On the Inertia Group of Elliptic Curves
in the Cremona Group of the Plane

Jérémy Blanc

1. Introduction

We work on some algebraically closed field $\mathbb{K}$. Let $\mathbb{P}^2 = \mathbb{P}^2(\mathbb{K})$ be the projective plane over $\mathbb{K}$, let $\mathrm{Bir}(\mathbb{P}^2)$ be its group of birational transformations, and let $C \subset \mathbb{P}^2$ be an irreducible curve. The *decomposition group* of C in $\mathrm{Bir}(\mathbb{P}^2)$, introduced in [G], is the group

$$\mathrm{Dec}(C) = \mathrm{Bir}(\mathbb{P}^2)_C = \{g \in \mathrm{Bir}(\mathbb{P}^2) \mid g(C) \subset C, \; g|_C : C \dashrightarrow C \text{ is birational}\}.$$

The *inertia group* of C in $\mathrm{Bir}(\mathbb{P}^2)$, also introduced in [G], is the group

$$\mathrm{Ine}(C) = \mathrm{Bir}(\mathbb{P}^2)_{0C} = \{g \in \mathrm{Bir}(\mathbb{P}^2)_C \mid g(p) = p \text{ for a general point } p \in C\}.$$

(In our context, since the variety $\mathbb{P}^2$ and the inherent group $\mathrm{Bir}(\mathbb{P}^2)$ will not change, we will prefer the notation $\mathrm{Dec}(C)$ and $\mathrm{Ine}(C)$ to that of Gizatullin.)

If φ is a birational transformation of $\mathbb{P}^2$ that does not collapse C (this latter condition is always true if C is nonrational), then φ conjugates the group $\mathrm{Dec}(C)$ (resp. $\mathrm{Ine}(C)$) to the group $\mathrm{Dec}(\varphi(C))$ (resp. $\mathrm{Ine}(\varphi(C))$). The conjugacy classes of the two groups are thus birational invariants.

On one hand, these groups are useful for describing the birational equivalence of curves of the plane. On the other hand, given two groups, the curves fixed by the elements are useful for deciding whether the groups are birationally conjugate and, moreover, are often the unique invariant needed (see [BaB; BBl; Bl; F]).

In the case where $\mathbb{K} = \mathbb{C}$, the inertia groups of curves of geometric genus ≥ 2 have been classically studied (see [C]); a modern precise classification may be found in [BlPV]. For the case of the decomposition groups, we refer to [P1; P2] and the references therein.

In this article we will study the case of the inertia group of curves of geometric genus 1 and, in particular, the case of plane smooth cubic curves, which constitute the only case in which nontrivial elements are known. We state now the three main results that we prove.

First is a Noether–Castelnuovo-like theorem for the generators of the inertia group. (The same result holds for the decomposition group; see [P2, Thm. 1.4].)

THEOREM 1. *The inertia group of a smooth plane cubic curve is generated by its elements of degree* 3, *which are—except the identity—its elements of lower degree.*

Next we describe the elements of finite order of the inertia group of any curve
of genus 1 (we announced a part of this result, without proof, in [Bl, Thms. 3.1
and 4.3]).

THEOREM 2.   *Assume that* $\mathrm{char}(\mathbb{K}) \neq 2, 3, 5$. *Let* $C \subset \mathbb{P}^2$ *be a curve of geomet-
ric genus* 1, *and let* $g \in \mathrm{Ine}(C)$ *be an element of finite order* $n > 1$. *Then there
exists a birational map* $\varphi \colon \mathbb{P}^2 \dashrightarrow S$ *that conjugates* g *to an automorphism* α *of a
Del Pezzo surface* S, *where* (α, S) *are given in the following table.*

n	Description of α	Equation of the surface S	In the variety
2	$x_0 \mapsto -x_0$	$\sum_{i=0}^{4} x_i^2 = \sum_{i=0}^{4} \lambda_i x_i^2 = 0$	$\mathbb{P}^4$
3	$x_0 \mapsto \zeta_3 x_0$	$x_0^3 + L_3(x_1, x_2, x_3)$	$\mathbb{P}^3$
4	$x_0 \mapsto \zeta_4 x_0$	$x_3^2 = x_0^4 + L_4(x_1, x_2)$	$\mathbb{P}(1,1,1,2)$
5	$x_0 \mapsto \zeta_5 x_0$	$x_3^2 = x_2^3 + \lambda_1 x_1^4 x_2 + x_1(\lambda_2 x_1^5 + x_0^5)$	$\mathbb{P}(1,1,2,3)$
6	$x_0 \mapsto \zeta_6 x_0$	$x_3^2 = x_2^3 + \lambda_1 x_1^4 x_2 + \lambda_2 x_1^6 + x_0^6$	$\mathbb{P}(1,1,2,3)$

Here $\zeta_n \in \mathbb{K}$ *is a primitive* nth *root of unity,* L_i *is a form of degree* i, *and* λ_i *are
parameters such that* S *is smooth.*

   Furthermore, any birational morphism $S \to \mathbb{P}^2$ *sends the fixed curve on a
smooth plane cubic curve.*

COROLLARY 3.   *Assume that* $\mathrm{char}(\mathbb{K}) \neq 2, 3, 5$, *let* $C \subset \mathbb{P}^2$ *be an irreducible
curve of geometric genus* 1, *and let* $g \in \mathrm{Ine}(C)$ *be a nontrivial element of finite
order. Then* (a) *there exists a birational transformation of* $\mathbb{P}^2$ *that sends* C *on a
smooth cubic curve and* (b) *the order of* g *is* 2, 3, 4, 5, *or* 6. *Furthermore, each
case occurs for any elliptic curve* C.

COROLLARY 4.   *Let* $m \geq 2$ *be an integer, and let* $C \subset \mathbb{P}^2$ *be an irreducible curve
of degree* $3m$ *that has nine points of multiplicity* m *and that is smooth at its other
points. Then the group* $\mathrm{Ine}(C)$ *contains no nontrivial element of finite order.*

To state the third theorem, we need the following classical construction (which
has been generalized in [G] in any dimension).

DEFINITION 5.   Assume that $\mathrm{char}(\mathbb{K}) \neq 2$. Let $C \subset \mathbb{P}^2$ be a smooth cubic curve.
For any point $p \in C$, we denote by σ_p the *cubic involution* centered at p defined as
follows: If D is a general line of $\mathbb{P}^2$ passing through p then we have $\sigma_p(D) = D$
and the restriction of σ_p to D is the involution that fixes $(D \cap C) \backslash \{p\}$.

The last result is the structure of the group generated by cubic involutions of the
inertia group.

THEOREM 6.   *Assume that* $\mathrm{char}(\mathbb{K}) \neq 2$ *and let* $C \subset \mathbb{P}^2$ *be a smooth cubic curve.
The subgroup of* $\mathrm{Ine}(C)$ *generated by all the cubic involutions centered at the
points of* C *is the free product*

$$\bigstar_{p \in C} \langle \sigma_p \rangle.$$

COROLLARY 7.   *Assume that* char$(\mathbb{K}) \neq 2$. *For any integer* $n > 0$ *and for any elliptic curve* Γ, *the free product* $\bigstar_{i=1}^{n} \mathbb{Z}/2\mathbb{Z}$ *acts biregularly on a smooth rational surface, where it fixes a curve isomorphic to* Γ.

