university of groningen / faculty of science and engineering

Bachelor's Thesis

An Introduction to Arithmetic Dynamics and Lattès Maps

Author

Jerzy Piotr Olszewski

s4727746

Supervisors

Prof. Dr. Cecília Salgado Guimarães da Silva

Mathematics, Algebra Group, University of Groningen

Prof. Dr. Jaap Top

Mathematics, Algebra Group, University of Groningen

Abstract

Arithmetic Dynamics is a relatively new field of study which combines the ideas of arithmetic and dynamics. It is concerned with rephrasing results and problems of arithmetic in the language of dynamical systems as well as giving number theoretic meaning to concepts in dynamics. In this text we give a brief introduction to arithmetic dynamics, presents results relating both fields of study and discuss the Lattès example with generalization to the surface given by two elliptic curves.

To fulfill the requirements for the degree of
Bachelor of Science in Mathematics
at the University of Groningen

July 31, 2024

Acknowledgements

I would like to thank professor Salgado her support and understanding during the writing of this text. Moreover, prof. Salgado's and prof. Top's contributions to teaching mathematics at RUG have been invaluable to me. Among many more I would like to give special thanks to Miquel Camprubi Bonet, Utku Erçetin and Jennifer Pearson for their unyielding support and friendship. A special thanks to Rokas Žukauskas for the aid in generating the images found in the text.

Contents

1 Introduction

One of the first instances in which arithmetic and dynamics were related is an example produced by Lattès in 1918, shortly before his untimely death. In this example, Lattès produces a family of rational maps on the Riemann sphere with the property that they have empty Fatou sets. Although as Milnor points out, similar maps have been discussed before by Schröder in 1871 (see [Mil04] sec. 6). The Lattès maps are constructed by requiring commutativity with an appropriate morphism of elliptic curves. Since then, this has inspired many generalizations of said construction to abelian varieties of arbitrary dimension and maps between projective n-spaces. A large part of the present text is devoted to discussing the Lattès example and related maps as well as a generalization to surfaces given by the product of two elliptic curves.

The field has seen significant development in the 1990s following a paper by Silverman in 1991 ([Sil91]) discussing dynamical analogues of problems in arithmetic; such as uniform boundedness of periodic points, periodic points on sub-varieties, integral points in orbits and more. This development has lead Silverman to write a book (2007) surveying the results of the field ([Sil07]) which has since become an inexcusable reference for any paper on arithmetic dynamics. Although arithmetic and dynamics by themselves are relatively old fields of research (in particular arithmetic which may be argued to be the origin of all mathematics), the ideas connecting the two are recent. In relating the concepts and methods we gain a new perspective on known problems which may lead to new developments in either field with the hope of proving difficult results. Nevertheless, the subject also provides problems which are interesting in their own right. The aim of this text is to give an introduction to arithmetic dynamics and the Lattès construction.

As mentioned above, the goal of *Arithmetic Dynamics* is to relate results and notions of Arithmetic Geometry with those of Dynamics. This is interesting for a number of reasons: firstly it showcases how different and seemingly distant mathematical disciplines can be related and secondly it relates results, thus allowing for the application of methods from one discipline to prove results in the other. This, of-course, requires a lot of care. Some of the relations are summarised in the following (for a more detailed survey of relations see [Sil22])

Arithmetic Geometry	**Discrete Dynamics**
$\mathbb{Z}$ and $\mathbb{Q}$ points on varieties	$\mathbb{Z}$ and $\mathbb{Q}$ points in orbits of rational maps
Torsion points of abelian varieties	Periodic and preperiodic points of rational maps
Orbit of $\alpha \in X$	Mordell-Weil group

We mainly focus on the second relation and explicitly compute examples of the rational maps relating torsion points to periodic and preperiodic points.

Organization of the text: In section 2 we begin with a summary of results and definitions in algebraic geometry, dynamical systems and arithmetic necessary for the discussion. A number of results related to preperiodic points can be shown using arithmetical tools such as height functions and good reduction, this is discussed in section 3. Some proofs are given, however, those requiring more auxiliary results are referenced. In section 4 we define *elliptic curves* and discuss the Lattès construction with explicit examples. In section 5 we discuss the example, due to Lattès, giving a rational map with empty Fatou set. This is followed by a generalization of the Lattès construction to other subgroups of the automorphisms on an elliptic curve. The natural question that follows this discussion, is weather this can be generalized to surfaces? We discuss this in section 6 and show how the Lattès construction can be extended to surfaces given by two elliptic curves. The first four examples of these surfaces given by two elliptic curves listed in section 5 of [Dup01] are computed, the last two requiring more auxiliary results.

2 Background

2.1 Algebraic Curves

Let $\Bbbk$ be a field and K an algebraically closed field, for convenience we assume these to be perfect. In this text we denote the affine and projective spaces over a field $\Bbbk$, by $\mathbb{A}^n_\Bbbk$ and $\mathbb{P}^n_\Bbbk$ respectively (see sections 1.2 and 4.1 of [Ful08]). If the field is apparent from context we may neglect the subscript $\Bbbk$ in notation. Elements of these spaces are called *points*, for example the n-tuple $(a_1, \ldots, a_n) \in \mathbb{A}^n$ is an affine point and the $(n+1)$-tuple $(a_1 : \ldots : a_{n+1}) \in \mathbb{P}^n$ is a projective point. As we deal with algebraic curves in such spaces, we begin by introducing the underlying definitions.

Definition 2.1. (algebraic varieties)
Let $S \subseteq \Bbbk[x_1, \ldots, x_n]$.

1. The set of affine points that are roots of every polynomial in S,
$$V(S) := \{p \in \mathbb{A}^n_\Bbbk \mid f(p) = 0 \ \forall f \in S\} \subseteq \mathbb{A}^n_\Bbbk, \tag{1}$$
is called the (affine) *vanishing set of* S. Such subsets of $\mathbb{A}^n_\Bbbk$ are called *(algebraic) affine varieties.* ([Gat21] 1.2.b)

2. If every polynomial in S is homogeneous, the set[1]
$$V(S) := \left\{p \in \mathbb{P}^{n-1}_\Bbbk \mid f(p) = 0 \ \forall f \in S\right\} \subseteq \mathbb{P}^{n-1}_\Bbbk, \tag{2}$$
is called the *projective vanishing set of* S. Such subsets of $\mathbb{P}^{n-1}_\Bbbk$ are called *(algebraic) projective varieties.* ([Gat23] 3.8)

Since we work over fields, it follows from *Hilbert's Basis Theorem* (see [Gat21] prop.1.1.5) that $V(S) = V(S_0)$ for some finite set of polynomials $S_0 \subsetneq \Bbbk[x_1, \ldots, x_n]$. Thus we take the notational convention of denoting $V(S) = V(\{f_1, \ldots, f_n\})$ by $V(f_1, \ldots, f_n)$.

Example 2.1. Let $\Bbbk$ be a field and consider the affine vanishing set of the polynomial $f(x, y) = x^3 + 1 - y^2$,
$$V(f) = \left\{(x, y) \in \mathbb{A}^2_\Bbbk \mid f(x, y) = 0 \ \right\} \subseteq \mathbb{A}^2_\Bbbk.$$
This gives an affine variety in $\mathbb{A}^2_\Bbbk$.
Similarly let us consider the projective vanishing set of the homogeneous polynomial $F(x, y, z) = x^3 + z^3 - y^2 z$,
$$V(F) = \left\{(x : y : z) \in \mathbb{P}^2_\Bbbk \mid F(x, y, z) = 0 \ \right\} \subseteq \mathbb{P}^2_\Bbbk.$$
This is a projective variety in $\mathbb{P}^2_\Bbbk$.

Note that the above polynomials are related via $F(x, y, z) = z^3 f(x/z, y/z)$. This is known as *homogenization* and it allows us to relate affine varieties to projective varieties. Indeed if we substitute $(x, y, 1)$ we recover all affine points. A variety is called *irreducible* if it cannot be written as a union of proper sub-varieties[2]. For convenience, we restrict to irreducible varieties. Certain projective varieties can be equipped with an operation on their points making them into a commutative group, these are referred to as *abelian varieties.* The specific definition is delicate and we refer the reader to [Mil08]. The projective curve given by $V(x^3 + z^3 - y^2 z)$ (as above) is an example of an abelian variety, this will be further discussed further in section 4.

