DOI: 10.1478/AAPP.951S1

AAPP | Atti della Accademia Peloritana dei Pericolanti
Classe di Scienze Fisiche, Matematiche e Naturali
ISSN 1825-1242

Vol. 95, No. 1, S1 (2017)

A FEW EXAMPLES OF POINTS OF FINITE ORDER ON SOME SMOOTH PLANE CUBICS

GIOIA FAILLA,[a*] JUAN BOSCO FRÍAS MEDINA,[bc] AND MUSTAPHA LAHYANE [b]

ABSTRACT. In this expository article we give a self-contained presentation on the rational points of finite order on smooth cubics. We mainly construct examples of points of order between four and twelve, except the eleven case of course. And, in some cases, we offer families of cubics having such kinds of points.

Introduction

It is well-known that from a given smooth cubic curve, one can always construct geometrically a group by considering the set of all rational points on such cubic. In fact, such construction arises from the geometric properties of the cubic curves and, based mainly, on the purely algebraic tool offered by *Bézout Theorem*. So, a naive and elementary problem is to find the rational points of finite order in any specific smooth cubic curve.

Billing and Mahler (1940) proved that any smooth cubic does not hold points of order eleven. Later Mazur (1977) and Mazur and Goldfeld (1978) proved the existence of cubics having points of order between two and twelve with the exception (of course) of the eleven case, and determined the group of rational points on such cubics. Nowadays, the problem of determining which are the possible orders for points of finite order is still open.

The aim of this expository article is to present with details a study of the rational points of finite order in a smooth cubic. Almost all the contents is based on Silverman and Tate (2015), but here we present details and computations that are not included in this book. Also, the content about the basic definitions for a cubic is based on Bix (2006) and some ideas of Knapp (1992) are used. All these are good references for the study of the rational points on cubics and further topics.

This survey is organized as follows. In the first section, we give concrete formulas for the group of rational points of a smooth cubic given by an equation in Weierstrass normal form. To do so, we introduce the concept of cubic curves, review some of their properties, and later on, construct the group of rational points of a smooth cubic and show that it is always possible to transform such a cubic to one defined by an equation in Weierstrass normal form.

This work is dedicated to Professors Daniel Sion Kubert, Joseph H. Silverman, and John T. Tate.

In the second section, we deal with Nagell-Lutz theorem which gives concrete properties of the rational points of finite order on a fixed smooth cubic with integer coefficients and which is defined by an equation in Weierstrass normal form. In order to reach this theorem, we study the rational points of finite order in a smooth cubic with integer coefficients defined over $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ that has order two and three, and later, we present a study on the rational points of finite order. Finally in the third section, we offer some concrete examples of points of higher order in some concrete smooth rational cubics. Moreover in some cases, we present families of cubics with rational points of finite order.

1. The Group of Rational Points on a Smooth Cubic

1.1. Cubic Curves. We begin this subsection by presenting the cubic curves. Throughout, we work with affine and projective curves.

Definition 1.1. An *affine cubic* is an affine algebraic curve in the affine plane $\mathbb{A}^2$ obtained as the zero set of a polynomial of degree three in two variables.

So, a polynomial determining an affine cubic is given by the following expression:

$$ax^3+bx^2y+cxy^2+dy^3+ex^2+fxy+gy^2+hx+iy+j,$$

where x and y are variables, and the coefficients a,b,c,d,e,f,g,h,i,j are in some fixed field k such that the 4-tuple (a,b,c,d) does not vanish. In particular, a polynomial which defines a given affine cubic is a k-linear combination of the monomials x^3, x^2y, xy^2, y^3, x^2, xy, y^2 x, y, and 1.
We say that an affine cubic is *rational* if all the coefficients in the above polynomial are rational numbers. Below, we will be interested mainly in such types of cubics.

Example 1.2. Very familiar rational affine cubics that appears naturally in Calculus are, for example, the ones whose polynomials are equal to $y-x^3$ and y^2-x^3 respectively.

Example 1.3. An affine cubic that is not rational is given, for example, by the polynomial $y^2-x^3+2\sqrt{2}x-x+\pi$.

Now, if we apply the homogenization process to a polynomial that defines an affine cubic, i.e., applying the method that makes every monomial in such polynomial to have the degree three, then this allows studying cubics in the projective plane. Giving thus a very convenient way of studying geometrically the cubics.

Definition 1.4. A *projective cubic* is a projective algebraic curve in the projective plane $\mathbb{P}^2$ obtained as the zero set of a homogeneous polynomial in degree three.

Consequently, the general polynomial that defines a projective cubic is given by:

$$\begin{aligned}&aX^3+bX^2Y+cXY^2+dY^3+eX^2Z\\&+fXYZ+gY^2Z+hXZ^2+iYZ^2+jZ^3,\end{aligned}$$

where the coefficients a,b,c,d,e,f,g,h,i,j are in some fixed field k not all equal to zero, and where X,Y and Z are variables.
So, a polynomial that defines a projective cubic is a non-zero k-linear combination of monomials of the form $X^rY^sZ^t$ such that the non-negative integers r,s and t satisfy the linear

equation $r+s+t=3$.
Similarly to the affine case, a projective cubic is *rational* if all its coefficients are rational numbers.

Remark 1.5. It is worth noting that if we apply the dehomogenization process to a polynomial that defines a projective cubic, then we obtain a polynomial in two variables (not necessary homogeneous). And using this polynomial, we may define an affine cubic in general. Therefore, using the homogenization and dehomogenization processes, we pass from an affine cubic to a projective one and vice versa. So, really it is, in general, not important the type of the cubic that we are studying at the beginning.

Example 1.6. The polynomial $X^3+X^2Z-YZ^2$ gives rise to a rational projective cubic.

Example 1.7. A projective cubic that is not rational is given, for example, by the polynomial $\sqrt{3}X^3-X^2Z-3Z^3$.

Remark 1.8. Throughout, if there is no confusion, the term *cubic* will be used for affine and projective cubics.

A cubic handles most importantly two special kinds of points, namely, the singular and the flex points. Below, we introduce such concepts and illustrate them with some examples.

Definition 1.9. Let C be a cubic (that could be affine or projective) determined by a polynomial f. Let P be a point of C. P is *singular* if P vanishes all the partial derivatives of f. Otherwise, it is said to be *non-singular*.
C is a *non-singular* whenever C has no singular points.

Example 1.10. The point P whose 2-tuple coordinates is equal to $(0,0)$ is singular for the rational cubic which is defined by the polynomial $f(x,y)=y^2-x^3$. Indeed,

$$\begin{aligned} f(0,0) &= (0)^2-(0)^3=0,\\ \frac{\partial f}{\partial x}(0,0) &= -3(0)^2=0, \ \textit{and}\\ \frac{\partial f}{\partial y}(0,0) &= 2(0)^1=0. \end{aligned}$$

Example 1.11. The rational affine cubic C defined by the polynomial $-2x^3+7x^2+5y-1$ is non-singular. Indeed, we may observe that the partial derivative with respect to y is a constant which is equal to 5. Consequently, each point of C does not vanish this partial derivative. So, we are done.

Definition 1.12. Let C be a cubic. A point P belonging to C is a *flex* if it is non-singular, and the multiplicity of the tangent line of C at P is equal to three.

Example 1.13. The points $P_1=(0,0)$, $P_2=(1,0)$, and $P_3=(2,0)$ are flex points of the rational cubic defined by the polynomial $f(x,y)=x(x-1)(x-2)-y^2$.

Also, a cubic can be studied depending on the behavior of a polynomial that defines it.

Definition 1.14. Let C be a cubic determined by a polynomial f. C is *irreducible* if f is irreducible. Otherwise, C is *reducible*, and in this case, the algebraic curves defined as the zeros of the irreducible polynomials given by the decomposition of f into irreducible factors are called the *components* of C.

With notation as in the last definition, we may observe that for a reducible cubic, there exists only two possibilities:

(1) f can be decomposed as the product of a polynomial of degree one (which is obviously irreducible) and an irreducible polynomial of degree two. This case occurs when, geometrically, C is the union of a line and a conic.
(2) f can be decomposed as the product of polynomials of degree one. This case occurs when, geometrically, C is the union of lines.

We end this subsection by discussing some geometric properties of cubics.

Theorem 1.15. *Two cubics having no common components intersect at most in nine points.*

Proof. We can assume without lost of generality that the cubics are projective ones. Indeed if we begin, for example, with two affine cubics, then we can homogenize the polynomials that define the cubics and work in the projective plane. Let C_1 and C_2 be projective cubics having no components in common. By Bézout's theorem, C_1 and C_2 intersect exactly nine times counting multiplicities, so, C_1 intersects C_2 at most in nine points. □

The next thing that we will handle is to discuss the problem of constructing a cubic which passes through an assigned set of points. For simplicity, we consider the affine case. Let $\mathscr{C}$ be the set of all affine cubics in $\mathbb{A}^2$. Using the fact that every cubic is defined by a polynomial of degree three, we can describe such set in the following way:

$$\mathscr{C} = \left\{ ax^3+bx^2y+cxy^2+dy^3+ex^2+fxy+gy^2+hx+iy+j \right. \\ \left. \Big| \; a,b,c,d,e,f,g,h,i,j \in k \;\text{ such that }\; (a,b,c,d) \neq (0,0,0,0) \right\}.$$

We may observe that in such a description, we need in total ten constants for handling a cubic. Now, let C be an affine cubic defined by the polynomial

$$f(x,y) = ax^3+bx^2y+cxy^2+dy^3+ex^2+fxy+gy^2+hx+iy+j,$$

where the coefficients of f are in some given field k. If we consider a non-zero constant multiple of f, then we are not changing the cubic C, because the set of zeros of the polynomial f are the set of zeros of the polynomial αf, for any $\alpha \in k^*$. In particular, assuming that a is not equal to zero, we can consider the polynomial $\frac{1}{a}f$ as the polynomial that defines C, and renaming the coefficients we have the following polynomial:

$$x^3+a'x^2y+b'xy^2+c'y^3+d'x^2+e'xy+f'y^2+g'x+h'y+i' = 0$$

We may observe that in this description, we only have nine coefficients. So, the space $\mathscr{C}$ is actually 9-dimensional. If we want that C passes through a given point $P_1 = (x_1, y_1)$ of $\mathbb{A}^2$, then we are imposing one linear condition on the coefficients:

$$x_1{}^3 + a'x_1{}^2y_1 + b'x_1y_1{}^2 + c'y_1{}^3 + d'x_1{}^2 + e'x_1y_1 + f'y_1{}^2 + g'x_1 + h'y_1 + i' = 0,$$

and, consequently, we obtain that

$$i' = -x_1{}^3 - a'x_1{}^2y_1 - b'x_1y_1{}^2 - c'y_1{}^3 - d'x_1{}^2 - e'x_1y_1 - f'y_1{}^2 - g'x_1 - h'y_1.$$

Thus, the space of cubics passing through one assigned point is 8-dimensional. Let us do one more case in order to clarify the idea: if we want that C passes through two given points

$P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ of $\mathbb{A}^2$. Consequently, we may assume that y_1 and y_2 are not equal. We are imposing two linear conditions on the coefficients:

$$x_1{}^3 + a'x_1{}^2y_1 + b'x_1y_1{}^2 + c'y_1{}^3 + d'x_1{}^2 + e'x_1y_1 + f'y_1{}^2 + g'x_1 + h'y_1 + i' = 0$$
$$x_2{}^3 + a'x_2{}^2y_2 + b'x_2y_2{}^2 + c'y_2{}^3 + d'x_2{}^2 + e'x_2y_2 + f'y_2{}^2 + g'x_2 + h'y_2 + i' = 0.$$

From the first condition, we may infer that

$$i' = -x_1{}^3 - a'x_1{}^2y_1 - b'x_1y_1{}^2 - c'y_1{}^3 - d'x_1{}^2 - e'x_1y_1 - f'y_1{}^2 - g'x_1 - h'y_1,$$

and using this expression in the second condition, we may get

$$h' = \frac{x_2{}^3 - x_1{}^3}{y_2 - y_1} - a'\frac{x_2{}^2y_2 - x_1{}^2y_1}{y_2 - y_1} - b'\frac{x_2y_2{}^2 - x_1y_1{}^2}{y_2 - y_1} - c'\frac{y_2{}^3 - y_1{}^3}{y_2 - y_1}$$
$$- d'\frac{x_2{}^2 - x_1{}^2}{y_2 - y_1} - e'\frac{x_2y_2 - x_1y_1}{y_2 - y_1} - f'\frac{y_2{}^2 - y_1{}^2}{y_2 - y_1} - g'\frac{x_2 - x_1}{y_2 - y_1}.$$

Therefore, the space of cubics which pass through two fixed points is 7-dimensional. If we continue with this procedure, one obtain hopefully a condition for each point that we are imposing to cubics. Finally, one gets that the space of cubics passing through eight points (in *general position*) is 1-dimensional. Using this fact, we are ready to prove the next result.

