PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

ASSOCIATIVE PROPERTY ON THE GROUP OF ELLIPTIC CURVES

Tesis para optar el Título de Licenciado en Matemáticas, que presenta el bachiller:

Iván Pérez Avellaneda

ASESOR: Alfredo B. Poirier Schmitz

Lima, setiembre de 2017

Acknowledgments

These notes would not exist without the support of my family, especially of my beloved mother and the everyday stronger memory of my father. To both I entirely dedicate this work and express my deepest gratitude.

I must thank the members of the Mathematics Section within the Sciences Department of Pontificia Universidad Católica del Perú, especially professor Alfredo Poirier, for his enthusiastic and enlightening guidance throughout the development of these notes and his promptness to help. Professors Richard Gonzales and Jaime Cuadros for taking their time to read this work. Professors Francisco Ugarte, Richard Chávez, Christiam Figueroa, Juan Montealegre, José Flores and Rubén Agapito, for their advice, encouragement or support through teaching assistantships.

Also, I thank DGI for granting me the PADET project with code 2016-6-0060.

Resumen

La conjetura de Fermat fue uno de los acertijos matemáticos más misteriosos hasta 1995. El problema fue formulado en 1637 por Pierre de Fermat. Él afirmó saber cómo resolverlo, sin embargo, no podía mostrar la prueba debido a que el espacio en el margen de su copia de *Arithmetica* de Diofanto era insuficiente. Desde entonces mucho misticismo rodeó a la conjetura. Mientras tanto, independientemente, nuevas ramas de las matemáticas se desarrollaban. La geometría algebraica y el análisis complejo permitieron a Andrew Wiles resolver finalmente la conjetura. La solución involucra, entre otras herramientas, el uso de curvas elípticas. Esto es suficiente motivo para estudiarlas.

En lineas generales las curvas elípticas son polinomios cúbicos no singulares en dos variables con un punto especial de coordenadas racionales en los que podemos establecer una estructura de grupo. Para manipular las operaciones cómodamente transformamos la ecuación de la curva elíptica en una más apropiada con menos términos. Para lograr esto exploramos los aspectos fundamentales de los espacios proyectivos que facilitarán la transición.

Como ya es conocido, existen casos en las matemáticas en los que hay un intercambio entre simpleza y elegancia. Uno debe profundizar un poco para alcanzar la estética. Nuestro objetivo es probar la propiedad de asociatividad del grupo en las curvas elípticas por medio del grupo de Picard de una variedad algebraica asociada. Esto provee una prueba alternativa de dicha propiedad y reemplaza los cálculos engorrosos de la prueba directa que usa solo la definición de la operación del grupo. Para lograr esto desarrollamos la teoría de divisores. Esto nos conduce al estudio de funciones racionales sobre las curvas y de este modo nos enfrentamos a uno de los resultados más importantes de la geometría algebraica: el teorema de Riemann-Roch. Basados en esto probamos que las curvas elípticas sobre los cuerpos de característica cero tienen genero uno.

Finalmente definimos el grupo de Picard. Este grupo mide el grado de cuánto del conjunto de divisores no tiene origen en las funciones racionales. Luego establecemos un homomorfismo entre este grupo y la curva elíptica:

esta es en una manera elaborada de afirmar que la asociatividad de una estructura se preserva en la otra.

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
FACULTAD DE CIENCIAS E INGENIERÍA
Tema de Tesis

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
Facultad de Ciencias e Ingeniería
04 SET. 2017
MIGUEL MEJIA PUENTE
DECANO

Para optar el título de licenciado en MATEMÁTICAS

Alumno: Iván PEREZ Avellaneda

Código: 2007.7107

Asesor: Dr. Alfredo Poirier

Tema: Associative property on the group of elliptic curves # 34

Descripción del tema u objetivos:

El objetivo principal de este trabajo será presentar la teoría de curvas elípticas con énfasis en la justicación de la asociatividad de la operación. Ello pasa por un estudio detallado de las propiedades algebraicas básicas de las mismas, definidas en cuerpos de cualquier característica. La meta final es lograr la demostración de la asociatividad de dicha operación en cuerpos de característica cero mediante la comparación con los correspondientes grupos de divisores.

A pedido del alumno, esta tesis podrá ser presentada en inglés; para ello se requerirá que la redacción esté sujeta a estándares mínimos de calidad.

Dr. Christiam Figueroa
Coordinador de Especialidad

Dr. Alfredo Poirier
Asesor

San Miguel, 31 de agosto del 2017

Máximo 100 páginas

Contents

Introduction

The Fermat conjecture was one of the most mysterious puzzles of mathematics until 1995. The problem was formulated in 1637 by Pierre de Fermat. He claimed that he knew how to solve it, but was however unable to exhibit the proof because of the lack of space on the margin of his copy of Diophantus's *Arithmetica*. Since then a lot of mysticism surrounded the conjecture. Meanwhile, independently, new branches of mathematics were developed. Algebraic geometry and complex analysis allowed Andrew Wiles to finally solve the conjecture. The solution involves, among other tools, the use of elliptic curves. That is enough reason for their study.

Roughly speaking elliptic curves are non-singular cubic polynomials in two variables with a special point of rational coordinates where a group structure can be set. In order to handle computations comfortably we transform the equation of the elliptic curve into an appropriate one with fewer terms. To achieve this goal we explore fundamental aspects of projective spaces which facilitate the transition.

As it is known, in some cases there is a trade-off in mathematics between simplicity and elegance. One must dig a little deep to reach aesthetics. We aim to prove the associativity law of the group on elliptic curves by means of the Picard group of an associated algebraic variety. This provides an alternative proof of the property and replaces the usual burdensome computations of the straight proof by definition of the group operation. In order to achieve this, we develop the theory of divisors. This leads us to the study of rational functions on curves, and thus face one of the crucial results of algebraic geometry: the Riemann-Roch theorem. Based on this we prove that elliptic curves over fields of characteristic zero have genus one.

Finally we define the Picard group. This group measures the extent of how much of the set of divisors fails to have its origin on rational functions. Then we establish a homomorphism between this group and the elliptic curve: this yields a fancy way of saying that associativy of one structure is preserved in the other.

Chapter 1

Non singular cubics

In this chapter we introduce elliptic curves and the equations that represent them. We also treat the basic and necessary aspects of projective spaces in order to simplify their representation.

1.1 Preliminaries

We consider a quadratic polynomial in $\mathbb{Q}[X, Y]$, and call its locus a **curve**, which we denote by $\mathcal{C}$. A dichotomy appears here: there is a pair of rational numbers that satisfies the equation, or there are not such pairs. The knowledge of a rational point over a curve will automatically reveal many of them. In order to justify this assertion, we fix a point $O \in \mathbb{Q} \times \mathbb{Q}$ on the curve together with a line L with coefficients in $\mathbb{Q}$. The idea is to parametrize the rest of the rational points on $\mathcal{C}$ through the rational points of L. Each rational point on L along with O determines a unique line, obviously rational. If $\mathcal{C}$ is irreducible, this line intersects $\mathcal{C}$ in exactly two points by Bezout's theorem. Of course one of them is O and the other P, say. To find numerically the coordinates of P one must set a pair of quadratic equations with rational coefficients. If one of the solutions is rational, the other will also be rational, thus P is rational. On the other hand, every rational $P \in \mathcal{C}$ determines along with O a rational line which intersects with L at a rational point (if $P = O$ the line is the tangent to $\mathcal{C}$ at O). In this way we have established a one to one correspondence between the rational points on $\mathcal{C}$ and the rational points on L. We state this fact as a proposition.

Proposition 1.1. *The locus of an irreducible quadratic polynomial in* $\mathbb{Q}[X, Y]$ *with at least one rational point is equivalent to the rational line.* □

Next we consider cubics of the form $y^2 = f(x)$, where $f(x) \in \mathbb{Q}[X]$ with $\deg(f) = 3$. We say that the curve has a **singular point at** $(x_0, 0)$ if $x_0 \in \mathbb{Q}$

is a root of $f(x) = 0$ with multiplicity at least 2. The equation can then be expressed as $y^2 = \lambda(x - x_0)^2(x - x_1)$. We claim that these curves reduce to a line as previously explained for curves of genus zero. Taking a rational line $y = m(x - x_0)$ through $(x_0, 0)$, we observe that the third meeting point between the line and the cubic is a rational point. Considering all the rational lines through this singular point and again projecting them stereographically to a rational line L we obtain a one to one correspondence between the rational points of the cubic and the line. We have proved the following.

Proposition 1.2. *Rational cubics of the form $y^2 = f(x)$ with a singular rational point are equivalent to rational lines.* □

Now we take a polynomial relation of degree 3 with coefficients in an arbitrary field K such as

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0. \tag{1.1}$$

We call a point $(x, y) \in K \times K$ that satisfies the equation a **K-rational point**.

Curves $f(x, y) = 0$ and $F(X, Y) = 0$ are called **equivalent** if there exists rational functions a, b, A, B with rational coefficients which satisfy

$$\begin{aligned} x &= a(X, Y), \\ y &= b(X, Y), \\ X &= A(x, y), \\ Y &= B(x, y) \end{aligned}$$

except for a finite number of points.

Consider the cubic curve

$$y^2 = P(x), \tag{1.2}$$

where $P(x)$ is polynomial of degree 3, and define $F(x, y) = y^2 - P(x)$. If the point (x_0, y_0) satisfies

$$\frac{\partial F}{\partial x}(x_0, y_0) = \frac{\partial F}{\partial y}(x_0, y_0) = 0, \tag{1.3}$$

then we have $y_0 = 0$ and $P'(x_0) = 0$. Evaluating at (x_0, y_0), this means that we have $P(x_0) = 0$, so it is a solution with multiplicity at least 2. In the other direction, if x_0 is a solution of $P(x)$ with multiplicity at least 2, then it must satisfy Relation (1.3).

In general, let $P(x, y)$ be a polynomial in $K[X, Y]$. We say that the point (x_0, y_0) is a **singular point of the curve** $P(x, y) = 0$ if we have also

$$\frac{\partial P}{\partial x}(x_0, y_0) = \frac{\partial P}{\partial y}(x_0, y_0) = 0.$$

The exclusion of singular points in the definition of the curve represented by Equation (1.2) will allow us to diversify in the algebraic aspect and regularize in the geometric sense.

