Elliptic subfields and automorphisms of genus 2 function fields

T. Shaska and H. Völklein

Department of Mathematics, University of Florida, Gainesville, FL 32611.

Abstract. We study genus 2 function fields with elliptic subfields of degree 2. The locus \( L_2 \) of these fields is a 2-dimensional subvariety of the moduli space \( M_2 \) of genus 2 fields. An equation for \( L_2 \) is already in the work of Clebsch and Bolza. We use a birational parametrization of \( L_2 \) by affine 2-space to study the relation between the j-invariants of the degree 2 elliptic subfields. This extends work of Geyer, Gaudry, 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 paper is dedicated to Professor Shreeram Abhyankar
on the occasion of his 70th birthday

1 Introduction

Sections 2 and 4 of this note are concerned with degree 2 elliptic subfields \( E \) of a genus 2 function field \( K \) (All function fields are over an algebraically closed field \( \mathbb{k} \) of char. \( \neq 2 \)). Jacobi [17] already noted that in this case \( K \) has generators \( X \) and \( Y \) with

\[
Y^2 = X^6 - s_1 X^4 + s_2 X^2 - s_3
\]

(1)

This generalized an example of Legendre. In the newer literature, Cassels [4] chapter 14 deals with arithmetic aspects of this. Gaudry/Schost [7] show that a genus 2 field \( K \) in char > 5 has at most two elliptic subfields of degree 2, up to isomorphism, and compute the j-invariants of these elliptic subfields in terms of Igusa invariants of \( K \).

On the other hand, there is a group theoretic aspect. Degree 2 elliptic subfields of \( K \) correspond to elliptic involutions in the automorphism group of \( K \) i.e. involutions different from the hyperelliptic involution \( e_0 \). Thus our topic is intimately related with the structure of \( G := Aut(K/k) \), and its quotient \( \bar{G} \) by \( < e_0 > \). Geyer [8] classifies the possibilities for \( \bar{G} \), gives a brief discussion of \( G \) and also notes some consequences for isogenies between elliptic subfields. His exposition is very brief because the main focus of his paper is on a different theme. We study the structure of \( G \) in section 3. We give a simple classification, based on group-theoretic properties of central extensions of \( \bar{G} \), and relate it to our \((u, v)\)-parametrization of \( L_2 \) (see below).
It follows that the number of $G$-classes of degree 2 elliptic subfields of $K$ is 0, 1 or 2; and this number is 1 if and only if $K$ has equation $Y^2 = X(X^4 - 1)$.

Brandt/Stichtenoth [3] more generally discuss automorphisms of hyperelliptic curves (in characteristic 0), whereas Brandt [2] (unpublished thesis) has a very comprehensive classification of automorphism groups of hyperelliptic curves in any characteristic and more generally, cyclic extensions of genus 0 fields.

The purpose of this note is to combine these two aspects, the geometric and the group theoretic one. E.g., Gaudry/Schost use only the reduced automorphism group, using $G$ itself would simplify their paper. They exclude characteristics 3 and 5 where other types of automorphism groups appear.

In section 2 and 4 we study the locus $\mathcal{L}_2$ of genus 2 fields with elliptic subfields of degree 2. Geyer [8] states that $\mathcal{L}_2$ is a rational surface whose singular locus is the curve corresponding to reduced automorphism group $V_4$ (see our section 3, case III). We give an explicit birational parametrization of $\mathcal{L}_2$ by parameters $u, v$; they are obtained by setting $s_3 = 1$ in (1) and symmetrizing $s_1, s_2$ by an action of $S_3$. More precisely, those $u, v$ parametrize genus 2 fields together with an elliptic involution of the reduced automorphism group (Thm 1). We express the $j$-invariants of degree 2 elliptic subfields in terms of $u, v$. The particular case that these $j$-invariants are all equal (for a fixed genus 2 field) yields a birational embedding of the moduli space $M_1$ of genus 1 curves into $M_2$.

In section 4 we use the coordinates on $M_2$ and $\mathcal{L}_2$ provided by invariant theory. Expressing these coordinates in terms of our $(u, v)$-parameters makes the parametrization of $\mathcal{L}_2$ explicit. From this we confirm the explicit equation found by Gaudry/Schost [7] that is satisfied by all points of $\mathcal{L}_2$; and we see directly that $\mathcal{L}_2$ is the full zero set of this equation.

More generally, there is literature on degree $n$ elliptic subfields, e.g., Frey [9], and Frey and Kani [10], and Lange [25]. The first author’s PhD thesis [26] deals with the case $n = 3$. We further intend to study the cases $n = 5$ and 7.

In the last section, we study the action of $\text{Aut}(K)$ on elliptic subfields $F$ of odd degree $n \geq 7$. The hyperelliptic involution fixes these subfields, hence they are permuted by $G$. It is easy to see that stabilizer $G_F$ in $G$ of $F$ has order $\leq 3$. We study those cases where $G_F \neq 1$, assuming $\text{char}(k) = 0$. This allows us to use Riemann’s Existence Theorem to parametrize the extensions $K/F$ of degree $n$ with non-trivial automorphisms by certain triples of permutations in $S_n$. To count the number of these triples of permutations is a difficult problem for general $n$. We use a computer search to construct all such triples for $n \leq 21$.

**Notation:** All function fields in this paper are over $k$, where $k$ is an algebraically closed field of characteristic $\neq 2$. Further, $V_4$ denotes the Klein 4-group and $D_{2n}$ (resp., $\mathbb{Z}_n$) the dihedral group of order $2n$ (resp., cyclic group of order $n$).
2 Genus 2 Curves with Elliptic Involutions

Let $K$ be a genus 2 field. Then $K$ has exactly one genus 0 subfield of degree 2, called $k(X)$. It is the fixed field of the hyperelliptic involution $e_0$ in $\text{Aut}(K)$. Thus $e_0$ is central in $\text{Aut}(K)$. Here and in the following, $\text{Aut}(K)$ denotes the group $\text{Aut}(K/k)$, more precisely. It induces a subgroup of $\text{Aut}(k(X))$ which is naturally isomorphic to $\text{Aut}(K) := \text{Aut}(K)/\langle e_0 \rangle$. The latter is called the reduced automorphism group of $K$.

**Definition 1.** An elliptic involution of $G = \text{Aut}(K)$ is an involution different from $e_0$. Thus the elliptic involutions of $G$ are in 1-1 correspondence with the elliptic subfields of $K$ of degree 2. An involution of $\bar{G} = \text{Aut}(K)$ is called elliptic if it is the image of an elliptic involution of $G$.

If $e_1$ is an elliptic involution in $G$ then $e_2 := e_0 e_1$ is another one. So the elliptic involutions come naturally in (unordered) pairs $e_1, e_2$. These pairs correspond bijectively to the elliptic involutions of $\bar{G}$. The latter also correspond to pairs $E_1 \hookrightarrow E_2$ of elliptic subfields of $K$ of degree 2 with $E_1 \setminus k(X) = E_2 \setminus k(X)$.

**Definition 2.** We will consider pairs $(K \hookrightarrow \varepsilon)$ with $K$ a genus 2 field and $\varepsilon$ an elliptic involution in $\bar{G}$. Two such pairs $(K \hookrightarrow \varepsilon)$ and $(K_0 \hookrightarrow \varepsilon_0)$ are called isomorphic if there is a $k$-isomorphism $\nu : K \to K_0$ with $\varepsilon_0 = \nu \varepsilon \nu^{-1}$.

Let $\varepsilon$ be an elliptic involution in $\bar{G}$. We can choose the generator $X$ of $\text{Fix}(e_0)$ such that $\varepsilon(X) = -X$. Then $K = k(X,Y)$ where $X, Y$ satisfy (1) with $s_1, s_2, s_3 \in k$, $s_3 \neq 0$ (follows from (10) and Remark 3 in section 3). Further $E_1 = k(X^2, Y)$ and $E_2 = k(X^2, YX)$ are the two elliptic subfields corresponding to $\varepsilon$. Let $j_1$ and $j_2$ be their j-invariants.

Preserving the condition $\varepsilon(X) = -X$ we can further modify $X$ such that $s_3 = 1$. Then

\[ Y^2 = X^6 - s_1 X^4 + s_2 X^2 - 1 \]  

where the polynomial on the right has non-zero discriminant.

