_2. So P_1 and P_2 are not Weierstrass points. Then $e_{\pi_E \circ \pi}(P_1) = e_\pi(P_1) \cdot e_{\pi_E}(\pi(P_1)) = 4$. Thus $e_{\pi_E}(P_1) \cdot e_\phi(\pi_C(P_1)) = 4$. Since $e_{\pi_E}(P_1) = 1$ then $e_\phi(\pi_C(P_1)) = 4$. So there is a point of index 4 in the fiber of q_1. The rest of the points are of ramification index 2, as in previous case, other then the $w_1, \ldots, w_6$, which are unramified.

ii) Suppose that w fixes P_1 and P_2. Thus P_1 and P_2 are Weierstrass points. Then $e_\pi(P_1) \cdot e_{\pi_E}(\pi(P_1)) = e_{\pi_E}(P_1) \cdot e_\phi(\pi_C(P_1)) = 4$. So $e_\phi(\pi_C(P_1)) = 2$. Thus, $\pi_C(P_1)$ have ramification index 2. The other points behave as in the previous case. So we have in each fiber of ϕ one unramified point and everything else has ramification index 2.

Suppose that P_1 and P_2 are in one of the fibers which have only one Weierstrass point.

iii) Then w has to permute them, so they are not Weierstrass points. As in case i) $e_\phi(\pi_C(P_1)) = 4$. So there is a point of index 4 in one of $\phi^{-1}(q_1)$, $\phi^{-1}(q_2)$, $\phi^{-1}(q_3)$ and everything else is of ramification index 2. The Weierstrass points are as in case i), unramified.

Case III: Let P be the ramified point of index 3. By lemma 1, $e_\pi(P) = 3$. But there is only one such point in C, so $P \in W$. Then $e_{\pi_E \circ \pi}(P) = e_\pi(P) \cdot$

$e_2(\pi_C(P)) = 6$. So $e_\omega(P) \cdot e_2(\pi_C(P)) = 6$. But $e_\omega(P) = 2$, because $P \in W$. Thus, $e_2(\pi_C(P)) = 3$.

ii) Q is in the fiber that contains three Weierstrass points. Then we have a point of ramification index three in $\omega^{-1}(q_4)$, two other Weierstrass points are unramified, and all the other points are of ramification index 2.

iii) Q is in one of the fibers that contains only one Weierstrass point. Then in one of $\omega^{-1}(q_1)$, $\omega^{-1}(q_2)$, $\omega^{-1}(q_3)$ there is a point of index 3 and everything else is of index 2.

□

4.2.2 The Case When n is Even

Let us assume now that $deg\,\omega = n$ is an even number. The following theorem classifies the Frey-Kani coverings in this case.

Theorem 4.4. *If n is an even number then the generic case for $\omega : C \longrightarrow E$ induce the following three cases for $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$:*

I. $\left((2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}, (2)\right)$

II. $\left((2)^{\frac{n-4}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)\right)$

III. $\left((2)^{\frac{n-1}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)\right)$

Each of the above cases has the following degenerations (two of the branch points collapse to one)

I. *1.* $\left((2)^{\frac{n}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}\right)$

2. $\left((2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (4)(2)^{\frac{n-4}{2}}, (2)^{\frac{n}{2}}\right)$

3. $\left((2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (4)(2)^{\frac{n-4}{2}}\right)$

4. $\left((3)(2)^{\frac{n-4}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}\right)$

II. *1.* $\left((2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

2. $\left((2)^{\frac{n-4}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

3. $\left((4)(2)^{\frac{n-8}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

4. $\left((2)^{\frac{n-4}{2}}, (4)(2)^{\frac{n-6}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

5. $\left((2)^{\frac{n-4}{2}}, (2)^{\frac{n-6}{2}}, (2)^{\frac{n-4}{2}}, (2)^{\frac{n}{2}}\right)$

6. $\left((3)(2)^{\frac{n-6}{2}}, (2)^{\frac{n-2}{2}}, (4)(2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

7. $\left((2)^{\frac{n-4}{2}}, (3)(2)^{\frac{n-4}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

III. 1. $\left((2)^{\frac{n-4}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (4)(2)^{\frac{n}{2}}\right)$

2. $\left((2)^{\frac{n-6}{2}}, (4)(2)^{\frac{n-4}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

3. $\left((2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (4)(2)^{\frac{n-10}{2}}\right)$

4. $\left((3)(2)^{\frac{n-6}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

Proof. We know that the number of Weierstrass points in the fibers of 2-torsion points is 0 mod (2). Combining this with the Riemann - Hurwitz formula we get the three cases of the general case.

To determine the degenerate cases we consider cases when there is one branch point for $\omega : C \longrightarrow E$.

I) First, assume that the branch point has two points P_1 and P_2 of index 2 (Case II). Then $w(P_1) = P_i$ for $i = 1, 2$ or $w(P_1) = P_2$. The first case implies that $P_1, P_2 \in W$. Then $\epsilon_\phi(w(P_1)) = \epsilon_\phi(w(P_2)) = 2$. So we have case I. 1. When $w(P_1) = P_2$ then $\epsilon_\phi(w(P_1)) = 4$. Thus, we have a point of index 4 in $\phi^{-1}(q)$ for $q \in \{q_1, \ldots, q_4\}$. Therefore cases 2 and 3. If there is $P \in C$ such that $\epsilon_\omega(P) = 3$, then $P \in W$ and $\epsilon_\phi(w(P)) = 3$. So we have case 4.

II) As in case I. if P_1 and P_2 are Weierstrass points then they can be in the fiber of the point which has 4 or 2 Weierstrass points. So we get two cases, namely 1 and 2. Suppose now that P_1 and P_2 are not Weierstrass points, thus $w(P_1) = P_2$ and $\epsilon_\phi(w(P_1)) = 4$. This point of index 4 can be in the same fiber with 4, 2 or none

Weierstrass points. So we get cases 3, 4, and 5 respectively. A point of index 3 is a Weierstrass point which can be in the fiber which has 4 or 2 Weierstrass points. So cases 6 and 7.

III) If P_1 and P_2 are Weierstrass points then they can be only in the fiber with 6 Weierstrass point so case 1. If they are not then we have a point of index 4 which can be in the fiber with all Weierstrass points or with none. Therefore, cases 2 and 3. The point of index 3 is a Weierstrass point so it can be in the fiber where all the Weierstrass points are, so case 4. This completes the proof.

□

1.3 Maximal Coverings $\varphi : C \longrightarrow E$.

Let $\varphi_1 : C \longrightarrow E_1$ be a covering of degree n from a curve of genus 2 to an elliptic curve. The covering $\varphi_1 : C \longrightarrow E_1$ is called a **maximal covering** if it does not factor nontrivialy. A map of algebraic curves $f : X \to Y$ induces maps between their Jacobians $f^* : J_Y \to J_X$ and $f_* : J_X \to J_Y$. When f is maximal then f^* is injective and $\ker(f_*)$ is connected, see [19] (p. 158) for details.

Let $\varphi_1 : C \longrightarrow E_1$ be a covering as above which is maximal. Then $\varphi_1^* : E_1 \to J_C$ is injective and the kernel of $\varphi_{1,*} : J_C \to E_1$ is an elliptic curve which we denote by E_2 (see [6] or [12]). For a fixed Weierstrass point $P \in C$, we can embed C to its Jacobian via

$$i_P : C \longrightarrow J_C$$

$$x \to [(x) - (P)]$$

Let $g : E_2 \to J_C$ be the natural embedding of E_2 in J_C, then there exists $g_* : J_C \to E_2$. Define $\varphi_2 = g_* \circ i_P : C \to E_2$. So we have the following exact sequence

$$0 \to E_2 \xrightarrow{g} J_C \xrightarrow{\varphi_1^*} E_1 \to 0$$

The dual sequence is also exact (see [6])

$$0 \to E_1 \xrightarrow{\varphi_1^*} J_C \xrightarrow{g_*} E_2 \to 0$$

If $deg(\varphi_1)$ is an odd number then the maximal covering $\varphi_2 : C \to E_2$ is unique (up to isomorphism of elliptic curves), see Kuhn [12]. If the cover $\varphi_1 : C \longrightarrow E_1$ is given, and therefore ϕ_1, we want to determine $\varphi_2 : C \longrightarrow E_2$ and ϕ_2. The study of the relation between the ramification structures of ϕ_1 and ϕ_2 provides information in this direction. The following lemma (see [6], p. 160) answers this question for the set of Weierstrass points $W = \{P_1, \ldots, P_6\}$ of C when the degree of the cover is odd.

Let $\varphi_i : C \longrightarrow E_i$, $i = 1, 2$, be maximal of odd degree n. Let $\mathcal{O}_i \in E_i[2]$ be the points which has three Weierstrass points in its fiber. Then we have the following:

Lemma 4.5 (Frey-Kani). *The map $\varphi_2 : C \to E_2$ is a maximal covering of degree n. The sets $\varphi_1^{-1}(\mathcal{O}_1) \cap W$ and $\varphi_2^{-1}(\mathcal{O}_2) \cap W$ form a disjoint union of W.*

When n is even the ramification of φ is more precise.

Lemma 4.6. *Let $\varphi : C \longrightarrow E$ is maximal of even degree n, and $Q \in E[2]$. Then $\varphi^{-1}(Q)$ has either none or two Weierstrass points.*

Proof. If there are no Weierstrass points in $\varphi^{-1}(Q)$ there is nothing to prove. Suppose there is one, from lemma 3.2 we know there are at least 2, say P_1, P_2. We embed $C \to J_C$ via $x \longrightarrow [(x) - (P_1)]$ and $E \longrightarrow J_E$ via $x \longrightarrow [(x) - (Q)]$.

$$\begin{array}{ccc} C & \xrightarrow{i_{P_1}} & J_C \\ \varphi \downarrow & & \downarrow \varphi_* \\ E & \xrightarrow{i_Q} & J_E \end{array}$$

Then $\varphi_*[(x) - (P_1)] = [(\varphi(x)) - (Q)]$.

Also, $\varphi_*\varphi^* = [n]$ is the multiplication by n in E. Since $2|n$ then $E[2]$ is a subgroup of $E[n]$. So $\varphi^*(E[2]) = ker(\varphi_*|_{J[2]})$, we call this group H. Suppose $P_3 \in \varphi^{-1}(Q)$. Then $\varphi_*(i_{P_1}(P_3)) = \mathcal{O}_E$, so $(P_1, P_3) \in H$, where the unordered pair (P_i, P_j) denotes the point $[(P_i) - (P_j)]$ of order 2 in J_C. By addition of points of order 2 in J_C, $(P_2, P_3) \in H$. So $H = \{0_J, (P_1, P_2), (P_1, P_3), (P_2, P_3)\}$ can't have any other

points, therefore $\varepsilon^{-1}(Q)$ has three Weierstrass points, which contradicts theorem 4.4. Thus, there are only two Weierstrass points in $\varepsilon^{-1}(Q)$.

□

The above lemma says that if ε is maximal of even degree then the corresponding Frey-Kani covering can have only type I ramification, see theorem 4.3.

CHAPTER 5
GENUS 2 FIELDS WITH DEGREE 3 ELLIPTIC SUBFIELDS

5.1 Introduction

In this chapter we study genus two curves defined over a field k, $k = \bar{k}$, of characteristic 0, whose function fields have a degree 3 elliptic subfield. Such curves were studied during the 19th century from Hermite, Goursat, Burkhardt, Brioschi, and Bolza, see Krazer [10] (p. 179).

We show that every such curve is in the form

$$Y^2 = (X^3 + aX^2 + bX + 1)(4X^3 + b^2X^2 + 2bX + 1) = F(X)G(X)$$

for $a, b \in k$.

Let $\mathcal{L}_3$ denote the locus of genus 2 fields with $\epsilon_3(K) > 1$. So $\mathcal{L}_3$ is parameterized by the pairs $(a, b) \in k^2$. We define invariants of two cubics F and G as

$$r_1(F, G) = \frac{H^3(F, G)}{R(F, G)}, \quad r_2(F, G) = \frac{H^4(F, G)}{D(F) \cdot D(G)}$$

where $R(F, G)$ is the resultant of the two cubics, $D(F)$ and $D(G)$ are the respective discriminants, and $H(F, G)$ the binary invariant of two cubics. The invariants r_1, r_2 give a birational parameterization of $\mathcal{L}_3$. This parameterization of $\mathcal{L}_3$ factors through ramified Galois coverings of degree 3 (resp. 2)

$$k^2 \to k^2 \to k^2$$

$$(a, b) \to (u, v) \to (r_1, r_2)$$

where $ab = u$ and $b^3 = v$. The equation of $\mathcal{L}_3$ is computed in terms of the absolute invariants and is displayed in the appendix.

In section four we show that if $\mathcal{C} \in \mathcal{L}_3$ then $Aut(\mathcal{C})$ is isomorphic to $\mathbb{Z}_2$, V_4, D_4 or D_6. Moreover, there are exactly six genus 2 curves with automorphism group D_4 or D_6.

In section 5 we determine the j-invariants of the elliptic subfields in terms of the parameters u and v. The involution $\nu \in Gal(k(u,v)/k(r_1,r_2))$ permutes these elliptic subfields. If one of the elliptic subfields, say E_2 is of degenerate type, then

$$j(E_1) = \frac{(j(E_2) - 432)^3}{729 j(E_2)}$$

5.2 Genus Two Fields With Degree 3 Elliptic Subfields

Let K be a genus 2 function field and J_2, J_4, J_6, J_{10} its classical invariants invariants as in chapter 3. We use another invariant J_{48} as in appendix (A.3). Then we have the following theorem which will be proved in section 5.

Theorem 5.1. *Let K be a genus 2 field and $e_3(K)$ the number of $Aut(K)$-classes of elliptic subfields of K of degree 3. Suppose $e_3(K) \geq 1$. Then the classical invariants of K satisfy the equation*

$$C_8 J_{10}^8 + C_7 J_{10}^7 + C_6 J_{10}^6 + C_5 J_{10}^5 + C_4 J_{10}^4 + C_3 J_{10}^3 + C_2 J_{10}^2 + C_1 J_{10} + C_0 = 0 \qquad (5.1)$$

where $C_0, \ldots, C_8$ are displayed in the appendix (A.1). If additionally $J_2 \neq 0$ and $J_{48} \neq 0$, then $e_3(K) \leq 2$.

