Chapter 3

Divisors

In this chapter we introduce some basic language and definitions from algebraic geometry that are fundamental to the understanding of cryptographic pairing computations. We continue with our example-driven approach and illustrate each concept and definition as it arises. We will essentially just be expanding on the more concise section found in Galbraith's chapter [Gal05, §IX.2]. However, we only focus on what we need to describe elliptic curve pairings, so we refer any reader seeking a more general and thorough treatment to Galbraith's new book [Gal12, Ch.7-9]. Since our exposition targets the newcomer, we begin by assuring such a reader that their persistence through the definitions and examples will be amply rewarded. On becoming comfortable with the language of divisors, one can immediately start to appreciate how pieces of the "pairings puzzle" fit together very naturally, and might even enjoy feeling intuition behind important theorems that would otherwise appear foreign.

The following statements apply to all curves C over any perfect field K and its closure $\overline{K}$ (see [Sil09, p. 17, p. 1] for the respective definitions). However, for now we place the discussion in our context and specialise to the case where C is an elliptic curve E over a finite field $K = \mathbb{F}_q$. Later in this chapter we will expand to more general examples and statements in time to present the important theorems in their full generality. A *divisor* D on E is a convenient way to denote a multi-set of points on E, written as the formal sum

$$D = \sum_{P \in E(\overline{\mathbb{F}}_q)} n_P(P),$$

where all but finitely many $n_P \in \mathbb{Z}$ are zero. The standard parentheses $(\cdot)$ around the P's and the absence of square parentheses $[\cdot]$ around the n_P's is what differentiates the formal sum in a divisor from an actual sum of points (i.e. using the group law) on E. The set of all divisors on E is denoted by $\mathrm{Div}_{\overline{\mathbb{F}}_q}(E)$ and forms a group, where addition of divisors is natural, and the identity is the divisor with all $n_P = 0$, the zero divisor $0 \in \mathrm{Div}_{\overline{\mathbb{F}}_q}(E)$. The *degree* of a divisor D is $\mathrm{Deg}(D) = \sum_{P \in E(\overline{\mathbb{F}}_q)} n_P$, and the *support* of D, denoted $\mathrm{supp}(D)$, is the set $\mathrm{supp}(D) = \{P \in E(\overline{\mathbb{F}}_q) : n_P \neq 0\}$.

Example 3.0.1 (Magma script). Let $P, Q, R, S \in E(\overline{\mathbb{F}}_q)$. Let $D_1 = 2(P) - 3(Q)$, and $D_2 = 3(Q) + (R) - (S)$, so that $\mathrm{Deg}(D_1) = 2 - 3 = -1$, and $\mathrm{Deg}(D_2) = 3+1-1 = 3$. The sum $D_1+D_2 = 2(P)+(R)-(S)$, and naturally $\mathrm{Deg}(D_1+D_2) = \mathrm{Deg}(D_1) + \mathrm{Deg}(D_2) = 2$. The supports are $\mathrm{supp}(D_1) = \{P, Q\}$, $\mathrm{supp}(D_2) = \{Q, R, S\}$, and $\mathrm{supp}(D_1 + D_2) = \{P, R, S\}$.

Associating divisors with a function f on E is a convenient way to write down the intersection points (and their multiplicities) of f and E. Let $\mathrm{ord}_P(f)$ count the multiplicity of f at P, which is positive if f has a zero at P, and negative if f has a pole at P. We write the *divisor of a function* f as (f), and it is defined as the divisor

$$(f) = \sum_{P \in E(\overline{\mathbb{F}}_q)} \mathrm{ord}_P(f)(P).$$

Example 3.0.2 (Magma script). We have already seen examples of functions on E in the previous section, namely the lines $\ell : y = \lambda x + \nu$ used in the chord-and-tangent rule, and it is natural that we are really only interested in the points of intersection of ℓ and E, which is exactly what the divisor (ℓ) tells us. The chord ℓ in Figure 3.1 intersects E in P, Q and $-(P+Q)$, all with multiplicity 1, and (as we will discuss further in a moment) ℓ also intersects E with multiplicity -3 at $\mathcal{O}$, i.e. ℓ has a pole of order 3 at $\mathcal{O}$. Thus, ℓ has divisor $(\ell) = (P) + (Q) + (-(P+Q)) - 3(\mathcal{O})$. The tangent ℓ in Figure 3.2 intersects E with multiplicity 2 at P, with multiplicity 1 at $-[2]P$, and again with multiplicity -3 at $\mathcal{O}$, so in this case $(\ell) = 2(P) + (-[2]P) - 3(\mathcal{O})$. Notice that in both cases

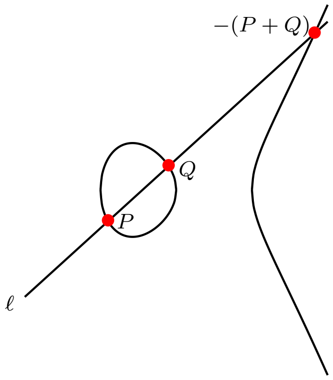

Figure 3.1: $(\ell) = (P) + (Q) + (-(P+Q)) - 3(\mathcal{O})$.

