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 $\mathcal{L}_2$ of these fields is a 2-dimensional subvariety of the moduli space $\mathcal{M}_2$ of genus 2 fields. An equation for $\mathcal{L}_2$ is already in the work of Clebsch and Bolza. We use a birational parametrization 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, 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 k of char. $\neq 2$). Jacobi [17] already noted that in this case K has generators X and Y with

$$Y^2 = X^6 - s_1 X^4 + s_2 X^2 - s_3 \tag{1}$$

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 $\mathcal{L}_2$ (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 $\mathcal{M}_1$ of genus 1 curves into $\mathcal{M}_2$.

In section 4 we use the coordinates on $\mathcal{M}_2$ 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 $\mathrm{Aut}(K)$ on elliptic subfields F of odd degree $n \geq 7$. The hyperelliptic involution fixes these subfields, hence they are permuted by $\bar{G}$. It is easy to see that stabilizer $\bar{G}_F$ in $\bar{G}$ of F has order ≤ 3. We study those cases where $\bar{G}_F \neq 1$, assuming $char(k) = 0$. 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, call it $k(X)$. It is the fixed field of the **hyperelliptic involution** e_0 in $\mathrm{Aut}(K)$. Thus e_0 is central in $\mathrm{Aut}(K)$. Here and in the following, $\mathrm{Aut}(K)$ denotes the group $\mathrm{Aut}(K/k)$, more precisely. It induces a subgroup of $\mathrm{Aut}(k(X))$ which is naturally isomorphic to $\overline{\mathrm{Aut}}(K) := \mathrm{Aut}(K)/ < e_0 >$. The latter is called the **reduced automorphism group** of K.

Definition 1. An **elliptic involution** of $G = \mathrm{Aut}(K)$ 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 $\bar{G} = \overline{\mathrm{Aut}}(K)$ 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, E_2 of elliptic subfields of K of degree 2 with $E_1 \cap k(X) = E_2 \cap k(X)$.

Definition 2. We will consider pairs (K, ϵ) with K a genus 2 field and ϵ an elliptic involution in $\bar{G}$. Two such pairs (K, ϵ) and (K', ϵ') are called isomorphic if there is a k-isomorphism $\alpha : K \to K'$ with $\epsilon' = \alpha\epsilon\alpha^{-1}$.

Let ϵ be an elliptic involution in $\bar{G}$. We can choose the generator X of $\mathrm{Fix}(e_0)$ such that $\epsilon(X) = -X$. 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 ϵ. Let j_1 and j_2 be their j-invariants.

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

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

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 ζ_6 is a primitive 6-th root of unity in k. (Thus $\zeta_6 = -1$ if $\mathrm{char}(k) = 3$). Here τ_1 maps (s_1, s_2) to $(\zeta_6^4 s_1, \zeta_6^2 s_2)$, and τ_2 switches s_1, s_2. Invariants of this action are:

$$\begin{aligned} u &:= s_1 s_2 \\ v &:= s_1^3 + s_2^3 \end{aligned} \tag{3}$$

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:

$$
\begin{aligned}
j_1 + j_2 &= 256 \frac{(v^2 - 2u^3 + 54u^2 - 9uv - 27v)}{\Delta} \\
j_1\, j_2 &= 65536 \frac{(u^2 + 9u - 3v)}{\Delta^2}
\end{aligned}
\tag{4}
$$

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 $\mathrm{char}(k) \neq 3$. 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 $\langle \tau_1, \tau_2 \rangle$.

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 α 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 $\langle \tau_1, \tau_2 \rangle$ 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, ϵ) where K is a genus 2 field and ϵ an elliptic involution of $\overline{Aut}(K)$. This parametrization is defined in Lemma 1. The j-invariants of the two elliptic subfields of K associated with ϵ are given by* (4)*.*

ii) The (u, v) satisfying additionally

$$
(v^2 - 4u^3)(4v - u^2 + 110u - 1125) \neq 0 \tag{5}
$$

bijectively parameterize the isomorphism classes of genus 2 fields with $Aut(K) \cong V_4$; 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 $\mathrm{Aut}(K)$ 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 $\mathrm{Aut}(K) \cong V_4$ 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, ϵ) 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 $\mathrm{Aut}(K) \geq D_8$ by Lemma 3(b) below. Under the condition $v = 9(u - 3)$ we get