Remark 5.2. The cases $e_3(K) = 4, 8$ occur for a finite (non-zero) number of cases and $e_3(K) = 1$ occurs for a 1-dimensional family of genus 2 curves, see section 5.

Lemma 5.3. *Let K be a genus 2 field and E an elliptic subfield of degree 3.*

i) Then $K = k(X, Y)$ such that

$$Y^2 = (4X^3 + b^2X^2 - 2bX - 1)(X^3 + aX^2 + bX + 1) \qquad (5.2)$$

for $a, b \in k$ such that

$$(4a^3 + 27 - 18ab - a^2b^2 + 4b^3)(b^3 - 27) = 0 \qquad (5.3)$$

The roots of the first (resp. second) cubic correspond to $W^{(1)}(K,E)$, (resp. $W^{(2)}(K,E)$) in the coordinates X,Y, (see theorem 4.3).

ii) $E = k(U,V)$ where

$$U = \frac{X^2}{X^3 + aX^2 + bX + 1}$$

and

$$V^2 = U^3 + 2\frac{ab^2 - 6a^2 + 9b}{R}U^2 + \frac{12a - b^2}{R}U - \frac{4}{R} \tag{5.4}$$

where $R = 4a^3 + 27 - 18ab - a^2b^2 + 4b^3 \neq 0$.

iii) Define

$$u := ab, \quad v := b^3$$

Let K' be a genus 2 field and $E' \subset K'$ a degree 3 elliptic subfield. Let a', b' be the associated parameters as above and $u' := a'b'$, $v = (b')^3$. Then, there is a k-isomorphism $K \to K'$ mapping $E \to E'$ if and only if exists a third root of unity $\xi \in k$ with $a' = \xi a$ and $b' = \xi^2 b$. If $b = 0$ then such ξ exists if and only if $v = v'$ and $u = u'$.

iv) The classical invariants of K satisfy equation (5.1).

Proof. Let $k(X)$ be the degree 2 subfield of genus 0 of K. Let $X = w_1, \ldots, w_6$ be the Weierstrass points of K and $W^{(1)} = \{w_1, w_2, w_3\}$. Let $k(U) = k(X) \cap E$, where $U = \phi(X) \in k(X)$. The Weierstrass points lie over 4 places $U = q_i$, $i = 1, \ldots, 4$, see 1.3. We can choose the labeling so that w_i lies over q_i, for $i = 1, 2, 3$. Then w_4, w_5, w_6 lie over q_4. The extension $k(X)/k(U)$ is ramified over 4 places, three of which are q_i, $i = 1, 2, 3$. We choose the coordinate U such that the fourth place is $U = 0$ and $q_4 = \infty$. We fix the coordinate X, up to multiplication by a third root of unity, by the conditions that 0 (resp. ∞) is the point of ramification index 2 (resp. unramified) over 0 and $w_4 w_5 w_6 = -1$. In the following figure bullets (resp. circles) represent points of ramification index 1 (resp. 2).

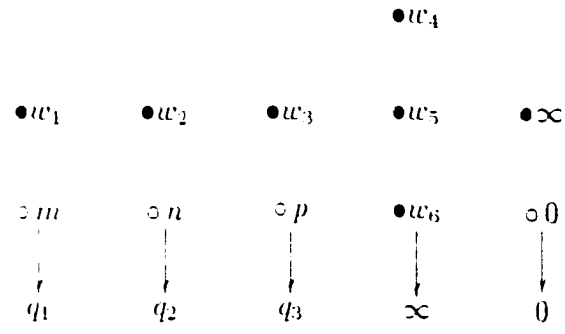

Figure 5.1: Ramification of ϕ_1

Let $a := -w_1 - w_3 - w_5$ and $b := w_1w_3 + w_1w_5 + w_3w_5$. Thus, $U = \phi(X) = l\frac{X^3}{X^3 + aX^2 + bX + 1}$, where l is a nonzero constant. We can make $l = 1$ by replacing U by $l^{-1}U$. Now the coordinate U is uniquely determined. Then,

$$U = \phi(X) = \frac{X^3}{X^3 + aX^2 + bX + 1} \tag{5.5}$$

The derivative of $\phi(X)$ is

$$\phi'(X) = -\frac{X(X^3 - bX - 2c)}{(X^3 + aX^2 + bX + c)^2}$$

Taking the resultant of the numerator of $\phi'(X)$ and $\frac{\phi(X)-\phi(Z)}{X-Z}$ we get

$$4Z^3 + b^2Z^2 + 2bZ + 1 = (Z - w_1)(Z - w_2)(Z - w_3) \tag{5.6}$$

Thus, K has equation

$$V^2 = (X^3 + aX^2 + bX + 1)(4X^3 + b^2X^2 + 2bX + 1) \tag{5.7}$$

Because $w_1, \ldots, w_6$ are all distinct, the discriminant of the sextic is not 0. So

$$(4a^3 + 27 - 18ab - a^2b^2 + 4b^3)^2(16b^3 - 432) \neq 0 \tag{5.8}$$

ii) Let $R = 4a^3 + 27 - 18ab - a^2b^2 + 4b^3$, then from part i) $R \neq 0$. We have

$$(U - q_1)(U - q_2)(U - q_3) = U^3 + 2\frac{ab^2 - 6a^2 + 9b}{R}U^2 + \frac{12a - b^2}{R}U - \frac{4}{R}$$

which we compute by taking the resultant with respect to Z of (5.6) and

$$U(Z^3 + aZ^2 + bZ + 1) - Z^2 = 0$$

By theorem 1.3, $E = k(U, V)$ where

$$V^2 = U^3 + 2\frac{ab^2 - 6a^2 - 9b}{R}U^2 + \frac{12a - b^2}{R}U - \frac{4}{R} \tag{5.9}$$

iii) The "if" part is clear. For the "only if" part we may assume $K = K'$ and $E = E'$. Then the claim follows from the uniqueness of the coordinates U and X, up to multiplication by a third root of unity.

iv) We denote by J_2, J_4, J_6, and J_{10} the classical invariants of the sextic in 5.2 defining K. Then we have:

$$\begin{aligned}
J_2 &= -2(3c^2 + 4a^2 + 12ac + 252a - 54c - 405)\\
J_4 &= \frac{1}{c}(-66a^3c - 24a^4 + 14580c - 36c^3 + 9a^2c^2 + 1188a^3 + 945c^2 - 8424ac\\
&\quad - 138ac^2 + a^4c + 297a^2c)\\
J_6 &= \frac{1}{c^2}(-1353996a^2c^2 + 1464a^3c^2 - 18756a^4c^2 + 3669786ac^2 - 4032c^4\\
&\quad - 315252c^3a - 75024c^3a^2 - 144a^6 - 40a^6c - 622323c^3 - 2821230c^2 + 3186c^5\\
&\quad - 204a^3c^4 + 2a^4c^4 + 564c^5a + 18c^5a^2 - 8a^5c^3 - 72c^6 + 4280a^3c^3 + 495a^4c^3\\
&\quad - 1038c^4a^2 + 106a^5c^2 + 160704a^4c - 104004a^3c + 1476a^5c + 2a^6c^2 - 33480c^4a)\\
J_{10} &= -16(c - 27)\frac{(27c^3 + 4a^9 - c^3a^2 + 4c^4 - 18c^3a)^3}{c^9}
\end{aligned} \tag{5.10}$$

One checks that J_2, J_4, J_6, and J_{10} satisfy equation (5.1). We will explain in the next section how we obtained the equation (5.1).

□

Let

$$F(X) := X^3 + aX^2 + bX + 1$$

$$G(X) := 4X^3 + b^2X^2 + 2bX + 1$$

Denote by $R = 4a^3 + 27 - 18ab - a^2b^2 + 4b^3$ the resultant of F and G. Then we have the following:

Lemma 5.4. *Let $a, b \in k$ satisfy equation (5.3). Then equation (5.2) defines a genus 2 field $K = k(X, Y)$. It has elliptic subfields of degree 3, $E_i = k(U_i, V_i)$, $i = 1, 2$, where U_i and V_i are as follows:*

$$U_1 = \frac{X^2}{F(X)}, \quad V_1 = Y\frac{X^3 - bX - 2}{F(X)^2}$$

$$U_2 = \begin{cases} \dfrac{(X-s)^2(X-t)}{G(X)} & if \quad b(b^3 - 4ba + 9) \neq 0 \\ \dfrac{(3X-a)}{3(4X^3+1)} & if \quad b = 0 \\ \dfrac{(bX-3)^2}{b^2G(X)} & if \quad (b^3 - 4ba + 9) = 0 \end{cases} \tag{5.11}$$

where

$$s = -\frac{3}{b}, \quad t = \frac{3a - b^2}{b^3 - 4ab + 9}$$

$$V_2 = \begin{cases} \dfrac{\sqrt{27 - b^3}Y}{G(X)^2}((4ab - 8 - b^3)X^3 - (b^2 - 4ab)X^2 + bX + 1) & if \quad b(b^3 - 4ba + 9) \neq 0 \\ Y\dfrac{8X^3 - 4aX^2 - 1}{(4X^3+1)^2} & if \quad b = 0 \\ \dfrac{8}{b}\sqrt{b}\dfrac{Y}{G(X)}(bX^3 + 9X^2 + b^2X + b) & if \quad (b^3 - 4ba + 9) = 0 \end{cases} \tag{5.12}$$

Proof. If a, b satisfy equation (5.3) then the sextic

$$(X^3 - aX^2 - bX - 1)(4X^3 - b^2X^2 + 2bX + 1)$$

has discriminant

$$D = (4a^3 + 27 - 18ab - a^2b^2 + 4b^3)^2(b^3 - 27) \neq 0$$

So there exists a genus 2 function field K given by equation (5.2).

Let $U_1 = \frac{X^2}{F(X)}$ and $V_1 = Y\frac{X^3-bX-2}{F(X)^2}$. Then U_1 and V_1 satisfy the equation

$$V_1^2 = RU_1^3 + 2(ab^2 - 6a^2 + 9b)U_1^2 + 12a - b^2U_1 - 4$$

The discriminant with respect to U_1 of the right hand side cubic is $b^3 - 27 \neq 0$, see (5.3). Thus, $k(U_1, V_1)$ is an elliptic subfield of K.

Let $b(b^3 - 4ba + 9) \neq 0$. Then U_2 and V_2 satisfy the equation

$$V_2^2 = c_3U_2^3 + c_2U_2^2 + c_1U_2 + c_0$$

where c_i are as follows:

$$\begin{aligned}
c_3 &= b^6(b^3 - 4ba + 9)^3 \\
c_2 &= b^4(-27b^2 + ab^3 + 54a)(b^3 - 4ba + 9)^2 \\
c_1 &= b^2(b^3 - 4ba + 9)(b^7 - 18ab^5 + 189b^4 + 54a^2b^3 - 972ab^2 + 729b + 729a^2) \\
c_0 &= -(27b^3 - 9ba + 27)^3
\end{aligned} \tag{5.13}$$

The discriminant of the cubic is

$$-b^{12}(b^3 - 27)^6(b^3 - 4ab + 9)R \neq 0$$

see (5.3). Thus, $k(U_2, V_2)$ is an elliptic subfield of K.

Let $b = 0$, then the discriminant of the sextic which defines K is $-27(4a^3 + 27)^2 \neq 0$. Then U_2 and V_2 satisfy the equation

$$V_2^2 = 27U_2^3 + 18aU_2^2 + 3a^2U_2 - 1$$

The discriminant is $4a^3 + 27 \neq 0$. So, $k(U_2, V_2)$ is an elliptic subfield of K.

Let $b^2 - 4ab + 9 = 0$ and Then, U_2, V_2 satisfy the equation

$$V_2^2 = b^4U_2^3 - b^4(b^3 - 18)U_2^2 + (81 - 9b^3)U_2 - b$$

The discriminant of the right hand side cubic is $b(b^3 - 27) \neq 0$. So, $k(U_2, V_2)$ is an elliptic subfield of K. This completes the proof.

□

5.3 Function Field of $\mathcal{L}_4$

The absolute invariants i_1, i_2, and i_3 in terms of u, v are

$$
\begin{aligned}
i_1 &= \frac{144}{v(-405+252u+4u^2-54v-12uv+3v^2)^2}(1188u^3-8424uv+u^4v-24u^4 \\
&\quad +14580v-66u^3v+138uv^2+297u^2v+945v^2-36v^3+9u^2v^2) \\
i_2 &= -\frac{864}{v^2(-405+252u+4u^2-54v-12uv+3v^2)^3}(-81v^3u^4+2u^6v^2+234u^5v^2 \\
&\quad +3162402uv^2-21384v^3u+26676v^4-473121v^3-72u^6v-5832v^4u+14850v^3u^2 \\
&\quad -72v^3u^3+324v^4u^2-650268u^3v-5940u^3v^2-3346110v^2+432u^6-1350u^4v^2 \\
&\quad +136080u^4v-7020u^5v-307638u^2v^2 \\
i_3 &= -243\frac{(v-27)(4u^3-u^2v-18uv+4v^2+27v)^3}{v^3(-405+252u+4u^2-54v-12uv+3v^2)^5}
\end{aligned}
\tag{5.14}
$$

Let u, v be independent transcendentals over k and $i_1, i_2, i_3 \in k(u, v)$ be given by equations (5.14). Further elements $\bar{r}_1, \bar{r}_2 \in k(u, v)$ are defined below.

From the resultants of equations in 5.14 we determine that $[k(\bar{v}) : k(\bar{i}_1, \bar{i}_2)] = 16$, $[k(v) : k(\bar{i}_2, \bar{i}_3)] = 40$, and $[k(\bar{v}) : k(\bar{i}_1, \bar{i}_3)] = 26$. We also can show that $\bar{u} \in k(\bar{i}_1, \bar{i}_2, \bar{i}_3, \bar{v})$, the expression is large and we display it on the appendix, see (A.4). Thus, $[k(u, v) : k(\bar{i}_1, \bar{i}_2, \bar{i}_3)] \leq 2$, see figure 5.2.