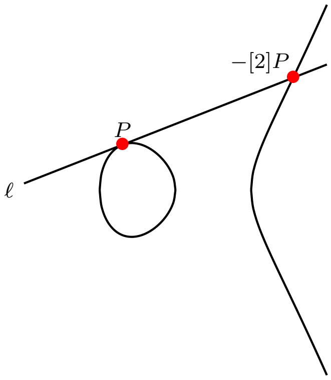

Figure 3.2: $(\ell) = 2(P) + (-[2]P) - 3(\mathcal{O})$.

we have $\mathrm{Deg}\left((\ell)\right) = 0$.

The balance that occurred between the zeros and poles in Example 3.0.2 that led to $\mathrm{Deg}((\ell)) = 0$ is not a coincidence. In fact, a fundamental result that lies at the heart of the discussion is that this always happens: namely, for any function f on E, we always have $\mathrm{Deg}((f)) = 0$. An instructive proof of this result is in Galbraith's book [Gal12, Th. 7.7.1], but roughly speaking this property follows from observing that the degree of the affine equation that solves for the zeros of f on E matches the degree of the projective equation that determines the multiplicity of the pole of f at $\mathcal{O}$, i.e. the projective version of f is g/h where g and h both have the same degree as f. We revisit Example 3.0.2 and illustrate in this special case.

Example 3.0.3 (Magma script). We already know that three zeros (counting multiplicities) will always arise from substituting $\ell : y = \lambda x + \nu$ into $E/\mathbb{F}_q : y^2 = x^3 + ax + b$, but we have only considered ℓ on the affine curve $E \cap \mathbb{A}^2$, where ℓ has no poles. To consider ℓ on E at $\mathcal{O} = (0:1:0)$ (in $\mathbb{P}^2(\mathbb{F}_q)$), we need to take $x = X/Z$ and $y = Y/Z$ which gives $(\frac{\lambda X + \nu Z}{Z})^2 = (\frac{X}{Z})^3 + a(\frac{X}{Z}) + b$, for which we clearly have a pole of order 3 when $Z = 0$.

The algebra between functions naturally translates across to the algebra between their divisors, so $(fg) = (f) + (g)$ and $(f/g) = (f) - (g)$, $(f) = 0$ if and only if f is constant, and thus if $(f) = (g)$, then $(f/g) = 0$ so f is a constant multiple of g, which means that the divisor (f) determines f up to non-zero scalar multiples.

Example 3.0.4 (Magma script). Let $\ell : y = \lambda_1 x + \nu_1$ be the chord (through P and

Q) with divisor $(\ell) = (P) + (Q) + (-(P+Q)) - 3(\mathcal{O})$, and let $\ell' : y = \lambda_2 x + \nu_2$ be the tangent at R with divisor $(\ell') = 2(R) + (-[2]R) - 3(\mathcal{O})$. The divisor of

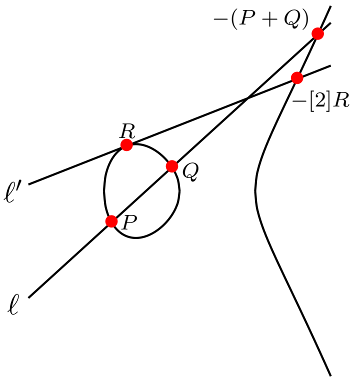

Figure 3.3: Two functions ℓ and ℓ' on E.

the function $\ell_{\text{prod}} = \ell\ell'$ is $(\ell_{\text{prod}}) = (\ell) + (\ell') = (P) + (Q) + 2(R) + (-(P+Q)) + (-[2]R) - 6(\mathcal{O})$. The divisor of $\ell_{\text{quot}} = \ell/\ell'$ is $(\ell_{\text{quot}}) = (\ell) - (\ell') = (P) + (Q) + (-(P+Q)) - 2(R) - (-[2]R)$. Notice that ℓ_{quot} does not intersect E at $\mathcal{O}$; projectifying $\ell/\ell' = \frac{y - \lambda_1 x + \nu_1}{y - \lambda_2 x + \nu_2}$ gives $\frac{Y - \lambda_1 X + \nu_1 Z}{Y - \lambda_2 X + \nu_2 Z}$, which does not give rise to any zeros or poles at $Z = 0$. Suppose we wanted to depict the function $\ell\ell'$ on E, and we multiplied out $(y - \lambda_1 x - \nu_1)(y - \lambda_2 x - \nu_2)$, substituted the y^2 for $x^3 + ax + b$ and wrote $y = \frac{x^3 + ax + b + (\lambda_1 x + \nu_1)(\lambda_2 x + \nu_2)}{(\lambda_1 + \lambda_2)x + \nu_1 + \nu_2}$. It does not make sense to try and depict this function since all the pictures we have used for illustrative purposes also show how the functions (on E) behave at points that are not on E, where the substitution $y^2 = x^3 + ax + b$ is not permitted.