These conditions determine $X$ up to coordinate change by the group $\langle \tau_1, \tau_2 \rangle$ where $\tau_1 : X \to \zeta_6 X$, $\tau_2 : X \to \frac{1}{X}$, and $\zeta_6$ is a primitive 6-th root of unity in $k$. (Thus $\zeta_6 = -1$ if $\text{char}(k) = 3$). Here $\tau_1$ maps $(s_1, s_2)$ to $(\zeta_6^3 s_1, \zeta_6^6 s_2)$, and $\tau_2$ switches $s_1, s_2$. Invariants of this action are:

\[ u := s_1 s_2 \]
\[ v := s_1^3 + s_2^3 \]  

In these parameters, the discriminant of the sextic polynomial on the right hand side of (2) equals $64 \Delta^2$, where

\[ \Delta = \Delta(u, v) = u^2 - 4v + 18u - 27 \neq 0 \]
Further, the $j$-invariants $j_1$ and $j_2$ are given by:

$$j_1 + j_2 = 256 \frac{(v^2 - 2u^3 + 54u^2 - 9uv - 27v)}{\Delta}$$

$$j_1 j_2 = 65536 \frac{(u^2 + 9u - 3v)}{\Delta^2}$$

(4)

The map $(s_1, s_2) \mapsto (u, v)$ is a branched Galois covering with group $S_3$ of the set $\{(u, v) \in k^2 : \Delta(u, v) \neq 0\}$ by the corresponding open subset of $s_1, s_2$-space if $\text{char}(k) \neq 3$. In any case, it is true that if $s_1, s_2$ and $s_1', s_2'$ have the same $u, v$-invariants then they are conjugate under $(\tau_1, \tau_2)$.

**Lemma 1.** For $(s_1, s_2) \in k^2$ with $\Delta \neq 0$, equation (2) defines a genus 2 field $K_{s_1, s_2} = k(X, Y)$. Its reduced automorphism group contains the elliptic involution $\epsilon_{s_1, s_2} : X \mapsto -X$. Two such pairs $(K_{s_1, s_2}, \epsilon_{s_1, s_2})$ and $(K_{s_1', s_2'}, \epsilon_{s_1', s_2'})$ are isomorphic if and only if $u = u'$ and $v = v'$ (where $u, v$ and $u', v'$ are associated with $s_1, s_2$ and $s_1', s_2'$, respectively, by (3)).

**Proof.** An isomorphism $\phi$ between these two pairs yields $K = k(X, Y) = k(X', Y')$ with $k(X) = k(X')$ such that $X, Y$ satisfy (2) and $X', Y'$ satisfy the corresponding equation with $s_1, s_2$ replaced by $s_1', s_2'$. Further, $\epsilon_{s_1, s_2}(X') = -X'$. Thus $X'$ is conjugate to $X$ under $(\tau_1, \tau_2)$ by the above remarks. This proves the condition is necessary. It is clearly sufficient.

**Theorem 1.** i) The $(u, v) \in k^2$ with $\Delta \neq 0$ bijectively parameterize the isomorphism classes of pairs $(K, \epsilon)$ where $K$ is a genus 2 field and $\epsilon$ an elliptic involution of $\text{Aut}(K)$. This parametrization is defined in Lemma 1. The $j$-invariants of the two elliptic subfields of $K$ associated with $\epsilon$ are given by (4).

ii) The $(u, v)$ satisfying additionally

$$(v^2 - 4u^3)(4v - u^2 + 110u - 1125) \neq 0$$

(5)

bijectively parameterize the isomorphism classes of genus 2 fields with $\text{Aut}(K) \cong V_4$; equivalently, genus 2 fields having exactly 2 elliptic subfields of degree 2. Their $j$-invariants $j_1, j_2$ are given in terms of $u$ and $v$ by (4).

**Proof.** i) follows from the Lemma.

iii) Condition (5) is equivalent to $\text{Aut}(K)$ being a Klein 4-group, and to the other stated condition, by 2.3, Case IV. The theorem follows.

**Remark 1.** (Isomorphic elliptic subfields) For each $j \in k, j \neq 0, 1728, -32678$ there is a unique genus 2 field $K$ with $\text{Aut}(K) \cong V_4$ such that the two elliptic subfields of $K$ of degree 2 have the same given $j$-invariant. This generalizes as follows: For each $j \in k, j \neq 0$, there is a pair $(K, \epsilon)$ as in the Theorem, unique up to isomorphism, such that the two associated elliptic subfields of $K$ have the same given $j$-invariant and the corresponding $u, v$ satisfy $v = 9(u - 3)$. 


Mapping \( j \in k \setminus \{0\} \) to the associated \( K \) gives an isomorphic embedding of \( \mathcal{M}_1 \setminus \{j = 0\} \) into \( \mathcal{M}_2 \). Here \( \mathcal{M}_g \) denotes the moduli space of genus \( g \) curves (over \( k \)).

**Proof.** From (4) we get that the discriminant of \((x - j_1)(x - j_2)\) is

\[
2^{16} (4u^3 - v^2)(v - 9u + 27)^2 \Delta^2
\]

Thus the condition \( j_1 = j_2 \) is equivalent to either \( v = 9(u - 3) \) or \( v^2 = 4u^3 \). The latter condition is equivalent to \( \text{Aut}(K) \geq D_8 \) by Lemma 3(b) below. Under the condition \( v = 9(u - 3) \) we get

\[
\begin{align*}
& u = 9 - \frac{j}{256}, \\
& v = 9(6 - \frac{j}{256})
\end{align*}
\]

where \( j := j_1 = j_2 \). There is only one point on the curve \( v = 9(u - 3) \) with \( \Delta(u, v) = 0 \), namely \( u = 9, \ v = 54 \); it corresponds to \( j = 0 \). Further, for \( j = 1728 \) (resp., \( j = -32678 \)) we have \( \text{Aut}(K) \cong D_8 \), (resp., \( D_{12} \)). For all the other values of \( j \), we have \( \text{Aut}(K) \cong V_4 \). This proves the first claim by part i). The rest is proved in section 3 using Igusa coordinates on \( \mathcal{M}_2 \).

**Remark 2.** (2- and 3-isogenous elliptic subfields) The modular 3-polynomial

\[
\Phi_3 = x^3 - x^2 y + y^3 + 232xy(x + y) - 1069956xy(x + y) + 36864000(x^3 + y^3)
\]

\[
+ 2587918086x^2 y^2 + 8900222976000xy(x + y) + 45298483200000(x^2 + y^2)
\]

\[
- 77084596633600000xy + 1855425871872000000000(x + y)
\]

(6)

is symmetric in \( j_1 \) and \( j_2 \) hence becomes a polynomial in \( u \) and \( v \) via (4). This polynomial factors as follows;

\[(4v - u^2 + 110u - 1125) \cdot g_1(u, v) \cdot g_2(u, v) = 0 \quad \text{(7)}\]

where \( g_1 \) and \( g_2 \) are

\[
g_1 = -27008u^6 + 256u^7 - 2432u^5v + v^4 + 7296u^5v^2 - 6692v^3u - 1755067500u
\]

\[
+ 2419308v^3 - 34553439v^4 + 127753092vu^2 + 16274844vu^3 - 1720730a^2v^2
\]

\[
- 1941120u^3 + 381631500v + 1018668150a^2 - 116158660u^2 + 52621974v^3
\]

\[
+ 387712u^4 - 483963660v + 334166676v^2 + 922640625
\]

(8)

\[
g_2 = 291350448u^6 - v^4u^2 - 998848u^6v - 3456u^7v + 4749840u^6v^2 + 17032u^6v^2
\]

\[
+ 4v^5 + 80368u^8 + 256u^9 + 6848224u^7 - 10535040v^3u^2 - 35872v^3u^3 + 26478u^4u
\]

\[
- 77908736u^5v + 9516699u^4v^2 + 307234984u^3v^2 - 419583744v^3u - 826436736v^3
\]

\[
+ 2750293296u^4 + 28808773632vu^2 - 23429955456vu^3 + 5455334016a^2v^2
\]

\[
- 4127824816v + 82556485632u^2 - 108737593344u^3 - 12123095040u^4v^2
\]

\[
+ 4127824816v + 3503554560u^4v + 53411019904u^5 - 2454612480u^4v
\]

(9)
Vanishing of the first factor is equivalent to $D_{12} \leq G$, see part II of the next section. (Here again $G = \text{Aut}(K)$). If $G = D_{12}$ then $K$ has two classes of elliptic involutions $e$, where $e$ and $e_0 e$ are non-conjugate; thus $K$ has two $G$-classes of elliptic subfields of degree 2, and subfields from different classes are 3-isogenous. This was noted in [7] (for $p \neq 5$). There are exactly two fields $K$ such that $D_{12}$ is properly contained in $G$, see part I of the next section. In these cases, $e$ and $e_0 e$ are conjugate (and the corresponding elliptic curves are 3-isogenous to themselves). In the case III of the next section, $G$ has two classes of elliptic involutions $e$; now $e$ and $e_0 e$ are conjugate, hence $j_1 = j_2$ in formula (4). Degree 2 elliptic subfields from different $G$-classes are now 2-isogenous, see [8].

