Behavior of primes in division fields of elliptic curves

Alex Braat
Student nr. 37796416
20 August 2020

Master Thesis
Mathematical Sciences
Utrecht University

Utrecht University

Supervisor: Prof. dr. Gunther Cornelissen
Second Reader: Dr. Valentijn Karemaker

Behavior of primes in division fields of elliptic curves

Alex Braat

Abstract

Given elliptic curve E, we consider a family of field extension generated by n-torsion points of E, called division fields. The main objective of this thesis is determine the behavior of primes of good reduction in these extensions. Depending on a divisibility criterion, we get a case distinction into unramified and (possibly) ramified primes. In the unramified case we find a matrix representative of the Frobenius conjugacy class in the Galois group, using information about the endomorphism ring of the reduced curve. We will generalize this to abelian varieties, which introduces some difficulties. Finally, we give a lower bound for the ramification index in the ramified case, using Newton polygons.

Contents

1 Introduction

Given an elliptic curve E over a number field K, we consider the family of Galois extensions of K given by the fields of definition of torsion subgroups of E. When E is given by a Weierstrass equation

$$y^2 = x^3 + ax + b, \tag{1}$$

the n-th division field $K(E[n])$ is obtained by adjoining to K the x- and y- coordinates of all n-torsion points. In this thesis we will look at how primes of K with good reduction for E split in these extensions.

In order to motivate this, we note that the construction of these fields is very similar to those of cyclotomic fields, where in the case of $K(\zeta_n)$ the n-torsion points of the multiplicative group $\overline{K}^*$ are adjoined to K. Cyclotomic extensions play an important role in number theory. They are well understood, and primes behave predictably.

Understanding division fields leads to a couple of applications. One type of application is studying number fields by embedding them into a division field if possible. For cyclotomic extensions we have the theorem of Kronecker-Weber, which states that any abelian extension of $\mathbb{Q}$ can be embedded into some cyclotomic extension $\mathbb{Q}(\zeta_n)$. For an imaginary quadratic field K, similar results can be achieved using division fields of any elliptic curve with complex multiplication by the ring of integers $\mathcal{O}_K$, see [Sil94, II.5.6].

Another such application is given in [DT02], where the splitting fields of certain non-solvable quintics can be embedded in the 5th division fields of corresponding elliptic curves.

A second type of application is studying the absolute Galois group $G_{\overline{K}/K}$ of K by ℓ-adic representations. In the cyclotomomic case, for any prime ℓ this leads to the 1-dimensional cyclotomic character

$$\chi_\ell \colon G_{\overline{K}/K} \to \mathbb{Z}_\ell^*, \tag{2}$$

defined by the action of Galois elements on ℓ-power roots of unity, explicitly given by $\sigma(\zeta_{\ell^n}) = \zeta_{\ell^n}^{\chi_\ell(a) \mod \ell^n}$ for $\sigma \in G_{\overline{K}/K}$. For division fields of elliptic curves we will see that we get a 2-dimensional ℓ-adic representation

$$\rho_\ell \colon G_{\overline{K}/K} \to \mathrm{GL}_2(\mathbb{Z}_\ell), \tag{3}$$

defined by the action of Galois elements on the ℓ-power torsion points of E. Such ℓ-adic representations are extensively studied by Serre in [Ser97].

A third type of application is determining the possible K-rational torsion subgroups for elliptic curves over a given number field K, or number fields K of a given degree. Over $\mathbb{Q}$ such a classification was first given by Mazur [Maz77, MG78]. These results have been generalized to number fields of higher degrees and the theory of sporadic points, see [Sut12]. In [Smi18] ramification in division fields is used to show that elliptic curves with certain supersingular reduction conditions cannot correspond to sporadic points on modular curves.

This thesis will be divided into 4 parts. In part I, we will take a closer look at torsion points and division fields in general. We will show that primes of good reduction will split into two classes, unramified and ramified, depending on whether the prime divides n.

In part II we will take a closer look at the unramified primes. In particular we will look at a result of Duke and Tóth [DT02], which gives a representative of the similarity class of the Frobenius for any unramified prime. We give an alternative proof, using the module structure of the endomorphism ring on Tate modules.

In part III we try to generalize the results of part II to abelian varieties, for which our alternative proof is more suited. We obtain partial results, depending on whether the endomorphism ring satisfies certain properties regarding fractional ideals.

In part IV we return to elliptic curves, but this time we look at the ramified primes. We will study lower bounds for the ramification index for primes with supersingular reduction, using Newton polygons on both division polynomials and the multiplication-by-p map in the formal group.

I would like to give very special thanks to my supervisor Gunther Cornelissen, for his excellent guidance and input, and for suffering through my sometimes irregular writing schedule. Furthermore, I would like to thank Stefano Marseglia, Valentijn Karemaker and Hanson Smith for answering my questions through Skype and email. Lastly, I want to express my gratitude to Reem Chaalan and Evie Roebroek for pushing and motivating me.

1.1 Prerequisites

We will assume the reader is familiar with the basic concepts of elliptic curves and algebraic number theory. For elliptic curves we refer the reader to Silverman's book [Sil09]. For algebraic number theory we point to the book [Neu13] by Neukirch, and Stevenhagen's lecture notes [Ste17] and [Ste02]. Local fields are covered in both [Neu13] and [Ste02], and for p-adic analysis we refer to [Gou97].

Note that in [Sil09] all field are assumed perfect. We will also make this assumption to make things simpler, since all the fields we want to consider are actually perfect.

Part I
Torsion points and division fields

2 Torsion points

In this section we will look at torsion points of elliptic curves in general. We describe the group structure of torsion subgroups, and see how we can study ℓ-power torsion using Tate modules. Then we consider some methods to calculate torsion points explicitly, using division polynomials and the multiplication-by-p map in the formal group.

2.1 Torsion subgroups

Let E be an elliptic curve over a perfect field K. For any integer $n \geq 1$, we can consider the n-torsion subgroup

$$E[n] := \{P \in E(\overline{K}) \colon nP = O\}. \tag{4}$$

The group structure of $E[n]$ is well known. If the base field K has characteristic 0, then for any integer $n \geq 1$ we have an isomorphism of abelian groups

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

If K has characteristic $p > 0$, then this still holds for all integers $n \geq 1$ coprime to p, and furthermore we have (see [Sil09, III.6.4])

$$E[p^k] \cong \begin{cases} \mathbb{Z}/p^k\mathbb{Z} & \text{if } E \text{ is ordinary,} \\ 0 & \text{if } E \text{ is supersingular.} \end{cases}$$

Remark 2.0.1. Again this is analogous to the case of n-th roots of unity $\mu_n \subset \overline{K}^*$, where if n is coprime to $p = \mathrm{char}(K)$ then $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$ and $\mu_{p^k} \cong 0$. However, for elliptic curves there is an extra case (when E is ordinary).

Example 2.1. Let E/K be an elliptic curve given by a short Weierstrass equation $y^2 = x^3 + ax + b$. Note that for $P = (x, y) \in E$, we have $-P = (x, -y)$. Therefore P is a non-zero 2-torsion point if and only if $y = 0$. Let $\alpha, \beta, \gamma \in \overline{K}$ be the roots of $x^3 + ax + b$. Then the 2-torsion points of E are given by

$$E[2] = \{(\alpha, 0), (\beta, 0), (\gamma, 0), O\}.$$

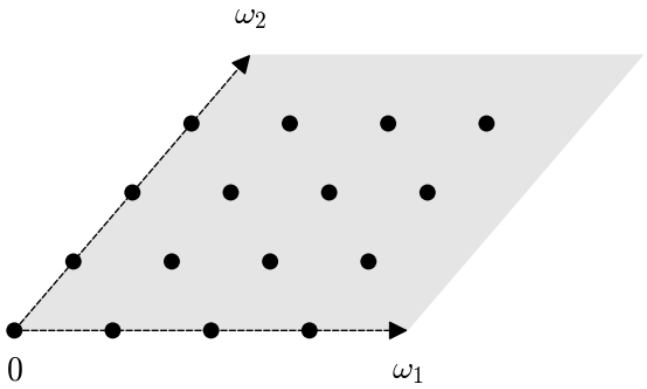


Figure 1: The 4-torsion points on the fundamental domain of $E \cong \mathbb{C}/\Lambda$ where $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$.

When $K = \mathbb{C}$, we have an alternative description for its n-torsion points. Recall that any elliptic curve E over $\mathbb{C}$ is isomorphic to a complex torus, i.e.

$$E \cong \mathbb{C}/\Lambda, \tag{5}$$

for some lattice $\Lambda \subset \mathbb{C}$. Under this isomorphism, $E[n]$ is the set of all points $z + \Lambda \in \mathbb{C}/\Lambda$ such that $nz \in \Lambda$, and thus

$$E[n] \cong \frac{1}{n}\Lambda/\Lambda. \tag{6}$$

If Λ is generated by $\omega_1, \omega_2 \in \mathbb{C}$, i.e. $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, then

$$E[n] \cong \left\{ \frac{a}{n}\omega_1 + \frac{b}{n}\omega_2 \in \mathbb{C}/\Lambda \colon 0 \leq a, b < n \text{ integers} \right\}. \tag{7}$$

For example, see figure 1. In particular we see that the group $E[n]$ in this case is indeed isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$.

2.2 ℓ-power torsion and Tate modules

In order to study torsion subgroups, it can be useful to break these up into their ℓ-power torsion parts, where ℓ ranges over all integer primes. This can be done by tensoring with the ℓ-adic integers $\mathbb{Z}_\ell$, which is made precise in the following lemma.

Lemma 2.2. *Let R be a ring.*

(a) *Let M be an R-module such that every element of M has finite additive order. Then we have a decomposition of R-modules*

$$M = \bigoplus_{\ell \text{ prime}} M_\ell, \tag{8}$$

where for each prime ℓ, M_ℓ is the $R \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$-module given by

$$M_\ell := M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell = M[\ell^\infty] := \{m \in M \colon \ell^n m = 0 \text{ for some } n \in \mathbb{Z}_{\geq 0}\}.$$

(b) *Let $N \subset M$ be R-modules. Then for any prime ℓ, we have a canonical isomorphism of $R \otimes \mathbb{Z}_\ell$-modules $(M/N) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong (M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)/(N \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)$.*

Proof. (a) We start by showing that $M \otimes \mathbb{Z}_\ell = M[\ell^\infty]$. Note that $\mathbb{Z}_\ell$ is a flat $\mathbb{Z}$-module, as it is torsion free. Therefore the exact sequence

$$0 \to M[\ell^\infty] \to M \to M/M[\ell^\infty] \to 0 \tag{9}$$

can be tensored with $\mathbb{Z}_\ell$ to obtain the exact sequence

$$0 \to M[\ell^\infty] \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to (M/M[\ell^\infty]) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to 0. \tag{10}$$

However, $M[\ell^\infty]$ already has a natural $\mathbb{Z}_\ell$-module structure, given as follows. Let $a \in \mathbb{Z}_\ell$ and $m \in M[\ell^\infty]$ have additive order ℓ^n. Then $am := a_0 m$ where a_0 is any integer such that $a \equiv a_0 \mod \ell^n$. This implies that $M[\ell^\infty] \otimes \mathbb{Z}_\ell = M[\ell^\infty]$. Also, as every element of $M/M[\ell^\infty]$ has finite additive order coprime to ℓ, it follows that $(M/M[\ell^\infty]) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell = 0$. This is because for every primitive tensor $\overline{m} \otimes_{\mathbb{Z}} a \in (M/M[\ell^\infty]) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$, we have

$$\overline{m} \otimes a = n\overline{m} \otimes n^{-1}a = 0 \otimes n^{-1}a = 0,$$

where n is the additive order of $\overline{m}$. We conclude that $M[\ell^\infty] = M \otimes \mathbb{Z}_\ell$.

Now let $M_\ell := M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell = M[\ell^\infty]$. In order to show that $M = \bigoplus_\ell M_\ell$, consider the R-linear maps

$$f \colon \bigoplus_\ell M[\ell^\infty] \to M, \qquad (m_\ell)_\ell \mapsto \sum_\ell m_\ell$$

$$g \colon M \to \bigoplus_\ell (M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell). \qquad m \mapsto (m \otimes 1)_\ell$$

It is not hard to check that these maps indeed are each other's inverse.

(b) Again we use that $\mathbb{Z}_\ell$ is a flat $\mathbb{Z}$-module. The exact sequence

$$0 \to N \to M \to M/N \to 0 \tag{11}$$

can be tensored with $\mathbb{Z}_\ell$ to obtain the exact sequence

$$0 \to N \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to (M/N) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to 0. \tag{12}$$

This gives us the desired result. □

We can apply this to the entire torsion subgroup E^{tors}. Let $R \subset \text{End}(E)$ be a commutative subring of the endomorphism ring of E (see section 5). Then E^{tors} is an R-module, and we have a decomposition

$$E^{\text{tors}} = \prod_{\ell \text{ prime}} E[\ell^\infty] \tag{13}$$

where $E[\ell^\infty]$ is the $R \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$-module given by all ℓ-power torsion points. Except for the special case where $\ell = \text{char}(K)$ and E is supersingular, $E[\ell^\infty]$ will have infinite size, and therefore cannot be finitely generated as $\mathbb{Z}$- or $\mathbb{Z}_\ell$-module (all finitely generated torsion groups are finite). Therefore it can be hard to work with.

However, it is possible to glue the ℓ-power torsion points together in another way. We can turn the subgroups $E[\ell^n]$ into an inverse system as follows: for integers $0 \le n \le m$, we have maps $E[\ell^m] \to E[\ell^n]$ given by $P \mapsto \ell^{m-n}P$. The Tate module $T_\ell(E)$ is defined as the inverse limit of this system, i.e.

$$T_\ell(E) := \varprojlim_n E[\ell^n] \tag{14}$$

In other words, $T_\ell(E)$ consists of sequences $(P_n)_{n\ge 0}$ with each $P_n \in E[\ell^n]$ and $P_{n-1} = \ell P_n$ for $n \ge 1$. In particular we have $P_0 = O$.

We define

$$V_\ell(E) := T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell, \tag{15}$$

which is the $\mathbb{Q}_\ell$-vector space generated by $T_\ell(E)$. It consists of sequences $(P_n)_{n\in\mathbb{Z}}$ with each $P_n \in E[\ell^\infty]$ such that $P_{n-1} = \ell P_n$. In particular there exists some $n \in \mathbb{Z}$ such that $P_n = P_{n-1} = P_{n-2} = \cdots = O$.

As inverse limit of subgroups of $E[\ell^\infty]$, the Tate module $T_\ell(E)$ inherits the component-wise $R \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$-module structure from $E[\ell^\infty]$. This extends naturally to an $R \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$-module structure on $V_\ell(E)$. In particular for $\ell \neq \text{char}(K)$, as each

$E[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^2$, we have that $T_\ell(E)$ is free of rank 2 as $\mathbb{Z}_\ell$-module and thus $V_\ell(E)$ has dimension 2 as $\mathbb{Q}_\ell$-vector space.

In other words, $T_\ell(E)$ is a $\mathbb{Z}_\ell$-lattice in $V_\ell(E)$. This allows us to give a description of $E[\ell^\infty]$ similar to the complex torus description $E \cong \mathbb{C}/\Lambda$ of elliptic curves over $\mathbb{C}$.

Proposition 2.3. *Let E an elliptic curve over a field K, and let $R \subset \mathrm{End}(E)$ be a commutative subring. Then for any prime ℓ, we have an isomorphism of $R \otimes \mathbb{Z}_\ell$-modules*

$$E[\ell^\infty] \cong V_\ell(E)/T_\ell(E). \tag{16}$$

Proof. Consider the map

$$f\colon V_\ell(E) \to E[\ell^\infty], \quad (P_n)_{n\in\mathbb{Z}} \mapsto P_0.$$

Both $V_\ell(E)$ and $E[\ell^\infty]$ are $R\otimes\mathbb{Z}_\ell$-modules, and it not hard to check that f is $R\otimes\mathbb{Z}_\ell$-linear. Note that $\ker(f) = \{(P_n)_{n\in\mathbb{Z}} \in V_\ell(E)\colon P_0 = O\} = T_\ell(E)$. Furthermore for $P \in E[\ell^\infty]$ consider any sequence $(P_n)_{n\in\mathbb{Z}} \in V_\ell(E)$ with $P_0 = P$. Then $f((P_n)_{n\in\mathbb{Z}}) = P$, and thus f is surjective. Therefore f induces the required isomorphism. □

Remark 2.3.1. All of the previous can be easily generalized with $R = \mathrm{End}(E)$, which is not necessarily commutative, by considering left R-modules. However, for our purposes this is not necessary.

Remark 2.3.2. In the cyclotomic case we have a similar description. Let $\mu_{\ell^\infty} \subset \overline{K}^*$ denote the ℓ-power roots of unity. Then for prime $\ell \neq \mathrm{char}(K)$ we have a group isomorphism $\mu_{\ell^\infty} \cong \mathbb{Q}_\ell/\mathbb{Z}_\ell$.

Example 2.4. If we again consider the case where $K = \mathbb{C}$ and thus $E \cong \mathbb{C}/\Lambda$, then torsion points of E can be identified with the Λ-equivalence classes of complex numbers $z \in \mathbb{C}$ such that $nz \in \Lambda$. Therefore

$$E^{\mathrm{tors}} \cong (\Lambda \otimes_{\mathbb{Z}} \mathbb{Q})/\Lambda.$$

Applying lemma 2.2 gives us

$$E[\ell^\infty] \cong (\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}_\ell)/(\Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_\ell).$$

In particular we have that the Tate module is isomorphic to

$$T_\ell(E) \cong \varprojlim_n \frac{1}{\ell^n}\Lambda/\Lambda \cong \varprojlim_n \Lambda/\ell^n\Lambda \cong \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_\ell.$$

and

$$V_\ell(E) \cong \Lambda \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$$

Remark 2.4.1. As we saw in the previous example, for ℓ-power torsion the Tate module ℓ-adically plays the role of the lattice Λ, even in positive characteristic when we do not have a complex torus description of E. This will play an important role later on when we look at unramified primes, as we will be able to copy arguments from the more familiar $K = \mathbb{C}$ case to finite fields.

2.3 Division polynomials

How can we calculate the n-torsion subgroup of any given elliptic curve? For this purpose, let E/K be given in short Weierstrass form

$$E\colon y^2 = x^3 + ax + b, \tag{17}$$

with $a, b \in K$.

We will follow exercise 3.7 from [Sil09] and define division polynomials $\psi_n \in \mathbb{Z}[a_1, \ldots, a_6, x, y]$ as follows:

$$\begin{aligned}
\psi_1 &:= 1,\\
\psi_2 &:= 2y,\\
\psi_3 &:= 3x^4 + 6ax^2 + 12bx - a^2\\
\psi_4 &:= 4y\left(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx + (-a^3 - 8b^2)\right),
\end{aligned}$$

$$\begin{aligned}
\psi_{2n+1} &= \psi_{n+2}\psi n^3 - \psi_{n-1}\psi_{n+1}^3 && (n \geq 2),\\
\psi_{2n} &= \frac{\psi_n}{\psi_2}(\psi_{n-1}^2\psi_{n+2} - \psi_{n-2}\psi_{m+1}^2) && (n \geq 3).
\end{aligned}$$

Furthermore, we define the polynomials

$$\begin{aligned}
\phi_n &= x\psi_n^2 - \psi_{n-1}\psi_{n+1},\\
\omega_n &= \frac{1}{2\psi_2}(\psi_{n-1}^2\psi_{n+2} - \psi_{n-2}\psi_{n+1}^2).
\end{aligned}$$

These division polynomials satisfy the following nice properties:

Proposition 2.5. *Let E/K be an elliptic curve. Then*

(a) *For $n \geq 1$, if n odd then $\psi_n \in \mathbb{Z}[a,b,x]$ and if n even then $\psi_n/\psi_2 \in \mathbb{Z}[a,b,x]$.*

(b) *For any nonzero point $P = (x,y) \in E$ and any integer $n \geq 1$, we have*

$$nP = \left(\frac{\phi_n(P)}{\psi_n(P)^2}, \frac{\omega_n(P)}{\psi_n(P)^3} \right). \tag{18}$$

(c) *For odd $n \geq 1$,*

$$\psi_n^2 = n^2 \prod_{P \in E[n] \setminus \{O\}} (x - x(P)), \tag{19}$$

and for even $n \geq 2$,

$$\frac{2\psi_n^2}{\psi_2} = n^2 \prod_{P \in E[n] \setminus \{O\}} (x - x(P)). \tag{20}$$

(d) *We have*

$$\operatorname{div}(\psi_n) = \sum_{P \in E[n]} P - nO \tag{21}$$

Proof. Although [Sil09] (among other sources) claims that this can be computed purely algebraically, I have not found a source in which this is worked out, and as it is highly computational I have not tried it myself. For elliptic curves with $K = \mathbb{C}$ a proof using elliptic functions is given in [Lan87, Ch. 2]. For any field K of characteristic not equal to 2, one can actually reduce to the case $K = \mathbb{C}$, see [Was08, Thm. 9.33]. □

Remark 2.5.1. There are also division polynomials for Weierstrass equations in long form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, see [Sil09, Excercise 3.7], with corrections [Sil15].

The previous proposition shows in particular that the non-zero n-torsion points are exactly the points $P \in E$ such that $\psi_n(P) = 0$. This allows us to calculate the n-torsion points.

Example 2.6. Let $E/\mathbb{Q}$ be given by $E\colon y^2 = x^3 + 1$. Then

$$\psi_3 = 3x^4 + 12x = 3x(x^3 + 4)$$

The roots of ψ_3 are $0, -\sqrt[3]{(4)}, -\zeta_3\sqrt[3]{(4)}, -\zeta_3^2\sqrt[3]{(4)}$. Then

$$E[3] = \{O, (0, \pm 1), (-\sqrt[3]{4}, \pm\sqrt{-3}), (-\zeta_3\sqrt[3]{(4)}, \pm\sqrt{-3}), (-\zeta_3^2\sqrt[3]{(4)}, \pm\sqrt{-3})\}$$

2.4 Torsion points in the formal group

To an elliptic curve we can associate a formal group law, for which we will recall some basic facts (see [Sil09, IV]). Let E be an elliptic curve given by a Weierstrass equation $y^2 = x^3 + ax + b$. After a change of coordinates

$$t = -\frac{x}{y}, \quad w = -\frac{1}{y} \tag{22}$$

we can use the Weierstrass equation to develop w as a power series $w(t) \in \mathbb{Z}[a, b][[t]]$. Reversing the change of variables we can derive Laurent series for x and y,

$$x(t) = \frac{t}{w(t)}, \quad y(t) = -\frac{1}{w(t)}. \tag{23}$$

We can then obtain a formal power $t_3 = F(t_1, t_2) \in \mathbb{Z}[a, b][[t]]$ series for the addition of $t_1, t_2 \in K$ according to the group law of E, by using the usual way to compute the group law in terms of x- and y-coordinates. This power series $F(t_1, t_2)$ is called the formal group law of E. This gives E the structure a formal group, which we will denote by $\hat{E}$.

Now suppose E is defined over a number field K and given by a Weierstrass equation $E\colon y^2 = x^3 + ax + b$ with $a, b \in \mathcal{O}_K$. Let $\mathfrak{p}$ be a prime of K with completion $K_\mathfrak{p}$. Then one can consider E as an elliptic curve over $K_\mathfrak{p}$ and one can show that the formal group law $F(t_1, t_2)$ of $\hat{E}$ converges $\mathfrak{p}$-adically for all $t_1, t_2 \in \mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}$, where $\mathcal{O}_{K_\mathfrak{p}}$ is the valuation ring of $K_\mathfrak{p}$. Furthermore the sum $t_3 = F(t_1, t_2) \in K_\mathfrak{p}$ actually belongs to $\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}$. This allows us compute the group law of E on $\{P \in E\colon t(P) \in \mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}\}$ using the power series $F(t_1, t_2)$.

Recursively, for $n \geq 0$, we can define the multiplication-by-n homomorphisms $[n]_{\hat{E}}$ on $\hat{E}$ as follows:

$$[0]_{\hat{E}}(t) = 0, \quad [n+1]_{\hat{E}}(t) = F([n]_{\hat{E}}(t), t). \tag{24}$$

One can show that in the formal group $\hat{E}(\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}})$ $[n]_{\hat{E}}\colon \hat{E} \to \hat{E}$ is a isomorphism of formal groups for all n not divisible by $\mathfrak{p}$ [Sil09, IV.2.3]. This implies that $\hat{E}(\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}})$ can only contain p-power torsion points. Such torsion points are given by the roots of the power series $[p^k]_{\hat{E}}(t)$.

We end this section by a small lemma regarding the shape of the power series $[p]_{\hat{E}}(t)$, which will be useful to us later on.

Lemma 2.7. *Let E be an elliptic curve over a field K, let p be a prime, and let $[p]_{\hat{E}}$ denote the multiplication-by-p homomorphism belonging to the formal group $\hat{E}$. Then there exists $f(t), g(t) \in \mathbb{Z}[a,b][[t]]$ with $f(0) = g(0) = 0$ and $f'(0) = 1$, such that*

$$[p]_{\hat{E}}(t) = pf(t) + g(t^p). \tag{25}$$

In particular we have

$$[p]_{\hat{E}}(t) = \sum_{i \geq 1} b_i t^i, \tag{26}$$

where $b_1 = p$ and $b_i \in p\mathbb{Z}[a,b]$ for i not divisible by p.

