Chapter 4

Elliptic curves as pairing groups

The purpose of this chapter is to define the elliptic groups that are used in cryptographic pairings. We start with the most abstract definition [Sil10]: a pairing is a *bilinear* map on an abelian group M taking values in some other abelian group R

$$\langle \cdot\, , \cdot \rangle : M \times M \to R.$$

Suppose that the binary group operations in M and R are respectively denoted by $+$ and $*$. The bilinearity property of the above map (that classifies it a pairing) means that, for $x, y, z \in M$, we have

$$\begin{aligned} \langle x + y, z \rangle &= \langle x, z \rangle * \langle y, z \rangle, \\ \langle x, y + z \rangle &= \langle x, y \rangle * \langle x, z \rangle. \end{aligned}$$

That is, the map $\langle \cdot, \cdot \rangle$ is linear in both inputs.

It is this bilinearity property that makes pairings such a powerful primitive in cryptography. For our purposes we often find it advantageous to slightly relax the condition that the two arguments in the map come from the same group, and allow them to come from cyclic groups of the same order (which are therefore isomorphic). Thus, in the abundance of literature related to cryptography, the

notation commonly used for the bilinear map is

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T.$$

Our primary objective in this chapter is to define the two groups $\mathbb{G}_1$ and $\mathbb{G}_2$. The definition of $\mathbb{G}_T$ will come with the definition of the pairings in the next chapter.

Currently, the only known instantiations of pairings suitable for cryptography are the Weil and Tate pairings on divisor class groups of algebraic curves, and in the simplest and most efficient cases, on elliptic curves. Let $\mathbb{F}_{q^k}$ be some finite extension of $\mathbb{F}_q$ with $k \geq 1$. The groups $\mathbb{G}_1$ and $\mathbb{G}_2$ are defined in $E(\mathbb{F}_{q^k})$, and the *target group* $\mathbb{G}_T$ is defined in the multiplicative group $\mathbb{F}_{q^k}^*$, so we usually write $\mathbb{G}_1$ and $\mathbb{G}_2$ additively, whilst we write $\mathbb{G}_T$ multiplicatively. Thus, for $P, P' \in \mathbb{G}_1$ and $Q, Q' \in G_2$, the bilinearity of e means that

$$\begin{aligned} e(P + P', Q) &= e(P, Q) \cdot e(P', Q), \\ e(P, Q + Q') &= e(P, Q) \cdot e(P, Q'), \end{aligned}$$

from which it follows that, for scalars $a, b \in \mathbb{Z}$, we have

$$e([a]P, [b]Q) = e(P, [b]Q)^a = e([a]P, Q)^b = e(P, Q)^{ab} = e([b]P, [a]Q). \tag{4.1}$$

Even though we are yet to define $\mathbb{G}_1$, $\mathbb{G}_2$ or $\mathbb{G}_T$, and we are still a while away from beginning the discussion of how the pairing $e(P, Q)$ is computed, it helps to immediately see the bilinearity property of pairings in context.

Example 4.0.1 (Magma script). Let $q = 7691$ and let $E/\mathbb{F}_q : y^2 = x^3 + 1$. Suppose $\mathbb{F}_{q^2}$ is constructed $\mathbb{F}_{q^2} = \mathbb{F}_q(u)$ where $u^2 + 1 = 0$. Let $P = (2693, 4312) \in E(\mathbb{F}_q)$ and $Q = (633u + 6145, 7372u + 109) \in E(\mathbb{F}_{q^2})$. $\#E(\mathbb{F}_q) = 2^2 \cdot 3 \cdot 641$ and $\#E(\mathbb{F}_{q^2}) = 2^4 \cdot 3^2 \cdot 641^2 = \#E(\mathbb{F}_q)^2$. P and Q were especially chosen (we will see why later) to be in different subgroups of the same prime order $r = |\langle P \rangle| = |\langle Q \rangle| = 641$. The Weil pairing $e(\cdot, \cdot)$ of P and Q is $e(P, Q) = 6744u + 5677 \in \mathbb{F}_{q^2}^*$. In fact, $r \mid \#\mathbb{F}_{q^2}$, and $e(P, Q)$ actually lies in a subgroup of $\mathbb{F}_{q^2}$, namely the r-th roots of unity $\mu_r \in \mathbb{F}_{q^2}$, meaning that $e(P, Q)^r = 1$. We are now in a position to illustrate some examples of bilinearity. Thus, take any $a \in \mathbb{Z}_r$ and $b \in \mathbb{Z}_r$, say $a = 403$ and $b = 135$, and see that $[a]P = (4903, 2231)$ and $[b]Q = (5806u + 1403, 6091u + 2370)$. We can compute $e([a]P, Q) = 3821u + 7025$

and verify that $e([a]P, Q) = 3821u + 7025 = (6744u + 5677)^{403} = e(P, Q)^a$; or $e(P, [b]Q) = 248u + 5$ to see that $e(P, [b]Q) = 248u + 5 = (6744u + 5677)^{135} = e(P, Q)^b$; or $e([a]P, [b]Q) = 2719u + 2731 = (6744u + 5677)^{561} = e(P, Q)^{a \cdot b \bmod r}$. Note that since $e(P, Q) \neq 1 \in \mu_r$, $e([a]P, [b]Q)$ will only be trivial if $r \mid ab$, which implies $r \mid a$ or $r \mid b$, meaning either (or both) of $[a]P$ or $[b]Q$ must be $\mathcal{O}$. Thus, $e(P, Q) \neq 1$ guarantees non-trivial pairings for non-trivial arguments; this is a cryptographically necessary property that is called *non-degeneracy*.

Following Example 4.0.1 above, if a pairing e is bilinear, non-degenerate and efficiently computable, e is called an *admissible pairing*.

Remark 4.0.1 (ECC vs. PBC). This informal remark is intended as a point of clarification for PBC newcomers. Our confusion in the early days of digesting the vast amount of literature was in part alleviated by one paragraph in Lynn's thesis that helped put the relationship between ECC and PBC in a wider context. The only known admissible pairings that are suitable for cryptography are the Weil and Tate pairings on algebraic curves. The fact that these pairings can be defined on elliptic curves, which were already a highly attractive cryptographic setting before pairings arrived on the scene, is, as Lynn puts it, a "happy coincidence". Cryptographers would have welcomed secure, admissible pairings in any suitable form, but the fact that they were handed down from the realm of algebraic geometry and are computed on elliptic curves makes them "even more attractive" [Lyn07, §2.9].

In cryptography we need more properties than the three which constitute an admissible pairing. The magic of the bilinearity property in (4.1) that gives pairing-based primitives increased functionality over traditional primitives is useless unless discrete logarithm related problems within all three groups remain intractable. Example 4.0.1 gives an admissible pairing, but because the toy sizes of $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ clearly offer no resistance in regards to their respective discrete logarithm problems, such a pairing instance would clearly never be used. However, if the size r of all three groups was inflated to be much larger (say 512 bits), then the corresponding pairing could meet current security requirements and resist all known attacks. We present an alternative bilinear pairing that meets the admissible requirements, but (regardless of how large the group sizes are) is still not suitable for PBC. This example too, is taken from Lynn's thesis [Lyn07, §1.9].

