Inflection Points of Planar Cubics

Tyler Zhu

May 15, 2019

We proceed by giving an elementary approach to describing the inflection points of planar cubic curves, and then discussing some of the properties relating to the equations describing these points. We then show that the Galois group of these nine inflections is isomorphic to a solvable group of order 216, known as the affine special linear group $\mathrm{ASL}(2, \mathbb{Z}/3\mathbb{Z})$.

1 The Structure of Flexes on Planar Cubics

To begin, we discover the structure of the inflection points with an elementary approach followed by [3]. We will show that every nonsingular planar cubic has nine inflections. There turns out to be a rich structure relating these points which is captured by the Hesse configuration. Then we can also solve for the coordinates in a simple case, which provides concrete evidence of our previous results.

1.1 Inflection Points and Hessians

We work in homogeneous coordinates. Let $f(x_1, x_2, x_3)$ be a homogeneous polynomial of the third degree, such that $f = 0$ has no singular point.

Choose a triangle of reference having the vertex $P = (0, 0, 1)$ on the cubic curve $f = 0$. Then there is no term involving x_3^3. In the terms $rx_1x_3^2$ and $sx_2x_3^2$, r and s are not both zero, since otherwise P would be singular (look at the partial of x_3).

We then make a series of transformations, first setting $rx_1 + sx_2$ as the new variable x_1, and then replacing x_3 with a linear combination of x_1, x_2, x_3. Our curve f becomes

$$f_1 = x_3^2x_1 + ex_3x_2^2 + C, \tag{1}$$

where C is a cubic function of x_1, x_2, whose second derivative with respect to x_i and x_j shall be designated by C_{ij}. The Hessian of f_1 is

$$h_1 = \begin{vmatrix} C_{11} & C_{12} & 2x_3 \\ C_{12} & C_{22} + 2ex_3 & 2ex_2 \\ 2x_3 & 2ex_2 & 2x_1 \end{vmatrix} = -8ex_3^3 + \dots \tag{2}$$

Thus $P = (0, 0, 1)$ is on $h_1 = 0$ if and only if $e = 0$.

Consider intersecting $x_1 = 0$ with our curve $f = 0$. Let d be the coefficient of x_2^3 in C. Then the points of intersection are described by $(ex_3 + dx_2)x_2^2 = 0$. Two of these points are identical with P, so that $x_1 = 0$ is tangent to $f_1 = 0$ at P. The three points coincide if and only if $e = 0$, and P is then called an *inflection* point of $f_1 = 0$ and $x_1 = 0$ the inflection tangent at P. Hence P is on $h_1 = 0$ if and only if it is an inflection point of $f_1 = 0$. As a result, we have

Theorem 1. Each intersection of a nonsingular cubic curve $f = 0$ with its Hessian curve $h = 0$ is an inflection point of $f = 0$, and conversely.

1.2 Counting the Inflection Points

We would like to count the number of inflection points on an arbitrary nonsingular cubic curve. There is at least one intersection of $f = 0$, $h = 0$. This follows by eliminating x_3, resulting in a homogeneous equation in x_1 and x_2.

Take this point as the vertex $(0, 0, 1)$ of a triangle of reference. As above, we get $f_1 = 0$, where now $e = 0, d \neq 0$. By scaling x_2, we can have $d = 1$. We add a suitable multiple of x_1 to x_2 to eliminate $x_2^2 x_1$, and get

$$F = x_3^2 x_1 + C, \quad C = x_2^3 + 3bx_2x_1^2 + ax_1^3. \tag{3}$$

Its Hessian H is the determinant h_1 from earlier but with $e = 0$. Thus

$$\begin{aligned} H &= 2x_1 \begin{vmatrix} C_{11} & C_{12} \\ C_{12} & C_{22} \end{vmatrix} - 4x_3^2 C_{22} \\ &= 72x_1(bx_2^2 + ax_1x_2 - b^2x_1^2) - 24x_3^2x_2. \end{aligned}$$

