*L'Enseignement Mathématique* (2) 63 (2017), 21–61 DOI 10.4171/LEM/63-1/2-2

# On real and complex cubic curves

Araceli Bonifant and John Milnor

**Abstract.** An expository description of smooth cubic curves in the real or complex projective plane.

**Mathematics Subject Classification (2010).** Primary: 14H52, 14H37, 14H50; Secondary: 14-03, 01-01, 14P99.

**Keywords.** Elliptic curve, Hesse normal form, standard normal form, projective equivalence, tangent process, flex point.

## 1. Introduction

This note will present elementary proofs for basic facts about smooth cubic curves $\mathcal{C}$ in the complex projective plane $\mathbb{P}^2(\mathbb{C})$, or the corresponding curves $\mathcal{C}_{\mathbb{R}}$ in the real projective plane $\mathbb{P}^2(\mathbb{R})$ when the defining equation has real coefficients. The presentation will center around two different normal forms, which we refer to as the *Hesse normal form*

$$x^3 + y^3 + z^3 = 3\,k\,x\,y\,z \tag{1}$$

(using homogeneous coordinates), and the *standard normal form*

$$y^2 = x^3 + ax + b \tag{2}$$

(using affine coordinates $(x : y : 1)$ with $z = 1$). We are particularly concerned with classification up to *projective equivalence* (that is up to a linear change of coordinates in the projective plane). The set of *flex points* (three in the real case and nine in the complex case) plays a central role in our exposition.

Although much of the material which follows is well known, there are a few things which we have not been able to find in the literature. One of these is the following concise classification (see Theorem 6.3):

> Every smooth irreducible real cubic curve $\mathcal{C}_{\mathbb{R}}$ is real projectively equivalent to one and only one curve $\mathcal{C}(k)_{\mathbb{R}}$ in the Hesse normal form. Here any real parameter $k \neq 1$ can occur. The curve $\mathcal{C}(k)_{\mathbb{R}}$ is connected if $k < 1$, and has two components if $k > 1$.

Another is the precise description of the automorphism group, consisting of projective transformations which map the curve to itself. This has order 6 in the real case, and order 18 for a generic complex curve; but has order 36 or 54 in the special case of a complex curve which has square or hexagonal symmetry. In all cases it has a maximal abelian subgroup which acts freely on the curve, and acts transitively on its set of flex points. (See Corollaries 3.10 and 6.7.) On the other hand, the group of birational automorphisms, which is canonically isomorphic to the group of conformal automorphisms, acts transitively on the entire curve (Corollaries 4.4 and 4.7).

One useful elementary remark is that the projective equivalence class of a curve in the standard normal form is uniquely determined by the *shape* of the "triangle" in the complex $x$-plane formed by the three roots of the equation $x^3 + ax + b = 0$. (See Figure 2, as well as Definition 3.7 and Proposition 3.8.)

The paper is organized as follows. Sections 2 through 5 concentrate on the complex case (although some arguments work just as well over an arbitrary subfield $\mathbb{F} \subset \mathbb{C}$). Section 2 studies flex points, reduction to Hesse normal form, and provides a preliminary description of the automorphism group. Section 3 studies reduction to the standard normal form, as well as the $J$-invariant

$$J(\mathcal{C}) = \frac{4a^3}{4a^3 + 27b^2},$$

and the computation of $J$ as a function of the Hesse parameter $k$. Section 4 discusses the conformal classification of $\mathcal{C}$ as a Riemann surface, and shows that a conformal diffeomorphism from $\mathcal{C}$ to $\mathcal{C}'$ extends to a projective automorphism of $\mathbb{P}^2$ if and only if it maps flex points to flex points. Section 5 describes the chord-tangent map $\mathcal{C} \times \mathcal{C} \to \mathcal{C}$ and the related additive group structure on the curve. Finally, Section 6 describes real cubic curves. In particular, it provides a canonical affine picture, so that the automorphisms are clearly visible, and so that any two real curves can be directly compared. (See Figure 10.)

**Notation.** We use the notation $(x, y, z)$ for a non-zero point of the complex 3-space $\mathbb{C}^3$, and the notation $(x : y : z)$ for the corresponding point of $\mathbb{P}^2$, representing the equivalence class consisting of all multiples $(\lambda\, x,\, \lambda\, y,\, \lambda\, z)$ with $\lambda \in \mathbb{C} \smallsetminus \{0\}$. However, it is sometimes convenient to represent a point of $\mathbb{P}^2$ by a single bold letter such as $\mathbf{p}$. Note that any linear automorphism of $\mathbb{C}^3$ gives rise to a *projective automorphism* of the projective plane $\mathbb{P}^2$.

**Historical Remarks.** Hesse's actually used a constant multiple of our $k$ as parameter. Our "standard normal form" is a special case of a form used by Newton, and is a close relative of the form which Weierstrass introduced much later. Our $J(\mathcal{C})$ is just Felix Klein's invariant $j(\mathcal{C})$ divided by 1728. (For the original papers, see [New], [Hes1, H2], [Weil, W2], and [Kl].) The "tangent" part of the chord-tangent map was used by Diophantus of Alexandria in the third century to construct new rational points on a cubic curve from known ones, although this was done in a purely algebraic way. More than thirteen centuries later, in the 1670's Newton used the "chord-tangent construction" to interpret the solutions of Diophantine equations given by Diophantus and Fermat. (Compare [Sti, Section 11.6].) Weil says that the chord process was first used by Newton, although Bashmakova claims that it was used already by Diophantus. (See [Weil] and [Ba].) The closely related additive structure is due to Poincaré [P], who was the first to study the arithmetic of algebraic curves. (Compare [Kna] and [Ba, p. 412].) Real cubic curves in the affine plane were studied by Newton. (Compare [New], as well as [BK].) For further historical remarks, see [AD], [Dol], and [RB]. For an elementary introduction to the field see [Gib]; and for real cubic curves from an older point of view, see [Whi].

## 2. Hesse Normal Form for Complex Cubic Curves

This section will be concerned with the work of Otto Hesse and its consequences. (See [Hes1, H2], both published in 1844.) Hesse introduced[1] the family of cubic curves $\mathcal{C}(k)$ consisting of all points $(x : y : z)$ in the projective plane $\mathbb{P}^2 = \mathbb{P}^2(\mathbb{C})$ which satisfy the homogeneous equation $\Phi_k(x, y, z) = 0$ where

$$(3) \qquad \Phi_k(x, y, z) = x^3 + y^3 + z^3 - 3\,k\,x\,y\,z\,.$$

Given a generic point $(x : y : z)$ in $\mathbb{P}^2$, we can solve the equation $\Phi_k(x, y, z) = 0$ for

$$k = \frac{x^3 + y^3 + z^3}{3\,x\,y\,z} \in \mathbb{C} \cup \{\infty\}.$$

(Thus for $k = \infty$ we define $\mathcal{C}(\infty)$ to be the locus $xyz = 0$.) However, there are nine *exceptional points*[2] where

$$\text{both} \qquad x^3 + y^3 + z^3 = 0 \qquad \text{and} \qquad x\,y\,z = 0,$$

[1] Gibson refers to the $\mathcal{C}(k)$ as "Steiner curves", presumably referring to [Ste].

[2] We will see in Remark 2.11 that these nine "exceptional points" on any smooth $\mathcal{C}(k)$ are precisely the nine flex points.

so that the parameter $k$ is not uniquely defined. All of the curves $\mathcal{C}(k)$ pass through all of these nine points, which have the form

$$(4) \qquad (0:1:-\gamma) \quad \text{or} \quad (-\gamma:0:1) \quad \text{or} \quad (1:-\gamma:0) \quad \text{with} \quad \gamma^3 = 1.$$

In the complement of these nine exceptional points, the space $\mathbb{P}^2(\mathbb{C})$ is the disjoint union of the Hesse curves.

**Definition 2.1.** A point of the curve $\Phi(x,y,z) = 0$ is *singular* if the partial derivatives $\Phi_x$, $\Phi_y$ and $\Phi_z$ all vanish at the point. The curve is called *smooth* if it has no singular points.

**Lemma 2.2.** *The Hesse curve $\mathcal{C}(k)$ has singular points if and only if either $k^3 = 1$ or $k = \infty$.*

*Proof.* For the curve $\mathcal{C}(k)$ with $k$ finite, a singular point must satisfy the equations

$$x^2 = kyz, \quad y^2 = kxz\,, \quad z^2 = kxy,$$

which imply that $x^3 = y^3 = z^3 = k\,xyz$, and hence $x^3y^3z^3 = k^3x^3y^3z^3$. For $k^3 \neq 1$ with $k$ finite, it follows easily that there are no singularities. On the other hand, if $k^3 = 1$, then it is not hard to check that $\mathcal{C}(k)$ is the union of three straight lines of the form $\alpha x + \beta y + z = 0$ with $\alpha^3 = \beta^3 = 1$ and $\alpha\beta = k$. Hence it is singular at the three points where two of these lines intersect.[3] Similarly the curve $\mathcal{C}(\infty)$ is clearly singular at the three points $(0:0:1)$, $(1:0:0)$ and $(0:1:0)$ where two of the lines $x = 0$, $y = 0$, and $z = 0$ intersect. □

Thus altogether there are twelve points in $\mathbb{P}^2$ which are singular for one of these curves. If we remove these twelve singular points and also the nine exceptional points from $\mathbb{P}^2$, then we obtain a smooth foliation by Hesse curves.

**Definition 2.3.** Let $\mathrm{Aut}(\mathbb{P}^2)$ be the group of all projective automorphisms of $\mathbb{P}^2$; and for any curve $\mathcal{C} \subset \mathbb{P}^2$ let $\mathrm{Aut}(\mathbb{P}^2, \mathcal{C})$ be the subgroup consisting of projective automorphisms which map $\mathcal{C}$ onto itself.

Curves defined by the Hesse equations (3) are clearly highly symmetric. Following is a precise statement.

**Lemma 2.4.** *The group $\mathrm{Aut}\big(\mathbb{P}^2(\mathbb{C})\big)$ contains an abelian subgroup*

$$N \cong \mathbb{Z}/3 \oplus \mathbb{Z}/3$$

[3] For $k = 1$, one such intersection point $(1:1:1)$ is clearly visible to the upper right in Figure 1, even though the rest of the two intersecting lines lie outside of the real projective plane.

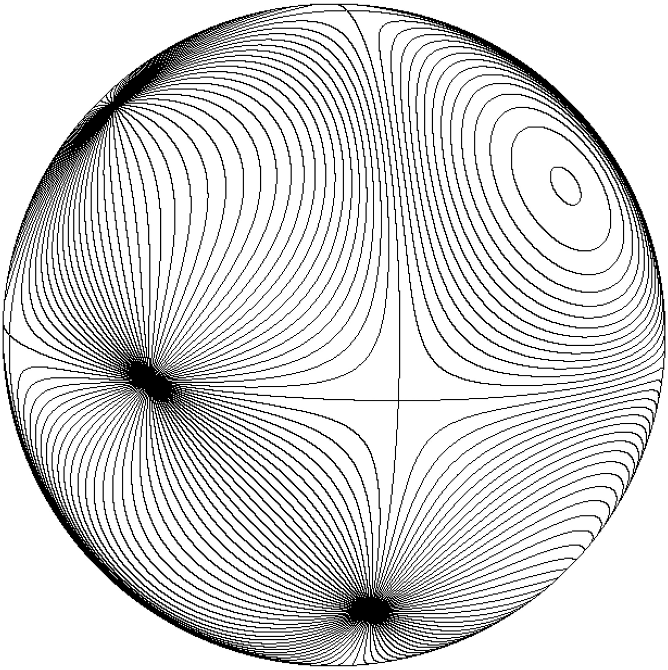


FIGURE 1

"Foliation" of the real projective plane by the Hesse pencil of curves $\mathcal{C}(k)_{\mathbb{R}} = \mathcal{C}(k) \cap \mathbb{P}^2(\mathbb{R})$. Here $\mathbb{P}^2(\mathbb{R})$ is represented as a unit sphere with antipodal points identified. Note the three exceptional points $(-1 : 1 : 0)$, $(0 : -1 : 1)$, and $(1 : -1 : 0)$ where all of the $\mathcal{C}(k)_{\mathbb{R}}$ intersect. Also note the three singular points where the components of $\mathcal{C}(\infty)_{\mathbb{R}} = \{x = 0\} \cup \{y = 0\} \cup \{z = 0\}$ intersect, and note the isolated singular point at $(1 : 1 : 1) \in \mathcal{C}(1)_{\mathbb{R}}$. The figure has 120° rotational symmetry about this point. (This figure has been borrowed from our paper [BDM], which studies rational maps preserving such cubic curves.)

*independent of $k$, which acts without fixed points on every smooth $\mathcal{C}(k)$, and acts simply transitively on the set of nine "exceptional points" of equation* (4)*. The group* $\mathrm{Aut}(\mathbb{P}^2)$ *also contains an element $\iota$ of order two, which maps each $\mathcal{C}(k)$ onto itself, and such that conjugation by $\iota$ maps each element of $N$ to its inverse.*

Thus the automorphism group $\mathrm{Aut}(\mathbb{P}^2, \mathcal{C}(k))$ contains at least 18 elements. In fact, we will show in Theorem 2.12 below that any smooth cubic curve $\mathcal{C}$ can be put into the form (3), so that the automorphism group $\mathrm{Aut}(\mathbb{P}^2, \mathcal{C})$ always contains a corresponding 18 element subgroup. (In most cases, this is the full automorphism group, but for some special curves there are extra symmetries, as described in Corollary 3.10.)

*Proof of Lemma* 2.4. A cyclic permutation of the three coordinates $x$, $y$, $z$ clearly acts effectively on every curve of the form (3). This action has just one fixed point $(1:1:1) \in \mathcal{C}(1) \subset \mathbb{P}^2$, but has no fixed points in $\mathcal{C}(k)$ for $k \neq 1$. If $\gamma$ is a primitive cube root of unity, then the transformation

$$(x:y:z) \quad \mapsto \quad (x:\gamma\, y:\gamma^2 z)$$

is another automorphism of order three which commutes with the cyclic permutation of coordinates. It is not difficult to check[4] that the abelian group $N$ generated by these two transformations has fixed points only on the singular Hesse curves with $k^3 = 1$ or $k = \infty$. Furthermore, it acts simply transitively on the set of exceptional points (4). Finally, the permutation $(x:y:z) \leftrightarrow (y:x:z)$ is an element $\iota$ of order two which carries each $\mathcal{C}(k)$ to itself, and has the required action on $N$. (This permutation does have four fixed points on each $\mathcal{C}(k)$, consisting of just one of the nine exceptional points, namely $(1:-1:0)$, together with the three points of $\mathcal{C}(k)$ which lie on the line $x = y$.) □

Although we are primarily interested in cubic curves, we will often use results which apply to curves of any degree $n \geq 2$. The most fundamental property of complex projective curves of specified degree is the following:

> For any smooth curve $\mathcal{C} \subset \mathbb{P}^2(\mathbb{C})$ of degree $n \geq 2$ and any line $L \subset \mathbb{P}^2$, the intersection $\mathcal{C} \cap L$ consists of $n$ points, counted with multiplicity.[5]

Here:

- A transverse intersection has multiplicity one.
- The intersection between $\mathcal{C}$ and its tangent line at a generic point has multiplicity two.
- At certain special "flex points" this tangential intersection will have multiplicity three or more.

