Elliptic Curves
– An Introduction –

Expanded notes from a mini-workshop held at

Mary Immaculate College
∼ University of Limerick ∼

29 and 30 November 2006

written by

Ciara Daly, Marina Franz, Madeeha Khalid and
Bernd Kreussler

Contents

1. Introduction 1
2. Solving Cubic Equations in Two Variables 7
3. Group law on the cubic curve 29
4. Theta Functions 53
5. Rank two vector bundles on elliptic curves 75

ELLIPTIC CURVES – AN INTRODUCTION

BERND KREUSSLER

The following four articles constitute expanded versions of talks given during a mini-workshop which took place at Mary Immaculate College, Limerick, on the 29th and 30th of November 2006. The titles of these talks were the following:

(1) *Solving Cubic Equations in Two Variables.*
(2) *Group Law on the Cubic Curve.*
(3) *Theta Functions.*
(4) *Rank two vector bundles on elliptic curves.*

Elliptic curves are very interesting because their study involves several fields of mathematics. The study of elliptic curves has a long history and still there are many unsolved problems. The goal of the mini-workshop was to provide an introduction for the non-specialist to several aspects of elliptic curves.

Elliptic curves reside at the crossroads of *arithmetic*, *geometry* and *analysis*. This was reflected in the talks as follows: talk (1) dealt with the arithmetic of elliptic curves whereas in talk (2) elliptic curves were studied from the point of view of complex algebraic geometry. The complex analytic side of elliptic curves was touched within talk (3). After these basics were laid down, talk (4) gave an introduction to the study of vector bundles on an elliptic curve. This highlighted the fact that it is not only interesting to study elliptic curves on their own but also to investigate other geometric objects of interest constructed on them.

It is clear from the number of pages used that the four articles can provide only a small bit of the available huge amount of knowledge and techniques related to elliptic curves. None of the many applications in physics, engineering and modern communication technology are discussed. To give the reader a first idea of the subject, a brief description of included and excluded material is given below.

I would like to thank Pat O'Sullivan for acting as a critical reader of the first drafts of all the four articles.

Solving Cubic Equations in Two Variables (Bernd Kreussler)

The first article starts with the elementary question of finding all Pythagorean triples of integers and goes on to apply similar ideas in order to find integer solutions of equations of degree three in two variables. The material is illustrated through many explicit examples. This part is probably suited for interested second-level students (in fact there was one among the audience for the first talk). The last section gives a brief overview of the most basic results about the Mordell-Weil group of a cubic curve.

However, there are many things which are not even mentioned in this article but which are no less important or fascinating than the material included. In particular, zeta-functions and L-functions are not included. As a consequence, the Birch and Swinnerton-Dyer conjecture is not formulated even though this is one of the Millennium Prize Problems. The important method of infinite descent as well as the Selmer and Tate-Shafarevich groups did not find their way into the article. The very interesting connection of elliptic curves with the solution of Fermat's Last Theorem (through the Frey curve) is another omission. The growing practical relevance of elliptic curves in modern cryptography is another issue missing. This list is certainly not complete. A few books which may help the interested reader to satisfy his or her thirst for knowledge are [6, 7, 13, 14, 15].

Group Law on the Cubic Curve (Madeeha Khalid)

The aim of the second article is to give an introduction to some basic concepts from complex algebraic geometry which allow a geometric understanding of the group structure introduced in the first talk. A brief introduction is given to complex manifolds, vector bundles on them and the Picard group (the group of all line bundles). Moreover the relationship between line bundles and divisors on a curve is explained, which allows a better understanding of the group structure introduced in the previous article.

The Weierstraß $\wp$-function and elliptic integrals are used to explain how complex analysis enters the picture. As a result, each cubic curve can also be seen as a complex torus, which comes with its own group structure. The gem of this article is a sketch of a proof that this analytically defined group structure coincides with the one introduced algebraically. This is based on Abel's Theorem. The analytic details are provided in the third article.

Again, many more things could have been included here. For example, higher dimensional Abelian Varieties and the Abel-Jacobi map which naturally emerge in the study of curves of higher genus are not mentioned. The idea of a scheme over an arbitrary commutative ring with unity are definitely beyond the scope of this article. To introduce the ideas of a moduli space and of a universal object would be a natural next step after the introduction of the Poincaré bundle. A higher dimensional analogue of an elliptic curve would be a so-called K3-surface. Their study has much in common with the theory of elliptic curves but they couldn't be touched either. There are many excellent textbooks available, among which are [3, 5, 16].

Theta Functions (Marina Franz)

This article gives a brief introduction to some basics in the modern theory of elliptic functions. The starting point are theta functions, which are nothing but global sections of line bundles on a one-dimensional complex torus. Their main properties are investigated from a purely analytic point of view. Moreover, these theta functions are related to the Weierstraß $\wp$-function, which can be considered to be the most basic elliptic function. A proof that this function satisfies a certain differential equation is given. This equation shows that a complex torus of dimension one can be embedded in the projective plane as a cubic curve. A proof of Abel's Theorem, which plays a major role in the previous article is also provided.

The same remark applies to this article as to the other two: there is much more material available than could be included. For example, an explicit description of the relationship between theta functions and holomorphic line bundles on elliptic curves is missing. Moreover, the fascinating theory of elliptic functions is only touched on. In particular, nothing is said about elliptic integrals. These arise, for example when the length of an ellipse is to be calculated. Historically, the study of elliptic integrals motivated the introduction of elliptic functions by Abel and Jacobi. Weierstraß built the theory of elliptic functions on the $\wp$-function, but beforehand Jacobi's elliptic functions $\mathsf{sn}(z), \mathsf{cn}(z), \mathsf{dn}(z)$ were the main players. Their role in mathematical applications in engineering are definitely beyond the scope of this short article. Theta functions are available on higher-dimensional tori as well, but this is not covered here. Such material and much more can be found in [12, 1, 10, 9].

Rank two vector bundles on elliptic curves (Ciara Daly)

In contrast to the three others, this fourth article is not primarily concerned with the group structure on an elliptic curve. But it is a direct continuation of these. Vector bundles of rank one and their sections were studied in the previous two articles. The moduli space interpretation of the Picard group is already mentioned in the second article. This article presents the main results about vector bundles of rank two on an elliptic curve. These go back to a seminal paper of Atiyah from 1959. This example is used to introduce to the theory of moduli, which is at the centre of modern algebraic geometry. The related notion of a stable vector bundle is also introduced.

Of course, there is much more that could be said in this context. Atiyah studied vector bundles of any rank, not only of rank two, but this did not find its way into this article. Also, the problems involved with the notion of stability of vector bundles on higher dimensional manifolds are not discussed. The theory of moduli of varieties as opposed to vector bundles is another huge area of algebraic geometry which is omitted. The relations of algebraic geometry to differential geometry and to theoretical physics through the theory of moduli spaces are not mentioned. Another quite recent development was the introduction of the space of stability conditions by Bridgeland. To define this invariant it would be necessary to introduce coherent sheaves and derived categories, so that this development could also not be covered here. The interested reader will find relevant starting points in [4, 8, 11, 17, 2].

References

[1] N.I. Akhiezer, *Elements of the theory of elliptic functions.* Translations of Mathematical Monographs 79, AMS (1990)

[2] T. Bridgeland, *Derived categories of coherent sheaves.* Proceedings of the international congress of mathematicians (ICM), Madrid, Spain, August 22–30, 2006, Volume II, 563–582 (2006)

[3] P. Griffiths, J. Harris, *Principles of algebraic geometry.* John Wiley & Sons (1978)

[4] D. Huybrechts, M. Lehn, *The geometry of moduli spaces of sheaves.* Aspects of Mathematics E 31, Vieweg (1997)

[5] F. Kirwan, *Complex algebraic curves.* London Mathematical Society Student Texts 23, Cambridge University Press (1992)

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

[7] N. Koblitz, *Algebraic Aspects of Cryptography.* Springer (2004)

[8] J. Le Potier, *Lectures on vector bundles.* Cambridge Studies in Advanced Mathematics 54, Cambridge University Press (1997)

[9] H. McKean, V. Moll, *Elliptic curves. Function theory, geometry, arithmetic.* Cambridge University Press (1999)

[10] G. Mittag-Leffler, *An introduction to the theory of elliptic functions.* Annals of Math. (2) 24, 271–351 (1923)

[11] S. Mukai, *An introduction to invariants and moduli.* Cambridge Tracts in Mathematics 81, Cambridge University Press (2003)

[12] D. Mumford, *Tata lectures on theta I, II, III.* Reprint of the 1991 edition, Modern Birkhäuser Classics, Birkhäuser (2007)

[13] J.H. Silverman, *The arithmetic of elliptic curves.* Graduate Texts in Mathematics 106, Springer (1986)

[14] J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics 151, Springer (1994)

[15] J.H. Silverman, J. Tate, *Rational points on elliptic curves.* Undergraduate Texts in Mathematics, Springer (1992)

[16] K. Ueno, *An introduction to algebraic geometry.* Translations of Mathematical Monographs 166, AMS (1997)

[17] E. Viehweg, *Quasi-projective moduli for polarized manifolds.* Ergebnisse der Mathematik und ihrer Grenzgebiete (3. Folge) 30, Springer (1995)

Mary Immaculate College, South Circular Road, Limerick, Ireland
E-mail address: bernd.kreussler@mic.ul.ie

SOLVING CUBIC EQUATIONS IN TWO VARIABLES

BERND KREUSSLER

Abstract. After recalling a geometric construction of all Pythagorean triples of integers, the same idea is applied to find rational solutions of cubic equations in two variables. This leads to the definition of the Mordell-Weil group. The final section collects some of the basic properties of this group.

1. Pythagoras

The aim of this introductory section is to recall the well-known geometric construction of all Pythagorean triples of integers. Three integers $a, b, c \in \mathbb{Z}$ form a *Pythagorean triple*, if

$$a^2 + b^2 = c^2.$$

Almost everybody knows the Pythagorean triple $(3, 4, 5)$ and many know $(5, 12, 13)$. However, not everybody has come across $(8, 15, 17)$ or $(20, 21, 29)$.

Clearly, if $n \in \mathbb{Z}$ and (a, b, c) is such a triple, (na, nb, nc) will also be one. In this way, starting with the well known triple $(3, 4, 5)$ we obtain $(6, 8, 10)$, $(-3, -4, -5)$, $(12, 16, 20)$ etc.

Note that a prime number which divides two of the three integers in a Pythagorean triple automatically divides the third in the triple. Therefore, it is enough to find all Pythagorean triples in which any two of the three integers are co-prime. We shall call such a Pythagorean triple *reduced*. Because the only Pythagorean triple with $c = 0$ is $(a, b, c) = (0, 0, 0)$, we shall assume in the sequel $c \neq 0$. This allows us to introduce the new variables

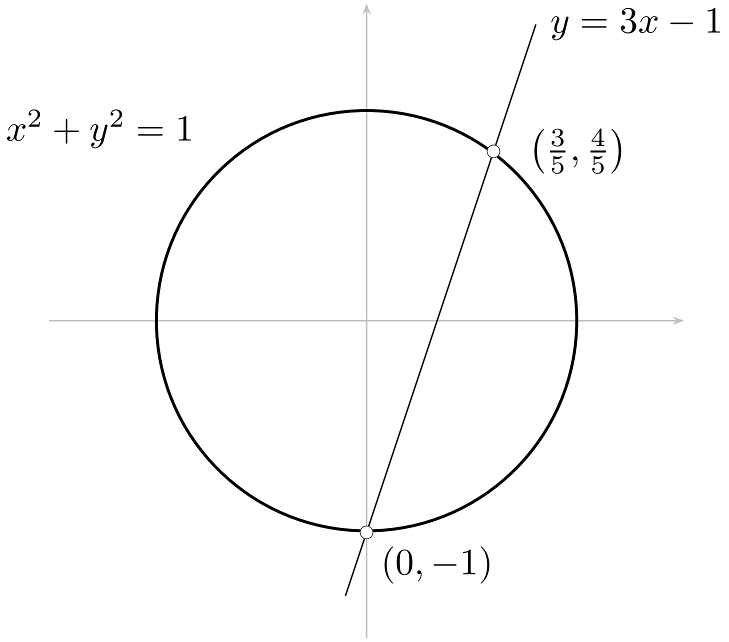
$$x = \frac{a}{c} \quad \text{and} \quad y = \frac{b}{c}.$$

Using these coordinates, the search for reduced Pythagorean triples translates into the problem to find all *rational* solutions of the equation

$$x^2 + y^2 = 1.$$

In other words, we would like to find all points on the unit circle whose coordinates are rational.

The key observation is that a line which connects two points with rational coordinates always has a rational slope. Therefore, we shall look at all lines in the plane which pass through the point $(0,-1)$ and which have rational slope $r \in \mathbb{Q}$.



Such a line is given by the equation $y = rx - 1$. Therefore, the x-coordinates of the two intersection points of this line with the unit circle satisfy the equation $x^2 + (rx-1)^2 = 1$, which is equivalent to $x\big((r^2+1)x - 2r\big) = 0$. The solution $x = 0$ corresponds to the point $(0,-1)$. The second intersection point has coordinates

$$x = \frac{2r}{r^2+1} \qquad \text{and} \qquad y = \frac{r^2-1}{r^2+1}.$$

The map which sends $r \in \mathbb{Q}$ to the point $\left(\frac{2r}{r^2+1}, \frac{r^2-1}{r^2+1}\right)$ on the unit circle gives a parametrisation of the set of all rational points on this curve. This completely solves our problem.

If we wish to derive a complete description of all Pythagorean triples of integers, we start by writing the slope r as $r = \frac{u}{v}$ with co-prime integers u, v. Using symmetry, we may assume $r > 1$. More precisely, switching from r to $-r$ corresponds to a sign change of x, whereas a sign change of y is achieved by switching from r to $\frac{1}{r}$. Thus, we assume $u > v > 0$ and u, v co-prime. Under these assumptions, $r = \frac{u}{v}$ produces the point with coordinates

$$x = \frac{2r}{r^2+1} = \frac{2uv}{u^2+v^2} \quad \text{and} \quad y = \frac{r^2-1}{r^2+1} = \frac{u^2-v^2}{u^2+v^2}.$$

Now it is not hard to see that each reduced Pythagorean triples in which a is odd can be written as

$$(a,b,c) = \left(uv, \frac{u^2-v^2}{2}, \frac{u^2+v^2}{2}\right)$$

with $u > v > 0$, both odd and co-prime. Up to interchanging a and b this gives us all reduced Pythagorean triples, because a and b are co-prime, hence at least one of these to integers is odd. For small values of u, v we obtain the following table

u	v	a	b	c
3	1	3	4	5
5	1	5	12	13
5	3	15	8	17
7	1	7	24	25
7	3	21	20	29

u	v	a	b	c
7	5	35	12	37
9	1	9	40	41
9	3	27	36	45
9	5	45	28	53
9	7	63	16	65

2. A cubic example

The aim of this section is to find integer solutions of cubic equations by using the geometric idea used in the previous section. We shall explain this method through the following example

$$b^2c = 4a^3 - 4ac^2 + c^3.$$

As before, we assume $c \neq 0$ and introduce new coordinates $x = \frac{a}{c}$ and $y = \frac{b}{c}$ in which the above equation becomes

$$y^2 = 4x^3 - 4x + 1. \tag{1}$$

This can be rewritten as

$$(y-1)(y+1) = 4(x+1)x(x-1).$$

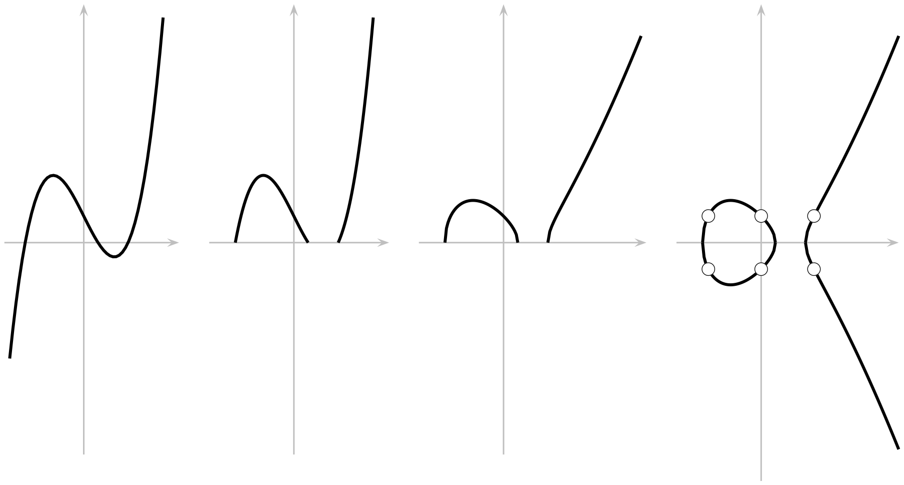
In this form it is obvious that we have the following six solutions

$$(-1, \pm 1), \ (0, \pm 1), \ (1, \pm 1).$$

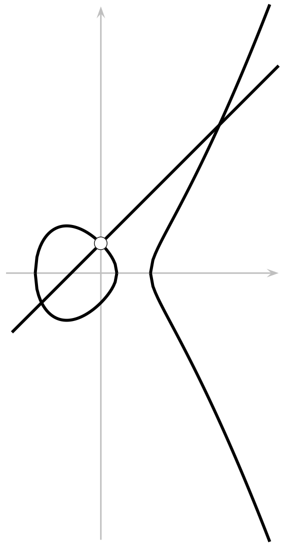
Question: Are these all the solutions of equation (1)?

It is not hard to produce a sketch of this curve in the real plane. This can be done through the following step-by-step approach. First, we draw the graph of the cubic polynomial $4x^3 - 4x + 1$. The intersection points with the x-axis can be found with Cardano's formula.

This polynomial has three real roots because its discriminant is positive. To get the second picture, we remove all points from the graph which have negative y-coordinate. The next picture is produced by applying the square root function. Finally, the cubic curve is obtained by adding in the mirror image along the x-axis, because (x, y) is on this curve if and only if $(x, -y)$ is so.



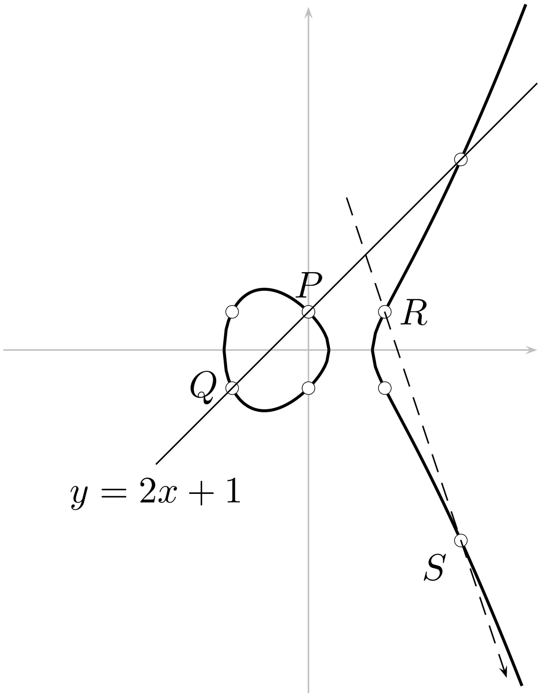
The six marked points in the picture are the points we found before. If we seek to find more rational points on this curve, we may try to use lines with rational slope which pass through one of the known points. This leads to a quadratic equation the solutions of which correspond to two further intersection points of this line with the curve given by equation (1).



For example, the line with slope 1 which passes through the point $(0, 1)$ has the equation $y = x+1$. The x-coordinates of its intersection with our curve are the solutions of the equation $(x+1)^2 = 4x^3-4x+1$ or equivalently $4x^3 - x^2 - 6x = 0$. The known solution corresponds to the factor x of this polynomial. The two new intersection points correspond to the solutions of the quadratic equation $4x^2-x-6=0$, these are the irrational numbers $\frac{1\pm\sqrt{97}}{8}$.

This example shows that we should allow for one new point only. In other words, we should work with a line connecting two of the known points.

Example 1. Let us see how this works with $P=(0,1)$ and $Q=(-1,-1)$. The line which connects these two points is given by the equation $y=2x+1$. Substituting this into equation (1) gives $4x^3-4x^2-8x=0$. The two points we started with give us two of the roots of this polynomial, namely $x_1=0$ and $x_2=-1$. Now, it is not hard to see that $4x^3-4x^2-8x=4x(x+1)(x-2)$. Hence $x_3=2$ is the third solution which corresponds to the point $(2,5)$ on our curve. We can even produce another new point, because the given equation does not change when we replace y by $-y$. This gives the point $S=(2,-5)$.



Example 2. We may now continue by using the line through $P=(0,1)$ and $S=(2,-5)$. Its equation is $y=-3x+1$. Therefore, we look at $4x^3-(-3x+1)^2-4x+1$ which has to be equal to $4x(x-2)(x-x_3)$. Comparing the coefficients of x^2 of these two polynomials leads to the equation $-9=-4(2+x_3)$. This gives $x_3=\frac{1}{4}$. The new points we obtain are $\left(\frac{1}{4},\pm\frac{1}{4}\right)$.

In general, if we are using a line with slope $r \in \mathbb{Q}$ which passes through two points on our curve whose x-coordinates are x_1 and x_2, we obtain the x-coordinate of the third point by comparing the coefficients of x^2 as above. The result will be $x_3 = \frac{r^2}{4} - x_1 - x_2 \in \mathbb{Q}$.

We may also use other points from the six found originally.

Example 3. The line connecting $S = (2, -5)$ with $R = (1, 1)$ has the equation $y = -6x + 7$. This gives a new point with coordinate $x_3 = 9 - 2 - 1 = 6$ and $y_3 = -6x_3 + 7 = -29$. So we have two new points $(6, -29)$ and $(6, 29)$ which are not visible in the picture.

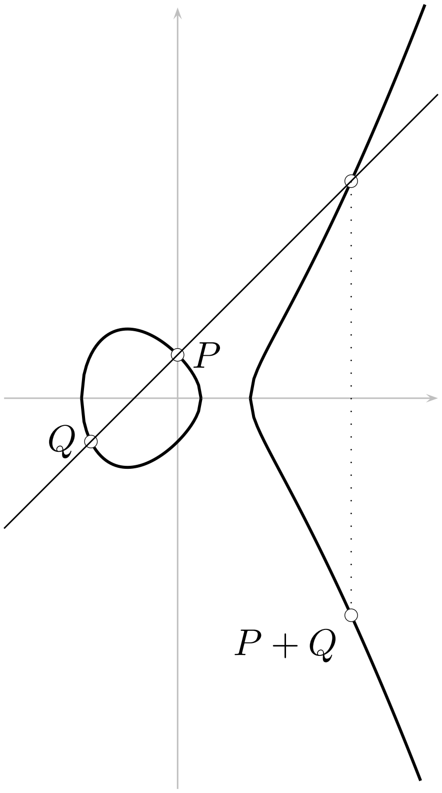
Note that we obtained $(6, 29)$ as follows. First we connected $P = (0, 1)$ and $Q = (-1, -1)$ by a line, whose third point of intersection with the cubic curve had $(2, -5)$ as its mirror image relative to the x-axis. Then we connected $(2, -5)$ and $R = (1, 1)$ by a line and obtained $(6, 29)$ as the mirror image of the third point of intersection. It is interesting to see what happens if we carry out these steps in another order. Let us first connect $Q = (-1, -1)$ and $R = (1, 1)$ by a line, reflect the third point on this line on the x-axis and connect this point in the second step with $P = (0, 1)$.

Example 4. The line which connects $Q = (-1, -1)$ and $R = (1, 1)$ has the equation $y = x$. This line has $\left(\frac{1}{4}, \frac{1}{4}\right)$ as its third point of intersection with the curve given by equation (1). Therefore, we shall connect its mirror image $\left(\frac{1}{4}, -\frac{1}{4}\right)$ with $P = (0, 1)$. The corresponding line has the equation $y = -5x + 1$. The new point produced this way is $(6, -29)$, the same as we obtained in Example 3.

This coincidence is not an accident. It is in fact a special case of a theorem from projective geometry which states that a cubic curve (in projective space) which passes through eight of the nine intersection points of two other cubics, must also contain the ninth of these intersection points.

A closer look at examples 3 and 4 suggest that we are dealing here with a kind of *associativity*. This can indeed be made precise by the following definition.

Definition 5. Let P, Q be points on the cubic curve given by equation (1). We define $P + Q$ to be the mirror image (relative to the x-axis) of the third point of intersection of the line which connects P and Q and the cubic curve.

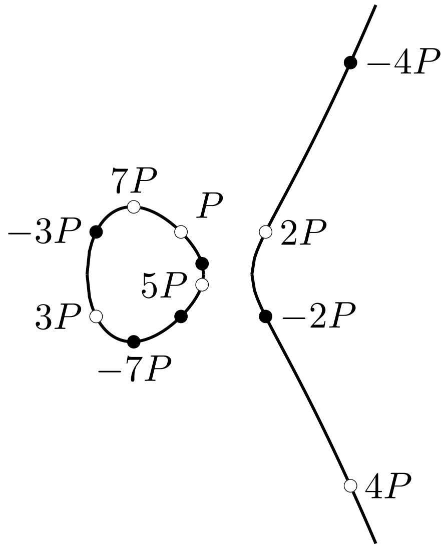


In this language, we have shown above $(P+Q)+R = P+(Q+R)$ where $P = (0,1)$, $Q = (-1,-1)$ and $R = (1,1)$. This definition also extends to give $P + P$, which is obtained by using the *tangent line* to our curve at P.

Example 6. Implicit differentiation reveals that the tangent line to our curve at $P = (0,1)$ has slope equal to -2. Therefore, this line is given by the equation $y = -2x + 1$. In the same way as before, we substitute $y = -2x+1$ into equation (1) and use the fact that $x = 0$ will be a double root of the cubic equation so obtained. Then, we get that the x-coordinate of the new point of intersection is equal to $x = 1$. This produces the known points $(1, \pm 1)$.

This example shows that we actually need to know only one rational point on our cubic in order to get started. As before, we can then produce many other points. Using the notation suggested by Definition 5, we obtain here:

$$P = (0,1), \qquad 2P = (1,1), \qquad 3P = (-1,-1),$$
$$4P = (2,-5), \qquad 5P = \left(\frac{1}{4}, \frac{1}{4}\right), \qquad 6P = (6,29).$$



We shall see in the next section that this is in fact the structure of an Abelian group in which for each point T, $-T$ is the mirror image of T with respect to the x-axis. The line which connects an arbitrary point T on our cubic with its mirror image $-T$ is a vertical line. Because $T + (-T) = 0$, we expect all these lines to go through the neutral element of this group. Therefore, we shall look for the neutral element "at infinity". This can be made more precise with the aid of the projective plane $\mathbb{P}^2$, introduced in the following section.

3. The complete picture

In order to see all points on our cubic curve we have to return to the original equation $b^2c = 4a^3 - 4ac^2 + c^3$. The key observation is here that (a, b, c) is a solution of this equation if and only if $(\lambda a, \lambda b, \lambda c)$ is a solution for all numbers λ. This means that the solution set is a union of lines which pass through the origin. When we switched to coordinates (x, y) in the previous two sections, we agreed that it is sufficient to know one point on each of these lines. But we missed those lines on which $c = 0$ due to our division by c. If we would like to keep these lines as well, we arrive at the idea of the projective plane. Set theoretically, the projective plane is defined to be the set of all lines in three-space which pass through the origin. This leads to the following useful description.

Before we proceed we need to fix our notion of "number". So far, we have dealt with rational numbers and integers. But in general it is much easier and more convenient to work with an algebraically closed field like the field $\mathbb{C}$ of complex numbers. Many things which will be said below are true for any field $\mathbb{K}$. Therefore, we shall formulate the next definition for any field $\mathbb{K}$. The reader who is not familiar with the concept of a field may substitute $\mathbb{Q}$ or $\mathbb{C}$ for $\mathbb{K}$.

Definition 7. The projective plane $\mathbb{P}^2(\mathbb{K})$ over the field $\mathbb{K}$ is the set of all equivalence classes $(z_0 : z_1 : z_2)$ of non-zero vectors $(z_0, z_1, z_2) \in \mathbb{K}^3$. Two such vectors (z_0, z_1, z_2) and (w_0, w_1, w_2) are equivalent if and only if there exits a non-zero $\lambda \in \mathbb{K}$ such that $(z_0, z_1, z_2) = \lambda(w_0, w_1, w_2)$. This implies

$$(z_0 : z_1 : z_2) = (\lambda z_0 : \lambda z_1 : \lambda z_2) \quad \text{for all} \quad \lambda \neq 0.$$

The notation $(z_0 : z_1 : z_2)$ for the equivalence class of the vector (z_0, z_1, z_2) is chosen in order to suggest that we are dealing with the ratios between the three numbers z_0, z_1 and z_2 only. A similar construction, of course, can be carried out in any dimension to produce $\mathbb{P}^n(\mathbb{K})$ for all $n \geq 1$. The one-dimensional case is particularly easy. If $\mathbb{K} = \mathbb{C}$ it leads to the Riemannian sphere. Notations used for the Riemannian sphere are $S^2 = \mathbb{C} \cup \infty = \overline{\mathbb{C}}$ and $\mathbb{P}^1(\mathbb{C})$, the notation we are going to use here. Its points are equivalence classes $(z_0 : z_1)$ of non-zero vectors $(z_0, z_1) \in \mathbb{C}^2$. All points in $\mathbb{P}^1(\mathbb{C})$ with $z_0 = 0$ are equivalent to $\infty = (0 : 1)$. Any point with $z_0 \neq 0$ is equivalent to $(1 : z)$ where $z = \frac{z_1}{z_0}$. This gives a bijection between $\mathbb{C}$ and $\mathbb{P}^1(\mathbb{C}) \setminus \{\infty\}$. A neighbourhood of ∞ would be the set of all those points of $\mathbb{P}^1(\mathbb{C})$ which have $z_1 \neq 0$. This is again in bijection with $\mathbb{C}$ by using $w = \frac{z_0}{z_1}$. The relationship between these two patches of $\mathbb{P}^1(\mathbb{C})$ is given by $w = \frac{1}{z}$. This actually makes $\mathbb{P}^1(\mathbb{C})$ into a complex manifold of dimension one, the simplest compact Riemann surface.

