ELSEVIER
Available online at www.sciencedirect.com
ScienceDirect
Journal of Algebra 303 (2006) 707–721
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

Representations of G_k-groups and twists of the genus two curve $y^2 = x^5 - x$

Gabriel Cardona [1]

Departament de Ciències Matemàtiques i Informàtica, Universitat de les Illes Balears, Edifici Anselm Turmeda, Campus UIB, Carretera Valldemossa, km. 7.5, E-07122 Palma de Mallorca, Spain

Received 17 May 2005

Available online 9 March 2006

Communicated by John Cremona

Abstract

In this paper we consider the twists of the single curve of genus 2 with group of automorphism isomorphic to $\tilde{S}_4$. To this end, we first study 2-dimensional representations of the quaternion group of 8 elements and of $\tilde{S}_4$, both with a given Galois action.

Keywords: G_k-groups; Quaternion group; Genus 2 curves; Twists of curves

0. Introduction

Let k be a perfect field of characteristic different from 2 and 5, $\bar{k}$ a fixed algebraic closure of k and G_k the absolute Galois group of k, $G_k = \mathrm{Gal}(\bar{k}/k)$. There is, up to $\bar{k}$-isomorphism, a single genus 2 curve defined over k with group of automorphisms isomorphic to $\tilde{S}_4$, the 2-covering of S_4 isomorphic to $\mathrm{GL}(2,3)$. Namely, one can take the curve with affine equation $y^2 = x^5 - x$ as a representative of this $\bar{k}$-isomorphism class. In this paper we are interested in the classification of curves of genus 2 with group of automorphisms isomorphic to $\tilde{S}_4$ up to k-isomorphism, that is, the k-twists of the curve $y^2 = x^5 - x$.

We will always assume that genus 2 curves are given by a hyperelliptic model,

$$C : y^2 = f(x),$$

E-mail address: gabriel.cardona@uib.es.

[1] Supported by grants BFM-2003-06768-C02-01 and 2005SGR-00443.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2006.02.005

where $f(x) \in k[x]$ is a polynomial of degree 5 or 6. Isomorphisms between genus 2 curves will always be given in terms of their hyperelliptic models:

$$(x, y) \mapsto \left(\frac{ax+b}{cx+d}, \frac{(ad-bc)y}{(cx+d)^3}\right), \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\bar{k}),$$

and we will identify such an isomorphism with the corresponding matrix. We recall that this identification preserves both the group law and the Galois action. In particular, the group of automorphism $\mathrm{Aut}(C)$ is a G_k-group isomorphic, as a G_k-group, to a sub-G_k-group of $\mathrm{GL}_2(\bar{k})$.

As a result, any k-isomorphism between two curves is given by a matrix $M \in \mathrm{GL}_2(k)$, and the groups of automorphisms of both curves are related, in terms of their matricial representation, by conjugation by M. Therefore, to any k-isomorphism class of curves of genus 2 there corresponds a subgroup of $\mathrm{GL}_2(\bar{k})$ up to $\mathrm{GL}_2(k)$-conjugation.

1. Quaternionic G_k-groups as groups of matrices

1.1. Galois actions on groups

Let H be a G_k-group, that is, H is a group with a given G_k-structure. By a G_k-structure (or, equivalently, a Galois action) on H we mean a continuous mapping, with respect to the Krull topology on G_k and the discrete topology on H,

$$\begin{aligned} G_k \times H &\to H, \\ (\sigma, x) &\mapsto {}^{\sigma}x, \end{aligned}$$

which defines an action of G_k on H (as a set) and is, moreover, compatible with the group structure of H, that is, ${}^{\sigma}(xy) = {}^{\sigma}x\,{}^{\sigma}y$. To give such an action is equivalent to giving a morphism of groups $\rho : G_k \to \mathcal{S} = \mathrm{Aut}(H)$, so that ${}^{\sigma}x = \rho(\sigma)(x)$. This morphism factors through a finite Galois extension K/k with Galois group isomorphic to a subgroup $\mathcal{T}$ of $\mathcal{S}$. We will call K the *field of definition* of the G_k-group (or of the Galois action). Then, any G_k-structure on H is defined by giving a Galois extension K/k together with an isomorphism

$$\mathrm{Gal}(K/k) \xrightarrow{\simeq} \mathcal{T} \subset \mathcal{S}.$$

A morphism $\varphi : H_1 \to H_2$ of G_k-groups, with respective Galois actions given by $\rho_i : G_k \to \mathrm{Aut}(H_i)$, is a morphism of groups that translates the given Galois actions; that is, $\varphi(\rho_1(\sigma)(x)) = \rho_2(\sigma)(\varphi(x))$. In particular, an isomorphism of G_k-groups is an isomorphism $\varphi : H_1 \to H_2$ such that $\rho_1 = \varphi^* \circ \rho_2$, where for any automorphism ψ of H_2, $\varphi^*(\psi)$ is the automorphism $\varphi^{-1}\psi\varphi$ of H_1. In other words, the condition is $\rho_1(\sigma) = \varphi^{-1}\rho_2(\sigma)\varphi$ for every $\sigma \in G_k$.

For the case of different G_k-structures on a group H, the condition for these actions to be equivalent is that the corresponding morphisms differ by an inner automorphism of $\mathcal{S}$; namely, using the notations in the paragraph above, the inner automorphism is conjugation by φ, which is an automorphism of H. Then,

$$\mathrm{Hom}(G_k, \mathcal{S}) / \mathrm{Inn}(\mathcal{S})$$

classifies G_k-structures on H, up to equivalence.