3 Automorphism Groups of Genus 2 Fields

3.1 Preliminaries

Let $K$ be a genus 2 field, $G$ its automorphism group and $e_0 \in G$ the hyperelliptic involution. Then $< e_0 > = \text{Gal}(K/k(X))$, where $k(X)$ is the unique genus 0 subfield of degree 2 of $K$. The reduced automorphism group $\overline{G} = G/ < e_0 >$ embeds into $\text{Aut}(k(X)/k) \cong \text{PGL}_2(k)$.

The extension $K/k(X)$ is ramified at exactly six places $X = p_1, \ldots, p_6$ of $k(X)$, where $p_1, \ldots, p_6$ are six distinct points in $\mathbb{P}^1 := \mathbb{P}^1_k$. Let $P := \{p_1, \ldots, p_6\}$. The corresponding places of $K$ are called the Weierstrass points of $K$. The group $G$ permutes the 6 Weierstrass points, and $\overline{G}$ permutes accordingly $p_1, \ldots, p_6$ in its action on $\mathbb{P}^1$ as subgroup of $\text{PGL}_2(k)$. This yields an embedding $\overline{G} \hookrightarrow S_6$. We have $K = k(X, Y)$, where

$$Y^2 = \prod_{p \neq \infty} (X - p)$$

Because $K$ is the unique degree 2 extension of $k(X)$ ramified exactly at $p_1, \ldots, p_6$, each automorphism of $k(X)$ permuting these 6 places extends to an automorphism of $K$. Thus, $G$ is the stabilizer in $\text{Aut}(k(X)/k) \cong \text{PGL}_2(k)$ of the 6-set $P$.

Let $\Gamma := \text{PGL}_2(k)$. If $l$ is prime to $\text{char}(k)$ then each element of order $l$ of $\Gamma$ is conjugate to $\begin{pmatrix} \epsilon_l & 0 \\ 0 & 1 \end{pmatrix}$, where $\epsilon_l$ is a primitive $l$-th root of unity. Each such element has 2 fixed points on $\mathbb{P}^1$ and other orbits of length $l$. If $l = \text{char}(k)$ then $\Gamma$ 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 $\mathbb{P}^1$.

Lemma 2. Let $g \in G$ and $\overline{g}$ its image in $\overline{G}$.

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

b) If $\overline{g}$ has order 4, then $g$ has order 8.
Proof. a) Suppose \( \bar{g} \) is an involution. We may assume \( \bar{g}(X) = -X \).
Assume first that \( \bar{g} \) fixes no points in \( P \). Then \( P = \{a, -a, b, -b, c, -c\} \) for certain \( a, b, c \in k \). Thus
\[
Y^2 = (X^2 - a^2)(X^2 - b^2)(X^2 - c^2)
\]
and so \( g(Y)^2 = Y^2 \). Hence \( g(Y) = \pm Y \), and \( g \) has order 2.
Now suppose \( \bar{g} \) fixes 2 points of \( P \). Then \( P = \{0, \infty, a, -a, b, -b\} \), hence
\[
Y^2 = X(X^2 - a^2)(X^2 - b^2)
\]
So \( g(Y)^2 = -Y^2 \) and \( g(Y) = \sqrt{1 - Y} \). Hence \( g \) has order 4.

b) Each element of \( \Gamma \) of order 4 acts on \( P \) with two fixed points and all other orbits of length 4. So if \( \bar{g} \) has order 4, then it fixes 2 points in \( P \). Thus \( g^2 \) has order 4, by a). Hence \( g \) has order 8.

Remark 3. The Lemma implies that an involution of \( \bar{G} \) is elliptic if and only if it fixes no point in its action on the 6-set \( P \); equivalently, if and only if it induces an odd permutation of \( P \).

Remark 4. (i) If a finite subgroup \( H \) of \( \Gamma \) with \( |H|, \text{char}(k) = 1 \) fixes a point of \( P^1 \) then \( H \) is cyclic: Indeed, we may assume \( H \leq \{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \} : b \in k^*, a \in k \}. The normal subgroup defined by \( b = 1 \) intersects \( H \) trivially, hence \( H \) embeds into its quotient which is isomorphic \( k^* \). Hence \( H \) is cyclic.

(ii) The degree 2 central extensions of \( S_4 \):
Their number is \( |H^2(S_4, C_2)| = 4 \) (see [3]). We construct them as follows. Let \( W \) be the subgroup of \( GL_4(3) \) generated by
\[
S' = \begin{pmatrix} S & 0 \\ 0 & I \end{pmatrix}, \quad T' = \begin{pmatrix} T & 0 \\ 0 & U \end{pmatrix}
\]
where \( S, T, U \in GL_2(3) = \langle S, T \rangle \) and \( S^3 = 1 = T^2 \), whereas \( U \) has order 4. Then \( W \) is a central extension of \( PGL_2(3) \cong S_4 \) with kernel \( \{1, w_1, w_2, w_3\} \), where
\[
w_1 = \begin{pmatrix} I & 0 \\ 0 & -I \end{pmatrix}, \quad w_2 = \begin{pmatrix} -I & 0 \\ 0 & -I \end{pmatrix}, \quad w_3 = w_1 w_2.
\]
The \( W_i = W/\langle w_i \rangle, i = 1, 2, 3 \) and the split extension comprise all degree 2 central extensions of \( S_4 \). They are inequivalent since \( W_3 \) has no elements of order 8 (as opposed to \( W_1 \) and \( W_2 \)), whereas transpositions of \( S_4 \) lift to involutions (resp., elements of order 4) in \( W_1 \) (resp., \( W_2 \)). Note that \( W_1 \cong GL_2(3) \).

Remark 5. Suppose \( f_1, f_2, f_3 \) are quadratic polynomials in \( k[z] \) such that their product has non-zero discriminant. Then there is an involution in \( \Gamma \) switching the two roots of each \( f_i \) if and only if \( f_1, f_2, f_3 \) are linearly dependent in \( k[z] \) (over \( k \)). See Cassels [4], Thm. 14.1.1, or Jacobi [17].
Lemma 3. Suppose $e$ is an elliptic involution of $G$ and $e$ its image in $\bar{G}$. Let $u, v$ be the parameters associated with the pair $(K, e)$ by Theorem 1.

(a) There exists an involution $d$ in $G$ such that the group $H = <d, e>$ acts transitively on the 6-set $P$ if and only if

$$4v - u^2 + 110u - 1125 = 0 \quad (11)$$

In this case, $<H, e_0> \cong D_{12}$ acts as $S_3$ (regularly) on $P$.

(b) There exists an involution $d$ in $G$ such that $H = <d, e>$ has an orbit $Q$ of length $4$ on $P$ if and only if

$$v^2 - 4u^3 = 0 \quad (12)$$

In this case, $H \cong D_8$ acts as $V_4$ on $Q$.

(c) If neither (a) nor (b) holds then $G \cong V_4$.

