10.2 The Group Structure on an Elliptic Curve

Let E be an elliptic curve over $\mathbb{C}$. In this section we will see how to put an abelian group structure on the set $E(\mathbb{C})$ in a natural way. The point $\mathcal{O} = (0:1:0) \in E(\mathbb{C})$ "at infinity" will serve as the 0 element of the group, and if $P, Q, R \in E(\mathbb{C})$ then $P+Q+R = \mathcal{O}$ if and only if P, Q, and R lie on a common line. There is a sense, which we will not make precise, in which elliptic curves are the only curves that can be endowed in a "natural way" with a group structure.

10.2.1 Divisors

We begin by defining a huge group associated to E.

Definition 10.2.1 (Divisors). The group $\mathrm{Div}(E)$ of *divisors on* E is the free abelian group on the elements of $E(\mathbb{C})$. Thus $\mathrm{Div}(E)$ is the set of all finite formal linear combinations

$$n_1 P_1 + n_2 P_2 + \cdots + n_i P_i$$

with $n_i \in \mathbb{Z}$ and $P_i \in E(\mathbb{C})$.

Because $\mathrm{Div}(E)$ is a *free* abelian group, there are no relations among the points; thus, e.g., if P, Q, and R are in $E(\mathbb{C})$ then *by definition* we will never have $P + Q = R$ in $\mathrm{Div}(E)$.

Example 10.2.2. If E is defined by $y^2 = x(x-1)(x+1)$, then

$$2(0,0) - 3(1,0) + (-1,0) + (2, \sqrt{6})$$

is an element of $\mathrm{Div}(E)$.

Note that $\mathrm{Div}(E)$ is a huge uncountable group, and there is no natural way in which its elements are in bijection with $E(\mathbb{C})$; it is much too large. We will cut it down significantly, by considering its quotient by the subgroup of *principal divisors*. This is analogous to considering the quotient of the nonzero ideals of a quadratic field by the equivalence relation $\sim$ as in Section 9.5.3.

10.2.2 Rational Functions

Definition 10.2.3 (Rational Function on $\mathbb{P}^2$). A *rational function* on $\mathbb{P}^2$ is an element of the field $\mathbb{C}(x,y)$ of all quotients $p(x,y)/q(x,y)$ where $p(x,y)$ and $q(x,y)$ are arbitrary polynomials in two variables with $q \neq 0$.

Definition 10.2.4 (Homogenous Polynomial). A *homogeneous polynomial* $P(x_1, \ldots, x_n)$ in n-variables is a polynomial such that for every constant λ,

$$P(\lambda x_1, \ldots, \lambda x_n) = \lambda P(x_1, \ldots, x_n).$$

Notice that $x^2 + y^2$ is homogenous polynomial, but $y^2 + x^3$ is not.

A rational function $f = p(x,y)/q(x,y) \in \mathbb{C}(x,y)$ determines an algebraic map $\mathbb{P}^2 \to \mathbb{P}^1$ as follows. Let $P(X,Y,Z) = Z^r p(X/Z, Y/Z)$ and $Q(X,Y,Z) = Z^s q(X/Z, Y/Z)$, where r and s are the degrees of p and q. If $s < r$, replace Q by $Z^{r-s}Q$ or if $r < s$ replace P by $Z^{s-r}P$, so that P and Q have the same degree. Then

$$(a\colon b\colon c) \mapsto (P(a,b,c) : Q(a,b,c))$$

is a well-defined algebraic map from $\mathbb{P}^2 \to \mathbb{P}^1$. It is *not* true that every map $\mathbb{P}^2 \to \mathbb{P}^1$ is induced by a rational function; for example, the constant function that sends every element of $\mathbb{P}^2$ to $(1 : 0)$ doesn't come from a rational function, since the rational function that induced it would have a denominator of 0.

Let E be the elliptic curve defined by $y^2 = x^3 + ax + b$.

Definition 10.2.5 (Rational Function on E). A *rational function* on E is an element of the field

$$K(E) = \mathbb{C}(x)[y]/(y^2 - (x^3 + ax + b)) = \mathbb{C}(x)(\sqrt{x^3 + ax + b}).$$

Thus $K(E)$ is the field generated by x and y where x is an indeterminate and y satisfies $y^2 = x^3 + ax + b$. Thus $K(E)$ is a quadratic field extension of $\mathbb{C}(x)$. Just as is the case for rational functions on $\mathbb{P}^2$, a rational function determines a map $E(\mathbb{C}) \to \mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$ (but not conversely).

The analogue of the ring of integers of $K(E)$ is called the "affine coordinate ring" of E.

Definition 10.2.6 (Affine Coordinate Ring of E). The *affine coordinate ring* of E is the subgroup

$$A(E) = \mathbb{C}[x,y]/(y^2 - (x^3 + ax + b)) = \mathbb{C}[x][\sqrt{x^3 + ax + b}].$$

One can prove that $A(E)$ is integrally closed in $K(E)$ (see Exercise 4 for some examples).