3.1 The divisor class group

We can now start introducing important subgroups of the group of divisors $\text{Div}_{\overline{\mathbb{F}}_q}(E)$ on E. We temporarily drop the subscript, and write $\text{Div}(E)$ as the group of all divisors on E. The set of degree zero divisors $\{D \in \text{Div}(E) : \text{Deg}(D) = 0\}$ forms a proper subgroup, which we write as $\text{Div}^0(E) \subset \text{Div}(E)$. If a divisor D on E is equal to the divisor of a function, i.e. $D = (f)$, then D is called a *principal* divisor, and the set of principal divisors naturally form a group, written as $\text{Prin}(E)$. We already know (from Example 3.0.3 and the preceding discussion) that principal divisors have degree zero, but there are also degree zero divisors that are not the divisors of a function, so the degree zero subgroup is strictly larger than the principal divisors, i.e. $\text{Prin}(E) \subset \text{Div}^0(E)$.

There is, however, an extra condition on elements of $\mathrm{Div}^0(E)$ that *does* allow us to write an "if-and-only-if": $D = \sum_P n_P(P) \in \mathrm{Div}^0(E)$ is principal if and only if $\sum_P [n_P]P = \mathcal{O}$ on E [Gal05, Th. IX.2]. We illustrate this statement, and the relationship between the three groups

$$\mathrm{Prin}(E) \subset \mathrm{Div}^0(E) \subset \mathrm{Div}(E) \tag{3.1}$$

in Example 3.1.1.

Example 3.1.1 (Magma script). Consider $E/\mathbb{F}_{103} : y^2 = x^3 + 20x + 20$, with points $P = (26, 20)$, $Q = (63, 78)$, $R = (59, 95)$, $S = (24, 25)$, $T = (77, 84)$, $U = (30, 99)$ all on E. The divisor $(S) + (T) - (P) \in \mathrm{Div}(E)$ is clearly not in the subgroup $\mathrm{Div}^0(E)$, since it has degree 1; there are also infinitely many other trivial examples. The divisor $(P) + (Q) - (R) - (S)$ is in $\mathrm{Div}^0(E)$, but is not principal since $P + Q - R - S = (18, 49) \neq \mathcal{O}$ on E. Thus, a function f with $(f) = (P) + (Q) - (R) - (S)$ does not exist. On the other hand, the divisor $(P)+(Q)-(R)-(T)$ is principal, since it is degree 0 and $P+Q-R-T = \mathcal{O}$ on E. Thus, there is some function f on E such that $(f) = (P) + (Q) - (R) - (T)$; it is $f = \frac{6y+71x^2+91x+91}{x^2+70x+11}$. The sum $R+T$ on E is actually U, thus $P+Q-U = \mathcal{O}$ on E, but this time there is no function with divisor $(P) + (Q) - (U)$ because the degree of this divisor is not zero; however, we can keep the sum on E as $\mathcal{O}$ but manipulate the degree by instead taking the divisor $(P) + (Q) - (U) - (\mathcal{O})$, which must be in $\mathrm{Prin}(C)$, guaranteeing the existence of a function g with $(g) = (P)+(Q)-(U)-(\mathcal{O})$, namely $g = \frac{y+4x+82}{x+73}$. Observe the difference between f and g in projective space, where $f = \frac{6YZ+71X^2+91XZ+91Z^2}{X^2+70XZ+11Z^2}$ and $g = \frac{Y+4X+82Z}{X+73Z}$. For f, the point at infinity $\mathcal{O} = (0 : 1 : 0)$ zeros both the numerator and denominator, giving a zero and a pole which cancels out its contribution to (f), whilst for g, the point at infinity only zeros the denominator, which is why $\mathcal{O} \in \mathrm{supp}((g))$, whereas $\mathcal{O} \notin \mathrm{supp}((f))$.

Returning to the subscript notation for a moment, the three subgroups (and other related groups) in Equation (3.1) are often accompanied by the field they apply to, e.g. for a general field K, they are written as $\mathrm{Prin}_K(E)$, $\mathrm{Div}^0_K(E)$, and $\mathrm{Div}_K(E)$. Here $\mathrm{Div}_K(E) \subset \mathrm{Div}(E)$ is formally defined as the set of divisors invariant under the action of $\mathrm{Gal}(\overline{K}/K)$, where $\sigma \in \mathrm{Gal}(\overline{K}/K)$ acts on $D = \sum_P n_P(P)$ to give $D^\sigma = \sum_P n_P(\sigma(P))$, so that $D \in \mathrm{Div}_K(E)$ if $D = D^\sigma$. This is very natural in the contexts we consider, so we will continue on without subscripts.

Before we define the *divisor class group* of E, we look at the important notion of divisor equivalence in $\mathrm{Div}(E)$. We call the divisors D_1 and D_2 *equivalent*, written as $D_1 \sim D_2$, if $D_1 = D_2 + (f)$ for some function f.