2. Reminders

We say that a point q is *in the first neighborhood* of $p \in \mathbb{P}^2$ if it belongs to the exceptional curve obtained by blowing up p; then we say that q is *in the ith neighborhood* of p if it belongs to the exceptional curve obtained by blowing up a point in the $(i - 1)$th neighborhood of p. A point is said to be *infinitely near to p* (and to $\mathbb{P}^2$) if it is in some neighborhood of $p \in \mathbb{P}^2$, and the set of all such points is called the *infinitesimal neighborhood* of p. The same notions apply when p is itself a point infinitely near to $\mathbb{P}^2$. If a is infinitely near to b then we say that a is *higher* than b and that b is *smaller* than a; this notion induces a partial order on the set of points infinitely near to $\mathbb{P}^2$.

We say that a point q *belongs as an infinitely near point* (or, more simply, *belongs*) to a curve $C \subset \mathbb{P}^2$ if it lies in the strict transform of the curve obtained after a sequence of blow-ups. In this case, we say that C *passes through* q.

Let $\varphi \in \mathrm{Bir}(\mathbb{P}^2)$ be defined by $(x : y : z) \dashrightarrow (P_1(x, y, z) : P_2(x, y, z) : P_3(x, y, z))$ for some homogeneous polynomials P_1, P_2, P_3 of the same degree but with no common divisor. The *degree* of φ is the degree d of the P_i. If $d = 2$ (resp. $d = 3$), we say that φ is *quadratic* (resp. *cubic*). The linear system of curves of degree d of the form $\sum_{i=1}^{3} a_i P_i(x, y, z) = 0$ for $(a_1 : a_2 : a_3) \in \mathbb{P}^2$ is the *homoloidal linear system* (or simply the *linear system*) *associated to* φ; we will denote it by Λ_φ. The *base points* of φ are the base points of its linear system (i.e., the points p_i through which all the curves of Λ_φ pass). These points may lie on $\mathbb{P}^2$ or be infinitely near to $\mathbb{P}^2$, and if such a point is not a proper point of $\mathbb{P}^2$ then it is in the first neighborhood of another base point. To any base point p_i is associated its multiplicity k_i, which is the multiplicity of the general curves of Λ_φ at p_i. If p_i is higher than p_j, then $k_i \leq k_j$. Note that the base points lying on $\mathbb{P}^2$ are exactly the points of $\mathbb{P}^2$ that have no image by φ. We say that a birational transformation is *simple* if all its base points are proper points of $\mathbb{P}^2$.

Computing the free intersection of Λ_φ and the genus of its curves, we obtain the following classical relations (see e.g. [A]):

$$\sum k_i = 3d - 3, \qquad \sum k_i^2 = d^2 - 1. \qquad (*)$$

These numerical conditions imply the following lemma on birational transformations of small degree.

LEMMA 8.   *Let* $\varphi \in \mathrm{Bir}(\mathbb{P}^2)$ *be of degree d and have r base points $p_1, \ldots, p_r$ with multiplicities $k_1, \ldots, k_r$. Then $r \leq 5$ if and only if $d \leq 3$.*

If $d = 1$, then $r = 0$ (and $\varphi \in \mathrm{PGL}(3, \mathbb{K})$). If $d = 2$, then $\{k_i\}_{i=1}^{r} = \{1, 1, 1\}$. If $d = 3$, then $\{k_i\}_{i=1}^{r} = \{2, 1, 1, 1, 1\}$.

Proof. Assume that $r \leq 5$. Computing Cauchy–Schwartz inequality with $(1, \ldots, 1)$ and $(k_1, \ldots, k_r)$ shows that $\left(\sum k_i\right)^2 \leq r \cdot \sum k_i^2$. Replacing in equations $(*)$ shows that $(3(d-1))^2 \leq r \cdot (d^2 - 1)$, whence $9(d-1) \leq r(d+1) \leq 5(d+1)$ and so $d \leq 3$.

Assume that $d \leq 3$. Replacing in equations $(*)$ yields the three possibilities given in the lemma and, in particular, that $r \leq 5$. $\square$

COROLLARY 9.   *Let $\varphi \in \mathrm{Bir}(\mathbb{P}^2)$ be of degree $d \leq 3$. Then φ is simple if and only if φ^{-1} is simple.*

Proof. This may be observed by the description of the decomposition of φ into the blow-up of $r \leq 5$ points and the blow-down of r curves. $\square$

We now recall two results of [P2] on the decomposition group of a smooth plane cubic curve. Note that these results were stated for $\mathbb{K} = \mathbb{C}$, although the proofs do not use this restriction.

PROPOSITION 10 [P2, Thms. 1.3 and 1.4].   *Let $C \subset \mathbb{P}^2$ be a smooth cubic curve, and let $g \in \mathrm{Dec}(C)$. Then*:
- *the base points of g belong to C as proper or infinitely near points*; *and*
- *the transformation g is generated by simple quadratic elements of $\mathrm{Dec}(C)$.*

3. Examples

In this section, we give some fundamental examples of elements of $\mathrm{Ine}(C)$ for some smooth cubic curve $C \subset \mathbb{P}^2$.

EXAMPLE 11.   Let $p \in \mathbb{P}^2$ be some point, let $C \subset \mathbb{P}^2$ be a smooth cubic curve passing through p, and let $C_d \subset \mathbb{P}^2$ be an irreducible curve of degree d passing through p with multiplicity $d-1$.

We define a birational transformation $\varphi \in \mathrm{Ine}(C)$ of $\mathbb{P}^2$ as follows: it is the unique birational map that leaves invariant a general line L passing through p, that fixes the two points of $(C - \{p\}) \cap L$, and that sends the point of $(C_d - \{p\}) \cap L$ on p.

A particular case of this example is the cubic involution σ_p of Definition 5. We next describe some properties of this transformation.

PROPOSITION 12.   *Assume that $\mathrm{char}(\mathbb{K}) \neq 2$, let $C \subset \mathbb{P}^2$ be a smooth cubic curve, let $p \in C$, and let $\sigma_p \in \mathrm{Ine}(C)$ be the element defined in Definition 5. Then the following statements hold.*
1. *The degree of σ_p is 3, and $\sigma_p^2 = 1$ (i.e., σ_p is a cubic involution).*
2. *The base points of σ_p are the point p (which has multiplicity 2) and the four points p_1, p_2, p_3, p_4 such that the line passing through p and p_i is tangent at p_i to C.*
3. *If p is not an inflexion point of C, then all the points $p_1, \ldots, p_4$ belong to $\mathbb{P}^2$. Otherwise, only three of them belong to $\mathbb{P}^2$ and the fourth is the point in the blow-up of p that corresponds to the tangent of C at p.*

Proof. Let $\eta \colon \mathbb{F}_1 \to \mathbb{P}^2$ be the blow-up of p, and let $\pi \colon \mathbb{F}_1 \to \mathbb{P}^1$ be the ruling on the surface. The restriction of π to the strict transform $\tilde{C}$ of C by η gives a double covering that (by the Hurwitz formula) is ramified over four points. On a general fibre, the involution $\eta^{-1}\sigma_p\eta$ is a biregular automorphism; the base points of σ_p are thus on the four special lines corresponding to the ramification points.

Let d be the degree of σ_p. Because σ_p leaves invariant the pencil of lines of $\mathbb{P}^2$ passing through p, the intersection of Λ_{σ_p} with this pencil is concentrated at p; that is, the point p is a base point of multiplicity $d - 1$. It follows from $(*)$ that there are $2d - 2$ other base points $p_1, \ldots, p_{2d-2}$, each of multiplicity 1. Furthermore, no two of them lie on the same line passing through p (for otherwise the intersection of Λ_{σ_p} with the line would be more than d). Hence $2d - 2 \leq 4$; that is, $d \leq 3$.