$$u = 9 - \frac{j}{256}, \quad v = 9(6 - \frac{j}{256})$$

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 $\mathrm{Aut}(K) \cong D_8$, (resp., D_{12}). For all the other values of j, we have $\mathrm{Aut}(K) \cong V_4$. 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

$$\begin{aligned}\Phi_3 = {} & x^4 - x^3y^3 + y^4 + 2232xy(x + y) - 1069956xy(x + y) + 36864000(x^3 + y^3) \\ & + 2587918086x^2y^2 + 8900222976000xy(x + y) + 452984832000000(x^2 + y^2) \\ & - 770845966336000000xy + 1855425871872000000000(x + y)\end{aligned} \tag{6}$$

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

$$(4v - u^2 + 110u - 1125) \cdot g_1(u, v) \cdot g_2(u, v) = 0 \tag{7}$$

where g_1 and g_2 are

$$\begin{aligned}g_1 = {} & -27008u^6 + 256u^7 - 2432u^5v + v^4 + 7296u^3v^2 - 6692v^3u - 1755067500u \\ & + 2419308v^3 - 34553439u^4 + 127753092vu^2 + 16274844vu^3 - 1720730u^2v^2 \\ & - 1941120u^5 + 381631500v + 1018668150u^2 - 116158860u^3 + 52621974v^2 \\ & + 387712u^4v - 483963660vu - 33416676v^2u + 922640625\end{aligned} \tag{8}$$

$$\begin{aligned}g_2 = {} & 291350448u^6 - v^4u^2 - 998848u^6v - 3456u^7v + 4749840u^4v^2 + 17032u^5v^2 \\ & + 4v^5 + 80368u^8 + 256u^9 + 6848224u^7 - 10535040v^3u^2 - 35872v^3u^3 + 26478v^4u \\ & - 77908736u^5v + 9516699v^4 + 307234984u^3v^2 - 419583744v^3u - 826436736v^3 \\ & + 27502903296u^4 + 28808773632vu^2 - 23429955456vu^3 + 5455334016u^2v^2 \\ & - 41278242816v + 82556485632u^2 - 108737593344u^3 - 12123095040v^2 \\ & + 41278242816vu + 3503554560v^2u + 5341019904u^5 - 2454612480u^4v\end{aligned} \tag{9}$$

Vanishing of the first factor is equivalent to $D_{12} \leq G$, see part II of the next section. (Here again $G = \mathrm{Aut}(K)$). 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 $< e_0 >= Gal(K/k(X))$, where $k(X)$ is the unique genus 0 subfield of degree 2 of K. The reduced automorphism group $\bar{G} = G/ < e_0 >$ embeds into $Aut(k(X)/k) \cong \mathrm{PGL}_2(k)$.

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

$$Y^2 = \prod_{\substack{p \in P \\ p \neq \infty}} (X - p) \tag{10}$$

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

Let $\Gamma := \mathrm{PGL}_2(k)$. If l is prime to $char(k)$ then each element of order l of Γ is conjugate to $\begin{pmatrix} \epsilon_l & 0 \\ 0 & 1 \end{pmatrix}$, where ϵ_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 $l = char(k)$ 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 $\mathbb{P}^1$.

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

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

b) If $\bar{g}$ 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 Γ 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 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 Γ with $(|H|, char(k)) = 1$ fixes a point of $\mathbb{P}^1$ then H is cyclic:* Indeed, we may assume $H \leq \{\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}^{\bullet} : b \in k^*, a \in k\}$. 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 Γ 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 ϵ its image in $\bar{G}$. Let u, v be the parameters associated with the pair (K, ϵ) 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

$$4v - u^2 + 110u - 1125 \quad = \quad 0 \tag{11}$$

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

$$v^2 \;-\; 4u^3 \quad = \quad 0 \tag{12}$$

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 $\epsilon = \epsilon_{s_1,s_2}$ 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 $c = \frac{1}{ab}$) into (3) expresses u, v as rational functions of a, b. Substituting these expressions for u, v in (11) and (12) yields