It is clear that equivalent G_k-structures are defined over the same field K, since K/k is a Galois extension. Two actions defined over the same field K are equivalent if the corresponding isomorphisms from $\mathrm{Gal}(K/k)$ to $\mathcal{T}_1, \mathcal{T}_2$ are conjugate. It follows that $\mathcal{T}_1, \mathcal{T}_2$ are conjugate subgroups of $\mathcal{S}$, but notice that non-equivalent structures could have conjugate associated subgroups, since not only the subgroups but also the morphisms must be conjugate. After this, and up to equivalence, we can fix a set of representatives of conjugacy classes of subgroups of $\mathcal{S}$, and assume that $\mathcal{T}$ is one of these subgroups. We will call $\mathcal{T}$ the *type* of the Galois structure. Given $\mathcal{T}$, the equivalence classes of G_k-structures with associated subgroup $\mathcal{T}$ are classified by $\mathrm{Aut}(\mathcal{T})/\mathrm{Inn}(\mathcal{S})|_{\mathcal{T}}$.

1.2. *Linear representations of G_k-groups*

Let $\mathcal{M}$ be a subgroup of $\mathrm{GL}_n(\bar{k})$. The natural Galois action on $\bar{k}$ gives a natural G_k-structure on $\mathcal{M}$, provided that $\mathcal{M}$ is closed under this action; in this case, we will call $\mathcal{M}$ a sub-G_k-group of $\mathrm{GL}_n(\bar{k})$. By an n-dimensional G_k-representation of a group H, we will mean an isomorphism of G_k-groups between H and a sub-G_k-group of $\mathrm{GL}_n(\bar{k})$. Namely, we mean an embedding

$$H \overset{\varphi}{\hookrightarrow} \mathrm{GL}_n(\bar{k})$$

such that

$$\varphi({}^{\sigma}x) = {}^{\sigma}\varphi(x)$$

for every $x \in H$ and $\sigma \in G_k$.

The general problem of deciding, given the G_k-group H and the dimension n, whether this embedding exists is, up to our knowledge, unsolved. Some 2-dimensional dihedral cases have been studied in [4].

All the groups we will consider have an unique non-trivial central element, that we will denote by -1. We will always assume that this element is represented by the matrix $-1 \in \mathrm{GL}_n(\bar{k})$.

1.3. *Galois actions on the quaternion group*

Let us now consider the case when H is the quaternion group,

$$H = \{\pm 1, \pm i, \pm j, \pm k\},$$

with, as usual, $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$. We recall that $\mathcal{S} = \mathrm{Aut}(H)$ is isomorphic to S_4, the symmetric group on 4 letters, and so is $\mathrm{Inn}(\mathcal{S})$. We will hereafter identify $\mathcal{S}$ with S_4; whenever an explicit identification is needed, we will use the following one:

$$(1,2,3,4) : (i, j, k) \mapsto (i, k, -j),$$
$$(1,2) : (i, j, k) \mapsto (-j, -i, -k).$$

The explicit computations with this group, and with $\tilde{S}_4$ in the next section, can be performed using a system for computational algebra such as GAP or Magma (see [6,8]).

Let us now remark some properties of this action that will be used afterwards:

(1) The isotropy subgroups of each non-central element in H are cyclic of order 4. Namely:

$$\mathcal{S}_i = \mathcal{S}_{-i} = \big\langle (1,2,3,4) \big\rangle,$$
$$\mathcal{S}_j = \mathcal{S}_{-j} = \big\langle (1,2,4,3) \big\rangle,$$
$$\mathcal{S}_k = \mathcal{S}_{-k} = \big\langle (1,3,2,4) \big\rangle.$$

(2) The isotropy subgroups of each of the three subgroups generated by each of the non-central elements in H, which are all of them cyclic of order 4, are isomorphic to D_8. Namely:

$$\mathcal{S}_{\langle i \rangle} = \big\langle (1,2,3,4), (1,3) \big\rangle,$$
$$\mathcal{S}_{\langle j \rangle} = \big\langle (1,2,4,3), (1,4) \big\rangle,$$
$$\mathcal{S}_{\langle k \rangle} = \big\langle (1,3,2,4), (1,2) \big\rangle.$$

(3) The inner automorphisms of H are identified with the normal subgroup of S_4 isomorphic to V_4, the Klein 4-group. Namely:

$$\gamma_i = (1,3)(2,4),$$
$$\gamma_j = (1,4)(2,3),$$
$$\gamma_k = (1,2)(3,4),$$

where γ_x denotes conjugation by x.

(4) Let ϵ_i be the mapping $\mathcal{S} \to \{\pm 1\}$ defined by

$$\epsilon_i(\sigma) = \begin{cases} 1, & \text{if } \sigma(i) \in \{i, j, k\}, \\ -1, & \text{if } \sigma(i) \in \{-i, -j, -k\}, \end{cases}$$

and define ϵ_j and ϵ_k analogously. Then, under the identification of $\mathcal{S}$ with S_4, the sign of an automorphism is given by

$$\operatorname{sgn}(\sigma) = \epsilon_i(\sigma)\epsilon_j(\sigma)\epsilon_k(\sigma).$$

Note that the sign of an element $\sigma \in \mathcal{S}$ does not depend on the isomorphism used to identify $\mathcal{S}$ with S_4. We will denote by $\mathcal{A}$ the subgroup of even automorphisms of H, which is isomorphic to A_4.

In order to classify all possible actions of G_k on H up to equivalence we follow the recipe at the end of Section 1.1. We fix a set of representatives of subgroups of $\mathcal{S}$ modulo conjugacy and label them according to its group structure, distinguishing with a label those that are isomorphic, see Table 1.

