Rev. Mat. Iberoam. **33** (2017), no. 1, 169–182
DOI 10.4171/RMI/931

Twists of non-hyperelliptic curves

Elisa Lorenzo García

Abstract. In this paper we present a method for computing the set of twists of a non-singular projective curve defined over an arbitrary (perfect) field k. The method is based on a correspondence between twists and solutions to a Galois embedding problem. When in addition, this curve is non-hyperelliptic we show how to compute equations for the twists. If $k = \mathbb{F}_q$ the method then becomes an algorithm, since in this case, it is known how to solve the Galois embedding problems that appear. As an example we compute the set of twists of the non-hyperelliptic genus 6 curve $x^7 - y^3 - 1 = 0$ when we consider it defined over a number field such that $[k(\zeta_{21}) : k] = 12$. For each twist equations are exhibited.

1. Introduction

The study of twists of curves can be a very useful tool for understanding some arithmetic problems. For example, it has been proved to be really helpful for exploring the Sato–Tate conjecture [8], [10], [11], [12],[14], as well as for solving some Diophantine equations [18] or computing $\mathbb{Q}$-curves realizing certain Galois representations [2], [7].

The twists of curves of genus ≤ 2 are well known. While the genus 0 and 1 cases date back a long time [20, X, Proposition 5.4], the genus 2 case is due to the work of Cardona and Quer over number fields [3], [5], and to Cardona over finite fields [4]. All genus 0, 1 or 2 curves are hyperelliptic (at least in the sense that they are not non-hyperelliptic, since genus 0 and 1 curves are not usually called hyperelliptic). However, for genus greater than 2 almost all curves are non-hyperelliptic. Only few twists of genus 3 curves over number fields have been previously computed [7], [18]. Over finite fields, more twists of curves of genus 3 have been computed [16], but, in this case, equations are not given.

We devote the present paper to presenting a method for computing twists of smooth curves of genus greater than 0, and in the particular case of non-hyperelliptic curves we show how to compute equations for the twists. The method

Mathematics Subject Classification (2010): Primary 11G30; Secondary 12F12, 14H99.
Keywords: Twists, non-hyperelliptic curves, Galois embedding problems.

is not completely original since it is based on well-known results, but as far as we know this is the first time that all the strategies used for computing twists are joined together and all the gaps are filled in order to produce a systematic method. In particular, when the field of definition of the curve has characteristic different from zero, the method gives rise to an algorithm.

In a forthcoming paper [15], this method will be useful for computing the twists of all non-hyperelliptic genus 3 curves defined over any number field.

1.1. Outline

The structure of this paper is as follows. Section 2 establishes a correspondence between the set of twists of any smooth and irreducible genus $g > 0$ curve C defined over a perfect field k and the set of solutions to a Galois embedding problem, see Theorem 2.2. In Section 3, we show how to compute equations of the twists in the particular case in which the curve C is non-hyperelliptic. We do this by studying the action of the Galois group of a certain extension of the field of definition of the curve C, in the vector space of regular differentials $\Omega^1(C)$. Section 4 describes in detail the method obtained for computing the twists of non-hyperelliptic curves. The first step is computing a canonical model of the curve. The second one is posing the corresponding Galois embedding problem, whose solutions are in bijection with the set of twists, and solving it. In general, if k is a number field, there is no known method for solving a Galois embedding problem over k, and this step should be treated on a case-by-case basis. We compute the solutions to an infinity family of such problems in Proposition 4.1. Nevertheless, if k is a finite field, it is known how to solve any Galois embedding problem over k (e.g., [19], Chapter 1). The third and last step is computing equations for the twists. Finally, in Section 5 we illustrate the method by computing all the twists of the non-hyperelliptic genus 6 curve $x^7 - y^3 - 1 = 0$ when it is considered to be defined over a number field such that $[k(\zeta_{21}) : k] = 12$.

1.2. Notation

We now fix some notation and conventions that will be valid through the paper. For any field F, we denote by $\bar{F}$ an algebraic closure of F, and by G_F the absolute Galois group $\mathrm{Gal}(\bar{F}/F)$. We recurrently consider the action of G_F on several sets, and this action is in general denoted by left exponentiation. For a field F, let $\mathrm{GL}_n(F)$ (resp. $\mathrm{PGL}_n(F)$) be the group of n by n invertible matrices with coefficients in F (resp. that are projective).

By k we always mean a perfect field. All field extensions of k that we consider are contained in a fixed algebraic closure $\bar{k}$. We write ζ_n to refer to a primitive n-th root of unity in $\bar{k}$. When k is a number field, we denote by $\mathcal{O}_k$ the ring of integers of k.

Given a projective, smooth and geometrically irreducible curve C/k we denote by $\mathrm{Aut}(C)$ the group of automorphisms of C defined over $\bar{k}$. By K we denote the minimal extension K/k where all the automorphism of C can be defined. The k-vector space of regular differentials of C is denoted by $\Omega^1(C)$.

Acknowledgments. The author would like to thank Joan-Carles Lario for bringing this problem to her attention and Francesc Fité for a careful reading of the manuscript and useful comments and suggestions. The author is also grateful to the anonymous referees for their valuable comments which helped to improve the clarity of the manuscript.

2. Galois embedding problems

Let k be a perfect field and C/k be a projective curve of genus $g>0$. Recall that K denotes the minimal field over which all the automorphisms of C can be defined. Since the curve C is defined over k, the extension K/k is Galois. Define the twisting group $\Gamma := \operatorname{Aut}(C) \rtimes \operatorname{Gal}(K/k)$, where $\operatorname{Gal}(K/k)$ acts naturally on $\operatorname{Aut}(C)$, and the multiplication rule is $(\alpha,\sigma)(\beta,\tau)=(\alpha\,{}^{\sigma}\beta,\sigma\tau)$ ([9], Section 2).

Define the following sets:

$$\operatorname{Twist}_k(C) := \left\{C'/k\,\text{curve} \mid \exists\,\overline{k}\text{-isomorphism } \phi\colon C'\to C\right\}/k\text{-isomorphism}, \tag{2.1}$$

$$\mathrm{H}^1(G_k,\operatorname{Aut}(C)) := \{\xi\colon G_k\to\operatorname{Aut}(C)\text{ continuous} \mid \xi_{\sigma\tau}=\xi_\sigma\cdot{}^{\sigma}\,\xi_\tau\}\,/\sim, \tag{2.2}$$

where the topology in G_k is the profinite one, and we consider the discrete topology in $\operatorname{Aut}(C)$. Two cocycles are cohomologous $\xi\sim\xi'$, if and only if, there is $\varphi\in\operatorname{Aut}(C)$ such that $\xi'_\sigma=\varphi\cdot\xi_\sigma\cdot{}^{\sigma}\varphi^{-1}$.

