FIELDS OF MODULI AND DEFINITION OF HYPERELLIPTIC COVERS

BY

YOLANDA FUERTES AND GABINO GONZÁLEZ-DIEZ

ABSTRACT. In this paper, for all genera $g > 1$, $g \equiv 1 \ mod\ 4$, we construct an explicit hyperelliptic curve whose field of moduli is $\mathbb{Q}$ such that the minimum subfield of $\mathbb{R}$ over which it can be hyperelliptically defined is a degree three extension of $\mathbb{Q}$. These examples are related to previous work by Earle, Shimura, and Mestre and to a recent conjecture by Shaska.

1. INTRODUCTION

We begin by recalling some basic notions relative to a non singular complex curve C.

The *field of moduli* of C is the minimum subfield $k_0 \subset \mathbb{C}$ such that for every $\sigma \in Gal(\mathbb{C}/k_0)$, C is isomorphic to the curve C^σ.

The curve C is said to be *defined over a field* $k \subset \mathbb{C}$ if there exists a curve C' defined over k such that C is isomorphic to C'. Clearly, the field of moduli is contained in any field of definition.

A hyperelliptic curve will be said to be *hyperelliptically defined* over a field $k \subset \mathbb{C}$ if it is birationally equivalent to a curve of the form $y^2 = q(x)$, where $q(x)$ is a polynomial with simple roots and coefficients in k.

In this paper, for all genera $g > 1$, $g \equiv 1 \ mod\ 4$, we construct an explicit hyperelliptic curve whose field of moduli is $\mathbb{Q}$ such that the minimum subfield of $\mathbb{R}$ over which it can be hyperelliptically defined is a degree three extension of $\mathbb{Q}$. The automorphism group of these curves has order 8. To put matters in perspective we make the following observations.

1) For even genus, Shimura ([15]) has produced examples of hyperelliptic curves of even genus which cannot be defined over $\mathbb{R}$ whose field of moduli is some subfield of $\mathbb{R}$. He also proves that a generic polarized abelian variety of odd dimension is defined over its field of moduli. (Now recall that an algebraic curve C of genus g uniquely defines a polarized abelian variety of dimension g, the jacobian of C, which can be defined over the same field and has the same field of moduli as the curve ([13] and [1])).

2) Earle ([2]), who also restricts the genus to be congruent to 1 modulo 4, has produced other algebraic curves having the same properties as those of Shimura which are discussed above. These algebraic curves are not hyperelliptic because, as it can be seen directly from the construction, they are smooth cyclic coverings of degree $4n$ of a genus two curve; however, according to [11], smooth hyperelliptic cyclic coverings of a hyperelliptic curve could only have degree two.

Key words and phrases. Hyperelliptic curves, automorphisms, field of moduli, field of definition.
2000 *Mathematics Subject Classification.* 14H37, 14H45, 14G99.

3) Mestre ([12]) has shown that being defined over k and being hyperelliptically defined over k are equivalent concepts for a curve of even genus.

4) It follows directly from Weil's seminal paper ([16]) that if a curve C has only the trivial automorphism, then the field of moduli is a field of definition. Recently, Shaska ([14]) has conjectured that if the automorphism group of a hyperelliptic curve has order bigger than two, then its field of moduli is also a field of definition.

We observe that, in particular, our examples show that either Mestre's result does not hold for odd genus or Shaska's conjecture is false.

Notation 1. *Throughout this paper i will denote a fixed square root of -1. (It will never be used as an index).*

2. Smooth hyperelliptic Galois coverings of hyperelliptic curves.

Let us begin by introducing the following hyperelliptic curve

$$C_{ljk}:\ y^2=\prod_{d\neq l,j,k}^{2g+2}\left(x^4-2\left(1-2\frac{\mu_l-\mu_k}{\mu_l-\mu_j}\frac{\mu_d-\mu_j}{\mu_d-\mu_k}\right)x^2+1\right) \tag{1}$$

where the parameters $\mu_{1,\dots,}\mu_{2g+2}$ are distinct complex numbers.

We observe that the coefficient

$$c(k,l,j,d):=\frac{\mu_l-\mu_k}{\mu_l-\mu_j}\frac{\mu_l-\mu_j}{\mu_d-\mu_k}$$

is, precisely, the *cross ratio* of μ_k,μ_l,μ_j,μ_d.

The relevance of this curve rests on the following result ([4], see also [10])

Theorem 2. *Let $S:y^2=\prod_{d=1}^{2g+2}(x-\mu_d)$ be an arbitrary hyperelliptic curve of genus g and $\{P_l=(\mu_l,0),P_j=(\mu_j,0),P_k=(\mu_k,0)\}$ any triple of Weierstrass points. Then, the curve C_{ljk} in (1) is, up to isomorphism, the unique unramified normal 4 to 1 hyperelliptic cover of S with the property that P_l,P_j,P_k are the only Weierstrass points of S which are not covered by Weierstrass points of the covering curve.*

All smooth normal hyperelliptic 4 to 1 coverings of S arise in this way.

