Geometric Aspects of Elliptic Curves

The goal of this project is to understand some of geometric aspects of *Elliptic Curves*. This project has a close relation to the project on *Elliptic Functions* which describes the functions on these curves. In the end we hint at a relationship to the project on p-adic numbers.

1. If X and Y are topological spaces, we can give the product space $X \times Y$ the *product topology*. The topology on $X \times Y$ has as a basis the sets $U \times V$ where U is an open set in X and V is open in Y. This means that the open sets of $X \times Y$ are arbitrary unions of such $U \times V$.

   (a) Show that this does indeed define a topology on $X \times Y$.

   (b) Denote the projection maps:

   $$X \times Y \xrightarrow{\pi_X} X \qquad X \times Y \xrightarrow{\pi_Y} Y$$

   $$(x, y) \longmapsto x \qquad (x, y) \longmapsto y$$

   Show that these maps are continuous when $X \times Y$ is given the product topology.

   (c) Give $\mathbb{C}$ has the "ball" topology which has as a basis the open balls:

   $$B_r(z) := \{w \in \mathbb{C} \mid |w - z| < r\} \quad z \in \mathbb{C} r > 0$$

   Show that if we give $\mathbb{C} \times \mathbb{C}$ the product topology, then this is the same as the topology on $\mathbb{C} \times \mathbb{C}$ which has as a basis the open balls:

   $$B_r(\underline{z}) := \{\underline{w} = (w_1, w_2) \in \mathbb{C} \times \mathbb{C} \mid d(\underline{w}, \underline{z}) < r\} \quad \underline{z} = (z_1, z_2) \in \mathbb{C} \times \mathbb{C}$$

   where:

   $$d(\underline{w}, \underline{z}) := \sqrt{|w_1 - z_1|^2 + |w_2 - z_2|^2}$$

   is the distance function.

2. A *topological group* is a topological space G which is also a group. In particular, if we denote the multiplication of the group $G \times G \xrightarrow{m} G$ and the inverse map by $G \xrightarrow{\mathbf{inv}} G$ then we require that m and **inv** are continuous maps (here we give $G \times G$ the product topology.)

   Let $(\mathbb{C}, +)$ be the set of complex numbers with the group structure given by addition. Show that $(\mathbb{C}, +)$ is a topological group.

3. A subset W of a topological space X is called *discrete* if for every $w \in W$ there is an open subset U_w containing w and such that $U_w \cap W = \{w\}$.

   We will show that there are three types of *discrete subgroups* of $(\mathbb{C}, +)$:

- The trivial subgroup $(\{0\}, +)$.
- For $\omega \in \mathbb{C} \setminus \{0\}$ define the subgroup:

$$(\{a\omega \mid a \in \mathbb{Z}\}, +)$$

- For ω_1 and ω_2 be two points in $\mathbb{C} \setminus \{0\}$ which do not lie on the same line through the origin define the subgroup:

$$\Omega := \Omega(\omega_1, \omega_2) := \{a\omega_1 + b\omega_2 \mid a, b \in \mathbb{Z}\}$$

We call Ω a *lattice* in $\mathbb{C}$ and say that ω_1 and ω_2 *generate* Ω. (Draw a picture of this subgroup.)

Show that these are the only discrete subgroups as follows. Suppose that G is a discrete subgroup of $\mathbb{C}$ which is not the trivial subgroup.

(a) Show there is some $\omega_1 \in G$ so that $|\omega_1| \leq |\omega|$ for all $\omega \in G$.

(b) Let L be the line through the origin and ω_1. Show that $H := \{a\omega_1 \mid a \in \mathbb{Z}\}$ is a subgroup of G contained in L.

(c) Suppose that $G \subseteq L$. Then show $G = H$.

(d) Suppose that $G \not\subseteq L$. Then show that $G \setminus L$ has an element ω_2 so that $|\omega_2|$ is minimal, and then that $H' := \{a\omega_1 + b\omega_2 \mid a, b \in \mathbb{Z}\}$ is a subgroup of G. Conclude by showing $H' = G$

4. A *fundamental region* or *fundamental parallelogram* for a lattice Ω is a parallelogram of the form:

$$\{a + s\omega + t\omega' \mid 0 \leq s, t < 1\}$$

where $a \in \mathbb{C}$ is fixed and ω and ω' generate the lattice (often we take $a = 0$).

(a) Draw a picture of several different fundamental regions for the lattice generated by $(1, i)$.

(b) Show that there is exactly one lattice point in every fundamental region.

5. We have described a lattice by giving a pair of generators (ω_1, ω_2). Some, in fact many, choices of generators are *equivalent*: Two different sets of generators generate the same lattice.

(a) As an example show that the lattice generated by the pair of elements $(1, i)$ is the same as the lattice generated by any choice of signs for the pair $(\pm 1, \pm i)$. Find some other sets of equivalent generators and draw a fundamental region for each.

(b) Show that our notion of 'equivalence' on the set of pairs (ω_1, ω_2) is in fact an equivalence relation.

