TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 359, Number 6, June 2007, Pages 2831–2849
S 0002-9947(07)04111-6
Article electronically published on January 4, 2007

CURVES OF GENUS 2 WITH GROUP OF AUTOMORPHISMS ISOMORPHIC TO D_8 OR D_{12}

GABRIEL CARDONA AND JORDI QUER

Abstract. The classification of curves of genus 2 over an algebraically closed field was studied by Clebsch and Bolza using invariants of binary sextic forms, and completed by Igusa with the computation of the corresponding three-dimensional moduli variety $\mathcal{M}_2$. The locus of curves with group of automorphisms isomorphic to one of the dihedral groups D_8 or D_{12} is a one-dimensional subvariety.

In this paper we classify these curves over an arbitrary perfect field k of characteristic $\operatorname{char} k \neq 2$ in the D_8 case and $\operatorname{char} k \neq 2, 3$ in the D_{12} case. We first parameterize the $\overline{k}$-isomorphism classes of curves defined over k by the k-rational points of a quasi-affine one-dimensional subvariety of $\mathcal{M}_2$; then, for every curve C/k representing a point in that variety we compute all of its k-twists, which is equivalent to the computation of the cohomology set $H^1(G_k, \operatorname{Aut}(C))$.

The classification is always performed by explicitly describing the objects involved: the curves are given by hyperelliptic models and their groups of automorphisms represented as subgroups of $\mathrm{GL}_2(\overline{k})$. In particular, we give two generic hyperelliptic equations, depending on several parameters of k, that by specialization produce all curves in every k-isomorphism class.

1. Preliminaries on hyperelliptic curves and curves of genus 2

This section contains basic definitions, notation, and some well-known facts on hyperelliptic curves and curves of genus 2. References are [2], [5], [6].

Throughout the paper, k is a perfect field of characteristic different from 2, and G_k is the Galois group of an algebraic closure $\overline{k}/k$. The Galois action on the elements of any G_k-set will be denoted exponentially on the left: $(\sigma, a) \mapsto {}^{\sigma}a$ for $\sigma \in G_k$ and a in a G_k-set. Whenever a cohomology group or set $H^i(G_k, A)$ is considered, we mean Galois cohomology, where cocycles are continuous with respect to the discrete topology on A and the Krull topology on G_k. We refer the reader to [7] for definitions and basic results on nonabelian Galois cohomology.

Some results are stated in terms of elements of $\mathrm{Br}_2(k) \simeq H^1(G_k, \{\pm 1\})$, the 2-torsion of the Brauer group of the field k. We denote by (a, b) the class of the quaternion algebra with basis $1, i, j, ij$ and multiplication defined by $i^2 = a, j^2 = b, ji = -ij$.

Received by the editors November 24, 2003 and, in revised form, June 7, 2005.
2000 *Mathematics Subject Classification.* Primary 11G30, 14G27.
Key words and phrases. Curves of genus 2, twists of curves.
The authors were supported by Grants BFM-2003-06768-C02-01 and SGR2005-00443.

©2007 American Mathematical Society

A curve C/k of genus g is hyperelliptic over k if there is a morphism $\pi : C \to \mathbb{P}^1$ of degree 2 defined over k. These curves have a model given by an equation

$$C: \quad Y^2 = F(X) \tag{1.1}$$

with $F(X) \in k[X]$ a polynomial of degree $2g+1$ or $2g+2$ without multiple roots. Conversely, every such equation is a model of a curve of genus g defined over k and hyperelliptic over k, with a unique singularity at the point at infinity that corresponds to one or two points in a regular model, depending on whether the degree of the polynomial $F(X)$ is odd or even. We call the equation (1.1) a *hyperelliptic equation*.

Every curve C/k of genus 2 is hyperelliptic over k. In general, we will implicitly assume that curves of genus 2 over k are given by hyperelliptic equations. The isomorphisms between two such curves correspond, in terms of hyperelliptic equations, to transformations of the type

$$X' = \frac{aX+b}{cX+d}, \qquad Y' = \frac{(ad-bc)Y}{(cX+d)^3}, \tag{1.2}$$

associated to a uniquely determined matrix

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\overline{k}).$$

The field of definition of that isomorphism is the field generated, over the common field of definition of the two curves, by the coefficients of the matrix M. In particular, for every curve C/k of genus 2, and once a hyperelliptic equation for C is fixed, the group of automorphisms $A = \mathrm{Aut}(C) = \mathrm{Aut}_{\overline{k}}(C)$ can be identified with a subgroup of $\mathrm{GL}_2(\overline{k})$ which is closed by the Galois action of the group G_k; this association preserves both the group law and the Galois action on both sides, i.e. is a morphism of G_k-groups.

Every hyperelliptic curve C/k has a canonical involution, the *hyperelliptic involution* ι, that is always defined over the ground field and commutes with every automorphism. In terms of a hyperelliptic model for C, it corresponds to $(X,Y) \mapsto (X,-Y)$, its matricial representation for the genus 2 case is given by the matrix -1, and it is the unique nontrivial automorphism given by a scalar matrix. The quotient group $A' = A/\langle\iota\rangle$ is known as the *reduced group of automorphisms*, and is identified with the isotropy subgroup of the set of ramified points of the covering $\pi : C \to \mathbb{P}^1$ under the action of $\mathrm{PGL}_2(\overline{k})$.

2. Parameterization over an algebraically closed field

The complete classification of curves of genus 2 over an algebraically closed field was obtained by Igusa in [4], completing previous work by Bolza and Clebsch. The classification is obtained in terms of invariants of binary sextic forms

$$a_0Y^6 + a_1Y^5X + a_2Y^4X^2 + a_3Y^3X^3 + a_4Y^2X^4 + a_5YX^5 + a_6X^6$$

attached to the polynomials $F(X) = \sum_{i=0}^{6} a_iX^i$ that correspond to hyperelliptic equations of the curves. An *invariant of binary sextic forms* of degree $d \geq 1$ is a polynomial expression $I \in k[a_0, \ldots, a_6]$ in the coefficients of the sextic form that

after a linear transformation of the variables changes by the d-th power of the determinant. Given an invariant I, we will denote by $I(F)$ (resp. $I(C)$) the value that the invariant takes when evaluated at some sextic form F (resp. some curve C).

The invariants that normally are used in the literature are the *Clebsch invariants*, denoted as A, B, C, D in [1] and [5], that we will denote by c_2, c_4, c_6, c_{10}, the *Igusa invariants* I_2, I_4, I_6, I_{10}, defined as symmetric expressions of the roots of F (cf. [4, pag. 620]), and the *Igusa arithmetic invariants* J_2, J_4, J_6, J_{10} (cf. [4, pag. 621]). In all cases of our notation, the subindices give the degrees of the invariants. It should be noticed that, in order to make explicit computations with invariants, Clebsch invariants reduce well in every characteristic different from 2, 3 and 5, Igusa invariants sort out the case of characteristic 5, and finally Igusa arithmetic invariants are suitable for any characteristic.

The *absolute invariants* are defined as the quotients of invariants of the same degree. As for the case of invariants, we will denote by $t(F)$ or $t(C)$ the value that an absolute invariant t takes when evaluated at some sextic form F or curve C.

The classification of curves of genus 2 up to $\overline{k}$-isomorphism is given by their absolute invariants: two curves C_1 and C_2 are isomorphic if, and only if, $t(C_1) = t(C_2)$ for every absolute invariant t.

The possible reduced groups of automorphisms of curves of genus 2 were determined by Bolza in terms of their invariants (cf. [1, pag. 70]), and the structure of the corresponding groups can be found in [3]. The picture, outside of characteristics 2, 3 and 5, is the following: the group $\mathrm{Aut}(C)$ is isomorphic to one of the groups

$$C_2, \quad V_4, \quad D_8, \quad D_{12}, \quad 2D_{12}, \quad \widetilde{S}_4, \quad C_{10},$$

with $2D_{12}$ and $\widetilde{S}_4$ denoting certain double covers of the dihedral group D_{12} and the symmetric group S_4, respectively.

The moduli space of curves of genus 2 is of dimension 3. The generic curve has group of automorphisms isomorphic to C_2, generated by the hyperelliptic involution. The curves with $V_4 \subseteq \mathrm{Aut}(C)$ cut out a surface in that 3-dimensional moduli space, and those with $D_8 \subseteq \mathrm{Aut}(C)$ or with $D_{12} \subseteq \mathrm{Aut}(C)$ describe two curves contained in that surface. Each of the three remaining groups is the group of automorphisms of a unique curve up to isomorphism.