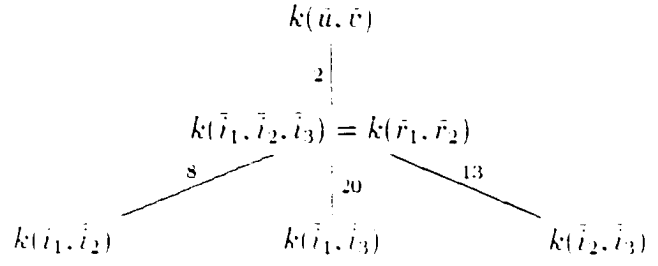

Figure 5.2:

Computing the equation (5.1) directly from the 5.14 exceeds available computer power. We use additional invariants $\bar{r}_1, \bar{r}_2$ to overcome this problem.

5.3.1 Invariants of Two Cubics

We define the following invariants of two cubic polynomials. For $F(X) = a_3X^3 + a_2X^2 + a_1X + a_0$ and $G(X) = b_3X^3 + b_2X^2 + b_1X + b_0$ define

$$H(F,G) := a_3b_0 - \frac{1}{3}a_2b_1 + \frac{1}{3}a_1b_2 - a_0b_3$$

We denote by $R(F,G)$ the resultant of F and G and by $D(F)$ the discriminant of F. Also,

$$r_1(F,G) = \frac{H(F,G)^3}{R(F,G)}, \quad r_2(F,G) = \frac{H(F,G)^4}{D(F)D(G)}$$

Remark 5.5. Note that $D(FG) = D(F) \cdot D(G) \cdot R^2(F,G)$.

For

$$F(X) = X^3 + aX^2 + bX + 1$$

$$G(X) = 4X^3 + b^2X^2 + 2bX - 1$$

from lemma 5.3 we have

$$\begin{aligned} r_1(F,G) &= 27\frac{v(v-9-2u)^3}{4v^2 - 18uv + 27v - u^2v + 4u^3} \\ r_2(F,G) &= -1296\frac{v(v-9-2u)^4}{(v-27)(4v^2 - 18uv + 27v - u^2v + 4u^3)} \end{aligned} \tag{5.15}$$

Remark 5.6. Note that r_1, r_2 are defined for any u, v by (5.3).

Taking the resultants from the above equations we get the following equations for u and v over $k(r_1, r_2)$:

$$\begin{aligned} &65536r_1r_2^3u^2 + (42467328\bar{r}_2^4 + 21233664\bar{r}_2^4\bar{r}_1 + 480\bar{r}_2\bar{r}_1^4 + 2\bar{r}_1^5 + 41472\bar{r}_2^2\bar{r}_1^3 \\ &+1548288\bar{r}_2^3\bar{r}_1^2 - 294912\bar{r}_2^3\bar{r}_1)u - 382205952\bar{r}_2^4 + 238878720\bar{r}_2^4\bar{r}_1 - 2654208\bar{r}_2^3\bar{r}_1 \\ &+13934592\bar{r}_2^3\bar{r}_1^2 + 285696\bar{r}_2^2\bar{r}_1^3 + 2400\bar{r}_2\bar{r}_1^4 + 7\bar{r}_1^5 = 0 \end{aligned} \tag{5.16}$$

$$\begin{aligned} &16384v^2\bar{r}_2^3 + (221184r_2^3\bar{r}_1 - r_1^4 + 11520r_2^2r_1^2 - 442368r_2^3 + 192r_2r_1^3)v \\ &-5971968\bar{r}_2^3\bar{r}_1 - 864\bar{r}_2\bar{r}_1^3 - 124416\bar{r}_2^2\bar{r}_1^2 - 2\bar{r}_1^4 = 0 \end{aligned} \tag{5.17}$$

In equation (5.16) express $\bar{r}_1$ and $\bar{r}_2$ in terms of $\bar{u}$ and $\bar{v}$. Roots of this equation are $\bar{u}$ and $\nu(\bar{u})$ where,

$$\nu(\bar{u}) = \frac{(\bar{v}-3\bar{u})(324\bar{u}^2+15\bar{u}^2\bar{v}-378\bar{u}\bar{v}-4\bar{u}\bar{v}^2+243\bar{v}+72\bar{v}^2)}{(\bar{v}-27)(4\bar{u}^3+27\bar{v}-18\bar{u}\bar{v}-\bar{u}^2\bar{v}+4\bar{v}^2)} \tag{5.18}$$

Similarly for v we get

$$\nu(v) = -\frac{4(v-3u)^3}{4u^3+27v-18uv-u^2v+4v^2} \tag{5.19}$$

Define a ring homomorphism

$$\nu : k[\bar{u},\bar{v}] \to k(u,v)$$

$$u \to \nu(u)$$

$$v \to \nu(v)$$

Then, we compute $\nu^2 = 1$. Thus, ν extends to an involutory automorphism of $k(\bar{u},\bar{v})$ which we again denote by ν. Since,

$$\tau : k(u,v) \to k(u,v)$$

$$u \to u$$

$$\bar{v} \to \nu(\bar{v})$$

is not involutory, then $[k(\bar{u},\bar{v}) : k(\bar{r}_1,\bar{r}_2)] = 2$ and $Gal_{k(u,v)/k(r_1,r_2)} = \langle\nu\rangle$.

Lemma 5.7. *The fields $k(\bar{i}_1,\bar{i}_2,\bar{i}_3)$ and $k(\bar{r}_1,\bar{r}_2)$ are the same. Moreover:*

$$\begin{aligned}
\bar{i}_1 &= \frac{9(13824\bar{r}_1^3\bar{r}_2^2+442368\bar{r}_1^2\bar{r}_2^3+5308416\bar{r}_1\bar{r}_2^4+192\bar{r}_1^4\bar{r}_2+\bar{r}_1^5+786432\bar{r}_1\bar{r}_2^3+9437184\bar{r}_2^4)}{\bar{r}_1(-1152\bar{r}_2^2+96\bar{r}_2\bar{r}_1+\bar{r}_1^2)^2} \\
\bar{i}_2 &= \frac{27}{8\bar{r}_1^2(-1152\bar{r}_2^2+96\bar{r}_2\bar{r}_1+\bar{r}_1^2)^3}(+7962624\bar{r}_1^4\bar{r}_2^4-4076863488\bar{r}_1^2\bar{r}_2^5+34560\bar{r}_1^6\bar{r}_2^2 \\
&\quad +12230590464\bar{r}_1^2\bar{r}_2^6+32614907904\bar{r}_1\bar{r}_2^6+14495514624\bar{r}_2^6+288\bar{r}_1^7\bar{r}_2+2211840\bar{r}_1^5\bar{r}_2^3 \\
&\quad +\bar{r}_1^8-21233664\bar{r}_1^3\bar{r}_2^4+1528823808\bar{r}_1^3\bar{r}_2^5-2359296\bar{r}_1^4\bar{r}_2^3) \\
\bar{i}_3 &= -521838526464\frac{\bar{r}_2^9}{\bar{r}_1^2(-1152\bar{r}_2^2+96\bar{r}_2\bar{r}_1+\bar{r}_1^2)^5}
\end{aligned} \tag{5.20}$$

Proof. It can be checked easily that ν fixes $\bar{i}_1, \bar{i}_2, \bar{i}_3$. So $\bar{i}_1, \bar{i}_2, \bar{i}_3 \in k(\bar{r}_1, \bar{r}_2)$. Since $[k(u,v) : k(\bar{r}_1, \bar{r}_2)] = 2$ and $[k(\bar{u}, \bar{v}) : k(\bar{i}_1, \bar{i}_2, \bar{i}_3)] \leq 2$, then $k(\bar{i}_1, \bar{i}_2, \bar{i}_3) = k(\bar{r}_1, \bar{r}_2)$.

To find $\bar{i}_1$ we eliminate $\bar{u}$ and $\bar{v}$ from the system of equations (5.14) and (5.15). In the same way we find $\bar{i}_2$ and $\bar{i}_3$. One can check the correctness by substituting in terms of $\bar{r}$ and $\bar{s}$. This completes the proof

□

Remark 5.8. To find equation (5.1) we eliminate $\bar{r}_1$ and $\bar{r}_2$ from the three equations of the above lemma. This equation has degree 8, 13, and 20 in $\bar{i}_1, \bar{i}_2, \bar{i}_3$ respectively.

5.4 Proof of Theorem 5.1

The map

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

generically has degree 2, by previous section. Denote the minors of the Jacobian matrix of θ by $M_1(u,v), M_2(u,v), M_3(u,v)$. The system

$$\begin{cases} M_1(u,v) = 0 \\ M_2(u,v) = 0 \\ M_3(u,v) = 0 \end{cases} \tag{5.21}$$

has solutions

$$8v^3 + 27v^2 - 54uv^2 - u^2v^2 + 108u^2v + 4u^3v - 108u^3 = 0 \tag{5.22}$$

and 7 further solutions which we display in the following table together with the corresponding values (i_1, i_2, i_3) and properties of the corresponding genus 2 field K.

Assume that equation (5.22) holds for some $(u,v) \in k^2$. Then the corresponding quantities J_i, $i = 1, 2, 3, 5$ from (5.10) satisfy the equation

$$F(J_2, J_4, J_6, J_{10}) = 0 \tag{5.23}$$

(a, c)	(i_1, i_2, i_3)	$Aut(K)$	$\epsilon_3(K)$
$(-\frac{7}{2}, 2)$	$J_{10} = 0$. no associated genus 2 field K		
$(-\frac{775}{8}, \frac{125}{96})$, $(\frac{25}{2}, \frac{250}{9})$	$-\frac{8619}{20}, -\frac{1240029}{200}, \frac{531441}{100000}$	D_4	2
$(27 - \frac{77}{2}\sqrt{-1}, 23 - \frac{77}{9}\sqrt{-1})$, $(27 + \frac{77}{2}\sqrt{-1}, 23 + \frac{77}{9}\sqrt{-1})$	$\frac{729}{2116}, \frac{1240029}{97336}, \frac{531441}{13181630464}$	D_4	2
$(-15 + \frac{45}{8}\sqrt{5}, \frac{45}{2} + \frac{45}{6}\sqrt{5})$, $(-15 - \frac{45}{8}\sqrt{5}, \frac{45}{2} - \frac{45}{6}\sqrt{5})$	$81, -\frac{5103}{25}, -\frac{729}{12500}$	D_6	2

Table 5.1:

where $F(J_2, J_4, J_6, J_{10})$ is displayed in the appendix, see (A.3). This is obtained by taking the resultants of equations (5.14) and (5.22). We define $J_{48} := F(J_2, J_4, J_6, J_{10})$. By previous section θ is generically a covering of degree 2. So exists a Zariski open subset $\mathcal{U}$ of k^2 with the following properties: Firstly, θ is defined everywhere on $\mathcal{U}$ and is a covering of degree 2 from $\mathcal{U}$ to $\theta(\mathcal{U})$. Further, if $\mathfrak{u} \in \mathcal{U}$ then all $\mathfrak{u}' \in k^2$ with θ defined at $\mathfrak{u}'$ and $\theta(\mathfrak{u}') = \theta(\mathfrak{u})$ also lie in $\mathcal{U}$. Suppose $\underline{i} \in k^3$ such that $|\theta^{-1}(\underline{i})| > 2$ and $det(Jac(\theta))$ does not vanish at any point of $\theta^{-1}(\underline{i})$. Then by implicit function theorem, there is an open ball B around each element of $\theta^{-1}(\underline{i})$ such that each point in $\theta(B)$ has > 2 inverse images under θ. But B has to intersect the Zariski open set $\mathcal{U}$. This is a contradiction. Thus, if $\underline{i} \in k^3$ and $|\theta^{-1}(\underline{i})| > 2$, then $det(Jac(\theta)) = 0$ at some point of $\theta^{-1}(\underline{i})$ and so J_{48} vanishes.

Let $\epsilon_3(K) > 1$ and $J_2 \neq 0$, $J_{48} \neq 0$. Then i_1, i_2, i_3 are defined and by previous paragraph $|\theta^{-1}(i_1, i_2, i_3)| \leq 2$. Thus, by lemma 5.3 part iii) $\epsilon_3(K) \leq 2$. This completes the proof of theorem 5.1.

5.5 Exceptional Cases for $J_2 = 0$

At present we do not yet have a full description of all possible values of $\epsilon_3(K)$. This will be done later. We consider the case when $J_2 = 0$. Thus,

$$J_2 = \frac{2}{3}(3c - 6a + 2a\sqrt{6} - 27 - 18\sqrt{6})(3c - 27 + 18\sqrt{6} - 6a - 2a\sqrt{6}) = 0$$

As for $n = 2$ we define the invariants

$$a_1 := \frac{J_4 \cdot J_6}{J_{10}}, \quad a_2 := \frac{J_6 \cdot J_{10}}{J_4^4} \tag{5.24}$$

for $J_4 \neq 0$ and $J_6 \neq 0$. These invariants determine genus two curves with $J_2 = 0$, up to isomorphism, see [13] or [17].

