AN OVERVIEW OF ALGEBRAIC GEOMETRY THROUGH THE LENS OF ELLIPTIC CURVES

BRIAN OSSERMAN

Modern algebraic geometry, and particularly the technical underpinnings which frequently form the basis of an introductory course in schemes, is very much like a well-stocked machine shop with instructions in a foreign language. It would be easy to spend the entire year simply translating all the instructions for the different tools in the shop, but this would provide little indication of what the tools could be used for, and by extension, why people thought it was a good idea to invent them in the first place.

We will certainly spend a great deal of time on familiarizing ourselves with the language and basic tools of algebraic geometry, but we will also try to motivate this technical subject with some indication of how the tools can be applied to concrete and classical questions. The sheer scale of the subject mandates that we take many shortcuts along the way, but it is my hope that you will emerge with not only a mastery of the technical underpinnings of modern algebraic geometry, but with some intuition for these topics, as well as a sense of some of the central theorems and problems in the field.

1. Plane curves

We begin with an overview of a number of concepts of algebraic geometry through the very concrete lens of the study of plane curves, and elliptic curves in particular. Many of the concepts alluded to here will be returned to (with varying degrees of completeness) over the course of the year, while a few serve only as hints to what lies beyond the scope of the course.

In algebraic geometry, few objects are as basic as the plane curve. We start with a single polynomial equation $f(x, y) = 0$ in two variables, which we will assume for the sake of simplicity has coefficients in $\mathbb{Z}$, so that we can conveniently consider the curve as defined over $\mathbb{Q}$ or over $\mathbb{Z}/p\mathbb{Z}$ for any p. There are then immediately a range of questions one can ask about the plane curve defined as the set of solutions of this equation:

- What do the real points of the curve look like? The complex points?
- Does the curve have a point with coordinates in $\mathbb{Q}$?
- What can one say about the number of solutions over $\mathbb{Q}$? Over a number field? Over a finite field?

Generally, if $f(x, y)$ is linear or quadratic, these questions can be answered in a rather complete manner. However, the cubic case becomes much deeper, and is the subject of the theory of elliptic curves.

2. Weierstrass equations

For our purposes, we start with the following simple definition:

Definition 2.1. The curve defined by $f(x, y) = 0$ is an **elliptic curve** if $f(x, y)$ is of the form $y^2 - x^3 - ax - b$ for some a, b, and $\Delta := -16(4a^3 + 27b^2)$ is non-zero. We then say that $f(x, y)$ is in **Weierstrass form**.

Why this definition? Over a field of characteristic $\neq 2, 3$, any plane curve given by an irreducible cubic polynomial can always be put in the above form after appropriate change of variables for some a, b. The condition that $\Delta \neq 0$ is more interesting, and already provides an indication of the interplay between algebra and geometry which is so characteristic of algebraic geometry.

Over $\mathbb{R}$ or $\mathbb{C}$, it makes sense to ask whether the curve defined by $f(x, y) = 0$ gives a one-dimensional manifold. By the inverse function theorem, one can check that this is the case if and only if there is no point with

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

For a plane curve defined by $f(x, y) = 0$, if this property is satisfied we say it is **smooth** or **non-singular**. Otherwise, any point satifying the above simultaneous vanishings is called a **singularity** of the curve.

Warning 2.2. In general, the notions of smooth and non-singular are not equivalent, but they are closely related, and for the purposes of this introduction we will use them interchangeably.

One then checks:

Proposition 2.3. *For $f(x, y)$ in Weierstrass form, smoothness is equivalent to $x^3 + ax + b$ having distinct roots, which is equivalent to having $\Delta \neq 0$.*

Over $\mathbb{R}$, it is not hard to see that the only possibilities for a curve in Weierstrass form are: a connected smooth curves with branches going off to infinity; a smooth curve with one component homeomorphic to a circle, and the other having branches going off to infinity; a curve with a "node", i.e., a point at which it crosses itself; or a curve with a "cusp", where it has a sharp point. Because of the hypothesis that $\Delta \neq 0$, only the first two correspond to elliptic curves.

3. Real points and compactification

If we consider an elliptic curve over $\mathbb{R}$, it is immediately clear that whether we are in the connected or disconnected case, the points do not form a compact set, as there are always branches which "go to infinity". [Indeed, one distinguishing trait of algebraic geometry is that no algebraic variety of dimension at least 1 contained in any affine space is compact, when you look at its complex points] However, if we add a single "point at infinity", we can compactify the set, in which case the set of real points becomes homeomorphic to either one or two copies of the circle.