Theorem 1.16. *Let C_1, C_2 and C_3 be three affine cubics. If C_3 contains eight of the nine points of the intersection of C_1 and C_2, then C_3 contains the ninth remaining point.*

Proof. Let $f_1(x,y)$ and $f_2(x,y)$ be the polynomials that define the cubics C_1 and C_2 respectively. For any elements a_1 and a_2 of k, not both equal to zero, we can find cubics that pass through the eight points of the intersection of C_1 and C_2 that C_3 contains, for example $a_1f_1(x,y) + a_2f_2(x,y)$. We denote this family by $\mathscr{K}$. Now, using the fact that the space of the cubics through eight general fixed points is 1-dimensional and the fact that $\mathscr{K}$ is also 1-dimensional, we have that the polynomial that defines C_3 is of the form $b_1f_1(x,y) + b_2f_2(x,y)$ for some $b_1, b_2 \in k$ not both equal to zero. By hypothesis, C_1 and C_2 meet in a ninth point, so the equations $f_1(x,y)$ and $f_2(x,y)$ vanish in such point, and consequently the equation $b_1f_1(x,y) + b_2f_2(x,y)$ vanishes also. We conclude that C_3 contains the ninth point. □

1.2. The Group Law on a Smooth Cubic. We start this subsection with an example that motivates the study of the geometric properties of a cubic. Consider the rational affine cubic in the affine plane $\mathbb{A}^2$ whose polynomial is given by the following:

$$f(x,y) = x^3 + y^3 - 1.$$

The problem here is to find the rational points of such cubic, i.e. the points whose entries are rational numbers. In the affine plane, this problem could be difficult precisely because we are interested in finding rational numbers instead of integer numbers. So, to avoid this difficulty, we could pass to the projective plane. In this new context, we are able to take a rational point and change its rational coordinates to a point whose coordinates are integer ones. Thus working in the projective plane $\mathbb{P}^2$, we obtain a projective cubic defined by the following polynomial:

$$F(X,Y,Z) = X^3 + Y^3 - Z^3,$$

and, in this case, we are interested in finding the integer solutions, i.e., we are interested in solving the equation $X^3+Y^3=Z^3$, that is, the first non-trivial case of Fermat's Last Theorem. Recall that in the case of the equation $X^2+Y^2=Z^2$, one can take a unitary circle with equation $x^2+y^2=1$ in which the coordinates are rational numbers, later consider a line that intersects the circle in two points, and consider the projection of such line. Unfortunately, this approach is not useful in the case of a cubic because in general, a line intersects a cubic in three points, and if we have one of such points is rational and we try to project the line, then it is possible that some points of the line correspond to two points in the cubic.

Fortunately, for a smooth rational cubic, we may use the following geometric approach: if P_1 and P_2 are rational points on the cubic, then we are able to find a third rational point by exploring the line between P_1 and P_2 (since such line is a rational one). To be concrete in our discussion and for simplicity, we deal with the affine case. Indeed, we assume that $P_1=(x_1,y_1)$ and $P_2=(x_2,y_2)$ are rational points on a smooth rational affine cubic C. Therefore, the slope of the line through these points is equal to

$$\lambda=\frac{y_2-y_1}{x_2-x_1},$$

and, it is obviously a rational number. Next, the equation of such line is given then by the following equation:

$$y=\lambda x-\lambda x_1+y_1,$$

and whose all coefficients are rational numbers. Renaming the constant term, we have the rational equation $y=\lambda x+\nu$. Now, if C is defined by the polynomial

$$ax^3+bx^2y+cxy^2+dy^3+ex^2+fxy+gy^2+hx+iy+j,$$

then intersecting the line through P_1 and P_2 with C, we infer the following equation:

$$(a+b\lambda+c\lambda^2)x^3+(b\nu+2c\lambda\nu+3d\lambda^2\nu+e+f\lambda)x^2+ \tag{1.1}$$

$$(c\nu^2+3d\lambda\nu^2+f\nu+2g\lambda\nu+h+i\lambda)x+(d\nu^3+g\nu^2+i\nu+j)=0.$$

Again, we get that every coefficient in this equation is a rational number. So, renaming all of them, we are dealing with the rational equation $\alpha x^3+\beta x^2+\gamma x+\delta$. Next by hypothesis, we are sure that x_1 and x_2 are solutions of this equation, and as a consequence, there exists a rational number x_3 that is solution of the Equation (**1.1**). Indeed, because x_1 and x_2 are rational numbers there exists another real number x_3 that is a solution of the Equation (**1.1**), therefore

$$\alpha x^3+\beta x^2+\gamma x+\delta=(x-x_1)(x-x_2)(x-x_3),$$

and using the equality of the constant term $\delta=-x_1x_2x_3$, we conclude that x_3 has to be rational.

This procedure suggests us a kind of operation with the set of rational points on a given rational cubic: take two rational points P and Q and draw the line that passes through P and Q, now, denote by $P*Q$ the third point of intersection of the line and the cubic.

Note also that if we have only one rational point P, then we are able to obtain a rational point. In fact, taking the tangent line to the cubic at P, we are considering the line that passes through P and P, and the "third" point of intersection is also a rational point.

So, with this technique we are able in general to find rational points on a cubic, the problem is to know if the cubic has a rational point or not. In fact, there does not exist a method that allows in a finite number of steps to decide if a smooth rational cubic has a rational point. In order to avoid this problem, from now on, we always suppose that our cubics contain a rational point that will be denoted by $\mathscr{O}$.

We may hope that the set of rational points on a smooth rational cubic has an algebraic structure of a group. If it is the case, then we need to have a rational point that should be the identity element under this operation, and a priori, we do not have such element. In order to solve this problem, we use the given rational point $\mathscr{O}$ as the identity element for our possible group. The group law that we consider for the set of rational points on a smooth rational cubic will be denoted by $+$ and is defined in the following way: if we want to sum the rational points P and Q on our cubic, then consider the line through P and Q and take the "third" intersection point $P*Q$ with the cubic. Then, consider the line through $P*Q$ and $\mathscr{O}$, the third point of intersection is $P+Q$.

Theorem 1.17. *Given a smooth rational cubic C with a rational point $\mathscr{O}$, the set of rational points on C is an abelian group with the above operation $+$ and with $\mathscr{O}$ as the identity element.*

Proof. Let P, Q, and R be rational points on the cubic C.

• Commutativity. It is clear that this operation is commutative because the line that passes through P and Q is the same line that passes through Q and P. Consequently, $P*Q$ is equal to $Q*P$ and henceforth $P+Q=Q+P$.

• Identity element. We declare that the point $\mathscr{O}$ is the identity element of our group, i.e. $P+\mathscr{O}=P$. Indeed, consider the line that passes through P and $\mathscr{O}$ and take the point $P*\mathscr{O}$. The line that passes through $P*\mathscr{O}$ and $\mathscr{O}$ is precisely the latter one. Therefore, $P+\mathscr{O}=P$.

• Inverse elements. The inverse element of the point P is given in the following manner: take the tangent line to the cubic at $\mathscr{O}$, such line intersects the cubic in another point S (we are using the fact that the cubic is smooth in order to ensure the existence of such tangent line), now, consider the line through P and S and the third intersection point will be $-P$. Let us check that this point is actually the inverse of P: by construction we have that $P*(-P)=S$ and also by construction $S*\mathscr{O}=\mathscr{O}$ (because the line that passes through S and $\mathscr{O}$ is the tangent line at $\mathscr{O}$). So, $P+(-P)=\mathscr{O}$.

• Associativity. It only remains to prove that $(P+Q)+R=P+(Q+R)$. If one try to draw and construct all the points involved in this sum, then one can observe quickly that the situation gets complex. In order to avoid such problem, note that if we are able to show that $(P+Q)*R=P*(Q+R)$, then as a consequence we certainly obtain that $(P+Q)+R=P+(Q+R)$. The point $P*(Q+R)$ is obtained, finding $Q+R$ and considering the third intersection point of the line that joins $Q+R$ with P. In Fig. 1 we draw the points $\mathscr{O}$, P, Q, R, $P*Q$, $P+Q$, $Q*R$, and $Q+R$, and it is worth noting that each of these points is in a blue or a red line.

Take the blue line that contains the points $P+Q$ and R, and also take the red line that contains the points P and $Q+R$. If we proved that the intersection of this lines is in the cubic, then we prove that $P*(Q+R)=(P+Q)*R$. Consider the eight points $\mathscr{O}$, P, Q, R, $P*Q$, $P+Q$, $Q*R$, and $Q+R$, and also consider the intersection point of the two lines, i.e. in total we are considering nine specific points. Note that in this case we have two

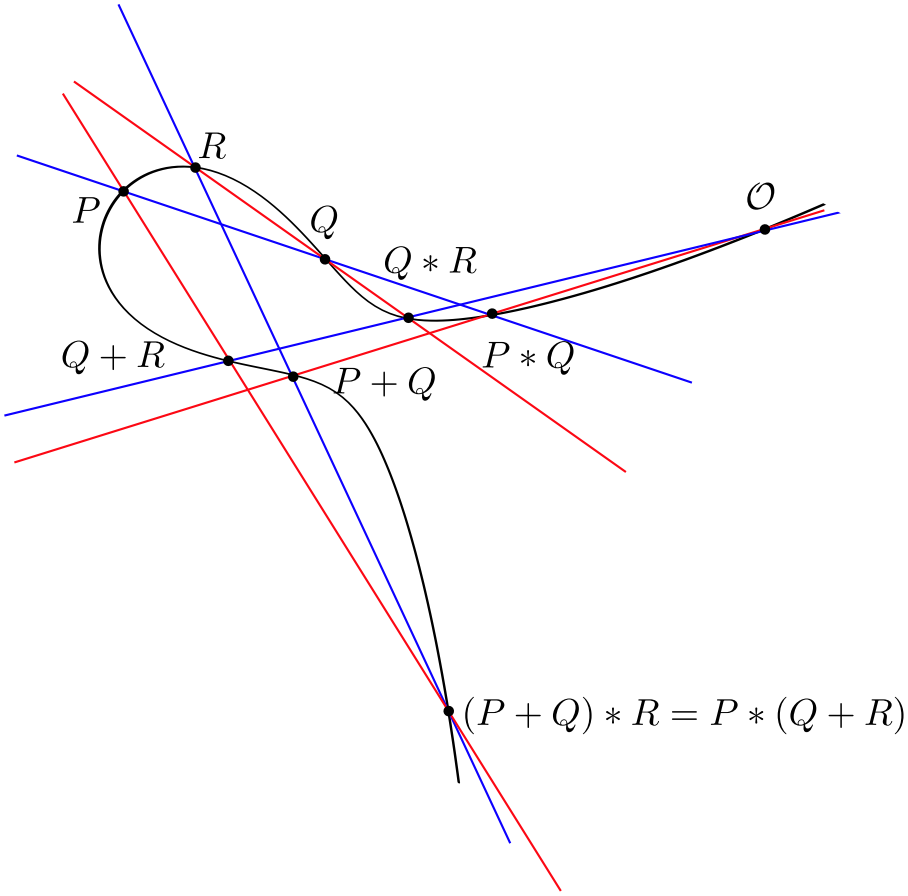

FIGURE 1. Associativity.

degenerate cubics, one constructed by the three blue lines and the another formed by the three red lines, and both contain the nine points. Applying Theorem **1.16**, the cubic C has to contain the intersection point of the lines because contains the other eight points that are in the both degenerate cubics. Finally, we have proved that $(P+Q)*R = P*(Q+R)$, and as a consequence we obtain the associativity of our operation. □

Notation 1.18. *If C is a smooth rational cubic, then the set consisting of all rational points on C will be denoted by $C(\mathbb{Q})$.*

The above theorem states that given a smooth rational cubic C and a rational point $\mathscr{O}$ on C, we are able to construct the group $C(\mathbb{Q})$ using $\mathscr{O}$ as the identity element. Now if in addition to $\mathscr{O}$, there is available another rational point $\mathscr{O}'$, then we can construct the group $C(\mathbb{Q})$ using $\mathscr{O}'$ as the identity element. A natural question arises: what are the relations between the two groups $(C(\mathbb{Q}),\mathscr{O})$ and $(C(\mathbb{Q}),\mathscr{O}')$?

Proposition 1.19. *With the above notation, there is an isomorphism of groups between* $(C(\mathbb{Q}),\mathscr{O})$ *and* $(C(\mathbb{Q}),\mathscr{O}')$.

Proof. Consider the application given by

$$\begin{aligned}\eta : (C(\mathbb{Q}),\mathscr{O}) &\to (C(\mathbb{Q}),\mathscr{O}')\\ P &\mapsto P+(\mathscr{O}'-\mathscr{O}).\end{aligned}$$

It turns out that η is a group homomorphism. Indeed, let P and Q be elements of $(C(\mathbb{Q}),\mathscr{O})$:

$$\begin{aligned}\eta(P+Q) &= \eta(P+Q-\mathscr{O})\\ &= P+Q-\mathscr{O}+(\mathscr{O}'-\mathscr{O})\\ &= P+(\mathscr{O}'-\mathscr{O})+Q-\mathscr{O}\\ &= P+(\mathscr{O}'-\mathscr{O})+Q+(\mathscr{O}'-\mathscr{O})\\ &= \eta(P)+\eta(Q).\end{aligned}$$

Now, we prove that η is injective: let P be an element of $(C(\mathbb{Q}),\mathscr{O})$ such that $P\in\ker\eta$. Consequently, we have that $P+(\mathscr{O}'-\mathscr{O})=\mathscr{O}'$ and using the fact that $\mathscr{O}$ is the identity element, the latter equality implies that $P=\mathscr{O}$.

Finally, we prove that η is surjective: let Q be a point in $(C(\mathbb{Q}),\mathscr{O}')$. Now, observe that $\eta(Q+\mathscr{O})=Q+\mathscr{O}+(\mathscr{O}'-\mathscr{O})=Q+\mathscr{O}'=Q$. □

Remark 1.20. It is important to keep in mind some special situations that could happen when we are joining the rational points on a smooth rational cubic C. Let P and Q be elements of $C(\mathbb{Q})$.

(1) If the line that contains P and Q is tangent to C at P, then the third point of intersection of this line with the cubic is Q.
(2) If P is a flex point, then the third point of the intersection of the tangent line to C at P is nothing but P.