The proof of a crucial property of the curve C_{ljk} will depend on the following

Lemma 3.

$$2^2c(k,l,j,d)\left(x^4-2\left(1-2c(j,k,l,d)\right)x^2+1\right)=$$

$$=(i-x)^4-2\left(1-2c(k,l,j,d)\right)(1+x^2)^2+(i+x)^4.$$

Proof. A simple calculation gives the following property of the cross ratio

$$c(j,k,l,d)=\frac{c(k,l,j,d)-1}{c(k,l,j,d)},\ \text{or equivalently}\ \ c(k,l,j,d)=\frac{1}{1-c(j,k,l,d)}.$$

Let us denote by $L(x)$ and $R(x)$ the left hand side and the right hand side of the equality, respectively. To prove that $L(x)=R(x)$ it is enough to check that the coefficient of the leading term, x^4, is the same for both polynomials and that $L(x)$ and $R(x)$ take the same value at the four numbers ±1 and $\pm i$. This is all easy using the above identities. We have

$$R(x) = (i-x)^4 - 2\,(1-2c(k,l,j,d))\,(1+x^2)^2 + (i+x)^4 =$$
$$= -2\,(1-2c(k,l,j,d))\,(1+2x^2+x^4) + 2 - 12x^2 + 2x^4 =$$
$$= 2x^4\,(2c(k,l,j,d)) + x^2\,(-12-4+8c(k,l,j,d)) - 2\,(1-2c(k,l,j,d)) + 2 =$$
$$= 4x^4 c(k,l,j,d) + x^2\,(-16+8c(k,l,j,d)) + 4c(k,l,j,d).$$

This proves the first part. As for the second part we see that

$$\begin{aligned} L(\pm 1) &= 4c(k,l,j,d)(1-2+4c(j,k,l,d)+1) = 16c(k,l,j,d)c(j,k,l,d) = \\ &= 16(c(k,l,j,d)-1), \\ L(\pm i) &= 4c(k,l,j,d)(1+2-4c(j,k,l,d)+1) = 16c(k,l,j,d)(1-c(j,k,l,d)) = 16 \end{aligned}$$

whereas

$$R(\pm 1) = 4c(k,l,j,d) + (-16+8c(k,l,j,d)) + 4c(k,l,j,d) = 16(c(k,l,j,d)-1),$$
$$R(\pm i) = 4c(k,l,j,d) - (-16+8c(k,l,j,d)) + 4c(k,l,j,d) = 16$$

as wanted. □

In the next proposition we list the properties of the curve C_{ljk} we will need

Proposition 4. *The curve C_{ljk} satisfies the following properties:*
I) The genus of C_{ljk} equals $4\,(g-1)+1$.
II) It admits a group of automorphisms $G \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ generated by $\psi(x,y) = (-x,-y)$, $\tau(x,y) = (1/x, -y/x^{4g-2})$ and $J(x,y) = (x,-y)$, the hyperelliptic involution.
III) The first two generate a Klein group $K = \langle \psi, \tau \rangle$ that acts freely on C_{ljk} with quotient C_{ljk}/K isomorphic to the curve $y^2 = \prod_{m=1}^{2g+2}(x-\mu_m)$.
IV) Let us fix the first three coefficients of our defining curve μ_1, μ_2, μ_3. Then, for the generic choice of the remaining $2g-1$ parameters $\mu_4, ..., \mu_{2g+2}$ the corresponding curves C_{ljk} have full group of automorphisms $Aut(C_{ljk})$ equal to G.
V) C_{klj} is isomorphic to C_{ljk} (resp. to C_{jkl}) by means of the isomorphism

$$\phi(x,y) = \left(\tfrac{i-x}{i+x},\ 2^{2g-1} c_{ljk} \tfrac{y}{(x+i)^{2(2g-1)}}\right)$$
$$\textit{(resp. } \Psi(x,y) = \left(-i\tfrac{1+x}{1-x},\ 2^{4g-2} c_{jkl} c_{ljk} \tfrac{y}{((1+i)(1-x))^{2(2g-1)}}\right) \textit{)}$$

where $c_{ljk}^2 = \prod_{d \neq l,j,k} c(k,l,j,d)$.