Example 4.0.2 (Magma script). Let $r > 1$ be an integer. Suppose $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ has $\mathbb{G}_1 = \mathbb{G}_T = \mathbb{Z}_r^*$ and $\mathbb{G}_2 = \mathbb{Z}_{r-1}^+$, and is defined by $e : (g, a) = g^a$. Notice that for $g, g' \in \mathbb{G}_1$, we have $e(g \cdot g', a) = e(g, a) \cdot e(g', a)$, and for $a, a' \in \mathbb{G}_2$ we have $e(g, a + a') = e(g, a) \cdot e(g, a')$. Although e is then clearly bilinear, the discrete logarithm problem in $\mathbb{G}_2$ is easy, so the power of the bilinear map becomes somewhat redundant. It is interesting to see, however, that we can still state some of the classical problems in terms of the above pairing. For example, if we set r to be a large prime, then the standard discrete logarithm problem becomes: given $g \in \mathbb{G}_1$, $h \in \mathbb{G}_T$, find $a \in \mathbb{G}_2$ such that $e(g, a) = h$.

4.1 The r-torsion

We now turn our focus towards concretely defining the groups $\mathbb{G}_1$ and $\mathbb{G}_2$. Having not yet seen how pairings are computed, we will need to make some statements regarding what we need out of $\mathbb{G}_1$ and $\mathbb{G}_2$ that will really only tie together when the definitions of the Weil and Tate pairings come in the following chapter. The main such statement is that computing the pairing $e(P, Q)$, in either the Weil or Tate sense, requires that P and Q come from disjoint cyclic subgroups of the same prime[1] order r. At this point we can only hint towards why by referring back to the stipulation of disjoint supports that was made in the statement of Weil reciprocity (Theorem 3.1), and claiming that if P and Q are in the same cyclic subgroup, then the pairing computation essentially fails because supports of the associated divisors are forced to undesirably coincide.

We have already seen an example (4.0.1) of how we can find more than one cyclic subgroup of order r, when $E(\mathbb{F}_q)$ itself only contains one subgroup. Namely, we extended $\mathbb{F}_q$ to $\mathbb{F}_{q^2}$ and saw that $E(\mathbb{F}_{q^2}) \setminus E(\mathbb{F}_q)$ had at least one other subgroup of order r, where we were able to define Q and subsequently compute $e(P, Q)$. This is precisely the way we obtain two distinct order-r subgroups in general: we find the smallest extension $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$ such that $E(\mathbb{F}_{q^k})$ captures more points of order r. The integer $k \geq 1$ that achieves this is called the *embedding degree*, and it plays a crucial role in pairing computation. Also at the heart of our discussion then, is the entire group of points of order r on $E(\overline{\mathbb{F}}_q)$, called the r-torsion, which is denoted by $E[r]$ and defined as $E[r] = \{P \in E : [r]P = \mathcal{O}\}$.

[1] There has been some work that exploits additional functionality if r is composite, e.g. an RSA modulus $n = pq$, but we do not consider this much less common and much less efficient setting – see [BGN05, Fre10, BRS11, Lew12] for more details.

The following result (see [ACD+05, Th. 13.13] or [Sil09, Ch. III, Cor. 6.4(b)]) is quite remarkable; it tells us not only the cardinality of $E[r]$, but its structure too. If K is any field with characteristic zero or prime to r, we have

$$E[r] \cong \mathbb{Z}_r \times \mathbb{Z}_r. \tag{4.2}$$

This means that in general, $\#E[r] = r^2$. Furthermore, since the point at infinity $\mathcal{O}$ overlaps into all order r subgroups, Equation (4.2) implies that (for prime r) the r-torsion consists of $r+1$ cyclic subgroups of order r. The following equivalent conditions for the embedding degree k also tell us precisely where $E[r]$ lies in its entirety. We note that the embedding degree is actually a function $k(q, r)$ of q and r, but we just write k since the context is usually clear.

- k is the smallest positive integer such that $r \mid (q^k - 1)$;
- k is the smallest positive integer such that $\mathbb{F}_{q^k}$ contains all of the r-th roots of unity in $\overline{\mathbb{F}}_q$ (i.e. $\mu_r \subset \mathbb{F}_{q^k}$);
- k is the smallest positive integer such that $E[r] \subset E(\mathbb{F}_{q^k})$.

If $r \| \#E(\mathbb{F}_q)$ (i.e. $r \mid \#E(\mathbb{F}_q)$ but $r^2 \nmid \#E(\mathbb{F}_q)$), then the r-torsion subgroup in $E(\mathbb{F}_q)$ is unique. In this case, $k > 1$ and (4.2) implies that $\mathbb{F}_{q^k}$ is the smallest field extension of $\mathbb{F}_q$ which produces any more r-torsion points belonging to $E(\mathbb{F}_{q^k}) \setminus E(\mathbb{F}_q)$. In other words, once the extension field is big enough to find one more point of order r (that is not defined over the base field), then we actually find all of the points in $E[r] \cong \mathbb{Z}_r \times \mathbb{Z}_r$. Scott [Sco04] describes this phenomenon more poetically:

> "... something rather magical happens when a curve with the same equation is considered over the field $\mathbb{F}_{q^k}$ for a certain value of k. The group structure undergoes a strange blossoming, and takes on a new, more exotic character."

We also find Scott's depiction of the torsion subgroup $E[r]$ especially instructive [Sco04, Sco07a], so we use it in the following examples and throughout the rest of this chapter.

Example 4.1.1 (Magma script). Let $q = 11$, and consider $E/\mathbb{F}_q : y^2 = x^3 + 4$. $E(\mathbb{F}_q)$ has 12 points, so take $r = 3$ and note (from Equation (4.2)) that there are 9 points in the 3-torsion. Only 3 of them are found in $E(\mathbb{F}_q)$, namely $(0, 2)$,

$(0, 9)$ and $\mathcal{O}$, which agrees with the fact that the embedding degree $k \neq 1$, since $(q^1 - 1) \not\equiv 0 \bmod r$. However, $(q^2 - 1) \equiv 0 \bmod r$ which means that the embedding degree is $k = 2$, so we form $\mathbb{F}_{q^2} = \mathbb{F}_q(u)$, with $u^2 + 1$. Thus, we are guaranteed to find the whole 3-torsion in $E(\mathbb{F}_{q^2})$, and it is structured as 4 cyclic subgroups of order 3; $\mathcal{O}$ overlaps into all of them – see Figure 4.1. We point out that although $\mathcal{O}$ is in the 3-torsion, it does not have order 3, but rather order 1 – points of order $d \mid r$ are automatically included in the r-torsion. Take any two

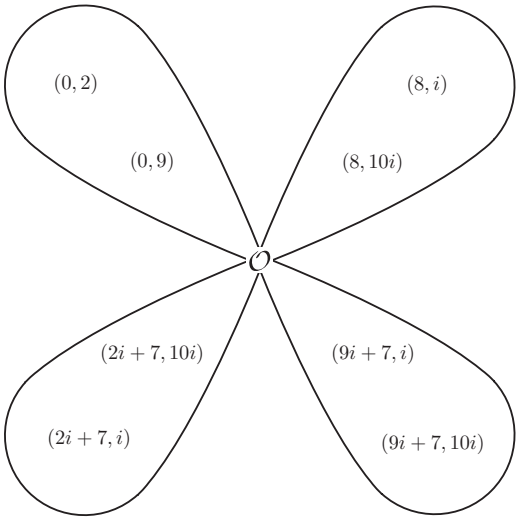

Figure 4.1: The 3-torsion: $E[3]$.

points $P, Q \in E[3] \setminus \{\mathcal{O}\}$ that are not in the same subgroup, neither of which are $\mathcal{O}$. The translation of Equation (4.2) is that any other point in $E[3]$ can be obtained as $[i]P + [j]Q$, $i, j \in \{0, 1, 2\}$. Fixing $P \neq \mathcal{O}$ and letting j run through $0, 1, 2$ lands $P + [j]Q$ in the other three subgroups of $E[3]$ (that are not $\langle Q \rangle$ – this corresponds to $P = \mathcal{O}$).