We denote by $\pi_2\colon\Gamma\to\operatorname{Gal}(K/k)$ (resp. π_1) the projection on the second (resp. first) component of the elements of Γ. A continuous group homomorphism $\Psi\colon G_k\to\Gamma$ (again with the profinite and discrete topologies respectively), such that the composition $\pi_2\circ\Psi : G_k\to\Gamma\to\operatorname{Gal}(K/k)$ equals the natural projection $G_k\twoheadrightarrow\operatorname{Gal}(K/k) : \sigma\twoheadrightarrow\bar\sigma$, is called a pro$_2$-morphism.

We also define

$$\widetilde{\operatorname{Hom}}(G_k,\Gamma) := \{\Psi\colon G_k\to\Gamma \mid \Psi\ \text{pro}_2\text{-morphism}\}\,/\sim, \tag{2.3}$$

We say that $\Psi\sim\Psi'$ are equivalent if there is $(\varphi,1)\in\Gamma$ such that $\Psi'_\sigma=(\varphi,1)\Psi_\sigma(\varphi,1)^{-1}$.

Definition 2.1. With notation above, we say that L is the splitting field of the twist $\phi\colon C'\to C$, if L is the minimal field where, for all $\alpha\in\operatorname{Aut}(C)$, the isomorphisms $\alpha\circ\phi$ are defined. Since the curves C and C' are defined over k, the extension L/k is Galois, and clearly $K\subseteq L$. Similarly, we define the splitting field of a cocycle ξ as the field L that satisfies the condition

$$\operatorname{Gal}(\bar k/L)=\bigcup_{\xi\sim\xi'}\operatorname{Ker}(\xi')\,.$$

Since $\operatorname{Aut}(C)$ is finite, there is a finite number of equivalent cocycles and their kernels are fundamental open sets in G_k. Thus, the field L is well-defined.

For an element $\Psi\in\widetilde{\operatorname{Hom}}(G_k,\Gamma)$, we define its splitting field as the field L such that $\operatorname{Gal}(\bar k/L)=\operatorname{Ker}(\Psi)$. Since Ψ is continuous, such field exists.

Note that the previous splitting fields are all of them finite extensions of k since we are considering curves of genus greater than 0, and then the group $\mathrm{Aut}(C)$ is finite.

Theorem 2.2. *There are natural one-to-one correspondences between the following three sets:*

$$\mathrm{Twist}_k(C) \longrightarrow \mathrm{H}^1(G_k, \mathrm{Aut}(C)) \longrightarrow \widetilde{\mathrm{Hom}}(G_k, \Gamma)$$

These correspondences send ϕ to $\xi_\sigma = \phi \cdot {}^\sigma\phi^{-1}$, and ξ to $\Psi_\sigma = (\xi_\sigma, \overline{\sigma})$. Moreover, the splitting fields of elements in these three sets are preserved by these correspondences.

Proof. The correspondence between the set (2.1) of twists $\mathrm{Twist}_k(C)$ and the first Galois cohomology set (2.2) is well known, and can be found in [20], X.2 Theorem 2.2. The statement about the splitting fields follows by definition. So, it only remains to prove that the map between the sets (2.2) and (2.3) is a bijection. Let us first prove that it is well-defined. Clearly, given $\xi \in \mathrm{H}^1(G_k, \mathrm{Aut}(C))$, we have that Ψ defined by $\Psi_\sigma := (\xi_\sigma, \overline{\sigma})$ defines an element in $\widetilde{\mathrm{Hom}}(G_k, \Gamma)$. Conversely, given an element $\Psi \in \widetilde{\mathrm{Hom}}(G_k, \Gamma)$, we have that $\xi := \pi_1(\Psi)$ defines an element in $\mathrm{H}^1(G_k, \mathrm{Aut}(C))$. Finally, it is a straightforward computation to check that this two maps are one inverse to the other and that they preserve the equivalence relations defined in both sets. □

For the reader's convenience, we recall here the definition of a Galois embedding problem.

Definition 2.3. (Definition 9.4.1 in [17]) A Galois embedding problem $\mathcal{E}(G, \varphi, \alpha)$ for the profinite group G is a diagram

$$\begin{tikzcd}
 & & & G \arrow[d, "\varphi"'] & \\
1 \arrow[r] & A \arrow[r] & E \arrow[r, "\alpha"'] & \bar{G} \arrow[r] & 1
\end{tikzcd}$$

with an exact sequence of profinite groups and a surjection π.

i) A solution of the embedding problem $\mathcal{E}$ is a homomorphism $\psi\colon G \to E$ such that $\alpha \circ \psi = \varphi$. A solution is called proper if ψ is surjective.

ii) Two solutions ψ and ψ' are called equivalent if $\psi'(\sigma) = a^{-1}\psi(\sigma)a$ for all $\sigma \in G$ with a fixed element $a \in A$.

Remark 2.4. Note that any element $\Psi \in \widetilde{\mathrm{Hom}}(G_k, \Gamma)$ can be reinterpreted as a solution to the following Galois embedding problem:

(2.4)
$$\begin{tikzcd}
 & & & G_k \arrow[d] \arrow[dl, dashed, "\Psi"'] & \\
1 \arrow[r] & \mathrm{Aut}(C) \arrow[r, hook] & \Gamma \arrow[r, "\pi"'] & \mathrm{Gal}(K/k) \arrow[r] & 1
\end{tikzcd}$$

Reciprocally, every solution Ψ of the above embedding problem is an element in $\widetilde{\operatorname{Hom}}(G_k, \Gamma)$ and gives rise to a twist of C. In order to keep track of the equivalence classes of twists we must here consider two solutions Ψ and Ψ' equivalent only under the restricted conjugations allowed in the definition of the set $\widetilde{\operatorname{Hom}}(G_k, \Gamma)$.

This remark and Theorem 2.2 allow us to reinterpret the set of twists of a curve as the set of solutions of a Galois embedding problem, which is the crucial observation in the method presented in this paper.