$$\begin{aligned}&(a^4b^3 - a + a^3b + b + 6a^2b^2 + ab^3 - b^4a^3)(a^4b^3 + a - a^3b + b + 6a^2b^2 - ab^3 + b^4a^3)\\&(a^4b^3 - a - a^3b + b - 6a^2b^2 - ab^3 - b^4a^3)(a^4b^3 + a + a^3b + b - 6a^2b^2 + ab^3 + b^4a^3) = 0\end{aligned} \tag{13}$$

respectively

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

(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 ϵ is the only elliptic involution in $\bar{G}$. Hence ϵ is central in $\bar{G}$. If γ is another involution in $\bar{G}$, it follows that $\gamma\epsilon$ is elliptic, contradiction. Thus ϵ is the only involution in $\bar{G}$. Hence either $\bar{G} =< \epsilon >$ or $\bar{G} \cong \mathbb{Z}_6$. The latter case cannot occur, see the case $m = 6$ in the next section.

3.2 The list of automorphism groups

Since $\bar{G} \hookrightarrow S_6$, all elements of $\bar{G}$ have order ≤ 6. For each $m = 4, 5, 6$ with $(p, m) = 1$ there is a unique genus 2 field K such that $\bar{G}$ 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 ∞ (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 $\bar{G}$ contains an element of order 5.

I. Sporadic cases: $\bar{G}$ 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., $\bar{G} \cong S_5$, acting as $\mathrm{PGL}_2(5)$ on $P \cong \mathbb{P}^1(\mathbb{F}_5)$) if $p \neq 5$ (resp., $p = 5$). In each case, $\bar{G}$ 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 $\bar{G}$ 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 $(3^2\ 5^2,\ 2\ 3^3\ 5^3)$. (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 $\cong D_8$. It is a Sylow 2-subgroup of G. Thus

$$G \;\cong\; \mathbb{Z}_3 \rtimes D_8$$

where elements of order 4 in D_8 act on $\mathbb{Z}_3$ by inversion.

$m = 5$: Here $p \neq 5$ and K has equation $Y^2 = X(X^5 - 1)$. Further, $\bar{G} \cong \mathbb{Z}_5$, $G \cong \mathbb{Z}_{10}$. There are no elliptic involutions in this case.

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

Here we assume $\bar{G}$ has an element γ 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 $(z - 1)(z - a)$, $(z - c)(z - c^2 a)$, $(z - c^2)(z - ca)$ have the same constant coefficient, hence are linearly dependent. Hence by Remark 3 there is an elliptic involution ϵ in $\bar{G}$ with $\epsilon(1) = a$, $\epsilon(c) = c^2 a$, $\epsilon(c^2) = ca$. The group $< \epsilon, \gamma >$ is $\cong S_3$, acting regularly on P. Hence by Lemma 3(a) the parameters associated with the pair (K, ϵ) satisfy (11):

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

Intersection of this curve with $\Delta = 0$ is the single point $(9, 54)$. Also the parameter values $(5^2, -2\ 5^3)$ and $(3^2\ 5^2,\ 2\ 3^3\ 5^3)$ 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 ϵ 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 Δ zero).

III. The 1-dimensional family with $G \cong D_8$

In the remaining cases, $\bar{G}$ has only elements of order ≤ 2. Hence $\bar{G} = \{1\}$, $\mathbb{Z}_2$ or V_4. Here we assume $\bar{G} \cong V_4$. Then two of its involutions are elliptic. By Lemma 3(b) it follows that $G \cong D_8$ and the u, v parameters satisfy

$$v^2 \quad = \quad 4u^3$$

Intersection of this curve with $\Delta = 0$ consists of the two points $(9, 54)$ and $(1, -2)$. The values $(0, 0)$, $(5^2, -2\ 5^3)$ and $(3^2\ 5^2,\ 2\ 3^3\ 5^3)$ from Case I are excluded.