In this paper we study the two families of curves of genus 2 with $\mathrm{Aut}(C) \simeq D_8$ or D_{12}. As explained in the previous paragraph, over an algebraically closed field these curves are one-dimensional families, and it is not difficult to find explicit parameterizations (cf. [1, pag. 50]). The next two propositions introduce parameterizations in terms of an absolute invariant. Our parameterizations are different from those of [1], which are the ones usually found in the literature, and have the advantage that the field of definition of the curve is also the field of definition of the corresponding point on the moduli space, that is, the field of moduli of the curve.

Proposition 2.1. *Let k be a field of characteristic different from 2. The $\overline{k}$-isomorphism classes of curves C/k of genus 2 with $\mathrm{Aut}(C) \simeq D_8$ are classified by the open subset of the affine line*

$$k \smallsetminus \{0, 1/4, 9/100\}.$$

An explicit bijection is obtained by evaluating at a given curve C the absolute invariant given by

$$t = \begin{cases} 1 + \dfrac{J_4}{J_2^2}, & \text{if } \operatorname{char} k = 5, \\ \dfrac{-J_2^2}{J_4}, & \text{if } \operatorname{char} k = 3, \\ \dfrac{8c_6(6c_4 - c_2^2) + 9c_{10}}{900c_{10}}, & \text{otherwise,} \end{cases}$$

and associating to an element $t \in k \smallsetminus \{0, 1/4, 9/100\}$ the curve with equation

$$Y^2 = X^5 + X^3 + t\,X.$$

Proof. The polynomial $X^5 + X^3 + t\,X$ has multiple roots for exactly the two values $t = 0, 1/4$, hence the equation $Y^2 = X^5 + X^3 + t\,X$ defines a hyperelliptic curve C_t of genus 2 for every $t \neq 0, 1/4$. It follows from a direct computation using expressions (1.2) that the two matrices

$$U = \begin{pmatrix} -\sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix}, \qquad V = \begin{pmatrix} 0 & t^{1/4} \\ t^{-1/4} & 0 \end{pmatrix},$$

give automorphisms of the curve, and they generate a group isomorphic to D_8. Moreover, the equality $\operatorname{Aut}(C) = \langle U, V \rangle$ holds if $t \neq 9/100$. For this value of t, the group of automorphisms of the curve is isomorphic to $2D_{12}$. Conversely, given a curve $C/\overline{k}$ with $\operatorname{Aut}(C) \simeq D_8$, its group of automorphisms is $\mathrm{GL}_2(\overline{k})$-conjugated to the group generated by two matrices U, V as above; the matrix giving this conjugation also gives an isomorphism between C and a curve of the form C_t for some $t \in \overline{k}$.

Using the formulas expressing the Clebsch and Igusa arithmetic invariants of a curve as polynomials on the coefficients of a polynomial of degree 5 or 6 in a hyperelliptic equation defining the curve, one checks that $t \in \overline{k}$ is the absolute invariant of the curve C_t given in the statement of the proposition in terms of invariants of the curve.

Since t is an absolute invariant of the curve C_t, it follows that if C_t and $C_{t'}$ are isomorphic, then $t = t'$, and the converse follows trivially.

As for the field of definition, if $t \in k$ the curve C_t is defined over k. Conversely, if a curve C is defined over k and C_t is a curve isomorphic to it, then $t \in k$, since t is an absolute invariant of C. □

Remark. Note that in characteristic 5, there is no need to exclude any other value than 0 and 1/4, and the parameterization above should be read $k \smallsetminus \{0, -1\}$. This remark also holds for proposition 2.2.

The next proposition is analogous for $\operatorname{Aut}(C) \simeq D_{12}$, and the proof is analogous, taking into account that for $t = -1/50$ one gets a curve with group of automorphisms isomorphic to $\widetilde{S}_4$.

Proposition 2.2. *Let k be a field of characteristic different from 2 and 3. The $\overline{k}$-isomorphism classes of curves C/k of genus 2 with $\operatorname{Aut}(C) \simeq D_{12}$ are classified by the open subset of the affine line*

$$k \smallsetminus \{0, 1/4, -1/50\}.$$

An explicit bijection is obtained by evaluating at a given curve C the absolute invariant given by

$$t = \begin{cases} -1 - \dfrac{J_4}{J_2^2}, & \text{if} \quad \operatorname{char} k = 5, \\ \dfrac{3c_4c_6 - c_{10}}{50c_{10}}, & \text{otherwise}, \end{cases}$$

and associating to an element $t \in k \smallsetminus \{0, 1/4, -1/50\}$ the curve with equation

$$Y^2 = X^6 + X^3 + t.$$

Remark. Over perfect fields of characteristic 3, the parameterization is obtained by now taking as an absolute invariant

$$t = \frac{-J_2^3}{J_6}$$

and as an equation for the curve

$$y^2 = t_*^{-1}x^6 + x^4 + x^2 + 1,$$

with $t_* \in k$ such that $t_*^3 = t$.

From now on we will use the invariants in these propositions to parameterize the curves up to $\overline{k}$-isomorphism, and for that we make the following definition.

Definition 2.3. Let C/k be a curve of genus 2 with $\mathrm{Aut}(C) \simeq D_8$ or D_{12}. The element $t = t(C) \in k$ defined as a quotient of invariants of the same degree by the formulas of the previous propositions will be called *the absolute invariant* of the curve C.

3. Galois structures on D_8 and D_{12}

In order to study the classification of curves of genus 2 over arbitrary fields in the next section, we will make use of Galois actions on groups isomorphic to D_8 and D_{12}. In this section we study such G_k-group structures, paying special attention to those that can be realized as subgroups of matrices.

Galois structures on groups. Let A be a finite group. The G_k-group structures on the group A (up to isomorphism of G_k-groups) are classified by the cohomology set

$$H^1(G_k, \mathrm{Aut}(A)) = \mathrm{Inn}(\mathrm{Aut}(A)) \backslash \mathrm{Hom}(G_k, \mathrm{Aut}(A))$$

with $\mathrm{Aut}(A)$ viewed as a G_k-group with trivial action. More precisely, a group action $(\sigma, a) \mapsto {}^{\sigma}a : G_k \times A \to A$ corresponds to a homomorphism $\rho : G_k \to \mathrm{Aut}(A)$, and isomorphic actions differ by conjugation by an element of $\mathrm{Aut}(A)$. The fixed field of $\ker \rho$ will be called the *field of definition* of the G_k-action on A (or of A viewed as a G_k-group), and from now on it will be denoted by K.

Let A be a G_k-group. From every 1-cocycle $\sigma \mapsto \xi_\sigma : G_k \to A$ we can define another action on the group A by the formula ${}^{\sigma}_{\xi}a = \xi_\sigma^{-1}\sigma a \xi_\sigma$. The corresponding G_k-group, denoted as ${}_{\xi}A$, depends only on the cohomology class of ξ and is known as the *twisted group*. A group action on A induces an action on the maximal abelian quotient A^{ab}, and it is clear that twisted actions induce the same action on that quotient.

Given a conjugation class T of subgroups of $\mathrm{Aut}(A)$, we say that a G_k-group structure on A is *of type* T if $\operatorname{im}\rho \in T$. Then, the action induces an isomorphism $\mathrm{Gal}(K/k) \simeq \operatorname{im}\rho$ and two G_k-group structures belonging to the same type T and

TABLE 1. G_k-group structures on D_8

$\operatorname{im}\rho$	K/k	K_2/k	K_1/k	Type	remarks
1	I	I	I	I	
$\langle t^2\rangle$	C_2	I	I	C_2^A	
$\langle s\rangle, \langle st^2\rangle$	C_2	C_2	I	C_2^B	
$\langle st\rangle, \langle st^3\rangle$	C_2	C_2	C_2	C_2^C	
$\langle t\rangle$	C_4	I	C_2	C_4	
$\langle s, t^2\rangle$	V_4	C_2	I	V_4^A	
$\langle st, t^2\rangle$	V_4	C_2	C_2	V_4^B	$K_1 = K_2$
$\langle s, t\rangle$	D_8	C_2	C_2	D_8	$\operatorname{Gal}(K/K_1) \simeq V_4$, $\operatorname{Gal}(K/K_2) \simeq C_4$

having the same field K as the field of definition, with corresponding maps $\rho, \rho' : G_k \to \operatorname{Aut}(A)$, differ by an isomorphism $\operatorname{im}\rho \simeq \operatorname{im}\rho'$, up to isomorphisms induced by conjugation by an element of $\operatorname{Aut}(A)$.