Example 4.1.2 (Magma script). In the rare case that $r^2 \mid \#E$, it is possible that the entire r-torsion can be found over $E(\mathbb{F}_q)$, i.e. that the embedding degree is $k = 1$. Consider $E/\mathbb{F}_{31} : y^2 = x^3 + 13$, which has 25 points, so take $r = 5$. Since $r \mid q - 1$, $k = 1$ and therefore $E[r] \subseteq E(\mathbb{F}_q)$; Figure 4.2 show the 6 cyclic subgroups of order 5 constituting $E[5] \cong \mathbb{Z}_5 \times \mathbb{Z}_5$. Of course, $r^2 \mid \#E(\mathbb{F}_q)$ does not necessarily imply that $E[r] \subseteq E(\mathbb{F}_q)$, as points of order r^2 are possible.

Before the next example, we introduce an important map that plays an intricate role within the r-torsion subgroups. Since we are working over finite extension fields of $\mathbb{F}_q$, it is natural that we find a useful contribution from Galois

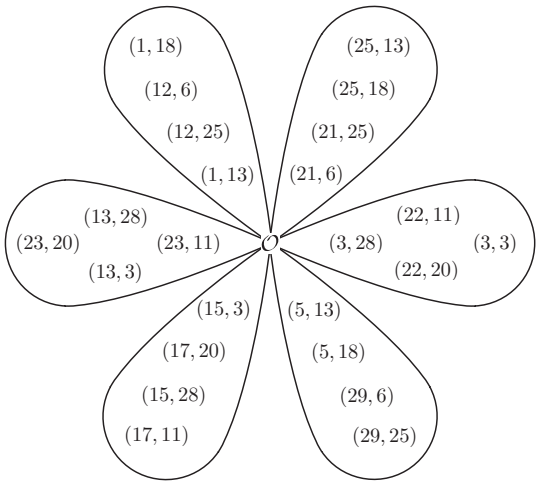

Figure 4.2: The 5-torsion: $E[5]$.

theory. Namely, the *trace map* of the point $P = (x, y) \in E(\mathbb{F}_{q^k})$ is defined as

$$\mathrm{Tr}(P) = \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q)} \sigma(P) = \sum_{i=0}^{k-1} \pi^i(P) = \sum_{i=0}^{k-1} (x^{q^i}, y^{q^i}),$$

where π is the q-power Frobenius endomorphism defined in Equation (2.7). Galois theory tells us that $\mathrm{Tr} : E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_q)$, so when $r \| \#E(\mathbb{F}_q)$ (which will always be the case from now on), then this map, which is actually a group homomorphism, sends all torsion points into one subgroup of the r-torsion. We illustrate in Example 4.1.3 before painting the general picture.

Example 4.1.3 (Magma script). We take $q = 11$ again, but this time with $E/\mathbb{F}_q : y^2 = x^3+7x+2$. $E(\mathbb{F}_q)$ has 7 points, so take $r = 7$. We already have $E(\mathbb{F}_q)[r]$, but to collect $E[r]$ in its entirety we need to extend $\mathbb{F}_q$ to $\mathbb{F}_{q^k}$. This time, the smallest integer k such that $(q^k - 1) \bmod 7 \equiv 0$ is $k = 3$, so we form $\mathbb{F}_{q^3} = \mathbb{F}_q(u)$ with $u^3 + u + 4 = 0$, and we are guaranteed that $E[7] \subset E(\mathbb{F}_{q^3})$. The entire 7-torsion has cardinality 49 and splits into 8 cyclic subgroups, as shown in Figure 4.2. To fit the points in, we use the power representation of elements in $\mathbb{F}_{q^3} = \mathbb{F}_q(u)$. In this case, for $P \in E(\mathbb{F}_{q^3})$, the trace map on E is $\mathrm{Tr}(P) = (x, y) + (x^q, y^q) + (x^{q^2}, y^{q^2})$. For the unique torsion subgroup $E(\mathbb{F}_q)[r]$, the Frobenius endomorphism is trivial ($\pi(P) = P$) so the trace map clearly acts as multiplication by k, i.e. $\mathrm{Tr}(P) = [k]P$. However, Tr will send every other element in the torsion into $E(\mathbb{F}_q)[r]$. For example, for $Q = (u^{481}, u^{1049})$ (in the subgroup pointing upwards), we have

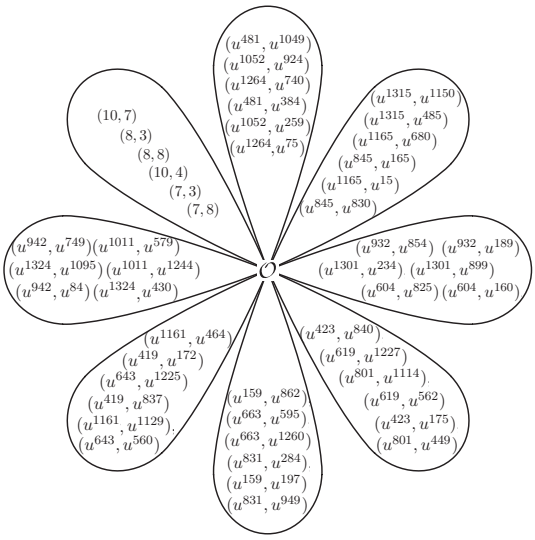

Figure 4.3: The 7-torsion: $E[7]$.

$\mathrm{Tr}(Q) = (8, 8)$; for $R = (u^{423}, u^{840})$ (the lower right subgroup), we have $\mathrm{Tr}(R) = (10, 7)$; for $S = (u^{1011}, u^{1244})$, we have $\mathrm{Tr}(S) = (8, 3)$. There is one other peculiar subgroup in $E[7]$ however, for which the trace map sends each element to $\mathcal{O}$. This occurs in general, and we are about to see that this has important consequences in PBC, but in our case this subgroup is the upper right group containing $T = (u^{1315}, u^{1150})$, i.e. $\mathrm{Tr}(T) = \mathcal{O}$, so $\mathrm{Tr} : \langle T \rangle \to \{\mathcal{O}\}$. One final point to note is that the embedding degree $k = 3$ also implies that the (six) non-trivial 7-th roots of unity are all found in $\mathbb{F}_{q^3}$ (but not before), i.e. $\mu_7 \setminus \{1\} \in \mathbb{F}_{q^3} \setminus \mathbb{F}_{q^2}$.

We now give a general depiction of the r-torsion $E[r]$. To do so, we need to discuss a few assumptions that apply most commonly to the scenarios we will be encountering. Firstly, we assume that $r \| \#E(\mathbb{F}_q)$ is prime and the embedding degree k (with respect to r) is $k > 1$. Thus, there is a unique subgroup of order r in $E[r]$ which is defined over $\mathbb{F}_q$, called the *base-field* subgroup; it is denoted by $\mathcal{G}_1$. Since the Frobenius endomorphism π acts trivially on $\mathcal{G}_1$, but nowhere else in $E[r]$, then it can be defined as $\mathcal{G}_1 = E[r] \cap \mathrm{Ker}(\pi - [1])$. That is, $\mathcal{G}_1$ is the $[1]$-*eigenspace* of π restricted to $E[r]$. There is another subgroup of $E[r]$ that can be expressed using an eigenspace of π. Referring back to Equation (2.8), we can easily deduce that the other eigenvalue of π is q, and we define another subgroup $\mathcal{G}_2$ of $E[r]$ as $\mathcal{G}_2 = E[r] \cap \mathrm{Ker}(\pi - [q])$. It turns out that this subgroup is precisely the peculiar subgroup we alluded to in Example 4.1.3. We call $\mathcal{G}_2$ the *trace zero* subgroup, since all $P \in \mathcal{G}_2$ have $\mathrm{Tr}(P) = \mathcal{O}$; this result is attributed

to Dan Boneh [Gal05, Lemma IX.16]. We illustrate in Figure 4.4.