[1] It may be worth noting that points in $\mathbb{P}^{n-1}_\Bbbk$ have n-many coordinates thus matching the number of possible variables in f.

[2] Proper subsets that are themselves varieties.

Definition 2.2. (Coordinate Ring)
Take $V = V(S)$ to be a variety (affine or projective) defined by $S \subseteq \Bbbk[x_1, \ldots, x_n]$ and let us denote the ideal of V by $I(V) := \{f \in \Bbbk[x_1, \ldots, x_n] \mid f(\alpha) = 0 \ \forall \alpha \in V\}$. The *coordinate ring of* $V(S)$ is the ring

$$\Gamma(V) := {}^{\Bbbk[x_1, \ldots, x_n]}\big/_{I(V)}. \tag{3}$$

([Gat21] 1.15)

Example 2.2. Take the affine variety as in example 2.1, given by $f(x, y) = x^3 + 1 - y^2$. Then, by definition, the ideal of V is

$$I(V) = \{g \in \Bbbk[x, y] \mid g(x, y) = 0 \ \forall (x, y) \in V\}.$$

Since $f \in \Bbbk[x, y]$ is prime ($\Bbbk[x, y]/(f)$ is a domain), it follows that $(f) = I(V)$. Hence the coordinate ring of V is

$$\Gamma(V) = {}^{\Bbbk[x, y]}\big/_{(f)}.$$

Given a coordinate ring $\Gamma(V)$, we can look the field of fractions of this ring, namely $\mathrm{Frac}(\Gamma(V))$. This is the *function field of* V and is denoted by $\Bbbk(V)$.

Definition 2.3. (Krull Dimension)
Given a commutative ring R, let (Y_i) denote a sequence of prime ideals of R such that $Y_i \subsetneq Y_{i+1}$ for all indices i and let $len(Y_i)$ denote the length[3] of such a sequence. Then the *Krull Dimension of* R is

$$\dim(R) := \sup_{(Y_i)} \{len(Y_i)\}. \tag{4}$$

([Har77] pg.6)

When applied to the coordinate ring of an algebraic variety, this definition gives a generalization of the notion of dimension which can be extended to projective spaces.

Definition 2.4. (Dimension of Varieties)
Let V be a variety with coordinate ring Γ, then

1. if V is affine, *the dimension of* V is $\dim \Gamma$. ([Har77] pg.6)
2. if V is projective, *the dimension of* V is $\dim \Gamma - 1$. ([Har77] ex.2.6)

A variety of dimension 1 is referred to as a *curve* and a variety of dimension 2 is referred to as a *surface*.

The following definition makes use of *continuous* maps and *open* sets; these notions should be understood with respect to the *Zariski* topology on the underlying space or variety. That is, the *closed* sets are the (sub-)varieties (see [Gat21] sec. 2). Let X be a variety over $\Bbbk$, then we define *the local ring at a point* P $\mathcal{O}_P(X) := \left\{\frac{f}{g} \in \Bbbk(X) | g(P) \neq 0\right\}$ and given an open $U \subseteq X$ we call the set of rational functions $U \dashrightarrow \Bbbk$ as $\mathcal{R}_U(X) = \bigcap_{P \in U} \mathcal{O}_P(X)$.

Definition 2.5. (Morphism)
Let V_1 and V_2 be varieties. A *morphism of varieties* from V_1 to V_2 is a continuous mapping $\varphi : V_1 \to V_2$ such that for all $U \subseteq V_2$ open we have that if $f \in \mathcal{R}_U(V_2)$ then $f \circ \varphi \in \mathcal{R}_{\varphi^{-1}(U)}(V_1)$. Furthermore, a morphism φ is called an *isomorphism* if it is bijective and φ^{-1} is also a morphism. ([Ful08] ch.6.3)

[3]That is to say the number of non-zero prime ideals in the sequence.

We also introduce the Riemann-Hurwitz formula as it is useful later on. This result requires the notion of a *genus* of a curve which is beyond the scope of this text to introduce in full generality, as such we refer the reader to [Ful08] sec 8.3 and [Har77] p.56. Nevertheless it can be thought of as (birational) invariant which classifies curves. For smooth plane curves (those in $\mathbb{P}^2$) it can be given by

$$g(X) = \frac{(d-1)(d-2)}{2} \tag{5}$$

where d is the degree of the variety $X \subseteq \mathbb{P}^2$ ([Gat21] ex. 16.14). It is important to note that the genus is preserved under isomorphism of varieties.

Example 2.3. Take the projective curve from example 2.1, namely the zero locus of $f = x^3 + z^3 - y^2 z$. This is a projective curve of degree 3, thus applying the formula above we have $g(V(f)) = 1$.

Example 2.4. Consider the curve given by the equation $z = 0$ in $\mathbb{P}^2$, this has genus 0 by the above equation. Note that this curve is isomorphic to the projective line $\mathbb{P}^1$. In particular $(x : y) \mapsto (x : y : 0)$ gives an isomorphism in the sense of definition 2.5. Thus we say that the projective line has genus 0.

It is important to note that the genus is a non-negative integer.

Theorem 2.1. *(Riemann-Hurwitz Formula)*
Given two smooth[4] *curves X and Y of genus $g(X)$ and $g(Y)$ respectively and a finite morphism $f : X \to Y$, then*

$$2g(X) - 2 = deg(f)(2g(Y) - 2) + \sum_{P \in X} (e_P - 1), \tag{6}$$

Where $e_P = ord_P(f - f(P))$ is the ramification index of f at $P \in X$.

Proof. The proof is rather involved, as such we refer the reader to [Har77] *IV*.2. ☐

2.2 Dynamics

We also introduce the dynamical concepts necessary for our investigation. With the exception of the multiplier and equicontinuity, these may be found in the introduction chapter of [Sil07]. The multiplier and equicontinuity are referenced to chapters 1.3 and 1.4 respectively.

Definition 2.6. (Dynamical System)
A *(discrete) dynamical system* is a pair (S, f) where S is a set and $f : S \to S$ a self map.

Dynamical systems are related to S-sequences, (x_i), generated by the rule $x_{i+1} = f(x_i)$. The study of these sequences and how they relate to the initial point $x \in S$ is a major objective of dynamics. To this end the following notions are useful.

Definition 2.7. (Orbit)
Given a dynamical system (S, f) and some $\alpha \in S$, we define the *orbit of α with respect to f* as:

$$\text{Orb}_f(\alpha) := \{f^n(\alpha)\}_{n \geq 0} \tag{7}$$

where $f^n := f^{\circ n}$ denotes the n-fold compositing of f with itself and $f^0 := id$ by convention. This notation is used throughout the text.

Definition 2.8. (Periodic and pre-Periodic points)
Given a dynamical system (S, f) we say that a point $\alpha \in S$ is:

[4] see [Gat21] 10.7 and 10.11 for definitions of smoothness. For varieties given as a locust of a single polynomial it suffices to show that all partial derivatives of that polynomial do not vanish at any point of the variety.

1. a *periodic point of* f if there exists an integer $n > 0$ such that $f^n(\alpha) = \alpha$. The set of all periodic points is denoted by

$$\mathrm{Per}_S(f) := \{\alpha \in S \mid \alpha \text{ is periodic for } f\}\,. \tag{8}$$

2. a *pre-periodic point of* f if there exist two distinct integers $n, m > 0$ such that $f^n(\alpha) = f^m(\alpha)$. The set of all pre-periodic points is denoted by

$$\mathrm{PrePer}_S(f) := \{\alpha \in S \mid \alpha \text{ is pre-periodic for } f\}\,. \tag{9}$$

Remark 2.1. Equivalently, a point $\alpha \in S$ is preperiodic for f if and only if there exists a positive integer i such that $f^i(\alpha)$ is periodic for f if and only if $\mathrm{Orb}_f(\alpha)$ is finite.