Note that for every type different from V_4^B and D_8, all the automorphisms are inner inside $\mathcal{S}$. For the two types V_4^B and D_8, the automorphism class modulo inner automorphisms is determined by the image of $\mathcal{A} \cap \mathcal{T}$, which is a C_2-subgroup for the type V_4^B and a V_4-subgroup for the type D_8.

Table 1

Type	Representative	Aut($\mathcal{T}$)	Aut($\mathcal{T}$)/ Inn($\mathcal{S}$)$\vert_{\mathcal{T}}$
1	1	1	1
C_2^A	$\langle(1,2)(3,4)\rangle$	1	1
C_2^B	$\langle(1,2)\rangle$	1	1
C_3	$\langle(1,2,3)\rangle$	C_2	1
C_4	$\langle(1,2,3,4)\rangle$	C_2	1
V_4^A	$\langle(1,2)(3,4),(1,3)(2,4)\rangle$	S_3	1
V_4^B	$\langle(1,2),(3,4)\rangle$	S_3	C_3
S_3	$\langle(1,2),(1,2,3)\rangle$	S_3	1
D_8	$\langle(1,2,3,4),(1,3)\rangle$	D_8	C_2
A_4	$\langle(1,2,3),(2,3,4)\rangle$	S_4	1
S_4	$\langle(1,2,3,4),(1,2)\rangle$	S_4	1

Note also that the structure of $\mathcal{A}\cap\mathcal{T}$ distinguishes the types C_2^A from C_2^B, where one gets C_2 for the first type and 1 for the second one, and V_4^A from V_4^B, where one gets V_4 for the first type and C_2 for the second one.

In terms of fields, we get from the discussion above that whenever the field of definition K of the Galois action does not uniquely identify the G_k-structure, it is determined by giving the quadratic or trivial subextension K_u/k fixed by $\rho^{-1}(\mathcal{T}\cap\mathcal{A})$. Namely:

- $\mathrm{Gal}(K/k)\simeq C_2$: If $K_u=k$, it is of type C_2^A; otherwise, it is of type C_2^B.
- $\mathrm{Gal}(K/k)\simeq V_4$: If $K_u=k$, it is of type V_4^A; otherwise, it is of type V_4^B, and the three different Galois structures correspond to the three different choices for K_u a quadratic subextension of K/k.
- $\mathrm{Gal}(K/k)\simeq D_8$: K_u/k is necessarily quadratic and the two different Galois structures correspond to the two quadratic subfields of K/k such that K/K_u is not cyclic.

For the sake of completeness, we give the fields K_u corresponding to the remaining cases:

- $\mathrm{Gal}(K/k)\simeq C_3, S_4$: K_u/k is trivial.
- $\mathrm{Gal}(K/k)\simeq C_4, S_3, S_4$: K_u/k is the only quadratic subfield of K/k.

We have thus proved the following proposition.

Proposition 1. *Any G_k-structure on the quaternion group is, up to equivalence, uniquely determined by its field of definition K and the quadratic (or trivial) extension K_u of k contained in K defined as the subfield of $\bar{k}$ fixed by $\rho^{-1}(\mathcal{A})$.*

In the following proposition we show how we can summarize all the data required to determine a G_k-structure in single quartic polynomial.

Proposition 2. *Any G_k-structure on the quaternion group is determined by giving a quartic polynomial $f(X)\in k[X]$ such that K is the splitting field of f and $K_u=k(\sqrt{\operatorname{disc} f})$.*

Proof. For S_4, A_4, D_8, and C_4 extensions the result is obvious.

For S_3, and C_3 extensions this is also true. Take any cubic polynomial $g(X)$ with splitting field K and consider the quartic polynomial

$$f(X) = Xg(X).$$

Then f and g have the same splitting field and their discriminants differ by a square.

For V_4 extensions, say $K = k(\sqrt{a}, \sqrt{b})$, we can take

$$f(X) = (X^2 - a)(X^2 - b),\ (X^2 - a)(X^2 - ab),\ (X^2 - b)(X^2 - ab),$$

whose discriminants are, respectively, ab, b, a modulo squares, or

$$f(X) = X^4 - 2(a+b)X^2 + (a-b)^2,$$

which is the minimal polynomial of $\sqrt{a} + \sqrt{b}$ over k and whose discriminant is a square.

For C_2 extensions, say $K = k(\sqrt{a})$, we can take

$$f(X) = X(X-1)(X^2 - a),$$

which has discriminant modulo squares equal to a, or

$$f(X) = (X^2 - a)(X^2 - 4a),$$

whose discriminant is a square. □

1.4. Linear 2-dimensional G_k-representations of quaternionic groups

Let H be a G_k-subgroup of $\mathrm{GL}_2(\bar{k})$ isomorphic to the quaternion group. Let K and K_u be the associated fields. The following proposition gives expressions for the matrices in H, up to conjugation by elements in $\mathrm{GL}_2(k)$.

Proposition 3. *Let H be a sub-G_k-group of $\mathrm{GL}_2(\bar{k})$ isomorphic to the quaternion group. Then H is $\mathrm{GL}_2(k)$-conjugate to the group generated by the matrices*:

$$M_1 = \begin{pmatrix} \alpha_1 & \beta_1 \\ \frac{-1-\alpha_1^2}{\beta_1} & -\alpha_1 \end{pmatrix}, \qquad M_2 = \begin{pmatrix} \alpha_2 & \beta_2 \\ \frac{-1-\alpha_2^2}{\beta_2} & -\alpha_2 \end{pmatrix}, \qquad M_3 = \begin{pmatrix} \alpha_3 & \beta_3 \\ \frac{-1-\alpha_3^2}{\beta_3} & -\alpha_3 \end{pmatrix},$$

where $\pm\beta_1, \pm\beta_2, \pm\beta_3$ are the roots of a polynomial of the form

$$g(X) = X^6 - C\,X^2 - D \in k[X],$$

with D and $\mathrm{disc}(X^3 - C\,X - D) = 4C^3 - 27D^2$ differing by a square in k, say $(4C^3 - 27D^2) = s^2D$, $s \in k^*$, and

$$\alpha_i = \frac{-3}{s}\beta_i^3 + \frac{2C}{sD}\beta_i^5, \quad i = 1, 2, 3.$$

Proof. Let K, K_u be the fields associated to the Galois action on H. In the following discussion we will suppose that $\mathrm{Gal}(K/k) \simeq S_4$, which is the most complicated case; for the other cases, the discussion goes analogously and the results are the same.