Proposition 10.2.7. *There is a natural bijection between the maximal ideals of the ring $A(E)$ and the points of $E(\mathbb{C})$.*

Proof. If $(\alpha, \beta) \in \mathbb{C}^2$ is a point on $E(\mathbb{C})$ let $\mathfrak{m} = (x - \alpha, y - \beta)$ be the ideal in $A(E)$ generated by $x - \alpha$ and $y - \beta$. Since $\mathfrak{m}$ is the kernel of the homomorphism $A(E) \to \mathbb{C}$ sending x to α and y to β, we see that $\mathfrak{m}$ is a maximal ideal.

Conversely, suppose that $\mathfrak{m}$ is a maximal ideal of $A(E)$. The inverse image of $\mathfrak{m}$ in $\mathbb{C}[x]$ is a nonzero prime ideal of $\mathbb{C}[x]$ (it is a general fact that the inverse image of any prime ideal under any homomorphism is a prime ideal), so it is of the form $(x - \alpha)$ for some $\alpha \in \mathbb{C}$. Thus $A(E)/\mathfrak{m}$ is a quotient of

$$R = \mathbb{C}[y]/(y^2 - \alpha^3 - a\alpha - b).$$

Since $\mathbb{C}$ is algebraically closed, the maximal ideals of R correspond to the points on E with x-coordinate α. Thus $\mathfrak{m}$ corresponds to a point (α, β) on E. □

10.2.3 Principal Divisors

Let $K(E)^\times$ denote the group of nonzero elements of $K(E)$, and suppose $f = p(x,y)/q(x,y) \in K(E)^\times$. Reduce $p(x,y)$ and $q(x,y)$ modulo the relation $y^2 = x^3 + ax + b$, so that the largest exponent of y occuring in each is at most 1. Let $P = (\alpha : \beta : 1) \in E(\mathbb{C})$ and let $\mathfrak{m} = (x - \alpha, y - \beta)$ be the corresponding maximal ideal of $A(E)$ as in Proposition 10.2.7. The order of vanishing of $p(x,y)$ at P is

$$\mathrm{ord}_P(p(x,y)) = \max\{n : p \in \mathfrak{m}^n\} \in \mathbb{Z},$$

and likewise the order of vanishing of $q(x,y)$ at P is

$$\mathrm{ord}_P(q(x,y)) = \max\{n : q \in \mathfrak{m}^n\} \in \mathbb{Z}.$$

The points P where $\mathrm{ord}_P(p(x,y)) > 0$, are the points where the graph of $p(x,y) = 0$ intersects E. Since $y^2 - (x^3 + ax + b)$ doesn't divide $p(x,y)$ (by assumption), there are only finitely many intersection points, so there are only finitely many points P where $\mathrm{ord}_P(p(x,y)) > 0$.

The *order* of the rational function f at P is

$$\mathrm{ord}_P(f) = \mathrm{ord}_P(p(x,y)) - \mathrm{ord}_P(q(x,y)) \in \mathbb{Z}.$$

Let $\mathcal{O} = (0 : 1 : 0)$ be the point at infinity on E. We define, in a seemingly totally ad hoc manner,

$$\mathrm{ord}_{\mathcal{O}}(f) = -\sum \mathrm{ord}_P(f) \in \mathbb{Z} \cup \{\infty\},$$

where the sum is over all $P = (\alpha : \beta : 1) \in E(\mathbb{C})$. This is the same value we would obtain if we were to define $A(E)$, etc., as above, but with U_3 replaced by U_2, but we will not prove this fact in this book (it is nontrivial).

Definition 10.2.8 (Divisor of a Function). Let $f \in K(E)^\times$. The *principal divisor* associated to f is

$$(f) = \sum_{\text{all } P \in E(\mathbb{C})} \mathrm{ord}_P(f) \cdot P \in \mathrm{Div}(E).$$

The map $K(E)^\times \to \mathrm{Div}(E)$ is a group homomorphism; this is just the assertion that the order of vanishing of the product of two functions on E is the sum of their orders of vanishing, a fact we will not prove in this book.

10.2.4 Picard's Group and the Group Law

Let $\mathrm{Prin}(E)$ be the subgroup of $\mathrm{Div}(E)$ of principal divisors.

Definition 10.2.9 (The Picard Group). The *Picard group* of E is

$$\mathrm{Pic}(E) = \mathrm{Div}(E)/\mathrm{Prin}(E).$$

Alternatively, $\mathrm{Pic}(E)$ is the set of equivalence classes of $\mathrm{Div}(E)$ with respect to the equivalence relation $\sim$ in which $D_1 \sim D_2$ if and only if there is $f \in K(E)^\times$ such that $D_1 - D_2 = (f)$.

The Picard group is much smaller than $\mathrm{Div}(E)$ and has a far more interesting structure. It is still too big though.