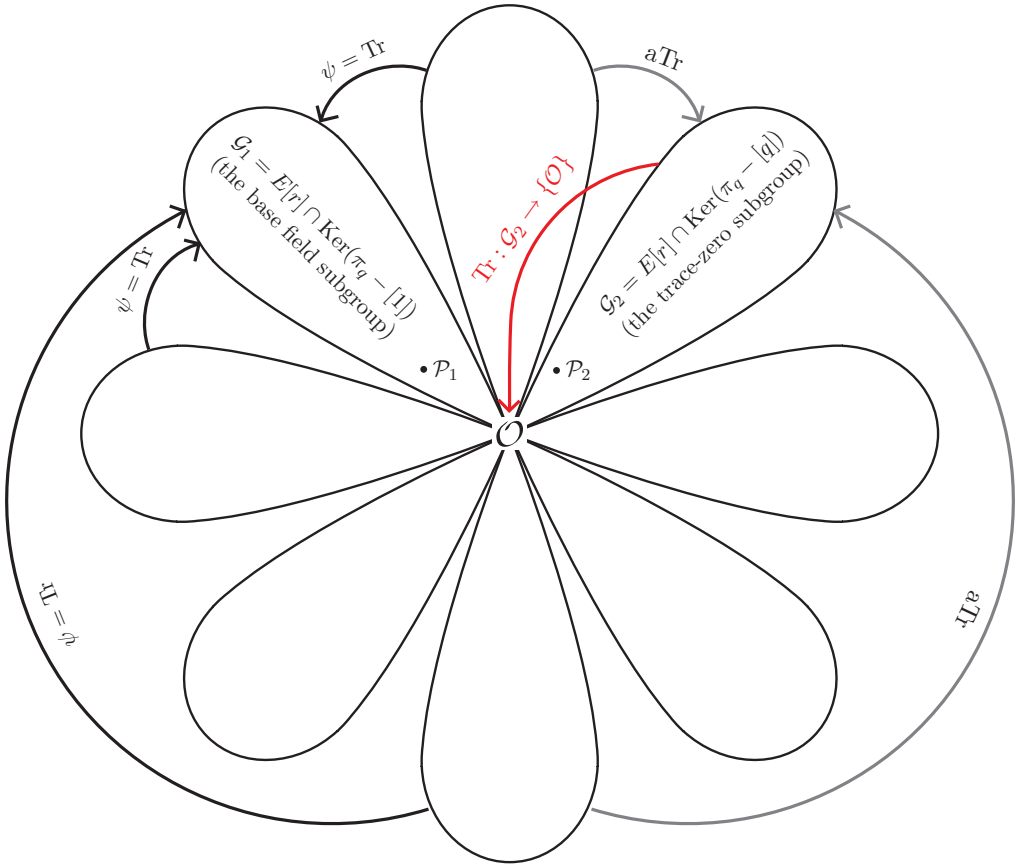

Figure 4.4: The behaviour of the trace and anti-trace maps on $E[r]$.

We can also map any $P \in E[r]$ to the trace zero subgroup $\mathcal{G}_2$ via the *anti-trace map* $\mathrm{aTr} : P \mapsto P' = [k]P - \mathrm{Tr}(P)$; showing that $\mathrm{Tr}(P') = \mathcal{O}$ is a worthwhile exercise for the reader.

To define our pairing, we need to specify the two groups $\mathbb{G}_1$ and $\mathbb{G}_2$: these $\mathbb{G}$'s are not to be confused with the $\mathcal{G}$'s that stand for two specific r-torsion subgroups, as $\mathbb{G}_1$ and $\mathbb{G}_2$ can be defined as any of the $r + 1$ groups in $E[r]$. As we will see however, there are many reasons we would like to specifically set $\mathbb{G}_1 = \mathcal{G}_1$ and $\mathbb{G}_2 = \mathcal{G}_2$, but as we will also see there are reasons that we may not want this to be the case. The existence of maps to and from the different torsion subgroups affects certain functionalities that cryptographers desire in a pairing-based protocol. These functionalities and the choices that are available to us will be discussed in a moment, but we must first look at one last map that

is available for a special class of curves.

Over prime fields, we call an elliptic curve E *supersingular*[2] if $\#E(\mathbb{F}_q) = q+1$. There are several other equivalent conditions [Sil09, Ch. V, Th. 3.1(a)], but the most meaningful property for our purposes is that a supersingular curve comes equipped with a *distortion map* ϕ; this is a non-($\mathbb{F}_q$-)rational map that takes a point in $E(\mathbb{F}_q)$ to a point in $E(\mathbb{F}_{q^k})$ [Gal05, §IX.7.2]. A curve which is not supersingular is called an *ordinary* curve, and it does not have such a map [Ver01, Th. 11]. We give two examples of elliptic curves that are supersingular, and show the behaviour of the distortion map ϕ within the torsion.

Example 4.1.4 (Magma script). Let $q = 59$, for which $E/\mathbb{F}_q : y^2 = x^3 + 1$ is supersingular, meaning $\#E(\mathbb{F}_q) = q + 1 = 60$, so take $r = 5$. The embedding degree is $k = 2$, so we construct the extension as $\mathbb{F}_{q^2} = \mathbb{F}_q(i)$, $i^2 + 1 = 0$. $\xi_3 = 24i + 29$ is a cube root of unity, for which the associated distortion map is $\phi : (x, y) \mapsto (\xi_3 x, y)$. The fact that ϕ^3 is equivalent to the identity map on E is illustrated in Figure 4.5.

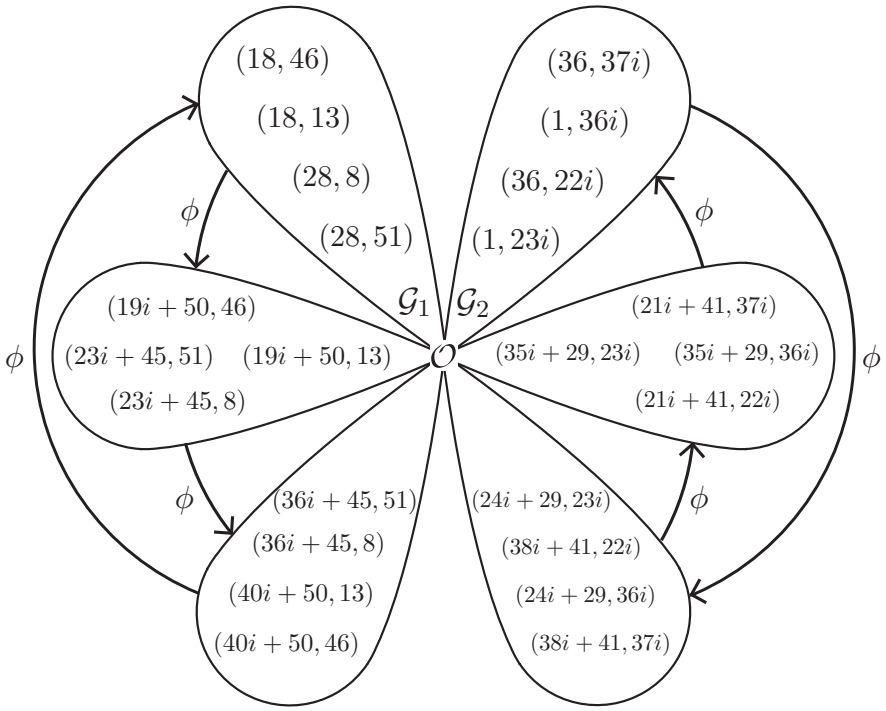

Figure 4.5: The distortion map $\phi : (x, y) \mapsto (\xi_3, y)$ on $E[5]$.