1.3. Weierstrass Normal Form. We begin our study by taking a smooth projective cubic C in $\mathbb{P}^2$ that is defined by the polynomial

$$\begin{aligned}F(X,Y,Z) = aX^3+bX^2Y+cXY^2+dY^3+eX^2Z\\ +fXYZ+gY^2Z+hXZ^2+iYZ^2+jZ^3,\end{aligned}$$

where the coefficients are elements of a fixed field k. The approach that we use is to change the coordinates in the projective plane in order to get the polynomial defining C in a simpler form, i.e. we use projective transformations in order to simplify the polynomial that defines our cubic. Using the hypothesis of the last section, we assume that there exists a rational point $\mathscr{O}$ on C, moreover, we suppose that $Z=0$ is the tangent line of C at the point $\mathscr{O}$. By Bézout's theorem, we know that such tangent line intersects C in another point, we take the line $X=0$ as the tangent line to this point. Finally, we fix the line $Y=0$ as any line different from $Z=0$ that passes through $\mathscr{O}$. Note that under these assumptions, we are supposing that $\mathscr{O}=(1:0:0)$, and that the point $(0:1:0)$ is on C. Observe that if $\mathscr{O}$ is a flex point, then we can take $X=0$ as any line that does not pass through $\mathscr{O}$.

The conditions we are imposing give some extra information on the polynomial that defines the cubic C. The point $(1:0:0)$ is on C, consequently $F(1,0,0)=0$ and this

implies that $a = 0$. In addition, the fact that the point $(0:1:0)$ is on C gives rise to $d = 0$ because $F(0,1,0) = 0$. Now, the fact that the line $Z = 0$ is the tangent line to C at $(1:0:0)$ implies that $b = 0$.

Indeed, the equation of the tangent line at $(1:0:0)$ is given by

$$\frac{\partial F}{\partial X}(1,0,0)\cdot X + \frac{\partial F}{\partial Y}(1,0,0)\cdot Y + \frac{\partial F}{\partial Z}(1,0,0)\cdot Z = 0,$$

that is,

$$\begin{aligned}(2bXY + cY^2 + 2eXZ + fYZ + hZ^2)|_{(1,0,0)}\cdot X +\\ (bX^2 + 2cXY + fXZ + 2gYZ + iZ^2)|_{(1,0,0)}\cdot Y +\\ (eX^2 + fXY + gY^2 + 2hXZ + 2iYZ + 3jZ^2)|_{(1,0,0)}\cdot Z = 0.\end{aligned}$$

Making the calculations in the left side, we have the equation $bY + eZ = 0$, and using the fact that the tangent is equal to $Z = 0$, we obtain that $b = 0$. Similarly, the fact that the tangent line at the point $(0:1:0)$ is equal to $X = 0$ implies that $g = 0$.

On the other hand, the equation of the tangent line at such point is given by the equation:

$$\frac{\partial F}{\partial X}(0,1,0)\cdot X + \frac{\partial F}{\partial Y}(0,1,0)\cdot Y + \frac{\partial F}{\partial Z}(0,1,0)\cdot Z = 0,$$

the calculations of the left side implies that $cX + gZ = 0$, and therefore, the polynomial that defines the cubic is the following:

$$F(X,Y,Z) = cXY^2 + eX^2Z + fXYZ + hXZ^2 + iYZ^2 + jZ^3.$$

Now, if we pass to the affine plane taking the coordinates $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$, then we obtain that the polynomial that defines the cubic in the xy-plane has the form

$$f(x,y) = cxy^2 + ex^2 + fxy + hx + iy + j.$$

So, the equation in which we are interested now is the equation

$$cxy^2 + ex^2 + fxy + hx + iy + j = 0.$$

Reordering the terms and diving by c (this is possible because $c \neq 0$, otherwise the polynomial is not defining a cubic) we have that

$$xy^2 + \frac{f}{c}xy + \frac{i}{c}y = -\frac{e}{c}x^2 - \frac{h}{c}x - \frac{j}{c}.$$

Renaming the coefficients and regrouping the terms, we have the following equation:

$$xy^2 + (\tilde{a}x + \tilde{b})y = \tilde{c}x^2 + \tilde{d}x + \tilde{e}.$$

Multiplying this equation by x, we get

$$(xy)^2 + (\tilde{a}x + \tilde{b})xy = \tilde{c}x^3 + \tilde{d}x^2 + \tilde{e}x,$$

and renaming xy as y_1, we have the equation:

$${y_1}^2 + (\tilde{a}x + \tilde{b})y_1 = \tilde{c}x^3 + \tilde{d}x^2 + \tilde{e}x.$$

Assuming that our field has characteristic different from two, we are able to complete the square of the left side in the above equation and therefore, we obtain:

$$(y_1 + \frac{\tilde{a}x + \tilde{b}}{2})^2 = \tilde{c}x^3 + (\tilde{d} + \frac{\tilde{a}^2}{4})x^2 + (\tilde{e} + \frac{\tilde{a}\tilde{b}}{2})x + \frac{\tilde{b}^2}{4}.$$

Making the change of variables $y_1 = \tilde{c}^2\tilde{y} - \frac{\tilde{a}x+\tilde{b}}{2}$ and $x = \tilde{c}\tilde{x}$, we get the following equation:

$$\tilde{c}^4\tilde{y}^2 = \tilde{c}^4\tilde{x}^3 + \tilde{c}^2(\tilde{d} + \frac{\tilde{a}^2}{4})\tilde{x}^2 + \tilde{c}(\tilde{e} + \frac{\tilde{a}\tilde{b}}{2})\tilde{x} + \frac{\tilde{b}^2}{4}$$

Finally, reducing by $\tilde{c}$ (note that $\tilde{c} \neq 0$) and renaming the coefficients, we infer the equation:

$$\tilde{y}^2 = \tilde{x}^3 + a'\tilde{x}^2 + b'\tilde{x} + c'.$$

This equation is the one that is called the *Weierstrass normal form*.

In addition, if our base field has characteristic different from three, then we are able to eliminate the quadratic term making the change of variables $\tilde{x} = x' - \frac{a}{3}$:

$$\tilde{y}^2 = (x')^3 + (\frac{7a^2}{3} + b)x' + (\frac{8a^3}{27} - \frac{ab}{3} + c),$$

then, renaming the coefficients, we find the polynomial

$$\tilde{y}^2 = (x')^3 + \alpha x' + \beta.$$

Remark 1.21. It is worth noting that in case our cubic is rational, the projective transformations that we are using are rational. For this reason, rational points of the original cubic go to rational points in the new cubic.

In order to clarify the above ideas, we present the following detailed worked example in which we transform the equation that defines an affine cubic to its Weierstrass normal equation.

Example 1.22. Consider the rational affine cubic C_A in $\mathbb{A}^2$ (defined over $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$) that is given by the following equation:

$$u^3 + v^3 = \alpha,$$

where α is a nonzero rational number. Passing to the projective plane, we have a projective cubic C defined by the polynomial

$$F(U,V,W) = U^3 + V^3 - \alpha W^3.$$

We want to find a rational point on this cubic such that the line at infinity $W = 0$ is the tangent line at this point. It is immediately seen that the point $(1 : -1 : 0)$ is a point on C. In addition, the tangent line at such point

$$\frac{\partial F}{\partial U}(1,-1,0)\cdot U + \frac{\partial F}{\partial V}(1,-1,0)\cdot V + \frac{\partial F}{\partial W}(1,-1,0)\cdot W = 0$$

is precisely $W = 0$. Thus, the point $(1 : -1 : 0)$ is a rational point on the cubic that has tangent line equal to $W = 0$ (moreover, such point is a flex point).

The next thing that we want to do is to make a change of coordinates from (U,V,W) to (X,Y,Z) such that $(1 : -1 : 0)$ goes to the point $(0 : 1 : 0)$ and such that $Z = U + V$ is the line at infinity (for simplicity, we are choosing the things in this manner).

We consider the projective transformation $\tau : C_{(U,V,W)} \to C_{(X,Y,Z)}$ induced by the matrix

$$M = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}.$$

So, the new coordinates are given by:

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} U \\ V \\ W \end{pmatrix} = \begin{pmatrix} W \\ U \\ U+V \end{pmatrix} = \begin{pmatrix} X \\ Y \\ Z \end{pmatrix},$$

and the point $(1:-1:0)$ goes to the point $(0:1:0)$ in the new coordinates (X,Y,Z). Moreover, the inverse of the transformation $\tau^{-1}: C_{(X,Y,Z)} \to C_{(U,V,W)}$ is given by the inverse matrix

$$M^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

and our original coordinates are given in the following way:

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} Y \\ Z-Y \\ X \end{pmatrix} = \begin{pmatrix} U \\ V \\ W \end{pmatrix}.$$

It follows that the polynomial that defines the cubic in the new coordinate system is

$$F(X,Y,Z) = Z^3 - 3Z^2Y + 3ZY^2 - \alpha X^3.$$

Going down to the affine plane with the coordinates $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$, we obtain an affine cubic given by the polynomial

$$f(x,y) = 1 - 3y + 3y^2 - \alpha x^3.$$

Now, we are interested in studying the equation

$$3y^2 - 3y = \alpha x^3 - 1.$$

Applying the transformation $x_1 = 3x$ and $y_1 = 9y$, we get that

$$y_1{}^2 - 9y_1 = \alpha x_1{}^3 - 27,$$

completing the square of the left side, one infers:

$$(y_1 - \frac{9}{2})^2 = \alpha x_1{}^3 - \frac{27}{4}.$$

The transformation $y_2 = y_1 - \frac{9}{2}$ applied to the above equation gives rise to

$$y_2{}^2 = \alpha x_1{}^3 - \frac{27}{4},$$

and if in addition, we apply the transformations $x_3 = 4x_1$ and $y_3 = 8y_2$, then we obtain

$$y_3{}^2 = \alpha x_3{}^3 - 432.$$

Finally, considering $\tilde{x} = \alpha x_3$ and $\tilde{y} = \alpha y_3$, we finally arrives to the Weierstrass normal form:

$$\tilde{y}^2 = \tilde{x}^3 - 432\alpha^2.$$

We denote by C_W the cubic defined by this polynomial.

Now, recall the coordinate changes that we made in the projective space, they were:

$$X = W, \quad Y = U, \quad Z = U + V,$$
$$U = Y, \quad V = Z - Y, \quad W = X,$$

and recall the coordinate changes that we are considering when we are passing to the affine planes:

$$u = \frac{U}{W}, \quad v = \frac{V}{W},$$
$$x = \frac{X}{Z}, \quad y = \frac{Y}{Z}.$$

Note that u satisfies the following equalities:

$$u = \frac{U}{W} = \frac{Y}{X} = \frac{\frac{Y}{Z}}{\frac{X}{Z}} = \frac{y}{x},$$

so, applying all the transformations that we used to find the Weierstrass normal form we are able to establish a relation between u with $\tilde{x}$ and $\tilde{y}$:

$$u = \frac{y}{x} = \frac{y_1}{3x_1} = \frac{9 + 2y_2}{6x_1} = \frac{36 + y_3}{6x_3} = \frac{36\alpha + \tilde{y}}{6\tilde{x}}.$$

Similarly, we have the following relations that v satisfy:

$$v = \frac{Z - Y}{X} = \frac{\frac{Z}{Z} - \frac{Y}{Z}}{\frac{X}{Z}} = \frac{1 - y}{x},$$

and applying the transformation that gives rise to the Weierstrass normal form we obtain a relation between v with $\tilde{x}$ and $\tilde{y}$:

$$v = \frac{1 - y}{x} = \frac{9 - y_1}{3x_1} = \frac{9 - 2y_2}{6x_1} = \frac{36 - y_3}{6x_3} = \frac{36\alpha - \tilde{y}}{6\tilde{x}}.$$

So far, we have found a relation between u with $\tilde{x}$ and $\tilde{y}$, and a relation between v and $\tilde{x}$ with $\tilde{y}$:

$$u = \frac{36\alpha + \tilde{y}}{6\tilde{x}}, \quad \text{and} \quad v = \frac{36\alpha - \tilde{y}}{6\tilde{x}}.$$

In addition, we can establish an inverse relation, due to the following computation:

$$u + v = \frac{36\alpha + \tilde{y}}{6\tilde{x}} + \frac{36\alpha - \tilde{y}}{6\tilde{x}} = \frac{12\alpha}{\tilde{x}},$$
$$u - v = \frac{36\alpha + \tilde{y}}{6\tilde{x}} - \frac{36\alpha - \tilde{y}}{6\tilde{x}} = \frac{\tilde{y}}{3\tilde{x}},$$
$$\frac{u - v}{u + v} = \frac{\tilde{y}}{36\alpha}.$$

Using such computation, we obtain that:

$$\tilde{x} = \frac{12\alpha}{u + v}, \quad \text{and} \quad \tilde{y} = 36\alpha \frac{u - v}{u + v}.$$

These relations imply that we can send rational points of C_A to rational points of C_W and vice versa using the following application:

$$\begin{aligned} \varphi : C_A &\to C_W \\ (u,v) &\mapsto \left(\frac{12\alpha}{u+v}, \frac{36\alpha(u-v)}{u+v}\right), \end{aligned}$$

Note that the points in this maps that are not defined are points that satisfy the condition $v=-u$, but these are precisely the points in the line at infinity. Finally, we conclude that finding the rational points on the cubic C_A is the same as finding rational points on the cubic C_W.

Remark 1.23. In general, the arguments used in the above example are true for any smooth rational cubic. The Weierstrass normal form could be very different from the original equation that defines the cubic, but there is a correspondence between the sets of the rational points on such equations. Therefore, the study of the set of rational points on a smooth rational cubic can be reduced to the study of rational points of a cubic which is defined by an equation in Weierstrass normal form.