Proof. I) is obvious. C_{ljk} is a hyperelliptic curve with $4(2g-1)$ Weierstrass points, the points with y-coordinate equal to zero.
II) is easily checked by hand.
III) is part of Theorem 2 contained in [4]. But it can be proved directly by checking that, in fact, the quotient map
$F : C_{klj} \to \left\{ y^2 = \prod_{m=1}^{2g+2}(x-\mu_m) \right\}$ results as composition of the double covers

$$\begin{aligned} F_1 : \quad C_{klj} \quad &\to \quad \left\{ y^2 = \textstyle\prod_{k \neq l,j} \left(x^2 - \frac{\mu_k - \mu_l}{\mu_k - \mu_j} \right) \right\} \\ (x,y) \quad &\to \quad \left(\tfrac{A_k(1+x^2)}{1-x^2}, \tfrac{2xyA_k \sqrt{\prod_{d \neq l,j,k}(A_k^2 - A_d^2)}}{(1-x^2)^{2g}} \right), \quad \text{with } A_k = \sqrt{\tfrac{\mu_k - \mu_l}{\mu_k - \mu_j}} \end{aligned}$$

and

$$\begin{aligned} F_2 : \left\{ y^2 = \textstyle\prod_{k \neq l,j} \left(x^2 - \frac{\mu_k - \mu_l}{\mu_k - \mu_j} \right) \right\} \quad &\to \left\{ y^2 = \textstyle\prod_{m=1}^{2g+2}(x-\mu_m) \right\} \\ (x,y) \quad &\to \left(\tfrac{\mu_l - \mu_j x^2}{1-x^2},\ xy(\mu_l - \mu_j) \tfrac{\sqrt{\prod_{d \neq l,j}(\mu_d - \mu_j)}}{(1-x^2)^{g+1}} \right) \end{aligned}$$

corresponding, respectively, to quotienting by the involution ψ of C_{klj} and the involution $\overline{\tau}$ that τ induces on $C_{klj}/\langle\psi\rangle \equiv \left\{y^2=\prod_{k\neq l,j}\left(x^2-\frac{\mu_k-\mu_l}{\mu_k-\mu_j}\right)\right\}$, namely $\overline{\tau}(x,y)=(-x,-y)$. These are all straightforward computations. For instance, proving that $\overline{\tau}(x,y)=(-x,-y)$ amounts to checking that $F_1\circ\tau(x,y) = F_1\left(\frac{1}{x},\frac{-y}{x^{4g-2}}\right)$ equals $\left(\frac{-A_k(1+x^2)}{1-x^2},\ \frac{-2xyA_k\sqrt{\prod_{d\neq k}(A_k^2-A_d^2)}}{(1-x^2)^{2g}}\right)$.

In order to prove IV) we observe that by III) the quotient of C_{ljk} by G is the same as the quotient of C_{ljk}/K by the automorphism induced by J, which is itself the hyperelliptic involution of C_{ljk}/K. By III) this is the projective line ramified over the set $\{\mu_1,\mu_2,\mu_3,\mu_4,...,\mu_{2g+2}\}$. This means (see [8]) that the set of points in $\mathcal{M}_{\widetilde{g}}$, the moduli space of genus $\widetilde{g}=4g-3$, representing curves admitting a group of automorphisms topologically conjugate to G conform an irreducible subvariety $\mathcal{M}_{\widetilde{g}}(G)\subsetneq\mathcal{M}_{\widetilde{g}}$ of complex dimension $2g-1$. This subvariety, or rather its normalization, is a finite cover (in fact of degree $\binom{2g+2}{3}$, see [10]) of $\mathcal{M}_{0,2+2g}$, the moduli space of $\mathbb{P}^1$ with $2+2g$ *marked points.* Once three of these marked points are chosen, say μ_1,μ_2,μ_3, $\mathcal{M}_{0,2+2g}$ is parametrized by the $2g-1$ remaining ones $\mu_3,\mu_4,...,\mu_{2g+2}$, up to a Möbius like action of the symmetric group Σ_{2g+2} (see[6]). Moreover, if G' is any group strictly containing G, then $\mathcal{M}_{\widetilde{g}}(G')$ is a subvariety of $\mathcal{M}_{\widetilde{g}}(G)$ of lower dimension. This is the content of statement IV).

V) We observe that Theorem 2 implies, in particular, that C_{klj} is isomorphic to C_{ljk}. To prove that, in fact, ϕ performs this isomorphy all one has to see is that $\phi(x,y)=\left(\frac{i-x}{i+x},\ 2^{2g-1}c_{ljk}\frac{y}{(x+i)^{2(2g-1)}}\right)$ lies indeed in C_{ljk}. In other words, one has to check that $\left(2^{2g-1}c_{ljk}\frac{y}{(x+i)^{2(2g-1)}}\right)^2=\prod_{d\neq l,j,k}\left(\left(\frac{i-x}{i+x}\right)^4-2\left(1-2c(k,l,j,d)\right)\left(\frac{i-x}{i+x}\right)^2+1\right)$ whenever $(x,y)\in C_{klj}$. Now, $(x,y)\in C_{klj}$ implies that $\left(2^{2g-1}c_{ljk}\frac{y}{(x+i)^{2(2g-1)}}\right)^2=$