The local structure of $\mathbb{P}^2(\mathbb{K})$ can be studied in a similar way. To this end, we define the three basic open sets which cover $\mathbb{P}^2(\mathbb{K})$ completely

$$\begin{aligned} U_0 &:= \{(z_0 : z_1 : z_2) \mid z_0 \neq 0\} \subset \mathbb{P}^2(\mathbb{K}) \\ U_1 &:= \{(z_0 : z_1 : z_2) \mid z_1 \neq 0\} \subset \mathbb{P}^2(\mathbb{K}) \\ U_2 &:= \{(z_0 : z_1 : z_2) \mid z_2 \neq 0\} \subset \mathbb{P}^2(\mathbb{K}). \end{aligned}$$

Each of these sets is in bijection with $\mathbb{K}^2$. For example, the map $U_0 \to \mathbb{K}^2$ given by $(z_0 : z_1 : z_2) \mapsto \left(\frac{z_1}{z_0}, \frac{z_2}{z_0}\right)$ has as its inverse the map $\mathbb{K}^2 \to U_0$ which sends (ξ_1, ξ_2) to $(1 : \xi_1 : \xi_2)$.

Similarly, on U_1 we can work with affine coordinates $\eta_j = \frac{z_j}{z_1}$, $j = 0, 2$ and on U_2 we have $\zeta_k = \frac{z_k}{z_2}$, $k = 0, 1$. The gluing maps between these three $\mathbb{K}^2$ are given by

$$\begin{aligned} \xi_1 &= \frac{1}{\eta_0} = \frac{\zeta_1}{\zeta_0} & \xi_2 &= \frac{\eta_2}{\eta_0} = \frac{1}{\zeta_0} \\ \eta_0 &= \frac{1}{\xi_1} = \frac{\zeta_0}{\zeta_1} & \eta_2 &= \frac{\xi_2}{\xi_1} = \frac{1}{\zeta_1} \\ \zeta_0 &= \frac{1}{\xi_2} = \frac{\eta_0}{\eta_2} & \zeta_1 &= \frac{\xi_1}{\xi_2} = \frac{1}{\eta_2}. \end{aligned}$$

If $\mathbb{K} = \mathbb{C}$ this defines the structure of a two dimensional complex manifold on $\mathbb{P}^2(\mathbb{C})$.

Let us apply this new language to the cubic equation $b^2c = 4a^3 - 4ac^2 + c^3$ studied in the previous section. As we have seen above, if we identify (a, b, c) with $(z_0, z_1, z_2) \in \mathbb{Q}^3$, the set of all solutions of this cubic equation is a well defined subset $E(\mathbb{Q}) \subset \mathbb{P}^2(\mathbb{Q})$. Our assumption $c \neq 0$ means that we restricted our attention to the set U_2. The complement of U_2 is the set of all those points which have $z_2 = 0$. These are the points of the form $(z_0 : z_1 : 0)$, hence the complement of U_2 in $\mathbb{P}^2(\mathbb{K})$ is in bijection with $\mathbb{P}^1(\mathbb{K})$. Therefore, we call

$$L_2 = \{(z_0 : z_1 : 0) \mid (z_0 : z_1) \in \mathbb{P}^1(\mathbb{K})\} \subset \mathbb{P}^2(\mathbb{K})$$

the *line at infinity*. In a similar way we may define lines at infinity L_0 and L_1 which are the complements of U_0 and U_1 respectively.

In order to see what we missed when restricting to U_2 we simply set $c = 0$ in our cubic equation. This leaves us with the equation $0 = 4a^3$. Therefore, the only point missed is the point $O = (0 : 1 : 0) \in L_2 \subset \mathbb{P}^2(\mathbb{Q})$. In order to see how $E(\mathbb{Q})$ looks like around this point, we restrict our attention to the set U_1. Using the coordinates (η_0, η_2) introduced above, $E(\mathbb{Q})$ is described by the equation

$$\eta_2 = 4\eta_0^3 - 4\eta_0\eta_2^2 + \eta_2^3.$$

The line at infinity L_2 intersects U_1 at the η_0-axis, given by the equation $\eta_2 = 0$. This line is a tangent line to the cubic curve with a triple contact at the point $O = (0, 0)$. The point O is an inflection point of our curve.

The main result of the previous section was that we introduced an “addition” of points in $E(\mathbb{Q})$ by the rule that $P + Q + R = O$ if and only if the three points P, Q, R are collinear. Therefore, we need to understand lines in the projective plane. These are given by linear equations. In general, a line in $\mathbb{P}^2(\mathbb{K})$ is the set of all solutions of an equation of the form

$$l_0 z_0 + l_1 z_1 + l_2 z_2 = 0$$

with $l_0, l_1, l_2 \in \mathbb{K}$ but not all three equal to zero. Because $\lambda l_0, \lambda l_1, \lambda l_2$ define the same line in $\mathbb{P}^2(\mathbb{K})$ if $\lambda \neq 0$, the set of all lines in $\mathbb{P}^2(\mathbb{K})$ is another $\mathbb{P}^2(\mathbb{K})$, called the *dual projective plane* and sometimes denoted $\mathbb{P}^2(\mathbb{K})^\vee$.

Each line in $\mathbb{P}^2(\mathbb{K})$ is isomorphic to $\mathbb{P}^1(\mathbb{K})$. The three lines at infinity introduced before are also lines in this sense, because L_j was given by the equation $z_j = 0$. In particular, the line L_2 corresponds to the point $(0 : 0 : 1) \in \mathbb{P}^2(\mathbb{K})^\vee$. Any other line, with coefficients $(0 : 0 : 1) \neq (l_0 : l_1 : l_2) \in \mathbb{P}^2(\mathbb{K})^\vee$ intersects U_2 in an ordinary line. The equation of this intersection is

$$l_0 x + l_1 y = -l_2$$

where we used $x = \frac{a}{c}, y = \frac{b}{c}$ instead of $\zeta_0 = \frac{z_0}{z_2}, \zeta_1 = \frac{z_1}{z_2}$ as coordinates on U_2. If $l_1 \neq 0$, this can be rewritten as $y = rx + s$ with $r = -\frac{l_0}{l_1}$ and $s = -\frac{l_2}{l_1}$. If, however, $l_1 = 0$ the equation becomes $l_0 x = -l_2$ and this defines a vertical line which intersects the x-axis at $-\frac{l_2}{l_1}$.

On the other hand, the point $O = (0 : 1 : 0)$ is on the line given by $l_0 z_0 + l_1 z_1 + l_2 z_2 = 0$ if and only if $l_1 = 0$. Hence, the vertical lines in U_2 correspond precisely to those lines in $\mathbb{P}^2(\mathbb{K})$ which pass through O and are different from L_2. Therefore, the point at infinity O is the correct choice for the neutral element of the group structure on $E(\mathbb{Q})$ and reflection at the x-axis corresponds to taking the additive inverse of a point.

With some background in projective geometry or by other means it can be shown that the addition of points on $E(\mathbb{Q})$ introduced in the previous section equips $E(\mathbb{Q})$ with the structure of an Abelian group. More about projective geometry and a geometric proof can be found in the article by M. Khalid [11].

Theorem 8. *$E(\mathbb{Q})$ is an Abelian group with neutral element O, its only point at infinity. The group structure is determined by saying that $P + Q + R = O$ if and only if P, Q and R are on a line in $\mathbb{P}^2(\mathbb{Q})$. This implies that $-P$ is obtained from P by changing the sign of the y-coordinate.*

Remark 9. This result is true for any field $\mathbb{K}$ and any cubic equation of the form

$$z_1^2z_2 = z_0^3 + pz_0z_2^2 + qz_2^3 \tag{2}$$

with $p, q \in \mathbb{K}$ satisfying $\Delta = -16(4p^3+27q^2) \neq 0$. If the characteristic of $\mathbb{K}$ is not equal to two or three (i.e. if $1+1 \neq 0$ and $1+1+1 \neq 0$ in $\mathbb{K}$), every regular cubic with a point over $\mathbb{K}$ can be given by such an equation. When working in characteristic zero (e.g. $\mathbb{K} = \mathbb{Q}$ or $\mathbb{K} = \mathbb{C}$), we can change coordinates so that (2) becomes

$$z_1^2z_2 = 4z_0^3 - g_2z_0z_2^2 - g_3z_2^3. \tag{3}$$

The discriminant of such an equation is $\Delta = g_2^3 - 27g_3^2$. A cubic equation of the form (3) is called a *Weierstraß* equation, named after Karl Weierstraß (1815–1897). The coefficient 4 at z_0^3 is used because it appears in the differential equation of the Weierstraß $\wp$-function. (See the article by M. Franz [5].)

The most basic structure result about the group $E(\mathbb{Q})$ was shown in 1922 by Mordell [17].

Theorem 10 (Mordell)**.** *If E is given by (2) with $p, q \in \mathbb{Q}$ and $4p^3 + 27q^2 \neq 0$ then the Abelian group $E(\mathbb{Q})$ is finitely generated.*

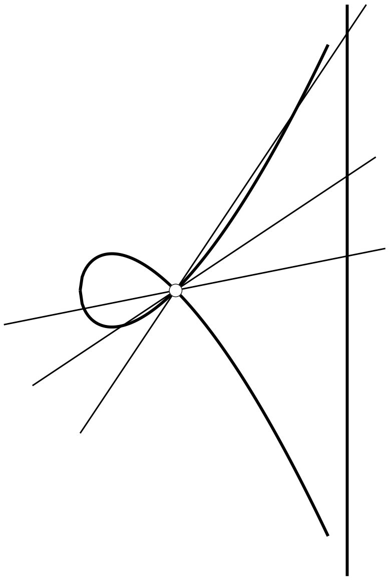
Remark 11. Theorem 10 has been generalised by A. Weil to Abelian varieties of arbitrary dimension over any number field [23]. Therefore Mordell's Theorem is also known as the Mordell-Weil Theorem and the group $E(\mathbb{Q})$ is sometimes called the Mordell-Weil group.

The curve studied in section 2 has $E(\mathbb{Q}) \cong \mathbb{Z}$ with generator $P = (0, 1)$. The discriminant of this curve is $\Delta = 37$.

Remark 12. The assumption $4p^3+27q^2 \neq 0$ in Mordell's Theorem is crucial. If $4p^3 + 27q^2 = 0$ the cubic polynomial $x^3 + px + q$ has a multiple root and this gives rise to a singular point on the cubic curve given by (2). This changes the situation completely, because singular cubics are rational. More explicitly, suppose $-4p^3 = 27q^2$ and $p, q \in \mathbb{Q} \setminus \{0\}$. A straightforward calculation shows that, under these assumptions,

$$x^3 + px + q = \left(x - \frac{3q}{p}\right)\left(x + \frac{3q}{2p}\right)^2.$$

This implies that $\left(-\frac{3q}{2p}, 0\right)$ is a singular point of the cubic which means that each line in $\mathbb{P}^2(\mathbb{Q})$ that passes through this point will have at most one other intersection point with the cubic curve (2). Just as in the case of the circle in section 1 this produces a bijection between $\mathbb{Q}$ (the set of slopes) and all rational points on a singular cubic apart from the singular point. This shows that the non-singular rational points on a singular cubic form a group which is not finitely generated.



Example 13. Look at the singular cubic $z_1^2 z_2 = 4z_0^3 - 3z_0 z_2^2 + z_2^3$, which has discriminant $\Delta = 3^3 - 27(-1)^2 = 0$. On U_2, using coordinates x, y as before, its equation is

$$y^2 = 4x^3 - 3x + 1.$$

From $4x^3 - 3x + 1 = (x+1)(2x-1)^2$ we see that the singular point has coordinates $\left(\frac{1}{2}, 0\right)$. Any line with rational slope r through this point will have equation $y = r\left(x - \frac{1}{2}\right)$, hence the new intersection point will be found by solving $\left(\frac{r}{2}\right)^2 (2x-1)^2 = (x+1)(2x-1)^2$. Therefore, the coordinates of this point are given by

$$x = \frac{r^2 - 4}{4} \quad \text{and} \quad y = \frac{r^3 - 6r}{4}.$$

The main difference between this and the non-singular case is that we cannot find such a closed formula for all rational solutions in the non-singular case. This is explained by the involvement of transcendental functions such as theta functions and the Weierstraß $\wp$-function (see the article [5]).

4. Further results

In this section we collect some general results known about the Mordell-Weil group $E(\mathbb{Q})$. We also discuss several normal forms of plane cubic curves.

Let us look at a cubic curve given by an equation of the form

$$y^2 = x^3 + px + q \qquad \text{with} \quad 4p^3 + 27q^2 \neq 0. \tag{4}$$

Such an equation is also called a Weierstraß equation or Weierstraß canonical form. However, as we shall see below, it is not canonical. To determine this we need to decide whether it is possible that two curves given by a Weierstraß equation with different (p, q) can be transformed into each other by a linear transformation of coordinates. Consider the following.

Given two curves $y^2 = x^3 + px + q$ and $\widetilde{y}^2 = \widetilde{x}^3 + \widetilde{p}\widetilde{x} + \widetilde{q}$ with $p, q, \widetilde{p}, \widetilde{q} \in \mathbb{Q}$, the only possible linear transformations of coordinates with rational coefficients which transform one of these equations into the other are of the form $\widetilde{x} = \lambda^2 x, \widetilde{y} = \lambda^3 y$ with $\lambda \in \mathbb{Q} \setminus \{0\}$. Such a transform is successful if and only if we have $\widetilde{p} = \lambda^4 p$ and $\widetilde{q} = \lambda^6 q$. This can be used, in particular, to obtain *integer* coefficients $p, q \in \mathbb{Z}$. Therefore, the following result is useful in broader generality than it first may seem.

Theorem 14 (Siegel, [20, 16, 18])**.** *The equation $y^2 = x^3 + px + q$ with $p, q \in \mathbb{Z}$ has only finitely many solutions $(x, y) \in \mathbb{Z}^2$, provided that $4p^3 + 27q^2 \neq 0$.*

A point $P \in E(\mathbb{Q})$ is called a *torsion point* if there exists a positive integer $n \in \mathbb{Z}$ such that $nP = O$ in the additive group $E(\mathbb{Q})$. In other words, the torsion points of $E(\mathbb{Q})$ are precisely the points of finite order in the group $E(\mathbb{Q})$. They form the *torsion subgroup* $E(\mathbb{Q})_{\text{tor}} \subset E(\mathbb{Q})$. For example, if the curve is given by a Weierstraß equation, the two-torsion points in $E(\mathbb{Q})$, i.e. the points $P \in E(\mathbb{Q})$ with $2P = O$, are precisely the intersection points of the curve E with the x-axis (and the point O). The example studied in section 2 did not have any two-torsion points apart from O, as the cubic equation $4x^3 - 4x + 1 = 0$ does not have a rational root. The following result sheds some light on the torsion subgroup more generally.

Theorem 15 (Lutz–Nagell, [13, 19])**.** *All torsion points of $y^2 = x^3 + px + q$ with $p, q \in \mathbb{Z}$ have integer coordinates $(x, y) \in \mathbb{Z}^2$, provided*

$4p^3 + 27q^2 \neq 0$. *Moreover, if* $(x, y) \in E(\mathbb{Q})_{tor}$ *then either* $y = 0$ *or* y^2 *divides* $4p^3 + 27q^2$.

Together with Siegel's Theorem this implies that $E(\mathbb{Q})_{\text{tor}}$ is finite. This, however, is already a consequence of Mordell's Theorem, because every finitely generated Abelian group G is isomorphic to

$$\mathbb{Z}^r \times \underbrace{\mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \ldots \times \mathbb{Z}/a_{s-1}\mathbb{Z} \times \mathbb{Z}/a_s\mathbb{Z}}_{G_{\text{tor}}}$$

with positive integers a_i. The number $r \geq 0$ is called the rank of this group. The possibilities for the rank of $E(\mathbb{Q})$ are not yet known, but it is conjectured that there exist cubic curves for which the rank of $E(\mathbb{Q})$ is as large as you want. The largest known rank at the moment seems to be 28, attained by an example found by N. Elkies in 2006.

On the other hand, the torsion subgroup of $E(\mathbb{Q})$ is much better understood. The main result is the following.

Theorem 16 (Mazur, [14, 15])**.** *If* $E(\mathbb{Q})$ *is given by the equation* $y^2 = x^3 + px + q$ *with* $p, q \in \mathbb{Q}$ *and* $4p^3 + 27q^2 \neq 0$*, then its torsion subgroup* $E(\mathbb{Q})_{tor}$ *is isomorphic to one of the fifteen groups in the following list:*

$$\mathbb{Z}/n\mathbb{Z}, \quad 1 \leq n \leq 10, \ \textit{or} \ n = 12,$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, \quad 1 \leq n \leq 4.$$

All these groups in fact occur as torsion subgroups.

Remark 17. This result is in sharp contrast to the situation over an algebraically closed field. If $\mathbb{K}$ is an algebraically closed field whose characteristic does not divide the positive integer m, then the m-torsion subgroup of $E(\mathbb{K})$, which consists of all the elements of $E(\mathbb{K})$ killed by m, is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. In the case $\mathbb{K} = \mathbb{C}$ this will be explained in the article of M. Khalid [11].

Example 18. Because $9 = 8 + 1$, it is not so hard to discover that $P = (2, 3)$ is an element of $E(\mathbb{Q})$, the solution set of the equation $y^2 = x^3 + 1$. The tangent line at P to this cubic curve has equation $y = 2x - 1$. If we substitute this into $y^2 = x^3 + 1$ we obtain $(2x-1)^2 = x^3 + 1$ or equivalently $0 = x^3 - 4x^2 + 4x = x(x-2)^2$. This means that this tangent line intersects the cubic at the new point $(0, -1)$, hence $2P = (0, 1)$. To find $3P$, we use the line which connects $P = (2, 3)$ and $2P = (0, 1)$. It has the equation $y = x + 1$ and intersects the cubic at $3P = (-1, 0)$. This point is on the x-axis, so it is a two-torsion point. This implies $6P = O$ and we obtain $4P = -2P = (0, -1)$ and $5P = -P = (2, -3)$. In fact, $E(\mathbb{Q})$ consists of the six points kP, $k = 0, 1, 2, 3, 4, 5$ only, i.e. $E(\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$. In [21] and [7] examples of cubic equations which realise all the other $E(\mathbb{Q})_{\mathrm{tor}}$ can be found.

The Tate canonical form, see (7) below, is very useful in the study of cubics whose Mordell-Weil group has torsion. More precisely, every cubic curve which has at least one point $P \in E(\mathbb{Q})_{\mathrm{tor}}$ of order at least four (i.e. $P \neq O$, $2P \neq O$ and $3P \neq O$) can be brought into Tate canonical form. For example, if $b = 1$ and $c = d$ in (7), it can be shown that the point $(0 : 0 : 1)$ is a point of order four.

A useful method which allows us to gain information about $E(\mathbb{Q})$ is *reduction modulo a prime number p*. This means that one studies solutions of a given cubic equation with coordinates in the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. These solutions form the group $E(\mathbb{F}_p)$. An interesting result in this context says that for each prime $p > 2$ which does not divide the discriminant Δ, the map which reduces the coordinates of a torsion point $P \in E(\mathbb{Q})$ modulo p embeds $E(\mathbb{Q})_{\mathrm{tor}}$ as a subgroup into $E(\mathbb{F}_p)$. This can be used to determine the group $E(\mathbb{Q})_{\mathrm{tor}}$. More on the issue of calculating the torsion subgroup of $E(\mathbb{Q})$ can be found for example in [22], [10] and [6].

Example 19. Let us show that $E(\mathbb{Q})_{\mathrm{tor}} = \{O\}$ for the cubic $y^2 = 4x^3 - 4x + 1$ studied in the previous section. The idea is to calculate $E(\mathbb{F}_3)$ and $E(\mathbb{F}_5)$ and show that these groups are of co-prime order. This is sufficient because 3 and 5 do not divide the discriminant $\Delta = 37$ of this cubic. If we reduce the equation $y^2 = 4x^3 - 4x + 1$ modulo 3 we obtain $y^2 = x^3 - x + 1$. Because $x^3 - x = x(x-1)(x+1)$ is equal to zero for all $x \in \mathbb{F}_3$, we see that $(0, \pm 1), (1, \pm 1), (2, \pm 1)$ are the only solutions of this equation with coefficients in the finite field $\mathbb{F}_3$. Therefore, $E(\mathbb{F}_3) = \{O, (0, \pm 1), (1, \pm 1), (2, \pm 1)\}$ is of order 7. Reducing the equation $y^2 = 4x^3 - 4x + 1$ modulo 5 gives $y^2 = -x^3 + x + 1$. Its solutions over $\mathbb{F}_5$ are $(0, \pm 1), (\pm 1, \pm 1)$ and $(2, 0)$. This means that $E(\mathbb{F}_5)$ is a group of order 8. Because $E(\mathbb{Q})_{\mathrm{tor}}$ is isomorphic to a sub-group of $E(\mathbb{F}_3)$ and of $E(\mathbb{F}_5)$, it must be trivial.

More generally, solutions in all finite fields of fixed characteristic p can be studied. If the number of solutions for such finite fields are put together in a kind of generating function, the so-called *zeta-function* is obtained. Lack of space forces us to skip the fascinating theory of zeta-functions of elliptic curves, the Weil conjectures and their proof by Deligne and, last but not least, the Birch and

Swinnerton-Dyer conjecture which is one of the millennium prize problems, a solution of which is worth one million US-Dollars (see `http://www.claymath.org/millennium/`). A starting point for the interested reader could be [12], [7] or [21]. We confine ourselves to look at Weierstraß equations and other canonical forms over more general fields $\mathbb{K}$ for the rest of this article.

There are several ways to proceed. One possibility would be to introduce the abstract notion of a smooth projective curve of arithmetic genus 1, defined over the field $\mathbb{K}$. If such a curve has a point with coordinates in $\mathbb{K}$, it is possible to show that the curve is isomorphic to a plane cubic curve which has an inflection point at $O = (0 : 1 : 0)$. In particular, if $\mathbb{K}$ is algebraically closed, such a point always exists. However, even in the case $\mathbb{K} = \mathbb{Q}$ an equation like $3z_0^3 + 4z_1^3 + 5z_2^3 = 0$ does not have a single point in $\mathbb{P}^2(\mathbb{K})$. Of course, we shall not proceed along these lines. The interested reader is referred to standard textbooks on algebraic geometry, such as [8].

We shall assume that we have a cubic equation $f(z_0, z_1, z_2) = 0$ which defines a plane cubic curve with at least one point in $\mathbb{P}^2(\mathbb{K})$. Let us first try to see whether any such curve can be described by a Weierstraß equation, whereby we allow linear transformations of coordinates only. The key to making progress is to understand inflection points. It is not hard to show that a point $P \in E(\mathbb{K})$ is an inflection point if and only if it is on the zero set of the *Hessian* of the cubic polynomial f. By definition, the Hessian of f is the determinant of the 3×3–matrix formed by the second partial derivatives of f. This is again a cubic polynomial and Bézout's Theorem implies that there are at most 9 inflection points (with coordinates in the algebraic closure of $\mathbb{K}$). As we have seen earlier, the only point at infinity O of a curve, which is given by a Weierstraß equation, is an inflection point. Therefore, a necessary condition for a cubic to be transformable to a Weierstraß equation is that at least one of the inflection points is defined over $\mathbb{K}$. Let us assume such a point exists on our curve. By a linear transformation of coordinates with coefficients in $\mathbb{K}$ we can arrange that this inflection point has coordinates $(0 : 1 : 0)$ and the tangent line to the curve at this point is the line at infinity with equation $z_2 = 0$. Under these assumptions and using coordinates x, y on $U_2 \subset \mathbb{P}^2(\mathbb{K})$, it is clear that the cubic equation is of the form

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

In order to simplify the left hand side to y^2 we have to complete the square, which means that $y + \frac{a_1x+a_3}{2}$ is going to be the new y-coordinate. This obviously requires that we are able to divide by 2 which is possible in full generality only if the characteristic of $\mathbb{K}$ is not equal to 2. On the other hand, in order to absorb the term a_2x^2 on the right hand side we complete the cube. This is possible in general only if the characteristic of $\mathbb{K}$ is not equal to 3. As a result we obtain that any non-singular cubic with an inflection point in $\mathbb{P}^2(\mathbb{K})$ can be given by a Weierstraß equation if the characteristic of $\mathbb{K}$ is not equal to 2 or 3. Moreover, if the characteristic of $\mathbb{K}$ is not equal to 2, we can easily switch between (2) and (3), both are known as the Weierstraß canonical form in the literature.

It seems that the Weierstraß canonical form is the most widely known one. There are other canonical forms for cubic equations, each of which has its own advantages. Usually, it is only possible to achieve such a canonical form under some additional assumptions.

These are the *Legendre canonical form* (Adrien Marie Legendre, 1752–1833)

$$z_1^2z_2 = z_0(z_0 - z_2)(z_0 - \lambda z_2), \tag{5}$$

the *Hesse canonical form* (Ludwig Otto Hesse, 1811–1874)

$$z_0^3 + z_1^3 + z_2^3 + tz_0z_1z_2 = 0 \tag{6}$$

and the *Tate canonical form* (John Tate, 1925–)

$$z_1^2z_2 + bz_0z_1z_2 + cz_1z_2^2 = z_0^3 + dz_0^2z_2. \tag{7}$$

If the cubic is given by (5) or (7), the only point at infinity will again be the inflection point $O = (0 : 1 : 0)$. Therefore, we may also consider

$$y^2 = x(x-1)(x-\lambda)$$

as the Legendre canonical form and

$$y^2 + bxy + cy = x^3 + dx^2$$

as the Tate canonical form.

The Tate canonical form can be achieved for a cubic curve which has at least one point of finite order $n > 3$. So, it is not a general normal form for all cubics but it is very useful in order to find the torsion subgroup of $E(\mathbb{K})$.

The Legendre canonical form exhibits our curve as a double cover of the projective line $\mathbb{P}^1$. This branched double cover is given by the map which forgets the y-coordinate (or z_1 in the projective setting).

The map so defined can be extended to a map which is also defined at the point O at infinity. It has four branch points, namely O and the three points given by the roots of the right hand side, these are $(0 : 0 : 1), (1 : 0 : 1)$ and $(\lambda : 0 : 1)$. These four points are precisely the 2-torsion points of $E(\mathbb{K})$, i.e. those points P which satisfy $P + P = O$. This shows that only those cubic curves which have four 2-torsion points with coordinates in the field $\mathbb{K}$ can be transformed into a Legendre canonical form. In particular, if $\mathbb{K} = \mathbb{C}$ or any other algebraically closed field of characteristic not equal to two, this is always possible.

On the other hand, an equation in Hesse normal form does not have triple contact with the line at infinity. If the field $\mathbb{K}$ contains three cubic roots of unity (e.g. $\mathbb{K} = \mathbb{C}$), it has three points at infinity, namely the solutions of $z_0^3 + z_1^3 = 0$. These are inflection points of the cubic. If $\mathbb{K} = \mathbb{Q}$, for example, we see only one of them; this is the point $(1 : -1 : 0)$. This point is available over any field $\mathbb{K}$ and can be taken as the origin for the group structure. Then, the set of three-torsion points is precisely the set of inflection points of this cubic. In particular, if $\mathbb{K}$ contains three cubic roots of unity, the cubic contains nine three-torsion points which lie on the three coordinate lines $z_i = 0$.

The configuration of these nine points was studied by O. Hesse [9] who found that the nine inflection points lie on 12 lines, each of which contains three of these points. Each of the nine points is contained in four of the 12 lines. This set of nine points and 12 lines is now called the Hesse configuration. A recent survey on the Hesse configuration and an application to the study of examples of K3-surfaces can be found in [1].

Finally, let us mention that it is not hard to give an explicit formula for the group structure on $E(\mathbb{Q})$ if the curve is given in Weierstaß canonical form $y^2 = x^3 + px + q$. For example, if $P = (x_1, y_1)$ and $Q = (x_2, y_2) \neq -P$, the point $P + Q = (x_3, y_3)$ has coordinates

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$y_3 = -\left(\frac{y_2 - y_1}{x_2 - x_1}\right) x_3 - \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}.$$

This can be obtained using precisely the same calculations as in our examples in section 2. Remarkably, this formula does not depend on p, q, which is due to the non-presence of x^2 in the Weierstraß canonical form. However, p, q explicitly appear in the formula which describes the coordinates of $2P$. For each normal form such a formula can be obtained.

A formula which is impressive because of its beauty and simplicity is obtained when we start with an equation of the following form

$$x^2 + y^2 = a^2 + a^2x^2y^2.$$

If $P = (x, y)$ and $P' = (x', y')$ are two solutions of this equation, the group structure on the solution set is given by

$$P + P' = \frac{1}{a} \cdot \left(\frac{xy' + yx'}{1 + xyx'y'}, \frac{yy' - xx'}{1 - xyx'y'} \right).$$

The point $O = (0, a)$ is easily seen to be the neutral element of this group. More on this formula can be found in the recent article [3].

Because the given equation is of degree four, it is not clear how this example fits into the theory explained so far. That the solution set of this equation indeed forms a Mordell-Weil group can be explained using projective geometry. The basic idea is to show that, apart from a small number of points, the curve defined by this equation of degree four is isomorphic to a plane cubic curve.

The given curve of degree four has two singular points at infinity, namely $(1 : 0 : 0)$ and $(0 : 1 : 0)$. If $a^5 \neq a$ the curve has no other singular point. We are going to show explicitly that a non-singular version of this curve is the plane cubic given by the equation

$$y^2 = x \left(x + \frac{1 - a^2}{1 + a^2} \right) \left(x + \frac{1 + a^2}{1 - a^2} \right). \tag{8}$$

The outline of the construction is the following. We construct a non-singular version of the degree 4 curve which is embedded in projective three-space in such a way that a certain projection from a centre outside this non-singular curve maps it to the original degree 4 curve. We then find another projection whose centre is on this non-singular curve in three-space and which maps it isomorphically onto the plane cubic given by equation (8).