Proof. We may assume that $K = K_{s_1, s_2}$ and $e = e_{s_1, s_2}$ as in Lemma 1. Then $P = \{a, -a, b, -b, c, -c\}$ for $a, b, c \in k$ with $abc = 1$, $a^2 + b^2 + c^2 = s_1$, $a^2b^2 + a^2c^2 + b^2c^2 = s_2$. Plugging this (with $c = \frac{1}{a}$) into (3) expresses $u, v$ as rational functions of $a, b$. Substituting these expressions for $u, v$ in (11) and (12) yields

$$\begin{align*}
& (a^3b^3 - a + a^2b + b + 6a^2b^2 + ab - b^4a^2)\left((a^3b^3 + a - a^2b + b + 6a^2b^2 - ab + b^4a^3)\right) \\
& (a^3b^3 - a^2b^2 - 6a^2b^2 - ab + b^2a^2)\left((a^3b^3 + a + a^2b^2 + b - 6a^2b^2 - ab + b^4a^3)\right) = 0 \quad (13)
\end{align*}$$

respectively

$$\begin{align*}
& (b - 1)^2(b + 1)^2(b^2 + b + 1)^2(b^2 - b + 1)^2(a - 1)^2(a + 1)^2(a^2 + a + 1)^2 \\
& (a^2 - a + 1)^2(ab - 1)^2(ab + 1)^2(a^2b^2 + ab + 1)^2(a^2b^2 - ab + 1)^2 = 0 \quad (14)
\end{align*}$$

(a) Such $d$ exists (by Lemma 2) if and only if there is an involution $\delta \in \Gamma$ fixing $P$ but no point in $P$, and no 4-set in $P$ fixed by $e$. By Remark 5, the latter is equivalent to the vanishing of certain determinants expressed in terms of $a, b$. These determinants exactly correspond to the factors in (13).

This proves the first claim in (a).

Let $\bar{H}$ the permutation group on the 6-set $P$ induced by $H$. We know $\bar{H}$ is dihedral and transitive, hence is (regular) $S_3$ or $D_{12}$. But $D_{12}$ is not generated by two involutions with no fixed points. This proves (a).

(b) The first claim is proved as in (a), using the factorization of $v^2 - 4u^3$ in (14). Now $\bar{H}$ is dihedral and transitive on the 4-set $Q$, hence is $V_4$ or $D_8$. But $D_8$ is not generated by two involutions with no fixed points. Thus $H \cong V_4$.

Since $de$ fixes the two points in $P \setminus Q$, it has order 4. The claim follows.

(c) Suppose neither (a) nor (b) holds. Then $e$ is the only elliptic involution in $G$. Hence $e$ is central in $G$. If $\gamma$ is another involution in $G$, it follows that $\gamma e$ is elliptic, contradiction. Thus $e$ is the only involution in $G$. Hence either $G = <e>$ or $G \cong \mathbb{Z}_6$. The latter case cannot occur, see the case $m = 6$ in the next section.
3.2 The list of automorphism groups

Since \( G \hookrightarrow S_6 \), all elements of \( G \) have order \( \leq 6 \). For each \( m = 4, 5, 6 \) with \( (p, m) = 1 \) there is a unique genus 2 field \( K \) such that \( G \) contains an element of order \( m \). Indeed, we may assume \( \gamma : x \mapsto cx \) with \( c \in k^* \) of order \( m \). We may further normalize the coordinate \( X \) such that \( 1 \in P \). Then \( P \) consists of all powers of \( c \) plus 0 (for \( m \leq 5 \)) and \( \infty \) (for \( m = 4 \)). Thus \( P \) is also invariant under \( x \mapsto 1/x \) for \( m = 4 \) and \( m = 6 \). For \( p = 5 \) there is also a unique genus 2 field \( K \) such that \( G \) contains an element of order 5.

I. Sporadic cases: \( G \) has elements of order \( m \geq 4 \).

\( m = 4 \): Here \( K \) has equation \( Y^2 = X(X^4 - 1) \), and \( \bar{G} \cong S_4 \) (resp., \( G \cong S_5 \), acting as \( \text{PGL}_2(5) \) on \( P \cong \mathbb{F}^3(F_5) \)) if \( p \neq 5 \) (resp., \( p = 5 \)). In each case, \( G \) is transitive on \( P \) and has exactly one class of elliptic involutions (corresponding to the transpositions in \( S_4 \) resp. \( S_5 \)). The associated value of \((u, v)\) is \((5^2, -2 \cdot 5^3)\). By Remark 4 and Lemma 2 we have

\[ G \cong GL_2(3) \quad \text{if } p \neq 5 \]

and

\[ G \cong 2^+S_5 \quad \text{if } p = 5 \]

(the degree 2 cover of \( S_5 \) where transpositions lift to involutions).

\( m = 6 \): If \( p = 5 \) then we are back to the previous case because \( S_5 \) has an element of order 6. The case \( p = 3 \) doesn’t occur here. Now assume \( p > 5 \). Then \( K \) has equation \( Y^2 = X^6 - 1 \) and \( \bar{G} \cong D_{12} \). Thus \( G \) has two classes of elliptic involutions, one of them consisting of the central involution. The two associated values of \((u, v)\) are \((0, 0)\) and \((3^2, 5^2), 2^3 3^2 5^3)\). (The first corresponds to the central involution \( x \mapsto -x \) of \( \bar{G} \)).

By Lemma 3(b), the inverse image in \( G \) of a Klein 4-subgroup of \( \bar{G} \) is \( \cong D_4 \). It is a Sylow 2-subgroup of \( G \). Thus

\[ G \cong Z_4 \rtimes D_8 \]

where elements of order 4 in \( D_8 \) act on \( Z_4 \) by inversion.

\( m = 5 \): Here \( p \neq 5 \) and \( K \) has equation \( Y^2 = X(X^5 - 1) \). Further, \( \bar{G} \cong Z_5 \), \( G \cong Z_{10} \). There are no elliptic involutions in this case.

II. The 1-dimensional family with \( G \cong D_{12} \)

Here we assume \( G \) has an element \( \gamma \) of order 3, but none of higher order. Suppose first \( p \neq 3 \). Then we may assume \( \gamma : x \mapsto cx \) with \( c \in k^* \) of order 3; also \( 1 \in P \). Then \( P = \{1, c, c^2, a, ac, ac^2\} \) for some \( a \in k^* \). The monic polynomials \((z-1)(z-a), (z-c)(z-c^2a), (z-c^2)(z-ca)\) have the same constant coefficient, hence are linearly dependent. Hence by Remark 3 there is an elliptic involution \( \epsilon \) in \( \bar{G} \) with \( \epsilon(1) = a, \epsilon(c) = c^2a, \epsilon(c^2) = ca \). The
group $<\epsilon, \gamma>$ is $\cong S_3$, acting regularly on $P$. Hence by Lemma 3(a) the
parameters associated with the pair $(K, \epsilon)$ satisfy (11):
$$4v - u^2 + 110u - 1125 = 0$$
Intersection of this curve with $\Delta = 0$ is the single point $(9, 54)$. Also the
parameter values $(5^2, -2 \cdot 5^3)$ and $(3^2 \cdot 5^2, 2 \cdot 3^3 \cdot 5^3)$ from the previous case are
excluded now. (These values satisfy (11) which is confirmed by the fact that
the corresponding groups $\bar{G}$ contain a regular $S_3$). In the present case,$S_3$ is
all of $\bar{G}$, and by Lemma 3(a) we have $G \cong D_{12}$. If $p = 3$ then we may assume
$\gamma : x \mapsto x + 1$, and $P = \{0, 1, 2, a, a + 1, a + 2\}$. As above we see there is an
elliptic involution $\epsilon$ in $\bar{G}$ with $<\epsilon, \gamma> \cong S_3$. The rest is as for $p \neq 3$ (only
that the parameter value $(0, 0)$ doesn’t occur because it makes
$\Delta$ zero).

III. The 1-dimensional family with $G \cong D_8$
In the remaining cases, $G$ has only elements of order $\leq 2$. Hence $\bar{G} = \{1\},$
$\mathbb{Z}_2$ or $V_4$. Here we assume $G \cong V_4$. Then two of its involutions are elliptic.
By Lemma 3(b) it follows that $G \cong D_8$ and the $u, v$ parameters satisfy
$$v^2 = 4u^3$$
Intersection of this curve with $\Delta = 0$ consists of the two points $(9, 54)$ and
$(1, -2)$. The values $(0, 0), (5^2, -2 \cdot 5^3)$ and $(3^2 \cdot 5^2, 2 \cdot 3^3 \cdot 5^3)$ from Case I are
excluded.