Galois structures on D_8. Consider the group $A \simeq D_8$, with presentation

$$A = \langle\, U, V \mid U^2 = V^4 = 1, VU = UV^3 \,\rangle.$$

The group $\operatorname{Aut}(A)$ is also isomorphic to D_8, and it is generated by the two automorphisms s and r defined by

$$\begin{aligned} s(U) &= U, & r(U) &= UV, \\ s(V) &= V^3, & r(V) &= V \end{aligned} \tag{3.1}$$

with the relations $s^2 = r^4 = 1, rs = sr^3$. The inner automorphisms of $\operatorname{Aut}(A)$ are the subgroup of $\operatorname{Aut}(\operatorname{Aut}(A))$, isomorphic to the Klein group V_4, generated by the conjugation by s and the conjugation by r.

The characteristic subgroups of A (the subgroups invariant by every automorphism) are, apart from the trivial subgroup and the group A itself, the subgroups $Z(A) = \langle V^2\rangle \simeq C_2$ and $\langle V\rangle \simeq C_4$. In particular, every G_k-group structure on A induces corresponding structures on these groups, and also on the quotients $A' = A/Z(A) \simeq V_4$ and $A/\langle V\rangle \simeq C_2$. We remark that $A' = A^{\mathrm{ab}}$.

For every G_k-group structure on A with field of definition K, we will denote by K_1 the field of definition of the induced action on A', and by K_2 the field of definition of the induced action on the subgroup $\langle V\rangle$. Then, $\operatorname{Gal}(K/k)$ is isomorphic to a subgroup of D_8 and $\operatorname{Gal}(K_i/k)$ can be trivial or isomorphic to the group C_2 for $i = 1, 2$. Throughout the rest of the paper, whenever a G_k-group A isomorphic to D_8 is considered, K, K_1 and K_2 will always denote the extensions of k that are the fields of definition of the Galois action on the group A, on the quotient A' and on the subgroup $\langle V\rangle$, respectively.

By examination of all the subgroups of $\operatorname{Aut}(A)$, one finds all the possible types of G_k-group structures, that are classified in Table 1. In this table, the first column contains the subgroups of $\operatorname{Aut}(A)$ grouped by conjugacy classes. The next three columns give the structure of the Galois group of the three extensions $K/k, K_2/k, K_1/k$. The column labeled "Type" gives a name to each type of structure, consisting of the Galois group of the field of definition of the Galois action

and an upper letter that distinguishes between the different types having the same group. Finally, the last column gives some remarks on the fields $K_1 = k(\sqrt{u})$ and $K_2 = k(\sqrt{v})$. Note also that the identity $(u, -v) = 1$ in $\mathrm{Br}_2(k)$ is always satisfied; for the types where this equality is not self-evident, it follows from the fact that K_1 can be embedded in the C_4-extension K, for the type C_4, and that $K_1 \cdot K_2$ can be embedded in the D_8-extension K, with K/K_2 cyclic, for the type D_8.

A G_k-group is completely determined, up to isomorphism, by only giving its type and the field K of definition of the action, except for the two V_4-types, where one has to specify which of the three quadratic subfields of K plays the role of K_2 (three choices for every K), and for type D_8, where one must specify which of the two quadratic subfields such that K is not cyclic over them plays the role of K_1 (two choices for every K).

For every row in the table, and given extensions K, K_1 and K_2 of k with the first containing the other two, having the Galois groups that appear in that row, and satisfying the conditions of the last column, there is a unique G_k-group structure on the group D_8 with the prescribed fields as fields of definition.

Explicit construction of fields of definition. The following two lemmas introduce explicit constructions of the fields of definition of G_k-groups isomorphic to D_8 in terms of radicals of elements of k.

Lemma 3.1. *Let* $\mathrm{char}\, k \neq 2$ *and let* A *be a* G_k*-group isomorphic to* D_8*. Write* $K_1 = k(\sqrt{u})$ *and* $K_2 = k(\sqrt{v})$ *for elements* $u, v \in k^*$*. Then, there exist elements* $z \in k$ *and* $w \in k^*$ *such that* $uv \equiv 1 - z^2 u \pmod{k^2}$ *and with*

$$K = k\Big(\sqrt{v}, \sqrt{\frac{w(1 \pm z\sqrt{u})}{2}}\Big). \tag{3.2}$$

Conversely, given elements $u, v, w \in k^*$ *and* $z \in k$ *with* $uv \equiv 1 - z^2 u \pmod{k^2}$ *there exists a* G_k*-group isomorphic to* D_8 *with fields of definition* $K_1 = k(\sqrt{u}), K_2 = k(\sqrt{v})$ *and* K *given by the expression (*3.2*).*

Proof. Assume that a G_k-group A isomorphic to D_8 is given.

Consider first the case $K_1 = k$. In this case the extension K/k is trivial, quadratic or biquadratic, and can be written as $K = k(\sqrt{v}, \sqrt{m})$ for some $m \in k^*$. Taking $z = 1/\sqrt{u}$ and $w = m$, it is straightforward to check that the conditions are satisfied.

Assume now that $K_1 \neq k$. Then, if $[K : k] = 2$ or 4, the field K can be obtained by adjoining to K_1 the square root of a nonzero element, and if $[K : k] = 8$, then $\mathrm{Gal}(K/k) \simeq D_8$ and the field K is the Galois closure of a quartic nonnormal extension of k obtained by adjoining to K_1 the square root of a nonzero element. In either case, let $\alpha = x + y\sqrt{u}$ be such a nonzero element. After multiplying it by a square if necessary, we may assume that x is nonzero, and then α may be written as $w(1 - z\sqrt{u})/2$ for some elements $w, z \in k$ with $w \neq 0$. Since the extension K/k is normal, the field K also contains the square root of the conjugate element $\overline{\alpha} = w(1 + z\sqrt{u})/2$ and then K is obtained as (3.2). It only remains to be checked that $1 - z^2 u \equiv uv \pmod{k^{*2}}$ for the element z we used, but this congruence is a consequence of the fact that the field K contains the element $\beta = \sqrt{\alpha}\sqrt{\overline{\alpha}} = \frac{w}{2}\sqrt{1 - z^2 u}$, and an element of G_k leaves β fixed if, and only if, it fixes the element $\sqrt{uv}$.

For the converse, given elements u, v, z, w with $1 - z^2 u \equiv uv \pmod{k^2}$, the field $K = k(\sqrt{v}, \sqrt{w(1 \pm z\sqrt{u})/2})$ is a normal extension of k with Galois group

isomorphic to a subgroup of D_8 and contains the fields $K_1 = k(\sqrt{u})$ and $K_2 = k(\sqrt{v})$ as subfields. Using Table 1, it is easy to check that there is a structure with the given fields as fields of definition. □

Lemma 3.2. *Let* $\operatorname{char} k \neq 2$ *and let* A *be a* G_k*-group isomorphic to* D_8*. Let* $u, v, w \in k^*$ *and* $z \in k$ *elements determining the fields* K, K_1 *and* K_2 *as in the previous lemma. Given an element* $w' \in k^*$ *there exists a* $z' \in k$ *such that* u, v, z', w' *give the same fields if, and only if,* $(-v, w) = (-v, w')$ *in* $\mathrm{Br}_2(k)$*.*

Proof. The equality for the fields K_1 and K_2 is clear. As for the field K, it is the decomposition field of the polynomial

$$g(X) = X^4 - wX^2 + \frac{1}{4}(1 - z^2u).$$

In order to also be the decomposition field of some polynomial of the form

$$g'(X) = X^4 - w'X^2 + \frac{1}{4}(1 - z'^2u),$$

there has to exist a Tschirnhaus transformation that sends g to g'; namely, one needs to find $a_1, \dots, a_4 \in k$ such that

$$g'(a_1 + a_2\alpha_i + a_3\alpha_i^2 + a_4\alpha_i^3) = 0 \quad \text{if, and only if,} \quad g(\alpha_i) = 0.$$

Computing explicitly the first term in the expression above, one finds that the condition is equivalent to the existence of $a_1, a_3 \in k$ such that

$$wa_1^2 + \frac{1}{4}uw^3z^2(1 - z^2u)a_3^2 = w',$$

which is equivalent to the fact that the quadratic form

$$\frac{w}{w'}X_1^2 + \frac{1}{4}\frac{uw^3z^2(1 - z^2u)}{w'}X_2^2$$

represents 1. A little computation in $\mathrm{Br}_2(k)$ shows that it is equivalent to have $(-v, w)(-v, w') = 1$, from which the result follows. □

Realization of G_k-groups isomorphic to D_8 as groups of matrices. Since the groups of automorphisms of curves of genus 2 are G_k-groups that can be represented as sub-G_k-groups of $\mathrm{GL}_2(\overline{k})$, we study these representations.