3. Equations of the twists

First of all, remark that a twist is not a curve, it is an equivalence class of curves, so when we say that we compute equations for a twist, what we mean is that we compute equations for some particular curve in the equivalence class. Secondly, note that a curve can have different models, and a particular model for a non-hyperelliptic curve is its canonical model, that is, the model given by the embedding defined by the canonical class. The method that we present in this section, is a method for computing the canonical model of a curve in the equivalence class of a twist defined by a cocycle.

This method is a generalization of the one used by Fernández, González and Lario [7], Section 4. They used it for computing equations of twists of some particular non-hyperelliptic genus 3 curves, a special case for which the canonical model coincides with the plane model.

Note that, in our context, finding equations for a twist that is given by a cocycle $\xi \in \mathrm{H}^1(G_k, \operatorname{Aut}(C))$, is actually equivalent to computing an inverse map for the correspondence in Theorem 2.2

$$\operatorname{Twist}_k(C) \longrightarrow \mathrm{H}^1(G_k, \operatorname{Aut}(C))\,.$$

Let $\Omega^1(C)$ be the k-vector space of regular differentials of C. Let $\omega_1, \dots, \omega_g$ be a basis of $\Omega^1(C)$, where g is the genus of C (the existence of such a basis can be deduced from the fact that there always exists a canonical divisor defined over the definition field k of the curves, which is a consequence of [20], II, Lemma 5.8.1). Given a cocycle $\xi\colon \mathrm{G}_k \to \operatorname{Aut}(C)$ and its splitting field L, we consider the extension of scalars $\Omega^1_L(C) = \Omega^1(C) \otimes_k L$ which is a k-vector space of dimension $g[L:k]$. We can then view the elements of $\Omega^1_L(C)$ as sums $\sum \lambda_i\, \omega_i$ where $\lambda_i \in L$. For every $\sigma \in \operatorname{Gal}(L/k)$, we consider the twisted action on $\Omega^1_L(C)$ defined as follows:

$$\Big(\sum \lambda_i\, \omega_i\Big)_\xi^\sigma := \sum {}^\sigma\lambda_i\, \xi_\sigma^{*-1}(\omega_i).$$

Here, $\xi_\sigma^* \in \operatorname{End}_K(\Omega^1(C))$ denotes the pull-back of $\xi_\sigma = \phi \cdot {}^\sigma \phi^{-1} \in \operatorname{Aut}_K(C)$. One readily checks that

$$\rho_\xi\colon \operatorname{Gal}(L/k) \to \operatorname{GL}(\Omega^1_L(C)), \quad \rho_\xi(\sigma)(\omega) := \omega_\xi^\sigma$$

is a k-linear representation. Indeed, since $\xi^*_{\sigma\tau} = {}^{\sigma}\xi^*_{\tau} \cdot \xi^*_{\sigma}$, we have

$$\begin{aligned}\rho_\xi(\sigma\tau)\Big(\sum \lambda_i\,\omega_i\Big) &= \sum {}^{\sigma\tau}\lambda_i\,\xi^{*-1}_{\sigma\tau}(\omega_i) = \sum {}^{\sigma\tau}\lambda_i\,\xi^{*-1}_{\sigma} \cdot^{\sigma} \xi^{*-1}_{\tau}(\omega_i)\\ &= \rho_\xi(\sigma)\Big(\sum {}^{\tau}\lambda_i\,\xi^{*-1}_{\tau}(\omega_i)\Big) = \rho_\xi(\sigma)\rho_\xi(\tau)\Big(\sum \lambda_i\,\omega_i\Big).\end{aligned}$$

Lemma 3.1. *Let $\phi\colon C \to C'$ be a twist such that $\phi \cdot^{\sigma} \phi^{-1} = \xi_\sigma$. Then, the following k-vector spaces are isomorphic:*

$$\Omega^1_L(C)^{\mathrm{Gal}(L/k)}_{\xi} \simeq \Omega^1(C')\,.$$

Proof. We claim that the map $\Omega^1_L(C)^{\mathrm{Gal}(L/k)}_{\xi} \to \Omega^1(C') : \omega \to \phi^*(\omega)$ is an isomorphism of k-vector spaces. The only non-trivial fact is the surjectivity. But this is a consequence of the equivalent result for function fields. Recall that the function field $k(C')$ may be reinterpreted as the fixed field $\overline{k}(C)^{G_k}_{\xi}$ where the action of the Galois group G_k on $\overline{k}(C)$ is twisted by ξ according to $f^{\sigma}_{\xi} := f \cdot \xi_\sigma$ ([20], X.2). □

We identify the previous vector spaces via an isomorphism as in Lemma 3.1, so, for explicit computations, we can use

$$\Omega^1(C') = \bigcap_{\sigma\in\mathrm{Gal}(L/k)} \mathrm{Ker}(\rho_\xi(\sigma) - \mathrm{Id})\,. \tag{3.1}$$

Consider the canonical morphism and the canonical model $\phi_K : C \to \mathcal{C} \subset \mathbb{P}^{g-1}$ given by the basis $\{\omega_1,\dots,\omega_g\}$ of $\Omega^1(C)$. Let

$$\mathcal{C} :\ \{F_h(\omega_1,\dots,\omega_g) = 0\}_h$$

be a set of polynomial equations defining the canonical model in $\mathbb{P}^{g-1}$. Let $\{\sum_{i=1}^g \mu^i_j\omega_i\}_j$ be a basis of $\Omega^1_L(C)^{\mathrm{Gal}(L/k)}_{\xi}$. We can then take a basis $\omega'_j = \sum_{i=1}^g \mu^i_j\omega_i$ of $\Omega^1(C')$ via an isomorphism as in Lemma 3.1. Thus, we can write

$$\omega_i = \sum_{j=1}^g \eta^i_j\,\omega'_j$$

for some $\eta^i_j \in L$. We then obtain equations for the canonical model $\mathcal{C}'$, given by the basis $\{\omega'_j\}$, of the twist C' via the substitution

$$\mathcal{C}' :\ \Big\{F_h\Big(\sum_{j=1}^g \eta^1_j\,\omega'_j,\dots,\sum_{j=1}^g \eta^g_j\,\omega'_j\Big) = F'_h(\omega'_1,\dots,\omega'_g) = 0\Big\}_h.$$

Note that the projective matrix $\eta = (\eta^i_j)_{ij}$ defines an isomorphism of canonical models $\eta\colon \mathcal{C}' \to \mathcal{C}$, and that $\eta \cdot^{\sigma} \eta^{-1} = (\xi^*_\sigma)^{-1}$. In general, on a canonical models level, any morphism of curves is given by a matrix, since a morphism of curves induces a linear morphism on the regular differential vector spaces.