The way to accomplish this formally is to work not in the affine plane $\mathbb{A}^2$, but in the **projective plane** $\mathbb{P}^2$.

Informally, one may think of the projective plane as the affine plane together with one "point at infinity" for each line through the origin in the affine plane. A plane curve goes through a given "point at infinity" if it has a branch with slope approaching the slope of the corresponding line. In the case of an elliptic curve, we note that the unbounded branches both have slopes which approach vertical, so the unique point at infinity which we have to add is the one which corresponds to a vertical line.

More formally, we can think of the projective plane as having three homogeneous coordinates X, Y, Z, with the points of $\mathbb{P}^2$ corresponding to triples (X_0, Y_0, Z_0) with not all three values equal to 0, and considered up to simultaneous scaling. With this description, the affine plane could be the open subset with $Z_0 \neq 0$; on this subset, we can always scale so that $Z_0 = 1$, so we find that the points correspond to points $(x, y, 1)$, as they should. The points at infinity are then the points with $Z_0 = 0$.

In this context, we can replace the Weierstrass equation $f(x, y) = y^2 - x^3 - ax - b$ with its **homogeneous** equivalent $F(X, Y, Z) = Y^2Z - X^3 - aXZ^2 - bZ^3$. If we set $Z = 1$, we recover the original equation. If we consider this equation for $Z = 0$, we see that we have $X^3 = 0$, so (up to scaling), the only solution is $(0, 1, 0)$, which is the unique point at infinity of the elliptic curve.

We will introduce a notion of compactness, called **properness** that makes sense over any field (and indeed more generally). We will show that projective space is always proper, from which it will follow that any variety defined by equations in projective space is also proper.

However, we will have a notion of abstract variety which cannot necessarily be imbedded in projective space, so we could ask:

- Can every variety be compactified?

The affirmative answer to this question is a very non-trivial theorem of Nagata. An even more difficult question is:

- Can every smooth variety be compactified to a smooth variety?

This is closely related to the question of **resolution of singularities**. It was proved to be possible in characteristic 0 by Hironaka in the 1950's, for which he received a Fields medal. The same question in characteristic p is still open.

However, one checks that the point at infinity of an elliptic curve is always a smooth point, so for our situation, there are no difficulties, and we always obtain a smooth compactification, and we will from now on always mean this compactified curve (which is still determined by the polynomial $f(x, y)$) when we refer to an elliptic curve E.

4. Complex points

Since we can now think of an elliptic curve E as smooth and compact, if we study the complex points of E, we will obtain a compact, complex manifold of dimension 1. Any complex manifold is necessarily orientable (the complex structure fixes an orientation), so we have a compact, orientable surface, which is determined topologically by the number of holes, called the **genus**. We then have the following theorem, which follows from Weierstrass' study of analytic parametrizations of elliptic curves:

Theorem 4.1. *Every elliptic curve E has genus 1. In fact, as a complex manifold, E is isomorphic to $\mathbb{C}/\Lambda$ for some lattice Λ in the complex plane.*

Note that the map $\mathbb{C} \to \mathbb{C}/\Lambda \to E$ defined in terms of the Weierstrass $\wp$ function is complex analytic, but very far from being algebraic.

We will give a more general notion of genus which works for smooth compact curves over any field. The statement that an elliptic curve has genus 1 is then a special case of the **degree-genus formula**:

Theorem 4.2. *Let C be a smooth curve defined by a polynomial of degree d in the projective plane. Then C has genus given by $\frac{(d-1)(d-2)}{2}$.*

We notice that the set $\mathbb{C}/\Lambda$ naturally has the structure of an abelian group, inherited from the addition law on $\mathbb{C}$. This means that for any elliptic curves considered over $\mathbb{C}$, the points have an abelian group structure as well.

Given this version of the group law, it is quite easy to describe the **n-torsion points** of E, i.e., the points P such that $nP = 0$. If Λ is generated by τ_1, τ_2, then the n-torsion points are of the form $\frac{a}{n}\tau_1 + \frac{b}{n}\tau_2$, for $0 \leq a, b \leq n$, so we see that the subgroup of n-torsion points is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

5. Intersection theory and the group law

It is a remarkable fact that under the isomorphism $\mathbb{C}/\Lambda \xrightarrow{\sim} E$ of complex manifolds, the addition law on $\mathbb{C}/\Lambda$ gives rises to an *algebraically-defined* addition law on E. This law may be described intrinsically in terms of algebraic geometry using rudimentary **intersection theory**.