Proposition 3.3. *Let* $\operatorname{char} k \neq 2$ *and let* A *be a sub-*G_k*-group of* $\mathrm{GL}_2(\overline{k})$ *isomorphic to* D_8*. For every* $u, v \in k^*$ *such that* $K_1 = k(\sqrt{u})$ *and* $K_2 = k(\sqrt{v})$ *there exists an element* $z \in k$ *such that the group* A *is* $\mathrm{GL}_2(k)$*-conjugated of the group generated by the two matrices*

$$U = \begin{pmatrix} \alpha & \beta \\ \beta/v & -\alpha \end{pmatrix}, \qquad V = \begin{pmatrix} 0 & -\sqrt{v} \\ 1/\sqrt{v} & 0 \end{pmatrix}, \tag{3.3}$$

with

$$\alpha = \sqrt{\frac{1 - z\sqrt{u}}{2}}, \qquad \beta = \sqrt{\frac{v(1 + z\sqrt{u})}{2}}. \tag{3.4}$$

In that case, the congruence $1 - z^2u \equiv uv \pmod{k^2}$ *is satisfied, say* $1 - z^2u = s^2uv$*, with* $s \in k$*.*

Conversely, given elements $u, v \in k^*$ *and* $z \in k$ *with* $1 - z^2u \equiv uv \pmod{k^2}$*, the matrices* U, V *defined as above generate a sub-*G_k*-group of* $\mathrm{GL}_2(\overline{k})$ *isomorphic to* D_8*.*

Proof. Let A be a G_k-subgroup of $\mathrm{GL}_2(\overline{k})$ isomorphic to D_8. Since the central element V^2 of order 2 must be represented by the matrix -1, the group is generated by matrices U and V with the relations

$$A = \langle\, U, V \mid U^2 = 1, V^2 = -1, UV = -VU \,\rangle.$$

The matrix V is defined over $k(\sqrt{v})$ and the matrix $V_0 = \sqrt{v}V$ is fixed by every Galois automorphism and has characteristic polynomial $X^2 + v$. After conjugation of the group A by a matrix of $\mathrm{GL}_2(k)$, if necessary, we may assume that V_0 is the companion matrix of that polynomial and then the matrix V is

$$V = \begin{pmatrix} 0 & -\sqrt{v} \\ 1/\sqrt{v} & 0 \end{pmatrix}.$$

The matrices $U \in \mathrm{GL}_2(\overline{k})$ of order two satisfying $UV = -VU$ are the matrices of the form

$$U = \begin{pmatrix} \alpha & \beta \\ \beta/v & -\alpha \end{pmatrix}, \qquad \alpha, \beta \in \overline{k}, \qquad \alpha^2 + \frac{\beta^2}{v} = 1.$$

The matrix U can have at most the four Galois conjugates $\pm U, \pm UV$. Hence, it is defined over a field K_U that contains the field $K_1 = k(\sqrt{u})$ and such that the extension K_U/K_1 is either trivial or quadratic, and the elements of $\mathrm{Gal}(K_U/K_1)$ send U to $\pm U$. It follows that α^2 and β^2 belong to the field K_1.

If $K_1 = k$, then we just define $z = (1 - 2\alpha^2)/\sqrt{u}$, and the elements α, β are expressed in terms of this element by the formulas (3.4).

Assume now that $K_1 \neq k$. Then, every $\sigma \in G_k$ that acts nontrivially on K_1 acts on the matrix U as ${}^{\sigma}U = \pm UV$, and since the matrix UV is of the form

$$UV = \begin{pmatrix} \beta/\sqrt{v} & -\sqrt{v}\alpha \\ -\alpha/\sqrt{v} & -\beta/\sqrt{v} \end{pmatrix},$$

we get ${}^{\sigma}\alpha^2 = \beta^2/v$. Now, if we express α^2 as an element of $k(\sqrt{u})$, say $\alpha^2 = (x - z\sqrt{u})/2$ with $x, z \in k$, then β^2 is the element $v(x + z\sqrt{u})/2$ of $k(\sqrt{u})$. From the identity $\alpha^2 + \beta^2/v = 1$ it follows that necessarily x must be 1 and α and β are given by the expressions (3.4).

For every $\sigma \in G_k$ we have ${}^{\sigma}(\alpha\beta) = \pm\alpha\beta$ depending on the action of σ on the field K_1. Hence $\alpha\beta$ differs from $\sqrt{u}$ by an element of k and

$$(\alpha\beta)^2 = \frac{v(1 - z^2u)}{4} \equiv u \pmod{k^2},$$

from which we get that $1 - z^2u \equiv uv \pmod{k^2}$.

As for the converse, let u, v, z be elements of k satisfying the required congruence. Then it is immediate to check that the matrices U and V defined by (3.3) and (3.4) generate a group isomorphic to D_8. If $\sigma \in G_k$, then ${}^{\sigma}V = \pm V$. Let

$$\overline{\alpha} = \sqrt{\frac{1 + z\sqrt{u}}{2}} = \frac{\beta}{\sqrt{v}}, \qquad \overline{\beta} = \sqrt{\frac{v(1 - z\sqrt{u})}{2}} = \alpha\sqrt{v}.$$

The Galois conjugates of α belong to the set $\{\pm\alpha, \pm\overline{\alpha}\}$. If ${}^{\sigma}\alpha = \pm\alpha$, then ${}^{\sigma}\beta = \pm\beta$ and ${}^{\sigma}U = \pm U$; if ${}^{\sigma}\alpha = \pm\overline{\alpha}$, then ${}^{\sigma}\beta = \mp\overline{\beta}$ and ${}^{\sigma}U = \pm UV$. Hence, the group $\langle U, V\rangle$ is closed by the Galois action. □

Theorem 3.4. *A G_k-group isomorphic to D_8 can be realized as a sub-G_k-group of $\mathrm{GL}_2(\overline{k})$ if, and only if, $(-v, w)$ is trivial in $\mathrm{Br}_2(k)$, with $v, w \in k^*$ as in lemma* 3.1.

TABLE 2. G_k-group structures on D_{12}

$\mathrm{im}(\rho)$	K/k	K_3/k	K_2/k	K_1/k	Type	remarks
1	I	I	I	I	I	
$\langle t^3\rangle$	C_2	I	I	C_2	C_2^A	
$\langle s\rangle, \langle st\rangle, \langle st^2\rangle$	C_2	C_2	C_2	I	C_2^B	
$\langle st^3\rangle, \langle st^4\rangle, \langle st^5\rangle$	C_2	C_2	C_2	C_2	C_2^C	
$\langle t^2\rangle$	C_3	C_3	I	I	C_3	
$\langle t\rangle$	C_6	C_3	I	C_2	C_6	
$\langle s, t^3\rangle, \langle st, t^3\rangle, \langle st^2, t^3\rangle$	V_4	C_2	C_2	C_2	V_4	$K_1 \neq K_2$
$\langle s, t^2\rangle$	D_6	D_6	C_2	I	D_6^A	
$\langle st^3, t^2\rangle$	D_6	D_6	C_2	C_2	D_6^B	
$\langle s, t\rangle$	D_{12}	D_6	C_2	C_2	D_{12}	$\mathrm{Gal}(K/K_1) \simeq D_6$, $\mathrm{Gal}(K/K_2) \simeq C_6$

Proof. From proposition 3.3 it follows that the G_k-group is isomorphic to a G_k-group of matrices if, and only if, the field of definition can be written as in lemma 3.1 with the value $w = 1$. By lemma 3.2, given any elements z, w determining the field of definition of the corresponding action as in lemma 3.1, there exist elements z', w' determining the same field with $w' = 1$ if, and only if, $(-v, w) = (-v, 1) = 1$. □

Galois structures on D_{12}. Now we consider the group $A \simeq D_{12}$, with presentation

$$A = \langle\ U, V \mid U^2 = V^6 = 1, VU = UV^5\ \rangle.$$

The group $\mathrm{Aut}(A)$ is also isomorphic to D_{12}, and it is generated by the two automorphisms s and r defined by

$$\begin{aligned} s(U) &= U, & r(U) &= UV, \\ s(V) &= V^5, & r(V) &= V \end{aligned} \tag{3.5}$$

with the relations $s^2 = r^6 = 1, rs = sr^5$. The inner automorphisms of $\mathrm{Aut}(A)$ are the subgroup of $\mathrm{Aut}(\mathrm{Aut}(A))$, isomorphic to the dihedral group D_6, generated by the conjugation by s and the conjugation by r.