Proposition 1.3. *A polynomial $P(x) \in K[X]$ of degree 3 has different roots if and only if at every point on the curve $y^2 = P(x)$ it is possible to define the tangent.* □

We can now introduce our object of study. By an **elliptic curve over the field** K we mean a non-singular cubic in $K[X, Y]$ which has at least one K-rational point.

1.2 Projective space

One of the biggest concerns of renaissance art was the analysis of perspectives; an obsession that motivated the foundations of projective geometry. We will recall the concepts and relevant results of this theory in order to manipulate elliptic curves on projective spaces.

We call **projective space of** K, and denote it by $\mathbb{P}^2(K)$, the set of equivalent classes of the quotient of $\mathbb{P}^2[K] = \{(a : b : c) : a, b, c \in K\} \setminus \{(0 : 0 : 0)\}$ modulo the equivalence relation $\sim$ given by $(a : b : c) \sim (a' : b' : c')$ when there is some $t \neq 0$ such that $a' = at$, $b' = bt$, $c' = ct$.

The sum of points in this "plane", as in a vector space, is senseless. For instance it has no meaning to try to compute $(0 : 1 : 0) + (1 : 1 : 1)$. At first glance the result must be $(1 : 2 : 1)$, nonetheless these elements are equivalence classes, so by taking other representatives for each point, say $(0 : 4 : 0)$ and $(2 : 2 : 2)$, we obtain $(2 : 6 : 2)$, which is not equivalent to the previous $(1 : 2 : 1)$. Therefore the sum, coordinate by coordinate, is meaningless in this object.

In order to set a relationship between projective space and the affine universe we look at the application

$$\begin{aligned} \mathbb{A}^2(K) &\to \mathbb{P}^2(K) \\ (x, y) &\mapsto (x : y : 1). \end{aligned}$$

This map is injective with inverse $(x : y : z) \mapsto (x/z, y/z)$ for $z \neq 0$. Because of this, the affine space can be construed as embedded in the projective

space. The points that do not belong to the affine space (those with $Z = 0$) are called **points at infinity**.

If our purpose is to study elliptic curves in projective space, we consider other kind of polynomials. A **homogeneous polynomial of degree d** is a polynomial $F(x, y, z) \in K[X, Y, Z]$ which satisfies $F(tx, ty, tz) = t^d F(x, y, z)$.

Now consider a polynomial $f(x, y) = \sum a_{i,j} x^i y^j$ in $K[X, Y]$ of degree d. **The homogenization** of f in $\mathbb{P}^2(K)$ is the formal sum

$$F(X : Y : Z) = \sum_{i,j} a_{i,j} X^i Y^j Z^{d-i-j}. \tag{1.4}$$

It is clear that the homogenization of a polynomial is a homogeneous polynomial in one more variable.

On the other hand, by handling and reorganizing the variable Z at the right hand side of the equation we get the following.

Proposition 1.4. *The homogenization of $f(x, y)$ is equal to*

$$Z^d f(X/Z, Y/Z). \tag{1.5}$$

Thus $f(X/Z, Y/Z)$ is the quotient of two polynomials of the same degree. □

This expression helps us return to the affine plane. Let $F(X : Y : Z)$ be the homogenization of $f(x, y)$. We call **the dehomogenization** with respect to Z the polynomial

$$F(X : Y : 1). \tag{1.6}$$

Homogeneous polynomials are the only ones that allow us to maintain certain coherence when working in projective space. Let $F(X : Y : Z)$ be a homogeneous polynomial of degree d. By definition we have then $F(tX : tY : tZ) = t^d F(X : Y : Z)$. If $F(X_0 : Y_0 : Z_0) = 0$, then necessarily every element $(X_1 : Y_1 : Z_1)$ in the equivalence class of $(X_0 : Y_0 : Z_0)$ also satisfies $F(X_1 : Y_1 : Z_1) = 0$.

Another important feature is that although it seems mystic to grab the infinite and reach it at the line $Z = 0$, this does not make the variable Z a distinguished one. One must understand that the dehomogenization of a curve in projective plane can take three different roads, namely $Z = 1$, $Y = 1$ and $X = 1$. Thus taking $Z = 1$ only means that we are going to work with certain coordinates of projective space. Most probably, picking $Z = 1$ is the most natural one if we started with x, y in the affine plane.

Singularities can also be defined in the projective plane in the same way as in the affine case. Let $F(X : Y : Z)$ be a polynomial in $\mathbb{P}^2(K)$. The point

$P = (X_0 : Y_0 : Z_0)$ is a **singular point on the curve** $F(X : Y : Z) = 0$ if it satisfies

$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0.$$

Proposition 1.5. *If $F(X : Y : Z)$ is a homogeneous polynomial of degree d, then each partial derivative is a homogeneous polynomial of degree $d - 1$.*

Proof. From the definition we have

$$t\frac{\partial}{\partial X}F(tX : tY : tZ) = t^d \frac{\partial}{\partial X}F(X : Y : Z),$$

and the result follows. We use the same argument for the other coordinates. □

We analyze the relationship between a singular point in an affine curve and its homogenized version in projective space.

Proposition 1.6. *The point $(x_0/z_0, y_0/z_0)$ in the curve $f(x, y)$ in the affine plane is singular if and only if the corresponding point (X_0, Y_0, Z_0) with $Z_0 \neq 0$ is singular in the homogenization $F(X : Y : Z)$.*

Proof. By Equation (1.5) we have $F(X : Y : Z) = Z^d f(X/Z, Y/Z)$. Differentiating with respect to X, Y, Z we obtain

$$\begin{aligned}
\frac{\partial F}{\partial X}(X : Y : Z) =& Z^{d-1}\frac{\partial f}{\partial X}(X/Z, Y/Z),\\
\frac{\partial F}{\partial Y}(X : Y : Z) =& Z^{d-1}\frac{\partial f}{\partial Y}(X/Z, Y/Z),\\
\frac{\partial F}{\partial Z}(X : Y : Z) =& dZ^{d-1}f(X/Z, Y/Z) \quad -\\
& - Z^{d-2}(X\frac{\partial f}{\partial X}(X/Z, Y/Z) + Y\frac{\partial f}{\partial Y}(X/Z, Y/Z)).
\end{aligned}$$

The stated equivalence is now clear. □

The equation of the tangent line to a curve defined by means of a homogeneous polynomial has a simple form.

Proposition 1.7. *Let $F(X : Y : Z)$ be a homogeneous polynomial of degree d with a non-singular point P. Then a homogeneous tangent line at P is given by*

$$\frac{\partial F}{\partial X}(P)X + \frac{\partial F}{\partial Y}(P)Y + \frac{\partial F}{\partial Z}(P)Z = 0. \tag{1.7}$$

Proof. First notice that F must be non-constant, as otherwise all points are singular; thus we take $d > 0$ without further comment. From the definition of homogeneous polynomial we have

$$F(tX : tY : tZ) = t^d F(X : Y : Z). \tag{1.8}$$

Differentiating the left hand side with respect to t we get

$$\left[\frac{\partial F}{\partial X}(tX : tY : tZ)\ \frac{\partial F}{\partial Y}(tX : tY : tZ)\ \frac{\partial F}{\partial Z}(tX : tY : tZ)\right][X\ Y\ Z]^T.$$

By Proposition 1.5 the partial derivatives are homogeneous polynomials of degree $d-1$. Therefore this side of the equation has the form

$$t^{d-1}\left[\frac{\partial F}{\partial X}(X : Y : Z)\ \frac{\partial F}{\partial Y}(X : Y : Z)\ \frac{\partial F}{\partial Z}(X : Y : Z)\right][X\ Y\ Z]^T.$$

Differentiating the right hand side of (1.8) and comparing it with the left hand side we obtain

$$\frac{\partial F}{\partial X}X + \frac{\partial F}{\partial Y}Y + \frac{\partial F}{\partial Z}Z = d \cdot F(X : Y : Z).$$

Finally we evaluate at P and achieve the desired result. □

We state a crucial theorem that we have used before without proof. For further details see [8, page 237].

Theorem 1.8. ***(Bezout)*** *For projective curves C_1 and C_2 without common factors, we have*

$$\sum_{P \in C_1 \cap C_2} I(C_1 \cap C_2, P) = (\deg C_1)(\deg C_2). \tag{1.9}$$

Here $I(C_1 \cap C_2, P)$ stands for the multiplicity of P at the intersection of C_1 and C_2 which can be interpreted as the degree of tangency of both curves at P. So, if we have a line and a cubic curve with two distinct points of intersection then a third point of intersection necessarily pops.

1.3 Weierstrass normal forms

By a **Weierstrass normal form** we mean any of the following polynomial relations

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.10}$$

$$y^2 = x^3 + ax^2 + bx + c, \tag{1.11}$$

$$y^2 = x^3 + ax + b. \tag{1.12}$$

Every elliptic curve can be transformed into one of these forms depending on the characteristic of the defined ground field.

First we reveal the universal nature of the point $O = (0 : 1 : 0)$ over the homogenized version of the curve (1.10). For that we first homogenize

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3. \tag{1.13}$$

Next we need the tangent line at O: following Proposition 1.7 we find the partial derivatives

$$\begin{aligned}\frac{\partial F}{\partial X}(O) &= 0,\\ \frac{\partial F}{\partial Y}(O) &= 0,\\ \frac{\partial F}{\partial Z}(O) &= 1.\end{aligned}$$

We conclude easily that $Z = 0$ is the tangent line at O. Next we intersect the curve in projective space with the projective line $Z = 0$ at infinite, the result being $X^3 = 0$; that is, the point O has a triple contact, which by definition is called an **inflexion point**.

Proposition 1.9. *Every elliptic curve can be transformed into a Weierstrass normal form.*

Proof. Suppose an elliptic curve has a rational point P. By the theorem of Bezout, the tangent at this point meets three times the curve. Two options emerge: the tangent line contacts three times the point P, and so is an inflexion point, or the line contacts P two times and one time a different point in the curve.