Let M_1, M_2, M_3 denote the matrices corresponding to the quaternions i, j, k. Since we are interested in matrices up to $\mathrm{GL}_2(k)$-conjugation, we can assume that the upper right entries of the matrices M_1, M_2, M_3 are non-zero, and since their square equals -1 we can assume that the matrices M_1, M_2, M_3 are of the form in the statement of the proposition. Note also that, using $\mathrm{GL}_2(k)$-conjugation, we can also ensure that $\beta_i \neq \pm\beta_j$ $(i \neq j)$.

From the relations defining the quaternion group, namely $M_1M_2 = M_3$ and $M_1M_2 = -M_2M_1$, it follows easily that

$$\beta_1^2 + \beta_2^2 + \beta_3^2 = 0. \tag{1}$$

Since H is closed under the action of G_k, the polynomial

$$g(X) = \left(x^2 - \beta_1^2\right)\left(x^2 - \beta_2^2\right)\left(x^2 - \beta_3^2\right)$$

has coefficients in k and, after (1), is of the form

$$g(X) = X^6 - CX^2 - D \in k[X].$$

Moreover, K is the splitting field of g, and since $\operatorname{disc} g = 64D(4C^3 - 27D^2)^2$, it follows that $K_u = k(\sqrt{D})$. The splitting field of $\tilde{g}(X) = X^3 - CX - D$ is an S_3-subextension of K/k with unique quadratic subfield $k(\sqrt{4C^3 - 27D^2})$. Therefore $4C^3 - 27D^2 = s^2D$ for some $s \in k^*$.

As for the coefficients α_i appearing above, taking into account how G_k operates on the matrices, it follows that $\alpha_i \in k(\beta_i)$, and α_i can be written as a linear combination of β_i and its powers. Since when ${}^\sigma\beta_i = -\beta_i$ we have that ${}^\sigma\alpha_i = -\alpha_i$, it follows that in the former linear combination, only odd powers will have non-zero coefficients. Now, since when ${}^\sigma\alpha_i = \alpha_j$, we have that ${}^\sigma M_i = M_j$, it follows that the coefficients in this linear combination are the same for each of the α_i. Then, we can assume

$$\alpha_i = a_1\beta_i + a_3\beta_i^3 + a_5\beta_i^5.$$

Now, and up to conjugation by the matrix $\left(\begin{smallmatrix} 1 & 0 \\ -t & 1 \end{smallmatrix}\right)$, we can replace α_i by $\alpha_i + t\beta_i$ for any $t \in k$; therefore, we can assume that $a_1 = 0$ and

$$\alpha_i = a_3\beta_i^3 + a_5\beta_i^5.$$

The considerations above, together with the condition that M_1, M_2, M_3 generate the quaternion group, lead to expressions for a_3, a_5 involving β_i,

$$a_3 = \frac{-(\beta_1^6 + \beta_2^6 + \beta_3^6)}{\delta}, \qquad a_5 = \frac{\beta_1^4 + \beta_2^4 + \beta_3^4}{\delta},$$

where

$$\delta = \beta_1\beta_2\beta_3\left(\beta_1^2 - \beta_2^2\right)\left(\beta_2^2 - \beta_3^2\right)\left(\beta_3^2 - \beta_1^2\right).$$

Writing the expressions found in terms of a k-base of K (see remark below) we get the result. $\square$

Remark 4. Let $L = k(\beta_1^2, \beta_2^2, \beta_3^2)$, which is the splitting field of $\tilde{g}(X)$; this is, in the generic case, an S_3-extension of k and we can take as a k-base of L

$$\{1, \beta_1^2, \beta_1^4, \beta_2^2, \beta_1^2\beta_2^2, \beta_1^4\beta_2^2\},$$

and any polynomial expression in the β_i^2 can be written as a linear combination of the elements above using the relations

$$\beta_1^2 + \beta_2^2 + \beta_3^2 = 0, \qquad \beta_1^4 + \beta_2^4 + \beta_1^2\beta_2^2 - C = 0, \qquad \beta_1^6 - C\beta_1^2 - D = 0.$$

Now, the extension K/L is biquadratic, and the set

$$\{1, \beta_1, \beta_2, \beta_3\}$$

is an L-base of K. In order to find the corresponding coefficients for any element in K we use that

$$\beta_1\beta_2\beta_3 = \sqrt{D} = \frac{\sqrt{4C^3 - 27D^2}}{s} = \frac{(\beta_1^2 - \beta_2^2)(\beta_2^2 - \beta_3^2)(\beta_3^2 - \beta_1^2)}{s} \in L$$

and

$$\beta_1\beta_2 = \frac{\beta_1\beta_2\beta_3}{\beta_3^2}\beta_3, \qquad \beta_1\beta_3 = \frac{\beta_1\beta_2\beta_3}{\beta_2^2}\beta_2, \qquad \beta_2\beta_3 = \frac{\beta_1\beta_2\beta_3}{\beta_1^2}\beta_1.$$

Then, we can find a k-base of K and explicitly find the corresponding coefficients for any element in K.