More specifically, using coordinates $(w : x : y : z)$ in $\mathbb{P}^3$, we define the curve $\widetilde{E}$ in $\mathbb{P}^3$ by the two simultaneous quadratic equations

$$xy - wz = 0$$
$$y^2 - a^2w^2 + x^2 - a^2z^2 = 0.$$

The projection with centre $(1:0:0:0)$ is the map which sends a point $(w:x:y:z) \in \mathbb{P}^3$ to the point $(x:y:z) \in \mathbb{P}^2$. This projection is not defined at the point $(1:0:0:0)$. All other points on the line in $\mathbb{P}^3$ through $(1:0:0:0)$ and $(0:x:y:z)$ are sent to the same point $(x:y:z) \in \mathbb{P}^2$. Because the line through $(1:0:0:0)$ and $(0:x:y:z)$ meets the curve $\widetilde{E}$ precisely when $z^2(x^2+y^2) = a^2z^4 + a^2x^2y^2$, the image of this projection is the plane curve of degree four given by this equation. Moreover, such a line has more than one intersection point with $\widetilde{E}$ if and only if it passes trough $(0:1:0:0)$ or $(0:0:1:0)$. Therefore, away from the two singular points we obtain an isomorphism between $\widetilde{E}$ and the image curve in $\mathbb{P}^2$.

The point $(0:0:-a:1)$ is on the curve $\widetilde{E}$. The projection with centre $(0:0:-a:1)$ is a map from $\mathbb{P}^3 \setminus \{(0:0:-a:1)\}$ to $\mathbb{P}^2$. It extends to a map which is defined on all of $\widetilde{E}$ and defines an isomorphism between $\widetilde{E}$ and its image curve in $\mathbb{P}^2$, which can be given by the cubic equation (8). The point on the curve $\widetilde{E} \subset \mathbb{P}^3$ which corresponds to the neutral element $O = (0, a)$, is the point $(0:0:a:1)$. The second projection sends this point to our usual neutral element $(0:1:0) \in \mathbb{P}^2$ at infinity. We leave the details of the calculations to the interested reader.

References

[1] M. Artebani, I. Dolgachev, *The Hesse pencil of plane cubic curves*, arXiv:math.AG/0611590

[2] J.W.S. Cassels, *Diophantine equations with special reference to elliptic curves.* J. Lond. Math. Soc. 41, 193–291 (1966); Corrigenda. Ibid. 42, 183 (1967)

[3] H.M. Edwards, *A normal form for elliptic curves.* Bull. Amer. Math. Soc. 44, 393–422 (2007)

[4] T. Ekedahl, *One semester of elliptic curves.* EMS Series of Lectures in Mathematics, European Mathematical Society Publishing House. (2006)

[5] M. Franz, *Theta Functions*, this issue.

[6] I. García-Selfa, M. A. Olalla, J. M. Tornero, *Computing the rational torsion of an elliptic curve using Tate normal form.* J. Number Theory 96, No. 1, 76–88 (2002)

[7] R.V. Gurjar et al., *Elliptic curves.* Praveshika Series. New Delhi: Narosa Publishing House/dist. by the AMS (2006)

[8] R. Hartshorne, *Algebraic geometry.* Graduate Texts in Mathematics 52, Springer (1977)

[9] O. Hesse, *Über die Wendepuncte der Curven dritter Ordnung.* J. Reine Angew. Math. 28, 97–107 (1844)

[10] D.H. Husemoller, *Elliptic curves.* Graduate Texts in Mathematics 111, Springer (1987)

[11] M. Khalid, *Group law on the cubic curve*, this issue.

[12] F. Kirwan, *Comples Algebraic Curves.* London Mathematical Society Study Texts 23, Cambridge University Press (1992)

[13] E. Lutz, *Sur l'équation* $y^2 = x^3 - Ax - B$ *dans les corps* $\mathfrak{p}$*-adiques.* J. reine angew. Math. 177, 238–247 (1937)

[14] B. Mazur, *Modular curves and the Eisenstein ideal.* Publ. Math., Inst. Hautes Étud. Sci. 47, 33–186 (1977)

[15] B. Mazur, *Rational isogenies of prime degree. (With an appendix by D. Goldfeld).* Invent. Math. 44, 129–162 (1978)

[16] L.J. Mordell, *Note on the integer solutions of the equation* $Ey^2 = Ax^3 + Bx^2 + Cx + D.$. Messenger (2) 51, 169–171 (1921)

[17] L.J. Mordell, O*n the rational solutions of the indeterminate equations of the third and fourth degrees.* Cambr. Phil. Soc. Proc. 21, 179–192 (1922)

[18] L.J. Mordell, *On the integer solutions of the equation* $ey^2 = ax^3 + bx^2 + cx + d.$ Lond. M. S. Proc. (2) 21, 415–419 (1923)

[19] T. Nagell, *Solution de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre.* Wid. Akad. Skrifter Oslo 1935, Nr. 1, 25 p (1935)

[20] C.L. Siegel, *The integer solutions of the equation* $y^2 = ax^n + bx^{n+1} + \cdots + k.$ (Extract from a letter to Prof. L. J. Mordell.) Journal L. M. S. 1, 66–68 (1926)

[21] J.H. Silverman, *The arithmetic of elliptic curves.* Graduate Texts in Mathematics 106, Springer (1986)

[22] J.T. Tate, *The arithmetic of elliptic curves.* Invent. Math. 23, 179–206 (1974)

[23] A. Weil, *Sur un théorème de Mordell.* Bulletin Sc. math. (2) 54, 182–191 (1930)

Mary Immaculate College, South Circular Road, Limerick, Ireland
E-mail address: bernd.kreussler@mic.ul.ie

GROUP LAW ON THE CUBIC CURVE

MADEEHA KHALID

Abstract. It is known that the set of rational points on a cubic curve E forms a group. The same procedure defines a group law on all points of E with complex coordinates. With the aid of the Weierstrass $\wp$-function one can show that E is isomorphic to a one dimensional complex torus, namely $E = \mathbb{C}/\Lambda$ where Λ is a rank 2 lattice in $\mathbb{C}$. The additive group structure of $\mathbb{C}$ descends to the quotient $\mathbb{C}/\Lambda$ and so we get another group structure on E. In fact these two group structures are the same. A nice proof of this fact follows from a classical result by Niels Henrik Abel (1802–1829), known as "Abel's theorem". In this article we introduce the notions of *divisors, line bundles*, and the *Picard group*, and then sketch the isomorphism between the two group structures.

1. Manifolds

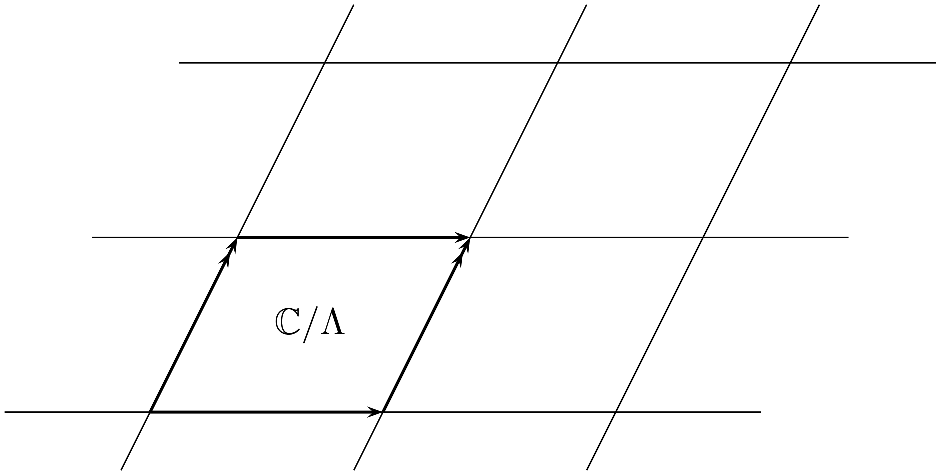
Throughout this article we work over $\mathbb{C}$, the field of complex numbers. We denote $\mathbb{P}^n(\mathbb{C})$ by $\mathbb{P}^n$.

An n dimensional complex manifold M is a topological space which locally looks like $\mathbb{C}^n$. This means that there exists an open cover U_α and co-ordinate maps $\phi_\alpha : U_\alpha \to \mathbb{C}^n$ such that $\phi_\alpha \phi_\beta^{-1} : \phi_\beta(U_\alpha \cap U_\beta) \to \mathbb{C}^n$ is holomorphic for all α, β. Similarly a function f on an open set $U \subset M$ is holomorphic if for all α, $f \circ \phi_\alpha^{-1}$ is holomorphic on $\phi_\alpha(U_\alpha \cap U) \subset \mathbb{C}^n$. A map $f : M \to N$ between two complex manifolds is holomorphic if it is given in terms of local holomorphic co-ordinates on N by holomorphic functions. Open subsets, products of complex manifolds and suitable quotients of complex manifolds are also complex manifolds.

The simplest example of a one dimensional complex manifold is just $\mathbb{C}$ itself. Then there is $\mathbb{P}^1$ (isomorphic to the Riemann sphere)

This work was supported by the IRCSET Embark Initiative Postdoctoral Fellowship Scheme.

which we have seen already in [9] Section 3. By $\mathbb{P}^1$ and $\mathbb{P}^2$ we mean the same objects as described in [9] Section 3, except that we replace $\mathbb{K}$ by $\mathbb{C}$. Let $\Lambda = \{n_1\omega_1 + n_2\omega_2 \mid n_i \in \mathbb{Z}\}$ be a rank two lattice in $\mathbb{C}$. Then Λ is an additive sub-group of $\mathbb{C}$ generated by two complex numbers ω_1, ω_2 which are linearly independent over the real numbers. Addition by elements of Λ defines a fixed point free discrete group action of Λ on $\mathbb{C}$ and hence the quotient $\mathbb{C}/\Lambda$ is a complex manifold. Since $\mathbb{R}/\mathbb{Z}$ is diffeomorphic to S^1 via the exponential map $r \mapsto \exp(2\pi i r)$, $\mathbb{C}/\Lambda$ is diffeomorphic to $S^1 \times S^1$ and is therefore called the one dimensional complex torus. Although all tori are diffeomorphic to each other, they may not be isomorphic as complex manifolds (see [3]).



The complex torus is a nice example of a one dimensional manifold which is easy to describe but which also has a very rich geometric and arithmetic structure. See for example *theta-functions* in the article by M. Franz [5], J. Silverman [11] on the arithmetic aspects of elliptic curves or the survey article by J. B. Bost [2] on construction of hyperelliptic Riemann surfaces.

A one dimensional complex manifold is called a *Riemann surface*. Any complex manifold is orientable so Riemann surfaces are orientable real surfaces. Compact Riemann surfaces are classified by their *genus* g which is a topological invariant and is equal to the number of holes in the surface. A more precise definition is that the first homology group of a Riemann surface of genus g is a free abelian group of rank $2g$, i.e. $H_1(S) \cong \mathbb{Z}^{2g}$.

So $\mathbb{P}^1$ has $g = 0$, the complex torus $\mathbb{C}/\Lambda$ which is diffeomorphic to $S^1 \times S^1$ has $g = 1$.

Each compact Riemann surface can be embedded holomorphically into some $\mathbb{P}^n$. In fact we can choose n to be 3. This is like an analogue of the Whitney embedding theorem which states that any compact n dimensional real manifold M can be embedded in $\mathbb{R}^{2n+1}$. A compact Riemann surface S together with an embedding $i : S \to \mathbb{P}^n$ is known as an *algebraic curve*. In this article however we will often refer to a compact Riemann surface as a *curve* without always necessarily specifying the embedding in $\mathbb{P}^n$.

Examples of two dimensional manifolds include $\mathbb{C}^2$, $\mathbb{P}^2$, and the two dimensional complex torus given by $\mathbb{C}^2/\Lambda$, where Λ is now a rank 4 lattice in $\mathbb{C}^2$. These lead to some simple examples in higher dimensions such as $\mathbb{C}^n$, $\mathbb{P}^n$, and $\mathbb{C}^n/\Lambda$ where Λ is a rank $2n$ lattice in $\mathbb{C}^n$.

Given a manifold M of dimension n, a subset $V \subset M$ given locally (i.e. on open subsets) as the zero set of a single holomorphic function f is called a *hypersurface* in M. For example $\mathbb{P}^1$ embeds in $\mathbb{P}^2$ as the zero set of the homogeneous linear function $z_1 = 0$. In local coordinates on U_1 it is given by $\{(\xi_1, \xi_2) \mid \xi_1 = 0\}$. Let $az_0+bz_1+cz_2$ be another linear equation. Then there is a matrix T in $\mathbb{P}GL(3)$ such that $T(z_1) = az_0 + bz_1 + cz_2$. Then $\{z_1 = 0\}$ gets mapped isomorphically to $\{az_0 + bz_1 + cz_2 = 0\}$. This shows that the zero set of *any* linear homogeneous equation in $\mathbb{P}^2$ is isomorphic to $\mathbb{P}^1$. Next we consider the zero sets of homogeneous equations of degree 2. If the equation is irreducible then this is is isomorphic to a conic which is again isomorphic to $\mathbb{P}^1$ ([9] Section 1).

In general we denote the zero set in $\mathbb{P}^2$ of a homogeneous polynomial of degree d by C, (also known as a *plane curve*) but when $d = 3$ we denote it by E (also known as a "cubic curve") for consistency with the notation in [9].

Suppose the plane curve $C = \{(z_0 : z_1 : z_2) \mid f(z_0, z_1, z_2) = 0\}$, is given by a (homogeneous) polynomial

$$f(z_0, z_1, z_2) = \sum_{i+j+k=d} a_{ijk} {z_0}^i {z_1}^j {z_2}^k$$

of degree d. Then, on open subsets of $\mathbb{P}^2$, the curve C is the zero set of a single holomorphic function. Recall that $\mathbb{P}^2 = U_0 \cup U_1 \cup U_2$ where $U_i = \{z_i \neq 0\}$. Affine coordinates on U_0 are $\xi_i = \frac{z_i}{z_0}$. Then $C \cap U_0 = \{(\xi_1, \xi_2) \mid F_0(\xi_1, \xi_2) = 0\}$, where $F_0(\xi_1, \xi_2) := \frac{f(z_0,z_1,z_2)}{{z_0}^d} =$

$\sum a_{ijk}{\xi_1}^j{\xi_2}^k$. So $C \cap U_0$ is the zero locus of the holomorphic function $F_0(\xi_1, \xi_2)$. The calculations for the other charts U_1 and U_2 are similar.

We say that $p \in C \cap U_0$ is a smooth point, if at least one of the partial derivatives $\frac{\partial F_0(\xi_1,\xi_2)}{\partial \xi_1}, \frac{\partial F_0(\xi_1,\xi_2)}{\partial \xi_2}$ is not equal to zero at p. We say C is smooth if every point in C is a smooth point. If C is smooth then in fact it is a *submanifold* of $\mathbb{P}^2$. Another example of a smooth curve is the curve given locally by ${\xi_1}^n + {\xi_2}^n = 1$. In homogeneous coordinates it is the zero locus of ${z_1}^n + {z_2}^n = {z_0}^n$ and is known as the *Fermat curve.*

There is a nice formula that computes the genus of a smooth plane curve C of degree d namely $g = \frac{(d-1)(d-2)}{2}$. So if C has degree d where $d \geq 3$ then $g \geq 1$ and hence C is not isomorphic to $\mathbb{P}^1$. The genus of the Fermat curve is $\frac{(n-1)(n-2)}{2}$ so for $n = 1$ and 2 it is isomorphic to $\mathbb{P}^1$ while for $n = 3$ it has genus one and is a complex torus.

The curve C' in $\mathbb{P}^2$ given by the equation $z_2{z_1}^2 - {z_0}^3 + {z_0}^2 z_2 = 0$ is not smooth as all the partial derivatives vanish at $(0 : 0 : 1)$. We say $(0 : 0 : 1)$ is a *singular* point of C'.

These notions of *smooth points* and *singular points* can also be extended to higher dimensional manifolds. In fact just as the implicit and inverse function hold in the differentiable case, so do their analytic versions. For example if V is a hypersurface given locally as the zero set of a single holomorphic function f and the jacobian matrix of f has rank 1 everywhere then V is a manifold of dimension $n - 1$.

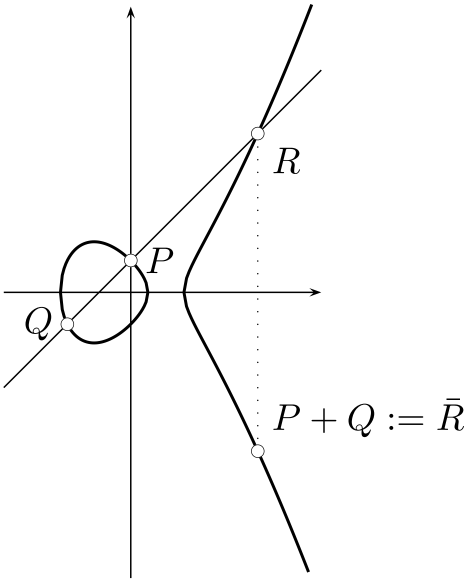
2. Cubic curves and the group law

It is mentioned in [9] that any smooth cubic E in $\mathbb{P}^2$ can be written as the zero set of the Weierstraß equation after an appropriate change of variables.

$$E = \{(z_0 : z_1 : z_2) \mid \ {z_1}^2 z_2 = 4{z_0}^3 - pz_0{z_2}^2 - q{z_2}^3\}.$$

Locally on U_2 this corresponds to $\{(x, y) \mid y^2 = 4x^3 - px - q\}$. In addition, the set of rational points on E forms a group, see [9] Theorem 8. In our case, i.e. when E is defined over $\mathbb{C}$, we show that this defines a group structure on all points of E with complex coordinates. As before, let O denote the point $(0 : 1 : 0)$. Let P and Q be any two points on E and consider the line in $\mathbb{P}^2$ containing

P and Q. Then, by the same prescription as in [9] Definition 5, we see that it meets E in a third point R. Now consider the line containing O and R. It meets E in a third point say $\bar{R}$. In the local coordinates (x, y), $\bar{R}$ is the reflection of R in the x-axis as mentioned in [9] Definition 5. We define $P + Q := \bar{R}$.



This is exactly the same as in [9] Theorem 8, except now we allow P and Q to have complex co-ordinates. In this way we get a group law on all of points of E with complex coordinates.

The choice of O as the *zero* element of the group E is not unique. In fact any point on E can be a *zero* ([10] Chapter 1, Section 2), however for E in the Weierstraß form this choice of the *zero* element simplifies the group law. We state the analogue of [9] Theorem 8 over $\mathbb{C}$.

Theorem 1. *Let E be a cubic curve in $\mathbb{P}^2$ given by the Weierstraß equation*

$$E = \{(z_0 : z_1 : z_2) \in \mathbb{P}^2 \mid \ {z_1}^2 z_2 = 4{z_0}^3 - g_2 z_0 {z_2}^2 - g_3 {z_2}^3\},$$

where g_2, g_3 are constants. Then there exists a unique group law on E such that $O := (0 : 1 : 0)$ is the zero element. The group structure is determined by requiring

$$P + Q + R = O \quad \textit{if and only if} \ \ P, Q, \ \textit{and } R \ \ \textit{are on a line.}$$

3. Complex torus

In this section we relate E to the one dimensional complex torus given as the quotient $\mathbb{C}/\Lambda$ of $\mathbb{C}$ by a rank 2 lattice Λ in $\mathbb{C}$. Since

$\mathbb{C}/\Lambda$ is diffeomorphic to $S^1 \times S^1$ it is like a hollow doughnut and so has genus 1. Recall that by the "genus formula" for smooth plane curves E also has genus 1. The following theorem shows that despite its different appearance E is isomorphic to $\mathbb{C}/\Lambda$.

Theorem 2. *Let Λ be a rank two lattice in $\mathbb{C}$. Then the one dimensional complex torus $\mathbb{C}/\Lambda$ can be embedded in $\mathbb{P}^2$ as a cubic in Weierstraß form.*

We sketch the main ideas of the proof and introduce the notion of *elliptic integrals*. For more details see [7] and [3]. Associated to Λ there is a meromorphic function on $\mathbb{C}/\Lambda$ called the Weierstraß $\wp$-function (Karl Weierstraß, 1802), defined as follows.

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

When viewed as a meromorphic function on $\mathbb{C}$, $\wp(z)$ is doubly periodic with respect to Λ and has poles of order 2 at all the lattice points. It satisfies the following differential equation.

$$\wp(z)'^2 = 4\wp(z)^3 - g_2\wp(z) - g_3. \tag{1}$$

The constants g_2, g_3 are related to Λ and are given by

$$g_2 = 60 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^4}, \quad g_3 = 140 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^6}.$$

A complete proof of Equation (1) and the derivations of g_2, g_3 is given in [5] Theorem 10.

The map $\mathbb{C}/\Lambda \to \mathbb{P}^2$ which identifies $\mathbb{C}/\Lambda$ with a cubic curve, is given as follows:

$$\tau([z]) = \begin{cases} (\wp(z) : \wp'(z) : 1) & \text{if } [z] \neq [0] \\ (0 : 1 : 0) & \text{if } [z] = [0]. \end{cases} \tag{2}$$

Since $\wp(z)$ satisfies the differential equation (1) we see that in the local co-ordinates (x, y) on U_2, the image of $\mathbb{C}/\Lambda$ via τ is given by

$$y^2 = 4x^3 - g_2x - g_3$$

which is the Weierstraß cubic equation. To justify the definition of $\tau([0])$, we observe that $\wp(z)$ has a pole of order 2 and $\wp'(z)$ has a pole of order 3 at $[0]$. So

$$\wp(z) = \frac{f(z)}{z^2} \quad \text{and} \quad \wp'(z) = \frac{g(z)}{z^3},$$

for some holomorphic functions f and g such that $f(0) \neq 0$, and $g(0) \neq 0$. Then, for values of $z \in \mathbb{C}$ close to $0 \in \mathbb{C}$, we have

$$\tau([z]) = (\wp(z) : \wp'(z) : 1) = (zf(z) : g(z) : z^3)$$

and at $z = 0$ we obtain $(zf(z) : g(z) : z^3) = (0 : 1 : 0)$, which is $\tau([0]) = O$, the zero element of the group structure on the cubic curve E. This shows that we get a holomorphic map $\tau : \mathbb{C}/\Lambda \to E$, where E is a cubic curve in Weierstraß form. One way of showing that it is an isomorphism is via an inverse mapping and this brings us to the topic of *elliptic integrals.*

An *elliptic integral* is an integral of the form

$$\int_{x_0}^{x_1} R(x,y)dx$$

where $R(x,y)$ is a rational function, and y^2 is a polynomial in x of degree 3 or 4 without multiple roots.

They are called *elliptic integrals* because they first arose in the context of determining the arc lengths of an ellipse and of other second order curves. Early work on such integrals goes back to Wallis, Bernoulli, MacLaurin, Riccati and D'Alembert. However for a long time the problem of inverting such integrals was unsolved. It was found that they cannot be expressed in terms of the known transcendental functions and also that only three types of new transcendents suffice to express all such integrals.

Building on work of Fagnano (Giulio Carlo Fagnano dei Toschi, 1682–1766), Euler discovered in 1756 an addition formula for such integrals. In modern language Euler's formula is an addition formula for elliptic functions such as the Weierstraß $\wp$-function. Much later, in the second half of the 19-th century, Weierstraß showed that in fact elliptic functions can be characterised by their property of possessing an algebraic addition theorem.

The mystery surrounding the mathematical nature of elliptic integrals was only unveiled by the works of Abel and Jacobi, simultaneously published in September 1827. The main new idea was to study the inverse of the function given by an elliptic integral. Nowadays, such functions are called *elliptic functions*. Abel also noted that while the elliptic integral itself is a highly complicated function of the point (x, y), sums of such integrals (known as *Abelian sums*)

$$\sum \int\limits_{x_0}^{x_i} R(x, y) dx$$

satisfy simpler relations. We state and use a special case of Abel's theorems later (Section 7, Theorem 22).

Liouville identified in 1844 that the property to be doubly periodic is the crucial one upon which their analytic study should be based. Jacobi's theta functions and the Weierstaß $\wp$-function form now the fundaments of a modern theory of elliptic functions. Their definition and basic properties can be found in the article by M. Franz [5].

Even though elliptic integrals are historically older than elliptic functions, we usually come across elliptic functions first. The reason being the work of Cauchy in the theory of complex analysis which has made the latter an easier object of study today than the integrals themselves. The elliptic integrals appear then as inverses of elliptic functions.

If $y^2 = 4x^3 - g_2 x - g_3$, an elliptic integral (of the first kind) which is of particular importance, is

$$\int\limits_{O}^{P} \frac{dx}{y}.$$

This is to be understood as a contour integral along a path $(x(t), y(t))$ in $\mathbb{C}^2$ which connects the point O with the point P. It is assumed the this path is completely contained in the curve given by the equation $y^2 = 4x^3 - g_2 x - g_3$ which we know is the curve E in terms of local coordinates (x, y). Since the genus of E is 1, the curve E is not simply connected and the integral depends on the choice of the path. However, this dependence is only modulo the *periods* of $\frac{dx}{y}$. This means that the value of the elliptic integral changes only by an additive constant of the form $n\omega_1 + m\omega_2$ with $m, n \in \mathbb{Z}$. Here the complex numbers ω_1 and ω_2 are given by

$$\omega_1 = \int\limits_{\gamma_1} \frac{dx}{y} \quad \text{and} \quad \omega_1 = \int\limits_{\gamma_2} \frac{dx}{y},$$

where γ_1, γ_2 are two closed paths representing a pair of generators of the fundamental group of E. The numbers ω_1, ω_2 are called periods because the inverse function of this integral (which is the Weierstraß $\wp$-function) is doubly periodic with *periods* ω_1, ω_2. The periods ω_1, ω_2 are linearly independent over $\mathbb{R}$ because the paths γ_1, γ_2 are generators of the fundamental group.

So $\Lambda = \{n\omega_1 + m\omega_2 \mid n, m \in \mathbb{Z}\}$ is a lattice in $\mathbb{C}$ and in this way we reconstruct the lattice Λ we started with. Moreover, if we set

$$\tau^{-1}(P) = \int_O^P \frac{dx}{y}$$

where O is the point at infinity and $P \in E$ any point, we obtain a well-defined map $\tau^{-1} : E \to \mathbb{C}/\Lambda$ which is the inverse of the map τ defined earlier. This gives an isomorphism of E with $\mathbb{C}/\Lambda$. The differential $\frac{dx}{y}$ is actually the familiar differential dz on the torus $\mathbb{C}/\Lambda$. That is because $x = \wp(z), y = \wp'(z)$ so we get $\tau^* \frac{dx}{y} = dz$, the integral of which is well defined modulo Λ.

In order for this procedure to work, all we need is that the cubic curve $y^2 = 4x^3 - g_2 x - g_3$ be smooth, i.e. $g_2^3 - 27g_3^2 \neq 0$. Since any smooth cubic curve in $\mathbb{P}^2$ is isomorphic to a cubic in Weierstraß form, it follows that every smooth cubic in $\mathbb{P}^2$ is isomorphic to a complex torus. For more details see [7] Chapter 2.

4. Divisors

In the previous section we saw that a plane cubic curve E is isomorphic to a complex torus $\mathbb{C}/\Lambda$. Now $\mathbb{C}/\Lambda$ inherits a group structure from $\mathbb{C}$ and hence induces a group structure on E via the isomorphism. In Section 2 we defined a group operation on E using geometry. How do these two compare?

The answer is: they coincide! In the subsequent sections we describe a proof which weaves together some pretty ideas from algebraic geometry. To do so we have to first introduce an important notion in algebraic geometry which is that of a *divisor*. In the case of a curve it has a simple description.

Definition 3. Let C be a smooth curve in $\mathbb{P}^2$. A divisor on C is a formal finite linear combination $D = a_1 \cdot P_1 + \cdots + a_m \cdot P_m$ of points $P_i \in C$ with integer coefficients a_i.

Divisors can be added or subtracted and hence form a group denoted $\mathrm{Div}(C)$.

Definition 4. The *degree* of a divisor $D = a_1 \cdot P_1 + \cdots + a_m \cdot P_m$ is defined to be $\deg D = \sum_{i=1}^{m} a_i$ and this gives a group homomorphism $\deg : \mathrm{Div}(C) \to \mathbb{Z}$.

Remark 5. The notion of a divisor extends also to higher dimensional manifolds. In that case a divisor is a linear combination of subsets given locally by zero sets of irreducible holomorphic functions.

The group $\mathrm{Div}(C)$ is very large, even in the one-dimensional case. Therefore we introduce the sub-group of principal divisors. The benefit is that the factor group of all divisors modulo principal divisors is finitely generated. This factor group will prove to be useful in Section 6 as well. In order to explain the definition of principal divisors, we need the notion of the *order* of a function at a point P

Let f be a holomorphic function on an open set $U \subset C$. Let $P \in U$ and let x be the local co-ordinate on U such that P is given by $x - \lambda$ for some $\lambda \in \mathbb{C}$. The order of f at P, denoted $\mathrm{ord}_P(f)$, is the largest integer $a \in \mathbb{Z}$ such that locally

$$f(x) = (x - \lambda)^a \cdot h(x)$$

where h is a holomorphic function with $h(\lambda) \neq 0$. Since f is holomorphic a is non negative. Note that for g, h any holomorphic functions

$$\mathrm{ord}_P(gh) = \mathrm{ord}_P(g) + \mathrm{ord}_P(h).$$

We would like to include the cases when $\mathrm{ord}_P(f)$ is negative. To do so we have to include what are known as *meromorphic functions.* A function f on C is called a *meromorphic function* if it can be written locally as a ratio $\frac{g}{h}$, where $g \neq 0$ and h are holomorphic functions which do not have a common zero. Then, by using a Laurent series expansion for f at P, we see that $\mathrm{ord}_P(f) = \mathrm{ord}_P(g) - \mathrm{ord}_P(h)$. So $\mathrm{ord}_P(f)$ is negative if $\mathrm{ord}_P(g) < \mathrm{ord}_P(h)$.