Eliminating x_3^2 between $F = 0$, $H = 0$, we get

$$x_2^4 + 6bx_2^2x_1^2 + 4ax_2x_1^3 - 3b^2x_1^4 = 0.$$

If $x_1 = 0$, then $x_2 = 0$ and we get the known inflection point $(0, 0, 1)$. For the remaining intersections, we may set $x_1 = 1$. Then for each root of

$$r^4 + 6bt^2 + 4ar - 3b^2 = 0, \tag{4}$$

we get two inflection points $(1, r, \pm s)$, where, by $F = 0$,

$$-s^2 = r^3 + 3br + a.$$

In fact, no root of (4) makes $s = 0$; in other words, (4) has no double root. For, by eliminating r between the quartic and cubic equations, we get $a^2 + 4b^3 = 0$, and one can show that no nonsingular curve will attain this condition. Hence, we have proved

Theorem 2. Any nonsingular plane cubic curve has exactly nine inflection points.

Remark. This result also follows from Bezout's theorem. We intersect $f_1 = 0$, a degree 3 curve, with $h_1 = 0$, a degree $3(3 - 2) = 3$ curve, which results in at most 9 intersections. However, it remains to be shown that they have only smooth transverse intersections (see Thm 2.10 in [**?**]). We also could have used the Plucker formula's to arrive at a similar result.

1.3 Inflection Triangles

For a fixed root r of Equation 4, the three points $P = (0, 0, 1), (1, r, \pm s)$ are collinear, being on the line $x_2 = rx_1$. We may start with any one of the nine inflection points in place of P. Hence, they lie by threes on $9 \cdot 4/3$ lines.

Theorem 3. The straight line joining any two flexes of a nonsingular cubic curve meets the curve in a new flex. The nine flexes lie by threes on twelve straight lines, four of which pass through any one of the nine points.[a]

[a] This was one of our homework problems.

The six inflection points not on a particular one of these lines lie by threes upon two further lines, and the three lines are said to form an inflection triangle. There are 12/3 such triangles.

Theorem 4. The nine flexes lie by threes upon the sides of any one of the four inflection triangles.

We can visualize these theorems through the *Hesse configuration.* In complex projective space it can be realized as the set of inflection points of a cubic curve, but there is no such realization in the Euclidean plane.

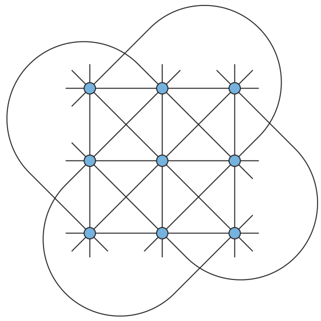

Figure 1: The Hesse configuration of inflection points on an elliptic curve.

1.4 Ternary Canonical Form

With some algebraic manipulations, we can arrive at the following canonical form for ternary cubics.

Theorem 5. Suppose $f = 0$ is a nonsingular cubic curve. Then under some projective transformation, the equation of the curve assumes the form

$$f = \alpha(z_1^3 + z_2^3 + z_3^3) + 6\beta z_1 z_2 z_3.$$

Furthermore, this curve is singular if and only if $\alpha^3 + 8\beta^2 = 0$.

Using the fact that a given cubic curve is nonsingular, our problem eventually reduces to finding the inflection points of the Fermat curve $x^3 + y^3 + z^3 = 0$. The Hessian is $h = 216xyz$, so at least one of x, y, z must be zero.

Suppose $z = 0$. Then we solve for the coordinate $[x : y : 0]$ for which $x^3 + y^3 = 0$. Working in homogenous coordinates, we can write this is $[x : 1 : 0]$ for which $x^3 + 1 = 0$. Solving them gives $x = -1, -\omega, -\omega^2$ where $\omega^3 = 1, \omega \neq 1$.