Following [5], we will call a quartic polynomial *principal* if both its cubic and quadratic coefficients are zero; analogously, we will call an extension K/k principal if it is the splitting field of some principal quartic polynomial; and a pair (K, K_u) principal if K is the splitting of a principal quartic polynomial and K_u is generated by the square root of its discriminant.

Proposition 5. *Let H be as in the previous proposition. Then, the pair of fields (K, K_u) associated to the Galois action on H is principal.*

Proof. We will use the same notations that those in the previous proof. Taking into account how G_k acts on the roots $\pm\beta_i$ of $g(X)$, which can be explicitly computed in terms of the identification of $\mathrm{Gal}(K/k)$ with S_4, we can find a defining polynomial for the non-normal quartic subextensions of K/k, whose composition is K. Namely, we can take

$$\begin{aligned} f(X) = {} & \big(X - \beta_1\beta_2\beta_3(\beta_1 - \beta_2 - \beta_3)\big)\big(X - \beta_1\beta_2\beta_3(-\beta_1 + \beta_2 - \beta_3)\big) \\ & \times \big(X - \beta_1\beta_2\beta_3(-\beta_1 - \beta_2 + \beta_3)\big)\big(X - \beta_1\beta_2\beta_3(\beta_1 + \beta_2 + \beta_3)\big). \end{aligned}$$

Using the identity (1), together with the natural expressions for C, D in terms of the β_i, we find that

$$f(X) = X^4 - 8D^2X + 4CD^2.$$

Moreover, $\operatorname{disc} f = 2^{12}D^6(4C^3 - 27D^2)$ and the result follows. □

We can now go further and characterize the quaternionic G_k-groups that can be represented by matrices.

Theorem 6. *Let H be a G_k-group isomorphic, as a group, to the quaternion group; let K and K_u be the associated fields. Then, H is G_k-representable in $\mathrm{GL}_2(\bar{k})$ if, and only if, (K, K_u) is a principal pair of fields.*

Proof. If H is representable by matrices, then by Proposition 5, the statement in the theorem holds.

Conversely, let $f = X^4 + AX + B$ be a principal polynomial with splitting field K, $d = \operatorname{disc} f$ and $K_u = k(\sqrt{d})$. Then, the polynomial $\tilde{f} = X^4 - 8A^4d^6X + 16A^4Bd^8$ defines the same extensions K and K_u, since the roots of $\tilde{f}$ are $-2Ad^2\gamma_i$, with γ_i a root of f. Taking $D = A^2d^3$ and $C = 4Bd^2$, one can construct the matrices M_1, M_2, M_3 as in Proposition 3; note that D and the discriminant d differ by a square. Since K and K_u determine the G_k-structure, the group generated by these matrices is G_k-isomorphic to H and the result follows. □

1.5. Some remarks on principality

In this section, we rewrite the condition of principality in terms of elements in $\mathrm{Br}_2(k)$. Namely, we find conditions for the fields K, K_u to be generated by, respectively, the roots of an separable principal quartic polynomial and the square root of its discriminant.

In the most generic case, let f be a quartic polynomial whose splitting field is K and $K_u = k(\sqrt{\operatorname{disc} f})$. By completing the cube, one can assume that the cubic coefficient of f is zero,

$$f = X^4 + a\,X^2 + b\,X + c.$$

Then, the obstruction to the existence of a principal quartic polynomial providing the same fields that f is given by

$$\bigl(2a \operatorname{disc} f, 2a^3 + 9b^2 - 8ac\bigr) = 1 \in \mathrm{Br}_2(k),$$

as is proved in [5].

When $\mathrm{Gal}(K/k)$ is isomorphic to either S_3 or C_3, the fields K and K_u can be given by a cubic polinomial, whose quadratic coefficient can be assumed to be zero,

$$f = X^3 + aX + b.$$

Then, the obstruction to the existence of a principal quartic polynomial providing the same fields that f is given by

$$\bigl(2a \operatorname{disc} f, 2a^3 + 9b^2\bigr) = 1 \in \mathrm{Br}_2(k).$$

When K/k is a trivial, quadratic or biquadratic extension, the descriptions of the fields and the obstructions can be simplified. In Table 2 we give a simple condition for principality in terms of the fields K and K_u.

Table 2

Type	K	K_u	Obstruction
1	k	k	$(-1,-1)$
C_2^A	$k(\sqrt{a})$	k	$(-a,-1)$
C_2^B	$k(\sqrt{a})$	$k(\sqrt{a})$	$(-a,-2)$
V_4^A	$k(\sqrt{a},\sqrt{b})$	k	$(-a,-b)$
V_4^B	$k(\sqrt{a},\sqrt{b})$	$k(\sqrt{a})$	$(-a,-2b)$

2. G_k-groups isomorphic to $\tilde{S}_4$ as groups of matrices

2.1. Galois actions on $\tilde{S}_4$

Let A be a G_k-group isomorphic, as a group, to $\tilde{S}_4$, the 2-covering of S_4 where transpositions lift to order 4 elements. One can give a presentation for A in terms of generators and relations as follows:

$$A = \langle -1, U, V \mid -1 \in Z(A),\ U^2 = (UV)^3 = 1,\ V^4 = -1 \rangle.$$

Note that A has a characteristic subgroup $H = \langle V^2, UV^2U\rangle$ isomorphic to the quaternion group, and hence H inherits a Galois structure.