We have just seen that the equation which defines a cubic can be transformed to the Weierstrass normal form which has the following form:

$$y^2 = f(x) = x^3 + ax^2 + bx + c.$$

where a, b, and c are in some fixed field k. In the case that we are working over $\mathbb{C}$, if we assume that all the complex roots of $f(x)$ are different, then such curve is called an *elliptic curve*. The name comes from the fact that these curves appear in Calculus when the problem of determining the arc length of an ellipse had been studied. After a substitution, the integral that gives the arc length of an ellipse involves the square root of a cubic or quartic polynomial, so, one has to integrate a function of type $y = \sqrt{f(x)}$ and the result is given in terms of certain functions on the "elliptic curve" $y^2 = f(x)$.

Now, assuming that we are working over $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ and that the coefficients a, b, and c of $f(x)$ are rational numbers (in particular they are real numbers), using the fact that $f(x)$ has degree three we know that $f(x)$ has at least one real root. Consequently, we can factor $f(x)$ in the real numbers as

$$f(x) = (x-\alpha)(x^2+\beta x+\gamma)$$

where α, β, and γ are real numbers. There are two possibilities for $f(x)$:

(1) $f(x)$ has only one real root and the other two are complex roots. In this case $f(x)$ has the form $(x-\alpha)(x^2+\beta x+\gamma)$ where the polynomial $x^2+\beta x+\gamma$ is irreducible over the real numbers.
(2) $f(x)$ has three real roots. In this case $f(x)$ has the form $(x-\alpha)(x-\delta)(x-\varepsilon)$ where δ and ε are real numbers.

Observe that in the first case the cubic will have the one component, and in the second case if we have that all the roots are different, then the cubic will have to components. If we have that $f(x)$ has a root with at least multiplicity two, then the cubic is singular. Indeed,

the polynomial that defines such cubic is $g(x,y) = y^2 - f(x)$, and the partial derivatives are

$$\frac{\partial g}{\partial x} = -f'(x), \quad \frac{\partial g}{\partial y} = 2y.$$

If f has a root x_0 with multiplicity at least two, then $f(x) = (x-x_0)^2(x-\alpha)$ where α is a real number, this implies that x_0 vanishes $f'(x)$ because $f'(x) = 2(x-x_0)(x-\beta) + (x-x_0)^2$. Consequently, the point $(x_0, 0)$ is a singular point in the cubic. Note that the converse is also true: if the cubic is singular, then we have that there exists a point (x_0, y_0) on the cubic that vanishes the partial derivatives, so $f'(x_0) = 0$ and $y_0 = 0$. Now, we know that $f(x) = (x-x_0)p(x)$ where $p(x)$ is a polynomial with real coefficients of degree two. Our hypothesis says that x_0 vanish $f'(x) = p(x) + (x-x_0)p'(x)$, so, x_0 has to vanish the polynomial $p(x)$ and consequently $f(x) = (x-x_0)^2(x-\beta)$ where β is a real number.

There are two possibilities for the singular point. If f has a double root, then the equation that defines the curve has the form

$$y^2 = (x-\zeta)(x-\xi)^2$$

where ζ and ξ are real numbers. In the case that the root is a triple root, the form of Weierstrass normal equation is

$$y^2 = (x-\zeta)^3,$$

where ζ is a real number. The cubics for the first possibility are called *nodal cubics* and the cubics of the second possibility are called *cuspidal cubics*.

Remark 1.24. At the moment, we are only dealing with smooth cubics, not with singular ones. The reason is that the behavior of the singular cubics is different of the behavior of the smooth cubics. At the beginning of this past section we discussed that the technique of consider the projection in a smooth cubic is not useful to find rational points, however, in the case of a singular cubic such technique works: if one consider the projection from the singular point to some line, then one has that the line that is tangent to the cubic at the singular point has multiplicity two in such point and consequently intersects the cubic only in one more point. Therefore, the projection of a singular cubic onto a line is one to one. By the other hand, when we proved that the set of rational points in a smooth rational cubic is a group we use the fact that the cubic is smooth.

1.4. Formulas for the Group Law on Smooth Cubics in Weierstrass Normal Form. The aim of this subsection is to give explicit formulas to compute the coordinates of the sum of two rational points on a smooth rational cubic. As an application, we give the formula to compute the coordinates of the double of a point,

We begin by considering a cubic C (defined over $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$) given by the Weierstrass normal equation

$$y^2 = x^3 + ax^2 + bx + c$$

Homogenizing such equation in order to work in the projective plane, we have a projective cubic defined by the polynomial

$$F(X,Y,Z) = X^3 + aX^2Z + bXZ^2 + cZ^3 - Y^2Z.$$

Our interest is the intersection of this cubic with the line at infinity $Z = 0$. A direct computation tells us that the intersection point of the cubic defined by F with the line $Z = 0$

is the point $(0:1:0)$ and its intersection multiplicity is equal to three, i.e is a flex point. So, the cubic has only one point at infinity that is equal to $(0:1:0)$, and we can think that this is the intersection point of all vertical lines (i.e. the lines of the form $x =$ constant). Moreover, the point $(0:1:0)$ is nonsingular. Indeed, computing the partial derivatives we obtain that

$$\frac{\partial F}{\partial X}(0,1,0) = 0, \quad \frac{\partial F}{\partial Y}(0,1,0) = 0, \quad \text{and} \quad \frac{\partial F}{\partial Z}(0,1,0) = -1.$$

Therefore, a cubic defined by Weierstrass normal equation has only one point at infinity that is smooth, and we denote it by $\mathscr{O}$.

The aim is to give explicit formulas to calculate the sum of a pair of rational points on C. In order to achieve this, we take the following convention: the point $\mathscr{O}$ will be considered as the rational point on C serving as the identity element for the group of rational points on C. With this convention, we have that

$$C(\mathbb{Q}) = \left\{P \in C \;\middle|\; P \text{ is a rational point}\right\} \cup \{\mathscr{O}\}.$$

Moreover, with this assumption we can realize that every line intersects the cubic C in exactly three points:

a) A line that is not vertical intersects C in three points in the affine plane.
b) A vertical line intersects C at two points in the affine plane and at the point $\mathscr{O}$.
c) The line at infinity intersects three times C at the point $\mathscr{O}$.

Now, we want to calculate explicit formulas for the group law. Let P and Q be rational points on C. Recall that the group law is defined in the following way: firstly, the point $P*Q$ is the third point of intersection of the line that passes through P and Q with C, and $P+Q$ is the third point of intersection of the line that pass through $P*Q$ and $\mathscr{O}$ with C. In our case, the line that joins $P*Q$ with $\mathscr{O}$ is a vertical line, and using the fact that a cubic given by Weierstrass normal equation is symmetric with respect to the x axis, $P+Q$ is precisely the point $P*Q$ reflected with respect to the x axis.

The inverse $-P$ of a point P is precisely the reflection of that point with respect to the x axis. Indeed, the third point of intersection of the line that pass through P and $-P$ with C is $\mathscr{O}$, so $P*(-P) = \mathscr{O}$. Now, the third point of intersection of the line that joins $\mathscr{O}$ and $\mathscr{O}$ with C is $\mathscr{O}$, so $P+(-P) = \mathscr{O}$. Therefore, if $P = (x,y)$ then we have that $-P = (x,-y)$. It is obvious that this formula does not work if $P = \mathscr{O}$, but also it is obvious that $-\mathscr{O} = \mathscr{O}$.

The next thing that we do is to present explicit formulas for the sum of two points on C. Let P and Q be rational points of C that are different to $\mathscr{O}$ and $P \neq Q$. Assume that

$$P = (x_1, y_1), \quad Q = (x_2, y_2), \quad \text{and} \quad P*Q = (x_3, y_3).$$

Our objective is determine the numbers x_3 and y_3 in terms of x_1, y_1, x_2, and y_2. In order to avoid the case of the inverse of a point, we assume that $y_1 \neq -y_2$. We begin considering the equation of the line that joins P with Q:

$$y = \lambda x + \nu,$$

where $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$ and $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$. Substituting the equation of this line in the equation of the cubic, we obtain an equation in one variable of degree three,

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = 0,$$

and the solutions of this equation gives the x coordinate of the points that are in the intersection of the line and the cubic. By hypothesis and construction, the numbers x_1, x_2, and x_3 are the solution of such equation, so we have that

$$x^3+(a-\lambda^2)x^2+(b-2\lambda\nu)x+(c-\nu^2)=(x-x_1)(x-x_2)(x-x_3).$$

Calculating the coefficients of the quadratic terms, one has the equality $\lambda^2-a=x_1+x_2+x_3$, and consequently

$$x_3=\lambda^2-a-x_1-x_2.$$

Finally, using the fact that the point (x_3,y_3) is on the line, we have that

$$y_3=\lambda x_3+\nu.$$

By our previous discussion, we conclude that the coordinates of $P+Q$ are given by

$$x\text{-coordinate of } P+Q=\lambda^2-a-x_1-x_2 \tag{1.2}$$

$$y\text{-coordinate of } P+Q=-\lambda x_3-\nu. \tag{1.3}$$

In the following examples we use the formulas that we found to illustrate how can be used.

Example 1.25. Consider the smooth rational cubic C_1 defined by the Weierstrass normal equation $y^2=x^3+2x^2-7x-4$. We want to compute the sum of the points $P=(-1,2)$ y $Q=(4,8)$. As first step, compute the slope and the constant term in the equation that joins P with Q:

$$\lambda=\frac{8-2}{4+1}=\frac{6}{5},\quad \text{and}\quad \nu=2-\left(\frac{6}{5}\right)(-1)=\frac{16}{5}.$$

As second step, we use the formulas (**1.2**) and (**1.3**):

$$x\text{-coordinate of } P+Q=\left(\frac{6}{5}\right)^2-2+1-4=-\frac{89}{25},$$

$$y\text{-coordinate of } P+Q=-\left(\frac{6}{5}\right)\left(-\frac{89}{25}\right)-\frac{16}{5}=\frac{134}{25}.$$

Therefore, we have that

$$P+Q=(-\frac{89}{25},\frac{134}{25}).$$

Example 1.26. Consider the smooth rational cubic C_2 defined by the Weierstrass normal equation $y^2=x^3-x+4$. We want to compute the sum of the points $P=(1,2)$ and $Q=(4,8)$. Firstly, we have to compute the slope and the constant term in the equation that joins P with Q:

$$\lambda=\frac{8-2}{4-1}=2,\quad \text{and}\quad \nu=2-(2)(1)=0.$$

Secondly, using (**1.2**) and (**1.3**) we obtain that

$$x\text{-coordinate of } P+Q=2^2-1-4=-1$$

$$y\text{-coordinate of } P+Q=-(2)(-1)=2.$$

Finally, we get that $P+Q=(-1,2)$.

At this moment, probably the reader has noted that formulas (**1.2**) and (**1.3**) involve the slope of the tangent line that passes through the points that we want to sum, this is the reason why we considered two different points when we obtain the formulas. So, a natural question is what happens if we want to sum a point with itself. Suppose that we have a point $P=(x,y)$ and we are interested in calculate $P+P=2P$. The procedure above needs the slope in order to find the equation that joins the points, thus, if we find the slope, then we can compute the equation of the tangent line at P and the procedure above will work also. So, using the equation $y^2=f(x)$ we can find the slope using implicit derivation:

$$\begin{aligned}\frac{d}{dx}y^2 &= \frac{d}{dx}f(x)\\ 2y\frac{dy}{dx} &= f'(x)\\ \lambda &= \frac{f'(x)}{2y}.\end{aligned}$$

Now, substituting the value of λ in (**1.2**) and (**1.3**), we get that

$$x\text{-coordinate of } 2P = \left(\frac{f'(x)}{2y}\right)^2 - a - 2x = \frac{(3x^2+2ax+b)^2}{4y^2} - a - 2x. \qquad \textbf{(1.4)}$$

$$y\text{-coordinate of } 2P = -\left(\frac{f'(x)}{2y}\right)(x\text{-coordinate of } 2P) - \nu. \qquad \textbf{(1.5)}$$

The above formulas are known as *duplication formulas*, and constitute great tools for computational purposes. The following examples illustrate the use of such formulas:

Example 1.27. Consider the cubic C_1 as in Example **1.25**. Compute $2P$ for $P=(-1,2)$. The slope and the constant term in the equation of the tangent line at P are

$$\lambda = \frac{3(-1)^2+4(-1)-7}{2(2)} = -2, \quad \text{and} \quad \nu = 2-(-2)(-1) = 0.$$

Now, using the formulas (**1.4**) and (**1.5**) we obtain that

$$\begin{aligned}x\text{-coordinate of } 2P &= (-2)^2-2-2(-1) = 4\\ y\text{-coordinate of } 2P &= -(-2)(4) = 8\end{aligned}$$

We conclude that $2P=(4,8)$.

Example 1.28. Consider the cubic C_2 as in Example **1.26**. We are interested in compute the double of the point $P=(4,8)$. In this case, the slope and the constant terms of the equation of the tangent line at P are given by

$$\lambda = \frac{3(4)^2-1}{2(8)} = \frac{47}{16}, \quad \text{and} \quad \nu = 8-\left(\frac{47}{16}\right)(4) = -\frac{15}{4}.$$

Then, using (**1.4**) and (**1.5**) we have that

$$\begin{aligned}x\text{-coordinate of } 2P &= \left(\frac{47}{16}\right)^2 - 2(4) = \frac{161}{256}\\ y\text{-coordinate of } 2P &= -\left(\frac{47}{16}\right)\left(\frac{161}{256}\right) + \frac{15}{4} = \frac{7793}{4096}\end{aligned}$$

Therefore, we have that

$$2P = (\frac{161}{256}, \frac{7793}{4096}).$$

We conclude this section with the following results that will be used in the last section.