Lemma 13 implies that $d = 3$. There are thus exactly four base points $p_1, \ldots, p_4$, corresponding to the intersection of $\tilde{C}$ with the special fibre of the ramification points. Assertions 2 and 3 follow directly from this observation. $\qquad\square$

LEMMA 13. *If $\varphi \colon \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ is a nonidentical birational map of degree d that fixes a (possibly reducible) curve C_n of degree n (i.e., if $\varphi \in \mathrm{Ine}(C_n)$), then $d \geq n$.*

Proof. Let us write

$$\varphi \colon (x_1 : x_2 : x_3) \dashrightarrow (P_1(x_1, x_2, x_3) : P_2(x_1, x_2, x_3) : P_3(x_1, x_2, x_3))$$

for some homogeneous polynomials P_1, P_2, P_3 of degree d (we forgo the standard (x, y, z)-coordinates here in order to simplify notation). Let Λ be the linear system generated by the three curves of equation $x_i P_j(x_1, x_2, x_3) = x_j P_i(x_1, x_2, x_3)$, $i \neq j$.

Take any point $p \in \mathbb{P}^2$, and take the two lines passing through p and graphing the respective equations $\sum_{i=1}^{3} a_i x_i = 0$ and $\sum_{i=1}^{3} b_i x_i = 0$. The relation

$$\left(\sum_{i=1}^{3} a_i x_i \right)\left(\sum_{i=1}^{3} b_i P_i \right) - \left(\sum_{i=1}^{3} b_i x_i \right)\left(\sum_{i=1}^{3} a_i P_i \right) = \sum_{i,j=1, i\neq j}^{3} a_i b_j (x_i P_j - x_j P_i)$$

shows that one curve of the system Λ pass through p.

Because the curve C_n is a fixed component of the system Λ, it must have degree strictly lower than the degree of the curves of Λ, which is $d + 1$. $\qquad\square$

4. The Cubic Elements Generate the Inertia Group

In this section, we prove Theorem 1 via the following lemma.

LEMMA 14. *Let $C \subset \mathbb{P}^2$ be a smooth cubic curve. Let p_1, p_2, p_3, p_4 be four distinct points such that:*

- *each of the four points belongs—as a proper or infinitely near point—to C;*
- *no three of the four points belong—as proper or infinitely near points—to a common line; and*
- *the points p_1, p_2 are proper points of the plane, and p_3 (resp. p_4) is either a proper point of the plane or a point in the first neighborhood of p_1 (resp. p_2).*

Let p' be the smallest point in the infinitesimal neighborhood of p_1 that belongs to C and not to $\{p_1, \ldots, p_4\}$. Then the following statements hold.

(i) *There exists a unique (possibly reducible) conic $C_2 \subset \mathbb{P}^2$ passing through $p_1, \ldots, p_4, p'$.*
(ii) *There exists a birational transformation φ of degree 3 that belongs to the inertia group of C and whose linear system is a system of codimension 1 of the system of cubics passing through $p_1, \ldots, p_4$, being singular at p_1.*
(iii) *The six points that belong—as proper or infinitely near points—to C and C_2 are base points of φ except for the higher such point in the neighborhood of p_1.*

REMARK 15.   The linear system of a cubic birational map is always singular at one point and always passes through four other points (Lemma 8).

Proof of Lemma 14. Up to a change of coordinates, we may assume that $p_1 = (1 : 0 : 0)$ and that the tangent of C at p_1 is the line $y = 0$.

We first prove that there exists a unique (and possibly reducible) conic C_2 passing through $p_1, \ldots, p_4, p'$. Suppose that three of the five points belong to a common line. By our hypotheses on the points $p_1, \ldots, p_4$, the three points are $\{p_1, p', p_i\}$ for some $i \in \{2, 3, 4\}$ and so the line is that of equation $y = 0$. Since no one of the two remaining points belongs to the line $y = 0$, the conic C_2 is the union of the line $y = 0$ with the line passing through the two remaining points and is unique. If no three of the five points belong to a common line, then there exists a unique irreducible conic C_2 passing through the points.

Observe that C_2 is tangent to C at p_1 and that C_2 is either a smooth conic or the union of two distinct lines, one of which does not pass through p_1; this implies that the equations of C and C_2 are (respectively)

$$F(x, y, z) = x^2 y + x F_2(y, z) + F_3(y, z),$$
$$G(x, y, z) = xy + G_2(y, z),$$

where the F_i, G_i are forms of degree i. We claim that the rational map $\varphi \colon \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ defined by

$$\varphi \colon (x : y : z) \dashrightarrow (x \cdot G(x, y, z) - F(x, y, z) : y \cdot G(x, y, z) : z \cdot G(x, y, z))$$

is the cubic birational transformation of Lemma 14(ii).

1. Let us first show that φ is birational. In the affine plane $z = 1$, φ becomes

$$(x, y) \dashrightarrow \left(\frac{xG(x, y, 1) - F(x, y, 1)}{G(x, y, 1)}, y \right)$$
$$= \left(\frac{x(G_2(y, 1) - F_2(y, 1)) - F_3(y, 1)}{xy + G_2(y, 1)}, y \right).$$

It is thus birational if and only if the matrix $\left(\begin{smallmatrix} G_2(y,1) - F_2(y,1) & -F_3(y,1) \\ y & G_2(y,1) \end{smallmatrix} \right)$ is invertible (i.e., belongs to $\mathrm{GL}(2, \mathbb{K}(y))$). Note that

$$G \cdot (G_2 - F_2) - y \cdot (xG - F)$$
$$= (yz + G_2) \cdot (G_2 - F_2) - y \cdot (x(G_2 - F_2) - F_3)$$
$$= (G_2 - F_2) \cdot G_2 + yF_3$$

is the homogenization of the determinant of the matrix. Since F is irreducible, it follows that the polynomials $xG - F$ and G have no common divisor and so $G \cdot (G_2 - F_2) \neq y \cdot (xG - F)$, whence φ is birational.

2. We find directly that φ belongs to the inertia group of C by replacing $F = 0$ in its equations. (A point $(x : y : z)$ such that $G(x, y, z) \neq 0$ and $F(x, y, z) = 0$ is sent by φ on $(xG : yG : zG) = (x : y : z)$.)

3. The degree of the linear system Λ_φ of φ is 3 because $xG - F$, yG, and zG have no common divisor (since this is the case for $xG - F$ and G).

4. We describe the base points of Λ_φ using the explicit form of φ. Observe that the point p_1 is a base point of multiplicity 2 and that the base points lying on $\mathbb{P}^2$ are exactly the points of $C \cap C_2$. Recall that all the base points belong—as proper or infinitely near points—to C (Proposition 10). Above a point $q \in C \cap C_2 \subset \mathbb{P}^2$ ($q \neq p_1$), the linear system Λ_φ passes through a point l if and only l belongs to both C and C_2. The curves C and C_2 intersect at six distinct points (belonging to $\mathbb{P}^2$ or infinitely near) and the system Λ_φ has five base points; therefore, the point of intersection of the strict transforms of C and C_2 that is the higher above p_1 is not a base point of Λ_φ. However, all other points of the intersection are base points. This shows in particular that p_2, p_3, and p_4 are base points, as stated in the lemma. $\square$

We are now able to prove Theorem 1—in other words, that the inertia group of a smooth plane cubic curve is generated by its elements of degree 3.