It is often convenient to neglect the set S in notation since it is usually apparent from the context. Hence we usually write $\mathrm{Per}(f)$ rather than $\mathrm{Per}_S(f)$ and likewise for preperiodic points. Given a pre-periodic point $\alpha \in S$, the smallest integer n such that $f^n(\alpha) = \alpha$ is called the *the exact period of* α (with respect to f).

Example 2.5. Take the system $(\mathbb{C}, f)$ where $f(z) = z^2 + 1$. consider the orbit at of f at i,

$$Orb_f(i) = \{i, 0, 1, 2, 5, 26, 677, 458330, \ldots\}\,.$$

Note that, due to the nature of f, the imaginary unit only appears as the first value and the remaining points are real. Also, the real points grow in magnitude, since we are squaring them in each iteration thus i (or in general real numbers) cannot be preperiodic for this f. If we start at ζ_3 we have the finite orbit,

$$Orb_f(\zeta_3) = \{\zeta_3, -\zeta_3\}$$

since $-\zeta_3$ is a fixed point of f.

Example 2.6. Take the dynamical system given by

$$S = \mathbb{C} \qquad \text{and} \qquad f(z) = \frac{z^4 - 8z}{4(z^3 + 1)}, \tag{10}$$

we can see that the roots of f are $0, 2, 2\zeta_3, 2\zeta_3^2$, and its poles are $-1, -\zeta_3, -\zeta_3^2$. Thus 0 is a fixed point, or a periodic point of exact period 1; the remaining fixed points are $-\sqrt[3]{4}, -\sqrt[3]{4}\zeta_3, -\sqrt[3]{4}\zeta_3^2$. The first four iterations of f are shown in the phase portraits below.

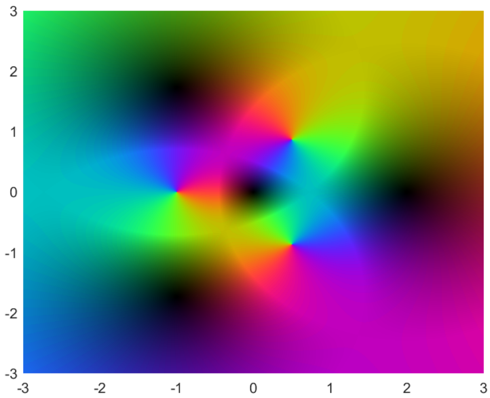

Figure 1: $f(z)$

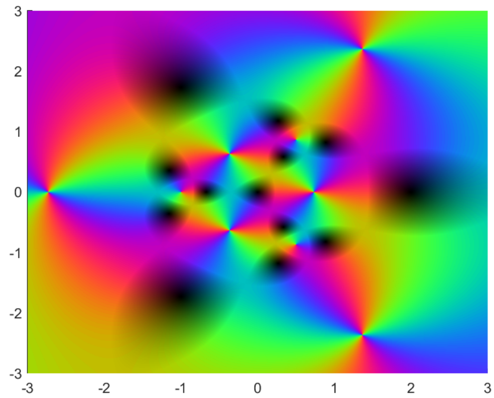

Figure 2: $f^2(z)$

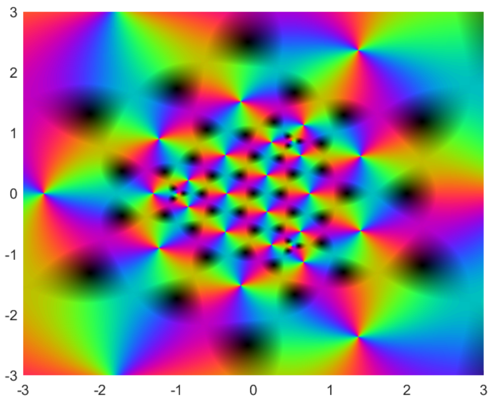

Figure 3: $f^3(z)$

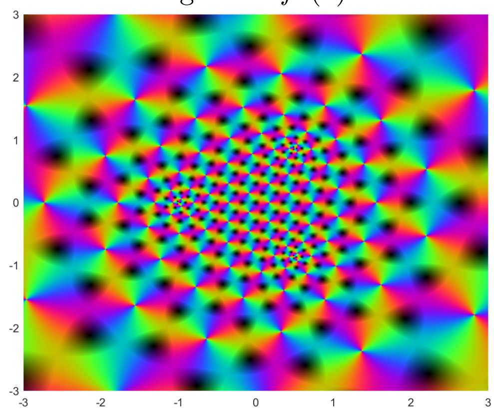

Figure 4: $f^4(z)$

Observe that the poles in figure 2.6 are indeed minus the three roots of unity (the bright singularities) and the roots are exactly 0 and twice the third roots of unity (the black spots). Another interesting observations is that almost all singularities of f^2, f^3 and f^4 appear to have multiplicity 2. As one may notice, the behaviour of f^n quickly increases in difficulty to analyse.

When considering dynamics of sufficiently differentiable functions of metric spaces, we can classify the local behaviour of points around some periodic point $\alpha \in \mathrm{Per}(f)$ by considering $(f^n)'$. This is motivated by the Taylor expansion of f^n at the fixed point α (periodic point of f),

$$f^n(x) = \alpha + (f^n)'(\alpha)(x-\alpha) + O((x-\alpha)^2)$$

where the O indicates the big O notation. In each iteration of f^n, the term $(f^n)'(\alpha)$ is multiplied by itself thus contributing to what happens to points in the neighbourhood of α.

Definition 2.9. (multiplier)
Let $\alpha \in \mathrm{Per}(f)$ be of exact period n and $f \in C^\infty$. We call the term $\lambda_\alpha(f) := (f^n)'(\alpha)$ the *multiplier of f at α.*

If $|\lambda_\alpha(f)| < 1$ then f is said to be *attracting* at α, if $|\lambda_\alpha(f)| = 1$ it is said to be *neutral* and if $|\lambda_\alpha(f)| > 1$ it is called *repelling*.

Definition 2.10. (equicontinuity)
Given that S is a metric space, f is said to be *equicontinuous at α* if $\forall \epsilon > 0$ there exists $\delta < 0$ such that[5] $\beta \in B_\delta(\alpha) \implies f^n(\beta) \in B_\epsilon(f^n(\alpha))$ for all $n > 0$.

[5] Here $B_\epsilon(x)$ denotes an open ball around x having radius ϵ.

The largest open set containing all points $\alpha \in S$ such that f is equicontinuous at α is called the *Fatou set of* f and is denoted by $\mathcal{F}(f)$; it's complements is called the *Julia set of* f and is denoted by $\mathcal{J}(f)$.

Note that by definition $\mathcal{F}$ is an open set and $\mathcal{J}$ is a closed set with respect to the topology on S. Moreover, if λ_α is attracting then $\alpha \in \mathcal{F}$ and if λ_α is repelling then $\alpha \in \mathcal{J}$.

2.3 Arithmetic

We introduce *height functions* and *good reduction*. These arithmetic notions are surprisingly usefully in analysing the preperiodic points arising from rational functions. These are tools meant for analysing $\mathbb{Q}$ and $\mathbb{Z}$ points on curves. We begin with height functions which, in their usual setting, give a measure of arithmetical complexity of rational numbers, or those in a finite extension of $\mathbb{Q}$. They are vital in the proof of the Mordell-Weil theorem for rational points on elliptic curves. In this section we restrict to $\mathbb{Q}$ and $\bar{\mathbb{Q}}$ unless stated otherwise.

Definition 2.11. (heights)
Let $\beta \in \bar{\mathbb{Q}}$ be a unit and f_β its minimal polynomial in $\mathbb{Q}$ with leading coefficient a and degree d. Without loss of generality assume that $f_\beta \in \mathbb{Z}[x]$ and is primitive. Then we define the *absolute multiplicative height function* as

$$H(\beta) := \left(|a| \prod_{\zeta \in V_{\bar{\mathbb{Q}}}(f_\beta)} \max\{1, |\zeta|\} \right)^{\frac{1}{d}}, \tag{11}$$

and the *absolute logarithmic*[6] *height function* as

$$h(\beta) := \log H(\beta). \tag{12}$$

For convention we also define $H(0) = H(\infty) := 1$.