The characteristic subgroups of A different from the trivial subgroup and from A itself are the subgroups $Z(A) = \langle V^3\rangle \simeq C_2$, $\langle V^2\rangle \simeq C_3$ and $\langle V\rangle \simeq C_6$. Every G_k-group structure on A induces G_k-group structures on these groups and also on the quotients $A' = A/Z(A) \simeq D_6$, $A/\langle V^2\rangle \simeq V_4$ and $A/\langle V\rangle \simeq C_2$. We remark that $A/\langle V^2\rangle = A^{\mathrm{ab}}$.

For every G_k-group structure on A with field of definition K, we will denote by K_1, K_2 and K_3 the fields of definition of the induced actions on the groups $A/\langle V^2\rangle, \langle V\rangle$ and A', respectively. We remark that the field of definition of $\langle V\rangle$ is the same than that of $\langle V^2\rangle$. The Galois group of the extension K/k is isomorphic to a subgroup of D_{12}, the subfield K_3/k has Galois group isomorphic to a subgroup of D_6 and the two extensions K_i/k for $i = 1, 2$ can be either trivial or quadratic, with $K_2 \subseteq K_3$.

In Table 2, we give the classification of the G_k-group structures on D_{12} by types, in an analogous way than we did before for the group D_8.

A G_k-group isomorphic to D_{12} is completely determined, up to isomorphism, by giving its type and the field of definition of the action K/k, except for type V_4, where one needs to specify which of the three quadratic subfields of K are the fields K_1 and K_2 (six choices for a given K), and for type D_{12}, where one must specify which of the two quadratic subfields such that K is not cyclic over them plays the role of K_1 (two choices for a given K).

Conversely, for every row in the table, and given extensions K, K_3, K_2, K_1 of k with the first containing the other three, K_3 containing K_2, with Galois groups as in that row and satisfying the restrictions of the last column, there is a unique G_k-group structure on the group D_{12} with the given fields as associated fields.

Realization of G_k-groups isomorphic to D_{12} as groups of matrices. Now we study the representations of these G_k-groups as groups of matrices in an analogous manner as we did before for the case D_8.

Proposition 3.5. *Let* $\operatorname{char} k \neq 2, 3$ *and let* A *be a sub-*G_k*-group of* $\mathrm{GL}_2(\overline{k})$ *isomorphic to* D_{12}*. For every element* $u \in k^*$ *such that* $K_1 = k(\sqrt{u})$ *and* $K_2 = k(\sqrt{v})$ *there exists an element* $z \in k$ *such that the group* A *is* $\mathrm{GL}_2(k)$*-conjugated of the group generated by the two matrices*

$$U = \frac{1}{\sqrt{u}} \begin{pmatrix} \alpha & \beta \\ \beta/v & -\alpha \end{pmatrix}, \qquad V = \frac{1}{2} \begin{pmatrix} 1 & \sqrt{v} \\ -3/\sqrt{v} & 1 \end{pmatrix}, \tag{3.6}$$

with $\alpha, \beta \in \overline{k}$ *such that*

$$\alpha^3 - \frac{3u}{4}\alpha - \frac{z}{4} = 0, \qquad \alpha^2 + \frac{\beta^2}{v} = u. \tag{3.7}$$

In that case, the congruence $u^3 - z^2 \equiv 3v \pmod{k^2}$ *is satisfied, say* $u^3 - z^2 = 3s^2 v$*, with* $s \in k$*.*

Conversely, given elements $u, v \in k^*$ *and* $z \in k$ *with* $u^3 - z^2 \equiv 3v \pmod{k^2}$*, the matrices* U, V *defined by* (3.6) *and* (3.7) *generate a group isomorphic to* D_{12} *invariant by Galois action.*

Proof. Let A be a G_k-subgroup of $\mathrm{GL}_2(\overline{k})$ isomorphic to D_{12}. Since the central element V^3 of order 2 must be represented by the matrix -1, the group can be written as

$$A = \langle\, U, V \mid U^2 = 1, V^3 = -1, VU = -UV^2 \,\rangle.$$

The matrix V is defined over the field K_2, and the Galois action either leaves it unchanged, if $K_2 = k$, or interchanges V with V^5, if $K_2 \neq k$. Since the characteristic polynomial of V is $X^2 - X + 1$ it follows that V must be $\mathrm{GL}_2(k)$-conjugated of the matrix

$$\frac{1}{2} \begin{pmatrix} 1 & \sqrt{v} \\ -3/\sqrt{v} & 1 \end{pmatrix}.$$

The matrices $U \in \mathrm{GL}_2(\overline{k})$ of order two satisfying $VU = -UV^2$ are the matrices of the form

$$U = \frac{1}{\sqrt{u}} \begin{pmatrix} \alpha & \beta \\ 3\beta/v & -\alpha \end{pmatrix}, \qquad \alpha, \beta \in \overline{k}, \qquad \alpha^2 + \frac{3\beta^2}{v} = u.$$

Since the set of matrices $\{\sqrt{u}\ U, \sqrt{u}\ UV^2, \sqrt{u}\ UV^4\}$ is closed by Galois action, it follows that the upper left entries of these three matrices are the roots of a

polynomial with coefficients in k. The identity $\alpha^2 + 3\beta^2/v = u$ implies that this polynomial must be of the form

$$X^3 - \frac{3u}{4}X - \frac{z}{4}$$

for some element $z \in k$, and α and β satisfy the conditions (3.7).

The congruence $u^3 - z^2 \equiv 3v \pmod{k^2}$ is a consequence of the fact that the roots of the polynomial $X^3 - \frac{3u}{4}X - \frac{z}{4}$ generate the field K_3, whose unique quadratic subfield is K_2, and the discriminant of the polynomial is $3^3 2^{-4}(u^3 - z^2)$.

Conversely, let u, v, z be elements satisfying the congruence, and let $\alpha, \beta \in \overline{k}$ be elements satisfying the conditions (3.7). Then it is immediate to check that the matrices U and V defined by (3.6) generate a group isomorphic to D_{12}. If $\sigma \in G_k$, then ${}^{\sigma}V \in \{V, V^2\}$. If the polynomial $X^3 - \frac{3u}{4}X - \frac{z}{4}$ has multiple roots, then α and β are in an at most quadratic extension of k and it is clear that $\langle U, V\rangle$ is closed by Galois action. If that polynomial is separable, then β can be written in terms of α as

$$\beta = \frac{u^2 + z\alpha - 2u\alpha^2}{3s},$$

for an element $s \in k$ such that $u^3 - z^2 = 3vs^2$. In terms of this element, the roots of the polynomial different from α are

$$\alpha', \alpha'' = \frac{u^2 + z\alpha - 2u\alpha^2 \pm s\alpha\sqrt{v}}{\pm\sqrt{v}},$$

and one has ${}^{\sigma}U \in \{U, UV^2, UV^4\}$, depending on ${}^{\sigma}\alpha \in \{\alpha, \alpha', \alpha''\}$. Hence, the group $\langle U, V\rangle$ is closed by the Galois action. □

Theorem 3.6. *A G_k-group isomorphic to D_{12} can be realized as a sub-G_k-group of $\mathrm{GL}_2(\overline{k})$ if, and only if, $(u, -3v)$ is trivial in $\mathrm{Br}_2(k)$, with u and v elements such that $K_1 = k(\sqrt{u})$ and $K_2 = k(\sqrt{v})$.*

Proof. If the group can be realized, then by proposition 3.5 there exists an element $z \in k$ satisfying the congruence $u^3 - z^2 \equiv 3v \pmod{k^2}$. Then, the quadratic form $uX^2 - 3vY^2$ represents a square over k and this implies the identity $(u, -3v) = 1$.

Let a G_k-group isomorphic to D_{12} be given and assume that the condition $(u, -3v) = 1$ is satisfied.

If $3 \nmid [K : k]$, then $K = k(\sqrt{u}, \sqrt{v})$. The identity on the Brauer group implies that the quadratic form $uX^2 - 3vY^2$ represents squares over k, and from a representation with nonzero X we obtain elements $\alpha, \beta \in k$ satisfying $\alpha^2 + 3\beta^2/v = u$. Then, the matrices defined by formulas (3.6) using these elements α, β generate a group of matrices isomorphic to the given G_k-group.

