Chapter 7

Curves and Divisor Class Groups

The purpose of this chapter is to develop some basic theory of divisors and functions on curves. We use this theory to prove that the set of points on an elliptic curve over a field is a group. There exist more elementary proofs of this fact, but I feel the approach via divisor class groups gives a deeper understanding of the subject.

We start by introducing the theory of singular points on varieties. Then we define uniformizers and the valuation of a function at a point on a curve. When working over a field $\mathbb{k}$ that is not algebraically closed it turns out to be necessary to consider not just points on C defined over $\mathbb{k}$ but also those defined over $\overline{\mathbb{k}}$ (alternatively, one can generalise the notion of point to places of degree greater than one; see [589] for details). We then discuss divisors, principal divisors and the divisor class group. The hardest result is that the divisor of a function has degree zero; the proof for general curves is given in Chapter 8. Finally, we discuss the "chord and tangent" group law on elliptic curves.

7.1 Non-Singular Varieties

The word "local" is used throughout analysis and topology to describe any property that holds in a neighbourhood of a point. We now develop some tools to study "local" properties of points of varieties. The algebraic concept of "localisation" is the main technique used.

Definition 7.1.1. Let X be a variety over $\mathbb{k}$. The **local ring** over $\mathbb{k}$ of X at a point $P \in X(\mathbb{k})$ is

$$\mathcal{O}_{P,\mathbb{k}}(X) = \{f \in \mathbb{k}(X) : f \text{ is regular at } P\}.$$

Define

$$\mathfrak{m}_{P,\mathbb{k}}(X) = \{f \in \mathcal{O}_{P,\mathbb{k}}(X) : f(P) = 0\} \subseteq \mathcal{O}_{P,\mathbb{k}}(X).$$

When the variety X and field $\Bbbk$ are clear from the context we simply write $\mathcal{O}_P$ and $\mathfrak{m}_P$.

Lemma 7.1.2. *Let the notation be as above. Then*

1. $\mathcal{O}_{P,\Bbbk}(X)$ *is a ring;*
2. $\mathfrak{m}_{P,\Bbbk}(X)$ *is an* $\mathcal{O}_{P,\Bbbk}(X)$*-ideal;*
3. $\mathfrak{m}_{P,\Bbbk}(X)$ *is a maximal ideal;*
4. $\mathcal{O}_{P,\Bbbk}(X)$ *is a Noetherian local ring.*

Proof: The first three parts are straightforward. The fourth part follows from the fact that, if X is affine, $\mathcal{O}_{P,\Bbbk}(X)$ is the localisation of $\Bbbk[X]$ (which is Noetherian) at the maximal ideal $\mathfrak{m} = \{f \in \Bbbk[X] : f(P) = 0\}$. Lemma A.9.5 shows that the localisation of a Noetherian ring at a maximal ideal is Noetherian. Similarly, if X is projective then $\mathcal{O}_{P,\Bbbk}(X)$ is isomorphic to a localisation of $R = \Bbbk[\varphi_i^{-1}(X)]$ (again, Noetherian) where i is such that $P \in U_i$. □

Note that, for an affine variety X,

$$\Bbbk \subseteq \Bbbk[X] \subseteq \mathcal{O}_P(X) \subseteq \Bbbk(X).$$

Remark 7.1.3. We remark that $\mathcal{O}_{P,\Bbbk}(X)$ and $\mathfrak{m}_{P,\Bbbk}(X)$ are defined in terms of $\Bbbk(X)$ rather than any particular model for X. Hence, if $\phi : X \to Y$ is a birational map over $\Bbbk$ of varieties over $\Bbbk$ and ϕ is defined at $P \in X(\Bbbk)$ then $\mathcal{O}_{P,\Bbbk}(X)$ is isomorphic as a ring to $\mathcal{O}_{\phi(P),\Bbbk}(Y)$ (precisely, if $f \in \mathcal{O}_{\phi(P),\Bbbk}(Y)$ then $\phi^*(f) = f \circ \phi \in \mathcal{O}_{P,\Bbbk}(X)$). Similarly, $\mathfrak{m}_{P,\Bbbk}(X)$ and $\mathfrak{m}_{\phi(P),\Bbbk}(Y)$ are isomorphic.

Let X be a projective variety, let $P \in X(\Bbbk)$, and let i such that $P \in U_i$. By Corollary 5.4.9, $\Bbbk(X) \cong \Bbbk(\varphi_i^{-1}(X))$ and so $\mathcal{O}_{P,\Bbbk}(X) \cong \mathcal{O}_{\varphi_i^{-1}(P),\Bbbk}(\varphi_i^{-1}(X \cap U_i))$. It is therefore sufficient to consider affine varieties when determining local properties of a variety.

Example 7.1.4. Let $X \subseteq \mathbb{A}^n$ be an affine variety and suppose $P = (0, \ldots, 0) \in X(\Bbbk)$. Then $\mathcal{O}_P = \mathcal{O}_{P,\Bbbk}(X)$ is the set of equivalence classes

$$\{f_1(x_1, \ldots, x_n)/f_2(x_1, \ldots, x_n) : f_1, f_2 \in \Bbbk[x_1, \ldots, x_n], f_2(0, \ldots, 0) \neq 0\}.$$

In other words, the ratios of polynomials such that the denominators always have non-zero constant coefficient. Similarly, $\mathfrak{m}_P$ is the $\mathcal{O}_P$-ideal generated by $x_1, \ldots, x_n$. Since $f_1(x_1, \ldots, x_n)$ can be written in the form $f_1 = c + h(x_1, \ldots, x_n)$ where $c \in \Bbbk$ is the constant coefficient and $h(x_1, \ldots, x_n) \in \mathfrak{m}_P$, it follows that $\mathcal{O}_P/(x_1, \ldots, x_n) \cong \Bbbk$. Hence $\mathfrak{m}_P$ is a maximal ideal.

Exercise 7.1.5. Let $X \subseteq \mathbb{A}^n$ be a variety over $\Bbbk$ and let $P = (P_1, \ldots, P_n) \in X(\Bbbk)$. Consider the **translation** morphism $\phi : X \to \mathbb{A}^n$ given by $\phi(x_1, \ldots, x_n) = (x_1 - P_1, \ldots, x_n - P_n)$. Show that $\phi(P) = (0, \ldots, 0)$ and that ϕ maps X to a variety Y that is isomorphic to X. Show further that $\mathcal{O}_{\phi(P),\Bbbk}(\phi(X))$ is isomorphic to $\mathcal{O}_{P,\Bbbk}(X)$ as a $\Bbbk$-algebra.

We now introduce the notion of singular points and non-singular varieties. These concepts are crucial in our discussion of curves: on a non-singular curve one can define the order of a pole or zero of a function in a well-behaved way. Since singularity is a local property of a point (i.e., it can be defined in terms of $\mathcal{O}_P$) it is sufficient to restrict attention to affine varieties. Before stating the definition we need a lemma.

Lemma 7.1.6. *Let $X \subseteq \mathbb{A}^n$ be an affine variety over $\Bbbk$ and let $P \in X(\Bbbk)$. Then the quotient ring $\mathcal{O}_{P,\Bbbk}(X)/\mathfrak{m}_{P,\Bbbk}(X)$ is isomorphic to $\Bbbk$ as a $\Bbbk$-algebra. Furthermore the quotient $\mathfrak{m}_{P,\Bbbk}(X)/\mathfrak{m}_{P,\Bbbk}(X)^2$ of $\mathcal{O}_{P,\Bbbk}(X)$-ideals is a $\Bbbk$-vector space of dimension at most n.*

Exercise 7.1.7. Prove Lemma 7.1.6.

As the following example shows, the dimension of the vector space $\mathfrak{m}_{P,\Bbbk}(X)/\mathfrak{m}_{P,\Bbbk}(X)^2$ carries information about the local geometry of X at the point P.

Example 7.1.8. Let $X = \mathbb{A}^2$ and $P = (0,0) \in X(\Bbbk)$. We have $\mathfrak{m}_P = (x,y)$, $\mathfrak{m}_P^2 = (x^2, xy, y^2)$ and so the $\Bbbk$-vector space $\mathfrak{m}_P/\mathfrak{m}_P^2$ has dimension 2. Note that X has dimension 2.

Let $X = V(y^2 - x) \subseteq \mathbb{A}^2$, which has dimension 1. Let $P = (0,0) \in X(\Bbbk)$. Then $\mathfrak{m}_P = (x,y)$ and $\{x,y\}$ span the $\Bbbk$-vector space $\mathfrak{m}_P/\mathfrak{m}_P^2$. Since $x = y^2$ in $\Bbbk(X)$ it follows that $x \in \mathfrak{m}_P^2$ and so $x = 0$ in $\mathfrak{m}_P/\mathfrak{m}_P^2$. Hence $\mathfrak{m}_P/\mathfrak{m}_P^2$ is a one-dimensional vector space over $\Bbbk$ with basis vector y.

Consider now $X = V(y^2 - x^3) \subseteq \mathbb{A}^2$, which has dimension 1. Let $P = (0,0)$. Again, $\{x,y\}$ spans $\mathfrak{m}_P/\mathfrak{m}_P^2$ over $\Bbbk$. Unlike the previous example, there is no linear dependence among the elements $\{x,y\}$ (as there is no polynomial relation between x and y having a non-zero linear component). Hence $\mathfrak{m}_P/\mathfrak{m}_P^2$ has basis $\{x,y\}$ and has dimension 2.

Exercise 7.1.9. Let $X = V(x^4 + x + yx - y^2) \subseteq \mathbb{A}^2$ over $\Bbbk$ and let $P = (0,0)$. Find a basis for the $\Bbbk$-vector space $\mathfrak{m}_{P,\Bbbk}(X)/\mathfrak{m}_{P,\Bbbk}(X)^2$. Repeat the exercise for $X = V(x^4 + x^3 + yx - y^2)$.

Example 7.1.8 motivates the following definition. One important feature of this definition is that it is in terms of the local ring at a point P and so applies equally to affine and projective varieties.

Definition 7.1.10. Let X be a variety (affine or projective) over $\Bbbk$ and let $P \in X(\overline{\Bbbk})$ be point. Then P is **non-singular** if $\dim_{\overline{\Bbbk}} \mathfrak{m}_{P,\overline{\Bbbk}}(X)/\mathfrak{m}_{P,\overline{\Bbbk}}(X)^2 = \dim(X)$ and is **singular** otherwise.[1] The variety X is **non-singular** or **smooth** if every point $P \in X\left(\overline{\Bbbk}\right)$ is non-singular.

Indeed, it follows from the arguments in this section that if $P \in X(\Bbbk)$ then P is non-singular if and only if $\dim_{\Bbbk} \mathfrak{m}_{P,\Bbbk}(X)/\mathfrak{m}_{P,\Bbbk}(X)^2 = \dim(X)$. The condition of Definition 7.1.10 is inconvenient for practical computation. Hence, we now give an equivalent condition (Corollary 7.1.13) for a point to be singular.

Suppose $X \subseteq \mathbb{A}^n$ is an affine variety and let $P = (0,\ldots,0)$. The key idea for Theorem 7.1.12 is to consider the map $\theta : \Bbbk[x_1,\ldots,x_n] \to \Bbbk^n$ defined by

$$\theta(f(x_1,\ldots,x_n)) = \left(\frac{\partial f}{\partial x_1}(P), \ldots, \frac{\partial f}{\partial x_n}(P)\right).$$

This is essentially the same map as used in the proof of Lemma 7.1.6, but there it was defined on $\mathfrak{m}_{P,\Bbbk}(X) \subseteq \mathcal{O}_{P,\Bbbk}(X)$ whereas θ is defined on $\Bbbk[x_1,\ldots,x_n]$. Note that θ is $\Bbbk$-linear. Let $\mathfrak{m}_0(\mathbb{A}^n)$ be the $\Bbbk[x_1,\ldots,x_n]$-ideal $(x_1,\ldots,x_n)$. Then $\theta(\mathfrak{m}_0(\mathbb{A}^n)) = \Bbbk^n$, $\ker(\theta) = \mathfrak{m}_0(\mathbb{A}^n)^2$ and θ induces an isomorphism of $\Bbbk$-vector spaces $\mathfrak{m}_0(\mathbb{A}^n)/\mathfrak{m}_0(\mathbb{A}^n)^2 \cong \Bbbk^n$.