Proof of Theorem 1. Take some birational transformation η that fixes the smooth plane cubic curve C (i.e., $\eta \in \text{Ine}(C)$). The Noether–Castelnuvo theorem shows that $\eta = \sigma_r \circ \cdots \circ \sigma_2 \circ \sigma_1$ for some simple quadratic transformations σ_i, $i = 1, \ldots, r$. Furthermore, since $\eta \in \text{Dec}(C)$, these transformations may be chosen to leave C invariant (Proposition 10); in particular, the base points of σ_i and σ_i^{-1} are proper points of C for $i = 1, \ldots, r$. We use induction on r to show that η is generated by cubic birational transformations of the inertia group of C. If $r \leq 1$, then $n \leq 2$ and Lemma 13 shows that φ is the identity. Hence we assume that $r \geq 2$ and that the theorem is true for $r - 1$.

We will study precisely σ_1, σ_2 and the composition $\psi = \sigma_2 \circ \sigma_1$. Denote by $A = \{a_1, a_2, a_3\} \subset \mathbb{P}^2$ the base points of σ_1 and by $B = \{b_1, b_2, b_3\} \subset \mathbb{P}^2$ those of σ_1^{-1}; thus, the pencil of lines passing through A_i is sent by σ_1 on the pencil of lines passing through B_i. In a similar way, we denote by $P = \{p_1, p_2, p_3\}$ and $Q = \{q_1, q_2, q_3\}$ the base points of σ_2 and σ_2^{-1}. The degree of the birational transformation ψ is 1, 2, 3, or 4 if the number of points of $B \cap P$ is (respectively) 3, 2, 1, or 0. We enumerate the possibilities as follows.

If ψ has degree 1, then η may be decomposed by fewer than r simple quadratic transformations; we apply the induction hypothesis to conclude.

If ψ has degree 2 then the set $B \cap P$ contains exactly two points; we may assume that $b_1 = p_1$, $b_2 = p_2$, and $b_3 \neq p_3$. The base points of ψ are then a_1, a_2, and another point u, corresponding to p_3; it is a proper point of $\mathbb{P}^2$ if and only if p_3 does not belong to one of the lines collapsed by σ_1^{-1}. If $u \in \mathbb{P}^2$, then η may be decomposed by fewer than r simple quadratic transformations and we are done. Otherwise, we may assume that u is infinitely near to a_1 and then write $u = a_1'$. Furthermore, u does not belong—as an infinitely near point—to one of the lines collapsed by σ_1, since p_3 is a proper point of the plane. In particular, the points a_1, a_2, and u do not belong to a common line. Denote by a_1'' the point in the first neighborhood of a_1' that belongs to C. A general conic passing through a_1, a_2, a_1', a_1'' (that is reducible if and only if a_1 is an inflexion point of C) intersects C at two other points a_4, a_5 that are proper points of $\mathbb{P}^2$. We choose a conic such that neither a_4 nor a_5 belongs to a curve collapsed by σ_1 and such that neither $\sigma_1(a_4)$ nor $\sigma_1(a_5)$ belongs to a curve collapsed by σ_2. Let $\varphi \in \text{Ine}(C)$ be an element of degree 3 whose linear system Λ_φ consists of cubics that are singular at a_1 and that pass through a_2, a_1', a_4, and a_5 (the existence of φ is given by Lemma 14). The image of Λ_φ by σ_1 consists of cubics that are singular at $b_1 = p_1$ and pass through $b_2 = p_2$, p_3, $\sigma_1(a_4)$, and $\sigma_1(a_5)$. Consequently, the image of Λ_φ by ψ consists of conics passing through q_1, $\psi(a_4)$, and $\psi(a_5)$; the birational map $\psi \circ \varphi^{-1}$ is thus a simple quadratic transformation. After applying the induction hypothesis to $\eta \circ \varphi^{-1} = (\sigma_r \circ \cdots \circ \sigma_3) \circ (\psi \circ \varphi^{-1})$, which is decomposed by fewer than r simple quadratic transformations, we are done.

If the degree of ψ is 3 then $P \cap B$ contains exactly one point, which we choose to be $p_1 = b_1$. Then the linear system Λ_ψ consists of cubics that are singular at a_1 and that pass through a_2, a_3, a_4, a_5, where a_4 and a_5 correspond (respectively) to p_2 and p_3 and are proper points of $\mathbb{P}^2$ if and only if the corresponding point does not lie on a line collapsed by σ_1^{-1}. Since p_2 is a proper point of the plane, it follows that the point a_4 does not belong to a line collapsed by σ_1. In particular, no three of the points $a_1, \ldots, a_4$ belong—as proper or infinitely near points—to a common line. This implies the existence (Lemma 14) of an element $\varphi \in \text{Ine}(C)$ of degree 3 whose linear system Λ_φ consists of cubics that are singular at a_1 and that pass through a_2, a_3, a_4. The image of Λ_φ by σ_1 is a system of conics passing through $b_1 = p_1$ and p_2. If p_3 is not a base point of this system, then the image of Λ_φ by ψ is a system of conics passing through q_1, q_2; otherwise, it is the system of the lines of the plane. Then $\psi \circ \varphi^{-1}$ is a birational map of degree at most 2 and is the composition of at most two simple quadratic transformations (because both q_1 and q_2 are proper points of $\mathbb{P}^2$). Applying one of the preceding cases to $\eta \circ \varphi^{-1} = (\sigma_r \circ \cdots \circ \sigma_3) \circ (\psi \circ \varphi^{-1})$, we are done.

If the degree of ψ is 4 then $P \cap B = \emptyset$, whence the linear system Λ_ψ consists of quartics singular at a_1, a_2, a_3 and that pass through three other points a_4, a_5, a_6 that correspond respectively to p_1, p_2, p_3 and are proper points of $\mathbb{P}^2$ if and only if the corresponding point does not lie on a line collapsed by σ_1^{-1}. Once again, the point p_4 does not belong to a line collapsed by σ_1 because p_1 is a proper point of the plane, and this yields the existence (using Lemma 14 once again) of an element $\varphi \in \text{Ine}(C)$ of degree 3 whose linear system Λ_φ is composed by cubics that are

singular at a_1 and that pass through a_2, a_3, a_4. The image of Λ_φ by σ_1 is a system of conics passing through b_1 and p_1. If p_2 (resp. p_3) is a base point of this system, then the image of Λ_φ by ψ is a system of conics passing through q_1 and q_2 (resp. q_3); otherwise, it is a system of cubics that are singular at q_1 and that pass through q_2 and q_3. In both cases, since the q_i are proper points of $\mathbb{P}^2$, the map $\psi \circ \varphi^{-1}$ is the composition of at most two simple quadratic transformations. Because the degree of $\psi \circ \varphi^{-1}$ is 2 or 3, we may apply one of the cases just treated to $\eta \circ \varphi^{-1} = (\sigma_r \circ \cdots \circ \sigma_3) \circ (\psi \circ \varphi^{-1})$. $\qquad \square$

5. The Elements of Finite Order

Proof of Theorem 2. We first use the fact that g has finite order n to conjugate g via a birational map to an automorphism of a smooth rational surface S (see e.g. [FE, Thm. 1.4]). The curve fixed by g thus becomes a smooth elliptic curve $C \subset S$, since the set of points of a smooth surface that are fixed by an automorphism is smooth. We may assume that the pair (g, S) is minimal (i.e., that every g-equivariant birational morphism $S \to S'$ is an isomorphism). Then, one of the following situations occurs (see [M]):

(i) $\operatorname{rk} \operatorname{Pic}(S)^g = 1$ and S is a Del Pezzo surface; or

(ii) $\operatorname{rk} \operatorname{Pic}(S)^g = 2$ and there exists a conic bundle structure $\pi : S \to \mathbb{P}^1$ that is invariant by the action of g (i.e., g sends a fibre to another fibre).