Lemma 1.29. *Let C be a smooth rational cubic given by an equation in Weierstrass normal form, let P and Q be points on C different from $\mathscr{O}$. If the x-coordinates of P and Q are equal, then $P = -Q$.*

Proof. The fact that the x-coordinates of P and Q are equal implies that the line that joins such points is vertical, so, the third point of intersection of this line with C is precisely $\mathscr{O}$, i.e. $P * Q = \mathscr{O}$. Later, by definition of the group law we have that $P + Q = \mathscr{O}$ and consequently $P = -Q$. □

Lemma 1.30. *Let C be a smooth rational cubic given by an equation in Weierstrass normal form, let $P = (x,y)$ be a point on C different from $\mathscr{O}$. If $P = -P$, then the y-coordinate of P is equal to zero.*

Proof. By construction of the group law, the coordinates of $-P$ are $(x,-y)$. Hence, the condition $P = -P$ implies that $y = -y$, and consequently, y vanishes. □

2. The Nagell-Lutz Theorem

Recall that if $(G,+)$ is an abelian group, and e is its identity element, an element g of G has *finite order* if there exists a positive integer m such that

$$mg = e \text{ (here mg stands for } \underbrace{g + g + \cdots + g}_{m\text{-times}} \text{)},$$

and $ng \neq e$, for any integer n such that $1 \leq n < m$. In this case, g has *order* m, otherwise g has *infinite order*. For example, e is of order one.

As we have seen in the last section, given a smooth rational cubic, the set of rational points on such cubic has naturally an algebraic structure of an abelian group, and also, we were able to offer explicit formulas for such operation. We are interested in studying those points of finite order on a given smooth rational cubic.

2.1. Points of Order Two and Three. In this subsection, we deal only with the points whose orders are two and three. To do so, let C be a smooth rational cubic whose Weierstrass normal form is given by the following equation:

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

where $f(x) = x^3 + ax^2 + bx + c$. The identity element $\mathscr{O}$ of the group of rational points is assumed to be the point at infinity as we have already discussed in Section **1.4**.

A point P on C different from $\mathscr{O}$ is of order two if it satisfies the algebraic equation $2P = \mathscr{O}$. To be more explicit, let $P = (x,y)$ be a point on C of order two. We may observe that the requirement $2P = \mathscr{O}$ is equivalent to the condition $P = -P$. And using Lemma **1.30**, we may infer that $y = 0$. Conversely, if we take a rational point on C of the form $Q = (\alpha, 0)$, then the equation of its tangent line is given by $x = 0$, and this implies that

$2P = \mathscr{O}$. Therefore, a point has order two, if and only if, its y-coordinate is equal to zero. The points of C that satisfy such condition are:

$$P_1 = (\alpha_1, 0), \quad P_2 = (\alpha_2, 0), \quad \text{and} \quad P_3 = (\alpha_3, 0),$$

where α_1, α_2, α_3 are the roots of the polynomial $f(x)$.
If we are considering points of C whose coordinates are complex numbers, then there are exactly three different points of order two (since the smoothness of C ensures that the roots of $f(x)$ are all different).

Next, consider the set consisting of all rational points on C of order two and the point $\mathscr{O}$, that is, the set $\Lambda = \{\mathscr{O}, P_1, P_2, P_3\}$. We may observe that Λ has an algebraic structure of a subgroup. Indeed, from the algebraic point of view, it is a fact, and from the geometric point of view, if we compute $P_i + P_j$ where $1 \leq i < j \leq 3$, then by construction we have that $P_i * P_j = P_k$ where $k \in \{1,2,3\} \backslash \{i, j\}$ (because the points are collinear), and the fact that the y-coordinate of P_k is equal to zero implies that $P_i + P_j = P_k$. Thus, Λ is a group of order four, moreover, from the fact that every element different from $\mathscr{O}$ has order two implies that Λ is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Consequently, we can determine explicitly the subgroup Λ depending on the field that we are dealing with:

1. Over the complex numbers, Λ is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ because $f(x)$ has all its roots.
2. Over the real numbers, then it occurs that $f(x)$ has three real roots or only one. Consequently, Λ is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ in the first case, or is isomorphic to $\mathbb{Z}_2$ in the second case.
3. Over the rational numbers, then it happens that $f(x)$ has three rational roots, one rational root or has no rational roots. Depending on the case, Λ is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, to $\mathbb{Z}_2$ or to $\{0\}$ respectively.

The next thing that we will do is to study the points of order three. Let $P = (x, y)$ be a rational point of C such that P and $2P$ are different from $\mathscr{O}$ such that $3P = \mathscr{O}$. Observe that the condition $3P = \mathscr{O}$ is equivalent to $2P = -P$. Hence, the x-coordinate of $2P$ is equal to the x-coordinate of $-P$ and henceforth the x-coordinate of $2P$ is equal to x. Conversely, if P is a point of C different from $\mathscr{O}$ such that the x-coordinate of $2P$ is equal to the x-coordinate of P, then Lemma **1.29** implies that $2P = -P$, and consequently $3P = \mathscr{O}$. Therefore, we have proved that a point P on C has an order three, if and only if, the x-coordinates of $2P$ and P are equal.

The condition that we have just found about the points of order three suggests us to have a convenient form to calculate the x-coordinate of a point. Using the formula that we have already obtained in Section **1.4**, we know that the x-coordinate of $2P$ is equal to $\left(\frac{f'(x)}{2y}\right)^2 - a - 2x$. Now, if we make the explicit calculation substituting the value of $[f'(x)]^2$ and y^2, we get that

$$x\text{-coordinate of } 2P = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}.$$

With this convenient formula, the condition on the points of order three is equivalent to

$$\frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} = x,$$

and after reducing, we obtain the equation $3x^4+4ax^3+6bx^2+12cx+(4ac-b^2)=0$. Therefore, a point $P=(x,y)$ on C is of order three, if and only if, x is a root of the polynomial $\rho(x)=3x^4+4ax^3+6bx^2+12cx+(4ac-b^2)$.

We are interested now in knowing the number of points of order three. Using the fact that the x-coordinate of $2P$ is equal to $\frac{f'(x)^2}{4f(x)}-a-2x$ and the condition about the points of order three, the following equality holds:

$$\frac{f'(x)^2}{4f(x)}-a-2x=x,$$

On the other hand, noting that $f''(x)=6x+2a$, it follows that $\rho(x)=2f(x)f''(x)-f'(x)^2$. We assert that ρ has four distinct complex roots, this is a consequence from the fact that $\rho(x)$ and $\rho'(x)$ have no common roots. Indeed, calculating the derivative of $\rho(x)$ using both descriptions that we have,

$$\rho'(x)=2f(x)f'''(x)=12f(x).$$

Consequently, if $\rho(x)$ and $\rho'(x)$ have a common root, then $2f(x)f''(x)-f'(x)^2$ and $12f(x)$ would have a common root, and that would imply that such root is also a common root of $f(x)$ and $f'(x)$, but this is not possible since C is smooth.

Now, let β_1, β_2, β_3 and β_4 the four complex roots of $\rho(x)$. From each β_i we obtain two points of order three, one per each root of $f(\beta_i)$. Indeed, none of $f(\beta_i)$ is equal to zero, otherwise we will have that $(\beta_i,0)$ is a point of order three but this is not possible because such kind of point has order two. Thus, in total we have eight points of order three $P_1,\ldots,P_8$. Now, note that the set $\Gamma=\{\mathscr{O},P_1,\ldots,P_8\}$ has obviously a structure of a subgroup.

Because Γ has order nine and there exists only one abelian group with that order in which every element distinct from the identity has order three, we conclude that Γ is isomorphic to $\mathbb{Z}_3\oplus\mathbb{Z}_3$. Using this fact, we can describe completely the group of points of order three depending on the field that we are working with:

1. Over the complex numbers, Γ is isomorphic to $\mathbb{Z}_3\oplus\mathbb{Z}_3$.
2. Over the real numbers, the polynomial $\rho(x)$ has exactly, two real roots and one of these roots does not satisfy the equation of the cubic. Therefore, Γ is isomorphic to $\mathbb{Z}_3$.
3. Over the rational numbers, it can occur that the only real root of $\rho(x)$ is rational or not. Consequently, Γ is isomorphic to $\mathbb{Z}_3$ if the root is rational or is $\{0\}$ if the root is not rational.

Remark 2.1. The points of order three are the flex points. If P is a flex point, then we have that $P*P=P$, this implies that $2P=-P$. Conversely, if P is point of order three satisfies that $2P=-P$, then one has that the third point of intersection of the tangent line at P is precisely the same P, so, the multiplicity of the tangent line at P is equal to three.

We collect the results obtained in this subsection in the following theorem:

Theorem 2.2. *Let C be a smooth rational cubic defined by an equation in Weierstrass normal form $y^2=x^3+ax^2+bx+c$. Let $P=(x,y)$ a point of C different from $\mathscr{O}$.*

a) *P has order two if and only if $y=0$.*

b) *The subgroup* Λ *of points of order two is isomorphic to* $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ *if we are working over* $\mathbb{C}$*, is isomorphic to either* $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ *or* $\mathbb{Z}_2$ *if we are working over* $\mathbb{R}$*, or is isomorphic to either* $\mathbb{Z}_2 \oplus \mathbb{Z}_2$*, or* $\mathbb{Z}_2$ *or* $\{0\}$ *if we are working over* $\mathbb{Q}$*.*

c) *P has order three if and only if x is a root of the polynomial* $\rho(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2)$*.*

d) *The subgroup* Γ *of points of order three is isomorphic to* $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ *if we are working over* $\mathbb{C}$*, is isomorphic to* $\mathbb{Z}_3$ *if we are working over* $\mathbb{R}$*, or is isomorphic to either* $\mathbb{Z}_3$ *or* $\{0\}$ *if we are working over* $\mathbb{Q}$*.*

2.2. The Coordinates of Points of Finite Order. The objective of this subsection is to show that a rational point of finite order on a smooth rational cubic with integer coefficients has integer coordinates. Throughout, p will denote a prime number.

Let C be a smooth rational cubic defined by an equation in Weierstrass normal form

$$y^2 = f(x) = x^3 + ax^2 + bx + c.$$

Observe that if we consider the transformation $\tilde{x} = d^2x$ and $\tilde{y} = d^3y$, then we obtain that $\tilde{y}^2 = \tilde{x}^3 + ad^2\tilde{x}^2 + bd^4\tilde{x} + cd^6$. So, choosing d equal to the least common multiple of the denominators of a, b and c, every coefficient in the equation will be an integer. Thus, without lost of generality, from now on we assume that the coefficients of our cubics given by Weierstrass normal form are integers.

Recall that any nonzero rational number r can be written in a unique way in the form $\frac{m}{n}p^\nu$, where m and n are integer numbers coprimes with p, n is positive, ν is an integer, and the fraction $\frac{m}{n}$ is reduced. The number ν is called the *order* of r and we denote

$$\mathrm{ord}_p(r) = \nu.$$

Note that r has a positive order if and only if p divides the numerator of r. Similarly, r has a negative order if and only if p divides the denominator of r. Hence, r has an order equal to zero if and only if both the numerator and denominator of r are not divisible by p.

Consider a smooth rational cubic C defined by the equation in Weierstrass normal form $y^2 = x^3 + ax^2 + bx + c$ and consider a rational point (x, y) on C. Assuming that p divides the denominator of x, we can write

$$x = \frac{m}{np^\mu}, \quad \text{and} \quad y = \frac{u}{wp^\sigma}$$

m, n, u, w, μ and σ are integers, μ, n and w are positive, p does not divide m, n, u and w, and the fractions $\frac{m}{n}$ and $\frac{u}{w}$ are reduced. By hypothesis such a point is on C, so, evaluating in the equation of the cubic we have that

$$(\frac{u}{wp^\sigma})^2 = (\frac{m}{np^\mu})^3 + a(\frac{m}{np^\mu})^2 + b(\frac{m}{np^\mu}) + c.$$

That is,

$$\frac{u^2}{w^2p^{2\sigma}} = \frac{m^3}{n^3p^{3\mu}} + \frac{am^2}{n^2p^{2\mu}} + \frac{bm}{np^\mu} + c.$$

Equivalently,

$$\frac{u^2}{w^2p^{2\sigma}} = \frac{m^3 + am^2np^\mu + bmn^2p^{2\mu} + cn^3p^{3\mu}}{n^3p^{3\mu}}.$$

Using the fact that p does not divide u and does not divide w, we get that

$$\operatorname{ord}_p\left(\frac{u^2}{w^2p^{2\sigma}}\right) = -2\sigma,$$

in addition, the fact that p does not divide m implies that

$$\operatorname{ord}_p\left(\frac{m^3+am^2np^{\mu}+bmn^2p^{2\mu}+cn^3p^{3\mu}}{n^3p^{3\mu}}\right) = -3\mu.$$

Consequently, we obtain that $2\sigma = 3\mu$, in particular, σ has to be positive since μ is positive. As a direct consequence of this, we infer that p divides the denominator of y. Moreover, the equality $2\sigma = 3\mu$ implies the existence of a positive integer ν such that $\mu = 2\nu$ and $\sigma = 3\nu$. If we use in the above calculation assuming the p divides the denominator of y instead of the denominator of x, with a similar procedure we obtain the same conclusion. Thus, if p appears in the denominator of one of the coordinates of the point, then p necessary appears in the denominator of the other coordinate, moreover, $p^{2\nu}$ is the power that appears in the denominator of x and $p^{3\nu}$ is the power that appears in the denominator of y for some positive integer ν. This suggests to define the following set:

$$C(p^{\nu}) = \left\{(x,y) \in C(\mathbb{Q}) \;\middle|\; \operatorname{ord}_p(x) \leq -2\nu \text{ and } \operatorname{ord}_p(y) \leq -3\nu\right\} \cup \{\mathscr{O}\}.$$

The reason to add the point $\mathscr{O}$ will be discussed soon. For example, a point P belongs to $C(p)$ if p appears in the denominator of its x-coordinate with at least power two and appears in the denominator of its y-coordinate with at least power three, or $P = \mathscr{O}$. Now, it is immediate that one has the inclusions

$$C(\mathbb{Q}) \supset C(p) \supset C(p^2) \supset C(p^3) \supset \ldots$$

In fact, let ν be a positive integer. Let (x,y) an element of $C(p^{\nu+1})$, so we have that $\operatorname{ord}_p(x) \leq -2(\nu+1)$ and $\operatorname{ord}_p(y) \leq -3(\nu+1)$. Later, using the fact that $-2\nu-2 \leq -2\nu$ and $-3\nu-3 \leq -3\nu$ we concluded that (x,y) is an element of $C(p^{\nu})$.

