Families of Defining Polynomials of Finite Fields through Prime Power Torsion on Elliptic Curves

Beerens, Pjotr

Families of Defining Polynomials of Finite Fields through Prime Power Torsion on Elliptic Curves

Bachelor's Thesis

Pjotr Beerens

p.beerens@umail.leidenuniv.nl

June 30, 2024

$$\mathbb{F}_{p^n} \cong \mathbb{F}_p[\mathrm{X}]/(f)$$

Supervisors: Dr. Peter Bruin (MI) & Dr. Nuša Zidarič (LIACS)

Contents

1 Introduction

A standard result from the study of fields, commutative rings where the invertible elements are precisely the non-zero elements, is a classification of all finite fields.

Theorem 1.1 [4, 22.1]
For every prime number p and integer $n \geq 1$ there is a unique, up to isomorphism, field with p^n elements. Conversely, every finite field is isomorphic to one of these. □

While the theory around finite fields is quite rich — all finite field automorphisms are powers of the Frobenius, the group of units of a finite field is cyclic, and we can calculate the number of irreducible polynomials over some finite field of specified degree — mathematics and computer science do not always coincide. From an implementation perspective we would like to know what these finite fields actually look like; how can we perform arithmetic in these fields? Which elements generate the group of units?

One way to realize a finite field with p^n elements is as the quotient $\mathbb{F}_p[\mathrm{X}]/(f)$ of $\mathbb{F}_p[\mathrm{X}]$ by some irreducible polynomial $f \in \mathbb{F}_p[\mathrm{X}]$ of degree n. This allows us to perform arithmetic in a finite field but it shifts the problem to finding irreducible polynomials of desired degree.
Rather than defining a finite field as a large degree n extension of $\mathbb{F}_p$ it might be easier to instead construct a field with p^n elements as several iterated extensions of smaller degree, provided that n has non-trivial divisors. An example of such a construction, introduced by Wiedemann in [6], will now be presented.

Fix some algebraic closure $\overline{\mathbb{F}_2}$ of $\mathbb{F}_2$ and consider a sequence $(\gamma_n)_{n\in\mathbb{N}} \subset \overline{\mathbb{F}_2}$ with the following property:

$$\gamma_0 = 1 \in \overline{\mathbb{F}_2} \qquad \text{and} \qquad \gamma_{n+1} + \gamma_{n+1}^{-1} = \gamma_n \text{ for all } n \geq 0.$$

Note that $\gamma_{n+1} + \gamma_{n+1}^{-1} = \gamma_n$ holds if and only if γ_{n+1} is a root of $\mathrm{X}^2 + \gamma_n \mathrm{X} + 1$. As $\overline{\mathbb{F}_2}$ is algebraically closed, such a root exists for every $n \geq 0$ and it follows that such a sequence $(\gamma_n)_{n\in\mathbb{N}} \subset \overline{\mathbb{F}_2}$ exists.

For $n \geq 0$, define $k_n := \mathbb{F}_2(\gamma_n)$ and $\mathrm{Tr}^{(n)} \colon k_n \to k_n,\ x \mapsto \sum_{i=0}^{2^n-1} x^{2^i}$.

Before stating and proving some results about the k_n and $\mathrm{Tr}^{(n)}$ we will introduce the following lemma.

Lemma 1.2 [6, p. 291]
Let k be a field of characteristic 2 and suppose $\alpha, \beta \in k$ satisfy $\alpha^2 = \alpha\beta + 1$. Then, for all $n \geq 1$, the equality

$$\alpha^{2^n} = \alpha\beta^{2^n-1} + \sum_{i=1}^{n} \beta^{2^n-2^i}$$

holds.

Proof: We will show the equality holds by induction on n. For $n = 1$ the equality holds by assumption. Now suppose the equality holds for some $n \geq 1$, we will show it holds for $n+1$. We compute

$$\begin{aligned}\alpha^{2^{n+1}} &= \left(\alpha^{2^n}\right)^2 \overset{\text{IH}}{=} \left(\alpha\beta^{2^n-1} + \sum_{i=1}^{n} \beta^{2^n-2^i}\right)^2 = \alpha^2\beta^{2^{n+1}-2} + \sum_{i=1}^{n} \beta^{2^{n+1}-2^{i+1}} \\ &= \alpha\beta^{2^{n+1}-1} + \beta^{2^{n+1}-2} + \sum_{i=2}^{n+1} \beta^{2^{n+1}-2^i} = \alpha\beta^{2^{n+1}-1} + \sum_{i=1}^{n+1} \beta^{2^{n+1}-2^i}\end{aligned}$$

as required. □

We will apply this lemma to our sequence $(\gamma_n)_{n\in\mathbb{N}}$. After all, for every $n \geq 0$, we have the equality $\gamma_{n+1}^2 = \gamma_{n+1}\gamma_n + 1$ which immediately follows from the definition of our sequence.

Corollary 1.3 [6, p. 291]
For all $n \geq 0$ the equality $\gamma_{n+1}^{2^{2^{n+1}}} = \gamma_{n+1}\gamma_n^{2^{2^{n+1}}-1} + \gamma_n^{2^{2^{n+1}}}[\mathrm{Tr}^{(n+1)}(\gamma_n^{-1})]^2$ holds.

Proof: Taking $\alpha = \gamma_{n+1}, \beta = \gamma_n$ and replacing n with 2^{n+1} in the statement of lemma 1.2 and further calculation yield

$$\begin{aligned}\gamma_{n+1}^{2^{2^{n+1}}} &\overset{1.2}{=} \gamma_{n+1}\gamma_n^{2^{2^{n+1}}-1} + \sum_{i=1}^{2^{n+1}} \gamma_n^{2^{2^{n+1}}-2^i} = \gamma_{n+1}\gamma_n^{2^{2^{n+1}}-1} + \gamma_n^{2^{2^{n+1}}} \sum_{i=1}^{2^{n+1}} (\gamma_n^{-1})^{2^i} \\ &= \gamma_{n+1}\gamma_n^{2^{2^{n+1}}-1} + \gamma_n^{2^{2^{n+1}}}[\mathrm{Tr}^{(n+1)}(\gamma_n^{-1})]^2\end{aligned}$$

as required. □

Using this corollary we can now prove some results about the fields k_n and the entries of our sequence $(\gamma_n)_{n\in\mathbb{N}}$.

Theorem 1.4 [6, p. 290-291]
For every $n \geq 0$, the following hold:

$$\gamma_{n+1} \notin k_n, \quad \#k_{n+1} = 2^{2^{n+1}}, \quad \text{and} \quad \mathrm{Tr}^{(n+1)}(\gamma_{n+1}) = \mathrm{Tr}^{(n+1)}(\gamma_{n+1}^{-1}) = 1.$$

Proof: We will prove this with induction on n. For $n = 0$ we have $\gamma_{n+1} \notin k_n = \mathbb{F}_2$ as γ_{n+1} is a root of $\mathrm{X}^2 + \gamma_n\mathrm{X} + 1 = \mathrm{X}^2 + \mathrm{X} + 1$. It follows that $\mathrm{X}^2 + \mathrm{X} + 1$ is the minimal polynomial of γ_{n+1} over $\mathbb{F}_2$ and therefore $\#k_{n+1} = 4 = 2^{2^{n+1}}$. Finally, we have the equalities

$$\mathrm{Tr}^{(n+1)}(\gamma_{n+1}) = \sum_{i=0}^{2^{n+1}-1} \gamma_{n+1}^{2^i} = \gamma_{n+1} + \gamma_{n+1}^2 \overset{*}{=} \gamma_{n+1} + \gamma_{n+1} + 1 = 1$$

where we have used the fact that γ_{n+1} is a root of the polynomial $\mathrm{X}^2 + \mathrm{X} + 1$. As γ_{n+1}^{-1} satisfies the same recurrence as γ_{n+1} it is a root of the same polynomial and $\mathrm{Tr}^{(n+1)}(\gamma_{n+1}^{-1}) = 1$ follows analogously. Now suppose the theorem holds for some $n - 1 \geq 0$, we will prove it holds for n. Suppose, by way of contradiction, that $\gamma_{n+1} \in k_n$. By induction hypothesis $\#k_n = 2^{2^n}$ holds, therefore, by corollary 1.3 and the induction hypothesis, we have the equalities

$$\gamma_{n+1} = \gamma_{n+1}^{2^{2^n}} \overset{\text{cor.}}{=} \gamma_{n+1}\gamma_n^{2^{2^n}-1} + \gamma_n^{2^{2^n}}\mathrm{Tr}^{(n)}(\gamma_n^{-1})^2 \overset{\text{IH}}{=} \gamma_{n+1} + \gamma_n.$$

As by definition γ_n must have an inverse and is therefore non-zero, we have reached a contradiction; $\gamma_{n+1} \notin k_n$. It follows that $\mathrm{X}^2 + \gamma_n\mathrm{X} + 1 \in k_n[\mathrm{X}]$ is irreducible and therefore that the extension $k_n(\gamma_{n+1})/k_n$ is quadratic. As $\gamma_n = \gamma_{n+1} + \gamma_{n+1}^{-1} \in k_{n+1}$, we have $k_n \subset k_{n+1}$ from which the equality $k_n(\gamma_{n+1}) = k_{n+1}$ follows. By induction hypothesis we now have $\#k_{n+1} = (\#k_n)^2 \overset{\text{IH}}{=} 2^{2^{n+1}}$. It follows that $\mathrm{Gal}(k_{n+1}/k_n)$ has order 2. Let $\sigma \in \mathrm{Gal}(k_{n+1}/k_n)$ be its non-identity element, that is $\sigma(x) = x^{2^{2^n}}$ for all $x \in k_{n+1}$. In particular, as γ_{n+1} and γ_{n+1}^{-1} have the same minimal polynomials over k_n, the equalities $\gamma_{n+1}^{2^{2^n}} = \sigma(\gamma_{n+1}) = \gamma_{n+1}^{-1}$ hold. We now calculate

$$\begin{aligned}\mathrm{Tr}^{(n+1)}(\gamma_{n+1}) &= \sum_{i=0}^{2^{n+1}-1} \gamma_{n+1}^{2^i} = \sum_{i=0}^{2^n-1} \gamma_{n+1}^{2^i} + \sum_{i=2^n}^{2^{n+1}-1} \gamma_{n+1}^{2^i} = \sum_{i=0}^{2^n-1} \gamma_{n+1}^{2^i} + \sum_{i=0}^{2^n-1} \gamma_{n+1}^{2^{2^n+i}} \\ &= \sum_{i=0}^{2^n-1} \gamma_{n+1}^{2^i} + \sum_{i=0}^{2^n-1} \left(\gamma_{n+1}^{2^{2^n}}\right)^{2^i} = \mathrm{Tr}^{(n)}(\gamma_{n+1} + \gamma_{n+1}^{-1}) = \mathrm{Tr}^{(n)}(\gamma_n) \overset{\text{IH}}{=} 1.\end{aligned}$$

Replacing γ_{n+1} by its inverse in the equalities above yields $\mathrm{Tr}^{(n+1)}(\gamma_{n+1}^{-1}) = 1$ which finishes the proof. □

So, for every $n \geq 0$, adjoining γ_{n+1} to k_n, or equivalently $\mathbb{F}_2$, yields a quadratic extension of k_n. This is the maximal size this extension can be, given the fact that γ_{n+1} is a root of a quadratic polynomial over k_n. From the theorem, the following corollary swiftly follows.

Corollary 1.5 [6, p. 291]
For every $n \geq 1$ the equality $\gamma_n^{F_{n-1}} = 1$, where $F_m := 2^{2^m} + 1$ is the m-th Fermat number, holds.

Proof: As $\gamma_{n+1}^{2^{2^n}} = \gamma_{n+1}^{-1}$ holds for all $n \geq 0$, we have $\gamma_{n+1}^{F_n} = 1$ for all $n \geq 0$. Replacing $n+1$ with n finishes the proof. □

This shows that the multiplicative order of γ_n, for $n \geq 1$, must be a divisor of F_{n-1}. One could wonder whether the order of γ_n in fact equals F_{n-1}. Using the factorizations of the first 12 Fermat numbers (starting at zero), it has been verified that the order of γ_n equals F_{n-1} for $1 \leq n \leq 12$ [1, 3.1]. Whether this remains true for larger n is still an open problem. The following theorem argues why it would be interesting to know whether this patterns holds true for all n.

Theorem 1.6 [6, p. 291]
Let $n \geq 1$. If $\mathrm{ord}(\gamma_i) = F_{i-1}$ holds for $1 \leq i \leq n$, then

$$\Gamma_n := \prod_{i=1}^{n} \gamma_i \in k_n$$

is primitive, i.e. it is a generator of the multiplicative group.

Proof: For every $n \geq 0$ we have the equalities

$$\prod_{i=0}^{n} F_i = F_{n+1} - 2 \overset{1.4}{=} \#k_{n+1}^{\times}$$

which can effortlessly be shown by induction. The first equality shows that F_{n+1} is coprime with F_i for $0 \leq i \leq n$. As n is arbitrary, the Fermat numbers are pairwise coprime. The order of Γ_n therefore equals the product of the orders of the γ_i for $1 \leq i \leq n$. Under the assumption of the theorem this is precisely $F_n - 2$; the number of elements in $k_n^{\times}$. □

While the exact order of the elements in our sequence $(\gamma_n)_{n\in\mathbb{N}}$ remains unknown, using techniques from elliptic curves it is possible to put a non-trivial lower bound on the order of γ_n.

Theorem 1.7 [5, 4.1]
There exists $\delta > 0$ such that, for all $n \geq 1$, $\mathrm{ord}(\gamma_n) \geq \exp(2^{\delta n})$ holds. Here $\mathrm{ord}(\gamma_n)$ denotes the multiplicative order of γ_n. □

The proof given by Voloch is an application of a more general theorem he introduced (see appendix B). While we will not concern ourselves with this theorem here, the manner in which Voloch applied this theorem is of key interest in this thesis:
Consider the elliptic curve E over $\mathbb{F}_2$ given by $y^2 + xy = x^3 + 1$. The Verschiebung of this elliptic curve – more details on this in chapter 3, specifically definition 3.18 – is given by $(x, y) \mapsto (x^2 + 1)/x$ on the first coordinate. As such, the γ_n correspond to first coordinates of points on the curve that, when multiplied by 2^n, have first coordinate equal to 1, the value of γ_0. From this perspective, Voloch was able to deduce this lower bound [5, 4.1].
In this thesis we will investigate and present precisely when we can expect extensions defined this way, i.e. by adjoining the first coordinate of a point of order p^n on an elliptic curve to $\mathbb{F}_p$, to increase with p degrees for every increment of n.

2 Algebraic curves

This chapter introduces some results from algebraic geometry which are required before we can move on to elliptic curves and their properties. As such, not all of the results stated will be proven here. In particular, the results that rely on topological properties of algebraic curves will not be proven so as to not move the focus away from elliptic curves.

2.1 Algebraic varieties

Throughout the following sections we will be working over some perfect field k and some fixed algebraic closure $\overline{k}$. If $C \subset \mathbb{P}^n := \mathbb{P}^n(\overline{k})$ is a curve, a variety of dimension 1, we will use the following notation.

i.) C/k to indicate that C is defined over k.

ii.) $\overline{k}(C)$ is the field of functions of C over $\overline{k}$.

iii.) $k(C)$ is the field of functions of C over k.

We have the following fact.

Proposition 2.1 [3, II.1.1]
If C is a curve and $P \in C$ a smooth point, then $\overline{k}[C]_P$, the local ring of C at P, is a discrete valuation ring. □

In the context of proposition 2.1 the maximal ideal $M_P \subset \overline{k}[C]_P$ is principal and a generator $t \in \overline{k}(C)$ of M_P is called a uniformizer for C at P.

Definition 2.2 [3, p. 40]
For a curve C and a smooth point P we define the valuation on $\overline{k}[C]_P$ as

$$\mathrm{ord}_P \colon \overline{k}[C]_P \to \mathbb{N} \cup \{\infty\}, \;\; f \mapsto \sup\{d \in \mathbb{Z} \;:\; f \in M_p^d\}$$

and extend this to the entirety of $\overline{k}(C)$ by $\mathrm{ord}_P(f/g) := \mathrm{ord}(f) - \mathrm{ord}(g)$.
Using this definition, uniformizers of C at P correspond to elements of valuation 1.

Uniformizers at a smooth point are in a sense the building blocks of $\overline{k}(C)$ with respect to this valuation. They come equipped with useful properties such as the following.

Lemma 2.3 [3, II.1.4]
Let k be a perfect field, let C/k be a curve, and let $t \in k(C)$ be a uniformizer at a smooth $P \in C(k)$. Then $k(C)$ is a finite separable extension of $k(t)$.

Proof: $k(C)$ and $k(t)$ both have transcendence degree 1 over k. The extension $k(t) \subset k(C)$ is therefore algebraic and as $k(C)$ is finitely generated over k it is also finitely generated over $k(t)$. The extension $k(t) \subset k(C)$ is therefore finite.
For separability let $x \in k(C)$. As x is algebraic over $k(t)$ there exists

$$\Phi(\mathrm{T}, \mathrm{X}) = \sum a_{ij} \mathrm{T}^i \mathrm{X}^j \in k[\mathrm{T}, \mathrm{X}]$$

of minimal degree in X such that $\Phi(t, x) = 0$ holds; $\Phi(t, \mathrm{X}) \in k(t)[\mathrm{X}]$ is the minimal polynomial of x over $k(t)$ if we take it to be monic. Let $p = \mathrm{char}(k)$. If Φ has a non-zero coefficient a_{ij} with $p \nmid j$ then x is separable over $k(t)$. If instead $\Phi(\mathrm{T}, \mathrm{X}) = \Psi(\mathrm{T}, \mathrm{X}^p)$ for some $\Psi \in k[\mathrm{T}, \mathrm{X}]$ we will reach a contradiction as follows. Because we have assumed k to be perfect, every polynomial of the form $F(\mathrm{T}^p, \mathrm{X}^p)$ is itself a p^{th}-power. We can therefore regroup $\Phi(\mathrm{T}, \mathrm{X})$ according to powers of T modulo p as follows

$$\Phi(\mathrm{T}, \mathrm{X}) = \phi(\mathrm{T}, \mathrm{X}^p) = \sum_{h=0}^{p-1} \left(\sum_{i,j} b_{ijh} \mathrm{T}^{ip} \mathrm{X}^{jp} \right) \mathrm{T}^h = \sum_{h=0}^{p-1} \phi_h(\mathrm{T}, \mathrm{X})^p T^h.$$

As we chose Φ such that $\Phi(t,x)=0$ holds but also have

$$\mathrm{ord}_P(\phi_h(t,x)^p t^h) = p\cdot \mathrm{ord}_P(\phi_h(t,x)) + h\cdot \mathrm{ord}_p(t) \equiv h \mod p$$

as t is a uniformizer, we find $\phi_h(t,x)=0$ for $h=0,\dots,p-1$. After all, each $\phi_h(t,x)t^h$ has a different order at P so the only way their sum can equal 0 is for all of them to equal 0.
As at least one of the $\phi_h(\mathrm{T},\mathrm{X})$ must have non-zero degree in X we have reached a contradiction. $\Phi(t,\mathrm{X})$ was a polynomial in $k(t)[\mathrm{X}]$ of minimal degree with x as a root but there is an h such that $\phi_h(t,x)=0$ holds while $\deg(\phi_h(t,\mathrm{X})) \leq \frac{1}{p}\deg(\Phi(t,\mathrm{X}))$. This contradiction yields that x is separable over $k(t)$. □

2.2 Maps between curves

Akin to any branch of mathematics, maps between the objects of study are of interest to us.