Collecting zeros and poles of a global meromorphic function f gives us a natural way to associated a divisor to it.

Definition 6. Let f be a *meromorphic function* on C. Then the divisor of f, called a *principal divisor* and denoted (f), is given by

$$(f) = \sum_{P \in C} \mathrm{ord}_P f \cdot P.$$

Example 7. Consider $\mathbb{P}^1$, the Riemann sphere with homogeneous co-ordinates $(z_0 : z_1)$. Then any ratio $f = \frac{g}{h}$, where g and h are homogeneous polynomials of the same degree d, is a global meromorphic function. So for instance if $f = \frac{{z_0}^2}{{z_1}^2+z_0z_1}$ then $(f) = 2 \cdot P_0 - P_1 - P_2$ where $P_0 = (0 : 1), P_1 = (1 : 0), P_2 = (1 : -1)$. Note that $\deg(f) = 0$.

Now we do the same thing for curves in $\mathbb{P}^2$. A meromorphic function f on $\mathbb{P}^2$ restricts to a meromorphic function on the curve C if the denominator in the local expression for f does not vanish identically on the curve. Its associated divisor (f) restricts to a divisor on C. As an example lets take the function $f = \frac{{z_0}^2+{z_1}^2+{z_2}^2}{{z_1}^2}$ and the line $L_0 = \{z_2 = 0\}$. Then a local computation shows that

$$(f) = (1 : i) + (1 : -i) - 2 \cdot (1 : 0).$$

Given any curve $C \subset \mathbb{P}^2$ and any divisor D on C, a natural question to ask is whether $D = (f)$ for some meromorphic function f on C? The following example is a partial answer to this question.

Example 8. Consider the line $L_2 = \{(z_0 : z_1 : z_2) | z_2 = 0\}$ in $\mathbb{P}^2$. (see [9] Section 3) and O the point $(0 : 1 : 0)$. Then $D = 2 \cdot O$ is a divisor on L_2. If $D = (f)$ for some meromorphic function on L_2, then f has a zero of order 2 at O and is holomorphic and nonzero everywhere else. Since L_2 is isomorphic to $\mathbb{P}^1$ there are no non-constant holomorphic functions on $\mathbb{P}^1$, $D \neq (f)$ for any f.

In the case of $\mathbb{P}^1$ the answer to the above question is very simple. A divisor $D = (f)$ if and only if $\deg D = 0$. For a cubic curve E the answer is not so simple. For instance there exist divisors of degree 0 which are not associated to any meromorphic function. In fact there are as many such divisors as there are points on E. We discuss this in more detail in Section 6. See also the article by C. Daly [4].

5. Line Bundles

Divisors are closely tied together to another geometric notion which is that of a *line bundle.* A line bundle is a rank 1 holomorphic vector bundle (Definition 10). In this section we discuss the relations between line bundles and divisors.

Let us for the moment refer back to Example 8. The homogeneous coordinates z_0, z_1 of $\mathbb{P}^2$ are also natural homogeneous coordinates on L_2, since $L_2 = \{(z_0 : z_1 : 0) \in \mathbb{P}^2\}$. Our aim is to associate to a homogeneous polynomial in the ring $\mathbb{C}[z_0, z_1]$ its "divisor of zeroes". For example consider the homogeneous quadratic polynomial z_0^2. Since it is a homogeneous polynomial it is invariant under scalar multiplication and so $D := \{z_0^2 = 0\}$ is a well defined subset of L_2.

This zero set has a local description. Recall from [9] Section 3 that L_2 is covered by two open charts $V_0 = \{z_0 \neq 0\}$ and $V_1 = \{z_1 \neq 0\}$. The affine coordinate on V_0 is $z = \frac{z_1}{z_0}$ and the affine coordinate on V_1 is $w = \frac{z_0}{z_1}$. On $V_0 \cap V_1$ we have the identification map $z = \frac{1}{w}$.

Consider $D \cap V_1 = \{(z_0 : z_1) \in V_1 \mid z_0^2 = 0\}$. If $(z_0 : z_1) \in D \cap V_1$ then certainly $(\lambda z_0 : \lambda z_1) \in D \cap V_1$, so we divide by z_1 to get that $D \cap V_1 = \{(\frac{z_0}{z_1} : 1) \mid \frac{z_0^2}{z_1^2} = 0\}$. In terms of the coordinate on V_1 this is just $\{w \in V_1 \mid w^2 = 0\}$.

Similarly $D \cap V_0 = \{(z_0 : z_1) \in V_0 \mid z_0^2 = 0\}$. In terms of the coordinate on V_0 this corresponds to $\{(1 : z) \mid \frac{z_0^2}{z_0^2} = 1 = 0\}$ which is just the empty set. So, locally D corresponds to the following subsets

$$\begin{aligned} D \cap V_0 &= \{z \in V_0 \mid 1 = 0\}, \\ D \cap V_1 &= \{w \in V_1 \mid w^2 = 0\}. \end{aligned}$$

Set $f_0 := 1$, $f_1 := w^2$, then $\{(V_0, f_0), (V_1, f_1)\}$ are *local defining functions* for D. Notice that on $V_0 \cap V_1$, we have $w^2 = \frac{1}{z^2} \neq 0$ and

$$f_0(z) = f_1(z) \cdot z^2.$$

Similarly $f_1(w) = f_0(w) \cdot w^2$ on $V_0 \cap V_1$, so the local defining functions are related by a nowhere vanishing factor.

Now $D \cap V_0 = \emptyset$ and $D \cap V_1$ is the origin $w = 0$ counted with multiplicity 2. The point $w = 0$ in V_1 corresponds to $(0 : 1 : 0)$ on L_2. Since this occurs with multiplicity 2, D is the divisor $2 \cdot O$ where $O = (0 : 1 : 0)$, as before.

The interesting thing is that from these local defining functions of D we construct a new manifold L called a *line bundle*. The non-vanishing factor that relates these local defining functions of D is known as a *transition function*. We give one more example before stating the definitions.

Example 9. Set

$$L := V_0 \times \mathbb{C} \cup V_1 \times \mathbb{C} / \sim$$

where $V_0 \times \mathbb{C}$ and $V_1 \times \mathbb{C}$ are open charts of L. The equivalence relation $\sim$ gives the "patching" condition on the overlap $(V_0 \cap V_1) \times \mathbb{C}$

and is defined as follows. For $w = \frac{1}{z} \in V_0 \cap V_1$ and $(w, \lambda) \in V_1 \times \mathbb{C}$, $(z, \mu) \in V_0 \times \mathbb{C}$ we define

$$(w, \lambda) \sim (z, \mu) \quad \iff \quad \mu = z^2 \lambda.$$

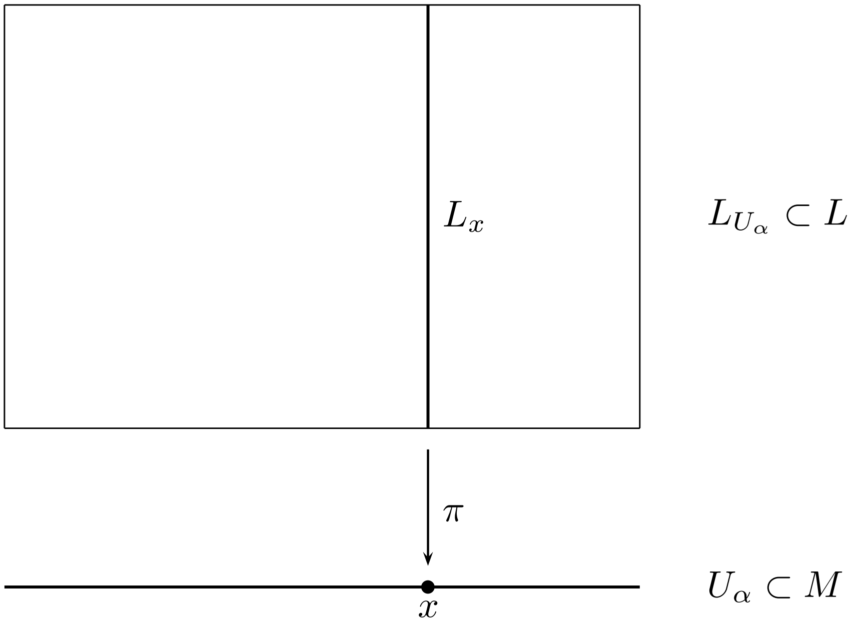
Note that we define the "patching" condition using z^2, the nowhere vanishing function on $V_0 \cap V_1$ relating the two local descriptions of D above.

This new manifold L is an example of a *line bundle*, (see Def. 10 below) and is often denoted $\mathcal{O}(D)$. The collection $\{(f_0, V_0), (f_1, V_1)\}$ of local defining functions for $D = 2 \cdot O$ defines a *section* (see subsection 5.2) of $\mathcal{O}(D)$ and the function z^2 relating these local functions on the overlap $V_0 \cap V_1$ is a *transition function* of $\mathcal{O}(D)$.

We now give the general definition of a line bundle.

Definition 10. Let M be a complex manifold. A *line bundle* $L \xrightarrow{\pi} M$ is a holomorphic vector bundle of rank 1. That is

(1) L is a complex manifold such that for any $x \in M$, $\pi^{-1}(x) = L_x$ is equipped with the structure of a one dimensional complex vector space.
(2) The projection mapping $\pi : L \to M$ is holomorphic.
(3) There is an open cover $\{U_\alpha\}$ of M and biholomorphic maps, $\phi_\alpha : \pi^{-1}(U_\alpha) \to U_\alpha \times \mathbb{C}$, compatible with the projections onto U_α, such that the restriction to the fibre $\phi_\alpha : L_x \to \{x\} \times \mathbb{C}$ is linear for all $x \in U_\alpha$. The pair (ϕ_α, U_α) is called a *trivialisation* of L over U_α.



Since L is a complex manifold, for any pair of trivialisations ϕ_α, ϕ_β the map $g_{\alpha\beta} : U_\alpha \cap U_\beta \to \mathbb{C}^*$ given by

$$\phi_\alpha\left(\phi_\beta^{-1}(x, v)\right) = (x, g_{\alpha\beta}(x) \cdot v)$$

is holomorphic. The maps $g_{\alpha\beta}$ are called *transition functions* of L with respect to the *trivialisations* $(\phi_\alpha, U_\alpha), (\phi_\beta, U_\beta)$. They determine the line bundle L and satisfy the following conditions

(1) $g_{\alpha\beta}(x) \cdot g_{\beta\alpha}(x) = 1$ for all $x \in U_\alpha \cap U_\beta$;
(2) $g_{\alpha\beta}(x) \cdot g_{\beta\gamma}(x) \cdot g_{\gamma\alpha}(x) = 1$ for all $x \in U_\alpha \cap U_\beta \cap U_\gamma$.

Condition (2) is known as the *cocycle condition.*

Conversely, given an open cover $\{U_\alpha\}$ of M and holomorphic maps $g_{\alpha\beta} : U_\alpha \cap U_\beta \to \mathbb{C}^*$, satisfying the conditions above, we can construct a line bundle L with transition functions $g_{\alpha\beta}$. Define an equivalence relation $\sim$ on the union over all α of $U_\alpha \times \mathbb{C}$ as follows. For $x \in U_\alpha \cap U_\beta$, $(x, \lambda) \in U_\beta \times \mathbb{C}$ and $(x, \mu) \in U_\beta \times \mathbb{C}$ set $(x, \lambda) \sim (x, \mu)$ if and only if $\mu = g_{\alpha\beta}(x) \cdot \lambda$. Then

$$L = \bigcup_\alpha U_\alpha \times \mathbb{C} / \sim$$

is a line bundle with transition functions $g_{\alpha\beta}$.

For ease of notation from now on we set $L_U = \pi^{-1}(U)$

Given L as above, for any collection of nowhere vanishing holomorphic functions f_α on U_α we can define alternative trivialisations ϕ'_α of L over U_α by multiplying the second component of $\phi_\alpha(x) \in U_\alpha \times \mathbb{C}$ with $f_\alpha(x)$. In a more sloppy way we write

$$\phi'_\alpha = f_\alpha \phi_\alpha. \tag{3}$$

The transition functions relative to (ϕ'_α, U_α) are

$$g'_{\alpha\beta} = \frac{f_\alpha}{f_\beta} g_{\alpha\beta}.$$

Any other trivialisation of L can be obtained in this way, so we see that the collections $\{g'_{\alpha\beta}\}$ and $\{g_{\alpha\beta}\}$ define the same line bundle *if and only if* there exist nowhere vanishing holomorphic functions f_α on U_α satisfying (3) above.

Example 11. The simplest example of a line bundle on a manifold is $M \times \mathbb{C}$ also known as the *trivial bundle* $\mathcal{O}_M$.

Example 12. The line bundle that we constructed in Example 9 is known as $\mathcal{O}_{\mathbb{P}^1}(2)$. All line bundles constructed in this way from a divisor defined by a homogeneous quadratic polynomial on $\mathbb{P}^1$ are isomorphic because for any two such polynomials there is an isomorphism of $\mathbb{P}^1$ which maps one to the other.

Remark 13. In fact given any $n \in \mathbb{Z}^+$ all line bundles obtained from divisors corresponding to a homogeneous polynomial of degree n on $\mathbb{P}^1$ are isomorphic and denoted by $\mathcal{O}_{\mathbb{P}^1}(n)$.

Example 14. Recall that $\mathbb{P}^1 = (\mathbb{C}^2 \setminus \{0\})/\sim$ where $(z_0, z_1) \sim (\lambda z_0, \lambda z_1)$ for all $\lambda \in \mathbb{C}^*$. This means, each line $l \subset \mathbb{C}^2$ through the origin corresponds to a point $[l] \in \mathbb{P}^1$. Let

$$\begin{aligned} L &= \{((z_0 : z_1), v) \in \mathbb{P}^1 \times \mathbb{C}^2 \mid v \in \mathbb{C} \cdot (z_0, z_1)\} \\ &= \{([l], v) \in \mathbb{P}^1 \times \mathbb{C}^2 \mid v \in l\} \end{aligned}$$

and denote projection onto the first factor by $\pi : L \to \mathbb{P}^1$. Then, in terms of local co-ordinates on U_0 and U_1 as before, we obtain

$$\begin{aligned} L_{U_0} &= \{(z, (\beta, \beta z)) \mid \beta \in \mathbb{C}\} \\ L_{U_1} &= \{(w, (\eta w, \eta)) \mid \eta \in \mathbb{C}\} \end{aligned}$$

with trivialisations

$$\begin{aligned} \phi_0 : L_{U_0} &\to U_0 \times \mathbb{C} & \qquad \phi_1 : L_{U_1} &\to U_1 \times \mathbb{C} \\ (z, (\beta, \beta z)) &\mapsto (z, \beta) & (w, (\eta w, \eta)) &\mapsto (w, \eta) \end{aligned}$$

The reader can check that the transition function g_{01} is;

$$g_{01}(z) = \phi_0 \phi_1^{-1} = \frac{1}{z}.$$

This vector bundle is also known as the *universal bundle* on $\mathbb{P}^1$ denoted $\mathcal{O}_{\mathbb{P}^1}(-1)$ and is an important example.

A nice property of line bundles is that they can be "pulled back". Suppose $f : M \to N$ is a holomorphic map of complex manifolds, and $\pi : L \to N$ is a line bundle on N. Then we define the *pull back bundle* f^*L by setting $(f^*L)_x = L_{f(x)}$. More precisely,

$$f^*L = \{(m, v) \mid f(m) = \pi(v)\} \subset M \times L.$$

If $\phi : L_U \to U \times \mathbb{C}$ is a trivialisation of L in a neighbourhood U of $f(x)$, then we obtain a trivialisation

$$f^*\phi : (f^*L)_{f^{-1}(U)} \to f^{-1}(U) \times \mathbb{C}$$

which is the composition

$$(f^*L)_{f^{-1}(U)} \subset f^{-1}(U) \times L_U \xrightarrow{\mathrm{Id} \times \phi} f^{-1}(U) \times U \times \mathbb{C} \xrightarrow{pr} f^{-1}(U) \times \mathbb{C}.$$

This gives f^*L its manifold structure over the open set $f^{-1}(U)$. The transition functions for f^*L are the pull backs $f^*(g_{\alpha\beta}) := g_{\alpha\beta} \circ f$ of the transition functions $g_{\alpha\beta}$ of L.

Remark 15. If D is a divisor on N with local defining functions $\{(h_\alpha, U_\alpha)\}$, we can pull it back to a divisor f^*D on M with local defining functions $\{(h_\alpha \circ f, f^{-1}(U_\alpha))\}$. If $L = \mathcal{O}(D)$, then $f^*(L) = \mathcal{O}(f^*D)$.

5.1. **Group structure on the set of all line bundles.** The tensor product of $\mathbb{C}$ with itself, $\mathbb{C} \otimes \mathbb{C}$ is $\mathbb{C}$ again. Similarly given two line bundles L_1 and L_2 with transition functions $g_{\alpha\beta}$ and $h_{\alpha\beta}$ respectively, we can define the tensor product $L_1 \otimes L_2$ and get a new line bundle L. The fibres of L are just the tensor product of fibres of L_1 and L_2. The transition functions $t_{\alpha\beta}$ of L are therefore the product of the transition functions of L_1 and L_2, i.e. for all $x \in U_\alpha \cap U_\beta$

$$t_{\alpha\beta}(x) = g_{\alpha\beta}(x)h_{\alpha\beta}(x).$$

This defines a binary operation on the set of line bundles. Tensoring with the trivial bundle $\mathcal{O}$ gives the same bundle back, so it is the *neutral element* of the group structure. Associated to each line bundle L with transition functions $g_{\alpha\beta}$, there is another line bundle L^* whose transition functions are $g_{\alpha\beta}^{-1}$. It is called the *dual bundle* of L. Since $L \otimes L^* = \mathcal{O}$, the dual bundle is like the *inverse* of L. Hence we get a group structure on the isomorphism classes of line bundles on M. This group is called the *Picard group* of M denoted $\mathrm{Pic}(M)$. In the next section we describe $\mathrm{Pic}(E)$ for E a smooth cubic curve in $\mathbb{P}^2$.

5.2. **Sections of a line bundle.** A *section* s of a line bundle L is a holomorphic map $s : M \to L$ such that $\pi \circ s = \mathrm{Id}$. Locally this means we have an open cover U_α and a collection of holomorphic functions $s_\alpha : U_\alpha \to \mathbb{C}$ such that

$$s_\alpha(x) = g_{\alpha\beta}(x) \cdot s_\beta(x) \quad \forall\ x \in U_\alpha \cap U_\beta.$$

An example of a section is given in Example 9. It may be the case that a line bundle does not have any holomorphic sections. Local holomorphic sections always exist but they may not satisfy the patching condition on overlaps.

For instance consider the line bundle $\mathcal{O}_{\mathbb{P}^1}(-1)$ as in Example 14. Suppose it has a local holomorphic section $s_1(w)$ on U_1 where $s_1(w)$ is a holomorphic function. Then on $U_0 \cap U_1$ it transforms to $s_0(z) =$

$s_1(\frac{1}{z}) \cdot \frac{1}{z}$ which is a meromorphic function on U_0 and certainly not holomorphic. This shows that $\mathcal{O}_{\mathbb{P}^1}(-1)$ does not have any global holomorphic sections and therefore we extend our definition to allow *meromorphic sections* of L. A collection of local meromorphic functions $\{s_\alpha : U_\alpha \to \mathbb{C}\}$ such that $s_\alpha = g_{\alpha\beta}s_\beta$ will be called a *meromorphic section* of L. The section $s_1(w) = 1, s_0(z) = \frac{1}{z}$ is a global meromorphic section of $\mathcal{O}_{\mathbb{P}^1}(-1)$ with a simple pole at $(1:0)$.

Finally we come to the correspondence between divisors and line bundles.

5.3. **Divisors and line bundles.** Let D be a divisor on a curve C and let $\{(f_\alpha, U_\alpha)\}$ be local defining functions for D. Then the functions $g_{\alpha\beta} = \frac{f_\alpha}{f_\beta}$ are holomorphic and non zero on $U_\alpha \cap U_\beta$. They also satisfy the cocycle condition on $U_\alpha \cap U_\beta \cap U_\gamma$ since

$$g_{\alpha\beta}g_{\beta\gamma}g_{\gamma\alpha} = \frac{f_\alpha}{f_\beta}\frac{f_\beta}{f_\gamma}\frac{f_\gamma}{f_\alpha} = 1 \text{ on } U_\alpha \cap U_\beta \cap U_\gamma.$$

So the collection $\{g_{\alpha\beta}\}$ defines a line bundle called the *associated line bundle of* D, and denoted $\mathcal{O}(D)$, (see also Example 9.)

Conversely since any curve C embeds in some projective space $\mathbb{P}^n$, given a line bundle L over a curve C, there exists a meromorphic section s of L (for a proof see [7] Chapter 1, Section 2, the proposition directly before the Lefschetz theorem on $(1,1)$ classes.) Consider a local representation $\{s_\alpha, U_\alpha\}$ of s. Then given any $P \in C$ we can define the *order of* s *at* P as

$$\mathrm{ord}_P(s) = \mathrm{ord}_P(s_\alpha)$$

Where α is arbitrary with $P \in U_\alpha$. This does not depend on the choice of α, since $\frac{s_\alpha(x)}{s_\beta(x)} = g_{\alpha\beta}(x) \in \mathbb{C}^*$ for all $x \in U_\alpha \cap U_\beta$ and so $\mathrm{ord}_P s_\alpha = \mathrm{ord}_P s_\beta$, if $P \in U_\alpha \cap U_\beta$. We take the divisor (s) of s to be

$$(s) = \sum_{P \in C} \mathrm{ord}_P(s) \cdot P.$$

If we were to take the line bundle associated to the divisor (s) we would recover L our original line bundle. So we get a map

$$\begin{aligned} \mathrm{Div}(C) &\to \mathrm{Pic}(C) & (4) \\ D &\mapsto \mathcal{O}(D) & (5) \end{aligned}$$

Remark 16. This correspondence still holds if we replace C by an algebraic complex manifold M.

In fact (4) is a group homomorphism. A good exercise is to check it is well defined. Suppose D_1, D_2 are two divisors. We can choose an open cover fine enough so that they are locally defined by $\{f_\alpha\}, \{h_\alpha\}$. Then $D_1 + D_2$ has local defining functions $\{f_\alpha h_\alpha\}$. The corresponding line bundle $\mathcal{O}(D_1 + D_2)$ has transition functions $t_{\alpha\beta} = \frac{f_\alpha h_\alpha}{f_\beta h_\beta}$. The line bundles $\mathcal{O}(D_1)$ and $\mathcal{O}(D_2)$ have transition functions $g_{\alpha\beta} = \frac{f_\alpha}{f_\beta}$ and $q_{\alpha\beta} = \frac{h_\alpha}{h_\beta}$ respectively. It is clear that $t_{\alpha\beta} = g_{\alpha\beta} q_{\alpha\beta}$, so $\mathcal{O}(D_1 + D_2) = \mathcal{O}(D_1) \otimes \mathcal{O}(D_2)$. In other words *addition of divisors in* $\mathrm{Div}(C)$ *maps to tensor product of line bundles in* $\mathrm{Pic}(C)$. If $D = (f)$ for some global meromorphic function then $f_\alpha = f_\beta$ so $g_{\alpha\beta} = 1$ and hence $\mathcal{O}(D)$ is the trivial line bundle. We say D_1 *is linearly equivalent to* D_2, denoted $D_1 \sim D_2$, *if and only if* there exists a global meromorphic function f on C such that $D_1 = D_2 + (f)$.

Lemma 17. *Let C be a curve. Let* $\mathrm{Div}(C)$ *denote the group of divisors and* $\mathrm{Pic}(C)$ *the group of line bundles on C. Then $\mathcal{O}(D)$ is trivial if and only if $D = (f)$ for some meromorphic function on C, i.e.* $\mathrm{Div}(C)/\sim\ \cong\ \mathrm{Pic}(C)$.

Proof. We have seen that (f) corresponds to the trivial line bundle so we just need to show that if $\mathcal{O}(D)$ is a trivial line bundle then $D = (f)$. Let $\{(f_\alpha, U_\alpha)\}$ be local defining functions for D. Then $\mathcal{O}(D)$ trivial implies there exist functions $h_\alpha : U_\alpha \to \mathbb{C}^*$ such that

$$\frac{f_\alpha}{f_\beta} = g_{\alpha\beta} = \frac{h_\alpha}{h_\beta} = 1.$$

Hence,

$$f = \frac{f_\alpha}{h_\alpha} = \frac{g_{\alpha\beta} f_\beta}{g_{\alpha\beta} h_\beta} = \frac{f_\beta}{h_\beta}$$

is a global meromorphic function on C with divisor D. □

Let L be a line bundle on C and s a meromorphic section of L. For the reader familiar with some differential geometry we now mention a nice relation between the first chern class of $\mathcal{O}(D)$ and D. Given a divisor D on C let η_D denote its Poincare dual in $H^2(C, \mathbb{Z})$. Let L be any line bundle. Then L admits a hermitian metric and there is a unique connection on L compatible with the metric and complex structure. Let Θ be the curvature form associated to this metric connection.

Theorem 18. *Let $L = \mathcal{O}(D)$ be a line bundle. Let Θ be the curvature form associated to a metric connection. Let η_D denote the Poincaré dual of D in $H^2_{DR}(C)$ and let $c_1(L)$ denote the first Chern class of L. Then*

$$c_1(L) = \left[\frac{\Theta i}{2\pi}\right] \; = \; \eta_D \in \; H^2_{DR}(C).$$

For a proof see [7] Chapter 1, Section 1. This implies

$$\frac{i}{2\pi}\int_C \Theta = \langle \eta_D, [C] \rangle = \deg D.$$

Remark 19. All the results of this section also hold when we replace C by a complex manifold M.

6. Poincaré Bundle

Now we restrict attention to the case of a plane cubic curve E and ask ourselves the following question. What does the set $\mathrm{Pic}^0(E)$ of all degree zero line bundles on E look like?

Here by degree of a line bundle we mean the degree of its associated divisor (Definition 4). In the case of $\mathbb{P}^1$ up to isomorphism there is only one line bundle of degree zero and that is the trivial bundle. However on E there are many non-trivial line bundles having degree zero as we shall soon see. In fact they form a family parametrised by E.

First let's take a point $P \in E$. This is a divisor of degree 1 on E, and it defines a line bundle $\mathcal{O}(P)$. Now choose another point Q distinct from P and take the divisor $P - Q$. This has degree zero and correspondingly defines a line bundle $\mathcal{O}(P - Q)$. One could ask is $\mathcal{O}(P - Q)$ isomorphic to the trivial bundle?

If so then by Lemma 17 there would exist some global meromorphic function f on E such that $P - Q = (f)$. This means that f has exactly a pole of order 1 at Q and a zero of order 1 at P and no other poles or zeroes. But then we can define a bijective map

$$\begin{array}{ccc} E & \longrightarrow & \mathbb{P}^1 \\ x & \longmapsto & (f(x):1) \end{array}$$

Under this mapping Q maps to the point at $\infty = (1:0)$ on $\mathbb{P}^1$. Since f is meromorphic with exactly one pole and holomorphic elsewhere it is an isomorphism. But E has genus 1 while $\mathbb{P}^1$ has genus 0 so they cannot be isomorphic. Therefore $P - Q \nsim 0$, i.e. P, Q are inequivalent divisors and define non isomorphic line bundles. The following theorem says that in fact the family of degree 0 line bundles on E is itself a manifold.

Theorem 20. *Let E be a cubic curve in $\mathbb{P}^2$. Then there is a bijection $E \cong \mathrm{Pic}^0(E)$.*

Proof. We just show that there is an injection from E to $\mathrm{Pic}^0(E)$. For a proof of surjectivity see [6] Chapter 6.

Fix a point in E (doesn't matter which one) for instance O. Then given any other point $P \in E$ we get a degree 0 line bundle $\mathcal{O}(P-O)$. This defines a map $E \to \mathrm{Pic}^0(E)$. For P and Q distinct points the line bundles $\mathcal{O}(P-O)$ and $\mathcal{O}(Q-O)$ are non isomorphic. Because if they were isomorphic then by Lemma 17 the divisor $P-O$ would be linearly equivalent to $Q-O$ which implies $P-Q \sim (f)$ for some meromorphic function f. But as we have already seen, in that case f defines an isomorphism between E and $\mathbb{P}^1$ which is a contradiction. Hence our map is bijective. □

In fact there is a more general theorem.

Theorem 21. *Let E be a cubic curve in $\mathbb{P}^2$. Then for all $n \in \mathbb{Z}$ we have $\mathrm{Pic}^n(E) \cong E$.*

The idea is that if we fix a point O on E then any line bundle L of degree n, can be mapped to a line bundle of degree zero by taking the tensor product $L \otimes \mathcal{O}(-nO)$ and vice versa.