Example 3.1.2 (Magma script). Consider $P = (57, 24)$, $Q = (25, 37)$, $R = (17, 32)$ and $S = (42, 35)$ on $E/\mathbb{F}_{61} : y^2 = x^3 + 8x + 1$. The divisors $D_1 = (P) + (Q) + (R)$ and $D_2 = 4(\mathcal{O}) - (S)$ are equivalent as follows. The function $f : y = 33x^2 + 10x + 24$, which intersects E at P, Q, R and S with multiplicity 1, and therefore has a pole of order 4 at infinity, has divisor $(f) = (P) + (Q) + (R) + (S) - 4(\mathcal{O})$, meaning $D_1 = D_2 + (f)$, so $D_1 \sim D_2$. Alternatively, if we did not want to find f, we could have used $D_1 - D_2 = (P) + (Q) + (R) + (S) - 4(\mathcal{O})$, which has degree zero, and computed that $P + Q + R + S - [4]\mathcal{O} = \mathcal{O}$ on E, which means $D_1 - D_2 \in \mathrm{Prin}(E)$, so that $D_1 - D_2 = (f)$ for some function f.

The *divisor class group*, or *Picard group*, of E is defined as the quotient group

$$\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\mathrm{Prin}(E), \tag{3.2}$$

i.e. the divisor class group is the group of all degree zero divisors modulo the principal divisors on E. At first read, this notion of equivalence (modulo divisors of functions) may seem a little abstract, but once we see it in action (particularly in more general scenarios than elliptic curves), it becomes very natural. We will first use this notion to describe the elliptic curve group law in terms of divisors, following along the lines of Galbraith [Gal05, §IX.2].

Example 3.1.3 (Magma script). Referring back to Figure 2.5 (or Figure 2.6 in the case that $Q = P$), the line ℓ joining P and Q has divisor $(\ell) = (P) + (Q) + (-R) - 3(\mathcal{O})$, whilst the vertical line $v = x - x_R$ has divisor $(v) = (-R) + (R) - 2(\mathcal{O})$. The quotient $\frac{\ell}{v}$ has divisor $(\frac{\ell}{v}) = (P) + (Q) - (R) - (\mathcal{O})$. Thus, the equation $R = P + Q$ on E is the same as the divisor equality $(R) - (\mathcal{O}) = (P) - (\mathcal{O}) + (Q) - (\mathcal{O}) - (\frac{\ell}{v})$, and the map of points to divisor classes $P \mapsto (P) - (\mathcal{O})$ is a group homomorphism. To concretely connect this back to Equation (3.2), both $(R) - (\mathcal{O})$ and $(P) + (Q) - 2(\mathcal{O})$ are clearly in $\mathrm{Div}^0(E)$, but they represent the same class in $\mathrm{Pic}^0(E)$, because the divisor $(\frac{l}{v}) = (P) + (Q) - (R) - (\mathcal{O})$ (which is their difference) is principal, and therefore zero in $\mathrm{Pic}^0(E)$.

3.2 A consequence of the Riemann-Roch Theorem

The notion of equivalence allows us to *reduce* divisors of any size $D \in \mathrm{Pic}^0(E)$ into much smaller divisors. We will make this statement precise after an example, but we must first define what we mean by "size". A divisor $D = \sum_P n_P(P)$ is called *effective* if $n_P \geq 0$ for all $P \in E$. The only divisor in $\mathrm{Div}^0(E)$ that is effective is the zero divisor. Thus, we define the *effective part* of a divisor D as $\epsilon(D) = \sum_P n_P(P)$, where $n_P \geq 0$. For example, the divisor $D = (P)+(Q)-2(\mathcal{O})$ is not effective, but the effective part is $\epsilon(D) = (P) + (Q)$. By the *size* of D, we mean the degree of the effective part, so in our example, although $\mathrm{Deg}(D) = 0$, it is size 2, since $\mathrm{Deg}(\epsilon(D)) = 2$.

Example 3.2.1 (Magma script). Consider the divisor $D = (P_1)+...+(P_{11})-11(\mathcal{O})$ (with $\mathrm{Deg}(\epsilon(D)) = 11$) as an element of $\mathrm{Pic}^0(E)$ on $E/\mathbb{F}_q : y^2 = x^3 + ax + b$, where the P_i are not necessarily distinct. To find a divisor that is equivalent to D, we can construct function $\ell_{10} : y = a_{10}x^{10} + ... + a_1x + a_0$ to interpolate the distinct points in $\mathrm{supp}(D)$ with appropriate multiplicities. Substituting ℓ_{10} into E gives a degree 20 polynomial in x, the roots of which reveals the 20 affine points of intersection (counting multiplicities) between ℓ_{10} and E. We already know 11 of these points (the P_i's), so let $P_1', ...P_9'$ be the other 9. An important point to note is that these points are not necessarily defined over $\mathbb{F}_q$. Since $(\ell_{10}) = \sum_{i=1}^{11}(P_i) + \sum_{i=1}^{9}(P_i') - 20(\mathcal{O}) \in \mathrm{Prin}(E)$, $D' = -(\sum_{i=1}^{9}(P_i') - 9(\mathcal{O}))$ is a divisor equivalent to D in $\mathrm{Pic}^0(E)$, i.e. $D' \sim D$. We can repeat this process, interpolating the points in $\mathrm{supp}(D')$ with a degree 8 polynomial ℓ_8 : $y = a_8'x^8 + ... + a_1'x + a_0'$, which will intersect E (in the affine sense) 16 times, giving 7 new intersection points, thereby finding a divisor $D'' = \sum_{i=1}^{7}(P_i'')-7(\mathcal{O})$ equivalent to D', meaning $D'' \sim D$. It is easy to infer that the number of new roots (maximum number of divisors in the consecutive supports) decreases each time by two, so that in two more steps we will arrive at $\tilde{D} = (\tilde{P}_1)+(\tilde{P}_2)+(\tilde{P}_3)-3(\mathcal{O})$. We can interpolate the three points in $\mathrm{supp}(\tilde{D})$ with a quadratic function $\tilde{\ell} : y = \tilde{a}_2x^2 + \tilde{a}_1x + \tilde{a}_0$ that clearly intersects E at one more affine point, say Q. That is, $(\tilde{\ell}) = (\tilde{P}_1) + (\tilde{P}_2) + (\tilde{P}_3) + (Q) - 4(\mathcal{O})$, and since $(\tilde{\ell}) \in \mathrm{Prin}(E)$, then $(\tilde{D}) \sim (\mathcal{O}) - (Q)$. Lastly, the vertical line $\tilde{v}$ has divisor $(\tilde{v}) = (Q) + (R) - 2(\mathcal{O})$, meaning $(\mathcal{O}) - (Q) \sim (R) - (\mathcal{O})$, which gives $(\tilde{D}) \sim (R) - (\mathcal{O})$. To summarise, we started with a divisor $D = (P_1) + ...(P_{11}) - 11(\mathcal{O})$ which had size 11, and