In the first case we want to resettle the point P in O and carry the tangent line at P to the line $Z = 0$. For this purpose we change coordinates through a linear inversible transformation. In this way we obtain the equation

$$aX^3+bX^2Y+cXY^2+dY^3+eX^2Z+fXYZ+gY^2Z+hXZ^2+iYZ^2+jZ^3 = 0$$

with $d = 0$ because the point $(0 : 1 : 0)$ belongs to the curve. Moreover, as the tangent line at this point is $Z = 0$, we find the partial derivatives

$$\begin{aligned}\frac{\partial F}{\partial X} &= 3aX^2 + 2bXY + cY^2 + 2eXZ + fYZ + hZ^2,\\ \frac{\partial F}{\partial Y} &= bX^2 + 2cXY + fXZ + 2gYZ + iZ^2,\\ \frac{\partial F}{\partial Z} &= eX^2 + fXY + gY^2 + 2hXZ + 2iYZ + 3jZ^2\end{aligned}$$

and evaluate at O to obtain

$$\frac{\partial F}{\partial X}(O) = c, \ \frac{\partial F}{\partial Y}(O) = 0, \ \frac{\partial F}{\partial Z}(O) = g.$$

In this way the tangent line is

$$cX + gZ = 0.$$

We get $c = 0$ and $g \neq 0$. Evaluating the curve at $Y = 1$ and $Z = 0$ gives us

$$X^2(aX + b) = aX^3 + bX^2 = 0.$$

In order to obtain a triple contact we must have $b = 0$ and $a \neq 0$. So far the equation of the curve reduces to

$$gY^2Z + fXYZ + iYZ^2 = -aX^3 - eX^2Z - hXZ^2 - jZ^3.$$

Changing the variables from X to $-agX$ and Y to a^2gY and returning to the affine space through the immersion $Z = 1$ we obtain

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

as desired.

Suppose now P is not an inflexion point. In this framework the tangent line has a double contact and intersects transversally the curve at Q, another rational point. If Q is an inflexion point, we start all over again using the just described method and proceed accordingly. Therefore we assume it is not an inflexion point. Then we trace the tangent at Q and by Bezout obtain the point R on the elliptic curve. As the three points P, Q, and R are not colinear, we can define a linear invertible transformation which carries P, Q and R to $(1 : 0 : 0)$, $(0 : 1 : 0)$ and $(0 : 0 : 1)$, respectively. Let the equation

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

describe the transformed elliptic curve. The coefficients a, d and j are null since the points $(1 : 0 : 0)$, $(0 : 1 : 0)$ and $(0 : 0 : 1)$ belong to the curve. Then the equation simplifies to

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

By the nature of the construction of P, Q and R, the tangent line at P will be carried to the line that passes through $(1 : 0 : 0)$ and $(0 : 1 : 0)$; this

is $Z = 0$. By the same reason the tangent line at Q is carried to $X = 0$ through the linear transformation. Setting these conditions in the curve, the coefficients of the tangent at $(1 : 0 : 0)$ become

$$\begin{aligned}\frac{\partial F}{\partial X}((1:0:0)) &= 0,\\ \frac{\partial F}{\partial Y}((1:0:0)) &= b,\\ \frac{\partial F}{\partial Z}((1:0:0)) &= e;\end{aligned}$$

hence we get $b = 0$ and $e \neq 0$. The coefficients of the tangent line at $(0 : 1 : 0)$ are

$$\begin{aligned}\frac{\partial F}{\partial X}((0:1:0)) &= c,\\ \frac{\partial F}{\partial Y}((0:1:0)) &= 0,\\ \frac{\partial F}{\partial Z}((0:1:0)) &= g;\end{aligned}$$

so we get $g = 0$ and $c \neq 0$. The defining polynomial is now

$$F(X, Y, Z) = cXY^2 + eX^2Z + fXYZ + hXZ^2 + iYZ^2. \tag{1.14}$$

We use the non linear transformations

$$\begin{aligned}\alpha(X, Y, Z) =&(XZ : XY : Z^2),\\ \beta(X, Y, Z) =&(X^2 : YZ : XZ)\end{aligned}$$

that take rational points into rational points. The compositions $\alpha \circ \beta$ and $\beta \circ \alpha$ work as the identity except for the points $(1 : 0 : 0)$, $(0 : 1 : 0)$ and $(0 : 0 : 1)$. Multiplying Equation (1.14) by XZ^2 and changing the variables to $U = XZ$, $V = XY$ and $W = Z^2$, we obtain

$$cV^2W + eU^3 + fUVW + hU^2W + iVW^2 = 0.$$

Dividing by e and replacing W by W/c, we obtain the Weierstrass form

$$V^2W + a_1UVW + a_3VW^2 = U^3 + a_2U^2W.$$

Finally we set $W = 1$, and conclude the proof. □

Working in a field K with $charK \neq 2$ allows us to accomplish the extra change of variable y by $y - (a_1x + a_3)/2$, and we obtain the equation $y^2 = x^3 + ax^2 + bx + c$. If the field is also such that $charK \neq 3$, we can make the further change of x by $x - a/3$ and obtain the equation $y^2 = x^3 + ax + b$.

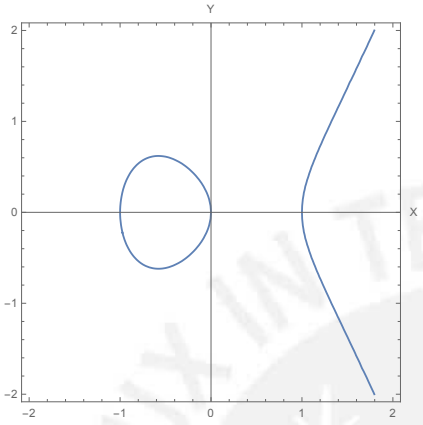

Figure 1.1: $y^2 = x^3 - x$

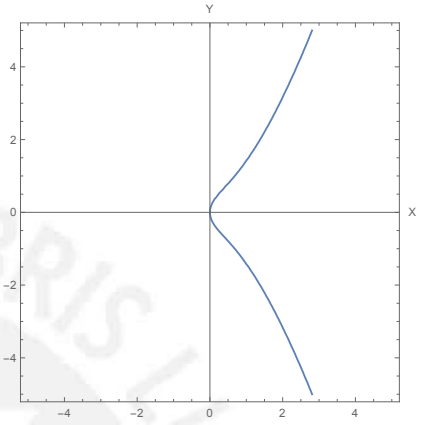

Figure 1.2: $y^2 = x^3 + x$

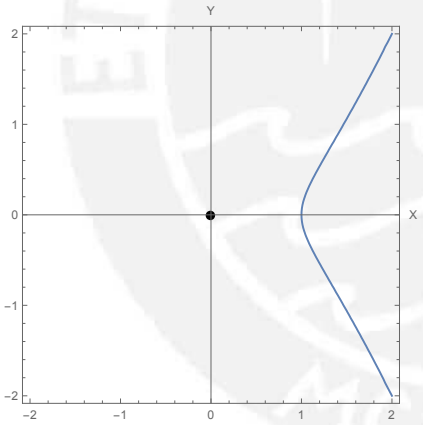

Figure 1.3: $y^2 = x^3 - x^2$

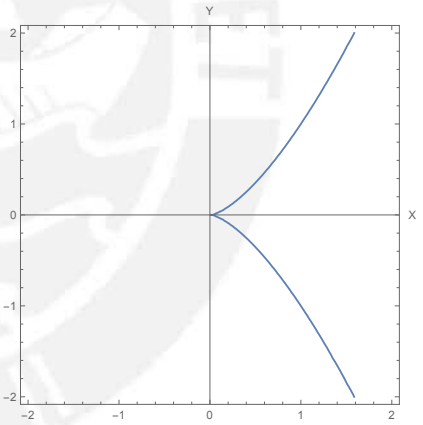

Figure 1.4: $y^2 = x^3$

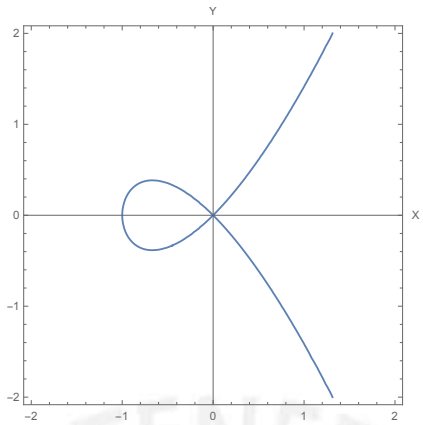

Figure 1.5: $y^2 = x^3 + x^2$

1.4 Examples

Example 1.10. Take the Fermat's elliptic curve $x^3+y^3 = 1$ of a field K with $charK \neq 2, 3$. We will obtain the three versions of the Weierstrass normal form.

The homogenized version of the curve is $X^3 + Y^3 - Z^3 = 0$. The point $(1 : -1 : 0)$ is an inflexion point with tangent line $X + Z = 0$. Applying the projective linear transformation $(X, Y, Z) \mapsto (Z - X - Y, X + Z, X + Y)$ we get

$$3Y^2Z + 6XYZ - 3YZ^2 = -X^3 + 6XZ^2.$$

Changing the variables X to $-3X$ and Y to $3Y$ results in the equation

$$Y^2Z - 2XYZ - \frac{1}{3}YZ^2 = X^3 - \frac{2}{3}XZ^2,$$

whose affine representation is given by

$$y^2 - 2xy - \frac{1}{3}y = x^3 - \frac{2}{3}x.$$

Then we change the variable y to $y + x + \frac{1}{6}$. After some toiling we obtain