For a cubic curve, note that the intersection multiplicity is three if and only if there are no other points of intersection between $\mathcal{C}$ and $L$.

**Definition 2.5.** For a curve $\mathcal{C}$ of any degree, a non-singular point is called an inflection point, or briefly a *flex point*, if the intersection multiplicity between $\mathcal{C}$ and its tangent line is three or more. (Of course in the cubic case, this intersection multiplicity is always precisely three, unless $\mathcal{C}$ contains an entire straight line, which implies that $\mathcal{C}$ contains singular points.)

[4] Here is a typical case. If $(x:y:z) = (y:\gamma z:\gamma^2 x)$ then, using the fact that $(x:y) = (u:v)$ if and only if $xv = yu$, we can check that $x^2 = \gamma yz$, $y^2 = \gamma xz$ and $z^2 = \gamma xy$. Therefore $x^3 = y^3 = z^3 = \gamma xyz$, hence $k = \gamma$ and the curve is singular.

[5] This is an special case of Bézout's theorem; but can also be proved just by restricting the defining equation $\Phi(x,y,z) = 0$ to the line $L$, and then using the Fundamental Theorem of Algebra.

We will prove in Theorem 2.10 that every smooth complex cubic curve has precisely nine flex points. However, the proof will be based on a more general discussion which applies to smooth curves of any degree.

**Definition 2.6.** Let $\Phi(x,y,z)$ be a homogeneous polynomial of degree $n$. The associated *Hessian determinant* is the homogeneous polynomial function

$$\mathcal{H}_\Phi(x,y,z) = \det\begin{pmatrix} \Phi_{xx} & \Phi_{xy} & \Phi_{xz} \\ \Phi_{yx} & \Phi_{yy} & \Phi_{yz} \\ \Phi_{zx} & \Phi_{zy} & \Phi_{zz} \end{pmatrix}, \tag{5}$$

of degree $3(n-2)$, where the subscripts on the right indicate partial derivatives.

**Theorem 2.7.** *Let $\mathcal{C}$ be any smooth curve of degree three or more with defining equation $\Phi(x,y,z)=0$. Then the set* $\text{Flex}(\mathcal{C})$ *consisting of all flex points in $\mathcal{C}$ is equal to the set of all points in $\mathcal{C}$ which satisfy the homogeneous equation $\mathcal{H}_\Phi(x,y,z)=0$ .*

As the first step in the proof, we must show that this locus $\mathcal{H}_\Phi = 0$ behaves properly under projective transformations. Let

$$(x,y,z) \;\mapsto A(x,y,z) = (u,v,w) \tag{6}$$

be a non-singular linear transformation, and let $A_* : \mathbb{P}^2(\mathbb{C}) \to \mathbb{P}^2(\mathbb{C})$ be the induced projective transformation. Note that $A_*$ maps the curve $\mathcal{C}$ defined by the equation $\Phi(x,y,z)=0$ to the curve $\mathcal{C}' = A_*(\mathcal{C})$ defined by the equation $\Psi(u,v,w)=0$, where $\Psi = \Phi \circ A^{-1}$ (or equivalently $\Phi = \Psi \circ A$), as one sees from the diagram

$$\begin{tikzcd}
\mathbb{C}^3 \arrow[r, "A"] \arrow[dr, "\Phi"] & \mathbb{C}^3 \arrow[d, "\Psi"] \\
 & \mathbb{C}.
\end{tikzcd}$$

**Lemma 2.8.** *With these notations, $A_*$ maps the curve defined by the equation $\mathcal{H}_\Phi(x,y,z)=0$ to the curve defined by $\mathcal{H}_\Psi(u,v,w)=0$. In particular, it maps the locus of points on $\mathcal{C}$ with $\mathcal{H}_\Phi(x,y,z)=0$ to the locus of points on $A_*(\mathcal{C})$ satisfying $\mathcal{H}_\Psi(u,v,w)=0$.*

*Proof.* For this proof only, it will be convenient to switch to matrix notation, representing a point in $\mathbb{C}^3$ by a column vector $\mathbf{X}$, and writing a linear change of coordinates $A : \mathbb{C}^3 \to \mathbb{C}^3$ as

$$\mathbf{X} \quad \mapsto \quad \mathbf{AX} = \mathbf{U} \qquad \text{where} \qquad \mathbf{X} = \begin{bmatrix} x \\ y \\ z \end{bmatrix} \qquad \text{and} \qquad \mathbf{U} = \begin{bmatrix} u \\ v \\ w \end{bmatrix},$$

and where $\mathbf{A}$ can be any non-singular $3 \times 3$ matrix. Let $\mathbf{M}_\Phi(\mathbf{X})$ be the matrix of second partial derivatives of $\Phi$, with determinant $\mathcal{H}_\Phi(\mathbf{X})$, and define $\mathbf{M}_\Psi(\mathbf{U})$ with determinant $\mathcal{H}_\Psi(\mathbf{U})$ similarly. Then we will prove that

$$\mathbf{M}_\Phi(\mathbf{X}) = \mathbf{A}^t\, \mathbf{M}_\Psi(\mathbf{AX})\, \mathbf{A}, \tag{7}$$

where $\mathbf{A}^t$ is the transpose matrix.

To prove (7), note that the Taylor series for $\Phi$ at a point $\mathbf{X}_0$ has the form

$$\Phi(\mathbf{X}_0{+}\mathbf{X}) = \Phi(\mathbf{X}_0) + (\text{linear terms}) + (\text{quadratic terms}) + (\text{higher order terms}),$$

where the quadratic terms can be written as $\frac{1}{2}\mathbf{X}^t\, \mathbf{M}_\Phi(\mathbf{X}_0)\, \mathbf{X}$. If we ignore all terms of degree other than two, then this can be written briefly as

$$\Phi(\mathbf{X}_0 + \mathbf{X}) = \cdots \ + \ \tfrac{1}{2}\mathbf{X}^t\, \mathbf{M}_\Phi(\mathbf{X}_0)\, \mathbf{X} \ + \ \cdots\,. \tag{8}$$

Similarly

$$\Psi(\mathbf{U}_0 + \mathbf{U}) = \cdots \ + \ \tfrac{1}{2}\mathbf{U}^t\, \mathbf{M}_\Psi(\mathbf{U}_0)\, \mathbf{U} \ + \ \cdots\,.$$

Now substituting $\mathbf{AX}$ for $\mathbf{U}$ and $\mathbf{AX}_0$ for $\mathbf{U}_0$, and recalling that $\Phi = \Psi \circ \mathbf{A}$, this last equation takes the form

$$\Phi(\mathbf{X}_0 + \mathbf{X}) = \Psi(\mathbf{U}_0 + \mathbf{U}) = \cdots \ + \ \tfrac{1}{2}\mathbf{X}^t \mathbf{A}^t\, \mathbf{M}_\Psi(\mathbf{AX}_0)\, \mathbf{AX} \ + \ \cdots\,.$$

Comparing this expression with (8), and noting that the two equations must agree for all $\mathbf{X}$, the required equation (7) follows.

Now taking the determinant of both sides of (7) and switching back to non-matrix notation, we obtain the identity

$$\mathcal{H}_\Phi(x,y,z) = \det(A)^2 \mathcal{H}_\psi(u,v,w), \quad \text{where} \quad (u,v,w) = A(x,y,x)\ . \tag{9}$$

Lemma 2.8 now follows easily, since the constant factor $\det(A)^2$ does not affect the induced transformation of projective space. □

*Proof of Theorem* 2.7. We must show that a point $(x_0 : y_0 : z_0) \in \mathcal{C}$ is a flex point if and only if $\mathcal{H}_\Phi(x_0, y_0, z_0) = 0$. Choose a linear change of coordinates which maps the given point $(x_0, y_0, z_0)$ to $(0,0,1)$. After a rotation of the $x, y$ coordinates, we may assume that the image curve is tangent to the line $y = 0$. Now, working with affine coordinates $(x : y : 1)$, we can solve locally for $y$ as a smooth function $y = f(x)$, where the derivative $dy/dx = f'(x)$ vanishes for $x = 0$. Differentiating the equation $\Phi(x,\ f(x),\ 1) = 0$ twice, we obtain

$$\Phi_x + \Phi_y f'(x) = 0 \qquad \text{and} \qquad \Phi_{xx} + 2\Phi_{xy} f'(x) + \Phi_{yy}(f'(x))^2 + \Phi_y f''(x) = 0$$

along the curve, where $\Phi_x(0,0,1) = 0$ but $\Phi_y(0,0,1) \neq 0$. In particular, at the specified point with $x = f'(x) = 0$, we see that

$$\Phi_{xx} = 0 \quad \Longleftrightarrow \quad f''(x) = 0 \quad \Longleftrightarrow \quad x \text{ is a flex point .}$$

To finish the proof of Theorem 2.7, we must show, with a choice of coordinates as above, that $\Phi_{xx}(0,0,1) = 0$ if and only if $\mathcal{H}_\Phi(0,0,1) = 0$. Note that $\Phi(x,y,z)$ can be written uniquely as a sum of monomials $c_{ijk}x^i y^j z^k$ with $i + j + k = n$. Since $\Phi(0,0,1) = 0$, we know that the coefficient of $z^n$ is zero, and it follows easily that $\Phi_{zz}(0,0,1) = 0$. Similarly, since $\Phi_x(0,0,1) = 0$, it follows easily that $\Phi_{xz}(0,0,1) = 0$; but $\Phi_y(0,0,1) \neq 0$ hence $\Phi_{yz}(0,0,1) \neq 0$. It is now straightforward to check that Hessian determinant reduces to $\mathcal{H}_\Phi = -\Phi_{xx}\Phi_{yz}^2$ at the point $(0,0,1)$, and the conclusion follows. □

**Remark 2.9.** More explicitly, whenever $\Phi_y(0,0,1) \neq 0$ so that $y$ can be expressed locally as a smooth function $y = f(x)$, we have the identity

$$\mathcal{H}_\Phi(0,0,1) = 4\Phi_y^3(0,0,1)\, f''(0).$$

In the case where $f'(0) = 0$, this follows from the proof above, together with the observation that $\Phi_{yz}(0,0,1) = 2\,\Phi_y(0,0,1)$. (This last equality can be checked by comparing the first derivative of the monomial $yz^2$ with respect to $y$, and the second derivative with respect to $y$ and $z$.)

The more general case where $f'(x) \neq 0$ can be dealt with by noting that the change of coordinates

$$(x, y, z) \mapsto (x,\, ax + y,\, z)$$

clearly does not affect $d^2y/dx^2$, and by noting that the locus $\mathcal{H}_\Phi = 0$ transforms by equation (9).

Even more generally we can write

$$\mathcal{H}_\Phi(x, f(x), 1) = 4\Phi_y^3(x, f(x), 1) f''(x) \tag{10}$$

at any point of the curve where $\Phi_y \neq 0$, since both sides of this equation are invariant under translation.

**Theorem 2.10.** *Every smooth cubic curve in $\mathbb{P}^2(\mathbb{C})$ has nine flex points.*

*Proof.* If a curve $\mathcal{C}_1$ of degree $n_1$ and a curve $\mathcal{C}_2$ of degree $n_2$ have only smooth transverse intersections, then it follows from Bézout's Theorem that the number of intersection points is precisely equal to the product $n_1 n_2$. (See for example [BK, Section 6.1] or [Ha, pp. 36, 54].) We are intersecting two curves $\{\Phi = 0\}$

and $\{\mathcal{H}_\Phi = 0\}$ which both have degree three. Thus to prove Theorem 2.10, we need only show that these two curves have only smooth transverse intersections.[6]

Since equation (10) holds at all points of $\mathcal{C}$ with $\Phi_y \neq 0$, we can differentiate with respect to $x$ to obtain

$$\frac{\partial \mathcal{H}_\Phi}{\partial x}(0,0,1) = \Phi_y^3(0,0,1)\, f'''(x)$$

whenever $f'(0) = 0$. But at a flex point of a smooth cubic curve, where $f''(0) = 0$, the third derivative $f'''(0)$ can never vanish, for this would imply that the entire tangent line at that point would have to be contained in $\mathcal{C}$. Thus $\partial\mathcal{H}_\Phi/\partial x \neq 0$ at a flex point; and it follows easily that the two curves $\{\mathcal{H}_\phi = 0\}$ and $\{\Phi = 0\}$ have a transverse intersection at every flex point. Thus every smooth cubic curve has exactly nine flex points; which completes the proof of Theorem 2.10. □

**Remark 2.11.** In the special case of a smooth Hesse curve $\mathcal{C}(k)$, the nine flex points coincide with the nine "exceptional points" of equation (4). To see this, taking $\Phi(x,y,z) = x^3+y^3+z^3-3\,k\,x\,y\,z$, note for example that $\Phi_{xx} = 6\,x$ and $\Phi_{xy} = -3\,k\,z$. A straightforward computation shows that the Hessian determinant is given by

$$\mathcal{H}_\Phi(x,y,z) = 3^3\big((8-2\,k^3)x\,y\,z \;-\; 2k^2(x^3+y^3+z^3)\big).$$

If $\Phi(x,y,z) = 0$, then we can substitute $3kxyz$ for $x^3+y^3+z^3$ on the right side of this equation. This yields $\mathcal{H}_\Phi(x,y,z) = 6^3(1-k^3)xyz$. If we are in the non-singular case, with $k^3 \neq 1$, then it follows that $\Phi$ and $\mathcal{H}_\Phi = 0$ are both zero only at the nine points with

$$x^3+y^3+z^3 = x\,y\,z = 0,$$

as in (4). (On the other hand, if $k^3 = 1$ then the Hessian is identically zero on $\mathcal{C}(k)$, which means that $\mathcal{C}(k)$ is a union of straight lines.)

The set of nine flex points together with the twelve lines joining them form a fascinating configuration. (Compare Figure 7 and Remark 5.7.)

**Reduction to Hesse normal form.** Recall that, two algebraic varieties in a projective space $\mathbb{P}^n$ are *projectively equivalent* if there exists a projective automorphism of $\mathbb{P}^n$ which carries one variety onto the other.

The following result is taken from a textbook published by Heinrich Weber in 1898. (See [Web, v.3, p.22]. We don't know whether this result was known earlier.)

[6] The curve $\{\mathcal{H}_\Phi = 0\}$ may have singular points, but is always non-singular near the intersection.