(c) Show that if $\Omega(\omega_1, \omega_2)$ is a lattice then the pair $(a\omega_1 + b\omega_2, c\omega_1 + d\omega_2)$ generates the same lattice if and only if $ad - bc = \pm 1$.

6. Let X be a topological space and $f : X \longrightarrow Y$ a function. We define the *induced* or *quotient* topology on Y by declaring a subset $U \subseteq Y$ to be open if and only if $f^{-1}(U)$ is open in X.

   Show that f is a continuous map for Y with the quotient topology.

7. Let Ω be a lattice in $(\mathbb{C}, +)$. Form the quotient:

   $$E := E(\Omega) := (\mathbb{C}, +)/\Omega$$

   (a) Show that E forms a group.

   (b) Describe/Draw a picture of E. (Hint: One of Homer Simpson's favorite foods)

   (c) Give E the quotient topology. Describe/Draw a picture of some the open sets.

   (d) Show that E is a topological group.

   E is called an *elliptic curve*. It has in fact more structure coming from the complex structure of $\mathbb{C}$, and we call this structure a *complex manifold*. You will be learning more about such things in your core classes this year. The natural functions of this structure correspond to *elliptic functions*.

8. Let Ω and Ω' be two lattices such that for some $\alpha \in \mathbb{C}$ we have $\alpha\Omega \subseteq \Omega'$.

   (a) Show that α induces a homomorphism of groups:

   $$\phi_\alpha : E \longrightarrow E'$$

   (b) Show that ϕ_α is a continuous map.

   (c) Show that if $\phi_\alpha = \phi_\beta$ then $\alpha = \beta$.

   If we knew a bit more about the complex manifold structure we could show that all such maps (group homomorphism which respect the complex manifold structure) arise this way.

9. We say that Ω and Ω' are *homothetic* if we have $\alpha\Omega = \Omega'$.

   Show that for Ω and Ω' homothetic we have two maps $\phi_\alpha : E \longrightarrow E'$ and $\phi_{\alpha^{-1}} : E' \longrightarrow E$ which gives an isomorphism of topological groups.

   Again, if we took time to develop the complex manifold structure, we could show that two lattices are homothetic if and only if the ϕ_α gives an isomorphism of the corresponding elliptic curves as complex manifolds.

   (a) Explain why we can think informally of homothety of lattices as a rotation and the use of a different measurement scale in $\mathbb{C}$. (Hint: What is the Euler form of a complex number?)

(b) Show that any lattice is homothetic to a lattice generated by $(1, \tau)$ with $\mathbf{Im}(\tau) \neq 0$.

(c) Use the equivalence relation to show that any lattice is homothetic to one generated by $(1, \tau)$ with $\mathbf{Im}(\tau) > 0$.

(d) Show that any lattice is is homothetic to to one generated by $(1, \tau)$ with $|\tau| \geq 1$ and $\mathbf{Im}(\tau) > 0$.

(e) Using the equivalent relation show that any lattice is now homothetic to one generated by $(1, \tau)$ with $|\tau| \geq 1$, $\mathbf{Im}(\tau) > 0$, and $\frac{-1}{2} \leq \mathbf{Re}(\tau) < \frac{1}{2}$

(f) Show that if such $|\tau| = 1$ we can further restrict τ so that $\frac{1}{2} \leq \mathbf{Re}(\tau) \leq 0$

(g) Describe/Draw a picture of the region of the τ obtained. **Memorize** this picture.

One can argue that if τ and τ' chosen from this region are distinct, then the corresponding elliptic curves are not homothetic. Thus this region *parameterizes* the set of elliptic curves.

10. Let E be an elliptic curve with identity/neutral element 0. Let $m \in \mathbb{Z}_{\geq 1}$ and consider the points:

$$E[\,m\,] := \{z \in E \mid \underbrace{z + z + \cdots + z}_{m-\text{times}} = 0\}$$

(a) Suppose the E comes from the lattice $(1, \tau)$. Illustrate the points $E[\,m\,]$ on a the fundamental parallelogram for $m = 3$ and $m = 9$.

(b) Show that the set $E[\,m\,]$ is a subgroup of E. What is its order?

(c) Suppose that we now have an elliptic curve E and choose a prime number l. (Yes, a prime number should be denoted p or q but trust me on this). Show that there is a natural group homomorphism:

$$E[\,l^{n+1}\,] \xrightarrow{[\,l\,]} E[\,l^n\,] \quad n \geq 0$$

(d) For $l = 3$ illustrate the maps $E[\,3\,] \xrightarrow{[\,3\,]} E[\,1\,] = \{0\}$ and $E[\,3^2\,] \xrightarrow{[\,3\,]} E[\,3\,]$ on a fundamental region. How many points are in the inverse image of a point of $E[\,1\,]$ or $E[\,3\,]$ under these maps?

These homomorphisms allows us to put together all of the points $E[l^n]$ into one gadget called the *Tate module* $T_l(E)$. This gadget is formed by taking the *inverse limit* and becomes a $\mathbb{Z}_l$-module (the l-adic integers). You may want to talk to one of the groups working on this p-adic numbers project.

A slight variant of this construction, coming from a more algebraic setting, gives information about really large Galois groups.