[2]This terminology should not be confused with the *singular* vs. *non-singular* definitions illustrated in, and discussed above, Figures 2.1-2.4.

Example 4.1.5 (Magma script). We take the same fields as the last example ($q = 59$, $\mathbb{F}_{q^2} = \mathbb{F}_q(i)$, $i^2 + 1 = 0$), but instead use the supersingular curve $E/\mathbb{F}_q : y^2 = x^3 + x$, which therefore also has $\#E(\mathbb{F}_q) = 60$. This time, the distortion map is $\phi : (x, y) \mapsto (-x, iy)$, from which it is easy to see that ϕ^4 is equivalent to the identity map on E. In Figure 4.6, we see that (in this case) the

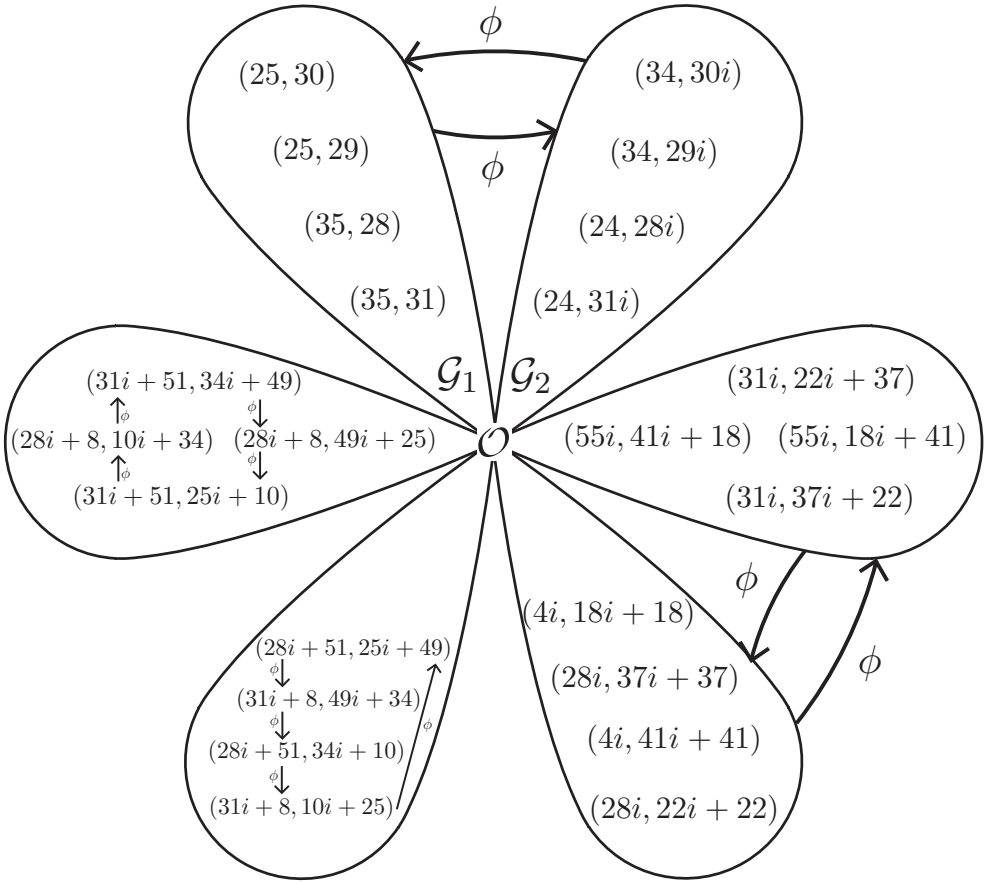

Figure 4.6: The distortion map $\phi : (x, y) \mapsto (-x, iy)$ on $E[5]$.

distortion map does not always move elements out of their subgroup, but rather restricting ϕ to, say the torsion subgroup generated by $(28i + 51, 25i + 49)$, gives an endomorphism on $\langle(28i + 51, 25i + 49)\rangle$. This hints towards one of the major optimisations in pairing computations. Namely, in Chapter 2 we saw the power of endomorphisms applied to ECC (specifically in Example 2.2.11), and in Chapter 7 we are going to see that endomorphisms on torsion subgroups (like the one above) can be used to great effect in PBC.

We summarise the available maps within the r-torsion. From any subgroup

in $E[r]$ that is not $\mathcal{G}_1$ or $\mathcal{G}_2$, we can always map into either $\mathcal{G}_1$ or $\mathcal{G}_2$ via the trace and anti-trace maps respectively. If E is ordinary, we do not have computable maps out of $\mathcal{G}_1$ or $\mathcal{G}_2$, otherwise if E is supersingular then the distortion map ϕ is a homomorphic map out of these two subgroups.

4.2 Pairing types

As we mentioned before the previous two examples, the interplay between the maps that are available in any given scenario gives rise to different functionalities within a pairing-based protocol. Galbraith *et al.* [GPS08] were the first to identify that all of the potentially desirable properties in a protocol cannot be achieved simultaneously, and therefore classified pairings into certain *types*. There are now four pairing types in the literature; Galbraith *et al.* originally presented three, but a fourth type was added soon after by Shacham [Sha05]. The pairing types essentially arise from observing the (practical) implications of placing $\mathbb{G}_1$ and $\mathbb{G}_2$ in different subgroups of $E[r]$; in fact, it will soon become obvious that it is always best to set $\mathbb{G}_1 = \mathcal{G}_1$, so the four types really are tied to the definition of $\mathbb{G}_2$. The main factors affecting the classification are the ability to hash and/or randomly sample elements of $\mathbb{G}_2$, the existence of an isomorphism $\psi : \mathbb{G}_2 \to \mathbb{G}_1$ which is often required to make security proofs work (see [GPS08]), and (as always) issues concerning storage and efficiency.

We follow the notation and descriptions of Chen *et al.* [CCS07], and describe each pairing type in turn. The illustrations of each type are in Figures 4.7-4.10, where the base-field group $\mathcal{G}_1 = E[r] \cap \mathrm{Ker}(\pi - [1])$ with generator $\mathcal{P}_1$ is always in the top left, whilst the trace-zero subgroup $\mathcal{G}_2 = E[r] \cap \mathrm{Ker}(\pi - [q])$ with generator $\mathcal{P}_2$ is always in the top right. Let P_1 be the generator of $\mathbb{G}_1$ and P_2 be the generator of $\mathbb{G}_2$. It should be born in mind that the pairing $e(P, Q)$ will only compute non-trivially if P and Q are in different subgroups.

- *Type 1 pairings.* This is the scenario where E is supersingular, meaning we can map out of $\mathcal{G}_1$ with ϕ. Thus, we set $\mathbb{G}_1 = \mathbb{G}_2 = \mathcal{G}_1$ (with $P_1 = P_2 = \mathcal{P}_1$). When it comes time to compute a pairing e between say P and Q, we can use ϕ to map Q to $\phi(Q)$ and define $e(P, Q) = \hat{e}(P, \phi(Q))$, where $\hat{e}$ is the Weil or Tate pairing. There are no hashing problems (getting into $E(\mathbb{F}_q)[r]$ requires a simple cofactor multiplication once we have hashed into $E(\mathbb{F}_q)$) and we trivially have an isomorphism ψ from $\mathbb{G}_2$ to $\mathbb{G}_1$. The drawback

of Type 1 pairings comes when considering bandwidth and efficiency: as we will see in Chapter 6, the condition that E be supersingular is highly restrictive when it comes to optimising the speed of computing the pairing. See Figure 4.7.