Suppose we have a line L in the plane. Our heuristic claim is as follows:

L intersects E in 3 points.

It is in fact true that L intersects E in at most 3 points. To make a precise statement that they intersect in exactly 3 points, we need to address three issues:

- L might miss E if we look at points over a non-algebraically closed field (e.g., $\mathbb{R}$);
- L intersects E in too few points if L happens to be vertical;
- L intersects E in too few points if L happens to be tangent to E.

The first point is easily addressed: we work over an algebraically closed field, such as $\mathbb{C}$ (in fact, we will be able to give a statement in the end which does not require this restriction, but the situation is quite special to elliptic curves). The second point is likewise simple to fix: we work in the projective plane, and note that when L is vertical, it also intersects E at the point at infinity. (This is one of many examples of objects being better-behaved when they are compact)

The third point is more substantive. In this case, it can be addressed on ad-hoc basis by saying if L is tangent to E at a point P, the intersection point should count for 2 or 3 points, depending on whether P is not an inflection points of E, or is an inflection point of E, respectively. More generally, for plane curves one can make a complicated set of geometric axioms for **intersection multiplicity**; see for instance [2, Thm. 3.18]. However, as we will see later, one of the great benefits of scheme theory (and particularly **non-reduced** schemes) is a very clean and simple definition of intersection multiplicity. In any case, once one has an appropriate definition of intersection multiplicity, our statement for lines and elliptic curves is a special case of Bezout's theorem:

Theorem 5.1. *Let C, D be distinct smooth curves in the projective plane, of degrees d, e, and defined over an algebraically closed field k. Then the number of points of $C \cap D$, counting multiplicity, is precisely $d \cdot e$.*

This is one of many examples of an application of a problem in **enumerative geometry** (in this case, counting the number of points in the intersection of two curves) to a problem having nothing to do with enumeration (constructing a group law on the set of points of an elliptic curve).

Given this, we can define an operation

$$* : E \times E \to E$$

by setting $P * Q$ to be the third point of intersection of E with the line L through P and Q (where if $P = Q$, we let L be the tangent line to E at that point).

If we denote by O the point at infinity of E, we can define the addition law

$$+ : E \times E \to E$$

by $P + Q := (P * Q) * O$. One then has:

Theorem 5.2. *The operation $+$ defines an abelian group law on E, with the identity element given by O, and the inverse of a point (x, y) given by $(x, -y)$.*

In fact, everything is easy to check except the associativity of the operation. Elementary proofs of associativity can be given either algebraically or geometrically, but either approach is rather Byzantine. There are however very elegant proofs which take a more sophisticated approach (see §10 below).

Furthermore, if points P, Q have coefficients in some field k, it is easy to check that $P * Q$, and hence $P + Q$, will have coefficients in k:

Lemma 5.3. *The group law on E makes $E(k)$, the points of E with coefficients in k, into a group, for any field k in which $\Delta(E) \neq 0$.*

One can also show:

Theorem 5.4. *The group law on $E(\mathbb{C})$ defined by intersection theory is the same as the group law on $E(\mathbb{C})$ defined by an isomorphism $\mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C})$ for some lattice Λ.*

From here, it is not hard to prove:

Corollary 5.5. *If k is an algebraically closed field contained in $\mathbb{C}$, then the subgroup of n-torsion points of $E(k)$ is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

This is a basic example of the usefulness of looking at the complex points of a curve, even if one is more fundamentally interested in what happens over, say, number fields.

6. Points over number fields

Generally some of the deepest and most difficult questions in (arithmetically-oriented) algebraic geometry involve understanding points over $\mathbb{Q}$, or more generally, over number fields. These topics are generally beyond what we will be able to cover this year, but provide such strong motivation for much of the modern theory of algebraic geometry that we would be remiss if we did not touch on them here.

The setup we have given for elliptic curve theory incorporates, in a sneaky way, the hypothesis that any elliptic curve E has a point defined over $\mathbb{Q}$, or in fact over any given field: namely, the point at infinity, which was $(0, 1, 0)$ in projective coordinates. However, it is quite possible not to have any other points over $\mathbb{Q}$, or to have infinitely many points, depending on the coefficients of the polynomial defined the curve.