The group of automorphisms of A is isomorphic to $C_2 \times S_4$, generated by a non-inner central involution ι and the two inner automorphisms given by conjugation by U and V,

$$\begin{aligned} &\iota(-1) = -1, && \iota(U) = -U, && \iota(V) = -V,\\ &\gamma_U(-1) = -1, && \gamma_U(U) = U, && \gamma_U(V) = UVU,\\ &\gamma_V(-1) = -1, && \gamma_V(U) = -VUV^3, && \gamma_V(V) = V. \end{aligned}$$

Then, giving a morphism ρ from G_k to $\mathrm{Aut}(A)$ is equivalent to giving a pair of morphisms from G_k to C_2 and S_4, respectively. Giving the first component is equivalent to giving the quadratic (or trivial) extension K_d/k through which the morphism factorizes; note that K_d is the subfield of $\bar{k}$ fixed by $\rho^{-1}(\mathrm{Inn}(A))$. As for the second component, according to the discussion above on the quaternion group case, and up to equivalence, it is determined by giving a pair of fields (K, K_u). We summarize these considerations in the following proposition.

Proposition 7. *Any G_k-structure on the group $\tilde{S}_4$ is uniquely determined, up to equivalence, by a triple of fields (K, K_u, K_d), where* $\mathrm{Gal}(K/k)$ *is isomorphic to a subgroup of S_4, K_u/k and K_d/k are quadratic (or trivial) extensions, and K_u/k is a subextension of K/k.*

2.2. Linear 2-dimensional G_k-representations of $\tilde{S}_4$

The goal of this section is to find conditions for a G_k-group isomorphic to $\tilde{S}_4$ to be G_k-representable by matrices.

From the table of characters for this group (see Table 3), it follows that any 2-dimensional representation has trace χ_4 (or $\chi_5 = \bar{\chi}_4$) and determinant χ_2. In particular, whenever $\mathrm{GL}_2(L)$ contains a subgroup isomorphic to $\tilde{S}_4$, the field L must contain $\sqrt{-2}$.

Table 3
Character table for $\tilde{S}_4$

	1A	2A	2B	3A	4A	6A	8A	8B
χ_1	1	1	1	1	1	1	1	1
χ_2	1	1	−1	1	1	1	−1	−1
χ_3	2	2	0	−1	2	−1	0	0
χ_4	2	−2	0	−1	0	1	ϵ	$-\epsilon$
χ_5	2	−2	0	−1	0	1	$-\epsilon$	ϵ
χ_6	3	3	−1	0	−1	0	1	1
χ_7	3	3	1	0	−1	0	−1	−1
χ_8	4	−4	0	1	0	−1	0	0

$\epsilon^2 = -2$

Proposition 8. *Let A be a sub-G_k-group of $\mathrm{GL}_2(\bar{k})$ isomorphic to $\tilde{S}_4$. Then A is $\mathrm{GL}_2(k)$-conjugate to the group generated by the matrices*

$$M_u = \frac{1}{\sqrt{-2}}(M_1 + M_2), \qquad M_v = \frac{-1}{\sqrt{-2}}(M_1 - I_2),$$

where M_1, M_2 are as in Proposition 3.

Proof. Let M_u, M_v be the matrices corresponding to the elements U, V. Since the group generated by V^2 and UV^2U is isomorphic to the quaternion group, we can assume that, up to $\mathrm{GL}_2(k)$-conjugation,

$$M_v^2 = M_1, \qquad M_u M_v^2 M_u = M_2,$$

with M_1, M_2 as in Proposition 3. A simple computation yields that

$$M_v = \frac{\pm 1}{\sqrt{2}} \begin{pmatrix} 1+\alpha_1 & \beta_1 \\ \frac{-1-\alpha_1^2}{\beta_1} & 1-\alpha_1 \end{pmatrix} \quad \text{or} \quad M_v = \frac{\pm 1}{\sqrt{-2}} \begin{pmatrix} \alpha_1 - 1 & \beta_1 \\ \frac{-1-\alpha_1^2}{\beta_1} & -1-\alpha_1 \end{pmatrix}.$$

Note that the respective traces of the matrices above are $\pm\sqrt{2}$ and $\pm\sqrt{-2}$; then, only the second option is possible and $M_v = \pm\frac{1}{\sqrt{-2}}(M_1 - I_2)$.

As for M_u, using the equality $M_u M_1 M_u = M_2$, one analogously obtains that

$$M_u = \frac{\pm 1}{\sqrt{2}} \begin{pmatrix} \alpha_1 + \alpha_2 & \beta_1 + \beta_2 \\ \frac{-\beta_1-\beta_2-\alpha_1^2\beta_2-\alpha_2^2\beta_1}{\beta_1\beta_2} & -\alpha_1 - \alpha_2 \end{pmatrix}.$$

As for the choices of signs, the condition $(UV)^3 = 1$ implies that the signs must be opposite, and the proposition follows. □

We can now describe which G_k-groups isomorphic to $\tilde{S}_4$ can be represented by a group of matrices with the same Galois action.

Theorem 9. *Let A be G_k-group isomorphic, as a group, to $\tilde{S}_4$; let K, K_u, K_d be the associated fields. Then, A is G_k-representable in $\mathrm{GL}_2(\bar{k})$ if, and only if, (K, K_u) is a principal pair of fields and $K_d = k(\sqrt{-2})$.*

Proof. If the G_k-group is representable by matrices, then, by Theorem 5, the pair of fields (K, K_u) is principal.