Definition 2.4 [3, p. 11-12]
Let C_1 and $C_2 \subset \mathbb{P}^n$ be curves. A rational map from C_1 to C_2 is a map of the form

$$\phi\colon C_1 \to C_2,\ \phi = [f_0 : \dots : f_n],$$

where $f_i \in \overline{k}(C_1)$ for $0\leq i\leq n$, with the property that, for every $P\in C_1$ where all f_i are defined, $\phi(P) = [f_0(P) : \dots : f_n(P)]$ holds.
We say a rational map $\phi = [f_0,\dots,f_n] : C_1 \to C_2$ is regular at $P\in C_1$ if there exists a $g\in\overline{k}(C_1)$ such that each gf_i is defined at P and for some i we have $(gf_i)(P)\neq 0$.
Provided such a g exists, and therefore that ϕ is regular at P, we set

$$\phi(P) = [(gf_0)(P) : \dots : (gf_n)(P)].$$

Note that for different $P\in C_1$ we might have to choose different $g\in\overline{k}(C_1)$.
If ϕ is regular at all $P\in C_1$ we call ϕ a morphism. If additionally, ϕ is bijective and its inverse is also a morphism, we call ϕ is an isomorphism.

The following proposition gives a convenient sufficient condition for checking regularity of rational maps.

Proposition 2.5 [3, II.2.1]
Let C_1, C_2 be curves, let $P\in C_1$ a smooth point, and let $\phi\colon C_1\to C_2$ be a rational map. Then ϕ is regular at P. In particular, if C_1 is a smooth curve, then ϕ is a morphism.

Proof: Write $\phi = [f_0,\dots,f_N]$ with $f_i\in\overline{k}(C_1)$ and choose a uniformizer $t\in\overline{k}(C_1)$ for C_1 at P. Define $n := \min\limits_{0\leq i\leq N} \mathrm{ord}_P(f_i)$. Then, for all $0\leq i\leq N$, we have

$$\mathrm{ord}_P(t^{-n}f_i) = -n\cdot\mathrm{ord}_P(t) + \mathrm{ord}_P(f_i) = -n + \mathrm{ord}_P(f_i) \geq 0$$

and, for $j\in \arg\min\limits_{0\leq i\leq N} \mathrm{ord}_P(f_i)$, we have

$$\mathrm{ord}_P(t^{-n}f_j) = 0.$$

It follows that ϕ is regular at P.
In particular, if C_1 is a smooth curve, then ϕ is regular at every $P\in C_1$ and therefore a morphism.
Note that we can replace C_2 with an arbitrary variety $V\subset\mathbb{P}^N$ in the statement and the proof. □

Morphisms between curves have the useful property that they come in two different shapes: constant and surjective.

Theorem 2.6 [3, II.2.3]
If $\phi\colon C_1\to C_2$ is a morphism of curves, then ϕ is either constant or surjective. □

Needless to say, constant rational maps between curves are not particularly interesting. On the other hand, non-constant rational maps of curves, which need not be morphisms, induce a map on the respective function fields in the reverse direction.

Definition 2.7 [3, p. 20]
Let C_1/k and C_2/k be curves and let $\phi\colon C_1 \to C_2$ be a non-constant rational map defined over k, that is, the f_i and g in definition 2.4 are taken to be elements of $k(C_1)$. Then we get an injection of function fields fixing k, denoted ϕ^*, given by

$$\phi^*\colon k(C_2) \hookrightarrow k(C_1),\ f \mapsto f \circ \phi.$$

As this is a homomorphism of fields it is injective.

These induced maps have the convenient property that they contain the same information as the original maps in the following sense.

Theorem 2.8 [2, II.6.8], [3, II.2.4]
Let C_1/k and C_2/k be curves.

i.) Let $\phi\colon C_1 \to C_2$ be a non-constant rational map defined over k. Then $k(C_1)$ is a finite extension of $\phi^*(k(C_2))$.

ii.) Let $\iota\colon k(C_2) \to k(C_1)$ be an injection of function fields which is the identity on k. Then there exists a unique non-constant rational map $\phi\colon C_1 \to C_2$ over k such that $\phi^* = \iota$ holds.

Proof: i.) Since $k(C_2) \cong_k \phi^*(k(C_2))$ holds, both $k(C_1)$ and $\phi^*(k(C_2))$ are finitely generated extensions of transcendence degree 1 of k. The extension $\phi^*(k(C_2)) \subset k(C_1)$ therefore has transcendence degree 0. As this extension is finitely generated and algebraic it is finite.
ii.) Let $C_2 \subset \mathbb{P}^N$ and assume, without loss of generality, that C_2 is not contained in the hyperplane $\mathrm{X}_0 = 0$. Let $g_i \in k(C_2)$ be the function corresponding to $\mathrm{X}_i/\mathrm{X}_0$ for $1 \leq i \leq N$.

$$\phi := [1 : \iota(g_1) : \ldots : \iota(g_N)]$$

then defines a map $\phi\colon C_1 \to C_2$ with $\phi^* = \iota$, where, as there is some non-constant g_i and ι is injective, ϕ is non-constant. To show uniqueness, consider another $\psi = [f_0, \ldots, f_N]$ with $\psi^* = \iota$. Then, for $1 \leq i \leq N$, we have

$$f_i/f_0 = \psi^*(g_i) = \iota(g_i).$$

Therefore $\psi = [1 : f_1/f_0 : \ldots : f_N/f_0] = [1 : \iota(g_1) : \ldots : \iota(g_N)] = \phi$ holds, which proves uniqueness. □

Using this theorem we make the following definition.

Definition 2.9 [3, p. 21]
Let $\phi\colon C_1 \to C_2$ be a rational map of curves defined over k. If ϕ is a constant map we define the degree of ϕ to be 0. Otherwise, we call ϕ a finite map and define its degree to be

$$\deg(\phi) := [k(C_1) : \phi^*(k(C_2))].$$

We call ϕ separable or (purely) inseparable if the field extension $\phi^*(k(C_2)) \subset k(C_1)$ is separable or (purely) inseparable respectively. Furthermore, we denote the separable and inseparable degrees of this extension by $\deg_s(\phi)$ and $\deg_i(\phi)$ respectively.
Using the fact that degrees of fields extensions are multiplicative in towers, we find, for another rational map $\psi\colon C_2 \to C_3$ of curves, the equality $\deg(\psi \circ \phi) = \deg(\psi) \cdot \deg(\phi)$. Note that this also holds if either of the maps is constant.

Because degrees are multiplicative over composition it is easy to see that an isomorphism has degree 1. If we assume our curves to be smooth, the converse is also true.

Proposition 2.10 [3, II.2.4.1]
Let C_1 and C_2 be smooth curves and let $\phi\colon C_1 \to C_2$ be a map of degree one, then ϕ is an isomorphism.

Proof: As $\deg(\phi) = 1$ holds we have $\phi^*(\overline{k}(C_2)) = \overline{k}(C_1)$, in other words, ϕ^* is an isomorphism of fields. Applying theorem 2.8.ii.) to $(\phi^*)^{-1}$ we get a rational map $\psi\colon C_2 \to C_1$ with $\psi^* = (\phi^*)^{-1}$. Since C_2 is smooth, this rational map ψ is a morphism by proposition 2.5. As $(\phi \circ \psi)^* = \psi^* \circ \phi^*$ is the identity on $\overline{k}(C_2)$ and $(\psi \circ \phi)^* = \phi^* \circ \psi^*$ the identity on $\overline{k}(C_1)$, the assertion of uniqueness in theorem 2.8.ii.) shows that $\phi \circ \psi$ and $\psi \circ \phi$ are the identity on C_2 and C_1 respectively. After all, it is easily checked the $(\mathrm{id}_C)^* = \mathrm{id}_{\overline{k}(C)}$ holds. □

We next consider the behavior of a map at a point.

Definition 2.11 [3, p. 23]
Let $\phi\colon C_1 \to C_2$ be a non-constant map of smooth curves and let $P \in C_1$. We define the ramification index of ϕ at P, which we will denote by $e_\phi(P)$, to be the quantity

$$e_\phi(P) := \mathrm{ord}_P(\phi^*(t_{\phi(P)})) \geq 1.$$

Here $t_{\phi(P)} \in k(C_2)$ is any uniformizer of C_2 at $\phi(P)$.

This enables us to relate points of the codomain to points in the domain as well as properties of the map as a whole.

Proposition 2.12 [3, II.2.6]
Let $\phi\colon C_1 \to C_2$ be a non-constant map of smooth curves. Then

i.) for every $Q \in C_2$

$$\sum_{P \in \phi^{-1}(\{Q\})} e_\phi(P) = \deg(\phi)$$

holds;

ii.) for all but finitely many $Q \in C_2$

$$\#\phi^{-1}(\{Q\}) = \deg_s(\phi)$$

holds. □

2.3 The Frobenius map

Similar to how fields of characteristic $p > 0$ come equipped with a Frobenius map, curves defined over a field of characteristic $p > 0$ also have a Frobenius map. Whereas fields are closed under multiplication, in the case of curves it cannot be guaranteed that raising all coordinates to the power of p in fact yields another point of the curve.

Definition 2.13 [3, p. 25]
Let k be a perfect field of characteristic $p > 0$ and let $q = p^r$ for some $r > 0$. For $f \in k[\mathrm{X}]$ we write $f^{(q)}$ for the polynomial in $k[\mathrm{X}]$ obtained by raising all coefficients of f to the power of q. For a curve C/k we can define the curve $C^{(q)}/k$ with homogeneous ideal given by

$$I(C^{(q)}) = \langle f^{(q)} : f \in I(C) \rangle.$$

There exists a natural map from C to $C^{(q)}$ called the q^{th}-power Frobenius morphism and it is given by

$$\phi\colon C \to C^{(q)}, \quad \phi([x_0 : \ldots : x_n]) = [x_0^q : \ldots : x_n^q]$$

which is easily checked to map to $C^{(q)}$ by $f^{(q)}(\phi(P)) = f^q(x_0^q, \ldots, x_n^q) = (f(x_0, \ldots, x_n))^q = 0$ for every $f \in I(C)$ and $P = [x_0, \ldots, x_n] \in C$.

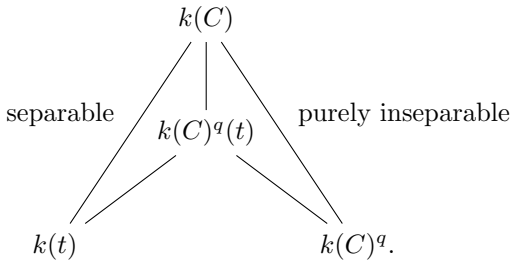
From this definition, the following properties swiftly follow.

Proposition 2.14 [3, II.2.11]
Let k be a perfect field of characteristic $p > 0$, let $q = p^r$ for some $r \geq 0$, let C/k be a curve, and let $\phi\colon C \to C^{(q)}$ be the q^{th}-power Frobenius morphism. Then

i.) $\phi^*(k(C^{(q)})) = k(C)^q$ holds and ϕ is purely inseparable;

ii.) $\deg(\phi) = q$ holds.

Proof: i.) As k is perfect, we have $(k[\mathrm{X}_0, \ldots, \mathrm{X}_n])^q = k[\mathrm{X}_0^q, \ldots, \mathrm{X}_n^q]$. The set of quotients $f(\mathrm{X}_0^q, \ldots, \mathrm{X}_n^q)/g(\mathrm{X}_0^q, \ldots, \mathrm{X}_n^q)$ and the set of quotients $f(\mathrm{X}_0, \ldots, \mathrm{X}_n)^q/g(\mathrm{X}_0, \ldots, \mathrm{X}_n)^q$ where f/g belongs to $k(C)$ are therefore equal. The first set is precisely $\phi^*(k(C^{(q)}))$ while the second is $k(C)^q$. It is clear that the extension $k(C)^q \subset k(C)$ is purely inseparable, that is, every element of the larger field raised to some power of p, is an element of the smaller field.
ii.) We may assume that there is a smooth k-rational point by replacing k with a finite extension if such a point does not exist. Let $t \in k(C)$ be a uniformizer at P. By lemma 2.3 the extension $k(t) \subset k(C)$ is separable. This yields the following tower of fields



It follows that the extension $k(C)^q(t) \subset k(C)$ has (in)separable degree one and therefore we have the equality $k(C) = k(C)^q(t)$. Using i.), we now find $\deg(\phi) = [k(C)^q(t) : k(C)^q]$. As clearly $t^q \in k(C)^q$ and as ϕ is purely inseparable it suffices to show that $t^{q/p} \notin k(C)^q$. By way of contradiction suppose that $t^{q/p} = f^q$ for some $f \in k(C)$. We then have the equalities

$$\frac{q}{p} = \mathrm{ord}_P(t^{q/p}) = q \cdot \mathrm{ord}_P(f)$$

which is a contradiction as $\mathrm{ord}_P(f)$ is an integer. We therefore have

$$\deg(\phi) = q.$$

□

With this knowledge of the Frobenius we can split a rational map into a 'separable' and an 'inseparable' part.

Corollary 2.15 [3, II.2.12]
Let $\psi\colon C_1 \to C_2$ be a non-constant map of curves over a field of characteristic $p > 0$. Then ψ factors as

$$C_1 \xrightarrow{\phi} C_1^{(q)} \xrightarrow{\lambda} C_2,$$

where $q = \deg_i(\psi)$, the map ϕ is the q^{th}-power Frobenius, and λ is separable.

Proof: Let K be separable closure of $\psi^*(k(C_2))$ in $k(C_1)$. Then the extension $K \subset k(C_1)$ is purely inseparable of degree q and therefore $k(C_1)^q \subset K$. By proposition 2.14 we have

$$k(C_1)^q = \phi^*(k(C_1^{(q)})) \qquad \text{and} \qquad [k(C_1) : \phi^*(k(C_1^{(q)}))] = q.$$

By comparing degrees, we find $\phi^*(k(C_1^{(q)})) = K$. We therefore have the following tower of fields

$$\psi^*(k(C_2)) \subset \phi^*(k(C_1^{(q)})) \subset k(C_1).$$

Theorem 2.8.ii) then yields a $\lambda\colon C_1^{(q)} \to C_2$ and by uniqueness we have $\psi = \lambda \circ \phi$. By comparing (in)separable degrees, we find that λ is separable. □

2.4 Divisors

In this subchapter we will introduce the group of divisors associated to a curve. This group itself is not particularly interesting but some of its subgroups and quotients by these subgroups enable us to make some definitions and prove several theorems later on.

Definition 2.16 [3, p. 27]
We define the divisor group of a curve C, denoted $\mathrm{Div}(C)$, to be the free abelian group generated by the points of C. That is

$$\mathrm{Div}(C) := \left\{ \sum_{P \in C} n_P(P) \mid n_P \in \mathbb{Z},\ n_P \neq 0 \text{ for finitely many } P \in C \right\}.$$

If $D = \sum_{P \in C} n_P(P) \in \mathrm{Div}(C)$ is a divisor, we define its degree to be

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

It is then easily checked that the divisors of degree 0 form a subgroup of $\mathrm{Div}(C)$, either by definition or noting that it is the kernel of the group homomorphism $\deg\colon \mathrm{Div}(C) \to \mathbb{Z}$;

$$\mathrm{Div}^0(C) := \{D \in \mathrm{Div}(C) : \deg(D) = 0\}.$$

If C is smooth, a non-zero $f \in \overline{k}(C)$ will have only finitely many roots and poles at points of C. This leads to the following definition.

Definition 2.17 [3, p. 27]
Let C be a smooth curve and let $f \in \overline{k}(C)^\times$. The divisor associated to f, denoted $\mathrm{div}(f)$, is then given by

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)(P).$$

As ord_P is a valuation, this map $\mathrm{div}\colon \overline{k}(C)^\times \to \mathrm{Div}(C)$ is a group homomorphism. As it turns out, $\deg(\mathrm{div}(f)) = 0$ holds for all $f \in \overline{k}(C)^\times$. Divisors that lie in the image of $\mathrm{div}\colon \overline{k}(C)^\times \to \mathrm{Div}^0(C) \subset \mathrm{Div}(C)$ are of special interest to us, we therefore make the following definition.

Definition 2.18 [3, p. 28]
A divisor $D \in \mathrm{Div}(C)$ is called principal if it is of the form $D = \mathrm{div}(f)$ for some $f \in \overline{k}(C)^\times$, i.e. it lies in the image of $\mathrm{div}\colon k(C)^\times \to \mathrm{Div}(C)$. The principal divisors therefore form a subgroup of $\mathrm{Div}(C)$. We name the quotient of the divisor group of C with its subgroup of principal divisors the Picard group or divisor class group of C and denote it $\mathrm{Pic}(C)$;

$$\mathrm{Pic}(C) := \mathrm{Div}(C)/\mathrm{div}(\overline{k}(C)^\times).$$

For $D_1, D_2 \in \mathrm{Div}(C)$ we write $D_1 \sim D_2$ if their classes in $\mathrm{Pic}(C)$ are the same, or equivalently, if $D_1 - D_2$ is principal.
As we have an inclusion $\mathrm{div}(\overline{k}(C)^\times) \subset \mathrm{Div}^0(C)$ we can also consider their quotient. We denote this quotient with $\mathrm{Pic}^0(C)$;

$$\mathrm{Pic}^0(C) := \mathrm{Div}^0(C)/\mathrm{div}(\overline{k}(C)^\times).$$

This is the image of $\mathrm{Div}^0(C)$ in $\mathrm{Pic}(C)$.