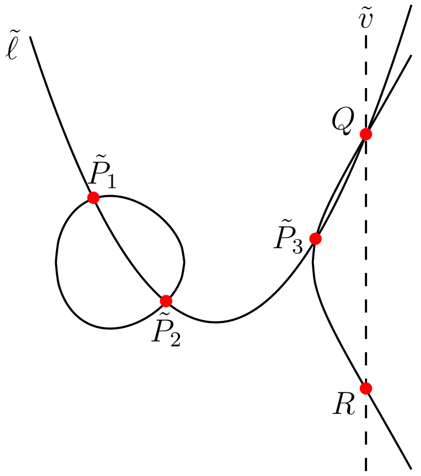

Figure 3.4: Reducing $\tilde{D}$ to $(R) - (\mathcal{O})$ in $\mathrm{Pic}^0(E)$.

reduced to the equivalent divisor $(R) - (\mathcal{O}) \sim D$ in $\mathrm{Pic}^0(E)$ which has size 1.

The above example illustrates a key consequence of one of the most central theorems in our study: the *Riemann-Roch* theorem. To present the theorem in its generality requires a few more definitions than we need for our exposition, so for the full story we refer the reader to any of [Ful08, §8], [Sil09, §II.5], [Gal12, §8.7]. The important corollary we use is the following: for any curve C, there is a unique minimal integer g, called the *genus* of C, such that any divisor $D \in \mathrm{Pic}^0(C)$ is equivalent to a divisor D' with $\mathrm{Deg}(\epsilon(D')) \leq g$. Elliptic curves E are curves of genus $g = 1$, meaning that every $D \in \mathrm{Pic}^0(E)$ can be written as $(P_1) - (Q_1)$; this is why we were able to *reduce* the divisor in Example 3.2.1 to $(R) - (\mathcal{O})$.

We will only be dealing with elliptic curves in this text, since they have proved most successful in the context of pairings, but for now it aids one's understanding to see where elliptic curves fit in a slightly broader context. Assuming an odd characteristic field, a general ("imaginary quadratic") hyperelliptic curve of genus g is a generalisation of an elliptic curve, which can be written as

$$C_g : y^2 = x^{2g+1} + f_{2g}x^{2g} + ... + f_1x + f_0. \tag{3.3}$$

Each divisor $D \in \mathrm{Pic}^0(C_g)$ has a unique *reduced* representative of the form

$$(P_1) + (P_2) + ... + (P_n) - n(\mathcal{O}),$$

where $n \leq g$, $P_i \neq -P_j$ for all $i \neq j$, and no P_i satisfying $P_i = -P_i$ appears more than once [BBC+09, §2.3]. The following examples illustrate this in the case of genus 2 and genus 3 respectively.

Example 3.2.2 (Magma script). A general (odd characteristic field) hyperelliptic curve of genus $g = 2$ is given (via Equation (3.3)) as $C_2 : y^2 = x^5 + f_4x^4 + ... + f_0$; we give a typical depiction in Figure 3.5. Suppose we have a divisor $D = (P_1) + (P_2) + (P_3) + (P_4) - 4(\mathcal{O}) \in \mathrm{Pic}^0(C_2)$, the affine support of which is depicted in red.

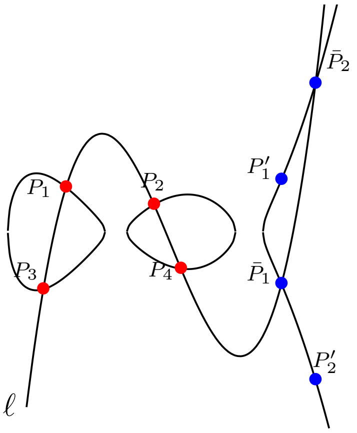

Figure 3.5: Reducing $D = \sum_{i=1}^{4}((P_i) - (\mathcal{O}))$ to $D' = \sum_{i=1}^{2}((P'_i) - (\mathcal{O})) \sim D$.