If $a := -\frac{1}{2}(3 + \sqrt{6})(-c + 9 + 6\sqrt{6})$ then

$$\begin{aligned} a_1 &= \frac{27 - 2\sqrt{6} - 5a}{81(-3c + 26 + 14\sqrt{6})^3}(-3c^2 + 153c + 12\sqrt{6}c - 960 - 440\sqrt{6})(-c^4 + 18c^3 + \\ &\quad 6\sqrt{6}c^3 - 297c^2 - 82\sqrt{6}c^2 - 312c - 1668\sqrt{6}c - 35992 - 14688\sqrt{6}) \\ a_2 &= \frac{82\sqrt{6} + 51(-3c + 26 + 14\sqrt{6})^3}{64(c - 27)(-3c^2 + 153c + 12\sqrt{6}c - 960 - 440\sqrt{6})^4}(-c^4 + 18c^3 + 6\sqrt{6}c^3 \\ &\quad - 297c^2 - 82\sqrt{6}c^2 - 312c - 1668\sqrt{6}c - 35992 - 14688\sqrt{6}) \end{aligned} \tag{5.25}$$

Then we have the following equation for a_1 and a_2.

$$\begin{aligned} &46656a_1^5a_2^3 + 7558272a_1^4a_2^3 + 1259712\sqrt{6}a_1^4a_2^3 - 15552a_1^4a_2^2 \\ &- 12427478784a_1^3a_2^2 + 4917635712\sqrt{6}a_1^3a_2^2 + 1728a_1^3a_2 - 6562175316544480a_1^2a_2^2 \\ &+ 2675712090340480\sqrt{6}a_1^2a_2^2 - 18441250056a_1^2a_2 + 7435255688\sqrt{6}a_1^2a_2 \\ &- 64a_1^2 - 6334497449472117312a_1a_2^2 + 2585860435265558832\sqrt{6}a_1a_2^2 \\ &+ 2308332398389992a_2a_1 - 942372270878402a_2a_1\sqrt{6} - 60124442997580503077a_2^2 \\ &+ 24542953925776438057 2a_2^2\sqrt{6} = 0 \end{aligned} \tag{5.26}$$

We denote the singular points of the above curve by P_1, P_2, P_3, P_4. They are displayed in table 5.2. The inverse images of P_1, P_2, P_3, P_4 are given respectively by the following equations:

$$9c^4+(-693-27\sqrt{6})c^3+(15141+1749\sqrt{6})c^2+(-66414-33396\sqrt{6})c$$
$$-1368\sqrt{6}+3388=0$$
$$3c^4+(-153-33\sqrt{6})c^3+(3129-1219\sqrt{6})c^2+(-10854-11556\sqrt{6})c$$
$$+176904\sqrt{6}+450036=0$$
$$-2001395624058 0c^3+2896020ac^3-5152107547080c^3\sqrt{6}+1077048\sqrt{6}ac^3$$
$$-86467887015304 5c^2-366454809ac^2+2105362512251 64c^2\sqrt{6}-149670624ac^2\sqrt{6}$$
$$-12007884954657636c+1100419362 0ac-5403860658681804c\sqrt{6}+448583118 0ac\sqrt{6}$$
$$-8589455872606114 8-9538451348 4a+3396330063483 1272\sqrt{6}-389605603 76a\sqrt{6}$$
$$3170527721 28c^4=0$$
$$2001395624058 0c^3+2896020ac^3+5152107547080c^3\sqrt{6}+1077048\sqrt{6}ac^3$$
$$-86467887015304 5c^2-366454809ac^2+2105362512251 64c^2\sqrt{6}+149670624ac^2\sqrt{6}$$
$$+12007884954657636c+1100419362 0ac+5403860658681804c\sqrt{6}+448583118 0ac\sqrt{6}$$
$$-8589455872606114 8-9538451348 4a-3396330063483 1272\sqrt{6}-389605603 76a\sqrt{6}$$
$$-3170527721 28c^4=0 \tag{5.27}$$

where $a=\sqrt{152154604614 9129-62106209059 2456\sqrt{6}}$.

If $x:=\frac{1}{2}c-\frac{93}{2}-\frac{1}{2}\sqrt{6}(c-27)$ then

$$a_1=\frac{27(-5-2\sqrt{6})}{8(-3c+26+14\sqrt{6})^3}(-3c^2+153c+12\sqrt{6}c-960-440\sqrt{6})$$
$$(-c^4+18c^3+6\sqrt{6}c^3+297c^2-82\sqrt{6}c^2-312c-1668\sqrt{6}c-35992-14688\sqrt{6})$$
$$a_2=\frac{8(5-2\sqrt{6})}{9(c-27)(-3c^2-153c+12\sqrt{6}c-960-440\sqrt{6})^4}(-3c+26+14\sqrt{6})^3$$
$$(-c^4+18c^3+6\sqrt{6}c^3-297c^2-82\sqrt{6}c^2-312c-1668\sqrt{6}c-35992-14688\sqrt{6}) \tag{5.28}$$

Then we have the following equation for a_1 and a_2.

$$2308332398389 92a_2a_1+9423722708784 0a_2a_1\sqrt{6}-1242747878 4a_1^3a_2^2$$
$$-4917635712\sqrt{6}a_1^3a_2^2+1728a_1^3a_2-15552a_1^4a_2^2-6562175316544 80a_1^4a_2^3$$
$$-2675712090344 80\sqrt{6}a_1^4a_2^3+46656a_1^5a_2^3-64a_1^5-6012444299758 05030777a_2^5$$
$$-2454295392577643 80572a_2^5\sqrt{6}-1844125056a_1^5a_2-7435255 68\sqrt{6}a_1^5a_2$$
$$-6334497449472117312a_1a_2^5-2585860435265558832\sqrt{6}a_1a_2^5+7558272a_1^4a_2^3$$
$$-1259712\sqrt{6}a_1^4a_2^3=0 \tag{5.29}$$

We denote the singular points of the above curve by Q_1, Q_2, Q_3, Q_4. They are displayed in table 5.2. The inverse images of Q_1, Q_2, Q_3, Q_4 are given respectively by the following equations.

$$\begin{aligned}
&9c^4+(-693+27\sqrt{6})c^3+(15141-1749\sqrt{6})c^2+(-66414+33396\sqrt{6})c\\
&\qquad +1368\sqrt{6}+3388=0\\
&3c^4+(-153-33\sqrt{6})c^3+(3129+1219\sqrt{6})c^2+(-10854+11556\sqrt{6})c\\
&\qquad -176904\sqrt{6}+450036=0\\
&-5988973837943 2-24449865553848\sqrt{6}-442888\bar{\alpha}\sqrt{6}-1084792\bar{\alpha}+7357705605c^3\\
&-34560c^5\sqrt{6}+302844792 6c^3\sqrt{6}+54\sqrt{6}\bar{\alpha}c^3+135\bar{\alpha}c^3-2096640c^4\sqrt{6}-3749760c^4\\
&-14405345183 4c^2-18102981702 6c^2\sqrt{6}-3294\bar{\alpha}c^2\sqrt{6}-8046\bar{\alpha}c^2+238464c^5\\
&-3456c^6+892933253542 8c+364561306819 2c\sqrt{6}+161964\alpha c+66096\alpha c\sqrt{6}=0\\
&-24449865553848\sqrt{6}-5988973837943 2+1084792\alpha+442888\alpha\sqrt{6}+7357705605c^3\\
&+238464c^5+302844792 6c^3\sqrt{6}-54\sqrt{6}\alpha c^3-135\alpha c^3-2096640c^4\sqrt{6}-3749760c^4\\
&-18102981702 6c^2\sqrt{6}-14405345183 4c^2+3294\alpha c^2\sqrt{6}+8046\alpha c^2+34560c^5\sqrt{6}\\
&-3456c^6+892933253542 8c+364561306819 2c\sqrt{6}-161964\bar{\alpha}c-66096\bar{\alpha}c\sqrt{6}=0
\end{aligned} \tag{5.30}$$

where α is the conjugate of α.

If $J_2=J_4=0$ and $J_6\neq 0$ then there are 4 distinct pairs (a,c) as below.

$$\begin{aligned}
a&=\frac{3}{8}\frac{(11c^3-606c^2+3655c+42600)}{(15c^2-912c+10190)}\\
&3c^4-306c^3+9435c^2-76800c-80000=0
\end{aligned} \tag{5.31}$$

They determine exactly one genus 2 field K, see chapter 3 or [13]. In this case $c_{10}(K)=4$.

If $J_2=J_6=0$ then (a,c) are as below.

$$\begin{aligned}
a&=\frac{1}{4}\frac{(109c^5-2943c^4-30783c^3+419649c^2+10575604c+44691480)}{(99c^4-3237c^3-9518c^2+435378c+7125048)}\\
&c^8-36c^7+17220c^5+228713c^4-2064816c^3-52428240c^2-271536000c\\
&+1000000-486c^6=0
\end{aligned} \tag{5.32}$$

	(a_1, a_2)	ϵ_3	G
P_1	$a_1 = -\frac{77169}{8} + \frac{30759}{8}\sqrt{6}, a_2 \frac{13783592}{23149125} + \frac{5629912}{23149125}\sqrt{6})$	4	V_4
P_2	$a_1 = -\frac{650835}{8} + \frac{268785}{8}\sqrt{6}, a_2 = -\frac{2984}{20002028625} - \frac{144872}{60006085875}\sqrt{6})$	4	V_4
P_3	$a_1 = -\frac{77169}{8} + \frac{30759}{8}\sqrt{6}, a_2 \frac{13783592}{23149125} + \frac{5629912}{23149125}\sqrt{6})$	4	V_4
P_4	$a_1 = \frac{81512265}{1024} - \frac{8560473}{256}\sqrt{6} - \frac{3}{1024}\alpha,$		
	$a_2 = \frac{19357551512642635 16}{1630518619797} - \frac{26092676190366818 0}{5435062065 99}\sqrt{6} + \frac{9735715883008}{4891555859391}(\frac{81512265}{1024}$		
	$-\frac{8560473}{256}\sqrt{6} - \frac{3}{1024}\alpha)\sqrt{6} + \frac{23288611604}{1630518619797}\alpha$	4	V_4
Q_1	$a_1 = -\frac{77169}{8} - \frac{30759}{8}\sqrt{6}, a_2 = \frac{13783592}{23149125} - \frac{5629912}{23149125}\sqrt{6})$	4	V_4
Q_2	$a_1 = -\frac{650835}{8} - \frac{268785}{8}\sqrt{6}, a_2 = -\frac{2984}{20002028625} + \frac{144872}{60006085875}\sqrt{6})$	4	V_4
Q_3	$a_1 = \frac{81512265}{1024} + \frac{8560473}{256}\sqrt{6} + \frac{3}{1024}\alpha,$		
	$a_2 = \frac{19357551512642635 16}{1630518619797} - \frac{26092676190366818 0}{5435062065 99}\sqrt{6} - \frac{9735715883008}{4891555859391}(\frac{81512265}{1024}$		
	$+\frac{8560473}{256}\sqrt{6} - \frac{3}{1024}\alpha)\sqrt{6} - \frac{23288611604}{1630518619797}\alpha$	4	V_4
Q_4	$a_1 = \frac{81512265}{1024} + \frac{8560473}{256}\sqrt{6} - \frac{3}{1024}\alpha),$		
	$a_2 = \frac{19357551512642635 16}{1630518619797} + \frac{26092676190366818 0}{5435062065 99}\sqrt{6} - \frac{9735715883008}{4891555859391}(\frac{81512265}{1024}$		
	$+\frac{8560473}{256}\sqrt{6} - \frac{3}{1024}\alpha)\sqrt{6} + \frac{23288611604}{1630518619797}\alpha)$	4	V_4
$J_3 = 0$	$\frac{J_2^5}{J_{10}} = \frac{13015494042248103}{320} - \frac{35120352004646841}{640}\sqrt{6}$	4	V_4
$J_4 = 0$	$\frac{J_2^5}{J_5^2}$ is too large to display	8	V_4

Table 5.2: Singular points for $J_2 = 0$

The discriminant of the above polynomial is

$$D = -2^{62} \cdot 3^4 \cdot 5^8 \cdot 23^2 \cdot 43^4 \cdot 6459242937529^2$$

Thus, there are 8 distinct pairs (a, c) which determine exactly one genus 2 field, see chapter 3 or [13]. So, $\epsilon_3(K) = 8$.

5.6 j-invariants

We express the the j-invariants j_i of the elliptic subfields E_i of K, from lemma 5.4, in terms of a and c as follows:

$$j_1 = 16c\frac{(cu^2+216u^2-126cu-972u+12c^2+405c)^3}{(c-27)^3(4c^2+27c+4u^3-18cu-cu^2)^2} \tag{5.33}$$

$$j_2 = -256\frac{(u^2-3c)^3}{c(4c^2+27c+4u^3-18cu-cu^2)} \tag{5.34}$$

where $c = 0.27$.

Remark 5.9. The automorphism $\nu \in Gal_{k(u,c)/k(r_1,r_2)}$ permutes the elliptic subfields. One can easily check that:

$$\nu(j_1) = j_2$$

$$\nu(j_2) = j_1$$

Define T and N as follows:

$$\begin{aligned}
T = {} & \frac{1}{16777216r_2^3r_1^8}(171228266496 0r_2^3r_1^6 + 152882380 8r_2^4r_1^6 + 49941577728r_2^4r_1^5 \\
& - 3892838 4r_2^5r_1^5 - 258048r_2^6r_1^4 + 1238630 4r_2^6r_1^3 + 90173697372979 2r_2r_1^{10} \\
& + 96613171 2r_2^5r_1^4 + 16231265527136256r_1^{10} + 480r_2^8r_1 + 101376r_2^7r_1^2 + 47904776729395 2r_2r_1^8 \\
& + 72477573 12r_2^5r_1^8 + 78275778969 60r_2^2r_1^9 + 27052109211893 76r_1^9 + 6196832501 76r_2^3r_1^7 \\
& + 21611687369515 008r_1^{12} + 32462531054272512r_1^{11} + r_2^9 + 37572373905 408r_2^3r_1^7 \\
& + 14089640214528 00r_2r_1^9 + 45595641249792r_2^4r_1^8) \\
N = {} & -\frac{1}{68719476736r_1^{12}r_2^3}(8493465 6r_1^7 + 1179648r_1^4r_2 - 5308416r_1^4 - 442368r_1^3r_2 \\
& - 13824r_1^2r_2^2 - 192r_1r_2^3 - r_2^4)^3
\end{aligned} \tag{5.35}$$

Lemma 5.10. *The j-invariants of the elliptic subfields satisfy the following quadratic equations over* $k(r_1, r_2)$*:*

$$j^2 - Tj + N = 0 \tag{5.36}$$

Proof. Substitute j_1 and j_2 as in (5.33) in equation (5.36).

□

5.6.1 Isomorphic Elliptic Subfields

Suppose that $E_1 \cong E_2$. Then, $j_1 = j_2$ implies that

$$8c^3 + 27c^2 - 54uc^2 - u^2c^2 + 108u^2c + 4u^3c - 108u^3 = 0 \tag{5.37}$$

or

$$\begin{aligned} &324c^4u^2 - 5832c^4u + 37908c^4 - 314928c^3u - 81c^3u^4 + 255879c^3 + 30618c^3u^2 \\ &- 864c^3u^3 - 6377292uc^2 + 8503056c^2 - 324u^5c^2 + 2125764u^2c^2 - 215784u^3c^2 \\ &- 14580u^4c^2 + 16u^6c^2 + 78732u^3c + 8748u^5c - 864u^6c - 157464u^4c + 11664u^5 = 0 \end{aligned} \tag{5.38}$$

The former equation is the condition that $det(Jac(\theta)) = 0$ see (5.23). From equation 5.23 and equations 5.14 we can express u as a rational function in i_1, i_2, and c. This is displayed in Appendix B. Also, $[k(c) : k(i_1)] = 8$ and $[k(c) : k(i_2)] = 12$. Eliminating c we get a curve in i_1 and i_2 which has degree 8 and 12 respectively. Thus, $k(u, c) = k(i_1, i_2)$. Hence, $\epsilon_3(K) = 1$ for any K such that the associated u and c satisfy equation (5.23).