We will put a partial ordering on $\mathrm{Div}(C)$ as follows.

Definition 2.19 [3, p. 33]
A divisor $D = \sum_{P \in C} n_P(P) \in \mathrm{Div}(C)$ is called positive, denoted $D \geq 0$, if $n_P \geq 0$ for every $P \in C$. For $D, D' \in \mathrm{Div}(C)$ we now write $D \geq D'$ if $D - D' \geq 0$ holds.
Using this definition, we associate to every divisor $D \in \mathrm{Div}(C)$, the set

$$\mathcal{L}(D) := \{f \in \overline{k}(C)^\times : \mathrm{div}(f) \geq -D\} \cup \{0\}$$

which turns out to be a finite-dimensional $\overline{k}$-vector space. We write $\ell(D)$ for its $\overline{k}$-dimension.

2.5 Differentials

Next we define the vector space of differential forms on a curve. The main purpose to include this here, is to formulate the Riemann-Roch theorem which defines the genus of a curve.

Definition 2.20 [3, p. 30]
Let C be a curve. We define the vector space of differential forms on C to be the $\overline{k}(C)$-vector space generated by the symbols dx where $x \in \overline{k}(C)$ together with the following relations:

i.) for all $x, y \in \overline{k}(C)$ $\quad d(x+y) = dx + dy$;
ii.) for all $x, y \in \overline{k}(C)$ $\quad d(xy) = xdy + ydx$;
iii.) for all $\lambda \in \overline{k}$ $\quad d\lambda = 0$.

We denote this vector space with Ω_C. This vector space has dimension 1 over $\overline{k}(C)$.

Proposition 2.21 [3, II.4.3]
Let C be curve, $P \in C$ and $t \in \overline{k}(C)$ be a uniformizer for the local ring of C at P. Then Ω_C enjoys the following properties:

i.) For every $\omega \in \Omega_C$ there exists a unique $g \in \overline{k}(C)$ such that $\omega = gdt$ holds.
We denote this unique $g \in \overline{k}(C)$ with ω/dt.

ii.) For $\omega \in \Omega_C \setminus \{0\}$ the value $\mathrm{ord}_P(\omega/dt)$ is independent of the choice of uniformizer t.
We denote this value by $\mathrm{ord}_P(\omega)$.

iii.) For $\omega \in \Omega_C \setminus \{0\}$ there are only finitely many $Q \in C$ with $\mathrm{ord}_Q(\omega) \neq 0$. □

Similar to what we did with elements of $\overline{k}(C)^\times$, we use proposition 2.21 to make the following definition.

Definition 2.22 [3, p. 32]
Let $\omega \in \Omega_C \setminus \{0\}$. The divisor associated to ω, denoted $\mathrm{div}(\omega)$, is given by

$$\mathrm{div}(\omega) := \sum_{P \in C} \mathrm{ord}_P(\omega)(P) \in \mathrm{Div}(C).$$

Remark 2.23 [3, p. 32]
Let $\omega_1, \omega_2 \in \Omega_C \setminus \{0\}$. As Ω_C is 1-dimensional over $\overline{k}(C)$ there exists $f \in \overline{k}(C)$ such that $\omega_1 = f\omega_2$. Therefore the equalities

$$\begin{aligned}\mathrm{div}(\omega_1) = \mathrm{div}(f\omega_2) &= \sum_{P \in C} \mathrm{ord}_P(fw_2) = \sum_{P \in C} \mathrm{ord}_P(f(w_2/dt_P)) \\ &= \sum_{P \in C} \mathrm{ord}_P(f) + \mathrm{ord}_P(\omega_2/dt_P) = \mathrm{div}(f) + \mathrm{div}(\omega_2)\end{aligned}$$

hold where $t_P \in \overline{k}(C)$ is a uniformizer for P. Here we use $(fw_2)/dt_P = f(w_2/dt)$. It follows that the classes of $\mathrm{div}(\omega_1)$ and $\mathrm{div}(\omega_2)$ in $\mathrm{Pic}(C)$ are the same.

This leads to the following definition.

Definition 2.24 [3, p. 32]
The canonical divisor class on C is the class of $\mathrm{div}(\omega)$ in $\mathrm{Pic}(C)$ for any non-zero differential $\omega \in \Omega_C$. Divisors in this canonical divisor class are called canonical divisors.

2.6 The Riemann-Roch theorem

With all these definitions at our disposal, we can now state this important theorem.

Theorem (Riemann-Roch) 2.25 [3, II.5.4]
Let C be a smooth curve. There is an integer $g \geq 0$ such that for every canonical divisor k_C on C and every divisor $D \in \mathrm{Div}(C)$ the equality

$$\ell(D) - \ell(k_C - D) = \deg(D) - g + 1$$

holds. This g is called the genus of C. □

Defining the genus aside, we will be using this theorem in the following forms.

Corollary 2.26 [3, II.5.5]
Let C be a smooth curve with genus g and let k_C be a canonical divisor on C. Then

i.) $\ell(k_C) = g$ holds;

ii.) $\deg(k_C) = 2g - 2$ holds;

iii.) for $D \in \mathrm{Div}(C)$ with $\deg(D) > 2g - 2$ the equality $\ell(D) = \deg(D) - g + 1$ holds.

Proof: i.) Applying theorem 2.25 (Riemann-Roch) to $D = 0$ yields the equality

$$\ell(0) - \ell(k_C) = \deg(0) - g + 1.$$

As $\mathcal{L}(0) = \overline{k} \subset \overline{k}(C)$ holds (the only $f \in \overline{k}(C)$ with no poles are constants) and $\deg(0) = 0$ holds, we find that $\ell(k_C) = g$ holds.
ii.) Applying theorem 2.25 (Riemann-Roch) to $D = k_C$ we find the equality

$$\ell(k_C) - \ell(0) = \deg(k_C) - g + 1.$$

Using i.) and the fact $\ell(0) = 1$ holds we get the equality $\deg(k_C) = 2g - 2$ as required.
iii.) Using ii.) we find $\deg(k_C - D) < 2g - 2 - (2g - 2) = 0$.
For any divisor $D' \in \mathrm{Div}(C)$ with $\mathcal{L}(D') \neq 0$ there exists non-zero $f \in \mathcal{L}(D')$. This yields

$$0 = \deg(\mathrm{div}(f)) \geq \deg(-D') = -\deg(D')$$

where we have used $\mathrm{div}(f) \geq -D'$. It follows that $\deg(D') \geq 0$ holds. The contrapositive of this tells us that divisors of negative degree, such as $k_C - D$, satisfy $\mathcal{L}(k_C - D) = 0$ and therefore $\ell(k_C - D) = 0$ holds.
Applying theorem 2.25 (Riemann-Roch) to D now yields the equality

$$\ell(D) = \deg(D) - g + 1$$

as required. □

3 Elliptic curves

Having defined the genus as well as having formulated and proven some results regarding general algebraic curves, we now narrow our focus to a specific kind of curve: an elliptic curve.

3.1 Weierstrass form

Definition 3.1 [3, p. 59]
An elliptic curve is a pair (E, O) where E is a nonsingular curve of genus one and $O \in E$. We say that (E, O) is defined over k, if E as a curve is defined over k and $O \in E(k)$.

Oftentimes, elliptic curves are introduced differently, namely as the vanishing of a polynomial of a certain form. The following theorem states that these definitions coincide.

Theorem 3.2 [3, III.3.1]
Let (E, O) be an elliptic curve defined over k. Then there exist functions $x, y \in k(E)$ such that

$$\phi\colon E \to \mathbb{P}^2,\ \phi = [x, y, 1]$$

gives an isomorphism of E/k to a curve given by

$$C\colon \mathrm{Y}^2 + a_1\mathrm{XY} + a_3\mathrm{Y} = \mathrm{X}^3 + a_2\mathrm{X}^2 + a_4\mathrm{X} + a_6 \tag{1}$$

where $a_1, \ldots, a_6 \in k$ and $\phi(O) = [0 : 1 : 0]$.

Proof: Because E has genus 1, corollary 2.26.iii.) (Riemann-Roch) tells us that the vector space $\mathcal{L}(n(O))$ has dimension n for $n \geq 1$. In particular there exist functions $x_0, y_0 \in k(E)$ such that $1, x_0$ forms a basis for $\mathcal{L}(2(O))$ and $1, x_0, y_0$ forms a basis for $\mathcal{L}(3(O))$[1]. Note that $x_0 \notin \mathcal{L}((O))$, therefore x_0 has a pole of order greater than 1 at O. Since $x_0 \in \mathcal{L}(2(O))$ this order is at most 2; x_0 has a pole of order 2 at O. Similarly, y_0 has a pole of order 3 at O. While $\mathcal{L}(6(O))$ has dimension 6, it contains the seven functions $1, x_0, y_0, x_0^2, x_0y_0, y_0^2, x_0^3$. We therefore have a (non-trivial) relation

$$A_1 + A_2x_0 + A_3y_0 + A_4x_0^2 + A_5x_0y_0 + A_6y_0^2 + A_7x_0^3 = 0$$

with $A_1, \ldots, A_7 \in k$[2]. Note that A_6 and A_7 are both non-zero, otherwise all terms would have different order poles at O so the only way their sum could equal 0 would be for all the A_i to be 0 which would make the relation trivial. If we define $x := -x_0/(A_6A_7)$ and $y := y_0/(A_6A_7^2)$, then substituting these into the non-trivial relation yields

$$A_1 - A_2A_6A_7x + A_3A_6A_7^2y + A_4A_6^2A_7^2x - A_5A_6^2A_7^3xy + A_6^3A_7^4y^2 - A_6^3A_7^4x^3 = 0.$$

Dividing this equation by $A_6^3A_7^4$ yields an equation of the form (1); the coefficients of x^3 and y^2 would be 1 (after moving x^3 to the right hand side).
In particular, the map

$$\phi\colon E \to \mathbb{P}^2,\ \phi = [x : y : 1]$$

lies in C, the vanishing of the curve we have just specified, given by an equation of the form (1). Since E is smooth, ϕ is a morphism by proposition 2.5 and it is surjective (to C) by theorem 2.6 (x is linearly independent from 1 so it is not constant). As y has a pole of higher order than x at O, we find $\phi(O) = [0 : 1 : 0]$.
We will show that C is smooth. Suppose that C, given by equation (1), is singular. By performing a linear change of coordinates we can assume, without loss of generality, that $(0, 0)$ is a singular point. In particular $a_6 = 0$ holds. By taking partial derivatives and evaluating in $(0, 0)$, which must yield 0, we additionally find $a_3 = a_4 = 0$. C is therefore given by $\mathrm{Y}^2 + a_1\mathrm{XY} = \mathrm{X}^3 + a_2\mathrm{X}^2$. The rational map

$$\psi\colon C \to \mathbb{P}^1, \quad (x, y) \mapsto [x : y]$$

[1] It is not obvious we can take these to be over k as opposed to $\overline{k}$, see appendix B.
[2] Again, it is not obvious we can take the A_i in k as opposed to $\overline{k}$.

has an inverse given by

$$\mathbb{P}^1 \to C, \quad [1:t] \mapsto (t^2 + a_1 t - a_2, t^3 + a_1 t^2 - a_2 t)$$

and therefore has degree 1 (degrees are multiplicative over composition and the identity has degree 1). So, if the C we have just defined were singular, we would have a rational map $\psi\colon C \to \mathbb{P}^1$ of degree 1. The composition $\psi \circ \phi\colon E \to \mathbb{P}^1$ would then be a degree 1 map between smooth curves and therefore, by proposition 2.10 an isomorphism. As E has genus one and $\mathbb{P}^1$ genus zero, this is a contradiction; C is smooth.
We will now show that $\phi\colon E \to C$ has degree one or equivalently that $k(E) = \phi^*(k(C))$ holds. Since ϕ is given by $[x:y:1]$ we have $\phi^*(k(C)) = k(x,y)$. Consider the map $[x:1]\colon E \to \mathbb{P}^1$ which has degree two by proposition 2.12, the function x has precisely one pole: an order two pole at O. It follows that $[k(E):k(x)] = 2$ holds. Similarly, by considering the map $[y:1]\colon E \to \mathbb{P}^1$ we find that $[k(E):k(y)] = 3$ holds. After all, y has precisely one pole; a pole of order 3 at O. Because degrees are multiplicative in towers, $[k(E):k(x,y)]$ must divide both 2 and 3 and is therefore 1. In other words, $\deg(\phi) = 1$ holds. We conclude that, as both E and C are smooth and ϕ has degree one, ϕ is an isomorphism $E \xrightarrow{\sim} C$ (proposition 2.10). □

Equation (1) is called a Weierstrass form of the elliptic curve E/k. In this form we implicitly take $O = [0:1:0]$. If E/k with $\mathrm{char}(k) = p > 0$ is given by a Weierstrass equation. Then $E^{(q)}$ with $q = p^e$ for some $e \geq 1$ is again an elliptic curve (the Weierstrass equation will again specify a non-singular curve of genus one). In particular, if $k = \mathbb{F}_q$, the q^{th}-power Frobenius is the identity on k and we have $E^{(q)} = E$.

3.2 The group law

One of the reasons to study elliptic curves is because of the following group structure they admit.

Composition Law 3.3 [3, III.2.1]
Let E/k be an elliptic curve given by a Weierstrass equation. Let $P, Q \in E$, let L be the line through P and Q where we take the tangent line on E through P in the case that $P = Q$ holds. Let R be the unique third point of intersection of L with E. If we let L' be the line through R and O then this also has a unique third point of intersection with E, we denote this third point with $P \oplus Q$.

That the lines L and L' have precisely three points of intersection with E is a consequence of Bézout's theorem (see appendix B). We will however present explicit formulas at the end of this subchapter so there is no need for this general theorem. We will later show that E forms an abelian group with identity element O using this composition. The most difficult part is showing that the composition is associative, the other properties required for an (abelian) group law are given here.

Proposition 3.4 [6, III.2.2]
The composition law 3.3 satisfies the following:

i.) If P, Q, R are the intersection points of a line L with E, then $(P \oplus Q) \oplus R = O$ holds.

ii.) For all $P \in E$: $P \oplus O = P$ holds.

iii.) For all $P, Q \in E$: $P \oplus Q = Q \oplus P$ holds.

iv.) For every $P \in E$ there is a $\ominus P \in E$ such that $P \oplus (\ominus P) = O$ holds.

Proof: i.) Notice that L is the line through P and Q as in 3.3. If we let L' be the line through its third intersection point R and O then the third intersection point of L' is $P \oplus Q$. If we now consider the line L_2 through $P \oplus Q$ and R as in 3.3 we know it's third intersection point to be O. It follows that $(P \oplus Q) \oplus R$ is the third intersection point of the tangent line of E at O which is O itself.
ii.) If L is the line through P and $Q := O$ as in 3.3 and R its third point of intersection. Then the line L' as in 3.3 through R and $O = Q$ will be the same line. We therefore know its third point of intersection to be P; $P \oplus O = P$.

iii.) The composition law is defined symmetrically in P and Q.
iv.) Let $R \in E$ be the third intersection point of the line through P and O. Applying i.) and ii.) we find

$$O = (P \oplus O) \oplus R = P \oplus R.$$

□

All that is left to show that E forms an abelian group under $\oplus$ is associativity, or in other words, that $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$ holds for all $P, Q, R \in E$. This is what we will do next, but proving this with the definition given in 3.3 is quite tedious as there are many different cases to consider depending on which points are the same or distinct. Instead, we move our perspective to an algebraic object and induce its group structure onto E. However, before we do this we state and proof the following lemma.

Lemma 3.5 [3, III.3.3]
Let C be a curve of genus $g = 1$ and let $P, Q \in C$. Then the following equivalence holds:

$$(P) \sim (Q) \qquad \text{if and only if} \qquad P = Q.$$

Proof: $\Rightarrow$: Write $(P) - (Q) = \operatorname{div}(f)$ for some $f \in \overline{k}(C)^\times$. It follows that $\operatorname{div}(f) \in \mathcal{L}((Q))$ as we have the inequality $(P) - (Q) \geq -(Q)$. By corollary 2.26.iii (Riemann-Roch) we have $\ell((Q)) = 1$ as $\deg((Q)) = 1 > 0 = 2g - 2$ holds. In other words, $\mathcal{L}((Q))$ is a 1-dimensional $\overline{k}$-vector space. As it is clear that it contains the constant functions we have $\overline{k} \subset \mathcal{L}((Q))$ and by comparing dimensions over $\overline{k}$ this is an equality. Therefore $f \in \overline{k}$, $\operatorname{div}(f) = 0$ and $P = Q$ hold.
$\Leftarrow$: Clear. □

We will now show that the composition law 3.3 and the addition of divisor classes in $\operatorname{Pic}^0(E)$ coincide for an elliptic curve E given by a Weierstrass equation.