Proof. See [Sil09, IV.2.3, IV.4.4]. □

3 Division fields of elliptic curves

In this section, we will define division fields and study some of their general properties. We also recall some theory about primes in Galois extension. For primes of good reduction, we will use the reduction map to make a classification between unramified and ramified primes, which we will study more in-depth in later sections.

3.1 Division fields

We start with the definition of division fields.

Definition 3.1. Given an elliptic curve E over a field K, the n-th division field of E is the minimal field of definition of the n-torsion subgroup $E[n]$, usually denoted by $K(E[n])$.

As mentioned in the introduction, if E is given by an Weierstrass equation

$$y^2 = x^3 + ax + b, \tag{27}$$

then $K(E[n])$ is obtained by adjoining to K the x- and y- coordinates of all n-torsion points.

Example 3.2. Let E/K be given by $y^2 = x^3 + ax + b$, as in example 2.1. Then we saw that

$$E[2] = \{(\alpha, 0), (\beta, 0), (\gamma, 0), O\}, \tag{28}$$

where $\alpha, \beta, \gamma \in \overline{K}$ are the roots of $x^3 + ax + b$. In particular we see that $K(E[2])$ is the splitting field of $x^3 + ax + b$ over K.

Just like cyclotomic extensions, division fields are Galois. Note that we assumed all our fields to be perfect.

Proposition 3.3. *Let E be an elliptic curve over a field K and $n \geq 1$ an integer. Then the n-th division field $K(E[n])$ is Galois over K.*

Proof. Let $G_{\overline{K}/K} = \mathrm{Gal}(\overline{K}/K)$ denote the absolute Galois group of K (here we use that K is perfect and thus $\overline{K} = K^{\mathrm{sep}}$). For any $\sigma \in G_{\overline{K}/K}$ and any $P \in E[n]$, we have that $n\sigma(P) = \sigma(nP) = \sigma(O) = O$. Therefore we have an action of $G_{\overline{K}/K}$ on $E[n]$, or equivalently group homomorphism

$$\overline{\rho}_n \colon G_{\overline{K}/K} \to \mathrm{Aut}(E[n]). \tag{29}$$

We claim that $K(E[n])$ is the fixed field of $\ker(\overline{\rho}_n)$. Clearly, if $\sigma \in \ker(\overline{\rho}_n)$, then σ fixes all n-torsion points, and therefore their coordinates. As these coordinates generate the field extension $K(E[n])/K$ we see that σ fixes $K(E[n])$. Conversely, if $\sigma \in G_{\overline{K}/K}$ fixes $K(E[n])$, then by definition σ fixes $E[n]$.

As $\ker(\overline{\rho}_n)$ is normal, Galois theory tells us that $K(E[n])$ is Galois over K with Galois group isomorphic to $G_{\overline{K}/K}/\ker(\rho_n)$. □

From the proof of the previous proposition, we see that we have a injective group homomorphism

$$\mathrm{Gal}(K(E[n])/K) \to \mathrm{Aut}(E[n]). \tag{30}$$

In particular, we can identify $\mathrm{Gal}(K(E[n])/K)$ with the image of this homomorphism, which we will denote by G_n. For n coprime to $\mathrm{char}(K)$, recall that $E[n]$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$ as abelian group, and thus after choosing a $(\mathbb{Z}/n\mathbb{Z})$-basis for $E[n]$ we get an isomorphism $\mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Therefore we can identify G_n as subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, which is well defined up to conjugacy.

Similar, for any prime ℓ, we can consider the action of the absolute Galois group $G_{\overline{K}/K}$ on the Tate module $T_\ell(E)$

$$\rho_\ell \colon G_{\overline{K}/K} \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(E)). \tag{31}$$

As $\mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$, this gives us a 2-dimensional ℓ-adic representation, which are extensively studied by Serre in [Ser97].

Now that we have a Galois correspondence, let us look at a couple of subfields of $K(E[n])$: the field $K(x(E[n]))$ generated by the x-coordinates of all n-torsion points and the cyclotomic field $K(\zeta_n)$.

For $n \geq 3$, note that the field $K(x(E[n]))$ is given as the splitting field of the division polynomial ψ_n if n odd and ψ_n/ψ_2 if n even.

The fact that $K(\zeta_n)$ is a subfield of $K(E[n])$ follows from the Weil pairing [Sil09, III.8], which is a Galois-invariant pairing

$$e_n \colon E[n] \times E[n] \to \mu_n. \tag{32}$$

In particular if P, Q is a $(\mathbb{Z}/n\mathbb{Z})$-basis of $E[n]$, then $e_n(P,Q)$ is a primitive root of unity, for any $\sigma \in G_{\overline{K}}$, $\sigma(e_n(P,Q)) = e_n(P,Q)^{\det(\overline{\rho}_n(\sigma))}$. In particular, if σ fixes $K(E[n])$, then $\det(\overline{\rho}_n(\sigma)) = 1$ and thus σ fixes $K(\zeta_n)$.

Proposition 3.4. *Let E be an elliptic curve over a field K and $n \geq 3$ an integer coprime to* $\mathrm{char}(K)$*. After a choice of basis for $E[n]$, identify* $\mathrm{Gal}(K(E[n])/K)$ *with*

a subgroup $G_n \subset \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Then we have a Galois correspondence as in the following diagram:

$$\begin{array}{cc} K(E[n]) & \{I\} \\ | & | \\ K(x(E[n])) & G_n \cap \{\pm I\} \\ | & | \\ K(\zeta_n) & G_n \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \\ | & | \\ K & G_n \end{array} \tag{33}$$

Proof. We start with the subfield $K(x(E[n]))$, and we have to show that it is the fixed field of $G_n \cap \{\pm I\}$. Let $P \in E[n]$ and let $\sigma \in G_n \cap \{\pm I\}$. Then $\sigma(P) = \pm P$ and as $x(P) = x(-P)$ (see [Sil09, III.2.3]) we see that $\sigma(x(P)) = x(P)$. Thus σ fixes $x(E[n])$ and thus also $K(x(E[n]))$. Conversely, suppose $\sigma \in G_n$ fixes $x(E[n])$. Let P, Q be a $\mathbb{Z}/n\mathbb{Z}$-basis for $E[n]$. Then P has exact order $n \geq 3$, and thus $P \neq -P$, and $x(P) = x(-P)$. However, by the Weierstrass equation, there are at most 2 points with x-coordinate $x(P)$. As $x(\sigma(P)) = \sigma(x(P)) = x(P)$, this implies that $\sigma(P) = \pm P$. The same holds for Q and $P + Q$, i.e. $\sigma(Q) = \pm Q$ and $\sigma(P + Q) = \pm(P + Q)$. Furthermore, the signs in $\sigma(P) = \pm P$ and $\sigma(Q) = \pm Q$ are the same. Suppose otherwise, for instance $\sigma(P) = P$ and $\sigma(Q) = -Q$. Then $\sigma(P + Q) = \sigma(P) + \sigma(Q) = P - Q \neq \pm(P + Q)$. Therefore $\sigma = \pm I$.

For $K(\zeta_n)$, this follows from the previously stated fact about the Weil pairing that implied that $\sigma(\zeta_n) = \zeta_n^{\det(\sigma)}$. In particular, we have that $\sigma \in G_n$ fixes $K(\zeta_n)$ if and only if $\det(\sigma) = 1$. □

It can be useful to be able to split up a division field into a compositum of prime-power division fields. This is made exact by the following lemma.

Lemma 3.5. *Let E be an elliptic curve over a field K and let $n \geq 1$ be an integer with prime decomposition $n = \ell_1^{e_1} \ell_2^{e_2} \dots \ell_r^{e_r}$. Then $K(E(n)) = K(E[\ell_1^{e_1}], \dots, E[\ell_r^{e_r}])$.*

Proof. By lemma 2.2, any n-torsion point $P \in E[n]$ can be written as a sum $P = P_1 + \dots + P_r$ where each $P_i \in E[\ell_i^{e_i}]$ is a $\ell_i^{e_i}$-torsion point. As the x- and y-coordinates of P are K-rational functions of the x- and y-coordinates of the P_i, we see that $K(E[n]) \subset K(E[\ell_1^{e_1}], \dots, E[\ell_r^{e_r}])$. As $E[\ell_i^{e_i}] \subset E[n]$, it immediately follows that also $K(E[\ell_1^{e_1}], \dots, E[\ell_r^{e_r}]) \subset K(E[n])$. □

Remark 3.5.1. We have to be careful not to overgeneralize the previous lemma to Galois groups. The usual Chinese remainder theorem decomposition $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/\ell_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/\ell_r^{e_r}\mathbb{Z}$ extends to a decomposition $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/\ell_1^{e_1}\mathbb{Z}) \times \cdots \times \mathrm{GL}_2(\mathbb{Z}/\ell_r^{e_r}\mathbb{Z})$. Then it follows that we can identify G_n as a subgroup of $G_{\ell_1^{e_1}} \times \cdots \times G_{\ell_r^{e_r}}$, however equality does not necessarily hold.

We can use the techniques we will develop in chapter 6 to find a counterexample over a finite field. Let $E/\mathbb{F}_{11}$ be given by $y^2 = x^3 + 6x + 11$. Then after choosing suitable bases, the Frobenius $\phi \in \mathrm{Gal}(\overline{\mathbb{F}_{11}}/\mathbb{F}_{11})$ acts as

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}), \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}), \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z}) \tag{34}$$

on $E[2]$, $E[3]$ and $E[6]$ respectively. In particular this means that ϕ has order 2 in G_2, G_3 and G_6. As the Frobenius generates all these Galois groups we see that they all have order 2 and thus $G_6 \ncong G_2 \times G_3$.

3.2 Primes in Galois extensions

We recall some basic facts we need about primes in Galois extensions.

Let L/K be a Galois extension of number fields with Galois group $G = \mathrm{Gal}(L/K)$, with respective ring of integers $\mathcal{O}_L$ and $\mathcal{O}_K$. Let $\mathfrak{p} \subset \mathcal{O}_k$ be a prime of K above $p \in \mathbb{Z}$. Then for any prime $\mathfrak{P} \subset \mathcal{O}_L$ of L above $\mathfrak{p}$, we can consider the completions $\mathbb{Q}_p \subset K_\mathfrak{p} \subset L_\mathfrak{P}$. Then $L_\mathfrak{P}/K_\mathfrak{p}$ is also a Galois extension whose Galois group is the decomposition group

$$G_\mathfrak{P} = \{\sigma \in G \colon \sigma\mathfrak{P} = \mathfrak{P}\} \tag{35}$$

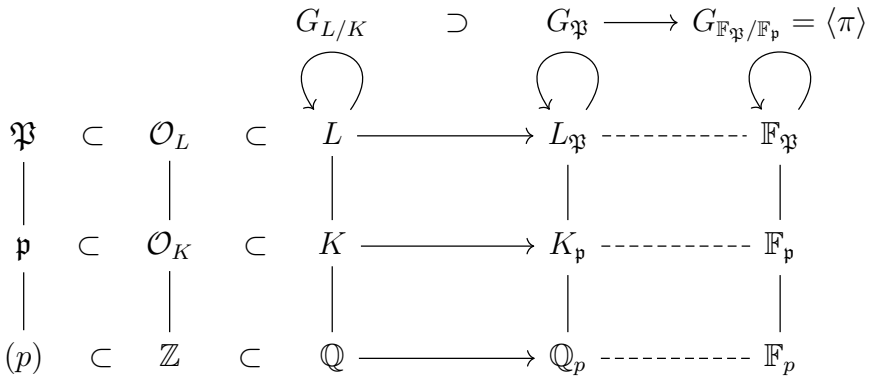
consisting of those elements of G that can be continuously extended with respect to the $\mathfrak{P}$-adic topology. Furthermore consider the residue fields $\mathbb{F}_\mathfrak{P} = \mathcal{O}_L/\mathfrak{P}$ and $\mathbb{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$. Then reduction modulo $\mathfrak{P}$ defines a surjective group homomorphism

$$\mathrm{red}_\mathfrak{P} \colon G_\mathfrak{P} \to G_{\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}}, \quad \sigma \mapsto (\overline{x} \mapsto \overline{\sigma(x)}).$$

Lastly, as the extension $\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}$ is an extension of finite fields, its Galois group $G_{\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}}$ is generated by the Frobenius

$$\pi \colon F_\mathfrak{P} \to F_\mathfrak{P}, \quad x \mapsto x^{N(\mathfrak{p})}.$$

The entire situation can be summarized by the following diagram:



(36)

We are mostly interested in how a given prime $\mathfrak{p}$ of K splits in L. Such a prime has a decomposition

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r},$$

where each $\mathfrak{P}_i$ is a prime of L. We call a prime $\mathfrak{P}_i$ unramified in L/K if $e_i = 1$ and ramified if $e_i > 1$. Similarly we call $\mathfrak{p}$ unramified in L/K if $e_1 = \dots = e_r = 1$, and ramified if $e_i > 1$ for some i. The next proposition shows that ramification behaves nicely in Galois extensions.

Proposition 3.6. *Let L/K be a Galois extension of number fields. Let $\mathfrak{P}$ be a prime of K and $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$ be its decomposition in L.*

(a) *We have $e_1 = \dots = e_r$.*

(b) *$\mathfrak{p}$ is unramified (i.e. $e_1 = \dots = e_r = 1$) if and only if the natural map $G_{\mathfrak{P}_i} \xrightarrow{\mathrm{red}_{\mathfrak{P}_i}} G_{\mathbb{F}_{\mathfrak{P}_i}/\mathbb{F}_{\mathfrak{p}}}$ is injective (i.e. an isomorphism) for some (all) i.*

Proof. See [Ste17, Ch. 8] □

In the case where $\mathfrak{p}$ is unramified, for any prime $\mathfrak{P}$ of L above $\mathfrak{p}$ we can pull back the Frobenius π under the isomorphism

$$\mathrm{red}_{\mathfrak{P}} \colon G_{\mathfrak{P}} \to G_{\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{P}}} \tag{37}$$

to a unique element $F_{\mathfrak{P}} := F_{L/K,\mathfrak{P}} \in G_{\mathfrak{P}} \subset G$ (which we also call the Frobenius) characterized by $F_{\mathfrak{P}}(x) \equiv x^{N(\mathfrak{p})} \mod \mathfrak{P}$ for all $x \in \mathcal{O}_L$. In particular, $F_{\mathfrak{P}}$ generates $G_{\mathfrak{P}}$. The Frobenius $F_{\mathfrak{P}}$ only depends on the choice of prime $\mathfrak{P}$ up to conjugacy. Therefore we define

$$F_{\mathfrak{p}} = F_{L/K,\mathfrak{p}} = \{F_{\mathfrak{P}} \in G \colon \mathfrak{P} \text{ prime of } L \text{ above } \mathfrak{p}\}. \tag{38}$$

as the conjugacy class of the Frobenius of any prime $\mathfrak{P}$ above $\mathfrak{p}$.

Example 3.7. Let $n \geq 1$ be an integer, and consider the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. This is Galois with Galois group G isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$. For every $a \in (\mathbb{Z}/n\mathbb{Z})^*$, let $\sigma_a \in G$ be given by $\zeta_n \mapsto \zeta_n^a$. Note that $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$.

For any prime p that does not divide n, the polynomial $X^n - 1$ is separable over $\mathbb{F}_p$, thus in particular the cyclotomic polynomial $\Phi_n \in \mathbb{Z}[X]$ (which is the minimal polynomial of ζ_n) is separable over $\mathbb{F}_p$ and thus splits into distinct irreducible factors $\overline{\Phi}_n = \overline{f}_1 \dots \overline{f}_r \in \mathbb{F}_p[X]$. Using Kummer-Dedekind [Ste17, Thm. 3.1], we get corresponding primes $\mathfrak{P}_i = (p, f_i(\zeta_n))$ of $\mathbb{Q}(\zeta_n)$ and we have that $p\mathbb{Z}[\zeta_n] = \mathfrak{P}_1 \dots \mathfrak{P}_r$. In particular we see that these primes are unramified. Then for each prime $\mathfrak{P}_i$, the Frobenius $F_{\mathfrak{P}_i}$ is the unique element decomposition group $G_{\mathfrak{P}_i} \subset G$ such that for every $x \in \mathbb{Z}[\zeta_n]$.

$$F_{\mathfrak{P}_i}(x) \equiv x^p \mod \mathfrak{P}_i$$

In particular this implies that $F_{\mathfrak{P}_i}(\zeta_n) \equiv \zeta_n^p \mod \mathfrak{P}_i$, and therefore $F_{\mathfrak{P}_i} = \sigma_p$. Then also $F_p = \sigma_p$ (note that G is abelian so every conjugacy class consists of a single element).

For prime p that divide n, write $n = p^k m$ with m not divisible by p. Then we can write $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{p^k}, \zeta_m)$. We split up the extension $\mathbb{Q}(\zeta_n)$ into 2 parts: $\mathbb{Q}(\zeta_{p^k})/\mathbb{Q}$ and $\mathbb{Q}(\zeta_m, \zeta_{p^k})/\mathbb{Q}(\zeta_{p^k})$. By a similar argument as above, the latter extension is unramified at p. As the ramification is multiplicative for towers of field extensions, the ramification index of p in $\mathbb{Q}(\zeta_n)$ is then equal to the ramification index of p in $\mathbb{Q}(\zeta_{p^k})$. Using Kummer-Dedekind, we find that $\overline{\Psi}_{p^k} = (X-1)^{\varphi(p^k)} \in \mathbb{F}_p[X]$, where $\varphi(p^k) = p^k - p^{k-1}$ is the Euler phi function. Therefore $p\mathbb{Z}[\zeta_{p^k}] = \mathfrak{P}^{\varphi(p^k)}$, with $\mathfrak{P} = (p, \zeta_{p^k} - 1)$. In particular, the ramification index of p in $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is equal to $e_{\mathfrak{P}/p} = \varphi(p^k)$.

Our goal will be to do something similar as we in the above example, but then for primes of good reduction in division fields of elliptic curves.

3.3 Unramified and ramified primes of good reduction

Going back to division fields of elliptic curves, let E be an elliptic curve over a number field K. A prime $\mathfrak{p}$ of K is said to have good reduction if there exists a Weierstrass equation for E with coefficients in $\mathcal{O}_K$ such that when one reduces this Weierstrass equation modulo $\mathfrak{p}$, one obtains an elliptic curve $E_\mathfrak{p}$ over $\mathbb{F}_\mathfrak{p}$ (i.e. the reduced curve has to be non-singular). Such a Weierstrass model is called a minimal model (as the $\mathfrak{p}$-adic valuation of its discriminant is minimal), and for primes $\mathfrak{p}$ not above 2 or 3 it can be chosen to be in short Weierstrass form.

If $\mathfrak{p}$ is a prime of good reduction then reduction modulo $\mathfrak{p}$ defines a map $\mathrm{red}_\mathfrak{p}\colon E(K) \to E_\mathfrak{p}(\mathbb{F}_\mathfrak{p})$, by rescaling a point $P = (x : y : z) \in E(K)$ such that $x, y, z \in \mathcal{O}_K$ and $\min(v_\mathfrak{p}(x), v_\mathfrak{p}(y), v_\mathfrak{p}(z)) = 0$, and then reducing it to $\overline{P} = (\overline{x} : \overline{y} : \overline{z}) \in E(\mathbb{F}_\mathfrak{p})$. However, for points $P \in E$ not defined over K, to define a their reduction $\overline{P} \in E_\mathfrak{p}$ we first need to choose a prime above $\mathfrak{p}$ in their field of definition.

Therefore, if we want to define reduction on n-torsion points, we need to first choose a prime $\mathfrak{P}$ of $K(E[n])$ above $\mathfrak{p}$. We then have a well defined reduction map $\mathrm{red}_\mathfrak{P}\colon E(K(E[n])) \to E(\mathbb{F}_\mathfrak{P})$. Note that this map preserves the group law of the respective curves, i.e. $\overline{P+Q} = \overline{P} + \overline{Q}$. Therefore reduction sends n-torsion points to n-torsion points, and we thus get a well defined group homomorphism

$$\mathrm{red}_\mathfrak{P}\colon E[n] \to E_\mathfrak{p}[n]. \tag{39}$$

Proposition 3.8. *Let E be an elliptic curve over a number field K, and let $\mathfrak{p}$ be a prime of K of good reduction with reduced curve $E_\mathfrak{p}$. Furthermore, let $n \geq 1$ be an integer and $\mathfrak{P}$ be a prime of $K(E[n])$ above $\mathfrak{p}$. Then the map $\mathrm{red}_\mathfrak{P}\colon E[n] \to E_\mathfrak{p}[n]$ is surjective, and its kernel is isomorphic to $\hat{E}[n] = \hat{E}(\mathfrak{P}\mathcal{O}_\mathfrak{P})[n]$, where $\mathcal{O}_\mathfrak{P}$ is the valuation ring of $K(E[n])_\mathfrak{P}$.*

Proof. Choose a minimal Weierstrass equation of E with respect to $\mathfrak{p}$.

We first show that $\mathrm{red}_\mathfrak{P}\colon E[n] \to E_\mathfrak{p}[n]$ is surjective. If n is odd, the x-coordinates of the n-torsion points of $E_\mathfrak{p}$ are given by the roots of $\psi_{\mathfrak{p},n}$. As $\psi_{\mathfrak{p},n} = \overline{\psi_n}$, and ψ_n splits completely in $\mathcal{O}_{(K(E[n]))}[X]$, for every torsion point $Q \in E_\mathfrak{p}[n]$ there exists some torsion point $P \in E[n]$ such that $\overline{x(P)} = x(Q)$. By substituting $x = x(P)$ in the Weierstrass equation we can then show that we can choose P such that $\overline{y(P)} = y(Q)$. Then $\overline{P} = Q$ and thus any n-torsion point is in the image of reduction.

For n even, we can do the same for ψ_n/ψ_2 to show that all n-torsion points that are not 2-torsion are in the image of the reduction. For the 2-torsion points, one can solve $\psi_2 = 0$ for y and substitute this into the Weierstrass equation and then repeat the same argument.

Now we prove that the kernel is isomorphic to $\hat{E}[n]$. Consider E as a curve over $K(E[n])_\mathfrak{P}$. Then by [Sil09, VII.2.2], the map $t \mapsto (x(t), y(t))$ gives an isomorphism of groups between $\hat{E}(\mathfrak{P}\mathcal{O}_\mathfrak{P})$ and the kernel of $\mathrm{red}_\mathfrak{P}\colon E(K(E[n])_\mathfrak{P}) \to E_\mathfrak{p}(\mathbb{F}_\mathfrak{P})$. Then $\hat{E}[n]$ is isomorphic to the kernel of $\mathrm{red}_\mathfrak{P}\colon E(K(E[n])_\mathfrak{P})[n] \to E_\mathfrak{p}(\mathbb{F}_\mathfrak{P})[n]$. As all n-torsion points of E are defined over $K(E[n])$, we have that $E(K(E[n])_\mathfrak{P})[n] = E(K(E[n]))[n] = E[n]$.

□

The previous proposition can be summarized in the following exact sequence:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \hat{E}[n] & \longrightarrow & E[n] & \xrightarrow{\mathrm{red}_{\mathfrak{P}}} & E_{\mathfrak{p}}[n] & \longrightarrow & 0 \\ & & \wr & & \wr & & \wr & & \\ & & ? & & (\mathbb{Z}/n\mathbb{Z})^2 & & ? & & \end{array} \tag{40}$$

The behavior of the prime $\mathfrak{p}$ in $K(E[n])/K$ depends on how $E[n]$ distributes over the groups $\hat{E}[n]$ and $E_{\mathfrak{p}}[n]$. But we already know how the n-torsion subgroup looks for an elliptic curve in characteristic p. Combined with the fact that $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$, we get the possibilities for $\hat{E}[n]$ and $E_{\mathfrak{p}}[n]$ as described in table 1.

	$\hat{E}[n]$	$E_{\mathfrak{p}}[n]$
n coprime to p	0	$(\mathbb{Z}/n\mathbb{Z})^2$
$n = p^k$ and $E_{\mathfrak{p}}$ ordinary	$\mathbb{Z}/p^k\mathbb{Z}$	$\mathbb{Z}/p^k\mathbb{Z}$
$n = p^k$ and $E_{\mathfrak{p}}$ supersingular	$(\mathbb{Z}/p^k\mathbb{Z})^2$	0

Table 1: Possibilities for the group structure of $\hat{E}[n]$ and $E_{\mathfrak{p}}[n]$.

For a given n, we can then divide the primes of good reduction into two groups: primes that do not divide n, and primes that do divide n.

For primes $\mathfrak{p}$ that do not divide n, we have a bijection $\mathrm{red}_{\mathfrak{P}} \colon E[n] \to E_{\mathfrak{p}}[n]$. Using this bijection, we can show that $\mathfrak{p}$ is unramified in $K(E[n])/K$. This will be studied in part II.