**Theorem 2.12.** *Every smooth cubic curve in $\mathbb{P}^2(\mathbb{C})$ is projectively equivalent to a curve $\mathcal{C}(k)$ in the Hesse normal form*

$$x^3 + y^3 + z^3 = 3\,k\,x\,y\,z,$$

*with $k \in \mathbb{C}$, $k^3 \neq 1$.*

*Proof.* Choose two distinct flex points for the given curve $\mathcal{C}$, and choose homogeneous coordinates $x$, $y$, $z$ so that:

- the line $x = 0$ is tangent to $\mathcal{C}$ at the first flex point,
- the line $y = 0$ is tangent at the second flex point, and
- the line $z = 0$ passes through both flex points.

Working in affine coordinates with $z = 1$, these conditions mean that $\mathcal{C}$ has no finite point on the lines $x = 0$ or $y = 0$. In other words the polynomial function $\Phi(x, y, 1)$ must take a non-zero constant value on these two lines; say $\Phi(x, y, 1) = 1$ whenever $xy = 0$. Hence it must have the form $\Phi(x, y, 1) = 1 + xy(ax + by + c)$. In homogeneous coordinates, this means that

$$\Phi(x, y, z) = z^3 + xy(ax + by) + cxyz.$$

Furthermore $a \neq 0$ since otherwise $(1 : 0 : 0)$ would be a singular point, and $b \neq 0$ since otherwise $(0 : 1 : 0)$ would be singular. Now to put this polynomial in the required form, we must express $xy(ax + by)$ as a sum of two cubes.[7] In fact, consider the identity

$$(\gamma\,p\,x + q\,y)^3 + (-p\,x - \gamma\,q\,y)^3 = 3i\sqrt{3}\,xy\big(-p^2q\,x + pq^2\,y\big),$$

where $\gamma = (-1 + i\sqrt{3})/2$. It is not difficult to choose $p$ and $q$ so as to satisfy the required equalities

$$-3i\sqrt{3}\,p^2q = a \qquad \text{and} \qquad 3i\sqrt{3}\,pq^2 = b,$$

since we can first solve for $p/q = -a/b$, and then solve for $p$. □

**Remark 2.13.** According to Lemma 2.2, a curve in Hesse form, with $k$ finite, is smooth if and only if $k^3 \neq 1$. This Hesse form is not unique, since there are several different ways of choosing the two flex points. We will see in Theorem 3.12 that, for a generic choice of the smooth curve $\mathcal{C}$, there are twelve different possible choices of the parameter $k$.

[7] More generally, any smooth cubic locus $\Psi(x, y) = 0$ in $\mathbb{P}^1(\mathbb{C})$ is just a union of three distinct points, and it is not hard to choose a projective equivalence (= fractional linear transformation) from the Riemann sphere $\mathbb{P}^1(\mathbb{C})$ to itself which carries one such triple to any other.

**Corollary 2.14.** *Every smooth complex cubic curve possesses an automorphism group of order at least 18 which acts transitively on its set of nine flex points.*

*Proof.* This follows immediately by combining Lemma 2.4 and Remark 2.11 with Theorem 2.12. □

(For a more precise description of the automorphism group, see Corollary 3.10.)

## 3. The standard normal form

Recall that a curve in standard normal form is defined by the equation

$$y^2 = x^3 + ax + b$$

in affine coordinates $(x : y : 1)$. Equivalently, using homogeneous coordinates $(x : y : z)$, it is defined by the equation $\Phi = 0$ where

$$\Phi(x, y, z) = -y^2z + x^3 + axz^2 + bz^3. \tag{11}$$

One virtue of this normal form is that is useful over many different fields.[8] For our purposes, the following level of generality will be convenient.

Let $\mathbb{F} \subset \mathbb{C}$ be any subfield of the complex numbers. A curve $\mathcal{C} \subset \mathbb{P}^2(\mathbb{C})$ is said to be *defined over* $\mathbb{F}$ if it is defined by a homogeneous polynomial equation $\Phi(x, y, z) = 0$ with coefficients in $\mathbb{F}$. Similarly, an $\mathbb{F}$*-projective transformation* will mean a projective transformation with coefficients in $\mathbb{F}$, or equivalently one which maps the projective space $\mathbb{P}^2(\mathbb{F})$ onto itself.

The notation $\mathcal{C}_\mathbb{F} \subset \mathbb{P}^2(\mathbb{F})$ will be used for the intersection $\mathcal{C} \cap \mathbb{P}^2(\mathbb{F})$, consisting of all points of $\mathcal{C}$ with coordinates in $\mathbb{F}$.

**Caution.** In this generality, there is no guarantee that $\mathcal{C}_\mathbb{F}$ will have any points at all. For example, the equation $3x^3 + 4y^3 + 5z^3 = 0$ has no non-zero solution with $x, y, z$ in the field of rational numbers $\mathbb{Q}$. In other words, the corresponding locus $\mathcal{C}_\mathbb{Q} \subset \mathbb{P}^2(\mathbb{Q})$ is vacuous. (See [Cas, p. 85].)

**Theorem 3.1.** *Let $\mathbb{F} \subset \mathbb{C}$ be any subfield of the complex numbers, and let $\mathcal{C} \subset \mathbb{P}^2(\mathbb{C})$ be an irreducible cubic curve, defined by a homogeneous equation $\Phi = 0$ with coefficients in $\mathbb{F}$. Then $\mathcal{C}$ is $\mathbb{F}$-projectively equivalent to a curve in the standard normal form* (11) *if and only if the set of non-singular points in $\mathcal{C}_\mathbb{F}$ contains a flex point.*

[8] More precisely, one can reduce to this normal form over any field of characteristic other than two or three.

**Remark 3.2.** This is a much easier variant of Trygve Nagell's Theorem, which can be stated as follows:

> Given a smooth complex cubic $\mathcal{C}$ which is defined over $\mathbb{F}$, and given an arbitrary point $\mathbf{p} \in \mathcal{C}_{\mathbb{F}}$, there is an $\mathbb{F}$-birational equivalence between $\mathcal{C}$ and some curve in standard normal form which takes $\mathbf{p}$ to the flex point at infinity.

See [Nag], as well as [Cas, p. 34] which implicitly includes a brief proof of the above Theorem 3.1. For further discussion, see Remark 4.6 below.

*Proof of Theorem* 3.1. Let $\mathcal{C}$ be a curve in the normal form (11). Along the "line at infinity" with equation $z = 0$, the equation $\Phi = 0$ reduces to $x^3 = 0$, yielding the single point $(0:1:0)$, counted with multiplicity three. Thus $(0:1:0)$ is a flex point (non-singular since $\partial\Phi/\partial z \neq 0$), and the line $z = 0$ is the tangent line at this flex point.

Conversely, given any irreducible $\mathcal{C}$ which is defined over $\mathbb{F}$ and any flex point $\mathbf{p} \in \mathcal{C}_{\mathbb{F}}$, we can put the curve into normal form in four steps, as follows.

**Step 1.** Choose an $\mathbb{F}$-linear change of coordinates which maps $\mathbf{p}$ to the point $(0:1:0)$ and maps the tangent line at $\mathbf{p}$ to the line $z = 0$. It is then easy to check that the image of $\mathcal{C}_{\mathbb{F}}$ will have defining equation of the form

$$\Phi(x, y, z) = x^3 + z\Psi(x, y, z),$$

where $\Psi$ is homogeneous quadratic with coefficients in $\mathbb{F}$. Note that the coefficient of $y^2 z$ in $\Phi$ must be non-zero. In fact it is easy to check that

$$\Phi_x(0:1:0) = \Phi_y(0:1:0) = 0$$

and that $\Phi_z(0,1,0)$ is equal to the coefficient of $y^2 z$. Since our flex point is assumed to be non-singular, this coefficient must be non-zero.

**Step 2.** If we make a linear change of coordinates, replacing $x$ by $\alpha x$ and $y$ by $\beta y$, and also replace $\Phi$ by $\Phi/\alpha^3$, then the equation will take the form $\widehat{\Phi} = 0$ where

$$\widehat{\Phi}(x, y, z) = x^3 + z\Psi(\alpha x, \beta y, z)/\alpha^3.$$

Thus the coefficient of $y^2 z$ is now multiplied by $\beta^2/\alpha^3$. Now choose $\alpha$ and $\beta$ so that the coefficient of $y^2 z$ will be $-1$. (As one example, there is a unique choice with $\alpha = \beta$.) Working in affine coordinates with $z = 1$, this means that our $\widehat{\Phi}$ will take the form

$$-y^2 + x^3 + px^2 + qx + r + y(sx + t),$$

with coefficients $p, q, r, s, t \in \mathbb{F}$.

**Step 3.** To get rid of the $y$ terms on the right, simply replace $y$ by $y+(sx+t)/2$. This will yield a function of the form

$$-y^2+x^3+p'x^2+q'x+r'.$$

**Step 4.** To eliminate the $x^2$ term, replace $x$ by $x-p'/3$. Our function will then be in the required form $-y^2+x^3+ax+b$. □

**Lemma 3.3.** *Using the normal form* (11) *with* $a, b \in \mathbb{F} \subset \mathbb{C}$, *the curve* $\mathcal{C}$ *is singular if and only if the equation* $x^3+ax+b=0$ *has a double root, which is necessarily in the subfield* $\mathbb{F}$, *or if and only if the discriminant* $-(4a^3+27b^2)$ *is zero.*

*Proof.* Over the complex numbers, there is always an essentially unique factorization

$$x^3+ax+b=(x-r_1)(x-r_2)(x-r_3).$$

Suppose that $(x:y:z)$ is a singular point of $\mathcal{C}$. Since $\Phi_z(0:1:0)=-1$, the unique point of $\mathcal{C}$ on the line $z=0$ is certainly non-singular, so it will suffice to work in affine coordinates with $z=1$. Every point with $y\neq 0$ is non-singular since $\Phi_y(x,y,1)=-2y\neq 0$. Thus it only remains to consider the three points $(r_j:0:1)$ on the line $y=0$. For example $\Phi_x(r_1,0,1)=(r_1-r_2)(r_1-r_3)$, so that the point $(r_1:0:1)\in\mathcal{C}$ is singular if and only if $r_1$ is a double root.

Next we need to check that a double root necessarily belongs to the subfield $\mathbb{F}\subset\mathbb{C}$. But the sum of the roots is zero, so if $r$ is a double root, then the third root is $-2r$. It follows easily that $a=-3r^2$ and $b=2r^3$, so that either $a=b=r=0\in\mathbb{F}$ or else $r=-3b/2a\in\mathbb{F}$.

Finally, we apply the classical discriminant identity

$$\prod_{i<j}(r_i-r_j)^2=-(4a^3+27b^2).$$

(See for example [BM].) This proves Lemma 3.3. □

**Lemma 3.4.** *A projective change of coordinates*

$$(x:y:z)\mapsto(X:Y:Z)$$

*which fixes the flex point* $(0:1:0)$ *will transform a curve in the standard normal form* $y^2=x^3+ax+b$ *to a curve* $Y^2=X^3+AX+B$ *in the same normal form if and only if this change of coordinates has the form*

$$X=t^2x, \quad Y=t^3y, \quad \textit{and hence} \quad A=t^4a \quad \textit{and} \quad B=t^6b \tag{12}$$

*for some non-zero* $t\in\mathbb{F}$.

*Proof.* If we make the substitutions (12) in the equation

$$Y^2 = X^3 + AX + B\,,$$

then we obtain the original equation $y^2 = x^3 + ax + b$ multiplied by $t^6$. To show that this is the only permissible change of coordinates, we proceed as follows.

Since the line $z = 0$ is tangent to our curve at the marked flex point, it must certainly map onto itself under any projective transformation which preserves this point and its tangent direction. Thus it will suffice to work in affine coordinates, with $z = 1$. The most general linear transformation then has the form

$$X = (\alpha x + \beta y) + \xi, \quad Y = (\gamma x + \delta y) + \eta,$$

with $\alpha, \beta, \gamma, \delta, \xi, \eta \in \mathbb{F}$, and with $\alpha\delta - \beta\gamma \neq 0$. Substituting these values into $X$ and $Y$, the equation $Y^2 = X^3 + AX + B$ should reduce to a constant multiple of $y^2 = x^3 + ax + b$ for suitably chosen $A$ and $B$. Here the coefficient $\beta$ must be zero so that there is no $x^2y$ term in the expansion, and $\gamma = 0$ so that there is no $xy$ term. Similarly $\xi = 0$ so that there is no $x^2$ term, and $\eta = 0$ so that there is no $y$ term. Thus $X = \alpha x$ and $Y = \delta y$. Finally, we must have $\delta^2 = \alpha^3$ so that the coefficients of $y^2$ and $x^3$ will be equal. Thus, setting $t = \delta/\alpha$, we have $t^2 = \delta^2/\alpha^2 = \alpha$ and $t^3 = \delta^3/\alpha^3 = \delta$. Thus we obtain

$$t^6y^2 = t^6x^3 + t^2Ax + B.$$

Dividing by $t^6$, the required equations $A = t^4a$ and $B = t^6b$ now follow. □

**Corollary 3.5.** *Every smooth complex cubic curve $\mathcal{C}$ can be reduced to the standard form (11) by a projective transformation; and two such curves are projectively equivalent if and only if they share the same value for the invariant*

$$J(\mathcal{C}) = \frac{4a^3}{4a^3 + 27b^2} \in \mathbb{C}. \tag{13}$$

*Here any value $J(\mathcal{C}) \in \mathbb{C}$ can occur.*

*Proof.* This follows directly from Theorem 3.1 and Lemma 3.4. There are three places where the restriction to the complex case is necessary. First, according to Theorem 2.10 every smooth cubic curve has a flex point. Second, according to Corollary 2.14, there is an automorphism which carries any flex point to any other flex point, so that it doesn't matter which flex point we choose for the reduction to normal form. Third, since every complex number has a complex square root, it follows easily that we can use the transformation $a \mapsto A = t^4a,\ b \mapsto B = t^6b$ for suitably chosen $t$ to convert the pair of coefficients $a, b$ to $A, B$, whenever the ratio $(a^3 : b^2) \in \mathbb{P}^1(\mathbb{C})$ is equal to $(A^3 : B^2)$.

However, this ratio $(a^3 : b^2)$ is a bit awkward to work with, since either $a$ or $b$ may be zero, and since the ratio $(-3^2 : 2^2)$ occurs only for singular curves. The equivalent invariant (13) is much more convenient since it takes all possible finite values for smooth curves, and is infinite only for singular curves by Lemma 3.3. Further details of the proof of Corollary 3.5 are straightforward. □

**Remark 3.6.** If the curve $\mathcal{C}$ is defined over a subfield $\mathbb{F} \subset \mathbb{C}$, then the invariant $J(\mathcal{C})$ must belong to $\mathbb{F}$. In fact, since the flex points are defined by algebraic equations with coefficients in $\mathbb{F}$, they are contained in[9] $\mathbb{P}^2(\mathbb{F}')$ for some finite Galois extension $\mathbb{F}' \supset \mathbb{F}$; hence $J(\mathcal{C}) \in \mathbb{F}'$. But $J(\mathcal{C})$ is invariant under all automorphisms of $\mathbb{F}'$ over $\mathbb{F}$, so it must belong to $\mathbb{F}$.