5.6.2 The Degenerate Case

We assume now that one of the extensions K/E_i from lemma 5.4 is degenerate, i.e. has only one branch point. The following lemma determines a relation between j_1 and j_2.

Lemma 5.11. *Suppose that K/E_2 has only one branch point. Then,*

$$729j_1j_2 - (j_2 - 432)^3 = 0$$

Proof. The hypothesis implies that $s = t$ in lemma 5.4. So $2b^3 - 9ab - 27 = 0$, i.e. $2c - 9u - 27 = 0$. Then,

$$j_1 = \frac{64}{729}\frac{(4c - 27)^3}{c}, \quad j_2 = 64c$$

Eliminating c we have:

$$729j_1j_2 - (j_2 - 432)^3 = 0$$

□

Making the substitution $T = -27j_1$ we get

$$j_1 = F_2(T) = \frac{(T+16)^3}{T}$$

where $F_2(T)$ is the Fricke polynomial of level 2.

If both K_{E_1} and K_{E_2} are degenerate then

$$\begin{cases} 729j_1j_2 - (j_1 - 432)^3 = 0 \\ 729j_1j_2 - (j_2 - 432)^3 = 0 \end{cases} \tag{5.39}$$

There are 7 solutions to the above system. Three of which give isomorphic elliptic curves

$$j_1 = j_2 = 1728, \quad j_1 = j_2 = \frac{1}{2}(297 \pm 81\sqrt{-15})$$

The other 4 solutions are given by:

$$\begin{cases} 729j_1j_2 - (j_1 - 432)^3 = 0 \\ j_1^2 - j_2^2 - 1296(j_1 - j_2) - j_1j_2 + 559872 = 0 \end{cases} \tag{5.40}$$

This corrects [10] where it is claimed there is only one solution $j_1 = j_2 = 1728$.

5.7 Intersection of $\mathcal{L}_2$ with $\mathcal{L}_4$

Theorem 5.12. *If $\#\mathrm{Aut}(\mathcal{C}) \geq 4$ then the automorphism group of $\mathcal{C}$ is one of the following: $\mathbb{Z}_2, V_4$, D_4, or D_6. Moreover: there are exactly 6 curves $\mathcal{C} \in \mathcal{L}_3$ with automorphism group D_4 and six curves $\mathcal{C} \in \mathcal{L}_3$ with automorphism group D_6. They are listed in tables 3 and 4 respectively.*

Proof. We denote by $G := \mathrm{Aut}(\mathcal{C})$. If $\mathcal{C}$ has no elliptic involutions then $G \cong \mathbb{Z}_2$ or $G \cong \mathbb{Z}_{10}$. If $G \cong \mathbb{Z}_{10}$, then $Y^2 = X^5 - X$, see 2.5. Thus, $J_2 = J_4 = J_6 = 0$, and $J_{10} = 3125$. They don't satisfy the equation (5.1). Then, the curve $Y^2 = X^6 - X$ has

no elliptic subcover of degree 3. If $\mathcal{C}$ has an elliptic involution. Then from theorem 4.3. we have the following cases:

i) $G \cong \mathbb{Z}_2 \times D_4$. $\mathcal{C}$ is isomorphic to $Y^2 = X^6 - 1$ Then.

$$J_2 = 240, J_4 = 1620, J_6 = 119880, J_{10} = 46656$$

and they don't satisfy equation of $\mathcal{L}_3$.

ii) $G \cong W_4$. $\mathcal{C}$ is isomorphic to $Y^2 = X^5 - X$. The corresponding absolute invariants are

$$J_2 = -40, J_4 = -80, J_6 = 320, J_{10} = -256$$

and they don't satisfy equation of $\mathcal{L}_3$.

iii) If $G \cong D_4$, then $\mathcal{C}$ is isomorphic to

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

for $\lambda \neq \pm 2$ see theorem 4.3. Igusa invariants are:

$$\begin{aligned} J_2 &= 16(\lambda^2 - 2\lambda + 16) \\ J_4 &= 4(\lambda^2 + 32\lambda + 76)(\lambda - 2)^2 \\ J_6 &= 8(3\lambda^4 + 70\lambda^3 + 460\lambda^2 + 1832\lambda + 3104)(\lambda - 2)^2 \\ J_{10} &= 64(\lambda - 2)^6(\lambda + 2)^2 \end{aligned} \tag{5.41}$$

Substituting in the equation of $\mathcal{L}_3$ we have the following values for λ.

$$\begin{aligned} &(\lambda^2 - 772\lambda - 1532)(4\lambda^2 - 12\lambda - 41)(\lambda^2 + 452\lambda - 124)(2\lambda + 5) \\ &(\lambda + 34)(\lambda^2 - 68\lambda - 124)(16\lambda^2 + 17\lambda + 226) = 0 \end{aligned} \tag{5.42}$$

We have the following cases:

a) If $\lambda = -\frac{5}{2}$ or $\lambda = -34$ then

$$t_1 = \frac{729}{2116}, t_2 = \frac{1240029}{97336}, t_3 = \frac{531441}{1318163046 4}$$

b) If $\lambda^2 - 772\lambda - 1532 = 0$ then

$$t_1 = \frac{4288}{1849}, t_2 = \frac{243712}{79507}, t_3 = \frac{64}{13230759 87}$$

c) If $\lambda^2 - 772\lambda - 1532 = 0$ or $\lambda = \frac{3}{2} - \frac{5}{2}\sqrt{2}$ then

$$i_1 = \frac{11715021}{5596820} + \frac{7020}{279841}\sqrt{2}, \quad i_2 = \frac{46539411219}{29607177800} + \frac{246294594}{148035889}\sqrt{2}$$

$$i_3 = \frac{44331236341524 9}{265129671767353600000} - \frac{1140762471381}{106051868706941 4400}\sqrt{2}$$

d) If $\lambda = -226 - 160\sqrt{2}$ or $\lambda = \frac{3}{2} + \frac{5}{2}\sqrt{2}$ then

$$i_1 = \frac{11715021}{5596820} - \frac{7020}{279841}\sqrt{2}, \quad i_2 = \frac{46539411219}{29607177800} - \frac{246294594}{148035889}\sqrt{2}$$

$$i_3 = \frac{44331236341524 9}{265129671767353600000} + \frac{1140762471381}{106051868706941 4400}\sqrt{2}$$

e) If $\lambda^2 - 68\lambda - 124 = 0$ then

$$i_1 = \frac{144}{49}, i_2 = \frac{3456}{8575}, i_3 = \frac{243}{52521875}$$

f) If $16\lambda^2 + 17\lambda + 226 = 0$ then

$$i_1 = -\frac{8019}{20}, i_2 = -\frac{1240029}{200}, i_3 = -\frac{531441}{10000}$$

Case	(i_1, i_2, i_3)	$e_3(K)$	$e_2(K)$	$Aut(K)$
a	$i_1 = \frac{729}{2116}, i_2 = \frac{1240029}{97336}, i_3 = \frac{531441}{131816304 64}$	2	2	D_4
b	$i_1 = \frac{1288}{1849}, i_2 = \frac{243712}{79507}, i_3 = \frac{64}{1323075987}$	2	2	D_4
c	$i_1 = \frac{11715021}{5596820} + \frac{7020}{279841}\sqrt{2}, i_2 = \frac{46539411219}{29607177800} + \frac{246294594}{148035889}\sqrt{2},$ $i_3 = \frac{44331236341524 9}{265129671767353600000} - \frac{1140762471381}{106051868706941 4400}\sqrt{2}$	2	2	D_4
d	$i_1 = \frac{11715021}{5596820} - \frac{7020}{279841}\sqrt{2}, i_2 = \frac{46539411219}{29607177800} - \frac{246294594}{148035889}\sqrt{2},$ $i_3 = \frac{44331236341524 9}{265129671767353600000} + \frac{1140762471381}{106051868706941 4400}\sqrt{2}$	2	2	D_4
e	$i_1 = \frac{144}{49}, i_2 = \frac{3456}{8575}, i_3 = \frac{243}{52521875}$	2	2	D_4
f	$i_1 = -\frac{8019}{20}, i_2 = -\frac{1240029}{200}, i_3 = -\frac{531441}{10000}$	2	2	D_4

Table 5.3: Curves of genus 2 with automorphism group D_4

Thus, there are exactly 6 genus 2 curves $\mathcal{C} \in \mathcal{L}_3$ with automorphism group D_4 which are displayed in Table 5.3.

v) If $G \cong D_6$ then $\mathcal{C}$ is isomorphic to a genus 2 curve in the form

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

for $\lambda \neq 0, 1$, see theorem 4.3.

$$\begin{aligned} J_2 &= 60(\lambda^2 - 38\lambda + 1) \\ J_4 &= 324\lambda(\lambda^2 + 7\lambda + 1) \\ J_6 &= 162\lambda(\lambda^4 - 58\lambda^3 - 858\lambda^2 - 58\lambda + 1) \\ J_{10} &= 729\lambda^2(\lambda - 1)^2 \end{aligned} \tag{5.43}$$

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

$$\begin{aligned} &(4\lambda - 1)(\lambda - 4)(15625\lambda^6 + 13131498\lambda^5 - 7690233\lambda^4 + 6970778\lambda^3 \\ &-7690233\lambda^2 + 13131498\lambda + 15625)(4\lambda^2 + 19\lambda + 4)(\lambda^2 - 18\lambda + 1) = 0 \end{aligned} \tag{5.44}$$

We have the following cases:

a) If $\lambda = 4$ or $\lambda = \frac{1}{4}$ then

$$i_1 = \frac{61}{5}, i_2 = -\frac{1088}{25}, i_3 = -\frac{1}{84375}$$

b) If $4\lambda^2 + 19\lambda + 4 = 0$ then,

$$i_1 = \frac{576}{361}, i_2 = \frac{60480}{6859}, i_3 = \frac{243}{2476099}$$

c) If $\lambda^2 - 18\lambda + 1 = 0$ then

$$i_1 = 81, i_2 = -\frac{5103}{25}, i_3 = -\frac{729}{12500}$$

The other values of λ are the solutions of the equation:

$$\begin{aligned} 15625\lambda^6 + 13131498\lambda^5 - 7690233\lambda^4 + 6970778\lambda^3 - 7690233\lambda^2 \\ +13131498\lambda + 15625 = 0 \end{aligned} \tag{5.45}$$

The above equation has the same coefficients for λ^j and λ^{6-j}. Hence, if λ is a root then $\frac{1}{\lambda}$ is also a root. We let $u := \lambda + \frac{1}{\lambda}$. Then, the above equation becomes

$$u^3 - \frac{13131498}{15625}u^2 - \frac{7737108}{15625}u - \frac{43444792}{15625} = 0$$

Solving for u we have three roots

$$u_1 = -\frac{504}{15625}\beta^{\frac{1}{3}} - \frac{20701097057466}{5579238276191265625}\beta^{\frac{2}{3}} + \frac{1767150}{35707124967624 1}\beta^{\frac{2}{3}}\sqrt{69} - \frac{4377166}{15625}$$

$$u_2 = \frac{252}{15625}\beta^{\frac{1}{3}} + \frac{1035054852873 3}{5579238276191265625}\beta^{\frac{2}{3}} - \frac{883575}{35707124967624 1}\beta^{\frac{2}{3}}\sqrt{69} - \frac{4377166}{15625}$$
$$- \frac{252}{15625}I\sqrt{3}\beta^{\frac{1}{3}} + \frac{1035054852873 3}{5579238276191265625}I\sqrt{3}\beta^{\frac{2}{3}} - \frac{883575}{35707124967624 1}I\sqrt{3}\beta^{\frac{2}{3}}\sqrt{69}$$

$$u_3 = \frac{252}{15625}\beta^{\frac{1}{3}} + \frac{1035054852873 3}{5579238276191265625}\beta^{\frac{2}{3}} - \frac{883575}{35707124967624 1}\beta^{\frac{2}{3}}\sqrt{69} - \frac{4377166}{15625}$$
$$- \frac{252}{15625}I\sqrt{3}\beta^{\frac{1}{3}} - \frac{1035054852873 3}{5579238276191265625}I\sqrt{3}\beta^{\frac{2}{3}} + \frac{883575}{35707124967624 1}I\sqrt{3}\beta^{\frac{2}{3}}\sqrt{69} \tag{5.46}$$

where $\beta = 65717768 4364 + 876562500\sqrt{69}$ and $I^2 = -1$.

	(i_1, i_2, i_3)	$e_3(K)$	$e_2(K)$	$Aut(K)$
a	$i_1 = \frac{64}{5}, i_2 = -\frac{1088}{25}, i_3 = -\frac{1}{84375}$	2	2	D_6
b	$i_1 = \frac{576}{361}, i_2 = \frac{60480}{6859}, i_3 = \frac{243}{2476099}$	2	2	D_6
c	$i_1 = 81, i_2 = -\frac{5103}{25}, i_3 = -\frac{729}{12500}$	2	2	D_6
d	$\delta_1, \delta_2, \delta_3$	2	2	D_6
e	ρ_1, ρ_2, ρ_3	2	2	D_6
f	η_1, η_2, η_3	2	2	D_6

Table 5.4: Curves of genus 2 with automorphism group D_6

To find λ we solve the equations $\lambda^2 - u_i\lambda + 1 = 0$, for $i = 1, 2, 3$. Each of these equations gives exactly one genus 2 curve.

d) The solutions of $\lambda^2 - u_1\lambda + 1 = 0$ give exactly one genus two curve with absolute invariants

$$i_1 = \delta_1, \quad i_2 = \delta_2, \quad i_3 = \delta_3$$

where δ_i, $i = 1, 2, 3$ are displayed in appendix (B.1).

e) The solutions of $\lambda^2 - u_2\lambda + 1 = 0$ give exactly one genus two curve with absolute invariants

$$i_1 = \rho_1, \quad i_2 = \rho_2, \quad i_3 = \rho_3$$

where ρ_i, $i = 1,2,3$ are displayed in appendix (B.2).

f) The solutions of $\lambda^2 - u_3\lambda + 1 = 0$ give exactly one genus two curve with absolute invariants

$$\iota_1 = \eta_1, \quad \iota_2 = \eta_2, \quad \iota_3 = \eta_3$$

where η_i, $i = 1,2,3$ are displayed in appendix (B.3).