$$=2^{4g-2}\prod_{d\neq klj}c(k,l,j,d)\frac{\prod_{d\neq k,l,j}\left(x^4-2(1-2c(j,k,l,d))x^2+1\right)}{(x+i)^{4(2g-1)}}=$$

$$=\prod_{d\neq l,j,k}\left(2^2c(k,l,j,d)\frac{\left(x^4-2(1-2c(j,k,l,d))x^2+1\right)}{(x+i)^4}\right)=$$

$$=\prod_{d\neq l,j,k}\left(\left(\frac{i-x}{i+x}\right)^4-2\left(1-2c(k,l,j,d)\right)\left(\frac{i-x}{i+x}\right)^2+1\right),$$

the last equality due to lemma 3 above. □

3. The example

The precise curve we shall work with is going to be

$$C:\ y^2=\prod_{d=4}^{2g+2}\left(x^4-2\left(1-2\frac{r_3-r_1}{r_3-r_2}\frac{q_d-r_2}{q_d-r_1}\right)x^2+1\right).$$

That is, C is the curve C_{123} studied in Proposition 4 in which the first three parameters μ_1,μ_2,μ_3 are chosen to be the (real) roots r_1,r_2,r_3 of x^3-3x+1 (or any other degree 3 polynomial $p(x)\in\mathbb{Q}[x]$ whose Galois group has order 3) and the remaining parameters $\mu_4,...,\mu_{2g+2}$ are distinct rational numbers $q_4,...,q_{2g+2}$ chosen so that $Aut(C)$ is isomorphic to $\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2$. This is possible by Proposition 4, IV).

Proposition 5. *I) C is hyperelliptically defined over $\mathbb{Q}(r_1)$.*

II) The field of moduli of C is $\mathbb{Q}$.

Proof. I) Obvious, by hypothesis $r_2, r_3 \in \mathbb{Q}(r_1)$.
II) Let σ be any element of the absolute Galois group $Gal(\overline{\mathbb{Q}})$. Its effect on the parameters μ_i is permuting the first three and preserving each of the remaining ones. Thus, applying σ to the coefficients defining $C = C_{123}$ produces a new curve $C_{123}^{\sigma} := C_{\sigma(1)\sigma(2)\sigma(3)}$ which is isomorphic to C_{123} by Proposition 4, V). □

The rest of the paper is devoted to showing that $\mathbb{Q}(r_1)$ is the minimun subfield of the reals over which C is hyperelliptically defined.

3.1. **The effect of Galois action on C.** Suppose we have a birational isomorphism of algebraic curves $f : C \to C_k$ where C_k is a curve defined over a number field k. Let γ be any element of the Galois group $Gal(\overline{\mathbb{Q}}/k)$. Letting γ act on the coefficients defining the curves C and C_k and the isomorphism f yields a new isomorphism $f^{\gamma} : C^{\gamma} \to C_k^{\gamma} = C_k$. We therefore have a commutative diagram

$$\begin{array}{ccc} C & \underrightarrow{h} & C^{\gamma} \\ f\downarrow & & \downarrow f^{\gamma} \\ C_k & \underrightarrow{id} & C_k \end{array}$$

where h is an isomorphism defined by $h = (f^{\gamma})^{-1} \circ f$. Here we are using the fact that f is also defined over $\overline{\mathbb{Q}}$ (see Remark 11).

We are interested in elements $\gamma \in Gal(\overline{\mathbb{Q}}/k)$ of two particular types.

Proposition 6. *If $\gamma \in Gal(\overline{\mathbb{Q}}/k(r_1))$ then $h = (f^{\gamma})^{-1} \circ f \in Aut(C)$.*

Proof. Obvious. In this case $C^{\gamma} = C$. □

The other kind of elements $\beta \in Gal(\overline{\mathbb{Q}}/k)$ we shall be interested in are those satisfying $\beta(r_1) = r_2$, and $\beta(i) = -i$. For those we have

Proposition 7. *Let $\beta \in Gal(\overline{\mathbb{Q}}/k)$ satisfying $\beta(r_1) = r_2$ and $\beta(i) = -i$, then $(f^{\beta^3})^{-1} \circ f$ is an automorphism of C equals either $\psi \circ \tau$ or $\psi \circ \tau \circ J$.*