IV. The 2-dimensional family with $G \cong V_4$

If $\bar{G} \cong \mathbb{Z}_2$ then its involution ϵ is elliptic. Indeed, we may assume $\epsilon : x \mapsto -x$ and $1 \in P$; if ϵ is not elliptic then $P = \{0, \infty, 1, -1, a, -a\}$ 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, ϵ) has u, v parameters with

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

V. The generic case $G \cong \mathbb{Z}_2$

This occurs if and only if K has no elliptic involutions and is not isomorphic to the field $Y^2 = X(X^5 - 1)$. 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 characteristic $\neq 2$ is isomorphic to $\mathbb{Z}_2$, $\mathbb{Z}_{10}$, V_4, D_8, D_{12}, $\mathbb{Z}_3 \rtimes D_8$, $GL_2(3)$, or 2^+S_5. In the first (resp., last) two cases, G has no (resp., exactly one) class of elliptic 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 $Y^2 = X(X^4 - 1)$.*

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:

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

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

$$
\begin{aligned}
J_2 :=& -240a_0a_6 + 40a_1a_5 - 16a_2a_4 + 6a_3^2 \\
J_4 :=& 48a_0a_4^3 + 48a_2^3a_6 + 4a_2^2a_4^2 + 1620a_0^2a_6^2 + 36a_1a_3^2a_5 - 12a_1a_3a_4^2 - 12a_2^2a_3a_5 + 300a_1^2a_4a_6 \\
&+ 300a_0a_5^2a_2 + 324a_0a_6a_3^2 - 504a_0a_4a_2a_6 - 180a_0a_4a_3a_5 - 180a_1a_3a_2a_6 + 4a_1a_4a_2a_5 \\
&- 540a_0a_5a_1a_6 - 80a_1^2a_5^2 \\
J_6 :=& 176a_1^2a_5^2a_3^2 + 64a_1^2a_5^2a_4a_2 + 1600a_1^3a_5a_4a_6 + 1600a_1a_5^3a_0a_2 \\
&- 160a_0a_4^4a_2 - 96a_0^2a_4^3a_6 + 60a_0a_4^3a_3^2 + 72a_1a_3^4a_5 - 24a_1a_3^3a_4^2 \\
&- 160a_2^4a_4a_6 - 96a_2^3a_0a_6^2 + 60a_2^3a_3^2a_6 - 24a_2^2a_3^3a_5 + 8a_2^2a_3^2a_4^2 \\
&- 900a_2^2a_1^2a_6^2 - 24a_2^3a_4^3 - 36a_2^4a_5^2 - 36a_1^2a_4^4 + 424a_0a_4^2a_2^2a_6 \\
&+ 492a_0a_4^2a_2a_3a_5 + 20664a_0^2a_4a_6^2a_2 + 3060a_0^2a_4a_6a_3a_5 - 468a_0a_4a_3^2a_2a_6 \\
&- 198a_0a_4a_3^3a_5 - 640a_0a_4a_2^2a_5^2 + 3472a_0a_4a_2a_5a_1a_6 - 18600a_0a_4a_1^2a_6^2 \\
&- 876a_0a_4^2a_1a_6a_3 + 492a_1a_3a_2^2a_4a_6 - 238a_1a_3^2a_2a_4a_5 + 76a_1a_3a_2a_4^3 \\
&+ 3060a_1a_3a_0a_6^2a_2 + 1818a_1a_3^2a_0a_6a_5 - 198a_1a_3^3a_2a_6 + 26a_1a_3a_2^2a_5^2 \\
&- 1860a_1^2a_3a_2a_5a_6 + 330a_1^2a_3^2a_6a_4 + 76a_2^3a_4a_3a_5 - 876a_2^2a_0a_6a_3a_5 \\
&+ 616a_2^3a_5a_1a_6 + 2250a_0^2a_5^3a_3 - 900a_0^2a_5^2a_4^2 - 10044a_0^2a_6^2a_3^2 \\
&+ 28a_1a_4^2a_2^2a_5 - 640a_1^2a_4^2a_2a_6 + 26a_1^2a_4^2a_3a_5 - 1860a_1a_4a_0a_5^2a_3 \\
&+ 616a_1a_4^3a_0a_5 - 18600a_0^2a_5^2a_6a_2 + 59940a_0^2a_5a_6^2a_1 + 330a_0a_5^2a_3^2a_2 \\
&- 119880a_0^3a_6^3 - 320a_1^3a_5^3 - 2240a_1^2a_5^2a_0a_6 + 2250a_1^3a_3a_6^2 + 162a_0a_6a_3^4 \\
J_{10} :=& a_6^{-1} Res_X(f, \frac{\partial f}{\partial X})
\end{aligned}
\tag{15}
$$