The remaining three cases are defined over ordinary elliptic curves, so (as we will again see in Chapter 6) there are no restrictions imposed on the choice of elliptic curve that lead to a loss of efficiency. For all these situations we have $\mathbb{G}_1 = \mathcal{G}_1$ and $P_1 = \mathcal{P}_1$ (where hashing is relatively easy), so we only need to discuss the choices for $\mathbb{G}_2$ and P_2.

- *Type 2 pairings.* In this situation we take $\mathbb{G}_2$ to be any of the $r-1$ subgroups in $E[r]$ that is not $\mathcal{G}_1$ or $\mathcal{G}_2$. We have the map $\psi : \mathbb{G}_2 \to \mathbb{G}_1$ as the trace map Tr. We can also use the anti-trace map to move elements from $\mathbb{G}_2$ into $\mathcal{G}_2$ for efficiency purposes. The drawback is that there is no known way of hashing into $\mathbb{G}_2$ specifically, or to generate random elements of $\mathbb{G}_2$. The best we can do here is to specify a generator $P_2 \in \mathbb{G}_2$ and generate elements via scalar multiplications of P_2, but this is often undesirable in protocols since we cannot generate random elements without knowing the discrete logarithm with respect to P_2. See Figure 4.8.

- *Type 3 pairings.* In this scenario we take $\mathbb{G}_2 = \mathcal{G}_2$, the trace zero subgroup. We can now hash into $\mathbb{G}_2$, at the very least by following a cofactor multiplication in $E(\mathbb{F}_{q^k})$ by the anti-trace map aTr : $E[r] \to \mathcal{G}_2$ (we will soon see that there is a much more efficient way than this). The ironic drawback here is that the only subgroup (besides $\mathcal{G}_1$) that we can hash into is also the only subgroup we can not find a map out of. An isomorphism $\psi : \mathbb{G}_2 \to \mathbb{G}_1$ trivially exists, we just do not have an efficient way to compute it. Thus, security proofs that rely on the existence of such a ψ are no longer applicable, unless the underlying problem(s) remains hard when the adversary is allowed oracle access to ψ [SV07]. See Figure 4.9.

- *Type 4 pairings.* In this situation we take $\mathbb{G}_2$ to be the whole r-torsion $E[r]$, which is a group of order r^2. Hashing into $\mathbb{G}_2$ is possible, but not very efficient, however we cannot hash into the particular subgroup generated by any specific P_2 (i.e. $\mathbb{G}_2$ is not cyclic). Note that hashing into $E[r]$ will only give an element in $\mathcal{G}_1$ or $\mathcal{G}_2$ (which is undesirable in this case) with negligibly low probability for large r. See Figure 4.10.

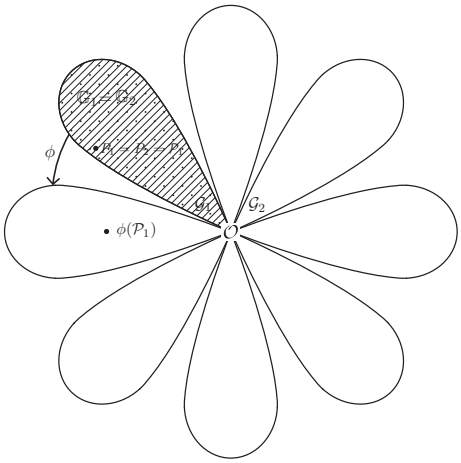

Figure 4.7: Type 1 pairings.

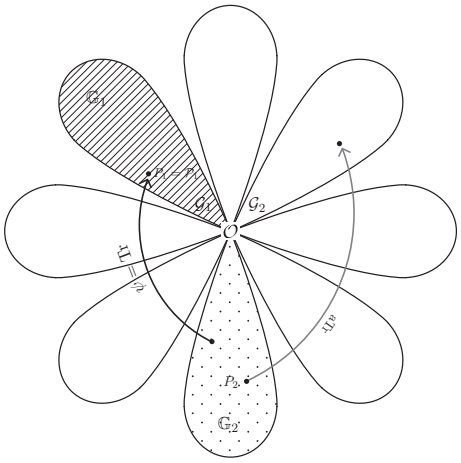

Figure 4.8: Type 2 pairings.

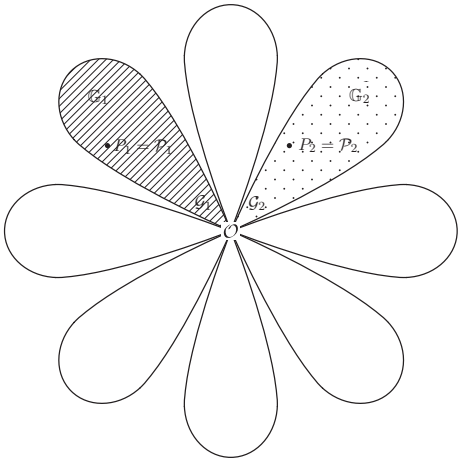

Figure 4.9: Type 3 pairings.

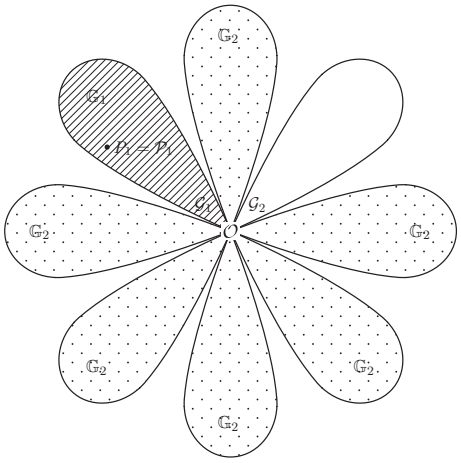

Figure 4.10: Type 4 pairings.

Prior to these different situations being brought to the attention of the PBC community [GPS08], authors publishing pairing-based protocols were often incorrectly assuming combinations of the associated properties that could not be achieved in practice. The message to designers of pairing-based protocols was that individual attention is required to prescribe the pairing type which best suits any particular pairing instantiation. Whilst some authors have since followed this advice closely, a good example being [CCS07, Tables 1-6], it still seems most common that designers of pairing protocols take the easy way out and assume a Type 1 pairing. This approach is somewhat justified, as it allows cryptographers to avoid getting bogged down in the complex details of pairings whilst still enjoying all their functional properties, but overall it is less than sat-

isfactory. The reason is that, at current levels of security, a Type 1 pairing is orders of magnitude more costly than say, a Type 3 pairing. Nowadays all of the state-of-the-art implementations of pairings take place on ordinary curves that assume the Type 3 scenario, where the only potential[3] sacrifice is the map $\psi : \mathbb{G}_2 \to \mathbb{G}_1$. Moreover, Chatterjee and Menezes [CM09] paid closer attention to the role of ψ in protocol (proof) designs and essentially argue that there is no known protocol/proof of security that cannot be translated into the Type 3 setting, claiming that Type 2 pairings (which are less efficient but have ψ) are merely inefficient implementations of Type 3 pairings. We note that their claim is only based on empirical evidence; they posed a counter-example as an open problem. Nevertheless, the final message of Menezes' related ECC2009 talk is that "protocol designers who are interested in the performance of their protocols should describe and analyse their protocols using Type 3 pairings" [Men09].