We get similar results for the other coordinates, leading us to the following nine inflection points:

$$\begin{array}{ccc} (0,1,-1) & (0,1,-\omega) & (0,1,-\omega^2) \\ (-1,0,1) & (-\omega,0,1) & (-\omega^2,0,1) \\ (1,-1,0) & (1,-\omega,0) & (1,-\omega^2,0) \end{array}$$

We can verify that our results from Section 3 still hold. The three points in the ith row of the table lie on the line $z_i = 0$. The three in the first, second, and third columns lie in the respective lines

$$z_1 + z_2 + z_3 = 0, \quad \omega^2 z_1 + \omega z_2 + z_3 = 0, \quad \omega z_1 + \omega^2 z_2 + z_3 = 0.$$

The three diagonals lie on a similar line. Given this, we also note that these nine points as a group have the same structure as $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$; in fact, they are isomorphic.

2 The Galois Group of Inflection Points

To assist us in this development, we will make use of *monodromy groups*, which will be isomorphic to the Galois groups under the settings that we care about. This allows us to take advantage of the rich geometric structure behind monodromy groups to arrive at our result. For this section, we follow the definitions in [6].

2.1 Galois and Monodromy Groups

Throughout the section, let X, Y be two irreducible algebraic varieties of the same dimension over the complex number C, and $\pi : Y \to X$ a generically finite map of degree d. Let $p \in X$ be a generic point so that $\pi^{-1}(p)$ consists of d distinct points $q_1, \ldots, q_d$. We also fix a numbering of these points. We define two groups associated to this setup:

Monodromy Group. This is a similar concept to monodromy in covering maps. The big idea is that we want to capture the behavior of our space as it runs around certain points (usually singularities). Typically in covering maps, we'd look at singular points and their ramifications, using monodromy groups of transformations to look at what happens as we go around these points.

Let $U \subset X$ be a sufficiently small Zariski open set so that π is an unbranched covering map of degree d restricted to $V = \pi^{-1}(U)$. We may also assume $p \in U$. For any loop $\gamma : [0,1] \to U$ based at p, and any lift q_i of p, there exists a unique lift of γ, denoted by $\widetilde{\gamma_i} : [0,1] \to V$ so that $\widetilde{\gamma_i}(0) = q_i$. The endpoint of $\widetilde{\gamma_i}$ is well defined up to a homotopy of γ. Therefore, we have an action of $\pi_1(U, p)$ on the set $\{q_1, \ldots, q_d\}$ so that the equivalence class of homotopic loops $[\gamma] \in \pi_1(U, p)$ sends p_i to the endpoint of the lifted arc $\widetilde{\gamma_i}$. With respect to the fixed numbering, this gives a homomorphism

$$\pi_1(U, p) \to S_d,$$

where S_d is the symmetric group of d elements, sometimes referred to as the *monodromy representation*. The image of this homomorphism is called the *monodromy group* of the covering map $\pi : V \to U$.

It may seem like at first this group depends on the choice of the Zariski open subset U, but our key result will show that it does not.

Galois Group. The construction is a little involved, so the interested reader is deferred to Section 2.6 of [6]. The important result is that we can define the Galois group of π in terms of a certain field extension L/K, which does not depend on any Zariski open set. Then we can get the following result.

Theorem 6 (Prop. 2.3 in [6]). For $\pi : Y \to X$ as above, the monodromy group equals the Galois group. In particular, the monodromy group does not depend on the choice of Zariski open subset U.

2.2 Monodromy Group of the Hesse Configuration

First, we define the *affine special linear* group $\mathrm{ASL}(n, k)$ of degree n over a field k to be the external semi-direct product of the vector space k^n by the special linear group $\mathrm{SL}(n, k)$. In other words,

$$\mathrm{ASL}(n, k) = k^n \rtimes \mathrm{SL}(n, k).$$

One way of viewing this (as suggested by [5]) is as a subgroup of the general affine group (AGL), which is the semidirect product of the vector space with the entire general linear group instead.

Using this, we can make the following claim.

Theorem 7. The monodromy group is $\mathrm{ASL}(2, \mathbb{Z}/3\mathbb{Z})$.