We can give this invariant $J \in \mathbb{C}$ a more geometric interpretation as follows. Recall that a curve in standard normal form is uniquely determined by the three roots $r_j$, which are distinct if and only if the curve is non-singular. We will use the word "***triangle***" as a convenient term for an unordered set consisting of three distinct points in the complex plane.

(**Caution:** The three points are allowed to lie in a straight line.)

**Definition 3.7.** We will say that two subsets of the complex plane have the same *shape* if there is a complex affine automorphism $x \mapsto px + q$ which takes one to the other.

**Proposition 3.8.** *For cubic curves of the form $y^2 = f(x)$, where $f(x)$ is a cubic polynomial with distinct roots $\{r_j\}$, the shape of the triangle formed by the three roots is a complete invariant for projective equivalence.*

In particular, this is true for curves in the normal form $y^2 = x^3 + ax + b$. Since $J(\mathcal{C})$ is also a complete invariant for projective equivalence, it follows that this "shape" is uniquely determined by the complex number $J$.

*Proof of Proposition* 3.8. It is not difficult to put a curve of the form $y^2 = f(x)$ into the standard form by an affine change of the $x$ variable. The conclusion then follows easily from Lemma 3.4. □

**Remark 3.9.** (See Figure 2 for some typical examples.) Note that:

$$J = 0 \quad \Leftrightarrow \quad a = 0 \quad \Leftrightarrow \quad \text{the triangle is equilateral, and}$$

$$J = 1 \quad \Leftrightarrow \quad b = 0 \quad \Leftrightarrow \quad \text{one vertex is the midpoint of the other two.}$$

[9] Suppose for example that $(x : y : 1) \in \mathbb{P}^2(\mathbb{C})$ is a flex point. Then the field $\mathbb{F}''$ obtained from $\mathbb{F}$ by adjoining $x$ and $y$ must be a finite extension of $\mathbb{F}$. For otherwise the inclusion map $\mathbb{F} \to \mathbb{C}$ would extend to infinitely many different embeddings of $\mathbb{F}''$ into $\mathbb{C}$, leading to infinitely many flex points. The required $\mathbb{F}'$ is now just the splitting field of $\mathbb{F}''$ over $\mathbb{F}$.

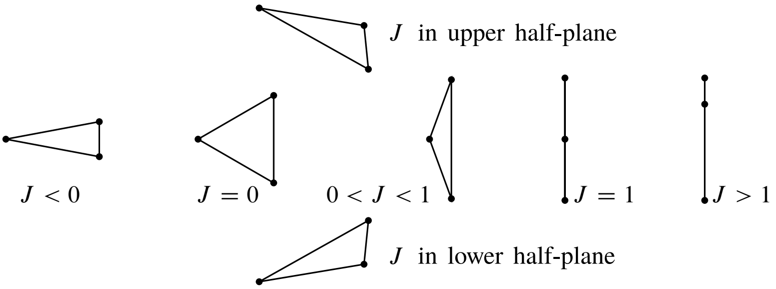


Figure 2
The $J$-invariant describes the shape of the (possibly degenerate) triangle in $\mathbb{C}$ with vertices $r_1, r_2, r_3$.

For real values of $J$, the triangle is isosceles if $J < 1$, but the three vertices lie on a straight line if $J \geq 1$. If we label the three edge lengths $|r_j - r_k|$ as $e_1 \leq e_2 \leq e_3$, then $J \not\in \mathbb{R}$ if and only if $e_1 < e_2 < e_3$ and $e_3 \neq e_1 + e_2$. In fact the corresponding edges lie in positive (or negative) cyclic order around the triangle according as $J$ lies in the upper (or lower) half-plane. For a sequence of curves, $|J|$ tends to infinity if and only if the ratio $e_3/e_1$ tends to infinity.

We can now give a precise description of the automorphism group (Compare Definition 2.3).

**Corollary 3.10.** *The automorphism group of any smooth complex cubic curve can be described by a split exact sequence*

$$1 \quad \to \quad N(\mathbb{P}^2, \mathcal{C}) \quad \to \quad \mathrm{Aut}(\mathbb{P}^2, \mathcal{C}) \quad \to \quad \mathrm{Aut}(\mathbb{P}^2, \mathcal{C}, \mathbf{p}_0) \quad \to \quad 1 \; .$$

*Here:*

$\mathbf{p}_0$ *can be any one of the nine flex points,*

$\mathrm{Aut}(\mathbb{P}^2, \mathcal{C}, \mathbf{p}_0)$ *is the subgroup of* $\mathrm{Aut}(\mathbb{P}^2, \mathcal{C})$ *consisting of all automorphisms which fix the point* $\mathbf{p}_0$*, and*

$N(\mathbb{P}^2, \mathcal{C}) \cong \mathbb{Z}/3 \oplus \mathbb{Z}/3$ *is the normal subgroup consisting of all automorphisms which have no fixed point on* $\mathcal{C}$*, together with the identity automorphism.*

*Furthermore,* $N$ *is a maximal abelian subgroup, and acts simply transitively on the set of nine flex points. The subgroup* $\mathrm{Aut}(\mathbb{P}^2, \mathcal{C}, \mathbf{p}_0)$ *is cyclic of order:*

**six** *if* $J(\mathcal{C}) = 0$*,*

**four** *if* $J(\mathcal{C}) = 1$*, but*

**two** *in all other cases.*

Thus the full automorphism group has order either 54, 36, or 18. Note that the exceptional cases $J=0$ and $J=1$ are precisely the cases where the "triangle" of Figure 2 has rotational symmetry of order three or two.

*Proof of Corollary* 3.10. The subgroup $N$ is normal since the property of acting without fixed points is invariant under inner automorphism. Since we know by Lemma 2.4 and Theorem 2.12 that $N$ acts simply transitively on the flex points, it follows that any automorphism can be expressed uniquely as the composition of an element of $N$ with an element of $\mathrm{Aut}(\mathbb{P}^2, \mathcal{C}, \mathbf{p}_0)$. To compute the latter group, using the standard normal form, take $\mathbf{p}_0$ to be the point $(0:1:0)$. According to Lemma 3.4, an automorphism fixing this point must have the form

$$(x:y:z) \;\mapsto\; (t^2x:t^3y:z), \quad \text{with} \quad a \mapsto t^4 a \quad \text{and} \quad b \mapsto t^6 b\ .$$

Thus when $a=0$ the coefficient $t$ can be any sixth root of unity, and when $b=0$ it can be any fourth root of unity, but otherwise it can only be $\pm 1$. (Expressed invariantly, the cyclic subgroup $\mathrm{Aut}(\mathbb{P}, \mathcal{C}, \mathbf{p}_0)$ acts on the tangent space to $\mathcal{C}$ at $\mathbf{p}_0$ by multiplication by a corresponding root of unity.) The conclusion follows. □

**From Hesse to standard normal form.** Since every cubic equation in Hesse normal form can be converted to one in the standard normal form (see the proof of Theorem 3.1), it follows that the invariant $J\big(\mathcal{C}(k)\big) \in \mathbb{C}$ can be computed as a function of the Hesse parameter $k$. In fact, since we can always multiply the parameter $k$ by a cube root of unity without changing the projective equivalence class, simply by dividing one of the coordinates by this root of unity, it follows that $J(\mathcal{C})$ can be computed as a function of $k^3 \in \mathbb{C}\smallsetminus\{1\}$. The computation is straightforward (if somewhat tedious), and yields the following result in our notation:

$$J\big(\mathcal{C}(k)\big) = \left(\frac{k(k^3+8)}{4(k^3-1)}\right)^3 . \tag{14}$$

(Compare [Fr], as well as [PP, Prop. 2.3].) It follows from this expression that the invariant $J\big(\mathcal{C}(k)\big)$ tends to infinity whenever $k^3$ tend to either infinity or $+1$. It also follows from this expression (or from Remark 3.6) that every rational value of $k$ corresponds to a rational value of $J$, or to $J=\infty$. (However, an irrational value of $k$ may correspond to a rational $J$. For example $k = 1 \pm \sqrt{3}$ yields $J=1$.)

One noteworthy property is the following. Let $\eta : \widehat{\mathbb{C}} \xrightarrow{\cong} \widehat{\mathbb{C}}$ be the Möbius involution

$$\eta(k) = \frac{k+2}{k-1}, \qquad \text{with} \qquad \eta\circ\eta(k) = k\ . \tag{15}$$

It will be convenient to use the abbreviated expression $J(k)$ for $J\big(\mathcal{C}(k)\big)$.

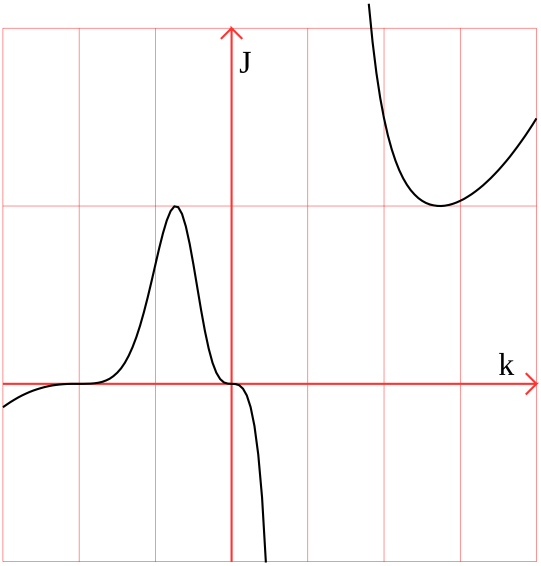


Figure 3

Graph of the map $k \mapsto J(\mathcal{C}(k))$ of equation (14) for real values of $k$, with $k \in [-3, 4]$ and $J \in [-1, 2]$. Note that every line $J =$ constant intersects the graph in exactly two points. As examples, for $J = 0$ we have $k = 0$ or $k = -2$, while for $J = 1$ we have $k = 1 \pm \sqrt{3}$. The graph is divided into two connected components: The component with $k < 1$ represents curves $\mathcal{C}(k)_{\mathbb{R}}$ which are connected, while the component with $k > 1$ represents curves with two connected components.

**Lemma 3.11.** *This function* $J(k) = J\big(\mathcal{C}(k)\big)$ *satisfies the identity*

$$J\big(\eta(k)\big) = J(k) \qquad \textit{for all} \qquad k \in \widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}.$$

In particular, it follows that the graph, shown in Figure 3, is invariant under the involution

$$(k, J) \quad \longleftrightarrow \quad \big(\eta(k),\, J\big),$$

which maps the region $k < 1$ to itself with fixed point $(1 - \sqrt{3},\, 1)$, and the region $k > 1$ to itself with fixed point $(1 + \sqrt{3},\, 1)$. (Note that both fixed points lie along the line $J = 1$.)

*First proof.* The equation $J\big(\eta(k)\big) = J(k)$ is an identity between two rational functions of degree twelve, which can be verified by direct computation. □

However, this argument gives no clue as to how to construct an actual projective equivalence between $\mathcal{C}(k)$ and $\mathcal{C}\big(\eta(k)\big)$. That can be remedied as follows.

*Second proof.* Let

$$\begin{aligned} X &= x + y + z \\ Y &= x + \gamma y + \overline{\gamma} z \\ Z &= x + \overline{\gamma} y + \gamma z \end{aligned}$$

where $\gamma = e^{2\pi i/3}$. Then it is not hard to check that

$$X^3 + Y^3 + Z^3 = 3\Big(x^3 + y^3 + z^3 \ + \ 6\,x\,y\,z\Big),$$

and that

$$X\,Y\,Z = x^3 + y^3 + z^3 \ - \ 3\,x\,y\,z.$$

Setting $k = (x^3 + y^3 + z^3)/(3\,x\,y\,z)$, it follows easily that

$$\frac{X^3 + Y^3 + Z^3}{3\,X\,Y\,Z} = \frac{k+2}{k-1},$$

and the conclusion follows. □

**Theorem 3.12.** *Let* $\Gamma$ *denote the group of Möbius transformations generated by the involution* $\boldsymbol{\eta}$ *and the rotation*

$$\boldsymbol{\rho}(k) = \gamma\,k.$$

*Then* $\Gamma$ *is equal to the twelve element* ***tetrahedral group****, consisting of all Möbius transformations from the Riemann sphere to itself which map the four point set* $\{1,\,\gamma,\,\overline{\gamma},\,\infty\}$ *to itself. Furthermore:*

(*1*) *Two Hesse curves* $\mathcal{C}(k)$ *and* $\mathcal{C}(k')$ *are projectively equivalent if and only if* $k' = \boldsymbol{\mu}(k)$ *for some* $\boldsymbol{\mu} \in \Gamma$.

(*2*) *The function* $k \mapsto J(k)$ *can be computed as*

$$J(k) = \frac{1}{64}\prod_{\boldsymbol{\mu}\in\Gamma}\boldsymbol{\mu}(k).$$

*Proof.* (Compare [AD].) Clearly $\boldsymbol{\eta} : 1 \leftrightarrow \infty$ under the involution $\boldsymbol{\eta}$, and it is not hard to check that $\boldsymbol{\eta} : \gamma \leftrightarrow \overline{\gamma}$. It then follows easily that $\Gamma$ can be identified with the group consisting of all even permutations of these four symbols.

To prove statement **(1)**, note that the quotient $\widehat{\mathbb{C}}\,/\,\Gamma$ is a Riemann surface, necessarily isomorphic to $\widehat{\mathbb{C}}$. Since the map $J : \widehat{\mathbb{C}} \to \widehat{\mathbb{C}}$ clearly has the property that $J \circ \boldsymbol{\mu} = J$ for every $\boldsymbol{\mu} \in \Gamma$, it follows that $J$ can be expressed as a composition

$$\begin{tikzcd} \widehat{\mathbb{C}} \arrow[r] \arrow[dr, "J"'] & \widehat{\mathbb{C}}/\Gamma \arrow[d, "h"] \\ & \widehat{\mathbb{C}}. \end{tikzcd}$$

Since both $J$ and the projection $\widehat{\mathbb{C}} \to \widehat{\mathbb{C}}/\Gamma$ have degree twelve, it follows that the holomorphic map $h$ has degree one, and hence is a conformal diffeomorphism. Since two curves $\mathcal{C}(k)$ and $\mathcal{C}(k')$ are projectively equivalent if and only if $J(k) = J(k')$, it follows that they are projectively equivalent if and only if $k$ and $k'$ have the same orbit under $\Gamma$.

To prove **(2)**, note that the function $k \mapsto \prod_{\boldsymbol{\mu}} \boldsymbol{\mu}(k)$ is also a rational map of degree twelve which is invariant under precomposition with any $\boldsymbol{\mu} \in \Gamma$. Furthermore, this function maps zero to zero and infinity to infinity, so it must be some constant multiple of $J$. To compute the precise constant, it is enough to understand one more example.