Remark 3.2. Note that for non-hyperelliptic curves and an isomorphism $\phi\colon C \to C'$ defined over L of canonical models defined over k, Lemma 3.1 is equivalent to the dimension of $\Omega^1_L(C)_\xi^{\mathrm{Gal}(L/k)}$ be equal to g, that is, to finding a matrix in $\eta \in \mathrm{GL}_g(L)$ such that $\eta \cdot^\sigma \eta^{-1} = (\xi^*_\sigma)^{-1}$. But this is a consequence of Hilbert's Theorem 90, since $(\xi^*)^{-1} \in \mathrm{H}^1(\mathrm{Gal}(L/k), \mathrm{GL}(\Omega^1_L(C)))$.

4. Description of the method

As above, let C be a smooth non-hyperelliptic genus g curve defined over a perfect field k, and we continue to assume that its automorphism group $\mathrm{Aut}(C)$ is known and let us denote by K the minimal field where $\mathrm{Aut}(C)$ is defined. We now proceed to describe a method for computing the set of twists of the curve C. In each step, we will compute different things:

Step 1: a canonical model

Firstly, we take a basis of $\Omega^1(C)$, and via this basis we obtain a canonical model $\mathcal{C}/k$ as the image of the canonical morphism $C \hookrightarrow \mathbb{P}^{g-1}$. Again, the existence of a canonical divisor defined over k implies that we can take the canonical model $\mathcal{C}$ also defined over k. Hence, $\mathcal{C}$ and C belong to the same class in $\mathrm{Twist}_k(\mathcal{C})$ and $\mathrm{Twist}_k(\mathcal{C}) = \mathrm{Twist}_k(C)$.

In addition, the automorphism group $\mathrm{Aut}(\mathcal{C})$ can be viewed in a natural way as a subgroup of $\mathrm{PGL}_g(K)$ (via the induced automorphism in $\mathbb{P}^{g-1}$ by the canonical morphism). Indeed, we can map it as a subgroup of $\mathrm{GL}_g(K)$ if we look at its action on $\Omega^1(C) \otimes_k K$ as a K-vector space. Furthermore, any isomorphism $\phi\colon \mathcal{C}' \to \mathcal{C}$ can be also viewed as a matrix in $\mathrm{PGL}_g(\bar{k})$.

Step 2: the set $\mathrm{Twist}_k(C)$

We will first compute the set $\widetilde{\mathrm{Hom}}(G_k, \Gamma)$. From this set, we will compute the cohomological set $\mathrm{H}^1(G_k, \mathrm{Aut}(\mathcal{C}))$ via the correspondence in Theorem 2.2.

Given an element $\Psi \in \widetilde{\mathrm{Hom}}(G_k, \Gamma)$, let L be its splitting field. We have the following isomorphisms: $\Psi(G_K) \simeq \mathrm{Gal}(L/K)$ and $\Psi(G_k) \simeq \mathrm{Gal}(L/k)$. Hence, we can see Ψ as a proper solution to the Galois embedding problem

$$\begin{tikzcd}
 & & & G_k \arrow[dl, dashed, "\Psi"'] \arrow[d] & \\
1 \arrow[r] & \Psi(G_K) \arrow[r] & \Psi(G_k) \arrow[r] & \mathrm{Gal}(K/k) \arrow[r] & 1
\end{tikzcd}$$

As it was noticed in Section 2, we have isomorphisms $\mathrm{Gal}(L/k) \simeq \mathrm{Image}(\Psi) \subseteq \Gamma$ and $\mathrm{Gal}(L/K) \simeq \Psi(G_K) \subseteq \mathrm{Aut}(\mathcal{C}) \rtimes \{1\}$. Hence, we can break the computation of $\widetilde{\mathrm{Hom}}(G_k, \Gamma)$, i.e., the solutions (proper or not) to the Galois embedding problem (2.4), into the computation of the proper solutions to some Galois embedding problems attached to a pair (G,H) as follows:

(4.1)
$$\begin{tikzcd}
 & & & G_k \arrow[dl, dashed, "\Psi"'] \arrow[d] & \\
1 \arrow[r] & H \arrow[r] & G \arrow[r] & \mathrm{Gal}(K/k) \arrow[r] & 1
\end{tikzcd}$$

where we consider all the pairs (G,H) such that $G \subseteq \Gamma$, $H = G \cap \mathrm{Aut}\,(C) \rtimes \{1\}$ and $[G:H] = |\mathrm{Gal}\,(K/k)|$ (up to conjugacy by elements $(\varphi,1) \in \Gamma$).

Every proper solution to a Galois embedding problem (4.1) can be lifted to a solution to the Galois embedding problem (2.4).

Note that the same field L can appear as the splitting field of more than one solution Ψ corresponding to a pair (G,H). This is because given an automorphism α of $\mathrm{Gal}(L/k)$ that leaves $\mathrm{Gal}(K/k)$ fixed, $\alpha\Psi$ is another solution that has L as splitting field. Two such solutions are equivalent if and only if there exists $\beta \in \mathrm{Aut}(\mathcal{C})$ such that $\alpha\Psi = \beta\Psi\beta^{-1}$. So, the number of non-equivalent solutions with splitting field L and $\Psi(\mathrm{G}_k) = G$ is the cardinality $n_{(G,H)}$ of the group ([5], Section 1.1):

$$\mathrm{Aut}_2\,(G)\,/\,\mathrm{Inn}_G\,(\mathrm{Aut}\,(\mathcal{C}) \rtimes \{1\})\,, \tag{4.2}$$

where $\mathrm{Aut}_2\,(G)$ is the group of automorphisms of G such that leave the second coordinate invariant and $\mathrm{Inn}\,(\mathrm{Aut}\,(\mathcal{C}) \rtimes \{1\})$ is the group of inner automorphisms of $\mathrm{Aut}\,(\mathcal{C}) \rtimes \{1\}$ lifted in the natural way to $\mathrm{Aut}\,(G)$.

We can then divide this step in two:

Step 2a: computing the pairs (G,H). The pairs (G,H) and the number $n_{(G,H)}$ defined above, can be, for example, computed with Magma [1] (cf. Appendix in [14] for an implemented code).