Proof. See pg. 15 of [6]. The first step is to see that the monodromy group is a subgroup of the affine general linear group $\mathrm{AGL}(2, \mathbb{Z}/3\mathbb{Z})$, as this group governs the affine space structure of of the set of flexes. The only step left then is to show that the stabilizer of each flex is $\mathrm{SL}(2, \mathbb{Z}/3\mathbb{Z})$. This can be done by using properties of the monodromy group. □

Finally, we can also show that $\mathrm{ASL}(2, \mathbb{Z}/3\mathbb{Z})$ is solvable. It turns out that the derivative from $\mathrm{ASL}(2, \mathbb{Z}/3\mathbb{Z})$ to $\mathrm{SL}(2, \mathbb{Z}/3\mathbb{Z})$ is a homomorphism whose kernel is the group of translations. $\mathrm{SL}(2, \mathbb{Z}/3\mathbb{Z})$ acts on $\mathbb{P}^1_{\mathbb{Z}/3\mathbb{Z}}$, which contains four points. As a result, $\mathrm{SL}(2, \mathbb{Z}/3\mathbb{Z})$ maps into S_4, the permutation group on 4 elements, with kernel $\pm I$. Hence, $\mathrm{SL}(2, \mathbb{Z}/3\mathbb{Z})$ is solvable. The group of translations is abelian, and hence solvable. Therefore, $\mathrm{ASL}(2, \mathbb{Z}/3\mathbb{Z})$ is solvable, as desired.

In [1], they use a different approach to show that the Galois group is isomorphic directly to the semi-direct product. They also remark that the Galois group is the subgroup of index 2 of $\mathrm{AGL}(2, \mathbb{Z}/3\mathbb{Z})$, from which it the order works out to be $432/2 = 216$.

3 Future Directions

Some other directions that were considered but not pursued are now mentioned.

One direction is a continuation of our elementary methods (motivated by [3]) to eventually show that the Galois group is solvable. This is summarized by the following theorem.

Theorem 8 (Theorem 16 in [3])**.** The flexes can be found by solving a quartic and two cubic equations, and the solution involves three cube roots and four square roots. For a general cubic curve, no one of these radicals can be avoided or expressed in terms of the others.

Another direction can be to follow [2], which looks at flex points from a computational viewpoint. It provides an algorithm for computing real flex points of cubics, which in real appications is what we care most about. Hilbert came up with an algorithm to compute real *and* complex flexes, but this exhaustive search is unnecessary if all we want are the real ones. As the paper states...

"To compute the real inflection points of $f = 0$, only two cubic polynomial equations need to be solved in our algorithm and it is unnecessary to solve numerically the quartic equation prescribed in Hilbert's solution. In addition, the invariants of $f = 0$ are used to analyze the singularity of a singular curve, since the number of the real inflection points of $f = 0$ depends on its singularity type."

References

[1] Artebani, Michela and Dolgachev, Igor. (2006). "The Hesse pencil of plane cubic curves." *L'Enseign Math.* 55. 10.4171/LEM/55-3-3. `http://www.math.lsa.umich.edu/~idolga/hesse09.pdf`.

[2] Chen, Falai and Wang, Wenping. "Computing real inflection points of cubic algebraic curves." *Computer Aided Geometric Design*, vol. 20, issue 2, 2003, pp. 101-117. *ScienceDirect*, `www.sciencedirect.com/science/article/pii/S0167839603000220`.

[3] Dickson, L. E. "The Points of Inflexion of a Plane Cubic Curve." *Annals of Mathematics*, vol. 16, no. 1/4, 1914, pp. 50–66. *JSTOR*, `www.jstor.org/stable/1968042`.

[4] Harris, Joe. "Galois groups of enumerative problems." *Duke Mathematical Journal*, vol. 46, no. 4, 1979, pp. 685-704.

[5] Special affine group, Group Properties Wiki. `https://groupprops.subwiki.org/wiki/Special_affine_group`.

[6] Zhang, Yongquan. (2019). "Galois groups of enumerative problems." Minor Thesis, `http://www.math.harvard.edu/ yqzhang/minor_thesis.pdf`