It is not hard to check[10] that the orbit of $1+\sqrt{3}$ consists of the following six points, each counted twice since $1+\sqrt{3}$ is a fixed point of $\boldsymbol{\eta}$.

$$1+\sqrt{3}, \quad (1+\sqrt{3})\gamma, \quad (1+\sqrt{3})\overline{\gamma}, \quad 1-\sqrt{3}, \quad (1-\sqrt{3})\gamma, \quad (1-\sqrt{3})\overline{\gamma}.$$

Since $(1+\sqrt{3})(1-\sqrt{3}) = -2$ and $\gamma\overline{\gamma} = 1$, the product $\prod_{\boldsymbol{\mu}} \boldsymbol{\mu}(1+\sqrt{3})$ is equal to $(-2)^6 = 64$. Comparing this with $J(1+\sqrt{3}) = 1$, the conclusion follows. □

## 4. Cubic curves as Riemann surfaces

**Theorem 4.1.** *Every smooth cubic curve is conformally diffeomorphic to a flat torus of the form $\mathbb{C}/\Omega$ where $\Omega$ is a* ***lattice*** *(that is, an additive subgroup generated by two complex numbers which are linearly independent over $\mathbb{R}$.) Here $\Omega$ is uniquely determined up to multiplication by a complex constant. Hence the shape of $\Omega$ (Definition 3.7) is a complete invariant for the conformal diffeomorphism class of $\mathcal{C}$.*

This will be an immediate consequence of two lemmas. The first lemma is based on methods introduced by Abel. (However Abel himself did not work in projective space or discuss algebraic curves. He simply studied integrals, for example of the form $\int dx/\sqrt{p(x)}$ where $p(x)$ is a polynomial.)

**Lemma 4.2.** *Every smooth cubic curve in $\mathbb{P}^2(\mathbb{C})$ possesses a holomorphic 1-form (= Abelian differential) which is well defined and nowhere zero. This 1-form is unique up to multiplication by a non-zero complex constant.*

*Proof.* We will use affine coordinates $(x : y : 1)$, and take the curve in the standard normal form $y^2 = x^3 + ax + b$, so that

[10] In particular, note that $\boldsymbol{\rho}^{-1} \circ \boldsymbol{\eta} \circ \boldsymbol{\rho}(1+\sqrt{3}) = 1-\sqrt{3}$. It is noteworthy that to pass between the two real points $1 \pm \sqrt{3}$ on the locus $J = 1$ we need to make use of a Möbius transformation with complex coefficients.

$$2\,y\,dy = (3\,x^2 + a)dx. \tag{16}$$

Consider the holomorphic 1-form[11] $dw$ which is defined by

$$dw = \frac{dx}{y} \qquad \text{whenever} \qquad y \neq 0,$$

and by

$$dw = \frac{2\,dy}{3\,x^2 + a} \qquad \text{whenever} \qquad 3\,x^2 + a \neq 0.$$

(It follows from Equation (16) that these two forms are equal when both are defined.) The two denominators cannot both be zero since the equations

$$\Phi_x = \Phi_y = 0$$

would imply that $\mathcal{C}$ is singular.) This form $dw$ is clearly well defined and non-zero at all points of $\mathcal{C}$ which lie within the affine plane. Since the intersection of $\mathcal{C}$ with the line at infinity is the single flex point $(0:1:0)$, it only remains to check what happens near this point. To do this, we will work with alternative affine plane in which $y = 1$, setting

$$x = X/Z \quad \text{and} \quad y = 1/Z \quad \text{so that} \quad (x:y:1) = (X:1:Z).$$

Using the equation

$$\Phi(X, 1, Z) = -Z + X^3 + aXZ^2 + bZ^3 = 0, \tag{17}$$

we see that $\Phi_X(0:1:0) = 0$ and $\Phi_Z(0:1:0) = -1$, so that $X$ can be used as a local uniformizing parameter on $\mathcal{C}$. In fact, we can express $Z$ locally as a function of $X$ of the form $Z = cX^n + O(X^{n+1})$, with $n \geq 2$ since $Z = 0$ is the tangent line. Substituting this expression for $Z$ in the right hand side of the equation $Z = X^3 + aXZ^2 + bZ^3$ it follows easily that $c = 1$ and $n = 3$, so that

$$Z = X^3 + O(X^5), \quad \text{and} \quad dZ = \big(3X^2 + O(X^4)\big)dX.$$

Now using the equation

$$dw = \frac{dx}{y} = \frac{d(X/Z)}{1/Z} = \frac{Z\,dX \,-\, X\,dZ}{Z}$$

it follows that

$$dw = \big(-2 \,+\, O(X^2)\big)\,dX.$$

Thus the holomorphic 1-form $dw$ is smooth and non-zero, even at the flex point $(0:1:0)$. Since any other holomorphic 1-form can be obtained by multiplying $dw$ by a holomorphic function from $\mathcal{C}$ to $\mathbb{C}$, which is necessarily constant since $\mathcal{C}$ is compact, this proves Lemma 4.2. □

[11] Caution: This notation is not intended to suggest that $dw$ is the total differential of a globally defined function. Of course we can integrate to find a function which is locally well defined up to an additive constant; but the integral is not well defined globally.

**Lemma 4.3.** *Let $\mathcal{C}$ be any compact Riemann surface which admits a nowhere zero holomorphic 1-form $\eta$. Then the set of integrals $\oint_\Lambda \eta \in \mathbb{C}$, where $\Lambda$ varies over all smooth closed loops in $\mathcal{C}$, forms a lattice $\Omega \subset \mathbb{C}$, and $\mathcal{C}$ is conformally diffeomorphic to the quotient Riemann surface $\mathbb{C}/\Omega$.*

*Proof.* (Compare [Don, p. 84].) Choose a base point $\mathbf{p}_0 \in \mathcal{C}$. Then the universal covering space $\widetilde{\mathcal{C}}$ can be described as the set of all pairs $\big(\mathbf{p}, \{P\}\big)$ where $\mathbf{p}$ can be any point of $\mathcal{C}$ and $\{P\}$ is any homotopy class of smooth paths from $\mathbf{p}_0$ to $\mathbf{p}$. Given any such pair, we can integrate along any $P \in \{P\}$ to obtain a complex number $w = \int_P \eta \in \mathbb{C}$ which does not depend on the choice of $P$ within its homotopy class. In other words, we have a well defined mapping

$$\big(\mathbf{p}\,, \{P\}\big) \;\mapsto w = \int_P \eta \qquad \text{from} \quad \widetilde{\mathcal{C}} \quad \text{to} \quad \mathbb{C}\ . \tag{18}$$

Further, the total differential $dw$ of this function $w$ is just the 1-form $\eta$, lifted to the universal covering.

Using the flat Riemannian metric $|dw|^2$, we see that this function (18) is a conformal isometry from $\widetilde{\mathcal{C}}$ onto the complex numbers. In fact the inverse map from $\mathbb{C}$ to $\widetilde{\mathcal{C}}$ sends each straight line from the origin in $\mathbb{C}$ to a corresponding geodesic in $\widetilde{\mathcal{C}}$.

Now suppose that we have two different paths $P_1$ and $P_2$ from $\mathbf{p}_0$ to $\mathbf{p}$, yielding two complex numbers $w_1$ and $w_2$. Then the difference can be expressed as

$$w_1 - w_2 = \int_\Lambda \eta,$$

where $\Lambda$ is the closed loop obtained by following $P_1$ from $\mathbf{p}_0$ to $\mathbf{p}$, and then following $P_2$ back to $\mathbf{p}_0$. Conversely, given any closed loop $\Lambda$ from $\mathbf{p}_0$ to itself, we can first follow $P_1$ and then follow $\Lambda$ to obtain a new path $P_2$ from $\mathbf{p}_0$ to $\mathbf{p}$. This proves that two points in $\widetilde{\mathcal{C}}$ map to the same point of $\mathcal{C}$ if and only if the difference between their images in $\mathbb{C}$ differ by an element of the additive group $\Omega \subset \mathbb{C}$.

Since the map from $\widetilde{\mathcal{C}}$ to $\mathcal{C}$ is a local diffeomorphism, it follows that $\Omega$ must be a discrete additive subgroup: that is, it cannot contain non-zero elements arbitrarily close to zero. Furthermore, since the quotient $\mathbb{C}/\Omega \cong \mathcal{C}$ is compact, $\Omega$ must contain two linearly independent elements. This proves Lemma 4.3; and Theorem 4.1 then follows easily. □

The converse assertion, that every flat torus $\mathbb{T} = \mathbb{C}/\Omega$ is conformally diffeomorphic to a smooth cubic curve, is due to Weierstrass ([Wei1], [Wei2]), and arose from his study of doubly periodic functions. Since this result is widely known (see for example [La, Sec.2]), we will give only a brief summary.

For any lattice $\Omega \subset \mathbb{C}$ the Weierstrass $\wp$-function is the unique holomorphic $\Omega$-periodic map from $\mathbb{C} \smallsetminus \Omega$ to $\mathbb{C}$ which has a pole of the form

$$\wp(w) = 1/w^2 + o(1) \qquad \text{as} \qquad w \to 0.$$

This satisfies a differential equation of the form

$$\big(\wp'(w)\big)^2 = 4\wp(w)^3 - g_2\wp(w) - g_3,$$

where the complex constants $g_2$ and $g_3$ can be computed from the lattice $\Omega$. In fact,

$$g_2 = 60\sum_{\omega\neq 0}\frac{1}{\omega^4} \quad \text{and} \quad g_3 = 140\sum_{\omega\neq 0}\frac{1}{\omega^6},$$

where $\omega$ ranges over all non-zero lattice elements. (Compare [Ser, p.83-84].) Setting

$$(X : Y : Z) = (\wp(w) : \wp'(w) : 1),$$

this yields a conformal diffeomorphism[12] from the torus $\mathbb{T} = \mathbb{C}/\Omega$ onto the cubic curve

$$Y^2 = 4\,X^3 - g_2X - g_3.$$

This can easily be transformed into our standard normal form by setting

$$Y = 2y \quad \text{and} \quad X = x, \qquad \text{with} \qquad g_2 = -4a \quad \text{and} \quad g_3 = -4b.$$

Felix Klein showed that the $J$-invariant can be computed as a holomorphic function of the lattice parameter $\tau$, where $\Omega = \mathbb{Z} \oplus \tau\mathbb{Z}$ with $\mathrm{Im}(\tau) > 0$. See for example [Ser, p.90].

**Corollary 4.4.** *The group* $\mathrm{Aut}(\mathcal{C}) \cong \mathrm{Aut}(\mathbb{T})$ *of conformal automorphisms of the curve* $\mathcal{C} \cong \mathbb{T}$ *can be described by a split exact sequence*

$$1 \;\to\; N(\mathbb{T}) \;\to\; \mathrm{Aut}(\mathbb{T}) \;\to\; \mathrm{Aut}(\mathbb{T}, 0) \;\to\; 1,$$

*where the normal subgroup* $N(\mathbb{T}) \cong \mathbb{T}$ *of automorphisms without fixed point can be identified with the group of translations of* $\mathbb{T} \cong \mathbb{C}/\Omega$*, and where the finite cyclic subgroup* $\mathrm{Aut}(\mathbb{T}, 0) \cong \mathrm{Aut}(\mathcal{C}, \mathbf{p}_0)$ *is naturally isomorphic to the group* $\mathrm{Aut}(\mathbb{P}^2, \mathcal{C}, \mathbf{p}_0)$ *of Corollary 3.10.*

[12] To check differentiability near $w = 0$, we can set $\wp(w) = w^{-2} + \epsilon(w)$ where $\epsilon(w)$ is holomorphic. Then $w$ maps to

$$(\wp : \wp' : 1) = \big(w^{-2} + \epsilon(w) : -2w^{-3} + \epsilon'(w) : 1\big) = \big(w + w^3\epsilon(w) : -2 + w^3\epsilon'(w) : w^3\big),$$

clearly yielding a local conformal diffeomorphism.

*Proof.* Note first that the derivative of any conformal automorphism of $\mathbb{T}$ is a holomorphic function from the compact surface $\mathbb{T}$ to $\mathbb{C}$, and hence must be constant. Hence any automorphism must be linear. But the only linear maps without fixed points are translations. Further details are easily supplied. □

**Corollary 4.5.** *Two smooth cubic curves are projectively equivalent if and only if they are conformally diffeomorphic. A given conformal diffeomorphism extends to an automorphism of* $\mathbb{P}^2(\mathbb{C})$ *if and only if it maps flex points to flex points.*

*Proof.* If the two curves are projectively equivalent, then they are certainly conformally diffeomorphic. Conversely, if they are conformally diffeomorphic, then it follows from the discussion above that they have a common $J$-invariant, hence by Corollary 3.5 they are projectively equivalent. Any projective equivalence between two curves certainly sends flex points to flex points. Conversely, given any conformal equivalence from $\mathcal{C}_1$ to $\mathcal{C}_2$ which sends flex points to flex points, we can choose a projective equivalence from $\mathcal{C}_2$ to $\mathcal{C}_1$. The composition will then be a conformal automorphism of $\mathcal{C}_1$ which sends flex points to flex points. Using Corollary 4.4, it is then not difficult to check that this composition is a projective equivalence from $\mathcal{C}_1$ to itself, and the conclusion follows. □

**Remark 4.6** (Birational Maps). In place of conformal diffeomorphisms, we could equally well work with the purely algebraic concept of birational maps. Let $\mathbf{f} = (f_1 : f_2 : f_3)$ be a non-zero triple of homogeneous polynomial maps $\mathbb{C}^3 \to \mathbb{C}$ of the same degree, well defined up to simultaneous multiplication by a non-zero complex constant. Let $\mathcal{I}(\mathbf{f}) \subset \mathbb{P}^2(\mathbb{C})$ be the locus of common zeros: $f_1 = f_2 = f_3 = 0$. Then the function $\mathbf{f} : \mathbb{P}^2(\mathbb{C}) \smallsetminus \mathcal{I}(\mathbf{f}) \to \mathbb{P}^2(\mathbb{C})$ defined by the formula

$$(x : y : z) \mapsto \big(f_1(x, y, z) : f_2(x, y, z) : f_3(x, y, z)\big)$$

is called a *rational map* of $\mathbb{P}^2(\mathbb{C})$.

It will be convenient to use the phrase *almost everywhere* to mean “except on a finite subset”. If $\mathcal{C}$ is a curve in projective space such that the intersection $\mathcal{C} \cap \mathcal{I}(\mathbf{f})$ is finite, and if the image $\mathbf{f}\big(\mathcal{C} \smallsetminus \mathcal{I}(\mathbf{f})\big)$ is contained in a curve $\mathcal{C}'$, then we obtain an almost everywhere defined map from $\mathcal{C}$ to $\mathcal{C}'$. Two such almost everywhere defined maps will be called *equivalent* if they agree almost everywhere. An equivalence class of such maps will be called a *rational map* from $\mathcal{C}$ to $\mathcal{C}'$. If a rational map has an inverse, so that the composition is the identity map almost everywhere, then it is called a *birational map* from $\mathcal{C}$ to $\mathcal{C}'$. Given a birational map, there are finite subsets $S \subset \mathcal{C}$ and $S' \subset \mathcal{C}'$ so that $\mathcal{C} \smallsetminus S$ maps to $\mathcal{C}' \smallsetminus S'$ by a conformal diffeomorphism. Since the “singularities” (as the word is used in complex function theory) at the points of $S$ are clearly removable, it follows that every birational map between smooth curves extends to a uniquely defined conformal diffeomorphism. In particular, the birational map can be assigned a unique well defined value at every point.