IV. The 2-dimensional family with $G \cong V_4$
If $G \cong \mathbb{Z}_2$ then its involution $\epsilon$ is elliptic. Indeed, we may assume $\epsilon : x \mapsto -$x + 1 and $\bar{P} = \{0, \infty, 1, -1, a, -a\}$ and so $\bar{G}$
contains the additional involution $x \mapsto -a/x$. Thus $G \cong V_4$. By I–III, this
case occurs if and only if the pair $(K, \epsilon)$ has $u, v$ parameters with
$$(4v - u^2 + 110u - 1125)(v^2 - 4u^3) \neq 0$$
V. The generic case $G \cong \mathbb{Z}_2$
This occurs if and only if $K$ has no elliptic involutions and is not isomor-
phic to the field $Y^2 = X(X^3 - 1)$. The existence of elliptic involutions is
equivalent to the condition in Theorem 3 (in terms of classical invariants).

Summarizing:

**Theorem 2.** The automorphism group $G$ of a genus 2 field $K$ in character-
istic $\neq 2$ is isomorphic to $\mathbb{Z}_2, \mathbb{Z}_{10}, V_4, D_8, D_{12}, \mathbb{Z}_3 \rtimes D_8, GL_2(3)$, or $2^4 S_5$.
In the first (resp., last) two cases, $G$ has no (resp., exactly one) class of el-
liptic involutions; in the other cases, it has two classes. Correspondingly, $K$ has either 0, 1 or 2 classes (under $G$-action) of degree 2 elliptic subfields; the
case of one class occurs if and only if $K$ has equation $Y^2 = X(X^3 - 1)$.

It was noted by Geyer [8] and Gaudry/Schost [7] that if $G = D_8$ (resp.,
$D_{12}$) then degree 2 elliptic subfields in different classes are 2-isogenous (resp.,
3-isogenous).
4 The locus of genus 2 curves with elliptic involutions

4.1 Classical invariants and the moduli space $\mathcal{M}_2$

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

$$f(X, Z) = a_6 X^6 + a_5 X^5 Z + \cdots + a_0 Z^6$$

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

\[
J_2 := -240a_0a_6 + 40a_1a_5 - 16a_2a_4 + 6a_3^2
\]

\[
J_4 := 48a_0^2a_6 + 4a_1^2a_5 + 1620a_3^2a_4 - 12a_1a_3a_5 - 12a_2a_4a_5 + 300a_1^2a_6 + 300a_0a_6a_2 + 324a_0a_6a_1 - 504a_0a_2a_3 - 180a_1a_3a_2 - 180a_1a_2a_5 + 4a_1a_2a_5 + 54a_0^2a_5 - 80a_0^2a_5
\]

\[
J_6 := 176a_0^3a_6^2 + 64a_1^3a_5^2 + 1600a_3^3a_4a_2 + 1600a_3^2a_4a_5 + 1600a_3^2a_4a_5 - 160a_1a_2a_3 + 96a_0a_5a_6 - 60a_0a_5a_6 + 72a_1a_3a_5 - 24a_1a_3a_5
\]

\[
-160a_2a_4a_6 - 60a_2a_5a_6 - 24a_2a_5a_6 + 8a_2a_5a_6
\]

\[
-900a_2a_4a_6 - 24a_2a_5a_6
\]

Here $J_{10}$ is the discriminant of $f$. It vanishes if and only if the binary sextic has a multiple linear factor. These $J_{2i}$ are invariant under the natural action of $SL_2(k)$ on sextics. Dividing such an invariant by another one of the same degree gives an invariant under $GL_2(k)$ action.

Two genus 2 fields $K$ (resp., curves) in the standard form $Y^2 = f(X, 1)$ are isomorphic if and only if the corresponding sextics are $GL_2(k)$ conjugate. Thus if $I$ is a $GL_2(k)$ invariant (resp., homogeneous $SL_2(k)$ invariant), then the expression $I(K)$ (resp., the condition $I(K) = 0$) is well defined. Thus the $GL_2(k)$ invariants are functions on the moduli space $\mathcal{M}_2$ of genus 2 curves. This $\mathcal{M}_2$ is an affine variety with coordinate ring

$$k[\mathcal{M}_2] = k[a_0, \ldots, a_6, J_{10}^{-1}]^{GL_2(k)} = subring of degree 0 elements in k[J_2, \ldots, J_{10}, J_{10}^{-1}]$$

see Igusa [16].
4.2 Classical invariants of genus 2 fields with elliptic involutions

Under the correspondence in Theorem 4 (resp., Remark 5), the classical invariants of the field $K$ are:

\begin{align*}
J_2 &= 240 + 16u \\
J_4 &= 48v + 4u^2 + 1620 - 504u \\
J_6 &= -20664u + 96v - 424u^2 + 24u^3 + 160uv + 119880 \\
J_{10} &= 64(27 - 18u - u^2 + 4v)^2
\end{align*}

(16)

respectively

\begin{align*}
J_2 &= 384 - \frac{1}{16}j \\
J_4 &= 2^{-14}j^2 \\
J_6 &= 2^{-21}j^2(-3j + 53248) \\
J_{10} &= 2^{-26}j^4
\end{align*}

**Proof of Remark 1, concluded:** The latter formulas explicitly define (in homogeneous coordinates) the map of $M_1 \setminus \{j = 0\}$ to $M_2$ from Remark 1. The function $\frac{J_4}{J_6} \in k[M_2]$ (resp., $\frac{J_2}{J_6}$) is a linear function in $j$ if $\text{char}(k) \neq 3$ (resp., $\text{char}(k) = 3$). Thus the map is an embedding. This completes the remaining part of the proof of Remark 1.

**Theorem 3.** The locus $\mathcal{L}_2$ of genus 2 fields with elliptic subfields of degree 2 is the closed subvariety of $M_2$ defined by the equation

\begin{align*}
8748J_{10}J_2^4J_6^6 - 507384000J_{10}J_2J_6^2 - 19245600J_{10}J_4J_6^2 - 592272J_{10}J_4J_6^2 + 77436J_{10}J_4J_6^2 \\
-81J_2^4J_6^6 - 3499200J_{10}J_2J_6^2 + 4743360J_{10}J_4J_6^2 - 870912J_{10}J_4J_6^2 + 3099960J_{10}J_4J_6^2J_6 \\
-78J_2^4J_6^6 - 1259712000J_{10}J_6^2 + 384J_6^2J_6 + 41472J_{10}J_6^2 + 159J_6^2J_6^2 - 236196J_{10}J_6^2J_6 - 80J_2^3J_6 \\
-47952J_{10}J_2J_6^2 + 10497600J_{10}J_2J_6^2 - 1728J_4J_6^2J_6 + 6048J_4J_6^2J_6 - 9331200J_{10}J_4J_6^2 \\
+12J_2^6J_6^6 + 29370J_2^4J_6^6 - 8910J_2^4J_6^6 - 2999520000J_{10}J_6^2J_6 + 31104J_6^2J_6 + 6912J_6^2J_6^2 \quad = 0
\end{align*}

(17)

The map $k^2 \setminus \{\Delta = 0\} \to \mathcal{L}_2$ described in Theorem 1 is given (in homogeneous coordinates) by the formulas (16). It is birational and surjective if $\text{char}(k) \neq 3$.