By setting $\infty = (1 : 0) \in \mathbb{P}^1_{\bar{\mathbb{Q}}}$ as the point at infinity and taking the affine coordinate otherwise, we consider heights of points on the projective line $\mathbb{P}^1_{\bar{\mathbb{Q}}}$. From the above definition, it follows that, if $\beta = a/b \in \mathbb{Q}$ then $H(\beta) = \max\{|a|, |b|\}$. Therefore, if we bound the height by some $C > 0$ then there can only be finely many $\beta \in \mathbb{Q}$ satisfying $H(\beta) < C$ or equivalently $h(\beta) < \log(C)$. In this sense, height functions measure arithmetic complexity of a given number. Taking the logarithm base 2 in the equation 12 makes $h(\beta)$ the number of bits required to express β. Many properties of the rational numbers can be generalized to finite extensions $\Bbbk$ of $\mathbb{Q}$.

Definition 2.12. (number fields)
A finite extension $\Bbbk$ of $\mathbb{Q}$ is called a *number field*.

Number fields are central in the study of algebraic number theory.

Theorem 2.2. *(Northcott)*
Let $f \in \bar{\mathbb{Q}}(x)$ be of degree $d \geq 1$, then:

1. *there exists a constant $C = C(f) > 0$ such that $|h(f(\beta)) - d \cdot h(\beta)| \leq C$, for all $\beta \in \mathbb{P}^1_{\bar{\mathbb{Q}}}$.*
2. *for all number fields $\Bbbk$, and for all $B > 0$, the set*

$$\left\{\beta \in \mathbb{P}^1_{\Bbbk} \mid h(\beta) \leq B\right\} \tag{13}$$

is finite.

[6] The base of the logarithm is inconsequential for most purposes as only the properties of the logarithm are used. For convenience one may take it to be 2 unless stated otherwise.

In other words, sets of bounded height have at most finitely many points in any number field $\Bbbk$.

Proof. We refer the reader to [Sil10] page 10. $\square$

Another useful arithmetic tool is reduction modulo p. This is often used to show that a certain polynomial has no integer solutions. Conversely, in certain cases, if a polynomial has a solution modulo a prime power it can be lifted via Hensel's lemma to a p-adic solution (p-adics are not discussed in this text). As such reduction plays an important role in arithmetic geometry; we look at how it affects the dynamics. For ease we restrict to $f \in \mathbb{Q}(x)$ such that $f = F/G$ with $F, G \in \mathbb{Z}[x]$ having no common factors and F/G primitive[7]. Then we reduce each component modulo a prime:

$$\tilde{f} = \frac{\tilde{F}}{\tilde{G}} \in \mathbb{F}_p(x). \tag{14}$$

Definition 2.13. $f = F/G \in \mathbb{Q}(x)$ is said to have *good reduction at p* if $\tilde{F}$ and $\tilde{G}$ have no common factors in $\mathbb{F}_p(x)$

There are only finitely many primes for which F and G have common factors, these are given by the primes dividing the resultant of F and G (see 6.1 of [Sil10]). This gives us local information about f and its preperiodic points.

Remark 2.2. Note that for any rational function $f \in \mathbb{Q}(x)$ with good reduction at p, we have that $\widetilde{f(\alpha)} = \tilde{f}(\tilde{\alpha})$, for all $\alpha \in \mathbb{P}^1_{\mathbb{Q}}$. i.e. the reduction commutes with evaluation.

3 On Heights and Good Reduction

We begin by analysing dynamics of rational maps over $\bar{\mathbb{Q}}$ through (logarithmic) height functions and good reduction. This establishes a first connection between dynamics and arithmetic.

3.1 Pre-periodic points and Heights

The theory of heights allows us to make global statements about $\mathrm{PrePer}_{\bar{\mathbb{Q}}}(f)$.

Notation 3.1. For ease of notation we write $\mathrm{PrePer}_K(f)$ to also mean $\mathrm{PrePer}_{\mathbb{P}^1_K}(f)$. i.e. we include the point at infinity in notation. Likewise for periodic points.

What follows is a direct application of *Northcott's theorem* 2.2 to preperiodic points. Together with the following corollary, this gives a dynamical parallel to the arithmetic 2.2.

Theorem 3.1. *Let $f \in \bar{\mathbb{Q}}(x)$ have degree $d \geq 2$ then* $\sup\left\{h(\beta) \mid \beta \in \mathrm{PrePer}_{\bar{\mathbb{Q}}}(f))\right\} < \infty$.

In other words the set of all preperiodic points of f in $\bar{\mathbb{Q}}$ has bounded height.

Proof. By theorem 2.2 there exists a constant $C > 0$ depending on f, such that for all $\alpha \in \mathbb{P}^1_{\bar{Q}}$,

[7]For a rational $f = F/G$ with $F(x) = a_d x^d + \ldots a_0$ and $G(x) = b_d x^d + \ldots + b_0$ we say that f is primitive if $gcd(a_d, \ldots, a_0, b_d, \ldots, b_0) = 1$.

$h(f(\alpha)) - dh(\alpha) \geq -C$. This is the lower bound on the absolute value. It follows that

$$\begin{aligned} h(f^n(\alpha)) &\geq dh(f^{n-1}(\alpha)) - C \\ &\geq d^2 h(f^{n-2}(\alpha) - dC - C \\ &\vdots \\ &\geq d^n h(\alpha) - C\sum_{i=0}^{n-1} d^i \\ &= d^n h(\alpha) - C\frac{d^n - 1}{d-1} \\ &\geq d^n h(\alpha) - C\frac{d^n}{d-1}. \end{aligned}$$

Take a periodic point α of exact period n. Then $f^n(\alpha) = \alpha$, applying the above inequality gives

$$h(\alpha) \geq d^n h(\alpha) - C\frac{d^n}{d-1} \tag{15}$$

$$\implies h(\alpha) \leq \frac{Cd^n}{(d-1)(d^n-1)} \tag{16}$$

$$\leq \frac{Cd}{(d-1)^2}. \tag{17}$$

Where the last simplification follows from the fact that $d^n - 1 = (d-1)(d^{n-1} + \ldots + 1)$. Note that this bound is independent of the point α. Take an arbitrary $\beta \in \text{PrePer}_{\bar{\mathbb{Q}}}(f)$. This implies that there exist an integer $i \geq 0$ and a periodic point α such that $f^i(\beta) = \alpha$. Applying the first bound we obtained to β and substituting $f^i(\beta) = \alpha$, we get

$$d^i h(\beta) \leq h(\alpha) + C\frac{d^i}{d-1} \tag{18}$$

and applying the second bound obtained for a periodic point α we conclude that

$$\begin{aligned} d^i h(\beta) &\leq \frac{Cd}{(d-1)^2} + C\frac{d^i}{d-1} \\ \implies h(\beta) &\leq C\left(\frac{d}{(d-1)^2 d^i} + \frac{1}{d-1}\right) \\ &\leq C\left(\frac{d}{(d-1)^2} + \frac{1}{d-1}\right) \\ &= C\frac{2d-1}{(d-1)^2}. \end{aligned}$$

Therefore $\forall \beta \in \text{PrePer}_{\bar{\mathbb{Q}}}(f)$

$$h(\beta) \leq C\frac{2d-1}{(d-1)^2}, \tag{19}$$

and thus the height of pre-periodic points is bounded. The statement follows. □

The result above becomes stronger when we restrict to preperiodic points in a number field $\Bbbk$, as then we can apply the second statement of theorem 2.2 giving us only finitely many such points.