Theorem 3.6 [3, III.3.4]
Let (E, O) be an elliptic curve. Then (E, O) enjoys the following properties.

i.) For every divisor $D \in \operatorname{Div}^0(E)$ of degree 0 there exists a unique $P \in E$ such that

$$D \sim (P) - (O).$$

Define $\sigma \colon \operatorname{Div}^0(E) \to E$ to be the map that sends D to this P.

ii.) This σ is surjective.

iii.) Let $D_1, D_2 \in \operatorname{Div}^0(E)$. Then the equivalence

$$\sigma(D_1) = \sigma(D_2) \qquad \text{if and only if} \qquad D_1 \sim D_2$$

holds. We therefore have an induced bijection $\sigma \colon \operatorname{Pic}^0(E) \to E$.

iv.) The inverse of this induced σ is the function

$$\kappa \colon E \to \operatorname{Pic}^0(E), \ P \mapsto \overline{(P) - (O)} \in \operatorname{Pic}^0(E).$$

v.) If E is given by a Weierstrass equation then κ satisfies

$$\kappa(P \oplus Q) = \kappa(P) + \kappa(Q) \quad \text{for all } P, Q \in E.$$

Proof: i.) Using the fact that E has genus 1, corollary 2.26.iii.) (Riemann-Roch) tells us that, for every $D \in \operatorname{Div}^0(E)$, $\ell(D + (O)) = 1$ holds. Therefore there exists a non-zero $f \in \mathcal{L}(D + (O))$. Because $\operatorname{div}(f) \geq -D - (O)$ and $\deg(\operatorname{div}(f)) = 0$ hold, we necessarily have $\operatorname{div}(f) = -D - (O) + (P)$ for some $P \in E$. After all, the difference of $\operatorname{div}(f)$ with $-D - (O)$ has degree 1 and must be greater than or equal to 0. In particular, we have $D \sim (P) - (O)$ which shows the existence of such a $P \in E$. Suppose a $P' \in E$ satisfies $D \sim (P') - (O)$. We then have

$$(P) \sim D + (O) \sim (P')$$

as $\sim$ respects our group operation. From lemma 3.5 we then conclude $P = P'$ which shows uniqueness.
ii.) Let $P \in E$. We then have the equality

$$\sigma((P) - (O)) = P$$

which shows that σ is surjective.
iii.) Let $D_i \in \mathrm{Div}^0(E)$ and define $P_i := \sigma(D_i)$ for $i = 1, 2$. By definition of σ we have $D_i \sim (P_i) - (O)$ for $i = 1, 2$. By subtracting these two equivalences we get

$$D_1 - D_2 \sim (P_1) - (P_2).$$

$\Leftarrow$: If $P_1 = P_2$ holds, we therefore have $D_1 - D_2 \sim 0$ or equivalently $D_1 \sim D_2$.
$\Rightarrow$: If $D_1 \sim D_2$, we find $(P_1) - (P_2) \sim 0$ or in other words $(P_1) \sim (P_2)$. Lemma 3.5 then yields $P_1 = P_2$ as required.
Taking the quotient of $\mathrm{Div}^0(E)$ with $\sim$, which is precisely the definition of $\mathrm{Pic}^0(E)$, therefore yields an injection $\mathrm{Pic}^0(E) \hookrightarrow E$. By ii.), this map is also surjective and as such a bijection.
iv.) For every $P \in E$ the divisor $(P) - (O)$ has degree 0 so κ is well-defined. We have already seen $\sigma \circ \kappa = \mathrm{id}_E$ to hold in ii.). Since we also know σ to be bijective, κ must then be its inverse.
v.) Let E be given by a Weierstrass equation and let $P, Q \in E$. Let the line L in $\mathbb{P}^2$ through P and Q as in composition law 3.3 be given by

$$f(\mathrm{X}, \mathrm{Y}, \mathrm{Z}) := a\mathrm{X} + b\mathrm{Y} + c\mathrm{Z} = 0.$$

Let R be third point of intersection of L with E and let L', the line through R and O as in composition law 3.3 be given by

$$g(\mathrm{X}, \mathrm{Y}, \mathrm{Z}) := a'\mathrm{X} + b'\mathrm{Y} + c'\mathrm{Z} = 0.$$

As the line given by $\mathrm{Z} = 0$ intersects E at $O = [0 : 1 : 0]$ with multiplicity 3, we the equalities

$$\mathrm{div}(f/\mathrm{Z}) = (P) + (Q) + (R) - 3(O) \qquad \text{and} \qquad \mathrm{div}(f/\mathrm{Z}) = (R) + (P \oplus Q) - 2(O).$$

We therefore have

$$0 \sim \mathrm{div}(f'/f) = \mathrm{div}(f'/\mathrm{Z}) - \mathrm{div}(f/\mathrm{Z}) = (P \oplus Q) - (P) - (Q) + (O)$$

and as such

$$\kappa(P \oplus Q) - \kappa(P) - \kappa(Q) = \overline{(P \oplus Q) - (P) - (Q) + (O)} = 0 \in \mathrm{Pic}^0(E).$$

In other words, $\kappa(P \oplus Q) = \kappa(P) + \kappa(Q)$ holds for all $P, Q \in E$. □

Corollary 3.7 [3, p. 62]
Let (E, O) be an elliptic curve given by a Weierstrass equation. Then $(E, \oplus)$ forms an abelian group. □

Now that we know $\oplus$ to define an (abelian) group structure on E, the notation $\ominus P$ for the/an additive inverse of $P \in E$ is justified; we know these to be unique. We will now provide a useful criterion for determining when divisors on an elliptic curve are principal.

Corollary 3.8 [3, III.3.5]
Let (E, O) be an elliptic curve and let $D = \sum_{p \in E} n_P(P) \in \mathrm{Div}(E)$ be a divisor on E. Then D is principal if and only if

$$\sum_{P \in E} n_P = 0 \qquad \text{and} \qquad \sum_{P \in E} n_P P = O$$

hold. Note that the former summation happens in $\mathbb{Z}$ and the latter in E using its group structure.

Proof: For a divisor $D = \sum_{p\in E} n_P(P) \in \mathrm{Div}^0(E)$ of degree 0 we have

$$\begin{aligned}
D \sim 0 &\iff \sigma(D) = O && \text{3.6.iii.)}\\
&\iff \sigma\left(\sum_{p\in E} n_P(P) - n_P(O)\right) = O && \deg(D) = 0\\
&\iff \sum_{P\in E} n_p\sigma((P)-(O)) = O && \text{3.6.iv-v.)}\\
&\iff \sum_{P\in E} n_p P = O && \sigma((P)-(O)) = P
\end{aligned}$$

where σ is the function introduced in theorem 3.6. This proves the implication from right to left. For the other implication we note that $\deg(\mathrm{div}(f)) = 0$ for all $f \in \overline{k}(E)$. The equivalence above then finishes the proof. □

The composition law as presented in 3.3 is rather abstract. Fortunately we can write down explicit formulas for the group operation.

Group Law Formulas 3.9 [3, III.2.3]
Let E be an elliptic curve given by the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Let $P_i = (x_i, y_i) \in E$ for $0 \le i \le 2$, then.

i.) $\ominus P_0 = (x_0, -y_0 - a_1x_0 - a_3)$ holds.

ii.) If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then $P_1 \oplus P_2 = O$. Otherwise, if we define λ and ν by

if	λ	ν
$x_1 \neq x_2$	$\dfrac{y_2 - y_1}{x_2 - x_1}$	$\dfrac{y_1x_2 - y_2x_1}{x_2 - x_1}$
$x_1 = x_2$	$\dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$	$\dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$

then $y = \lambda x + \nu$ is the line through P_1 and P_2 or the tangent to E in P_1 if $P_1 = P_2$ holds.

iii.) If we set $(x_3, y_3) := P_1 \oplus P_2$, then

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \qquad \text{and} \qquad y_3 = -(\lambda + a_1)x_3 - \nu - a_3$$

hold, with λ, ν as in ii.) (here we again assume $P_2 \neq \ominus P_1$).

Proof: i.) The line trough P_0 and O is given by $L\colon x - x_0 = 0$ (in Weierstrass coordinates). Substituting in the given Weierstrass equation to find the intersection points yields

$$y^2 + (a_1x_0 + a_3)y - x_0^3 - a_2x_0^2 - a_4x_0 - a_6 = 0.$$

We already know the root y_0 so it is a simple calculation to verify that the other root is given by $-y_0 - a_1x_0 - a_3$. Therefore, the line through P_0 and $(x_0, -y_0 - a_1x_0 - a_3)$ intersects E in O and this second point is therefore the inverse of the first. Note that even if P_0 and $(x_0, -y_0 - a_1x_0 - a_3)$ are the same point, the specified line intersects this point with multiplicity 2 so the statement still holds true.
ii.) The first part we have shown to be true in i.) so assume $P_2 \neq \ominus P_1$. In the case that $x_1 \neq x_2$ holds, the formula for the line through P_1 and P_2 is standard and independent of E. In the other case $x_1 = x_2$ holds and we have already ruled out the possibility that $P_2 = \ominus P_1$ holds, therefore the equality $P_1 = P_2$

follows. Define $F(x,y) := y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$. Then the tangent at P_1 is given by

$$\begin{aligned}
& \frac{\partial}{\partial y}F(P_1)(y-y_1) = -\frac{\partial}{\partial x}F(P_1)(x-x_1) \\
\rightsquigarrow \quad & (2y_1 + a_1x_1 + a_3)(y-y_1) = -(a_1y_1 - 3x_1^2 - 2a_2x_1 - a_4)(x-x_1) \\
\rightsquigarrow \quad & y = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}(x-x_1) + y_1 \\
\rightsquigarrow \quad & y = \lambda x + \frac{-3x_1^3 - 2a_2x_1^2 - a_4x_1 + 2a_1y_1x_1 + 2y_1^2 + a_3y_1}{2y_1 + a_1x_1 + a_3} \\
\rightsquigarrow \quad & y = \lambda x + \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1 + 2F(x_1,y_1)}{2y_1 + a_1x_1 + a_3} \\
\rightsquigarrow \quad & y = \lambda x + \nu.
\end{aligned}$$

This shows that in either case the line L as in composition law 3.3 is given by $y = \lambda x + \nu$.
iii.) Let $P_4 = (x_4, y_4)$ be the third intersection point of L with E. By proposition 3.4.i we have $(P_1 \oplus P_2) \oplus P_4 = O$ and therefore $P_4 = \ominus(P_1 \oplus P_2)$ holds. By evaluating F in $(x, \lambda x + \nu)$ we find

$$\begin{aligned}
F(x, \lambda x + \nu) &= \lambda^2x^2 + 2\lambda\nu x + \nu^2 + a_1\lambda x^2 + a_3\lambda x + a_3\nu - x^3 - a_2x^2 - a_4x - a_6 \\
&= -x^3 + (\lambda^2 + a_1\lambda - a_2)x^2 + (2\lambda\nu + a_3\lambda - a_4)x + \nu^2 + a_3\nu - a_6.
\end{aligned}$$

The roots of this polynomial give the x-coordinates of points in the intersection of L with E. As we already know these roots, x_1, x_2, and x_4, we get $x_1 + x_2 + x_4 = \lambda^2 + a_1\lambda - a_2$, the coefficient of x^2 (note the minus sign before x^3). It follows that $x_4 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$ and $y_4 = \lambda x_4 + \nu$ hold. As $P_3 = \ominus P_4$ holds, we can apply the formula proven in i.) which yields

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \qquad \text{and} \qquad y_3 = -(\lambda + a_1)x_3 - \nu - a_3.$$

□

As these formulas are given by rational functions, one could wonder if the group operations (addition and negation) are in fact morphisms. The answer to this question is affirmative.

Theorem 3.10 [3, III.3.6]
Let E/k be an elliptic curve given by a Weierstrass equation. Then the maps

$$\begin{aligned}
\oplus\colon E \times E &\to E, \\
(P_1, P_2) &\mapsto P_1 \oplus P_2,
\end{aligned}
\qquad \text{and} \qquad
\begin{aligned}
\ominus\colon E &\to E, \\
P &\mapsto \ominus P,
\end{aligned}$$

are morphisms.

Proof: By 3.9 the negation map is given by

$$(x,y) \mapsto (x, -y - a_1x - a_3)$$

except at the point O. As this map is clearly rational and as E is smooth it is a morphism by proposition 2.5.
For an arbitrary point $Q \neq O$ of E we can consider the translation-by-Q map

$$\tau\colon E \to E, \quad P \mapsto P \oplus Q.$$

By the group law formulas given in 3.9 this is a rational map and as E is smooth it is again a morphism by 2.5. As it has an inverse morphism, translation-by-$\ominus Q$, it is an isomorphism.
From the addition formula $\oplus\colon E \times E \to E$ given in 3.9 it follows that $\oplus$ is given by a rational map, except possibly at points of the form

$$(P,P), \quad (P, \ominus P), \quad (P,O), \quad (O,P). \tag{2}$$

For arbitrary $Q_1, Q_2 \neq O$ on E with translation maps τ_1, τ_2 we can consider the following composition

$$\phi\colon E \times E \xrightarrow{\tau_1 \times \tau_2} E \times E \xrightarrow{\oplus} E \xrightarrow{\tau_1^{-1}} E \xrightarrow{\tau_2^{-1}} E.$$

This map acts as follows:

$$(P_1, P_2) \xmapsto{\tau_1 \times \tau_2} (P_1 \oplus Q_1, P_2 \oplus Q_2) \xmapsto{\oplus} P_1 \oplus Q_1 \oplus P_2 \oplus Q_2 \xmapsto{\tau_1^{-1}} P_1 \oplus P_2 \oplus Q_2 \xmapsto{\tau_2^{-1}} P_1 \oplus P_2.$$

Therefore, ϕ and the addition $\oplus$ agree. As the translation maps are isomorphisms it follows that ϕ is given by a rational map except possibly at points of the form

$$(P \ominus Q_1, P \ominus Q_2), \quad (P \ominus Q_1, \ominus P \ominus Q_2), \quad (P \ominus Q_1, \ominus Q_2), \quad (\ominus Q_1, P \ominus Q_2)$$

which are precisely the points of the form (2) were we to apply $\tau_1 \times \tau_2$. As Q_1 and Q_2 are arbitrary points ($\neq O$) we can, by varying Q_1 and Q_2, find rational maps

$$\phi_1, \ldots, \phi_n\colon E \times E \to E$$

all of which agree with the addition $\oplus$ such that for all $(P_1, P_2) \in E \times E$ there is a ϕ_i that is defined at (P_1, P_2). It follows that $\oplus\colon E \times E \to E$ is a morphism. □

3.3 Isogenies

Now that we have defined and familiarized ourselves with elliptic curves, it makes sense to investigate maps between elliptic curves. As elliptic curves have both a group structure and a geometric structure it might not be immediately clear what these maps should look like. As it turns out, if the geometric structure is respected, the group structure will follow. This, we will see in theorem 3.13.

Definition 3.11 [3, p. 66]
Let (E_1, O_1) and (E_2, O_2) be elliptic curves. An isogeny from E_1 to E_2 is a morphism

$$\phi\colon E_1 \to E_2 \quad \text{satisfying} \quad \phi(O_1) = O_2.$$

When $E_1 = E_2$ holds, an important family of isogenies are the multiplication-by-m maps with respect to the group structure.

Definition 3.12 [3, p. 67,69]
Let (E, O) be an elliptic curve and let $m \in \mathbb{Z}$. We define the multiplication-by-m isogeny

$$[m]\colon E \to E, \quad P \mapsto mP.$$

That is

$$[m](P) = \begin{cases} \overbrace{P \oplus \ldots \oplus P}^{m \text{ terms}}, & \text{if } m > 0; \\ O, & \text{if } m = 0; \\ \underbrace{\ominus P \ominus \ldots \ominus P}_{-m \text{ terms}} & \text{if } m < 0. \end{cases}$$

For $m = 0$ this is clearly a morphism. For $m > 0$ it is the composition $[m] = \oplus \circ ([m-1] \times \mathrm{id}_E) \circ d$ where d is the diagonal morphism

$$d\colon E \to E \times E, \quad P \mapsto (P, P)$$

and is therefore a morphism by induction. Finally, for $m < 0$ we have $[m] = \ominus \circ [-m]$ so it is a morphism. As $[m](O) = O$ holds for all $m \in \mathbb{Z}$, the multiplication-by-m map is an isogeny for all $m \in \mathbb{Z}$. We denote its kernel $\ker([m])$ with $E[m]$, the m-torsion subgroup of E.

As E forms an abelian group, the multiplication-by-m isogenies are also group homomorphisms. The same turns out to be true for general isogenies.

Theorem 3.13 [3, III.4.8]
Let (E_1, O_1) and (E_2, O_2) be elliptic curves and let $\phi\colon E_1 \to E_2$ be an isogeny. Then

$$\phi(P \oplus Q) = \phi(P) \oplus \phi(Q)$$

holds for all $P, Q \in E_1$.

Proof: If ϕ is the constant map $P \mapsto O_2$, the theorem is clear. Otherwise, ϕ induces a homomorphism

$$\phi_*\colon \mathrm{Pic}^0(E_1) \to \mathrm{Pic}^0(E_2), \qquad \overline{\sum_{P\in E_1} n_P(P)} \mapsto \overline{\sum_{P\in E_1} n_P(\phi(P))}.$$

We also have group isomorphisms

$$\kappa_i\colon E_i \to \mathrm{Pic}^0(E_i), \qquad P \mapsto \overline{(P) - (O_i)}$$

for $i = 1, 2$ by theorem 3.6. This yields the following diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{\sim}_{\kappa_1} & \mathrm{Pic}^0(E_1) \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi_*} \\ E_2 & \xrightarrow{\sim}_{\kappa_2} & \mathrm{Pic}^0(E_2) \end{array}$$

which commutes because $\phi(O_1) = O_2$ holds:

$$\phi_*(\kappa_1(P)) = \phi_*\left(\overline{(P) - (O_1)}\right) = \overline{(\phi(P)) - (\phi(O_1))} = \overline{(\phi(P)) - (O_2)} = \kappa_2(\phi(P)).$$

In particular, as κ_1, κ_2 and ϕ_* are all group homomorphisms with κ_2 injective, ϕ must also be a group homomorphism (κ_2 is of course invertible, but for this argument injectivity suffices). □

Because isogenies are also group homomorphisms they have more structure then a general morphism of curves. We can therefore strengthen some previous results on top of introducing new results.

Proposition 3.14 [3, III.4.10]
Let $\phi\colon (E_1, O_1) \to (E_2, O_2)$ be a non-zero isogeny. Then

i.) for every $Q \in E_2$ the equality $\#\phi^{-1}(\{Q\}) = \deg_s(\phi)$ holds;

ii.) the map

$$\ker(\phi) \to \mathrm{Aut}(\overline{k}(E_1)/\phi^*(\overline{k}(E_2))), \quad T \mapsto \tau_T^*$$

is an isomorphism. Here τ_T is the translation-by-T map defined in the proof of theorem 3.10 and τ_T^* is the endomorphism (which will be an automorphism as τ_T is invertible) it induces on $\overline{k}(E_1)$;

iii.) if ϕ is separable, $\#\ker(\phi) = \deg(\phi)$ holds and $\overline{k}(E_1)$ is a Galois extension of $\phi^*(\overline{k}(E_2))$.