**Proof.** The map is surjective by Theorem 1 and its image is contained in the subvariety of $M_2$ defined by (17); the latter is checked simply by substituting the values of $J_{2i}$ from (16). (We found equation (17) by eliminating $u$ and $v$ from equations (16); this equation in different coordinates was also found in [7]).
Conversely assume $K$ is a genus 2 field with equation $Y^2 = f(X)$ whose classical invariants satisfy (17). We have to show that $K$ has an elliptic involution. We may assume

$$f(X) = X(X - 1)(X - a_1)(X - a_2)(X - a_3)$$

by a coordinate change. Expressing the classical invariants of $K$ in terms of $a_1, a_2, a_3$, substituting this into (17) and factoring the resulting equation yields

$$(a_1a_2 - a_2 - a_3a_2 + a_3)^2(a_1a_2 - a_1 + a_3a_1 - a_3a_2)^2(a_1a_2 - a_3a_1 - a_3a_2 + a_3)^2$$

$$(a_3a_1 - a_1 - a_3a_2 + a_3)^2(a_1a_2 + a_1 - a_3a_1 - a_2)^2(a_1a_2 - a_1 - a_3a_1 + a_3)^2$$

$$(a_3a_1 + a_2 - a_3 - a_3a_2)^2(-a_1 + a_3a_1 + a_2 - a_3)^2(a_1a_2 - a_1 - a_2 + a_3)^2$$

$$(a_1a_2 - a_1 + a_2 - a_3a_2)^2(a_1 - a_2 + a_3a_2 - a_3)^2(a_1a_2 - a_3a_1 - a_2 + a_3a_2)^2$$

$$(a_1a_2 - a_1)^2(a_1 - a_3a_2)^2(a_3a_1 - a_3)^2 = 0$$

(18)

$K$ has an elliptic involution if and only if there is an involution $\epsilon \in PGL_2(k)$ permuting the set \{0, 1, \infty, a_1, a_2, a_3\} fixed point freely. By Remark 5, the latter is equivalent to the vanishing of certain determinants expressed in terms of $a_1, a_2, a_3$. These determinants exactly correspond to the factors in (17). This proves that $\mathcal{L}_2$ is the closed subvariety of $\mathcal{M}_2$ defined by (17).

It remains to show the map in the Theorem is birational. By Theorem 1 we know it is bijective on an open subvariety of $k^2$. This implies that the corresponding function field extension $k(u, v)/k(\mathcal{L}_2)$ is purely inseparable, hence its degree $d$ is a power of $p = char(k)$ (or is 1 in characteristic 0). We need to show $d = 1$. For this we use the functions

$$\frac{J_4}{J_2^2}, \frac{J_2 J_4 - 3 J_6}{J_2^3}, \frac{J_{10}}{J_2^5}$$

in $k(\mathcal{M}_2)$. The images of these functions in $k(u, v)$ are:

$$i_1 = \frac{1}{64} \frac{12v + u^2 + 405 - 126u}{(15 + u)^2}$$

$$i_2 = -\frac{1}{512} \frac{(-1404v + 729u^2 - 3645 + 4131u - 36uv + u^3)}{(15 + u)^3}$$

$$i_3 = \frac{1}{16384} \frac{(-27 + 18u + u^2 - 4v)^2}{((15 + u)^6}$$

(19)

We compute that $u$ satisfies an equation of degree $\leq 3$ over the field $k(i_1, i_2)$ whose coefficients are not all zero:

$$(128i_2 - 48i_1 + 1)u^3 + (5760i_2 + 117 - 3312i_1)u^2 + (86400i_2 - 66960i_1 - 2349)u + 432000i_2 - 421200i_1 + 10935 = 0$$

(20)
Thus \( d = 1 \) (since \( p > 3 \)) and this completes the proof.

Remark 6. In characteristic 3 one needs to replace \( v \) by \( s_1 + s_2 \) to get a birational parametrization.

5 Action of \( \text{Aut}(K) \) on degree \( n \) elliptic subfields

In this section we assume \( \text{char}(k) = 0 \). Let \( k(X), K, G, \bar{G} \) as in section 3.1 and let \( p_1, \ldots, p_6 \) the 6 places of \( k(X) \) ramified in \( K \).

5.1 Elliptic subfields of \( K \) of odd degree

Consider an elliptic subfield \( F \) of \( K \) of odd degree \( n = [K : F] \geq 7 \). We assume the extension \( K/F \) is primitive, i.e., has no proper intermediate fields. The following facts are well-known (see [9], [11]): The hyperelliptic involution of \( K \) fixes \( F \), hence \( [F : k(Z)] = 2 \), where \( k(Z) = F \cap k(X) \). Let \( q_1, \ldots, q_r \) be the places of \( k(Z) \) ramified in \( k(X) \). Then \( r = 4 \) or \( r = 5 \), and we can label \( p_1, \ldots, p_6 \) such that the following holds:

1. \( r = 5 \). All places of \( k(X) \) over \( q_1, \ldots, q_4 \) different from \( p_1, \ldots, p_6 \) have ramification index 2; the \( p_i \)'s have index 1.
2. \( r = 4 \). Here and in the following cases we have \( r = 4 \). Here there is one place \( p_i \) of ramification index 4 over \( q_4 \). All other places of \( k(X) \) over \( q_1, \ldots, q_4 \) different from \( p_1, \ldots, p_6 \) have ramification index 2; the \( p_i \)'s have index 1.
3. Like case (2), only that \( p_i \) lies over \( q_4 \).
4. Like case (4), only now \( p_4 \) has index 3.
5. Like case (3), only that \( p_i \) lies over \( q_4 \).

5.2 Elliptic subfields of \( K \) fixed by an automorphism of \( K \)

Let \( g \neq 1 \) in \( \bar{G} = \overline{\text{Aut}}(K) \). Suppose \( g \) fixes \( F \). (This is a well-defined statement because the hyperelliptic involution — generating the kernel of \( G \to \bar{G} \) — fixes \( F \).) Then \( g \) has order 2 or 3. If \( g \) has order 2 it is not an elliptic involution, and either we are in case (4) and \( n \equiv 3 \) mod 4, or we are in case (5) and \( n \equiv 1 \) mod 4. If \( g \) has order 3 then either we are in case (1) and \( n \equiv 1 \) mod 3, or we are in case (2) and \( n \equiv 2 \) mod 3.

Proof: \( g \) acts on \( k(X) \) and \( k(Z) \), permuting the ramified places of the extension \( k(X)/k(Z) \). Thus \( g \) fixes the sets \( \{p_1, p_2, p_3\} \) and \( \{p_4, p_5, p_6\} \), and the places \( p_i \) resp. \( p_i \). Thus \( g \) cannot have order > 3. Suppose \( g \) has order 2. Then it fixes two of the \( p_i \)'s, hence is not an elliptic involution and there is no \( p_i \) or \( p_i \). Thus we are in case (4) or (5). In case (4) (resp., (5)), \( g \)
permutes the $(n-3)/2$ (resp., $(n-5)/2$) places over $q_1$ (resp., $q_4$) of index 2 fixed point freely, hence $n \equiv 3 \mod 4$ (resp., $n \equiv 1 \mod 4$).

Now suppose $g$ has order 3. Then $g$ permutes $p_1, p_2, p_3$ (resp., $p_4, p_5, p_6$) transitively, hence we are in case (1) or (2). In case (1) (resp., (2)), $g$ fixes $p^{(i)}$ (resp., $p^{(i)}$), hence permutes the $n-2$ (resp., $(n-7)/2$) places over $q_5$ (resp., $q_4$) of index 1 (resp., 2); since it fixes at most one of those places, we have $n \not\equiv 1 \mod 3$ (resp., $n \not\equiv 2 \mod 3$).

5.3 Application of Riemann’s existence theorem

Let $\zeta_3$ be a primitive third root of 1 in $k$. Let $g$ and $F$ as above. We can choose the coordinate $Z$ such that $g(Z) = \zeta Z$, where $\zeta = \zeta_2$ (resp., $\zeta = -1$) in cases (1) and (2) (resp., (4) and (5)). We can further normalize $Z$ such that in case (1) (resp., (2) resp., (4) resp., (5)) the places $q_1, ..., q_r$ have $Z$-coordinates $\zeta^2, 1, \zeta, 0, \infty$ (resp.., $\infty, 1, \zeta, \zeta^2$ resp., $0, \infty, 1, -1$ resp., $0, \infty, 1, -1$).

As used in [11], by Riemann’s existence theorem the equivalence classes of primitive extensions $k(X)/k(Z)$ of degree $n$ with fixed branch points $q_1, ..., q_r$ and ramification behavior as in (1)–(5) correspond to classes of tuples $(\sigma_1, ..., \sigma_r)$ generating the symmetric group $S_n$ or alternating group $A_n$ such that $\sigma_1 \cdots \sigma_r = 1$ and

(1): $\sigma_i$ is an involution with exactly one fixed point for $i = 1, 2, 3$, resp., three fixed points for $i = 4$, and $\sigma_5$ is a transposition.

(2): $\sigma_i$ is an involution with exactly one fixed point for $i = 1, 2, 3$, and $\sigma_4$ has three fixed points, one 4-cycle and the rest are 2-cycles.