The Riemann-Roch theorem guarantees a (unique) equivalent divisor of the form $(P'_1) + (P'_2) - 2(\mathcal{O})$. We find it by constructing the cubic function $\ell : y = a_3x^3 + ... + a_0$ that has 4 zeros corresponding to the effective part of D, and therefore 4 poles at $\mathcal{O}$. Substitution of ℓ into E reveals two more points of intersection, $\bar{P}_1$ and $\bar{P}_2$, meaning $(\ell) = (P_1)+(P_2)+(P_3)+(P_4)+(\bar{P}_1)+(\bar{P}_2)-6(\mathcal{O})$. Since $(\ell) \in \mathrm{Prin}(C_2)$, then $D = D - (\ell)$ in $\mathrm{Pic}^0(C_2)$ meaning $D \sim 2(\mathcal{O}) - (\bar{P}_1) - (\bar{P}_2)$. As usual, we reverse the ordering (so the effective part is affine) by making use of the vertical lines v_1 and v_2 with divisors $(v_1) = (\bar{P}_1) + (P'_1) - 2(\mathcal{O})$ and $(v_2) = (\bar{P}_2) + (P'_2) - 2(\mathcal{O})$, to write $2(\mathcal{O}) - (\bar{P}_1) - (\bar{P}_2) = 2(\mathcal{O}) - (\bar{P}_1) - (\bar{P}_2) + (v_1) + (v_2) = (P'_1) + (P'_2) - 2(\mathcal{O}) = D'$, meaning $D \sim D'$. We have reduced a divisor D with $\mathrm{Deg}(\epsilon(D)) = 4$ to a divisor D' with $\mathrm{Deg}(\epsilon(D')) = 2 \leq g$. Note that the points in the support of D' are not necessarily defined over $\mathbb{F}_q$. Also note that trying to reduce D' any further, say by running a line $\ell' : y = \lambda x + \nu$ through P'_1 and P'_2, will not work in general, since this line will intersect E in 3 more places, creating an unreduced divisor D'' with $\mathrm{Deg}(\epsilon(D'')) = 3 > g$.

Example 3.2.3 (Magma script). Consider a general genus 3 hyperelliptic curve $C_3 : y^2 = x^7 + f_6x^6 + ... + f_0$; a typical depiction is given in Figure 3.6, with a vertically magnified Figure version in 3.7. Consider the divisor $D = \sum_{i=1}^{6}((P_i) - (\mathcal{O})) \in \mathrm{Pic}^0(C_3)$, the affine support of which is the red points in Figure 3.6.

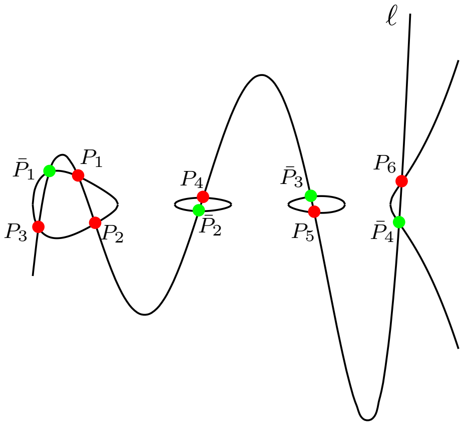

Figure 3.6: The first stage of reducing $D = \sum_{i=1}^{6}((P_i) - (\mathcal{O}))$.

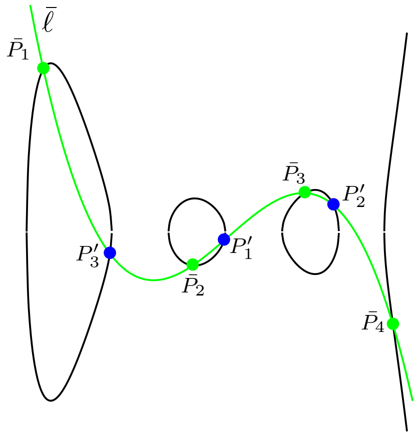

Figure 3.7: The second (and final) stage of divisor reduction.

We reduce D by determining the other points of intersection between the quintic interpolator $\ell : y = a_5x^5 + \ + a_0$ and C_3, of which there are 4: $\bar{P}_1, ..., \bar{P}_4$ depicted in green on C_3. $(\ell) = 0$ in the divisor class group so $\sum_{i=1}^{6}((P_i) - (\mathcal{O})) + \sum_{i=1}^{4}((\bar{P}_i) - (\mathcal{O})) = 0$, but the degree of the effective part of $\sum_{i=1}^{4}((\bar{P}_i) - (\mathcal{O}))$ is still larger than g, so obtaining the unique reduced divisor requires further reduction. Namely, the cubic function $\bar{\ell} : y = \bar{a}_3x^3 + ... + \bar{a}_0$ (depicted in green) interpolates the four green points and (when substituted into C_3) clearly intersects C_3 in another 3 affine points, depicted in blue. Thus, $\sum_{i=1}^{4}((\bar{P}_i) - (\mathcal{O})) + \sum_{i=1}^{3}((P_i') - (\mathcal{O})) = 0$, which means that $D \sim D' = \sum_{i=1}^{3}((P_i') - (\mathcal{O}))$ in the divisor class group, and D' is the unique representative of D since $\mathrm{Deg}(\epsilon(D')) = 3 \leq g$.