For primes $\mathfrak{p}$ that do divide n, ramification can occur. We will study the ramification in part IV using Newton polygons. When $E_{\mathfrak{p}}$ is supersingular, all p-power torsion points can be found in the formal group $\hat{E}$ and we use this to to calculate a lower bound for the ramification index.

Part II
Unramified primes: elliptic curves

4 Fractional ideals

The reader is most likely familiar with the concept of fractional ideals for orders in number fields. In this section we will recall some basic properties and expand upon these. Furthermore, as we will be dealing with orders in product of number fields or ℓ-adic fields, we will generalize the notion of fractional ideals.

Our main interest is to understand when proper fractional ideals are invertible, as this will play a role when we will try to find a representative of the Frobenius in section 6 and generalize this to abelian varieties in section 8. This leads us to consider two special type of orders, namely Gorenstein and Bass orders.

Note that we assume all rings to be commutative.

4.1 Fractional ideals in Z-orders

Let Z be a principal ideal domain (think $Z = \mathbb{Z}$ or $Z = \mathbb{Z}_\ell$) and let Q be its field of fractions. We will call the irreducible elements of Z primes, usually denoted by ℓ. We will assume algebras to be commutative. A finite-dimensional Q-algebra L is separable if it is isomorphic to a product $L \cong L_1 \times \cdots \times L_r$, where each L_i is a separable field extension of Q.

We call a Z-algebra R a Z-order (or just order if Z is clear from context) if it is free of finite rank as Z-module, and its total ring of fractions $L = R \otimes_Z Q$ is a separable finite-dimensional Q-algebra. Equivalently, if we start with a separable Q-algebra L of finite dimension n, then a Z-order in L is a Z-subalgebra $R \subset L$ that has finite rank n as Z-module.

Example 4.1. The Gaussian integers $\mathbb{Z}[i]$ form a $\mathbb{Z}$-order in the 2-dimensional $\mathbb{Q}$-algebra $\mathbb{Q}(i)$. If we tensor with $\mathbb{Z}_5$, we get the $\mathbb{Z}_5$-order $\mathbb{Z}[i] \otimes \mathbb{Z}_5$ in the 2-dimensional $\mathbb{Q}_5$-algebra $\mathbb{Q}(i) \otimes \mathbb{Q}_5$. Note that, by Hensel's lemma, the polynomial $X^2 + 1 \in \mathbb{Z}[X]$ splits in $\mathbb{Q}_5$ and denote its solutions by $\pm i$. Then

$$\begin{aligned}
\mathbb{Q}(i) \otimes \mathbb{Q}_5 &\cong (\mathbb{Q}[X]/(X^2+1)) \otimes \mathbb{Q}_5 \\
&\cong \mathbb{Q}_5[X]/(X^2+1) \\
&\cong \mathbb{Q}_5[X]/(X-i) \times \mathbb{Q}_5[X]/(X+i) \\
&\cong \mathbb{Q}_5 \times \mathbb{Q}_5,
\end{aligned}$$

and under this isomorphism of $\mathbb{Q}(i) \otimes \mathbb{Q}_5 \cong \mathbb{Q}_5 \times \mathbb{Q}_5$, the order $\mathbb{Z}[i] \otimes \mathbb{Z}_5$ corresponds to $\mathbb{Z}_5 \times \mathbb{Z}_5$.

The previous example motivates our generalization to orders in separable finite-dimensional Q-algebras. In general, given any Z-order R and a prime ℓ of Z, we can freely tensor it (over Z) with the ℓ-adic completion $Z_\ell = \varprojlim_n Z/\ell^n Z$ and always get a Z_ℓ-order $R_\ell = R \otimes_Z Z_\ell$ of the same rank. The fraction field of Z_ℓ is given by $Q_\ell = Q \otimes Z_\ell$, and the total ring of fractions of R_ℓ is given by $L_\ell = L \otimes_Z Z_\ell = L \otimes_Q Q_\ell$. We will fix this notation throughout the rest of the section. Furthermore, for each prime ℓ, we will identify L with its image under the canonical embedding into L_ℓ.

Definition 4.2. A fractional R-ideal $\mathfrak{a}$ is an R-submodule of L that is free Z-module of the same rank as R. Equivalently, $\mathfrak{a}$ is a finitely generated R-submodule of L such that $\mathfrak{a} \otimes_Z Q = L$, or equivalently $\mathfrak{a}$ is a R-submodule of L such that there exists some $x \in L^*$ such that $x\mathfrak{a} \subset R$ (in particular we can choose $x \in Z$ not a zero-divisor).

Given two fractional R-ideals $\mathfrak{a}$ and $\mathfrak{b}$, we have the usual ideal operations $\mathfrak{a} + \mathfrak{b}$ and $\mathfrak{ab}$, which are again fractional ideals. Furthermore, we have the fractional ideal quotient

$$\mathfrak{a} : \mathfrak{b} = \{x \in L \colon x\mathfrak{a} \subset \mathfrak{b}\},$$

and one can check that this is again a fractional R-ideal. Two special quotients are given by

$$\mathfrak{a}^{-1} := R : \mathfrak{a} = \{x \in L \colon x\mathfrak{a} \subset R\},$$

called the inverse of $\mathfrak{a}$, and

$$r(\mathfrak{a}) := \mathfrak{a} : \mathfrak{a} = \{x \in L \colon x\mathfrak{a} \subset \mathfrak{a}\}.$$

called the multiplier ring of $\mathfrak{a}$, which is an order in L that contains R.

Lastly, for any prime ℓ, we can consider the ℓ-adic completion of $\mathfrak{a}$. This is obtained by tensoring $\mathfrak{a}$ with Z_ℓ, denoted by

$$\mathfrak{a}_\ell := \mathfrak{a} \otimes_Z Z_\ell,$$

and is a fractional R_ℓ-ideal.

Next follow a series of lemma regarding ℓ-adic completions. The first one says that every fractional R_ℓ-ideal can be generated by elements of L.

Lemma 4.3. *Any fractional R_ℓ-ideal $\mathfrak{a} \subset L_\ell$ can be generated as Z_ℓ-module by elements of L, i.e.*

$$\mathfrak{a} = Z_\ell x_1 \oplus \cdots \oplus Z_\ell x_n, \tag{41}$$

where $x_1, \ldots, x_n \in L$.

Proof. Consider $\mathfrak{a}_{(\ell)} = L \cap \mathfrak{a}$. We claim that this a fractional $R_{(\ell)}$-ideal, where $R_{(\ell)} = R \otimes_Z Z_{(\ell)}$ is the localization of R at $Z \setminus (\ell)$. As $L = R_{(\ell)} \otimes_Z Q$ and $R_\ell = R_{(\ell)} \otimes_Z Z_\ell$, we see that both L and R_ℓ are $R_{(\ell)}$-modules and thus so is $\mathfrak{a}_{(\ell)}$.

In order to show that $\mathfrak{a}_{(\ell)}$ is free of the correct rank as $Z_{(\ell)}$-module, notice that as $\mathfrak{a}$ is a fractional R_ℓ-module, there exists some integer $n, m \geq 1$ such that $\ell^n \mathfrak{a} \subset R_\ell$ and $\ell^m R_\ell \subset \mathfrak{a}$. This implies that $\ell^n \mathfrak{a}_{(\ell)} \subset R_{(\ell)}$ and $\ell^m R_{(\ell)} \subset \mathfrak{a}_{(\ell)}$. Therefore $\mathfrak{a}_{(\ell)}$ is indeed free of the same rank as $R_{(\ell)}$ as $Z_{(\ell)}$-module and thus $\mathfrak{a}_{(\ell)}$ is a fractional $R_{(\ell)}$-ideal.

Let $\mathfrak{a}_\ell = \mathfrak{a}_{(\ell)} \otimes_Z Z_\ell$. As $\mathfrak{a}_{(\ell)}$ is generated by elements $x_1, \ldots, x_n \in L$ as $Z_{(\ell)}$-module, $\mathfrak{a}_\ell$ is generated by these same elements as Z_ℓ-module. To complete the proof, we will show that $\mathfrak{a} = \mathfrak{a}_\ell$. The inclusion $\mathfrak{a}_\ell \subset \mathfrak{a}$ follows from $\mathfrak{a}_{(\ell)} \subset \mathfrak{a}$. As ℓ lies in the Jacobson radical of Z_ℓ, Nakayama's lemma [AM69, Prop. 2.8] implies that $\mathfrak{a}_\ell = \mathfrak{a}$ if and only if $\overline{x}_1, \ldots, \overline{x}_n$ form a $Z/\ell Z$-basis of $\mathfrak{a}/\ell\mathfrak{a}$. Let $a_1, \ldots, a_n \in Z$ such that

$$a_1 x_1 + \cdots + a_n x_n \in \ell\mathfrak{a}.$$

Note that this actually lies in L, so we have

$$a_1 x_1 + \cdots + a_n x_n \in \ell\mathfrak{a}_{(\ell)}.$$

But the x_i form a $Z_{(\ell)}$-basis of $\mathfrak{a}_{(\ell)}$ and thus this can only happen if each $a_i \in \ell Z_\ell$. This completes the proof. □

Another nice property of ℓ-adic completion is that it commutes with the other fractional ideal operations.

Lemma 4.4. *Let $\mathfrak{a}, \mathfrak{b}$ be fractional R-ideals, and let ℓ be a prime of Z. Then*

(a) $(\mathfrak{a} + \mathfrak{b})_\ell = \mathfrak{a}_\ell + \mathfrak{b}_\ell$.

(b) $(\mathfrak{a}\mathfrak{b})_\ell = \mathfrak{a}_\ell \mathfrak{b}_\ell$.

(c) $(\mathfrak{a} : \mathfrak{b})_\ell = \mathfrak{a}_\ell : \mathfrak{b}_\ell$.

Proof. Parts (a) and (b) follow from applying the definitions to primitive tensors.

(c) To prove that $(\mathfrak{a} : \mathfrak{b})_\ell \subset \mathfrak{a}_\ell : \mathfrak{b}_\ell$, it is sufficient to prove that for every primitive tensor $x \otimes y \in (\mathfrak{a} : \mathfrak{b})_\ell$ and every primitive tensor $b \otimes z \in \mathfrak{b}_\ell$ we have that $(x \otimes y)(b \otimes z) \subset \mathfrak{a}_\ell$. However, $(x \otimes y)(b \otimes z) = xb \otimes yz$, and as $x \in \mathfrak{a} : \mathfrak{b}$, we have $xb \in \mathfrak{a}$. Thus indeed $xb \otimes yz \in \mathfrak{a}_\ell$.

Next we show that $(\mathfrak{a} : \mathfrak{b})_\ell \supset \mathfrak{a}_\ell : \mathfrak{b}_\ell$. By lemma 4.3, $\mathfrak{a}_\ell : \mathfrak{b}_\ell$ can be generated by elements $x_1, \ldots, x_n \in L$ as Z_ℓ-module. Therefore it is sufficient to show that

each $x_i \in (\mathfrak{a} : \mathfrak{b})_\ell$. As $x_i\mathfrak{b}_\ell \subset \mathfrak{a}_\ell$, clearly $x_i\mathfrak{b} \subset L \cap \mathfrak{a}_\ell$. This implies that there exists some $a \in Z$ coprime to ℓ such that $ax_i\mathfrak{b} \subset \mathfrak{a}$. Thus $ax_i \in \mathfrak{a} : \mathfrak{b}$ and therefore $x_i = ax_i \otimes a^{-1} \in (\mathfrak{a} : \mathfrak{b})_\ell$. □

The next lemma shows that we can actually retrieve a fractional R ideal from its ℓ-adic localizations. Combined with the previous lemma this shows that we can compute fractional ideal operations ℓ-adically.

Lemma 4.5. *Let $\mathfrak{a}$ be a fractional R-ideal and for each prime ℓ, identify L with its image under the canonical embedding $L \to L_\ell$. Then*

$$\mathfrak{a} = \bigcap_\ell L \cap \mathfrak{a}_\ell. \tag{42}$$

Proof. Let $\mathfrak{a} = Zx_1 \oplus \cdots \oplus Zx_n$. Then by a similar argument as in the proof of lemma 4.3, we have $L \cap \mathfrak{a}_\ell = Z_{(\ell)}x_1 \oplus \ldots Z_{(\ell)}x_n$. As $\bigcap_\ell Z_{(\ell)} = Z$, we see that

$$\bigcap_\ell L \cap \mathfrak{a}_\ell = \bigcap_\ell (Z_{(\ell)}x_1 \oplus \cdots \oplus Z_{(\ell)}x_n) = Zx_1 \oplus \cdots \oplus Zx_n = \mathfrak{a}. \tag{43}$$

□

The main properties of fractional ideals that are we interested in are the following:

Definition 4.6. We call a fractional R-ideal $\mathfrak{a}$ <u>invertible</u> if $\mathfrak{a}\mathfrak{a}^{-1} = R$, <u>proper</u> if $r(\mathfrak{a}) = R$, and <u>reflexive</u> if $(\mathfrak{a}^{-1})^{-1} = \mathfrak{a}$.

Later on we will express torsion subgroups of elliptic curves in terms of fractional ideals of the endomorphism ring. Our main tool will be the following proposition, which relates properness, invertibility and ℓ-adic localizations.

Proposition 4.7. *Let $\mathfrak{a}$ be a fractional R-ideal. The following are equivalent:*

(a) *$\mathfrak{a}$ is proper and reflexive.*

(b) *$\mathfrak{a}$ is invertible.*

(c) *$\mathfrak{a}$ is locally free of rank 1, i.e. for any prime ideal $\mathfrak{p} \subset R$, the localization $\mathfrak{a}_\mathfrak{p}$ is a free $R_\mathfrak{p}$-module of rank 1.*

(d) *$\mathfrak{a}$ is ℓ-adically principal, i.e. for any prime $\ell \in Z$, the fractional R_ℓ-ideal $\mathfrak{a}_\ell = \mathfrak{a} \otimes_Z Z_\ell$ is principal.*

For its proof we need the following lemma:

Lemma 4.8. *Let $\mathfrak{a}$ be a fractional R-ideal. If $\mathfrak{a} \subsetneq R$, then $\mathfrak{a}^{-1} \supsetneq R$.*

Proof of lemma. See [Con, Lem. 3.2(2)]. □

Proof of proposition. (a) $\Rightarrow$ (b) Suppose $\mathfrak{a}$ is reflexive but not invertible. Then we have $\mathfrak{a}^{-1}\mathfrak{a} \subsetneq R$, and therefore $(\mathfrak{a}^{-1}\mathfrak{a})^{-1} \supsetneq R$ by the previous lemma. Let $x \in (\mathfrak{a}^{-1}\mathfrak{a})^{-1} \setminus R$. Then $x\mathfrak{a}^{-1}\mathfrak{a} \subset R$ and thus $x\mathfrak{a} \subset (\mathfrak{a}^{-1})^{-1} = \mathfrak{a}$. Thus $\mathfrak{a}$ is not proper.

(b) $\Rightarrow$ (c) We follow [Ste17, Thm. 2.7]. As $\mathfrak{a}^{-1}\mathfrak{a} = R$, there exist $x_i \in \mathfrak{a}$ and $y_i \in \mathfrak{a}^{-1}$ such that $\sum_{i=1}^{r} x_i y_i = 1$, with each $x_i y_i \in R$. Let $\mathfrak{p}$ be a prime ideal of R. As $1 \notin \mathfrak{p}$, we have that $x_i y_i \notin \mathfrak{p}$ for some i. Then $x_i y_i \in R_{\mathfrak{p}}^*$ and for any $x \in \mathfrak{a}$ we have

$$x = x_i \left(\frac{x y_i}{x_i y_i} \right) \in x_i R_{\mathfrak{p}}. \tag{44}$$

Therefore $\mathfrak{a}_{\mathfrak{p}} = x_i R_{\mathfrak{p}}$.

(c) $\Rightarrow$ (d) Let ℓ be a prime of Z. As ℓ lies in the Jacobson radical of R_ℓ, by Nakayama's lemma [AM69, Prop. 2.8] it is sufficient to show that $\mathfrak{a}_\ell/\ell\mathfrak{a}_\ell = \mathfrak{a}/\ell\mathfrak{a}$ is a free of rank 1 as $R/\ell R$-module. Note that R is Noetherian, and thus by [AM69, Thm. 7.13] every ideal has a primary decomposition. Let $\ell R = \mathfrak{q}_1 \dots \mathfrak{q}_r$ be the primary decomposition of ℓR, where each $\mathfrak{q}_i$ is a $\mathfrak{p}_i$-primary ideal for some prime ideal $\mathfrak{p}_i \subset R$. Then the Chinese remainder theorem implies that

$$R/\ell R \cong R/\mathfrak{q}_1 \times \cdots \times R/\mathfrak{q}_r, \quad \mathfrak{a}/\ell\mathfrak{a} \cong \mathfrak{a}/\mathfrak{q}_1\mathfrak{a} \oplus \cdots \oplus \mathfrak{a}/\mathfrak{q}_r\mathfrak{a}. \tag{45}$$

We claim that each $\mathfrak{a}/\mathfrak{q}_i\mathfrak{a}$ is free of rank 1 as $R/\mathfrak{q}_i$-module. Note that $R/\mathfrak{q}_i = R_{\mathfrak{p}_i}/(\mathfrak{q}_i)_{\mathfrak{p}_i}$ and similarly $\mathfrak{a}/\mathfrak{q}_i\mathfrak{a} = \mathfrak{a}_{\mathfrak{p}_i}/(\mathfrak{q}_i)_{\mathfrak{p}_i}\mathfrak{a}_{\mathfrak{p}_i}$. By assumption we have $\mathfrak{a}_{\mathfrak{p}_i} \cong R_{\mathfrak{p}_i}$, which extends to the required isomorphism $\mathfrak{a}/\mathfrak{q}_i\mathfrak{a} \cong R/\mathfrak{q}_i$. Then this implies that $\mathfrak{a}/\ell\mathfrak{a} = (R/\ell R)a$ for some $a \in \mathfrak{a}/\ell\mathfrak{a}$, and by Nakayama's lemma, any lift of a to $\mathfrak{a}_\ell$ generates $\mathfrak{a}_\ell$ as R_ℓ-module.

(d) $\Rightarrow$ (a) As fore each prime ℓ, $\mathfrak{a}_\ell$ is a principal fractional R_ℓ-ideal, it is easy to check that $\mathfrak{a}_\ell$ is proper and reflexive. Then the properness and reflexiveness of $\mathfrak{a}$ follow from lemma's 4.4 and 4.5, as we have

$$r(\mathfrak{a}) = \bigcap_\ell L \cap r(\mathfrak{a})_\ell = \bigcap_\ell L \cap r(\mathfrak{a}_\ell) = \bigcap_\ell R_\ell = R \tag{46}$$

and

$$(\mathfrak{a}^{-1})^{-1} = \bigcap_\ell L \cap ((\mathfrak{a}^{-1})^{-1})_\ell = \bigcap_\ell L \cap (\mathfrak{a}_\ell^{-1})^{-1} = \bigcap_\ell L \cap \mathfrak{a}_\ell = \mathfrak{a}. \tag{47}$$

□

4.2 Over-orders and fractional ideal classes

Again, let R be a Z-order. Then as R is finitely generated over Z, every element of R is integral over Z, i.e. every element of R satisfies some monic polynomial in $Z[X]$. Every separable finite-dimensional Q-algebra L contains a maximal order, given by all Z-integral elements (elements of L which satisfy monic polynomial with coefficients in Z). This maximal order is called the ring of integers of L and is denoted by $\mathcal{O}_L$. If we write $L = L_1 \times \cdots \times L_r$ where each L_i is a finite separable field extension of Q, then $\mathcal{O}_L = \mathcal{O}_{L_1} \times \cdots \times \mathcal{O}_{L_r}$.

Let R be a Z-order with total ring of fractions L. Then any order S such that $R \subset S \subset \mathcal{O}_L$ is called an over-order of R. Note that every over-order S corresponds to some R-submodule of $\mathcal{O}_L/R$, however the converse does not necessarily hold. If Z/aZ is finite for all non-zero $a \in Z$ (as is the case for $Z = \mathbb{Z}$ or $Z = \mathbb{Z}_\ell$), then $\mathcal{O}_L/R$ is finite and thus there are only finitely many over-orders of R.

Example 4.9. Consider the order $R = \mathbb{Z}[\alpha] = \mathbb{Z}[X]/(X^2 - 36)$. Then $L = \mathbb{Q}[X]/(X^2 - 36) = \mathbb{Q}[X]/(X - 6)(X + 6) \cong \mathbb{Q} \times \mathbb{Q}$. If we identify L and R with their images under this isomorphism, then $\alpha = (6, -6)$, $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \colon a \equiv b \bmod 12\}$ and $\mathcal{O}_L = \mathbb{Z} \times \mathbb{Z}$. Therefore we have $\mathcal{O}_L/R \cong \mathbb{Z}/12\mathbb{Z}$. The subgroups of $\mathbb{Z}/12\mathbb{Z}$ are exactly $\{\mathbb{Z}/n\mathbb{Z} \colon n \text{ divides } 12\}$, where each $\mathbb{Z}/n\mathbb{Z}$ corresponds to an over-order $\mathbb{Z}[(6 + \alpha)/n]$ of R.

Let R be a Z-order. Then we denote the set of fractional R-ideals by $\mathcal{I}(R)$ and the set of principal fractional R-ideals by $\mathcal{P}(R)$. Note that $\mathcal{I}(R)$ is a commutative monoid, with multiplication given by ideal multiplication and identity R. Also note that $\mathcal{P}(R)$ is a subgroup of $\mathcal{I}(R)$, as it is closed under multiplication. We can define the ideal class monoid by the monoid quotient

$$\mathrm{ICM}(R) = \mathcal{I}(R)/\mathcal{P}(R). \tag{48}$$

It is easy to check that the fractional ideal properties proper and invertible are preserved under multiplication by principal ideals. This allows us to define the set of proper ideal classes

$$\mathrm{ICP}(R) = \{\text{proper } \mathfrak{a} \in \mathcal{I}(R)\}/\mathcal{P}(R) \tag{49}$$

and the class group of invertible ideal classes

$$\mathrm{Cl}(R) = \{\text{invertible } \mathfrak{a} \in \mathcal{I}(R)\}/\mathcal{P}(R). \tag{50}$$

As the name suggest, the class group $\mathrm{Cl}(R)$ is a group, as it is closed under multiplication and every class $[\mathfrak{a}] \in \mathrm{Cl}(R)$ has an inverse $[\mathfrak{a}^{-1}]$. However, $\mathrm{ICP}(R)$ is not

necessarily even closed under multiplication and thus we cannot assume any monoid structure on it.

These are extensively studied in [Mar20] in the case $Z = \mathbb{Z}$, but most of the result extend effortlessly to the general Z-order case.

We are mostly interested in the case where Z is already ℓ-adically complete, in particular when $Z = \mathbb{Z}_\ell$. In this case every invertible ideal is principal by proposition 4.7, and thus the class group is trivial. Then one can calculate $\mathrm{ICP}(R)$ using [Mar20, 5.1].

4.3 Gorenstein and Bass orders

As L is a finite-dimensional Q-algebra, we can view each element of $x \in L$ as a Q-linear operator $m_x \colon L \to L$, given by multiplication-by-x. This allows us to define the trace $\mathrm{Tr}_{L/Q} \colon L \to Q$, defined by $\mathrm{Tr}_{L/Q}(x) = \mathrm{Tr}(m_x)$.

For a fractional R-ideal $\mathfrak{a}$, we define its trace dual by

$$\mathfrak{a}^\dagger := \{x \in L \colon \mathrm{Tr}_{L/Q}(xy) \in \mathbb{Z} \text{ for all } y \in \mathfrak{a}\}.$$

One can check that $\mathfrak{a}^\dagger$ is again a fractional R-ideal, and as the name suggests, we have $(\mathfrak{a}^\dagger)^\dagger = \mathfrak{a}$. If R is monogenic, i.e. of the form $R = Z[\alpha]$ for some $\alpha \in L$ with minimal polynomial $f \in Z[X]$, then it is well-known that $R^\dagger = f'(\alpha)^{-1}R$ (see [Ste17, Excercise 4.29]).

We will be interested in a special class of Z-orders R, called Gorenstein orders, which satisfy the following property.

Definition 4.10. An Z-order R is called Gorenstein if every fractional R-ideal $\mathfrak{a}$ is reflexive, i.e. $(\mathfrak{a}^{-1})^{-1} = \mathfrak{a}$.

There are couple of equivalent conditions:

Proposition 4.11. *Let R be an order. The following are equivalent:*

(a) *R is Gorenstein, i.e. every fractional R-ideal is reflexive.*

(b) *Every proper fractional R-ideal is invertible.*

(c) *$R^\dagger$ is invertible.*

Proof. See [JT15, 4.2]. □

In particular we see that monogenic orders are Gorenstein as $R^\dagger = f'(\alpha)^{-1}R$ is indeed invertible, and so it the ring of integers $\mathcal{O}_L$. Also, note that if R is both Gorenstein and ℓ-adically complete, then every proper ideal is principal, i.e. $\mathrm{ICP}(R)$ is trivial. We will use this later on.

A even more stronger requirement than Gorenstein, is being Bass.

Definition 4.12. An Z-order R is called Bass if every over-order $R \subset S \subset \mathcal{O}_L$ is Gorenstein.