Towards proving this statement we first note that for such elements β we have $\beta(r_1) = r_2$, $\beta(r_2) = r_3$ and $\beta(r_3) = r_1$. Therefore, iterating the previous diagram we obtain a larger commutative diagram as follows

$$\begin{array}{ccccccccc} C = C_{123} & \underrightarrow{h} & C_{123}^{\beta} = C_{231} & \underrightarrow{h^{\beta}} & C_{123}^{\beta^2} = C_{312} & \underrightarrow{h^{\beta^2}} & C_{123}^{\beta^3} = C_{123} \\ f\downarrow & & \downarrow f^{\beta} & & \downarrow f^{\beta^2} & & \downarrow f^{\beta^3} \\ C_k & \underrightarrow{id} & C_k & \underrightarrow{id} & C_k & \underrightarrow{id} & C_k. \end{array}$$

We now introduce the following

Notation 8. *For a given isomorphism $\varphi : C_{123} \to C_{123}^{\beta} = C_{231}$, we will denote by $\{\varphi\}$ the automorphism of C_{123} given by $\{\varphi\} = \varphi^{\beta\beta} \circ \varphi^{\beta} \circ \varphi$.*

Note that with this notation $(f^{\beta^3})^{-1}\circ f=\{h\}$, with $h=(f^{\beta})^{-1}\circ f$.

In Proposition 4 we gave a candidate for $\varphi: C_{123}\to C_{123}^{\beta}$, namely $\varphi=\phi$, with

$$\phi(x,y)=\left(\frac{i-x}{i+x},\ 2^{2g-1}c_{231}\frac{y}{(x+i)^{2(2g-1)}}\right).$$

Lemma 9. *We have the following identities*

$$\begin{array}{ll} I) & \psi\circ\phi=\phi\circ\psi\circ\tau, \qquad \psi\circ\phi^{\beta}=\phi^{\beta}\circ\psi\circ\tau.\\ II) & \tau\circ\phi=\phi\circ\psi, \qquad \tau\circ\phi^{\beta}=\phi^{\beta}\circ\psi.\\ III) & J\circ\phi=\phi\circ J, \qquad J\circ\phi^{\beta}=\phi^{\beta}\circ J.\\ IV) & \psi\circ\tau\circ\phi=\phi\circ\tau, \qquad \psi\circ\tau\circ\phi^{\beta}=\phi^{\beta}\circ\tau. \end{array}$$

Here ψ, τ and J are defined by the expressions given in Proposition 4 regardless whether they operate on C_{123} or on C_{123}^{β}.

Proof. The identities on the right hand side are deduced by applying β to the identities of the left hand side as the action of β does not alter the expressions defining ψ, τ and J. Those are easily checked by hand

I) $\phi\circ\psi\circ\tau(x,y)=\phi\left(\frac{-1}{x},\ \frac{y}{x^{2(2g-1)}}\right)=\left(\frac{i+\frac{1}{x}}{i-\frac{1}{x}},\ 2^{2g-1}c_{231}\frac{\frac{y}{x^{2(2g-1)}}}{\left(-\frac{1}{x}+i\right)^{2(2g-1)}}\right)=$

$=\left(\frac{xi+1}{xi-1},\ 2^{2g-1}c_{231}\frac{y}{(-1+xi)^{2(2g-1)}}\right)=\left(\frac{i-x}{-i-x},\ 2^{2g-1}c_{231}\frac{y}{-(x+i)^{2(2g-1)}}\right)=$

$=-\left(\frac{i-x}{i+x},\ 2^{2g-1}c_{231}\frac{y}{(x+i)^{2(2g-1)}}\right)=\psi\circ\phi(x,y).$

II) $\tau\circ\phi(x,y)=\tau\left(\frac{i-x}{i+x},\ 2^{2g-1}c_{231}\frac{y}{(x+i)^{2(2g-1)}}\right)=\left(\frac{i+x}{i-x},-2^{2g-1}c_{231}\frac{y}{(i-x)^{2(2g-1)}}\right)=$

$=\left(\frac{i-(-x)}{i+(-x)},\ 2^{2g-1}c_{231}\frac{-y}{(-x+i)^{2(2g-1)}}\right)=\phi\circ\psi(x,y).$

III) is obvious and IV) follows from combination of I) and II). □

Now Proposition 7 is a consequence of the following lemma.