(3): $\sigma_i$ is an involution with exactly one fixed point for $i = 1, 2, 3$, and with three fixed points for $i = 4$; and $\sigma_1$ has one fixed point, one 4-cycle and the rest are 2-cycles.

(4): $\sigma_i$ is an involution with exactly one fixed point for $i = 2, 3$, and with three fixed points for $i = 4$; and $\sigma_1$ has no fixed points, one 3-cycle and the rest are 2-cycles.

(5): $\sigma_i$ is an involution with exactly one fixed point for $i = 1, 2, 3$, and $\sigma_4$ has two fixed points, one 3-cycle and the rest are 2-cycles.

By "classes of tuples" we mean orbits under the action of $S_n$ by inner automorphisms (applied component-wise to tuples). In the case $k = \mathbb{C}$, the above correspondence depends on the choice of a "base point" $q_0$ in $\mathbb{P}^1 \setminus \{q_1, ..., q_r\}$ and standard generators $\gamma_1, ..., \gamma_r$ of the fundamental group $\Gamma(q_0) := \pi_1(\mathbb{P}^1 \setminus \{q_1, ..., q_r\}, q_0)$. In particular, $\gamma_1 \cdots \gamma_r = 1$. As "base point" we can take any simply connected subset of $\mathbb{P}^1 \setminus \{q_1, ..., q_r\}$. The corresponding extensions $\mathbb{C}(X)/\mathbb{C}(Z)$ are defined over $\mathbb{Q}$, and so one can immediately pass to the case of general $k$ (algebraically closed of char. 0). Here is our choice of the $\gamma_i$ in case (1); we depict them together with their images $\gamma_i^k$ under the map $z \mapsto \zeta z$. We depict $\gamma_1, ..., \gamma_4$, then $\gamma_5$ is given by the basic relation $\gamma_1 \cdots \gamma_5 = 1$. All loops are oriented counter-clockwise.
Here we choose \( q_0 \) as depicted. Let \( Q_0 \) be the line segment joining \( q_0 \) and \( \zeta q_0 \). We identify \( \Gamma(q_0) \) and \( \Gamma(\zeta q_0) \) via the canonical isomorphisms \( \Gamma(q_0) \cong \Gamma(Q_0) \cong \Gamma(\zeta q_0) \). This yields the above formulas expressing the \( \gamma_i' \) in terms of the \( \gamma_i \).

The tuples \( (\sigma_1, \ldots, \sigma_r) \) corresponding to the extension \( C(X)/C(Z) \), where \( Z = \phi(X) \), are now obtained as follows (see e.g., [29], Ch. 4): Let \( \phi \) also denote the map \( \mathbb{P}^1 \to \mathbb{P}^1 \), \( x \mapsto \phi(x) \). Then lifting of paths gives an action of \( \Gamma(q_0) \) on \( \phi^{-1}(q_0) \), hence a homomorphism of \( \Gamma(q_0) \) to \( S_n \). (This homomorphism is determined up to composition by an inner automorphism of \( S_n \) — re-labeling of the \( n \) elements of \( \phi^{-1}(q_0) \).) Finally, take \( \sigma_i \) to be the image of \( \gamma_i \) under this homomorphism.

This correspondence between tuples and extensions of \( C(Z) \) depends also on the choice of the coordinate \( Z \) (but not on the choice of \( X \)). If we replace \( Z \) by \( Z' := \zeta Z \), then the tuple \( (\sigma_1, \ldots, \sigma_r) \) gets replaced by \( (\sigma'_1, \ldots, \sigma'_r) \), where \( \sigma'_i \) is given in terms of \( \sigma_1, \ldots, \sigma_r \) by the same formula that expresses \( \gamma' i \) in terms of \( \gamma_1, \ldots, \gamma_r \); see Figure 1 above in case (1). In the other cases (where \( r = 4 \)) these formulas appear already in [23] and [21].

\[
\begin{align*}
\gamma'_1 &= \gamma_2 \\
\gamma'_2 &= \gamma_3 \\
\gamma'_3 &= \gamma_4' \gamma_1 \gamma_4^{-1} \\
\gamma'_4 &= \gamma_4 \\
\gamma'_5 &= \gamma_1^{-1} \gamma_3 \gamma_1
\end{align*}
\]

Fig. 1. The case \( q_1, \ldots, q_r = \zeta^2, 1, \zeta, 0, \infty \), where \( \zeta = \zeta_3 \)
Elliptic subfields and automorphisms of genus 2 function fields

(2)
\[ \sigma'_1 = \sigma_2 \\
\sigma'_2 = \sigma_3 \\
\sigma'_3 = \sigma_1 \\
\sigma'_4 = \sigma_1^{-1} \sigma_4 \sigma_1 \]

(4) and (5)
\[ \sigma'_1 = \sigma_2 \sigma_3 \sigma_2^{-1} \\
\sigma'_2 = \sigma_2 \\
\sigma'_3 = \sigma_1 \\
\sigma'_4 = \sigma_1^{-1} \sigma_4 \sigma_1 \]

Since \( Z' = g(Z) = g(\phi(X)) = \phi(g(X)) \), where \( g(X) \) is another generator of \( \mathbb{C}(X) \), we see that the tuple \( (\sigma'_1, \ldots, \sigma'_r) \) is in the same class as \( (\sigma_1, \ldots, \sigma_r) \). Conversely, the latter condition is also sufficient for the automorphism \( Z \mapsto \zeta Z \) to extend to an automorphism of \( \mathbb{C}(X) \). It will permute \( p_1, \ldots, p_6 \), hence extend to an automorphism of \( K \) fixing \( F \).

5.4 Symmetric tuples

Primitive extensions \( K/F \), where \( K \) is a genus 2 field and \( F \) an elliptic subfield of odd degree \( n \geq 7 \) with fixed branch points of \( k(X)/k(Z) \) correspond to classes of tuples \( (\sigma_1, \ldots, \sigma_r) \) generating \( S_n \) or \( A_n \) with \( \sigma_1 \cdots \sigma_r = 1 \) as in (1)—(5). Let \( T_j(n) \) be the set of such tuple classes in case \( (j) \), \( j = 1, \ldots, 5 \). The number of these tuple classes grows polynomially with \( n \). (Kani has an exact formula, proved through a different interpretation of this number, see [14]). E.g., for \( n = 7, 9, 11, 13 \) we have \( |T_1(n)| = 168, 432, 1100 \) and \( 2184 \), respectively.

The condition that \( F \) is fixed by an automorphism of \( K \) (different from the identity and the hyperelliptic involution) means that \( (\sigma_1, \ldots, \sigma_r) \) is in the same class as the tuple \( (\sigma'_1, \ldots, \sigma'_r) \) defined in (21). Call such tuples symmetric. Let \( S_j(n) \) be the set of symmetric tuple classes in \( T_j(n) \). The set \( S_j(n) \) can be parameterized by certain triples, which we describe in the next section. This allows us to compute the cardinality of \( S_j(n) \) for \( n \leq 21 \), using a random search to find the triples and the structure constant formula [22], Prop. 5.5, to show that we have found all. This is based on GAP [6] and in particular [19]. The result is stated in Table 1.