$$y^2 = x^3 + x^2 - \frac{1}{3}x + \frac{1}{36}.$$

Finally we replace the variable x by $x - 2$ to get

$$y^2 = x^3 - \frac{2}{3}x + \frac{23}{108}.$$

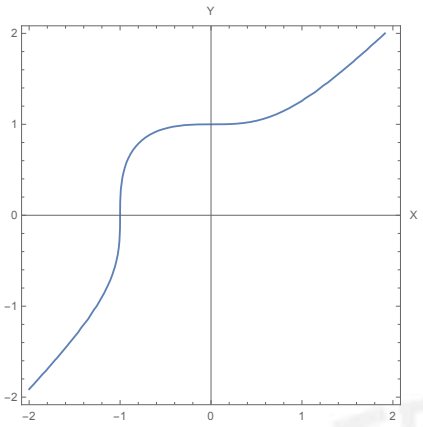

Figure 1.6: $x^3 + y^3 = 1$

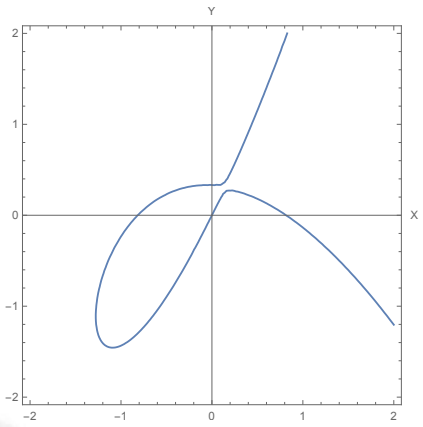

Figure 1.7: $y^2 - 2xy - \frac{1}{3}y = x^3 - \frac{2}{3}x$

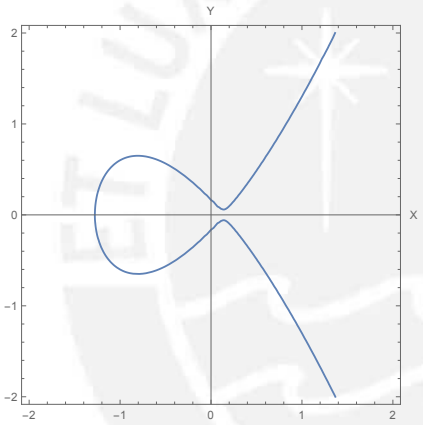

Figure 1.8: $y^2 = x^3 + x^2 - \frac{1}{3}x + \frac{1}{36}$

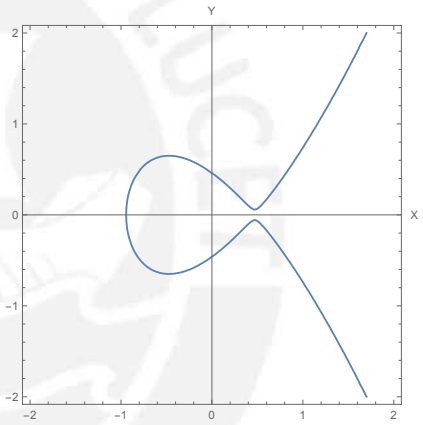

Figure 1.9: $y^2 = x^3 - \frac{2}{3}x + \frac{23}{108}$

Example 1.11. Consider the non-singular cubic equation $x^3+y^3+x^2-y^2+1=0$, whose homogenized version is $X^3 + Y^3 + X^2Z - Y^2Z + Z^3 = 0$. The point $(1 : -1 : 0)$ is an inflexion point of the curve. We apply the projective linear transformation $(X, Y, Z) \mapsto (X + Y + Z, -X - Y, X)$ and obtain

$$3Y^2Z + 8XYZ + 3YZ^2 = -X^3 - 5X^2Z - 4XZ^2 - Z^3.$$

Changing the variables X to $-3X$ and Y to $3Y$, we get

$$Y^2Z - 8/3XYZ + 1/3YZ^2 = X^3 - 5/3X^2Z + 4/9XZ^2 - 1/27Z^3$$

whose representation in the affine plane is given by

$$y^2 - \frac{8}{3}xy + \frac{1}{3}y = x^3 - \frac{5}{3}x^2 + \frac{4}{9}x - \frac{1}{27}.$$

Replacing y by $y - (-8/3x + 1/3)/2$ results in

$$y^2 = x^3 + \frac{1}{9}x^2 - \frac{1}{108};$$

and replacing x by $x - 1/27$ results in

$$y^2 = x^3 - \frac{1}{243}x - \frac{721}{78732}.$$

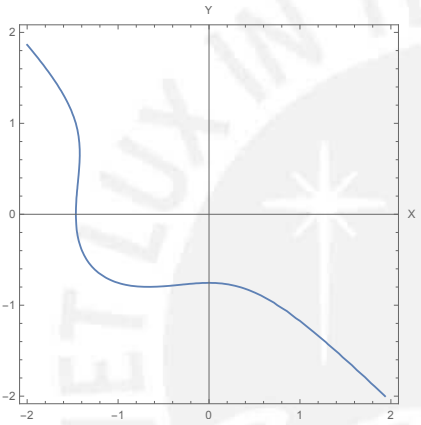

Figure 1.10: $x^3+y^3+x^2-y^2+1=0$

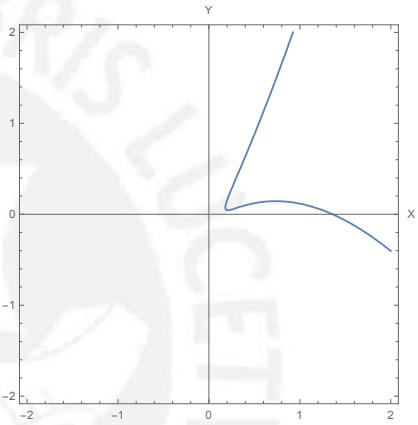

Figure 1.11: $y^2 - \frac{8}{3}xy + \frac{1}{3}y = x^3 - \frac{5}{3}x^2 + \frac{4}{9}x - \frac{1}{27}$

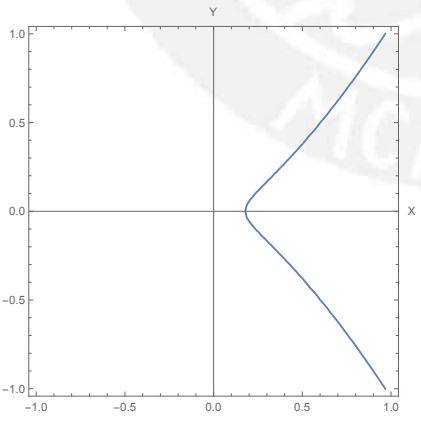

Figure 1.12: $y^2 = x^3+\frac{1}{9}x^2-\frac{1}{108}$

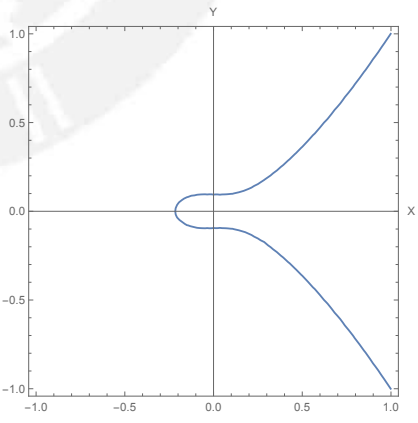

Figure 1.13: $y^2 = x^3 - \frac{1}{243}x - \frac{721}{78732}$

Chapter 2

Groups over elliptic curves

In the present chapter we are concerned with the structural aspects of elliptic curves from the purely algebraic point of view. In particular we define a group over its set of rational points.

2.1 Preliminaries

An easy application of Bezout's theorem states that every line over $K[X, Y]$ that intersects an elliptic curve twice in fact cuts it a third time. This is the starting point to set a group structure in an elliptic curve.

As before, we are going to work with elliptic curves of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{2.1}$$

with a preferred point $O = (0 : 1 : 0)$, which happens to be an inflexion point and the unique point of the curve at infinity.

We state the following proposition about a defining property of the projective lines that meet the curve at infinity.

Proposition 2.1. *The projective lines of the form $X = x_0Z$ are the only ones different from $Z = 0$ that cut the curve at infinity.*

Proof. In general a projective line has the form $\alpha_1X + \alpha_2Y + \alpha_3Z = 0$. As O is the only point of the curve at infinity, then O must belong to the projective line, therefore we get $\alpha_2 = 0$. Also as we are not considering $Z = 0$ we must have $\alpha_1 \neq 0$, so we get $X = -\alpha_3/\alpha_1 Z$. By setting $x_0 = -\alpha_3/\alpha_1$ and dehomogenizing we obtain the result. □

Next take points P and Q on the elliptic curve $\mathcal{C}$. Recalling Bezout's theorem we know that if we draw the line through P and Q, this line must

intercept the curve at another point: call this point $P * Q$ (compare Figure 2.1). In this way the operation $* : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ is established. Notice that there is no extra burden in finding a third point if we have $P = Q$: it simply happens that the line becomes the tangent line. Also, as O is an inflexion point we have $O * O = O$. To familiarize ourselves with $*$ we state the following preliminary result.

Proposition 2.2. *Take points P, Q in the elliptic curve. The operation $*$ is commutative and satisfies $(P * Q) * P = Q$.*

Proof. Commutativity follows inmediately by definition because the line from P to Q is the same as the line from Q to P. The other claim is clear because $P * Q$ is the third point on the curve resulting from the intersection of the line that joins P and Q and the curve. Focusing on $P * Q$ and P now the third point must be Q. □

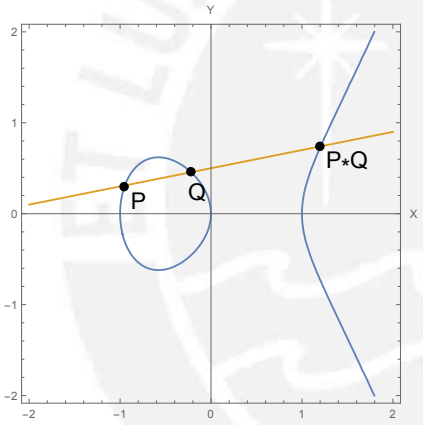

Figure 2.1: P, Q and $P * Q$

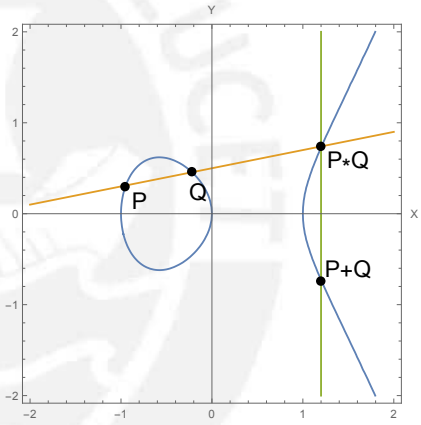

Figure 2.2: $P + Q$

2.2 Sum of points

Take points P, Q on the elliptic curve $\mathcal{C}$. We define the **sum of P and Q** to be

$$P + Q = (P * Q) * O. \tag{2.2}$$

It turns out that this simple operation satisfies several important relations.