On the other hand, it is worth noting that for a fixed positive integer ν, if $(x,y) \in C(p^{\nu})$, then it follows that $\operatorname{ord}_p(x) = 2(\nu+z)$ and $\operatorname{ord}_p(y) = 3(\nu+z)$ for some nonnegative integer z. Indeed, by hypothesis we have that $\operatorname{ord}_p(x) = -2\nu-\zeta$ and $\operatorname{ord}_p(y) = -3\nu-\xi$ for some nonnegative integers ζ and ξ. Substituting the point in the equation of the cubic and making similar computations we obtain the equation $2(3\nu+\xi) = 3(2\nu+\zeta)$, this implies that $2\xi = 3\zeta$ and as before we obtain that there exists a nonnegative integer z such that $\zeta = 2z$ and $\xi = 3z$.

Recall that the objective of this subsection is to show that a rational point (x,y) of finite order has integer coordinates. The natural technique that we will use is to show that for every prime number p, both denominators of x and y are not divisible by p. Translating this idea with the definition above, we want to show that (x,y) is not contained in $C(p)$. In order to reach our goal, we need to prove that $C(p^{\nu})$ is a subgroup of $C(\mathbb{Q})$ for any positive integer ν, that is the reason for adding the point $\mathscr{O}$ to $C(p^{\nu})$. Let ν be a positive integer.

Now, to prove that $C(p^{\nu})$ has an algebraic structure of a group, we introduce a coordinate change such that we are able to move the point at infinity $\mathscr{O}$ to the affine plane and that will be convenient for our purpose. Consider the coordinate change given by:

$$t = \frac{x}{y} \quad \text{and} \quad s = \frac{1}{y}.$$

Applying this transformation to the equation that defines the cubic we obtain the equation:

$$y^2 = x^3 + ax^2 + bx + c.$$

That is,

$$\frac{1}{s^2} = \frac{t^3}{s^3} + a\frac{t^2}{s^2} + b\frac{t}{s} + c.$$

Equivalently,

$$s = t^3 + at^2 s + bts^2 + cs^3.$$

in the ts-plane. Clearly, we can return to the original xy-plane using the coordinate change $x = \frac{t}{s}$ and $y = \frac{1}{s}$. Note that the element $\mathscr{O}$ in the ts-plane corresponds to the origin, and all the points of the xy-plane appear here except for those having $y = 0$. We can interpret this in the following way: in the xy-plane we are able to see every point of C with the exception of the point at infinity $\mathscr{O}$, while in the ts-plane we are able to see the point at infinity $\mathscr{O}$ and every point of C in the xy-plane with the exception of those whose order is equal to two.

Also, observe that if we are not considering the point at infinity and the points of order two, then we have a one to one correspondence between the points of C in the xy-plane and the points of C in the ts-plane. Moreover, if we have a line in the xy-plane with equation $y = \delta x + \varepsilon$, then such line under the coordinate change also defines a line in ts-plane. Indeed, applying the transformation to such line we obtain the equation

$$\frac{y}{\varepsilon y} = \frac{\delta x}{\varepsilon y} + \frac{\varepsilon}{\varepsilon y}.$$

That is,

$$\frac{1}{\varepsilon} = \frac{\delta}{\varepsilon}\frac{x}{y} + \frac{1}{y}.$$

Equivalently,

$$s = -\frac{\delta}{\varepsilon}t + \frac{1}{\varepsilon}.$$

Thus, we are able to compute the sum of two points in the ts-plane similarly as we do in the xy-plane.

On the other hand, we introduce a particular ring that will help us in the calculations:

$$R_p = \left\{ \frac{m}{n} \in \mathbb{Q} \;\middle|\; p \text{ does not divide } n \right\}.$$

It is immediately seen that R_p is a ring with the usual operations of rational numbers: the elements 0 and 1 clearly are in R_p, and if $\frac{m_1}{n_1}$ and $\frac{m_2}{n_2}$ are elements of R_p, it occurs that p does not divide $n_1 n_2$ and this implies that $\frac{m_1}{n_1} - \frac{m_2}{n_2}$ and $\frac{m_1}{n_1}\frac{m_2}{n_2}$ are in R_p. With the terminology that we are using, we can say that R_p is the set of nonzero rational numbers such that their order are nonnegative and considering $\mathrm{ord}_p(0)$ as infinity. In addition, we consider the following subgroup of R_p for any positive integer μ:

$$p^\mu R_p = \left\{ p^\mu r \;\middle|\; r \in R_p \right\}.$$

Let us see what happens with the divisibility in the new coordinate system with respect to the powers of p, in particular, we are interested in the points of $C(p)$. Let (x,y) be a

rational point on C (in the xy-plane) belonging to $C(p^\nu)$. By our previous discussion we can write

$$x = \frac{m}{np^{2(\nu+z)}} \quad \text{and} \quad y = \frac{u}{wp^{3(\nu+z)}}$$

m, n, u, w, ν and z are integers numbers, n and w are positive, z is nonnegative, p does not divide m, n, u and w, and the fractions $\frac{m}{n}$ and $\frac{u}{w}$ are reduced. Applying the coordinate change to this point we obtain that

$$t = \frac{x}{y} = \frac{mw}{nu}p^{\nu+z} \quad \text{and} \quad s = \frac{1}{y} = \frac{w}{u}p^{3(\nu+z)}.$$

So, we have that $t \in p^\nu R_p$ and $s \in p^{3\nu}R_p$.

Thus, the point (t,s) belongs to $C(p^\nu)$, if and only if, t and s are in $p^\nu R$ and $s \in p^{3\nu}R$ respectively. Therefore, we conclud that p^ν divides the numerator of t and $p^{3\nu}$ divides the numerator of s.

In order to show that $C(p^\nu)$ has a structure of a subgroup, we have to sum a pair of elements of $C(p^\nu)$ and show that an adequate power of p divides the t-coordinate of such element, and also we have to prove that $C(p^\nu)$ contains the inverse elements. Let $P_1 = (t_1, s_1)$ and $P_2 = (t_2, s_2)$ be rational points that belongs to $C(p^\nu)$. If $t_1 = t_2$, then the points are collinear and that implies that $P_1 = -P_2$, so $P_1 + P_2$ is the identity element and is in $C(p^\nu)$. Suppose that $t_1 \neq t_2$, and let

$$s = \alpha t + \beta \tag{2.1}$$

the equation of the line that passes through P_1 and P_2. We know that the slope α is given by $\alpha = \frac{s_2 - s_1}{t_2 - t_1}$, but we consider another form of the slope that will be more convenient for us. By hypothesis P_1 and P_2 satisfy the equation $s = t^3 + at^2 s + bts^2 + cs^3$, so, substituting the values of the points and subtracting them we obtain that

$$\begin{aligned}
s_2 - s_1 &= t_2^3 + at_2^2 s_2 + bt_2 s_2^2 + cs_2^3 \\
&\quad -(t_1^3 + at_1^2 s_1 + bt_1 s_1^2 + cs_1^3) \\
s_2 - s_1 &= (t_2^3 - t_1^3) + a(t_2^2 s_2 - t_1^2 s_1) \\
&\quad + b(t_2 s_2^2 - t_1 s_1^2) + c(s_2^3 - s_1^3) \\
s_2 - s_1 &= (t_2 - t_1)[(t_2^2 + t_2 t_1 + t_1^2) + a(t_2 + t_1) + bs_2^2] \\
&\quad + (s_2 - s_1)[at_1^2 + bt_1(s_2 + s_1) + c(s_2^2 + s_2 s_1 + s_1^2)],
\end{aligned}$$

and consequently, we get that

$$\alpha = \frac{s_2 - s_1}{t_2 - t_1} = \frac{t_2^2 + t_2 t_1 + t_1^2 + a(t_2 + t_1) + bs_2^2}{1 - at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_2 s_1 + s_1^2)}. \tag{2.2}$$

For the case that $P_1 = P_2$, the slope of the tangent line of C at P_1 is given by the equation $\alpha = \frac{ds}{dt}(P_1)$, and we have that

$$\begin{aligned}
\frac{ds}{dt} &= \frac{1}{dt}(t^3 + at^2 s + bts^2 + cs^3) \\
\frac{ds}{dt} &= 3t^2 + 2ats + at^2\frac{ds}{dt} + bs^2 + 2bts\frac{ds}{dt} + 3cs^2\frac{ds}{dt}
\end{aligned}$$

$$\frac{ds}{dt} = \frac{3t^2 + 2ats + bs^2}{1 - at^2 - 2bts - 3cs^2}.$$

Consequently, evaluating the above expression in P_1, we obtain:

$$\alpha = \frac{ds}{dt}(P_1) = \frac{3t_1^2 + 2at_1s_1 + bs_1^2}{1 - at_1^2 - 2bt_1s_1 - 3cs_1^2}.$$

Moreover, this expression for α is the expression that one may infer from the right side of **2.2** considering $t_1 = t_2$ and $s_1 = s_2$. Therefore, we can use (**2.2**) in any case. Let $P_3 = (t_3, s_3)$ be the three point of intersection of the line $s = \alpha t + \beta$ with the cubic. The polynomial of degree three which has the roots t_1, t_2 and t_3 is obtained by substitution of the equation of the line in the equation of the cubic $s = t^3 + at^2 + bts^2 + cs^3$, such substitution gives rise to the polynomial

$$\begin{aligned}
\alpha t + \beta = t^3 + at^2(\alpha t + \beta) + bt(\alpha t + \beta)^2 + c(\alpha t + \beta)^3 \\
t^3 + \frac{a\beta + 2b\alpha\beta + 3c\alpha^2\beta}{1 + a\alpha + b\alpha^2 + c\alpha^3}t^2 \\
+ \frac{b\beta^2 + 3c\alpha\beta^2 - \alpha}{1 + a\alpha + b\alpha^2 + c\alpha^3}t \\
+ \frac{c\beta^3 - \beta}{1 + a\alpha + b\alpha^2 + c\alpha^3} = 0.
\end{aligned}$$

By construction, such polynomial can be written in the following way:

$$(t - t_1)(t - t_2)(t - t_3) = t^3 - (t_1 + t_2 + t_3)t^2 + (t_1t_2 + (t_1 + t_2)t_3)t - t_1t_2t_3,$$

and comparing the coefficients of the term t^2 we obtain the equality

$$t_1 + t_2 + t_3 = -\frac{a\beta + 2b\alpha\beta + 3c\alpha^2\beta}{1 + a\alpha + b\alpha^2 + c\alpha^3}. \tag{2.3}$$

The latter expression gives us a formula to compute explicitly t_3, it only remains to find and expression for s_3. Consider the line that passes through (t_3, s_3) and $(0,0)$ and take the third point of intersection. Note that in general, if a point (t_0, s_0) is in the curve, then one has immediately that the point $(-t_0, -s_0)$ is also on the curve:

$$\begin{aligned}
-s = -t^3 - at^2s - bts^2 - cs^3 \\
s = t^3 + at^2s + bts^2 + cs^3.
\end{aligned}$$

Therefore, the third point of intersection of the line is $(-t_3, -s_3)$.

Now, consider (**2.2**). The numerator of α is in $p^{2\nu}R$ because t_1, s_1, t_2 and s_2 are elements of $p^\nu R$. For the same reason we have that $-at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_2s_1 + s_1^2)$ is an element of $p^{2\nu}R$, and thus the denominator of α is a unit in R. It follows that α is in $p^{2\nu}R$. Then, using the fact that $s_1 \in p^{3\nu}R$, $\alpha \in p^{2\nu}R$ and $t_1 \in p^\nu R$, the equation (**2.1**) implies that $\beta = s_1 - \alpha t_1$ and consequently we obtain that β is an element of $p^{3\nu}R$. Moreover, using the expression (**2.3**), we see that $t_1 + t_2 + t_3$ is an element of $p^\nu R$. In addition, we have that t_1 and t_2 are in $p^\nu R$, this implies that t_3 and $-t_3$ also are in such ring.

Summarizing, we proved that if the t-coordinate of the points P_1 and P_2 is in $p^\nu R$, then the t-coordinate of $P_1 + P_2$ also is in $p^\nu R$. Moreover, we proved that if the t-coordinate of a point $P = (t, s)$ is in $p^\nu R$, then the t-coordinate of the point $-P = (-t, -s)$ is in $p^\nu R$.