As for the field K_d, note that, by definition, $\sigma \in G_k$ fixes K_d if, and only if, $\rho(\sigma)$ is inner, that is, there exists $M \in A$ such that

$${}^{\sigma}M_u = M M_u M^{-1}, \qquad {}^{\sigma}M_v = M M_v M^{-1}.$$

Using that $M_u = \frac{1}{\sqrt{-2}}(M_1 + M_2)$ and $M_v = \frac{-1}{\sqrt{-2}}(M_1 - I_2)$, if σ acts as an inner automorphism, then

$$\begin{aligned}
{}^{\sigma}M_u &= {}^{\sigma}\left(\frac{1}{\sqrt{-2}}(M_1 + M_2)\right) = \frac{1}{{}^{\sigma}\sqrt{-2}}\left({}^{\sigma}M_1 + {}^{\sigma}M_2\right) \\
&= M M_u M^{-1} = \frac{1}{\sqrt{-2}}\left(M M_1 M^{-1} + M M_2 M^{-1}\right) = \frac{1}{\sqrt{-2}}\left({}^{\sigma}M_1 + {}^{\sigma}M_2\right),
\end{aligned}$$

and ${}^{\sigma}\sqrt{-2} = \sqrt{-2}$; conversely, if ${}^{\sigma}\sqrt{-2} = \sqrt{-2}$, then

$${}^{\sigma}M_u = \frac{1}{\sqrt{-2}}\left({}^{\sigma}M_1 + {}^{\sigma}M_2\right), \qquad {}^{\sigma}M_v = \frac{-1}{\sqrt{-2}}\left({}^{\sigma}M_1 - I_2\right).$$

Since all the automorphisms of H are inner inside $\tilde{S}_4$, it follows that σ acts as an inner automorphism. Therefore, $K_d = k(\sqrt{-2})$.

Conversely, from the condition that (K, K_u) is a principal pair of fields, and after Theorem 5, one can construct the matrices M_u, M_v as in Proposition 8 that generate a sub-G_k-group of $\mathrm{GL}_2(K \cdot K_d)$; the fields associated to this group are, by construction, K, K_u, K_d, and since these fields determine the Galois structure, it follows that these matrices provide a representation of the G_k-group A. □

3. Twists of the curve $y^2 = x^5 - x$

We can now give a solution to the problem of classifying the k-twists over any perfect field of the genus 2 curve given by the hyperelliptic equation

$$C : y^2 = x^5 - x.$$

The reduced group of automorphisms of this curve, which is defined as

$$\mathrm{Aut}'(C) = \mathrm{Aut}(C)/\langle -1 \rangle,$$

where -1 is the hyperelliptic involution on C, is isomorphic to S_4 (cf. [1,7]), while its full automorphism group $\mathrm{Aut}(C)$ is isomorphic to $\tilde{S}_4$. We remark that this curve is, up to $\bar{k}$-isomorphism, the unique curve with maximal automorphism group. The goal of this section is to classify all its k-twists, that is, classify all the k-isomorphism classes of curves $\bar{k}$-isomorphic to the given one. Note that the equation for C defines a smooth curve over any field of characteristic different from 2, but in characteristic 5 its automorphism group is even larger, isomorphic to $\tilde{S}_5$. For the number of twists over any finite field of odd characteristic, we refer the reader to [2], and for the characteristic 2 case to [3].

The set of twists of a curve C over a field k, $\mathrm{Twi}(C/k)$, is a pointed set, whose distinguished point is the k-isomorphism class of C, isomorphic to $H^1(G_k, \mathrm{Aut}(X))$, the first cohomology set of G_k with values in the G_k-group $\mathrm{Aut}(C)$. We will call the *hyperelliptic twist* of a genus 2 curve associated to $k(\sqrt{e})/k$ the twist obtained from the morphism $G_k \to \langle -1\rangle \subset \mathrm{Aut}(C)$ that factors through $k(\sqrt{e})$, and we will denote it by C_e. Note that if $y^2 = f(x)$ is a hyperelliptic equation for C, then $ey^2 = f(x)$ is a hyperelliptic equation for its hyperelliptic twist C_e.

Since k-isomorphisms fix the G_k-structure of the group of automorphisms, it makes sense to group the k-isomorphism classes with the same G_k-structure on the automorphism group; moreover, hyperelliptic twists also fix this Galois structure. Also, since the group of automorphisms of a genus 2 curve can be represented by matrices, one only needs to consider representable G_k-structures. We have thus reduced the problem of classifying the twists of the curve $y^2 = x^5 - x$ to:

(1) Decide which representable G_k-structures on $\tilde{S}_4$ correspond to the automorphism group of a curve of genus 2.
(2) For each of the possibilities above, classify k-isomorphism classes of curves with the given G_k-structure on its automorphism group.

The answer to the first question (see Proposition 10) is that every G_k-group isomorphic to $\tilde{S}_4$ representable by matrices is the group of automorphisms of a genus 2 curve. As for the second one, the set of curves with fixed Galois structure on its automorphisms are all obtained by hyperelliptic twists (see Proposition 12), and we can give an explicit description of the hyperelliptic twists that are defined over the base field (see Proposition 13).

Proposition 10. *Let A be the subgroup of $\mathrm{GL}_2(\bar{k})$ isomorphic to $\tilde{S}_4$ generated by M_u and M_v as in Proposition 8. Then, the curve of genus 2 given by the hyperelliptic equation*

$$y^2 = a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0,$$

with

$$\begin{aligned}
a_6 &= \left(64C^{12} - 848D^2C^9 + 3020D^4C^6 - 4023D^6C^3 + 5832D^8\right)s,\\
a_5 &= -4C\left(4C^3 - 27D^2\right)\left(32C^9 - 416D^2C^6 + 1098D^4C^3 - 243D^6\right),\\
a_4 &= 5C^2D\left(4C^3 - 27D^2\right)\left(16C^6 - 248D^2C^3 + 513D^4\right)s,\\
a_3 &= -20D^3\left(27D^2 - 20C^3\right)\left(27D^2 - 4C^3\right)^2,\\
a_2 &= -5CD^2\left(4C^3 - 27D^2\right)^2\left(4C^3 + 9D^2\right)s,\\
a_1 &= 8C^2D^2\left(4C^3 - 27D^2\right)^3,\\
a_0 &= D^3\left(27D^2 - 4C^3\right)^3 s,
\end{aligned}$$

has A as its group of automorphisms.