Step 2b: computing the proper solutions to the Galois embedding problems (4.1). The solutions should be computed case-by-case for each pair (G,H). If k is a finite field this is known how to be done (e.g. Theorem 1.1 in [19]), and the method described in this paper becomes then an algorithm. Unfortunately, if k is a number field there is no known systematic method for solving these problems

The next proposition, which is a generalization of Lemma 9.6 in [6] for $q=3$, will be useful for solving some of these Galois embedding problems.

Proposition 4.1. *Let be $q = p^r$, where p is a prime number, let k be a number field, and let ζ be a fixed q-th primitive root of the unity in $\bar{k}$. We denote $K = k(\zeta)$ and we assume $[k(\zeta):k] = p^{r-1}(p-1)$. Let us define $G_q := \mathbb{Z}/q\mathbb{Z} \rtimes (\mathbb{Z}/q\mathbb{Z})^*$[1]with the multiplication rule $(a,b)(a',b') = (a+ba',bb')$. Let us consider the Galois embedding problem:*

$$\begin{tikzcd}
 & & & G_k \arrow[d, "\pi"'] & \\
1 \arrow[r] & \mathbb{Z}/q\mathbb{Z} \arrow[r] & G_q \arrow[r] & (\mathbb{Z}/q\mathbb{Z})^* \arrow[r] & 1
\end{tikzcd},$$

where the horizontal morphisms are the natural ones, and the projection π is given by $\pi(\sigma) = (0,b)$ if $\sigma(\zeta) = \zeta^b$.

Then, the splitting fields of the proper solutions to this Galois embedding problem are of the form $L = K(\sqrt[q]{m}\,)$ where $m \in \mathcal{O}_k$ is an integer that is not a p-power. Moreover, every such field is the splitting field for a solution Ψ to the above Galois embedding problem.

The proof of this proposition uses very similar arguments to the ones used in Kummer theory (e.g., Section 2 in [21]).

Proof. Note first that there exist proper solutions Ψ to the Galois embedding problem. Given a field $L = K(\sqrt[q]{m})$ with $m \in k$ and not a p-power, there is a natural isomorphism $\mathrm{Gal}(L/k) \simeq G_q$ compatible with the projection $G_q \to (\mathbb{Z}/q\mathbb{Z})^*$. The natural projection $G_k \twoheadrightarrow \mathrm{Gal}(L/k)$ then provides a solution to the Galois embedding problem above.

Now, let Ψ be any proper solution to the problem, and let us denote by L its splitting field. Let G be the subgroup of G_q that contains all the elements of the form $(0, b)$, and let $\sigma \in G_k$ be such that $\Psi(\sigma) = (1, 1)$.

Let α be a primitive element of the extension L^G/k that moreover is an algebraic integer. We then have that $L = K(\alpha)$. This is because $[K : k] = p^{r-1}(p-1)$, $\left[L^G : k\right] = q$ and $L^G \cap K = k$. Define for $i = 0, 1, \ldots, q-1$ the numbers

$$u_i = \alpha + \zeta^i\sigma^{-1}(\alpha) + \zeta^{2i}\sigma^{-2}(\alpha) + \cdots + \zeta^{(q-1)i}\sigma^{-(q-1)}(\alpha).$$

Then $\sigma(u_i) = \zeta^i u_i$ and for any $\tau \in G_k$ such that $\Psi(\tau) = (0, b)$ we have $\Psi(\tau\sigma^j) = (0, b)(j, 1) = (bj, 1)(0, b) = \Psi(\sigma^{bj}\tau)$, so $\tau(u_i) = u_i$. In particular, we have that u_0, $u_1^q, \ldots,$ $u_{q-1}^q \in \mathcal{O}_k$. Hence, if $u_j \neq 0$ for some $j > 0$, we have that $L = K(u_j)$, since $L^G = k(u_j)$. So, if we put $m = u_j^q \in \mathcal{O}_k$, we get $L = K(\sqrt[q]{m})$. Otherwise, that is, if $u_1 = u_2 = \cdots = u_{q-1} = 0$, then $u_0 = u_0 + u_1 + \cdots + u_{q-1} = q\alpha \in \mathcal{O}_k$, what is a contradiction with α being a primitive element of the extension L^G/k. □

For each proper solution Ψ to a Galois embedding problem (4.1) attached to a pair (G, H), we trivially compute the corresponding cocycle ξ via the correspondence between the sets (2.2) and (2.3) in Theorem 2.2.

Step 3: Equations

We want to compute equations for a twist corresponding to a given cocycle ξ. For this purpose we use the method explained in Section 3. Computing equations for a twist turns out to be equivalent to computing an isomorphism $\phi\colon C' \to C$, that is, to explicitly computing the inverse map to the correspondence between sets (2.1) and (2.2) in Theorem 2.2.

5. An example

In order to illustrate the method, we will apply it to the smooth non-hyperelliptic genus 6 curve which admits the affine plane model

$$C : x^7 - y^3 - 1 = 0\,.$$

[1] This is the group of affine maps on $\mathbb{F}_q$, that is sometimes denote by $\mathrm{AGL}_2(q)$.

As the only point at infinity, that we denote by ∞, is singular, the projectivization of this plane model is not smooth. However, there is a unique curve, up to $\mathbb{Q}$-isomorphism, which is smooth and birationally equivalent to C. So, they have the same function field. We will apply the method for this smooth curve, which is non-hyperelliptic and has genus equal to 6.

Step 1

First, we must find a canonical model by the usual procedure: finding a basis of holomorphic differentials. Let us compute the divisor associated to the functions x and y.

$$\begin{aligned}\operatorname{div}(x) &= (0:-1:1)+(0:-\zeta_3:1)+(0:-\zeta_3^2:1)-3(0:1:0)\\ &= P_1+P_2+P_3-3\infty\,,\\ \operatorname{div}(y) &= Q_1+Q_2+Q_3+Q_4+Q_5+Q_6+Q_7-7\infty\,,\end{aligned}$$

where $Q_i=(\zeta_7^i:0:1)$. Then, dx is an uniformizer for all points except for the Q_i, because the tangent space to the curve at these points have equation $x-\alpha=0$ for some $\alpha\in\bar{k}$. Then, for the points Q_i we have to use the expression

$$dx=-\frac{3y^2}{7x^6}\,dy$$

Thus, by [20], II, Proposition 4.3, we finally get a canonical divisor

$$\operatorname{div}(dx)=2(Q_1+Q_2+Q_3+Q_4+Q_5+Q_6+Q_7)-4\infty\,.$$

We obtain the following basis of holomorphic differentials:

$$\omega_1=\frac{dx}{y^2},\ \omega_2=\frac{x\,dx}{y^2},\ \omega_3=\frac{x^2\,dx}{y^2},\ \omega_4=\frac{dx}{y},\ \omega_5=\frac{x^3\,dx}{y^2},\ \omega_6=\frac{x\,dx}{y}\,.$$