All the cases are summarized in table 5.1. This completes the proof.

□

CHAPTER 6
GENUS 2 FIELDS WITH DEGREE 5 OR 7 ELLIPTIC SUBFIELDS

In this chapter we discuss briefly the spaces $\mathcal{L}_5$ and $\mathcal{L}_7$. Since the computations are quite long and the results very large for display, we treat only the cases when the covering has a point of ramification index 4.

6.1 Curves of Genus 2 with Degree 5 Elliptic Subfields, 4-cycle Case.

Notice that the case II. i) does not occur when $n = 5$. So we will consider only case II. iii). We will prove the following lemma:

Lemma 6.1. *Let $\varphi : C \to E_1$ be a covering of degree 5 such that the corresponding Frey-Kani cover is of ramification type II. iii) (theorem 4.3). Then the genus two curve can be given by*

$$Y^2 = x(x-1)(x-d)(x^3 - ux^2 + vx - w)$$

where

$$d = \frac{(3u^2 - 4u - 4v + 1)^2}{(2u-3)(6u^2 - 10u + 5 - 8v)}, \qquad w = -\frac{(u^2 - 6u + 4v + 5)(u^2 - 4v)}{8(2u-3)}$$

and u and v satisfy

$$15u^4 - 82u^3 - 8vu^2 + 159u^2 - 140u + 56vu - 16v^2 - 52v + 50 = 0$$

Moreover, an equation of E_1 is $y^2 = z(z-1)(z-t)$, where

$$t = \frac{(u^2 - 4v)(-8u^4 + 24u^3 - 63u^2 + 64v^2 - 192uv + 196v + 16u^2v - 180u + 100)}{(2u-3)(6u^2 - 10u + 5 - 8v)}$$

Proof. Take the genus 2 curve to be

$$Y^2 = x(x-1)(x-d)(x^3 - ux^2 + v - w)$$

Let φ_1 be the Frey-Kani covering with $deg(\varphi_1) = 5$ such that $\varphi_1(w_1) = \varphi_1(w_2) = \varphi_1(w_3) = t$, $\varphi_1(0) = 0$, $\varphi_1(1) = 1$, and $\varphi_1(d) = \infty$. Take ∞ to be the point of

ramification index 4 such that $\phi_1(\infty) = \infty$. Then ϕ_1 is given by

$$z = k_1 \frac{x(x^2 - ax + b)^2}{(x - d)}$$

Solving the corresponding system we get the above result. □

6.2 Curves of Genus 2 with Degree 7 Elliptic Subfields, 4-cycle Case.

The case $n = 7$ is the first case that all degenerations occur. However, it is very difficult to compute the space of genus 2 curves with degree 7 elliptic subcovers. We discuss only one degenerate case, namely case II. iii) of theorem 4.3. We will assume that the genus two curve is given by

$$C : Y^2 = x(x - 1)(x - d)(x^3 - ax^2 + bx - c)$$

and the elliptic curve in Legendre form $E_1 : y^2 = z(z - 1)(z - t)$. Moreover, let's assume that the corresponding Frey-Kani covering $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ is of type II. i) of theorem 4.3. Take the coordinates such that, $\phi(0) = 0$, $\phi(1) = 1$, $\phi(d) = t$, and three distinct roots of $x^3 - ax^2 + bx - c$ are in the fiber of infinity. Let the point of ramification index 4 be infinity, which is in the same fiber as roots of $x^3 - ax^2 + bx - c$. Then the cover is given by,

$$z = k \frac{x\, P_1^2(x)}{x^3 - ax^2 + bx - c}$$

where $P_1(x)$ is a cubic polynomial which represents the three points of order 2 in the fiber of 0. Solving the corresponding system we get,

$$\begin{aligned} a = \frac{-1}{4A}(&7d^{20} + 424t^4d^8 - 11072d^{12}t^3 + 2368t^3d^{13} - 872d^{16}t^2 - 1532d^{17}t - 21568d^{14}t^2 - 56d^{19}t \\ &+ 478d^{18}t + 36t^5d - 42t^5d^2 + 18160t^3d^{11} - 4356t^3d^{10} - 624t^4d^6 + 8t^5d^3 - 736t^4d^7 \\ &- 52594t^2d^{12} + 624td^{14} - 2576td^{15} + 2725td^{16} + 736td^{13} - 36d^{19} - 2368t^2d^7 + 42d^{18} \\ &+ 6112d^{15}t^2 - 29576t^3d^9 - 7t^5 + 52594t^3d^8 - 44496t^3d^7 + 2576t^4d^5 - 2725t^4d^4 \\ &- 1532t^4d^3 - 56t^4d + 872t^3d^4 - 6112t^3d^5 - 478t^4d^2 - 18160d^9t^2 - 424d^{12}t + 11072d^8t^2 \\ &- 8d^{17} - 44496t^2d^{13} - 21568t^3d^6 + 4356d^{10}t^2 + 29576t^2d^{11}) \end{aligned} \tag{6.1}$$

$$b = \frac{1}{16A}(-14d^{21} - 77d^{20} + 400d^9t^4 - 3496t^4d^8 + 94280d^{12}t^3 + 1680t^3d^{14} - 21232t^3d^{13}$$
$$+ 1008d^{17}t^2 + 35d^{17}t + 31612d^{14}t^2 + 84d^{20}t - 616d^{19}t + 1313d^{18}t - 77t^5d + 121t^5d^2$$
$$- 10356t^4d^6 - 72t^5d^3 + 9016t^4d^7 + 20t^5d^4 - 139344t^2d^{13} + 269886t^2d^{12} - 9016td^{14}$$
$$- 5222td^{16} - 3496td^{13} - 121d^{19} - 1680t^2d^7 - 20d^{17} + 72d^{18} + 5352d^{15}t^2 - 269886t^3d^9$$
$$+ 139344t^3d^8 - 31612t^3d^7 + 5222t^4d^5 - 35t^4d^4 - 5352t^3d^6 - 1313t^4d^3 - 84t^4d - 1008t^3d^4$$
$$+ 616t^4d^2 - 94280d^9t^2 - 400d^{12}t + 21232d^8t^2 + 219712d^{10}t^2 - 308478t^2d^{11} + 308478t^3d^{10}$$
$$- 219712t^3d^{11} - 5080t^3d^5 - 5080d^{16}t^2 + 10356td^{15} + 14t^5)$$

$$c = -\frac{1}{448A}(28d^{11} - 7d^{12} - 561d^4t^2 - 1800d^7t + 84d^{10}t + 12t^2d + 364t^2d^3 - 118t^2d^2 + t^3$$
$$- 20d^7 + 120td^4 - 608td^5 + 1400td^6 + 1311td^8 - 42d^{10} - 140d^6t^2 - 504d^9t + 440d^5t^2)^2 \tag{6.2}$$

where,

$$A = d^{19} - 90d^4t^2 - 36d^7t - 9t^2d - 84t^2d^3 + 36t^2d^2 - t^3 - d^9 + 36td^4 - 90td^5 + 84td^6 + 9td^8$$
$$- 36d^5t^2 + 168td^7 - t^2 - 168td^5 - 20td^3 + 6t^2d - 10t^2d^2 + 5t^2d^3 + 90td^4 - 90d^7t + 20td^8$$
$$- 6d^{10} + d^{11} + 10d^7 - 5d^8) \tag{6.3}$$

Also, t and d satisfy the equation,

$$d^{20} - 16td^{15} + t^3d) + 120td^{14} - 560td^{13} + (400t^2 + 1420t)d^{12} - (2400t^2 + 1968t)d^{11}$$
$$+ (6608t^2 + 1400t)d^{10} - (11040t^2 + 400t)d^9 + 12870t^2d^8 - (400t^3 + 11040t^2)d^7 + 120t^3d^2$$
$$+ (1400t^3 + 6608t^2)d^6 - (1968t^3 + 2400t^2)d^5 + (1120t^3 + 400t^2)d^4 - 560t^3d^3 + t^4 = 0 \tag{6.4}$$

A complete treatment of spaces $\mathcal{L}_5$ and $\mathcal{L}_7$ will be given later.

APPENDIX A
EQUATION OF $\mathcal{L}_3$

We display coefficients $C_0, \ldots, C_8$ of the equation (5.1).

[illegible]

$$+ 15637511592200340\, J_2^6 J_4^2 J_6^5 - 1271050688292456\,96\, J_4^{10} J_2^2 J_6 + 614908581517421568\, J_4^9 J_2 J_6^2 - 233744194313602076\,16\, J_4^4 J_2^2 J_6^5$$

$$+ 1508868948605946984\, J_2^6 J_4^3 J_6^3 - 579504029447062\,3824\, J_2^5 J_4^4 J_6^4 + 140949838965116301\,12\, J_2^4 J_4^3 J_6^5 + 1033174375200\, J_2^{10} J_4^3 J_6^3$$

$$- 2113416308022202\,5024\, J_2^3 J_4^2 J_6^6 + 1800240211917633\,2544\, J_2^2 J_4 J_6^7 - 1539209193724\,0080\, J_2^5 J_4 J_6^6)$$

(A.1)

$$
\begin{aligned}
\text{[illegible]} = {} & \text{[illegible]} - \text{[illegible]}\,J_4^{1?}\,J_2\,J_6 - \text{[illegible]}\,J_2\,J_4\,J_6^{?} + \text{[illegible]}4150086\,J_4^{10}\,J_2^{7}\,J_6 + 39738952224288\,J_2^{3}\,J_6^{9} \\
& - 36311136215244\,J_2^{?}\,J_4^{?}\,J_6 - 996173640\,J_2^{12}\,J_4^{6}\,J_6^{2} + 5977041840\,J_2^{11}\,J_4^{5}\,J_6^{3} - 22413906900\,J_2^{10}\,J_4^{4}\,J_6^{4} - 37501414009508\,J_4^{13}\,J_2^{4} \\
& + \text{[illegible]}\,J_2^{6}\,J_4^{?}\,J_6^{4} + 862549188855807 68\,J_2^{4}\,J_4^{4}\,J_6^{6} - 111444977082978432\,J_2^{3}\,J_4^{3}\,J_6^{7} + 27908893977856\,J_4^{14}\,J_2^{2} \\
& + \text{[illegible]}825152\,J_2^{2}\,J_4^{2}\,J_6^{8} - 4294298096876548 8\,J_2^{5}\,J_4^{5}\,J_6^{5} - 10736445647473\,J_4^{11}\,J_2^{8} + 61746352553318400\,J_4^{4}\,J_2\,J_6^{7} \\
& + 1109588804546 88\,J_4^{12}\,J_2^{3}\,J_6 - 140592520576604 16\,J_4^{3}\,J_6^{8} - 164365980986649 6\,J_4^{11}\,J_2^{2}\,J_6^{2} + 4418327787417 90\,J_2^{8}\,J_4^{8}\,J_6^{2} \\
& - 3128599551108636\,J_2^{7}\,J_4^{7}\,J_6^{3} + 281595049543065 6\,J_4^{10}\,J_2\,J_6^{3} + 1229124488517115 2\,J_4^{8}\,J_2^{5}\,J_6^{3} + 1579225145\,J_2^{12}\,J_4^{9} \\
& - 228635178991 3249\,J_4^{9}\,J_2^{6}\,J_6^{2} - 403004765256293 52\,J_4^{7}\,J_2^{4}\,J_6^{4} + 8170704379892908 8\,J_4^{6}\,J_2^{3}\,J_6^{5} - 25936092270\,J_2^{6}\,J_6^{8} \\
& - \text{[illegible]}7448 9088\,J_4^{5}\,J_2^{2}\,J_6^{6} + \text{[illegible]}\,J_4^{1?}\,J_2^{4}\,J_6^{2} - \text{[illegible]}\,J_4^{1?}\,J_2^{?}\,J_6 + \text{[illegible]} \\
& - \text{[illegible]}\,J_4^{4}\,J_2^{3}\,J_6^{3} + 247\text{[illegible]}\,J_4^{8}\,J_2^{2}\,J_6^{4} - 26\text{[illegible]}\,J_4^{7}\,J_2\,J_6^{5} - 6755065089024\,J_4^{15} \\
& + \text{[illegible]} - 466\text{[illegible]}\,J_2^{8}\,J_4^{?}\,J_6^{?} + \text{[illegible]}\,J_2^{?}\,J_4\,J_6^{7} + 9487368 0\,J_2^{13}\,J_4^{7}\,J_6 \\
& \text{[illegible]} \\
& - \text{[illegible]} - \text{[illegible]}\,J_2^{4}\,J_4\,J_6^{8} - 796509786 50\,J_2^{11}\,J_4^{8}\,J_6 \\
& - \text{[illegible]}\,J_4^{?}\,J_6^{4} + \text{[illegible]}\,J_4^{6}\,J_6^{6} + 22075242832281 6\,J_4^{12}\,J_6^{2} + 1322792799725\,J_2^{10}\,J_4^{10} - 1953070\,J_2^{14}\,J_4^{8})
\end{aligned} \tag{A.2}
$$

$$
\begin{aligned}
\text{[illegible]}_1 = {} & -2^{8}\,\text{[illegible]}\,J_4^{8}\,J_2 - 182125808\,J_4^{7}\,J_6 + 16021872\,J_4^{7}\,J_2^{3} - 211022400\,J_4^{6}\,J_2^{2}\,J_6 - 26594919\,J_4^{6}\,J_2^{5} \\
& + \text{[illegible]}\,J_4^{5}\,J_2\,J_6^{2} + 330158928\,J_4^{5}\,J_2^{4}\,J_6 - 215198\,J_2^{7}\,J_4^{5} - 1227105712\,J_4^{4}\,J_6^{3} - 1525734368\,J_4^{4}\,J_2^{3}\,J_6^{2} \\
& + 2\text{[illegible]}\,J_4^{4}\,J_2^{6}\,J_6 - 363\,J_2^{9}\,J_4^{4} + 3162070656\,J_4^{3}\,J_2^{2}\,J_6^{3} - 16471998\,J_4^{3}\,J_2^{5}\,J_6^{2} + 4356\,J_4^{3}\,J_2^{8}\,J_6 - 19602\,J_4^{2}\,J_2^{7}\,J_6^{2} \\
& - 24\text{[illegible]}162240\,J_4^{2}\,J_2\,J_6^{4} + 17961936\,J_4^{2}\,J_2^{4}\,J_6^{3} + 39204\,J_4\,J_2^{6}\,J_6^{3} - 72369936\,J_4\,J_2^{3}\,J_6^{4} + 746496\,J_4\,J_6^{5} - 29403\,J_2^{5}\,J_6^{4} \\
& + \text{[illegible]}\,J_2^{2}\,J_6^{5})\,(J_4^{3} - J_2^{2}\,J_4^{2} + 6\,J_2\,J_6\,J_4 - 9\,J_6^{2})^{3} \\
\text{[illegible]} = {} & 2^{8}\,(768\,J_4^{2} - 416\,J_4\,J_2^{2} - J_2^{4} + 1536\,J_2\,J_6)\,(J_4^{3} - J_2^{2}\,J_4^{2} + 6\,J_2\,J_6\,J_4 - 9\,J_6^{2})^{6}
\end{aligned}
$$