Now consider the case $3 \mid [K : k]$. Then, K_3/k is cyclic of degree 3 or dihedral of degree 6. We want to see that this extension is the field of decomposition of some polynomial of the form $X^3 - \frac{3u}{4}X - \frac{z}{4}$. Let $f(X) = X^3 - aX - b \in k[X]$ be any irreducible polynomial with K_3 as its field of decomposition, and let $\alpha \in \overline{k}$ be a root of this polynomial. Then $4a^3 - 27b^2 \equiv v \pmod{k^{*2}}$, since the field $K_2 = k(\sqrt{v})$ is contained in K_3. If $a = 0$, then the extension $k(\alpha)$ can always be written as the field of decomposition of a polynomial as claimed. Assume $a \neq 0$. Computing the irreducible polynomial of a generic element of $k(\alpha)$ of zero trace one obtains the polynomials $f_1(X) = X^3 - a_1X - b_1$ with $a_1 = ax^2 + 3avy^2$ and $x, y \in k$. The formula for the discriminant of $f(X)$ in terms of a and b shows that the quadratic

form $avX^2 - 3vY^2$ represents squares in k and hence $(av, -3v) = 1$. Since by hypothesis $(u, -3v) = 1$ also, it follows that $(avu, -3v) = (3au, -3v) = 1$, and from this identity one deduces the existence of elements $x, y \in k$ with $a_1 = ax^2 + 3avy^2 = 3u/4$. Taking $z = 4b_1$ for the corresponding coefficient b_1 the extension K_3/k is the field of decomposition of a polynomial of the type $X^3 - \frac{3u}{4}X - \frac{z}{4}$ as claimed. Now, the matrices defined by formulas (3.6) using a root α of this polynomial and a root β of $\alpha^2 + \beta^2/v = u$ generate a sub-G_k-group of $\mathrm{GL}_2(\overline{k})$ isomorphic to the group we started with. □

Two technical lemmas. We end this section with two technical lemmas. The first one studies a particular cohomology class with values in a G_k-group isomorphic to D_8 that will be used later. The second lemma shows that two isomorphic G_k-groups realized as groups of matrices that are isomorphic to D_8 or D_{12} are conjugated by some matrix with coefficients in the base field k.

Lemma 3.7. *Let A be a G_k-group isomorphic to D_8 as a group and let $K_2 = k(\sqrt{v})$ for some $v \in k^*$. The 1-cocycle Ξ defined by*

$$\Xi_\sigma = \begin{cases} 1, & {}^\sigma\sqrt{v} = \sqrt{v}, \\ V, & {}^\sigma\sqrt{v} = -\sqrt{v} \end{cases}$$

is cohomologous to a one-cocycle with values in $\{\pm 1\}$ if, and only if, $K_2 = k$ or $K_2 = K_1$.

Proof. We just multiply the cocycle Ξ by all the coboundaries, which are the maps of the form $\sigma \mapsto {}^\sigma W \cdot W^{-1}$ for elements $W \in A$, and check that one gets a cocycle with values in $\{\pm 1\}$ for some W exactly when one of the conditions $K_2 = k$ or $K_2 = K_1$ hold. □

Lemma 3.8. *Let A_1 and A_2 be two finite G_k-subgroups of $\mathrm{GL}_2(\overline{k})$ of order not divisible by $\mathrm{char}\, k$. Assume that they are isomorphic as G_k-groups and, as groups, admit a unique irreducible two-dimensional representation over $\overline{k}$. Then, A_1 and A_2 are $\mathrm{GL}_2(k)$-conjugate.*

In particular, this holds for G_k-subgroups of $\mathrm{GL}_2(\overline{k})$ isomorphic to D_8 or D_{12} in characteristics $\mathrm{char}\, k \neq 2$ and $\mathrm{char}\, k \neq 2, 3$, respectively.

Proof. Since the groups have a unique irreducible two-dimensional representation, every group isomorphism between A_1 and A_2 is obtained by conjugation by some matrix of $\mathrm{GL}_2(\overline{k})$. Let $\psi : A_1 \to A_2$ be an isomorphism as G_k-groups, and let $M \in \mathrm{GL}_2(\overline{k})$ be a matrix such that $\psi(W) = MWM^{-1}$ for all $W \in A_1$. Then, and since ψ respects the Galois action, we have

$$M {}^\sigma W M^{-1} = \psi({}^\sigma W) = {}^\sigma\psi(W) = {}^\sigma M {}^\sigma W {}^\sigma M^{-1}$$

for every $W \in A_1$ and $\sigma \in G_k$.

For every $\sigma \in G_k$, the conjugation by the matrix $M^{-1} \cdot {}^\sigma M$ acts as the identity on the group A_1, hence this matrix belongs to the centralizer of this group in $\mathrm{GL}_2(\overline{k})$, and by Schur's lemma it is a homothety, which we identify with an element of $\overline{k}^*$. The map $\sigma \mapsto M^{-1} \cdot {}^\sigma M \in k^*$ is a 1-cocycle of G_k with values in the multiplicative group $\overline{k}^*$ and, by the theorem 90 of Hilbert, its cohomology class is trivial. Let $a \in \overline{k}^*$ be an element such that $M^{-1} \cdot {}^\sigma M = a \cdot {}^\sigma a^{-1}$. Then, the matrix Ma is Galois invariant, hence it belongs to $\mathrm{GL}_2(k)$, and the isomorphism ψ is also obtained by conjugation by this matrix. □

4. Parametrization over arbitrary fields

The main object of this section is the classification of curves of genus 2 with group of automorphisms isomorphic to D_8 or D_{12} up to k-isomorphisms.

Twisting curves. For every curve C defined over a field k, the set of its twists, $\mathrm{Twist}(C/k)$, is the set of k-isomorphism classes of curves C'/k that are $\overline{k}$-isomorphic to C. The map sending an isomorphism $\phi : C' \to C$ to the class of the 1-cocycle ${}^{\sigma}\phi \circ \phi^{-1} : G_k \to \mathrm{Aut}(C)$ is a bijection between the set of k-twists of C and the cohomology set $H^1(G_k, \mathrm{Aut}(C))$. If C' is the twist of C obtained from a cohomology class $\xi \in H^1(G_k, \mathrm{Aut}(C))$, then $\mathrm{Aut}(C')$ is isomorphic, as a G_k-group, to ${}_{\xi}\mathrm{Aut}(C)$.

For curves C/k of genus 2 given by hyperelliptic equations, the equation of a twist corresponding to a cohomology class is easily computed from the identification of $\mathrm{Aut}(C)$ with a subgroup of $\mathrm{GL}_2(\overline{k})$. Indeed, given a 1-cocycle $\sigma \mapsto \xi_\sigma$ of G_k with values in $\mathrm{Aut}(C)$ we may view it as taking values in $\mathrm{GL}_2(\overline{k})$. Since the cohomology set $H^1(G_k, \mathrm{GL}_2(\overline{k}))$ is trivial, there is a matrix $M \in \mathrm{GL}_2(\overline{k})$ such that $\xi_\sigma = {}^{\sigma}M \cdot M^{-1}$. Then, the curve C' obtained from C and the matrix M using (1.2) is the twist of C corresponding to the cohomology class of the 1-cocycle ξ.

Hyperelliptic twists. Let A and A' be, respectively, the group of automorphisms and the reduced group of automorphisms of a genus 2 curve C. The sequence $1 \to \langle\iota\rangle \to A \to A' \to 1$ is an exact sequence of G_k-groups. Since the group on the left is contained in the center of the group in the middle, one obtains (cf. [7, Section 8.3]) the long exact sequence of cohomology sets

$$\ldots \longrightarrow {A'}^{G_k} \xrightarrow{\delta} H^1(G_k, \langle\iota\rangle) \longrightarrow H^1(G_k, A) \longrightarrow H^1(G_k, A') \xrightarrow{\Delta} H^2(G_k, \langle\iota\rangle),$$

from which one deduces the exact sequence

$$1 \longrightarrow H^1(G_k, \langle\iota\rangle)/\delta({A'}^{G_k}) \longrightarrow H^1(G_k, A) \longrightarrow H^1(G_k, A')[\Delta] \longrightarrow 1, \tag{4.1}$$

where $H^1(G_k, A')[\Delta]$ denotes the kernel of Δ. The group $H^1(G_k, \langle\iota\rangle)$ acts on the set $H^1(G_k, A)$, and the orbits of that action are in bijection with the cohomology set $H^1(G_k, A')[\Delta]$ (cf. [7, Section 8.4]).