Proof: i.) By proposition 2.12.ii), the statement holds for all but finitely many $Q \in E_2$. As ϕ is a group homomorphism, every fiber contains the same number of elements and therefore $\phi^{-1}(\{Q\}) = \deg_s(\phi)$ holds for all $Q \in E_2$.
ii.) Notice that for $T \in \ker(\phi)$ and $f \in \overline{k}(E_2)$ we have

$$\tau_T^*(\phi^*(f)) = (\phi \circ \tau_T)^*(f) = \phi^*(f)$$

as $\phi \circ \tau_T = \phi$ holds. Therefore, τ_T^* fixes $\phi^*(\overline{K_2}(E_2))$ so the specified map is well-defined. Furthermore, we have the equalities

$$\tau_T^* \circ \tau_S^* = (\tau_S \circ \tau_T)^* = (\tau_{S\oplus T})^* = (\tau_{T\oplus S})^*$$

which show that the map is a homomorphism. From i.) it follows that $\#\ker(\phi) = \deg_s(\phi)$ holds while it is basic field theory that $\#\mathrm{Aut}(\overline{k}(E_1)/\phi^*(\overline{k}(E_2))) \leq \deg_s(\phi)$ holds. It therefore suffices to show that the specified map is injective. If τ_T^* fixes the entirety of $\overline{k}(E_1)$ for some $T \in \ker(\phi)$, then every element of $\overline{k}(E_1)$ takes the same value at T and O_1. In particular, a Weierstrass coordinate function x has a pole at O_1 and no other poles. Therefore, $T = O_1$ holds and the specified map is an isomorphism.
iii.) Assuming ϕ is separable we have, by i.), for all $Q \in E_2$ the equalities

$$\#\phi^{-1}(\{Q\}) = \deg_s(\phi) = \deg(\phi).$$

Taking $Q = O_2$ shows the first part of the statement. For the second we note that, using ii.), we now have

$$\#\mathrm{Aut}(\overline{k}(E_1)/\phi^*(\overline{k}(E_2))) = \#\ker(\phi) = \deg(\phi) = [\overline{k}(E_1) : \phi^*(\overline{k}(E_2))]$$

and therefore the extension $\phi^*(\overline{k}(E_2)) \subset \overline{k}(E_1)$ is Galois. □

Corollary 3.15 [3, III.4.11]
Let $\phi\colon (E_1, O_1) \to (E_2, O_2)$ and $\psi\colon (E_1, O_1) \to (E_3, O_3)$ be non-constant isogenies with ϕ separable and $\ker(\phi) \subset \ker(\psi)$. Then there exists a unique isogeny $\lambda\colon (E_2, O_2) \to (E_3, O_3)$ such that $\psi = \lambda \circ \phi$ holds.

Proof: As ϕ is separable, proposition 3.14.iii.) tells us that the extension $\phi^*(\overline{k}(E_2)) \subset \overline{k}(E_1)$ is Galois. Using the fact that $\ker(\phi) \subset \ker(\psi)$ and the identification given in 3.14.ii.), it follows that every element of $\mathrm{Gal}(\overline{k}(E_1)/\phi^*(\overline{k}(E_2)))$ also fixes $\psi^*(\overline{k}(E_3))$. In particular, we have inclusions

$$\psi^*(\overline{k}(E_3)) \subset \phi^*(\overline{k}(E_2)) \subset \overline{k}(E_1).$$

Theorem 2.8.ii) now yields a map $\lambda\colon E_2 \to E_3$ with $\phi^* \circ \lambda^* = \psi^*$. By the uniqueness assertion in theorem 2.8.ii) it then follows that $\lambda \circ \phi = \psi$ holds. Finally, we have

$$\lambda(O_2) = \lambda(\phi(O_1)) = \psi(O_1) = O_3,$$

showing that λ is an isogeny. □

3.4 The dual isogeny

Next we will introduce the dual of an isogeny. For this we will need the following fact.

Lemma 3.16 [3, p. 82]
Let E/k be an elliptic curve where $\mathrm{char}(k) = p > 0$. Then $[p]$ is not separable. □

Theorem 3.17 [3, III.6.1]
Let $\phi\colon (E_1, O_1) \to (E_2, O_2)$ be a non-constant isogeny of degree m. Then there exists a unique isogeny

$$\hat{\phi}\colon E_2 \to E_1 \qquad \text{such that} \qquad \hat{\phi} \circ \phi = [m]$$

holds. This $\hat{\phi}$ is called the dual of ϕ or the dual isogeny to ϕ.
For the zero-map we take the dual to be the zero-map in the other direction.

Proof: To see that such $\hat{\phi}$, if it exists, is unique we consider another such isogeny $\hat{\phi}'$. Their pointwise difference $\hat{\phi} - \hat{\phi}$ is again an isogeny which follows from theorem 3.10. We now find the equalities

$$(\hat{\phi} - \hat{\phi}') \circ \phi = [m] - [m] = [0].$$

As ϕ is non-constant, $\hat{\phi} - \hat{\phi}'$ must be constant by theorem 2.6 and as $(\hat{\phi} - \hat{\phi}')(O_2) = O_1$ we find $\hat{\phi} = \hat{\phi}'$. We will now show that for another isogeny $\psi\colon (E_2, O_2) \to (E_3, O_3)$ of degree n we have $\widehat{\psi \circ \phi} = \hat{\phi} \circ \hat{\psi}$ if the latter (and therefore the former) exist. We calculate

$$(\hat{\phi} \circ \hat{\psi}) \circ (\psi \circ \phi) = \hat{\phi} \circ [n] \circ \phi \overset{!}{=} [n] \circ \hat{\phi} \circ \phi = [nm]$$

where we have used the fact that $\hat{\phi}$ is a homomorphism (theorem 3.13) and therefore commutes with multiplication-by-n maps. In particular, $\widehat{\psi \circ \phi} = \hat{\phi} \circ \hat{\psi}$ holds. Therefore, if we are able to write an isogeny as a composition of isogenies it suffices to show the existence of a dual to every isogeny in the composition. We will show the existence of a dual of an arbitrary isogeny $\phi\colon E_1 \to E_2$ of degree m in two cases.

Case 1; ϕ is separable. Because ϕ is separable, proposition 3.14.iii.) tells us that $\#\ker(\phi) = m$ holds. In particular every element of $\ker(\phi)$ has order dividing m. This yields the inclusion $\ker(\phi) \subset \ker([m])$. Corollary 3.15 then yields an isogeny $\hat{\phi}\colon E_2 \to E_1$ with $\hat{\phi} \circ \phi = [m]$.

Case 2; ϕ is inseparable. Let $p^e = q = \deg_i(\phi)$. Then by corollary 2.15 we can write

$$\phi = \lambda \circ F_e \circ F_{e-1} \ldots \circ F_1$$

where λ is separable and the F_i are p^{th}-power Frobenius maps. We have already shown that λ has a dual as it is separable. To see that a p^{th}-power Frobenius F has a dual we use lemma 3.16 and again corollary 2.15 that allows us to write $[p] = \psi \circ F'_r \circ \ldots \circ F'_2 \circ F$ for $p^r = \deg_i([p]) \geq p$ and where the F'_j are Frobenius maps. In particular, we have

$$(\psi \circ F'_r \circ \ldots \circ F'_2) \circ F = [p]$$

where $p = \deg(F)$ holds by proposition 2.14.ii.). We can therefore take $\hat{F} = \psi \circ F'_r \circ \ldots \circ F'_2$. Note that $r \geq 1$ holds, so F does in fact appear in the composition. □

Definition 3.18
Let E/k be an elliptic curve with $\text{char}(k) = p > 0$ and let F be the p^{th}-power Frobenius. The dual of F is called the Verschiebung of E and we denote it with V.

Duals to isogenies come equipped with numerous properties some of which are given in the following theorem. All of these are rather straightforward to prove, given the previous properties, except for the third property, especially in characteristic $p > 0$. We therefore omit proving these properties.

Theorem 3.19 [3, III.6.2]
Let $\phi\colon E_1 \to E_2$ be an isogeny.

i.) Let $m = \deg(\phi)$. Then $\hat{\phi} \circ \phi = [m]$ holds on E_1 and $\phi \circ \hat{\phi} = [m]$ holds on E_2.

ii.) Let $\lambda\colon E_2 \to E_3$ be an isogeny. Then $\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$ holds.

iii.) Let $\psi\colon E_1 \to E_2$ be an isogeny. Then $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$, where $+$ denotes the pointwise sum, holds.

iv.) For all $m \in \mathbb{Z}$ the equalities $\widehat{[m]} = [m]$ and $\deg([m]) = m^2$ hold.

v.) $\deg(\hat{\phi}) = \deg(\phi)$ holds.

vi.) $\hat{\hat{\phi}} = \phi$ holds. □

Remark 3.20
From theorem 3.19.iv.) it follows that the ring homomorphism

$$[\ ]\colon \mathbb{Z} \to \text{End}(E) := \{\phi\colon E \to E \mid \phi \text{ is an isogeny}\}$$

is injective; only [0] has degree 0.

Using these properties of duals to isogenies we can investigate the torsion subgroups of an elliptic curve.

Corollary 3.21 [3, III.6.4]
Let (E, O) be an elliptic curve and let $m \in \mathbb{Z}$. If $\mathrm{char(k)} = p$ and $p \nmid m$, so m is non-zero in k, then

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Proof: Because $\deg([m]) = m^2$ holds by theorem 3.19.iv.), the map $[m]$ is separable. After all, if it were inseparable, $p > 0$ would hold, $[m]$ would factor through a non-trivial power of the Frobenius, and its degree would therefore be a multiple of p. By proposition 3.14.iii.) we therefore have the equality $\#E[m] = \deg([m]) = m^2$. As this also holds for every divisor d of m; $\#E[d] = d^2$, the only abelian group $E[m]$ can be, is $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. □

Corollary 3.22 [3, III.6.4]
Let (E, O) be an elliptic curve. Assume $\mathrm{char}(k) = p > 0$ and that k is perfect. Then one of the following holds

i.) $E[p^e] = \{O\}$ for all $e \geq 1$;

ii.) $E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}$ for all $e \geq 1$.

Proof: Suppose $e \geq 1$. Consecutively applying proposition 3.14.i.), the definition of a dual, and proposition 2.14.i.) yields

$$\#E[p^e] = \deg_s([p^e]) = \deg_s(V)^e \cdot \deg_s(F)^e = \deg_s(V)^e$$

where F is the p^{th}-power Frobenius and V the Verschiebung; its dual. By 3.19.v.) and 2.14.ii.) we have the equalities

$$\deg(V) = \deg(F) = p.$$

In the case that V is inseparable we therefore have $\deg_s(V) = 1$ and therefore $E[p^e]$ is trivial for all $e \geq 1$. Otherwise V is separable, $\deg_s(V) = p$, and we have $\#E[p^e] = p^e$ for all $e \geq 1$. To see that $E[p^e]$ must therefore be cyclic we note that $\#E[p^e]$ is strictly greater than $\#E[p^{e-1}]$. Therefore there exist elements in E with order dividing p^e and order not dividing p^{e-1}. In other words, there are elements of order p^e in E and therefore $E[p^e]$ is cyclic of order p^e. □

This gives rise to the following definition.

Definition 3.23 [3, p. 145]
Let (E, O) be an elliptic curve. Assume $\mathrm{char}(k) = p > 0$ and that k is perfect. If corollary 3.22.i.) holds we call E supersingular. In the other case, that is, corollary 3.22.ii.) holds, we call E ordinary.

We will now introduce the notion of a (positive definite) quadratic form. As we will see later, the degree map of isogenies adheres to this notion.

Definition 3.24 [3, p. 85]
Let A be an abelian group. A function $d\colon A \to \mathbb{R}$ is called a quadratic form if

i.) $d(\alpha) = d(-\alpha)$ holds for all $\alpha \in A$,

ii.) the map $A \times A \to \mathbb{R}, \quad (\alpha, \beta) \mapsto d(\alpha + \beta) - d(\alpha) - d(\beta)$ is bilinear.

Additionally, a quadratic form d is called positive definite if

iii.) $d(\alpha) \geq 0$ holds for all $\alpha \in A$,

iv.) $d(\alpha) = 0$ holds if and only if $\alpha = 0$ holds.

Theorem (Cauchy-Schwarz Inequality) 3.25 [3, V.1.2]
Let A be an abelian group and let $d\colon A \to \mathbb{Z}$ be a positive definite quadratic form. Then

$$|d(\alpha-\beta)-d(\alpha)-d(\beta)| \leq 2\sqrt{d(\alpha)d(\beta)}$$

holds for all $\alpha, \beta \in A$.

Proof: Let $\alpha, \beta \in A$ and let $L(\alpha,\beta) := d(\alpha+\beta)-d(\alpha)-d(\beta)$ be the bilinear form associated to d. First we notice that, for all $m \in \mathbb{Z}$, we have the equalities

$$md(2\alpha)-2md(\alpha) = mL(\alpha,\alpha) = L(m\alpha,\alpha) = d((m+1)\alpha)-d(m\alpha)-d(\alpha) \quad \text{and}$$
$$-d(2\alpha) = d(\alpha)-d(2\alpha)-d(\alpha) = L(2\alpha,-\alpha) = 2L(\alpha,-\alpha) = -4d(\alpha).$$

Therefore $d(2\alpha) = 4d(\alpha)$ and $d((m+1)\alpha) = d(m\alpha)+(2m+1)d(\alpha)$ hold. By induction we therefore have $d(m\alpha) = m^2 d(\alpha)$ for all $m \geq 0$. As $d(\alpha) = d(-\alpha)$ holds, we find $d(m\alpha) = m^2 d(\alpha)$ for all $m \in \mathbb{Z}$. Because d is positive definite we find, for all $m, n \in \mathbb{Z}$,

$$0 \leq d(m\alpha - n\beta) = L(m\alpha, -n\beta) + d(m\alpha) + d(n\beta) = mnL(\alpha,-\beta) + m^2 d(\alpha) + n^2 d(\beta).$$

Setting $m = -L(\alpha,-\beta)$ and $n = 2d(\alpha)$ yields

$$0 \leq d(\alpha)(4d(\alpha)d(\beta) - L(\alpha,-\beta)^2).$$

From this, the inequality follows as long as $d(\alpha)$ is non-zero. This happens precisely when α is non-zero. If $\alpha = 0$ holds, the inequality trivially holds. □

Proposition 3.26 [3, III.6.3]
Let (E_1, O_1) and (E_2, O_2) be elliptic curves. The degree map $\deg\colon \mathrm{Hom}(E_1,E_2) \to \mathbb{Z}$ is a positive definite quadratic form. Here we take $\mathrm{Hom}(E_1,E_2) := \{\phi\colon E_1 \to E_2 \mid \phi \text{ is an isogeny}\}$.

Proof: Clearly, properties i.), iii.) and iv.) are satisfied. To see that

$$\langle \phi, \psi \rangle := \deg(\phi+\psi) - \deg(\phi) - \deg(\psi)$$

is bilinear we use the injection $[\ ]\colon \mathbb{Z} \to \mathrm{End}(E_1)$. By employing theorem 3.19.iii.) we calculate, for $\phi, \psi \in \mathrm{Hom}(E_1,E_2)$,

$$[\langle\phi,\psi\rangle] = [\deg(\phi+\psi)] - [\deg(\phi)] - [\deg(\psi)] = \widehat{(\phi+\psi)} \circ (\phi+\psi) - \hat{\phi}\circ\phi - \hat{\psi}\circ\psi$$
$$= (\hat{\phi}+\hat{\psi})\circ(\phi+\psi) - \hat{\phi}\circ\phi - \hat{\psi}\circ\psi = \hat{\phi}\circ\psi + \hat{\psi}\circ\phi.$$

Again by theorem 3.19.iii.), this is linear in both ϕ and ψ. It follows that $\langle\ \rangle$ is bilinear. □

3.5 The Weil pairing

Let (E,O) defined over k be an elliptic curve, let $\mathrm{char}(k) = p$, not necessarily greater than 0, and let $m \geq 2$ be an integer such that $p \nmid m$. We have seen that $E[m] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. We will introduce a pairing that associates an m^{th} root of unity to every ordered pair of m-torsion elements.
Let $T \in E[m]$. By corollary 3.8 there exists $f \in \overline{k}(E)$ with $\mathrm{div}(f) = m(T) - m(O)$. Let $T' \in E$ be a point satisfying $[m]T' = T$ which exists as $[m]$ is non-constant (and therefore surjective). By corollary 3.8 there then exists $g \in \overline{k}(E)$ with

$$\mathrm{div}(g) = [m]^*((T)) - [m]^*((O)) = \sum_{Q \in E[m]} ((T' \oplus Q) - (Q)).$$

Here $[m]^*$ is defined by

$$[m]^*\colon \mathrm{Div}(E) \to \mathrm{Div}(E), \qquad (Q) \mapsto \sum_{P \in [m]^{-1}(\{Q\})} e_{[m]}(P)(P).$$

We furthermore notice that the rightmost term has degree 0 and

$$\sum_{Q\in E[m]} (T' \oplus Q \ominus Q) = \sum_{Q\in E[m]} T' = [m^2](T') = O$$

holds. This shows that the conditions for corollary 3.8 are satisfied. Let $\phi = [m]$, we calculate

$$\operatorname{div}(f\circ\phi) = m\left(\sum_{P\in\phi^{-1}(\{T\})} e_\phi(P)(P) - \sum_{P\in\phi^{-1}(\{O\})} e_\phi(P)(P)\right) = m(\phi^*((T)) - \phi^*((O))) = \operatorname{div}(g^m).$$

As such, $(f\circ[m])/g^m$ has associated divisor 0 and is therefore constant. By replacing f with a scalar multiple, we may assume $f\circ[m] = g^m$ holds. If we now take another m-torsion point $S \in E[m]$, not necessarily distinct from T, we find, for all $P \in E$,

$$g(P\oplus S)^m = f([m](P)\oplus[m](S)) = f([m](P)) = g(P)^m.$$

The function $P \mapsto g(P\oplus S)/g(P)$, where this is defined, therefore only takes on m^{th} roots of unity. The morphism

$$E \to \mathbb{P}^1, \qquad P \mapsto [g(P\oplus S)/g(P) : 1]$$

is therefore not surjective and must, by theorem 2.6, be constant. If we let $\boldsymbol{\mu}_m := \{\lambda \in \overline{k}^\times : \lambda^m = 1\}$ be the group of m^{th} roots of unity in k we can define the pairing

$$e_m\colon E[m]\times E[m] \to \boldsymbol{\mu}_m, \qquad (S,T)\mapsto g(P\oplus S)/g(P)$$

where g is constructed as above and $P \in E$ is any point such that both $g(P\oplus S)$ and $g(P)$ are defined and non-zero. As given some $T \in E[m]$, g is defined uniquely up to scalar multiplication, the pairing does not depend on this choice [3, p. 93-94].

Definition 3.27 [3, p. 94]
This pairing $e_m\colon E[m]\times E[m]\to\boldsymbol{\mu}_m$ is called the Weil e_m-pairing.