We consider the rational map

$$C\to\mathbb{P}^5:\ (x,y)\to(1,x,x^2,y,x^3,xy).$$

The ideal of the image of this map clearly contains the homogeneous polynomials:

$$\begin{aligned}&f_1=\omega_1\omega_6-\omega_2\omega_4\,, && f_2=\omega_2^2-\omega_1\omega_3\,, && f_3=\omega_2\omega_3-\omega_1\omega_5\,,\\ &f_4=\omega_2\omega_5-\omega_3^2\,, && f_5=\omega_2\omega_6-\omega_3\omega_4\,, && f_6=\omega_3\omega_6-\omega_4\omega_5\,,\\ &f_7=\omega_4^3-\omega_3^2\omega_5+\omega_1^3\,, && f_8=\omega_5^3-\omega_4\omega_6^2-\omega_1\omega_2^2\,.\end{aligned}$$

Now, we claim that the ideal generated by these polynomials gives a smooth curve. To see this, note that, if $\omega_1\neq 0$, the deshomogenization of this ideal with respect to ω_1 gives the affine curve C. Now, we isolate from f_2 and f_3 the variables ω_3 and ω_5 and we plug them into f_7. Therefore, C is birationally equivalent to $\mathcal{C}\cap\{\omega_1\neq 0\}$. Next, if $\omega_1=0$, then the vanishing locus of f_2,f_4,f_7,f_8 is the point $(0:0:0:0:0:1)$. To check that $\mathcal{C}$ is non-singular at this point we consider the partial derivatives of the polynomials: f_1,f_5,f_6,f_8. Thus, $\mathcal{C}$ is a canonical model of the initial smooth non-hyperelliptic genus 6 curve.

The automorphism group $\mathrm{Aut}(C)$ is generated by the automorphisms (Section 4, figure 5 in [22])

$$(x,y) \to (x, \zeta_3 y) \text{ and } (x,y) \to (\zeta_7 x, y).$$

Then, the automorphism group of the canonical model $\mathcal{C}$ is generated by the matrices in $\mathrm{PGL}_6\left(\bar{\mathbb{Q}}\right)$:

$$r = \begin{pmatrix} \zeta_3 & 0 & 0 & 0 & 0 & 0 \\ 0 & \zeta_3 & 0 & 0 & 0 & 0 \\ 0 & 0 & \zeta_3 & 0 & 0 & 0 \\ 0 & 0 & 0 & \zeta_3^2 & 0 & 0 \\ 0 & 0 & 0 & 0 & \zeta_3 & 0 \\ 0 & 0 & 0 & 0 & 0 & \zeta_3^2 \end{pmatrix}, \quad s = \begin{pmatrix} \zeta_7 & 0 & 0 & 0 & 0 & 0 \\ 0 & \zeta_7^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & \zeta_7^3 & 0 & 0 & 0 \\ 0 & 0 & 0 & \zeta_7 & 0 & 0 \\ 0 & 0 & 0 & 0 & \zeta_7^4 & 0 \\ 0 & 0 & 0 & 0 & 0 & \zeta_7^2 \end{pmatrix}.$$

Step 2a. Let k be a number field and consider the curve $\mathcal{C}/k$. We want to compute its twists over k. Let $K = k(\zeta_7, \zeta_3)$ and assume that $[K : k] = 12$. Then, the Galois group $\mathrm{Gal}(K/k)$ is generated by the elements $\tau_1 : \zeta_3, \zeta_7 \to \zeta_3^2, \zeta_7$ and $\tau_2 : \zeta_3, \zeta_7 \to \zeta_3, \zeta_7^3$. We compute using Magma the following possibilities for the pairs (G, H):

	ID(G)[2]	ID(H)	gen(H)	$n_{(G,H)}$
1	$< 12, 5 >$	$< 1, 1 >$	1	1
2	$< 36, 12 >$	$< 3, 1 >$	r	2
3	$< 84, 7 >$	$< 7, 1 >$	s	6
4	$< 252, 26 >$	$< 21, 2 >$	$r,\ s$	12

The fourth column in this table exhibits generators of the group H. In all the cases G is the group generated by the elements $(g, 1)$, for g in H, together with the elements $(1, \tau_1)$ and $(1, \tau_2)$. The fifth column exhibits the cardinality of the set in Formula (4.2) for each pair (G, H).

Step 2b. Now, we have to find the proper solutions to the Galois embedding problems associated to each of the pairs (G, H).

(1) The first case is clear: $L = K$.

(2) For the second one, note that $L = k(\zeta_7)M$, for some M/k a solution to the Galois embedding problem in Proposition 4.1 with $q = 3$. Hence, $L = k(\zeta_3,\ \zeta_7,\ \sqrt[3]{m}\,)$, for some $m \in \mathcal{O}_k$ that is not a 3-power.

(3) In this case, we can write $L = k(\zeta_3)M$, for some M/k a solution to the Galois embedding problem in Proposition 4.1 with $q = 7$. Hence, $L = k(\zeta_3,\ \zeta_7,\ \sqrt[7]{n}\,)$, for some $n \in \mathcal{O}_k$ that is not a 7-power.

(4) In the last case, $L = M_1 M_2$, for some M_i/k solutions to the Galois embedding problem in Proposition 4.1 with $q = 3, 7$. Hence, $L = k(\zeta_3,\ \zeta_7,\ \sqrt[3]{m},\ \sqrt[7]{n}\,)$, for some $m, n \in \mathcal{O}_k$, such that m is not a 3-power and n is not a 7-power.

[2] By ID(G) we mean the corresponding SmallGroup Library-GAP [13] notation for the group G, where the group $< N, r >$ denotes the group of order N that appears in the r-th position.