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

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

$k[J_2, \ldots, J_{10}, J_{10}^{-1}]$, 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:

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

respectively

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

Proof of Remark 1, concluded: The latter formulas explicitly define (in homogeneous coordinates) the map of $\mathcal{M}_1 \backslash \{j = 0\}$ to $\mathcal{M}_2$ from Remark 1. The function $\frac{J_4 J_6}{J_{10}} \in k[\mathcal{M}_2]$ (resp., $\frac{J_2 J_4}{J_6}$) is a linear function in j if $char(k) \neq 3$ (resp., $char(k) = 3$). 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 $\mathcal{M}_2$ defined by the equation*

$$\begin{aligned} &8748 J_{10} J_2^4 J_6^2 - 507384000 J_{10}^2 J_4^2 J_2 - 19245600 J_{10}^2 J_4 J_2^3 - 592272 J_{10} J_4^4 J_2^2 + 77436 J_{10} J_4^3 J_2^4 \\ &-81 J_2^3 J_6^4 - 3499200 J_{10} J_2 J_6^3 + 4743360 J_{10} J_4^3 J_2 J_6 - 870912 J_{10} J_4^2 J_2^3 J_6 + 3090960 J_{10} J_4 J_2^2 J_6^2 \\ &-78 J_2^5 J_4^5 - 125971200000 J_{10}^3 + 384 J_4^6 J_6 + 41472 J_{10} J_4^5 + 159 J_4^6 J_2^3 - 236196 J_{10}^2 J_2^5 - 80 J_4^7 J_2 \\ &-47952 J_2 J_4 J_6^4 + 104976000 J_{10}^2 J_2^2 J_6 - 1728 J_4^5 J_2^2 J_6 + 6048 J_4^4 J_2 J_6^2 - 9331200 J_{10} J_4^2 J_6^2 \\ &+12 J_2^6 J_4^3 J_6 + 29376 J_2^2 J_4^2 J_6^3 - 8910 J_2^3 J_4^3 J_6^2 - 2099520000 J_{10}^2 J_4 J_6 + 31104 J_6^5 - 6912 J_4^3 J_6^3 4 \\ &-J_2^7 J_4^4 - 5832 J_{10} J_2^5 J_4 J_6 - 54 J_2^5 J_4^2 J_6^2 + 108 J_2^4 J_4 J_6^3 + 972 J_{10} J_2^6 J_4^2 + 1332 J_2^4 J_4^4 J_6 = 0 \end{aligned} \tag{17}$$

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 $char(k) \neq 3$.*

Proof. The map is surjective by Theorem 1 and its image is contained in the subvariety of $\mathcal{M}_2$ 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

$$\begin{aligned}(a_1a_2 - a_2 - a_3a_2 + a_3)^2(a_1a_2 - a_1 + a_3a_1 - a_3a_2)^2(a_1a_2 - a_3a_1 - a_3a_2 + a_3)^2\\ (a_3a_1 - a_1 - a_3a_2 + a_3)^2(a_1a_2 + a_1 - a_3a_1 - a_2)^2(a_1a_2 - a_1 - a_3a_1 + a_3)^2\\ (a_3a_1 + a_2 - a_3 - a_3a_2)^2(-a_1 + a_3a_1 + a_2 - a_3)^2(a_1a_2 - a_1 - a_2 + a_3)^2\\ (a_1a_2 - a_1 + a_2 - a_3a_2)^2(a_1 - a_2 + a_3a_2 - a_3)^2(a_1a_2 - a_3a_1 - a_2 + a_3a_2)^2\\ (a_1a_2 - a_3)^2(a_1 - a_3a_2)^2(a_3a_1 - a_2)^2 = 0\end{aligned} \tag{18}$$