Theorem 3.28 [3, III.8.1]
The Weil e_m-pairing enjoys the following properties.

i.) It is bilinear; for all $S_1, S_2, T_1, T_2 \in E[m]$ the equalities

$$e_m(S_1\oplus S_2, T_1) = e_m(S_1,T_1)e_m(S_2,T_1),$$
$$e_m(S_1, T_1\oplus T_2) = e_m(S_1,T_1)e_m(S_1,T_2)$$

hold.

ii.) It is alternating; for all $T \in E[m]$ the equality $e_m(T,T) = 1$ holds.

iii.) It is nondegenerate; if $e_m(S,T) = 1$ holds for all $S \in E[m]$, then $T = O$ holds.

iv.) It is compatible; $e_{mm'}(S,T) = e_m([m']S,T)$ holds for all $S \in E[mm']$ and $T \in E[m]$.

Proof: i.) For linearity in the first component we notice

$$e_m(S_1\oplus S_2,T_1) = \frac{g(P\oplus S_1\oplus S_2)}{g(P)} = \frac{g(P\oplus S_1\oplus S_2)}{g(P\oplus S_1)}\frac{g(P\oplus S_1)}{g(P)} = e_m(S_2,T_1)e_m(S_1,T_1).$$

Here g is a rational function depending on T_1 as in the definition of the pairing and $P \in E$ is any point such that the evaluations in g are defined and non-zero.
For linearity in the second component we let $f_1, f_2, f_3, g_1, g_2, g_3$ be functions for the points T_1, T_2, and

$T_3 := T_1 \oplus T_2$ as in the definition of the pairing. By employing corollary 3.8, choose an $h \in \overline{k}(E)$ with divisor $\mathrm{div}(h) = (T_3) - (T_1) - (T_2) + (O)$. Then

$$\mathrm{div}\left(\frac{f_3}{f_1 f_2}\right) = m(T_3) - m(T_1) - m(T_2) + m(O) = m \cdot \mathrm{div}(h) = \mathrm{div}(h^m)$$

holds and therefore $f_3 = c f_1 f_2 h^m$ for some $c \in \overline{k}$. Using $f_i \circ [m] = g_i^m$ for $i = 1, 2, 3$ and taking m^{th} roots, yields $g_3 = c' g_1 g_2 (h \circ [m])$ for some $c' \in \overline{k}$. We now compute

$$\begin{aligned} e_m(S_1, T_1 \oplus T_2) &= \frac{g_3(P \oplus S_1)}{g_3(P)} = \frac{g_1(P \oplus S_1) g_2(P \oplus S_1) h([m](P) \oplus [m](S_1))}{g_1(P) g_2(P) h([m](P))} \\ &= e_m(S_1, T_1) e_m(S_1, T_2) \end{aligned}$$

where $P \in E$ is a point such that all evaluations are defined and non-zero and we have used the fact that $[m](S_1) = O$ holds.
ii.) Let $T \in E[m]$ and let f and g be as in the definition of the pairing. We calculate

$$\mathrm{div}\left(\prod_{i=0}^{m-1} f \circ \tau_{[i]T}\right) = m \sum_{i=0}^{m-1} \big(([1-i](T)) - ([-i](T))\big) = 0$$

where τ_P is the translation-by-P map. Therefore, $\prod_{i=0}^{m-1} f \circ \tau_{[i](T)}$ is constant. If we now choose some $T' \in E$ with $[m](T') = T$, then

$$\begin{aligned} \left(\prod_{i=0}^{m-1} g \circ \tau_{[i](T')}\right)^m &= \prod_{i=0}^{m-1} g^m \circ \tau_{[i](T')} = \prod_{i=0}^{m-1} f \circ [m] \circ \tau_{[i](T')} = \prod_{i=0}^{m-1} f \circ \tau_{[i](T)} \circ [m] \\ &= \left(\prod_{i=0}^{m-1} f \circ \tau_{[i](T)}\right) \circ [m] \end{aligned}$$

holds. As the rightmost term is constant, $\prod_{i=0}^{m-1} g \circ \tau_{[i](T')}$ must be constant as well. In particular, it takes the same values at P and $P \oplus T'$:

$$\prod_{i=0}^{m-1} g(P \oplus [i](T')) = \prod_{i=0}^{m-1} g(P \oplus [i+1](T')).$$

Cancelling like factors, where we pick P such that none of the factors are 0, yields

$$g(P) = g(P \oplus [m]T') = g(P \oplus T).$$

In other words,

$$e_m(T, T) = g(P \oplus T)/g(P) = 1$$

holds.
iii.) Let $T \in E[m]$ such that $e_m(S, T) = 1$ holds for all $S \in E[m]$ and let f, g be functions as in the definition of the pairing. It follows that $g(P \oplus S) = g(P)$ for all $S \in E[m]$. Proposition 3.14.ii) then yields that $g \in [m]^*(\overline{k}(E))$ or, put differently, $g = h \circ [m]$ for some $h \in \overline{k}(E)$. We then get the equalities

$$h^m \circ [m] = (h \circ [m])^m = g^m = f \circ [m]$$

from which $h^m = f$ follows. Now, $m \cdot \mathrm{div}(h) = \mathrm{div}(f) = m(T) - m(O)$ holds and we therefore have the equality $\mathrm{div}(h) = (T) - (O)$. From lemma 3.5 we can now conclude that $T = O$ holds.
iv.) Taking f and g as in the definition of the pairing with m, we have $\mathrm{div}(f^{m'}) = mm'(T) - mm'(O)$ and, as $g^m = f \circ [m]$ holds, $(g \circ [m'])^{mm'} = (f \circ [mm'])^{m'}$ holds as well. We therefore have

$$e_{mm'}(S, T) = \frac{(g \circ [m]')(P \oplus S)}{(g \circ [m'])(P)} = \frac{g([m'](P) \oplus [m']S)}{g([m'](P))} = e_m([m']S, T)$$

where $P \in E$ is any point for which the evaluations are defined and non-zero. □

Were we to consider two elliptic curves with an isogeny ϕ from one to the other, then each would have their own Weil pairings. We can relate these pairings using ϕ in the following sense.

Theorem 3.29 [3, III.8.2]
Let $\phi\colon (E_1, O_1) \to (E_2, O_2)$ be an isogeny, then for all $S \in E_1[m]$ and $T \in E_2[m]$ the equality

$$e_m(S, \hat{\phi}(T)) = e_m(\phi(S), T)$$

holds.

Proof: Let f and g be as in the definition of the pairing for T. Using corollary 3.8, choose an $h \in \overline{k}(E_1)$ such that

$$\phi^*((T)) - \phi^*((O_2)) = (\hat{\phi}(T)) - (O_1) + \operatorname{div}(h)$$

holds. We now observe

$$\operatorname{div}\left(\frac{f \circ \phi}{h^m}\right) = \phi^*(\operatorname{div}(f)) - m \cdot \operatorname{div}(h) = m(\phi^*((T)) - \phi^*((O_2)) - \operatorname{div}(h)) = m(\hat{\phi}(T)) - m(O)$$

and

$$\left(\frac{g \circ \phi}{h \circ [m]}\right)^m = \frac{f \circ [m] \circ \phi}{h^m \circ [m]} = \left(\frac{f \circ \phi}{h}\right) \circ [m].$$

We therefore have the equalities

$$e_m(S, \hat{\phi}(T)) = \frac{((g \circ \phi)/(h \circ [m]))(P \oplus S)}{((g \circ \phi)/(h \circ [m]))(P)} = \frac{g(\phi(P) \oplus \phi(S))}{g(\phi(P))} \frac{h([m](P))}{h([m](P) \oplus [m](S))} = e_m(\phi(S), T)$$

where we have used $[m](S) = O_1$ and $P \in E$ is a point such that all evaluations are defined and non-zero. □

This theorem states that ϕ and $\hat{\phi}$ are adjoint with respect to the Weil pairing.

Definition 3.30 [3, p. 88]
Let (E, O) be an elliptic curve and let $\ell \in \mathbb{Z}$ be prime. The ℓ-adic Tate module of E is the group

$$T_\ell(E) := \varprojlim_n E[\ell^n]$$

where the inverse limit is being taken with respect to

$$E[\ell^{n+1}] \xrightarrow{[l]} E[\ell^n].$$

Similarly, we define the Tate module of k to be the group

$$T_\ell(\boldsymbol{\mu}) := \varprojlim_n \boldsymbol{\mu}_{\ell^n}$$

with respect to the maps

$$\boldsymbol{\mu}_{\ell^{n+1}} \xrightarrow{\zeta \mapsto \zeta^\ell} \boldsymbol{\mu}_{\ell^n}.$$

Remark 3.31
Notice that $E[\ell^n]$ has a natural $\mathbb{Z}/\ell^n\mathbb{Z}$-module structure. $T_\ell(E)$ therefore has a $\mathbb{Z}_\ell$-module structure.
From corollaries 3.21 and 3.22 it immediately follows that

$$T_\ell(E) \cong \begin{cases} \mathbb{Z}_\ell \times \mathbb{Z}_\ell, & \ell \neq \mathrm{char}(k); \\ 0 \quad \text{or} \quad \mathbb{Z}_\ell, & \ell = \mathrm{char}(k) \end{cases}$$

as $\mathbb{Z}_\ell$-modules.

These Tate-modules will prove useful as they allow us study isogenies in a different setting. Let $\phi\colon (E_1, O_1) \to (E_2, O_2)$ be an isogeny. As ϕ is a group homomorphism by theorem 3.13, we find $[\ell] \circ \phi = \phi \circ [\ell]$. In particular, ϕ restricts to a map $\phi|_{E_1[\ell^n]}\colon E_1[\ell^n] \to E_2[\ell^n]$ and hence induces a $\mathbb{Z}_\ell$-linear map

$$\phi_\ell\colon T_\ell(E_1) \to T_\ell(E_2)$$

on the Tate modules. As these maps are $\mathbb{Z}_\ell$-linear we can use some concepts from linear algebra to study these induced maps.

Let (E, O) be an elliptic curve. Like isogenies we can also lift the Weil pairings

$$e_{\ell^n}\colon E[\ell^n] \times E[\ell^n] \to \boldsymbol{\mu}_{\ell^n}$$

into an ℓ-adic Weil pairing on the Tate modules;

$$e\colon T_\ell(E) \times T_\ell(E) \to T_\ell(\boldsymbol{\mu}).$$

In order for such a lift to be well-defined, the pairings would have to be compatible with the maps with respect to which we take inverse limits. In other words, we would have to show that

$$e_{\ell^n}([l](S), [l](T)) = e_{\ell^{n+1}}(S, T)^\ell$$

holds for all $S, T \in E[\ell^{n+1}]$. For this we will use theorem 3.28. Let $S, T \in E[\ell^{n+1}]$. We compute

$$e_{\ell^{n+1}}(S, T)^\ell \overset{\text{i.)}}{=} e_{\ell^{n+1}}(S, [\ell](T)) \overset{\text{iv.)}}{=} e_{\ell^n}([\ell](S), [\ell](T))$$

and as such, the pairings lift to a pairing $e\colon T_\ell(E) \times T_\ell(E) \to T_\ell(\boldsymbol{\mu})$. This pairing inherits bilinearity, alternativity, and nondegeneracy as in theorem 3.28 as well as the fact that a (lifted) isogeny and its (lifted) dual are adjoints for the pairing [3, p. 97-98].

Proposition 3.32 [3, III.8.6]
Let (E, O) be an elliptic curve and $l \neq \mathrm{char}(k)$ be a prime.
For every $\phi \in \mathrm{End}(E)$ the equalities

$$\det(\phi_\ell) = \deg(\phi) \qquad \text{and} \qquad \mathrm{tr}(\phi_\ell) = 1 + \deg(\phi) - \deg(1 - \phi)$$

hold. In particular, the determinant and trace of ϕ_ℓ are independent of ℓ.

Proof: Let v_1, v_2 form a $\mathbb{Z}_\ell$-basis for $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ and let

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}(2 \times 2, \mathbb{Z}_\ell)$$

be the matrix associated to ϕ_ℓ with respect to this basis. Employing properties of the pairing and duals we now compute

$$\begin{aligned} e(v_1, v_2)^{\deg(\phi)} &= e(\deg(\phi) \cdot v_1, v_2) = e(\hat{\phi}_l(\phi_l(v_1)), v_2) = e(\phi_l(v_1), \hat{\hat{\phi}}_l(v_2)) = e(\phi_l(v_1), \phi_l(v_2)) \\ &= e(av_1 + cv_2, bv_1 + dv_2) = e(v_1, v_1)^{ab} e(v_1, v_2)^{ad} e(v_2, v_1)^{bc} e(v_2, v_2)^{dc} \\ &= e(v_1, v_2)^{ad-bc} = e(v_1, v_2)^{\det(\phi_\ell)}. \end{aligned}$$

Because the pairing e is nondegenerate we must therefore have $\deg(\phi) = \det(\phi_\ell)$. As for any 2×2-matrix A we have $\det(\mathrm{T}\cdot I_2 - A) = \mathrm{T}^2 - \mathrm{tr}(A)\mathrm{T} + \det(A)$, we find, by setting $T = 1$,

$$\mathrm{tr}(\phi_l) = 1 + \det(\phi_l) - \det(1-\phi_l) = 1 + \det(\phi_l) - \det((1-\phi)_l) = 1 + \deg(\phi) - \deg(1-\phi).$$

□

3.6 The trace of Frobenius

In this subchapter, we will be further investigating the Frobenius map on an elliptic curve defined over a finite field with $q = p^n$ elements. For this, we will need the following fact.

Lemma 3.33 [3, III.5.5]
Let (E, O) be an elliptic curve defined over the field $\mathbb{F}_q$, let ϕ be its q^{th}-power Frobenius map, and let $m, n \in \mathbb{Z}$. Then the map $m + n\phi$ is separable if and only if $p \nmid m$. In particular, $1 - \phi\colon E \to E$ is separable. □

When an elliptic curve is defined over a finite field $\mathbb{F}_q$ one could wonder how many $\mathbb{F}_q$-rational points there are. It is easy to give an upper bound, after all, when given by a Weierstrass equation, for each $x \in \mathbb{F}_q$ there are at most two $y \in \mathbb{F}_q$ such that (x, y) forms an $\mathbb{F}_q$-rational point of the curve. Including the point at infinity, therefore gives an upper bound of $2q + 1$. The following theorem gives a non-trivial bound.

Theorem (Hasse) 3.34 [3, V.1.1]
Let $E/\mathbb{F}_q$ be an elliptic curve. Then

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$$

holds.

Proof: Choose a Weierstrass equation for E with coefficients in $\mathbb{F}_q$ and let $\phi\colon E \to E^{(q)} = E$ denote the q^{th}-power Frobenius on E. For a point $P \in E(\overline{\mathbb{F}_q})$ we then have the equivalence

$$P \in E(\mathbb{F}_q) \qquad \Longleftrightarrow \qquad \phi(P) = P.$$

It follows that $E(\mathbb{F}_q) = \ker(1-\phi)$ holds. As lemma 3.33 tells us that $1 - \phi$ is separable, applying proposition 3.14.iii.) then yields the equality $\#\ker(1-\phi) = \deg(1-\phi)$. By the Cauchy-Schwarz inequality 3.25 and by proposition 3.26 we have

$$|\deg(1-\phi) - \deg(1) - \deg(\phi)| \leq 2\sqrt{\deg(1)\deg(\phi)}.$$

Substituting $\deg(1-\phi) = \#E(\mathbb{F}_q), d(1) = 1$, and $d(\phi) = q$ (by proposition 2.14) yields

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$$

as required. □

The value whose absolute we have bound above in this theorem turns out to be a useful constant of a curve. In the next theorem we name this value and justify its name in the proof.

Theorem 3.35 [3, V.2.3.1]
Let $E/\mathbb{F}_q$ be an elliptic curve, let $\phi\colon E \to E^{(q)} = E$ be the q^{th}-power Frobenius endomorphism, and let $a_q := q + 1 - \#E(\mathbb{F}_q)$. Then

$$\phi^2 - a_q\phi + q = 0$$

holds. We call the value a_q the trace of (the q^{th}-power) Frobenius.

Proof: Let $\ell \neq p$ be a prime. In the proof of theorem 3.34 we have seen that $\#E(\mathbb{F}_q) = \deg(1-\phi)$ holds. By proposition 3.32 we have the equalities

$$\begin{aligned} \det(\phi_\ell) &= \deg(\phi) \overset{2.14}{=} q, \\ \operatorname{tr}(\phi_\ell) &= 1 + \deg(\phi) - \deg(1-\phi) = 1 + q - \#E(\mathbb{F}_q) = a_q. \end{aligned}$$

The characteristic polynomial of ϕ_ℓ therefore equals $\mathrm{T}^2 - a_q\mathrm{T} + q$. By the Cayley-Hamilton theorem, ϕ_ℓ is a root of this polynomial. By again employing proposition 3.32 we now find

$$\deg(\phi^2 - a_q\phi + q) = \det((\phi^2 - a_q\phi + q)_\ell) = \det(\phi_\ell^2 - a_q\phi_\ell + q) = \det(0) = 0.$$

In particular, $\phi^2 - a_q\phi + q$ is the zero map $[0]\colon E \to E$. □

Corollary 3.36 [3, p.150]
Let $E/\mathbb{F}_q$ be an elliptic curve with trace of Frobenius a_q. Then the equivalence

$$E \text{ is supersingular} \quad \Longleftrightarrow \quad a_q \equiv 0 \mod p$$

holds.

Proof: Let $\phi\colon E \to E^{(q)} = E$ be the q^{th}-power Frobenius. By theorem 3.35 the equality $\phi^2 - a_q\phi + q = 0$ holds. In particular, we have $q = (a_q - \phi)\circ\phi$. It follows that $\hat{\phi} = a_q - \phi$ holds. By lemma 3.33 this map is inseparable if and only if $p \mid a_q$. Furthermore, in the proof of corollary 3.22 we see that $E[p^n] = \{O\}$ holds if and only if $\hat{\phi}$ is inseparable. Therefore, E is supersingular if and only if $a_q \equiv 0 \mod p$. □

4 A construction of $\mathbb{F}_{p^{p^n}}$

In this section we will present a construction of the field $\mathbb{F}_{p^{p^n}}$. This will be done by further investigating the p^n torsion subgroups of an ordinary elliptic curve.

4.1 Theory behind the construction

As we know the p^n-torsion subgroups of an ordinary elliptic curve defined over a field of characteristic $p > 0$ to be cyclic of order p^n, their automorphism group is given by $(\mathbb{Z}/p^n\mathbb{Z})^\times$. We will first compute some orders of elements in this automorphism group.