Lemma 7.1.11. *Let $X \subseteq \mathbb{A}^n$ be an affine variety over $\Bbbk$ and let $P \in X(\Bbbk)$. Define*[2] *$\mathfrak{m} = \{f \in \Bbbk[X] : f(P) = 0\}$. Then $\Bbbk[X]/\mathfrak{m} \cong \Bbbk$ and $\mathfrak{m}/\mathfrak{m}^2 \cong \mathfrak{m}_{P,\Bbbk}(X)/\mathfrak{m}_{P,\Bbbk}(X)^2$ as $\Bbbk$-vector spaces.*

[1] The dimension of the vector space $\mathfrak{m}_{P,\Bbbk}(X)/\mathfrak{m}_{P,\Bbbk}(X)^2$ is always greater than or equal to $\dim(X)$, but we don't need this.

[2] We stress that $\mathfrak{m}$ is different from the ideals $\mathfrak{m}_{P,\Bbbk}(X)$ and $\mathfrak{m}_0(\mathbb{A}^n)$ above. One has $\mathfrak{m} \subseteq \mathfrak{m}_{P,\Bbbk}(X)$ and, for $P = (0,\ldots,0)$, $\mathfrak{m} = \mathfrak{m}_0(\mathbb{A}^n)/I_{\Bbbk}(X)$.

Proof: We assume without loss of generality that $P = (0, \ldots, 0)$. Since $\Bbbk[X] = \Bbbk[x_1, \ldots, x_n]/I_\Bbbk(X)$ it follows that $\mathfrak{m}$ is the $\Bbbk[X]$-ideal $(x_1, \ldots, x_n)$. The first statement is then immediate. For the second statement note that one has $\Bbbk[X] \subseteq \mathcal{O}_{P,\Bbbk}(X)$, $\mathfrak{m} = \mathfrak{m}_{P,\Bbbk}(X) \cap \Bbbk[X]$ and $\mathfrak{m}_{P,\Bbbk}(X)$ is the $\mathcal{O}_{P,\Bbbk}(X)$-ideal generated by $\mathfrak{m}$. Similarly, $\mathfrak{m}^2 = \mathfrak{m}_{P,\Bbbk}(X)^2 \cap \Bbbk[X]$.

We now construct a ring isomorphism $\omega : \mathcal{O}_{P,\Bbbk}(X)/\mathfrak{m}_{P,\Bbbk}(X)^2 \to \Bbbk[X]/\mathfrak{m}^2$. Every $f \in \mathcal{O}_{P,\Bbbk}(X)$ has a representation f_1/f_2 where $f_1, f_2 \in \Bbbk[X]$ and $f_2(P) \neq 0$. Write $f_2 = a_0 + f_3 + f_4$ where $a_0 \in \Bbbk$, $a_0 \neq 0$, $f_3 \in \mathfrak{m}$ and $f_4 \in \mathfrak{m}^2$. Define $g = a_0^{-1} - a_0^{-2} f_3 \notin \mathfrak{m}$. Then $f_2 g - 1 \in \mathfrak{m}^2$ and so g is f_2^{-1} in $\Bbbk[X]/\mathfrak{m}^2$. It follows that

$$f_1/f_2 \equiv f_1 g$$

in $\mathcal{O}_{P,\Bbbk}(X)/\mathfrak{m}_{P,\Bbbk}(X)^2$. Hence, if $f = f_1/f_2 \in \mathcal{O}_{P,\Bbbk}(X)$ with $f_1, f_2 \in \Bbbk[X]$ then we define $\omega(f) = f_1 g$. One can verify that ω is a well-defined ring homomorphism, that ω is surjective, and that $\ker(\omega) = \mathfrak{m}_{P,\Bbbk}(X)^2$. Hence ω is an isomorphism of rings as claimed.

Finally, if $f = f_1/f_2 \in \mathfrak{m}_{P,\Bbbk}(X)$ with $f_1, f_2 \in \Bbbk[X]$ then $f_1 \in \mathfrak{m}$ and $f_2 \in \Bbbk[X] - \mathfrak{m}$ and so $\omega(f) \in \mathfrak{m}$. It follows that $\mathfrak{m}_{P,\Bbbk}(X)/\mathfrak{m}_{P,\Bbbk}(X)^2 \cong \mathfrak{m}/\mathfrak{m}^2$. □

Theorem 7.1.12. *Let $X = V(f_1, \ldots, f_m) \subseteq \mathbb{A}^n$ be a variety defined over $\Bbbk$ and let $P \in X(\Bbbk)$. Let d_1 be the dimension of the $\Bbbk$-vector space $\mathfrak{m}_{P,\Bbbk}/\mathfrak{m}_{P,\Bbbk}^2$. Let d_2 be the rank of the **Jacobian matrix***

$$J_{X,P} = \left(\frac{\partial f_i}{\partial x_j}(P) \right)_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}.$$

Then $d_1 + d_2 = n$.

Proof: By Exercise 7.1.5 we may assume without loss of generality that $P = (0, \ldots, 0)$. Let the notation be as in Lemma 7.1.11. We have $d_1 = \dim_\Bbbk(\mathfrak{m}/\mathfrak{m}^2)$. Recall the map $\theta : \Bbbk[x_1, \ldots, x_n] \to \Bbbk^n$ from above, which gives an isomorphism from $\mathfrak{m}_0(\mathbb{A}^n)/\mathfrak{m}_0(\mathbb{A}^n)^2$ to $\Bbbk^n$.

Now, $\mathfrak{m}$ is the image of $\mathfrak{m}_0(\mathbb{A}^n)$ in $\Bbbk[X] = \Bbbk[x_1, \ldots, x_n]/I_\Bbbk(X)$. Similarly, $\mathfrak{m}^2$ is the image of $\mathfrak{m}_0(\mathbb{A}^n)^2$ in $\Bbbk[X]$. Hence $\mathfrak{m}/\mathfrak{m}^2$ is isomorphic as a $\Bbbk$-vector space to $\mathfrak{m}_0(\mathbb{A}^n)/(\mathfrak{m}_0(\mathbb{A}^n)^2, I_\Bbbk(X))$. Similarly, the span of the rows of the matrix $J_{X,P}$ in $\Bbbk^n$ is $\theta(I_\Bbbk(X))$, which is isomorphic as a $\Bbbk$-vector space to $(I_\Bbbk(X), \mathfrak{m}_0(\mathbb{A}^n)^2)/\mathfrak{m}_0(\mathbb{A}^n)^2$. One therefore has $\dim_\Bbbk(\mathfrak{m}/\mathfrak{m}^2) + \operatorname{rank}(J_{X,P}) = n$. □

Corollary 7.1.13. *Let $X = V(f_1(\underline{x}), \ldots, f_m(\underline{x})) \subseteq \mathbb{A}^n$ be an affine variety over $\Bbbk$ of dimension d. Let $P \in X(\Bbbk)$. Then $P \in X(\Bbbk)$ is a **singular point** of X if and only if the Jacobian matrix $J_{X,P}$ has rank not equal to $n - d$. The point is **non-singular** if the rank of $J_{X,P}$ is equal to $n - d$.*

Corollary 7.1.14. *Let $X = V(f(x_1, \ldots, x_n)) \subseteq \mathbb{A}^n$ be irreducible and let $P \in X(\Bbbk)$. Then P is singular if and only if*

$$\frac{\partial f}{\partial x_j}(P) = 0$$

for all $1 \leq j \leq n$

Exercise 7.1.15. Prove Corollaries 7.1.13 and 7.1.14.

Exercise 7.1.16. Let $\Bbbk$ be a field such that $\operatorname{char}(\Bbbk) \neq 2$ and let $F(x) \in \Bbbk[x]$ be such that $\gcd(F(x), F'(x)) = 1$. Show that

$$X : y^2 = F(x)$$

is non-singular as an affine algebraic set. Now consider the projective closure $\overline{X} \subseteq \mathbb{P}^2$. Show that if $\deg(F(x)) \geq 4$ then there is a unique point in $\overline{X} - X$ and that it is a singular point.

Finally we can define what we mean by a curve.

Definition 7.1.17. A **curve** is a projective non-singular variety of dimension 1. A **plane curve** is a curve that is given by an equation $V(F(x,y,z)) \subseteq \mathbb{P}^2$.

Remark 7.1.18. We stress that in this book a curve is always projective and non-singular. Note that many authors (including Hartshorne [278] and Silverman [564]) allow affine and/or singular dimension 1 varieties X to be curves. A fact that we won't prove is that every finitely generated, transcendence degree 1 extension K of an algebraic closed field $\overline{\Bbbk}$ is the function field $\overline{\Bbbk}(C)$ of a curve (see Theorem I.6.9 of Hartshorne [278]; note that working over $\overline{\Bbbk}$ is essential as there are finitely generated, transcendence degree 1 extensions of $\Bbbk$ that are not $\Bbbk(C)$ for a curve C defined over $\Bbbk$). It follows that every irreducible algebraic set of dimension 1 over $\Bbbk$ is birational over $\overline{\Bbbk}$ to a non-singular curve (see Theorem 1.1 of Moreno [439] for the details). Hence, in practice one often writes down an affine and/or singular equation X that is birational to the projective, non-singular curve C one has in mind. In our notation, the commonly used phrase "singular curve" is an oxymoron. Instead one can say "singular equation for a curve" or "singular model for a curve".

The following result is needed in a later proof.

Lemma 7.1.19. *Let C be a curve over $\Bbbk$. Let $P, Q \in C(\overline{\Bbbk})$. Then $\mathcal{O}_{P,\overline{\Bbbk}} \subseteq \mathcal{O}_{Q,\overline{\Bbbk}}$ implies $P = Q$.*

Proof: By Exercise 5.2.23 we may assume that $P, Q \in U_n(\overline{\Bbbk}) \subseteq \mathbb{P}^n(\overline{\Bbbk})$ and applying φ_n^{-1} we have $P, Q \in \varphi_n^{-1}(C) \subseteq \mathbb{A}^n(\overline{\Bbbk})$. Let $R = \overline{\Bbbk}[\varphi_n^{-1}(C)]$ and define $\mathfrak{m} = \mathfrak{m}_{P,\overline{\Bbbk}} \cap R = \{f \in R : f(P) = 0\}$ as in Lemma 7.1.11. By Lemma 7.1.11, $R/\mathfrak{m} \cong \overline{\Bbbk}$ and so $\mathfrak{m}$ is a maximal R-ideal. Finally, $P \in V(\mathfrak{m})$ since every polynomial in $\mathfrak{m}_{P,\overline{\Bbbk}}$ vanishes at P, and by the Nullstellensatz $V(\mathfrak{m}) = \{P\}$.

If $\mathcal{O}_{P,\overline{\Bbbk}} \subseteq \mathcal{O}_{Q,\overline{\Bbbk}}$ then the inclusion map gives rise to $\mathcal{O}_{P,\overline{\Bbbk}} \to \mathcal{O}_{Q,\overline{\Bbbk}}/\mathfrak{m}_{Q,\overline{\Bbbk}}$ with kernel $\mathcal{O}_{P,\overline{\Bbbk}} \cap \mathfrak{m}_{Q,\overline{\Bbbk}}$. In other words, $\mathcal{O}_{P,\overline{\Bbbk}}/(\mathcal{O}_{P,\overline{\Bbbk}} \cap \mathfrak{m}_{Q,\overline{\Bbbk}})$ injects into $\mathcal{O}_{Q,\overline{\Bbbk}}/\mathfrak{m}_{Q,\overline{\Bbbk}} \cong \overline{\Bbbk}$. Hence $\mathcal{O}_{P,\overline{\Bbbk}} \cap \mathfrak{m}_{Q,\overline{\Bbbk}}$ is a maximal ideal and so $\mathfrak{m}_{P,\overline{\Bbbk}} \subseteq \mathfrak{m}_{Q,\overline{\Bbbk}}$. Therefore $\mathfrak{m} \subseteq \mathfrak{n} := \mathfrak{m}_{Q,\overline{\Bbbk}} \cap R$. But $\mathfrak{m}$ is maximal in R and $1 \notin \mathfrak{n}$ so $\mathfrak{m} = \mathfrak{n}$. Since $V(\mathfrak{m}) = \{P\}$ and $V(\mathfrak{n}) = \{Q\}$ we have $P = Q$.