Again, we have equivalent conditions:

Proposition 4.13. *Let R be a Z-order, with quotient ring $L = R \otimes Q$ with maximal order $\mathcal{O}$. The following are equivalent:*

(a) *R is Bass, i.e. every subring S such that $R \subset S \subset \mathcal{O}$ is Gorenstein.*

(b) *The R-module $\mathcal{O}/R$ is cyclic.*

(c) *Every ideal of R can be generated by two elements.*

Proof. See [LW85, 2.1]. □

The ring of integers $\mathcal{O}_L$ is always Bass, and so are quadratic orders.

In some cases we will need to determine the possible structures of an R-submodule $M \subset L^e$ that is free of finite rank as Z-module such that $M \otimes_Z Q = L^e$. In general this is a very hard problem. However, if R is Bass and ℓ-adically closed, there is a very nice description.

Proposition 4.14. *Let R be Bass and ℓ-adically closed. Let $M \subset L^e$ be a R-submodule that is also a Z-lattice in L^e, i.e. M is free of finite rank as Z-module and $M \otimes_Z Q = L^e$. Then*

$$M \cong S_1 \oplus \cdots \oplus S_e, \tag{51}$$

where $R \subset S_1 \subset \cdots \subset S_e \subset \mathcal{O}_L$ are over-orders of R. In particular, $S_1 = r(M) = \{x \in L \colon xM \subset M\}$.

Proof. Consequence of [LW85, 7.1]. □

5 Endomorphism rings and complex multiplication

5.1 Endomorphism ring of an elliptic curve

We recall some basic facts about endomorphisms of elliptic curves which can be found in [Sil09, Ch. III].

Let E be an elliptic curve over a field K. A map $\phi\colon E \to E$ is called an endomorphism if it is both a morphism of curves and a homomorphism of groups. The set of endomorphisms of E defined over K form a ring, denoted by $\mathrm{End}(E) := \mathrm{End}_K(E)$, with addition extended by the addition on E, and multiplication given by composition. There are three possibilities for the structure of $\mathrm{End}(E)$: either it is isomorphic to $\mathbb{Z}$ (i.e. the only endomorphisms are the multiplication-by-n maps), isomorphic to an order in imaginary quadratic field, or an order in a quaternion algebra. The last case can only happen in positive characteristic. When $\mathrm{End}_{\overline{K}}(E) \supsetneq \mathbb{Z}$, we say that E has complex multiplication (CM). For elliptic curves over number fields, complex multiplication is the exception, while over finite fields all elliptic curves have complex multiplication (see [Sil09, Remark III.9.4] and [Sil09, Remark C.11.3.2]).

Note that in our definition of $\mathrm{End}(E)$ we required the endomorphisms to be defined over K. It is possible that $\mathrm{End}_{\overline{K}}(E)$ is strictly larger than $\mathrm{End}(E)$, see for instance example 5.2.

Example 5.1. The main example of endomorphisms are the multiplication-by-n maps. For any integer $n \in \mathbb{Z}$, this map is denoted by

$$[n]\colon E \to E, \quad P \mapsto nP, \tag{52}$$

which is always defined over K.

Every endomorphism $\phi \in \mathrm{End}(E)$ has a dual endomorphism $\hat{\phi} \in \mathrm{End}(E)$, such that $\phi \circ \hat{\phi} = \hat{\phi} \circ \phi = [\deg(\phi)]$, which we will write as $\phi\hat{\phi} = \hat{\phi}\phi = \deg(\phi)$. Every endomorphism satisfies its characteristic polynomial, given by

$$\chi_\phi = X^2 - \mathrm{tr}(\phi)X + \deg(\phi) \in \mathbb{Z}[X], \tag{53}$$

where $\mathrm{tr}(\phi) = \phi + \hat{\phi}$.

Example 5.2. For an example of an endomorphism that is not multiplication by an integer, let $E/\mathbb{Q}$ be the elliptic curve defined by $y^2 = x^3 + x$. Then the map

$$[i]\colon E \to E, \quad (x, y) \mapsto (-x, iy) \tag{54}$$

is an endomorphism of E defined over $\mathbb{Q}(i)$. Note that the notation $[i]$ is justified, as $[i]^2 = [-1]$, and $\chi_{[i]} = X^2 + 1$. As a matter of fact, $\mathrm{End}_{\mathbb{Q}}(E) \cong \mathbb{Z}$ and $\mathrm{End}_{\mathbb{Q}(i)}(E) \cong \mathbb{Z}[i]$.

Example 5.3. For elliptic curves over finite fields, an important endomorphism is the Frobenius: for an elliptic curve E over a finite field $\mathbb{F}_q$, the Frobenius is given by

$$\pi \colon E \to E, \quad (x, y) \mapsto (x^q, y^q). \tag{55}$$

Clearly, π is defined over $\mathbb{F}_q$. Its characteristic polynomial is

$$\chi_\pi = X^2 - aX + q, \tag{56}$$

where $a = \mathrm{tr}(\pi)$. The curve E is supersingular if and only if p divides a (see [Sil09, proof of V.4.1]).

It is easy to check that endomorphisms send n-torsion points to n torsion points. Therefore $E[n]$ naturally has a left $\mathrm{End}(E)$-module structure (note that $\mathrm{End}(E)$ is not necessarily commutative), given by a ring homomorphism $\mathrm{End}(E) \to \mathrm{End}(E[n])$. Similarly for any prime ℓ we get a R-module structure for $T_\ell(E)$, by acting componentswise. This extends naturally to a $\mathrm{End}(E) \otimes \mathbb{Z}_\ell$-module structure on $T_\ell(E)$, which is faithful, as the map

$$\mathrm{End}(E) \otimes \mathbb{Z}_\ell \to \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(E)) \tag{57}$$

is injective (see [Sil09, III.7.4]).

We can consider the endomorphism algebra $\mathrm{End}^0(E) = \mathrm{End}(E) \otimes \mathbb{Q}$. As mentioned before, $\mathrm{End}^0(E)$ is either equal to $\mathbb{Q}$, an imaginary quadratic field, or an quaternion algebra. Note that for any element $\phi \in \mathrm{End}^0(E)$, there exists some integer $n \geq 1$ such that $n\phi \in \mathrm{End}(E)$. Therefore the following lemma and proposition allow us give conditions for whether certain elements of $\mathrm{End}^0(E)$ are endomorphisms.

Remark 5.3.1. Note that $\mathrm{End}^0_{\overline{K}}(E)$ can be strictly larger than $\mathrm{End}^0(E)$. However, all endomorphism of E defined over $\overline{K}$ that belong to $\mathrm{End}^0(E)$ are actually defined over K. This can be easily checked using that if $\phi \in \mathrm{End}^0(E) \cap \mathrm{End}_{\overline{K}}(E)$, then $n\phi \in \mathrm{End}(E)$, together with the characterization that ϕ is defined over K if and only if ϕ commutes with all $\sigma \in G_{\overline{K}/K}$.

Lemma 5.4. *Let E, E', E'' be three elliptic curves over an algebraically closed field K. Let $\phi \colon E \to E'$ and $\psi \colon E \to E''$ be non-zero isogenies, ψ separable with $\ker(\psi) \subset \ker(\phi)$. Then there exists an unique isogeny $\theta \colon E'' \to E'$ such that $\phi = \theta \circ \psi$.*

Proof. Using the equivalence of categories between curves and their function fields (see [Sil09, II.2.5.]), there is a bijective correspondence between isogenies (up to isomorphism) from E and elliptic subfields of $\mathbb{K} := K(E)$, given by assigning to an isogeny $\phi\colon E \to E'$ the subfield $\mathbb{K}^\phi := \phi^* K(E') \subset \mathbb{K}$. Let $\phi\colon E \to E'$ and $\psi\colon E \to E''$ be as in the statement of the lemma. Then the existence of $\theta\colon E'' \to E'$ such that $\phi = \theta \circ \psi$ is equivalent to the inclusion of elliptic subfields $\mathbb{K}^\phi \subset \mathbb{K}^\psi \subset \mathbb{K}$.

For an point $P \in E$, we can consider the translation morphism (of curves) $\tau_p\colon E \to E$ given by $\tau_P(Q) = Q + P$. As ψ is separable, we have (by [Sil09, III.4.10]) that $\mathbb{K}^\psi$ is the fixed field of the subgroup

$$T_\psi := \{\tau_P^*\colon P \in \ker \psi\} \subset \mathrm{Aut}_K(\mathbb{K}).$$

Since $\ker(\psi) \subset \ker(\phi)$, it follows that $\mathbb{K}^\phi$ is also fixed under T_ψ. Therefore $\mathbb{K}^\phi \subset \mathbb{K}^\psi \subset \mathbb{K}$ and thus we have an isogeny $\theta\colon E'' \to E'$ such that $\phi = \theta \circ \psi$.

Uniqueness follows immediately from ψ being non-zero and therefore surjective. □

Proposition 5.5. *Let E be an elliptic curve over a field K with $p = \mathrm{char}(K) \geq 0$. Denote its endomorphism ring by $R = \mathrm{End}(E)$.*

(a) *For any integer n coprime to p, and any endomorphism $\phi \in \mathrm{End}(E)$, we have that $\frac{1}{n}\phi \in \mathrm{End}(E)$ if and only if $E[n] \subset \ker \phi$.*

(b) *For any prime $\ell \neq p$, any integer $n \geq 1$, and any endomorphism $\phi \in \mathrm{End}(E)$, we have that $\frac{1}{\ell^n}\phi \in \mathrm{End}(E)$ if and only if ϕ maps $T_\ell(E)$ into $\ell^n T_\ell(E)$.*

Proof. (a) If $\psi = \frac{1}{n}\phi \in \mathrm{End}(E)$, then for any n-torsion point $P \in E[n]$, we have $\phi(P) = n\psi(P) = \psi(nP) = 0$. For the converse, if $E[n] \subset \ker(\phi)$, then as n coprime to p, we have that $[n]$ is separable. Therefore by the previous lemma, there exists $\theta \in \mathrm{End}(E)$ such that $\phi = n\theta$. Thus $\theta = \frac{1}{n}\phi \in \mathrm{End}(E)$.

(b) If $\psi = \frac{1}{\ell^n}\phi \in \mathrm{End}(E)$ then $\phi = \ell^n\psi$ and thus $\phi T_\ell(E) = \ell^n \psi T_\ell(E) \subset \ell^n T_\ell(E)$. For the converse, if $\phi T_\ell(E) \subset \ell^n T_\ell(E)$, then $\phi E[\ell^n] = \phi T_\ell(E)/\ell^n T_\ell(E) = 0$. Thus $E[\ell^n] \subset \ker(\phi)$ and therefore by part (a) we have $\frac{1}{\ell^n}\phi \in \mathrm{End}(E)$. □

5.2 Complex multiplication over $\mathbb{C}$

Let E be an elliptic curve over $\mathbb{C}$. After a suitable isomorphism we can identify E as a complex torus $\mathbb{C}/\Lambda$. Then the endomorphism ring $R := \mathrm{End}(E)$ is equal to the multiplier ring of Λ (see [Sil09, Ch. V]), i.e.

$$R = \{z \in \mathbb{C}\colon x\Lambda \subset \Lambda\}. \tag{58}$$

We will assume that E has complex multiplication, i.e. $R \neq \mathbb{Z}$. This implies that R is an order in an imaginary quadratic field. We can use this to deduce some results about the structure of such curves.

Proposition 5.6. *Let R be an order in an imaginary quadratic field L.*

(a) *Let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by R. Then $E \cong \mathbb{C}/\mathfrak{a}$ for some invertible fractional R-ideal $\mathfrak{a} \subset L$.*

(b) *There is a bijection between the isomorphism classes of elliptic curves over $\mathbb{C}$ with complex multiplication by R and ideal classes in the class group $\mathrm{Cl}(R)$.*

(c) *The j-invariants of the isomorphism classes of elliptic curves over $\mathbb{C}$ with complex multiplication by R form a transitive set of conjugate algebraic integers.*

Proof. (a) Write $E \cong \mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$. Let $z \in \Lambda$ be non-zero and let $\mathfrak{a} = z^{-1}\Lambda$. Note that $1 \in \mathfrak{a}$. Furthermore, as Λ and $\mathfrak{a}$ are homothetic, we have that $E \cong \mathbb{C}/\mathfrak{a}$ and $\mathfrak{a}$ also has multiplier ring R.

We claim that $\mathfrak{a}$ is a proper fractional R ideal. Since $1 \in \mathfrak{a}$ and $R\mathfrak{a} \subset \mathfrak{a}$, we see that $R \subset \mathfrak{a}$. As both R and $\mathfrak{a}$ are free of rank 2 as $\mathbb{Z}$-modules we have $L = R \otimes \mathbb{Q} = \mathfrak{a} \otimes \mathbb{Q}$. In particular we see that $\mathfrak{a} \subset L$. We conclude that $\mathfrak{a}$ is a finitely generated R-submodule of L with multiplier ring R. Then by definition, $\mathfrak{a}$ is a proper R-fractional ideal.

Now we use that R is monogenic and thus Gorenstein, which implies that $\mathfrak{a}$ is invertible.

(b) From part (a) we know that any elliptic curve over $\mathbb{C}$ with endomorphism ring R is isomorphic to a complex torus of the form $\mathbb{C}/\mathfrak{a}$ where $\mathfrak{a}$ is an invertible fractional R-ideal. Two such curves are isomorphic if and only if the corresponding fractional ideals are homothetic, which is equivalent to belonging to the same class in $\mathrm{Cl}(R)$.

(c) The proof of this is quite involved. See [Sil94] for when $R = \mathcal{O}_L$ is the maximal order in L.

□

The last part of this proposition has a couple of useful consequences. First of all, it implies that any curve over $\mathbb{C}$ with complex multiplication can be defined over some number field. Second of all, it allows us to check whether a curve has complex multiplication by a given order R. Given an imaginary quadratic order R of discriminant Δ, its Hilbert class polynomial is defined as

$$H_R(X) := H_\Delta(X) := \prod_{[\mathfrak{a}] \in \mathrm{Cl}(R)} (X - j(\mathfrak{a})), \tag{59}$$

which belongs to $\mathbb{Z}[X]$ by part (c) of the previous proposition. Note that a given elliptic curve E over $\mathbb{C}$ has complex multiplication by R if and only if $H_R(j(E)) = 0$.

Furthermore, this polynomial can be computed quite efficiently. We can use the equivalence between the ideal class group of R and the class group of primitive positive definite quadratic forms of discriminant Δ, of which the latter can be computed quite efficiently (see [Cox11, Ch. 1.3]). Under this isomorphism a quadratic form $f = ax^2 + bxy + cy^2$ gets mapped to the fractional ideal $\mathfrak{a} = \mathbb{Z} \oplus \mathbb{Z}(-b + \sqrt{\Delta})/2a$. Using q-expansion of j, given by

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \ldots, \qquad q = e^{2\pi i \tau}, \tag{60}$$

we can calculate $j(\mathfrak{a}) = j((-b + \sqrt{\Delta})/2a)$ up to a desired precision. This gives us a numerical approximation for $H_R(X)$, which only has to be calculated to a precision where we can round-off to the nearest integer.

5.3 Reducing and lifting endomorphisms

Due to the work of Deuring, we have a theory that links complex multiplication over finite fields and complex multiplication over $\mathbb{C}$.

Let E be an elliptic curve over a number field K. Furthermore, let $\mathfrak{p}$ be a prime of K of good reduction, and let $E_\mathfrak{p}$ denote the reduced curve. Then we get a map

$$\mathrm{red}_\mathfrak{p} \colon \mathrm{End}(E) \to \mathrm{End}(E_\mathfrak{p}),$$

which can be defined as follows. For $\phi \in \mathrm{End}(E)$, we have that ϕ is defined over over K and given by a rational map with coefficients in K. After suitably rescaling these coefficients if necessary, we can reduce this rational map modulo $\mathfrak{p}$ to get a rational map $\overline{\phi} = \mathrm{red}_\mathfrak{p}(\phi)$ from $E_\mathfrak{p}$ to itself. As $E_\mathfrak{p}$ is smooth and $\overline{\phi}$ fixes the point at infinity, we have $\overline{\phi} \in \mathrm{End}(E_\mathfrak{p})$. One can show that this does not depend on the choice of rational map.

From the definition it is clear that we have the commutative diagram:

$$\begin{array}{ccc} E(K) & \xrightarrow{\phi} & E(K) \\ {\scriptstyle \mathrm{red}_\mathfrak{p}}\downarrow & & \downarrow{\scriptstyle \mathrm{red}_\mathfrak{p}} \\ E_\mathfrak{p}(\mathbb{F}_\mathfrak{p}) & \xrightarrow{\overline{\phi}} & E_\mathfrak{p}(\mathbb{F}_\mathfrak{p}) \end{array}$$

Using this, one can show that $\mathrm{red}_\mathfrak{p} \colon \mathrm{End}(E) \to \mathrm{End}(E_\mathfrak{p})$ is an injective ring homomorphism.

Proposition 5.7. *Let E be an elliptic curve over a number field K with complex multiplication by an order R in an imaginary quadratic field L. Let $\mathfrak{p}$ be a prime of K above p of good reduction. Then:*

(a) *The reduction $E_\mathfrak{p}$ is ordinary if and only if p splits in R.*

(b) *If this is the case, then $\mathrm{End}(E_\mathfrak{p})$ is equal to the smallest over-order of R that is maximal at p.*

Proof. See [Lan87, Ch. 13: Thm. 12]. □

Proposition 5.8 (Deuring's lifting theorem)**.** *Let E be an elliptic curve over a field k of characteristic $p > 0$ and let $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$ be an endomorphism. Then there exists an elliptic curve $\tilde{E}$ over some number field K, an endomorphism $\tilde{\alpha} \in \mathrm{End}(\tilde{E})$ and some prime $\mathfrak{p}$ of K above p such that $\tilde{E}$ has good reduction at $\mathfrak{p}$, such that the reduced curve $\tilde{E}_\mathfrak{p}$ is isomorphic to E and $\tilde{\alpha}$ maps to α under this isomorphism.*

Proof. When E is ordinary, see [Lan87, Ch. 13: Thm. 14]. For the supersingular case, see [Deu41]. □

5.4 Calculating the endomorphism ring

Given an elliptic curve E over a finite field $\mathbb{F}_q$, our goal will be to express the action of the Frobenius endomorphism $\pi \in \mathrm{End}(E)$ on torsion in terms of how π lies in the subring $R = \mathrm{End}(E) \cap \mathbb{Q}(\phi)$. In order to apply this, we will need to be able to determine the ring R.

Lemma 5.9. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$ with Frobenius endomorphism $\pi \in \mathrm{End}(E)$. Then $R = \mathrm{End}(E) \cap \mathbb{Q}(\pi)$ is maximal at p, i.e. p does not divide $[\mathcal{O}_{\mathbb{Q}(\pi)} : R]$.*

Proof. If E is supersingular, then this follows from [Lan87, Ch. 13.2]. If E is ordinary, then the discriminant of $\mathbb{Z}[\pi]$ is equal to $\Delta = a^2 - 4q$, where $a = \mathrm{tr}(\pi)$. As E ordinary, a is not divisible by p and therefore Δ is not divisible by p. Thus $\mathbb{Z}[\pi]$ is already maximal at p, and as $\mathbb{Z}[\pi] \subset R$, so is R. □

For ordinary elliptic curves, we will follow [DT02], using reduction and lifting combined with Hilbert class polynomials to calculate R.

Proposition 5.10. *Let E be an ordinary elliptic curve over a finite field $\mathbb{F}_q$, and let R be an order in an imaginary quadratic field L such that R is maximal at p. Let $\overline{H_R} \in \mathbb{F}_p[X]$ denote the reduction of the Hilbert class polynomial $H_R \in \mathbb{Z}[X]$ modulo p. Then $R \cong \mathrm{End}(E)$ if and only if $\overline{H_R}(j(E)) = 0$.*

Proof. Let $R = \mathrm{End}(E) = \mathbb{Z}[\theta]$. Then by Deuring's lifting theorem, we can lift the pair (E, θ) to a pair $(\tilde{E}, \tilde{\theta})$, where $\tilde{E}$ is an elliptic curve over a number field K and $\tilde{\theta} \in \mathrm{End}(\tilde{E})$ such that there exists some prime $\mathfrak{p}$ of K above p such that $\tilde{E}$ reduces to E and $\tilde{\theta}$ reduces to θ. Therefore $R \subset S = \mathrm{End}(\tilde{E})$. As R is maximal at p by the previous lemma, so is S, and therefore $R = S$ by proposition 5.7. Thus we have, $H_R(j(\tilde{E})) = 0$, which after reducing modulo $\mathfrak{p}$ gives $\overline{H_R}(j(E)) = 0$.

Conversely, suppose that $\overline{H_R}(j(E))) = 0$. Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ represent the ideal classes in $\mathrm{Cl}(R)$. Consider the field $K = L(j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_n))$, and let $\mathfrak{p}$ be a prime of K above p. Then as H_R splits over $\mathcal{O}_K[X]$, we have that $\overline{H_R}$ splits over the residue field $\mathbb{F}_\mathfrak{p}$. In particular, there exists an i such that $j(E)$ is the reduction of $j(\mathfrak{a}_i)$ modulo $\mathfrak{p}$.

Consider the curve $\tilde{E} = \mathbb{C}/\mathfrak{a}_i$, which can be defined over K as $j(\tilde{E}) = j(\mathfrak{a}) \in K$. As $j(\tilde{E})$ is integral, $\tilde{E}$ has potentially good reduction at $\mathfrak{p}$ (see [Sil09, VII.5.5]). This means that there exists some field extension K'/K and a prime $\mathfrak{p}'$ of K' above $\mathfrak{p}$ such that E has good reduction at $\mathfrak{p}'$, and let E' denote the reduced curve. Then $j(E) = j(E')$, and thus E and E' are isomorphic over $\overline{\mathbb{F}_q}$. Therefore, $\mathrm{End}_{\overline{\mathbb{F}_q}}(E) = \mathrm{End}_{\overline{\mathbb{F}_q}}(E')$. As ordinary elliptic curves have all their endomorphisms defined over their base field (combine $\mathrm{End}^0_{\overline{F_q}}(E) = \mathrm{End}^0_{F_q}(E) = \mathbb{Q}(\pi)$ with remark 5.3.1), we have that $\mathrm{End}_{\mathbb{F}_q}(E) = \mathrm{End}_{\mathbb{F}_q}(E')$. However, by proposition 5.7, $\mathrm{End}_{\mathbb{F}_q}(E') = \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(E')$ is the smallest over-order of $R = \mathrm{End}_{K'}(\tilde{E})$ which is maximal at p, which is R itself. □

For ordinary curves, this allows us to calculate the ring $R = \mathrm{End}(E) \cap \mathbb{Q}(\pi) = \mathrm{End}(E)$ as follows: first we determine the trace of Frobenius a by computing $\#E(\mathbb{F}_q)$, either by counting points directly or by Schoof's algorithm [Sch95]. Then apply the formula (see [Sil09, Remark V.2.6])

$$a = q + 1 - \#E(\mathbb{F}_q). \tag{61}$$

Then we have that

$$\chi_\pi = X^2 - aX + q, \quad \Delta_\pi = a^2 - 4q. \tag{62}$$

Then for each integer $b \geq 1$ dividing $[\mathcal{O}_L : \mathbb{Z}[\pi]] = \sqrt{\Delta_\pi/\Delta_L}$, we compute $\overline{H_{b^2\Delta_L}}(j(E))$ until we find some b for which it is zero. Then R is the unique order with discriminant $\Delta_R = b^2\Delta_L$.

Example 5.11. Consider the elliptic curve $E\colon y^2 = x^3 + 2x + 7$ over $\mathbb{F}_{13}$. Then by counting points we find

$$\chi_\pi = X^2 + 2X + 13, \quad \Delta_\pi = -48, \tag{63}$$

and thus we see that E is ordinary. The possibilities for R are characterized by $\Delta_R \in \{-3, -12, -48\}$. Calculating H_Δ for $\Delta \in \{-3, -12, -48\}$ and evaluating the reduction $\overline{H_\Delta}$ modulo 13 at $j(E) = 11$, gives us

$$\begin{aligned} H_{-3}(X) &= X, & \overline{H_{-3}}(11) &= 11, \\ H_{-12}(X) &= X - 54000, & \overline{H_{-12}}(11) &= 0, \\ H_{-48}(X) &= X^2 - 2835810000X + 6549518250000, & \overline{H_{-48}}(11) &= 9. \end{aligned}$$

Therefore we see that $\Delta_R = -12$, and thus $R = \mathbb{Z}[\frac{1}{2}\pi] \cong \mathbb{Z}[\sqrt{-12}]$.