In case (i), the surface S is the blow-up $\pi : S \to \mathbb{P}^2$ of $1 \le r \le 8$ points of the plane (it may not be $\mathbb{P}^1 \times \mathbb{P}^1$ or $\mathbb{P}^2$, because C has positive genus). Since g is birationally conjugate by π to a birational transformation having at most r base points, Lemmas 8 and 13 imply that $r \ge 5$. Since $\operatorname{rk} \operatorname{Pic}(S)^g = 1$, the divisor of C is equivalent to a multiple of K_S. Since C is a smooth elliptic curve, we find that $C = -K_S$ and, in particular, that any birational morphism $S \to \mathbb{P}^2$ sends C to a smooth cubic. Denote by $d = 9 - r \le 4$ the degree of the Del Pezzo surface S. The anticanonical morphism induced by $|-K_S|$ is a g-equivariant morphism $\varphi : S \to \mathbb{P}^d$, and the image of C is contained in a hyperplane of $\mathbb{P}^d$ that is fixed by g.

If the order of g (denoted by n) were divisible by $\operatorname{char}(\mathbb{K})$, then the action of g on $\mathbb{P}^d$ would have the form

$$(x_0 : \cdots : x_d) \mapsto (x_0 : x_1 + x_0 : \lambda_2 x_2 + \mu_2 x_1 : \cdots : \lambda_d x_d + \mu_d x_{d-1})$$

for some $\lambda_i, \mu_i \in \mathbb{K}$. Given that $\operatorname{char}(\mathbb{K}) \ne 2, 3, 5$, that our varieties are smooth, and that the degree ≤ 6, this case is not possible. Hence the action of g on $\mathbb{P}^d$ will be of the form $x_0 \mapsto \zeta_n x_0$, where $\zeta_n \in \mathbb{K}$ is a primitive nth root of unity.

We use the classical description of φ and S that depends on the degree d of S (see [BaB; B; F; K]).

If $d = 4$, then φ is an isomorphism from S to a surface $X_{2,2} \subset \mathbb{P}^4$ that is the intersection of two quadrics. The equations of the quadrics may be chosen to be $\sum x_i^2 = \sum \lambda_i x_i^2$, and g is an involution of the form $x_0 \mapsto -x_0$ (these automorphisms have been studied in [B]). Note that every birational involution of $\mathbb{P}^2$ that

fixes a curve of geometric genus 1 is birationally conjugate to this case, since two such involutions are conjugate if and only if they fix the same curve (see [BaB]). In the sequel, we will therefore not study the case $n = 2$.

If $d = 3$, then φ is an isomorphism from S to a cubic surface of $\mathbb{P}^3$. Thus, $n \leq 3$ and g is of the form $x_0 \mapsto \zeta_n x_0$.

If $d = 2$, then φ is a double covering of $\mathbb{P}^2$ ramified over a smooth quartic and S has equation $x_3^2 = L_4(x_0, x_1, x_2)$ in the weighted space $\mathbb{P}(1, 1, 1, 2)$, where φ corresponds to the projection on the first three factors. Thus, $n \leq 4$ and g acts on $\mathbb{P}(1, 1, 1, 2)$ as $x_0 \mapsto \zeta_n x_0$. If $n = 3$, then we may assume (since S is smooth) that $L_4 = x_0^3(x_1 + \lambda_1 x_2) + x_1^4 + x_2^4$. But then the trace on S of the equation $x_1 + \lambda_1 x_2 = 0$ is a curve, equivalent to $-K_S$, that is decomposed into two curves (both invariant by g), whence $\mathrm{rk} \, \mathrm{Pic}(S)^g > 1$.

If $d = 1$, then φ is an elliptic fibration with one base point. The surface S has equation $x_3^2 = x_2^3 + x_2 \cdot L_4(x_0, x_1) + L_6(x_0, x_1)$ in $\mathbb{P}(1, 1, 2, 3)$ for some forms L_i of degree i, and φ is the projection on the first two factors. We see that $n \leq 6$ and that the action of g on $\mathbb{P}(1, 1, 2, 3)$ is of the form $x_0 \mapsto \zeta_n x_0$. The cases $n = 5, 6$ are given in the proposition; it remains to take care of the cases $n = 3, 4$. If $n = 3$, then the equation of S becomes

$$x_3^2 = x_2^3 + x_2 x_1 \cdot (\lambda_1 x_0^3 + \lambda_2 x_1^3) + \lambda_3 x_0^6 + \lambda_4 x_0^3 x_1^3 + \lambda_5 x_1^6$$

for some $\lambda_i \in \mathbb{K}$. Replacing $x_2 = \mu x_1^2$ into this equation yields

$$x_3^2 = (\lambda_3) x_0^6 + (\mu \lambda_1 + \lambda_4) x_0^3 x_1^3 + (\mu^3 + \mu \lambda_2 + \lambda_5) x_1^6.$$

For the correct choice of $\mu \in \mathbb{K}$, the right side of the equality becomes a square and thus the curve on S of equation $x_2 = \mu x_1^2$ (which is equivalent to $-2K_S$) decomposes into two g-equivariant curves, whence $\mathrm{rk} \, \mathrm{Pic}(S)^g > 1$. Assume now that $n = 4$, which implies that the equation of S is

$$x_3^2 = x_2^3 + x_2 \cdot (\lambda_1 x_0^4 + \lambda_2 x_1^4) + x_1^2 \cdot (\lambda_3 x_0^4 + \lambda_4 x_1^4)$$

for some $\lambda_i \in \mathbb{K}$. Once again, for the correct choice of $\mu \in \mathbb{K}$, the curve on S of equation $x_2 = \mu x_1^2$ decomposes into two g-equivariant curves; therefore, $\mathrm{rk} \, \mathrm{Pic}(S)^g > 1$.

It remains to study case (ii). Because g fixes a nonrational curve, its action on the base $\mathbb{P}^1$ is trivial. The automorphism g^2 leaves invariant any component of every singular fibre (which is the union of two exceptional curves). After blowing down one exceptional curve in any fibre, this conjugates g^2 to an automorphism of some Hirzebruch surface. Since g^2 fixes a nonrational curve it is the identity, whence $n = 2$. As indicated previously, the element g is birationally conjugate to an automorphism of a Del Pezzo surface of degree 4.   □

REMARK 16.   Let $C \subset \mathbb{P}^2$ be a smooth cubic curve. Theorem 2 implies that, for any $p \in C$, the involution σ_p is conjugate to an automorphism of a Del Pezzo surface of degree 4. If the five base points of σ_p are proper points of $\mathbb{P}^2$, then the conjugation may be done by blowing up the five points.

Furthermore, by [BaB], for a given curve C all the elements σ_p are conjugate in the Cremona group.

6. The Group Generated by Cubic Involutions

Let us fix some notation for this section.

We shall assume that $\operatorname{char}(\mathbb{K}) \neq 2$, and we denote by $C \subset \mathbb{P}^2$ a smooth cubic curve and by $\Omega_0 \subset C$ a finite subset. Our aim is to study the group generated by $\{\sigma_p\}_{p \in \Omega_0}$ and then prove that it is a free product of the groups of order 2 generated by the σ_p.