The group $H^1(G_k, \langle\iota\rangle)/\delta({A'}^{G_k})$, which is in bijection with the orbit of the trivial element in $H^1(G_k, A)$, can be identified with a quotient of the group k^*/k^{*2} by a finite subgroup, and the 1-cocycles representing its elements are homomorphisms $\xi : G_k \to \langle\iota\rangle$. If $k(\sqrt{d})$ is the fixed field of the kernel of this homomorphism, then the curve obtained by twisting a curve with equation $Y^2 = F(X)$ by the element of $H^1(G_k, A)$ corresponding to ξ is the curve with equation $Y^2 = dF(X)$ or, up to k-isomorphism, with equation $dY^2 = F(X)$. We call these twists *hyperelliptic twists*, and we say that two twists of a curve differ by a hyperelliptic twist if they correspond to two elements of $H^1(G_k, A)$ with the same image in the set $H^1(G_k, A')$, which is equivalent to the fact that the two curves admit hyperelliptic models (1.1) with polynomials $F(X)$ that differ only by the multiplication by some nonzero element of k.

It is immediate to check that if two curves differ by a hyperelliptic twist, then their groups of automorphisms are isomorphic as G_k-groups.

The following proposition gives an explicit description of the hyperelliptic twists of a genus 2 curve with group of automorphisms isomorphic to D_8 or D_{12}, which depend only on the G_k-structure on $A = \mathrm{Aut}(C)$.

Proposition 4.1. *Let* $\mathrm{char}\, k \neq 2$ *and let* A *be a sub-*G_k*-group of* $\mathrm{GL}_2(\overline{k})$ *isomorphic to* D_8*. Then,*

$$H^1(G_k, \{\pm 1\})/\delta(A'^{G_k}) \simeq \begin{cases} k^*/(k^{*2} \cdot vk^{*2} \cdot mk^{*2} \cdot vmk^{*2}), & \text{if} \quad K_1 = k, \\ k^*/(k^{*2} \cdot vk^{*2}), & \text{if} \quad K_1 \neq k, \end{cases}$$

with $K_2 = k(\sqrt{v})$ *and, if* $K_1 = k$*, then* $K = k(\sqrt{v}, \sqrt{m})$*, for elements* $v, m \in k^*$*.*

Let $\mathrm{char}\, k \neq 2, 3$ *and let* A *be a sub-*G_k*-group of* $\mathrm{GL}_2(\overline{k})$ *isomorphic to* D_{12}*. Then,*

$$H^1(G_k, \{\pm 1\})/\delta(A'^{G_k}) \simeq \begin{cases} k^*/(k^{*2} \cdot uk^{*2}), & \text{if} \quad 3 \nmid [K : k], \\ k^*/k^{*2}, & \text{if} \quad 3 \mid [K : k], \end{cases}$$

with $K_1 = k(\sqrt{u})$ *for an element* $u \in k^*$*.*

Proof. For each possibility for A, one can explicitly find the set of elements in A' fixed by G_k and its image by δ. □

Classification of twists in the D_8 case. Let $\mathcal{C}_t^{(8)}$ be the set of k-isomorphism classes of curves of genus 2 with group of automorphisms isomorphic to D_8 and with $\overline{k}$-isomorphism class corresponding to some $t \in k$. Since k-isomorphisms fix the Galois action on the group of automorphisms, it makes sense to pack together those k-isomorphism classes with a fixed G_k-structure on $\mathrm{Aut}(C)$. We will denote by $\mathcal{C}_{t,A}^{(8)}$ each of these subsets. It has to be noted that a necessary condition for $\mathcal{C}_{t,A}^{(8)}$ to be nonempty is that A can be realized as a group of matrices; therefore, from now on we will only consider such G_k-structures.

The following proposition shows that each $\mathcal{C}_{t,A}^{(8)}$ contains at most two classes of curves up to a hyperelliptic twist.

Proposition 4.2. *Let* $C_i \in \mathcal{C}_{t,A}^{(8)}$*,* $i = 1, 2$*. Then, the curves* C_i *differ by a twist of the type* ξ *or* $\xi\Xi$*, with* ξ *a hyperelliptic twist and* Ξ *the twist of lemma* 3.7*.*

Proof. By lemma 3.8 we may assume, changing one of the curves by a k-isomorphic one if necessary, that the groups of automorphisms of the two curves, viewed as subgroups of $\mathrm{GL}_2(\overline{k})$, are the same group. By proposition 3.3, and again up to a k-isomorphism, we may assume that this common group $A = \mathrm{Aut}(C_i)$ is a group generated by two matrices U and V as in proposition 3.3. Let $M \in \mathrm{GL}_2(\overline{k})$ be the matrix associated to an isomorphism between these two curves. Conjugation by M gives an automorphism of the group A. We recall that the identity and the automorphism r defined in (3.1) represent the two cosets of $\mathrm{Aut}(A)$ modulo inner automorphisms. Up to multiplying M by an element of A, which gives another isomorphism between the curves, we may assume that the conjugation by M is either the identity or the automorphism r on A.

If conjugation by M is the identity on A, then M must be a scalar matrix. For every $\sigma \in G_k$ the matrix $\xi_\sigma = {}^\sigma M \cdot M^{-1} \in A$ is also scalar and hence it must be ± 1. In this case, the two curves are hyperelliptic twists of each other by ξ.

Assume now that conjugation by M gives the automorphism r. Let C_2' be the curve obtained by applying to C_2 the transformation given by the matrix

$$\Phi = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & \sqrt{v} \\ \frac{-1}{\sqrt{v}} & 1 \end{pmatrix} \in \mathrm{GL}_2(\overline{k}).$$

The curves C_2' and C_2 are twists corresponding to the element $\xi_2\Xi$, with $\xi_2 : G_k \to \{\pm 1\}$ the one-cocycle corresponding to the extension $k(\sqrt{2})$. One checks that conjugation by Φ induces the automorphism r of the group of matrices $\mathrm{Aut}(C_i) = \langle U, V\rangle$. Then, the curves C_1 and C_2' also have the same group of automorphisms, and there is an isomorphism between them that induces, by conjugation, the identity on $\langle U, V\rangle$. By the previous argument, the curves C_2 and C_2' differ by a hyperelliptic twist ξ and hence C_1 and C_2 are related by the twist $\xi\xi_2\Xi$. □

Our next goal is to give representatives for this set of classes modulo hyperelliptic twists. Given t and A such that $K_1 = k(\sqrt{t})$, we fix elements $u = t, v, z, s$ as in proposition 3.3 and define the two curves of genus 2

$$C^{(8)}_{t,A,\pm} : Y^2 = (1 \pm 2uz)X^6 \mp 8suvX^5 + v(3 \mp 10uz)X^4 + v^2(3 \mp 10uz)X^2 \pm 8suv^3X + v^3(1 \pm 2uz).$$

In the next proposition we prove that $C^{(8)}_{t,A,\pm}$ belongs to $\mathcal{C}^{(8)}_{t,A}$.

Proposition 4.3. *The curves $C^{(8)}_{t,A,\pm}$ have group of automorphisms isomorphic to D_8 generated by the matrices U, V of proposition 3.3, that is, $\mathrm{Aut}(C^{(8)}_{t,A,\pm})$ and A are isomorphic as G_k-groups, and the absolute invariant of the curves is $t(C^{(8)}_{t,A,\pm}) = t$.*

Proof. By a direct computation, one checks that the substitutions corresponding to the matrices U and V are automorphisms of the given equations, and computes the absolute invariant t in terms of invariants of sextic forms by the formulas given in proposition 2.1. □

In the following proposition we prove that the curves constructed as above give, up to a hyperelliptic twist and a k-isomorphism, all the possibilities for curves of genus 2 with group of automorphism isomorphic to D_8.

Proposition 4.4. *Every curve C/k of genus 2 with $\mathrm{Aut}(C) \simeq D_8$ is k-isomorphic to a hyperelliptic twist of a curve $C^{(8)}_{t,A,\pm}$.*

Proof. Given such a curve C/k, let t be its absolute invariant, and let $A = \mathrm{Aut}(C)$. Then, the field K_1 corresponding to the Galois action on A is $k(\sqrt{t})$. Indeed, the curve of genus 2 with equation $C_t : Y^2 = X^5 + X^3 + t\,X$ is $\overline{k}$-isomorphic to the curve C, and hence the G_k-group $A_t = \mathrm{Aut}(C_t)$ is twisted of A by some one-cocycle $\xi : G_k \to A$. Hence, the Galois action on the quotients A^{ab} and A_t^{ab} are the same. If K_1 denotes the field of definition of A^{ab}, then $K_1 = k(\sqrt{t})$, since $k(\sqrt{t})$ is the field of definition of A_t^{ab}.