Lemma 10. *For any isomorphism $\varphi: C\to C^{\beta}$, we have either $\{\varphi\}=\psi\circ\tau$ or $\{\varphi\}=\psi\circ\tau\circ J$.*

Proof. We first note that, while the action of β does not alter the expressions defining ψ, τ and J, it transforms c_{231}^2 into $(c_{231}^2)^{\beta}=c_{312}^2$ which implies that ${c_{231}}^{\beta}=\pm c_{312}$, etc. Hence, it transforms $\phi(x,y)=\left(\frac{i-x}{i+x},\ 2^{2g-1}c_{231}\frac{y}{(x+i)^{2(2g-1)}}\right)$ into

$$\phi^{\beta}(x,y)=\left(\frac{-i-x}{-i+x},\ \pm 2^{2g-1}c_{312}\frac{y}{(x-i)^{2(2g-1)}}\right)$$

and ϕ^{β} into

$$\phi^{\beta\beta}(x,y)=\left(\frac{i-x}{i+x},\ \pm 2^{2g-1}c_{123}\frac{y}{(x+i)^{2(2g-1)}}\right).$$

Since the full automorphism group of C has order 8, there are 8 possibilities for φ. We now check the statement for each of them, using the identities in Lemma 9.
1) For any Weierstrass point $(x,0)$ of C, we have

$\{\phi\}(x,0) = \phi^{\beta\beta}\circ\phi^{\beta}\circ\phi(x,0) = \phi^{\beta\beta}\circ\phi^{\beta}\left(\frac{i-x}{i+x},\ 0\right) = \phi^{\beta\beta}\left(\frac{-i-\frac{i-x}{i+x}}{-i+\frac{i-x}{i+x}},\ 0\right) =$

$= \phi^{\beta\beta}\left(-i\frac{1+x}{1-x},\ 0\right) = \left(\frac{i+i\frac{1+x}{1-x}}{i-i\frac{1+x}{1-x}},\ 0\right) = \left(\frac{-1}{x},\ 0\right) = \psi\circ\tau(x,0).$

In other words $\{\phi\}$ and $\psi\circ\tau$ coincide on the Weierstrass points of C. Therefore, we must have either $\{\phi\} = \psi\circ\tau$ or $\{\phi\} = \psi\circ\tau\circ J$ (see [3] or [4]).

2) $\{\phi\circ J\} = \phi^{\beta\beta}\circ J\circ\phi^{\beta}\circ J\circ\phi\circ J = \{\phi\}\circ J.$

3) $\{\phi\circ\psi\} = \phi^{\beta\beta}\circ\psi\circ\phi^{\beta}\circ\psi\circ\phi\circ\psi = \phi^{\beta\beta}\circ\phi^{\beta}\circ\psi\circ\tau\circ\psi\circ\phi\circ\psi =$

$= \phi^{\beta\beta}\circ\phi^{\beta}\circ\tau\circ\phi\circ\psi = \phi^{\beta\beta}\circ\phi^{\beta}\circ\phi\circ\psi\circ\psi = \phi^{\beta\beta}\circ\phi^{\beta}\circ\phi = \{\phi\}.$

4) $\{\phi\circ\tau\} = \phi^{\beta\beta}\circ\tau\circ\phi^{\beta}\circ\tau\circ\phi\circ\tau = \phi^{\beta\beta}\circ\phi^{\beta}\circ\psi\circ\tau\circ\phi\circ\tau =$

$= \phi^{\beta\beta}\circ\phi^{\beta}\circ\phi\circ\tau\circ\tau = \{\phi\}.$

5) $\{\phi\circ\psi\circ J\} = \{\phi\circ\psi\}\circ J = \{\phi\}\circ J.$

6) $\{\phi\circ\tau\circ J\} = \{\phi\circ\tau\}\circ J = \{\phi\}\circ J.$

7) $\{\phi\circ\psi\circ\tau\} = \phi^{\beta\beta}\circ\psi\circ\ \tau\circ\phi^{\beta}\circ\psi\circ\tau\circ\phi\circ\psi\circ\tau =$

$= \phi^{\beta\beta}\circ\phi^{\beta}\circ\tau\circ\phi\circ\tau\circ\psi\circ\tau = \phi^{\beta\beta}\circ\phi^{\beta}\circ\phi\circ\psi\circ\tau\circ\psi\circ\tau = \{\phi\}.$

8) $\{\phi\circ\psi\circ\tau\circ J\} = \{\phi\circ\psi\circ\tau\}\circ J = \{\phi\}\circ J.$ □

3.2. **On the field of definition of C.** Let us now assume that C is hyperelliptically defined over a number field k. Thus, from now on, $f : C \to C_k$ denotes a birational isomorphism between our curve C and a curve C_k of the form

$$C_k\colon y^2 = q(x),\ \text{ with }\ q(x)\in k[x]\ \text{ without multiple roots.}$$

Let $(x,y)\in C_k$ with $x\in\mathbb{Q}$ and let $(a,b)\in C$ such that $f(a,b) = (x,y)$ hence, by the uniqueness of the hyperelliptic involution, $f(a,-b) = (x,-y)$.

We now analyze the effect of applying a Galois element $\gamma\in Gal\left(\overline{\mathbb{Q}}/k(r_1)\right)$ to the point (a,b).