We denote by Ω the union of the base points of the σ_p for $p \in \Omega_0$ ($\subset \Omega$). Because this set is finite, we may denote by $\pi \colon S \to \mathbb{P}^2$ the blow-up of each point of Ω. For any point $p \in \Omega_0$, we denote by σ_p' the birational transformation $\pi^{-1}\sigma_p\pi$ of S (which is biregular, since π blows up the base points of σ_p plus a finite set of points fixed by σ_p). Since σ_p' is an automorphism of S, it acts on $\operatorname{Pic}(S)$; we may thus write $\sigma_p'(D)$ for any divisor $D \in \operatorname{Pic}(S)$.

Given two points $a, b \in \Omega$, we say that $b \succ a$ if $a \neq b$ and a is a base point of σ_b. We remark that if $b \succ a_1$, $b \succ a_2$, and $a_1 \neq a_2$, then $a_1 \not\succ b$, $a_2 \not\succ b$, $a_1 \not\succ a_2$, and $a_2 \not\succ a_1$. (This follows from the geometric description of Proposition 12: if b is not an inflexion point, then the line passing through a_i and b is tangent to C at a_i and not at b, and the line passing through a_1 and a_2 is not tangent to C at either a_1 or a_2; the case where b is an inflexion point is similar.) We associate to any point $p \in \Omega$ its exceptional divisor $E_p = \pi^{-1}(p) \in \operatorname{Pic}(S)$ and will denote by L the pull-back by π of a general line of $\mathbb{P}^2$. The set $\{\{E_p\}_{p \in \Omega}, L\}$ is a basis of the free $\mathbb{Z}$-module $\operatorname{Pic}(S)$. Any effective divisor $D \in \operatorname{Pic}(S)$ that is not collapsed by π is equal to $mL - \sum_{p \in \Omega} m_p E_p$ for some nonnegative integers m, m_p with $m > 0$. Hence we define

$$\Delta_b(D) = 2m - 2m_b - \sum_{b \succ c} m_c \quad \text{and}$$

$$\Lambda_{b,a}(D) = m - m_b + m_a - \sum_{\substack{b \succ c \\ c \neq a}} m_c$$

for any points $a, b \in \Omega$ with $b \succ a$.

Lemma 17. *Let $p \in \Omega_0$. Then, for any $a \in \Omega$,*

$$\sigma_p'(L) = 3L - 2E_p - \sum_{p \succ b} E_b;$$

$$\sigma_p'(L - E_p) = L - E_p;$$

$$\sigma_p'(E_a) = \begin{cases} 2L - E_p - \displaystyle\sum_{p \succ b} E_b & \text{if } a = p, \\ L - E_p - E_a & \text{if } p \succ a, \\ E_a & \text{otherwise.} \end{cases}$$

Proof. Recall that σ_p is a cubic involution, that its base points are p with multiplicity 2, and that the points $b \in \Omega$ are such that $p \succ b$ with multiplicity 1 (Proposition 12); as a consequence, we have $\sigma_p'(L) = 3L - 2E_p - \sum_{p \succ b} E_b$. The

second equality follows because σ_p leaves invariant the pencil of lines of $\mathbb{P}^2$ passing through p; the third equality follows directly.

Since the line passing through p and one other base point q is collapsed on q, we see that $\sigma'_p(L - E_p - E_q) = E_q$. The remaining part follows from the fact that σ_p is an involution that fixes the curve C on which all the points of Ω lie (as proper or infinitely near points). □

LEMMA 18. *Let $D \in \operatorname{Pic}(S)$ be some divisor, and let $p \in \Omega_0$ be some point. Writing $\delta_q = \Delta_q(D)$ and $\lambda_{r,q} = \Lambda_{r,q}(D)$ for any points $q, r \in \Omega$ with $r \succ q$, we have the relations*

$$\Delta_a(\sigma'_p(D)) = \begin{cases} -\delta_a & \text{if } a = p, \\ \delta_a + \delta_p & \text{if } a \succ p, \\ \delta_a + 2\lambda_{p,a} & \text{if } p \succ a, \\ \delta_a + 2\delta_p & \text{otherwise} \end{cases}$$

and

$$\Lambda_{b,a}(\sigma'_p(D)) = \begin{cases} -\lambda_{b,a} & \text{if } b = p, \\ \lambda_{b,a} + 2\delta_p & \text{if } a = p, \\ \lambda_{b,a} & \text{if } b \succ p \neq a, \\ \lambda_{b,a} + \lambda_{p,b} & \text{if } p \succ b, \\ \lambda_{b,a} + 2\delta_p & \text{otherwise} \end{cases}$$

for any points $a, b \in \Omega$ with $b \succ a$.

Proof. Write $D = nL - \sum_{q \in \Omega} n_q E_q$ for some integers n, n_q. Lemma 17 implies that $\sigma'_p(D) = mL - \sum_{q \in \Omega} m_q E_q$, where $m = 2n - n_p - \sum_{p \succ b} n_b$ and

$$m_q = \begin{cases} 2n - 2n_p - \displaystyle\sum_{p \succ b} n_b & \text{if } a = p, \\ n - n_p - n_q & \text{if } p \succ q, \\ n_q & \text{otherwise.} \end{cases}$$

By substituting these values, we find the values of

$$\Delta_a(\sigma'_p(D)) = 2m - 2m_a - \sum_{a \succ c} m_c \quad \text{and}$$

$$\Lambda_{b,a}(\sigma'_p(D)) = m - m_b + m_a - \sum_{\substack{b \succ c \\ c \neq a}} m_c$$

as linear combinations of

$$\Delta_a(D) = 2n - 2n_a - \sum_{a \succ c} n_c \quad \text{and}$$

$$\Lambda_{b,a}(D) = n - n_b + n_a - \sum_{\substack{b \succ c \\ c \neq a}} n_c.$$

(We leave the details to the interested reader.) □

We are now able to prove the following proposition, whose assertion (1) induces Theorem 6 and Corollary 7. The proof of Proposition 19 is rather tricky even

though it uses only simple relations of Lemma 18, so we have tried to make it as readable as possible.

PROPOSITION 19. *Let $D = \sigma'_{p_m} \circ \sigma'_{p_{m-1}} \circ \cdots \circ \sigma'_{p_1}(L)$, where $m \geq 0$, $p_1, \ldots, p_m \in \Omega$, and $p_i \neq p_{i+1}$ for $1 \leq i \leq m - 1$. Writing $p = p_m$ (if $m = 0$ there is no p) as well as $\delta_q = \Delta_q(D)$ and $\lambda_{r,q} = \Lambda_{r,q}(D)$ for any points $q, r \in \Omega$ with $r \succ q$, we have the following relations.*

(1) $\delta_p < 0$.
(2) $\delta_a > 0$ if $a \neq p$.
(3) $-\delta_p < \delta_a$ if $a \neq p$ and $a \not\succ p$.
(4) $i\delta_a + j\lambda_{b,a} + k\delta_b > 0$ for $b \succ a$, $i \geq 1$, $j \geq 2$, and

$$\begin{cases} i = j, & k = -1, & a \neq p; \\ i = j + 1, & k = 1, & a \neq p; \\ i = j, & k = 1, & b \neq p; \\ i = j - 1, & k = -1, & b \neq p. \end{cases}$$

(5) $i(\delta_a + 2\lambda_{b,a}) + j\delta_{a'} + k\delta_b > 0$ for $b \succ a$, $b \succ a'$, $a \neq a'$, $i, j \geq 1$, and

$$\begin{cases} i = j, & k = 1, & b \neq p; \\ i = j + 1, & k = -1, & b \neq p; \\ i = j, & k = -1, & a' \neq p; \\ i = j - 1, & k = 1, & a' \neq p. \end{cases}$$

(6) $\delta_a + 2\lambda_{p,a} + \delta_r > \delta_p$ for $p \succ a$ and $r \neq p$, where $a, b, a', r \in \Omega$ and $i, j, k \in \mathbb{Z}$. In particular, $D \neq L$ if $m > 0$.