Corollary 3.2. *Let $f \in \bar{\mathbb{Q}}(x)$ have degree $d \geq 2$ and fix a number field $\Bbbk/\mathbb{Q}$ then f has at most finitely many $\Bbbk$-preperiodic points.*

Proof. Consider the set of $\mathbb{k}$-preperiodic points,

$$\mathrm{PrePer}_{\mathbb{k}}(f) \subseteq \mathrm{PrePer}_{\bar{\mathbb{Q}}}(f) \tag{20}$$

But by theorem 3.1 the second set has bounded height, thus $\mathrm{PrePer}_{\mathbb{k}}(f)$ has bounded height. Applying the second point of theorem 2.2 implies that $\mathrm{PrePer}_{\mathbb{k}}(f)$ is finite. □

As mentioned in section 2.2, we can often relate preperiodic points of rational maps to torsion points of abelian varieties. If this is the case, then the above corollary implies there can only be finitely many $\mathbb{k}$-torsion points.
A similar result holds for higher dimensional self-morphisms of $\mathbb{A}^n$ however one must restrict to periodic points. Namely, given $f : \mathbb{A}^n \to \mathbb{A}^n$ is a regular affine morphism, then $\mathrm{Per}(f)$ is a set of bounded height (given a generalization of heights) and over number fields is finite ([Sil07] thm. 7.9).

3.2 Periodic points and Good Reduction

In studying the dynamics of rational maps we can also consider the related dynamics of the same maps over finite fields and how they relate. These dynamics over finite fields are often much easier since every point is necessarily preperiodic.

Theorem 3.3. *Let $f \in \mathbb{Q}(x)$ have good reduction at p and let $\alpha \in \mathrm{PrePer}_{\mathbb{Q}}(f)$, then $\tilde{\alpha} \in \mathrm{PrePer}_{\mathbb{F}_p}(f)$. Furthermore if α is periodic of exact period n then $\tilde{\alpha}$ is periodic of exact period $m|n$.*

Proof. We claim that $\widetilde{f^n} = (\tilde{f})^n$. This follows by induction; for $n = 1$ this is the definition, thus assume it holds for some n then $\widetilde{f^{n+1}} = \widetilde{f(f^n)} = \tilde{f}(\widetilde{f^n})$ where the last equality follows from remark 2.2. Applying the induction hypothesis proofs the claim.
By the claim and remark 2.2, it follows that if $f^n(\alpha) = f^k(\alpha)$ then $\tilde{f}^n(\tilde{\alpha}) = \tilde{f}^k(\tilde{\alpha})$ hence $\tilde{\alpha} \in \mathrm{PrePer}_{\mathbb{F}_p}(\tilde{f})$. This also shows that if α is periodic, so must be $\tilde{\alpha}$.
Let m be the exact period of $\tilde{\alpha}$ and write $n = mt + r$ for some positive integers t, r such that $0 \leq r < m$. Thus $\tilde{\alpha} = \tilde{f}^n(\tilde{\alpha}) = \tilde{f}^{mt+r}(\tilde{\alpha}) = \tilde{f}^r(\tilde{f}^{mt}(\tilde{\alpha})) = \tilde{f}^r(\tilde{\alpha})$. But since m is the exact period of $\tilde{\alpha}$, it is the smallest positive integer such that $\tilde{\alpha} = \tilde{f}^m(\tilde{\alpha})$ hence $r = 0$ and $m|n$. □

Theorem 3.4. *Let $f \in \mathbb{Q}(x)$ have degree $d \geq 2$, p be a prime of good reduction for f and let $\alpha \in \mathrm{Per}_{\mathbb{Q}}(f)$ have exact period n, then $n \leq p^3 - p$. Moreover if $p \geq 5$ then the bound can be reduced to $n \leq p^2 - 1$*

Proof. We refer the reader to chapter 2.6 of [Sil07]. □

Remark 3.1. Taking p to be the smallest prime of good reduction gives the best bound.

Example 3.1. Take again the rational map defined in example 2.6, $f(z) = \frac{z^4-8z}{4(z^3+1)}$. It has good reduction at 5, indeed

$$\tilde{f} = f \mod 5 = \frac{z^4 + 2z}{-1(z^3+1)},$$

and $z^4 + 2z$ has no factors in common with $z^3 + 1$ modulo 5. The bound above implies that all periodic points of f have period $n \leq 24$. Computing these points is still difficult as the rational map f^{24} may have degree 4^{24}. Modulo 5 all points are preperiodic, since $\mathbb{Z}/5\mathbb{Z}$ is a finite group and for this example we can easily compute all orbits:

$$\mathrm{Orb}_{\tilde{f}}(\tilde{0}) = \{\tilde{0}\},\ \mathrm{Orb}_{\tilde{f}}(\tilde{1}) = \{\tilde{1}\},\ \mathrm{Orb}_{\tilde{f}}(\tilde{2}) = \{\tilde{2}, \tilde{0}\},\ \mathrm{Orb}_{\tilde{f}}(\tilde{3}) = \{\tilde{3}, \tilde{1}\},\ \mathrm{Orb}_{\tilde{f}}(\tilde{4}) = \{\tilde{4}, \infty\}. \tag{21}$$

Where ∞ denotes the point $(1 : 0) \in \mathbb{P}^1_{\mathbb{F}_5}$. Moreover, looking at the curve projectively we find that $(1 : 0)$ is a fixed point.

4 Elliptic Curves

Let K be an algebraically closed field of characteristic not 2 or 3 ([ST92] sec. 1.3).

Definition 4.1. (Elliptic Curve)
An *elliptic curve over* K (in short Weierstraß form) is a projective curve defined by a homogeneous polynomial of the form $x^3 + axz^2 + bz^3 - y^2z \in K[x, y, z]$, where $a, b \in K$ such that $4a^3 + 27b^2 \neq 0$. The corresponding variety is denoted by $\mathcal{E}$,

$$\mathcal{E} := \{(x : y : z) \in \mathbb{P}^2_K \mid y^2z = x^3 + axz^2 + bz^3\}. \tag{22}$$

In short, we write

$$\mathcal{E} : \; y^2z = x^3 + axz^2 + bz^3.$$

Given that $\mathcal{E}$ is an elliptic curve over K and $\Bbbk \subseteq K$ a sub-field. The set of $\Bbbk$-points on $\mathcal{E}$ is denoted by $\mathcal{E}(\Bbbk)$.

This curve has only one point with zero z-coordinate, namely $(0 : 1 : 0) =: \mathcal{O}$. By considering the line $z = 0$ as the line at infinity, $\mathcal{O}$ is the unique point at infinity. With this choice, the corresponding affine equation is obtained by taking the substitution $X := x/z$ and $Y := y/z$. Throughout the text, we use the variables X and Y to indicate this substitution and that we work with the affine model of $\mathcal{E}$.

Example 4.1. The projective curve introduced in example 2.1 is an elliptic curve with $a = 0$ and $b = 1$. In short,

$$\mathcal{E} : zy^2 = x^3 + z^3. \tag{23}$$

Its affine equation is given by $Y^2 = X^3 + 1$, which we plot over $\mathbb{R}$ and show a branch over $\mathbb{C}$[8] below.

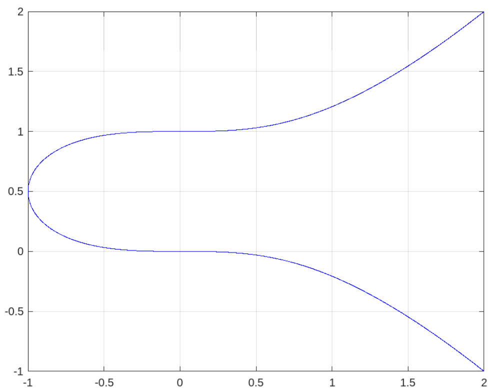

Figure 5: $\mathcal{E}(\mathbb{R})$

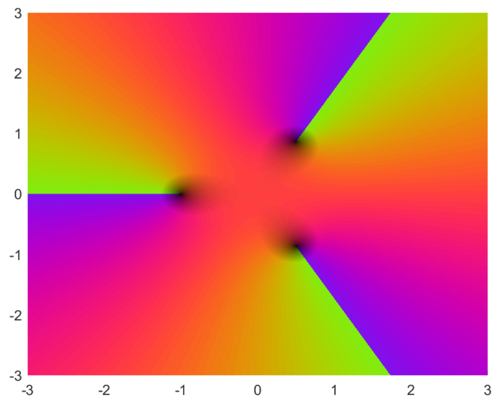

Figure 6: a branch of $\mathcal{E}(\mathbb{C})$

The points on elliptic curves have the structure of an abelian group, as defined in section 1.4 of [ST92], with the point $\mathcal{O}$ as the identity element. As is common for abelian groups, the group operation is denoted with the addition symbol $+$. It is worth noting that, for a curve defined over $\mathbb{Q}$, $\mathcal{E}(\mathbb{Q})$ is finitely generated. This is a major called Mordell's theorem (see [Sil09] VIII.4).