We have $f^{\gamma}(a^{\gamma},b^{\gamma}) = (f(a,b))^{\gamma} = (x,y)^{\gamma} = (x,\pm y) = f(a,\pm b) = f^{\gamma}\circ h(a,\pm b)$, where $h := (f^{\gamma})^{-1}\circ f\in Aut(C)$ as $C^{\gamma} = C$ and $C_k^{\gamma} = C_k$. It follows that $(a^{\gamma},b^{\gamma}) = h(a,\pm b)$. Now by Proposition 4, we explicitly know the (eight) possibilities for h. Therefore, we can equate the first coordinates in the last identity to find that $a^{\gamma} = \pm a,\ \pm a^{-1}$(resp. $\gamma(a^2) = a^{\pm 2}$). From here we draw the following consequences

a) $k(r_1,a)$ *(resp.* $k\left(r_1,a^2\right)$*) is a Galois extension of* $k(r_1)$ *of degree* $1,2$ *or* 4 (resp. 1 or 2).

b) If $\gamma = \beta^3$*, for some* β *as in Proposition 7, then* $a^{\gamma} = \beta^3(a) = -1/a$, since in that case h equals either $\psi\circ\tau$ or $\psi\circ\tau\circ J$.

c) If $k\subset\mathbb{R}$ and we take $\gamma =$ *complex conjugation*, we see that $\gamma(a) = \overline{a} = a,\ -a,\ a^{-1}$, as $\overline{a} = -a^{-1}$ cannot occur.

d) If $r_1\notin k$ then $k(r_1,a,i)$ *is a Galois extension of* k *of degree* 3, 6, 12 or 24.

Remark 11. *In the above discussion we have tacitly used the fact that the isomorphisms* f *and* f^{-1}*, hence the point* (a,b)*, are defined over* $\overline{\mathbb{Q}}$ *(see* [7]*).*

We shall need the following elementary observation in Galois theory.

Lemma 12. *Let k be a number field admitting a Galois extension L of k of degree $3n$, with n prime to 3, such that $r_1 \in L \setminus k$. Then, there exists $\gamma \in Gal(L/k)$ of order three such that $\gamma(r_1) = r_2$.*

Proof. By Cauchy's theorem there is $\gamma \in Gal(L/k)$ of order 3. Moreover it cannot occur $\gamma(r_1) = r_1$ for in that case γ would induce an element of $Gal(L/k(r_1))$ but the degree of $L/k(r_1)$ is not a multiple of 3. Thus, by replacing, if necessary, γ by γ^2 we can assume that $\gamma(r_1) = r_2$. □

Next we construct a Galois element β as required in Proposition 7.

Proposition 13. *Let us assume that $r_1 \notin k \subset \mathbb{R}$ and let L be the field $L = k(r_1, a, i)$. Then, there exist $\beta \in Gal(L/k)$ such that $\beta(r_1) = r_2$, $\beta(i) = -i$ and $\beta^3(a) \neq -1/a$.*

Proof. i) Suppose first that $a \in k(r_1, i)$.
We apply Lemma 12 to obtain $\gamma \in Gal(L/k)$ such that $\gamma(r_1) = r_2$ and $ord(\gamma) = 3$, hence $\gamma(i) = i$. Next we let β be defined by $\beta(x) = \overline{\gamma(x)}$. It is clear that $\beta(r_1) = r_2$, $\beta(i) = -i$ and $\beta^3(a) = \overline{a} \neq -1/a$.
ii) Assume now that $a \notin k(r_1, i)$.
We split this case into two subcases according to whether or not $a^2 \in k(r_1, i)$.
ii.a) If $a^2 \in k(r_1, i)$ we argue as above to find $\beta' \in Gal(L'/k)$ with $L' = k\left(r_1, a^2, i\right) = k(r_1, i)$ such that $\beta'(r_1) = r_2$, $\beta'(i) = -i$ and $\beta'^3(a^2) = \overline{a}^2$. We claim that there is an extension $\beta \in Gal(L/k)$ of β' satisfying $\beta^3(a) = \overline{a}$, as in the previous case.
Towards proving our claim, we first observe that, since $a \notin L'$, the group $Gal(L/k)$ has order 12 and that the minimum polynomial of a over L' is $X^2 - a^2$. It follows that β' admits two distinct extensions to L, say β_1, $\beta_2 \in Gal(L/k)$, both satisfying $\beta_d^3(a) = \pm\overline{a}$, hence both of order 6. Moreover, β_1 and β_2 generate different subgroups isomorphic to $\mathbb{Z}_6$, because, $\beta_2 \neq \beta_1^5$, as can be seen by applying both elements to r_1. This, in turn, implies that our group $Gal(L/k)$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_6$, as the latter is the unique group of order 12 with more than one subgroup isomorphic to $\mathbb{Z}_6$ (see, e.g., [9] pp. 98-99). Now, direct inspection inside $\mathbb{Z}_2 \times \mathbb{Z}_6$ shows that $\beta_2^3 \neq \beta_1^3$. Therefore one of these two elements must satisfy $\beta_d^3(a) = \overline{a}$ as claimed.
ii.b) If $a^2 \notin k(r_1, i)$ then $i \notin L' := k\left(r_1, a^2\right)$, for $i \in L'$ would imply $k(r_1, i) = k\left(r_1, a^2\right)$ as both are extensions of degree 2 of $k(r_1)$. We can now extend the element $\gamma \in Gal(L'/k)$ with $\gamma(r_1) = r_2$ and $ord(\gamma) = 3$ given in Lemma 12 to an element $\beta \in Gal(L/k)$ by setting $\beta(i) = -i$. We will have $\beta^3(a^2) = \gamma^3(a^2) = a^2 \neq 1/a^2$ since, by condition ii), $a^2 \neq \pm 1$. This obviously implies that $\beta^3(a) \neq -1/a$. □