Proposition 2.3. *Take points P, Q, R on the elliptic curve. Then the sum $+$ must satisfy the following properties:*

1. $P + Q = Q + P$,

2. $P + O = P$,

3. *if the points* P, Q, R *are colinear, then*

$$(P + Q) + R = O, \tag{2.3}$$

4. *there exists a point* $-P$ *of the curve which satisfies*

$$P + (-P) = O. \tag{2.4}$$

Proof. As the operation $*$ is commutative we have $P * Q = Q * P$. Thus we get $P + Q = (P * Q) * O = (Q * P) * O = Q + P$. By definition of $+$ we have $P + O = (P * O) * O$. Again by the commutativity of the operation $*$ we get $(P*O)*O = (O*P)*O$. Thus by Proposition 2.2 we obtain $(P*O)*O = P$, which is equivalent to $P + O = P$. Next, if P, Q, R are colinear we get $P + Q = (P * Q) * O = R * O$. In this way $(P + Q) + R = ((R * O) * R) * O$. From Proposition 2.2 we know that $(R * O) * R = O$ holds, and this yields $(P + Q) + R = O * O = O$. Finally take O, P, R colinear. By the preceding item we have $(P + O) + R = O$, therefore it is enough to set $R = -P$. □

In the next chapter, we develop the theory of divisors in order to proof the associative property; this gives us an elegant proof of this fact. If we take this for granted, then the preceding proposition shows that the K-rational points together with $+$ ensemble a group on elliptic curves.

2.3 Explicit expression of the sum

We find the explicit expression for the sum of points over an elliptic curve of the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ in $K[X, Y]$. To achieve this goal we take the line $y = \alpha x + \beta$ that passes through the distinct rational points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, where $\alpha = (y_2 - y_1)/(x_2 - x_1)$ and $\beta = (y_1x_2 - x_1y_2)/(x_2 - x_1)$. We plug in the equation of the line in the equation of the elliptic curve and obtain the cubic equation

$$x^3 + (a_2 - \alpha^2 - a_1\alpha)x^2 + (a_4 - 2\alpha\beta - a_1\beta - a_3\alpha)x + a_6 - \beta^2 - a_3\beta = 0,$$

whose solutions represent the x-coordinates of the three points of intersection of the line with the curve. In particular we realize that $x_3 + x_2 + x_1 = -a_2 + \alpha^2 + a_1\alpha$ holds, and so we have

$$\begin{aligned} x_3 &= \alpha^2 + a_1\alpha - a_2 - (x_1 + x_2), \\ y_3 &= \alpha^3 + a_1\alpha^2 - (a_2 + x_1 + x_2)\alpha + \beta. \end{aligned}$$

We replace x_3 in the equation of the elliptic curve in order to obtain

$$y^2 + (a_1x_3 + a_3)y - (x_3^3 + a_2x_3^2 + a_4x_3 + a_6) = 0. \tag{2.5}$$

In view of the K-rational nature of one solution of the latter equation, the other one must also be K-rational. In addition, the sum of the solutions of this equation is equal to the negative of the associated coefficient of y. Thus the second solution is precisely $\widetilde{y}_3 = -y_3 - (a_1x_3 + a_3)$. According to Proposition 2.1 the point $(x_3, \widetilde{y}_3)$ represents $P + Q$.

2.4 Examples

Example 2.4. For the elliptic curve

$$y^2 = x^3 + 17, \tag{2.6}$$

the points $P = (4, 9)$ and $Q = (8, 23)$ are points within. We want to find $-P$ and $-Q$. According to the previous explanation this is an easy task. We just have to find the points $P*O$ and $Q*O$ on the curve. As mentioned early, this is equivalent to find the other points of intersection of the curve and the lines $x = x_P$, $x = x_Q$, respectively. Since this elliptic curve is symetrical respect to the x-axis, the points $-P$ and $-Q$ are $(4, -9)$ and $(8, -23)$, accordingly.

Another interesting computation is associated to the double of a point. Now we are looking for the point $2P$, which must lay on the curve. As we are performing the sum $P + P$, this means that the intersecting line is now the tangent line to the curve on P, which is

$$3y - 8x + 5 = 0. \tag{2.7}$$

The resulting equation that expresses this intersection is

$$9x^3 - 64x^2 + 80x + 128 = 0. \tag{2.8}$$

So we have $x_{P*P} = 64/9 - 2 \times 4 = -8/9$, and thus also $y_{P*P} = -109/27$. We finally get $2P = (-8/9, 109/27)$ by intersecting the curve with the vertical line $x = -8/9$ or just reflecting $P * P$ along the x-axis.

Next we compute $P + Q$ following the previously explained algorithm. First, we note that the equation of the line that passes through P and Q is

$$14x - 4y - 20 = 0. \tag{2.9}$$

Then we get the x-coordinate of $P * Q$ by intersecting it with the elliptic curve in order to get the system

$$\begin{aligned} y^2 - x^3 - 17 &= 0, \\ 14x - 4y - 20 &= 0. \end{aligned}$$

Replacing y in the first equation we obtain

$$x^3 - (7/2)^2 x^2 + 35x - 8 = 0. \tag{2.10}$$

Then we get

$$\begin{aligned} x_{P*Q} &= 49/4 - (x_P + x_Q) \\ &= 49/4 - (4 + 8) \\ &= 1/4. \end{aligned}$$

We replace x_{P*Q} in the equation of the line and obtain $y_{P*Q} = -33/8$. Therefore, we have $P*Q = (1/4, -33/8)$. Finally we get $P+Q$ by intersecting the elliptic curve with $x = 1/4$, and so we end up with $P + Q = (1/4, 33/8)$.

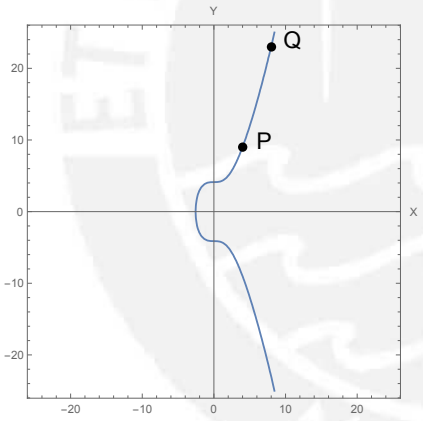

Figure 2.3: Curve $y^2 = x^3 + 17$ and points P, Q

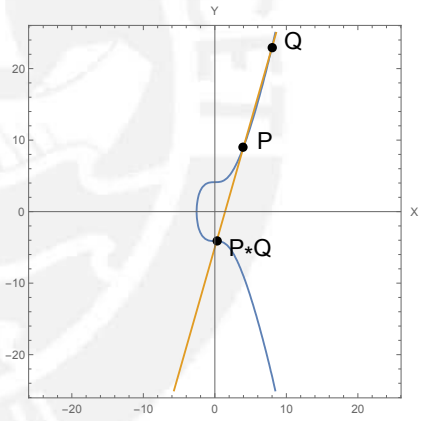

Figure 2.4: Curve $y^2 = x^3 + 17$ and point $P * Q$

Example 2.5. Another interesting example is the elliptic curve $y^2 = x^3 + 1$, which has $P = (2, 3)$ as rational point. According to the method just described we obtain $2P = (0, 1)$. Adding $P + 2P$ we get $3P = (-1, 0)$. Performing the sum repeatedly we have $4P = (0, -1)$ and $5P = (2, -3)$. We notice the equality $5P = -P$, so $6P = P + 5P = P - P = O$. Therefore the set $\{O, P, 2P, 3P, 4P, 5P\}$ is a subgroup of the set of rational points on the elliptic curve.