Given that the elliptic curve is in the form of equation 22, the group inverse of a point $P = (x : y : z)$ is the point $(x : -y : z)$ and is denoted by $-P$. With this we can define multiplication from $\mathbb{Z}$ on $\mathcal{E}$. Let $P \in \mathcal{E}$ and $d \in \mathbb{Z}$, then define

$$[d] : \mathcal{E} \longrightarrow \mathcal{E} \quad \text{by} \quad P \longmapsto \begin{cases} \mathcal{O} & , d = 0 \\ \operatorname{sign}(d) \sum_{i=1}^{|d|} P & , \text{otherwise} \end{cases}$$

[8]Note that figure 6 is a phase portrait of the complex function $f(z) = \sqrt{z^3 + 1}$, and the lines protruding from the three roots due to branch cuts.

For convenience, we usually neglect the parentheses in notation and write $d \cdot P$ to mean $[d](P)$. Note that this defines a scalar multiplication on $\mathcal{E}$ giving it a $\mathbb{Z}$-module structure. Thus $\mathrm{End}(\mathcal{E})$ always contains a sub-ring isomorphic to $\mathbb{Z}$, however, there are examples in which this is not the entire endomorphism ring of $\mathcal{E}$. A specific example is treated in 4.4.2, though it should be noted that in most cases this does not occur. The order of a point $P \in \mathcal{E}$ is defined as the minimal integer $d > 1$ such that $dP = \mathcal{O}$.

Notation 4.1. We refer to points, on $\mathcal{E}$, of order d as d-torsion points and reserve the notation 'of order d ' for the order of an elements $\mu \in \mathrm{End}(\mathcal{E})$ and the order of elements in other groups. Moreover, when we refer to $\mathrm{End}(\mathcal{E})$ as a group, this should be understood to be the group of endomorphisms with respect to composition.

4.1 Projection of Elliptic curves onto a Projective Line

Notation 4.2. We refer to the map $[-1]$ as σ.

Note that σ is an involution and thus has order 2 as an element of the endomorphism group. It has at most (in an algebraically closed fields exactly) 4 fixed points, namely $\mathcal{O}$ and the three points of the form $(x : 0 : z)$. These are precisely the 2-torsion points of $\mathcal{E}$. Furthermore, σ commutes with all endomorphisms of $\mathcal{E}$ since it simply gives the inverses of the elements.

Consider the subgroup $\langle\sigma\rangle = \{\sigma, id\}$ of $\mathrm{Aut}(\mathcal{E})$, the automorphism group of $\mathcal{E}$, and the corresponding quotient $\mathcal{E}/\langle\sigma\rangle$ [9]. This allows us to take the natural projection $\pi : \mathcal{E} \to \mathcal{E}/\langle\sigma\rangle$.

Lemma 4.1. *Let $\mathcal{E}$ be an elliptic curve over K and $\langle\sigma\rangle \leq Aut(\mathcal{E})$ be as above, then*

$$\mathcal{E}/\langle\sigma\rangle \cong \mathbb{P}^1_K.$$

Proof. We make use of the Hurwitz formula in 2.1. Consider the map $\pi : \mathcal{E} \to \mathcal{E}/\langle\sigma\rangle$ as above and note that it is a morphism of curves. Also $g(\mathcal{E}) = 1$ (as in example 2.3). Since $\langle\sigma\rangle$ has order 2 we have that the projection is a 2-to-1 map (except at finely many points) and thus $\deg(\pi) = 2$. Denoting $R = \sum_{P\in\mathcal{E}}(e_P - 1)$ and applying the Hurwitz formula we obtain

$$2(1) - 2 = 2(2g(\mathcal{E}/\langle\sigma\rangle) - 2) - \deg(R) \implies g(\mathcal{E}/\langle\sigma\rangle) = 1 - \frac{R}{4}. \tag{24}$$

Since genera are non-negative integer quantities, we have that $R \in \{0, 4\}$. It also cannot be 0 since there exist ramification points, namely the four fixed points of σ mentioned above. Thus $R = 4$ and substituting into 24 gives $g(\mathcal{E}/\langle\sigma\rangle) = 0$. It follows that $\mathcal{E}/\langle\sigma\rangle \cong \mathbb{P}^1_K$ ([Poo09] 34.13). □

4.2 Morphisms of Elliptic Curves and Rational Maps

In what follows, we study how maps between elliptic curves behave with respect to the projection π onto $\mathbb{P}^1_K$. Under the necessary assumptions, we can find a family of maps (or morphisms) which commute with this projection thus allowing us to directly relate many of their properties.

Proposition 4.2. *Let $\mathcal{E}$ and $\mathcal{E}'$ be elliptic curves and let $\varphi : \mathcal{E} \to \mathcal{E}'$ be a morphism such that $\varphi \circ \sigma = \sigma' \circ \varphi$, where σ and σ' are the involution on $\mathcal{E}$ and $\mathcal{E}'$ respectively. Then there exists a unique $\tilde{\varphi}$ such that the diagram*

$$\begin{array}{ccc} \mathcal{E} & \xrightarrow{\varphi} & \mathcal{E}' \\ \pi\downarrow & & \downarrow\pi \\ \mathcal{E}/\langle\sigma\rangle & \xrightarrow{\tilde{\varphi}} & \mathcal{E}'/\langle\sigma'\rangle \end{array} \tag{25}$$

commutes.

[9]In this quotient a point P is identified with $\sigma(P) = -P$.

Proof. Given a point P on an elliptic curve, define the set $S_P := \{\mu(P) \mid \mu \in \langle\sigma\rangle\}$, respectively for $\mathscr{E}'$ by replacing σ with σ'. Let $P, Q \in \mathscr{E}$, then $S_P := \{P, \sigma(P)\}$, likewise for σ'. Note that $S_P = S_Q$ if and only if $Q \in S_P$ and otherwise $S_P \cap S_Q = \varnothing$. By assumption we have that $\sigma'(\varphi(P)) = \varphi(\sigma(P))$, therefore $\varphi(S_P) = S_{\varphi(P)}$. By definition of the projection $\pi(S_P) = \{\pi(P)\}$ and, since the projection π is surjective, for all $\alpha \in \mathbb{P}^1_K$ there a exists a unique set $S_P \subseteq \mathscr{E}$ such that $\pi^{-1}(\alpha) = S_P$. Thus we uniquely define $\tilde{\varphi}$ by applying $\pi \circ \varphi$ to any representative of S_P. □

Corollary 4.3. *Given two elliptic curves $\mathscr{E}$ and $\mathscr{E}'$, and a morphism $\varphi : \mathscr{E} \to \mathscr{E}'$ commuting with σ, then there exists a unique map $f_\varphi : \mathbb{P}^1_K \to \mathbb{P}^1_K$ such that the diagram*

$$\begin{array}{ccc} \mathscr{E} & \xrightarrow{\varphi} & \mathscr{E}' \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ \mathbb{P}^1_K & \xrightarrow{f_\varphi} & \mathbb{P}^1_K \end{array} \tag{26}$$

commutes.