The above proof was influenced by Lemma I.6.4 of Hartshorne [278], but it was pointed out to me by Noel Robinson that there should be a simpler proof: If $P \neq Q$ then one can write down a function f such that $f \in \mathcal{O}_{P,\overline{\Bbbk}}$ but $f \notin \mathcal{O}_{Q,\overline{\Bbbk}}$ as follows: Letting, as above, $P = (a_1, \ldots, a_n)$ and $Q = (b_1, \ldots, b_n)$ in some affine patch, then $P \neq Q$ implies $a_i \neq b_i$ for some index i. Then the function $f = 1/(x_i - b_i)$ has a pole at Q but is regular at P. □

7.2 Weierstrass Equations

Definition 7.2.1. Let $a_1, a_2, a_3, a_4, a_6 \in \Bbbk$. A **Weierstrass equation** is a projective algebraic set E over $\Bbbk$ given by

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3. \tag{7.1}$$

The **affine Weierstrass equation** is

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{7.2}$$

Exercise 7.2.2. Let E be a Weierstrass equation as in Definition 7.2.1. Let $\iota(x : y : z) = (x : -y - a_1x - a_3z : z)$. Show that if $P \in E(\Bbbk)$ then $\iota(P) \in E(\Bbbk)$ and that ι is an isomorphism over $\Bbbk$ from E to itself.

Lemma 7.2.3. *Let $H(x), F(x) \in \Bbbk[x]$, $\deg(F) = 3$, $\deg(H) \leq 1$. Then $E(x, y) = y^2 + H(x)y - F(x)$ is irreducible over $\overline{\Bbbk}$.*

Proof: A non-trivial factorisation of $E(x, y)$ in $\Bbbk[x, y]$ must be of the form $E(x, y) = (y + M(x))(y + N(x))$ for some $M(x), N(x) \in \Bbbk[x]$. Then $\deg(M) + \deg(N) = 3$ and, without loss of generality, $\deg(M) \geq 2$ and $\deg(N) \leq 1$. But then $\deg(M + N) \geq 2$, which is incompatible with $M + N = H$. □

Theorem 5.3.10 therefore implies a Weierstrass equation describes a projective variety. By Exercise 5.6.5, the variety has dimension 1. Not every Weierstrass equation gives a curve, since some of them are singular. We now give conditions for when a Weierstrass equation is non-singular.

Exercise 7.2.4. Show that a Weierstrass equation has a unique point with $z = 0$. Show that this point is not a singular point.

Definition 7.2.5. Let E be a Weierstrass equation over $\Bbbk$. The point $(0 : 1 : 0) \in E(\Bbbk)$ is denoted by $\mathcal{O}_E$ and is called the **point at infinity**.

Exercise 7.2.6. Show that if $\mathrm{char}(\Bbbk) \neq 2, 3$ then every Weierstrass equation over $\Bbbk$ is isomorphic over $\Bbbk$ to a Weierstrass equation

$$y^2z = x^3 + a_4xz^2 + a_6z^3 \tag{7.3}$$

for some $a_4, a_6 \in \Bbbk$. This is called the **short Weierstrass form**. Show that this equation is non-singular if and only if the **discriminant** $4a_4^3 + 27a_6^2 \neq 0$ in $\Bbbk$.

Exercise 7.2.7. Show that if $\mathrm{char}(\Bbbk) = 2$ then every Weierstrass equation over $\Bbbk$ is isomorphic over $\Bbbk$ to a Weierstrass equation

$$y^2z + xyz = x^3 + a_2x^2z + a_6z^3 \quad \text{or} \quad y^2z + yz^2 = x^3 + a_4xz^2 + a_6z^3. \tag{7.4}$$

The former is non-singular if $a_6 \neq 0$ and the latter is non-singular for all $a_4, a_6 \in \Bbbk$.

Formulae to determine whether a general Weierstrass equation is singular are given in Section III.1 of [564].

Definition 7.2.8. An **elliptic curve** is a curve given by a non-singular Weierstrass equation.

The following easy result is useful for explicit calculations.

Lemma 7.2.9. *Let E be an elliptic curve over $\Bbbk$. Then every function $f \in \Bbbk(E)$ restricts to a function on the affine Weierstrass equation of E that is equivalent to a function of the form*

$$\frac{a(x) + b(x)y}{c(x)} \tag{7.5}$$

where $a(x), b(x), c(x) \in \Bbbk[x]$. Conversely, every such function on the affine curve corresponds to a unique[3] function on the projective curve.

[3]By unique we mean that there is only one function on the projective curve corresponding to a given function on the affine curve. The actual polynomials $a(x), b(x)$ and $c(x)$ are, of course, not unique.

Proof: Write U for the affine algebraic set obtained from E by setting $z = 1$. Note that $U\left(\overline{\Bbbk}\right) \neq \varnothing$. Corollary 5.4.9 shows that $\Bbbk(E) \cong \Bbbk(U)$ and so it is sufficient to consider functions on U. Every such function can be written in the form of equation (7.5) since any denominators can be cleared by multiplying through by appropriate polynomials (the polynomial $(a(x) + b(x)y)(a(x) + b(x)\iota(y))$ is a polynomial in x only) and y^n for $n > 1$ can be replaced using the equation $y^2 = (x^3 + a_2x^2 + a_4x + a_6) - y(a_1x + a_3)$. Both claims of the Lemma follow immediately. □

7.3 Uniformizers on Curves

Let C be a curve over $\Bbbk$ with function field $\Bbbk(C)$. It is necessary to formalise the notion of multiplicity of a zero or pole of a function at a point. The basic definition will be that $f \in \mathcal{O}_{P,\overline{\Bbbk}}(C)$ has multiplicity m at P if $f \in \mathfrak{m}^m_{P,\overline{\Bbbk}}$ and $f \notin \mathfrak{m}^{m+1}_{P,\overline{\Bbbk}}$. However, there are a number of technicalities to be dealt with before we can be sure this definition makes sense. We introduce uniformizers in this section as a step towards the rigorous treatment of multiplicity of functions.

First we recall the definition of non-singular from Definition 7.1.10: Let C be a non-singular curve over $\Bbbk$ and $P \in C(\Bbbk)$, then the quotient $\mathfrak{m}_{P,\Bbbk}(C)/\mathfrak{m}_{P,\Bbbk}(C)^2$ (which is a $\Bbbk$-vector space by Lemma 7.1.6) has dimension one as a $\Bbbk$-vector space.

Lemma 7.3.1. *Let C be a curve (in particular, non-singular) over a field $\Bbbk$ and let $P \in C(\Bbbk)$. Then the ideal $\mathfrak{m}_{P,\Bbbk}(C)$ is principal as an $\mathcal{O}_{P,\Bbbk}(C)$-ideal.*

Proof: Write $\mathfrak{m}$ for $\mathfrak{m}_{P,\Bbbk}(C)$. Since C is non-singular, $\dim_{\Bbbk} \mathfrak{m}_{P,\Bbbk}(C)/\mathfrak{m}_{P,\Bbbk}(C)^2 = 1$. Let $x \in \mathfrak{m}$ be such that $\{\mathfrak{m}^2 + x\}$ is a $\Bbbk$-vector space basis for $\mathfrak{m}/\mathfrak{m}^2$. Let $\mathfrak{n}$ be the $\mathcal{O}_{P,\Bbbk}(C)$-ideal (x). Then $\mathfrak{n} \subseteq \mathfrak{m}$. For every $y \in \mathfrak{m}$ we have $y = f + ux$ where $u \in \Bbbk$ and $f \in \mathfrak{m}^2$. Hence, $\mathfrak{m} = (\mathfrak{n}, \mathfrak{m}^2)$. Let A be the $\mathcal{O}_{P,\Bbbk}(C)$-module $\mathfrak{m}/\mathfrak{n}$. We want to prove that $A = 0$. This follows by Nakayama's Lemma (see Proposition 2.6 of [15]) but we give a direct proof.

First note that $\mathfrak{m}A = \mathfrak{m}(\mathfrak{m}/\mathfrak{n}) = (\mathfrak{m}^2, \mathfrak{n})/\mathfrak{n} = A$ (the middle equality since $y(\mathfrak{n} + z) = \mathfrak{n} + yz$ for all $y, z \in \mathfrak{m}$). Suppose now that $A \neq 0$. Since $\mathcal{O}_{P,\Bbbk}(C)$ is Noetherian it follows that $\mathfrak{m}$ is finitely generated as an $\mathcal{O}_{P,\Bbbk}(C)$-module and so A is finitely generated as an $\mathcal{O}_{P,\Bbbk}(C)$-module. Let $\{a_1, \ldots, a_k\}$ be a minimal set of generators for A. Since $A = \mathfrak{m}A$ we have

$$a_1 = \sum_{j=1}^{k} m_j a_j$$

for $m_j \in \mathfrak{m}$. Hence,

$$a_1(1 - m_1) = \sum_{j=2}^{k} m_j a_j.$$

Note that $1 - m_1 \notin \mathfrak{m}$ and so, since $\mathfrak{m}$ is a maximal ideal, $(1 - m_1)$ is a unit in $\mathcal{O}_{P,\Bbbk}(C)$. Hence, $a_1 \in (a_2, \ldots, a_k)$, which contradicts the minimality of the generating set. Hence $A = 0$ and $\mathfrak{m} = \mathfrak{n} = (x)$. □

Definition 7.3.2. Let C be a curve (in particular, non-singular) over $\Bbbk$ and $P \in C(\overline{\Bbbk})$. A **uniformizer** (or **uniformizing parameter**) at P is an element $t_P \in \mathcal{O}_{P,\overline{\Bbbk}}(C)$ such that $\mathfrak{m}_{P,\overline{\Bbbk}}(C) = (t_P)$ as an $\mathcal{O}_{P,\overline{\Bbbk}}(C)$-ideal.

One can choose t_P to be any element of $\mathfrak{m}_{P,\overline{\Bbbk}}(C) - \mathfrak{m}_{P,\overline{\Bbbk}}(C)^2$; in other words, the uniformizer is not unique. If P is defined over $\Bbbk$ then one can take $t_P \in \mathfrak{m}_{P,\Bbbk}(C) -$

$\mathfrak{m}_{P,\Bbbk}(C)^2$, i.e., take the uniformizer to be defined over $\Bbbk$; this is typically what one does in practice.

For our presentation it is necessary to know uniformizers on $\mathbb{P}^1$ and on a Weierstrass equation. The next two examples determine such uniformizers.

Example 7.3.3. Let $C = \mathbb{P}^1$. For a point $(a : 1) \in U_1 \subseteq \mathbb{P}^1$ one can work instead with the point a on the affine curve $\mathbb{A}^1 = \varphi_1^{-1}(U_1)$. One has $\mathfrak{m}_a = (x - a)$ and so $t_a = (x - a)$ is a uniformizer at a. In terms of the projective equation one has $t_a = (x - az)/z$ being a uniformizer. For the point $\infty = (1 : 0) \in U_0 \subseteq \mathbb{P}^1$ one again works with the corresponding point $0 \in \varphi_0^{-1}(U_0)$. The uniformizer is $t_a = z$ which, projectively, is $t_a = z/x$. A common abuse of notation is to say that $1/x$ is a uniformizer at ∞ on $\mathbb{A}^1 = \varphi_1^{-1}(U_1)$.

Example 7.3.4. We determine uniformizers for the points on an elliptic curve. First consider points (x_P, y_P) on the affine equation

$$E(x, y) = y^2 + a_1xy + a_3y - \left(x^3 + a_2x^2 + a_4x + a_6\right).$$

Without loss of generality we can translate the point to $P_0 = (0, 0)$, in which case write $a'_1, \ldots, a'_6$ for the coefficients of the translated equation $E'(x, y) = 0$ (i.e., $E'(x, y) = E(x + x_P, y + y_P)$). One can verify that $a'_6 = 0$, $a'_3 = (\partial E/\partial y)(P)$ and $a'_4 = (\partial E/\partial x)(P)$. Then $\mathfrak{m}_{P_0} = (x, y)$ and, since the curve is not singular, at least one of a'_3 or a'_4 is non-zero.