Proof. It follows from a direct computation that the given equation corresponds to curve of genus 2 and that the matrices M_u, M_v, which generate a sub-G_k-group of $\mathrm{GL}_2(\bar{k})$ isomorphic to $\tilde{S}_4$, are automorphisms of the curve. □

Remark 11. The result above is obtained by taking an arbitrary genus 2 curve and finding conditions on its coefficients to make the matrices M_u and M_v be automorphisms of the curve. With this procedure, one easily finds expressions for these coefficients in terms of the roots β_i of $g(X)$, and then use k-base of K (see Remark 4) to find the expressions above. Moreover, by using this method one obtains that the given genus 2 curve is unique up to hyperelliptic twists.

Proposition 12. *Let C, C' be curves of genus 2 with $\mathrm{Aut}(C) \simeq \mathrm{Aut}(C') \simeq \tilde{S}_4$. If the G_k-structures on both automorphism groups are equivalent, then C and C' differ by, at most, a hyperelliptic twist and a k-isomorphism.*

Proof. A direct proof of this proposition is given in Remark 11. A more algebraic proof can be easily obtained by adapting the proof of [4, Theorem 4.8]. □

Proposition 13. *Let C be a curve of genus 2 with $\mathrm{Aut}(C) \simeq \tilde{S}_4$, and C_e the hyperelliptic twist of C over $k(\sqrt{e})$. Let K, $K_u = k(\sqrt{u})$, $K_d = k(\sqrt{-2})$ be the associated fields to the G_k-structure on $\mathrm{Aut}(C)$. Then, C and C_e are k-isomorphic if, and only if, $e \in E \cap k^*$, where E is defined as:*

(1) $E = k^{*2}$ *if* $3 \mid [K:k]$,
(2) $E = (K \cdot K_d)^{*2}$ *if* $[K:k] \leqslant 2$,
(3) $E = K_d^{*2}$ *if* $\mathrm{Gal}(K/k) \simeq C_4$,
(4) $E = K^{*2}$ *if* $\mathrm{Gal}(K/k) \simeq V_4$ *and* $K_u = k$,
(5) $E = (K_u \cdot k(\sqrt{-2v}))^{*2}$ *if* $\mathrm{Gal}(K/k) \simeq V_4$, *with* $K = k(\sqrt{u}, \sqrt{v})$,
(6) $E = k(\sqrt{v})^{*2}$ *if* $\mathrm{Gal}(K/k) \simeq D_8$, *where* $K/k(\sqrt{v})$ *is cyclic.*

Proof. Note that C and C_e are k-isomorphic if, and only if, there exists $\varphi \in \mathrm{Aut}(C)$ defined over $k(\sqrt{e})$ such that ${}^\sigma\varphi = \pm\varphi$ for all $\sigma \in G_k$. Indeed, since $\psi_e = \sqrt{e} I_2$ defines an isomorphism between C and C_e, any other isomorphism is of the form $\psi_e\varphi$, with $\varphi \in \mathrm{Aut}(C)$, and this isomorphism is defined over k when φ is as claimed. The result is now obtained by explicitly finding the Galois action on $\mathrm{Aut}(C)$ for each of the possibilities. □

The results obtained allow us to give a parametrization of the set of k-isomorphism classes of curves of genus 2 with group of automorphisms isomorphic to $\tilde{S}_4$, or, equivalently, the set of twists of the curve $y^2 = x^5 - x$ over any field k.

Theorem 14. *The set of k-isomorphism classes of curves of genus 2 with group of automorphisms isomorphic to $\tilde{S}_4$ is parameterized by the set of triples (K, K_u, e), where (K, K_u) is a pair of principal fields and $e \in k^*/(E \cap k^*)$, with E as in Proposition 13. A representative corresponding to some triple (K, K_u, e) is obtained by taking the genus 2 curve $ey^2 = f(x)$, with $f(x)$ as in Proposition 10.*

References

[1] O. Bolza, On binary sextics with linear transformations into themselves, Amer. J. Math. 10 (1888) 47–70.
[2] G. Cardona, On the number of curves of genus 2 over a finite field, Finite Fields Appl. 9 (4) (2003) 505–526.
[3] G. Cardona, E. Nart, J. Pujolàs, Curves of genus two over fields of even characteristic, Math. Z. 250 (1) (2005) 177–201.
[4] G. Cardona, J. Quer, Curves of genus 2 with group of automorphisms isomorphic to D_8 or D_{12}, Trans. Amer. Math. Soc. (2006), in press.

[5] J. Fernández, J.-C. Lario, A. Rio, Octahedral Galois representations arising from **Q**-curves of degree 2, Canad. J. Math. 54 (6) (2002) 1202–1228.
[6] The GAP Group, GAP—Groups, Algorithms, and Programming, Version 4.4, http://www.gap-system.org, 2004.
[7] J.-I. Igusa, Arithmetic variety of moduli for genus two, Ann. of Math. 72 (3) (1960) 612–649.
[8] School Mathematics and Statistics, University of Sydney, The Magma Computational Algebra System, http://magma.maths.usyd.edu.au/magma/, 2004.