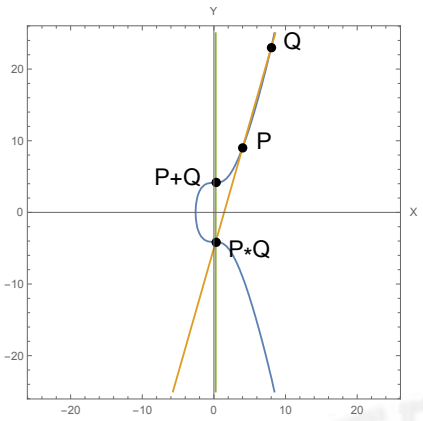

Figure 2.5: Curve $y^2 = x^3 + 17$ and point $P + Q$

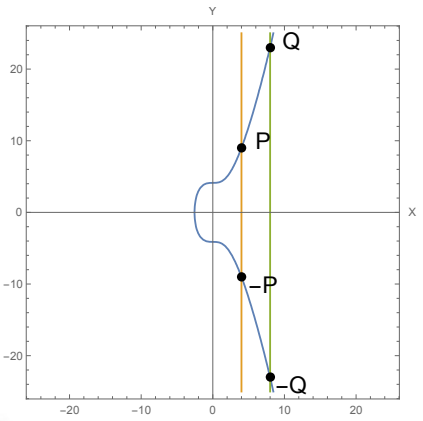

Figure 2.6: Curve $y^2 = x^3 + 17$ and points $-P, -Q$

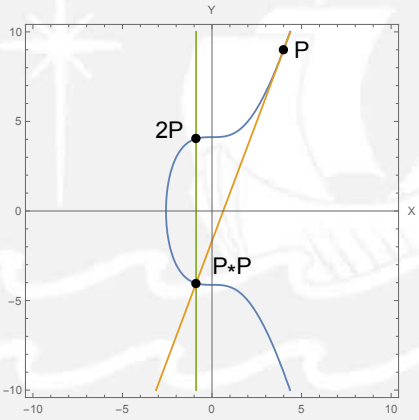

Figure 2.7: Curve $y^2 = x^3 + 17$ and point $2P$

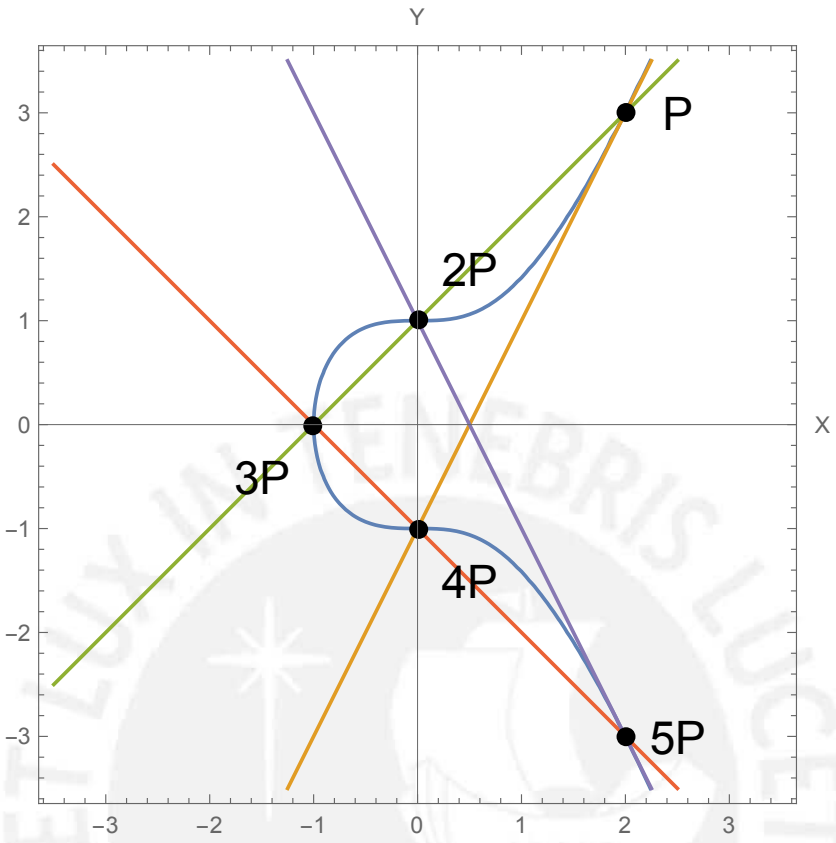

Figure 2.8: Curve $y^2 = x^3 + 1$ and the orbit of the point $P = (2, 3)$; the iterate $6P = O$ is at infinity.

Chapter 3

Associativity

In the previous chapter we learned how an inflexion point within an elliptic curve allows us to define a "sum". We showed that this structure satisfies all group properties but associativity. In this chapter we are concerned with this delicate task. To accomplish it we need the help of a tool from algebraic geometry: divisors. We are going to introduce key results about them that will help us build a proof.

Because of technical reasons, from now on we will focus in the case of fields of characteristic 0.

3.1 Divisors

A function f with poles in a finite set $S \subset X$ is called **meromorphic** if f is holomorphic on $X \setminus S$. We take a meromorphic function f, and denote the **order of f at the point P** as $ord_P(f)$. If $ord_P(f) > 0$ then f has a zero at P; if $ord_P(f) < 0$, then f has a pole at P. For the sake of completeness we write $ord_P(0) = +\infty$.

Proposition 3.1. *Let f, g be two meromorphic functions. Then the order at a point P satisfies the inequality*

$$ord_P(f+g) \geq min\{ord_P(f), ord_P(g)\}.$$

Proof. This is clear by writing f and g in coordinates. □

Another helpful fact is the logarithmic behavior of the order of a function at a point. This will help us provide a group structure in a set of divisors associated to rational functions.

Proposition 3.2. *Take f and g meromorphic functions. The order of a function at a point P satisfies*

$$ord_P(fg) = ord_P(f) + ord_P(g). \tag{3.1}$$

Proof. Again, this must be clear enough. □

A fundamental element in algebraic geometry is the concept of formal sum. A **divisor** is a formal sum of points

$$\sum_{P \in X} n_P P. \tag{3.2}$$

Here all the coefficients are in $\mathbb{Z}$ and only a finite number of them are non-zero.

We impose an algebraic structure on this new set of elements.

Proposition 3.3. *The set of divisors with sum defined as*

$$D_1 + D_2 = \sum_{P \in X} (n_P + m_P)P, \tag{3.3}$$

where $D_1 = \sum_{P \in X} n_P P$ and $D_2 = \sum_{P \in X} m_P P$, forms a group.

Proof. Clear; in fact, this group is abelian and free. □

We define an important homomorphism to be used later. Take a divisor $D = \sum_{P \in X} n_P P$. By the **degree** of the divisor D we mean the sum of its coefficients, this is, the integer

$$\deg(D) = \sum_{P \in X} n_P. \tag{3.4}$$

Now we provide another structural feature that would allow us compare two divisors in a similar fashion as how we compare a pair of natural numbers. However, in our case, the comparison will not be available for every pair of divisors. Let D_1 and D_2 be two divisors with coefficients n_P and m_P, respectively. An order $\geq$ is defined in the set of divisors by setting

$$D_1 \geq D_2 \tag{3.5}$$

whenever $n_P \geq m_P$ for every P.

Fix a point P, and note that the divisor P is always greater than the divisor $-P$. Anyhow, here we are unable to compare the divisors $D_1 = P - Q$, $D_2 = -P + Q$ even in this case in which we have $D_1 = -D_2$.

Now let f be a meromorphic function. By the **divisor** of f we mean the sum

$$div(f) = \sum_{P \in X} ord_P f \cdot P. \tag{3.6}$$

Similarly, we define an induced order: take two functions f and g and write

$$div(f) \geq div(g) \tag{3.7}$$

if $ord_P f \geq ord_P g$ for every P.

A **rational function** is the quotient of two polynomials. We call a divisor **principal** if it is the divisor of a rational function in the curve.

For the following examples consider the elliptic curve

$$y^2 = (x - x_1)(x - x_2)(x - x_3), \tag{3.8}$$

with x_1, x_2, x_3 different.

Example 3.4. Take the rational function given by

$$x - x_1. \tag{3.9}$$

(Actually, for this to be a rational function, we must express it in projective coordinates). We are looking for zeros and poles of this function. For this purpose we pass to projective coordinates and obtain

$$Y^2 Z = (X - x_1 Z)(X - x_2 Z)(X - x_3 Z), \tag{3.10}$$

for the elliptic curve, and

$$\frac{X - x_1 Z}{Z}, \tag{3.11}$$

for the rational function. Handling the equation of the elliptic curve we get

$$\frac{Y^2}{(X - x_2 Z)(X - x_3 Z)} = \frac{X - x_1 Z}{Z}. \tag{3.12}$$

This sets an equivalence between the analyzed function on the right hand side and another rational function on the left side. The equation also provides an example of the fact that a rational function on an elliptic curve does not have a unique presentation. Thus we can take advantage of this phenomenon and evaluate points where we feel more comfortable.

The left hand side can be expressed as

$$\frac{Y}{X - x_2 Z} \times \frac{Y}{X - x_3 Z} \tag{3.13}$$

where each factor has a simple pole at $(0:1:0)$ and a zero at $(x_1:0:1)$. Writing $P_1 = (x_1:0:1)$, $P_2 = (x_2:0:1)$ and $P_3 = (x_3:0:1)$, we conclude that the divisor of the rational function is given by

$$div(x - x_1) = 2P_1 - 2O. \tag{3.14}$$

Example 3.5. Consider the rational function

$$\frac{y}{x - x_1}, \tag{3.15}$$

with projective version equal to

$$\frac{Y}{X - x_1 Z}. \tag{3.16}$$

Again, handling the equation of the elliptic curve we arrive at

$$\frac{Y}{(X - x_1 Z)} = \frac{(X - x_2 Z)(X - x_3 Z)}{YZ}. \tag{3.17}$$

If we evaluate the points $(x_2:0:1)$ and $(x_3:0:1)$ on the right hand side we obtain $0/0$, yet the left side indicates us that these points are different zeroes of the rational function. In a similar manner we conclude that the poles are precisely $(x_1:0:1)$ and $(0:1:0)$. Thus we get

$$div(y/(x - x_1)) = P_2 + P_3 - P_1 - O. \tag{3.18}$$

Example 3.6. Given the rational function x we want to find its poles. Expressing the elliptic curve as $y^2 = x^3 + ax^2 + bx + c$ we obtain $x = (y^2 - c)/(x^2 + ax + b)$. Passing to projective coordinates we have

$$\frac{X}{Z} = \frac{Y^2 - cZ^2}{X^2 + aXZ + bZ^2} = \frac{Y^2 - cZ^2}{(X + dZ)(X + eZ)}. \tag{3.19}$$

The conclusion is that x has zeroes at $(0:\pm\sqrt{c}:1)$ as well as a pole of order two at $(0:1:0)$.

Notice that in all our examples the degree of the divisor was zero. As we will show briefly, this is not mere coincidence.

Proposition 3.7. *For f, g meromorphic functions, we have*

$$div(fg) = div(f) + div(g).$$

Proof. This is a direct consequence of the formula $ord_P(fg) = ord_P(f) + ord_P(g)$ of Proposition 3.2. □

Proposition 3.8. *The set of principal divisors forms a subgroup of the divisor group.*

Proof. This is clear from Proposition 3.2 since fg is a meromorphic function that satisfies

$$D_1 + D_2 = \sum_{P \in X} ord_P(fg)P, \tag{3.20}$$

while the inverse of an element, say D_1, is just $\sum_{P\in X}(ord_P f^{-1})P = \sum_{P\in X} -(ord_P f)P$. □

Next we disclose a relevant property valid for rational functions.

Proposition 3.9. *The degree of every principal divisor is zero.*

Proof. Consider the rational function $f = g/h$. Set G/H a projective version; here G and H are polynomials of the same degree in projective space. By Bezout, as none of the polynomials can have common factors with the elliptic curve, each one must intersect the elliptic curve an equal number of times, say $3m$. As the divisor of f is $div(f) = div(G) - div(H)$, we get $\deg(div(f)) = 3m - 3m = 0$. □

Divisors provide another interpretation of intersection of curves. For example take two curves C_1 and C_2 with no common factor represented by polynomials in two variables. Take f for the curve C_2. We analize the divisors associated to f on the first curve. Passing to the projective plane, by definition we have

$$div(f) = \sum_{P \in C_1} (n_P)P. \tag{3.21}$$

But the zeroes of f are the points at which both curves intersect each other, and by Bezout, we know this number. Hence we can write alternatively

$$div(f) = \sum_{P \in C_1 \cap C_2} I(P) \cdot P - \sum_{Q \in T \cap C_2} n_Q Q, \tag{3.22}$$

where I is the index function as in the Bezout theorem and T is the set of poles of f, each element counted with multiplicity n_Q.