Despite this variation, the group structure on the points allows a more systematic study of them. **Mordell's theorem** states:

Theorem 6.1. *Let E be an elliptic curve, and K a number field. The abelian group $E(K)$ of points of E over K is finitely generated.*

Mordell also made a conjecture, later proved by Faltings (in a paper of less than 20 pages for which he was awarded a Fields medal):

Theorem 6.2. *(***Mordell conjecture-Faltings' theorem***) Let C be a curve of genus at least 2, defined over a number field K. Then the number of points of C defined over K is finite.*

7. Points over finite fields

Let E be an elliptic curve, and p a prime such that $\Delta(E)$ is non-zero modulo p, so that we can consider E as an elliptic curve over $\mathbb{F}_p$. For any r, we have that E can only have finitely many points over the finite field $\mathbb{F}_{p^r}$, and we denote the number of such points (including the point at infinity) by $N_r(E)$. It is a rather remarkable fact that for any given elliptic curve E, the first $N_1(E)$ determines $N_r(E)$ for all r.

Following E. Artin, we encode the data of all the $N_r(E)$ by defining the zeta function associated to E (as a curve over $\mathbb{F}_p$) by the formula

$$Z_E(t) = \exp\left(\sum_{r=1}^{\infty} N_r(E)\frac{t^r}{r}\right).$$

(This definition may appear *ad hoc*, but in fact is strongly motivated by the Riemann and Dedekind zeta functions, and (if one sets $t = p^{-s}$) is a special case of the zeta function associated to a global field, which generalizes all of them simultaneously)

One can then show:

Theorem 7.1. *$Z_E(t) = \frac{1-a_E t+pt^2}{(1-t)(1-pt)}$, where $a_E := p + 1 - N_1(E)$.*

One also has the Riemann hypothesis for elliptic curves, which (after adjusting for the fact that our variable t should really be q^{-s}) states that the roots of $Z_E(t)$ have norm $\sqrt{p}$. It is elementary to check that this is equivalent to the assertion that

$$|a_E| \leq 2\sqrt{p},$$

which was conjectured by Artin and proved by Hasse:

Theorem 7.2. *For any elliptic curve E over $\mathbb{F}_p$, we have*

$$|p + 1 - N_1(E)| \leq 2\sqrt{p}.$$

We note if we suppose that as x varies over $\mathbb{F}_p$, the values of $x^3 + ax + b$ varies uniformly over squares and non-squares of $\mathbb{F}_p$, we obtain the estimate that $N_1(E)$ should be roughly $p+1$, so we see that the Riemann hypothesis for elliptic curves is equivalent to a bound on the deviation of the number of points from the expected value, much as the classical Riemann hypothesis is equivalent to a bound on the deviation of the number of primes from the value predicted by the prime number theorem.

Finally, we mention that the above description of the properties of a zeta function of an elliptic curve were generalized by Weil to arbitrary curves, and he also made conjectures in the case of higher-dimensional varieties, known as the Weil conjectures. A basic observation is that the $\mathbb{F}_{p^r}$ points of a variety are the fixed points of the rth power of the Frobenius map, so the idea which started with Weil

and was further developed by Grothendieck was to invent a cohomology theory which behaves like singular cohomology for varieties over $\mathbb{C}$, but works for varieties over any field. One could then apply tools like the Lefschetz fixed-point theorem to study the number of points over $\mathbb{F}_{p^r}$. These ideas were finally developed into the theory of **etale cohomology**, and used by Deligne to prove the Weil conjectures. Deligne won a Fields medal for his troubles, Grothendieck having already won one. See [1, Appendix C] for further discussion.

8. Plane imbeddings and the Brill-Noether problem

We defined an elliptic curve as a plane cubic, and stated that every plane cubic has genus 1. Accepting for the moment that there is an idea of an abstract algebraic curve, and a definition of genus for such curves, we can invert the question as follows:

Question 8.1. Does every curve of genus 1 have an imbedding in the plane?

(Note that by the degree-genus formula, such an imbedding is necessarily of degree 3)

In fact, the answer to this is yes, as can be proved easily by the **Riemann-Roch theorem** (see [1, Prop. IV.4.6]), using the tools of **sheaf cohomology**.

It is frequently useful to have an explicit representation of a curve inside some projective space (indeed, we have used our explicit Weierstrass form for elliptic curves repeatedly, for instance in defining the group law using intersections with lines). This motivates the following generalization of the previous question:

Question 8.2. For what triples (g, r, d) does every curve of genus g have a map to $\mathbb{P}^r$ of degree less than or equal to d?