As mentioned prior to these higher genus examples, the reason this text will only be discussing (genus 1) elliptic curves is because in the arena of pairing-based cryptography, the raw speed of elliptic curves is currently unrivalled by their higher genus counterparts, and all of the state-of-the-art implementations take place in the genus 1 setting.

The elliptic curve group law enjoys a (relatively speaking) very simple, almost entirely elementary description, the only exception being the introduction of projective space for the formal definition of $\mathcal{O}$. Namely, we were able to describe the chord-and-tangent rule without the language of divisors or the definition of the divisor class group, which is not the case for other curves or general abelian varieties. This is because of the one-to-one correspondence between the divisor class group $\mathrm{Pic}^0(E)$ and the points on E we briefly mentioned in Example 3.1.3, i.e. the group homomorphism $P \mapsto (P) - (\mathcal{O})$ (see [Sil09, III.3.4] [Gal12, Th. 7.9.8, Th. 7.9.9]). Thus, in the elliptic curve setting, we can simply talk about the group elements being points, rather than divisors. In higher genera this does not happen; group elements are no longer points, but rather divisor classes in $\mathrm{Pic}^0(E)$ with multiple elements in their support.

Nevertheless, as we will see in the coming chapters, the language of divisors is absolutely essential in the description of elliptic curve pairings, where the objective is to compute very large (degree) functions on E with prescribed divisors, and then evaluate these functions at other divisors[1]. Evaluating a function $f \in \mathbb{F}_q(E)$ at a divisor $D = \sum_{P \in E} n_P(P)$ has a natural definition, provided the divisors (f) and D have disjoint supports:

$$f(D) = \prod_{P \in E} f(P)^{n_P}. \tag{3.4}$$

The stipulation of disjoint supports is clearly necessary for $f(D)$ to be non-trivial, since $P \in \mathrm{supp}((f))$ implies P is a zero or pole of f on E, meaning $f(P)^{n_P}$ would be either zero or infinity respectively.

Example 3.2.4 (Magma script). Consider $E/\mathbb{F}_{163} : y^2 = x^3 - x - 2$, with $P = (43, 154)$, $Q = (46, 38)$, $R = (12, 35)$ and $S = (5, 66)$ all on E. Let $\ell_{P,Q}$, $\ell_{P,P}$ and $\ell_{Q,Q}$ be the lines joining P and Q, tangent to P, and tangent to Q on E respectively, computed as $\ell_{P,Q} : y{+}93x{+}85$, $\ell_{P,P} : y{+}127x{+}90$, $\ell_{Q,Q} : y{+}13x{+}16$. Let $D_1 = 2(R) + (S)$, $D_2 = 3(R) - 3(S)$ and $D_3 = (R) + (S) - 2(\mathcal{O})$. We can compute $\ell_{P,Q}(D_1) = (y_R + 93x_R + 85)^2(y_S + 93x_S + 85) = 122$, or $\ell_{P,P}(D_2) = (y_R + 127x_R + 90)^3/(y_S + 127x_S + 90)^3 = 53$, but we can not evaluate any of these functions at D_3, since $\mathcal{O} \in \mathrm{supp}(D_3)$, and $\mathcal{O}$ is also in the supports of $(\ell_{P,Q})$, $(\ell_{P,P})$, $(\ell_{Q,Q})$. Let $\ell'_{P,P} = 17\ell_{P,P}$ so that $\ell'_{P,P} = 17y + 40x + 63$, and that $\ell'_{P,P}(D_2) = (17y_R + 40x_R + 63)^3/(17y_S + 40x_S + 63)^3 = 53 = \ell_{P,P}(D_2)$. This is true in general, i.e. that if $g = cf$ for some constant $c \in \overline{\mathbb{F}}_q$, then $f(D) = g(D)$

[1] We will also see that we do not actually compute these very large functions explicitly before evaluating them.

if D has degree zero; the constant c will cancel out because $\mathrm{Deg}(D) = 0$ implies the numerator and denominator of $f(D)$ (identically $g(D)$) have the same total degree.

3.3 Weil reciprocity

We conclude our chapter on divisors (as Galbraith does [Gal05, §IX.2, Th. IX.3], where he also gives a proof) with a central theorem that lies at the heart of many of the proofs of cryptographic pairing properties.

Theorem 3.1 (Weil reciprocity). *Let f and g be non-zero functions on a curve such that (f) and (g) have disjoint supports. Then $f((g)) = g((f))$.*

Most of the functions on E that we have seen so far contain $\mathcal{O}$ in their support. In the first example (3.3.1) we will choose one of the functions such that this is not the case, meaning that Theorem 3.1 can be applied instantly, whilst in the second example we will show how to alleviate this problem when it arises by modifying either of the functions.