This shows that $C(p^\nu)$ is closed under the addition and have the inverse elements, therefore, $C(p^\nu)$ is a subgroup of $C(\mathbb{Q})$. In fact, we proved that if P_1 and P_2 are elements in $C(p^\nu)$, the

$$(t\text{-coordinate of } P_1)+(t\text{-coordinate of } P_2)-(t\text{-coordinate of } P_1+P_2) \in p^{3\nu}R.$$

This relation suggests us to pass to the quotient:

$$(t\text{-coordinate of } P_1+P_2))+p^{3\nu}R = (t\text{-coordinate of } P_1)+(t\text{-coordinate of } P_2)+p^{3\nu}R. \tag{2.4}$$

Note that the sum that appears on the left side is the sum in the cubic, while the sum on the right side is the sum of rational numbers. From this fact, we can define the following map:

$$\begin{aligned} \xi : C(p^\nu) &\to \frac{p^\nu R}{p^{3\nu}R} \\ (t,s) &\mapsto t+p^{3\nu}R \\ \mathscr{O} &\mapsto 0 \end{aligned}$$

By (**2.4**), it follows immediately that ξ is a homomorphism of groups. Noting that the kernel of that homomorphism is precisely the set of points such that their t-coordinate is in $p^{3\nu}R$, i.e. $\ker\xi = C(p^{3\nu})$, we conclude that the induced homomorphism

$$\zeta : \frac{C(p^\nu)}{C(p^{3\nu})} \to \frac{p^\nu R}{p^{3\nu}R}$$

is one to one.

The results that we have found can be stated in the following proposition:

Proposition 2.3. *Let p be a prime number and let C be a smooth cubic with integer coefficients defined by an equation in Weierstrass normal form.*

a) *If $P=(x,y)$ is a rational point of C and p divides the denominator of one of the coordinates, then p divides the denominator of the other coordinate.*
b) *For every positive integer ν, the set $C(p^\nu)$ is a subgroup of the group of rational points $C(\mathbb{Q})$.*
c) *The homomorphism*

$$\begin{aligned} \zeta : \quad \frac{C(p^\nu)}{C(p^{3\nu})} &\to \frac{p^\nu R}{p^{3\nu}R} \\ (x,y)+C(p^{3\nu}) &\mapsto \frac{x}{y}+p^{3\nu}R \\ \mathscr{O}+p^{3\nu}R &\mapsto 0 \end{aligned}$$

is one to one.

Using this result we prove now that the coordinates of a point of finite order have to be integer numbers.

Corollary 2.4. *Let C be a smooth cubic with integer coefficients defined by an equation in Weierstrass normal form.*

(1) *If p is a prime number, then the unique point of finite order in $C(p)$ is $\mathscr{O}$.*
(2) *A point of finite order different from the identity element has integer coordinates.*

Proof. For the fist statement, let $P=(x,y)$ be a rational point of order m, where m is positive integer, different from $\mathscr{O}$. Note that necessarily m has to be greater than one. Let p be a prime number and suppose that $P\in C(p)$. If one takes a look at the denominators of x and y, then one can find a nonnegative integer number ν such that $P\in C(p^{\nu})$ but $P\notin C(p^{\nu+1})$: Consider indeed $\nu=-\frac{\mathrm{ord}_p(x)}{2}$ (this is an integer number because our previous discussion). We considerer two cases in the proof:

a) p does not divide m. Using the equality in the quotient (see (**2.4**)), we have for the point P that

$$t\text{-coordinate of } mP+p^{3\nu}R_p = m(t\text{-coordinate of } P)+p^{3\nu}R_p.$$

Using the fact that $mP=\mathscr{O}$, we have that the t-coordinate of mP is equal to zero. On the other hand, because m is coprime with p we have that m is a unit in R_p. Thus,

$$t\text{-coordinate of } P+p^{3\nu}R_p = 0+p^{3\nu}R_p,$$

and this implies that $P\in C(p^{3\nu})$, a contradiction with the fact that $P\notin C(p^{\nu+1})$.

b) p divides m. This hypothesis tell us that there exists a positive integer n such that $m=pn$. Define $\tilde{P}=nP$. Using the fact that P has order m we know that $\tilde{P}$ has order p: indeed, $p\tilde{P}=pnP=mP=\mathscr{O}$. In addition, note that $\tilde{P}$ is in $C(p)$ since the assumption that $P\in C(p)$. Now, we know that there exists a positive integer μ such that $\tilde{P}\in C(p^{\mu})$ but $\tilde{P}\notin C(p^{\mu+1})$. Similarly to the previous case, we find that

$$p(t\text{-coordinate of } \tilde{P})+p^{3\mu}R = t\text{-coordinate of } p\tilde{P}+p^{3\mu}R = 0,$$

and this implies that the t-coordinate of $\tilde{P}+p^{3\mu-1}R_p$ is equal to zero. Finally, observe that $3\mu-1\geq\mu+1$, a contradiction with the fact that $\tilde{P}$ is not an element of $C(p^{\mu+1})$.

For the second statement, let $P=(x,y)$ be a point of finite order different from $\mathscr{O}$. By the first statement we have that P is not a element of $C(p)$ for every prime number p, this implies that the denominators of the coordinates of P cannot be divided by any prime number, this implies that the coordinates have to be integer numbers. □

2.3. Nagell-Lutz Theorem. In this subsection, we prove the Nagell-Lutz theorem which establishes a way to find points of finite order. In order to reach this objective, it is necessary to introduce the following concept:

Definition 2.5. Let C be a smooth cubic with integer coefficients given by the equation in Weierstrass normal form $y^2=f(x)=x^3+ax^2+bx+c$. The *discriminant* of the cubic C is the integer

$$D=-4a^3c+a^2b^2+18abc-4b^3-27c^2.$$

It is worth noting that using the polynomial ring $\mathbb{Z}[x]$ in one variable x and with integer coefficients, the discriminant D belongs to the ideal generated by $f(x)$ and $f'(x)$, i.e., there exist polynomials $r(x)$ and $s(x)$ with integer coefficients such that $D=r(x)f(x)+s(x)f'(x)$. Indeed, taking $r(x)=(18b-6a^2)x-(4a^3-15ab+27c)$ and $s(x)=(2a^2-6b)x^2+(2a^3-7ab+9c)x+(a^2b+3ac-4b^2)$, we have that

$$\begin{aligned}D=&[(18b-6a^2)x-(4a^3-15ab+27c)]f(x)\\&+[(2a^2-6b)x^2+(2a^3-7ab+9c)x+(a^2b+3ac-4b^2)]f'(x).\end{aligned}$$

With the help of such polynomials, we are able to prove the following property:

Lemma 2.6. *Let C be a smooth cubic with integer coefficients given by the equation in Weierstrass normal form $y^2 = f(x) = x^3 + ax^2 + bx + c$. If $P = (x_1, y_1)$ is a point on C such that P and $2P$ have integer coordinates, then y_1 is either equal to zero or divides the discriminant D.*

Proof. We assume that y_1 is not equal to zero and we will prove that y_1 divides D. The hypothesis that $y_1 \neq 0$ implies that $2P \neq \mathscr{O}$ since Theorem **2.2**, and consequently we can write $2P = (x_2, y_2)$. Recall that by assumption x_1, y_1, x_2 and y_2 are integer numbers. The duplication formula in the x-coordinate (see Equation (**1.4**)) tells us that $2x_1 + x_2 = \lambda^2 - a$, where $\lambda = \dfrac{f'(x_1)}{2y_1}$. Note that λ is an integer. So, this fact and the fact that $f'(x_1)$ and $2y_1$ are integers implies that $2y_1 | f'(x_1)$, in particular, $y_1 | f'(x_1)$. Moreover, it follows that $y_1 | f(x_1)$ since the equation $y^2 = f(x)$. Finally, observe that evaluating the equation $D = r(x)f(x) + s(x)f'(x)$ in x_1, and noting that $r(x_1)$ and $s(x_1)$ are integer numbers, we conclude that $y_1 | D$. □

Now, we are ready to state and prove the Nagell-Lutz theorem.

Theorem 2.7 (Nagell-Lutz theorem)**.** *Let C be a smooth cubic with integer coefficients and which is defined by the equation in Weierstrass normal form $y^2 = x^3 + ax^2 + bx + c$. If $P = (x, y)$ is a rational point on C of finite order, then x and y are integers. Moreover,*

a) *If P has order two, then $y = 0$.*
b) *If the order of P is different from two, then y divides the discriminant D of C.*

Proof. By Corollary **2.4**, we have that a point of finite order has integer coordinates. If P has order two, then by Theorem **2.2** we have that $y = 0$. If P is a rational point with finite order different from two, then Theorem **2.2** implies that $y \neq 0$. In addition, the fact that P has finite order implies that $2P$ also has finite order: indeed, if m is the order of P, then $2mP = \mathscr{O}$. Consequently, $2P$ has integer coordinates too, and using that y is different from zero, Lemma **2.6** implies that y divides the discriminant. □

Nagell-Lutz theorem is used to prove that a rational point on a cubic in Weierstrass normal form with integer coefficients has infinite order. The idea is to compute iterated sums of P until one reaches some positive integer n such that nP has not integer coordinates. Consequently, the Nagell-Lutz theorem implies that nP has no finite order, and consequently P also has infinite order.

Remark 2.8. If C has rational coefficients, then it is possible to find rational points of finite order which may not have integer coefficients. For example, see Propositions **3.1**, **3.2** and **3.3**.

Remark 2.9. The Nagell-Lutz theorem does not give necessary and sufficient conditions. It is possible to find points on the cubic with integer coordinates and such that the y-coordinate divides the discriminant, but having no finite order. Usually, the Nagell-Lutz theorem is used to add points to the list of finite order points, but it is not a criterion to decide if a point has a finite order or not.

3. Examples of Points of Higher Finite Order

Through the discussion of this section, we are considering a smooth rational cubic defined by a Weierstrass normal form and also we consider a rational point P on such cubic different from the identity element $\mathscr{O}$ which is the only point on our cubic at infinity. Recall that P has order m (a positive integer) if $mP = \mathscr{O}$ and $nP \neq \mathscr{O}$ for any integer n such that $1 \leq n \leq m-1$.

3.1. Order Four. Note that the condition of $4P = \mathscr{O}$ is equivalent to $2P = -2P$ and by Lemma **1.30**, the latter condition implies that the y-coordinate of $2P$ is equal to zero. On the other hand, if $P \neq \mathscr{O}$ and the y-coordinate of $2P$ is equal to zero, then by Theorem **2.2**, we know that $2P$ has order two. Therefore, we have a necessary and sufficient condition to find points of order four:
A point P not equal to $\mathscr{O}$ is of order four if the y-coordinate of $2P$ is equal to zero and the y-coordinate of P is different from zero.

Proposition 3.1. *For every nonzero rational number t, the point $P = (t,t)$ is a point of order four on the smooth rational cubic C defined by the Weierstrass normal form $y^2 = x^3 + (1-2t)x^2 + t^2x$.*

Proof. Our hypothesis on t ensures the smoothness of our cubic cubic C. Indeed, if $t = 0$, then $(0,0)$ is a singular point. Using the duplication formula for the x-coordinate, we have that

$$x\text{-coordinate of } 2P = 0,$$

and this implies that $2P = (0,0)$. Therefore, the y-coordinate of $2P$ is equal to zero. Since P is not equal to $\mathscr{O}$ and has a nonzero y-coordinate, it follows immediately that the order of the point $P = (t,t)$ is four. □

3.2. Order Five. Observe that $5P = \mathscr{O}$ if and only if $3P = -2P$, and this implies that the x-coordinate of $3P$ is equal to the x-coordinate of $2P$ by the definition of the group law. Conversely, if P is a point different from $\mathscr{O}$ such that the x-coordinates of $3P$ and $2P$ are equal, then $3P = -2P$ by Lemma **1.29**. Therefore, a point P not equal to $\mathscr{O}$ has the order five if the x-coordinate of $3P$ is equal to the x-coordinate of $2P$.

Proposition 3.2. *For every nonzero rational number t, the point $P = (0, -\frac{t}{2})$ has the order five on the smooth rational cubic C defined by the equation $y^2 = x^3 + \big(-t + (\frac{t-1}{2})^2\big)x^2 + \frac{1}{2}t(t-1)x + \frac{t^2}{4}$.*

Proof. The hypothesis $t \neq 0$ guarantees that C is nonsingular. In fact, if $t = 0$, then C is the singular cubic $y^2 = x^2(x + \frac{1}{4})$ at the point $(0,0)$. The duplication formulas give that

$$x\text{-coordinate of } 2P = t.$$

$$y\text{-coordinate of } 2P = \frac{t^2}{2}.$$

Now computing the x-coordinate of $3P = P + 2P$, one infers the following:

$$x\text{-coordinate of } 3P = t,$$

$$y\text{-coordinate of } 3P = \frac{-t^2}{2}.$$

The facts that $2P$ and $3P$ have the same x-coordinate and $P \neq \mathscr{O}$ imply that the order of $P = (0, -\frac{t}{2})$ is five. □

3.3. Order Six. We have that $6P = \mathscr{O}$, if and only if, $3P = -3P$. Thus, Lemma **1.30** tells us that the y-coordinate of $3P$ has to be equal to zero. Conversely, if the y-coordinate of $3P$ is equal to zero and $P \neq \mathscr{O}$, then Theorem **2.2** implies that $3P$ has order two, i.e. $6P = \mathscr{O}$. Therefore, to ensure that P has order six we have to be sure that the y-coordinate of $3P$ is equal to zero, the y-coordinate of P has to be different from zero, and the x-coordinate of P is not a root of the polynomial $\rho(x)$ (otherwise, P will have order three, see Theorem **2.2**).

Proposition 3.3. *For every nonzero rational number t not equal to -1, the point $P = \big(0, \frac{-t(t+1)}{2}\big)$ is a point of order six on the smooth rational cubic C defined by the equation* $y^2 = x^3 - \frac{(3t^2+6t-1)}{4}x^2 + \frac{t(t^2-1)}{2}x + \frac{t^2(t+1)^2}{4}$.