However, for supersingular elliptic curves, the subring $R = \mathrm{End}(E) \cap \mathbb{Q}(\pi)$ is not necessarily determined by the j-invariant of E. Suppose we have two elliptic curves E, E' over $\mathbb{F}_q$ with $j(E) = j(E')$ and let $\pi \in \mathrm{End}(E)$, $\pi' \in \mathrm{End}(E')$ be the respective Frobenius endomorphisms. Then E and E' are isomorphic over some field extension $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$. Therefore we can identify $\mathrm{End}_{\overline{\mathbb{F}_q}}(E) = \mathrm{End}_{\overline{\mathbb{F}_q}}(E')$, and under this identification $\pi^k = \pi'^k$. However, if $\pi^k = \pi'^k \in \mathbb{Z}$, then it is possible that $\mathbb{Q}(\pi)$ and $\mathbb{Q}(\pi')$ are different (possibly isomorphic) quadratic subfields of the quaternion algebra $\mathrm{End}_{\overline{\mathbb{F}_q}}(E)$. Therefore it is possible that the subrings $R = \mathrm{End}(E) \cap \mathbb{Q}(\pi)$ and $R' = \mathrm{End}(E') \cap \mathbb{Q}(\pi')$ are not isomorphic.

	χ_π	Δ_π	Δ_R	R
$q = p$	$X^2 + p$	$-4p$	$-p$ or $-4p$	$\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$ or $\mathbb{Z}[\sqrt{-p}]$
	$X^2 \pm 2X + 2$	-4	-4	$\mathbb{Z}[i]$
	$X^2 \pm 3X + 3$	-3	-3	$\mathbb{Z}[\zeta_3]$
$q = p^2$	$X^2 + p^2$	$-4p^2$	-4	$\mathbb{Z}[i]$
	$X^2 \pm pX + p^2$	$-3p^2$	-3	$\mathbb{Z}[\zeta_3]$
	$X^2 \pm 2pX + p^3$	0	-	$\mathbb{Z}$
$q = p^3$	$X^2 + p^3$	$-4p^3$	$-p$ or $-4p$	$\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$ or $\mathbb{Z}[\sqrt{-p}]$
	$X^2 + cpX + p^3$ $(p \not| c)$	$p^2(c - 4p)$	$\Delta_R \mid c - 4p$	over-order of $\mathbb{Z}[\sqrt{c - 4p}]$
	$X^2 \pm 4X + 8$	-16	-4	$\mathbb{Z}[i]$
	$X^2 \pm 9X + 27$	-27	-3	$\mathbb{Z}[\zeta_3]$

Table 2: Possibilities for $R = \mathrm{End}(E) \cap \mathbb{Q}(\pi)$ when $E/\mathbb{F}_q$ is supersingular with Frobenius $\pi \in \mathrm{End}(E)$, for small powers $q = p^k$.

In table 2, we have determined the possibilities for R for small powers $q = p^k$. We determined the possible characteristic polynomials χ_π, using the fact that for supersingular curves $a = \mathrm{tr}(\pi)$ is divisible by p, combined with the Hasse bound

$|a| \leq 2\sqrt{q}$ (see [Sil09, V.1.1]). As R is maximal at p by lemma 5.9, in most cases this limits R to one or two possibilities.

We will finish this chapter with a small lemma for the case $\chi_\pi = X^2 + p^k$ with $k \geq 1$ odd, such that we can completely determine R when $q = p$ or $q = p^2$.

Lemma 5.12. *Let $p \geq 3$ be a prime, and suppose E is a supersingular elliptic curve over the finite field $\mathbb{F}_{p^k}$, with $k \geq 1$ odd. Furthermore, suppose that E is given by a Weierstrass equation $y^2 = f(x)$ where $f(x) \in \mathbb{F}_{p^k}[x]$ is monic and separable of degree 3. Also suppose that the Frobenius endomorphism $\pi \in \mathrm{End}(E)$ has characteristic polynomial*

$$\chi_\pi = X^2 + p^k \in \mathbb{Z}[X]. \tag{64}$$

Then $R = \mathrm{End}(E) \cap \mathbb{Q}(\pi)$ is isomorphic to $\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$ if $p \equiv 3 \mod 4$ and $f(x)$ splits completely over $\mathbb{F}_{p^k}$. Otherwise, R is isomorphic to $\mathbb{Z}[\sqrt{-p}]$.

Proof. Note that $\chi_\pi = X^2 + p^k$ has discriminant $\Delta_\pi = -4p^k$. As R has to be maximal at p and k is odd, this leaves us with the options: just $\Delta_R = -4p$ if $p \not\equiv 3 \mod 4$, and $\Delta_R = -4p$ or $\Delta_R = -p$ if $p \equiv 3 \mod 4$.

In case $p \equiv 3 \mod 4$, then we note that $\Delta_R = -p$ if and only if $\frac{1-\pi}{2} \in R$. Then by proposition 5.5, this holds if and only if $E[2] \subset \ker(1 - \pi)$. In other words, π fixes $E[2]$ and thus $E[2] \subset E(\mathbb{F}_{p^k})$. As

$$E[2] = \{O, (\alpha_1, 0), (\alpha_2, 0), (\alpha_3, 0)\}, \tag{65}$$

where $\alpha_1, \alpha_2, \alpha_3$ are the roots of f, we see that $E[2] \subset E(\mathbb{F}_{p^k})$ if and only if f splits completely over $\mathbb{F}_{p^k}$. □

6 Representative of the Frobenius

In this section we will look at the unramified case for elliptic curves. We will show that primes $\mathfrak{p}$ of good reduction are unramified in every extension $K(E[n])/K$ where n is not divisible by $\mathfrak{p}$. After that we will spend the rest of this section giving a method to find a representative of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$-similarity class of the Frobenius $F_\mathfrak{p} = F_{K(E[n])/K,\mathfrak{p}}$, by studying the module structure of endomorphisms on torsion subgroups.

6.1 Unramified primes of good reduction

If E/K is an elliptic curve over a number field, and $\mathfrak{p}$ a prime of K of good reduction with reduced curve $E_\mathfrak{p}$, then for any integer $n \geq 1$ not divisible by $\mathfrak{p}$, reduction gives an isomorphism

$$E[n] \xrightarrow{\mathrm{red}_\mathfrak{P}} E_\mathfrak{p}[n] \tag{66}$$

where $\mathfrak{P}$ is any prime of $K(E[n])$ above $\mathfrak{p}$.

This isomorphism actually is enough to show that $\mathfrak{p}$ is unramified in the extension $K(E[n])/K$.

Proposition 6.1. *Let E/K be an elliptic curve over a number field and let $n \geq 1$ be an integer. Then any prime $\mathfrak{p}$ of good reduction that does not divide n is unramified in the extension $K(E[n])/K$.*

Proof. Let $\mathfrak{P}$ be any prime of $K(E[n])$ above $\mathfrak{p}$. By proposition 3.8 and table 1 we have an isomorphism $E[n] \xrightarrow{\mathrm{red}_\mathfrak{P}} E_\mathfrak{p}[n]$. This extends naturally to an isomorphism $\mathrm{Aut}(E[n]) \xrightarrow{\mathrm{red}_\mathfrak{P}} \mathrm{Aut}(E_\mathfrak{p}[n])$ and we have the following commutative diagram

$$\begin{array}{ccc} G_\mathfrak{P} & \xrightarrow{\mathrm{red}_\mathfrak{P}} & \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}) \\ \downarrow & & \downarrow \\ \mathrm{Aut}(E[n]) & \xrightarrow{\mathrm{red}_\mathfrak{P}} & \mathrm{Aut}(E_\mathfrak{p}[n]) \end{array} \tag{67}$$

where we recall that $G_\mathfrak{P}$ is the decomposition group of $\mathrm{Gal}(K(E[n])/K)$ belonging to $\mathfrak{P}$. The commutativity of the diagram follows immediately from the definition of the top map: for any $\sigma \in G_\mathfrak{P}$ and any $x \in \mathcal{O}_{K(E[n])}$, we have $\overline{\sigma}(\overline{x}) = \overline{\sigma(x)}$.

However, as the left and bottom maps are injective, the top map $G_\mathfrak{P} \xrightarrow{red_\mathfrak{P}} \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ also has to be injective and thus by proposition 3.6 $\mathfrak{p}$ is indeed unramified. □

6.2 Representative of the Frobenius

We continue to use the notation from the previous subsection. As $\mathfrak{p}$ is unramified in the extension $K(E[n])/K$, for any prime $\mathfrak{P}$ of $K(E[n])$ above $\mathfrak{p}$ there is a unique lift $F_{\mathfrak{P}} \in G_{\mathfrak{P}}$ of $\pi \in G_{\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}}$. Our goal will be to determine the $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$-similarity class of $F_{\mathfrak{P}}$, determined by its action on $E[n]$. However, by the commutativity of the diagram (67), this is the same as finding the $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$-similarity class of π determined by its action on $E_{\mathfrak{p}}[n]$. Since π actually defines an endomorphism $\pi\colon E_{\mathfrak{p}} \to E_{\mathfrak{p}}$, we can assume more structure on it than on $F_{\mathfrak{P}}$ (which is not necessarily an endomorphism). We will use this to our advantage.

Proposition 6.2. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$ with Frobenius endomorphism $\pi \in \mathrm{End}(E)$. Consider the endomorphism subring $R = \mathrm{End}(E) \cap \mathbb{Q}(\pi)$. Then for any n coprime to q, $E[n]$ is a free R/nR-module of rank $2/[R\colon Z]$.*

Proof. This will be a special case of proposition 6.6. □

This proposition allows us to express the action of $R = \mathrm{End}(E_{\mathfrak{p}}) \cap \mathbb{Q}(\pi)$ (and thus the action of π) on $E_{\mathfrak{p}}[n]$ as the action of R on a integral basis of itself, modulo n.

Let $\chi_\pi = X^2 - a_{\mathfrak{p}}X + N(\mathfrak{p}) \in \mathbb{Z}[X]$ be the characteristic polynomial of π, with discriminant $\Delta_\pi = a_{\mathfrak{p}}^2 - 4N(\mathfrak{p})$. First suppose $R \neq \mathbb{Z}$, then R is an order in an imaginary quadratic field. Therefore the order R is completely determined by its discriminant $\Delta_{\mathfrak{p}}$, and has integral basis $\{1, \theta\}$, where

$$\theta = \frac{\delta_{\mathfrak{p}} + \sqrt{\Delta_{\mathfrak{p}}}}{2}, \text{ with } \delta_{\mathfrak{p}} \in \{0, 1\} \text{ such that } \delta_{\mathfrak{p}} \equiv \Delta_{\mathfrak{p}} \mod 4. \tag{68}$$

If we identify π with the root of χ_π in the upper half-plane, i.e.

$$\pi = \frac{a_{\mathfrak{p}} + \sqrt{\Delta_\pi}}{2}, \tag{69}$$

then $\pi = (a_{\mathfrak{p}} - \delta_{\mathfrak{p}} b_{\mathfrak{p}})/2 + b_{\mathfrak{p}}\theta$, where $b_{\mathfrak{p}} = [R : \mathbb{Z}[\pi]] = \sqrt{\Delta_\pi/\Delta_{\mathfrak{p}}}$. Then the action of π on the integral basis $\{1, \theta\}$ is given by

$$M_\pi = \begin{pmatrix} (a_{\mathfrak{p}} - \delta_{\mathfrak{p}} b_{\mathfrak{p}})/2 & b_{\mathfrak{p}}(\Delta_{\mathfrak{p}} - \delta_{\mathfrak{p}})/4 \\ b_{\mathfrak{p}} & (a_{\mathfrak{p}} + \delta_{\mathfrak{p}} b_{\mathfrak{p}})/2 \end{pmatrix} \tag{70}$$

If $R = \mathbb{Z}$, then $\pi = a_{\mathfrak{p}}/2 \in \mathbb{Z}$, and therefore if we define $b_{\mathfrak{p}} = \Delta_{\mathfrak{p}} = 0$, the action of π is again given by M_π, but now on the standard basis of $\mathbb{Z}^2$.

Assuming proposition 6.2, this shows that

Proposition 6.3 (Duke-Tóth (2002))**.** *Let E be an elliptic curve over a number field K, and let $\mathfrak{p}$ be a prime of good reduction. For any integer n not divisible by $\mathfrak{p}$, let G_n denote the Galois group of $K(E[n])/K$ embedded into $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Then the $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$-similarity class of the Frobenius $F_\mathfrak{p}$ in G_n can be represented by the matrix $M_\pi \mod n$.*

The next two subsections will be devoted to proving proposition 6.2. First we will solve a similar statement for the more familiar case over $\mathbb{C}$, and then we will try to extend our argument to finite fields.

6.3 Module structure of torsion over $\mathbb{C}$

Let E be an elliptic curve over $\mathbb{C}$ with endomorphism ring $R = \mathrm{End}(E)$. Then for any integer $n \geq 1$, $E[n]$ has a natural R-module structure, and as nR annihilates $E[n]$, this extends to an R/nR-module structure. Our goal is to prove that $E[n]$ is free as R/nR-module.

If E does not have complex multiplication, then $R = \mathbb{Z}$. We already know that $E[n]$ is free of rank 2 as $\mathbb{Z}/n\mathbb{Z}$-module. So what is left to prove is the case where E does have complex multiplication.

As it does not require much extra effort, we will prove something a bit more general. For any ideal $\mathfrak{b} \subset R$, we consider the subgroup

$$E[\mathfrak{b}] = \{P \in E \colon \psi(P) = O \text{ for all } \psi \in \mathfrak{b}\}. \tag{71}$$

Using that $E \cong \mathbb{C}/\mathfrak{a}$ for some proper fractional R-ideal $\mathfrak{a} \subset L$ and example 2.4, we see that

$$E^{\mathrm{tors}} \cong (\mathfrak{a} \otimes \mathbb{Q})/\mathfrak{a} = L/\mathfrak{a} \quad \text{and} \quad E[\mathfrak{b}] \cong (\mathfrak{a} : \mathfrak{b})/\mathfrak{a}, \tag{72}$$

where $(\mathfrak{a} \colon \mathfrak{b}) = \{x \in L \colon \mathfrak{b}x \subset \mathfrak{a}\}$ is the usual fractional ideal quotient.

We will show that for any invertible ideal $\mathfrak{b} \subset R$, $E[\mathfrak{b}]$ is free of rank 1 as $R/\mathfrak{b}$-module. This is a well-known result of CM-theory, see for instance [Sil94, II.1.4] for the case where R is equal to the ring of integers $\mathcal{O}_L$.

Proposition 6.4. *Let E be an elliptic curve over $\mathbb{C}$, with complex multiplication by an order R in an imaginary quadratic field L, i.e. $\mathrm{End}(E) = R$, and let $\mathfrak{b} \subset R$ be an invertible ideal. Then $E[\mathfrak{b}]$ is a free $R/\mathfrak{b}$-module of rank 1.*

Proof. By part (a) of proposition 5.6, we have $E \cong \mathbb{C}/\mathfrak{a}$ for some invertible fractional ideal $\mathfrak{a} \subset L$. As $\mathfrak{b}$ is invertible, we get

$$E[\mathfrak{b}] \cong (\mathfrak{a} : \mathfrak{b})/\mathfrak{a} = \mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a}. \tag{73}$$

We claim that $\mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a}$ is isomorphic to $R/\mathfrak{b}$ as R-modules. Since $\mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a}$ is a finite R-module, it follows from lemma 2.2 that we can decompose it into its ℓ-adic localizations, i.e.

$$\mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a} = \bigoplus_{\ell} (\mathfrak{b}^{-1}\mathfrak{a} \otimes \mathbb{Z}_\ell)/(\mathfrak{a} \otimes \mathbb{Z}_\ell) = \bigoplus_{\ell} \mathfrak{b}_\ell^{-1}\mathfrak{a}_\ell/\mathfrak{a}_\ell. \tag{74}$$

Similarly we get

$$R/\mathfrak{b} = \bigoplus_{\ell} R_\ell/\mathfrak{b}_\ell. \tag{75}$$

Therefore it suffices to show that for any prime ℓ, we have $\mathfrak{b}_\ell^{-1}\mathfrak{a}_\ell/\mathfrak{a}_\ell \cong R_\ell/\mathfrak{b}_\ell$. As both $\mathfrak{a}$ and $\mathfrak{b}$ are invertible fractional R-ideals, by proposition 4.7 both $\mathfrak{a}_\ell$ and $\mathfrak{b}_\ell$ are principal fractional R_ℓ-ideals. Thus there exist $a_\ell, b_\ell \in R \otimes \mathbb{Q}_\ell$ such that $\mathfrak{a}_\ell = a_\ell R_\ell$ and $\mathfrak{b}_\ell = b_\ell R_\ell$. Therefore the map $x \mapsto a_\ell^{-1} b_\ell x$ defines an R-module isomorphism from $\mathfrak{b}_\ell^{-1}\mathfrak{a}_\ell/\mathfrak{a}_\ell$ to $R_\ell/\mathfrak{b}_\ell$. □

6.4 Module structure of torsion over finite fields

If we want to apply the same argument over $\mathbb{C}$ from proposition 6.4 to elliptic curves over finite fields, we run into two problems. Firstly, we lose the complex torus description $E \cong \mathbb{C}/\Lambda$. Secondly, we gain the possibility for $\mathrm{End}(E)$ to be an order in a quaternion algebra.

We will first tackle the second problem. If $\mathrm{End}(E)$ is an order in a quaternion algebra, then it is no longer commutative, and it has rank 4 as $\mathbb{Z}$-module. As $E[n]$ has rank 2 as $\mathbb{Z}/n\mathbb{Z}$-module, it can never be a free $\mathrm{End}(E)/n\,\mathrm{End}(E)$-module. However, our main interest is the action of the Frobenius π on $E[n]$, and therefore we can avoid this problem by always restricting to the commutative subring $R = \mathrm{End}(E) \cap \mathbb{Q}(\pi)$. This is again either $\mathbb{Z}$ or an order in a quadratic imaginary field L.

To solve the first problem, we will look at two possible solutions. The first one is the direction that Duke and T'oth take in [DT02]. Using work of Deuring with respect to reducing and lifting endomorphism, we can lift our curve to a curve over $\mathbb{C}$ with complex multiplication by R. Since we already proved our proposition in this case and the R-module structure is preserved under reduction, this also proves it in the finite field case.

The second solution is to repeat the argument locally, using the Tate modules to replace the lattice. For any prime ℓ, we will denote $R_\ell = R \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ and $L_\ell = L \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = R_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$.

Proposition 6.5. *Let E be a elliptic curve over a finite field $\mathbb{F}_q$ with Frobenius endomorphism $\pi \in \mathrm{End}(E)$. Suppose that the subring $R = \mathrm{End}(E) \cap \mathbb{Q}(\pi)$ is an*

order in an imaginary quadratic field $L = \mathbb{Q}(\pi)$. Then for any prime $\ell \neq p$, $V_\ell(E)$ is a free L_ℓ-module of rank 1. If we fix an isomorphism $V_\ell(E) \cong L_\ell$, then the image of $T_\ell(E)$ under this isomorphism is a proper fractional R_ℓ-ideal.

Proof. Let $\ell \neq p$ be a prime. The faithful R_ℓ-module structure on $T_\ell(E)$ extends naturally to a faithful L_ℓ-module structure on $V_\ell(E)$. If $V_\ell(E)$ is free as L_ℓ-module, then it has to be free of rank 1, as both L_ℓ and $V_\ell(E)$ have $\mathbb{Q}_\ell$-dimension 1.

Note that if $\chi_\pi \in \mathbb{Z}_\ell[X]$ stays irreducible over $\mathbb{Z}_\ell$, then $L_\ell \cong \mathbb{Q}_\ell[X]/(\chi_\pi)$ is a finite extension of $\mathbb{Q}_\ell$. In particular, as it is a field, any faithful L_ℓ-module is free.

If $\chi_\pi = (X-a)(X-b) \in \mathbb{Z}_\ell[X]$ splits over $\mathbb{Z}_\ell$, then $L_\ell \cong \mathbb{Q}_\ell[X]/(\chi_\pi) \cong \mathbb{Q}_\ell[X]/(X-a) \times \mathbb{Q}_\ell[X]/(X-b) \cong \mathbb{Q}_\ell \times \mathbb{Q}_\ell$. As we already know that $V_\ell(E) \cong \mathbb{Q}_\ell \oplus \mathbb{Q}_\ell$, we see that $V_\ell(E)$ is free as L_ℓ-module.

Now fix an isomorphism $V_\ell(E) \cong L_\ell$. We will identify $T_\ell(E)$ with its image under this isomorphism. Then by definition, $T_\ell(E)$ is a fractional R_ℓ-ideal. To show that $T_\ell(E)$ is proper, suppose $\phi \in L_\ell$ such that $\phi T_\ell(E) \subset T_\ell(E)$. As $\phi \in L_\ell$, there exists some integer $n \geq 0$ such that $\ell^n \phi \in R_\ell$. Now let $\psi \in R$ such that $\psi - \ell^n \phi \in \ell^n R_\ell$. Then $\ell^n \phi T_\ell(E) \subset \ell^n T_\ell(E)$ implies that $\psi T_\ell(E) \subset \ell^n T_\ell(E)$. Therefore, by proposition 5.5, $\psi = \ell^n \theta$ with $\theta \in R$. In particular we have $\theta \in R_\ell$ and $\theta - \phi \in R_\ell$. We conclude that $\phi \in R_\ell$ and thus $T_\ell(E)$ is indeed proper. □

Now that we again have reduced our problem to fractional ideals, we can just repeat the same argument we used over $\mathbb{C}$.

Proposition 6.6. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$ with Frobenius endomorphism $\pi \in \mathrm{End}(E)$ and let $R = \mathrm{End}(E) \cap \mathbb{Q}(\pi)$. Then for any invertible ideal $\mathfrak{b} \subset R$ with norm $N(\mathfrak{b})$ coprime to q, we have that $E[\mathfrak{b}]$ is a free $R/\mathfrak{b}$-module of rank $2/[R:\mathbb{Z}]$.*

Proof. The case $R = \mathbb{Z}$ is again trivial. Therefore suppose that R is an order in imaginary quadratic field L.

For any prime ℓ, denote $R_\ell = R \otimes \mathbb{Z}_\ell$. Using lemma 2.2, we have a decomposition of R-modules $E[\mathfrak{b}] = \bigoplus_\ell E[\mathfrak{b}]_\ell$ where each $E[\mathfrak{b}]_\ell = E[\mathfrak{b}] \otimes \mathbb{Z}_\ell = E[\mathfrak{b}] \cap E[\ell^\infty]$ is an R_ℓ-module. Therefore it is enough to show that for each prime ℓ, $E[\mathfrak{b}]_\ell$ is a free $R_\ell/\mathfrak{b}_\ell$-module of rank 1.

For $\ell \neq p$, identify $E[\mathfrak{b}]_\ell$ with its image under the R-module isomorphism $E[\ell^\infty] \cong V_\ell(E)/T_\ell(E)$ from proposition 2.3. As $V_\ell(E)$ is a free L_ℓ-module of rank 1, we can identify $V_\ell(E)$ with L_ℓ (non-canonically). Note that then both $\mathfrak{b}_\ell$ and $T_\ell(E)$ are invertible fractional R_ℓ-ideals, and we have

$$E[\mathfrak{b}]_\ell = (T_\ell(E) : \mathfrak{b}_\ell)/T_\ell(E) = \mathfrak{b}_\ell^{-1} T_\ell(E)/T_\ell(E). \tag{76}$$

However, as $\mathfrak{b}_\ell$ and $T_\ell(E)$ are invertible and thus principal (R_ℓ Gorenstein and ℓ-adically complete), we have that $\mathfrak{b}_\ell = b_\ell R_\ell$ and $T_\ell(E) = a_\ell R_\ell$. Then the map $x \mapsto b_\ell a_\ell^{-1}$ defines an R_ℓ-module isomorphism $E[\mathfrak{b}]_\ell \to R_\ell/\mathfrak{b}_\ell$.

For $\ell = p$, we claim that $E[\mathfrak{b}]_p = R_\ell/\mathfrak{b}_\ell = 0$. First we note that $\mathfrak{b}$ contains an element ϕ with norm $N_{R/\mathbb{Z}}(\phi)$ not divisible by p. As there exists $\psi \in R$ such that $\phi\psi = N_{R/\mathbb{Z}}(\phi)$, we see that ϕ is a unit in R_ℓ. Therefore $\mathfrak{b}_\ell = R_\ell$ and thus $R_\ell/\mathfrak{b}_\ell = 0$. Furthermore, as $\deg(\phi) = N_{R/\mathbb{Z}}(\phi)$, we see that ϕ does not contain a non-zero ℓ-power torsion point in its kernel. Thus $E[\mathfrak{b}]_\ell \subset E[\phi]_\ell = E[\phi] \cap E[\ell^\infty] = 0$. □

Proposition 6.2 now follows directly, and thus this concludes our alternative proof of the proposition by Duke and Tóth.

6.5 Some examples

Now that we know how to determine the representative of the Frobenius, let us go through some examples.

Example 6.7. Consider the elliptic curves over $\mathbb{Q}$ given by

$$E_1 \colon y^2 = x^3 + x + 1, \quad E_2 \colon y^3 = x^3 + 3x. \tag{77}$$

In table 3, we have determined for both curves the representative matrices for all primes $p < 50$ of good reduction. This done by calculating the characteristic polynomial of Frobenius π of the reduced curve E_p and then applying the methods from section **??** to find the discriminant Δ_p of the ring $R_p = \mathrm{End}(E_p) \cap \mathbb{Q}(\pi)$. Using this we can calculate the representative M_p from proposition 6.3.