Example 3.3.1 (Magma script). Let $E/\mathbb{F}_{503} : y^2 = x^3 + 1$. Consider the functions $f : \frac{20y+9x+179}{199y+187x+359} = 0$ and $g : y + 251x^2 + 129x + 201 = 0$ on E. The divisor of f is $(f) = 2(433, 98) + (232, 113) - (432, 27) - 2(127, 258)$, and the divisor of g is $(g) = (413, 369) + (339, 199) + (147, 443) + (124, 42) - 4(\mathcal{O})$. The supports are clearly disjoint, so we first compute $f((g))$ as

$$\frac{\left(\frac{20\cdot369+9\cdot413+179}{199\cdot369+187\cdot413+359}\right)\cdot\left(\frac{20\cdot199+9\cdot339+179}{199\cdot199+187\cdot339+359}\right)\cdot\left(\frac{20\cdot443+9\cdot147+179}{199\cdot443+187\cdot147+359}\right)\cdot\left(\frac{20\cdot42+9\cdot124+179}{199\cdot42+187\cdot124+359}\right)}{\left(\frac{20\cdot1+9\cdot0+179\cdot0}{199\cdot1+187\cdot0+359\cdot0}\right)^4} = 321.$$

Notice that f was cast into projective space as $f : \frac{20Y+9X+179Z}{199Y+187X+359Z}$ for the evaluation at $\mathcal{O} = (0 : 1 : 0)$ on the denominator. Now, for $g((f))$ we have

$$\frac{\left(98 + 251\cdot433^2 + 129\cdot433 + 201\right)^2\cdot\left(113 + 251\cdot232^2 + 129\cdot232 + 201\right)}{\left(258 + 251\cdot127^2 + 129\cdot127 + 201\right)^2\cdot\left(27 + 251\cdot432^2 + 129\cdot432 + 201\right)} = 321.$$

Example 3.3.2 (Magma script). Let $P, Q, R, S, T, U \in E$, such that $T = -(R + S)$. Further let $\ell' : y = (\lambda' x + \nu')$ be the tangent to E at P and $\ell : y = (\lambda x + \nu)$ be the line between R, S and T depicted in Figure 3.8, so that $(\ell') = 2(P) + (-[2]P) - 3(\mathcal{O})$ and $(\ell) = (R) + (S) + (T) - 3(\mathcal{O})$. Suppose we wish to compute $\ell(\ell')$.

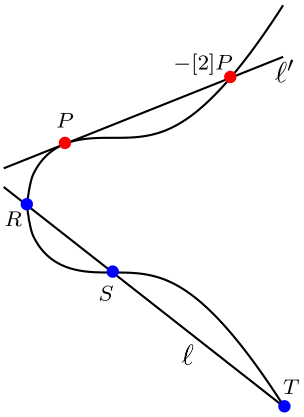

Figure 3.8: $\mathrm{supp}(\epsilon((\ell)))$ and $\mathrm{supp}(\epsilon((\ell')))$.

At this point it does not make sense to compute $\ell(\ell')$ (or $\ell'(\ell)$) since $\mathrm{supp}((\ell))\cap\mathrm{supp}((\ell')) = \{\mathcal{O}\}$. We can fix this by finding a divisor equivalent to, say (ℓ), whose support is disjoint to $\mathrm{supp}((\ell'))$. This is easily done by picking a random point $U \notin \mathrm{supp}(\ell')$ and defining $D = (R+U)+(S+U)+(T+U)-3(U)$. To see that $D \sim \ell$, observe that $(R+U)-(U) = (R)-(\mathcal{O})$ by writing down the divisor of the quotient of the sloped and vertical lines in the addition of R and U on E. Computing $\ell(\ell')$ is therefore the same as computing $D(\ell')$, but this computation would then require finding a new function on E with divisor D, so we can invoke Theorem 3.1 and instead compute $\ell'(D)$ as

$$\ell'(D) = \frac{(y_{R'} - (\lambda' x_{R'} + \nu'))\,(y_{S'} - (\lambda' x_{S'} + \nu'))\,(y_{T'} - (\lambda' x_{T'} + \nu'))}{(y_U - (\lambda' x_U + \nu'))^3},$$

where $R' = (x_{R'}, y_{R'}) = R+U$, $S' = (x_{S'}, y_{S'}) = S+U$ and $T' = (x_{T'}, y_{T'}) = T+U$ are all such that $R', S', T' \notin \mathrm{Supp}(\ell')$, so that $\ell'(D)$ is the same as $\ell(\ell')$ by Weil reciprocity.

3.4 Chapter summary

We introduced the important concept of divisors on curves. We illustrated their particular usefulness when used to describe functions on curves, since such a function is well defined (up to constant) by its points of intersection with a curve, and these are precisely what the divisor of the function encapsulates. We defined the *divisor class group* of a (hyperelliptic) curve and discussed that for the case of elliptic curves, there is a bijection between this group and the set of points on the curve, so that we can simply talk about group elements as points on E rather than divisors. We further illustrated several useful properties and theorems that play a big role in the realm of algebraic geometry, most notably the Riemann-Roch theorem and Weil reciprocity. For the most part we specified the context to elliptic curves over finite fields, but all of the results and properties discussed above apply to arbitrary curves over arbitrary fields.