Step 3

For each of the previous fields L, we will compute equations of a twist that has L as splitting field. The other twists, with splitting field L, will be then easily computed by considering symmetries. Let us consider a solution Ψ (that is, a particular twist) to the Galois embedding problem with pair (G, H) and splitting field L by fixing an isomorphism between the group H and the group $\mathrm{Gal}(L/K)$:

$$(r,1):\ \sqrt[3]{m}\,,\ \sqrt[7]{n} \to \zeta_3\sqrt[3]{m}\,,\ \sqrt[7]{n}\,,$$
$$(s,1):\ \sqrt[3]{m}\,,\ \sqrt[7]{n} \to \sqrt[3]{m}\,,\ \zeta_7\sqrt[7]{n}\,.$$

Now, we compute equations for a twist in each case:

(1) Clearly, this solution gives us the trivial twist, so we have the curve $\mathcal{C}/k$.

(2) The correspondence between the sets (2.2) and (2.3) gives us the cocycle given by $\xi_{\tau_1} = 1$, $\xi_{\tau_2} = 1$ and $\xi_{(r,1)} = r$. If we take the basis of $\Omega^1_L(\mathcal{C})$ given by $\{(a,b,c,i)\} := \left\{\sqrt[3]{m^a}\zeta_3^b\zeta_7^c\omega_i\right\}$ with $a, b \in \{0,1,2\}$, $c \in \{0,1,\ldots,6\}$ and $i \in \{1,\ldots,6\}$, we obtain the twisted action of $\mathrm{Gal}(L/k)$ on $\Omega^1_L(\mathcal{C})$ given in Section 3:

$$\tau_1(a,b,c,i) = (a,2b,c,i),\ \tau_2(a,b,c,i) = (a,b,3c,i)$$
$$(r,1)(a,b,c,i) = \begin{cases} (a, a+b+2, c, i) & \text{if } i = 4,6 \\ (a, a+b+1, c, i) & \text{otherwise} \end{cases}$$

Now, we use formula (3.1) and get a basis of $\Omega^1(\mathcal{C}') \simeq \Omega^1_L(\mathcal{C})_\xi^{\mathrm{Gal}(L/k)}$ given by:

$$\left\{\sqrt[3]{m^2}\,\omega_1,\ \sqrt[3]{m^2}\,\omega_2,\ \sqrt[3]{m^2}\,\omega_3,\ \sqrt[3]{m}\,\omega_4,\ \sqrt[3]{m^2}\,\omega_5,\ \sqrt[3]{m}\,\omega_6\right\}.$$

So we get the generators of the ideal defining the twist:

$$\begin{array}{llll} \omega_1\omega_6 - \omega_2\omega_4, & \omega_2^2 - \omega_1\omega_3, & \omega_2\omega_3 - \omega_1\omega_5, & \omega_2\omega_5 - \omega_3^2, \\ \omega_2\omega_6 - \omega_3\omega_4, & \omega_3\omega_6 - \omega_4\omega_5, & m\omega_4^3 - \omega_3^2\omega_5 + \omega_1^3, & \omega_5^3 - m\omega_4\omega_6^2 - \omega_1\omega_2^2 \end{array}$$

We obtain generators for the other solution Ψ that has L as splitting field by exchanging m by m^2.

(3) In this case, the correspondence between the sets (2.2) and (2.3) gives us the cocycle given by $\xi_{\tau_1} = 1$, $\xi_{\tau_2} = 1$ and $\xi_{(s,1)} = s$. If we take the basis of $\Omega^1_L(\mathcal{C})$ given by $\{(a,b,c,i)\} := \left\{\sqrt[7]{n^a}\zeta_3^b\zeta_7^c\omega_i\right\}$, with $a, c \in \{0,1,\ldots,6\}$, $b \in \{0,1,2\}$ and $i \in \{1,\ldots,6\}$, we obtain the twisted action of $\mathrm{Gal}(L/k)$ on it given in Section 3:

$$\tau_1(a,b,c,i) = (a,2b,c,i),\ \tau_2(a,b,c,i) = (a,b,3c,i)$$
$$(r,1)(a,b,c,i) = \begin{cases} (a, a+b+1, c, i) & \text{if } i = 1,4 \\ (a, a+b+2, c, i) & \text{if } i = 2,6 \\ (a, a+b+3, c, i) & \text{if } i = 3 \\ (a, a+b+4, c, i) & \text{if } i = 5 \end{cases}$$

Now, we use formula (3.1) again and get a basis of $\Omega^1(\mathcal{C}') \simeq \Omega^1_L(\mathcal{C})_\xi^{\mathrm{Gal}(L/k)}$

given by

$$\big\{\sqrt[7]{n^6}\,\omega_1,\ \sqrt[7]{n^5}\,\omega_2,\ \sqrt[7]{n^4}\,\omega_3,\ \sqrt[7]{n^6}\,\omega_4,\ \sqrt[7]{n^3}\,\omega_5,\ \sqrt[7]{n^5}\,\omega_6\big\}.$$

Then, we get the set of generators of the ideal defining the twist:

$$\begin{array}{llll} \omega_1\omega_6-\omega_2\omega_4, & \omega_2^2-\omega_1\omega_3, & \omega_2\omega_3-\omega_1\omega_5, & \omega_2\omega_5-\omega_3^2,\\ \omega_2\omega_6-\omega_3\omega_4, & \omega_3\omega_6-\omega_4\omega_5, & \omega_4^3-n\omega_3^2\omega_5+\omega_1^3, & n\omega_5^3-\omega_4\omega_6^2-\omega_1\omega_2^2 \end{array}$$

We compute generators for the other solutions Ψ that have splitting field equal to L by exchanging n by n^2, n^3, n^4, n^5, n^6.

(4) In the last case, we have the cocycle given by $\xi_\tau=1$, $\xi_{(r,1)}=r$ and $\xi_{(s,1)}=s$. We take the basis of $\Omega^1_L(\mathcal{C})$ given by $\{(a,b,c,d,i)\}:=\big\{\sqrt[3]{m^a}\sqrt[7]{n^b}\zeta_3^c\zeta_7^d\omega_i\big\}$ with $a,c\in\{0,1,2\}$, $b,d\in\{0,\dots,6\}$ and $i\in\{1,\dots,6\}$, and we consider on $\Omega^1_L(\mathcal{C})$ the twisted action of $\mathrm{Gal}(L/k)$ given in Section 3. Thus, formula (3.1) provides a basis of $\Omega^1(\mathcal{C}')\simeq\Omega^1_L(\mathcal{C})_\xi^{\mathrm{Gal}(L/k)}$ given by

$$\big\{\sqrt[3]{m^2}\sqrt[7]{n^6}\,\omega_1,\ \sqrt[3]{m^2}\sqrt[7]{n^5}\,\omega_2,\ \sqrt[3]{m^2}\sqrt[7]{n^4}\,\omega_3,\\ \sqrt[3]{m}\sqrt[7]{n^6}\,\omega_4,\ \sqrt[3]{m^2}\sqrt[7]{n^3}\,\omega_5,\ \sqrt[3]{m}\sqrt[7]{n^5}\,\omega_6\big\}\,.$$