This is known as the **Brill-Noether problem**, and the answer, although usually called the Brill-Noether theorem, was not completely proved until a 1980 paper of Griffiths and Harris, building on earlier work of Castelnuovo, Kleiman, and others:

Theorem 8.3. *Given a triple (g, r, d) as in the above question, every curve of genus g has a map to $\mathbb{P}^r$ of degree at most d if and only if $(r+1)(d-r) - rg \geq 0$.*

9. Isomorphisms and automorphisms

Another very natural question begins with the observation that we have described elliptic curves in terms of their equations in the plane, and not as abstract curves. One might therefore wonder whether there are different plane curves which we ought to consider to be equivalent, and if so, what the right notion of **isomorphism** should be.

The way in which we have normalized our equations rule out certain kinds of obvious changes of variable: for instance, we can't simply translate the x or y coordinates without taking $f(x, y)$ out of Weierstrass form. However, if we scale the coordinates appropriately, we can get a new equation: for a given a, b, if we choose any c, we see that the equation $y^2 = x^3 + c^4ax + c^6b$ is related to $y^2 = x^3 + ax + b$ by scaling x, y and dividing through by c^6.

In fact, there is an abstract notion of an isomorphism of curves, and if we further impose the condition that the point at infinity be sent to itself (a necessary condition if, for instance, we want to obtain a homomorphism of the group of points), the above-described isomorphisms turn out to be the only ones. It is a remarkable fact that any isomorphism (and more generally, any morphism, as long as it

sends the point at infinity to itself) between two elliptic curves will induce a group homomorphism.

However, there is a relatively simple invariant for determining whether two elliptic curves are isomorphic:

Definition 9.1. The j-invariant of an elliptic curve $y^2 = x^3 + ax + b$ is given by

$$j(E) := 1728\frac{4a^3}{4a^3 + 27b^2}.$$

One then checks easily the following:

Proposition 9.2. *Let k be an algebraically closed field. Two elliptic curves over k are isomorphic (over k) if and only if they have the same j-invariant.*

This fails over a non-algebraically closed field, because sometimes an isomorphism between two curves defined over k is only defined over some extension of k.

Example 9.3. (Quadratic twists) Let E be an elliptic curve given by an equation $y^2 = x^3 + ax + b$ over a non-algebraically closed field k, and let $c \in k$ be any element not a perfect square in k. Then we can make another curve E_c over k, called a **quadratic twist** of E, by the equation $cy^2 = x^3 + ax + b$, or appropriately rescaled, $y^2 = x^3 + c^2ax + c^3b$. This is isomorphic to E over $k(\sqrt{c})$, but not over k.

However, as long as we work over an algebraically closed field, the notion of j-invariant works quite well, suggesting that we should think of elliptic curves being parametrized by the affine line, which gives us a first example of a **moduli space**, i.e., a situation where a certain set of algebro-geometric objects are naturally parametrized in some sense by an algebraic variety. We can even write down a "universal curve" over almost the entire affine line:

$$y^2 = x^3 - \frac{27j}{4(j - 1728)}x - \frac{27j}{4(j - 1728)}.$$

One checks that this has j-invariant j, and discriminant $\Delta = -1728 \cdot 27^3 \frac{j^2}{(j-1728)^3}$, so gives a valid elliptic curve for $j \neq 0, 1728$.

It is not a coincidence that there are two j-values for which the universal family doesn't work: $j = 0$, and $j = 1728$, corresponding to the curves $y^2 = x^3 + 1$ and $y^2 = x^3 - x$ respectively. What makes these curves special? At first blush, it may look unrelated, but we turn to the notion of **automorphisms** (isomorphisms from the curve to itself) for the answer. One can easily see that these two curves have "extra automorphisms", in the following sense: any elliptic curve has a natural automorphism which sends $(x, y) \mapsto (x, -y)$. On the level of groups, this corresponds to sending each point to its inverse. However, while most elliptic curves have only this single non-trivial automorphism, we see that the special curves above have addition automorphisms, at least over suitable quadratic extensions of $\mathbb{Q}$.

Example 9.4. Over $\mathbb{Q}(\omega)$, with ω a cube root of unity, the curve $y^2 = x^3 + 1$ has the additional automorphisms (of order 3) given by $(x, y) \mapsto (\omega x, y)$ and $(x, y) \mapsto (\omega^2 x, y)$, so the group of automorphisms has order 6.