For the remainder of this text then, and unless otherwise stated, the reader should assume we are in the Type 3 scenario where $\mathbb{G}_1 = \mathcal{G}_1 = E[r] \cap \mathrm{Ker}(\pi - [1])$ and $\mathbb{G}_2 = \mathcal{G}_2 = E[r] \cap \mathrm{Ker}(\pi - [q])$.

4.3 Twisted curves

Before moving our focus to the algorithm for computing pairings, we have one final point to discuss; namely, the most efficient way to hash to, and represent elements in $\mathbb{G}_2$. This discussion brings up the crucial notion of *twists* of elliptic curves, which was first applied to pairings by Barreto *et al.* [BLS03]. We start with an example.

Example 4.3.1 (Magma script). Recall the curve used in Example 4.1.1: $q = 11$, $E/\mathbb{F}_q : y^2 = x^3 + 4$, $\#E(\mathbb{F}_q) = 12$ and $r = 3$. Excluding $\mathcal{O}$, the trace zero subgroup $\mathcal{G}_2$ consists of points defined in $E(\mathbb{F}_{q^2})$, namely $(8, i)$ and $(8, 10i)$. Define the curve $E'/\mathbb{F}_q : y^2 = x^3 - 4$ and observe that the map Ψ^{-1} defined by $\Psi^{-1} : (x, y) \mapsto (-x, iy)$ takes points from E to E', i.e. $\Psi^{-1} : E \to E'$. Restricting Ψ^{-1} to $\mathcal{G}_2$ actually gives a map that takes elements defined over $\mathbb{F}_{q^2}$ to elements defined over $\mathbb{F}_q$: $\Psi^{-1}((8, i)) = (3, 10)$ and $\Psi^{-1}((8, 10i)) = (3, 1)$. The convention is to write Ψ for the reverse map $\Psi : E' \to E$ which in this case is defined by $\Psi : (x', y') \mapsto (-x', y'/i) = (-x', -y'i)$. We call E' a *twist* of E. Every twist

[3]The are some protocols whose security actually relies on the inability to compute ψ efficiently.

has a degree d, which tells us the extension field of $\mathbb{F}_q$ where E and E' become isomorphic. For our purposes, d is also the degree of its field of definition of E' as a subfield of $\mathbb{F}_{q^k}$, i.e. a degree d twist E' of E will be defined over $\mathbb{F}_{q^{k/d}}$. In this example, $k = 2$ and E' is defined over $\mathbb{F}_q$, so we are using a $d = 2$ twist, called a *quadratic twist*. Ordinarily, computations in the group $\mathbb{G}_2 = \mathcal{G}_2$ would

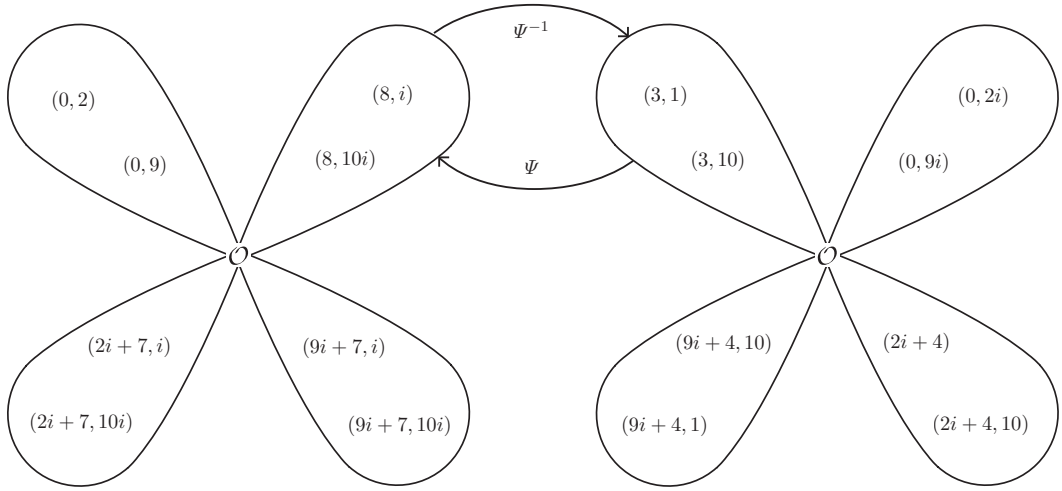

Figure 4.11: E (left) and the quadratic twist E' (right).

require (point doubling/addition) operations in the extension field $\mathbb{F}_{q^2}$, but we can use Ψ^{-1} to instead perform these operations in $E'(\mathbb{F}_q)$, before mapping the result back with Ψ. Moreover, if we restrict the maps to $E[r]$, then Ψ^{-1} takes elements of the trace zero subgroup $\mathcal{G}_2$ of E and moves them to the base field subgroup $\mathcal{G}_1'$ of E'. Note that computing Ψ and Ψ^{-1} is essentially cost free.

We give a larger example that better illustrates the power of employing twisted curves.

Example 4.3.2 (Magma script). Let $q = 103$ and consider $E/\mathbb{F}_q : y^2 = x^3 + 72$, which has $\#E(\mathbb{F}_q) = 84$, so let $r = 7$. The embedding degree (with respect to r) is $k = 6$, so form $\mathbb{F}_{q^6} = \mathbb{F}_q(u)$ with $u^6 + 2 = 0$. The trace zero subgroup $\mathcal{G}_2 = E[r] \cap \mathrm{Ker}(\pi - [q])$ is defined over $\mathbb{F}_{q^6}$, and is generated by $(35u^4, 42u^3)$ (see Figure 4.12). We define the degree $d = 6$ *sextic twist* E' of E as $E' : y^2 = x^3 + 72u^6$, where the back-and-forth isomorphisms are defined as $\Psi : E' \to E$, $(x', y') \mapsto (x'/u^2, y'/u^3)$ and $\Psi : E \to E'$, $(x, y) \mapsto (u^2 x, u^3 y)$. Observe that Ψ^{-1} maps elements in $\mathcal{G}_2 \in E(\mathbb{F}_{q^k})[r] = E(\mathbb{F}_{q^6})[r]$ to elements in $E'(\mathbb{F}_{q^{k/d}})[r] = E'(\mathbb{F}_q)[r]$. Thus, when performing group operations in $\mathbb{G}_2 = \mathcal{G}_2$, we gain the advantage of working over

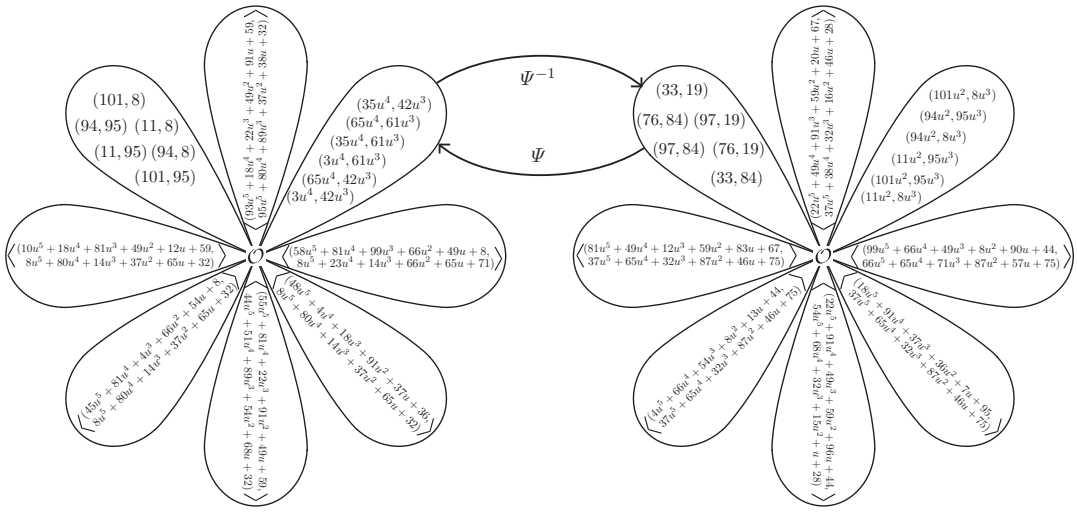

Figure 4.12: E (left) and the (correct) sextic twist E' (right)

$\mathbb{F}_q$ instead of $\mathbb{F}_{q^6}$, a dramatic improvement in computational complexity.