If $a'_3 = 0$ then[4]

$$x(x^2 + a'_2x + a'_4 - a'_1y) = y^2.$$

Since $(x^2 + a'_2x + a'_4 - a'_1y)(P_0) = a'_4 \neq 0$ we have $(x^2 + a'_2x + a'_4 - a'_1y)^{-1} \in \mathcal{O}_{P_0}$ and so

$$x = y^2(a'_4 + a'_2x + x^2 - a'_1y)^{-1}.$$

In other words, $x \in (y^2) \subseteq \mathfrak{m}_{P_0}^2$ and y is a uniformizer at P_0.

Similarly, if $a'_4 = 0$ then $y(a'_3 + a'_1x + y) = x^2(x + a'_2)$ and so $y \in (x^2) \subseteq \mathfrak{m}_{P_0}^2$ and x is a uniformizer at P_0. If $a'_3, a'_4 \neq 0$ then either x or y can be used as a uniformizer. (Indeed, any linear combination $ax + by$ except $a'_3y - a'_4x$ can be used as a uniformizer; geometrically, any line through P, except the line which is tangent to the curve at P, is a uniformizer.)

Now consider the point at infinity $\mathcal{O}_E = (x : y : z) = (0 : 1 : 0)$ on E. Taking $y = 1$ transforms the point to $(0, 0)$ on the affine curve

$$z + a_1xz + a_3z^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3. \tag{7.6}$$

It follows that

$$z(1 + a_1x + a_3z - a_2x^2 - a_4xz - a_6z^2) = x^3$$

and so $z \in (x^3) \subseteq \mathfrak{m}_P^3$ and so x is a uniformizer (which corresponds to x/y in homogeneous coordinates).

In practice it is not necessary to move P to $(0, 0)$ and compute the a'_i. We have shown that if $P = (x_P, y_P)$ then $t_P = x - x_P$ is a uniformizer unless $P = \mathcal{O}_E$, in which case $t_P = x/y$, or $P = \iota(P)$,[5] in which case $t_P = y - y_P$.

Lemma 7.3.5. *Let C be a curve over $\Bbbk$, let $P \in C(\overline{\Bbbk})$ and let t_P be a uniformizer at P. Let $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. Then $\sigma(t_P)$ is a uniformizer at $\sigma(P)$.*

[4] We will see later that $a'_3 = 0$ implies $(0, 0)$ has order 2 (since $-(x, y) = (x, -y - a'_1x - a'_3)$).

[5] i.e., has order 2.

Proof: Since $\sigma(f)(\sigma(P)) = \sigma(f(P))$ the map $f \mapsto \sigma(f)$ is an isomorphism of local rings $\sigma : \mathcal{O}_{P,\overline{\Bbbk}}(C) \to \mathcal{O}_{\sigma(P),\overline{\Bbbk}}(C)$. It also follows that $\sigma(\mathfrak{m}_P) = \mathfrak{m}_{\sigma(P)}$. Since $\mathfrak{m}_P = (t_P)$ one has $\mathfrak{m}_{\sigma(P)} = (\sigma(t_P))$, which completes the proof. □

We now give an application of uniformizers. It will be used in several later results.

Lemma 7.3.6. *Let C be a non-singular curve over $\Bbbk$ and let $\phi : C \to Y \subseteq \mathbb{P}^n$ be a rational map for any projective variety Y. Then ϕ is a morphism.*

Exercise 7.3.7. Prove Lemma 7.3.6.

7.4 Valuation at a Point on a Curve

The aim of this section is to define the multiplicity of a zero or pole of a function on a curve. For background on discrete valuation rings see Chapter 1 of Serre [542], Section I.7 of Lang [365] or Sections XII.4 and XII.6 of Lang [367].

Definition 7.4.1. Let K be a field. A **discrete valuation** on K is a function $v : K^* \to \mathbb{Z}$ such that:

1. for all $f, g \in K^*$, $v(fg) = v(f) + v(g)$;
2. for all $f, g \in K^*$ such that $f + g \neq 0$, $v(f + g) \geq \min\{v(f), v(g)\}$;
3. there is some $f \in K^*$ such that $v(f) = 1$ (equivalently, v is surjective to $\mathbb{Z}$).

Lemma 7.4.2. *Let K be a field and v a discrete valuation.*

1. *$v(1) = 0$.*
2. *If $f \in K^*$ then $v(1/f) = -v(f)$.*
3. *$R_v = \{f \in K^* : v(f) \geq 0\} \cup \{0\}$ is a ring, called the **valuation ring**.*
4. *$\mathfrak{m}_v = \{f \in K^* : v(f) > 0\}$ is a maximal ideal in R_v, called the **maximal ideal** of the valuation.*
5. *If $f \in K$ is such that $f \notin R_v$ then $1/f \in \mathfrak{m}_v$.*
6. *R_v is a local ring.*

Exercise 7.4.3. Prove Lemma 7.4.2.

Lemma 7.4.4. *Let C be a curve over $\Bbbk$ and $P \in C(\Bbbk)$. For every non-zero function $f \in \mathcal{O}_{P,\Bbbk}(C)$ there is some $m \in \mathbb{N}$ such that $f \notin \mathfrak{m}_{P,\Bbbk}^m$.*

Proof: We drop the terms $\Bbbk$ and C in $\mathcal{O}_{P,\Bbbk}(C)$ and $\mathfrak{m}_{P,\Bbbk}(C)$. If $f \notin \mathfrak{m}_P$ then $m = 1$ and we are done, so suppose $f \in \mathfrak{m}_P$. Let t_P be a uniformizer at P. Then $f = t_P f_1$ for some $f_1 \in \mathcal{O}_P$. If $f_1 \notin \mathfrak{m}_P$ then $f \notin \mathfrak{m}_P^2$ and we are finished. If $f_1 \in \mathfrak{m}_P$ then $f_1 = t_P f_2$ for some $f_2 \in \mathcal{O}_P$. Continuing this way, if $f \in \mathfrak{m}_P^m$ for all $m \in \mathbb{N}$ one obtains an infinite sequence of functions $f_i \in \mathfrak{m}_P$. Consider the chain of $\mathcal{O}_P$-ideals $(f_1) \subseteq (f_2) \subseteq \cdots$. We have $(f_i) \neq (f_{i+1})$ since $f_i = t_P f_{i+1}$ and $t_P^{-1} \notin \mathcal{O}_P$ (if $t_P^{-1}(P) \in \Bbbk$ then $1 = 1(P) = (t_P t_P^{-1})(P) = t_P(P) t_P^{-1}(P) = 0$, which is a contradiction). Since $\mathcal{O}_P$ is Noetherian (Lemma 7.1.2) the ascending chain of ideals is finite, hence $f \in \mathfrak{m}_P^m$ for some $m \in \mathbb{N}$. □

Definition 7.4.5. Let C be a curve over $\Bbbk$ and $P \in C(\Bbbk)$. Let $\mathfrak{m}_P = \mathfrak{m}_{P,\Bbbk}(C)$ be as in Definition 7.1.1 and define $\mathfrak{m}_P^0 = \mathcal{O}_{P,\Bbbk}(C)$. Let $f \in \mathcal{O}_{P,\Bbbk}(C)$ be such that $f \neq 0$ and define the **order** of f at P to be $v_P(f) = \max\{m \in \mathbb{Z}_{\geq 0} : f \in \mathfrak{m}_P^m\}$. If $v_P(f) = 1$ then f has a **simple zero** at P. (We exclude the constant function $f = 0$, though one could define $v_P(0) = \infty$.)

We stress that $v_P(f)$ is well-defined. If $f, h \in \mathcal{O}_{P,\Bbbk}(C)$ and $f \equiv h$ then $f - h = 0$ in $\mathcal{O}_{P,\Bbbk}(C)$. Hence, if $f \in \mathfrak{m}_P^m$ then $h \in \mathfrak{m}_P^m$ (and vice versa).

Exercise 7.4.6. Show that $v_P(f)$ does not depend on the underlying field. In other words, if $\Bbbk'$ is an algebraic extension of $\Bbbk$ in $\overline{\Bbbk}$ then $v_P(f) = \max\{m \in \mathbb{Z}_{\geq 0} : f \in \mathfrak{m}_{P,\Bbbk'}(C)^m\}$.

Lemma 7.4.7. *Let C be a curve over $\Bbbk$ and $P \in C(\overline{\Bbbk})$. Let $t_P \in \mathcal{O}_{P,\overline{\Bbbk}}(C)$ be any uniformizer at P. Let $f \in \mathcal{O}_{P,\overline{\Bbbk}}(C)$ be such that $f \neq 0$. Then $v_P(f) = \max\{m \in \mathbb{Z}_{\geq 0} : f/t_P^m \in \mathcal{O}_{P,\overline{\Bbbk}}(C)\}$ and $f = t_P^{v_P(f)}u$ for some $u \in \mathcal{O}_{P,\overline{\Bbbk}}(C)^*$.*

Exercise 7.4.8. Prove Lemma 7.4.7.

Writing a function f as $t_P^{v_P(f)}u$ for some $u \in \mathcal{O}_{P,\overline{\Bbbk}}(C)^*$ is analogous to writing a polynomial $F(x) \in \Bbbk[x]$ in the form $F(x) = (x-a)^m G(x)$ where $G(x) \in \Bbbk[x]$ satisfies $G(a) \neq 0$. Hopefully the reader is convinced that this is a powerful tool. For example, it enables a simple proof of Exercise 7.4.9. Further, one can represent a function f as a formal power series $\sum_{n=v_P(f)}^{\infty} a_n t_P^n$ where $a_n \in \Bbbk$; see Exercises 2-30 to 2-32 of Fulton [216]. Such expansions will used in Chapters 25 and 26 but we don't develop the theory rigorously.

Exercise 7.4.9. Let C be a curve over $\Bbbk$ and $P \in C(\overline{\Bbbk})$. Let $f, h \in \mathcal{O}_{P,\overline{\Bbbk}}(C)$ be such that $f, h \neq 0$. Show that $v_P(fh) = v_P(f) + v_P(h)$.

Lemma 7.4.10. *Let C be a curve over $\Bbbk$, let $P \in C(\overline{\Bbbk})$ and let $f \in \Bbbk(C)$. Then f can be written as f_1/f_2 where $f_1, f_2 \in \mathcal{O}_{P,\overline{\Bbbk}}(C)$.*

Proof: Without loss of generality C is affine. By definition, $f = f_1/f_2$ where $f_1, f_2 \in \Bbbk[C]$. Since $\Bbbk[C] \subset \overline{\Bbbk}[C] \subset \mathcal{O}_{P,\overline{\Bbbk}}(C)$ the result follows. □

Definition 7.4.11. Let C be a curve over $\Bbbk$ and let $f \in \Bbbk(C)$. A point $P \in C(\overline{\Bbbk})$ is called a **pole** of f if $f \notin \mathcal{O}_{P,\overline{\Bbbk}}(C)$. If $f = f_1/f_2 \in \Bbbk(C)$ where $f_1, f_2 \in \mathcal{O}_{P,\overline{\Bbbk}}(C)$ then define $v_P(f) = v_P(f_1) - v_P(f_2)$.

Exercise 7.4.12. Show that if $P \in C(\overline{\Bbbk})$ is a pole of $f \in \Bbbk(C)$ then $v_P(f) < 0$ and P is a zero of $1/f$.

Lemma 7.4.13. *For every function $f \in \Bbbk(C)$ the order $v_P(f)$ of f at P is independent of the choice of representative of f.*

Proof: Suppose $f_1/f_2 \equiv g_1/g_2$ where $f_1, f_2, g_1, g_2 \in \mathcal{O}_P$. Then $f_1g_2 - f_2g_1 \in I_\Bbbk(C)$ and so $f_1g_2 = f_2g_1$ in $\mathcal{O}_P$. Since v_P is well-defined in $\mathcal{O}_P$ we have $v_P(f_1g_2) = v_P(f_2g_1)$. Applying Exercise 7.4.9 gives $v_P(f_1) + v_P(g_2) = v_P(f_2) + v_P(g_1)$. Re-arranging and applying Definition 7.4.11 proves the result. □

We now give some properties of $v_P(f)$.