Proof. By lemma 4.1, $\mathscr{E}/\langle\sigma\rangle \cong \mathbb{P}^1_K$. Thus any morphism $\mathscr{E}/\langle\sigma\rangle \to \mathscr{E}'/\langle\sigma\rangle$ descends uniquely to a morphism $\mathbb{P}^1_K \to \mathbb{P}^1_K$ and we can extend diagram 25 to

$$\begin{array}{ccc} \mathscr{E} & \xrightarrow{\varphi} & \mathscr{E}' \\ \downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi} \\ \mathscr{E}/\langle\sigma\rangle & \xrightarrow{!\tilde{\varphi}} & \mathscr{E}'/\langle\sigma\rangle \\ \downarrow{\scriptstyle\cong} & & \downarrow{\scriptstyle\cong} \\ \mathbb{P}^1_K & \xrightarrow{!f_\varphi} & \mathbb{P}^1_K \end{array}, \tag{27}$$

which commutes in each square. It follows that f_φ is the unique map making 26 commute. □

Over the field of Complex numbers such maps are referred to as Lattès maps (formally defined in [Mil04]) which are historically the first examples of rational maps with empty Fatou set. In what follows we do not restrict to the complex numbers as the construction is still valid over any algebraically closed field (of characteristic not 2 or 3) and the most useful dynamical properties remain true.

4.3 The Dynamical Approach

To relate the points on an elliptic curve to dynamical notions we take $\mathscr{E}' = \mathscr{E}$ and $\varphi : \mathscr{E} \to \mathscr{E}$ a self morphisms commuting with σ. This allows us to consider the dynamics of $(\mathscr{E}, \varphi)$ and in time relate the torsion points on $\mathscr{E}$ to preperiodic points of rational maps as in the table in section 2.2. This relation is what, in large, motivates the study of arithmetic dynamics. By commutativity of diagram 26, we can study properties of these morphisms by studying the related maps of projective lines.

Proposition 4.4. *Given an elliptic curve $\mathscr{E}$ and a morphism $\varphi : \mathscr{E} \to \mathscr{E}$ commuting with σ, let $f_\varphi : \mathbb{P}^1_K \to \mathbb{P}^1_K$ be the unique map making diagram 26 commute with respect to φ. Then for all $n \in \mathbb{Z}_{>0}$, f_φ^n is the unique map making 26 commute with respect to φ^n.*

Proof. We do induction on n. For $n = 1$ it follows from the assumption, let us assume that f_φ^{n-1} is the unique map making 26 commute with respect to φ^{n-1}. It follows that, for n, we have the diagram

$$\begin{array}{ccccc} \mathscr{E} & \xrightarrow{\varphi^{n-1}} & \mathscr{E} & \xrightarrow{\varphi} & \mathscr{E} \\ \downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi} \\ \mathbb{P}^1_K & \xrightarrow{f_\varphi^{n-1}} & \mathbb{P}^1_K & \xrightarrow{f_\varphi} & \mathbb{P}^1_K \end{array} \tag{28}$$

where the top row is φ^n and the bottom row f_φ^n. By assumption and hypothesis both squares commute therefore the whole diagram commutes. Thus f_φ^n makes diagram 26 commute with respect to φ^n which concludes the induction. □

This allows us to consider the dynamics of the related maps. Let us look at how the preperiodic points of these relate to one another.

Proposition 4.5. *Let $\mathcal{E}$ be an elliptic curve and take φ and f_φ as above and let $P \in \mathcal{E}$. Then P is a preperiodic point of φ if an only if $\pi(P)$ is a preperiodic point of f_φ.*

Proof. Let P be such that $\varphi^n(P) = \varphi^m(P)$ for some $n, m \in \mathbb{Z}_{\geq 0}$ distinct. By proposition 4.4 we have that $\pi \circ \varphi^n(P) = f_\varphi^n \circ \pi(P)$ and $\pi \circ \varphi^m(P) = f_\varphi^m \circ \pi(P)$, therefore $f_\varphi^n(\pi(P)) = f_\varphi^m(\pi(P))$ and $\pi(P)$ is a preperiodic point of f.

Conversely, let $\pi(P)$ be a preperiodic point[10] of f, then $f_\varphi^n(\pi(P)) = f_\varphi^m(\pi(P))$ for some $n, m \in \mathbb{Z}_{\geq 0}$ distinct. By the commutativity of 26, we have that $\pi \circ \varphi^n(P) = \pi \circ \varphi^m(P)$. With the same notation as in the proof of proposition 4.2, this gives $S_{\varphi^n(P)} = S_{\varphi^m(P)}$ hence $\varphi^n(P) \in S_{\varphi^m(P)}$. This gives two possibilities; either $\varphi^n(P) = \varphi^m(P)$, in which case we are done, or $\varphi^n(P) = -\varphi^m(P)$. In the second case let us assume that $m < n$ and write $n = k + m$ thus $\varphi^{k+m}(P) = -\varphi^m(P)$. Set $s = 2k + m$, thus

$$\begin{aligned}
\varphi^s(P) &= \varphi^{2k+m}(P) \\
&= \varphi^k \circ \varphi^{k+m}(P) \\
&= \varphi^k(-\varphi^m(P)) \\
&= -\varphi^{k+m}(P) \\
&= \varphi^m(P)
\end{aligned}$$

Where we use the assumption that φ commutes with σ. Therefore P is a preperiodic point of φ. □

Remark 4.1. (exact period)
Take notation as in the proof above and consider the special case of periodic points of f_φ. By commutativity, $\pi(P) = f_\varphi^n \circ \pi(P) = \pi \circ \varphi^n(P)$. This implies that $\varphi^n(P) \in S_P$, hence if n is the exact period of $\pi(P)$ with respect to f_φ then P has exact period n or $2n$ with respect to φ.

This confirms that we may look at the dynamics of $(\mathcal{E}, \varphi)$ and $(\mathbb{P}^1_K, f_\varphi)$ almost interchangeably. There is a particularly interesting family of maps $\varphi = [d]$ (for $d > 1$) which allows us to look at torsion points as preperiodic points. The same applies when $d < -1$, though including it in the statement makes it unnecessarily convoluted. Note that $[d]^n(P) = [d^n](P) = d^n P$. We approach this by considering the dynamics on $(\mathcal{E}, [d])$.

Corollary 4.6. *Let $\mathcal{E}$ be an elliptic curve, then $\forall d \in \mathbb{Z}_{>1}$, $\mathrm{PrePer}(f_{[d]}) = \pi(Tor(\mathcal{E}))$.*

Proof. Fix an arbitrary $d \in \mathbb{Z}_{>1}$, by proposition 4.5 we have that $\mathrm{PrePer}(f_{[d]}) = \pi(\mathrm{PrePer}([d]))$ since σ commutes with all endomorphisms, thus it suffices to show that $\mathrm{PrePer}([d]) = Tor(\mathcal{E})$.

Assume that P is a torsion point of $\mathcal{E}$, hence there exists an integer $k > 1$ such that $kP = \mathcal{O}$. Consider the set of values given by iterating the map $[d]$ on P,

$$\mathrm{Orb}_{[d]}(P) = \left\{P, dP, d^2P, d^3P, d^4P, \dots\right\} = \left\{d^nP \mid n \in \mathbb{Z}_{\geq 0}\right\}. \tag{29}$$

Since $kP = \mathcal{O}$, we have that the above set is in bijection with the set

$$\{d^n \mod k \mid n \in \mathbb{Z}_{\geq 0}\}, \tag{30}$$

[10] By surjectivity of π, all points of $\mathbb{P}^1_K$ can be written as $\pi(P)$ for some $P \in \mathcal{E}$.

which is finite since its elements are those of a finite group. Thus the orbit is finite implying that the point P is preperiodic for $[d]$, hence $Tor(\mathcal{E}) \subseteq \mathrm{PrePer}([d])$.