Next we define J_{18}.

$$
\begin{aligned}
J_{18} = {} & -\text{[illegible]}\,J_4^{?}\,J_2^{9} - 2545581\text{[illegible]}140640\,J_4^{11}\,J_2^{2} - 20707\text{[illegible]}00653300\,J_2^{3}\,J_6^{7} \\
& + \text{[illegible]}1067888741 2\text{[illegible]}\,J_4^{3}\,J_2^{6}\,J_6^{4} - 6726467885718107787 3420\,J_4^{6}\,J_2^{9}\,J_6 - \text{[illegible]}7165356\,J_4^{?}\,J_2^{5}\,J_6^{3} \\
& + \text{[illegible]}\,J_4^{3}\,J_2^{8}\,J_6^{2} + \text{[illegible]}2201007820\,J_4^{8}\,J_2^{7}\,J_6 - 8288714614593\text{[illegible]}80952\,J_4^{5}\,J_2^{11}\,J_6 \\
& - \text{[illegible]}1688601956652 2\,J_4^{7}\,J_2^{4}\,J_6^{2} + 1670066951248087682779025460\,J_4^{6}\,J_2^{3}\,J_6^{3} - 8700\text{[illegible]}187500\,J_4^{2}\,J_2^{11}\,J_6^{3} \\
& + 10\text{[illegible]}20101400856441930430\,J_4\,J_2^{4}\,J_6^{6} + 4722077830745904211\text{[illegible]}785\,J_4^{2}\,J_2^{8}\,J_6^{4} + 7262519785066586252061 0\,J_4^{4}\,J_2^{10}\,J_6^{2} \\
& + 22565940681515768597163841875\,J_6^{6} + 8618448214\text{[illegible]}908105648\,J_2^{4}\,J_4^{4}\,J_6^{4} + 42064041955852065250635 48\,J_4^{10}\,J_2^{4} \\
& - \text{[illegible]}0292387640800690 40\,J_4^{5}\,J_2^{2}\,J_6^{4} + 264482\text{[illegible]}\,J_4^{14}\,J_4^{?}\,J_?^{?} - \text{[illegible]}08999259500\,J_4^{3}\,J_6^{6} \\
& - \text{[illegible]}\,J_4^{?}\,J_2^{3}\,J_6 - 4446215416819\text{[illegible]}\,J_4^{3}\,J_2^{7}\,J_6^{3} - 11954025451555067941715 52\,J_4\,J_2^{7}\,J_6^{5} \\
& + \text{[illegible]}25960\,J_4^{8}\,J_2^{2}\,J_6^{2} - 8867147\text{[illegible]}80876992549800\,J_4^{7}\,J_2\,J_6^{3} + 262175897182080411549 64\,J_4^{7}\,J_2^{10} \\
& \text{[illegible]} \\
& + \text{[illegible]}10823\,J_4^{6}\,J_2^{12} + 597436504352707279446490\,J_4^{8}\,J_2^{8} - 494418285498712523376610 59000\,J_2\,J_4\,J_6^{7} \\
& + \text{[illegible]} - 18440\text{[illegible]}\,J_2^{?}\,J_4^{?}\,J_6 - 5877\text{[illegible]}562500\,J_2^{15}\,J_4^{3}\,J_6 \\
& - 40224014576499000000\,J_4^{4}\,J_2^{13}\,J_6 - 5289644619140625 00\,J_2^{13}\,J_4\,J_6^{3} + 6183877872118077519741700200\,J_4^{4}\,J_2\,J_6^{5} \\
& + 240581884124440625 0\,J_4^{5}\,J_2^{14} - 586185566487416780733027 00\,J_4^{9}\,J_6^{2} + 4006598628468215589492840 50\,J_4^{6}\,J_6^{4} \\
& + 489781909179687 5\,J_2^{16}\,J_4^{4} - 911901251294928562500\,J_2^{9}\,J_6^{5} + 4716420540951557 6\text{[illegible]}409125000\,J_2^{7}\,J_4^{2}\,J_6^{6} \\
& + 39672\text{[illegible]}46435546875\,J_2^{12}\,J_6^{4} + 677889761667446328934698\,J_2^{6}\,J_6^{6} - 1846845498901606762338536256\,J_2^{5}\,J_4^{5}\,J_6^{3} \\
& + 2154117579827\text{[illegible]}491343936 70\,J_2^{6}\,J_4^{6}\,J_6^{2} - 3368755111891005676495 80\,J_4^{3}\,J_2^{2}\,J_6^{3} + 947026423817466 75\,J_4^{12}
\end{aligned} \tag{A.3}
$$

Now we display $\bar{u}$ as a rational function in $\bar{i}_1, \bar{i}_2, \bar{i}_3$, and $\bar{e}$.

$$
\bar{u} = \frac{A}{B} \tag{A.4}
$$

where A and B are:

$$
\begin{aligned}
\dot{v} = {} & -[\text{illegible}]\,v^{7} - [\text{illegible}]\,v^{6} - 4855592464187548884\,v_1^{4}v_2 + 16763981518938931121\,v_1^{7} \\
& + 1110[\text{illegible}]\,v^{5} + 1764184749921\,v_1^{12} + 2528446510810312\,v_1^{9} + 4777013072226451456601\,v_1^{6} - 2944071752834093049446\,v_1^{2} \\
& + 5406874[\text{illegible}]\,v^{4} - 1[\text{illegible}]\,v_1^{15} - 661374269881402920550\,v_1^{3} + 81207912539750401\,v_1^{6} \\
& - 1987211955[\text{illegible}]\,v_1^{4} + 1795766815922\,v_1^{11} + 6828132294987954405121\,v_1^{5} - 1019176434722\,v_1^{12}v_2^{2} \\
& + 1996360251871196000\,v_1^{7} - 76129241\,v_1^{13} + 111292574394\,v_1^{11} - 27007507944\,v_1^{14} - 3864833234458023884\,v_1^{7} \\
& + 1477956307619114000\,v_1^{5} - 22268258547600601\,v_1^{7} - 351611123607884\,v_1^{10} - 765262229566238384139521\,v_1^{2}v^{2} \\
& - 489231000822205368627201\,v_1^{3}v^{3} + 4074339452989401368985681\,v_1^{4} - 43167052308945593659008\,v_1^{4}v^{5} - 11747434455692582401\,v_1^{6} \\
& + 27426425199016061\,v_1^{9} + 16325344950971225248161\,v_1^{6} - 5472905429913891844\,v_1^{7} + 2554759372879226881\,v_1^{7} \\
& - 1057952495001681\,v_1^{9} - 6412249008011\,v_1^{11} + 44160506797406749196288011\,v_1^{2} - 151481923744321\,v_1^{10} + 1044141349119742240011\,v_1^{3} \\
& + 1121176016926316574310401\,v_1^{2}v + 5589\,v_1^{15} - 2268648\,v_1^{14} - 71736114299590400000001\,v_1^{3} - 1071694955410640\,v_1^{6}v_1^{2} \\
& - 2865[\text{illegible}]\,v_1^{12}v_1^{2} + 1711924911865311107102721\,v_1^{4}v_2 - 272383554140000640\,v_1^{6} - 5498502219927990721\,v_1^{6}v_1^{2} \\
& + 1[\text{illegible}]\,v^{4} - 67011738451038603250752\,v_1^{5}v_2 + 46510077981269081\,v_1^{7}v_1^{2} + 38033809211\,v_1^{13}v_1^{2} \\
& - 42[\text{illegible}]\,v_1^{10}v_1 + 78[\text{illegible}]\,v_1^{5} - 6627138059159939488001\,v_1^{3} - 111489047127017641520\,v_1^{5}v_2 \\
& + 4[\text{illegible}]\,v_1^{6}v_2 + 72619995[\text{illegible}]\,v_1^{8}v_2 - 111540775652104111751\,v_1^{8}v_2 \\
& + [\text{illegible}]\,v_1^{2} - [\text{illegible}]\,v_1^{7}v_2 + 1625265401761522\,v_1^{9}v_1 \\
& + [\text{illegible}]\,v_1^{8}v_2 + 1[\text{illegible}]\,v_1^{13} + 1099[\text{illegible}]\,v_1^{4} - 4387167084252672\,v_1^{7}v_1 + 20419814834353908\,v_1^{7}v_1^{2} \\
& - [\text{illegible}]\,v_1^{4} - 2525[\text{illegible}]\,v_1^{6} + 4217288\,v_1^{14}v_1^{2} - 5589\,v_1^{15}v_1^{2} - 1250111618323464\,v_1^{11} \\
& + [\text{illegible}]\,v_1^{7} + 1565[\text{illegible}]\,v_1^{7} - 688703184241962729062401\,v_1^{3} \\
& - [\text{illegible}]\,v_1^{12} + 1[\text{illegible}]\,v_1^{9} + 1[\text{illegible}]\,v_1^{10} - 5871827619583244521\,v_1^{9}v_1 + 2231987184\,v_1^{13}v_2 \\
& - 5071721[\text{illegible}]\,v_1^{10}v_1^{2} + 1062121\,v_1^{14} - 4316178561284\,v_1^{10}v_2 - 1554351121\,v_1^{13} + 4[\text{illegible}]\,v_1^{12} \\
& + [\text{illegible}]\,v^{5} - 771942387555658940\,v_1^{6}v^{6} - 67612089954638321\,v_1^{6}v^{4} + 4552992204280561\,v_1^{9}v^{3} - 1296625710421\,v_1^{12}v^{2} \\
& + 2444021854113041\,v_1^{7}v^{7} - 1077767669368\,v_1^{10}v^{2} - 5352911706900401\,v_1^{10}v_1 + 751140[\text{illegible}]\,v_1^{9}v^{7} + 1049[\text{illegible}]\,v_1^{14}v_1^{2} \\
& + [\text{illegible}] - [\text{illegible}] - 1[\text{illegible}]\,v_1^{5}v_2^{2} - 1[\text{illegible}]\,v_1^{2}v_2^{2} - [\text{illegible}]\,v_1^{5}v_2 + 1115588901614\,v_1^{2}v_1^{11} \\
& + [\text{illegible}]\,v_1^{11}v_1^{2} + 2210[\text{illegible}]\,v_1^{7} - 2444[\text{illegible}]\,v_1^{7}v_1^{2} + 1177[\text{illegible}]\,v_1^{7}v_1^{2} \\
& + [\text{illegible}]\,v_1^{13}v_1^{2} + 2066598701[\text{illegible}]\,v_1^{7}v_1 + 1961881961\,v_1^{13} - 2104073047771945704961\,v_1^{5} - 21102121\,v_1^{14}v_1^{2} \\
& + [\text{illegible}]\,v_1^{2} + [\text{illegible}]\,v_1^{8}v_1^{2} + 88[\text{illegible}]\,v_1^{8}v_1^{2} - 150897872915368\,v_1^{10}v_1^{2} \\
& - [\text{illegible}]\,v_1^{12}v_1^{2} - 1031[\text{illegible}]\,v_1^{8}v_1^{2} + 155422730719312938270721\,v_1^{4} + 6060756436623034594099201\,v_1^{2}v_2 \\
& - [\text{illegible}]\,v_1^{15}v_2 + 1591221[\text{illegible}]\,v_1^{14}v_2 + 1498034393856\,v_1^{10} + 938628273050741931041\,v_1^{4} + 1403020863810621\,v_1^{11}v_1^{2} \\
& + 42[\text{illegible}]\,v_1^{8} + 1[\text{illegible}]\,v_1^{2} + 1[\text{illegible}]\,v_1^{4}v_1 - 1554583867458899452021\,v_1^{5}v_1^{2} \\
& + 6112[\text{illegible}]\,v_1^{7}v_1^{2} - 41801160752985094697777921\,v_1^{3} - 1342567906077885595648\,v_1^{4} + 788026466102580001\,v_1^{7}v_1 \\
& + 71[\text{illegible}] + 1838789325441630567176601621\,v_1^{2} - 3896278459221\,v_1^{12} + 27954990429449022001\,v_1^{6} \\
& - [\text{illegible}]\,v_1^{10} + [\text{illegible}] + [\text{illegible}]\,v_1^{4} - [\text{illegible}] + [\text{illegible}] \\
& + 4549[\text{illegible}]\,v_1^{5} - 6539683797511868883996\,v_1^{6} - 1019382072642\,v_1^{12}v_1^{2} + 1226729632\,v_1^{12}v_1 \\
& - 2291[\text{illegible}]\,v_1^{3} - 29764752714969923736\,v_1^{8}v_2 + 2659679270633652\,v_1^{9}v_1^{2} - 52519007836202872\,v_1^{9}v_1^{2} \\
& + 2975671417401780643\,v_1^{7}v_2 + 1417410750023814367840\,v_1^{4}v_2 - 7668451011059866748\,v_1^{8}v_1^{2} + 25309938593684537247744\,v_1^{2} \\
& + [\text{illegible}] + 4981[\text{illegible}]\,v_1^{3} - 6[\text{illegible}]\,v_1^{7} - 59367622862919988881\,v_1^{6} + 2203045871100184841\,v_1^{7} \\
& + [\text{illegible}] + 4254[\text{illegible}]\,v_1^{2} - 484117789777210800001\,v_1^{5} - 30357678538471248\,v_1^{5}v_1^{2} \\
& + 1075[\text{illegible}]\,v_1^{4} + 1039508394226012721280\,v_1^{4}v_2 + 218684035838189174401\,v_1^{3} - 1478788\,v_1^{14}v_1 \\
& - 1567[\text{illegible}]\,v_1^{13}v_1^{2} - 241\,v_1^{15}v_1 + 2070630380063482490880\,v_1^{2}v_1 - 4557841258275670358753280\,v_1 - 66436449067016210350080001\,v_2 \\
& - 2902608[\text{illegible}]\,v_1^{14}v_1 + 1406482517780321\,v_1^{8}v_2 + 13682132372881\,v_1^{9}v_2 - 45776142410098\,v_1^{7}v_1^{2} - 1111361290\,v_1^{13}v_1 \\
& - 1222[\text{illegible}] + 1980693571484484\,v_1^{6}v_2 - 3534644758011869739040\,v_1^{3}v_2 + 40714851012414582370713601\,v_1^{2} \\
& - 2[\text{illegible}]\,v_1^{6} + 9711\,v_1^{15}v_1 - 88391304\,v_1^{13}v_1^{2} - 1984030361\,v_1^{13}v_1^{2} \\
& + [\text{illegible}] - 1[\text{illegible}]\,v_1^{5} + 1[\text{illegible}]\,v_1^{4} + 1[\text{illegible}]\,v_1^{11}v_1 - 1267871270560000001\,v_1^{5}v_1 \\
& + 2564[\text{illegible}]\,v_1^{8}v_1^{2} + 1731254597086800960\,v_1^{6}v_2 + 1531137105792000000001\,v_1^{2} - 71222357841426432000001\,v_1 \\
& + 2405[\text{illegible}] + 3465870120\,v_1^{12} - 25019281\,v_1^{13} + 1067555811456\,v_1^{11} + 866950332120000001\,v_1^{2} \\
& + 1068[\text{illegible}] + 4288215222215473459200001\,v_1^{2} - 76492035070867296001\,v_1^{3} - 401344005628152631296001\,v_1^{2} \\
& + [\text{illegible}] + 2588[\text{illegible}] - 1339786852992000000\,v_1^{3}v_1 - 2586003810278400000\,v_1^{4}v_2 \\
& + 5485[\text{illegible}] + 189043890848579232000\,v_1^{4}v_2 + 1056854628\,v_1^{13}v_1
\end{aligned}
$$