Lemma 7.4.14. *Let $P \in C(\overline{\Bbbk})$. Then v_P is a discrete valuation on $\Bbbk(C)$. Furthermore, the following properties hold.*

1. *If $f \in \overline{\Bbbk}^*$ then $v_P(f) = 0$.*
2. *If $c \in \overline{\Bbbk}$ and if $v_P(f) < 0$ then $v_P(f + c) = v_P(f)$.*
3. *If $f_1, f_2 \in \Bbbk(C)^*$ are such that $v_P(f_1) \neq v_P(f_2)$ then $v_P(f_1+f_2) = \min\{v_P(f_1), v_P(f_2)\}$.*
4. *Suppose C is defined over $\Bbbk$ and let $P \in C(\overline{\Bbbk})$. Let $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. Then $v_P(f) = v_{\sigma(P)}(\sigma(f))$.*

Proof: Let t_P be a uniformizer at P. Then $v_P(t_P) = 1$, which proves the third property of Definition 7.4.1. The property $v_P(fg) = v_P(f) + v_P(g)$ follows by the same argument as Exercise 7.4.9. Similarly, if$f = t_P^v u_1$ and $g = t_P^w u_2$ with $v \leq w$ and $g \neq -f$ then $f+g = t_P^v(u_1 + t_P^{w-v}u_2)$ so $v_P(f+g) \geq \min\{v_P(f), v_P(g)\}$. Hence v_P satisfies Definition 7.4.1.

We turn to the rest of the proof. The third statement is just a refinement of the above argument. Without loss of generality, $v_P(f_1) < v_P(f_2)$. Then $f_1 = t_P^v u_1$ and $f_2 = t_P^{v+m}u_2$ for some $u_1, u_2 \in \mathcal{O}_P^*$, $v \in \mathbb{Z}$ and $m \in \mathbb{N}$. Then $f_1 + f_2 = t_P^v(u_1 + t_P^m u_2) \neq 0$ and $u_1 + t_P^m u_2 \in \mathcal{O}_P^*$ so $v_P(f_1 + f_2) = v_P(f_1)$.

The first statement follows since $f(P) \neq 0$. Statement 2 is just a special case of statement 3.

For the fourth statement, recall from Lemma 7.3.5 that one can take $t_{\sigma(P)} = \sigma(t_P)$. If $f = t_P^v u$ where $u(P) \neq 0$ then $\sigma(f) = \sigma(t_P)^v \sigma(u)$ and $\sigma(u)(\sigma(P)) = \sigma(u(P)) \neq \sigma(0) = 0$ (see Exercise 5.4.13). The result follows. □

Having shown that every v_P is a discrete valuation on $\mathbb{k}(C)$ it is natural to ask whether every discrete valuation on $\mathbb{k}(C)$ is v_P for some point $P \in C(\mathbb{k})$. To make this true over fields that are not algebraically closed requires a more general notion of a point of C defined over $\mathbb{k}$. Instead of doing this, we continue to work with points over $\overline{\mathbb{k}}$ and show in Theorem 7.5.2 that every discrete valuation on $\overline{\mathbb{k}}(C)$ is v_P for some $P \in C(\overline{\mathbb{k}})$. But first we give some examples.

Example 7.4.15. Let $E : y^2 = x(x-1)(x+1)$ over $\mathbb{k}$ and let $P = (1,0) \in E(\mathbb{k})$. We determine $v_P(x), v_P(x-1), v_P(y)$ and $v_P(x+y-1)$.

First, $x(P) = 1$ so $v_P(x) = 0$. For the rest, since $P = \iota(P)$ we take the uniformizer to be $t_P = y$. Hence $v_P(y) = 1$. Since

$$x - 1 = y^2/(x(x+1))$$

and $1/(x(x+1)) \in \mathcal{O}_P$ we have $v_P(x-1) = 2$.

Finally, $f(x,y) = x + y - 1 = y + (x-1)$ so $v_P(f(x,y)) = \min\{v_P(y), v_P(x-1)\} = \min\{1,2\} = 1$. One can see this directly by writing $f(x,y) = y(1 + y/x(x+1))$.

Lemma 7.4.16. *Let E be an elliptic curve. Then $v_{\mathcal{O}_E}(x) = -2$ and $v_{\mathcal{O}_E}(y) = -3$.*

Proof: We consider the projective equation, so that the functions become x/z and y/z then set $y = 1$ so that we are considering x/z and $1/z$ on

$$z + a_1xz + a_3z^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

As in Example 7.3.4 we have $z \in (x^3)$ and so $v_{\mathcal{O}_E}(x) = 1, v_{\mathcal{O}_E}(z) = 3$. This implies $v_{\mathcal{O}_E}(1/z) = -3$ and $v_{\mathcal{O}_E}(x/z) = -2$ as claimed. □

7.5 Valuations and Points on Curves

Let C be a curve over $\mathbb{k}$ and $P \in C(\overline{\mathbb{k}})$. We have shown that $v_P(f)$ is a discrete valuation on $\overline{\mathbb{k}}(C)$. The aim of this section is to show (using the weak Nullstellensatz) that every discrete valuation v on $\overline{\mathbb{k}}(C)$ arises as v_P for some point $P \in C(\overline{\mathbb{k}})$.

Lemma 7.5.1. *Let C be a curve over $\mathbb{k}$ and let v be a discrete valuation on $\mathbb{k}(C)$. Write $R_v, \mathfrak{m}_v$ for the corresponding valuation ring and maximal ideal (over $\overline{\mathbb{k}}$). Suppose $C \subset \mathbb{P}^n$ with coordinates $(x_0 : \cdots : x_n)$. Then there exists some $0 \leq i \leq n$ such that $\overline{\mathbb{k}}[\varphi_i^{-1}(C)]$ is a subring of R_v (where φ_i^{-1} is as in Definition 5.2.24).*

Proof: First we prove there exists some $0 \leq i \leq n$ such that $x_0/x_i, \ldots, x_n/x_i \in R_v$. To do this define $S_i = \{j : 0 \leq j \leq n, x_i/x_j \in R_v\}$. We claim that $S_0 \cap \cdots \cap S_n \neq \varnothing$ and prove this by induction. First, note that $i \in S_i$ so $S_0 \neq \varnothing$. Suppose, that $j \in S_0 \cap \cdots \cap S_k$ for $k \geq 0$. If $j \in S_{k+1}$ then we are done. If $j \notin S_{k+1}$ then we have $x_{k+1}/x_j \notin R_v$ and so $x_j/x_{k+1} \in R_v$. Since $x_i/x_j \in R_v$ for $0 \leq i \leq k$ by the inductive hypothesis it follows that $(x_i/x_j)(x_j/x_{k+1}) = x_i/x_{k+1} \in R_v$ for $0 \leq i \leq k+1$. It follows that $S_0 \cap \cdots \cap S_{k+1} \neq \varnothing$.

To prove the result, suppose i is such that $x_0/x_i, \ldots, x_n/x_i \in R_v$ Then $\overline{\Bbbk}[\varphi_i^{-1}(C)] = \overline{\Bbbk}[x_0/x_i, \ldots, x_n/x_i]$ is a subring of R_v. □

Theorem 7.5.2. *Let C be a curve over $\Bbbk$ and let v be a discrete valuation on $\overline{\Bbbk}(C)$. Then $v = v_P$ for some $P \in C(\overline{\Bbbk})$.*

Proof: (Sketch) Let R_v be the valuation ring of v and $\mathfrak{m}_v$ the maximal ideal. Let i be as in Lemma 7.5.1 so that $R = \overline{\Bbbk}[\varphi_i^{-1}(C)] \subseteq R_v$. Note that R is the affine coordinate ring of an affine curve.

By Lemma A.9.2, $\mathfrak{m} = R \cap \mathfrak{m}_v$ is a prime ideal in R. Furthermore, $\mathfrak{m} \neq \varnothing$ and $\mathfrak{m} \neq R$. Since R has Krull dimension 1, $\mathfrak{m}$ is a maximal ideal.

Theorem 5.1.20 (weak Nullstellensatz) shows that $\mathfrak{m}$ is equal to $\mathfrak{m}_P \cap \overline{\Bbbk}[\varphi_i^{-1}(C)]$ for some point $P \in C(\overline{\Bbbk})$. It follows that the restriction of v to $\overline{\Bbbk}[\varphi_i^{-1}(C)]$ is equal to v_P. Finally, since $\Bbbk(C)$ is the field of fractions of $\overline{\Bbbk}[\varphi_i^{-1}(C)]$ it follows that $v = v_P$.

For full details see Corollary I.6.6 of Hartshorne [278] or Theorem VI.9.1 of Lorenzini [394]. □

7.6 Divisors

A divisor is just a notation for a finite multi-set of points. As always, we work with points over an algebraically closed field $\overline{\Bbbk}$.

Definition 7.6.1. Let C be a curve over $\Bbbk$ (necessarily non-singular and projective). A **divisor** on C is a formal sum

$$D = \sum_{P \in C(\overline{\Bbbk})} n_P(P) \tag{7.7}$$

where $n_P \in \mathbb{Z}$ and only finitely many $n_P \neq 0$. The divisor with all $n_P = 0$ is written 0. The **support** of the divisor D in equation (7.7) is $\mathrm{Supp}(D) = \{P \in C(\overline{\Bbbk}) : n_P \neq 0\}$. Note that many authors use the notation $|D|$ for the support of D. Denote by $\mathrm{Div}_{\overline{\Bbbk}}(C)$ the set of all divisors on C. Define $-D = \sum_P (-n_P)(P)$. If $D' = \sum_{P \in C(\overline{\Bbbk})} n'_P(P)$ then define

$$D + D' = \sum_{P \in C(\overline{\Bbbk})} (n_P + n'_P)(P).$$

Write $D \geq D'$ if $n_P \geq n'_P$ for all P. So $D \geq 0$ if $n_P \geq 0$ for all P, and such a divisor is called **effective**.

Example 7.6.2. Let $E : y^2 = x^3 + 2x - 3$ over $\mathbb{Q}$ and let $P = (2,3), Q = (1,0) \in E(\mathbb{Q})$. Then

$$D = 5(P) - 7(Q)$$

is a divisor on E. The support of D is $\mathrm{Supp}(D) = \{P, Q\}$ and D is not effective.

Definition 7.6.3. The **degree** of a divisor $D = \sum_P n_P(P)$ is the integer

$$\deg(D) = \sum_{P \in C(\overline{\Bbbk})} n_P.$$

(We stress that this is a finite sum.) We write $\mathrm{Div}^0_{\overline{\Bbbk}}(C) = \{D \in \mathrm{Div}_{\overline{\Bbbk}}(C) : \deg(D) = 0\}$.

Lemma 7.6.4. *$\mathrm{Div}_{\overline{\Bbbk}}(C)$ is a group under addition, and $\mathrm{Div}^0_{\overline{\Bbbk}}(C)$ is a subgroup.*

Exercise 7.6.5. Prove Lemma 7.6.4.

Definition 7.6.6. Let C be a curve over $\Bbbk$ and let $D = \sum_{P \in C(\overline{\Bbbk})} n_P(P)$ be a divisor on C. For $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ define $\sigma(D) = \sum_P n_P(\sigma(P))$. Then D is **defined over** $\Bbbk$ if $\sigma(D) = D$ for all $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. Write $\mathrm{Div}_{\Bbbk}(C)$ for the set of divisors on C that are defined over $\Bbbk$.

Since $\mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ is an enormous and complicated object it is important to realise that testing the field of definition of any specific divisor is a finite task. There is an extension $\Bbbk'/\Bbbk$ of finite degree containing the coordinates of all points in the support of D. Let $\Bbbk''$ be the Galois closure of $\Bbbk'$. Since $\Bbbk''$ is normal over $\Bbbk$, any $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ is such that $\sigma(\Bbbk'') = \Bbbk''$. Hence, it is sufficient to study the behaviour of D under $\sigma \in \mathrm{Gal}(\Bbbk''/\Bbbk)$.

Example 7.6.7. Let $C : x^2 + y^2 = 6$ over $\mathbb{Q}$ and let $P = (1+\sqrt{2}, 1-\sqrt{2}), Q = (1-\sqrt{2}, 1+\sqrt{2}) \in C(\mathbb{Q}(\sqrt{2})) \subseteq C(\overline{\mathbb{Q}})$. Define

$$D = (P) + (Q).$$

It is sufficient to consider $\sigma(D)$ for $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$. The only non-trivial element is $\sigma(\sqrt{2}) = -\sqrt{2}$ and one sees that $\sigma(P) = Q$ and $\sigma(Q) = P$. Hence $\sigma(D) = D$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ and D is defined over $\mathbb{Q}$. Note that $C(\mathbb{Q}) = \varnothing$, so this example shows it is possible to have $\mathrm{Div}_{\Bbbk}(C) \neq \{0\}$ even if $C(\Bbbk) = \varnothing$.