Definition 10.2.10 (Degree). The *degree* of a divisor $\sum n_i P_i \in \mathrm{Div}(E)$ is $\sum n_i \in \mathbb{Z}$. Suppose f is a nonzero rational function on E with divisor $(f) = \sum n_i P_i$. Then the *degree* of f is the sum of the n_i such that n_i is positive.

Notice that the map $\mathrm{Div}(E) \to \mathbb{Z}$ is a group homomorphism. Let $\mathrm{Div}^0(E)$ denote the subgroup of divisors of degree 0. Because of how we defined $\mathrm{ord}_{\mathcal{O}}(f)$ for $\mathcal{O} = (0:1:0)$, it is trivially true that $\mathrm{Prin}(E) \subset \mathrm{Div}^0(E)$. Let

$$\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\mathrm{Prin}(E).$$

Lemma 10.2.11. *There are no rational functions of degree* 1 *on an elliptic curve.*

Proof. A rational function of degree 1 would define an isomorphism between E and $\mathbb{P}^1$, which is impossible because E is a torus and $\mathbb{P}^1$ is a sphere.[2] □ 2

Theorem 10.2.12. *The map $\Phi : E(\mathbb{C}) \to \mathrm{Pic}^0(E)$ that associates to a point $P \in E(C)$ the class of the degree 0 divisor $P - \mathcal{O}$ is a bijection. Since $\mathrm{Pic}^0(E)$ is a group, this bijection induces a group structure on $E(\mathbb{C})$. In this group, if P, Q, and R are colinear points on E, then $P + Q + R = 0$.*

Proof. First we show that Φ is injective. If $\Phi(P) = \Phi(Q)$ with $P \neq Q$, then $P - \mathcal{O} \sim Q - \mathcal{O}$. Thus $P \sim Q$, so there is a rational function f on E of degree 1, which contradicts Lemma 10.2.11. Thus Φ is injective.

To show that Φ is surjective, we must show that every element of $\mathrm{Div}^0(E)$ is equivalent to an element of the form $P - \mathcal{O}$ for some $P \in E(\mathbb{C})$. Suppose $\sum n_i P_i$ is an element of $\mathrm{Div}^0(E)$. Then $\sum n_i P_i = \sum n_i (P_i - \mathcal{O})$ since $\sum n_i = 0$. By induction it thus suffices to show that $(P - \mathcal{O}) \pm (Q - \mathcal{O}) \sim R - \mathcal{O}$ for some R. We do this using rational functions of the form

[2]This proof is incomplete, given the theory developed thus far in this course.

$f = ax + by + c$. Because E is defined by a cubic equation $y^2 = x^3 + ax + b$, the divisor of f is

$$(f) = P + Q + R - 3\mathcal{O},$$

where P, Q, and R are the three points of intersection of the line $f = 0$ with E, counted with multiplicity. Thus

$$(P - \mathcal{O}) + (Q - \mathcal{O}) + (R - \mathcal{O}) \sim 0.$$

If $R = (x, y)$, let $\tilde{R} = (x, -y)$. Then using a vertical line we see that $R + \tilde{R} + \mathcal{O} \sim 3\mathcal{O}$, so

$$(R - \mathcal{O}) + (\tilde{R} - \mathcal{O}) \sim 0.$$

Thus $(P - \mathcal{O}) + (Q - \mathcal{O}) \sim (\tilde{R} - \mathcal{O})$. Likewise, $(P - \mathcal{O}) - (Q - \mathcal{O}) \sim (P - \mathcal{O}) + (\tilde{Q} - \mathcal{O})$, so $(P - \mathcal{O}) - (Q - \mathcal{O})$ is equivalent to a divisor of the desired form. This completes the proof. $\square$

Remark 10.2.13. If E is replaced by a curve X of higher degree (without singularities), then everything that we stated about divisors is true up to the theorem, which is false. Instead we have only an injective map $X \hookrightarrow \mathrm{Pic}^0(X)$. The group $\mathrm{Pic}^0(X)$ is called the *Jacobian* of X and has additional geometric structure (e.g., it is a complex manifold of dimension $(d-1)(d-2)/2$, where d is the degree of X). Thus, though $X(\mathbb{C})$ doesn't have a natural group structure, it embeds in a geometric object which does.

Just as for binary quadratic forms, the group structure is induced by multiplication of ideal classes. Let $\mathcal{I}$ denote the set of nonzero ideals of the affine coordinate ring $A(E)$ of E. One can prove that every element of $\mathcal{I}$ is a product of maximal ideals of $A(E)$. By Proposition 10.2.7, these maximal ideals are in bijection with the points $E(\mathbb{C})$. Define an equivalence relation $\sim$ on $\mathcal{I}$ by $I \sim J$ if there are $f, g \in A(E)$ such that $(f)I = (g)J$, and let $\mathrm{Cl}(E)$ denote the group of equivalence classes of nonzero ideals under multiplication. Then the map $\mathrm{Cl}(E) \to \mathrm{Pic}^0(E)$ which sends the class of the maximal ideal $\mathfrak{m}$ corresponding to a point P to the class of the divisor $P - \mathcal{O}$ is an isomorphism.