There is a special line bundle on $E \times \mathrm{Pic}^0(E) \cong E \times E$ called the *Poincaré bundle* $\mathcal{P}$. It has the property that $\mathcal{P}_{|_{E\times\{P\}}} \cong \mathcal{O}_E(P-O)$. We construct this line bundle as follows. Let (x,y) be the local coordinates on $E \times E$. Consider the subset $\Delta = \{(x,y)|x=y\}$ called the *diagonal.* It is a divisor since it is given by the zero locus of a single equation. Its associated line bundle $\mathcal{O}(\Delta)$ has the property that $\mathcal{O}(\Delta)_{|_{E\times\{P\}}} \cong \mathcal{O}_E(P)$. The idea is simple, by Remark 15 $\mathcal{O}(\Delta)_{|_{E\times\{P\}}} = \mathcal{O}(\Delta_{|_{E\times\{P\}}})_{|_{E\times\{P\}}}$. Let p_1, p_2 denote projection of $E \times \mathrm{Pic}^0(E) \cong E \times E$ onto the first and second factor respectively. Consider the line bundle $\mathcal{P} := \mathcal{O}(\Delta) \otimes p_1^*\mathcal{O}(-O)$. Then $p_1^*\mathcal{O}(-O)$ is just the line bundle associated to the divisor $-(\{O\} \times E)$ in $E \times E$.

$$\begin{aligned}
\mathcal{P}_{|_{E\times\{p\}}} &= \mathcal{O}(\Delta) \otimes {p_1}^*\mathcal{O}(-O)_{|_{E\times\{P\}}} \\
&= \mathcal{O}(\Delta)_{|_{E\times\{P\}}} \otimes \mathcal{O}(-(O \times E))_{|_{E\times\{P\}}} \\
&\cong \mathcal{O}_E(P) \otimes \mathcal{O}_E(-O) = \mathcal{O}_E(P-O)
\end{aligned}$$

The point P in the second factor of $E \times E$ represents the line bundle $\mathcal{O}(P - O)$ when viewing $E \times E$ as $E \times \mathrm{Pic}^0(E)$ via the isomorphism

$$\begin{array}{ccc} E & \rightarrow & \mathrm{Pic}^0(E) \\ P & \mapsto & \mathcal{O}(P - O) \end{array}$$

So we see that $\mathcal{P}|_{E \times \{P\}}$ is isomorphic to the corresponding element $\mathcal{O}_E(P - O)$ in $\mathrm{Pic}^0(E)$. This is an example of a **moduli space** and its **universal bundle.** The *moduli space* of degree zero line bundles on E is isomorphic to E. The *universal line bundle* on $E \times \mathrm{Pic}^0(E)$ is given by $\mathcal{P}$ characterised by the property that for any $P \in \mathrm{Pic}^0(E)$, $\mathcal{P}|_{E \times \{P\}}$ is a line bundle of degree zero belonging to the isomorphism class of $P \in \mathrm{Pic}^0(E)$. For more details about moduli spaces of vector bundles on elliptic curves see the article by C. Daly[4].

7. Abel's Theorem; group law revisited

In Section 3 we showed that a cubic curve E is isomorphic to a complex torus $\mathbb{C}/\Lambda$. We now have all the pieces to put together a proof of the fact that the geometric group structure on E is the same as the group structure on $\mathbb{C}/\Lambda$.

The main result involved in proving this is the following classical theorem known as **Abel's theorem** [1] (1827).

Theorem 22. *Let Λ be a rank two lattice in $\mathbb{C}$, let $n_1, \dots, n_n$ and $m_1, \dots, m_m$ be integers and let $[a_1], \dots, [a_n]$ and $[b_1], \dots, [b_m]$ denote points in $\mathbb{C}/\Lambda$.*

Then there exists a meromorphic function $f : \mathbb{C}/\Lambda \to \mathbb{C}$ with zeroes at $[a_i]$ of order n_i and poles at $[b_j]$ of order m_j if and only if

$$\sum_{i=1}^{n} n_i = \sum_{j=1}^{m} m_j \quad \textit{and} \quad \sum_{i=1}^{n} n_i[a_i] = \sum_{j=1}^{m} m_j[b_j] \in \mathbb{C}/\Lambda.$$

Moreover this function is unique up to a constant factor.

For a proof of Abel's theorem involving a nice application of *theta-functions* see [5] Theorem 7.

Theorem 23. *Let E be a smooth cubic curve in $\mathbb{P}^2$. Then $E \cong \mathbb{C}/\Lambda$ for some rank 2 lattice Λ in $\mathbb{C}$. The geometric group structure on E as defined in Theorem 1 is isomorphic to the group structure on $\mathbb{C}/\Lambda$.*

Proof. Consider three points P_1, P_2, P_3 on E which lie on a line L. This is equivalent to saying $P_1 + P_2 + P_3 = O$. Let $[z_1], [z_2], [z_3]$ be the unique points on the complex torus $\mathbb{C}/\Lambda$ which are mapped to P_1, P_2, P_3 under the isomorphism τ, i.e. $\tau([z_i]) = P_i$ (see Section 3 for the definition of τ.) If we can show that $[z_1]+[z_2]+[z_3] = 0$ then we are done.

Suppose $L = \{(z_0 : z_1 : z_2) \in \mathbb{P}^2 \mid l_0z_0 + l_1z_1 + l_2z_2 = 0\}$. Then since z_2 is not identically zero on L the meromorphic function $F = \frac{l_0z_0+l_1z_1+l_2z_2}{z_2}$ on $\mathbb{P}^2$ restricts to a meromorphic function f on E. The divisor of F in $\mathbb{P}^2$ has a simple zero along the line L and a simple pole along the line $L_2 = \{(z_0 : z_1 : z_2) \mid z_2 = 0\}$. So the divisor of F restricted to E is $(f) = \sum P_i - \sum Q_j$ where $\{P_i\} = L \cap E$ and $\{Q_j\} = L_2 \cap E$ with multiplicities. Implicit differentiation shows that O is an inflection point of E and hence O is a triple point of contact of the line L_2 and E. So L_2 meets E at O with multiplicity 3. Therefore $(f) = P_1 + P_2 + P_3 - 3O$. Now f pulls back to a meromorphic function τ^*f on $\mathbb{C}/\Lambda$ with zeroes of order one each at $[z_1], [z_2], [z_3]$ and a pole of order three at $[0]$. By Abel's theorem this is the case *if and only if* $[z_1] + [z_2] + [z_3] = 3[0]$ in $\mathbb{C}/\Lambda$, i.e. if the points $[z_1], [z_2], [z_3]$ sum to zero in $\mathbb{C}/\Lambda$. □

This concludes our overview of the group structure on an elliptic curve E in $\mathbb{P}^2$. For other interesting features of elliptic curves and moduli spaces of vector bundles on elliptic curves see the article by C. Daly [4].

In two dimensions the only compact complex manifold that admits a group structure is a complex torus. However one can consider families of elliptic curves called *elliptic fibrations*. The geometry of these elliptic fibrations is very interesting and has been studied in detail. In the complex analytic case they have been classified by Kodaira (see [8]). Recently there has also been much interest in higher dimensional elliptically fibred manifolds in the context of mathematical physics.

References

[1] N. H. Abel *Recherches sur les fonctions elliptiques* J. reine angew. Math. 2, pages 101-181 (1827).

[2] J. B. Bost, *An introduction to compact Riemann surfaces, jacobians and Abelian varieties*, From number theory to Physics, M.Waldschmidt et.al (eds), Springer Verlag (1992).

[3] C. H. Clemens, *A scrap book of complex curve theory*, American Mathematical Society 2002 edition.

[4] C. Daly, *Rank two vector bundles on elliptic curves.* this issue

[5] M. Franz, *Theta functions.* this issue

[6] A. Gathmann, *Lecture Notes from "Algebraic geometry", taught at University of Kaiserslautern, 2002/2003.*

[7] P. Griffiths, J. Harris, *Principles of algebraic geometry*, John Wiley and Sons Inc 1994 edition.

[8] K. Kodaira, *On the structure of compact complex analytic surfaces I*, Am. J. math. 86 (1964) 751-798.

[9] B. Kreussler, *Solving cubic equations in two variables.* this issue

[10] M. Reid, *Undergraduate algebraic geometry*, London Mathematical Society Student texts 12, Cambridge university Press 2001.

[11] J. Silverman *The arithmetic of elliptic curves*, Springer Verlag 1986.

Department of Mathematics, Institute of Technology Tralee, Clash, Tralee, Co. Kerry, Ireland

E-mail address: Madeeha.Khalid@staff.ittralee.ie

THETA FUNCTIONS

MARINA FRANZ

Abstract. On our analytic way to the group structure of an elliptic function we meet so called theta functions. These complex functions are entire and quasi-periodic with respect to a lattice Λ. In the proof of Abel's theorem we use their properties to charcterise all meromorphic functions $f : \mathbb{C}/\Lambda \to \mathbb{C}$. Finally we have a closer look at a very special and interesting Λ-periodic meromorphic function, the Weierstraß $\wp$-function. This function delivers an analytic way to give a group structure to an algebraic variety.

1. Introduction

First of all, we want to analyse periodic complex functions $f : \mathbb{C} \to \mathbb{C}$ with respect to a lattice Λ. So let us fix once and for all a complex number $\tau \in \mathbb{C}$ with Im $\tau > 0$ and consider the lattice $\Lambda := \mathbb{Z} \oplus \tau\mathbb{Z} \subset \mathbb{C}$.

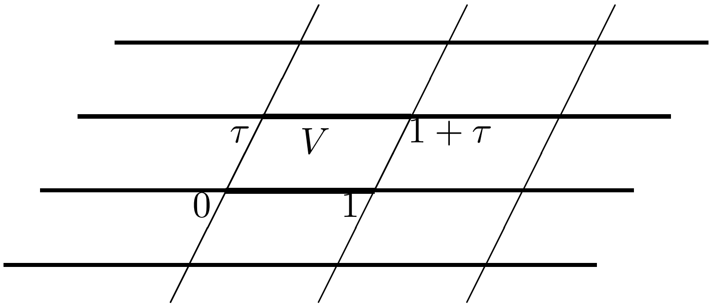


Figure 1. The lattice $\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$ and its fundamental parallelogram $V = \{z = t_1 + t_2\tau \in \mathbb{C} : 0 \leq t_1, t_2 < 1\}$.

Lemma 1. *An entire and doubly-periodic complex function is constant.*

To prove this lemma we need Liouville's Theorem, which we know from complex analysis. It states that each entire (i.e. holomorphic, i.e. complex differentiable, everywhere in $\mathbb{C}$) and bounded complex function $f : \mathbb{C} \to \mathbb{C}$ is constant.

Proof. The values of a doubly-periodic function are completely determined by the values on the closure of the fundamental parallelogram $\overline{V} = \{z \in \mathbb{C} : z = t_1 + t_2\tau \text{ for some } 0 \leq t_1, t_2 \leq 1\}$ which is a compact set. But a continuous function on a compact set is bounded. Hence our function is entire and bounded. Therefore it is constant by Liouville's Theorem. □

As we have seen, that *entire doubly-periodic* functions are not very intersting (as they are constant), in the following we will consider *entire quasi-periodic* functions and use them to prove Abel's Theorem which says what *meromorphic doubly-periodic* functions look like.

2. Theta Functions and Abel's Theorem

Definition. The *basic theta function* is defined to be the function $\theta : \mathbb{C} \to \mathbb{C}$ given by

$$\theta(z) := \theta(\tau)(z) := \sum_{n \in \mathbb{Z}} \exp(\pi i n^2 \tau) \exp(2\pi i n z)$$

Note. The function θ depends on τ. So for each $\tau \in \mathbb{C}$ with $\operatorname{Im} \tau > 0$ we get a (not necessarily different) basic theta function. Hence there is a whole family of basic theta functions $\{\theta(\tau)\}_{\tau \in \mathbb{C}, \operatorname{Im}\, \tau > 0}$. But here we assume τ to be fixed, so we have only one basic theta function.

Remark. As the series in the definition above is locally uniformly unordered convergent (without proof) our basic theta function is an entire function.

Lemma 2. *The basic theta function is quasi-periodic.*

Proof. Consider $\theta(z + \lambda)$ for $\lambda \in \Lambda$, i.e. $\lambda = p\tau + q$ for p, $q \in \mathbb{Z}$.

For $\lambda = 1$, i.e. for $p = 0$ and $q = 1$ we have

$$\begin{aligned}
\theta(z+1) &\overset{def}{=} \sum_{n\in\mathbb{Z}} \exp(\pi i n^2 \tau)\exp(2\pi i n(z+1)) \\
&= \sum_{n\in\mathbb{Z}} \exp(\pi i n^2\tau + 2\pi i n z + 2\pi i n) \\
&= \sum_{n\in\mathbb{Z}} \exp(\pi i n^2\tau)\exp(2\pi i n z) \underbrace{\exp(2\pi i n)}_{=1 \text{ for all } n\in\mathbb{Z}} \\
&= \sum_{n\in\mathbb{Z}} \exp(\pi i n^2\tau)\exp(2\pi i n z) \\
&\overset{def}{=} \theta(z)
\end{aligned}$$

Hence the basic theta function is periodic with respect to the x-direction.

For $\lambda = \tau$, i.e. for $p = 1$ and $q = 0$ we have

$$\begin{aligned}
\theta(z+\tau) &\overset{def}{=} \sum_{n\in\mathbb{Z}} \exp(\pi i n^2\tau)\exp(2\pi i n(z+\tau)) \\
&= \sum_{n\in\mathbb{Z}} \exp(\pi i n^2\tau + 2\pi i n z + 2\pi i n\tau)
\end{aligned}$$

if we complete the square and rearrange the summands then

$$\begin{aligned}
&= \sum_{n\in\mathbb{Z}} \exp\big(\pi i n^2\tau + 2\pi i n\tau + \pi i\tau - \pi i\tau \\
&\qquad +2\pi i n z + 2\pi i z - 2\pi i z) \\
&= \exp(-\pi i\tau - 2\pi i z)\sum_{n\in\mathbb{Z}} \exp(\pi i(n+1)^2\tau)\exp(2\pi i(n+1)z)
\end{aligned}$$

if we make a simple index shift $m = n + 1$ then

$$\begin{aligned}
&= \exp(-\pi i\tau - 2\pi i z)\sum_{m\in\mathbb{Z}} \exp(\pi i m^2\tau)\exp(2\pi i m z) \\
&\overset{def}{=} \exp(-\pi i\tau - 2\pi i z)\theta(z)
\end{aligned}$$

Hence the basic theta function is not periodic with respect to the τ-direction as in general $\exp(-\pi i\tau - 2\pi i z) \neq 1$.

In the general case we obtain

$$\begin{aligned}\theta(z+\lambda) &= \theta(z+p\tau+q)\\ &\overset{def}{=} \sum_{n\in\mathbb{Z}} \exp(\pi i n^2\tau)\exp(2\pi i n(z+p\tau+q))\\ &= \sum_{n\in\mathbb{Z}} \exp(\pi i n^2\tau + 2\pi i n z + 2\pi i n p\tau + 2\pi i n q)\end{aligned}$$

if we complete the square and rearrange the summands then

$$\begin{aligned}&= \sum_{n\in\mathbb{Z}} \exp\big(\pi i n^2\tau + 2\pi i n p\tau + \pi i p^2\tau - \pi i p^2\tau\\ &\qquad +2\pi i n z + 2\pi i p z - 2\pi i p z + 2\pi i n q)\\ &= \exp(-\pi i p^2\tau - 2\pi i p z)\\ &\qquad \cdot\sum_{n\in\mathbb{Z}} \big[\, \exp(\pi i(n+p)^2\tau)\exp(2\pi i(n+p)z)\\ &\qquad\qquad \underbrace{\exp(2\pi i n q)}_{=1 \text{ for all } n\in\mathbb{Z}} \;\big]\\ &= \exp(-\pi i p^2\tau - 2\pi i p z)\\ &\qquad \cdot\sum_{n\in\mathbb{Z}} \exp(\pi i(n+p)^2\tau)\exp(2\pi i(n+p)z)\end{aligned}$$

if we make a simple index shift $m = n + p$ then

$$\begin{aligned}&= \exp(-\pi i p^2\tau - 2\pi i p z)\sum_{m\in\mathbb{Z}} \exp(\pi i m^2\tau)\exp(2\pi i m z)\\ &\overset{def}{=} \exp(-\pi i p^2\tau - 2\pi i p z)\theta(z)\end{aligned}$$

Hence the basic theta function θ is quasi-periodic with

$$\begin{aligned}\theta(z+\lambda) &= \theta(z+p\tau+q)\\ &= \exp(-\pi i p^2\tau - 2\pi i p z)\theta(z)\end{aligned}$$

for all $\lambda = p\tau + q \in \Lambda$ and $z \in \mathbb{C}$. □

Definition. We define

$$e(\lambda, z) := \exp(-\pi i p^2\tau - 2\pi i p z)$$

and call this the *automorphy factor*.

Remark. We have $e(\lambda_1 + \lambda_2, z) = e(\lambda_1, z + \lambda_2)e(\lambda_2, z)$ for all λ_1, $\lambda_2 \in \Lambda$.

Let λ_1, $\lambda_2 \in \Lambda$, i.e. $\lambda_1 = p_1\tau + q_1$ and $\lambda_2 = p_2\tau + q_2$ for some p_1, p_2, q_1, $q_2 \in \mathbb{Z}$, and thus $\lambda_1 + \lambda_2 = (p_1 + p_2)\tau + (q_1 + q_2) \in \Lambda$. Then

$$\begin{aligned}
e(\lambda_1 + \lambda_2, z) &= e((p_1 + p_2)\tau + (q_1 + q_2), z) \\
&\overset{def}{=} \exp(-\pi i(p_1 + p_2)^2\tau - 2\pi i(p_1 + p_2)z)) \\
&= \exp(-\pi i p_1^2\tau - 2\pi i p_1 p_2\tau - \pi i p_2^2\tau - 2\pi i p_1 z - 2\pi i p_2 z) \\
&\overset{def}{=} \exp(-\pi i p_1^2\tau - 2\pi i p_1 p_2\tau - 2\pi i p_1 z)e(\lambda_2, z) \\
&= \exp(-\pi i p_1^2\tau - 2\pi i p_1 z - 2\pi i p_1 p_2\tau - \underbrace{2\pi i p_1 q_2}_{\exp(2\pi i p_1 q_2)=1}) \\
&\qquad \cdot e(\lambda_2, z) \\
&= \exp(-\pi i p_1^2\tau - 2\pi i p_1(z + \lambda_2))e(\lambda_2, z) \\
&\overset{def}{=} e(\lambda_1, z + \lambda_2)e(\lambda_2, z)
\end{aligned}$$

Summary. The basic theta function $\theta : \mathbb{C} \to \mathbb{C}$ is entire and quasi-periodic with automorphy factor e, i.e. we have

$$\theta(z + \lambda) = e(\lambda, z)\theta(z) = \exp(-\pi i p^2\tau - 2\pi i p z)\theta(z) \tag{1}$$

for all $\lambda = p\tau + q \in \Lambda$ and all $z \in \mathbb{C}$.

Now we want to enlarge our cathegory of theta functions. So far we have only one (basic) theta function corresponding to the point $0 \in \mathbb{C}$ (and each point $q \in \mathbb{Z} \subset \mathbb{C}$). Now, for our fixed τ, we will define a new theta function for each point in $\mathbb{C}$. Therefore let's start with our old theta function and translate z by a fixed ξ, i.e. consider $\theta(z + \xi)$ for $\xi = a\tau + b$ for some fixed a, $b \in \mathbb{R}$:

$$\begin{aligned}
\theta(z + \xi) &= \theta(z + a\tau + b) \\
&\overset{def}{=} \sum_{n\in\mathbb{Z}} \exp(\pi i n^2\tau) \exp(2\pi i n(z + a\tau + b)) \\
&= \sum_{n\in\mathbb{Z}} \exp(\pi i n^2\tau + 2\pi i n z + 2\pi i n a\tau + 2\pi i n b)
\end{aligned}$$

If we complete the square and rearrange the summands then we obtain

$$\begin{aligned}\theta(z+\xi) &= \sum_{n\in\mathbb{Z}} \exp\big(\pi i n^2\tau + 2\pi i n a\tau + \pi i a^2\tau - \pi i a^2\tau \\ &\qquad\qquad +2\pi i n(z+b) + 2\pi i a(z+b) - 2\pi i a(z+b)) \\ &= \exp(-\pi i a^2\tau - 2\pi i a(z+b)) \\ &\qquad \cdot \sum_{n\in\mathbb{Z}} \exp(\pi i(n+a)^2\tau)\exp(2\pi i(n+a)(z+b))\end{aligned}$$

Note that the sum $\sum_{n\in\mathbb{Z}} \exp(\pi i(n+a)^2\tau)\exp(2\pi i(n+a)(z+b))$ looks very similar to the sum in the definition of our basic theta function above.

Definition. For $\xi = a\tau+b$ and $a, b \in \mathbb{R}$ the $modified\, theta function$ is defined to be the function $\theta_\xi : \mathbb{C} \to \mathbb{C}$ given by

$$\theta_\xi(z) := \theta_\xi(\tau)(z) := \sum_{n\in\mathbb{Z}} \exp(\pi i(n+a)^2\tau)\exp(2\pi i(n+a)(z+b))$$

and ξ is called *theta characteristic.*

Note. From the calculation above we obtain a relation between the basic theta function and the modified theta function with characteristic $\xi = a\tau + b$ for some fixed $a, b \in \mathbb{R}$:

$$\begin{aligned}\theta_\xi(z) &= \sum_{n\in\mathbb{Z}} \exp(\pi i(n+a)^2\tau)\exp(2\pi i(n+a)(z+b)) && (2)\\ &= \exp(\pi i a^2\tau + 2\pi i a(z+b))\theta(z+\xi) && (3)\end{aligned}$$

for all $z \in \mathbb{C}$.

Remark. As the series in the definition is locally uniformly unordered convergent (without proof) the modified theta functions are entire functions.

Lemma 3. *Modified theta functions are quasi-periodic functions.*

Proof. Let a, $b \in \mathbb{R}$ such that $\xi = a\tau + b$ is the characteristic of the modified theta function θ_ξ. Consider $\theta_\xi(z+\lambda)$ for $\lambda = p\tau + q \in \Lambda$.

$$\begin{aligned}\theta_\xi(z+\lambda) &\overset{(3)}{=} \exp(\pi i a^2\tau + 2\pi i a(z+\lambda+b))\theta(z+\lambda+\xi)\\ &\overset{(1)}{=} \exp(\pi i a^2\tau + 2\pi i a(z+\lambda+b))e(\lambda, z+\xi)\theta(z+\xi)\\ &\overset{(3)}{=} \exp(\pi i a^2\tau + 2\pi i a(z+\lambda+b))e(\lambda, z+\xi)\\ &\qquad\quad \cdot \exp(-\pi i a^2\tau - 2\pi i a(z+b))\theta_\xi(z)\\ &= \exp(2\pi i a\lambda)\exp(-\pi i p^2\tau - 2\pi i p(z+\xi))\theta_\xi(z)\\ &= \exp(2\pi i a\lambda - \pi i p^2\tau - 2\pi i p(z+\xi))\theta_\xi(z)\end{aligned}$$

Hence the modified theta function θ_ξ is quasi-periodic with

$$\begin{aligned}\theta_\xi(z+\lambda) &= \theta_{a\tau+b}(z+p\tau+q)\\ &= \exp(2\pi i a\lambda - \pi i p^2\tau - 2\pi i p(z+\xi))\theta_\xi(z)\end{aligned}$$

for all $\lambda = p\tau + q \in \Lambda$ and $z \in \mathbb{C}$. □

Definition. Let a, $b \in \mathbb{R}$ be fixed and let $\xi = a\tau + b$. We define

$$e_\xi(\lambda, z) := \exp(2\pi i a\lambda - \pi i p^2\tau - 2\pi i p(z+\xi))$$

and call this the *automorphy factor*.

Remark. Let a, $b \in \mathbb{R}$ be fixed and let $\xi = a\tau + b$. We have $e_\xi(\lambda_1+\lambda_2, z) = e_\xi(\lambda_1, z+\lambda_2)e_\xi(\lambda_2, z)$ for all λ_1, $\lambda_2 \in \Lambda$.

Let λ_1, $\lambda_2 \in \Lambda$, i.e. $\lambda_1 = p_1\tau + q_1$ and $\lambda_2 = p_2\tau + q_2$ for some p_1, p_2, q_1, $q_2 \in \mathbb{Z}$, and $\lambda_1 + \lambda_2 = (p_1+p_2)\tau + (q_1+q_2) \in \Lambda$.

$$\begin{aligned}
e_\xi(\lambda_1+\lambda_2,z) &= e_\xi((p_1+p_2)\tau+(q_1+q_2),z)\\
&\overset{def}{=} \exp\big(2\pi i a(\lambda_1+\lambda_2)-\pi i(p_1+p_2)^2\tau\\
&\qquad -2\pi i(p_1+p_2)(z+\xi)\big)\\
&= \exp\big(2\pi i a\lambda_1+2\pi i a\lambda_2-\pi i p_1^2\tau-2\pi i p_1p_2\tau-\pi i p_2^2\tau\\
&\qquad -2\pi i p_1(z+\xi)-2\pi i p_2(z+\xi)\big)\\
&\overset{def}{=} \exp(2\pi i a\lambda_1-\pi i p_1^2\tau-2\pi i p_1p_2\tau-2\pi i p_1(z+\xi))\\
&\qquad e_\xi(\lambda_2,z)\\
&= \exp\big(2\pi i a\lambda_1-\pi i p_1^2\tau-2\pi i p_1p_2\tau- \underbrace{2\pi i p_1q_2}_{\exp(2\pi i p_1q_2)=1}\\
&\qquad -2\pi i p_1(z+\xi)\big)\, e_\xi(\lambda_2,z)\\
&= \exp(2\pi i a\lambda_1-\pi i p_1^2\tau-2\pi i p_1(z+\lambda_2+\xi))e_\xi(\lambda_2,z)\\
&\overset{def}{=} e_\xi(\lambda_1,z+\lambda_2)e_\xi(\lambda_2,z)
\end{aligned}$$

Summary. Let $\xi = a\tau + b$ with a, $b \in \mathbb{R}$ fixed. The modified theta function with characteristic ξ is entire and quasi-periodic with automorphy factor e_ξ, i.e. we have

$$\begin{aligned}
\theta_\xi(z+\lambda) &= e_\xi(\lambda,z)\theta_\xi(z) && (4)\\
&= \exp(2\pi i a\lambda-\pi i p^2\tau-2\pi i p(z+\xi))\theta_\xi(z) && (5)
\end{aligned}$$

for all $\lambda = p\tau + q \in \Lambda$ and all $z \in \mathbb{C}$.

Now we want to determine all zeros of all theta functions. Therefore we consider a special modified theta function, the theta function with characteristic $\sigma := \frac{1}{2}\tau + \frac{1}{2}$. In this case the determination of zeros is very simple because the zeros are easy to describe.

Lemma 4. *θ_σ is an odd function, i.e. $\theta_\sigma(-z) = -\theta_\sigma(z)$ for all $z \in \mathbb{C}$.*

In particular we have $\theta_\sigma(0) = 0$.

Proof.

$$\begin{aligned}
\theta_\sigma(-z) &= \theta_{\frac{1}{2}\tau+\frac{1}{2}}(-z) \\
&\overset{def}{=} \sum_{n\in\mathbb{Z}} \Bigg[\exp\left(\pi i \left(n+\frac{1}{2}\right)^2 \tau\right) \\
&\qquad \exp\left(2\pi i \left(n+\frac{1}{2}\right)\left(-z+\frac{1}{2}\right)\right)\Bigg]
\end{aligned}$$

if we make a simple index shift $m = -n-1$ then

$$\begin{aligned}
&= \sum_{m\in\mathbb{Z}} \Bigg[\exp\left(\pi i \left(-m-\frac{1}{2}\right)^2 \tau\right) \\
&\qquad \exp\left(2\pi i \left(-m-\frac{1}{2}\right)\left(-z+\frac{1}{2}\right)\right)\Bigg] \\
&= \sum_{m\in\mathbb{Z}} \Bigg[\exp\left(\pi i \left(m+\frac{1}{2}\right)^2 \tau\right) \\
&\qquad \exp\left(2\pi i \left(m+\frac{1}{2}\right)\left(z+\frac{1}{2}\right) - 2\pi i\left(m+\frac{1}{2}\right)\right)\Bigg] \\
&= \sum_{m\in\mathbb{Z}} \Bigg[\exp\left(\pi i \left(m+\frac{1}{2}\right)^2 \tau\right) \\
&\qquad \exp\left(2\pi i \left(m+\frac{1}{2}\right)\left(z+\frac{1}{2}\right)\right) \\
&\qquad \underbrace{\exp(-2\pi i m)\exp(-\pi i)}_{=-1 \text{ for all } m\in\mathbb{Z}}\ \Bigg] \\
&\overset{def}{=} -\theta_\sigma(z)
\end{aligned}$$

□

From complex analysis we know a simple way to count zeros and poles of a meromorphic function $f : \mathbb{C} \to \mathbb{C}$:

$$\frac{1}{2\pi i}\int_\gamma \frac{f'}{f}(z)\,dz = \text{total number of zeros - total number of poles}$$

where γ is a piecewise smooth path that runs around each zero and each pole exactly one time. We will use this integral to determine all zeros of the theta functions θ_σ with $\sigma = \frac{1}{2}\tau + \frac{1}{2}$.

Lemma 5. *We have $\theta_\sigma(z) = 0$ precisely for all $z \in \Lambda$ and all zeros are simple zeros.*

Proof. Consider the fundamental parallelogram $V := \{z \in \mathbb{C} : z = t_1\tau + t_2 \text{ for some } 0 \leq t_1, t_2 < 1\}$.

Choose $w \in \mathbb{C}$ such that the border of $V_w := w + V$ contains no zeros of θ_σ and $0 \in V_w$.

Further consider the following paths along the border of V_w:

$$\begin{aligned}
\alpha &: [0,1] \to \mathbb{C}; t \mapsto w + t \\
\beta &: [0,1] \to \mathbb{C}; t \mapsto w + 1 + t\tau \\
\gamma &: [0,1] \to \mathbb{C}; t \mapsto w + (1-t) + \tau \\
\delta &: [0,1] \to \mathbb{C}; t \mapsto w + (1-t)\tau
\end{aligned}$$

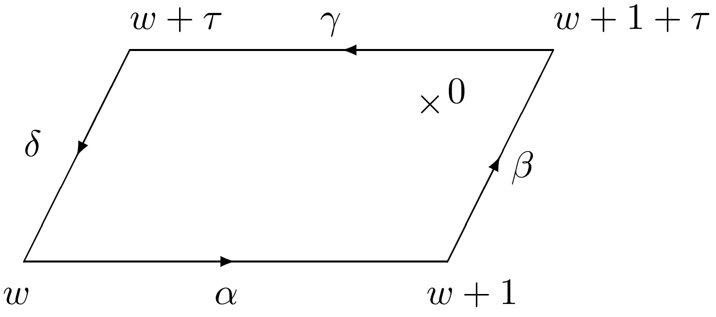


FIGURE 2. $w \in \mathbb{C}$ is chosen such that the border of the parallelogram $V_w = w + V$ contains no zeros of f and such that $0 \in V_w$. The paths α, β, γ and δ run along the border of V_w.