7.7 Principal Divisors

This section contains an important and rather difficult result, namely that the number of poles of a function on a curve (counted according to multiplicity) is finite and equal to the number of zeros (counted according to multiplicity). The finiteness condition is essential to be able to represent the poles and zeroes of a function as a divisor. The other condition is required to show that the set of all divisors of functions is a subgroup of $\mathrm{Div}^0_{\Bbbk}(C)$.

In this chapter, finite poles and finite zeroes is only proved for plane curves and $\deg(\mathrm{div}(f)) = 0$ is proved only for elliptic curves. The general results are given in Section 8.3 in the next Chapter.

Theorem 7.7.1. *Let C be a curve over $\Bbbk$ and $f \in \Bbbk(C)^*$. Then f has finitely many poles and zeroes.*

Proof: (Special case of plane curves.) Let $C = V(F(x,y,z)) \subseteq \mathbb{P}^2$ where F is irreducible. If $F(x,y,z) = z$ then the result follows from Exercise 5.2.35 (there are only finitely many points at infinity). So we can restrict to the affine case $C = V(F(x,y))$.

Let $f = f_1(x,y)/f_2(x,y)$ with $f_1, f_2 \in \Bbbk[x,y]$. Then f is regular whenever $f_2(P) \neq 0$ so the poles of f are contained in $C \cap V(f_2)$. Without loss of generality, $f_2(x,y)$ contains monomials featuring x. The resultant $R_x(f_2(x,y), F(x,y))$ is a polynomial in y with a finite number of roots hence $C \cap V(f_2)$ is finite.

To show there are finitely many zeroes write $f = f_1/f_2$. The zeroes of f are contained in $C \cap (V(f_1) \cup V(f_2))$ and the argument above applies. □

Definition 7.7.2. Let $f \in \overline{\Bbbk}(C)^*$ and define the **divisor of a function** (this is a divisor by Theorem 7.7.1)

$$\mathrm{div}(f) = \sum_{P \in C(\overline{\Bbbk})} v_P(f)(P).$$

The divisor of a function is also called a **principal divisor**. Note that some authors write $\mathrm{div}(f)$ as (f). Let

$$\mathrm{Prin}_{\Bbbk}(C) = \{\mathrm{div}(f) : f \in \Bbbk(C)^*\}.$$

Exercise 7.7.3. Show that the zero element of $\mathrm{Div}_{\Bbbk}(C)$ lies in $\mathrm{Prin}_{\Bbbk}(C)$.

Lemma 7.7.4. *Let C be a curve over $\Bbbk$ and let $f, f' \in \Bbbk(C)^*$.*

1. $\mathrm{div}(ff') = \mathrm{div}(f) + \mathrm{div}(f')$.
2. $\mathrm{div}(1/f) = -\mathrm{div}(f)$.
3. $\mathrm{div}(f + f') \geq \sum_P \min\{v_P(f), v_P(f')\}(P)$.
4. $\mathrm{div}(f^n) = n\mathrm{div}(f)$ *for* $n \in \mathbb{Z}$.
5. *Let* $f \in \overline{\Bbbk}(C)$ *and let* $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. *Then* $\mathrm{div}(\sigma(f)) = \sigma(\mathrm{div}(f))$.

Exercise 7.7.5. Prove Lemma 7.7.4.

Lemma 7.7.6. *With notation as above,* $\mathrm{Prin}_{\Bbbk}(C)$ *is a subgroup of* $\mathrm{Div}_{\Bbbk}(C)$ *under addition.*

Exercise 7.7.7. Prove Lemma 7.7.6.

Lemma 7.7.8. *In* $\mathbb{P}^1(\Bbbk)$ *every degree 0 divisor is principal.*

Proof: Let $D = \sum_{i=1}^n e_i(x_i : z_i)$ where $\sum_{i=1}^n e_i = 0$. Define

$$f(x, z) = \prod_{i=1}^{n} (xz_i - zx_i)^{e_i}. \tag{7.8}$$

Since $\sum_{i=1}^n e_i = 0$ it follows that $f(x, z)$ is a ratio of homogeneous polynomials of the same degree and therefore a rational function on $\mathbb{P}^1$. Using the uniformizers on $\mathbb{P}^1$ from Example 7.3.3 one can verify that $v_{P_i}(f) = e_i$ when $P_i = (x_i : z_i)$ and hence that $D = \mathrm{div}(f)$. □

Note that if D is defined over $\Bbbk$ then one can show that the function $f(x, z)$ in equation (7.8) is defined over $\Bbbk$.

Exercise 7.7.9. Prove that if $f \in \Bbbk(\mathbb{P}^1)$ then $\deg(\mathrm{div}(f)) = 0$.

Lemma 7.7.10. *Let $E : y^2 + H(x)y = F(x)$ be a Weierstrass equation over $\Bbbk$ and let $P = (x_i, y_i) \in E(\overline{\Bbbk})$ be a non-singular point. Then* $\mathrm{div}(x - x_i) = (P) + (\iota(P)) - 2(\mathcal{O}_E)$.

Proof: There are one or two points $P \in E(\overline{\Bbbk})$ with x-coordinate equal to x_i, namely $P = (x_i, y_i)$ and $\iota(P) = (x_i, -y_i - H(x_i))$ (and these are equal if and only if $2y_i + H(x_i) = 0$). By Example 7.3.4 one can take the uniformizer $t_P = t_{\iota(P)} = (x - x_i)$ unless $(\partial E/\partial y)(P) = 2y_i + H(x_i) = 0$, in which case the uniformizer is $t_P = (y - y_i)$. In the former case we have $v_P(x - x_i) = v_{\iota(P)}(x - x_i) = 1$. In the latter case write

$F(x) = (x-x_i)g(x)+F(x_i) = (x-x_i)g(x)+y_i^2+H(x_i)y_i$ and $H(x) = (x-x_i)a_1+H(x_i)$. Note that $a_1y_i - g(x_i) = (\partial E/\partial x)(P) \neq 0$ and so $g_1(x) := 1/(a_1y - g(x)) \in \mathcal{O}_P$. Then

$$\begin{aligned} 0 &= y^2 + H(x)y - F(x) \\ &= (y-y_i)^2 + 2yy_i - y_i^2 + (x-x_i)a_1y + H(x_i)y - (x-x_i)g(x) - y_i^2 - H(x_i)y_i \\ &= (y-y_i)^2 + (x-x_i)(a_1y - g(x)) + (y-y_i)(2y_i + H(x_i)). \end{aligned}$$

Hence, $x - x_i = (y-y_i)^2 g_1(x)$ and $v_P(x-x_i) = 2$. Finally, the function $(x-x_i)$ corresponds to

$$\frac{x - x_i z}{z} = \frac{x}{z} - x_i$$

on the projective curve E. Since $v_{\mathcal{O}_E}(x/z) = -2$ it follows from part 2 of Lemma 7.4.14 that $v_{\mathcal{O}_E}(x-x_i) = -2$. Hence, if $P = (x_i, y_i)$ then, in all cases, $\mathrm{div}(x-x_i) = (P) + (\iota(P)) - 2(\mathcal{O}_E)$ and $\deg(\mathrm{div}(x-x_i)) = 0$. □

Exercise 7.7.9 and Lemma 7.7.10 determine the divisor of certain functions, and in both cases they turns out to have degree zero. This is not a coincidence. Indeed, we now state a fundamental[6] result which motivates the definition of the divisor class group.

Theorem 7.7.11. *Let C be a curve over $\Bbbk$. Let $f \in \Bbbk(C)^*$. Then* $\deg(\mathrm{div}(f)) = 0$.

Theorem 7.7.11 is proved for general curves in Theorem 8.3.14. Exercise 7.7.9 already proved it for $\mathbb{P}^1$. We prove Theorem 7.7.11 in the case of elliptic curves in this section (essentially, using the same method as Charlap and Robbins [127]). First, we state and prove a lemma.

Lemma 7.7.12. *Let $E : y^2 + H(x)y = F(x)$ be a Weierstrass equation over $\Bbbk$. Recall the morphism $\iota(x,y) = (x, -y-H(x))$ from Exercise 7.2.2. For $f \in \Bbbk(E)$ define $\iota^*(f) = f \circ \iota$. Let $P \in E(\Bbbk)$ be a non-singular point, $Q = \iota(P)$ and let t_Q be a uniformizer at Q. Then $\iota^* t_Q$ is a uniformizer at P and $v_Q(f) = v_P(\iota^*(f))$.*

Proof: One can verify that ι^* is a field automorphism of $\Bbbk(C)$. By definition, $(\iota^* f)(P) = f(\iota(P)) = f(Q)$. and so ι^* gives an isomorphism $\iota^* : \mathcal{O}_Q \to \mathcal{O}_P$. The result follows. □

We can now give a proof of Theorem 7.7.11 for elliptic curves. In some sense, our proof reduces the problem to a polynomial function on $\mathbb{P}^1$ (and the result for $\mathbb{P}^1$ is already known by Exercise 7.7.9). The proof given in Theorem 8.3.14 essentially follows the same logic of reducing to $\mathbb{P}^1$.

Proof: (Proof of Theorem 7.7.11 in the case of elliptic curves.) Write $E(x,y) = y^2 + H(x)y - F(x)$.

First consider a polynomial $a(x) \in \Bbbk[x]$ of degree d as a function on the affine elliptic curve $y^2 + H(x)y = F(x)$ (obtained by taking $z = 1$). The function has no poles on the affine part $E \cap \mathbb{A}^2$. Write $a(x) = \prod_{i=1}^n (x-x_i)^{e_i}$ where all $x_i \in \overline{\Bbbk}$ are distinct, $e_i \in \mathbb{N}$, and $\sum_{i=1}^n e_i = d$. It suffices to compute the divisor of $(x-x_i)$ and show that it has degree 0. The result therefore follows from Lemma 7.7.10.

Now consider a function of the form $a(x) + b(x)y$ on the affine curve $E \cap \mathbb{A}^2$. By Lemma 7.7.12 one has $v_P(a(x)+b(x)y) = v_{\iota(P)}(a(x) + b(x)(-y - H(x)))$ for all points

[6] This innocent-looking fact is actually the hardest result in this chapter to prove. There are several accessible proofs of the general result: Stichtenoth (Theorem I.4.11 of [589]; also see Moreno [439] Lemma 2.2) gives a proof based on "weak approximation" of valuations and this is probably the simplest proof for a reader who has already got this far through the current book; Fulton [216] gives a proof for projective plane curves based on Bézout's theorem; Silverman [564], Shafarevich [543], Hartshorne [278] and Lorenzini [394] all give proofs that boil down to ramification theory of $f : C \to \mathbb{P}^1$, and this is the argument we will give in the next chapter.

$P \in E(\overline{\Bbbk})$. Hence, if $\mathrm{div}(a+by) = \sum_P n_P(P)$ then $\mathrm{div}(a+b(-y-H)) = \sum_P n_P(\iota(P))$ and $\deg(\mathrm{div}(a+by)) = \deg(\mathrm{div}(a+b(-y-H)))$.

Since $(a+by)(a+b(-y-H)) = a^2+ab(y-y-H)+b^2(-y^2-Hy) = a^2-Hab-Fb^2$ is independent of y it follows by the first part of the proof that the affine parts of the divisors of the functions $(a+by)$ and $a+b(-y-H)$ have degree

$$\max\{2\deg(a), \deg(H)+\deg(a)+\deg(b), 3+2\deg(b)\}. \tag{7.9}$$

One can check that the degree in equation (7.9) is $2\deg(a)$ when $\deg(a) \geq \deg(b)+2$ and is $3+2\deg(b)$ when $\deg(a) \leq \deg(b)+1$.

To study the behaviour at infinity consider $(a(x,z)+b(x,z)y)/z^d$ where $d = \max\{\deg(a), \deg(b)+1\}$. By the same argument as before one has $v_{\mathcal{O}_E}(a(x,z)/z^d) = -2\deg(a)$. Similarly, $v_{\mathcal{O}_E}(b(x,z)y/z^d) = v_{\mathcal{O}_E}(b(x,z)/z^{d-1}) + v_{\mathcal{O}_E}(y/z) = -2\deg(b)-3$. It follows by part 3 of Lemma 7.4.14 that $\deg(\mathrm{div}((a(x,z)+b(x,z)y)/z^d)) = 0$.