Our next concern is divisor classification. For this we establish a criterion to determine equivalence among divisors. Two divisors D_1 and D_2 are **equivalent**, and we write $D_1 \sim D_2$, if $D_1 - D_2$ is principal.

Example 3.10. Take the points P, Q, $P+Q$ and O on a fixed elliptic curve. Define the divisors $D_1 = P + Q$ and $D_2 = (P + Q) + O$ and set $\mathcal{L}_1$ to be the projective line that passes through P and Q, and $\mathcal{L}_2$ the one that passes through $P + Q$ and O. By the imposed group structure, $\mathcal{L}_1$ and $\mathcal{L}_2$ intersect the elliptic curve at a common point $R = P * Q$. Let L_1 and L_2 be the equations of the corresponding projectives lines. Then $div(L_1) = P + Q + R$ and $div(L_2) = (P + Q) + R + O$. We define the rational function f on the elliptic curve as L_1/L_2. Thus we obtain

$$\begin{aligned} div(f) &= div(L_1) - div(L_2), \\ &= P + Q - (P + Q) - O, \\ &= D_1 - D_2. \end{aligned}$$

We conclude that $D_1 = P + Q$ and $D_2 = (P + Q) + O$ are equivalent.

3.2 Canonical divisors

We present 1-forms on curves. These elements enrich the structure by adding differentiable features to curves. We will focus on extending the concepts defined for divisors to the vector space of 1-forms.

We denote $\bar{K}(\mathcal{C})$ the field of rational functions on the elliptic curve $\mathcal{C}$ with coefficients in $\bar{K}$, an algebraic closure of K.

We call **uniformizer** of $\mathcal{C}$ at P a generator of the maximal ideal at P of the coordinate ring.

Fix an elliptic curve $\mathcal{C}$ and consider the $\bar{K}(\mathcal{C})$-vector space generated by the forms df, where $f \in \bar{K}(\mathcal{C})$. The following basic relations are satisfied:

1. $d(f + g) = df + dg$, for all $f, g \in \bar{K}(\mathcal{C})$,
2. $d(fg) = fdg + gdf$, for all $f, g \in \bar{K}(\mathcal{C})$,
3. $d\alpha = 0$, for all $\alpha \in \bar{K}$.

We call this vector space **the space of differential forms on** $\mathcal{C}$ and we denote it by $\Omega_{\mathcal{C}}$.

We require two results in order to continue (the second one without proof since its justification involves a broader view of algebraic geometry and is outside the scope of these notes. For more details we refer to [7, page 31]).

Proposition 3.11. *The space $\Omega_{\mathcal{C}}$ is a $\bar{K}(\mathcal{C})$-vector space of dimension 1.*

Proof. In some sense it is clear that the space $\Omega_{\mathcal{C}}$ lies inside the two dimensional space spaned by dx and dy because in affine space we have $dz = 0$. We make this precise first.

Notice, as in the previous sections, that the rational function x only makes sense as X/Z, while y is really a shorthand for Y/Z. For them we have

$$dx = \frac{dX}{Z} - \frac{X dZ}{Z^2}, \qquad dy = \frac{dY}{Z} - \frac{Y dZ}{Z^2}.$$

Because the curve interects the line at infinity at a single point, it is trivial to see that all rational functions on $\mathcal{C}$ can be expressed as a quotient $F(X/Z, Y/Z)/G(X/Z, Y/Z)$ for suitable chosen polynomials F and G. A straight-forward calculation yields then

$$d\left(\frac{F}{G}\right) = \frac{F_x}{G}dx + \frac{F_y}{G}dy - \frac{F}{G^2}(G_x dx + G_y dy),$$

which clearly belongs to the $\overline{K}(\mathcal{C})$-span of dx and dy as $F(\frac{X}{Z}, \frac{Y}{Z})$, $G(\frac{X}{Z}, \frac{Y}{Z})$, $F_x(\frac{X}{Z}, \frac{Y}{Z})$ and $G_x(\frac{X}{Z}, \frac{Y}{Z})$ are rational functions on $\mathcal{C}$. Thus dx and dy are enough to generate $\Omega_{\mathcal{C}}$.

For $F(x, y) = 0$, the equation of the curve, we get $dF = \frac{\partial F}{\partial x}dx + \frac{\partial F}{\partial y}dy$. However we have $dF = 0$, and thus also $dy = \frac{\partial F}{\partial x}/\frac{\partial F}{\partial y}dx$, which is well defined because the curve is nonsingular. Therefore we need dx alone in order to generate $\Omega_{\mathcal{C}}$. □

Proposition 3.12. *Fix the curve $\mathcal{C}$ together with a point P in it. For a uniformizer $t \in \bar{K}(\mathcal{C})$ at P, we have the following.*

- *There exists a unique function $g \in \bar{K}(\mathcal{C})$ for each differential form $\omega \in \Omega_{\mathcal{C}}$ (which depends on ω and the uniformizer t) that satisfies*

$$\omega = g dt. \tag{3.23}$$

  This function g will be symbolized by ω/dt.

- *Take $\omega \in \Omega_{\mathcal{C}}$, with $\omega \neq 0$. The quantity*

$$ord_P(\omega/dt) \tag{3.24}$$

  depends only on ω and P in the sense that it is independent of the uniformizer t. We call this value ***the order of*** *ω* ***at*** *P and denote it by $ord_P(\omega)$.*

- *For $f \in \bar{K}(\mathcal{C})$ and P such that $x(P) = 0$ we have*

$$ord_P(fdx) = ord_P(f) + ord_P(x) - 1. \tag{3.25}$$

□

Consider a differential form $\omega \in \Omega_{\mathcal{C}}$. Define its **associated divisor** as

$$div(\omega) = \sum_{P \in \mathcal{C}} ord_P(\omega)(P). \tag{3.26}$$

From Proposition 3.11, as $\Omega_{\mathcal{C}}$ is a one dimensional vector space in $\bar{K}(\mathcal{C})$, any given two forms ω_1 and ω_2 are related by $\omega_2 = f\omega_1$, for a certain $f \in \bar{K}(\mathcal{C})$. In such case we have

$$div(\omega_2) = div(f) + div(\omega_1). \tag{3.27}$$

We call **canonical divisor class** the class on $\Omega_{\mathcal{C}}$ of the divisors of the differential forms modulo principal divisors and its elements **canonical divisors**.

Example 3.13. The differential form dx/y on an elliptic curve has associated the canonical divisor $div(dx/y)$.

From Formula 3.27 we conclude that all canonical divisors have the same degree.

3.3 Riemann-Roch

We will face one of the main theorems in algebraic geometry, the Riemann-Roch theorem. In order to understand its details we need a profound knowledge of the topic, which is out of our scope. The interested reader can take a look at [9] for a deeper insight.

Take a divisor D, and define the **Riemann-Roch space** of D as the set

$$\mathcal{L}(D) = \{g \in \bar{K}(\mathcal{C})^* \mid div(g) + D \geq 0\} \cup \{0\}, \tag{3.28}$$

where $\bar{K}(\mathcal{C})^*$ is the set of non-zero elements of the function field of rational functions on $\mathcal{C}$ over $\bar{K}$, an algebraic closure of K.

Proposition 3.14. *For a divisor D, the set $\mathcal{L}(D)$ is a $\bar{K}(\mathcal{C})$-vector space.*

Proof. Let $D = \sum n_P P$. For rational functions $f, g \in \mathcal{L}(D)$ and λ a non zero constant, by Proposition 3.7, we have $div(\lambda f) = div(\lambda) + div(f)$. But as we have $div(\lambda) = 0$, we get then $div(\lambda f) = div(f)$; hence $\lambda f \in \mathcal{L}(\mathcal{D})$. By Proposition 3.1 we know that $ord_P(f+g) \geq \min\{ord_P(f), ord_P(g)\}$ holds, and by hypothesis we have $\min\{ord_P(f), ord_P(g)\}+n_P \geq 0$. Putting together these two facts we achieve $ord_P(f+g) + n_P \geq 0$, and this boils down to $f + g \in \mathcal{L}(\mathcal{D})$. □

Proposition 3.15. *For D_1 and D_2 divisors subject to $D_1 \sim D_2$, the spaces $\mathcal{L}(D_1)$ and $\mathcal{L}(D_2)$ are isomorphic.*

Proof. By hypothesis we have $D_1 = div(f) + D_2$ with f a rational function on the curve. For $g \in \mathcal{L}(D_1)$, this is, with $div(g) + D_1 \geq 0$, we get $div(gf) + D_2 \geq 0$, and so we have $gf \in \mathcal{L}(D_2)$. In the same way we show that $g \in \mathcal{L}(D_2)$ implies $g/f \in \mathcal{L}(D_1)$. In this way the isomorphism is clearly established. □

Notice that the last proposition delivers the following result in particular: canonical divisors have assigned isomorphic Riemann-Roch spaces.

Proposition 3.16. *If D is a divisor subject to $\deg(D) < 0$, we have $\mathcal{L}(D) = \{0\}$ for its Riemann-Roch space.*

Proof. Suppose we have $\deg(D) \leq 0$ and that there exists a non null rational function $f \in \mathcal{L}(\mathcal{D})$. By definition of the Riemann-Roch space for the divisor D, we have $div(f) + D \geq 0$. Then, applying the homomorphism deg, we get $\deg(div(f)) + \deg(D) = \deg(D) < 0$. This is a contradiction to $f \in \mathcal{L}(D)$; hence the result. □

Set $l(D)$ for the **dimension** of $\mathcal{L}(D)$.

Notice that if $K_\mathcal{C}$ is a canonical divisor $\mathcal{L}(K_\mathcal{C})$ might depend on our choice. However, Proposition 3.15 makes it clear that the number $l(K_\mathcal{C})$ is indeed canonical.

To keep things in perspective, we state the following theorem without proof (compare Zuñiga [9]).

Theorem 3.17. ***(Riemann-Roch theorem)*** *Let $\mathcal{C}$ be a smooth curve and $K_\mathcal{C}$ a canonical divisor on $\mathcal{C}$. Then there is an integer $g \geq 0$, which we call the **genus** of $\mathcal{C}$, that satisfies the relation*

$$l(D) - l(K_\mathcal{C} - D) = \deg(D) - g + 1$$

for all divisors D. □

Corollary 3.18. *For a fixed curve $\mathcal{C}$ we have*

1. $l(K_{\mathcal{C}}) = g$,
2. $\deg K_{\mathcal{C}} = 2g - 2$,
3. *if* $\deg(D) > 2g - 2$, *then* $l(D) = \deg(D) - g + 1$.