In both Example 4.3.1 and Example 4.3.2 above, we had $k = d$, so the twist allowed us to work in the base field $\mathbb{F}_q$, rather than $\mathbb{F}_{q^k}$. In the general case though, the twist will pull computations back into the subfield $\mathbb{F}_{q^{k/d}}$ of $\mathbb{F}_{q^k}$. For example, if the embedding degree was $k = 12$, a quadratic twist ($d = 2$) would allow computations in $\mathbb{G}_2$ to be performed in $\mathbb{F}_{q^6}$ rather than $\mathbb{F}_{q^{12}}$, whilst a sextic twist ($d = 6$) would allow us to instead work in $\mathbb{F}_{q^2}$. Thus, we would clearly prefer the degree d of the twist to be as high as possible. As it turns out, $d = 6$ is the highest degree available on elliptic curves, where the only possibilities are $d \in \{2, 3, 4, 6\}$ [Sil09, Prop. X.5.4]. For $d > 2$, we also require special subclasses of curves that depend on d, so following [Sil09, Prop. X.5.4] (see also [HSV06, Prop. 6, Prop. 8]) we describe all four cases individually. In the general case according to our context, a twist of $E : y^2 = x^3 + ax + b$ is given by $E' : y^2 = x^3 + a\omega^4 x + b\omega^6$, with $\Psi : E' \to E : (x', y') \mapsto (x'/\omega^2, y'/\omega^3)$, $\omega \in \mathbb{F}_{q^k}$. We can only achieve specific degrees d through combinations of zero and non-zero values for a and b.

- $d = 2$ *quadratic twists.* Quadratic twists are available on any elliptic curve, so if $E/\mathbb{F}_q : y^2 = x^3 + ax + b$, then a quadratic twist is given by $E'/\mathbb{F}_{q^{k/2}} : y^2 = x^3 + a\omega^4 x + b\omega^6$, with $\omega \in \mathbb{F}_{q^k}$ but $\omega^2 \in \mathbb{F}_{q^{k/2}}$. Since $\omega^3 \in \mathbb{F}_{q^k}$, the isomorphism $\Psi : E' \to E$ defined by $\Psi : (x', y') \mapsto (x'/\omega^2, y'/\omega^3)$ will take elements in $E'(\mathbb{F}_{q^{k/2}})$ to elements in $E(\mathbb{F}_{q^k})$, whilst Ψ^{-1} will do the

opposite.

- $d = 3$ *cubic twists.* Degree $d = 3$ twists can only occur when $a = 0$, so if $E/\mathbb{F}_q : y^2 = x^3 + b$, then $E'/\mathbb{F}_{q^{k/3}} : y^2 = x^3 + b\omega^6$, with $\omega^3, \omega^6 \in \mathbb{F}_{q^{k/3}}$, but $\omega^2 \in \mathbb{F}_{q^k} \setminus \mathbb{F}_{q^{k/3}}$. Thus, the isomorphism $\Psi : E' \to E$ (defined as usual) will take elements in $E'(\mathbb{F}_{q^{k/3}})$ to elements in $E(\mathbb{F}_{q^k})$, whilst Ψ^{-1} does the opposite.

- $d = 4$ *quartic twists.* Degree $d = 4$ twists are available when $b = 0$, so if $E/\mathbb{F}_q : y^2 = x^3 + ax$, then $E'/\mathbb{F}_{q^{k/4}} : y^2 = x^3 + a\omega^4 x$, with $\omega^4 \in \mathbb{F}_{q^{k/4}}$, $\omega^2 \in \mathbb{F}_{q^{k/2}}$ and $\omega^3 \in \mathbb{F}_{q^k} \setminus \mathbb{F}_{q^{k/2}}$. Thus, Ψ will move elements in $E'(\mathbb{F}_{q^{k/4}})$ up to elements in $E(\mathbb{F}_{q^k})$, whilst Ψ^{-1} will move elements from $E(\mathbb{F}_{q^k})$ down to $E'(\mathbb{F}_{q^{k/4}})$.

- $d = 6$ *sextic twists.* Sextic twists are only available when $a = 0$, so if $E/\mathbb{F}_q : y^2 = x^3 + b$, then $E'/\mathbb{F}_{q^{k/6}} : y^2 = x^3 + b\omega^6$, with $\omega^6 \in \mathbb{F}_{q^{k/6}}$, $\omega^3 \in \mathbb{F}_{q^{k/3}}$ and $\omega^2 \in \mathbb{F}_{q^{k/2}}$. Thus, Ψ pushes elements in $E'(\mathbb{F}_{q^{k/6}})$ up to $E(\mathbb{F}_{q^k})$, whilst Ψ^{-1} pulls elements from $E(\mathbb{F}_{q^k})$ all the way down to $E'(\mathbb{F}_{q^{k/6}})$.

We make the remark that, for our purposes, a specific twist can only be applied if the curve is of the corresponding form above *and* the embedding degree k has d as a factor. Thus, attractive embedding degrees are those which have any of $d = \{2, 3, 4, 6\}$ as factors, but preferably $d = 4$ or $d = 6$ for increased performance. This will be discussed in detail in Chapter 6. Very fortunately, we will also see in that chapter that almost all of the popular techniques for constructing curves suitable for pairing computation give rise to curves of the form $y^2 = x^3 + b$ or $y^2 = x^3 + ax$, which facilitate the high-degree twists above.

4.4 Chapter summary

We started by discussing that cryptographic pairings are bilinear maps from two elliptic curve groups to a third (finite field) group $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. We then claimed that, in general, to define a useful pairing on $\mathbb{G}_1$ and $\mathbb{G}_2$, we must be able to define more than one subgroup in the r-torsion of E, where the most cryptographically useful case is that r is a large prime. We then defined the embedding degree k of E (with respect to r), and showed that we must extend

the field $\mathbb{F}_q$ to $\mathbb{F}_{q^k}$ in order to find more than one such subgroup. In fact, we showed that $E(\mathbb{F}_{q^k})$ actually contains the entire r-torsion, which has cardinality r^2 and consists of $r+1$ cyclic subgroups of order r. These $r+1$ subgroups (and the existence of maps between them) facilitate several choices for the definitions of $\mathbb{G}_1$ and $\mathbb{G}_2$, which gives rise to four pairing types. We argued that the most popular pairing type is a Type 3 pairing, which sets $\mathbb{G}_1$ and $\mathbb{G}_2$ as the two eigenspaces of the Frobenius endomorphism, namely $\mathbb{G}_1 = \mathcal{G}_1 = E[r] \cap \mathrm{Ker}(\pi - [1])$ is the base field subgroup, and $\mathbb{G}_2 = \mathcal{G}_2 = E[r] \cap \mathrm{Ker}(\pi - [q])$ is the trace zero subgroup.

The definitions of the Weil and Tate pairings in the next chapter inherently justify the claim we made in this chapter that, in general, the arguments P and Q in the pairing $e(P, Q)$ must come from distinct torsion subgroups.