Finally, consider $f(x,y,z) = f_1(x,y,z)/f_2(x,y,z)$ where f_1 and f_2 are homogeneous of degree d. By the above, $\deg(\mathrm{div}(f_1(x,y,z)/z^d)) = \deg(\mathrm{div}(f_2(x,y,z)/z^d)) = 0$ and the result follows. □

Corollary 7.7.13. *Let C be a curve over $\Bbbk$ and let $f \in \Bbbk(C)^*$. The following are equivalent:*

1. $\mathrm{div}(f) \geq 0$.
2. $f \in \Bbbk^*$.
3. $\mathrm{div}(f) = 0$.

Proof: Certainly statement 2 implies statement 3 and 3 implies 1. So it suffices to prove 1 implies 2. Let $f \in \Bbbk(C)^*$ be such that $\mathrm{div}(f) \geq 0$. Then f is regular everywhere, so choose some $P_0 \in C(\overline{\Bbbk})$ and define $h = f - f(P_0) \in \overline{\Bbbk}(C)$. Then $h(P_0) = 0$. If $h = 0$ then f is the constant function $f(P_0)$ and, since f is defined over $\Bbbk$, it follows that $f \in \Bbbk^*$. To complete the proof suppose that $h \neq 0$ in $\overline{\Bbbk}(C)$. Since $\deg(\mathrm{div}(h)) = 0$ by Theorem 7.7.11 it follows that h must have at least one pole. But then f has a pole, which contradicts $\mathrm{div}(f) \geq 0$. □

Corollary 7.7.14. *Let C be a curve over $\Bbbk$. Let $f, h \in \Bbbk(C)^*$. Then $\mathrm{div}(f) = \mathrm{div}(h)$ if and only if $f = ch$ for some $c \in \Bbbk^*$.*

Exercise 7.7.15. Prove Corollary 7.7.14.

7.8 Divisor Class Group

We have seen that $\mathrm{Prin}_{\Bbbk}(C) = \{\mathrm{div}(f) : f \in \Bbbk(C)^*\}$ is a subgroup of $\mathrm{Div}^0_{\Bbbk}(C)$. Hence, since all the groups are Abelian, one can define the quotient group; we call this the divisor class group. It is common to use the notation Pic for the divisor class group since the divisor class group of a curve is isomorphic to the Picard group of a curve (even though the Picard group is usually defined differently, in terms of line bundles).

Definition 7.8.1. The (degree zero) **divisor class group** of a curve C over $\Bbbk$ is $\mathrm{Pic}^0_{\Bbbk}(C) = \mathrm{Div}^0_{\Bbbk}(C)/\mathrm{Prin}_{\Bbbk}(C)$.

We call two divisors $D_1, D_2 \in \mathrm{Div}^0_{\Bbbk}(C)$ **linearly equivalent** and write $D_1 \equiv D_2$ if $D_1 - D_2 \in \mathrm{Prin}_{\Bbbk}(C)$. The equivalence class (called a **divisor class**) of a divisor $D \in \mathrm{Div}^0_{\Bbbk}(C)$ under linear equivalence is denoted $\overline{D}$.

Example 7.8.2. By Lemma 7.7.8, $\mathrm{Pic}^0_{\Bbbk}(\mathbb{P}^1) = \{0\}$.

Theorem 7.8.3. *Let C be a curve over $\Bbbk$ and let $f \in \overline{\Bbbk}(C)$. If $\sigma(f) = f$ for all $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ then $f \in \Bbbk(C)$. If $\mathrm{div}(f)$ is defined over $\Bbbk$ then $f = ch$ for some $c \in \overline{\Bbbk}$ and $h \in \Bbbk(C)$.*

Proof: The first claim follows from Remark 5.4.14 (also see Remark 8.4.11 of Section 8.4).

For the second statement, let $\mathrm{div}(f)$ be defined over $\Bbbk$. Then $\mathrm{div}(f) = \sigma(\mathrm{div}(f)) = \mathrm{div}(\sigma(f))$ where the second equality follows from part 4 of Lemma 7.4.14. Corollary 7.7.14 implies $\sigma(f) = c(\sigma)f$ for some $c(\sigma) \in \overline{\Bbbk}^*$. The function $c : \mathrm{Gal}(\overline{\Bbbk}/\Bbbk) \to \overline{\Bbbk}^*$ is a 1-cocycle (the fact that $c(\sigma\tau) = \sigma(c(\tau))c(\sigma)$ is immediate, the fact that $c : \mathrm{Gal}(\overline{\Bbbk}/\Bbbk) \to \overline{\Bbbk}^*$ is continuous also follows). Hence, Theorem A.7.2 (Hilbert 90) implies that $c(\sigma) = \sigma(\gamma)/\gamma$ for some $\gamma \in \overline{\Bbbk}^*$. In other words, taking $h = f/\gamma \in \overline{\Bbbk}(C)$, we have

$$\sigma(h) = \sigma(f)/\sigma(\gamma) = f/\gamma = h.$$

By the first part of the theorem $h \in \Bbbk(C)$. □

Theorem 7.8.3 has the following important corollary, namely that $\mathrm{Pic}^0_{\Bbbk}(C)$ is a subgroup of $\mathrm{Pic}^0_{\Bbbk'}(C)$ for every extension $\Bbbk'/\Bbbk$.

Corollary 7.8.4. *Let C be a curve over $\Bbbk$ and let $\Bbbk'/\Bbbk$ be an algebraic extension. Then $\mathrm{Pic}^0_{\Bbbk}(C)$ injects into $\mathrm{Pic}^0_{\Bbbk'}(C)$.*

Proof: Suppose a divisor class $\overline{D} \in \mathrm{Pic}^0_{\Bbbk}(C)$ becomes trivial in $\mathrm{Pic}^0_{\Bbbk'}(C)$. Then there is some divisor D on C defined over $\Bbbk$ such that $D = \mathrm{div}(f)$ for some $f \in \Bbbk'(C)^*$. But Theorem 7.8.3 implies $D = \mathrm{div}(h)$ for some $h \in \Bbbk(C)$ and so the divisor class is trivial in $\mathrm{Pic}^0_{\Bbbk}(C)$. □

Corollary 7.8.5. *Let $\Bbbk$ be a finite field. Let C be a curve over $\Bbbk$. Define*

$$\mathrm{Pic}^0_{\overline{\Bbbk}}(C)^{\mathrm{Gal}(\overline{\Bbbk}/\Bbbk)} = \left\{\overline{D} \in \mathrm{Pic}^0_{\overline{\Bbbk}}(C) : \sigma(\overline{D}) = \overline{D} \text{ for all } \sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)\right\}.$$

Then $\mathrm{Pic}^0_{\overline{\Bbbk}}(C)^{\mathrm{Gal}(\overline{\Bbbk}/\Bbbk)} = \mathrm{Pic}^0_{\Bbbk}(C)$.

Proof: (Sketch) Let $G = \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. Theorem 7.8.3 already showed that $\mathrm{Prin}_{\overline{\Bbbk}}(C)^G = \mathrm{Prin}_{\Bbbk}(C)$ but we re-do the proof in a more explicitly cohomological way, as we need further consequences of the argument.

Take Galois cohomology of the exact sequence

$$1 \to \overline{\Bbbk}^* \to \overline{\Bbbk}(C)^* \to \mathrm{Prin}_{\overline{\Bbbk}}(C) \to 0$$

to get

$$1 \to \Bbbk^* \to (\overline{\Bbbk}(C)^*)^G \to \mathrm{Prin}_{\overline{\Bbbk}}(C)^G \to H^1(G, \overline{\Bbbk}^*) \to H^1(G, \overline{\Bbbk}(C)^*) \to H^1(G, \mathrm{Prin}_{\overline{\Bbbk}}(C)) \to H^2(G, \overline{\Bbbk}^*).$$

Since $(\overline{\Bbbk}(C)^*)^G = \Bbbk(C)$ (Theorem 7.8.3) and $H^1(G, \overline{\Bbbk}^*) = 0$ (Hilbert 90) we have $\mathrm{Prin}_{\overline{\Bbbk}}(C)^G = \mathrm{Prin}_{\Bbbk}(C)$. Further, $H^2(G, \overline{\Bbbk}^*) = 0$ when $\Bbbk$ is finite (see Section X.7 of [542]) and $H^1(G, \overline{\Bbbk}(C)^*) = 0$ (see Silverman Exercise X.10). Hence, $H^1(G, \mathrm{Prin}_{\overline{\Bbbk}}(C)) = 0$.

Now, take Galois cohomology of the exact sequence

$$1 \to \mathrm{Prin}_{\overline{\Bbbk}}(C) \to \mathrm{Div}^0_{\overline{\Bbbk}}(C) \to \mathrm{Pic}^0_{\overline{\Bbbk}}(C) \to 0$$

to get

$$\mathrm{Prin}_{\Bbbk}(C) \to \mathrm{Div}^0_{\overline{\Bbbk}}(C)^G \to \mathrm{Pic}^0_{\overline{\Bbbk}}(C)^G \to H^1(G, \mathrm{Prin}_{\overline{\Bbbk}}(C)) = 0.$$

Now, $\mathrm{Div}^0_{\overline{\Bbbk}}(C)^G = \mathrm{Div}^0_{\Bbbk}(C)$ by definition and so the result follows. □

We minimise the use of the word Jacobian in this book, however we make a few remarks here. We have associated to a curve C over a field $\Bbbk$ the divisor class group $\mathrm{Pic}^0_{\Bbbk}(C)$. This group can be considered as an algebraic group. To be precise, there is a variety J_C (called the **Jacobian variety** of C) that is an algebraic group (i.e., there is a morphism[7] $+ : J_C \times J_C \to J_C$) and such that, for any extension $\mathbb{K}/\Bbbk$, there is a bijective map between $\mathrm{Pic}^0_{\mathbb{K}}(C)$ and $J_C(\mathbb{K})$ that is a group homomorphism.

One can think of Pic^0 as a functor that, given a curve C over $\Bbbk$, associates with every field extension $\Bbbk'/\Bbbk$ a group $\mathrm{Pic}^0_{\Bbbk'}(C)$. The Jacobian variety of the curve is a variety J_C over $\Bbbk$ whose $\Bbbk'$-rational points $J_C(\Bbbk')$ are in one-to-one correspondence with the elements of $\mathrm{Pic}^0_{\Bbbk'}(C)$ for all $\Bbbk'/\Bbbk$. For most applications it is sufficient to work in the language of divisor class groups rather than Jacobians (despite our remarks about algebraic groups in Chapter 4).

7.9 Elliptic Curves

The goal of this section is to show that the 'traditional' **chord-and-tangent rule** for elliptic curves does give a group operation. Our approach is to show that this operation coincides with addition in the divisor class group of an elliptic curve. Hence, elliptic curves are an algebraic group.

First we state the chord-and-tangent rule without justifying any of the claims or assumptions made in the description. The results later in the section will justify these claims (see Remark 7.9.4). For more details about the chord-and-tangent rule see Washington [626], Cassels [122], Reid [497] or Silverman and Tate [567].

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on the affine part of an elliptic curve E. Draw the line $l(x, y) = 0$ between P_1 and P_2 (if $P_1 \neq P_2$ then this is called a chord; if $P_1 = P_2$ then let the line be the tangent to the curve at P_1). Denote by R the third point[8] of intersection (counted according to multiplicities) of the line with the curve E. Now draw the line $v(x) = 0$ between $\mathcal{O}_E$ and R (if $R = \mathcal{O}_E$ then this is the "line at infinity" and if R is an affine point this is a vertical line so a function of x only). Denote by S the third point of intersection of this line with the curve E. Then one defines $P_1 + P_2$ to be S. Over the real numbers this operation is illustrated in Figure 7.1.

We now transform the above geometric description into algebra, and show that the points R and S do exist. The first step is to write down the equation of the line between $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$. We state the equation of the line as a definition and then show that it corresponds to a function with the correct divisor.

Definition 7.9.1. Let $E(x, y)$ be a Weierstrass equation for an elliptic curve over $\Bbbk$. Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(\Bbbk) \cap \mathbb{A}^2$. If $P_1 = \iota(P_2)$ then the line between P_1 and P_2 is[9] $v(x) = x - x_1$.