Proof. 1. The result follows by taking $D = 0$, as $\mathcal{L}(0)$ is the space of constants.

2. Taking $D = K_{\mathcal{C}}$ in the Riemann-Roch theorem, we have $l(K_{\mathcal{C}}) - 1 = \deg(K_{\mathcal{C}}) - g + 1$. By the previous item we get then $\deg K_{\mathcal{C}} = 2g - 2$.

3. If $\deg(D) > 2g - 2$, then $\deg(-D) + 2g - 2 < 0$. By previous item we get $\deg(K_{\mathcal{C}} - D) < 0$. By Proposition 3.16 we obtain then $l(K_{\mathcal{C}} - D) = 0$. Using the Riemann-Roch we achieve the desired result. □

For the following statement we rely in most properties of the theory of divisors developed so far.

Proposition 3.19. *The genus of the elliptic curve*

$$\mathcal{C} : y^2 = (x - x_1)(x - x_2)(x - x_3) \tag{3.29}$$

is 1.

Proof. Key here is to show that the canonical divisor $div(dx/y)$ is equal to 0 and then apply the Riemann-Roch theorem to it.

By definition we have $div(dx/y) = div(dx) - div(y)$. In this way we focus on calculating simpler divisors.

Taking the divisor operator on both sides of the equation of the elliptic curve we get

$$div(y^2) = div(x - x_1) + div(x - x_2) + div(x - x_3). \tag{3.30}$$

As we have $div(y^2) = 2div(y)$, by Example 3.4 this reduces to

$$2div(y) = 2P_1 + 2P_2 + 2P_3 - 6O; \tag{3.31}$$

hence we get

$$div(y) = P_1 + P_2 + P_3 - 3O. \tag{3.32}$$

Now, for dx notice the equality $dx = d(x - x_1)$. So from Proposition 3.12, third part, and Example 3.4 we get

$$\begin{aligned} ord_{P_1} d(x - x_1) &= ord_{P_1}(1) + ord_{P_1}(x - x_1) - 1 \\ &= 0 + 2 - 1 \\ &= 1. \end{aligned}$$

Similarly for $ord_{P_2}d(x-x_2)$ and $ord_{P_3}d(x-x_3)$. Also, since we have $dx = -x^2 d(1/x)$, from Example 3.6 we obtain

$$\begin{aligned} ord_O(-x^2 d(1/x)) &= ord_O(-x^2) + ord_O(1/x) - 1, \\ &= 2ord_O(x) + ord_O(1/x) - 1, \\ &= 2ord_O(x) - ord_O(x) - 1, \\ &= ord_O(x) - 1, \\ &= -2 - 1 \\ &= -3. \end{aligned}$$

Thus we get

$$div(dx) = P_1 + P_2 + P_3 - 3O, \tag{3.33}$$

which conduces to $div(dx/y) = 0$, as claimed.

Then the class of the canonical divisors is trivial and we can take $K_{\mathcal{C}} = 0$ as a representative. Finally by Corolary 3.18, part one, we obtain $g = 1$. □

As elliptic curves have genus 1, the following corollary follows from the Riemann-Roch theorem.

Corollary 3.20. *In an elliptic curve the condition* $\deg(D) > 0$ *implies*

$$l(D) = \deg(D). \tag{3.34}$$

Proof. We obtain the result directly by item 3 of Corollary 3.18 because of $g = l(K_{\mathcal{C}}) = l(0) = 1$. □

3.4 The Picard group

Quotients are important in algebra and from this perspective we define a tool that measures the extend of the failure of the set of principal divisors to be the whole set of divisors. The **Picard group** of the curve $\mathcal{C}$, denoted $Pic(\mathcal{C})$, is the quotient of the group of divisors on $\mathcal{C}$ modulo the subgroup of principal divisors. We denote $Div^0(\mathcal{C})$ the set of divisors with degree zero and $Pic^0(\mathcal{C})$ the quotient between $Div^0(\mathcal{C})$ and the group of principal divisors.

Proposition 3.21. *Let P and Q be two points on the elliptic curve $\mathcal{C}$. Then $P \sim Q$ if and only if $P = Q$.*

Proof. If we suppose $P \sim Q$, then we have $div(f) = P - Q$ for a certain $f \in \bar{K}(\mathcal{C})$. We can write $div(f) + Q = P > O$, so by definition we get $f \in \mathcal{L}(Q)$. By Corollary 3.20 we have $l(Q) = \deg Q = 1$. As the vector space

of constant functions is included in $\mathcal{L}(Q)$ and is one dimensional, both are equal. Therefore f is constant and we get $div(f) = 0$, so $P = Q$.

The reciprocal is trivial. □

Proposition 3.22. *Let D be a degree 0 divisor. There exists a point P on the elliptic curve which satisfies*

$$D \sim P - O. \tag{3.35}$$

Furthermore, this point is unique.

Proof. By hypothesis we have $\deg(D+O) = \deg(D) + \deg(O) = 1$. Then by Corollary 3.20 we get $l(D+O) = 1$. In this way $\mathcal{L}(D+O)$ is generated by one element. Take f non trivial in this vector space. Then, by definition we get $div(f) \geq -D - O$, which implies $div(f) = -D - O + P$ for certain P as we have $\deg(div(f)) = 0$. By definition we obtain $D \sim P - O$.

For uniqueness, let $\widetilde{P}$ be a point with $\widetilde{P} \sim D + O$ so that $\widetilde{P} \sim P$. Then Proposition 3.21 implies $\widetilde{P} = P$. □

Now we define a map $\sigma : Div^0(\mathcal{C}) \to \mathcal{C}$ which sends D to P according to the last proposition. Here $Div^0(\mathcal{C})$ is the set of zero degree divisors on $\mathcal{C}$. Take an arbitrary point $P \in \mathcal{C}$. Trivially we have $P - O \sim P - O$, and therefore $\sigma(P - O) = P$. Hence σ is surjective.

Proposition 3.23. *Take $D_1, D_2 \in Div^0(\mathcal{C})$. We have $\sigma(D_1) = \sigma(D_2)$ if and only if $D_1 \sim D_2$.*

Proof. Let $P = \sigma(D_1)$ and $Q = \sigma(D_2)$ with $D_1, D_2 \in Div^0(\mathcal{C})$. We have then $D_1 \sim P - O$ and $D_2 \sim Q - O$, so by definition we have $div(f_1) = P - O - D_1$ and $div(f_2) = Q - O - D_2$ for some rational functions f_1, f_2 on C. These expressions together mean $div(f_1/f_2) = div(f_1) - div(f_2) = P - Q - (D_1 - D_2)$; hence we get $P - Q \sim D_1 - D_2$. The rest is easy. If $\sigma(D_1) = \sigma(D_2)$, we have $P = Q$ and therefore $D_1 - D_2 \sim 0$. And reciprocally, if $D_1 \sim D_2$ we get $P - Q \sim O$, and Proposition 3.21 yields $P = Q$. □

The previous proposition says in simple terms that σ induces a bijection $\tilde{\sigma} : Pic^0(\mathcal{C}) \to \mathcal{C}$ with an inverse $k : \mathcal{C} \to Pic^0(\mathcal{C})$ that maps P to the divisor class of $P - O$.

Theorem 3.24. *There exists a homomorphism between the elliptic curve $\mathcal{C}$ and $Pic^0(\mathcal{C})$.*

Proof. Fix $P, Q \in \mathcal{C}$ and call L_1 the line through them. This line intersects $\mathcal{C}$ at a third point R. Let L_2 be the line through R and O. By Equation (1.13) $Z = 0$ intersects $\mathcal{C}$ with multiplicity three. Then $div(L_1/Z) = P+Q+R-3O$ and $div(L_2/Z) = R+(P+Q)+O-3O = R+(P+Q)-2O$ hold. Therefore we get

$$\begin{aligned} div(L_1/L_2) =& div(L_1/Z) - div(L_2/Z) \\ =& P + Q + R - 3O - R - (P + Q) + 2O \\ =& P + Q - (P + R) - O. \end{aligned}$$

As L_1/L_2 is a rational function we have $div(L_1/L_2) \sim 0$. Thus we obtain $P - O + Q - O - (P + R) + O = 0$. Finally from the definition of k, this last relation is equivalent to $k(P) + k(Q) = k(P + Q)$. □

As a consequence of this theorem the associativity of the operation on the elliptic curve holds. To see this take points P, Q and R on the elliptic curve and do as follows:

$$\begin{aligned} k((P + Q) + R) &= k(P + Q) + k(R), \\ &= k(P) + k(Q) + k(R), \\ &= k(P) + k(Q + R) \\ &= k(P + (Q + R)). \end{aligned}$$

Taking inverses we obtain

$$(P + Q) + R = P + (Q + R),$$

as we aimed to prove.

Bibliography

[1] Cassels, J.W.S., *Lectures on elliptic curves*; Cambrige University Press, 1991.

[2] Duif, Niels, *Transforming a general cubic elliptic curve equation to Weierstrass form*; https://trac.sagemath.org/raw-attachment/ticket/3416/cubic_to_weierstrass_documentation.pdf (electronic resource).

[3] Fulton, William, *Algebraic curves: an introduction to algebraic geometry*; Addison-Wesley Publishing Company, 1989.

[4] Lozano-Robledo, Álvaro, *Elliptic curves, modular forms and their L-functions*; American Mathematical Society, Institute for Advance Study, 2011.

[5] Miranda, Rick, *Algebraic curves and Riemann surfaces*; American Mathematical Society, 1995.

[6] Shafarevich, Igor R., *Basic algebraic geometry 1*; Springer Verlag, 2013.

[7] Silverman, Joseph H., *The arithmetic of elliptic curves*; Springer Verlag, 2009.

[8] Silverman, Joseph H. and Tate, John T., *Rational points on elliptic curves*; Springer Verlag, 2015.

[9] Zuñiga, Javier, *El teorema de Riemann-Roch*; Tesis de licenciatura en Matemáticas, Pontificia Universidad Católica del Perú, 2001.