Lemma 4.1
Let p be an odd prime, $m \geq l \geq 1$, and $a \in \mathbb{Z}$. Then $\overline{1+ap^l} \in (\mathbb{Z}/p^m\mathbb{Z})^\times$ has order dividing p^{m-l}.

Proof: We will proof this with induction on m. For $m = 1$ the truth of the statement is clear. Now suppose the statement is true for some $m \geq 1$, we will show it to be true for $m+1$. Suppose $l, a \in \mathbb{Z}$ with $m+1 \geq l \geq 1$. The case where $m+1 = l$ holds is again clear. In the case that $m+1 > l$ holds we have $m \geq l$ and therefore by induction hypothesis that $(1+ap^l)^{p^{m-l}} \equiv 1 \mod p^m$ holds. Therefore we have $(1+ap^l)^{p^{m-l}} \equiv 1 + bp^m \mod p^{m+1}$ for some $b \in \mathbb{Z}$. Taking p-th powers on both sides yields

$$(1+ap^l)^{p^{m+1-l}} \equiv (1+bp^m)^p \equiv \sum_{i=0}^{p} \binom{p}{i} b^i p^{mi} \overset{*}{\equiv} 1 \mod p^{m+1}$$

where we have used that $\binom{p}{i}$ is divisible by p for $0 < i < p$ and that $mp \geq m+1$ holds. This shows that the order of $\overline{1+ap^l} \in (\mathbb{Z}/p^{m+1}\mathbb{Z})^\times$ must divide p^{m+1-l}. □

Corollary 4.2
Let p be an odd prime and $m \geq 1$, then

i.) the elements of order p^{m-1} in $(\mathbb{Z}/p^m\mathbb{Z})^\times$ are precisely the elements of the form $\overline{1+ap}$ where $p \nmid a$,

ii.) the elements of order $2p^{m-1}$ in $(\mathbb{Z}/p^m\mathbb{Z})^\times$ are precisely the elements of the form $\overline{-1+ap}$ where $p \nmid a$.

Proof: i.) If $m = 1$ holds, it is clear that $\overline{1} = \overline{1+p}$ is the only element of order p^{m-1} and that $\overline{1+ap} = \overline{1}$ for all $a \in \mathbb{Z}$ with $p \nmid a$.
Now suppose $m > 1$. Notice that there are precisely p^{m-1} elements of the form $\overline{1+ap}$ in $(\mathbb{Z}/p^m\mathbb{Z})^\times$ where $a \in \mathbb{Z}$ is arbitrary. Similarly there are precisely p^{m-2} elements of the form $\overline{1+ap^2}$ in $(\mathbb{Z}/p^m\mathbb{Z})^\times$ where $a \in \mathbb{Z}$ is arbitrary. As we know $(\mathbb{Z}/p^m\mathbb{Z})^\times$ to be cyclic of order $(p-1)p^{m-1}$ there are precisely p^{m-1} elements with order dividing p^{m-1}. By lemma 4.1 these elements are therefore precisely the elements of the form $\overline{1+ap}$. Similarly there are precisely p^{m-2} elements of $(\mathbb{Z}/p^m\mathbb{Z})^\times$ with order dividing p^{m-2}. By lemma 4.1 these are the elements of the form $\overline{1+ap^2}$. It follows that the elements with order *equal* to p^{m-1} are the elements of the form $\overline{1+ap}$ that are not also of the form $\overline{1+a'p^2}$ which happens precisely when $p \nmid a$.
ii.) Notice that the elements of the form $\overline{-1+ap}$ with $p \nmid a$ are precisely the elements of the form $\overline{1+a'p}$ with $p \nmid a'$ multiplied by -1. As -1 has order 2 and p is coprime with 2, the order of $\overline{-1+ap}$ with $p \nmid a$ will equal $2p^{m-1}$. As there are also precisely $(p-1)p^{m-2}$ elements of order $2p^{m-1}$ in $(\mathbb{Z}/p^m\mathbb{Z})^\times$, this describes all such elements. □

Next, we shift our focus back to the p^n-torsion subgroups of an elliptic curve in an attempt to better understand the Frobenius, which is an automorphism of these subgroups.

Lemma 4.3
Let p be an odd prime and let $E/\mathbb{F}_p$ be an ordinary elliptic curve, then, for every $n \geq 0$, the p^{th}-power Frobenius $F\colon E[p^n] \to E[p^n]$ acts as multiplication by $a_p - \frac{1}{a_p}p + mp^2$ for some $m \in \mathbb{Z}$. Here $\frac{1}{a_p}$ should be interpreted as the inverse of a_p in $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

Proof: If E is supersingular, then $E[p^n]$ is trivial and the statement is true. Suppose that E is ordinary, then $T_p(E) \cong \mathbb{Z}_p$ and the lift F_p to $\mathbb{Z}_p$ of the Frobenius is a root of $\mathrm{T}^2 - a_p\mathrm{T} + p$ by theorem 3.35. Notice that modulo p^2 this polynomial factors as

$$\mathrm{T}^2 - a_p\mathrm{T} + p \equiv \left(\mathrm{T} - a_p + \frac{p}{a_p}\right)\left(\mathrm{T} - \frac{p}{a_p}\right) \mod p^2$$

where we take the inverse of a_p modulo p^2. As $-a_p + \frac{p}{a_p}$ and $-\frac{p}{a_p}$ are incongruent modulo p, the first is nonzero while the second is zero, p will divide at most one of these factors. It follows that the roots of $\mathrm{T}^2 - a_p\mathrm{T} + p$ modulo p^2 are precisely the roots of $\mathrm{T} - a_p + \frac{p}{a_p}$ and $\mathrm{T} - \frac{p}{a_p}$ modulo p^2. In particular, modulo p^2 the Frobenius acts as multiplication by $a_p + \frac{p}{a_p}$ or as multiplication by $\frac{p}{a_p}$. As multiplication by $\frac{p}{a_p}$ is not injective, the Frobenius acts as multiplication by $a_p + \frac{p}{a_p}$ modulo p^2. It follows that, for $n \geq 0$, the Frobenius acts as multiplication by $a_p - \frac{1}{a_p}p + mp^2$ on $E[p^n]$ for some $m \in \mathbb{Z}$. □

Definition 4.4
Let p be prime. Define $d\colon \overline{\mathbb{F}_p} \to \mathbb{Z}_{\geq 1},\ x \mapsto [\mathbb{F}_p(x) : \mathbb{F}_p]$. We will refer to $d(x)$ as the degree of x.
We extend this definition to $\overline{\mathbb{F}_p} \times \overline{\mathbb{F}_p}$ by sending (x, y) to $[\mathbb{F}_p(x, y) : \mathbb{F}_p]$.

Remark 4.5
Note that for $x \in \overline{\mathbb{F}_p}$ the value $d(x)$ is precisely the length of the Frobenius orbit of x;

$$d(x) = \#\left\{x^{p^n} : n \geq 0\right\}.$$

Similarly, for $(x, y) \in \overline{\mathbb{F}_p} \times \overline{\mathbb{F}_p}$, we have

$$d(x, y) = \#\left\{\left(x^{p^n}, y^{p^n}\right) : n \geq 0\right\}.$$

We therefore have the equality $d(x, y) = \mathrm{lcm}(d(x), d(y))$.

The degree of a point (x, y) on an elliptic curve can be related to the degree of x in the following sense.

Lemma 4.6
Let p be an odd prime, let $E/\mathbb{F}_p$ be an elliptic curve given by a Weierstrass equation and let $(x, y) \in E(\overline{\mathbb{F}_p})$.
If $d(x) = p^n$ for some $n \geq 0$, then $d(x, y) = \varepsilon p^n$ holds for some $\varepsilon \in \{1, 2\}$.
Conversely,

i.) if $d(x, y) = p^n$ for some $n \geq 0$ then $d(x) = p^n$;

ii.) if $d(x) \leq p^n$ for some $n \geq 0$ and $d(x, y) = 2p^n$ then $d(x) = p^n$.

Proof: Given $d(x) = p^n$ holds, we consider $\varepsilon := [\mathbb{F}_p(x, y) : \mathbb{F}_p(x)]$. As y is the root of a degree 2 polynomial with coefficients in $\mathbb{F}_p(x)$, this degree is either 1 or 2. It follows that

$$d(x, y) = [\mathbb{F}_p(x, y) : \mathbb{F}_p] = [\mathbb{F}_p(x, y) : \mathbb{F}_p(x)] \cdot [\mathbb{F}_p(x) : \mathbb{F}_p] = \varepsilon \cdot d(x) = \varepsilon p^n$$

holds with $\varepsilon \in \{1, 2\}$ as required.
For converse i.) we find $p^n = d(x, y) = \mathrm{lcm}(d(x), d(y))$ so both degrees are powers of p and the largest is equal to p^n. Because the degree of y is at most twice as large as that of x (as y is the root of a degree 2 polynomial with coefficients in $\mathbb{F}_p(x)$) and $p > 2$ we find $d(x) = p^n$.
For ii.) we have

$$2p^n = d(x, y) = [\mathbb{F}_p(x, y) : \mathbb{F}_p] = [\mathbb{F}_p(x, y) : \mathbb{F}_p(x)] \cdot [\mathbb{F}_p(x) : \mathbb{F}_p] = [\mathbb{F}_p(x, y) : \mathbb{F}_p(x)] \cdot d(x).$$

As $[\mathbb{F}_p(x, y) : \mathbb{F}_p(x)] \leq 2$ and $d(x) \leq p^n$ hold, both of these must be equalities. In particular, $d(x) = p^n$ as required. □

Theorem 4.7
Let $p > 5$ be prime and let $E/\mathbb{F}_p$ be an elliptic curve given by a Weierstrass equation. Suppose $(x, y) \in E(\overline{\mathbb{F}_p})$ has order p^n for some $n \geq 1$, then

$$\#\mathbb{F}_p(x) = p^{p^{n-1}} \quad \text{if and only if} \quad a_p = \pm 1.$$

Proof: If E is supersingular, then there are no points of order p^n with $n \geq 1$ so the theorem holds. Suppose E is ordinary and suppose $(x, y) \in E(\overline{\mathbb{F}_p})$ has order p^n for some $n \geq 1$.
$\Rightarrow$: If $\#\mathbb{F}_p(x) = p^{p^{n-1}}$ holds we have $d(x) = p^{n-1}$. Therefore, by lemma 4.6, we have $d(x, y) = \varepsilon p^{n-1}$ for some $\varepsilon \in \{1, 2\}$. As (x, y) has order p^n it generates $E[p^n]$ and the order of the Frobenius F on this torsion subgroup is determined by the length of the orbit of (x, y); the Frobenius has order εp^n on this subgroup. By corollary 4.2 this means the Frobenius acts as multiplication by $\varepsilon' + ap$ for some $\varepsilon' \in \{\pm 1\}$ and $a \in \mathbb{Z}$ with $p \nmid a$. By lemma 4.3, however, we know it acts as multiplication by $a_p - \frac{1}{ap} + mp^2$ for some $m \in \mathbb{Z}$. It follows that $\varepsilon' + ap \equiv a_p - a_p^{-1}p + mp^2 \mod p^n$ holds. By further reducing this modulo p we find $\varepsilon' \equiv a_p \mod p$ so $a_p = \varepsilon' + bp$ for some integer b. As we have $|a_p| < p - 1$ by theorem 3.34 (here we use $p > 5$) it follows that $b = 0$ holds and $a_p \in \{\pm 1\}$ as required.
$\Leftarrow$: If $a_p = 1$ holds, the Frobenius will have order p^{n-1} as an automorphism of $E[p^n]$, this follows from lemma 4.3 and corollary 4.2. As (x, y) generates $E[p^n]$ the length of its Frobenius orbit will equal this order; $d(x, y) = p^{n-1}$. From lemma 4.6 it now follows that $d(x) = p^{n-1}$ holds, or equivalently, $\#\mathbb{F}_p(x) = p^{p^{n-1}}$ holds.
If $a_p = -1$ holds, the Frobenius will have order $2p^{n-1}$ as an automorphism of $E[p^n]$, this follows from lemma 4.3 and corollary 4.2. As (x, y) generates $E[p^n]$ the length of its Frobenius orbit will equal this order; $d(x, y) = 2p^{n-1}$. Let x_0 be the first coordinate of the point $[p^{n-1}](x, y) \in E[p]$. As the Frobenius acts as -1 on this group and a point and its inverse share their first coordinate (group law formulas 3.9.i)) we find $F(x_0) = x_0$ and as such $x_0 \in \mathbb{F}_p$. By repeatedly applying the group law formulas given in 3.9 and substituting the Weierstrass equation for y, the first component of $[p^{n-1}]$ can be written as a rational function with numerator and denominator of degree at most $(p^{n-1})^2$. As the multiplication-by-p map factors through the Frobenius F, the multiplication-by-p^{n-1} map factors through F^{n-1}. In particular, the numerator and denominator are of the form $f(\mathrm{X}^{p^{n-1}})$ and $g(\mathrm{X}^{p^{n-1}})$ with $f, g \in \mathbb{F}_p(\mathrm{X})$ of degree at most p^{n-1}. Notice that $f(\mathrm{X}^{p^{n-1}}) = f(\mathrm{X})^{p^{n-1}}$ and $g(\mathrm{X}^{p^{n-1}}) = g(\mathrm{X})^{p^{n-1}}$ hold. We now find the equalities

$$x_0 = \frac{f(x^{p^{n-1}})}{g(x^{p^{n-1}})} = \frac{f(x)^{p^{n-1}}}{g(x)^{p^{n-1}}} = \left(\frac{f(x)}{g(x)}\right)^{p^{n-1}}.$$

As taking p^{th}-powers is injective and $x_0^p = x_0$ holds, we find $f(x)/g(x) = x_0$ and as such $f(x) - x_0 g(x) = 0$. This shows that x is the root of a degree p^{n-1} polynomial with coefficients in $\mathbb{F}_p$. In particular, $d(x) = [\mathbb{F}_p(x) : \mathbb{F}_p] \leq p^{n-1}$ holds. From lemma 4.6 it now follows that $d(x) = p^{n-1}$ holds, or equivalently, $\#\mathbb{F}_p(x) = p^{p^{n-1}}$ holds. □

Remark 4.8
For $p = 3, 5$ the right hand side of the equivalence can be replaced with "$a_p \equiv \pm 1 \mod p$".

What makes the elliptic curves with $a_p = \pm 1$ special is that the elements of order p have first coordinate in $\mathbb{F}_p$. What happens if we move our frame of reference away from $\mathbb{F}_p$? That is, if $(x, y), (x', y') \in E$ are elements of order p^n respectively p^{n+1} for some $n \geq 1$, can we expect the degree $[\mathbb{F}_p(x') : \mathbb{F}_p]$ to be p times the degree $[\mathbb{F}_p(x) : \mathbb{F}_p]$, similar to what we have observed in theorem 4.7? As it turns out, this does not hold true. Take, for example, the elliptic curve E over $\mathbb{F}_p$ with $p = 5$ given by

$$y^2 = x^3 + 4x + 2.$$

This curve has trace of Frobenius $a_p = 3$ and $\#E(\mathbb{F}_{p^4}) = 675 = 25 \cdot 27$ holds. In particular, we have the inclusion $E[p^2] \subset E(\mathbb{F}_{p^4})$. Here, the first coordinates of points of order p^2 certainly do not have degree p times as large as first coordinates of points of order p. This is in line with lemma 4.3; $a_p = 3$ has order 4 in $(\mathbb{Z}/5\mathbb{Z})^\times$ and $a_p - a_p^{-1} \cdot 5 = 3 - 17 \cdot 5 = 18 \in (\mathbb{Z}/25\mathbb{Z})^\times$ also has order 4. From this, the inclusion $E[p^2] \subset E(\mathbb{F}_{p^4})$ follows. In a sense, theorem 4.7 cannot easily be generalized to make statements relating arbitrary a_p to the degrees of first coordinates of points of order p^n.

4.2 Implementation of the construction

In the part of the proof where $a_p = -1$ holds, we notice that x is the root of the degree p^{n-1} polynomial $f - x_0 \cdot g$. As x has degree p^{n-1}, this must be the minimal polynomial (up to scalars) of x. We can use this observation to algorithmically calculate this minimal polynomial.

Verschiebung Algorithm 4.9

Input:

- a prime p;
- coefficients $a, b \in \mathbb{F}_p$ that define an elliptic curve given by $y^2 = x^3 + ax + b$.

Output:

- Polynomials $f, g \in \mathbb{F}_p[\mathrm{X}]$ such that, on the first coordinate, multiplication by p is the composition of f/g with the p^{th}-power Frobenius. In other words, the Verschiebung V of the elliptic curve specified in the input is given by f/g on the first coordinate.

Algorithm:

i.) By repeatedly doubling, calculate explicit formulas for $[2^n](x, y)$ with (x, y) indeterminate on E and $n = 0, 1, \ldots, \lfloor \log_2(p) \rfloor =: m$. This can be achieved using the group law formulas 3.9, in particular, the case where $x_1 = x_2$ holds.

ii.) Write $p = c_0 2^0 + \ldots + c_m 2^m$ with $c_i \in \{0, 1\}$, the binary representation of p. Using the formula for the case $x_1 \neq x_2$, add the formulas for $[2^i](x, y)$ with $c_i \neq 0$. This yields rational functions for $[p](x, y)$.

iii.) In this expression for $[p]$, y will only occur as a square on the first coordinate function (if simplified). Replace all these occurrences with $x^3 + ax + b$. This yields a rational function in x on the first coordinate.

iv.) The rational function on the first coordinate is of the form $f(x^p)/g(x^p)$ with $f, g \in \mathbb{F}_p[\mathrm{X}]$. Extract f and g by dividing all exponents of x in this first coordinate function by p.

v.) Multiply f and g with an appropriate constant such that f becomes monic.

vi.) Return f, g.

If $p \neq 2, 3$ holds, then for any elliptic curve E defined over $\mathbb{F}_p$ there are $a, b \in \mathbb{F}_p$ such that E is isomorphic to the elliptic curve given by $y^2 = x^3 + ax + b$. Therefore, the fact that the algorithm restricts itself to curves given by such an equation need not restrict its applicability outside of characteristic 2 and 3.
As we will be applying theorem 4.7, in our case $a_p = \pm 1$ holds. Instead of calculating $[p]$ it might be faster or easier to calculate $[a_p] - F$ where F is the p^{th}-power Frobenius. As seen in the proof of corollary 3.36, this equals the Verschiebung.