Proof. We will use the relations of Lemma 18 to prove Proposition 19 by induction on m.

Suppose first that $m = 0$, and note the simple relations $\Delta_a(L) = 2$ and $\Lambda_{b,a}(L) = 1$ for any points $b \succ a \in \Omega$. Assertions (1), (3), and (6) do not apply if $m = 0$ because then there is no p. Assertion (2) is self-evident and (4) and (5) may be verified by replacing δ by 2 and λ by 1 and then using that $i, j \geq 1$ and $k = \pm 1$.

Suppose now that $m \geq 1$. We write $\bar{D} = \sigma'_{p_{m-1}} \circ \cdots \circ \sigma'_{p_1}(L)$ (and so $D = \sigma'_p(\bar{D})$) as well as $\bar{\delta}_a = \Delta_a(\bar{D})$ and $\bar{\lambda}_{b,a} = \Lambda_{b,a}(\bar{D})$ for any points $a, b \in \Omega$ with $b \succ a$. We use assertions (1)–(6) for $m - 1$ (i.e., for the $\bar{\delta}$s and $\bar{\lambda}$s) together with Lemma 18 to prove the same assertions for m (i.e., for the δs and λs).

(1) Since $p \neq p_{m-1}$ we have $\bar{\delta}_p > 0$ by (2), whence $\delta_p = -\bar{\delta}_p < 0$.

(2) and (3) Taking $a \neq p$, Lemma 18 asserts that

$$\delta_a = \begin{cases} \bar{\delta}_a + \bar{\delta}_p & \text{if } a \succ p, \\ \bar{\delta}_a + 2\bar{\lambda}_{p,a} & \text{if } p \succ a, \\ \bar{\delta}_a + 2\bar{\delta}_p & \text{otherwise.} \end{cases}$$

If $p \succ a$, we may use (4) for $i = 1$, $j = 2$, and $k = -1$ to see that $\delta_a = \bar{\delta}_a + 2\bar{\lambda}_{p,a} > \bar{\delta}_p = -\delta_p$. We therefore obtain $\delta_a > -\delta_p > 0$ and thus (2) and (3) together. If $p \not\succ a$, we prove first that $\bar{\delta}_a + \bar{\delta}_p$ is positive. If $a = p_{m-1}$ then this follows from

(3), which shows that $-\overline{\delta_a} = -\overline{\delta_{p_{m-1}}} < \overline{\delta_p}$; if $a \neq p_{m-1}$ then the sum is positive because both $\overline{\delta_a}$ and $\overline{\delta_p}$ are positive (assertion (2)). If $a \succ p$, then δ_a is equal to $\overline{\delta_a} + \overline{\delta_p}$ and thus is positive (we obtain (2)); otherwise, δ_a is equal to $\overline{\delta_a} + 2\overline{\delta_p}$ and is therefore larger than $\overline{\delta_p} = -\delta_p > 0$ (we thus obtain (2) and (3) together).

(4) Take $a, a', b \in \Omega$ such that $b \succ a$, $b \succ a'$, and $a \neq a'$. We list the changes of (respectively) δ_a, $\lambda_{b,a}$, and δ_b after the action of σ'_p in the following table.

	$\delta_a - \overline{\delta_a}$	$\lambda_{b,a} - \overline{\lambda_{b,a}}$	$\delta_b - \overline{\delta_b}$
$p = a$	$-2\overline{\delta_p}$	$2\overline{\delta_p}$	$\overline{\delta_p}$
$p = b$	$2\overline{\lambda_{p,a}}$	$-2\overline{\lambda_{p,a}}$	$-2\overline{\delta_p}$
$b \succ p \neq a$	$2\overline{\delta_p}$	0	$\overline{\delta_p}$
$a \succ p \succ b$	$\overline{\delta_p}$	$\overline{\lambda_{p,b}}$	$2\overline{\lambda_{p,b}}$
$a \succ p \not\succ b$	$\overline{\delta_p}$	$\overline{\delta_p}$	$2\overline{\delta_p}$
$a \not\succ p \succ b$	$2\overline{\delta_p}$	$\overline{\lambda_{p,b}}$	$2\overline{\lambda_{p,b}}$
otherwise	$2\overline{\delta_p}$	$\overline{\delta_p}$	$2\overline{\delta_p}$

We first prove that $\delta_a + 2\lambda_{b,a} - \delta_b$ is positive if $b \neq p$ (assertion (4) with $i = 2$, $j = 1$, and $k = -1$). Assume that $p \neq b$. The table shows that $\delta_a + 2\lambda_{b,a} - \delta_b = \overline{\delta_a} + 2\overline{\lambda_{b,a}} - \overline{\delta_b} + k\overline{\delta_p}$ for some integer $k \geq 1$. If $p_{m-1} \neq b$, then $\overline{\delta_a} + 2\overline{\lambda_{b,a}} - \overline{\delta_b}$ is positive (the same assertion for $m - 1$); if $p_{m-1} = b$, then (6) shows that $\overline{\delta_a} + 2\overline{\lambda_{b,a}} - \overline{\delta_b} + \overline{\delta_p}$ is positive. In both cases we see that $\delta_a + 2\lambda_{b,a} - \delta_b$ is positive.

Next we prove (4) in general (i.e., for all specified values of $i, j, k \in \mathbb{Z}$ and $a, b \in \Omega$). If $p \notin \{a, b\}$ then $\delta_a, \delta_b > 0$, whence

$$i\delta_a + j\lambda_{b,a} + k\delta_b = \frac{j}{2} \cdot (\delta_a + 2\lambda_{b,a} - \delta_b) + \left(\left(i - \frac{j}{2}\right)\delta_a + \left(\frac{j}{2} + k\right)\delta_b\right)$$

is positive because $i - j/2$ and $j/2 + k$ are nonnegative. Assume now that $p = a$ and either that $i = j$ and $k = 1$ or that $i = j - 1$ and $k = -1$ (as in the statement of (4)). We compute

$$i\delta_a + j\lambda_{b,a} + k\delta_b = i \cdot (-\overline{\delta_a}) + j \cdot (\overline{\lambda_{b,a}} + 2\overline{\delta_a}) + k \cdot (\overline{\delta_b} + \overline{\delta_a})$$
$$= i' \cdot \overline{\delta_a} + j\overline{\lambda_{b,a}} + k\overline{\delta_b},$$

where $i' = (2j - i + k)$. We use (4) for $m - 1$ (since $a = p$ and $a \neq p_{m-1}$). If $i = j$ and $k = 1$, then $i' = j - 1$. If $i = j - 1$ and $k = -1$, then $i' = j$. The case of $p = b$ is similar. We compute

$$i\delta_a + j\lambda_{b,a} + k\delta_b = i \cdot (\overline{\delta_a} + 2\overline{\lambda_{b,a}}) + j \cdot (-\overline{\lambda_{b,a}}) + k \cdot (-\overline{\delta_b})$$
$$= i \cdot \overline{\delta_a} + j'\overline{\lambda_{b,a}} + k'\overline{\delta_b},$$

where $j' = (2i - j)$ and $k' = -k$. If $i = j$ and $k = 1$, then $i = j'$ and $k' = -1$; if $i = j - 1$ and $k = -1$, then $i' = j' + 1$ and $k' = 1$. Since $b \neq p_{m-1}$, assertion (4) for $m - 1$ may be used to conclude.