Proof. The assumptions $t \neq 0$ and $t \neq -1$ ensure that C is a smooth cubic. In fact, if $t = 0$, then C is the singular cubic $y^2 = x^2(x + \frac{1}{4})$, and if $t = -1$, then C is the cuspidal cubic. In this case, zero is not a root of $\rho(x)$, since $\rho(0) = -t^3(t+1)^3$. Using the duplication formulas, we have that

$$x\text{-coordinate of } 2P = t(t+1),$$
$$y\text{-coordinate of } 2P = \frac{1}{2}t^2(t+1).$$

Now, we compute the y-coordinate of $3P$:

$$x\text{-coordinate of } 3P = t$$
$$y\text{-coordinate of } 3P = 0.$$

Therefore, we conclude that $\big(0, \frac{-t(t+1)}{2}\big)$ is a point of order six. □

3.4. Order Seven. An equivalent condition to $7P = \mathscr{O}$ is $3P = -4P$, and the latter implies the equality of the x-coordinates of $3P$ and $4P$. Conversely, if P is not equal to $\mathscr{O}$ and satisfies the property that the x-coordinates of $3P$ and $4P$ are equal, then we have that $3P = -4P$ (see Lemma **1.29**). Consequently, $P \neq \mathscr{O}$ has the order seven if the x-coordinates of $3P$ and $4P$ are equal.

Proposition 3.4. *For every nonzero rational number t not equal to 1, the point $P = \big(0, -\frac{\lambda}{2}\big)$ is a point of order seven on the smooth rational cubic C defined by the equation* $y^2 = x^3 + \big(-\lambda + \frac{1}{4}\mu^2\big)x^2 + \frac{1}{2}\lambda\mu x + \frac{1}{4}\lambda^2$. *Here, $\lambda = t^2(t-1)$ and $\mu = t^2 - t - 1$.*

Proof. By the duplication formulas, we obtain that

$$x\text{-coordinate of } 2P = t^2(t-1),$$
$$y\text{-coordinate of } 2P = \frac{1}{2}t^3(t-1)^2,$$

and computing the x-coordinate of $3P$, one finds that it is equal to

$$x\text{-coordinate of } 3P = t(t-1).$$

Here, the y-coordinate of $3P$ is equal to $-\frac{1}{2}t(t-1)^3$. Now applying the duplication formula to the x-coordinate of $2P$, one gets the following coordinates of $4P$:

$$x\text{-coordinate of } 4P = t(t-1).$$

$$\text{And the } y\text{-coordinate of } 4P = \frac{1}{2}t(t-1)^3.$$

Thus, the x-coordinates of $3P$ and $4P$ are equal. Consequently, we infer that the order of the point $P = \big(0, -\frac{\lambda}{2}\big)$ is equal to seven. □

3.5. Order Eight. Observe that $8P = \mathscr{O}$ is equivalent to $4P = -4P$, and applying Lemma **1.30** we obtain that the y-coordinate of $4P$ has to be zero. On the other hand, if the y-coordinate of $4P$ is equal to zero and $P \neq \mathscr{O}$, then Theorem **2.2** implies that $4P$ has order two. So, a point P not equal to $\mathscr{O}$ has the order eight if the y-coordinate of $4P$ is equal to zero, and the y-coordinate of P and $2P$ are different from zero.

Proposition 3.5. *For every nonzero rational number t not equal to 1 and $\frac{1}{2}$, the point $P = \big(0, -\frac{1}{2}\lambda\big)$ is a point of order eight on the smooth cubic C given by the equation $y^2 = x^3 - \big(\lambda - \frac{1}{4}(1-\frac{\lambda}{t})^2\big)x^2 - \frac{1}{2}\lambda(1-\frac{\lambda}{t})x + \frac{1}{4}\lambda^2$. Here, $\lambda = (t-1)(2t-1)$.*

Proof. Applying the duplication formulas, we have that

$$x\text{-coordinate of } 2P = (t-1)(2t-1),$$

$$y\text{-coordinate of } 2P = \frac{(t-1)^2(2t-1)^2}{2t}.$$

If we apply again the duplication formulas to $2P$, we obtain that

$$x\text{-coordinate of } 4P = t(t-1),$$

$$y\text{-coordinate of } 4P = 0.$$

This implies that $P = \big(0, -\frac{1}{2}\lambda\big)$ is a point of order eight on C. □

3.6. Order Nine. Now, if we are interested in the condition $9P = \mathscr{O}$, then it is worth noting that this is equivalent to $6P = -3P$, and the definition of the group law implies that the x-coordinates of $6P$ and $3P$ have to be equal. In addition, if x-coordinates of $6P$ and $3P$ are equal, then we have that $6P = -3P$ by Lemma **1.29**. Thus, a point P not equal to $\mathscr{O}$ has the order nine if the x-coordinates of $6P$ and $3P$ are equal, and the x-coordinate of P is not a root of $\rho(x)$ (otherwise, P will have order three, see Theorem **2.2**).

Proposition 3.6. *For every nonzero rational number t not equal to 1. The point $P = \big(0, -\frac{1}{2}\mu\big)$ is a point of order nine on the smooth cubic C given by the equation $y^2 = x^3 + \big(-\mu + \frac{1}{4}[1-t^2(t-1)]^2\big)x^2 - \frac{1}{2}[1-t^2(t-1)]\mu x + \frac{1}{4}\mu^2$. Here, μ is equal to $t^2(t-1)[1+t(t-1)]$.*

Proof. The duplication formula gives the following equalities:

$$x\text{-coordinate of } 2P = \mu,$$
$$y\text{-coordinate of } 2P = \frac{1}{2}t^4(t-1)^2(1+t(t-1)).$$

Next, the x-coordinate of $3P$ is given by

$$x\text{-coordinate of } 3P = t^2(t-1).$$

While its y-coordinate is given by

$$y\text{-coordinate of } 3P = -\frac{1}{2}t^3(t-1)^3.$$

Applying the duplication formula to the x-coordinate of the point $3P$, we obtain that

$$x\text{-coordinate of } 6P = t^2(t-1).$$

While $\rho(0) = -t^6(t-1)^3[1+t(t-1)]^3$. Consequently, $P = \big(0, -\frac{1}{2}\mu\big)$ is a point of order nine on C. □

3.7. Order Ten. Similarly to the previous cases, the condition $10P = \mathscr{O}$ is equivalent to the condition $5P = -5P$, and by the definition of the group law, we have that the y-coordinate of $5P$ is equal to zero. Reciprocally, if the point P is not equal to the point of the cubic at infinity and the y-coordinate of $5P$ is equal to zero, then Theorem **2.2** ensures that $5P$ has order two. So, if the y-coordinate of $5P$ is equal to zero, the y-coordinate of P is not equal to zero (otherwise, P will have order two), and the x-coordinate of $2P$ and $3P$ are different (otherwise, P will have order five), then P has the order ten.

Proposition 3.7. *For every nonzero rational number t not equal to 1 and $\frac{1}{2}$, the point $P = \big(0, -\frac{1}{2}\delta\big)$ is a point of order ten on the smooth cubic C given by the equation $y^2 = x^3 + \big(-\delta + \frac{1}{4}[1-t(d-1)]^2\big)x^2 - \frac{1}{2}\delta[1-t(d-1)]x + \frac{1}{4}\delta^2$. Here, $\delta = td(d-1)$, and $d = \dfrac{t^2}{t-(t-1)^2}$.*

Proof. The duplication formulas imply that the coordinates of $2P$ are given by

$$x\text{-coordinate of } 2P = \delta,$$
$$y\text{-coordinate of } 2P = \frac{1}{2}t^2d(d-1)^2.$$

On the other hand, the x-coordinate of the point $3P$ is

$$x\text{-coordinate of } 3P = t(d-1),$$

and so, P is not of order five. Moreover, the y-coordinate of the point $3P$ is

$$y\text{-coordinate of } 3P = -\frac{1}{2}t(t-1)(d-1)^2,$$

The last step is to compute the coordinates of the point $5P$:

$$x\text{-coordinate of } 5P = td(t-1),$$
$$y\text{-coordinate of } 5P = -\frac{1}{2}td[t^2 + d(t^2-3t-1)] = 0.$$

Therefore, the order of the point $\left(0,-\frac{1}{2}\delta\right)$ is ten. □

3.8. Order Twelve. Note that the condition $12P=\mathscr{O}$ is the same condition as $6P=-6P$, and the latter implies that the y-coordinate of $6P$ has to be zero by the definition of the group law. Conversely, if the point P is not equal to $\mathscr{O}$ and the y-coordinate of $6P$ is equal to zero, then $6P$ has the order two because of Theorem **2.2**. Thus, if one proves that P is such that the y-coordinate of $6P$ is equal to zero, the y-coordinates of P, $2P$ and $3P$ are different from zero, and the x-coordinate of P is not a root of the polynomial $\rho(x)$ (otherwise, P will have order three, see Theorem **2.2**), then it follows that P has the order twelve.

Proposition 3.8. *For every nonzero rational number t not equal to 1 and $\frac{1}{2}$, the point $P=\left(0,-\frac{1}{2}\gamma\right)$ is a point of order twelve on the smooth cubic C given by the equation $y^2=x^3+\left(-\gamma+\frac{1}{4}[1-f(d-1)]^2\right)x^2-\frac{1}{2}\gamma[1-f(d-1)]x+\frac{1}{4}\gamma^2$. Here, $\gamma=fd(d-1)$, $f=\frac{m}{1-t}$, $d=m+t$ and $m=\frac{1-3t+3t^2}{1-t}$.*

Proof. Similarly as in previous cases, making a substitution the x-coordinate of P (that is zero) is not a root of the polynomial $\rho(x)$ since $\rho(0)$ is equal to $-f^3d^3(d-1)^3$. On the other hand, the duplication formulas give us the coordinates of $2P$:

$$x\text{-coordinate of } 2P=\gamma,$$
$$y\text{-coordinate of } 2P=\frac{1}{2}f^2d(d-1)^2.$$

Now, the computation of the coordinates of the point $3P$ gives

$$x\text{-coordinate of } 3P=f(d-1),$$
$$y\text{-coordinate of } 3P=-\frac{1}{2}f(f-1)(d-1)^2.$$

Finally, applying the duplication formulas to the point $3P$, we get the coordinates of the point $6P$:

$$x\text{-coordinate of } 6P=\frac{f(d-1)(d-f)}{(f-1)^2},$$
$$y\text{-coordinate of } 6P=0.$$

We conclude that P has the order twelve, so we are done. □

Remark 3.9. For more detailed computations and original contributions see Kubert (1976).

Acknowledgments

The research that led to the present paper was partially supported by a grant of the group GNSAGA of INdAM. It was also partially supported during 2016 and 2017 by the *Coordinación de la Investigación Científica de la Universidad Michoacana de San Nicolás de Hidalgo* (UMSNH), Morelia, Mexico. The authors warmly thank the two Referees for their suggestions. The second author acknowledges a financial support of *Consejo Nacional de Ciencia y Tecnología* under the Grant Number 339809 ending on August 31, 2016 and the support of *Fondo Institucional de Fomento Regional para el Desarrollo Científico,*

Tecnológico y de Innovación, FORDECYT 265667, starting from October 1, 2016. The third author thanks Dr. Ricardo Becerril Bárcenas, former director of the Institute of Physics and Mathematics (IFM), as well as Dr. Medardo Serna González, Rector (Chancellor) of UMSNH, for a sabbatical leave.

References

Billing, G. and Mahler, K. (1940). "On exceptional points on cubic curves". *Journal of the London Mathematical Society* **s1-15**, 32–43. DOI: 10.1112/jlms/s1-15.1.32.

Bix, R. (2006). *Conics and cubics. A concrete introduction to algebraic curves*. 2nd ed. Springer, New York. DOI: 10.1007/0-387-39273-4.

Knapp, A. W. (1992). *Elliptic curves*. Vol. 40. Mathematical Notes. Princeton University Press.

Kubert, D. S. (1976). "Universal bounds on the torsion of elliptic curves". *Proceedings of the London Mathematical Society* **s3-33**(2), 193–237. DOI: 10.1112/plms/s3-33.2.193.

Mazur, B. (1977). "Modular curves and the Eisenstein ideal". *Publications Mathématiques de l'IHÉS* **47**(1), 33–186. DOI: 10.1007/BF02684339.

Mazur, B. and Goldfeld, D. (1978). "Rational isogenies of prime degree". *Inventiones Mathematicae* **44**(2), 129–162. DOI: 10.1007/BF01390348.

Silverman, J. H. and Tate, J. T. (2015). *Rational points on elliptic curves*. 2nd ed. Springer International Publishing. DOI: 10.1007/978-3-319-18588-0.

---

[a] Università Mediterranea di Reggio Calabria, Dipartimento DIIES,
Via Graziella, Feo di Vito, Reggio Calabria, Italy

[b] Universidad Michoacana de San Nicolás de Hidalgo (UMSNH), Instituto de Física y Matemáticas (IFM),
Edificio C-3, Ciudad Universitaria, Avenida Francisco J. Múgica s/n, Colonia Felicitas del Rio,
C. P. 58040, Morelia, Michoacán, Mexico

[c] Current address: Universidad Nacional Autónoma de México, Instituto de Matemáticas,
Área de la Investigación Científica, Circuito Exterior, Ciudad Universitaria
Coyoacán, C.P. 04510, Ciudad de México, México
and Unidad Académica de Matemáticas, Universidad Autónoma de Zacatecas,
Calzada Solidaridad entronque Paseo a la Bufa, C.P. 98000, Zacatecas, Zac., México

[*] To whom correspondence should be addressed | email: gioia.failla@unirc.it

Communicated 1 December 2015; manuscript received 31 May 2016; published online 15 May 2017