Theorem 14. *$\mathbb{Q}(r_1)$ is the minimum subfield of $\mathbb{R}$ over which the curve $C = C_{123}$ admits a hyperelliptic model. In particular C does not have a hyperelliptic model over $\mathbb{Q}$.*

Proof. If $\beta \in Gal(\overline{\mathbb{Q}})$ is any element satisfying the properties required in Proposition 7 then, as observed in point b) of the above discussion, $\beta^3(a) = -1/a$. But in Proposition 13 such an element satisfying $\beta^3(a) \neq -1/a$ has been constructed. The contradiction must come from our assumption that $r_1 \notin k \subset \mathbb{R}$. □

Acknowledgements. We are grateful to G. Cardona and B. Poonen for clarifying to us several points concerning the subject of this paper.

We are also grateful to the referee for suggesting the present short proof of Lemma 3 to us.

Both authors are partially supported by Grant BFM2003–04964 of the MCYT.

References

[1] W.L. Baily. *On the Theory of θ-Functions*, The Moduli of Abelian Varieties, and the Moduli of Curves. Annals of Math. **75**, N^o 2, March (1962), 281-342.

[2] C. Earle. *On the moduli of closed Riemann surfaces with symmetry*, pp 119-130, Advances in the theory of riemann surfaces, Ann. of Math. Studies **66**, Princeton 1971.

[3] H. Farkas and I. Kra. *Riemann surfaces*. Springer-Verlag, Berlin and New York, 1980.

[4] Y. Fuertes and G. González-Diez. *Smooth normal coverings of hyperelliptic curves,* submitted.

[5] Y. Fuertes and G. González-Diez. *On the number of coincidences of morphisms between closed Riemann surfaces*. Publicacions Matematiques, Vol. **37** (1993), 339-353.

[6] G. González-Diez. *Loci of curves which are prime Galois coverings of* $\mathbb{P}^1$. Proc. London Math. Soc., (3) **62** (1991), 469-489.

[7] G. González-Diez. *Variations on Belyi's theorem,* submitted.

[8] G. González-Diez and W.J. Harvey. *Moduli of Riemann surfaces with symmetry*. Discrete Groups and Geometry. London Math. Soc. Lecture Note Series **173**.

[9] T.W. Hungerford. *Algebra*, Springer-Verlag, New York, 1974.

[10] R. Horiuchi. *Normal coverings of hyperelliptic Riemann surfaces*, J. Math. Kyoto Univ. **19-3** (1979), 497-523.

[11] C. Maclachlan. *Smooth coverings of hyperelliptic surfaces*, Quart. J. Math. Oxford Ser(2). **22** (1971), 117-123.

[12] J-F Mestre. *Construction de courbes de genre 2 à partir de leur modules*. Effective methods in algebraic geometry (Castiglionello, 1990), 313-334. Prog. Math. **94**. Birkhäuser Boston, MA, 1991.

[13] J.S. Milne. *Jacobians Varieties*, 167-212 in: G. Cornell, J.H. Silverman (ed.): Arithmetic Geometry, Springer-Verlang (1986).

[14] T. Shaska. *Computational algebra and algebraic curves*. ACM SIGSAM Bulletin, Vol. **37**, N^o 4, December 2003.

[15] G. Shimura. *On the field of rationality for an abelian variety*. Nagoya Math. J. **45** (1972), 167-178.

[16] A. Weil. *The field of definition of a variety*. Amer. J. Math. **78** (1956), 509-524.

Departamento de Matemáticas,
U. Autónoma de Madrid,
28049 Madrid, Spain.
E-mail address: yolanda.fuertes@uam.es, gabino.gonzalez@uam.es