(5) Similarly, we now prove (5) for all the specified values of $i, j, k \in \mathbb{Z}$ and $a, a', b \in \Omega$. If $p \notin \{a', b\}$, then $\delta_a + 2\lambda_{b,a} > \delta_b$ (assertion (4), already proved) and $\delta_{a'} > 0$, whence $i(\delta_a + 2\lambda_{b,a}) + j\delta_{a'} + k\delta_b > (i + k)\delta_b + j\delta_{a'} > 0$ because $i + k \geq 0$ and $j > 0$. Assume now that $p = a'$ and either that $i = j$ and $k = 1$ or that $i = j + 1$ and $k = -1$ (as in the statement of (5)). We compute

$$i(\delta_a + 2\lambda_{b,a}) + j\delta_{a'} + k\delta_b = i(\overline{\delta_a} + 2\overline{\delta_{a'}} + 2\overline{\lambda_{b,a}}) + j \cdot (-\overline{\delta_{a'}}) + k(\overline{\delta_b} + \overline{\delta_{a'}})$$
$$= i(\delta_a + 2\lambda_{b,a}) + j'\delta_{a'} + k\delta_b,$$

where $j' = 2i - j + k$. We use (5) for $m - 1$, since $a' = p$ and $a' \neq p_{m-1}$. If $i = j$ and $k = 1$, then $i = j' - 1$. If $i = j + 1$ and $k = -1$, then $i = j'$. The case of $p = b$ is similar. We compute

$$i(\delta_a + 2\lambda_{b,a}) + j\delta_{a'} + k\delta_b$$
$$= i(\overline{\delta_a} + 2\overline{\lambda_{b,a}} - 2\overline{\lambda_{b,a}}) + j(\overline{\delta_{a'}} + 2\overline{\lambda_{b,a'}}) + k \cdot (-\overline{\delta_b})$$
$$= i'(\overline{\delta_{a'}} + 2\overline{\lambda_{b,a'}}) + j'(\overline{\delta_a}) + k' \cdot (\overline{\delta_b}),$$

where $i' = j$, $j' = i$, and $k' = -k$. We use (5) for $m - 1$, exchanging the roles of a and a' and using that $p_{m-1} \neq p = q$.

(6) It remains only to prove (6). Take $a, r \in \Omega$ with $p \succ a$ and $r \neq p$, as in the statement. We first compute $\delta_a + 2\lambda_{p,a} - \delta_p = \overline{\delta_a} + 2\overline{\lambda_{p,a}} - 2\overline{\lambda_{p,a}} + \overline{\delta_p} = \overline{\delta_a} + \overline{\delta_p}$ and recall that $\overline{\delta_p}$ is positive. If $\overline{\delta_a} + \overline{\delta_p}$ is nonnegative then $\delta_a + 2\lambda_{p,a} + \delta_r - \delta_p$ is positive, as stated in assertion (6). If $r = a$, then $\delta_a = \overline{\delta_a} + 2\overline{\lambda_{p,a}}$ and so $\delta_a + 2\lambda_{p,a} + \delta_r - \delta_p$ is equal to $2\overline{\delta_a} + 2\overline{\lambda_{p,a}} + \overline{\delta_p}$, which is positive by (4) for $m - 1$ with $i = j = 2$, $k = 1$, and $p \neq p_{m-1}$. If $p \succ r$ and $r \neq a$, then $\delta_r = \overline{\delta_r} + 2\overline{\lambda_{p,r}}$. Hence $\delta_a + 2\lambda_{p,a} + \delta_r - \delta_p$ is equal to $\overline{\delta_a} + \overline{\delta_p} + \overline{\delta_r} + 2\overline{\lambda_{p,r}}$, which is positive by (5) for $m - 1$ with $i = j = 1$, $k = 1$, and $p \neq p_{m-1}$. The remaining case is when $r \neq a$, $p \not\succ r$, and $\overline{\delta_a} + \overline{\delta_p} < 0$. The condition on r implies that $\delta_r > \overline{\delta_r}$, and the latter implies that $a = p_{m-1}$. Since $r \neq p$ it follows that $r \not\succ a$, whence $\overline{\delta_r} > -\overline{\delta_a}$. This shows that $\delta_a + 2\lambda_{p,a} + \delta_r - \delta_p > \overline{\delta_a} + \overline{\delta_p} + \overline{\delta_r} > 0$, and we are done. $\qquad\square$

References

[A] M. Alberich-Carramiñana, *Geometry of the plane Cremona maps,* Lecture Notes in Math., 1769, Springer-Verlag, Berlin, 2002.

[BaB] L. Bayle and A. Beauville, *Birational involutions of* $\mathbb{P}^2$, Asian J. Math. 4 (2000), 11–17.

[B] A. Beauville, *p-elementary subgroups of the Cremona group,* J. Algebra 314 (2007), 553–564.

[BBl] A. Beauville and J. Blanc, *On Cremona transformations of prime order,* C. R. Acad. Sci. Paris Sér. I Math. 339 (2004), 257–259.

[Bl] J. Blanc, *Finite Abelian subgroups of the Cremona group of the plane,* C. R. Acad. Sci. Paris Sér. I Math. 344 (2007), 21–26.

[BlPV] J. Blanc, I. Pan, and T. Vust, *Sur un théorème de Castelnuovo,* Bull. Braz. Math. Soc. (N.S.) 39 (2008), 61–80.

[C] G. Castelnuovo, *Sulle transformazioni cremoniane del piano, che ammettono una curva fissa,* Rend. Accad. Lincei (1892); Memorie scelte, Zanichelli, Bologna, 1937.

[F] T. de Fernex, *On planar Cremona maps of prime order,* Nagoya Math. J. 174 (2004), 1–28.

[FE] T. de Fernex and L. Ein, *Resolution of indeterminacy of pairs,* Algebraic geometry, pp. 165–177, de Gruyter, Berlin, 2002.

[G] M. H. Gizatullin, *The decomposition, inertia and ramification groups in birational geometry,* Algebraic geometry and its applications (A. Tikhomirov, A. Tyurin, eds.), Aspects Math., E25, pp. 39–45, Vieweg, Braunschweig, 1994.

[K] J. Kollár, *Rational curves on algebraic varieties,* Ergeb. Math. Grenzgeb. (3), 32, Springer-Verlag, Berlin, 1996.

[M] J. I. Manin, *Rational surfaces over perfect fields, II,* Mat. Sb. (N.S.) 72 (1967), 141–168.

[P1] I. Pan, *Sur le degré dynamique des transformations de Cremona du plan qui stabilisent une courbe irrationnelle non-elliptique,* C. R. Acad. Sci. Paris Sér. I Math. 341 (2005), 439–443.

[P2] ———, *Sur le sous-groupe de décomposition d'une courbe irrationnelle dans le groupe de Cremona du plan,* Michigan Math. J. 55 (2007), 285–298.

Université de Grenoble I
UFR de Mathématiques
UMR 5582 du CNRS
Institut Fourier, BP 74
38402 Saint-Martin d'Hères
France

Jeremy.Blanc@fourier.ujf-grenoble.fr