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

$$\frac{J_4}{J_2^2}, \quad \frac{J_2J_4 - 3J_6}{J_2^3}, \quad \frac{J_{10}}{J_2^5}$$

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

$$\begin{aligned} i_1 &= \frac{1}{64}\frac{12v + u^2 + 405 - 126u}{(15+u)^2}\\ i_2 &= -\frac{1}{512}\frac{(-1404v + 729u^2 - 3645 + 4131u - 36uv + u^3)}{(15+u)^3}\\ i_3 &= \frac{1}{16384}\frac{(-27 + 18u + u^2 - 4v)^2}{((15+u)^5}\end{aligned} \tag{19}$$

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

$$\begin{aligned}(128i_2 - 48i_1 + 1)u^3 + (5760i_2 + 117 - 3312i_1)u^2 + (86400i_2\\ -66960i_1 - 2349)u + 432000i_2 - 421200i_1 + 10935 = 0\end{aligned} \tag{20}$$

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 $Aut(K)$ on degree n elliptic subfields

In this section we assume char$(k) = 0$. Let $k(X)$, K, G, $\bar{G}$ as in section 3.1 and let $p_1, ..., p_6$ 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 $q_1, ..., q_r$ be the places of $k(Z)$ ramified in $k(X)$. Then $r = 4$ or $r = 5$, and we can label $p_1, ..., p_6$ such that the following holds: p_i lies over q_i for $i = 1, 2, 3$, and p_4, p_5, p_6 lie over q_4. Further one of the following holds:

(1): Here $r = 5$. All places of $k(X)$ over $q_1, ..., q_4$ different from $p_1, ..., p_6$ have ramification index 2; the p_i's have index 1. Finally, there is one place $p^{(2)}$ of ramification index 2 over q_5, and all other places over q_5 have index 1.
(2): Here and in the following cases we have $r = 4$. Here there is one place $p^{(4)}$ of ramification index 4 over q_4. All other places of $k(X)$ over $q_1, ..., q_4$ different from $p_1, ..., p_6$ have ramification index 2; the p_i's have index 1.
(3): Like case (2), only that $p^{(4)}$ lies over q_1.
(4): All places of $k(X)$ over $q_1, ..., q_4$ different from $p_1, ..., p_6$ have ramification index 2. The p_i's have index 1 except for p_1, which has index 3.
(5): Like case (4), only now p_4 has index 3.

5.2 Elliptic subfields of K fixed by an automorphism of K

Let $g \neq 1$ in $\bar{G} = \overline{Aut}(K)$. 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 $n \not\equiv 1 \mod 3$, or we are in case (2) and $n \not\equiv 2 \mod 3$.

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 $p^{(2)}$ resp. $p^{(4)}$. 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 $p^{(2)}$ or $p^{(4)}$. 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 $n \equiv 3 \bmod 4$ (resp., $n \equiv 1 \bmod 4$).

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 $p^{(2)}$ (resp., $p^{(4)}$), 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 $n \not\equiv 1 \bmod 3$ (resp., $n \not\equiv 2 \bmod 3$).

5.3 Application of Riemann's existence theorem

Let ζ_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 $\zeta = \zeta_3$ (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): σ_i is an involution with exactly one fixed point for $i = 1, 2, 3$, resp., three fixed points for $i = 4$, and σ_5 is a transposition.

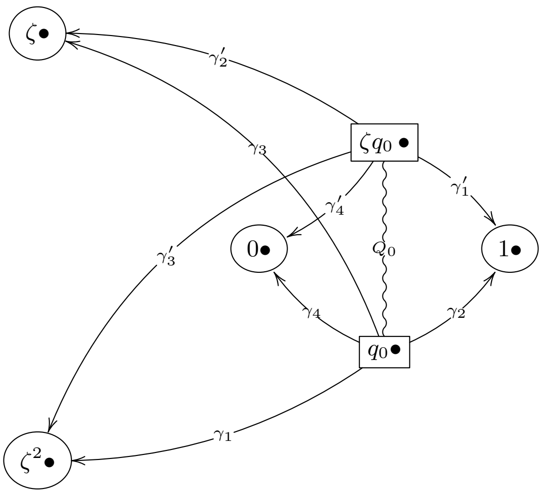
(2): σ_i is an involution with exactly one fixed point for $i = 1, 2, 3$, and σ_4 has three fixed points, one 4-cycle and the rest are 2-cycles.

