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

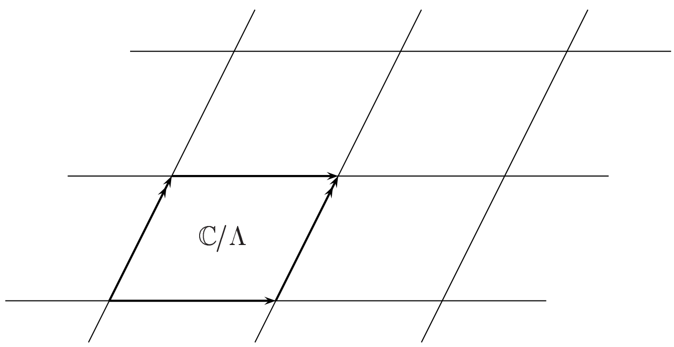
Throughout this article we work over $\mathbb{C}$, the field of complex numbers. We denote $\mathbb{P}^n(\mathbb{C})$ by $\mathbb{P}^n$.

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'.

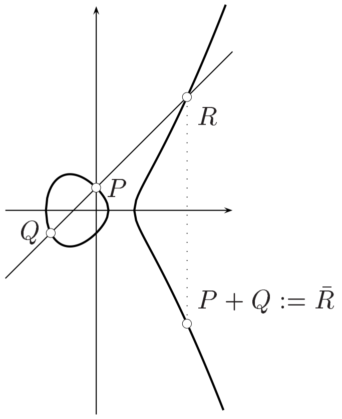
These notions of *smooth points* and *singular points* can also be extended to higher dimensional manifolds. In fact just as the implicit and inverse function hold in the differentiable case, so do their analytic versions. For example if V is a hypersurface given locally as the zero set of a single holomorphic 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.

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

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

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

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*)

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

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 $y^2 = 4x^3 - g_2x - g_3$, an elliptic integral (of the first kind) which is of particular importance, is

$$\int_O^P \frac{dx}{y}.$$

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

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

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 $f = \frac{z_0{}^2}{z_1{}^2 + z_0 z_1}$ 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

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

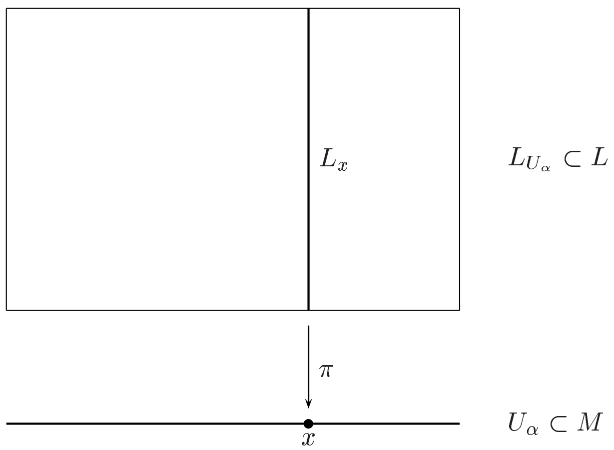
Note that we define the "patching" condition using z^2, the nowhere vanishing function on $V_0 \cap V_1$ relating the two local descriptions of D above.

This new manifold L is an example of a *line bundle* (Definition 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

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

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 $\operatorname{ord}_P s_\alpha = \operatorname{ord}_P s_\beta$, if $P \in U_\alpha \cap U_\beta$. We take the divisor (s) of s to be

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

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

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

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

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

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

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

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

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

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 $L = \{(z_0 : z_1 : z_2) \in \mathbb{P}^2 \mid l_0 z_0 + l_1 z_1 + l_2 z_2 = 0\}$. Then since z_2 is not identically zero on L the meromorphic function $F = \frac{l_0 z_0 + l_1 z_1 + l_2 z_2}{z_2}$ 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 $\tau^* f$ 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.

Acknowledgement: The author would like to thank Bernd Kreussler for organising the workshop "Elliptic curves" and the series of articles.

REFERENCES

[1] N. H. Abel, *Recherches sur les fonctions elliptiques*, J. reine angew. Math. 2, 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"*, 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.

Madeeha Khalid,
Department of Mathematics,
Institute of Technology Tralee,
Clash,
Tralee, Co. Kerry, Ireland
madeeha.khalid@staff.ittralee.ie

Received in final form on 23 August 2007.