If we combine this discussion with Nagell's Theorem, as described in Remark 3.2, then we obtain the following.

**Corollary 4.7.** *Every conformal diffeomorphism between smooth cubic curves is birational. Hence the group of all birational maps from a smooth cubic $\mathcal{C}$ to itself can be identified with the Lie group* $\mathrm{Aut}(\mathcal{C})$ *consisting of all conformal automorphisms of* $\mathcal{C}$.

*Proof.* First note that every projective equivalence is birational. From the discussion above, we see that every birational map is a conformal diffeomorphism.

Let $f:\mathcal{C}\to\mathcal{C}'$ be a conformal diffeomorphism between smooth cubic curves, and let $\mathbf{p}\in\mathcal{C}$ be a flex point. By Nagell's Theorem there is a smooth curve $\mathcal{C}''$ and a birational map $g:\mathcal{C}'\to\mathcal{C}''$ taking $f(\mathbf{p})$ to a flex point $\mathbf{p}''\in\mathcal{C}''$. By Corollary 4.5 there exists a projective equivalence $h:\mathcal{C}''\to\mathcal{C}$, and by Corollary 3.10 we may choose $h$ so that it maps $\mathbf{p}''$ to $\mathbf{p}$. Since the composition $h\circ g\circ f$ maps $\mathbf{p}$ to itself, it follows by Corollary 3.10 that this composition is a projective equivalence. Since $g$, $h$, and $h\circ g\circ f$ are all birational equivalences, it follows that $f$ is also. □

**Remark 4.8.** One curious invariant of the lattice $\Omega$ is the tiling of the complex plane by *Voronoi cells* $V_\omega=\omega+V_0$, where $\omega$ varies over $\Omega$, and where $V_0=V_0(\Omega)$ is the compact convex polygon consisting of all $z\in\mathbb{C}$ such that

$$|z|=\min_{\omega\in\Omega}|z-\omega|.$$

This polygon $V_0$ is a canonically defined fundamental domain for the additive action of $\Omega$ on $\mathbb{C}$; and is a complete invariant for $\Omega$, since $\Omega$ is the additive group generated by the reflections of zero in the edges of $V_0$. The shape of $V_0$ is evidently a complete invariant for the conformal diffeomorphism class of $\mathcal{C}\cong\mathbb{T}$ (where two polygons centered at the origin have the same "shape" if a complex linear automorphism maps one to the other). In particular, the group $\mathrm{Aut}(\mathbb{T},0)$ can be identified with the group of rotational symmetries of $V_0$. This has order 6 if $V_0$ is a regular hexagon (with $J=0$), order 4 if $V_0$ is a square (with $J=1$), and order 2 otherwise. In most cases $V_0$ is a non-regular hexagon (as in Figure 4). However, it is a rectangle if $J$ is real with $J>1$.

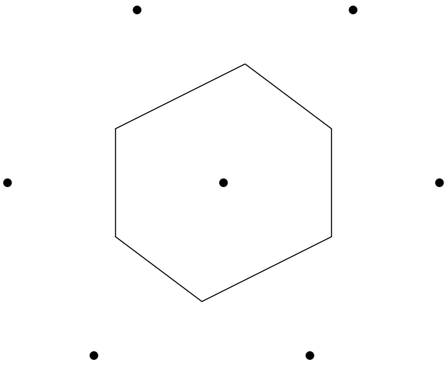


FIGURE 4
Voronoi hexagon for the lattice $\mathbb{Z} \oplus \tau\mathbb{Z}$ with $\tau = (3+4i)/5$. The Voronoi polygon for any lattice has 180° rotational symmetry. In this example, since the lattice has two generators of equal length, it also has an orientation reversing symmetry, which implies that the $J$-invariant is real.

## 5. The chord-tangent map and additive group structure

We first discuss the chord-tangent map. Let $\mathcal{C} \subset \mathbb{P}^2(\mathbb{C})$ be a smooth cubic curve. Recall that an arbitrary line $L \subset \mathbb{P}^2$ intersects $\mathcal{C}$ in exactly three points, counted with multiplicity. It will be convenient to call an unordered list $(\mathbf{p},\, \mathbf{q},\, \mathbf{r})$ of three (not necessarily distinct) points of $\mathcal{C}$ a *collinear triple* if it can be obtained in this way, indicating multiplicity by duplication.

**Definition 5.1.** The correspondence $(\mathbf{p},\, \mathbf{q}) \mapsto \mathbf{r}$, where $(\mathbf{p}, \mathbf{q}, \mathbf{r})$ is any collinear triple, will be called the *chord-tangent map* from $\mathcal{C} \times \mathcal{C}$ to $\mathcal{C}$, and will be denoted by

$$(\mathbf{p},\, \mathbf{q}) \quad \mapsto \quad \mathbf{p} * \mathbf{q}\ . \tag{19}$$

Note that the equation $\mathbf{p} * \mathbf{q} = \mathbf{r}$ is invariant under any permutation of $\mathbf{p}$, $\mathbf{q}$, $\mathbf{r}$, and simply means that $(\mathbf{p},\, \mathbf{q},\, \mathbf{r})$ is a collinear triple.

For example, if $\mathbf{p} = \mathbf{q} \neq \mathbf{r}$, then the equation $\mathbf{p} * \mathbf{p} = \mathbf{r}$ means that $(\mathbf{p},\, \mathbf{p},\, \mathbf{r})$ is a collinear triple, and hence that the tangent line to $\mathcal{C}$ at $\mathbf{p}$ also intersects the curve $\mathcal{C}$ at the point $\mathbf{r}$.

**Lemma 5.2.** *For any smooth complex cubic $\mathcal{C}$, this chord-tangent map*

$$(\mathbf{p},\, \mathbf{q}) \to \mathbf{p} * \mathbf{q}$$

*is holomorphic as a map from $\mathcal{C} \times \mathcal{C}$ to $\mathcal{C}$.*

*Proof.* It is first necessary to show that the line $L$ determined by two points $\mathbf{p}$ and $\mathbf{q}$ in $\mathcal{C}$ depends holomorphically on the pair $(\mathbf{p},\,\mathbf{q})$. This is clear if $\mathbf{p}\ne\mathbf{q}$, but we must also consider the limiting case as $\mathbf{p}$ and $\mathbf{q}$ tend to a common limit. Using affine coordinates $(x,\,y,\,1)$, and assuming that the slope $s$ is finite, so that $L$ is defined by an equation $y=sx+c$, it clearly suffices to prove that $s$ depends holomorphically on $\mathbf{p}$ and $\mathbf{q}$ as $\mathbf{p}$ and $\mathbf{q}$ tend to a common point. Describing the curve locally by a holomorphic function $y=f(x)$, the slope of the line between $\big(x_1,\,f(x_1)\big)$ and $\big(x_2,\,f(x_2)\big)$ is defined by

$$s(x_1,\,x_2)=\begin{cases}\dfrac{f(x_1)-f(x_2)}{x_1-x_2} & \text{if}\quad x_1\ne x_2\,,\quad\text{but}\\ f'(x) & \text{if}\quad x_1=x_2=x.\end{cases}$$

A standard power series argument shows that $s$ is holomorphic as a function of two variables.

Let $\Phi(x,y,1)=0$ be the defining equation for the affine curve. Assuming that we have chosen coordinates so that the point $\mathbf{r}=\mathbf{p}*\mathbf{q}$ also belongs to the affine plane, the function $\Phi(x,y,1)$ restricted to the line $y=sx+c$ determined by $\mathbf{p}$ and $\mathbf{q}$ can be expressed as a cubic polynomial

$$\Phi|_L=c_0x^3+c_1x^2+c_2x+c_3\qquad\text{with}\qquad c_0\ne 0,$$

where the coefficients $c_j$ depend holomorphically on $\mathbf{p}$ and $\mathbf{q}$. Factoring this polynomial as $c_0(x-p)(x-q)(x-r)$, we have $p+q+r=-c_1/c_0$. Therefore $r=-p-q-c_1/c_0$ also depends holomorphically on $\mathbf{p}$ and $\mathbf{q}$. Thus the $x$-coordinate of the required point $\mathbf{r}=\mathbf{p}*\mathbf{q}\in L$ varies holomorphically, so $\mathbf{r}$ does also. □

**Remark 5.3.** As in §3, it is interesting to see what happens over an arbitrary subfield $\mathbb{F}\subset\mathbb{C}$ Assuming that $\mathcal{C}$ is defined by equations with coefficients in $\mathbb{F}$, recall that $\mathcal{C}_{\mathbb{F}}$ is defined to be the intersection $\mathcal{C}\cap\mathbb{P}^2(\mathbb{F})$. If $(\mathbf{p},\,\mathbf{q},\,\mathbf{r})$ is a collinear triple for $\mathcal{C}$, with $\mathbf{p}$ and $\mathbf{q}$ in $\mathcal{C}_{\mathbb{F}}$, then it is not hard to check that $\mathbf{r}\in\mathcal{C}_{\mathbb{F}}$ also[13]. Thus the chord-tangent map $(\mathbf{p},\,\mathbf{q})\mapsto\mathbf{p}*\mathbf{q}$ is well defined as a map from $\mathcal{C}_{\mathbb{F}}\times\mathcal{C}_{\mathbb{F}}$ to $\mathcal{C}_{\mathbb{F}}$.

In the case that $\mathbb{F}$ is the field $\mathbb{Q}$ of rational numbers, the map $\mathbf{p}\mapsto\mathbf{p}*\mathbf{p}$ was used by Diophantus of Alexandria in the third century to construct new points of $\mathcal{C}_{\mathbb{Q}}$ out of known ones. (For examples, see [Cas, pp. 24–25].)

Next we will use the chord-tangent map to describe the additive group structure of a smooth cubic curve.

[13] If a polynomial equation has coefficients in $\mathbb{F}$, note that then sum of its roots is also in $\mathbb{F}$.

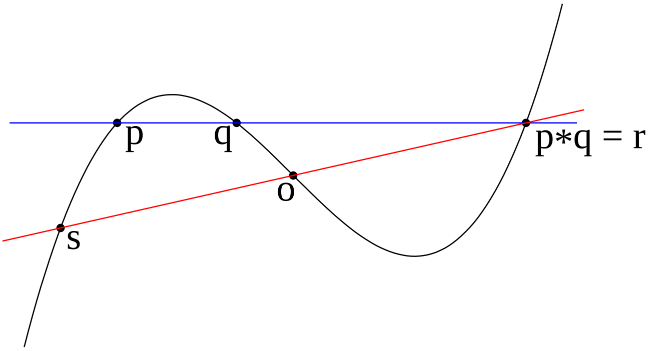


FIGURE 5
Constructing the sum $\mathbf{p}+\mathbf{q}=\mathbf{s}$

**Lemma 5.4.** *Let* $\mathbf{o}$ *be an arbitrarily chosen base point*[14] *in the smooth cubic curve* $\mathcal{C}\subset\mathbb{P}^2(\mathbb{C})$. *Then* $\mathcal{C}$ *admits one and only one additive group structure with the following two properties:*

(1) *The base point* $\mathbf{o}$ *is the zero element, so that* $\mathbf{o}+\mathbf{p}=\mathbf{p}$ *for any* $\mathbf{p}\in\mathcal{C}$.

(2) *The triple* $(\mathbf{p},\mathbf{q},\mathbf{r})$ *is collinear (as defined above) if and only if the sum* $\mathbf{p}+\mathbf{q}+\mathbf{r}$ *takes a constant value which depends only on the choice of* $\mathbf{o}$.

*Proof of uniqueness.* Assume that such a group structure exists. For any $\mathbf{p}$ and $\mathbf{q}$, let $\mathbf{r}=\mathbf{p}*\mathbf{q}$ and let $\mathbf{s}=\mathbf{r}*\mathbf{o}$ as in Figure 5, using the notation (19). Then by Property (2) we have the identity

$$\mathbf{p}+\mathbf{q}+\mathbf{r}=\mathbf{r}+\mathbf{o}+\mathbf{s}.$$

Canceling the $\mathbf{r}$'s and using Property (1), it follows that $\mathbf{p}+\mathbf{q}=\mathbf{s}$, or in other words

$$\mathbf{p}+\mathbf{q}=(\mathbf{p}*\mathbf{q})*\mathbf{o}. \tag{20}$$

This proves uniqueness. □

**Remark 5.5.** The constant $\mathbf{p}+\mathbf{q}+\mathbf{r}$ in Property **(2)** is necessarily equal to $\mathbf{o}*\mathbf{o}$, as we see by considering the collinear triple $\mathbf{o},\,\mathbf{o},\,\mathbf{o}*\mathbf{o}$. Similarly, since $\mathbf{p},\ \mathbf{o}*\mathbf{o},\ (\mathbf{o}*\mathbf{o})*\mathbf{p}$ forms a collinear triple, we see that the additive inverse $-\mathbf{p}$ is equal to $(\mathbf{o}*\mathbf{o})*\mathbf{p}$.

[14] The term *elliptic curve* is often reserved for a smooth cubic curve together with a specified base point.

*Proof of existence.* Define the sum operation by the formula (20), setting $\mathbf{r} = \mathbf{p}*\mathbf{q}$ and $\mathbf{p}+\mathbf{q} = \mathbf{r}*\mathbf{o}$ as illustrated by Figure 5. Note the identity $(\mathbf{p}*\mathbf{q})*\mathbf{q} = \mathbf{p}$ for all $\mathbf{p}$ and $\mathbf{q}$. In particular, taking $\mathbf{q} = \mathbf{o}$, we have

$$\mathbf{p}+\mathbf{o} = (\mathbf{p}*\mathbf{o})*\mathbf{o} = \mathbf{p}$$

for all $\mathbf{p}$. Thus $\mathbf{o}$ is indeed a zero element for the sum operation.

For any collinear triple $(\mathbf{p}, \mathbf{q}, \mathbf{r})$, as in the diagram, we can compute the sum

$$(\mathbf{p}+\mathbf{q})+\mathbf{r} = \mathbf{s}+\mathbf{r} = (\mathbf{s}*\mathbf{r})*\mathbf{o} \ \ = \mathbf{o}*\mathbf{o},$$

which is constant, as required.

This sum operation is clearly commutative. Over a general field, the proof of associativity is somewhat tricky. (Compare [Cas].) However, in the complex case it is quite easy: First note that for fixed $\mathbf{q} \neq \mathbf{o}$ the mapping $\mathbf{p} \mapsto \mathbf{p}+\mathbf{q}$ from $\mathcal{C}$ to itself has no fixed points. In fact, with $\mathbf{r}*\mathbf{p} = \mathbf{q}$ and $\mathbf{r}*(\mathbf{p}+\mathbf{q}) = \mathbf{o}$ as in Figure 5, the equation $\mathbf{p} = \mathbf{p}+\mathbf{q}$ would imply that $\mathbf{q} = \mathbf{o}$.