(3): σ_i is an involution with exactly one fixed point for $i = 2, 3$, and with three fixed points for $i = 4$; and σ_1 has one fixed point, one 4-cycle and the rest are 2-cycles.

(4): σ_i is an involution with exactly one fixed point for $i = 2, 3$, and with three fixed points for $i = 4$; and σ_1 has no fixed points, one 3-cycle and the rest are 2-cycles.

(5): σ_i is an involution with exactly one fixed point for $i = 1, 2, 3$, and σ_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 $\bar{\mathbb{Q}}$, and so one can immediately pass to the case of general k (algebraically closed of char. 0). Here is our choice of the γ_i in case (1); we depict them together with their images γ_i' under the map $z \mapsto \zeta z$. We depict $\gamma_1, ..., \gamma_4$, then γ_5 is given by the basic relation $\gamma_1 \cdots \gamma_5 = 1$. All loops are oriented counter-clockwise.



$$\gamma_1' = \gamma_2$$
$$\gamma_2' = \gamma_3$$
$$\gamma_3' = \gamma_4\gamma_1\gamma_4^{-1}$$
$$\gamma_4' = \gamma_4$$
$$\gamma_5' = \gamma_1^{-1}\gamma_5\gamma_1$$

Fig. 1. The case $q_1, ..., q_r = \zeta^2, 1, \zeta, 0, \infty$, where $\zeta = \zeta_3$

Here we choose q_0 as depicted. Let Q_0 be the line segment joining q_0 and ζq_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 γ_i' in terms of the γ_i.

The tuples $(\sigma_1, ..., \sigma_r)$ corresponding to the extension $\mathbb{C}(X)/\mathbb{C}(Z)$, where $Z = \phi(X)$, are now obtained as follows (see e.g., [29], Ch. 4): Let ϕ 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 σ_i to be the image of γ_i under this homomorphism.

This correspondence between tuples and extensions of $\mathbb{C}(Z)$ 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 $(\sigma_1, ..., \sigma_r)$ gets replaced by $(\sigma_1', ..., \sigma_r')$, where σ_i' is given in terms of $\sigma_1, ..., \sigma_r$ by the same formula that expresses γ_i' in terms of $\gamma_1, ..., \gamma_r$; see Figure 1 above in case (1). In the other cases (where $r = 4$) these formulas appear already in [23] and [21].

(1)

$$\begin{aligned}\sigma_1' &= \sigma_2 \\ \sigma_2' &= \sigma_3 \\ \sigma_3' &= \sigma_4\sigma_1\sigma_4^{-1} \\ \sigma_4' &= \sigma_4 \\ \sigma_5' &= \sigma_1^{-1}\sigma_5\sigma_1\end{aligned} \tag{21}$$

(2)

$$\begin{aligned}\sigma_1' &= \sigma_2 \\ \sigma_2' &= \sigma_3 \\ \sigma_3' &= \sigma_1 \\ \sigma_4' &= \sigma_1^{-1}\sigma_4\sigma_1\end{aligned}$$

(4) and (5)

$$\begin{aligned}\sigma_1' &= \sigma_2\sigma_3\sigma_2^{-1} \\ \sigma_2' &= \sigma_2 \\ \sigma_3' &= \sigma_1 \\ \sigma_4' &= \sigma_1^{-1}\sigma_4\sigma_1\end{aligned}$$

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 $(\sigma_1', ..., \sigma_r')$ is in the same class as $(\sigma_1, ..., \sigma_r)$. 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 $p_1, ..., p_6$, 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 $(\sigma_1, ..., \sigma_r)$ generating S_n or A_n with $\sigma_1 \cdots \sigma_r = 1$ as in (1)—(5). Let $\mathcal{T}_j(n)$ be the set of such tuple classes in case (j), $j = 1, ..., 5$. 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 $|\mathcal{T}_1(n)| = 168, 432, 1100$ and 2184, respectively.