Then, we get the set of generators of the ideal defining the twist

$$\begin{array}{llll} \omega_1\omega_6-\omega_2\omega_4, & \omega_2^2-\omega_1\omega_3, & \omega_2\omega_3-\omega_1\omega_5, & \omega_2\omega_5-\omega_3^2,\\ \omega_2\omega_6-\omega_3\omega_4, & \omega_3\omega_6-\omega_4\omega_5, & m\omega_4^3-n\omega_3^2\omega_5+\omega_1^3, & n\omega_5^3-m\omega_4\omega_6^2-\omega_1\omega_2^2 \end{array}$$

We compute generators for the other solutions Ψ that have L as splitting field by exchanging m and n by m, m^2 and n, n^2, n^3, n^4, n^5, n^6.

We can summarize these results as follows:

Proposition 5.1. *The twists of the curve $\mathcal{C}/k$ defined above where k is a number field such that $[k(\zeta_{21}):k]=12$, are in one-to-one correspondence with the curves given by the ideals generated by the following homogeneous polynomials:*

$$\begin{array}{llll} \omega_1\omega_6-\omega_2\omega_4, & \omega_2^2-\omega_1\omega_3, & \omega_2\omega_3-\omega_1\omega_5, & \omega_2\omega_5-\omega_3^2,\\ \omega_2\omega_6-\omega_3\omega_4, & \omega_3\omega_6-\omega_4\omega_5, & m\omega_4^3-n\omega_3^2\omega_5+\omega_1^3, & n\omega_5^3-m\omega_4\omega_6^2-\omega_1\omega_2^2 \end{array}$$

where $m\in\mathcal{O}_k^*/(\mathcal{O}_k^*)^3$ and $n\in\mathcal{O}_k^*/(\mathcal{O}_k^*)^7$. Equivalently, we can consider the (singular) plane models

$$nx^7-my^3z^4-z^7=0\,.$$

References

[1] Bosma, W., Cannon, J. and Playoust, C.: The Magma algebra system. I. The user language., *J. Symbolic Comput.* **24** (1997), no. 3-4, 235–265.

[2] Bruin, N., Fernández, J., González, J. and Lario, J.-C.: Rational points on twists of $X_0(63)$. *Acta Arith.* **126** (2007), no. 4, 361–385.

[3] Cardona, G.: *Models racionals de corbes de genere* 2. PhD Thesis, Universitat Politècnica de Catalunya, 2001.

[4] Cardona, G.: On the number of curves of genus 2 over a finite field. *Finite Fields Appl.* **9** (2003), no. 4, 505–526.

[5] Cardona, G.: Representations of G_k-groups and twists of the genus two curve $y^2 = x^5 - x$. *J. Algebra* **303** (2006), no. 2, 707–721.

[6] Cox, D.: *Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication.* A Wiley-Interscience Publication, John Wiley & Sons, 1989.

[7] Fernández, J., González, J. and Lario, J.-C.: Plane quartic twists of $X(5, 3)$. *Canad. Math. Bull.* **50** (2007), no. 2, 196–205.

[8] Fité, F., Kedlaya, K., Rotger, V. and Sutherland, A. V.: Sato–Tate distributions and Galois endomorphism modules in genus 2. *Compos. Math.* **148** (2012), no. 5, 1390–1442.

[9] Fité, F. and Lario, J.-C.: The twisting representation of the L-function of a curve. *Rev. Mat. Iberoam.* **29** (2013), no. 3, 749–764.

[10] Fité, F., Lorenzo García, E. and Sutherland, A. V.: Sato–Tate distributions of twists of the Fermat and Klein quartics. *Preprint.*

[11] Fité, F. and Sutherland, A. V.: Sato–Tate distributions of twists of $y^2 = x^5 - x$ and $y^2 = x^6 + 1$. *Algebra Number Theory* **8** (2014), no. 3, 543–585.

[12] Fité, F. and Sutherland, A. V.: Sato–Tate groups of $y^2 = x^8 + c$ and $y^2 = x^7 - cx$. In *Frobenius distributions: Lang–Trotter and Sato–Tate conjectures,* 103–126. Contemp. Math. 663, Amer. Math. Soc., Providence, RI, 2016.

[13] The GAP Group, GAP-Groups, *Algorithms and Programming*, Version 4.5.7, 2012, (`http://www.gap-system.org`).

[14] Lorenzo García, E.: *Arithmetic properties of non-hyperelliptic curves.* PhD Thesis, Universitat Politècnica de Catalunya, 2014.

[15] Lorenzo García, E.: Twists of non-hyperelliptic genus 3 curves. Preprint, arXiv: `1604.02410`, 2016.

[16] Meagher, S. and Top, J.: Twists of genus three curves over finite fields. *Finite Fields Appl.* **16** (2010), no. 5, 347–368.

[17] Neukirch, J., Schmidt, A. and Wingberg, K.: *Cohomology of number fields.* Grundlehren der mathematischen Wissenschaften 323, Springer-Verlag, Berlin, 2000.

[18] Poonen, B., Schaefer, E. F. and Stoll, M.: Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$. *Duke Math. J.* **137** (2007), no. 1, 103–158.

[19] Serre, J.-P.: *A Course in arithmetic.* Graduate Texts in Mathematics 7, Springer-Verlag, New York-Heidelberg, 1973.

[20] Silverman, J. H.: *The arithmetic of elliptic curves.* Graduate Texts in Mathematics 106, Springer-Verlag, New York, 1986

[21] Stevenhagen, P.: *Kummer theory and reciprocity laws.* Algebra course notes, 2002.

[22] Swinarski, D.: Equations of Riemann surfaces with automorphims. Preprint, arXiv: `1607.04778`, 2016.

Received March 11, 2015; revised September 13, 2015.

Elisa Lorenzo: IRMAR, Université de Rennes 1, Campus de Beaulieu, 35042, Rennes Cedex, France.
E-mail: elisa.lorenzogarcia@univ-rennes1.fr