Now choose a conformal diffeomorphism $\psi : \mathcal{C} \xrightarrow{\cong} \mathbb{T}$ to the appropriate torus $\mathbb{T} = \mathbb{C}/\Omega$, normalized by the requirement that $\psi(\mathbf{o}) = 0$. Then translation by $\mathbf{q} \neq \mathbf{o}$ on $\mathcal{C}$ corresponds to a fixed point free conformal diffeomorphism from $\mathbb{T}$ to itself which maps zero to $\psi(\mathbf{q})$. But the only such isomorphism is the translation by $\psi(\mathbf{q})$. It follows easily that the transformation $\psi$ is not only a conformal diffeomorphism but also preserves the sum operation. Therefore the sum is associative; and $\psi$ is an isomorphism of additive groups. □

**Remark 5.6.** If $\mathbf{o} \in \mathcal{C}_{\mathbb{F}}$ for some subfield $\mathbb{F} \subset \mathbb{C}$, then it follows that $\mathcal{C}_{\mathbb{F}}$ is a subgroup of $\mathcal{C}$. This construction is particularly convenient when $\mathcal{C}_{\mathbb{F}}$ has a flex point. In this case, we can choose a flex point as base point $\mathbf{o}$, so that $\mathbf{o}*\mathbf{o} = \mathbf{o}$, and so that $\mathbf{p}+\mathbf{q}+\mathbf{r} = \mathbf{o}$ for any collinear triple. As an example, with this choice the classical "tangent process" $\mathbf{p} \mapsto \mathbf{p}*\mathbf{p}$ is given by the formula

$$\mathbf{p} \quad \mapsto \quad -2\mathbf{p}.$$

One important consequence is that: *the line joining any two distinct flex points must contain a third flex point.* (Compare Figure 6.) With this choice of base point, the flex points are precisely the elements of order three, satisfying $\mathbf{p}+\mathbf{p}+\mathbf{p} = \mathbf{o}$ within the additive group. In the complex case, this additive group of flex points has order nine, and hence, is isomorphic to $\mathbb{Z}/3 \oplus \mathbb{Z}/3$.

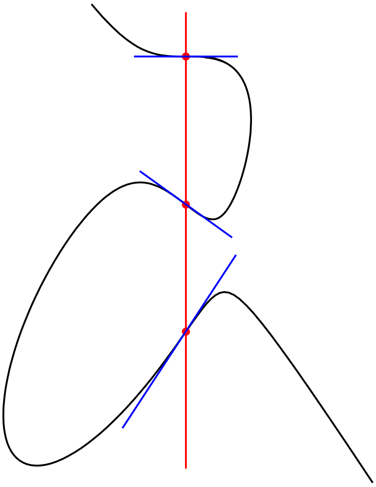


FIGURE 6

The line between two distinct flex points always intersects $C$ in a third flex point.

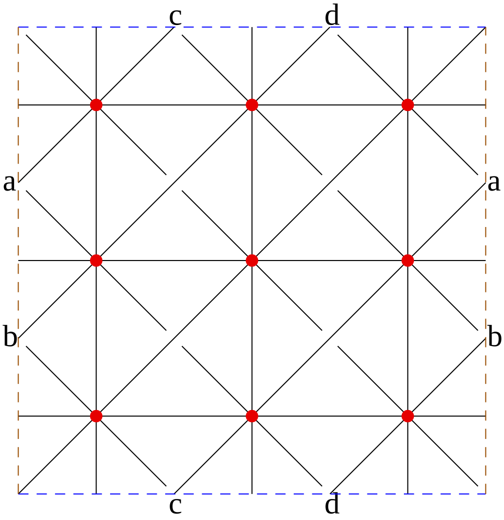


FIGURE 7

A schematic picture of the Hesse configuration consisting of nine flex points together with the twelve lines joining them, placed on a square with opposite sides identified. (Compare [Hes2, Lehrsatz 12], as well as [AD].) This configuration has the nice property that any two points determine a line and any two lines determine a point. This configuration cannot be realized by straight lines in $\mathbb{R}^3$, but can be more or less realized on a flat torus, as illustrated.

**Remark 5.7.** It follows easily that every smooth complex cubic contains a configuration of nine flex points which joined by twelve lines, where every two points determine a line and every two lines determine a point. This "*Hesse configuration*" can never be realized by real[15] straight lines, even in a high dimensional real space. However, it can almost be realized on a flat torus, as illustrated schematically in Figure 7.

## 6. Real cubic curves

This section is concerned with cubic curves $\mathcal{C}_{\mathbb{R}} \subset \mathbb{P}^2(\mathbb{R})$ defined by equations $\Phi(x, y, z) = 0$ with real coefficients. We will describe the curve $\mathcal{C}_{\mathbb{R}}$ as *smooth and irreducible* if the locus $\mathcal{C}_{\mathbb{R}}$ itself contains no singular points and contains no line.[16] *This is equivalent to the requirement that the associated full complex locus $\mathcal{C} \subset \mathbb{P}^2(\mathbb{C})$ must have no singular points.* In fact, if $\mathcal{C}$ has just one singular point, then it must be invariant under the complex conjugation map $(x : y : z) \leftrightarrow (\overline{x} : \overline{y} : \overline{z})$, and hence must belong to $\mathcal{C}_{\mathbb{R}}$. If there are two complex conjugate singular points, then the complex line joining them must have intersection multiplicity at least two with each point, hence this entire line must be contained in the curve $\mathcal{C}$. Since this line is self-conjugate, its intersection with $\mathbb{P}^2(\mathbb{R})$ will be a line in $\mathcal{C}_{\mathbb{R}}$.

The problem of classifying real cubic curves was studied already by Isaac Newton (but in the affine plane; see [New] and compare [BK, p. 284]). In general, the projective classification of real curves is parallel to the complex classification, however there are important differences. In looking at pictures of real cubic curves, it is important to remember that the real projective plane is a non-orientable manifold, and that every real cubic curve has a non-orientable neighborhood, which can never be completely pictured within an affine plane (Remark 6.6).

**Lemma 6.1.** *Every smooth irreducible real cubic curve contains a flex point.*

*Proof of Lemma 6.1.* Since the full complex curve $\mathcal{C}$ is smooth, it has nine flex points. The complex conjugation map from $\mathcal{C}$ to itself, with fixed point set $\mathcal{C}_{\mathbb{R}}$, must permute these nine points. Since it is an involution, it must fix at least one of them. □

[15] Remember that three generic points on a complex line lie on a real circle, not on a real line.

[16] Thus we do not allow examples such as $\Phi(x, y, z) = x(x^2 + y^2 + z^2)$. In this example, the real locus is just a non-singular line $x = 0$; but the complex locus has singular points at $(0 : \pm i : 1)$ where the two irreducible components intersect.

Thus it follows from Theorem 3.1 that we can put $\mathcal{C}_{\mathbb{R}}$ into the standard form

$$y^2 = x^3 + ax + b$$

by a real projective transformation. In particular, it follows that the invariant $J(\mathcal{C}_{\mathbb{R}}) = 4a^3/\big(4a^3 + 27b^2\big)$ is a real number.

**Lemma 6.2.** *For each $J \in \mathbb{R}$ there are two essentially different smooth irreducible real cubic curves. A complete invariant for smooth real curves in this normal form, up to real projective equivalence, is provided by:*

- *this invariant $J(\mathcal{C}_{\mathbb{R}})$ together with*
- *the sign of $b$ if $b \neq 0$, or*
- *the sign of $a$ if $b = 0$.*

(Note that $a$ and $b$ cannot both be zero since $\mathcal{C}_{\mathbb{R}}$ is smooth.)

*Proof.* According to Lemma 3.4, the only allowable transformations replace the pair of coefficients $(a, b)$ by $(t^4 a, t^6 b)$ for some non-zero real number $t$. Since $t^4 > 0$ and $t^6 > 0$, the signs of $a$ and $b$ are both invariants. However, if we are given both $b$ and $J$ then we can solve uniquely for $a^3$, provided that $b \neq 0$, so the sign of $a$ is uniquely determined. The conclusion then follows easily. □

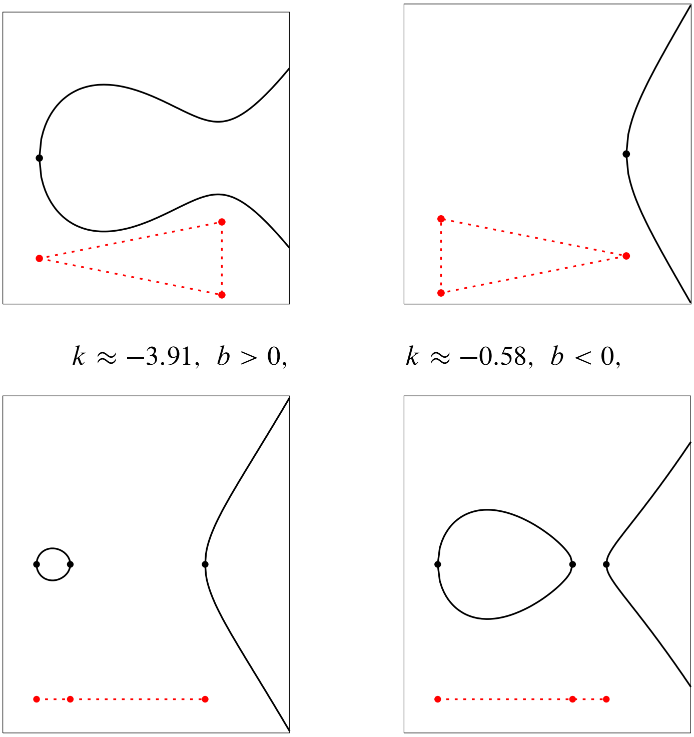
More geometrically, if the transformation

$$x \mapsto t^2 x\,, \quad y \mapsto t^3, \quad a \mapsto t^4 a\,, \quad b \mapsto t^6 b$$

is to change the sign of $b$ without changing $a$, then we must have $t^2 = -1$. Thus we must also change the sign of $x$. In particular, the associated triangle in the complex $x$-plane will be rotated by $180°$. But we we must also multiply $y$ by $\sqrt{-1}$, which makes a drastic change in the real curve. Compare Figures 2 and 8. Similarly, a change in the sign of $a$ corresponds to a $90°$ rotation of the complex $x$-plane.

Now compare Figure 3. This graph shows that each real $J$ corresponds to two possible values of the Hesse parameter $k$ (although the case $J = 1 \Leftrightarrow b = 0$ seems quite different from the other cases). For $J \neq 1$ the two distinct real values of $k$ are related by the involution $k \leftrightarrow \eta(k)$ of equation (15). In fact, we have the following statement.

**Theorem 6.3.** *Every smooth real cubic curve $\mathcal{C}_{\mathbb{R}}$ is real projectively equivalent to the real Hesse curve $\mathcal{C}(k)_{\mathbb{R}}$ for one and only one real $k \neq 1$. This curve $\mathcal{C}(k)_{\mathbb{R}}$ is connected if $k < 1$, and has two components if $k > 1$.*



$k \approx -3.91, \;\; b > 0,$ $k \approx -0.58, \;\; b < 0,$

$k \approx 1.63, \;\; b < 0,$ $k \approx 5.75, \;\; b > 0.$

Figure 8

Examples of pairs of distinct real curves in standard normal form which have the same $J$ invariant, giving the corresponding value of the Hesse $k$ invariant. (See Theorem 6.3.) The curve in the real $(x, y)$-plane is shown in solid curves, and the corresponding triangle in the complex $x$-plane is shown below in dotted lines. For the two top figures we have $J = -.583$, and for the bottom figures, $J = 3.43$.

To begin the proof, note that $\mathcal{C}_{\mathbb{R}}(k)$ is smooth if and only if $k \neq 1$. (Compare Lemma 2.2.)

**Lemma 6.4.** *For $k \neq 1$, putting this curve into the standard normal form $y^2 = x^3 + ax + b$, we have $b < 0$ if and only if*

$$1 - \sqrt{3} \;<\; k \;<\; 1 + \sqrt{3},$$

*and $b = 0$ if and only if $k = 1 \pm \sqrt{3}$, with $b > 0$ otherwise.*

*Proof.* Note first that $J = 1$, or equivalently $b = 0$, if and only if $k = 1 \pm \sqrt{3}$. (Compare Figure 3, together with the accompanying discussion.) The two extremal points $k = 1 \pm \sqrt{3}$, together with the separating value $k = 1$, cut the real line into four subintervals such that $J \neq 1 \Leftrightarrow b \neq 0$ on each subinterval. Thus it is enough to check one example on each subinterval, as shown for example in Figure 8. □

**Note.** In the case $k < 1$ with $\mathcal{C}$ connected, a pair of test examples which is even easier to work with is the following: The Hesse curve $\mathcal{C}(-2)_{\mathbb{R}}$ is projectively equivalent to the curve $y^2 = x^3 + x$ in standard form, while $\mathcal{C}(0)_{\mathbb{R}}$ is projectively equivalent to $y^2 = x^3 - x$. (These two examples, with $k \in (-\infty, 1-\sqrt{3})$ and $k \in (1-\sqrt{3}, 1)$ respectively, both correspond to the case $J = 0$.) For $k > 1$, a more geometric discussion will be given in Remark 6.10 below.

*Proof of Theorem 6.3.* It follows easily from Lemma 6.4 that, for each $J \in \mathbb{R}$, the two distinct values of $k$ correspond to two real curves which are not real projectively equivalent since they are distinguished by the sign of $b$ (if $J \neq 1$), or the sign of $a$ if $J = 1$. Thus there is a one-to-one correspondence between real projective equivalence classes and real parameters $k \neq 1$.

Finally, since the number of connected components cannot change as $k$ varies over either of the connected intervals $(-\infty, 1)$ and $(1, +\infty)$, it is enough to count the number of components for one example in each interval. □

**Corollary 6.5** (Flex Points). *Every smooth real cubic curve $C_{\mathbb{R}}$ has exactly three flex points.*

*Proof.* In Hesse normal form, the flex points are just the “exceptional points” listed in Equation (4). Evidently exactly three of these points are real, namely the three points $(x : y : z)$ with

$$x + y + z = xyz = 0.$$

The conclusion follows. □

**Remark 6.6** (Topology). By definition, a simple closed curve in the real projective plane is *essential* if it generates the homology group

$$H_1\big(\mathbb{P}^2(\mathbb{R}); \mathbb{Z}\big) \cong \mathbb{Z}/2.$$

Every essential simple closed curve has a neighborhood which is a Möbius band; while every inessential one bounds a topological disk. As an example, every line in $\mathbb{P}^2(\mathbb{R})$ is essential. Two simple closed curves with transverse intersections have an odd number of intersections if and only if both curves are essential. If we think of $\mathbb{P}^2(\mathbb{R})$ as a unit sphere with antipodal points identified, then an essential curve is covered by a simple closed curve which cuts the sphere into two antipodal pieces; while an inessential curve is covered by a pair of simple closed curves which cut the sphere into three pieces.