The condition that F is fixed by an automorphism of K (different from the identity and the hyperelliptic involution) means that $(\sigma_1, ..., \sigma_r)$ is in the same class as the tuple $(\sigma_1', ..., \sigma_r')$ defined in (21). Call such tuples **symmetric**. Let $\mathcal{S}_j(n)$ be the set of symmetric tuple classes in $\mathcal{T}_j(n)$. The set $\mathcal{S}_j(n)$ can be parameterized by certain triples, which we describe in the next section. This allows us to compute the cardinality of $\mathcal{S}_j(n)$ 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.

	$n=7$	$n=9$	$n=11$	$n=13$	$n=15$	$n=17$	$n=19$	$n=21$
$j=1$	–	3	2	–	6	3	–	2
$j=2$	1	0	–	2	0	–	4	0
$j=4$	2	–	3	–	4	–	5	–
$j=5$	–	3	–	3	–	4	–	5

Table 1. $|\mathcal{S}_j(n)|$ = number of symmetric tuple classes

5.5 Parametrization of symmetric tuples

Let $(\sigma_1, ..., \sigma_5)$ be a tuple representing an element of $\mathcal{S}_1(n)$. Thus there is $\tau \in S_n$ with $\sigma_i' = \sigma_i^\tau$ for $i = 1, ..., 5$. Then $\sigma_i^{\tau^3} = \sigma_i^{\sigma_4}$, hence $\tau^3 = \sigma_4$. Thus all σ_i can be expressed in terms of τ and $\sigma := \sigma_1$:

$$\sigma_1 = \sigma, \quad \sigma_2 = \sigma^\tau, \quad \sigma_3 = \sigma^{\tau^2}, \quad \sigma_4 = \tau^3, \quad \sigma_5 = (\sigma\tau^{-1})^3 \qquad (22)$$

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

$$\mathrm{Ind}\ (\rho) \quad \leq \begin{cases} \dfrac{5(n-3)}{6} + 2 & \text{if } n \equiv 0 \mod 3 \\ \dfrac{5(n-5)}{6} + 3 & \text{if } n \equiv 2 \mod 3 \end{cases} \qquad (23)$$

where equality holds if and only if τ 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

$$\mathrm{Ind}\ (\rho) \quad \leq \begin{cases} \dfrac{2(n-3)}{3} + 1 & \text{if } n \equiv 0 \mod 3 \\ \dfrac{2(n-2)}{3} + 1 & \text{if } n \equiv 2 \mod 3 \end{cases} \qquad (24)$$

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

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

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

j=1: *ρ has one 2-cycle, at most one fixed point and the rest are 3-cycles; τ has one 3-cycle, at most one 2-cycle and the rest are 6-cycles.*

j=2: *τ has at most one fixed point and its other cycles are all 3-cycles;*
ρ has one 4-cycle, one 3-cycle, at most one 2-cycle and the rest are 6-cycles.

j=4: *ρ has one fixed point, one 2-cycle and the rest are 4-cycles;*
τ has one 3-cycle and the rest are 4-cycles.

j=5: *ρ has one 2-cycle, one 3-cycle and the rest are 4-cycles;*
τ 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 σ, τ, ρ as in the Lemma, formulas (22) define a tuple $(\sigma_1, ..., \sigma_5)$ representing an element of $\mathcal{S}_1(n)$. First one verifies that the tuple $(\sigma_1', ..., \sigma_5')$ defined as in (21) is conjugate to $(\sigma_1, ..., \sigma_5)$ under τ. This implies that $< \sigma_1, ..., \sigma_5 >$ is normal in $< \sigma, \tau >= S_n$, hence equals S_n (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 supplém ent. 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 á partir de leurs modules. In T. Mora and C. Traverso, editors, *Effective methods in algebraic geometry*, volume 94. *Prog. Math.* , 313-334. Birkhäuser, 1991. Proc. Congress in Livorno, Italy, April 17-21, (1990).
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, Cambr. Studies in Adv. Math. 53, Cambridge Univ. Press 1996.