Applying proposition 3.3 to the group A, viewed as a group of matrices, with the choice of parameters $u = t$ and $v \in k^*$ any element with $K_2 = k(\sqrt{v})$, we obtain an element $z \in k^*$ and an $s \in k$ such that $1 - z^2t = s^2tv$. The curves $C^{(8)}_{t,A,\pm}$ defined from these parameters are isomorphic to the curve C, since they have the same absolute invariant, and have group of automorphisms isomorphic to A as G_k-groups, since both groups are conjugated by means of a matrix of $\mathrm{GL}_2(k)$. By propositions 4.2 and 4.3, at least one of the two curves $C^{(8)}_{t,A,+}$ and $C^{(8)}_{t,A,-}$ differ from C by a hyperelliptic twist. □

In order to complete our description of the k-twists we need to know when the two curves $C^{(8)}_{t,A,\pm}$ differ by a hyperelliptic twist.

Lemma 4.5. *The two curves with equations $C^{(8)}_{t,A,+}$ and $C^{(8)}_{t,A,-}$ are twists of each other by the element $\Xi \in H^1(G_k, A)$ of lemma 3.7, up to a hyperelliptic twist.*

Proof. One checks that the matrix Φ in the proof of proposition 4.2 gives an isomorphism between these two curves. The map $\sigma \mapsto {}^{\sigma}\Phi \cdot \Phi^{-1}$ is the product of the one-cocycle Ξ of lemma 3.7 by the one-cocycle with values in $\{\pm 1\}$ corresponding to the field $k(\sqrt{2})$. □

Proposition 4.6. *The two curves with equations $C^{(8)}_{t,A,+}$ and $C^{(8)}_{t,A,-}$ are a hyperelliptic twist of each other if $K_2 = k$ or $K_2 = K_1$, and a nonhyperelliptic twist of each other if $k \neq K_2 \neq K_1$. The last possibility corresponds to Galois actions on $\mathrm{Aut}(C)$ of types C_2^B, V_4^A and D_8.*

Proof. The result follows from the previous lemma together with lemma 3.7. □

Summarizing what has been done in this section, we have the following theorem.

Theorem 4.7. *The set $\mathcal{C}^{(8)}_t$ is parameterized by the set of 3-tuples (A, e, d), where:*

- *A is a G_k-structure on D_8 that can be realized as a group of matrices and with associated field $K_1 = k(\sqrt{t})$;*
- *$e \in \{-1, +1\}$ if A is of type C_2^B, V_4^A or D_8; otherwise, $e = 1$;*
- *$d \in k^*/H$, with H depending on A as in proposition 4.1.*

Proof. Each set $\mathcal{C}^{(8)}_{t,A}$ contains, up to hyperelliptic twists, either one or two classes of curves depending on the condition in proposition 4.6. For each of these, one only needs to take into account the hyperelliptic twists, which are described in proposition 4.1. □

Classification of twists in the D_{12} case. We define $\mathcal{C}^{(12)}_t$ and $\mathcal{C}^{(12)}_{t,A}$ analogously to what we did for the previous case. In this case, the situation is slightly easier, since now all curves in $\mathcal{C}^{(12)}_{t,A}$ differ by a hyperelliptic twist, as the following proposition proves.

Proposition 4.8. *Let $C_i \in \mathcal{C}^{(12)}_{t,A}$, $i = 1, 2$. Then the curves C_i differ by a hyperelliptic twist.*

Proof. By lemma 3.8, we may assume, changing one of the curves by a k-isomorphic one if necessary, that the groups of automorphisms of the two curves, viewed as subgroups of $\mathrm{GL}_2(\overline{k})$, are the same group. Again up to k-isomorphism, we may assume that this common group $A = \mathrm{Aut}(C_i)$ is the group generated by two matrices U and V as in proposition 3.5. Let $M \in \mathrm{GL}_2(\overline{k})$ be the matrix associated to an isomorphism between these two curves. Conjugation by M gives an automorphism of the group A. We recall that the identity and the automorphism r^3 defined in (3.5) represent the two cosets of $\mathrm{Aut}(A)$ modulo inner automorphisms. Up to multiplying M by an element of A, which gives another isomorphism between the curves, we may assume that the conjugation by M is the identity or the automorphism r^3.

If conjugation by M is the automorphism r^3 of A, consider Φ the matrix

$$\Phi = \begin{pmatrix} 0 & -v/3 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(k),$$

which also acts by conjugation on A as the automorphism r^3. After changing one of the curves by a k-isomorphic one with the isomorphism given by Φ, we may assume that conjugation by M is the identity on A.

Now, in any case, M must be a scalar matrix. For every $\sigma \in G_k$ the element $\xi_\sigma = {}^\sigma M \cdot M^{-1} \in A$ is also scalar and hence it must be ± 1. Then, the two curves are hyperelliptic twists of each other by ξ. □

As in the previous case, we need to give representatives for this set of classes modulo a hyperelliptic twist. Given t and A such that $K_1 = k(\sqrt{t})$, we fix elements $u = t, v, z, s$ as in proposition 3.5 and define the curve of genus 2:

$$C_{t,A}^{(12)} : Y^2 = 27(u+2z)X^6 - 324svX^5 + 27v(u-10z)X^4 + 360sv^2X^3 + 9v^2(u+10z)X^2 - 36sv^3X + v^3(u-2z).$$

The same arguments as in proposition 4.3 prove that $C_{t,A}^{(12)}$ belongs to $\mathcal{C}_{t,A}^{(12)}$.

In the following proposition we prove that the curves constructed as above give, up to a hyperelliptic twist and a k-isomorphism, all the possibilities for curves of genus 2 with group of automorphism isomorphic to D_{12}.

Proposition 4.9. *Every curve C/k of genus 2 with $\mathrm{Aut}(C) \simeq D_{12}$ is isomorphic to a hyperelliptic twist of a curve $C_{t,A}$.*

Proof. The proof is analogous to the one for the D_8 case. Perhaps the only thing that should be remarked is that, also in this case, the field K_1 corresponding to a G_k-group A isomorphic to D_{12} is the field of definition of the action on the quotient group A^{ab}, which is invariant by twisting the action, and hence is an invariant of the $\overline{k}$-isomorphism class of the curve. □

As we did before in the D_8 case, we summarize the results for the D_{12} case in the following theorem.

Theorem 4.10. *The set $\mathcal{C}_t^{(12)}$ is parameterized by the set of 2-tuples (A, d), where:*

- *A is a G_k-structure on D_{12} that can be realized as a group of matrices and with associated field $K_1 = k(\sqrt{t})$;*
- *$d \in k^*/H$, with H depending on A as in proposition 4.1.*

References

[1] O. Bolza, *On binary sextics with linear transformations between themselves*, Amer. J. Math. 10, 1888, 47–70. MR1505464

[2] J.W.S. Cassels, E.V. Flynn, Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2, LMS Lecture Note Series 230, Cambridge Univ. Press, 1996. MR1406090 (97i:11071)

[3] G. Cardona, J. González, J.-C. Lario, A. Rio, *On curves of genus 2 with jacobian of GL_2-type*, Manuscripta Math. 98, 1999, 37–54. MR1669607 (99j:11068)

[4] J.-I. Igusa, *Arithmetic variety of moduli for genus 2*, Ann. of Math. 72 (3), 1960, 612–649. MR0114819 (22:5637)

[5] J.-F. Mestre, *Construction de courbes de genre 2 à partir de leurs modules*, Effective methods in Algebraic Geometry (Castiglioncello, 1990), Birkhäuser, 1991, 313–334. MR1106431 (92g:14022)

[6] B. Poonen, *Computational aspects of curves of genus at least 2*, Algorithmic Number Theory (H. Cohen, Ed.), Lecture Notes in Computer Science 1122, Springer-Verlag, 283–306. MR1446520 (98c:11059)

[7] J.-P. Serre, Galois Cohomology, Springer-Verlag GTM number 155 (1992). MR1466966 (98g:12007)

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

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

Departament Matemàtica Aplicada II, Universitat Politècnica de Catalunya, Ed. Omega, Campus Nord, Jordi Girona, 1-3, E-08034 – Barcelona, Spain

E-mail address: jordi.quer@upc.edu