(A 5)

$$
B = [\text{illegible}]r_2 v^5 + 431848120987680768v^5 - 299264368956044 4r_1^4 v^5 r_2 + 483401465694464 0r_1 v^7 - 150643881r_1^4 v^{12}
$$

$$
+ [\text{illegible}]r_2 v^9 - 2302672843031 52384r_2 v^6 - 4179222638384445230 2848r_2 v^2 + 16766396022030336v^6 + 401922r_1^4 v^{13}
$$

$$
- [\text{illegible}]r_1^3 v^3 - 8089535380608r_1 v^8 + 65383636541159915 2872r_1^3 v^4 + 9696619998r_1^4 v^{11}
$$

[illegible]

This is u in terms of r_1 and v

$$u = \frac{C}{4D}$$

$$\begin{aligned}
&= -129600r^5 + 81r_1r^8 - 2295709784r_1^2r^2 + 528058440r_1^2r^3 - 59073912r_1^2r^4 + 3446828r_1^2r^5 \\
&\quad - 101937r_1^2r^6 + 1287r_1^2r^7 + 7652750400r_1^2r - 5618412r_1r^5 + 1339231320000r_1^2 - 3147662592r_1r^3 \\
&\quad + [illegible]r_1r^3 + 47558[illegible]958440r_1r + 15253642656r_1r^2 + 10187341332480 - 25101021312000r_1 \\
&\quad - 36[illegible]27403008r + 39700522352r^3 - 63407183616r^2 + 23193r_1r^6 - 56671488r^4 \qquad (A.7) \\
D &= 57054875504r_1r - 7062260400r_1^2r + 1013922360r_1^2r^2 - 85626720r_1^2r^3 + 4178095r_1^2r^4 + 6426r_1r^5 \\
&\quad - 110010r_1^2r^5 + 1269r_1^2r^6 + 243r_1r^6 + 261786384r_1r^3 + 317801718000r_1^2 - 336174021600r_1 - 5152023r_1r^4 \\
&\quad - 1257564605440r - 134160r^4 - 42301440r^3 + 10225437502[illegible] + 4704791040r^2 - 5268457840r_1r^2
\end{aligned}$$

APPENDIX B
INTERSECTION OF $\mathcal{L}_2$ WITH $\mathcal{L}_3$

Here we treat cases $d)$, $e)$, $f)$ of theorem (5.12).

d) The solution of $\lambda^2 - u_1\lambda + 1 = 0$ gives:

$$
\begin{aligned}
u_1 &= \frac{5397132429}{1407338645} - \frac{7990191587952}{26592534050334205} s - \frac{95155372620}{5318706810066841} s\sqrt{69} \\
&- \frac{17462888982953127}{502520168687817697633445} s^2 + \frac{211465570561245}{100504033737563539526689} s^2\sqrt{69} \\
u_2 &= -\frac{728334107575011}{1180546002235825} + \frac{2384733751243785018}{2230798603812284786425} s + \frac{75467344848925328}{49231944152491391457} s\sqrt{69} \\
&+ \frac{10442537526985012606311}{[illegible]} s^2 - \frac{33360714007375166181}{[illegible]22706} s^2\sqrt{69} \\
u_3 &= \frac{2297084111423867922949}{106614280394657992595712500} + \frac{688986062807104752272163}{313948908435707270568147389412500} s \\
&- \frac{288301830732087724629}{[illegible]0600} s\sqrt{69} + \frac{120009636816570722325994983279}{4745985490394599945878183992663773700000} s^2 \\
&- \frac{2634487752666289651995541}{179678839231487995670254719413101869600} s^2\sqrt{69}
\end{aligned}
\tag{B.1}
$$

e) The solution of $\lambda^2 - u_2\lambda + 1 = 0$ gives:

$$
\begin{aligned}
u_1 &= \frac{5397132429}{1407338645} + \frac{3995095793976}{26592534050334205} s + \frac{47577686310}{5318706810066841} s\sqrt{69} + \frac{17462888982953127}{1005040337375635395266890} I\sqrt{3}s^2 \\
&- \frac{3995095793976}{26592534050334205} I\sqrt{3}s - \frac{142733058930}{5318706810066841} Is\sqrt{23} - \frac{211465570561245}{201008067475127079053378} s^2\sqrt{69} \\
&+ \frac{17462888982953127}{1005040337375635395266890} s^2 - \frac{634396711683735}{201008067475127079053378} I\sqrt{23}s^2 \\
&+ \frac{1000982112022125498541}{6744624696060414010557045412} [illegible] - \frac{7773367242462664}{49231944152491391457} [illegible] + \frac{33360714007375166181}{6744624696060414010557045412} s^2\sqrt{69} \\
&- \frac{[illegible]66875621892509}{[illegible]78603812284786425} s + \frac{11320101727387992}{49231944152491391457} Is\sqrt{23} + \frac{1192366875621892509}{2230798603812284786425} I\sqrt{3}s \\
&- \frac{10442537526985012606311}{168615617401510350263926135300} I\sqrt{3}s^2 - \frac{10442537526985012606311}{168615617401510350263926135300} s^2 - \frac{728334107575011}{1180546002235825} \\
u_3 &= \frac{2297084111423867922949}{106614280394657992595712500} + \frac{688986062807104752272163}{627897816871414541136294778825000} I\sqrt{3}s + \frac{2634487752666289651995541}{759357678462975991340509438826203739200} s^2\sqrt{69} \\
&+ \frac{464905492196263173887}{10046365069942632658180716461200} Is\sqrt{23} - \frac{288301830732087724629}{10046365069942632658180716461200} s\sqrt{69} \\
&- \frac{688986062807104752272163}{627897816871414541136294778825000} s - \frac{120009636816570722325994983279}{949197098078719989177563679853275467400000} I\sqrt{3}s^2 \\
&- \frac{120009636816570722325994983279}{949197098078719989177563679853275467400000} s^2 + \frac{7903462057998868955986623}{759357678462975991340509438826203739200} I\sqrt{23}s^2
\end{aligned}
\tag{B.2}
$$

f) The solution of $\lambda^2 - u_3\lambda + 1 = 0$ gives:

$$[illegible] = \frac{[illegible]}{[illegible]}([illegible] + [illegible] I\, s^{\frac{1}{3}}\sqrt{23} + 16776143224330380912\, s^{\frac{1}{3}}$$

$$+ [illegible]\, s^{\frac{2}{3}}\sqrt{23}\sqrt{3} - 19403209981059031\, I\sqrt{3}\, s^{\frac{2}{3}} + 19403209981059031\, s^{\frac{2}{3}} + 152442617602075\, I\sqrt{23}\, s^{\frac{2}{3}}$$

$$- [illegible]\, s^{\frac{2}{3}}\sqrt{69} + 16776143224330380912\, I\sqrt{3}\, s^{\frac{1}{3}}$$

$$[illegible] = \frac{189}{[illegible]}(-55040670893891835809039090236 - [illegible]28522808191200\, I\, s^{\frac{1}{3}}\sqrt{23}$$

$$- [illegible]986464607396\, I\sqrt{3}\, s^{\frac{2}{3}} - 476854111543986464607396\, s^{\frac{2}{3}} - [illegible]0400\, s^{\frac{1}{3}}\sqrt{23}\sqrt{3}$$

$$+ [illegible]\, I\sqrt{3}\, s^{\frac{2}{3}} + 44127928581184082255\, s^{\frac{2}{3}}\sqrt{23}\sqrt{3} - [illegible]\, I\sqrt{23}\, s^{\frac{2}{3}}$$

$$[illegible] = \frac{[illegible]}{[illegible]}(-[illegible]\, I\sqrt{23}\, s^{\frac{2}{3}} - 1482671211922[illegible]1139827098559\, s^{\frac{2}{3}}$$

$$- [illegible]\, s^{\frac{2}{3}} - [illegible]\, s^{\frac{1}{3}}\sqrt{69} + [illegible]\, s^{\frac{2}{3}}\sqrt{69}$$

$$- [illegible]\, I\, s^{\frac{1}{3}}\sqrt{23} + 1482671211922[illegible]1139827098559\, I\sqrt{3}\, s^{\frac{2}{3}}) - 1620192978[illegible]6091526086381459436142[illegible]$$

$$- [illegible]866261[illegible]\, I\sqrt{3}\, s^{\frac{1}{3}}$$

[illegible]

REFERENCES

[1] Blake I. Seroussi G. Smart N. Elliptic Curves in Cryptography. LMS. 265. (1999).

[2] Brandt R. Stichtenoth H. Die Automorphismengruppen Hyperelliptischer Kurven. *Man. Math.* 55. 83-92. (1986).

[3] Brandt R. Über Die Automorphismengruppen von Algebraischen Funktionenkörpen. (unpublished) PhD thesis. Universität-Gesamthochschule Essen. (1988).

[4] Clebsch A. Theorie der Binären Algebraischen Formen. Verlag von B.G. Teubner. Leipzig. (1872).

[5] Frey G. 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).

[6] Frey G. Kani E. 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).*

[7] Fried M. Twisted Modular Curves (in press)

[8] Fried M. Völklein H. The inverse Galois problem and rational points on moduli spaces. *Math. Annalen* **290** (1991). 771-800.

[9] Howe E. Leprévost F. Poonen B. Large torsion subgroups of split Jacobians of curves of genus two or three. Forum Math. **(12)**. (2000). 315-364

[10] Kani E. Schanz H. Modular diagonal quotient surfaces Math. Z 227. (1988). 337-366

[11] Krazer A. Lehrbuch der Thetafunctionen. Chelsea. New York. (1970).

[12] Kuhn M. R. Curves of genus 2 with split Jacobian. *Trans. Amer. Math. Soc* **307** (1988). 41-49

[13] Igusa J. Arithmetic Variety Moduli for genus 2. *Ann. of Math.* (2). 72. 612-649. (1960).

[14] Jacobi C. Anzeige von Legendre. Théorie des fonctions elliptiques. Troiseme supplément. 1832. Ges. Werke Bd. 1. Berlin (1881). p. 373.

[15] Mumford D. The Red Book of Varieties and Schemes. Springer. New York (1999).

[16] Mestre P. 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. —it Prog. Math., 313-334. Birkhäuser, 1991. Proc. Congress in Livorno, Italy, April 17-21, (1990).

[17] Gaudry P. Schost E. Invariants des quotients de la Jacobienne d'une courbe de genre 2. (in press)

[18] Geyer W. Invarianten Binarer Formen. *Lecture Notes in Mathematics*, Springer, New York, (1972).

[19] Serre J. Groupes algebriques et corps de classes. Hermann, Paris, (1959).

[20] Silverman J. The Arithmetic of Elliptic Curves, Springer-Verlag, New York, (1986).

[21] Voelklein H. Groups as Galois Groups: An introduction, *Cambridge Studies in Advanced Mathematics* **53**, London, (1996).

[22] Voelklein H. Moduli spaces for covers of the Riemann sphere, *Israel J. Math* **85** (1994), 407-430, (1997).

[23] Voelklein H. Cyclic covers of $\mathbb{P}^1$, and galois action on their division points, *Contemp. Math* **186**, 91-107, (1995).

BIOGRAPHICAL SKETCH

Tanush Shaska was born in Vlora, Albania, where he finished high school. He was denied the right to attend the university because of his family opposition to the communist government. After spending two years in the Albanian army he enrolled briefly at the University of Tirana. He emigrated to the United States in October of 1991. In January of 1992 he enrolled at the University of Michigan and graduated with high distinction in 1994. After working for two years as a consultant/programmer he started graduate school at the University of Florida in the fall of 1996. He has been to many conferences and given many talks. During the year 2000 he visited the University of Erlangen as a DFG fellow.

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.

Helmut Voelklein, Chairman
Professor of Mathematics

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.

John Thompson
Graduate Research Professor of Mathematics

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.

Chat Ho
Professor of Mathematics

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.

Pham Tiep
Assistant Professor of Mathematics

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.

Jörg Peters
Professor of Computer and Information Science and Engineering

This dissertation was submitted to the Graduate Faculty of the Department of Mathematics in the College of Liberal Arts and Sciences and to the Graduate School and was accepted as partial fulfillment of the requirements for the degree of Doctor of Philosophy.

May 2001

Dean, Graduate School