Over $\mathbb{Q}(i)$, the curve $y^2 = x^3 - x$ has the additional automorphism given by $(x, y) \mapsto (-x, iy)$, so the group of automorphisms has order 4.

While the relationship between automorphisms and moduli spaces is deep and somewhat subtle, for now we suffice it to assert that it is precisely, in a way that can be made fully rigorous, the fact that these two curves have extra automorphisms that prevents the universal curve above from being extended to cover these two cases. Furthermore, it is the omnipresence of the automorphism sending each point to its inverse for every elliptic curve that is responsible for the phenomenon of the quadratic twists discussed above, which prevent the j-invariant from fully classifying curves over non-algebraically closed fields.

10. Line bundles

Finally, we discuss another a different type of moduli problem, that of line bundles on an elliptic curve. This is a slightly more technical topic, so we will be a bit vaguer with definitions, although they will not be hard to make precise later. For the purposes of this section, we will think of elliptic curves as abstract curves (i.e., if they are over $\mathbb{C}$, as compact complex manifolds of dimension and genus 1) over a given algebraically closed field k.

Let E be such an elliptic curve. A **line bundle** L on E associates a line to every point of E; more precisely, L is an algebraic variety with a map $L \to E$ such that the preimage of every point is isomorphic to the affine line $\mathbb{A}^1_k$, and moreover, such that there is an open cover $\{U_i\}$ of E such that the preimage of each U_i is isomorphic to $U_i \times \mathbb{A}^1_k$. If we fix isomorphisms $L|_{U_i} \cong U_i \times \mathbb{A}^1_k$ for each i, then for each i, j we have a nowhere-vanishing **transition function** $\varphi_{i,j}$ on $U_i \cap U_j$ obtained by the composition

$$\begin{aligned}(U_i \cap U_j) \times \mathbb{A}^1_k = (U_i \times \mathbb{A}^1_k)_{U_i \cap U_j} &\cong (L|_{U_i})|_{U_i \cap U_j} \\ &= (L|_{U_j})|_{U_i \cap U_j} \cong (U_j \times \mathbb{A}^1_k)_{U_i \cap U_j} = (U_i \cap U_j) \times \mathbb{A}^1_k.\end{aligned}$$

Conversely, given transition functions (satisfying a cocycle condition) we can construct a line bundle.

The set of line bundles on E have a natural group structure, given by tensor product. On the level of transition functions, assumed we have two line bundles presented with respect to a given cover $\{U_i\}$ (which is always possible by taking a common refinement), we take the tensor product simply by multiplying together the transition functions for each line bundle. The resulting group is called the **Picard group**, and denoted by $\mathrm{Pic}(E)$.

The **trivial line bundle** $E \times \mathbb{A}^1_k$ has all transition functions equal to 1, so is the identity for this group law.

Remark 10.1. Note to aspiring number theorists: the definition of Picard group can be generalized to more general schemes, and when one applies it to rings of integers, one recovers the ideal class group.

It turns out that line bundles have a natural integer associated to them, called the **degree**, which is additive under the group structure, so that the subset $\mathrm{Pic}^0(E)$ of line bundles of degree 0 is in fact a subgroup of $\mathrm{Pic}(E)$. We leave the definition of degree until we have discussed divisors more generally. However, the following fact is key:

Theorem 10.2. *Let L be a line bundle of degree 0 on an elliptic curve E. Then either L is trivial, or L has a section s, which is unique up to scaling, such that:*

- *s is defined away from the point at infinity;*
- *s has a single, simple zero at a point P_L.*

Thus, for each non-trivial line bundle of $\mathrm{Pic}^0(E)$, we get a naturally associated point of E, the P_L of the theorem. If we associate the point at infinity to the trivial line bundle, we see:

Corollary 10.3. *There is a natural bijection between $\mathrm{Pic}^0(E)$ and the points of E.*

Thus we can think of the line bundles of degree 0 on E as being parametrized by E itself; this is therefore a second example of a moduli space.

A remarkable fact is the following:

Theorem 10.4. *The bijection $\mathrm{Pic}^0(E) \xrightarrow{\sim} E$ is an isomorphism of groups.*

In fact, one can use this approach to give a simple (but not at all elementary) proof that the group law we have defined for elliptic curves is associative! See [1, p. 321].

References

1. Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, 1977.
2. Frances Kirwan, *Complex algebraic curves*, Student Texts, no. 23, London Mathematical Society, 1992.