If one studies table 3 for a while, one will start notice that the table for E_2 is much more repetitive than the table for E_1. This is because E_2 has complex multiplication, while E_1 does not. In particular E_2 has CM by $\mathbb{Z}[i]$ and therefore by proposition 5.7, it has ordinary reduction whenever p splits in $\mathbb{Z}[i]$, and in this case $R_p = \mathbb{Z}[i]$ (i.e. $\Delta_p = -4$). It is well-known that p splits in $\mathbb{Z}[i]$ exactly when $p \equiv 1 \mod 4$. When $p \equiv 3 \mod 4$, we have supersingular reduction and we can use lemma 5.12 to determine Δ_p. We see that $\Delta_p = -p$ when $x^3 + 3x = x(x^2 + 3)$ splits completely over $\mathbb{F}_p$. This happens exactly when -3 is a square mod p, or equivalently (by quadratic reciprocity) when $p \equiv 1 \mod 3$. Otherwise, if $p \equiv -1 \mod 3$, then $\Delta_p = -4p$.

p	Reduction	χ_π	Δ_π	Δ_p	a_p	b_p	M_p
3	Sup.	X^2-3X+3	-3	-3	3	1	$\left(\begin{smallmatrix}1 & -1\\ 1 & 2\end{smallmatrix}\right)$
7	Sup.	X^2+7	-28	-28	0	1	$\left(\begin{smallmatrix}0 & -7\\ 1 & 0\end{smallmatrix}\right)$
11	Ord.	$X^2+5X+11$	-19	-19	-5	1	$\left(\begin{smallmatrix}-3 & -5\\ 1 & -2\end{smallmatrix}\right)$
13	Ord.	$X^2+2X+13$	-48	-12	-2	2	$\left(\begin{smallmatrix}-1 & -6\\ 2 & -1\end{smallmatrix}\right)$
17	Ord.	$X^2-6X+17$	-32	-32	6	1	$\left(\begin{smallmatrix}3 & -8\\ 1 & 3\end{smallmatrix}\right)$
19	Ord.	$X^2-2X+19$	-72	-8	2	3	$\left(\begin{smallmatrix}1 & -6\\ 3 & 1\end{smallmatrix}\right)$
23	Ord.	$X^2+3X+23$	-83	-83	-3	1	$\left(\begin{smallmatrix}-2 & -21\\ 1 & -1\end{smallmatrix}\right)$
29	Ord.	$X^2-10X+29$	-16	-16	10	1	$\left(\begin{smallmatrix}5 & -4\\ 1 & 5\end{smallmatrix}\right)$
31	Ord.	$X^2-7X+31$	-75	-75	7	1	$\left(\begin{smallmatrix}3 & -19\\ 1 & 4\end{smallmatrix}\right)$
37	Ord.	$X^2-4X+37$	-132	-132	4	1	$\left(\begin{smallmatrix}2 & -33\\ 1 & 2\end{smallmatrix}\right)$
41	Ord.	$X^2+7X+41$	-115	-115	-7	1	$\left(\begin{smallmatrix}-4 & -29\\ 1 & -3\end{smallmatrix}\right)$
43	Ord.	$X^2+9X+43$	-91	-91	-9	1	$\left(\begin{smallmatrix}-5 & -23\\ 1 & -4\end{smallmatrix}\right)$
47	Sup.	X^2+47	-188	-47	0	2	$\left(\begin{smallmatrix}-1 & -24\\ 2 & 1\end{smallmatrix}\right)$

(a) $E_1\colon y^2 = x^3 + 2x - 7$

p	Reduction	χ_π	Δ_π	Δ_p	a_p	b_p	M_p
5	Ord.	X^2+4X+5	-4	-4	-4	1	$\left(\begin{smallmatrix}-2 & -1\\ 1 & -2\end{smallmatrix}\right)$
7	Sup.	X^2+7	-28	-7	0	2	$\left(\begin{smallmatrix}-1 & -4\\ 2 & 1\end{smallmatrix}\right)$
11	Sup.	X^2+11	-44	-44	0	1	$\left(\begin{smallmatrix}0 & -11\\ 1 & 0\end{smallmatrix}\right)$
13	Ord.	$X^2+6X+13$	-16	-4	-6	2	$\left(\begin{smallmatrix}-3 & -2\\ 2 & -3\end{smallmatrix}\right)$
17	Ord.	$X^2+8X+17$	-4	-4	-8	1	$\left(\begin{smallmatrix}-4 & -1\\ 1 & -4\end{smallmatrix}\right)$
19	Sup.	X^2+19	-76	-19	0	2	$\left(\begin{smallmatrix}-1 & -10\\ 2 & 1\end{smallmatrix}\right)$
23	Sup.	X^2+23	-92	-92	0	1	$\left(\begin{smallmatrix}0 & -23\\ 1 & 0\end{smallmatrix}\right)$
29	Ord.	$X^2-4X+29$	-100	-4	4	5	$\left(\begin{smallmatrix}2 & -5\\ 5 & 2\end{smallmatrix}\right)$
31	Sup.	X^2+31	-124	-31	0	2	$\left(\begin{smallmatrix}-1 & -16\\ 2 & 1\end{smallmatrix}\right)$
37	Ord.	$X^2+2X+37$	-144	-4	-2	6	$\left(\begin{smallmatrix}-1 & -6\\ 6 & -1\end{smallmatrix}\right)$
41	Ord.	$X^2-8X+41$	-100	-4	8	5	$\left(\begin{smallmatrix}4 & -5\\ 5 & 4\end{smallmatrix}\right)$
43	Sup.	X^2+43	-172	-43	0	2	$\left(\begin{smallmatrix}-1 & -22\\ 2 & 1\end{smallmatrix}\right)$
47	Sup.	X^2+47	-188	-188	0	1	$\left(\begin{smallmatrix}0 & -47\\ 1 & 0\end{smallmatrix}\right)$

(b) $E_2\colon y^2 = x^3 + 3x$

Table 3: Calculating a representative M_p of the Frobenius for primes $p < 50$ of good reduction for the curves E_1 and E_2 over $\mathbb{Q}$.

Part III
Unramified primes: abelian varieties

7 Abelian varieties

In this section we will introduce the basic concepts of abelian varieties needed in order to generalize the results of section 6. We mostly follow [MvdGE] and [Mil08].

7.1 Definition and examples

Definition 7.1. An abelian variety A is a projective variety that is also an abelian group, such that the group operations are morphisms (of varieties).

We will restrict ourselves to a couple classes of examples:

- Elliptic curves are abelian varieties. These all have dimension 1, and every abelian variety of dimension 1 is an elliptic curve.
- More generally, Jacobians of curves are varieties.
- Finite produts of abelian varieties are again abelian varieties.

Example 7.2. Let K be a field and consider the hyperelliptic curve $C\colon y^2 = f(x)$, with $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in K[x]$ separable of degree d. Then the genus g of C is equal to $g = (d-1)/2$ if d odd and $g = (d-2)/2$ if d even. The Jacobian $J(C)$ is defined as the quotient $\mathrm{Div}^0(C)/\mathcal{P}(C)$, where $\mathrm{Div}(C)$ is the set of divisors of zero degree and $\mathcal{P}$ is the set of principal divisors, which is the set of divisors that can be given by the divisor of some function in the function field of C. Then the Jacobian $J(C)$ is a abelian variety of dimension g.

An abelian variety A is called simple if it contains no sub-abelian variety B not equal to 0 or A itself. For example, any elliptic curve is simple. Simpleness is preserved under isogeny, and any abelian variety A is uniquely isogenous (up to isogeny) to a product of simple abelian varieties. In other words,

$$A \sim A_1^{e_1} \times \cdots \times A_r^{e_r}, \tag{78}$$

where the A_i are abelian varieties uniquely determined up to isogeny.

7.2 Torsion points

If A is an abelian variety of dimension g over a field K, then we can again consider the n-torsion subgroup

$$A[n] = \{P \in A(\overline{K}) \colon nP = O\}. \tag{79}$$

When $\mathrm{char}(K) = 0$ or n is coprime to $p = \mathrm{char}(K) > 0$, we have

$$A[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}. \tag{80}$$

If $p = \mathrm{char}(K) > 0$, then there exists $0 \leq k \leq g$ such that for all $n \geq 1$,

$$A[p^n] \cong (\mathbb{Z}/p^n\mathbb{Z})^k. \tag{81}$$

Similarly as in the elliptic curve case, we can define the Tate modules

$$T_\ell(A) = \varprojlim_n A[\ell^n], \quad V_\ell(A) = T_\ell(A) \otimes \mathbb{Q}_\ell, \tag{82}$$

which, for $\ell \neq p$, are free or rank $2g$ as $\mathbb{Z}_\ell$-modules resp. $\mathbb{Q}_\ell$-vector spaces. These Tate modules can again be used to describe ℓ-power torsion, using the isomorphism

$$A[\ell^\infty] \cong V_\ell(A)/T_\ell(A). \tag{83}$$

Example 7.3. Let C/K be hyperelliptic curve given by $C \colon y^2 = f(x)$, with $d = \deg(f)$ odd. Let $J = J(C)$ denote its Jacobian, which is an abelian variety of dimension $g = (d-1)/2$. Let $\alpha_1, \ldots, \alpha_d \in \overline{K}$ be the roots of f, and denote $D_i = (\alpha_i, 0) - \infty$, where ∞ is the unique point at infinity. Then by [Cor01, 2.1], $J[2]$ is generated by $D_1, \ldots, D_{d-1}$ as $\mathbb{F}_2$-vector space.

7.3 Endomorphisms

Most of results about endomorphisms of elliptic curves hold for abelian varieties as well, given one replaces 2 by $2g$ here and there. For instance, any isogeny $\phi \in \mathrm{End}(A)$ satisfies a characteristic polynomial χ_ϕ of degree $2g$, and any commutative subring R of the endomorphism ring $\mathrm{End}(A)$ is an order of rank $[R : \mathbb{Z}]$ dividing $2g$.

However, when A is not simple, one has to be careful as not every non-zero endomorphism is an isogeny, therefore does not have finite kernel. Luckily we have a similar proposition as proposition 5.5.

Proposition 7.4. *Let A be an abelian variety over a field K with $p = \mathrm{char}(K) \geq 0$. Denote its endomorphism ring by $R = \mathrm{End}(A)$.*

(a) *For any integer n coprime to p, and any endomorphism $\phi \in \mathrm{End}(A)$, we have that $\frac{1}{n}\phi \in \mathrm{End}(A)$ if and only if $A[n] \subset \ker \phi$.*

(b) *For any prime $\ell \neq p$, any integer $n \geq 1$, and any endomorphism $\phi \in \mathrm{End}(A)$, we have that $\frac{1}{\ell^n}\phi \in \mathrm{End}(A)$ if and only if ϕ maps $T_\ell(A)$ into $\ell^n T_\ell(A)$.*

Proof. Repeat the argument from proposition 5.5, however now instead of using the lemma one has to show that we can divide out seperable isogenies using group scheme quotients (see [MvdGE, Ch. 4]). □

8 Representative of the Frobenius

In this section we will try to generalize the results from section 6 to abelian varieties to find a representative of the Frobenius for unramified primes.

Explicitly, if A is an abelian variety of dimension g over a number field K and $\mathfrak{p}$ is a prime of K of good reduction, then for any integer $n \geq 1$ not divisible by $\mathfrak{p}$ we have that $\mathfrak{p}$ is unramified in the division field $K(A[n])$. In this case we are interested in finding a representative for the $\mathrm{GL}_{2g}(\mathbb{Z}/n\mathbb{Z})$-similarity class of the Frobenius in the Galois group $G_n = G_{K(A[n])/K}$, when considered under the map

$$\overline{\rho}_n \colon G_n \to \mathrm{Aut}(A[n]) \cong \mathrm{GL}_{2g}(\mathbb{Z}/n\mathbb{Z}). \tag{84}$$

Just as in the elliptic curve case, this is equivalent to finding a representative of the action of the Frobenius endomorphism $\pi \in \mathrm{End}(A_{\mathfrak{p}})$ of the reduced variety on $A_{\mathfrak{p}}[n]$.

In the case where E is an elliptic curve over a finite field $\mathbb{F}_q$, we showed that the action of $\pi \in \mathrm{End}(E)$ on $E[n]$ for $n \geq 1$ coprime to q only depends on how π lies in the ring $R = \mathrm{End}(E)$. We proved this by showing that for any prime ℓ coprime to q, the Tate module $T_\ell(E)$ can be viewed as a principal $R_\ell = R \otimes \mathbb{Z}_\ell$-module, which in particular implied that as R-modules,

$$E[n] \cong \bigoplus_\ell T_\ell(E)/nT_\ell(E) \cong \bigoplus_\ell R_\ell/nR_\ell \cong R/nR. \tag{85}$$

After choosing an integral basis for R and writing multiplication-by-π acting on this basis as a matrix $M_\pi \in \mathrm{GL}_2(\mathbb{Z})$, the matrix $M_\pi \mod n \in \mathrm{GL}_2(Z/n\mathbb{Z})$ represents the action of π on R/nR and thus also on $E[n]$, which gives us the desired representative.

Trying to do something similar for abelian varieties runs into a couple of problems. In the elliptic curve case our ring R was at most quadratic. Therefore it is always Gorenstein (and even Bass), which means that every proper fractional $R \otimes \mathbb{Z}_\ell$-ideal is principal, which is a key argument for our proof. Secondly, the rank of R over Z is always equal to one of the extremes: the rank is equal to 1 or to $2 = 2g$. For abelian varieties more cases show up, which introduce difficulties.

8.1 Frobenius algebra $\mathbb{Q}[\pi]$

Let A be an abelian variety of dimension g over a finite field $\mathbb{F}_q$. Consider the Frobenius endomorphism $\pi \in \mathrm{End}(E)$ with characteristic polynomial $\chi_\pi \in \mathbb{Z}[X]$ of degree $2g$.

We can then consider the finite-dimensional $\mathbb{Q}$-algebra $\mathbb{Q}[\pi]$. Remarkably, this is always a separable algebra, as we can "ignore" repeated factors in χ_π, as shown in the following proposition.

Proposition 8.1. *Let A be an abelian variety over a finite $\mathbb{F}_q$ of dimension g. Let $\pi \in \mathrm{End}(A)$ denote the Frobenius endomorphism, with characteristic polynomial $\chi_\pi = f_1^{e_1} \dots f_r^{e_r} \in \mathbb{Z}[X]$ such that all the $f_i \in Z[X]$ are square-free and have no common factors.*

(a) *Then $\mathbb{Q}[\pi] = L_1 \times \cdots \times L_r$ where each $L_i \cong \mathbb{Q}[X]/(f_i)$.*

(b) *Furthermore, for each prime $\ell \neq p$, we have a corresponding decomposition $V_\ell(A) = V_1 \oplus \cdots \oplus V_r$, where each V_i is free of rank e_i as $L_{i,\ell}$-module.*

Proof. (a) We claim that the minimal polynomial m_π of π is equal to $f_1 \dots f_r$. Note that A is isogenous over $\mathbb{F}_q$ to a product of simple abelian varieties, i.e. we have an isogeny

$$\psi \colon A \to B = A_1^{c_1} \times \cdots \times A_r^{c_r},$$

where for all i we have that A_i is simple with Frobenius π_i and $\chi_{\pi_i} = f_i^{e_i/c_i}$. As ψ is an isogeny, there exists an isogeny $\hat{\psi} \colon B \to A$ such that $\hat{\psi} \circ \psi = [\deg(\psi)]_A$ and $\psi \circ \hat{\psi} = [\deg(\psi)]_B$. Therefore ψ induces a ring homomorphism

$$\psi' \colon \mathrm{End}(A) \otimes \mathbb{Q} \to \mathrm{End}(B) \otimes \mathbb{Q}, \quad \theta \mapsto \frac{1}{\deg(\psi)} \psi \circ \theta \circ \hat{\psi}.$$

Note that ψ' has inverse $\hat{\psi}'$ and thus is an isomorphism. As ψ is defined over $\mathbb{F}_q$ it commutes the Frobenius, i.e. $\psi \circ \pi_A = \pi_B \circ \psi$. Then $\psi'(\pi_A) = \pi_B$. Thus the minimal polynomial of π_A is equal to the minimal polynomial of π_B.

Note that the minimal polynomial of the Frobenius on B is the least common multiple of the minimal polynomials of Frobenius on $A_i^{c_i}$. However, the minimal polynomial of Frobenius on $A_i^{c_i}$ is the same as the minimal polynomial on A_i which is equal to f_i. Thus $m_{\pi_A} = m_{\pi_B} = \mathrm{lcm}(f_1, \dots, f_r) = f_1 \dots f_r$.

(b) We generalize the first part of proposition 6.5. As $\mathbb{Q}[\pi] = L_1 \times \cdots \times Ł_r$, we have that $\mathbb{Q}[\pi]_\ell = L_{1,\ell} \times \cdots \times L_{r,\ell}$. As $V_\ell(A)$ is a faithful $\mathbb{Q}[\pi]_\ell$-module, there is a corresponding decomposition $V_\ell(A) = V_1 \oplus \cdots \oplus V_r$ where each V_i is a faithful $L_{i,\ell}$-module. Now fix i, and let $f_i = g_{i1} \dots g_{is} \in \mathbb{Z}_\ell[X]$ with each $g_{ij} \in \mathbb{Z}_\ell[X]$ irreducible. Then $L_{i,\ell} = M_1 \times \cdots \times M_s$ where each $M_j = \mathbb{Q}_\ell[X]/(g_{ij})$ is a field. Again, we get a corresponding decomposition $V_i = V_{i1} \oplus \cdots \oplus V_{is}$ such that each V_{ij} is a faithful

M_j-vector space. Let $d_{ij} = \dim_{M_j}(V_{ij})$. Note that the characteristic polynomial of π acting on V_{ij} is equal to $\chi_{V_{ij}} = g_{ij}^{d_{ij}}$. Then,

$$\chi_\pi = \prod_{i,j} \chi_{V_{ij}} = \prod_{i,j} g^{d_{ij}}, \tag{86}$$

which implies that $d_{ij} = e_i$. Therefore,

$$V_i \cong M_1^{e_i} \oplus \cdots \oplus M_s^{e_i} \cong L_{i,\ell}^{e_i}. \tag{87}$$

□

Using this decomposition we can try to tackle the problem of determining the R_ℓ-module structure of $T_\ell(A)$.

8.2 Characteristic polynomial is square-free

First we will consider the case where the characteristic polynomial χ_π of the Frobenius is square-free. Then for any prime $\ell \neq p$, we can apply proposition 8.1 with $r = 1$, $f_1 = \chi_\pi$ and $e_1 = 1$ to find that $V_\ell(A) \cong \mathbb{Q}[\pi]_\ell$. This allows us to obtain a fractional ideal description for $T_\ell(A)$.

Proposition 8.2. *Let A be an abelian variety of dimension g over a finite field $\mathbb{F}_q$ with Frobenius endomorphism $\pi \in \mathrm{End}(A)$. Suppose that the characteristic polynomial χ_π of the Frobenius is square-free, and let $R = \mathrm{End}(A) \cap \mathbb{Q}[\pi]$. Let $\ell \neq p$ be a prime and fix an isomorphism $V_\ell(A) \cong \mathbb{Q}[\pi]_\ell$. Then the image of $T_\ell(A)$ under this isomorphism is a proper fractional R_ℓ-ideal.*

Proof. To prove that $T_\ell(A)$ is a proper fractional R_ℓ-idea, copy the argument from proposition 6.5, replacing proposition 5.5 by proposition 7.4. □

For elliptic curves the next step of the argument would be to so show that every proper fractional R_ℓ-ideal is principal, and then for any invertible ideal $\mathfrak{b} \subset R$, we have that $E[\mathfrak{b}]_\ell \cong \mathfrak{b}_\ell^{-1} T_\ell(E)/T_\ell(E) \cong R_\ell/\mathfrak{b}_\ell$. However, for abelian varieties, R_ℓ is not necessarily Gorenstein, so we cannot repeat this argument. However, we can show that the structure of $A[\mathfrak{b}]_\ell$ depends only the ideal class $[T_\ell(X)] \in \mathrm{ICP}(R_\ell)$. Clearly, if $[\mathfrak{a}] = [T_\ell(A)]$, then there exists an $a \in \mathbb{Q}[\pi]_\ell$ such that $a\mathfrak{a} = T_\ell(A)$. In particular, if we write $\mathfrak{b}_\ell = bR_\ell$, then multiplication by ab^{-1} gives an isomorphism $\mathfrak{b}_\ell^1 T_\ell(A)/T_\ell(A) \cong \mathfrak{a}/\mathfrak{b}_\ell\mathfrak{a}$.

This leads to the following proposition:

Proposition 8.3. *Let A be an abelian variety of dimension g over a finite field $\mathbb{F}_q$ with Frobenius endomorphism $\pi \in \mathrm{End}(A)$. Suppose that the characteristic polynomial χ_π of the Frobenius is square-free, and let $R = \mathrm{End}(A) \cap \mathbb{Q}[\pi]$. Let $\mathfrak{b} \subset R$ be an invertible ideal with norm coprime to p, and suppose that $\mathfrak{a}$ be a fractional R-ideal such that $\mathfrak{a}_\ell$ and $T_\ell(A)$ are in the same fractional R_ℓ-ideal class for any prime ℓ dividing $N(\mathfrak{b})$. Then $A[\mathfrak{b}] \cong R/\mathfrak{a}$ as R-modules. In particular, if R is Gorenstein then $A[\mathfrak{b}] \cong R/\mathfrak{b}$.*

8.3 Characteristic polynomial is power of square-free

If $\chi_\pi = f^e \in \mathbb{Z}[X]$, where $f \in \mathbb{Z}[X]$ is square-free and $e > 1$, then by proposition 8.1 we have that $V_\ell(A) \cong (\mathbb{Q}[\pi]_\ell)^e$ for all $\ell \neq p$. Under this isomorphism we can identify $T_\ell(A)$ as an R-submodule of $(\mathbb{Q}[\pi]_\ell)^e$.

In general it is even a hard problem to classify such submodules, however when R is Bass ℓ-adically, such a classification is given by proposition 4.14. In this case,

$$T_\ell(A) \cong R_\ell \oplus S_2 \oplus \cdots \oplus S_e, \tag{88}$$

where $R_\ell \subset S_2 \subset \cdots \subset \mathcal{O}_{\mathbb{Q}[\pi]_\ell}$ are over-orders of R_ℓ.

Then for any invertible ideal $\mathfrak{b}$ with norm coprime to p, we find that $A[\mathfrak{b}]_\ell = T_\ell(A)/\mathfrak{b}T_\ell(A) \cong R_\ell/\mathfrak{b}_\ell \oplus \cdots \oplus S_e/\mathfrak{b}_\ell S_e$. Therefore we get the proposition:

Proposition 8.4. *Let A be an abelian variety of dimension g over a finite field $\mathbb{F}_q$ with Frobenius endomorphism $\pi \in \mathrm{End}(A)$. Suppose that the characteristic polynomial χ_π of the Frobenius is the power of a square-free polynomial. Let Σ be a set of primes ℓ such that R_ℓ is Bass.*

(a) *Then there exists over-orders $R \subset S_2 \subset \cdots \subset S_e \subset \mathcal{O}_{\mathbb{Q}(\pi)}$ such that for all primes $\ell \in \Sigma$, $T_\ell(A) \cong R_\ell \oplus S_{2,\ell} \oplus \cdots \oplus S_{e,\ell}$.*

(b) *Let $\mathfrak{b} \subset R$ be an invertible ideal with norm $N(\mathfrak{b})$ coprime to p such that all prime divisors $N(B)$ lie in Σ. Then $A[\mathfrak{b}] \cong R/\mathfrak{b} \oplus S_2/\mathfrak{b}S_2 \oplus \cdots \oplus S_e/\mathfrak{b}S_e$.*

(c) *In particular, if R is maximal of for all primes in Σ, then $T_\ell(A) \cong R_\ell^e$ and for any $\mathfrak{b}$ as in part (b) we have $A[\mathfrak{b}] = (R/\mathfrak{b})^e$.*

8.4 General case

In the general case where $\chi_\pi = f_1^{e_1} \dots f_r^{e_r}$, where the $f_i \in \mathbb{Z}[X]$ are square-free with no common factors, and the e_i are distinct, we get a decomposition $\mathbb{Q}[\pi] = L_1 \times \cdots \times L_r$

with $L_i \cong \mathbb{Q}[X]/(f_i)$ and a corresponding decomposition $V_\ell(A) = V_1 \oplus \cdots \oplus V_r$, as per proposition 8.1. It is quite hard to say anything about the structure of $T_\ell(A)$, even when considered as R_ℓ-submodule of $L_{1,\ell}^{e_1} \oplus \cdots \oplus L_{r,\ell}^{e_r}$.

However, if R_ℓ permits a decomposition

$$R_\ell = R_1 \times \cdots \times R_r, \tag{89}$$

with each R_i an order in $L_{i,\ell}$, then we get a corresponding decomposition

$$T_\ell(A) = T_1 \oplus \cdots \oplus T_r, \tag{90}$$

where each T_i is a R_i-submodule of $V_i \cong L_{i,\ell}^{e_i}$. We can then try to find the R_i-module structure of each T_i using the previous cases.