Note

$$\gamma(t) = w + (1-t) + \tau = \alpha(1-t) + \tau$$

and

$$\delta(t) = w + (1-t)\tau = \beta(1-t) - 1$$

We want to show that $\displaystyle\frac{1}{2\pi i}\int_{\partial V_w} \frac{\theta_\sigma'}{\theta_\sigma}(z)\,dz = 1.$

Therefore we will show

$$\frac{1}{2\pi i}\int_\gamma \frac{\theta'_\sigma}{\theta_\sigma}(z)\ dz = 1 - \frac{1}{2\pi i}\int_\alpha \frac{\theta'_\sigma}{\theta_\sigma}(z)\ dz$$

and

$$\frac{1}{2\pi i}\int_\delta \frac{\theta'_\sigma}{\theta_\sigma}(z)\ dz = -\frac{1}{2\pi i}\int_\beta \frac{\theta'_\sigma}{\theta_\sigma}(z)\ dz$$

$$\begin{aligned}
\frac{1}{2\pi i}\int_\gamma \frac{\theta'_\sigma}{\theta_\sigma}(z)\ dz &= \frac{1}{2\pi i}\int_0^1 \frac{\theta'_\sigma}{\theta_\sigma}(\gamma(t))\gamma'(t)\ dt \\
&= \frac{1}{2\pi i}\int_0^1 \frac{\theta'_\sigma}{\theta_\sigma}(\alpha(1-t)+\tau)(-1)\ dt \\
&= -\frac{1}{2\pi i}\int_\alpha \frac{\theta'_\sigma}{\theta_\sigma}(z+\tau)\ dz \\
&= -\frac{1}{2\pi i}\int_\alpha \frac{e'_\sigma(\tau,z)\theta_\sigma(z)+e_\sigma(\tau,z)\theta'_\sigma(z)}{e_\sigma(\tau,z)\theta_\sigma(z)}\ dz \\
&= -\frac{1}{2\pi i}\int_\alpha \frac{e'_\sigma(\tau,z)}{e_\sigma(\tau,z)}\ dz - \frac{1}{2\pi i}\int_\alpha \frac{\theta'_\sigma}{\theta_\sigma}(z)\ dz
\end{aligned}$$

when we use

$$e_\sigma(\tau,z) = \exp(2\pi i\frac{1}{2}\tau - \pi i\tau - 2\pi i(z+\sigma))$$

then

$$\begin{aligned}
&= -\frac{1}{2\pi i}\int_\alpha \frac{\exp'(-2\pi i(z+\sigma))}{\exp(-2\pi i(z+\sigma))}\ dz \\
&\qquad - \frac{1}{2\pi i}\int_\alpha \frac{\theta'_\sigma}{\theta_\sigma}(z)\ dz \\
&= -\frac{1}{2\pi i}\int_\alpha -2\pi i\ dz - \frac{1}{2\pi i}\int_\alpha \frac{\theta'_\sigma}{\theta_\sigma}(z)\ dz \\
&= 1 - \frac{1}{2\pi i}\int_\alpha \frac{\theta'_\sigma}{\theta_\sigma}(z)\ dz
\end{aligned}$$

$$\begin{aligned}\frac{1}{2\pi i}\int_\delta \frac{\theta'_\sigma}{\theta_\sigma}(z)\,dz &= \frac{1}{2\pi i}\int_0^1 \frac{\theta'_\sigma}{\theta_\sigma}(\delta(t))\delta'(t)\,dt\\ &= \frac{1}{2\pi i}\int_0^1 \frac{\theta'_\sigma}{\theta_\sigma}(\beta(1-t)-1)(-\tau)\,dt\\ &= -\frac{1}{2\pi i}\int_\beta \frac{\theta'_\sigma}{\theta_\sigma}(z-1)\,dz\\ &= -\frac{1}{2\pi i}\int_\beta \frac{e'_\sigma(-1,z)\theta_\sigma(z)+e_\sigma(-1,z)\theta'_\sigma(z)}{e_\sigma(-1,z)\theta_\sigma(z)}\,dz\\ &= -\frac{1}{2\pi i}\int_\beta \frac{e'_\sigma(-1,z)}{e_\sigma(-1,z)}\,dz - \frac{1}{2\pi i}\int_\beta \frac{\theta'_\sigma(z)}{\theta_\sigma(z)}\,dz\end{aligned}$$

when we use

$$e_\sigma(-1,z) = \exp(-2\pi i\frac{1}{2})$$

then

$$\begin{aligned}&= -\frac{1}{2\pi i}\int_\beta \frac{\exp'(-\pi i)}{\exp(-\pi i)}\,dz - \frac{1}{2\pi i}\int_\beta \frac{\theta'_\sigma(z)}{\theta_\sigma(z)}\,dz\\ &= -\frac{1}{2\pi i}\int_\beta \frac{\theta'_\sigma(z)}{\theta_\sigma(z)}\,dz\end{aligned}$$

Then we have

$$\begin{aligned}\frac{1}{2\pi i}\int_{\partial V_w} \frac{\theta'_\sigma}{\theta_\sigma}(z)\,dz &= \frac{1}{2\pi i}\int_\alpha \frac{\theta'_\sigma}{\theta_\sigma}(z)\,dz + \frac{1}{2\pi i}\int_\beta \frac{\theta'_\sigma}{\theta_\sigma}(z)\,dz\\ &\qquad + \frac{1}{2\pi i}\int_\gamma \frac{\theta'_\sigma}{\theta_\sigma}(z)\,dz + \frac{1}{2\pi i}\int_\delta \frac{\theta'_\sigma}{\theta_\sigma}(z)\,dz\\ &= 1\end{aligned}$$

As θ_σ is holomorphic in $\overline{V_w}$, i.e. it doesn't have any poles, we know that θ_σ has a single zero. And by Lemma 4 this zero is in 0.
Now consider $\overline{V}_w + \lambda = \overline{V}_{w+\lambda}$ for some $\lambda \in \Lambda$. As $\theta_\sigma(z+\lambda) = e_\sigma(\lambda,z)\theta_\sigma(z)$ we obtain that θ_σ has the only zero $0+\lambda=\lambda$ in $\overline{V}_{w+\lambda}$ and this is a simple zero. But $\mathbb{C} = \cup_{\lambda\in\Lambda}\overline{V}_{w+\lambda}$. Hence θ_σ has zeros exactly in Λ and all zeros are simple. □

Corollary 6. *Let $\xi = a\tau + b$ with a, $b \in \mathbb{R}$. We have $\theta_\xi(z) = 0$ precisely for all $z \in \sigma - \xi + \Lambda$ and all its zeros are simple.*

Proof. We know $\theta_\sigma(z) = 0$ if and only if $z \in \Lambda$ and all the zeros are simple. Hence

$$\begin{aligned}
\theta_\xi(z) = 0 &\overset{(3)}{\Leftrightarrow} \exp(\pi i a^2\tau + 2\pi i a(z+b))\theta(z+\xi) = 0 \\
&\overset{(3)}{\Leftrightarrow} \exp\big(\pi i a^2\tau + 2\pi i a(z+b)\big) \\
&\qquad \cdot \exp\left(-\pi i \left(\frac{1}{2}\right)^2 \tau\right. \\
&\qquad\qquad \left. -2\pi i \frac{1}{2}\left(z+\xi-\frac{1}{2}\tau-\frac{1}{2}+\frac{1}{2}\right)\right) \\
&\qquad \cdot \theta_\sigma(z+\xi-\sigma) = 0 \\
&\Leftrightarrow z+\xi-\sigma \in \Lambda \\
&\Leftrightarrow z \in \sigma-\xi+\Lambda
\end{aligned}$$

In particular we have $\theta(z) = 0$ if and only if $z \in \sigma + \Lambda$. □

So far we have considered entire quasi-periodic functions. Now we want to use our knowledge about them to see what meromorphic doubly-periodic functions with given zeros a_i and poles b_j of given order n_i resp. m_j and number n resp. m look like. Futhermore we will decide whether such a function exists or not and whether it is unique or not.

Abel's Theorem 7. *There is a meromorphic function on $\mathbb{C}/\Lambda$ with zeros $[a_i]$ of order n_i for $1 \le i \le n$ and poles $[b_j]$ of order m_j for $1 \le j \le m$ if and only if $\sum_{i=1}^n n_i = \sum_{j=1}^m m_j$ and $\sum_{i=1}^n n_i[a_i] = \sum_{j=1}^m m_j[b_j]$.*

Moreover, such a function is unique up to a constant factor.

Proof. "⇒" Let $f : \mathbb{C}/\Lambda \to \mathbb{C}$ be a meromorphic function with zeros $[a_i]$ of order n_i and poles $[b_j]$ of order m_j. Choose $w \in \mathbb{C}$ such that $V_w = \{w + z \in \mathbb{C} : z = t_1\tau + t_2 \text{ for some } 0 \le t_1, t_2 < 1\}$ contains a representative a_i resp. b_j for every zero resp. pole of f. Further consider the paths

$$\begin{aligned}
\alpha &: [0,1] \to \mathbb{C}; t \mapsto w + t \\
\beta &: [0,1] \to \mathbb{C}; t \mapsto w + 1 + t\tau \\
\gamma &: [0,1] \to \mathbb{C}; t \mapsto w + (1-t) + \tau \\
\delta &: [0,1] \to \mathbb{C}; t \mapsto w + (1-t)\tau
\end{aligned}$$

along the border of V_w and the paths

$$\alpha_i : [0,1] \to \mathbb{C}; t \mapsto a_i + r_i e^{2\pi i t}$$
$$\beta_j : [0,1] \to \mathbb{C}; t \mapsto b_j + s_j e^{2\pi i t}$$

around the zeros resp. poles of f where r_i resp. s_j is chosen small enough that $D_i = \{z \in \mathbb{C} : |z - a_i| < r_i\}$ resp. $D'_j = \{z \in \mathbb{C} : |z - b_j| < s_j\}$ contains no other zeros or poles of f.

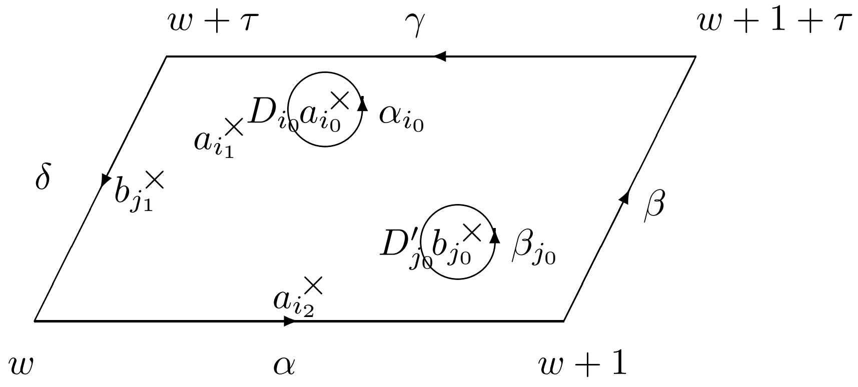


FIGURE 3. $w \in \mathbb{C}$ is chosen such that the parallelogram $V_w = w + V$ contains a representative a_i resp. b_j for every zero resp. pole of f. The paths α, β, γ and δ run along the border of V_w, the paths α_{i_0} around the zero a_{i_0} of f and the path β_{j_0} around the pole b_{j_0} of f.

First we show that $\sum_{i=1}^n n_i a_i - \sum_{j=1}^m m_j b_j \in \Lambda$ as follows:

$$\sum_{i=1}^n n_i a_i - \sum_{j=1}^m m_j b_j = \sum_{i=1}^n \frac{1}{2\pi i} \int_{\alpha_i} z \frac{f'}{f}(z)\, dz + \sum_{j=1}^m \frac{1}{2\pi i} \int_{\beta_j} z \frac{f'}{f}(z)\, dz$$
$$= \frac{1}{2\pi i} \int_{\partial V_w} z \frac{f'}{f}(z)\, dz \in \Lambda$$

To establish the first equality note that we can write

$$f(z) = c_i (z - a_i)^{n_i} h_i(z)$$

for a constant c_i and with $h_i(a_i) = 1$ around a_i and hence

$$f'(z) = c_i n_i (z - a_i)^{n_i - 1} \overline{h}_i(z)$$

with $\overline{h}_i(a_i) = 1$. We obtain

$$z\frac{f'}{f}(z) = z\frac{n_i}{z - a_i}\frac{\overline{h}_i}{h_i}(z)$$

with $\frac{\overline{h}_i}{h_i}(a_i) = 1$. Hence we have

$$\frac{1}{2\pi i}\int_{\alpha_i} z\frac{f'}{f}(z)\,dz = n_i a_i$$

by Cauchy's integral formula for discs. The same holds for the poles of f.

The second equality is clear since V_w contains a representative for every zero and pole of f in $\mathbb{C}/\Lambda$.

To see, that $\frac{1}{2\pi i}\int_{\partial V_w} z\frac{f'}{f}(z)\,dz$ is an element of Λ, note that

$$\begin{aligned}\frac{1}{2\pi i}\int_{\gamma} z\frac{f'}{f}(z)\,dz &= \frac{1}{2\pi i}\int_0^1 \gamma(t)\frac{f'}{f}(\gamma(t))\gamma'(t)\,dt\\ &= \frac{1}{2\pi i}\int_0^1 (\alpha(1-t)+\tau)\frac{f'}{f}((\alpha(1-t)+\tau))(-1)\,dt\\ &= -\frac{1}{2\pi i}\int_0^1 \alpha(1-t)\frac{f'}{f}(\alpha(1-t))\,dt\\ &\qquad - \frac{1}{2\pi i}\int_0^1 \tau\frac{f'}{f}(\alpha(1-t))\,dt\\ &= -\frac{1}{2\pi i}\int_{\alpha} z\frac{f'}{f}(z)\,dz - \tau\frac{1}{2\pi i}\int_{\alpha}\frac{f'}{f}(z)\,dz\end{aligned}$$

and

$$\begin{aligned}\frac{1}{2\pi i}\int_{\delta} z\frac{f'}{f}(z)\,dz &= \frac{1}{2\pi i}\int_0^1 \delta(t)\frac{f'}{f}(\delta(t))\delta'(t)\,dt\\ &= \frac{1}{2\pi i}\int_0^1 (\beta(1-t)-1)\frac{f'}{f}((\beta(1-t)-1))(-\tau)\,dt\\ &= -\frac{1}{2\pi i}\int_0^1 \beta(1-t)\frac{f'}{f}(\beta(1-t))\tau\,dt\\ &\qquad + \frac{1}{2\pi i}\int_0^1 \frac{f'}{f}(\beta(1-t))\tau\,dt\\ &= -\frac{1}{2\pi i}\int_{\beta} z\frac{f'}{f}(z)\,dz + \frac{1}{2\pi i}\int_{\beta}\frac{f'}{f}(z)\,dz\end{aligned}$$

hence

$$\begin{aligned}\frac{1}{2\pi i}\int_{\partial V_w} z\frac{f'}{f}(z)\,dz &= \frac{1}{2\pi i}\int_{\alpha} z\frac{f'}{f}(z)\,dz + \frac{1}{2\pi i}\int_{\beta} z\frac{f'}{f}(z)\,dz \\ &\quad + \frac{1}{2\pi i}\int_{\gamma} z\frac{f'}{f}(z)\,dz + \frac{1}{2\pi i}\int_{\delta} z\frac{f'}{f}(z)\,dz \\ &= -\tau\frac{1}{2\pi i}\int_{\alpha} \frac{f'}{f}(z)\,dz + \frac{1}{2\pi i}\int_{\beta} \frac{f'}{f}(z)\,dz \in \Lambda\end{aligned}$$

since $\frac{1}{2\pi i}\int_\beta \frac{f'}{f}(z)\,dz$, $\frac{1}{2\pi i}\int_\alpha \frac{f'}{f}(z)\,dz \in \mathbb{Z}$.

Secondly we show that

$$\begin{aligned}\sum_{i=1}^{n} n_i - \sum_{j=1}^{m} m_j &= \frac{1}{2\pi i}\int_{\partial V_w} \frac{f'}{f}(z)\,dz \\ &= 0\end{aligned}$$

Again the first equality is clear, since V_w contains a representative for every zero and pole of f in $\mathbb{C}/\Lambda$.

The second equality follows from:

$$\begin{aligned}\frac{1}{2\pi i}\int_{\gamma} \frac{f'}{f}(z)\,dz &= \frac{1}{2\pi i}\int_0^1 \frac{f'}{f}(\gamma(t))\gamma'(t)\,dt \\ &= \frac{1}{2\pi i}\int_0^1 \frac{f'}{f}(\alpha(1-t)+\tau)(-1)\,dt \\ &= -\frac{1}{2\pi i}\int_0^1 \frac{f'}{f}(\alpha(1-t))\,dt \\ &= -\frac{1}{2\pi i}\int_{\alpha} \frac{f'}{f}(z)\,dz\end{aligned}$$

and

$$\begin{aligned}\frac{1}{2\pi i}\int_{\delta} \frac{f'}{f}(z)\,dz &= \frac{1}{2\pi i}\int_0^1 \frac{f'}{f}(\delta(t))\delta'(t)\,dt \\ &= \frac{1}{2\pi i}\int_0^1 \frac{f'}{f}(\beta(1-t)-1)(-\tau)\,dt \\ &= -\frac{1}{2\pi i}\int_0^1 \frac{f'}{f}(\beta(1-t))\tau\,dt \\ &= -\frac{1}{2\pi i}\int_{\beta} \frac{f'}{f}(z)\,dz\end{aligned}$$

hence

$$\begin{aligned}\frac{1}{2\pi i}\int_{\partial V_w}\frac{f'}{f}(z)\,dz &= \frac{1}{2\pi i}\int_{\alpha}\frac{f'}{f}(z)\,dz + \frac{1}{2\pi i}\int_{\beta}\frac{f'}{f}(z)\,dz \\ &\qquad + \frac{1}{2\pi i}\int_{\gamma}\frac{f'}{f}(z)\,dz + \frac{1}{2\pi i}\int_{\delta}\frac{f'}{f}(z)\,dz \\ &= 0\end{aligned}$$

"$\Leftarrow$" Now let $[a_i]$, $[b_j] \in \mathbb{C}/\Lambda$ and n_i, $m_j \in \mathbb{N}$ for $1 \leq i \leq n$ and $1 \leq j \leq m$ be such that $\sum_{i=n}^{n} n_i = \sum_{j=m}^{m} m_j$ and $\sum_{i=1}^{n} n_i[a_i] = \sum_{j=1}^{m} m_j[b_j]$. We will contruct a meromorphic function $f : \mathbb{C}/\Lambda \to \mathbb{C}$ with zeros $[a_i]$ of order n_i and poles $[b_j]$ of order m_j. We choose representatives a_i, $b_j \in \mathbb{C}$ for $[a_i]$ resp. $[b_j]$ such that $\sum_{i=1}^{n} n_i a_i = \sum_{j=1}^{m} m_j b_j$ and define the function

$$g : \mathbb{C} \to \mathbb{C}; z \mapsto \frac{\prod_{i=1}^{n} \theta_\sigma(z-a_i)^{n_i}}{\prod_{j=1}^{m} \theta_\sigma(z-b_j)^{m_j}}$$

where θ_σ is the theta function with characteristic $\frac{1}{2}\tau + \frac{1}{2}$. Obviously g is a meromorphic function with zeros in $a_i + \Lambda$ of order n_i and poles in $b_j + \Lambda$ of order m_j. We have to show that g is doubly-periodic w.r.t. Λ. Therefore we have to show that $g(z+\lambda) = g(z)$ for all $\lambda \in \Lambda$. It suffices to show that $g(z+1) = g(z)$ and $g(z+\tau) = g(z)$.

$$g(z+1) = \frac{\prod_{i=1}^{n} \theta_\sigma(z+1-a_i)^{n_i}}{\prod_{j=1}^{m} \theta_\sigma(z+1-b_j)^{m_j}} = \frac{\prod_{i=1}^{n} \theta_\sigma(z-a_i)^{n_i}}{\prod_{j=1}^{m} \theta_\sigma(z-b_j)^{m_j}} = g(z)$$

and

$$\begin{aligned}g(z+\tau) &= \frac{\prod_{i=1}^{n} \theta_\sigma(z+\tau-a_i)^{n_i}}{\prod_{j=1}^{m} \theta_\sigma(z+\tau-b_j)^{m_j}} \\ &= \frac{\prod_{i=1}^{n} (e_\sigma(\tau, z-a_i)\theta_\sigma(z-a_i))^{n_i}}{\prod_{j=1}^{m} (e_\sigma(\tau, z-b_j)\theta_\sigma(z-b_j))^{m_j}} \\ &= \frac{\prod_{i=1}^{n} e_\sigma(\tau, z-a_i)^{n_i}}{\prod_{j=1}^{m} e_\sigma(\tau, z-b_j)^{m_j}} \frac{\prod_{i=1}^{n} \theta_\sigma(z-a_i)^{n_i}}{\prod_{j=1}^{m} \theta_\sigma(z-b_j)^{m_j}} \\ &= \frac{\prod_{i=1}^{n} e_\sigma(\tau, z-a_i)^{n_i}}{\prod_{j=1}^{m} e_\sigma(\tau, z-b_j)^{m_j}} \cdot g(z)\end{aligned}$$

but

$$\begin{aligned}\frac{\prod_{i=1}^n e_\sigma(\tau, z-a_i)^{n_i}}{\prod_{j=1}^m e_\sigma(\tau, z-b_j)^{m_j}} &= \frac{\prod_{i=1}^n \exp(-2\pi i(z-a_i+\sigma))^{n_i}}{\prod_{j=1}^m \exp(-2\pi i(z-b_j+\sigma))^{m_j}} \\ &= \frac{\prod_{i=1}^n \exp(-2\pi i(z+\sigma))^{n_i}}{\prod_{j=1}^m \exp(-2\pi i(z+\sigma))^{m_j}} \\ &\qquad \cdot \frac{\prod_{i=1}^n \exp(2\pi i a_i)^{n_i}}{\prod_{j=1}^m \exp(2\pi i b_j)^{m_j}} \\ &= \frac{\exp(-2\pi i(z+\sigma))^{\sum_{i=1}^n n_i}}{\exp(-2\pi i(z+\sigma))^{\sum_{j=1}^m m_j}} \\ &\qquad \cdot \frac{\exp(2\pi i \sum_{i=1}^n n_i a_i)}{\exp(2\pi i \sum_{j=1}^m m_j b_j)} \\ &= 1\end{aligned}$$

So $g(z+\tau) = g(z)$ as well. Hence g is doubly periodic w.r.t. Λ and the function $f : \mathbb{C}/\Lambda \to \mathbb{C}$ with $f([z]) = g(z)$ is well-defined and a solution.

Now suppose we are given two meromorphic functions f, g : $\mathbb{C}/\Lambda \to \mathbb{C}$ with zeros $[a_i]$ of order n_i and poles $[b_j]$ of order m_j. Then $\frac{f}{g}$ has no zeros or poles. Hence it is constant. □

3. Weierstrass ℘-function

Now we want to capitalize on our work above. Therefore we consider a very special periodic function, the Weierstraß ℘-function.

Definition. The *Weierstraß* $\wp - function$ is defined to be the function $\wp : \mathbb{C} \to \mathbb{C}$ given by

$$\wp(z) = \frac{1}{z^2} + \sum_{0 \neq \lambda \in \Lambda} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right)$$

Proposition 8. *(without proof) $\wp$ is a Λ-periodic meromorphic function with poles of order 2 exactly in Λ.*

The following lemma gives a connection between the Weierstraß ℘-function and our well known theta function with characteristic $\sigma = \frac{1}{2} + \frac{1}{2}\tau$.

Lemma 9. *There is a constant $c \in \mathbb{C}$ such that*

$$\wp(z) = -\left(\frac{\theta'_\sigma}{\theta_\sigma}\right)'(z) + c$$

Note. The quotient $\frac{\theta'_\sigma}{\theta_\sigma}$ isn't doubly-periodic, but the derivative $\left(\frac{\theta'_\sigma}{\theta_\sigma}\right)'$ is doubly-periodic.
To see this consider $\frac{\theta'_\sigma}{\theta_\sigma}(z+\lambda)$ for some $\lambda = p\tau + q \in \Lambda$.

$$\begin{aligned}
\frac{\theta'_\sigma}{\theta_\sigma}(z+\lambda) &\overset{(5)}{=} \frac{(e_\sigma(\lambda,z)\theta_\sigma(z))'}{e_\sigma(\lambda,z)\theta_\sigma(z)} \\
&= \frac{e'_\sigma(\lambda,z)\theta_\sigma(z) + e_\sigma(\lambda,z)\theta'_\sigma(z)}{e_\sigma(\lambda,z)\theta_\sigma(z)} \\
&\overset{def}{=} \frac{\exp'(\pi i\lambda - \pi i p^2\tau - 2\pi i p(z+\sigma))\theta_\sigma(z) + e_\sigma(\lambda,z)\theta'_\sigma(z)}{e_\sigma(\lambda,z)\theta_\sigma(z)} \\
&= \frac{-2\pi i p e_\sigma(\lambda,z)\theta_\sigma(z) + e_\sigma(\lambda,z)\theta'_\sigma(z)}{e_\sigma(\lambda,z)\theta_\sigma(z)} \\
&= -2\pi i p + \frac{\theta'_\sigma}{\theta_\sigma}(z) \\
&\neq \frac{\theta'_\sigma}{\theta_\sigma}(z)
\end{aligned}$$

as in general $p \neq 0$. From the equation $\frac{\theta'_\sigma}{\theta_\sigma}(z+\lambda) = -2\pi i p + \frac{\theta'_\sigma}{\theta_\sigma}(z)$ above it follows directly that $\left(\frac{\theta'_\sigma}{\theta_\sigma}\right)'$ is doubly-periodic.

Proof. We know that θ_σ is holomorphic and has its zeros precisely in the lattice points $\lambda \in \Lambda$. That means that the expansion of $\frac{\theta'_\sigma}{\theta_\sigma}$ in a Laurent series around 0 looks like

$$\frac{\theta'_\sigma}{\theta_\sigma}(z) = a_{-1}\frac{1}{z} + a_0 + a_1 z + a_2 z^2 + a_3 z^3 + \text{ terms of higher order}$$

for some constants $a_i \in \mathbb{C}$. We can choose a neighborhood U of 0 such that 0 is the only zero of θ_σ in U. As 0 is a single zero we know that

$$a_{-1} = \text{Res}_0\left(\frac{\theta'_\sigma}{\theta_\sigma}\right) = \int_\alpha \frac{\theta'_\sigma}{\theta_\sigma}(z)\,dz = 1$$

where $\alpha : [0,1] \to \mathbb{C}; t \mapsto re^{2\pi i t}$ for some suitable r. We conclude

$$\frac{\theta'_\sigma}{\theta_\sigma}(z) = \frac{1}{z} + a_0 + a_1 z + a_2 z^2 + a_3 z^3 + \text{ terms of higher order}$$

and calculate

$$\left(\frac{\theta'_\sigma}{\theta_\sigma}\right)'(z) = -\frac{1}{z^2} + a_1 + 2a_2 z + 3a_3 z^2 + \text{ terms of higher order}$$

If we add $\wp$ and $\left(\frac{\theta'_\sigma}{\theta_\sigma}\right)'$ then we obtain

$$\wp(z)+\left(\frac{\theta'_\sigma}{\theta_\sigma}\right)'(z)=\sum_{0\neq\lambda\in\Lambda}\left(\frac{1}{(z-\lambda)^2}-\frac{1}{\lambda^2}\right)+a_1+2a_2z+3a_3z^2+\dots$$

From this sum we see directly that $\wp+\left(\frac{\theta'_\sigma}{\theta_\sigma}\right)'$ doesn't have any poles in U. Hence $\wp+\left(\frac{\theta'_\sigma}{\theta_\sigma}\right)'$ is holomorphic in a neighborhood of 0 and thus holomorphic everywhere. As it is in addition doubly-periodic (since $\wp$ is as well as $\left(\frac{\theta'_\sigma}{\theta_\sigma}\right)'$ doubly-periodic) we know from our very first lemma that it must be constant. □

The Weierstraß $\wp$-function satisfies a number of equations and differential equation. This feature makes the Weierstraß $\wp$-function to be of interest. The most important differential equation that is satisfied by the Weierstraß $\wp$-function is the following:

Theorem 10. *The Weierstraß $\wp$ -function satisfies the differential equation*

$$\wp'(z)^2=c_3\wp(z)^3+c_2\wp(z)^2+c_1\wp(z)+c_0$$

where the constants

$$c_3=4\ ,\ c_2=0\ ,\ c_1=-60\sum_{0\neq\lambda\in\Lambda}\frac{1}{\lambda^4}\ \textit{and}\ c_0=-140\sum_{0\neq\lambda\in\Lambda}\frac{1}{\lambda^6}$$

depend on the lattice Λ.