From the table it appears that the necessary conditions in section 5.2 (for the existence of extensions \( K/F \) with non-trivial automorphisms) are sufficient in most cases (at least for those \( n \) in reach of computer calculation). It is intriguing that the number of these extensions seems to be very small, but mostly \( > 1 \).
\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|c|c|c|c|c|}
\hline
$n$ & 7 & 9 & 11 & 13 & 15 & 17 & 19 & 21 \\
\hline
$j=1$ & $-$ & 3 & 2 & $-$ & 6 & 3 & $-$ & 2 \\
\hline
$j=2$ & 1 & 0 & $-$ & 2 & 0 & $-$ & 4 & 0 \\
\hline
$j=4$ & 2 & $-$ & 3 & $-$ & 4 & $-$ & 5 & $-$ \\
\hline
$j=5$ & $-$ & 3 & $-$ & 3 & $-$ & 4 & $-$ & 5 \\
\hline
\end{tabular}
\caption{$|S_j(n)|$ = number of symmetric tuple classes}
\end{table}

5.5 Parametrization of symmetric tuples

Let $(\sigma_1, \ldots, \sigma_5)$ be a tuple representing an element of $S_1(n)$. Thus there is $\tau \in S_n$ with $\sigma_i^\tau = \sigma_i^r$ for $i = 1, \ldots, 5$. Then $\sigma_i^3 = \sigma_i^r$, hence $\tau^3 = \sigma_4$. Thus all $\sigma_i$ can be expressed in terms of $\tau$ and $\sigma := \sigma_1$:

$$
\sigma_1 = \sigma, \quad \sigma_2 = \sigma^7, \quad \sigma_3 = \sigma^r, \quad \sigma_4 = \tau^3, \quad \sigma_5 = (\sigma \tau^{-1})^3
$$

(22)

Passing from $(\sigma, \tau, \rho)$ to $(\sigma_1, \ldots, \sigma_5)$ is a case of "translation", see [13] and [21]. Recall that the index $\text{Ind}(\pi)$ of $\pi \in S_n$ is defined as $n$ minus the number of orbits of $\pi$. Since $\sigma = \sigma_1$ is an involution with exactly one fixed point, we have $\text{Ind}(\sigma) = (n - 1)/2$. From $\tau^3 = \sigma_4$ it follows that

$$
\text{Ind}(\rho) \leq \begin{cases} 
\frac{5(n - 3)}{6} + 2 & \text{if } n \equiv 0 \mod 3 \\
\frac{5(n - 5)}{6} + 3 & \text{if } n \equiv 2 \mod 3 
\end{cases}
$$

(23)

where equality holds if and only if $\tau$ has cycle type as in the Lemma below (case $j = 1$). Further, for $\rho := \sigma \tau^{-1}$ we have $\rho^3 = \sigma_5$ (a transposition). Hence

$$
\text{Ind}(\rho) \leq \begin{cases} 
\frac{2(n - 3)}{3} + 1 & \text{if } n \equiv 0 \mod 3 \\
\frac{2(n - 2)}{3} + 1 & \text{if } n \equiv 2 \mod 3 
\end{cases}
$$

(24)

where equality holds if and only if $\rho$ is as in the Lemma below (case $j = 1$).

It follows that $\text{Ind}(\sigma) + \text{Ind}(\tau) + \text{Ind}(\rho) \leq 2(n - 1)$. The reverse inequality holds by the Riemann Hurwitz formula since $<\sigma, \tau, \rho> = S_n$. Hence $\tau$ and $\rho$ are of cycle type as claimed in the following Lemma.

\textbf{Lemma 4.} There is a bijection between $S_j(n)$ and the set of classes of triples $(\sigma, \tau, \rho)$ generating $S_n$ (resp., $A_n$) with $\rho \tau = \sigma$, where $\sigma$ is an involution with exactly one fixed point and $\tau, \rho$ are of the following cycle type:

$j=1$: $\rho$ has one 2-cycle, at most one fixed point and the rest are 3-cycles; $\tau$ has one 3-cycle, at most one 2-cycle and the rest are 6-cycles.
j=2: \( \tau \) has at most one fixed point and its other cycles are all 3-cycles;
\( \rho \) has one 4-cycle, one 3-cycle, at most one 2-cycle and the rest are 6-cycles.

j=4: \( \rho \) has one fixed point, one 2-cycle and the rest are 4-cycles;
\( \tau \) has one 3-cycle and the rest are 4-cycles.

j=5: \( \rho \) has one 2-cycle, one 3-cycle and the rest are 4-cycles;
\( \tau \) has one fixed point and its other cycles are all 4-cycles.

Proof. We only discuss case (1), the other cases are similar. In this case, it remains to show that for given \( \sigma, \tau, \rho \) as in the Lemma, formulas (22) define a tuple \( (\sigma_1, \ldots, \sigma_5) \) representing an element of \( S_5 \). First one verifies that the tuple \( (\sigma'_1, \ldots, \sigma'_5) \) defined as in (21) is conjugate to \( (\sigma_1, \ldots, \sigma_5) \) under \( \tau \). This implies that \( < \sigma_1, \ldots, \sigma_5 > \) is normal in \( < \sigma, \tau >= S_5 \), hence equals \( S_5 \) (since it contains a transposition).

References

1. I. Blake, G. Seroussi and N. Smart, Elliptic Curves in Cryptography, LMS, 265, (1999).
2. R. Brandt, Über Die Automorphismengruppen von algebraischen Funktionenkörpern, (unpublished) PhD thesis. Universität-Gesamthochschule Essen, 1988.
3. R. Brandt and H. Stichtenoth, Die Automorphismengruppen hyperelliptischer Kurven, Man. Math. 55, 83-92, 1986.
4. J. Cassels and V. Flynn, Prolegomena to a Middlebrow Arithmetic of Curves of Genus, LMS, 230, 1996.
5. A. Clebsch, Theorie der binären algebraischen Formen, Verlag von B.G. Teubner, Leipzig, (1872).
6. The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.2, Aachen, St Andrews, 2000, (http://www-gap.dcs.st-and.ac.uk/~gap).
7. P. Gaudry and E. Schost, Invariants des quotients de la Jacobienne d’une courbe de genre 2, (in press)
8. W. Geyer, Invarianten binärer Formen, Lecture Notes in Math., Springer, New York, (1972).
9. G. Frey, On elliptic curves with isomorphic torsion structures and corresponding curves of genus 2. Elliptic curves, modular forms, and Fermat’s last theorem (Hong Kong, 1993), 79-98, Ser. Number Theory, I, Internat. Press, Cambridge, MA, (1995).
10. G. Frey and E. Kani, Curves of genus 2 covering elliptic curves and an arithmetic application. Arithmetic algebraic geometry (Texel, 1989), 153-176, Progr. Math., 89, Birkhäuser, Boston, MA, (1991).
11. G. Frey, E. Kani and H. Völklein, in preparation.
12. M. Fried and H. Völklein, The inverse Galois problem and rational points on moduli spaces, Math. Annalen 290 (1991), 771-800.
13. D. Frohardt and K. Magaard, Composition factors of monodromy groups, to appear in Annals of Math.
14. Kani, E. The number of curves of genus two with elliptic differentials. J. Reine Angew. Math. 485 (1997), 93-121.
15. A. Krazer, Lehrbuch der Thetafunctionen, Chelsea, New York, (1970).
16. J. Igusa, Arithmetic variety of moduli for genus 2. Ann. of Math. (2), 72, 612-649, (1960).
17. C. Jacobi, Review of Legendre, Théorie des fonctions elliptiques. Troiseme supplement, 1832. J. reine angew. Math. 8, 413-417.
18. Maple 6, Waterloo Maple Inc, 2000.
19. K. Magaard, S. Shpectorov, and H. Völklein, Computing the braid group action, in preparation.
20. K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein, The locus of curves with prescribed automorphism group, RIMS Kyoto Technical Report Series, Communications in Arithmetic Fundamental Groups and Galois Theory, 2001, edited by H. Nakamura.
21. G. Malle, Genus zero translates of three point ramified Galois extensions, Manuscr. Math. 71 (1991), 97–111.
22. G. Malle and B.H. Matzat, Inverse Galois Theory, Springer, 1999.
23. B.H. Matzat, Konstruktive Galoistheorie, Lect. Notes in Math. 1284 (1987), Springer, Berlin.
24. P. Mestre, Construction de courbes de genre 2 à partir de leurs modules. In T. Mora and C. Traverso, editors, Effective methods in algebraic geometry, volume 94. Prog. Math., 313-334. Birkhäuser, 1991. Proc. Congress in Livorno, Italy, April 17-21, (1990).
25. H. Lange, Über die Modulvarietät der Kurven vom Geschlecht 2. J. Reine Angew. Math., 281, 80-96, 1976.
26. T. Shaska, Curves of Genus Two Covering Elliptic Curves, PhD thesis, University of Florida, 2001.
27. T. Shaska, Genus 2 curves with (n,n)-decomposable Jacobians, Jour. Symb. Comp., Vol 31, no. 5, pg. 603-617, 2001.
28. T. Shaska, Genus 2 curves with (3,3)-split Jacobian and large automorphism group, ANTS V, Lect. Notes in Comp. Sci., vol. 2369, pg. 100-113, Springer, 2002.
29. H. Völklein, Groups as Galois Groups – an Introduction, Camb. Studies in Adv. Math. 53, Cambridge Univ. Press 1996.