In particular, using resultants (see [GKZ08]), this is possible for the following primes:

Lemma 8.5. *Let $\ell \neq p$ be a prime such that ℓ does not divide any of the pairwise resultants $R(f_i, f_j)$ with $i \neq j$. Then $R_\ell = R_1 \times \ldots R_r$, where each R_i is the projection of R_ℓ to $L_{i,\ell}$.*

Proof. Note that ℓ not dividing the resultants $R(f_i, f_j)$ means that the ideals $f_i\mathbb{Z}_\ell[X]$ are all pairwise comaximal. Therefore

$$(\mathbb{Z}[\pi])_\ell \cong \mathbb{Z}_\ell[X]/(f_1 \ldots f_r) \cong \mathbb{Z}_\ell[X]/(f_1) \times \mathbb{Z}_\ell[X]/(f_r). \tag{91}$$

In particular as $(\mathbb{Z}[\pi])_\ell \subset R_\ell$, we see that R_ℓ contains all basis vectors $v_i \in L_{i,1} \times \cdots \times L_{r,\ell}$. The projection R_i of R_ℓ to $L_{i,\ell}$ is then given by $R_i = v_i R_\ell \subset R_\ell$. Therefore $R_1 \times \cdots \times R_r \subset R_\ell$. As the other inclusion is trivial, we indeed get the required decomposition. □

8.5 An example

Let us now look at an example.

Example 8.6. Consider the hyperelliptic curve C over $\mathbb{Q}$ given by $C\colon y^2 = x^5 + 1$, with Jacobian $J = J(C)$. Note that $\mathrm{End}_{\overline{Q}}(J) = \mathbb{Z}[\zeta_5]$, with

$$[\zeta_5]\colon J \to J, \quad (x, y) \mapsto (\zeta_5 x, y). \tag{92}$$

Therefore we are in the complex multiplication case (here meaning $[\mathrm{End}_{\overline{Q}}(J) : \mathbb{Z}] = 2g = 4$), and we would like to expect similar results as in the CM case for elliptic

curves. See table 4 for the characteristic polynomial of the Frobenius $\pi \in \mathrm{End}(J_p)$ for primes $p < 32$ of good reduction. As in the elliptic curves case, we would like to find a matrix M_p such that $M_p \mod n$ represents the action of π on $J[n]$ for all n coprime to p.

When $p \equiv 1 \mod 5$, then p splits completely in $\mathbb{Z}[\zeta_5]$, and the corresponding reduced abelian variety J_p is ordinary. In particular, by a reduction of endomorphisms argument, $\mathrm{End}(J_p) = \mathbb{Z}[\zeta_5]$. Therefore for $p = 11$, $\chi_\pi = x^4 - 4x^3 + 6x^2 - 44x + 121$, which has discriminant $\Delta_\pi = 61952000$. As expected, $\mathbb{Z}[\pi]$ is an order in $L = \mathbb{Q}(\zeta_5)$. Since $\mathcal{O}_L = \mathbb{Z}[\zeta_5]$, which has discriminant $\Delta_L = 125$, we have $[\mathbb{Z}[\pi] : \mathcal{O}_L] = \sqrt{\Delta_\pi/\Delta_L} = 704$. Similar holds for $p = 31$, with $[\mathbb{Z}[\pi] : \mathcal{O}_L] = 21824$. Using SageMath, for $p = 11$ and $p = 31$ we can calculate the action of π on an integral basis of $\mathbb{Z}[\zeta_5]$, which gives

$$M_{11} = \begin{pmatrix} -385 & -286 & -484 & -968 \\ 968 & 715 & 1210 & 2420 \\ -402 & -296 & -501 & -1002 \\ 70 & 52 & 88 & 175 \end{pmatrix}, \quad M_{31} = \begin{pmatrix} -3875 & -62062 & -42284 & -84568 \\ 3348 & 53599 & 36518 & 73036 \\ 1578 & 25276 & 17221 & 34442 \\ -3068 & -49126 & -33470 & -66941 \end{pmatrix}.$$

From the table, it appears that when $p \equiv 2, 3 \mod 5$, then $\chi_\pi = X^4 + p^2$. As then $\Delta_\pi = 2^8 p^6$, we see that $\mathbb{Z}[\pi]$ is maximal outside 2 and p. Using SageMath one can calculate that for such primes in table 4, $\mathcal{O}_{\mathbb{Q}(\pi)} = \mathbb{Z}[\pi, \frac{1}{p}\pi^2]$ and that $\mathbb{Z}[\pi]$ is therefore maximal outside p. In particular this means that for any prime $\ell \neq p$, $\mathrm{End}(J) \otimes_Z \mathbb{Z}_\ell = \mathbb{Z}[\pi] \otimes_{\mathbb{Z}} \mathbb{Z}_\ell = \mathcal{O}_{\mathbb{Q}(\pi)} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$, which is maximal in $\mathbb{Q}(\pi)_\ell$, and thus for any integer n coprime to p, we have $J[n] = \mathbb{Z}[\pi]/n\mathbb{Z}[\pi]$. Therefore we can take M_p to be the matrix associated with π acting on the basis $1, \pi, \pi^2, \pi^3$, i.e.

$$M_p = \begin{pmatrix} 0 & 0 & 0 & -p^2 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{93}$$

For primes $p \equiv 4 \mod 5$, from the table it appears that $\chi_\pi = (x^2 + p)^2$. Then $\mathbb{Z}[\pi] = \mathbb{Z}[x]/(x^2 + p)$, which is quadratic and therefore Bass, with discriminant $-4p$. Then if $p \not\equiv 3 \mod 4$, we see that $\mathbb{Z}[\pi]$ has to be maximal and thus we know by proposition 8.4 that $J[n] \cong (\mathbb{Z}[\pi]/n\mathbb{Z}[\pi])^2$ for all n coprimes to p. Else if $p \equiv 3 \mod 4$, then there are $S_1, S_2 \in \{\mathbb{Z}[\pi], \mathbb{Z}[\frac{1+\pi}{2}]\}$ such that $J[n] \cong S_1/nS_1 \oplus S_2/nS_2$. However, suppose that $S_1 = \mathbb{Z}[\frac{1+\pi}{2}]$. Then π fixes the 2 dimensional $\mathbb{F}_2$-subspace of $J[2]$ corresponding to $S_1/2S_1$. However, using example 7.3, one can compute that the eigenspace corresponding to the eigenvector 1 of π on $J[2]$ is spanned by $D_1 =$

p	$p \mod 5$	χ_π	factorization χ_π
3	3	x^4+9	(x^4+9)
7	2	x^4+49	(x^4+49)
11	1	$x^4-4x^3+6x^2-44x+121$	$(x^4-4x^3+6x^2-44x+121)$
13	3	x^4+169	(x^4+169)
17	2	x^4+289	(x^4+289)
19	4	x^4+38x^2+361	$(x^2+19)^2$
23	3	x^4+529	(x^4+529)
29	4	x^4+58x^2+841	$(x^2+29)^2$
31	1	$x^4-4x^3+46x^2-124x+961$	$(x^4-4x^3+46x^2-124x+961)$

Table 4: Factorization of the characteristic polynomial χ_π of the Frobenius $\pi \in \mathrm{End}(J_p)$ for the reduction J_p for primes $p < 32$ of good reduction of the Jacobian $J = J(C)$ of the hyperelliptic curve $C/\mathbb{Q}\colon y^2 = x^5 + 1$.

$(1,0) - \infty$, and therefore is one-dimensional. Therefore we see that $S_1 = S_2 = \mathbb{Z}[\pi]$ and we can take M_p to be the matrix associated to the action of π on the basis $(1,0), (\pi,0), (0,1), (0,\pi)$ of $\mathbb{Z}[\pi] \oplus \mathbb{Z}[\pi]$, i.e.

$$M_p = \begin{pmatrix} 0 & -p & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -p \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{94}$$

Part IV
Ramified primes: elliptic curves

9 Newton polygons

In this section we will discuss a technique from p-adic analysis used to study the p-adic valuation of the roots of a polynomial or power series. We will mostly follow [Gou97].

9.1 Newton polygons for polynomials

Let K be a finite extension of $\mathbb{Q}_p$. Then there is a unique extension of the p-adic valuation of $\mathbb{Q}_p$ to K, which we will denote by v_p.

Given a non-zero polynomial $f = a_0 + a_1 X + \cdots + a_n X^n \in K[X]$, we can consider the set of points

$$\{(i, v_p(a_i)) \in \mathbb{R}^2 \colon i \geq 0, a_i \neq 0\}. \tag{95}$$

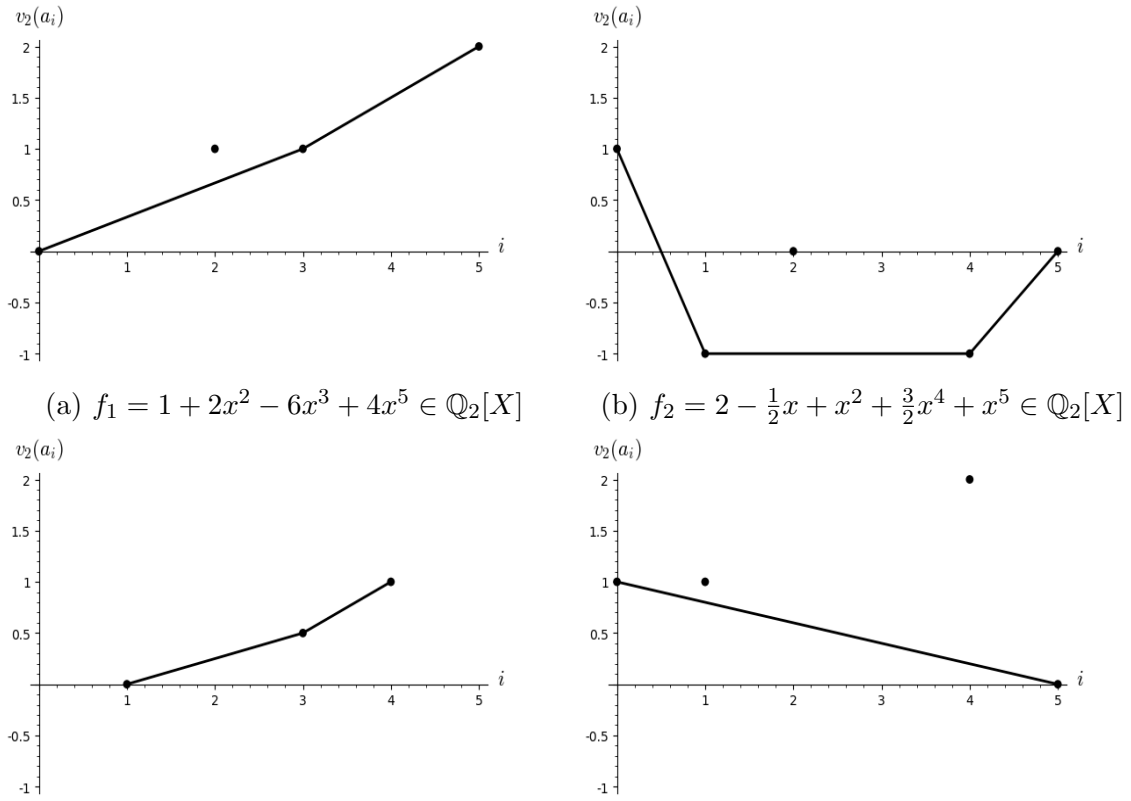
From this set of points we can construct the Newton polygon of f as the lower convex hull of this set of points. The lower convex hull is the set of line segments constructed as follows:

- Start with the smallest index i such that $a_i \neq 0$, which we denote by i_0.
- Given i_{j-1}, let i_j be the largest index greater than i_{j-1} such that $a_{i_j} \neq 0$ and the slope of the line segment L_j from $(i_{j-1}, v_p(a_{i_{j-1}}))$ to $(i_j, v_p(a_{i_j}))$ is minimal, i.e.
$$i_j = \operatorname*{argmin}_{\substack{i > i_{j-1}, \\ a_i \neq 0}} \frac{v_p(a_i) - v_p(a_{i_{j-1}})}{i - i_{j-1}}. \tag{96}$$
Add this line segment L_j to the Newton polygon of f.
- Terminate when i_j is the largest index such that $a_{i_j} = 0$.

For examples, see figure 2.

Given each line segment L_j in the Newton polygon of f, we consider can consider its slope s_j and length l_j, given by

$$s_j = \frac{v_p(a_{i_j}) - v_p(a_{i_{j-1}})}{i_j - i_{j-1}}, \quad l_j = i_j - i_{j-1}. \tag{97}$$



(a) $f_1 = 1 + 2x^2 - 6x^3 + 4x^5 \in \mathbb{Q}_2[X]$ (b) $f_2 = 2 - \frac{1}{2}x + x^2 + \frac{3}{2}x^4 + x^5 \in \mathbb{Q}_2[X]$

(c) $f_3 = x + \sqrt{2}x^3 - 2x^4 = \mathbb{Q}_2(\sqrt{2})[X]$ (d) $f_4 = 2 - 6x + 4x^4 + x^5 \in \mathbb{Q}_2[X]$

Figure 2: Examples of Newton polygons.

We can deduce the p-adic valuation of the non-zero roots of f from its Newton polygon.

Proposition 9.1. *Let K be a finite extension of $\mathbb{Q}_p$ and let $f = a_0 + \cdots + a_n X^n \in K[X]$. Then the valuation of the non-zero roots of f can be deduced from its Newton polygon in the following way: for each line segment L_j there exists exactly l_j (counted with multiplicity) roots of f in $\overline{\mathbb{Q}}_p$ with valuation $-s_j$, and all non-zero roots of f are obtained in this way.*

Proof. See [Gou97, Thm. 6.5.7]. □

Let L denote the splitting field of f. Then we can use the Newton polygon of f to determine a lower bound for the ramification index of the extension L/K. Recall

that the ramification index is given by the index of the value groups, i.e.

$$e_{L/K} = \#(v_p(L^*)/v_p(K^*)). \tag{98}$$

Example 9.2. Considering the polynomial $f_1 = 1 + x^2 - 6x^3 + 4x^5 \in \mathbb{Q}_2[X]$ and let L be its splitting field. The Newton polygon of f_1 (see figure 2) consists of two segments with slopes $s_1 = 1/3, s_2 = 1/2$ and lengths $l_1 = 3, l_2 = 2$. Therefore f_1 has exactly 3 roots of 2-adic valuation $-1/3$ and 2 roots of 2-adic valuation $-1/2$. As these roots belong to L, we see that $\frac{1}{6}\mathbb{Z} \subset v_2(L^*)$. As $v_2(\mathbb{Q}_2) = \mathbb{Z}$ this implies that 6 divides $e_{L/\mathbb{Q}_2}$.

9.2 Newton polygons for power series

Again consider the same situation where K is a finite extension of $\mathbb{Q}_p$ but now let $f = a_0 + a_1X + a_2X^2 + \cdots \in K[[X]]$ be a power series. We again consider the set of points

$$\{(i, v_p(a_i)) \in \mathbb{R}^2 \colon i \geq 0, a_i \neq 0\}. \tag{99}$$

We have a similar construction of the Newton polygon of f in this case:

- Start with the smallest index i such that $a_i \neq 0$, which we denote by i_0.
- Given i_{j-1}, check if there exists an index $i > i_{j-1}$ with $a_i \neq 0$ such that the slope of the line segment from $(i_{j-1}, v_p(a_{i_{j-1}}))$ to $(i, v_p(a_i))$ is minimal.
  - If there exist no $i > i_{j-1}$ such that $a_i \neq 0$, terminate.
  - Else, if no minimum is obtained, add a final infinite line segment L_j to the Newton polygon, starting at $(i_{j-1}, v_p(a_{i_{j-1}}))$ with slope equal to the infimum of all possible slopes, and then terminate.
  - If there exists infinitely many i such that the minimum is obtained, add a final infinite segment L_j to the Newton polygon, starting at $(i_{j-1}, v_p(a_{i_{j-1}}))$ with slope equal to this minimum, and then terminate.
  - If there exist only finitely many i such that the minimum is obtained, let i_j be the largest one and add the corresponding line segment L_j to the Newton polygon.

Remark 9.2.1. Note that if the last segment L_N is infinite but contains no points, then it is possible that the slopes of the last two segments agree, i.e. $s_{N-1} = s_N$.

Again, we can something about the valuations of the roots of f.

Proposition 9.3. *Let K be a finite extension of $\mathbb{Q}_p$ and suppose $f = a_0 + a_1X + a_2X^2 + \cdots \in K[[X]]$ is a power series that converges on the closed disk $\{x \in \overline{\mathbb{Q}}_p \colon v_p(x) \geq c\}$, and let s_N be the largest slope such that the segment L_N is finite and $s_N \leq -c$. Then for each slope segment L_j with $j \leq N$ there are exactly l_j roots (counted with multiplicity) of f in $\overline{Q}_p$ of valuation $-s_j$ and every non-zero root of f in the closed disk $\{x \in \overline{\mathbb{Q}}_p \colon v_p(x) \geq c\}$ is obtained this way.*

Proof. See [Gou97, Cor. 6.5.11]. □

Example 9.4. Consider the power series $f(X) \in \mathbb{Z}_p[[X]]$ given by

$$\begin{aligned} f(X) &= p^2 \sum_{n\geq 0} X^{4n} + p \sum_{n\geq 0} X^{4n+1} + \sum_{n\geq 0} X^{4n+3} \\ &= p^2 + pX + X^3 + p^2X^4 + pX^5 + X^7 + p^2X^8 + \dots. \end{aligned}$$

Note that f converges in the closed ball $B = \{x \in \mathbb{Q}_p \colon v_p(x) \geq 1\}$. The Newton polygon of f is given in figure 3. Then by the previous proposition, f has exactly 3 roots in B, one of valuation 1 and two of valuation $1/2$.

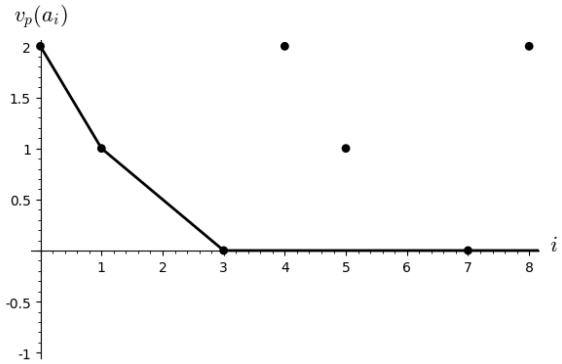


Figure 3: Newton polygon of the powerseries $f(X) = p^2 \sum_{n\geq 0} X^{3n} + p \sum_{n\geq 0} X^{3n+1} + \sum_{n\geq 0} X^{3n+2} \in \mathbb{Z}_p[[X]]$.

10 Lower bound for ramification index

10.1 Newton polygons of division polynomials

Let E be an elliptic over a number field K and $\mathfrak{p}$ a prime of K of good reduction above p (we assume $p \neq 2, 3$ for simplicity). Suppose E is given by a short Weierstrass equation that is minimal for $\mathfrak{p}$,

$$E\colon y^2 = x^3 + ax + b, \tag{100}$$

with $a, b \in \mathcal{O}_K$.

Let $n \geq 1$, and let $\mathfrak{P}$ be a prime of $K(E[p^n])$ above $\mathfrak{p}$. Then we have local fields $\mathbb{Q}_p \subset K_\mathfrak{p} \subset K(E[p^n])_\mathfrak{P}$. By identifying $K(E[p^n])$ with its image in $K(E[p^n])_\mathfrak{P}$, we can extend the regular p-adic valuation on $\mathbb{Q}$ to $K(E[p^n])$. Explicitly, this is defined by $v_p(x) = e^{-1}_{\mathfrak{P}/p} v_\mathfrak{P}(x)$ for any $x \in K(E[p^n])$.

Consider the division polynomial ψ_{p^n}, as defined in section ??. As we assumed $p \neq 2, 3$, ψ_{p^n} is a polynomial in $\mathbb{Z}[a, b, x]$. The roots of ψ_{p^n} are exactly the x-coordinates of the p^n-torsion points of E, and we can find their valuations using Newton polygons as described in the previous section.

Example 10.1. Let E_1 be the elliptic curves over $\mathbb{Q}$ be given by $E_1\colon y^2 = x^3 + 1$. Then

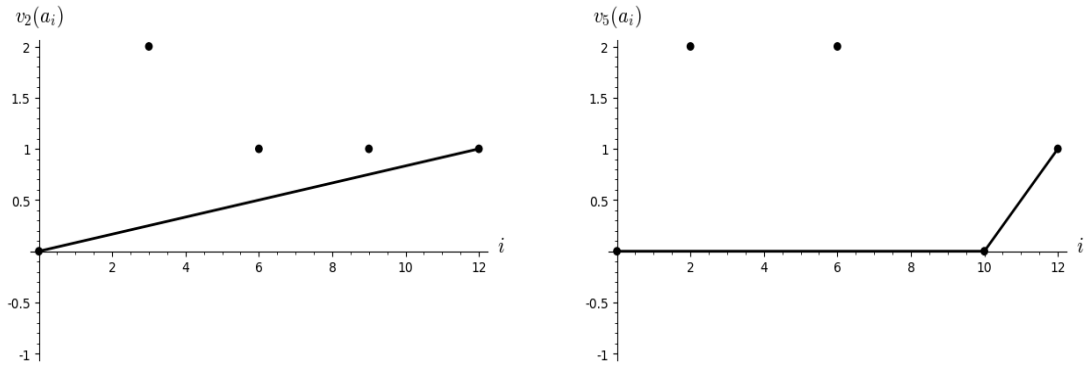
$$\psi_5 = 5x^{12} + 380x^9 - 240x^6 - 1600x^3 - 256 \tag{101}$$

In particular, the Newton polygon of ψ_5 at the prime $p = 5$ has exactly one segment with slope $s_1 = \frac{1}{12}$ (see figure ??). This means that the corresponding roots have p-adic valuation $-\frac{1}{12}$. In particular, by lemma ?? we know that these are supersingular points and that the ramification index of $p = 5$ in $\mathbb{Q}(E[5])/\mathbb{Q}$ is divisible by 24.

Example 10.2. Let E_2 be the elliptic curves over $\mathbb{Q}$ be given by $E_2\colon y^2 = x^3 + x$. Then

$$\psi_5 = 5x^{12} + 62x^{10} - 105x^8 - 300x^6 - 125x^4 - 50x^2 + 1 \tag{102}$$

In particular, the Newton polygon of ψ_5 at the prime $p = 5$ has two segments with slope $s_1 = 0$ and $s_2 = \frac{1}{2}$ (see figure ??). This means that the corresponding roots have p-adic valuation 0 and $-\frac{1}{2}$ respectively. In particular, by lemma ?? we know that the latter correspond to supersingular points and that the ramification index of $p = 5$ in $\mathbb{Q}(E[5])/\mathbb{Q}$ is divisible by 4.



(a) $E_1 \colon y^2 = x^3 + 1$ (b) $E_2 \colon y^2 = x^3 + x$

Figure 4: Newton polygon of ψ_5 at the prime $p = 5$.

However, can we say anything about the Newton polygon of ψ_{p^n} without knowing its coefficients explicitly? First, in order to simplify our task somewhat, note that ψ_{p^m} divides ψ_{p^n} for all $m \leq n$. Thus consider the primitive p^n-th division polynomial

$$\psi_{p^n,\text{prim}} = \psi_{p^n}/\psi_{p^{n-1}}, \tag{103}$$

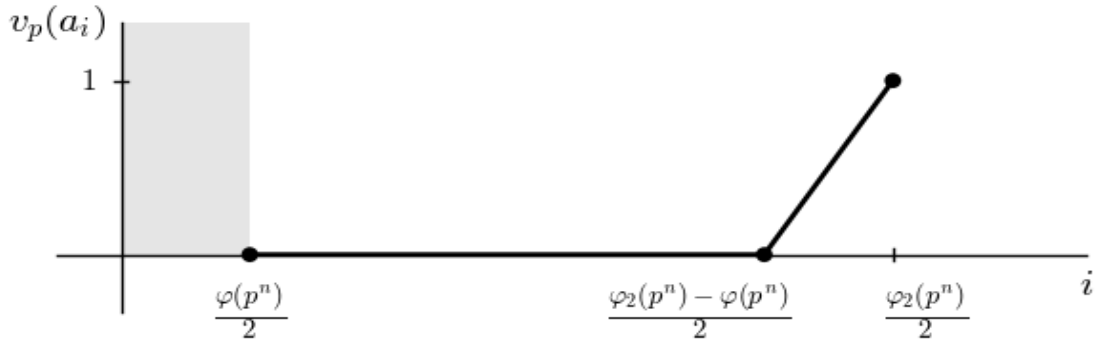
whose roots are exactly the x-coordinates of the primitive p^n-torsion points of E. As there are exactly $\varphi_2(p^n) := p^{2n} - p^{2n-2}$ primitive p^n torsion points, we see that $\deg(\psi_{p^n,\text{prim}}) = \varphi_2(p^n)/2$.

If the reduced curve $E_\mathfrak{p}$ is ordinary, then there are exactly p^n supersingular p^n-torsion points. Out of these, $\varphi(p^n) = p^n - p^{n-1}$ are primitive. This means that $\varphi(p^n)/2$ of the roots of $\psi_{p^n,\text{prim}}$ have negative valuation. Using the techniques from the next subsection applied to ordinary reduction, one can show that all these roots have the same p-adic valuation $2/\varphi(p^n)$.