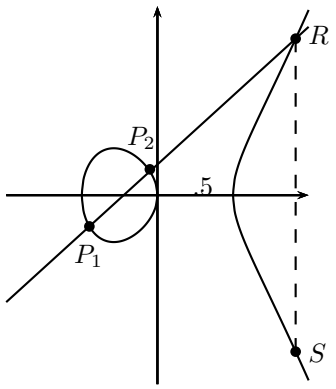
If $P_1 \neq \iota(P_2)$ then there are two subcases. If $P_1 = P_2$ then define $\lambda = (3x_1^2 + 2a_2x_1 + a_4)/(2y_1 + a_1x_1 + a_3)$ and if $P_1 \neq P_2$ then define $\lambda = (y_2 - y_1)/(x_2 - x_1)$. The line between P_1 and P_2 is then

$$l(x, y) = y - \lambda(x - x_1) - y_1.$$

We stress that whenever we write $l(x, y)$ then we are implicitly assuming that it is not a vertical line $v(x)$.

[7] To make this statement precise requires showing that $J_C \times J_C$ is a variety.
[8] Possibly this point is at infinity.
[9] This includes the case $P_1 = P_2 = \iota(P_1)$.

Figure 7.1: Chord and tangent rule for elliptic curve addition.



Warning: Do not confuse the line $v(x)$ with the valuation v_P. The notation $v(P)$ means the line evaluated at the point P. The notation $v_P(x)$ means the valuation of the function x at the point P.

Exercise 7.9.2. Let the notation be as in Definition 7.9.1. Show that if $P_1 = \iota(P_2)$ then $v(P_1) = v(P_2) = 0$ and if $P_1 \neq \iota(P_2)$ then $l(P_1) = l(P_2) = 0$.

Lemma 7.9.3. *Let $P_1 = (x_1, y_1) \in E(\Bbbk)$ and let $P_2 = \iota(P_1)$. Let $v(x) = (x - x_1)$ as in Definition 7.9.1. Then* $\mathrm{div}(v(x)) = (P_1) + (P_2) - 2(\mathcal{O}_E)$.

Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(\Bbbk)$ be such that $P_1 \neq \iota(P_2)$ and let $l(x, y) = y - \lambda(x - x_1) - y_1$ be as in Definition 7.9.1. Then there exists $x_3 \in \Bbbk$ such that $E(x, \lambda(x - x_1) + y_1) = -\prod_{i=1}^{3}(x - x_i)$ and $\mathrm{div}(l(x, y)) = (P_1) + (P_2) + (R) - 3(\mathcal{O}_E)$ *where $R = (x_3, \lambda(x_3 - x_1) + y_1)$.*

Proof: The first part is just a restatement of Lemma 7.7.10.

For the second part, set $G(x) = -E(x, \lambda(x - x_1) + y_1)$, which is a monic polynomial over $\Bbbk$ of degree 3. Certainly x_1 and x_2 are roots of $G(x)$ over $\Bbbk$ so if $x_1 \neq x_2$ then $G(x)$ has a third root x_3 over $\Bbbk$. In the case $x_1 = x_2$ we have $P_1 = P_2 \neq \iota(P_2)$. Make a linear change of variables so that $(x_1, y_1) = (x_2, y_2) = 0$. The curve equation is $E(x, y) = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x)$ and $a_3 \neq 0$ since $(0, 0) \neq \iota(0, 0)$. Now, by definition, $l(x, y) = a_4x/a_3$ and one has

$$G(x) = E(x, a_4x/a_3) = (a_4x/a_3)^2 + a_1x(a_4x/a_3) + a_4x - (x^3 + a_2x^2 + a_4x)$$

which is divisible by x^2. Hence $G(x)$ splits completely over $\Bbbk$.

For the final part we consider $l(x, y)$ as a function on the affine curve. By Lemma 7.4.14 and Lemma 7.4.16 we have $v_{\mathcal{O}_E}(l(x, y)) = \min\{v_{\mathcal{O}_E}(y), v_{\mathcal{O}_E}(x), v_{\mathcal{O}_E}(1)\} = -3$. Since $\deg(\mathrm{div}(l(x, y))) = 0$ there are three affine zeroes counted according to multiplicity.

Define $\overline{l}(x, y) = y + (a_1x + a_3) + \lambda(x - x_1) + y_1$. Note that $\overline{l} = -l \circ \iota$ so $v_P(l(x, y)) = v_{\iota(P)}(\overline{l}(x, y))$ (also see Lemma 7.7.12). One can check that

$$l(x, y)\overline{l}(x, y) = -E(x, \lambda(x - x_1) + y_1) = \prod_{i=1}^{3}(x - x_i) \tag{7.10}$$

where the first equality is equivalence modulo $E(x,y)$, not equality of polynomials. Hence, for any point $P \in E(\Bbbk)$,

$$v_P(l(x,y)) + v_P(\overline{l}(x,y)) = v_P\left(\prod_{i=1}^{3}(x - x_i)\right).$$

Write $P_i = (x_i, y_i)$, let e_i be the multiplicity of x_i in the right hand side of equation (7.10) and recall that $v_{P_i}(x - x_i) = 1$ if $P_i \neq \iota(P_i)$ and 2 otherwise. Also note that $l(P_i) = 0$ implies $\overline{l}(P_i) \neq 0$ unless $P_i = \iota(P_i)$, in which case $v_{P_i}(l(x,y)) = v_{P_i}(\overline{l}(x,y))$. It follows that $v_{P_i}(l(x,y)) = e_i$, which proves the result. □

Remark 7.9.4. It follows from the above results that it does make sense to speak of the "third point of intersection" R of $l(x,y)$ with E and to call $l(x,y)$ a tangent line in the case when $P_1 = P_2$. Hence, we have justified the assumptions made in the informal description of the chord-and-tangent rule.

Exercise 7.9.5. Let $E(x,y,z)$ be a Weierstrass equation for an elliptic curve. The line $z = 0$ is called the line at infinity on E. Show that $z = 0$ only passes through $(0,0)$ on the affine curve given by the equation $E(x,1,z) = 0$.

Exercise 7.9.6. Prove that the following algebraic formulae for the chord-and-tangent rule are correct. Let $P_1, P_2 \in E(\Bbbk)$, we want to compute $S = P_1 + P_2$. If $P_1 = \mathcal{O}_E$ then $S = P_2$ and if $P_2 = \mathcal{O}_E$ then $S = P_1$. Hence we may now assume that $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are affine. If $y_2 = -y_1 - H(x_1)$ then $S = \mathcal{O}_E$. Otherwise, set λ to be as in Definition 7.9.1 and compute $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$ and $y_3 = -\lambda(x_S - x_1) - y_1$. The sum is $S = (x_3, y_3)$.

Before proving the main theorem, we state the following technical result, whose proof is postponed to the next chapter (Corollary 8.6.5).

Theorem 7.9.7. *Let $P_1, P_2 \in E(\Bbbk)$ be a points on an elliptic curve such that $P_1 \neq P_2$. Then $(P_1) - (P_2)$ is not a principal divisor.*

We now consider the divisor class group $\mathrm{Pic}^0_{\Bbbk}(E)$. The following result is usually obtained as a corollary to the Riemann-Roch theorem, but we give an ad-hoc proof for elliptic curves. One can consider this result as the Abel-Jacobi map in the case of genus 1 curves.

Theorem 7.9.8. *There is a one-to-one correspondence between $E(\Bbbk)$ and $\mathrm{Pic}^0_{\Bbbk}(E)$, namely $P \mapsto (P) - (\mathcal{O}_E)$.*

Proof: We first show that the map is injective. Suppose $(P_1) - (\mathcal{O}_E) \equiv (P_2) - (\mathcal{O}_E)$. Then $(P_1) - (P_2)$ is principal, and so Theorem 7.9.7 implies $P_1 = P_2$.

It remains to show that the map is surjective. Let $D = \sum_P n_P(P)$ be any effective divisor on E. We prove that D is equivalent to a divisor of the form

$$(P) + (\deg(D) - 1)(\mathcal{O}_E). \tag{7.11}$$

We will do this by replacing any term $(P_1) + (P_2)$ by a term of the form $(S) + (\mathcal{O}_E)$ for some point S.

The key equations are $(P) + (\iota(P)) = 2(\mathcal{O}_E) + \mathrm{div}(v(x))$ where $v(x)$ is as in Definition 7.9.1, or, if $P_1 \neq \iota(P_2)$, $(P_1) + (P_2) = (S) + (\mathcal{O}_E) + \mathrm{div}(l(x,y)/v(x))$. The first equation allows us to replace any pair $(P) + (\iota(P))$, including the case $P = \iota(P)$, by $2(\mathcal{O}_E)$. The second equation allows us to replace any pair $(P_1) + (P_2)$, where $P_1 \neq \iota(P_2)$

(but including the case $P_1 = P_2$) with $(S)+(\mathcal{O}_E)$. It is clear that any pair of affine points is included in one of these two cases, and so repeating these operations a finite number of times reduces any effective divisor to the form in equation (7.11).

Finally, let D be a degree zero divisor on E. Write $D = D_1 - D_2$ where D_1 and D_2 are effective divisors of the same degree. By the above argument we can write $D_1 \equiv (S_1) + (\deg(D_1) - 1)(\mathcal{O}_E)$ and $D_2 \equiv (S_2) + (\deg(D_1) - 1)(\mathcal{O}_E)$. Hence $D \equiv (S_1) - (S_2)$. Finally, adding the divisor of the vertical line function through S_2 and subtracting the divisor of the line between S_1 and $\iota(S_2)$ gives $D \equiv (S)-(\mathcal{O}_E)$ for some point S as required. □

Since $E(\Bbbk)$ is in bijection with the group $\mathrm{Pic}^0_{\Bbbk}(E)$ it follows that $E(\Bbbk)$ is a group, with the group law coming from the divisor class group structure of E. It remains to show that the group law is just the chord-and-tangent rule. In other words, this result shows that the chord-and-tangent rule is associative. Note that many texts prove that both $E(\Bbbk)$ and $\mathrm{Pic}^0_{\Bbbk}(E)$ are groups and then prove that the map $P \mapsto (P) - (\mathcal{O}_E)$ is a group homomorphism; whereas we use this map to prove that $E(\Bbbk)$ is a group.

Theorem 7.9.9. *Let E be an elliptic curve over a field $\Bbbk$. The group law induced on $E(\Bbbk)$ by pulling back the divisor class group operations via the bijection of Theorem 7.9.8 is the chord-and-tangent rule.*

Proof: Let $P_1, P_2 \in E(\Bbbk)$. To add these points we map them to divisor classes $(P_1)-(\mathcal{O}_E)$ and $(P_2) - (\mathcal{O}_E)$ in $\mathrm{Pic}^0_{\Bbbk}(E)$. Their sum is $(P_1) + (P_2) - 2(\mathcal{O}_E)$, which is reduced to the form $(S) - (\mathcal{O}_E)$ by applying the rules in the proof of Theorem 7.9.8. In other words, we get $(P_1) + (P_2) - 2(\mathcal{O}_E) = (S) - (\mathcal{O}_E) + \mathrm{div}(f(x, y))$ where $f(x, y) = v(x)$ if $P_1 = \iota(P_2)$ or $f(x, y) = l(x, y)/v(x)$ in the general case, where $l(x, y)$ and $v(x)$ are the lines from Definition 7.9.1. Since these are precisely the same lines as in the description of the chord-and-tangent rule it follows that the point S is the same point as produced by the chord-and-tangent rules. □

A succinct way to describe the elliptic curve addition law (since there is a single point at infinity) is that three points sum to zero if they lie on a line. This is simply a restatement of the fact that if P, Q and R line on the line $l(x, y, z) = 0$ then the divisor $(P) + (Q) + (R) - 3(\mathcal{O}_E)$ is a principal divisor.

Exercise 7.9.10. One can choose any $\Bbbk$-rational point $P_0 \in E(\Bbbk)$ and define a group law on $E(\Bbbk)$ such that P_0 is the identity element. The sum of points P and Q is defined as follows: let l be the line through P and Q (taking the tangent if $P = Q$, which uniquely exists since E is non-singular). Then l hits E at a third point (counting multiplicities) R. Draw a line v between P_0 and R. This hits E at a third point (again counting with multiplicities) S. Then $P + Q$ is defined to be the point S. Show that this operation satisfies the axioms of a group.