Proof. Consider $\wp(z)-\frac{1}{z^2}=\sum_{0\neq\lambda\in\Lambda}\left(\frac{1}{(z-\lambda)^2}-\frac{1}{\lambda^2}\right)$. This function is holomorphic in a neighborhood of 0. We can expand the summands $\frac{1}{(z-\lambda)^2}-\frac{1}{\lambda^2}$:

$$\begin{aligned}\frac{1}{(z-\lambda)^2}-\frac{1}{\lambda^2}&=\frac{1}{\lambda^2}\left(\frac{1}{\left(1-\frac{z}{\lambda}\right)^2}-1\right)\\&=\frac{1}{\lambda^2}\left(\left(\sum_{n=0}^{\infty}\left(\frac{z}{\lambda}\right)^n\right)^2-1\right)\\&=\frac{1}{\lambda^2}\left(2\frac{z}{\lambda}+3\frac{z^2}{\lambda^2}+4\frac{z^3}{\lambda^3}+5\frac{z^4}{\lambda^4}+\dots\right)\\&=2\frac{z}{\lambda^3}+3\frac{z^2}{\lambda^4}+4\frac{z^3}{\lambda^5}+5\frac{z^4}{\lambda^6}+\dots\end{aligned}$$

This sum is absolutly convergent for all $z \in \mathbb{C}$ with $|z| < |\lambda|$; in particular in a neigborhood of 0.
To simplify the big sum from above we define $s_n := \sum_{0 \neq \lambda \in \Lambda} \frac{1}{\lambda^{n+2}}$ for $n \in \mathbb{N}$. Note that $s_n = 0$ for all odd $n \in \mathbb{N}$. We obtain

$$\begin{aligned} \wp(z) &= \frac{1}{z^2} + 2s_1 z + 3s_2 z^2 + 4s_3 z^3 + 5s_4 z^4 + \dots \\ &= \frac{1}{z^2} + 3s_2 z^2 + 5s_4 z^4 + 7s_6 z^6 \dots \end{aligned}$$

which is true in a neigborhood of 0. With the constants

$$c_3 = 4 \ , \ c_2 = 0 \ , \ c_1 = -60 \sum_{0 \neq \lambda \in \Lambda} \frac{1}{\lambda^4} \text{ and } c_0 = -140 \sum_{0 \neq \lambda \in \Lambda} \frac{1}{\lambda^6}$$

we obtain

$$\wp(z) = \frac{1}{z^2} - \frac{c_1}{20} z^2 - \frac{c_0}{28} z^4 + \text{ terms of higher order}$$

hence

$$\wp'(z) = -\frac{2}{z^3} - \frac{c_1}{10} z - \frac{c_0}{7} z^3 + \text{ terms of higher order}$$

$$\wp'(z)^2 = \frac{4}{z^6} + \frac{2c_1}{5} \frac{1}{z^2} + \frac{4c_0}{7} + \text{ terms of higher order}$$

and

$$\wp(z)^3 = \frac{1}{z^6} - \frac{3c_1}{20} \frac{1}{z^2} - \frac{3c_0}{28} + \text{ terms of higher order}$$

Now consider

$$f(z) := \wp'(z)^2 - c_3 \wp(z)^3 - c_1 \wp(z) - c_0$$

The series of f has only positive powers of z. Hence f is holomorphic around 0. Hence it is holomorphic everywhere. And as it is doubly-periodic, it is constant. But the constant part of the series is $\frac{4}{7} c_0 + 4 \cdot \frac{3}{28} c_0 - c_0 = 0$. Hence $f = 0$. □

We will mention one more equation that is satisfied by the Weierstraß $\wp$-function:

Remark. Remember that our lattice Λ is generated by 1 and τ. Hence the set of zeros of $\wp'$ is given by $\left(\frac{1}{2} + \Lambda\right) \cup \left(\frac{\tau}{2} + \Lambda\right) \cup \left(\frac{1+\tau}{2} + \Lambda\right)$. Set $e_1 := \wp\left(\frac{1}{2}\right)$, $e_2 := \wp\left(\frac{\tau}{2}\right)$, $e_3 := \wp\left(\frac{1+\tau}{2}\right) \in \mathbb{C}$. Then we have

$$(\wp')^2 = 4(\wp - e_1)(\wp - e_2)(\wp - e_3)$$

and

$$\begin{aligned} e_1 + e_2 + e_3 &= 0 \\ e_1e_2 + e_1e_3 + e_2e_3 &= \frac{1}{4}c_1 \\ e_1e_2e_3 &= -\frac{1}{4}c_0 \end{aligned}$$

where c_0 and c_1 are the constants from above.

Finally we will see how to use the Weierstraß $\wp$-function to give a group structure to an elliptic curve.

Remark. If we consider the elliptic curve

$$C := \{(x, y) \in \mathbb{C}^2 \text{ such that } y^2 = c_3x^3 + c_2x^2 + c_1x + c_0\}$$

for the constants

$$c_3 = 4\ ,\ c_2 = 0\ ,\ c_1 = -60 \sum_{0 \neq \lambda \in \Lambda} \frac{1}{\lambda^4} \text{ and } c_0 = -140 \sum_{0 \neq \lambda \in \Lambda} \frac{1}{\lambda^6}$$

from the theorem above then we have a bijection

$$\mathbb{C}/\Lambda \setminus \{0\} \to C \text{ given by } z \mapsto (\wp(z), \wp'(z))$$

In particular we can give the variety C the group structure of $\mathbb{C}/\Lambda$.

This can be extended to an embedding of $\mathbb{C}/\Lambda$ into the projective plane. For more details see the article of M. Khalid [2].

References

[1] A. Gathmann *Algebraic Geometry*, Notes for a class taught at the University of Kaiserslautern 2002/2003, available at http://www.mathematik.uni-kl.de/ gathmann/de/pub.html

[2] M. Khalid *Group Law on the Cubic Curve*, this issue

[3] D. Mumford *Tata Lectures on Theta*, Progress in Mathematics Vol 28, Birkhauser Verlag, 1983

[4] G. Trautmann *Complex Analysis II*, Notes for a class taught at the University of Kaiserslautern 1996/1997

Marina Franz, Fachbereich Mathematik, Technische Universität Kaiserslautern, Postfach 3049, 67653 Kaiserslautern, Germany.

E-mail address: franz@mathematik.uni-kl.de

RANK TWO VECTOR BUNDLES ON ELLIPTIC CURVES

CIARA DALY

Abstract. The aim of this paper is to give an overview of rank two vector bundles on an elliptic curve. It also aims to provide an outline of stability of vector bundles to serve as a motivation for the study of moduli spaces of vector bundles over elliptic curves. The first section outlines basic definitions and theorems. We will then study vector bundles on $\mathbb{P}^1$. From here, we go on to classify indecomposable rank two vector bundles over an elliptic curve. The final section introduces the notion of stability of vector bundles.

1. Introduction

Nowadays, vector bundles play an inportant role in many areas of mathematics such as algebraic geometry, algebraic topology and differential geometry, in the theory of partial differential equations.

The theory of vector bundles and the mathematical formalism developed over the years, for the study of vector bundle related concepts leads to the clarification or solution of many mathematical problems. Some of the vector bundle related concepts are generalisations of well-known classical notions. For instance, the notion of a section of a vector bundle over a space X is a generalization of a vector valued function on X.

One of the important problems is the problem of classification of bundles. The problem of classification of vector bundles over an elliptic curve (i.e. a nonsingular projective curve of arithmetic genus one) has been completely solved by Atiyah in [1].

2. Preliminaries

For the purpose of this paper, X will denote a complex manifold, unless otherwise specified. We will be working over $\mathbb{C}$, the field of complex numbers, throughout this paper.

Definition 2.1. A *complex vector bundle* of rank n is a holomorphic map $p : E \to X$ of complex manifolds which satisfy the following conditions:

(1) For any point $x \in X$, the preimage $E_x := p^{-1}(x)$ (called a *fibre*) has a structure of an n-dimensional $\mathbb{C}$-vector space.

(2) The mapping p is locally trivial, i.e. for any point $x \in X$, there exists an open neighbourhood U_i containing x and a biholomorphic map $\varphi_i : p^{-1}(U_i) \to U_i \times \mathbb{C}^n$ such that the diagram

$$\begin{tikzcd}
p^{-1}(U_i) \arrow[rr, "\varphi_i"] \arrow[dr, "p"'] & & U_i \times \mathbb{C}^n \arrow[dl, "pr_1"] \\
& U_i &
\end{tikzcd}$$

commutes.

Moreover, φ_i takes the vector space E_x isomorphically onto $\{x\} \times \mathbb{C}^n$ for each $x \in U_i$; φ_i is called a *trivialisation* of E over U. Note that for any pair of trivialisations φ_i and φ_j, the map

$$g_{ij} : U_i \cap V_j \to \mathrm{GL}(n, \mathbb{C})$$

given by

$$g_{ij}(x) = \varphi_i \circ (\varphi_j|_{\{x\}\times\mathbb{C}^n})^{-1}$$

is holomorphic; the maps g_{ij} are called *transition functions* for E relative to the trivialisations φ_i, φ_j. The transition functions of E necessarily satisfy the identities

$$g_{ij}(x) \cdot g_{ji}(x) = I \qquad \text{for all } x \in U_i \cap U_j$$

$$g_{ij}(x) \cdot g_{jk}(x) \cdot g_{ki}(x) = I \qquad \text{for all } x \in U_i \cap U_j \cap U_k.$$

Conversely, given an open cover $\{U_i\}$ of X and transition functions $g_{ij} : U_i \cap U_j \to \mathrm{GL}(n, \mathbb{C})$, for all i, j, then we can define a vector bundle, E with transition functions g_{ij} using the glueing construction as follows: We glue $U_i \times \mathbb{C}^n$ together by taking the union over all i of $U_i \times \mathbb{C}^n$ to get $E := \bigsqcup(U_i \times \mathbb{C}^n)/\sim$, where $(x, v) \sim (x, g_{ij}(x)(v))$, for all $x \in U_i \cap U_j, v \in \mathbb{C}^n$.

A vector bundle of rank 1 is called a *line bundle* (See [7] Section 5 for more details).

Example 2.2. The simplest example is known as the *trivial vector bundle* of rank n, i.e. $pr_1 : X \times \mathbb{C}^n \to X$, where pr_1 denotes projection to the first factor.

The trivial line bundle on X, i.e. $X \times \mathbb{C} \to X$ will be denoted by $\mathcal{O}_X$, (or simply $\mathcal{O}$ if it is clear which X we are referring to).

Example 2.3. The set $\mathcal{O}(-1) \subset \mathbb{P}^n \times \mathbb{C}^{n+1}$ that consists of all pairs $(\ell, z) \in \mathbb{P}^n \times \mathbb{C}^{n+1}$ with $z \in \ell$ forms in a natural way a line bundle over $\mathbb{P}^n$. To see this, consider the projection $p : \mathcal{O}(-1) \to \mathbb{P}^n$, where p is the projection to the first factor. Let $\mathbb{P}^n = \bigcup_{i=0}^n U_i$ be the standard open covering. A canonical trivialisation of $\mathcal{O}(-1)$ over U_i is given by $\varphi_{U_i} : p^{-1}(U_i) \cong U_i \times \mathbb{C}, (\ell, z) \mapsto (\ell, z_i)$. The transition functions $g_{ij}(\ell) : \mathbb{C} \to \mathbb{C}$ are given by $w \mapsto \frac{z_i}{z_j} \cdot w$, where $\ell = (z_0 : \cdots : z_n)$.

Definition 2.4. Let $p : E \to X$ and $p' : E' \to X$ be two complex vector bundles on X. A holomorphic map $f : E \to E'$ is called a *morphism* of vector bundles if the diagram

$$\begin{tikzcd}
E \arrow[rr, "f"] \arrow[dr, "p"'] & & E' \arrow[dl, "p'"] \\
& X &
\end{tikzcd}$$

commutes and for each point $x \in X$ the map $f|_{E_x} : E_x \to E'_x$ is a homomorphism of vector spaces.

Let E and E' be vector bundles over X with rank r and r', respectively and let $\{U_i\}$ be an open cover of X such that E and E' are trivial over U_i for each i. A morphism $f : E \to E'$ can be described locally by holomorphic functions, f_i, as follows. For each i, using trivialisations of E and E', f induces maps

$$U_i \times \mathbb{C}^r \to U_i \times \mathbb{C}^{r'}, \quad (x, v) \mapsto (x, f_i(x)v)$$

where $f_i : U_i \to \mathrm{Mat}_{r' \times r}(\mathbb{C})$. These holomorphic functions necessarily satisfy

$$f_i(x) \cdot g_{ij}(x) = g'_{ij}(x) \cdot f_j(x) \text{ for all } x \in U_i \cap U_j$$

where g_{ij} and g'_{ij} are transition functions of E and E', respectively. Note that a set of functions $\{f_i\}$ defines an isomorphism of vector bundles if an only if $f_i(x)$ are invertible matrices for all i and x.

Remark 2.5. It is important to note that this definition of a morphism of vector bundles does not make the category of vector bundles into an abelian category. For instance, if $f : E \to E'$ is a morphism of vector bundles and the rank of f is non-constant then $\dim(\ker(f_x))$ jumps and so $\ker f$ cannot form a vector bundle. The same would be true for $\operatorname{coker} f$. On the contrary if $\dim(\ker(f_x))$ is constant on x, then both $\ker f$ and $\operatorname{coker} f$ are vector bundles. This can be shown locally by a rank argument. It is necessary to use strict morphisms if an abelian category is required.

Definition 2.6. Let E be a vector bundle on X and let $\{U_i\}$ be an open cover of X. If the transition functions of E are g_{ij}, then the *dual bundle*, E^*, of E is given by transition functions

$$h_{ij}(x) := {}^t g_{ij}(x)^{-1} \quad \forall x \in U_i \cap U_j$$

Definition 2.7. A sequence of morphisms of vector spaces

$$0 \longrightarrow A \xrightarrow{\quad f \quad} B \xrightarrow{\quad g \quad} C \longrightarrow 0$$

is called a *short exact sequence* if $\ker g = \operatorname{im} f$, and if f is injective and g is surjective.

Definition 2.8. A sequence of morphisms of vector bundles over X

$$0 \longrightarrow E' \longrightarrow E \longrightarrow E'' \longrightarrow 0$$

is an *exact sequence of vector bundles* if

$$0 \longrightarrow E'_x \longrightarrow E_x \longrightarrow E''_x \longrightarrow 0$$

is an exact sequence of vector spaces for all $x \in X$. The vector bundle E' is called a subbundle of E, and E'' is called a quotient bundle of E.

We also say that an exact sequence of vector bundles

$$0 \longrightarrow E' \longrightarrow E \longrightarrow E'' \longrightarrow 0$$

is an extension of E'' by E'. In this case E is called an extension of E'' by E'.

Definition 2.9. Let U be an open set in X. A holomorphic map $s : U \to E$ is called a *holomorphic section* of E over U if $p \circ s = id_U$. Sections over X are called *global sections* of E. Global sections can be added and multiplied with a scalar, so the space of global sections is in fact a vector space. It will be denoted by $H^0(X, E)$.

Remark 2.10. Let $f : E' \to E$ be a morphism of vector bundles. This induces a linear map of spaces of sections $H^0(f) : H^0(E') \to H^0(E)$ by $H^0(f)(s') := f \circ s'$.

2.1. **Cohomology:** Given a short exact sequence of vector bundles over X

$$0 \longrightarrow E' \xrightarrow{f} E \xrightarrow{g} E'' \longrightarrow 0$$

we can take global sections to get an exact sequence

$$0 \longrightarrow H^0(X, E') \xrightarrow{H^0(f)} H^0(X, E) \xrightarrow{H^0(g)} H^0(X, E'') \qquad (1)$$

in which the last map $H^0(g) : H^0(X, E) \to H^0(X, E'')$ is not in general surjective. For a counter example to $H^0(g)$ being surjective see [4] Chapter 8.

Since we get the exact sequence (1) above, we say that the global section functor is left exact. This global section sequence extends to a long cohomology exact sequence. For any vector bundle E on X, the natural cohomology groups $H^i(X, E)$ (also denoted $H^i(E)$ if it is clear which X we are referring to), for all $i > 0$, can be defined satisfying the following property. Given a short exact seqence

$$0 \longrightarrow E' \longrightarrow E \longrightarrow E'' \longrightarrow 0$$

of vector bundles, there is an induced long exact sequence of cohomology groups

$$0 \to H^0(X, E') \to H^0(X, E) \to H^0(X, E'') \to H^1(X, E') \to \cdots$$

I will not define these cohomology groups in this paper, except to note that they exist and are very useful in computations. The dimension of $H^i(X, E)$ will be denoted $h^i(X, E)$. In the case of a curve X the cohomology groups $H^i(X, E)$, vanish for all $i > 1$, where 1 is the dimension of X, i.e. only the cohomology groups $H^0(X, E)$ and $H^1(X, E)$ are nonzero. (In fact $H^i(X, E)$ vanish for all $i > \dim X$ for a more general X than just a curve though we do not need this fact in this paper. See [4] Chapter 8 for more details).

2.2. **Ext groups:** If E and E' are vector bundles over X, we denote by $\mathrm{Hom}_X(E, E')$ (or $\mathrm{Hom}(E, E')$ if it is clear which X we are referring to) the vector space of vector bundle morphisms. For a fixed E, $\mathrm{Hom}(E, \cdot)$ is a left exact covariant functor from the category of vector bundles to the category of vector spaces, i.e. given a short exact sequence of vector bundles

$$0 \longrightarrow F' \longrightarrow F \longrightarrow F'' \longrightarrow 0$$

we get another exact sequence in which the last map is not surjective in general

$$0 \longrightarrow \mathrm{Hom}(E,F') \longrightarrow \mathrm{Hom}(E,F) \xrightarrow{g} \mathrm{Hom}(E,F'') \tag{2}$$

And so in a similar fashion to the way we defined cohomology groups $H^i(E)$, we can define what are called the Ext groups, which allow us to extend our short exact sequence (2) to a long exact sequence as follows:

$$\begin{array}{l} 0 \longrightarrow \mathrm{Hom}(E,F') \longrightarrow \mathrm{Hom}(E,F) \longrightarrow \mathrm{Hom}(E,F'') \\ \longrightarrow \mathrm{Ext}^1(E,F') \longrightarrow \mathrm{Ext}^1(E,F) \longrightarrow \cdots \end{array}$$

We say that $\mathrm{Ext}^i(E,\cdot)$ are the right derived functors of $\mathrm{Hom}(E,\cdot)$. So in particular we have $\mathrm{Ext}^0(E,\cdot) = \mathrm{Hom}(E,\cdot)$. We have the following proposition to see the relationship between the cohomology groups H^i and the Ext groups (for a full proof of this proposition see [5] Proposition 6.3).

Proposition 2.11. *For any vector bundle E on a complex manifold X we have:*
$\mathrm{Ext}^i(\mathcal{O}_X, E) \cong H^i(E)$ *for all* $i \geq 0$.
Similarly we have:
$\mathrm{Ext}^i(E, \mathcal{O}_X) \cong H^i(E^*)$ *for all* $i \geq 0$.

Proof. Here we will just give a proof of the first statement, where $i = 0$. Let $f \in \mathrm{Hom}(\mathcal{O}, E)$, a fibre-wise holomorphic morphism such that the following diagram commutes

$$\begin{tikzcd} X \times \mathbb{C} \arrow[rr, "f"] \arrow[dr, "pr_1"'] & & E . \arrow[dl, "p"] \\ & X & \end{tikzcd}$$

Let $s : X \to E$ be a holomorphic section of E, i.e. $p \circ s = \mathrm{id}_x$. Define two linear maps

$$\alpha : \mathrm{Hom}(\mathcal{O}, E) \to H^0(E)$$

and

$$\beta : H^0(E) \to \mathrm{Hom}(\mathcal{O}, E)$$

as follows: Define $\alpha(f)(x) := f(x,1)$ and $\beta(s)(x,\lambda) := \lambda \cdot s(x)$.

We see that $\beta(\alpha(f)) = f$ as follows:

$\beta(\alpha(f))(x,\lambda) = \lambda \cdot (\alpha(f)(x)) = \lambda \cdot f(x,1) = f(x,\lambda)$, where the last equality uses the fact that f is linear on fibres.

Similarly we obtain $\alpha(\beta(s))(x) = \beta(s)(x,1) = s(x)$, so $\alpha(\beta(s)) = s$. Hence α and β are inverses of one another and we get

$$\operatorname{Hom}(\mathcal{O}, E) \cong H^0(E).$$

□

Remark 2.12. Given a vector bundle E, and given that $H^0(E) \neq 0$, then from Proposition 2.11 we know that $\operatorname{Hom}(\mathcal{O}, E) \neq 0$. So we have $f : \mathcal{O} \to E$. We can say that $\mathcal{O} \subset E$, though here '$\subset$' does not denote a subbundle, but rather a 'subsheaf'. Vector bundles can also be described as sheaves (in particular locally free sheaves) though we have not built up this language in this paper. It suffices to know that if $\mathcal{O} \subset E$ as a subsheaf then we can extend this to get a line subbundle $M \subset E$ on X, a smooth curve (See [9] Chapter 10 for more details). This will be useful in proofs later on.

The notion of a degree of a line bundle on a curve was introduced in [7] (Section 5). We can extend this definition to vector bundles of arbitrary rank. To do so we must first define the determinant line bundle.

Definition 2.13. Given a vector bundle E of rank r, it's *determinant line bundle* is defined to be the r-th exterior power of E, denoted:

$$\det E := \wedge^r E.$$

where the fibres of X for any $x \in X$ are canonically isomorphic to $\wedge^r E_x$.

For those of you who are unfamiliar with exterior power, we can reformulate the definition as follows: Given an open cover $\{U_i\}$ of X and a vector bundle E over X with transition functions g_{ij}, the determinant line bundle of E is given by transition functions h_{ij} where

$$h_{ij}(x) := \det g_{ij}(x) \in \mathrm{GL}(1, \mathbb{C}), \quad \text{for all } x \in U_i \cap U_j$$

This now allows us to define the degree of a vector bundle as follows.

Definition 2.14. The *degree* $\deg E \in \mathbb{Z}$ of a vector bundle is the degree of its determinant line bundle $\det E$.

Remark 2.15. Recall from [7] that the degree of a line bundle is the degree of it's associated divisor and every line bundle can be written as $\mathcal{O}(D)$, with D a divisor on X.

If E lies in an exact sequence of vector bundles on X as follows:

$$0 \to E' \to E \to E'' \to 0$$

then there is an isomorphism

$$\det E' \otimes \det E'' \cong \det E.$$

Since $\det E'$ and $\det E''$ are line bundles we get $\deg E = \deg E' + \deg E''$ (as in general $\deg(L \otimes L') = \deg L + \deg L'$, where L and L' line bundles). In other words, degree is additive on exact sequences. As a special case, if a vector bundle $E = L_1 \oplus L_2$ is the direct sum of two line bundles L_1 and L_2, then we have

$$0 \to L_1 \to E \to L_2 \to 0$$

with $\deg E = \deg L_1 + \deg L_2$.

Remark 2.16. Let E be a vector bundle of rank r over a complex manifold X. If we tensor E with a line bundle L, then $\deg(E \otimes L) = \deg E + r \deg L$. In particular for E of rank 2 we have $\deg(E \otimes L) = \deg E + 2 \deg L$. To see this let's look at an example:

Let $E = L_1 \oplus L_2$ for line bundles L_1 and L_2. Tensor this with another line bundle L to get

$$E \otimes L = (L_1 \oplus L_2) \otimes L = (L_1 \otimes L) \oplus (L_2 \otimes L)$$

Now

$$\begin{aligned} \deg(E \otimes L) &= \deg(L_1 \otimes L) + \deg(L_2 \otimes L) \\ &= \deg L_1 + \deg L + \deg L_2 + \deg L \\ &= \deg L_1 + \deg L_2 + 2 \deg L \\ &= \deg E + 2 \deg L. \end{aligned}$$

In this way, when considering vector bundles of rank 2, it is enough to consider vector bundles of degree -1 or 0 (or indeed, any even and odd degree), then by tensoring with a line bundle of appropriate degree we get all other degrees. We call this the "tensor product trick".

Definition 2.17. An exact sequence of vector bundles

$$0 \to E' \to E \to E'' \to 0$$

splits if and only if there exists a homomorphism $f : E'' \to E$ for which the composition $E'' \xrightarrow{f} E \longrightarrow E''$ is an isomorphism.

In this case, the map f is called a *splitting* of the sequence.

Now consider, on any curve, a short exact sequence of vector bundles

$$\mathbb{E}: \quad 0 \longrightarrow M \xrightarrow{\alpha} E \xrightarrow{\beta} L \longrightarrow 0.$$

By applying $\operatorname{Hom}(L, -)$ to this sequence we get the following morphism:

$$\operatorname{Hom}(L, L) \xrightarrow{\delta} \operatorname{Ext}^1(L, M)$$

Definition 2.18. The image under the coboundary map δ of $\mathrm{id}_L \in \operatorname{Hom}(L, L)$, which we will denote by

$$\delta(\mathrm{id}_L) \in \operatorname{Ext}^1(L, M) \cong H^1(L^* \otimes M),$$

is called the *extension class* of $\mathbb{E}$.

By exactness of

$$\operatorname{Hom}(L, E) \xrightarrow{\rho} \operatorname{Hom}(L, L) \xrightarrow{\delta} \operatorname{Ext}^1(L, M),$$

if $\delta(\mathrm{id}_L) = 0$, then there exists a homomorphism $f : L \to E$ for which the $\mathrm{id}_L = \beta \circ f : L \to L$, i.e. the sequence $\mathbb{E}$ splits. Moreover, if $\mathbb{E}$ splits, there exists $f : L \to E$ such that $\mathrm{id}_L = \beta \circ f$. Because the composition, $\rho \circ \delta$ is zero, we have $\delta(\mathrm{id}_L) = 0$. Hence we have the following proposition:

Proposition 2.19. *The sequence* $\mathbb{E}$*, i.e.*

$$0 \to M \to E \to L \to 0.$$

splits if and only if $\operatorname{Ext}^1(L, M) = 0$*. In particular, if* $\operatorname{Ext}^1(L, M) \cong H^1(L^* \otimes M) = 0$*, then every exact sequence* $\mathbb{E}$ *splits.*

Remark 2.20. For each $\alpha \in \operatorname{Ext}^1(E'', E')$ there exists an extension

$$0 \to E' \to E_\alpha \to E'' \to 0 \tag{3}$$

with a vector bundle, E_α, in such a way that α is the extension class of (3). Moreoever, $E_\alpha \cong E_\beta$ if and only if there exists $\lambda \in \mathbb{C}^*$ such that $\alpha = \lambda\beta$. (See [10] Section 3.4 for more details)

2.3. **Riemann-Roch Formula for curves.** We have a very useful tool, called the Riemann-Roch formula, which tells us a lot about the cohomology groups of a vector bundle E, $H^0(E)$ and $H^1(E)$, once we know the rank and degree of E. The Riemann-Roch formula is as follows: If E is a vector bundle of rank r on a curve of genus g, then:

$$h^0(E) - h^1(E) = \deg E - r(g-1).$$

In addition to the Riemann-Roch formula, one of the other major tools we have in dealing with cohomology is Serre duality. The following proposition outlines Serre duality, though will not be proved as the proof is too involved for this paper.

Proposition 2.21. (**Serre duality**) *Let X be a smooth projective curve. Let E be a vector bundle on X. Let K_X be a canonical line bundle on X. Then there are canonical isomorphisms*

$$H^0(X,E) \cong H^1(X, K_X \otimes E^*)^*.$$

and

$$H^1(X,E) \cong H^0(X, K_X \otimes E^*)^*.$$

In particular it follows that $H^0(X,E)$ and $H^1(X, K_X \otimes E^*)$ have the same dimension.

While I have not defined K_X, the canonical line bundle, for the purpose of this paper it will suffice to know what K_X is in the case of a curve. This is outlined below:

$$X = \mathbb{P}^1 : \quad K_X = \mathcal{O}_{\mathbb{P}^1}(-2), \quad \deg(K_X) = -2$$

$$X = \text{elliptic curve} : \quad K_X = \mathcal{O}_X, \quad \deg(K_X) = 0$$

$$X = \text{curve of genus } g \geq 2 : \quad \deg(K_X) = 2g-2.$$

Refer to [5] Section III.7 for more details on Serre duality.

Lemma 2.22. *Let L be a line bundle on a curve, C, of genus g. Then we have the following:*

(a) $H^0(L) = 0$ *if* $\deg L < 0$.
(b) $H^1(L) = 0$ *if* $\deg L > 2g-2$.
(c) $L \cong \mathcal{O}$ *if* $\deg L = 0$ *and* $s \in H^0(L), s \neq 0$.

The proof of (a) and (c) of the lemma above uses the correspondence between line bundles and divisors (see again [7]) and the fact that the divisor defined by a nonzero holomorphic section of a line bundle is always positive. The proof of (b) follows from Serre duality and part (a).

Lemma 2.23. *If E is a vector bundle on a curve C of genus g, then the degree of its subbundles $F \subset E$ is bounded above.*

Proof. ([9], Corollary 10.9) Since the global sections functor is left exact, we get

$$H^0(F) \subset H^0(E)$$

This implies that $h^0(F) \leq h^0(E)$. Now by Riemann-Roch we know

$$h^0(F) - h^1(F) = \deg(F) + \operatorname{rk}(F) \cdot (1-g).$$

From this we get

$$\deg(F) + \operatorname{rk}(F) \cdot (1-g) + h^1(F) \leq h^0(E)$$

and by rearranging we have

$$\deg(F) \leq h^0(E) - \operatorname{rk}(F) \cdot (1-g) - h^1(F)$$

Now if $g = 1$, we see that $\deg(F) \leq h^0(E) - h^1(F)$ and since $h^1(F) \geq 0$, we get $\deg(F) \leq h^0(E)$.

If $g = 0$, then $\deg(F) \leq h^0(E) - \operatorname{rk}(F) - h^1(F)$ and since $\operatorname{rk}(F) \geq 0$ and $h^1(F) \geq 0$, we see that $\deg(F) \leq h^0(E)$.

If $g \geq 2, \deg(F) \leq h^0(E) + \operatorname{rk}(F) \cdot (g-1) - h^1(F) \leq h^0(E) + \operatorname{rk}(E) \cdot (g-1) - h^1(F)$ (since $\operatorname{rk}(F) \leq \operatorname{rk}(E)$). Again, since $h^1(F) \geq 0$, we get $\deg(F) \leq h^0(E) + \operatorname{rk}(E) \cdot (g-1)$. Hence we see that in any case the degree of $F \subset E$ is bounded above. □

3. Vector bundles on $\mathbb{P}^1$

Before we move on to vector bundles on an elliptic curve (i.e. a curve of genus one), it makes sense to look at vector bundles on a curve of genus zero ($\mathbb{P}^1$). Let us now restate Lemma 2.22 in the case of $\mathbb{P}^1$, where genus $g = 0$, to see how the cohomology of line bundles on $\mathbb{P}^1$ is particularly simple.