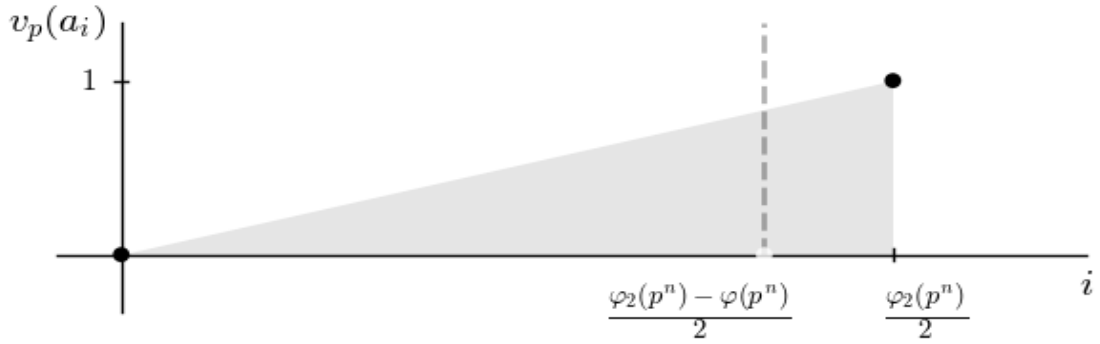
Furthermore, depending on whether there exists a primitive p^n-torsion point of $E_\mathfrak{p}$ with x-coordinate equal to zero, there are either $\varphi(p^n)/2$ or 0 roots with positive valuation. This implies that for ordinary reduction, the Newton polygon has to be of the form as show in figure 5. Note that in general, the most we can deduce from this Newton polygon is that $\varphi(p^n)$ divides the ramification index $e_{\mathfrak{P}/p}$ of $\mathfrak{P}$ over the integer prime p. However, we already knew this as $K(\zeta_n) \subset K(E[n])$.

For supersingular reduction, all p^n-torsion points are supersingular, and thus every root of $\psi_{p^n,\text{prim}}$ has negative valuation. This can lead to more interesting possibilities (see figure 5). However, the nature of the recursion for the division

polynomials makes it very awkward to prove things. As the kernel of reduction modulo $\mathfrak{P}$ is contained in the formal group $\hat{E}(\mathfrak{P}\mathcal{O}_{K(E[n])_{\mathfrak{P}}})$, it is easier to try to deduce lower bounds there.



(a) Ordinary reduction



(b) Supersingular reduction

Figure 5: Possible Newton polygon structures for $\psi_{p^n,\mathrm{prim}}$.

10.2 Newton polygons of multiplication-by-p in formal group

We will generalize the methods of [BG03, 4.7] to determine the p-adic valuation of p-power torsion points for an elliptic curve E with supersingular reduction, using the Newton polygon of the multiplication-by-p power series in the formal group $\hat{E}$.

Let E be an elliptic curve with good reduction over a finite extension K of $\mathbb{Q}_p$ (we can always reduce the number field case to this by completion). As explained in section 2.4, the p-power torsion points that are in the kernel of the reduction belong

to the formal group $\hat{E}(\mathfrak{m}_K)$, where $\mathfrak{m}_K$ is the maximal ideal of the valuation ring $\mathcal{O}_K$. In particular, when E has supersingular reduction, all the p-power torsion belong to the formal group.

Points that are in the formal group are completely determined by their value at the uniformizer at infinity $t = -x/y$. The following lemma relates the valuation of $t(P)$ and the valuations $t(x)$ and $t(y)$.

Lemma 10.3. *Let E be an alliptic curve over a finite extension K of $\mathbb{Q}_p$. Then for any point $P \in \hat{E}(\mathfrak{m}_K)$, we have*

$$v_p(x(P)) = -2v_p(t(P)), \quad v_p(y(P)) = -3v_p(t(P)). \tag{104}$$

Proof. Note that as P is in the kernel of reduction, we have $v_p(x(P))$ and $v_p(y(P))$ must be negative. Then using the Weierstrass equation for E (for simplicity we use a short Weierstrass equation, however the argument extends to a general Weiestrass equation)

$$y(P)^2 = x(P)^3 + ax(P) + b, \tag{105}$$

we find that $2v_p(y(P)) = 3v_p(x(P))$ (see [Smi18, 5.1] for details). This implies that $v_p(x(P)) = -2k$ and $v_p(y(P)) = -3k$ for some positive integer k. In particular $v_p(t(P)) = v_p(x(P)) - v_p(y(P)) = k$.

□

We see that in order to study the valuation of a p-power torsion points of curves with supersingular reduction, it is sufficient to understand the valuation of their values at the uniformizer t. However, these will occur exactly as roots of the multiplication-by-p map and thus we can apply our Newton polygon methods again. First we look at the shape of $[p]_{\hat{E}}(t)$.

Lemma 10.4. *Let E be an elliptic curve over K a finite extension of $\mathbb{Q}_p$, with supersingular reduction. Let $\mu \in \mathbb{Q}_{\geq 0}$ be the p-adic valuation of the coefficient of t^p in $[p]_{\hat{E}}(t)$. Then the two possible Newton polygon shapes of $[p]_{\hat{E}}(t)$ are given as in figure 6, depending on whether $\mu < p/(p+1)$.*

Proof. We copy the argument from [BG03, 4.7]. As $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^2$, it is acted on by $(\mathbb{Z}/p\mathbb{Z})^*$, and we can consider the $p+1$ orbits of the primitive p-torsion points under this action. Using

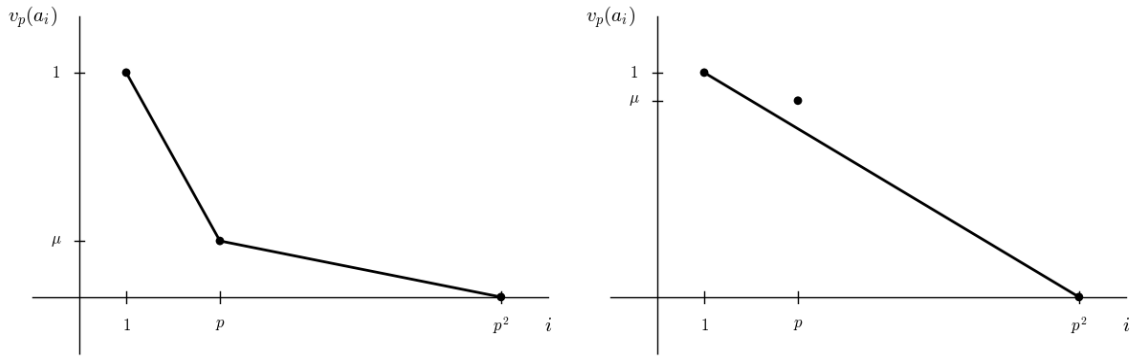
$$t(aP) = at(P) + \text{ higher order terms}, \tag{106}$$

one finds that $v_p(t(aP)) = v_p(t(P))$ for any integer a not divisible by p. In particular the valuations of p-torsion points in a given orbit are all the same. If all orbits have the same situation, it leads to figure 6 (b).

Otherwise, there are at least two orbits with different valuations. Then we can choose P_1, P_2 to be a basis for $E[p]$ such that $v_p(t(P_1)) < v_p(t(P_2))$. Then any p-torsion point $Q = aP_1 + bP_2$, we have

$$t(Q) = t(aP_1 + bP_2) = at(P_1) + bt(P_2) + \text{ higher order terms.} \tag{107}$$

If Q is not in the orbit of P_1 or P_2, then p divides neither a or b and we have $v_p(t(Q)) = \min(v_p(at(P_1)), v_p(bt(P_2))) = v_p(t(P_1))$. Therefore we see that all other orbits have valuation equal to $v_p(t(P_1))$. This leads to figure 6 (a). □



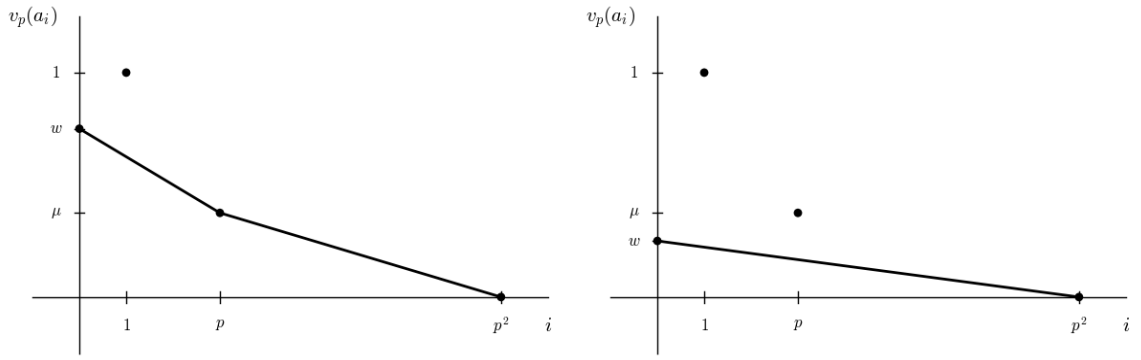
(a) $\mu < p/(p+1)$ (b) $\mu \geq p/(p+1)$

Figure 6: Possible Newton polygon shapes for $[p]_{\hat{E}}(t)$, where μ is the p-adic valuation of the coefficient of t^p.

In order to properly classify the valuations of the p-power torsion points, we will define rational numbers $w_{n,k}$ and integers $N_{n,k}$ as follows. Given a rational number $\mu > 0$, let r be the smallest non-negative integer such that $\mu \geq 1/(p^r + p^{r-1})$. Then, for each integer $n \geq 1$, let $m_n = \min(n, r)$ and define:

$$\begin{aligned}
w_{n,0} &:= \frac{1}{p^{2n} - p^{2n-2}}, & N_{n,0} &= p^{2n} - p^{2n-2}, & (r = 0),\\
w_{n,k} &:= \frac{\mu}{\varphi(p^{2n-2k})}, & N_{n,k} &= \varphi(p^k)\varphi(p^{2n-2k}), & (r \geq 1,\ k < m_{n,r}),\\
w_{n,m_n} &:= \frac{1 - p^{m_n - 1}\mu}{\varphi(p^{2n-m_n})}, & N_{n,m_n} &= \varphi(p^{2n-m_n}), & (r \geq 1).
\end{aligned}$$

These have the following properties.



(a) $w > p\mu/(p-1)$ (b) $w \leq p\mu/(p-1)$

Figure 7: Possible Newton polygon shapes for $[p]_{\hat{E}}(t) - t_0$, where $w = v_p(t_0) < 1$.

Lemma 10.5. *Let $n \geq 1$ be an integer and for each $0 \leq k \leq m_n$, let $w_{n,k}$ and $N_{n,k}$ be as above.*

(a) *Then $w_{n,0} < w_{n,1} < \cdots < w_{n,m_n} < 1$.*

(b) *For $0 \leq k < m_n$, we have*

$$w_{n+1,k} = \frac{w_{n,k}}{p^2}, \qquad N_{n+1,k} = p^2 N_{n,k}.$$

(c) *If $n \geq r$, then $m_{n+1} = m_n$, and we have*

$$w_{n+1,m_{n+1}} = \frac{w_{n,m_n}}{p^2}, \qquad N_{n+1,m_{n+1}} = p^2 N_{n,m_n}.$$

(d) *If $n < r$, then $m_{n+1} = m_n + 1$, and we have*

$$w_{n+1,m_n} = \frac{\mu}{p^2 - p}, \qquad N_{n+1,m_n} = (p^2 - p) N_{n,m_n}$$
$$w_{n+1,m_n+1} = \frac{w_{n,m_n} - \mu}{p}, \qquad N_{n+1,m_n+1} = p N_{n,m_n}.$$

Proof. Straightforward calculation, which we will leave to the reader. □

Now we can give the valuations of the p-power torsion points in terms of the $w_{n,k}$, which in turn are completely determined by μ.

Proposition 10.6. *Let E be an elliptic curve over K a finite extension of $\mathbb{Q}_p$, with supersingular reduction. Let $\mu \in \mathbb{Q}_{>0}$ be the p-adic valuation of the coefficient of t^p in $[p]_{\hat{E}}(t)$. Let r be the smallest non-negative integer such that $\mu \geq 1/(p^r + p^{r-1})$, and define the rational numbers $w_{n,k}$ and $N_{n,k}$ as above. Then for each integer $n \geq 1$ and each integer $0 \leq k \leq m_n = \min(n, r)$, there are exactly $N_{n,k}$ primitive p^n-torsion points $P \in E[p^n]$ of valuation $v_p(t(P)) = w_{n,k}$.*

Proof. We use induction on n. To start the induction, suppose $n = 1$. The primitive p-torsion points are given by the non-zero roots of $[p]_{\hat{E}}(t)$. Consider the Newton polygon of $[p]_{\hat{E}}(t)$ given in figure 6. If $r = 0$ and thus $\mu \geq p/(p+1)$, then there is just one segment of length $N_{1,0} = p^2 - 1$ and slope $-w_{1,0} = -1/(p^2-1)$. Else, if $r \geq 1$ and thus $\mu < p/(p+1)$, there is one segment of length $N_{1,1} = p - 1$ of slope $-w_{1,1} = (1-\mu)/(p-1)$, and one segment of length $N_{1,0} = p^2 - p$ and slope $-w_{1,0} = \mu/(p^2-p)$. This proves the case $n = 1$.

To continue the induction, suppose the proposition holds for some $n \geq 1$. Then the primitive p^{n+1} torsion points are given by the non-zero roots of $[p]_{\hat{E}}(t) - t(Q)$, where Q ranges over the primitive p^n-torsion points. Then by the previous lemma, $v(t(Q)) < 1$, and thus figure 7 shows the possible shapes of the Newton polygon on $[p]_{\hat{E}}(t) - t(Q)$. Therefore we see for each $0 \leq k \leq m_n$:

- If $w_{n,k} \leq p\mu/(p-1)$, then for each primitive p^n-torsion point Q with $v(t(Q)) = w_{n,k}$ there are p^2 primitive p^{n+1}-torsion points P of valuation $v_p(t(P)) = w_{n,k}/p^2$.
- If $w_{n,k} > p\mu/(p-1)$, then for each primitive p^n-torsion point Q with $v(t(Q)) = w_{n,k}$ there are p primitive p^{n+1}-torsion points P of valuation $v_p(t(P)) = (w_{n,k} - \mu)/p$ and $p^2 - p$ primitive p^{n+1} torsion points P of valuation $v_p(t(P)) = \mu/(p^2 - p)$.

Note that, by the previous lemma, we are done if we prove that the latter case $w_{n,k} > p\mu/(p-1)$ only happens whenever $k = m_n$ and $n < r$.

If $r = 0$, then $\mu \geq p/(p+1)$, and thus $p\mu/(p-1) \geq p^2/(p^2-1) > w_{n,0}$.

Now suppose $r \geq 1$. If $k < m_n$, we have $w_{n,k} = \mu/\varphi(p^{2n-2k}) < p\mu/(p-1)$. If $k = m_n$, then

$$w_{n,m_n} = \frac{1 - p^{m_n - 1}\mu}{\varphi(p^{2n-m_n})} > \frac{p\mu}{p-1} \tag{108}$$

can be simplified to

$$1 - p^{m_n-1}\mu > p^{2n-m_n}\mu, \tag{109}$$

which is equivalent to $\mu < 1/(p^{2n-m_n} + p^{m_n-1})$.

Note that $p^{2n-m_n} + p^{m_n-1}$ obtains its minimum when $m_n = n$, i.e.

$$\mu < \frac{1}{p^{2n-m_n} + p^{m_n-1}} \leq \frac{1}{p^n + p^{n-1}}, \tag{110}$$

and thus by definition of r, we have $n < r$. Conversely, if $n < r$, then $m_n = n$ and thus by definition of r, we have $\mu \geq 1/(p^n + p^{n-1}) = 1/(p^{2n-m_n} + p^{m_n-1})$, which we showed is equivalent to $w_{n,m_n} \leq p\mu/(p-1)$. This completes the proof. □

This allows us to give bounds for the valuation of primitive p^n-torsion in the supersingular case.

Corollary 10.7. *Assume the same situation as the above proposition. Then there exists a primitive p^n-torsion point $P \in E[p^n]$ with valuation*

$$0 < v(t(P)) \leq \frac{1}{p^{2n} - p^{2n-2}}, \tag{111}$$

with strict inequality if $r \geq 1$. Furthermore, all primitive p^n-torsion points $P \in E[p^n]$ have valuation

$$0 < v(t(P)) \leq \frac{1}{p^n - p^{n-2}}. \tag{112}$$

Proof. If $r = 0$, the corollary is trivial. Therefore suppose $r \geq 1$. Then, since $w_{n,0} < w_{n,1} < \cdots < w_{n,m_n}$, it is sufficient to show that $w_{n,0} < 1/(p^{2n} - p^{2n-2})$ and $w_{n,m_n} \leq 1/(p^n - p^{n-2})$.

In order to prove $w_{n,0} < 1/(p^{2n} - p^{2n-2})$, note that by assumption $\mu < p/(p+1)$ and thus

$$w_0 = \frac{\mu}{\varphi(p^{2n})} < \frac{p}{(p+1)\varphi(p^{2n})} = \frac{p}{p^{2n+1} - p^{2n-1}} = \frac{1}{p^{2n} - p^{2n-2}}. \tag{113}$$

For $w_{n,m_n} \leq 1/(p^n - p^{n-2})$, note that by assumption $\mu \geq 1/(p^r + p^{r-1})$. Therefore

$$1 - p^{m_n-1}\mu \leq 1 - \frac{p^{r-1}}{p^r + p^{r-1}} = \frac{p}{p+1}, \tag{114}$$

and

$$\varphi(p^{2n-m_n}) \geq \varphi(p^{2n-n}) = \varphi(p^n). \tag{115}$$

If we combine these two inequalities we get

$$w_{n,m_n} = \frac{1 - p^{m_n-1}\mu}{\varphi(p^{2n-m_n})} \leq \frac{p}{(p+1)\varphi(p^n)} = \frac{1}{p^n - p^{n-2}}. \tag{116}$$

□

Reducing the number field case to the local field case, it immediately follows that:

Corollary 10.8. *Let E be an elliptic curve over a number field K, let $\mathfrak{p}|p$ be a prime of K of supersingular reduction, and let $\mathfrak{P}$ be a prime of $K(E[p^n])$ above $\mathfrak{p}$. Then the ramification index of $\mathfrak{P}$ over p is at least*

$$e_{\mathfrak{P}/p} \geq \frac{1}{p^{2n} - p^{2n-2}}, \tag{117}$$

Furthermore, if $P \in E[p^n]$ is any primitive p^n torsion point, then any prime $\mathfrak{p}'$ of $K(P)$ above $\mathfrak{p}$ has ramification index over p of at least

$$e_{\mathfrak{p}'/p} \geq \frac{1}{p^n - p^{n-2}}. \tag{118}$$

Remark 10.8.1. This gives theorem 5.1 and a corrected version of theorem 5.4 from [Smi18]. In particular, theorem 5.4 states that every prime $\mathfrak{p}'$ above $\mathfrak{p}$ in $K(P)$ for any primitive p^n-torsion point P has ramification index over p strictly divisible by $\varphi(p^n)$. However, this is not true, as it is only strictly greater than $\varphi(p^n)$ (as implied by the previous corollary), but not necessarily divisible.

The advantage we gained over the division polynomial method is that we only have to determine the valuation μ of the coefficient of t^p in the power series $[p]_{\hat{E}}(t)$, in order to efficiently compute the valuations $v(t(P))$ for all p-power torsion points P.

Example 10.9. Let $e \geq 1$ be an integer, and let $\pi = 7^{1/e}$. Consider the elliptic curve E over the field $K = \mathbb{Q}(\pi)$, given by

$$y^2 = x^3 + x + \pi. \tag{119}$$

Note that the prime 7 is totally ramified in K, with $7\mathcal{O}_K = (\pi)^e$. Then E has supersingular reduction at π, and one can compute (using SageMath for instance) that the coefficient of t^7 in $[7]_{\hat{E}}(t)$ is equal to 352944π, which has 7-adic valuation $\mu = 1/e$. Then r is the smallest non-negative integer such that $e \leq 7^r + 7^{r-1}$. In particular if we choose $e = 10$, then $r = 2$. Then the primitive 49-torsion points have valuations

$$w_{2,0} = \frac{1}{20580}, \quad w_{2,1} = \frac{1}{420}, \quad w_{2,2} = \frac{1}{140}. \tag{120}$$

We can compare this to calculating the division polynomial $\psi_{49,\mathrm{prim}}$, which has degree 1176 and Newton polygon given by the vertices

$$\{(0,0), (1029, 1/10), (1155, 7/10), (1176, 1)\}, \tag{121}$$

which indeed gives the corresponding valuations of the x-coordinates

$$-\frac{1}{10290}, \quad -\frac{1}{210}, \quad -\frac{1}{70}. \tag{122}$$

References

[AM69] Michael Atiyah and Ian Macdonald. Introduction to commutative algebra. Addison-Wesley, 1969.

[BG03] John Boxall and David Grant. Singular torsion points on elliptic curves. Mathematical Research Letters, 10(6):847–865, 2003.

[Con] Keith Conrad. The conductor ideal. https://kconrad.math.uconn.edu/blurbs/gradnumthy/conductor.pdf.

[Cor01] Gunther Cornelissen. Two-torsion in the jacobian of hyperelliptic curves over finite fields. Archiv der Mathematik, 77(3):241–246, 2001.

[Cox11] David Cox. Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication, volume 34. John Wiley & Sons, 2011.

[Deu41] Max Deuring. Die typen der multiplikatorenringe elliptischer funktionenkörper. In Abhandlungen aus dem mathematischen Seminar der Universität Hamburg, volume 14, pages 197–272. Springer, 1941.

[DT02] William Duke and Árpad Tóth. The splitting of primes in division fields of elliptic curves. Experimental Mathematics, 11(4):555–565, 2002.

[GKZ08] Israel Gelfand, Mikhail Kapranov, and Andrey Zelevinsky. Discriminants, resultants and multidimensional determinants. Reprint of the 1994 edition. Birkhäuser Boston, Inc., Boston, MA, 2008.

[Gou97] Fernando Gouvêa. p-adic Numbers. Springer, 1997.

[JT15] Christian Jensen and Anders Thorup. Gorenstein orders. Journal of Pure and Applied Algebra, 219(3):551–562, 2015.

[Lan87] Serge Lang. Elliptic functions. Springer, 1987.

[LW85] Lawrence Levy and Roger Wiegand. Dedekind-like behavior of rings with 2-generate ideals. Journal of Pure and Applied Algebra, 37:41–58, 1985.

[Mar20] Stefano Marseglia. Computing the ideal class monoid of an order. Journal of the London Mathematical Society, 101(3):984–1007, 2020.

[Maz77] Barry Mazur. Modular curves and the eisenstein ideal. Publications Mathématiques de l'Institut des Hautes Études Scientifiques, 47(1):33–186, 1977.

[MG78] Barry Mazur and Dorian Goldfeld. Rational isogenies of prime degree. Inventiones mathematicae, 44(2):129–162, 1978.

[Mil08] James Milne. Abelian varieties (v2.00), 2008. Available at https://www.jmilne.org/math/CourseNotes/av.html.

[MvdGE] Ben Moonen, Gerard van der Geer, and Bas Edixhoven. Abelian varieties. Preliminary version available at https://www.math.ru.nl/~bmoonen/research.html#bookabvar.

[Neu13] Jürgen Neukirch. Algebraic number theory, volume 322. Springer Science & Business Media, 2013.

[Sch95] René Schoof. Counting points on elliptic curves over finite fields. Journal de théorie des nombres de Bordeaux, 7(1):219–254, 1995.

[Ser97] Jean-Pierre Serre. Abelian l-adic representations and elliptic curves. CRC Press, 1997.

[Sil94] Joseph Silverman. Advanced topics in the arithmetic of elliptic curves, volume 151 of Graduate Texts in Mathematics. Springer Science & Business Media, 1994.

[Sil09] Joseph Silverman. The arithmetic of elliptic curves, volume 106 of Graduate Texts in Mathematics. Springer Science & Business Media, 2009.

[Sil15] Joseph Silverman. Errata and Corrections to The Arithmetic of Elliptic Curves 2nd Edition. 2015. https://www.math.brown.edu/~jhs/AEC/AECErrata.pdf.

[Smi18] Hanson Smith. Ramification in the division fields of elliptic curves and an application to sporadic points on modular curves. arXiv preprint arXiv:1810.04809, 2018.

[Ste02] Peter Stevenhagen. Voortgezette getaltheorie. 2002. http://websites.math.leidenuniv.nl/algebra/localfields.pdf.

[Ste17] Peter Stevenhagen. Number rings. 2017. http://websites.math.leidenuniv.nl/algebra/ant.pdf.

[Sut12] Andrew Sutherland. Torsion subgroups of elliptic curves over number fields. 2012. https://math.mit.edu/~drew/MazursTheoremSubsequentResults.pdf.

[Was08] Lawrence Washington. Elliptic curves: number theory and cryptography. CRC press, 2008.