It is not hard to see that every smooth irreducible real cubic $\mathcal{C}_\mathbb{R}$ has a unique essential connected component, which contains the three flex points. If there is a second component, then it must be inessential.

**Corollary 6.7** (Automorphisms). *The projective automorphism group* $\mathrm{Aut}\big(\mathbb{P}^2(\mathbb{R}),\, \mathcal{C}_\mathbb{R}\big)$ *is non-abelian of order six and can be identified with the group of permutations of the three flex points. That is, every permutation of the flex points extends uniquely to a projective automorphism of the pair* $\big(\mathbb{P}^2(\mathbb{R}),\, \mathcal{C}_\mathbb{R}\big)$.

*Proof.* Using the Hesse normal form, it follows easily that the permutations of the three coordinates yield a group of six automorphisms, which can be identified with the group of six permutations of the three flex points. To finish the proof, we must show that any automorphism which fixes all three flex points is the identity. However, any real automorphism clearly extends to a complex automorphism, so we can apply Corollary 2.14. Any automorphism which fixes one flex point $\mathbf{p}_0$ acts on the curve by a rotation by a root of unity around $\mathbf{p}_0$; but the only real roots of unity are $+1$, which corresponds to the identity automorphism, and $-1$ which interchanges the other two flex points. The conclusion follows. □

**Remark 6.8** (Visualizing Automorphisms). If we use the standard normal form, or indeed almost any projectively equivalent form, then the six automorphisms are very hard to visualize. The picture becomes much clearer if we choose a spherical metric for the projective plane which is invariant under these automorphisms, as in Figure 9. However, it can still be confusing. For example, each of the three involutions can be described either as a 180° rotation about one of the flex points (which lifts to an orientation preserving rotation of the covering 2-sphere), or as a reflection about the line of symmetry (= great circle) which passes through the north-south pole, and crosses the equator halfway between the other two flex points. With the second description, it evidently lifts to an orientation reversing reflection of the 2-sphere.

**Remark 6.9** (Canonical Position). Every real cubic curve can also be represented by a canonical picture in the affine plane which makes its six symmetries evident. Simply put the three flex points line at infinity, and put the center of symmetry at the origin. The tangent lines at the three flex points will then appear as asymptotic

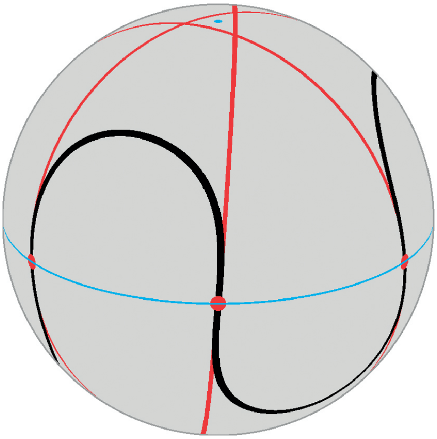


Figure 9

Showing a typical real Hesse curve $\mathcal{C}(-2.4)_{\mathbb{R}}$, with the projective plane $\mathbb{P}^2(\mathbb{R})$ represented as a sphere with opposite points identified. The tangent lines at the three *flex points* of this curve are also shown, as well as the center of symmetry (the north-south pole), and the line through the three flex points (the equator).

lines. If we choose a Euclidean metric so that the automorphisms are Euclidean isometries, then the picture will be unique up to rotation and scale. Finally, we can choose a rotation so that the reflection $(x, y) \leftrightarrow (-x, y)$ about the $y$ axis is one of the automorphisms, and choose the scale so that $(0, 1)$ is the unique point on the $y$-axis which belongs to the essential component of $\mathcal{C}_{\mathbb{R}}$. Then we will have a uniquely determined picture for each $\mathcal{C}(k)_{\mathbb{R}}$. Some typical examples are shown in Figure 10.

As an extra bonus, this picture tends to a well defined limit as we approach any one of the singular cases, at $k = 1$ or $k = \pm\infty$. The limit as $k \to 1$ is a smooth curve plus an isolated point at the origin, while the limit as $k \to \pm\infty$ is a union of three lines.

**Remark 6.10.** In the case $k > 1$ when $\mathcal{C}(k)_{\mathbb{R}}$ has two components, there is a direct geometric relationship between this canonical picture and the shape invariant of Proposition 3.8. Choose an axis of symmetry, for example the $y$-axis, in any of the pictures in Figure 10. Then the curve intersects this axis in three distinct points. As a fourth distinct point, choose the intersection point of this axis of symmetry with the horizontal asymptotic line. Labeling the coordinates of these points along the line in order as $y_1$, $y_2$, $y_3$, $y_4$, we can form a variant of the cross-ratio:

$$\chi = \frac{(y_1 - y_4)(y_2 - y_3)}{(y_1 - y_2)(y_3 - y_4)} \;>\; 0.$$

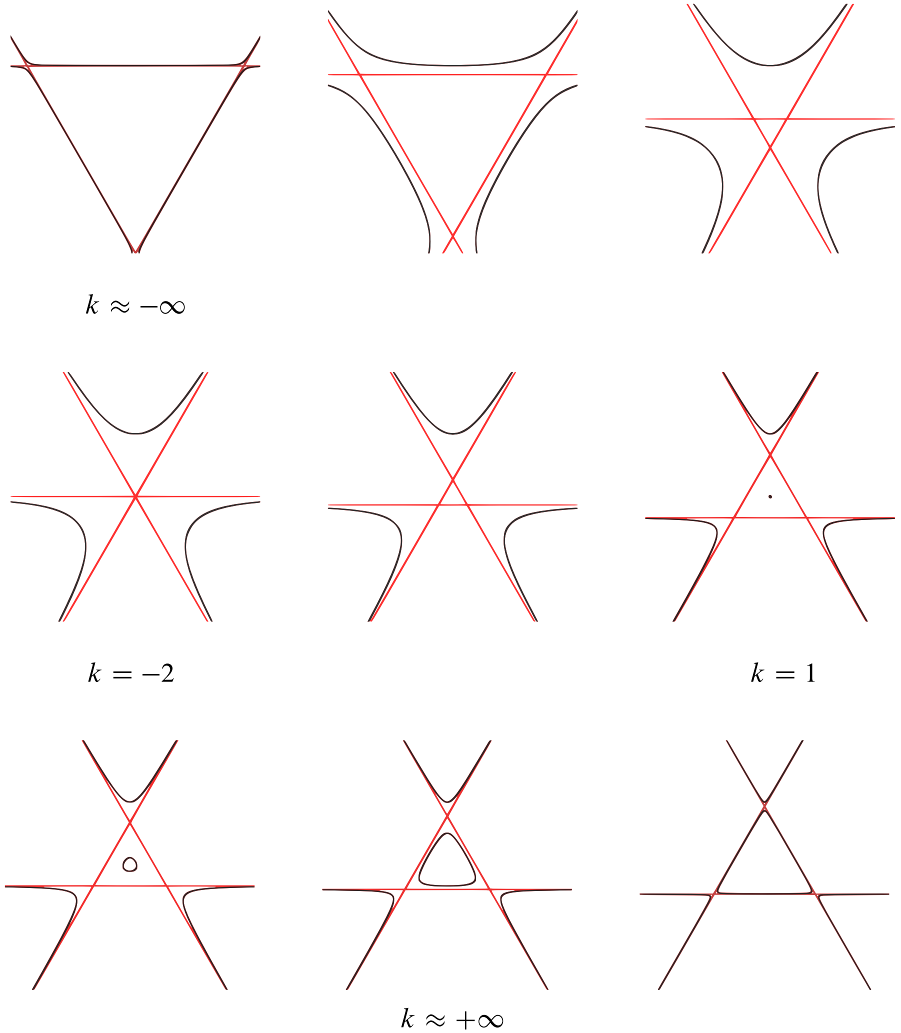


Figure 10

Nine pictures of real cubic curves in canonical form, with Hesse invariant $k$ increasing from near $-\infty$ in the first picture, to near $+\infty$ in the last. Note that the curve tends to a union of three straight lines as $k$ tends to $\pm\infty$. The case $k = 1$ is also singular, with an isolated point at the origin. The case $k = -2$ (with $J = 0$) is noteworthy, since this is the only case where the three asymptotic lines meet at a common point.

Now choose a projective equivalence between $\mathcal{C}(k)_{\mathbb{R}}$ and a corresponding curve in standard normal form, with the axis of symmetry corresponding to the $x$-axis in standard coordinates. Then the points $y_j$ will correspond to the points

$r_1, r_2, r_3, \infty$, where the $r_j$ are the roots of $x^3 + ax + b$. Hence $\chi$ is equal to the cross-ratio

$$\chi = \frac{r_2 - r_3}{r_1 - r_2}.$$

Now if we change the sign of the coefficient $b$, then we must rotate the complex $x$-plane by $180°$. This will interchange $r_1$ and $r_3$, and hence replace $\chi$ by $1/\chi$. Inspecting Figure 10, we see that $\chi$ tends to zero as $k \to 1$, and that $\chi$ tends to infinity as $k \to +\infty$.

## References

[AD] M. Artebani and I. Dolgachev, The Hesse pencil of plane cubic curves. *Enseign. Math.* (2) **55** (2009) 235–273. Zbl 1192.14024 MR 2583779

[Ba] I. G. Bashmakova, Arithmetic of algebraic curves from Diophantus to Poincaré. *Historia Mathematica* **8** (1981) 393–416. Zbl 0471.01003 MR 0635360

[BM] G. Birkhoff and S. MacLane, *A Survey of Modern Algebra*. Macmillan 1953.

[BDM] A. Bonifant, M. Dabija and J. Milnor, Elliptic curves as attractors in $\mathbb{P}^2$, Part 1: Dynamics, *Experiment. Math.* (4) **16** (2007), 385–420. (Also available in: *Collected Papers of John Milnor VII: Dynamical Systems* (*1984–2012*) (2014), 329–385.) Zbl 1136.37026

[BK] E. Brieskorn and H. Knörrer, *Plane Algebraic Curves*. Birkhäuser, 1986. Zbl 0588.14019

[Cas] J. W. S. Cassels, *Lectures on Elliptic Curves*. London Mathematical Society Student Texts No. **24**, Cambridge University Press, 1995. Zbl 0752.14033 MR 1144763

[Dol] I. V. Dolgachev, *Classical Algebraic Geometry: A Modern View*. Cambridge University Press, 2012. Zbl 1252.14001

[Don] S. Donaldson, *Riemann Surfaces*. Oxford University Press, 2011. Zbl 1235.30001 MR 2856237

[Fr] H. R. Frium, The group law on elliptic curves in Hesse form, Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001), 123–151, Springer, Berlin, 2002. Zbl 1057.14038 MR 1995332

[Gib] C. G. Gibson, *Elementary Geometry of Algebraic Curves: An Undergraduate Introduction*. 1st edition, Cambridge University Press, 1998. Zbl 0997.14500 MR 1663524

[Ha] R. Hartshorne, *Algebraic Geometry*. Springer, 1977. Zbl 0367.14001

[Hes1] O. Hesse, Über die Elimination der Variabeln aus drei algebraischen Gleichungen vom zweiten Grade mit zwei Variabeln. *Journal für die reine und angewandte Mathematik* **28** (1844), 68–96. ERAM 028.0817cj MR 1578418

[Hes2] —— Über die Wendepunkte der Curven dritter Ordnung. *Journal für die reine und angewandte Mathematik* **28** (1844), 97–107.

[Kl] F. Klein, Über die Transformation der elliptischen Funktionen und die Auflösung der Gleichungen fünten Grades. *Math. Annalen* **14** (1878–79), 111–172. JFM 10.0069.01

[Kna] A. Knapp, *Elliptic Curves*. Princeton University Press, 1992. Zbl 0804.14013 MR 1193029

[La] S. Lang, Elliptic Functions. Springer, 1987. Zbl 0615.14018 MR 0890960

[Nag] T. Nagell, Sur les propriétés arithmétiques des cubiques planes du premier genre. *Acta Math.* **52** (1928), 93–126. JFM 54.0403.03 MR 1555271

[New] I. Newton, Enumeratio Linearum Terti Ordinis, Appendix to *Optics*. London, 1704.

[P] H. Poincaré, Sur les propriété arithmétiques des courbes algébriques. *Journal de mathèmatiques* **7** (1901), 161–233 (Œvres **5**). JFM 32.0564.06

[PP] P. Popescu-Pampu, Iterating the Hessian. A dynamical system on the moduli space of elliptic curves and dessins d'enfants. *Noncommutativity and singularities. Proceedings of French-Japanese symposia held at IHÉS, Bures-sur-Yvette, France, November 20–23 and November 15–18, 2006*, ed. by J.-P. Bourguignon. Mathematical Society of Japan, 83–98, Tokyo, 2009. Zbl 1180.14022 MR 2463492

[RB] A. Rice and E. Brown, Why ellipses are not elliptic curves. *Mathematics Magazine* **85** (2012), 163–176. Zbl 1260.14038 MR 2924153

[Ser] J.-P. Serre, *A Course in Arithmetic*. Springer, 1973. Zbl 0256.12001 MR 0344216

[Ste] J. Steiner, Allgemeine Eigenschaften der algebraischen Curven. *Journal für die reine und angewandte Mathematik* **47** (1854), 1–6. ERAM 047.1255cj MR 1578853

[Sti] J. Stillwell, *Mathematics and its History*. 3rd. edition, Springer, 2010. Zbl 1207.01003 MR 2667826

[Web] H. Weber, *Lehrbuch der Algebra*. Braunschweig, 1898. Third edition 1908 republished by Chelsea, New York. JFM 39.0508.06

[Wei1] K. Weierstrass, Zur Theorie der elliptischen Functionen. *Sitzungsber. Königl. Akad. Wiss. Berlin* (1882), 443–451. Zbl 14.0387.03

[Wei2] —— *Formeln und Lehrsätze zum Gebrauche der elliptischen Functionen.* Nach Vorlesungen und Aufzeichnungen des Herrn K. Weierstrass bearbeitet und herausgegeben von H. A. Sch. Zweite Ausgabe. Erste Abteilung. Springer, 1893. JFM 25.0757.01

[Weil] A. Weil, *Number Theory. An Approach Through History from Hammurapi to Legendre*. Birkhäuser, 1984. Zbl 0531.10001

[Whi] H. S. White, *Plane Curves of the Third Order*. Harvard University Press, 1925. JFM 51.0509.01

(*Reçu le 30 mars 2016*)

Araceli Bonifant, Mathematics Department, University of Rhode Island,
5 Lippitt Hall, Kingston, RI 02881, USA

*e-mail:* bonifant@uri.edu

John Milnor, Institute for Mathematical Sciences, Stony Brook University,
Stony Brook, NY 11794-3660, USA

*e-mail:* jack@math.stonybrook.edu