Algorithm for Constructing $\mathbb{F}_{p^{p^n}}$ 4.10

Input:

- a prime $p > 5$;
- coefficients $a, b \in \mathbb{F}_p$ that define an elliptic curve given by $y^2 = x^3 + ax + b$ with trace of Frobenius $a_p = \pm 1$;
- the trace of Frobenius a_p of the elliptic curve;
- a positive integer n.

Output:

- An irreducible polynomial $h \in \mathbb{F}_p[\mathrm{X}]$ of degree p^n such that a root of h appears as the first coordinate of a point of order p^{n+1} on the specified elliptic curve.
- The field with p^{p^n} elements realized as $\mathbb{F}_p[\mathrm{X}]/(h)$.

Algorithm:

i.) Apply algorithm 4.9 to calculate f and g such that f/g gives the first coordinate function of the Verschiebung of the specified elliptic curve.

ii.) If $a_p = 1$:

- Find $x_0 \in \mathbb{F}_p$ such that $y^2 = x_0^3 + ax_0 + b$ has a solution in $\mathbb{F}_p$. In other words, such that $x_0^3 + ax_0 + b$ is a square in $\mathbb{F}_p$.

Else:

- Find $x_0 \in \mathbb{F}_p$ such that $y^2 = x_0^3 + ax_0 + b$ *does not* have a solution in $\mathbb{F}_p$. In other words, such that $x_0^3 + ax_0 + b$ is *not* a square in $\mathbb{F}_p$.

Note that in either case precisely $\frac{p-1}{2}$ such $x_0 \in \mathbb{F}_p$ exist. Therefore, this can be done by uniformly choosing an $x_0 \in \mathbb{F}_p$ until it satisfies the condition. Each independent choice has probability $\frac{p-1}{2p} \xrightarrow{p\to\infty} \frac{1}{2}$ of satisfying the condition. Further note that checking whether an element is square in $\mathbb{F}_p$ can be done by raising the element to the power of $\frac{p-1}{2}$; squares will yield 1, non-squares -1.

iii.) Define $h_1(\mathrm{X}) := f(\mathrm{X}) - x_0 \cdot g(\mathrm{X})$.

iv.) For $i = 2, \ldots, n$, define

$$h_i(\mathrm{X}) := g(\mathrm{X})^{p^{i-1}} h_{i-1}\left(\frac{f(\mathrm{X})}{g(\mathrm{X})}\right) \in \mathbb{F}_p(\mathrm{X}).$$

v.) Return h_n, $\mathbb{F}_p[\mathrm{X}]/(h_n)$.

For the correctness of this algorithm we note that x_0 appears as the first coordinate of a point of order p on the specified curve E. After all, if $a_p = 1$ holds, there are precisely p $\mathbb{F}_p$-rational points, including O, on the curve. The subgroup $E(\mathbb{F}_p)$ therefore has order p and must therefore equal $E[p]$. Any point different from O in $E(\mathbb{F}_p)$ is therefore an element of order p. In the case that $a_p = -1$ holds, we know, by lemma 4.3, that the p^{th}-power Frobenius F acts as multiplication by -1 on $E[p]$. The points of order p therefore have first coordinate in $\mathbb{F}_p$ and second coordinate in a quadratic extension of $\mathbb{F}_p$. As $a_p = -1$ holds, there are precisely $p - 1$ such points on E and these must therefore be the points of order p. In either case, x_0 appears as the first coordinate of a point of order p.
We now define sets $A_i \subset \overline{\mathbb{F}_p}$ for $i \geq 0$. We let A_i be the set of $a \in \overline{\mathbb{F}_p}$ for which a appears as the first coordinate of a point P_a of order p^{i+1} where $[p^i](P_a)$ has first coordinate x_0. In other words

$$A_i := \pi_x([p^i]^{-1}(\{P_{x_0}, \ominus P_{x_0}\}))$$

where π_x denotes projection on the first coordinate and P_{x_0} is a point on E with first coordinate x_0. A visualization of these set can be found in figure 1. Let $a \in A_1$ and let P_a be a point on E with a as its first coordinate. We compute

$$x_0 = \pi_x([p](P_a)) = \pi_x(FV(P_a)) = F(\pi_x(V(P_1))) = F\left(\frac{f(a)}{g(a)}\right)$$

where F and V are the Frobenius and Verschiebung respectively. As F is injective and $F(x_0) = x_0$ holds, we find $f(a)/g(a) = x_0$ from which $h_1(a) = f(a) - x_0 \cdot g(a) = 0$ follows.
Let $a \in A_{i+1}$ with $i \geq 0$ and let P_a be a point on E with first coordinate a. We then have $\pi_x([p](P_a)) \in A_i$. On the other hand, we also have

$$\pi_x([p](P_a)) = \pi_x(FV(P_a)) = F(\pi_x(V(P_a))) = F\left(\frac{f(a)}{g(a)}\right)$$

As h_i has coefficients in $\mathbb{F}_p$ we know that $f(a)/g(a)$ is a root of h_i if and only if $F(f(a)/g(a))$ is a root. It now follows by induction that for every $i \geq 1$ and $a \in A_i$ the equality $h_i(a) = 0$ holds. After all, we have shown that every $a \in A_1$ is a root of h_1 and we have shown that, for every $a \in A_{i+1}$ with $i \geq 1$, $F(f(a)/g(a))$ is an element of A_i. Therefore $f(a)/g(a)$ is a root of h_i and by definition of h_{i+1} we see that a must then be a root of h_{i+1}.

If we now let $(x_n, y_n) \in E$ be a point with $\pi_x([p^n](x_n, y_n)) = x_0$, that is $x_n \in A_n$, then by theorem 4.7 x_n has degree p^n and we have just shown it is the root of the degree p^n polynomial h_n. It follows that h_n is irreducible. In fact, h_n is the minimal polynomial of x_n.

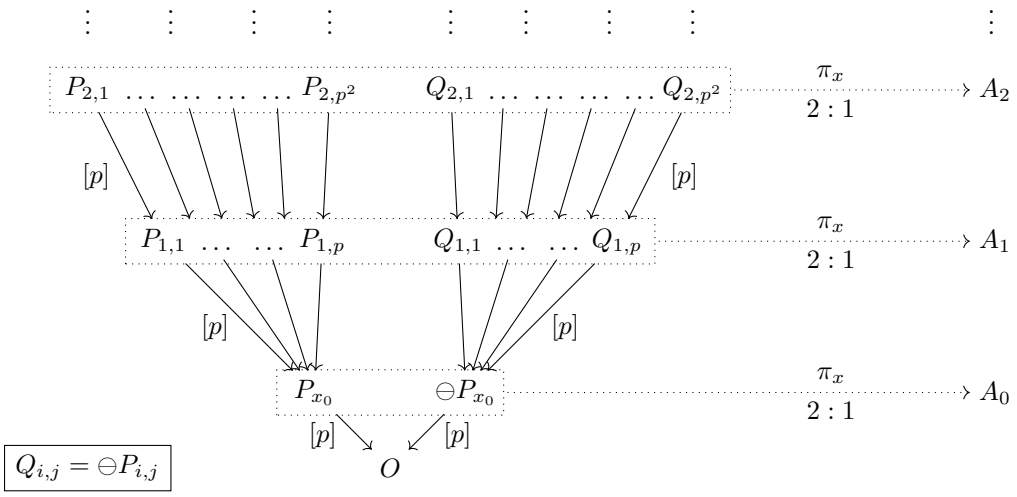


Figure 1: A visualization of the sets $A_i \subset \overline{\mathbb{F}_p}$.

Alternatively, rather than taking an immediate degree p^n extension of $\mathbb{F}_p$, the field $\mathbb{F}_{p^{p^n}}$ can also be realized by iteratively taking degree p extensions starting at $\mathbb{F}_p$ for a total of n times. This can be done as follows:

i.) Calculate f, g, x_0 as in algorithm 4.10 and define $k_0 := \mathbb{F}_p$.

ii.) For $i = 1, \ldots, n$ define

$$f_i(\mathrm{X}_i) := f(\mathrm{X}_i) - \mathrm{X}_{i-1} \cdot g(\mathrm{X}_i) \in k_{i-1}[\mathrm{X}_i] \qquad \text{and} \qquad k_i := k_{i-1}[\mathrm{X}_i]/(f_i(\mathrm{X}_i)).$$

Each k_i will then be a field with p^i elements and $f_i \in k_{i-1}[\mathrm{X}_i]$ will be irreducible of degree p. This is precisely what happens in the construction of Wiedemann from the introduction. There, $f(\mathrm{X}) = \mathrm{X}^2 + 1$ and $g(\mathrm{X}) = \mathrm{X}$ hold and the X_i are precisely the γ_i. A short implementation of step ii.) in the GAP programming language can be found in appendix A.

Applying theorem 4.1 from [5] which can be found in appendix B, we get the following result.

Theorem 4.11
Let p be an odd prime and let $E/\mathbb{F}_p$ be an elliptic curve with $a_p = \pm 1$. Then there exists $\delta > 0$ such that for every $n \geq 1$ the first coordinate of a point of order p^n on E has multiplicative order greater than $\exp(p^{\delta n})$. In particular, in the context of algorithm 4.10 there exists $\delta > 0$ depending on the prime p and the specified curve, such that for every $n \geq 1$ a root of h_n has multiplicative order at least $\exp(p^{\delta n})$. □

Using the construction presented in this thesis we therefore get a non-trivial lower bound on the multiplicative order of the roots of the polynomial(s) used to define the extensions.

Future work

It would be interesting to further study elliptic curves with $a_p \neq \pm 1$. In particular, when we can expect higher order torsion points to consistently yield larger field extensions when adjoining their first coordinate to $\mathbb{F}_p$. After theorem 4.7, a quick counterexample was presented that shows this need not be the case when $p = 5$ and $a_p = 3$ hold. However, $\mathbb{F}_5^\times$ comes equipped with another element of order 4, namely 2. The Frobenius of an elliptic curve $E/\mathbb{F}_5$ with $a_p = 2$ would act as an order 4 automorphism of $E[p]$ and as an order 20 automorphism of $E[p^2]$. In this case we do get a degree p extension when adjoining the first coordinate of a point of order p^2 to $\mathbb{F}_p$ over the field obtained by adjoining the first coordinate of a point of order p to $\mathbb{F}_p$. For the 'bad' case $a_p = 3$ we have the 'good' case $a_p = 2$, both of which have the same order in $\mathbb{F}_5^\times$. It would be interesting to study whether this is perhaps a general truth, that is, does there exist a 'good' case for every 'bad' case. Perhaps, it would also (or instead) be possible to make a classification of precisely when these 'bad' cases occur, if at all.

References

[1] Aart Blokhuis, Xiwang Cao, Wun-Seng Chou, and Xiang-Dong Hou. On the roots of certain dickson polynomials. *Journal of Number Theory*, 188:229–246, 01 2018.

[2] Robin Hartshorne. *Algebraic Geometry*, volume 52. Springer, New York, first edition, 1977.

[3] Joseph Hillel Silverman. *The Arithmetic of Elliptic Curves*, volume 106. Springer, New York, second edition, 2016.

[4] Peter Stevenhagen. *Algebra III*. Universiteit Leiden, Leiden, 2020.

[5] José Felipe Voloch. Elements of high order on finite fields from elliptic curves. *Bulletin of the Australian Mathematical Society*, 81(3):425–429, 2010.

[6] Doug Wiedemann. An iterated quadratic extension of GF(2). *The Fibonacci Quarterly*, 26, 01 1988.

Appendix

A Code

Some elliptic curves with $a_p = \pm 1$ for $2 \leq p \leq 59$ were precomputed using SageMath. SageMath has an elliptic curve class with implementations of the multiplication-by-m map and allows for easy calculation of the trace of Frobenius. The code below is a GAP implementation of step ii.) introduced at the end of chapter 4.

```
#############################################################################
##
##  <#GAPDoc Label="ECTorsionConstruction">
##  <ManSection>
##  <Meth Name="ConstructFieldOfPPNElements" Arg="p, n"/>
##  <Meth Name="ConstructionInformation" Arg="p"/>
##
##  <Description>
##  Returns a list. The first element of the list is a field with
##  p^p^n elements recursively defined using degree p field extensions.
##  The remaining n elements are the defining polynomials used to realize
##  these extensions in order of use: the second element is an irreducible
##  polynomial of degree p over <C>GF(p)</C>. The third element is an
##  irreducible polynomial of degree p over <C>GF(p^p)</C>, etc.
##  Use the <C>ConstructionInformation</C> method to find more details on
##  the specifics of the construction for a given prime.
##  </Description>
##  </ManSection>
##  <#/GAPDoc>

DeclareOperation( "ConstructFieldOfPPNElements" , [IsInt, IsInt]); #tst
DeclareOperation( "ConstructionInformation" , [IsInt]); #tst

#############################################################################

ConstructFieldOfPPNElements:=function(p, n)
    local x, VerschiebungNumerator, VerschiebungDenominator, coefficients, i, \\
          F, rootOfDefiningPolynomial, definingPolynomial, returnList;

    #Handle non-primes
    if p < 2 or p > 59 or not IsPrime(p) then
        Print("No construction using elliptic curves has been implemented for \\
               p = ", p);
        return;
    fi;

    #Handle non-positive n
    F:=GF(p);
    returnList:=[F];
    if n <= 0 then
        return returnList;
    fi;

    #Used to define extension fields of GF(p)
    x:=Indeterminate(F, "x");

    #Construct Verschiebung numerator
    coefficients:=EvalString(Concatenation("RecursionNumerator", String(p)));
```

```
    VerschiebungNumerator:=0;
    for i in [1..Length(coefficients)] do
        VerschiebungNumerator:=VerschiebungNumerator+((coefficients[i])*\\
                                                    (x^(i-1)));
    od;

    #Construct Verschiebung denominator
    coefficients:=EvalString(Concatenation("RecursionDenominator", String(p)));
    VerschiebungDenominator:=0;
    for i in [1..Length(coefficients)] do
        VerschiebungDenominator:=VerschiebungDenominator+((coefficients[i])*\\
                                                        (x^(i-1)));
    od;

    #Construct the extension of degree p^n
    rootOfDefiningPolynomial:=EvalString(Concatenation("RecursionStartingPoint"\\
                                                      , String(p)));
    for i in [1..n] do
        definingPolynomial:=VerschiebungNumerator-rootOfDefiningPolynomial*\\
        VerschiebungDenominator;
        Append(returnList, [definingPolynomial]);
        F:=FieldExtension(F, definingPolynomial);
        returnList[1]:=F;
        rootOfDefiningPolynomial:=RootOfDefiningPolynomial(F);
    od;

    return returnList;

end;

ConstructionInformation:=function(p)
    local weierstrassCoefficients, traceOfFrobenius;
    if p < 2 or p > 59 or not IsPrime(p) then
        Print("No construction using elliptic curves has been implemented for \\
               p = ", p);
        return;
    fi;

    weierstrassCoefficients:=EvalString(Concatenation("WeierstrassCoefficients"\\
                                                      , String(p)));
    traceOfFrobenius:=EvalString(Concatenation("TraceOfFrobenius", String(p)));
    if p = 2 then
        Print("The roots of the defining polynomial for the field with p^p^n \\
               elements occur \nas x-coordinates of points of order p^{n+1} \\
               of the elliptic curve given by", "\n");
        Print("\t\t\ty^2 + xy = x^3 + 1.\n");
    elif p = 3 then
        Print("The roots of the defining polynomial for the field with p^p^n \\
               elements occur \nas x-coordinates of points of order p^n of \\
               the elliptic curve given by", "\n");
        Print("\t\t\ty^2 = x^3 + x^2 + 2.\n");
    else
        Print("The roots of the defining polynomial for the field with p^p^n \\
               elements occur \nas x-coordinates of points of order p^n of \\
               the elliptic curve given by", "\n");
        Print("\t\t\ty^2 = x^3 + ", weierstrassCoefficients[1], "x + ", \\
```

```
                weierstrassCoefficients[2], ".\n");
    fi;
    Print("This elliptic curve has trace of Frobenius equal to ", \\
          traceOfFrobenius, ".\n");
end;
```

B Additional theorems

Proposition [3, II.5.8]
Let $G_{\overline{k}/k}$ denote the Galois group of $\overline{k}$ over k and let C/k be a smooth curve. Let $\mathrm{Div}_k(C)$ denote the divisors fixed by the action of $G_{\overline{k}/k}$. For every $D \in \mathrm{Div}_k(C)$ the $\overline{k}$-vector space $\mathcal{L}(D)$ has a basis consisting of functions in $k(C)$.

Theorem (Bézout) [2, I.7.8]
Let C_1, C_2 be distinct planar curves of degree m and n. Then C_1 and C_2 intersect in precisely mn points, counting multiplicity.

Theorem [5, 4.1]
Let E be an elliptic curve and y a non-constant function on E, with both y and E defined over $\mathbb{F}_q$. Given $\varepsilon > 0$, there exist $\delta > 0$ and $d_0 \in \mathbb{Z}$ such that, if $P \in E$ satisfies

i.) $d := [\mathbb{F}_q(P) : \mathbb{F}_q] > d_0$,

ii.) the group generated by P is invariant under the q^{th}-power Frobenius,

iii.) the order of P, say r, satisfies $r < d^{\frac{3}{2}-\varepsilon}$,

then $y(P)$ has multiplicative order at least $\exp(d^{\delta})$.

C List of symbols

symbol	clarification		
$\oplus$	14	i, j, l, m, n	indices/integers
$[m]$	19	k	field
a_q	29	$\overline{k}$	algebraic closure of k
C	curve	$k^\times$	group of units of k
$C(k)$	k-rational points of C	k_C	12
$\deg(D)$	10	k_n	2
$\deg(\phi)$	7	$k(C)$	5
$\mathrm{Div}(C), \mathrm{Div}^0(C)$	10	$\mathcal{L}(D)$	11
$\mathrm{div}(f)$	10	$\ell(D)$	11
$\mathrm{div}(\omega)$	11	$\boldsymbol{\mu}_m$	25
E	elliptic curve	$\mathrm{ord}_P(f)$	5
$E[m]$	19	Ω_C	11
$E^{(q)}$	14	$\mathrm{Pic}(C), \mathrm{Pic}^0(C)$	10
e	28	$\hat{\phi}$	21
e_m	25	ϕ^*	7
$e_\phi(P)$	8	ϕ_ℓ	28
F_n	4	$T_\ell(E)$	27
$\mathbb{F}_{p^n}$	field with p^n elements	$T_\ell(\boldsymbol{\mu})$	27
g	12	$\mathrm{Tr}^{(n)}$	2
γ_n	2	$\mathbb{Z}_\ell$	ℓ-adic integers