THE ISOMORPHISM BETWEEN A TORUS TO CORRESPONDING ELLIPTIC CURVE

Abstract. An elliptic curve (EC) is a plane algebraic curve defined by an equation of the form $y^2 = x^3 + ax + b$. Using the theory of elliptic functions, it can be shown that elliptic curves defined over the complex numbers correspond to the embeddings of the torus into the complex projective plane. More precisely, there exists an isomorphism from a torus $\mathbb{C}/L$ to the elliptic curve $y^2 = x^3 + ax + b$. We will present this connection between lattice and elliptic curves and give a sketch of proof.

1. Introduction

As mentioned in the abstract, an elliptic curve is the zero set of some equation of the form $y^2 = x^3 + ax + b$ and we can plug in any number from the underlying field into a and b. In the scope of this talk, we have $a, b \in \mathbb{C}$. Then let's write down a specific example, for example, we can plug in $a = -1$ and $b = 0$ and we get an elliptic curve defined by

$$y^2 = x^3 - x. \tag{1.1}$$

This elliptic curve is isomorphic to a complex lattice L and to understand this connection, we need some knowledge of elliptic functions and Weierstrass p function $\wp$.

2. Lattice and Weierstrass P Function

We begin with the definition of a lattice in the complex plane.

Definition 2.1. A lattice $L = [w_1, w_2]$ is an additive subgroup $= w_1\mathbb{Z} + w_2\mathbb{Z}$ of $\mathbb{C}$ generated by complex numbers w_1 and w_2 that are independent over $\mathbb{R}$.

Definition 2.2. An elliptic function for a lattice L is a complex function $f(z)$ such that f is meromorphic and periodic with respect to L.

The total number of poles of an elliptic function is called its order and every elliptic function of order m has m zeros in P_0. Then we can define the Weierstrass $\wp$-function of a lattice, which is an elliptic function.

Definition 2.3. The Weierstrass $\wp$-function of a lattice L is defined by

$$\wp(z) = \frac{1}{z^2} + \sum_{w \in \Lambda^*} [\frac{1}{(z+w)^2} - \frac{1}{w^2}]. \tag{2.4}$$

It's clear from definition that this $\wp(z)$ has a pole of order 2 at each lattice point and in fact it is actually holomorphic at every other point. Furthermore, if we assume the lattice has period 1 and τ, we can prove that $\wp$ is an elliptic function with period 1 and τ. We gather this result in a theorem:

Theorem 2.5. *The function $\wp$ is an elliptic function that has periods 1 and τ, and double poles at the lattice points.*

Proof. To prove this, we look at the derivative $\wp'$:

$$\wp'(z) = -2 \sum_{n,m\in\mathbb{Z}} \frac{1}{(z+n+m\tau)^3}. \tag{2.6}$$

Notice that the differentiated series converges absolutely whenever z is not a lattice point and $\wp'$ is clearly doubly periodic with periods 1 and τ. Hence there exist two constants a and b such that

$$\wp(z+1) = \wp(z); \wp(z+\tau) = \wp(z). \tag{2.7}$$

By definition of $\wp$, it is even and if we plug in $z = -1/2$ and $-\tau/2$, immediately we have $a = b = 0$. □

3. Isomorphism between Lattice and Elliptic Curves

We will then construct the isomorphism between lattice and our elliptic curve using the Weierstrass $\wp$ function but at first we need to further analyze the properties of $\wp$.

Since $\wp'$ is odd by the fact that $\wp$ is even, we know that $\wp'$ has three zeroes $1/2, \tau/2$ and $(1+\tau)/2$. $\wp'$ is elliptic and has order 3 so these are the only roots of $\wp'$ with multiplicity 1. Therefore if we define $e_1 = \wp(1/2)$, $e_2 = \wp(\tau/2)$ and $e_3 = \wp((1+\tau)/2)$, $\wp(z) = e_i$ has double roots at e_i nad no other solutions in the fundamental parallelogram. Also e_i are distinct since otherwise we'll have two double roots in the fundamental parallelogram. From these observations, we have the following theorem:

Theorem 3.1. $(\wp')^2 = 4(\wp - e_1)(\wp - e_2)(\wp - e_3)$.

Proof. Both sides have double roots at points $1/2$, $\tau/2$ and $(1+\tau)/2$ and poles of order 6 at lattice points. Consequently, there quotient is holomorphic and still doubly-periodic and hence constant by Liouville's theorem. By looking at z near 0, the constant is 4. □

Then return to our example, by plugging in $e_1 = 1$, $e_2 = -1$ and $e_3 = 0$, we notice that $(\wp(z), \wp'(z)/2)$ is a solution to our elliptic curve $y^2 = x^3 - x$ and thus the corresponding lattice L is a subset of the elliptic curve. The remaining task is to prove that this is an isomorphism, i.e, injective, surjective and preserves group structure, which is stated as the following theorem:

Theorem 3.2. *Let L be a lattice, and let E be the elliptic curve $y^2 = 4(x-e_1)(x-e_2)(x-e_3)$ over $\mathbb{C}$. The map $\Phi : \mathbb{C}/L \to E(\mathbb{C})$ that sends $z \in L$ to 0 and each other z to the affine point $(\wp(z), \wp'(z))$ on $E(\mathbb{C})$ is isomorphism between the additive group $\mathbb{C}/L$ and $E(\mathbb{C})$.*

The complete proof is beyond the scope of this talk and I will just mention several key points.

By previous theorem, every such points $(\wp(z), \wp'(z)) \in E(\mathbb{C})$.

To show surjectivity, given $(x_0, y_0) \in E(\mathbb{C})$, we look at the zeroes of $f(z) = \wp(z) - x_0$ and neither of these is 0, since f has a pole at 0. Further, we can show that one of these two zeroes is the preimage of (x_0, y_0).

To show injectivity, we prove by contradiction, suppose there exist $z_1 \neq z_2$ such that $\Phi(z_1) = \Phi(z_2)$ and assume that $, 2z_1, 2z_2$ are not lattice points. Then look at the zeros of $g(z) = \wp(z) - \wp(z_1)$ and thus z_2 should be one of them. By analyzing

the derivatives, we can show that the only possibility is $z_1 = z_2$.
This map preserves group structure is much harder to prove and really beyond this talk so I would just mention it is true here.

4. Application

Next I'll talk about some applications. I think the best part of this theorem is it enables us to examine both lattices from elliptic curves and elliptic curves from lattices. The fact that $E(\mathbb{C}) = \mathbb{C}/L$ enables us to compute the homology and cohomology group of $E(\mathbb{C})$ by simply computing the homology group of $\mathbb{C}/L$. Further since the quotient $\mathbb{C}/L$ can be identified as the torus $S^1 \times S^1$, we know that $H_0 = H_2 = \mathbb{Z}$ and $H_1 = \mathbb{Z}^2$. I basically use this as well as the Lefschetz fixed point theorem to analyze the cardinality of $E(\mathbb{F}_q)$ in a finite field $\mathbb{F}_q$. Besides, I read something like two lattices are homothetic if and only if their corresponding elliptic curves are isomorphic