Lemma 3.1. *Let L be a line bundle on $\mathbb{P}^1$. Then we have the following:*

(a) $H^0(L) = 0$ *if* $\deg L \leq -1$.

(b) $H^1(L) = 0$ *if* $\deg L \geq -1$.

By Riemann-Roch we also have,

$$h^0(L) - h^1(L) = \deg L + 1.$$

Remark 3.2. We have seen from [7] that for L a line bundle, L^* is the inverse of the line bundle L in the Picard group. We have also seen that $\deg : \operatorname{Pic} X \to \mathbb{Z}$ is a homomorphism (where $\operatorname{Pic} X$ denotes the set of line bundles over X) and so we get $\deg L^* = -\deg L$.

Lemma 3.3. *The homomorphism* $\deg : \operatorname{Pic}\mathbb{P}^1 \to \mathbb{Z}$ *is an isomorphism.*

Proof. See [4] Lemma 6.2.11. □

We have a classification for all vector bundles on $\mathbb{P}^1$ as follows:

Lemma 3.4. *Every rank* 2 *vector bundle on* $\mathbb{P}^1$ *is isomorphic to a direct sum of two line bundles*
Proof. ([9], Lemma 10.30) Let E be a rank 2 vector bundle on $\mathbb{P}^1$. Tensoring with a line bundle if necessary, it is enough to assume that $\deg E = 0$ or -1. First, by the Riemann-Roch formula we note that $H^0(E) \neq 0$, and so from Remark 2.12 above we get a line bundle $M \subset E$, and $M \cong \mathcal{O}(D)$ for some positive divisor $D \geq 0$. In particular, $\deg M \geq 0$, and denoting the quotient by $L := E/M$, we have an exact sequence

$$0 \to M \to E \to L \to 0.$$

Now $\deg E = \deg L + \deg M$, hence $\deg(L^* \otimes M) = \deg M - \deg L = -\deg E + 2\deg M \geq -\deg E \geq 0$. From Lemma 3.1 (b), we get $H^1(L^* \otimes M) = 0$. By Proposition 2.19, therefore, the sequence splits. □

Grothendieck's Theorem 3.5. *Every vector bundle on* $\mathbb{P}^1$ *is isomorphic to a direct sum of line bundles*
Proof. ([9] Theorem 10.31) Let E be a vector bundle of rank r on $\mathbb{P}^1$. Proof is by induction on the rank $r \geq 2$ of E, starting with the previous lemma. Serre's Theorem ([5] II.5.17) tells us that there exists a line subbundle in E. Now let $M \subset E$ be the line subbundle whose degree, $m = \deg M$, is maximal among line subbundles of E (Lemma 2.23). Let $F := E/M$ be a vector bundle of rank $r-1$.

Claim: Every line subbundle $L \subset F$ has $\deg L \leq m$.

Now we have a short exact sequence as follows:

$$0 \to M \to E \to F \to 0$$

By considering the preimage $\tilde{L} \subset E$ of L under the quotient morphism $E \to F$ we get a diagram as follows:

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] & E \arrow[r] & F \arrow[r] & 0 \\
0 \arrow[r] & M \arrow[r] \arrow[u, equal] & \tilde{L} \arrow[r] \arrow[u, hook] & L \arrow[r] \arrow[u, hook] & 0
\end{tikzcd}$$

Clearly $\tilde{L}$ is a rank 2 vector bundle, and we see $\deg \tilde{L} = m + \deg L$. By Lemma 3.4, we know $\tilde{L} \cong L_1 \oplus L_2$ for some line bundles L_1 and L_2. Now $\deg(\tilde{L}) = \deg(L_1) + \deg(L_2)$ so one of L_1 or L_2 must have deg at least $\deg(\tilde{L})/2$. Let N denote that line subbundle, of degree at least $\deg \tilde{L}/2$. Because N is a subbundle of E, as well as our choice of M we get $m \geq \deg N \geq (\deg \tilde{L})/2 = \frac{m+\deg L}{2}$ and the claim follows easily from this.

By the inductive hypothesis, we know the quotient bundle F is isomorphic to a direct sum $F = L_1 \oplus \cdots \oplus L_{r-1}$ of line bundles and the claim gives us $\deg L_i \leq m$. Since $H^1(L_i^* \otimes M) = 0$ for each i. It follows that the exact sequence

$$0 \to M \to E \to \bigoplus_{i=1}^{r-1} L_1 \to 0$$

splits. □

Definition 3.6. A vector bundle, E, is called *decomposable* if it is isomorphic to the direct sum $E_1 \bigoplus E_2$ of two nonzero vector bundles; otherwise, E is called *indecomposable.*

By definition of decomposability, every vector bundle is the direct sum of indecomposable ones. Therefore, it suffices to know the indecomposable vector bundles on a curve in order to know them all. We have seen that all vector bundles on rational curves are the direct sum of line bundles. As well as the notion of an indecomposable vector bundle, we also have the notion of a simple vector bundle.

Definition 3.7. A vector bundle E is *simple* if its only endomorphisms are scalars, $\operatorname{End} E = \mathbb{C}$. Every line bundle is simple.

A simple vector bundle is necessarily indecomposable. To see this let us start with a decomposable vector bundle $E \oplus F$. Consider $f : E \oplus F \to E \oplus F$, where $f = \mathrm{id}_E \oplus 0_F$ where id_E is the identity map on E and 0_F is the zero map on F. Clearly then $\operatorname{End}(E \oplus F) \neq \mathbb{C}$, i.e. F is not simple.

Note that the converse is not true, i.e. an indecomposable vector bundle is not necessarily simple (This can be seen by a counterexample, Example 4.4 below).

4. Classification of all indecomposable rank two vector bundles on an elliptic curve C

We are now ready to look at the case of a nonsingular curve of arithmetic genus one (i.e. an elliptic curve). Atiyah's paper of 1957 ([1]) provided us with an answer to this case. We have already seen in Lemma 3.3 that there is exactly one line bundle on $\mathbb{P}^1$ for every degree. In particular $\operatorname{Pic}^0(\mathbb{P}^1) = \{\mathcal{O}\}$, where $\operatorname{Pic}^0(\mathbb{P}^1)$ denotes the set of line bundles of degree 0 on $\mathbb{P}^1$. However it turns out ([7] Theorem 20) on an elliptic curve, C, that $\operatorname{Pic}^0(C)$ is in bijection to C and so on elliptic curves there are more vector bundles in the sense that nontrivial extensions appear. For the purpose of this paper we will be concentrating on rank 2 vector bundles on an elliptic curve. In this section we will give a classification of all indecomposable rank 2 vector bundles on the elliptic curve C.

First let me return to the Riemann-Roch formula for a vecor bundle E, this time looking at a curve of genus 1, i.e.

$$h^0(E) - h^1(E) = \deg E$$

Note that every line bundle, L, on C satisfies:

$$h^0(L) - h^1(L) = \deg L$$

The next lemma follows from the above equation and Lemma 2.22:

Lemma 4.1. *Let L be a line bundle on an elliptic curve. Then we have the following:*

(a) $H^0(L) = 0$ if $\deg L < 0$.

(b) $H^1(L) = 0$ if $\deg L > 0$.

(c) If $\deg L = 0$ and $L \ncong \mathcal{O}$, then $H^0(L) = H^1(L) = 0$.

Lemma 4.2. *If E is an indecomposable vector bundle of rank 2 on a smooth projective curve, X, then every line subbundle $L \subset E$ satisfies*

$$2 \deg L \leq \deg E + 2g - 2$$

Proof. Let M be the quotient line bundle E/L. This gives us the following short exact sequence:

$$0 \to L \to E \to M \to 0$$

which corresponds to an element in $\operatorname{Ext}^1(M, L) \cong H^1(M^* \otimes L)$. Now since E is indecomposable, this sequence cannot split and hence $H^1(M^* \otimes L) \neq 0$ by Proposition 2.19. By Serre duality, this implies that $0 \neq H^0((M^* \otimes L)^* \otimes K_X)^* = H^0(M \otimes L^* \otimes K_X)^*$. This in turn implies that $\deg(M \otimes L^* \otimes K_X) = \deg M - \deg L + 2g - 2 \geq 0$ from Lemma 2.22 (a). Now from the short exact sequence above we know that $\deg E = \deg M + \deg L$, i.e. $\deg M = \deg E - \deg L$. Hence we get

$$\deg E - \deg L - \deg L + 2g - 2 \geq 0$$

From this, we get the inequality in the lemma. □

Let $\mathcal{E}(r,d)$ denote the set of isomorphism classes of indecomposable vector bundles of rank r and degree d over X, an elliptic curve.

Theorem 4.3. *(a) There exists a vector bundle $E_r \in \mathcal{E}(r,0)$, unique up to isomorphism, with $H^0(E_r) \neq 0$. Moreover, we have an exact sequence:*

$$0 \to \mathcal{O}_X \to E_r \to E_{r-1} \to 0$$

(b) Let $E \in \mathcal{E}(r,0)$, then $E \cong E_r \otimes L$, where L is a line bundle of degree zero, unique up to isomorphism.

Proof. See [1] Theorem 5. □

Example 4.4. The bundles E_r of Theorem 4.3 are sometimes called the Atiyah bundles. For $r \geq 2$, they are examples of indecomposable vector bundles which are not simple. Let us prove now that E_2 is not simple.

We know E_2 sits in an exact sequence as follows:

$$\begin{tikzcd} 0 \arrow[r] & \mathcal{O}_X \arrow[r, "f"] & E_2 \arrow[r] & \mathcal{O}_X \arrow[r] & 0 \end{tikzcd}$$

Applying $\mathrm{Hom}(-, E_2)$ to this sequence, we get

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Hom}(\mathcal{O}, E_2) \arrow[r] & \mathrm{Hom}(E_2, E_2) \arrow[r, "\beta"] & \mathrm{Hom}(\mathcal{O}, E_2) \end{tikzcd}$$

Now $\mathrm{Hom}(\mathcal{O}, E_2) \cong H^0(E_2)$ from Proposition 2.11. From our assumption on E_2, we know $H^0(E_2) \neq 0$, i.e. $h^0(E_2) \geq 1$. Now let id_{E_2} denote $\mathrm{id} \in \mathrm{Hom}(E_2, E_2)$. We know, under the morphism β, that $\mathrm{id}_{E_2} \mapsto f \in \mathrm{Hom}(\mathcal{O}, E_2) \neq 0$, i.e. $\beta(\mathrm{id}_{E_2}) = f \neq 0$. This implies $\beta \neq 0$. So we get the following short exact sequence:

$$0 \to \mathrm{Hom}(\mathcal{O}, E_2) \to \mathrm{Hom}(E_2, E_2) \to \mathrm{im}(\beta) \to 0$$

Since $\beta \neq 0$, we know that $\dim(\mathrm{im}(\beta)) \geq 1$. Now since dim is additive on exact sequences, $\dim(\mathrm{Hom}(E_2, E_2)) = \dim(\mathrm{Hom}(\mathcal{O}, E_2)) + \dim(\mathrm{im}(\beta)) \geq 2$. Hence by the definition of a simple vector bundle (Definition 3.7), we know that E_2 is not simple.

Let us now classify all indecomposable rank 2 vector bundles on an elliptic curve. We first consider the case of even degree.

Proposition 4.5. *On a curve, C, of genus* 1 *every indecomposable rank* 2 *vector bundle, E, of even degree is an extension of the form*

$$0 \longrightarrow M \longrightarrow E \longrightarrow M \longrightarrow 0$$

for some line bundle M on E
Proof. ([9] Proposition 10.48) Using the tensor product trick, it is enough to consider the case where $\deg E = 2k$. If $M_1 \in \mathrm{Pic}^k(C)$, i.e. M_1 is a line bundle of degree k, then $E \otimes M_1$ is of degree 0. In other words, $E \otimes M_1 \in \mathcal{E}(r, 0)$. By Theorem 4.3, we know that there exists $M_2 \in \mathrm{Pic}^0(C)$ such that $E \otimes M_1 \cong E_2 \otimes M_2$, where E_2 is the so-called Atiyah bundle from Theorem 4.3. Then E_2 sits in a nonsplit exact sequence as follows

$$0 \to \mathcal{O}_C \to E_2 \to \mathcal{O}_C \to 0.$$

If $M := M_2 \otimes M_1^*$, we obtain $E \cong E_2 \otimes M$ and tensoring this sequence by M, gives a short exact sequence

$$0 \to M \to E \to M \to 0.$$

□

The following proposition contains the odd degree case.

Proposition 4.6. *On a curve, C, of genus* 1*, given a line bundle L of odd degree, there exists, up to isomorphism, a unique indecomposable rank* 2 *vector bundle E with* $\det E \cong L$*.*

We refer to [9] Proposition 10.47 for the proof.

Theorem 4.7. *For each integer n, there is a one-to-one correspondence between the set of isomorphism classes of indecomposable vector bundles of rank* 2 *and degree n on the elliptic curve C, and the set of points on C.*

Sketch of correspondence We will denote by $\mathrm{Pic}^n(C)$, the set of degree n line bundles on C. Recall from [7], Theorem 20, that there is an isomorphism of manifolds $C \cong \mathrm{Pic}^0(C)$ and in fact ([7], Theorem 21) there is an isomorphism $C \cong \mathrm{Pic}^n(C)$ for all $n \in \mathbb{Z}$.

Now let E be an indecomposable rank 2 vector bundle of degree n on C. If n is odd, from Proposition 4.6, we know that there is a unique indecomposable rank 2 vector bundle E of degree n, with $\det E \cong L$. Hence use $\mathrm{Pic}^n(C) \cong C$ to obtain the result.

If n is even from Theorem 4.3 we know there exists, L, a line bundle of degree zero, unique up to isomorphism such that $E \otimes L$ is isomorphic to the unique nontrivial extenstion of $\mathcal{O}_C$ by $\mathcal{O}_C$. Since $\operatorname{Pic}^0(C) \cong C$ again we obtain the result.

5. Stability

The notion of stability comes from the theory of moduli spaces. The variety, $\operatorname{Pic}^0(C)$ with the Poincaré bundle, of degree 0 line bundles on an elliptic curve (See [7] Section 6) is an example of a moduli space. Loosely described a moduli space is an algebraic variety which parametrises the set of equivalence classes of some objects. For example we could consider the moduli space of rank two vector bundles on an elliptic curve, C. It turns out that the set of isomorphism classes of vector bundles of rank 2 and degree d on an elliptic curve is unbounded (briefly, this means that we can find families of arbitrarily high dimension which gives us vector bundles of rank 2 and degree d. See [6] Chapter 1), which poses a problem when constructing the corresponding moduli space. To overcome this problem we restrict our study of vector bundles. One form of restriction is to study 'stable' vector bundles. Using stable bundles, one to construct the moduli space of (stable) vector bundles of rank 2 and degree d on C.

We will begin by giving a more explicit definition of a subbundle and quotient vector bundle.

Definition 5.1. Let F and E be vector bundles of rank r and n respectively, with $r \leq n$ and $F \subset E$ is a submanifold. Then, F is called a *subbundle* of E if there exists an open covering $\{U_i\}$ and transition functions $g_{ij} : U_i \cap U_j \to \mathrm{GL}(r, \mathbb{C})$ for F and $h_{ij} : U_i \cap U_j \to \mathrm{GL}(n, \mathbb{C})$ for E such that

$$h_{ij}(x) = \begin{pmatrix} g_{ij}(x) & * \\ 0 & f_{ij}(x) \end{pmatrix}.$$

The *quotient bundle* $G = E/F$ is described by transition functions f_{ij}.

Now we are ready to define the stability of a vector bundle.

Definition 5.2. A vector bundle, E on a curve, is *stable* (resp. *semi-stable*) if every nonzero vector subbundle $F \subset E$ satisfies

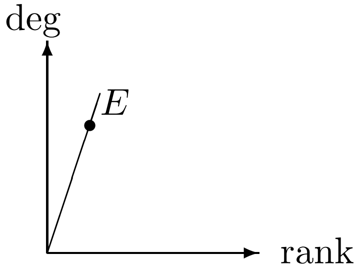
$$\frac{\deg F}{\operatorname{rk} F} < \frac{\deg E}{\operatorname{rk} E} \quad (\textit{resp.} \leq).$$

(Or equivalently, we can also say that a vector bundle E is stable (resp. semi-stable) if $\frac{\deg G}{\operatorname{rk} G} > \frac{\deg E}{\operatorname{rk} E}$ (resp. $\geq$) for every non-zero quotient G of E).

From this definition we can see that a vector bundle E of $\operatorname{rk} 2$ is stable (resp. semi-stable) if every line subbundle $F \subset E$ satifies

$$\deg F < \frac{1}{2} \deg E \quad (resp. \leq).$$

We call the rational number $\frac{\deg E}{\operatorname{rk} E}$ the *slope* of E. The picture below illustrates the reason for this name.



The definition of stability above is often referred to as slope-stability.

Lemma 5.3. *Let E be a vector bundle of rank 2. If $\deg E$ is odd, then stability and semi-stabilty are equivalent.*

Proof. Clearly if E is stable, then E is semi-stable. For the other direction, we assume E is semi-stable with degree n. Now let $F \subset E$ be a nonzero subbundle of E, so $\deg F \leq \frac{n}{2}$. Since $\deg F$ is an integer, $\deg F \neq \frac{n}{2}$ as n is odd. Hence $\deg F < \frac{n}{2}$, i.e. E is stable. □

Lemma 5.4. *If E_1 and E_2 are semi-stable , and $\frac{\deg E_1}{\operatorname{rk} E_1} > \frac{\deg E_2}{\operatorname{rk} E_2}$, then* $\operatorname{Hom}(E_1, E_2) = 0$

Proof. Let $f : E_1 \to E_2$ be a morphism, and let $F \subset E_2$ be it's image. Since E_2 is semi-stable, if $F \neq 0$, then $\frac{\deg F}{\operatorname{rk} F} \leq \frac{\deg E_2}{\operatorname{rk} E_2}$. But E_1 is semi-stable and F is a quotient of E_1, and therefore $\frac{\deg E_1}{\operatorname{rk} E_1} \leq \frac{\deg F}{\operatorname{rk} F}$, a contradiction unless $F = 0$. □

5.1. **Jordan-Hölder filtrations.** Consider a rational number μ and let $C(\mu)$ denote the category of semi-stable vector bundles of slope μ. This turns out to be an abelian category (See [8] Chapter 5 for more details). This allows us to define Jordan-Hölder filtrations for each semi-stable bundle: these filtrations are important in order to understand the points of the moduli space of stable vector bundles of rank 2 and degree d (or indeed any fixed rank and degree).

Definition 5.5. Let E be a semi-stable vector bundle of slope μ. A Jordan-Hölder filtration of E is a filtration of vector subbundles

$$0 \subset E_1 \subset E_2 \subset \cdots \subset E_k = E$$

in $C(\mu)$ such that the quotient $\mathrm{gr}_i = E_i/E_{i-1}$ is a stable bundle in $C(\mu)$. The integer k is called the *length* of the filtration and the direct sum $\bigoplus_i \mathrm{gr}_i$ is called the *associated grading.*

Let us now see how to get such a filtration. Consider first if E is stable, i.e. $\forall E_i \subset E, \mu(E_i) < \mu(E)$. In this case, the filtration is clear. Namely

$$0 \subset E_1 = E$$

Now we consider when E is strictly semi-stable, then there exists subbundles in $C(\mu)$ and one of these, E_1 must be stable. If not then we can construct an infinite descending sequence of subbundles in $C(\mu)$ in which the rank strictly decreases but this is impossible as the rank of nonzero subbundles of E is bounded below by 1. So E/E_1 is also in $C(\mu)$ and we can continue the construction until we obtain our filtration as above.

5.2. **Harder-Narasimhan filtrations.**

Lemma 5.6. *(a) Let $d, d', r, r' \in \mathbb{Z}$ with $r, r' > 0$.*

(i) If $\frac{d}{r} > \frac{d'}{r'}$, then $\frac{d}{r} > \frac{d+d'}{r+r'} > \frac{d'}{r'}$.

(ii) If $\frac{d}{r} = \frac{d+d'}{r+r'}$ or $\frac{d'}{r'} = \frac{d+d'}{r+r'}$ then $\frac{d}{r} = \frac{d'}{r'}$.

(b) Let $0 \to E' \to E \to E'' \to 0$ be a short exact sequence of nonzero vector bundles on X.

(i) If $\lambda \in \mathbb{R}$ such that $\mu(E') \leq \lambda$ and $\mu(E'') \leq \lambda$, then $\mu(E) \leq \lambda$.

(ii) If $\mu(E') = \mu(E)$ or $\mu(E) = \mu(E'')$ then $\mu(E') = \mu(E'')$.

(c) If

$$0 = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_n = E$$

is a filtration by subbundles of E such that $\mu(E_i/E_{i-1}) \leq \lambda$ for all $i = 1, \ldots, n$:

(i) then $\mu(E_i) \leq \lambda$ for all $i = 1, \ldots, n$. In particular, $\mu(E) \leq \lambda$.

(ii) If, for at least one i, we have $\mu(E_i/E_{i-1}) < \lambda$, then $\mu(E) < \lambda$.

Proof. (a) The proof of this is a simple calculation.

(b) Because of the fact that $\mathrm{rk}(E) = \mathrm{rk}(E') + \mathrm{rk}(E'')$ and $\deg(E) = \deg(E') + \deg(E'')$, this follows immediately from (a).

(c) This follows from (b) using exact sequences

$$0 \to E_{i-1} \to E_i \to E_i/E_{i-1} \to 0$$

for all $i = 2, \dots n$. □

Each vector bundle admits a canonical increasing filtration whose successive quotients are semi-stable. This allows us to classify bundles which are not semi-stable in terms of semi-stable bundles.

Proposition 5.7. *Let E be a vector bundle on a curve X. Then E has an increasing filtration by vector subbundles*

$$0 = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_k = E$$

where the quotient $\mathrm{gr}_i = E_i/E_{i-1}$ satisfies the following conditions:

(1) *the quotient gr_i is semi-stable;*
(2) *$\mu(\mathrm{gr}_i) > \mu(\mathrm{gr}_{i+1})$ for $i = 1, \cdots, k-1$.*

Proof. ([8] Proposition 5.4.2) If E is already semi-stable then the result is trivial. Assume, therefore that E is not semi-stable. We will prove this by induction on the rank of E. If $\mathrm{rk}(E) = 1$, then the result is trivial as all line bundles are automatically stable. Now assume $\mathrm{rk}(E) \geq 2$. We know, from Lemma 2.23, that the degree of all subbundles of E is bounded above. On the other hand, subbundles can only have ranks $1, 2, \dots, \mathrm{rk}(E) - 1$, hence the slope of the subbundles of E is bounded above. Among all the subbundles of maximal slope, let E_1 be the one of maximal rank. Then E_1 is semi-stable because it has maximal slope. Let $E' = E/E_1$, then we have the following short exact sequence:

$$0 \to E_1 \to E \to E' \to 0$$

where $\mathrm{rk}(E') < \mathrm{rk}(E)$.

By inductive assumption E' has an increasing filtration satisfying the conditions of the proposition, i.e.

$$0 \subset F_2 \subset F_3 \subset \cdots \subset F_k = E'$$

with

$$\mu(F_2) > \mu(F_3/F_2) > \cdots > \mu(F_k/F_{k-1})$$

and F_j/F_{j-1} is semistable for $2 \leq j \leq k$. In particular, F_2 is semistable.

Let $E_j \subset E$ be the preimage of $F_j \subset E'$ under $E \to E'$. This way we obtain commutative diagrams with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & E_1 \arrow[r] & E_{j+1} \arrow[r] & F_{j+1} \arrow[r] & 0 \\
0 \arrow[r] & E_1 \arrow[r] \arrow[u, equal] & E_j \arrow[r] \arrow[u, hook] & F_j \arrow[r] \arrow[u, hook] & 0.
\end{tikzcd}$$

Hence $E_{j+1}/E_j \cong F_{j+1}/F_j$ are semistable.

Now we need to prove $\mu(F_2) < \mu(E_1)$, in order to show condition 2 holds. Since E_1 has maximal slope, $\mu(E_2) \leq \mu(E_1)$. Moreover, since E_1 has maximal rank among the subbundles with slope $\mu(E_1), \mu(E_2) < \mu(E_1)$. From the diagram above we know that $\deg(F_2) = \deg(E_2) - \deg(E_1)$ and $\mathrm{rk}(F_2) = \mathrm{rk}(E_2) - \mathrm{rk}(E_1)$. So we know $\mu(F_2) = \frac{\deg(E_2)-\deg(E_1)}{\mathrm{rk}(E_2)-\mathrm{rk}(E_1)}$. We can also write this as $\mu(F_2) = \frac{\mathrm{rk}(E_2)\mu(E_2)-\mathrm{rk}(E_1)\mu(E_1)}{\mathrm{rk}(E_2)-\mathrm{rk}(E_1)}$. Then we have

$$\frac{\mathrm{rk}(E_2)\mu(E_2) - \mathrm{rk}(E_1)\mu(E_1)}{\mathrm{rk}(E_2) - \mathrm{rk}(E_1)} < \frac{\mathrm{rk}(E_2)\mu(E_1) - \mathrm{rk}(E_1)\mu(E_1)}{\mathrm{rk}(E_2) - \mathrm{rk}(E_1)}$$

i.e. $\mu(F_2) < \mu(E_1)$. Now since $E_2/E_1 = F_2$, we have $\mu(E_1) > \mu(E_2/E_1)$. We can the repeat the process until we obtain a quotient E/E_{k-1} which is semi-stable. □

Lemma 5.8. *If*

$$0 = E_0 \subset E_1 \subset \cdots \subset E_n = E$$

is a filtration of E satsifying the conditions of Proposition 5.7 above and $E' \subset E$ is a nontrivial subbundle of E then $\mu(E') \leq \mu(E_1)$ and if $\mu(E') = \mu(E_1)$, then $E' \subset E_1$.

Proof. We define a filtration of E' by $E'_i := E' \cap E_i$ for all $i = 1, \dots, n$. Because $E'_i = E_i \cap E'_{i+1}$ we obtain $E'_{i+1}/E'_i \subset E_{i+1}/E_i$ for $i = 1, \dots, n-1$. Now since E_{i+1}/E_i is semistable, we have either $\mu(E'_{i+1}/E'_i) \leq \mu(E_{i+1}/E_i)$ or $E'_{i+1} = E'_i$. Because $\mu(E_{i+1}/E_i) \leq \mu(E_1)$ for $i = 1, 2, \dots, n-1$, we obtain from Lemma 5.6 (c) that $\mu(E') \leq \mu(E_1)$. Now if $i \geq 1$ and $E'_{i+1} \neq E'_i$ then $\mu(E'_{i+1}/E'_i) \leq \mu(E_{i+1}/E_i) < \mu(E_1)$. Hence by Lemma 5.6 (c) again, if $\mu(E') = \mu(E_1)$ we must have $E'_{i+1} = E'_i$ for $i = 1, 2, \dots, n-1$, i.e. $E' \subset E_1$. □

Proposition 5.9. *This filtration of Proposition 5.7 is unique.*

Proof. ([8] Proposition 5.4.2) Assume $(E_i)_{i=1,\dots,n}$ and $(F_j)_{j=1,\dots,m}$ are two filtrations of E satisfying the conditions of Proposition 5.7 above. Now using the notation of Lemma 5.8 if we let $E' := F_1$ we get $\mu(F_1) \leq \mu(E_1)$. Similarly if we allow $E' := E_1$, we get $\mu(E_1) \leq \mu(F_1)$. Clearly then, $\mu(F_1) = \mu(E_1)$.

Lemma 5.8 again implies $E_1 \subset F_1$ and $F_1 \subset E_1$, hence $E_1 = F_1$. Using E/E_1 and F/F_1 we can proceed by induction as in the proof of Proposition 5.7 to conclude that the filtration is unique. □

The filtration of Proposition 5.7 is called the *Harder-Narasimhan filtration* of E.

6. Conclusion

In conclusion, it is fair to say that the theory of vector bundles is vast and indeed very interesting. We have seen how vector bundles on $\mathbb{P}^1$ are not very complex, in the sense that they can be written as a direct sum of line bundles. We have also seen a classification for indecomposable rank 2 vector bundles on elliptic curves.

One could also go on to study higher rank vector bundles on elliptic curves or on curves of a higher genus, or even on higher dimensional complex manifolds. These are all very interesting in their own right.

In Section 5, we studied slope stability for vector bundles on curves. As was mentioned, stable bundles are required when constructing moduli spaces of vector bundles. For the reader interested in stability, from here you could go on to study Bridgeland stability conditions ([2] and [3]) and the space of all stability conditions on a particular complex manifold (e.g. an elliptic curve).

References

[1] M. F. Atiyah: *Vector bundles over an elliptic curve*, Proc. London Math. Soc. (3) 7 (1957) 414-452.

[2] T. Bridgeland: *Stability Conditions on Triangulated Categories*, preprint arXiv:math.AG/0212237.

[3] T. Bridgeland: *Spaces of Stability Conditions*, arXiv:math.AG/0611510.

[4] A. Gathmann: *Algebraic Geometry*, Notes for a class taught at the University of Kaiserslauten (2002/2003) available at http://www.mathematik.uni-kl.de/∼gathmann/class/alggeom-2002/main.pdf.

[5] R. Hartshorne: *Algebraic Geometry*, Graduate Texts in Mathematics, Springer, (1977).

[6] D. Huybrechts, M. Lehn: *The geometry of moduli spaces of sheaves* Aspects of Mathematics, E31. Friedr. Vieweg & Sohn, Braunschweig, (1997).

[7] M. Khalid: *Group law on the cubic curve*, this issue.

[8] J. Le Potier: *Lectures on Vector Bundles* Cambridge studies in advanced mathematics, Cambridge University Press (1997).

[9] S. Mukai: *An Introduction to Invariants and Moduli*, Cambridge studies in advanced mathematics, Cambridge University Press, (2003).

[10] C. A. Weibel: *An introduction to homological algebra*, Cambridge studies in advanced mathematics, Cambridge University Press, (1994).

Department of Mathematics, Mary Immaculate College, South Circular Road, Limerick, Co. Cork, Ireland

E-mail address: Ciara.Daly@mic.ul.ie