Conversely, Let $P \in \mathrm{PrePer}([d])$. Thus $d^n P = d^m P$ for some distinct $n, m \in \mathbb{Z}_{>0}$, it follows that $(d^n - d^m)P = \mathcal{O}$. Therefore there exists an integer $k|(d^n - d^m)$ such that $kP = \mathcal{O}$ hence $\mathrm{PrePer}([d]) \subseteq Tor(\mathcal{E})$. Thus $\mathrm{PrePer}([d]) = Tor(\mathcal{E})$ which concludes the proof. □

Remark 4.2. For a given elliptic curve, all maps of the form $f_{[d]}$ have the same preperiodic points. Furthermore, the proof of the above indicates that: P is an l-torsion point and l is coprime to $d \in \mathbb{Z}$ if and only if P is a *periodic* point and $\#\mathrm{Orb}_{[d]}(P) = \mathrm{ord}(d \mod l) =: N$ is the exact period of P with respect to $[d]$. As mentioned in remark 4.1, this is either exactly or twice the period of $\pi(P)$. Hence in this special case, the exact period of $\pi(P)$ with respect to $f_[d]$ is either $\frac{N}{2}$ or N. In the particular case of the map $[2]$, a point P is periodic if and only if it is an l-torsion point and l is odd.

Example 4.2. Let P be a 9-torsion point and take the doubling map $[2]$. Then the Orbit of P is

$$\begin{aligned}\mathrm{Orb}_{[2]}(P) &= \{P, 2P, 4P, 8P, 16P, 32P, 64P, \ldots\} \\ &= \{P, 2P, 4P, 8P, 7P, 5P\} \\ &= S_P \dot{\cup} S_{2P} \dot{\cup} S_{4P}.\end{aligned}$$

Note that $[2]^3(P) = 8P = -P$, thus $\pi(P)$ is a *periodic* point of $f_{[2]}$ with exact period 3. However, the point P is a *periodic* point of $[2]$ with exact period $6 = \mathrm{ord}(2 \mod 9)$.

4.4 The Related Rational Maps

The specific projection $\pi : \mathcal{E} \to \mathbb{P}^1_K$ can be given by $(x : y : z) \mapsto (x : z)$ for $z \neq 0$ and $\mathcal{O} \mapsto (1 : 0)$. With respect to this projection we compute the following examples.

4.4.1 The doubling map

Take an elliptic curve $\mathcal{E}$, in short Weierstraß form with coefficients $a, b \in K$ as in definition 4.1. As mentioned above all maps $[d]$ have the same preperiodic points. We look at the simplest case $[2]$, the doubling map on $\mathcal{E}$. By corollary 4.6 one can compute the torsion points of $\mathcal{E}$ by computing the preperiodic points of the respective f_φ map. Let us first consider points P on the chosen affine patch of $\mathcal{E}$ (points of the form $(X : Y : 1)$). By commutativity of 26, the function $f_{[2]}$ satisfies $\pi(2P) = f_{[2]} \circ \pi(P) = f_{[2]}((X : 1))$. Applying the addition formulas for a points on $\mathcal{E}$ ([ST92] ch.1.4) we have that

$$\begin{aligned}2P =& P + P = \left(\lambda^2 - 2X : \lambda(3X - \lambda^2) - Y : 1\right), \\ &\text{where} \quad \lambda = \frac{3X^2 + a}{2Y}.\end{aligned}$$

Therefore $\pi(2P) = (\lambda^2 - 2X : 1) = f_{[2]}((X : 1))$. Computing it explicitly we get:

$$\begin{aligned}f_{[2]}((X : 1)) &= \left(\lambda^2 - 2X : 1\right) \\ &= \left(\frac{(3X^2 + a)^2}{4Y^2} - 2X : 1\right) \\ &= \left(\frac{X^4 - 2aX^2 - 8bX + a^2}{4(X^3 + aX + b)} : 1\right) \\ &= \left(x^4 - 2az^2x^2 - 8bz^3x + a^2z^4 : 4(zx^3 + az^3x + bz^4)\right) \\ &=: f_{[2]}((x, z))\end{aligned}$$

Where in the third line we use that $Y^2 = X^3 + aX + b$, and in the forth line we substitute $X = \frac{x}{z}$ (since by assumption $z \neq 0$), clear out the powers of z and multiply out into the second coordinate. Therefore for $z \neq 0$ the above $f_{[2]}$ is a well defined map of projective lines. To show that it is well defined everywhere it suffices to check that the image of the special point $(1 : 0) = \pi((0 : 1 : 0))$ coincides with the above equation. Indeed it does since $f_{[2]}(1 : 0) = (1 : 0)$, moreover it is a fixed point of $f_{[2]}$ and $\pi \circ [2](0 : 1 : 0) = \pi(0 : 1 : 0) = (1 : 0) = f_{[2]}(1 : 0) = f_{[2]} \circ \pi(0 : 1 : 0)$, it makes diagram 26 commute. Hence $f_{[2]} : \mathbb{P}^1_K \longrightarrow \mathbb{P}^1_K$ defined by

$$f_{[2]}((x : z)) = \left(x^4 - 2az^2x^2 - 8bz^3x + a^2z^4 : 4(zx^3 + az^3x + bz^4)\right) \tag{31}$$

is the unique map making 26 commute. Note that its degree is 4 which is necessarily also the degree of the multiplication map. As one may suspect this degree grows as we choose larger d and since the preperiodic points of $f_{[d]}$ are the same for all $d \neq 0$ it may seem sufficient to consider only this case, however, the exact period of the same point may differ and its periodic/preperiodic nature may vary as per remark 4.2. As such, in some applications it may be beneficial to compute such maps for higher values of $[d]$. If we restrict to the case $K = \bar{\mathbb{Q}}$ and look at the affine part of f_φ, then corollary 2.2 allows us to conclude that it has only finitely many $\Bbbk$-preperiodic points for any number field $\Bbbk/\mathbb{Q}$. In particular there are only finely many $\mathbb{Q}$-preperiodic points which, by corollary 4.6, implies that there are at most finitely many $\mathbb{Q}$-torsion points on the elliptic curve.

Example 4.3. Consider the elliptic curve from example 2.1 given by $zy^2 = x^3 + z^3$. Here $a = 0$ and $b = 1$ thus by equation 31 we have that

$$f_{[2]}(x, z) = \left(x^4 - 8z^3x : 4(zx^3 + z^4)\right) \tag{32}$$

for this specific curve. Which, in the affine representation, is the rational map

$$f_{[2]}(X) = \frac{X^4 - 8X}{4(X^3 + 1)}. \tag{33}$$

Recall that this is the rational map of example 2.6. By theorem 2.2 (Northcott) and Corollary 4.6, we have that $Tor(\mathcal{E}(\Bbbk))$ is finite over any number field $\Bbbk/\mathbb{Q}$. Furthermore the bound of theorem 3.4, as in example 3.1, implies that the exact period of $\pi(P) \in \mathrm{Per}_{\mathbb{Q}}(f_{[2]})$ is at most 24 and as discussed in remark 4.1 this implies that P has exact period at most 48. This is still rather far from the maximal possible torsion order which is 12 by Mazur's theorem ([Sch04]), nevertheless it does give a bound.

4.4.2 Complex multiplication

An elliptic curve, $\mathcal{E}$, is said to have complex multiplication when the endomorphism ring of $\mathcal{E}$ is not isomorphic to $\mathbb{Z}$ ([ST92] ch.6). Since it always contains $\mathbb{Z}$ this means that there are other endomorphisms. Take for example the curve

$$\mathcal{E} : zy^2 = x^3 + xz^2.$$

Here we have the extra endomorphism given by $(x : y : z) \mapsto (-x : iy : z)$, let it be denoted by φ. Through the addition formulas it may be verified that his is indeed a homomorphism of groups. We look at the corresponding map f_φ making 26 commute. Similarly to the above examples we require that $f_\varphi((X : 1)) = \pi \circ \varphi((X : Y : 1)) = (-X : 1) = (-x : z)$ whenever $z \neq 0$. Thus we define $f_\varphi((x : z)) := (-x : z)$ and note that it indeed fixes $(1 : 0)$ and by construction makes 26 commute. This is a rather simple rational map on the affine patch, however, it doesn't give much information about the torsion points.

4.4.3 Translation

Now consider the morphism φ defined by $Q \mapsto Q+P$. In other words we translate all points by P, note that this doesn't fix the group identity $(0:1:0)$ (unless $P=(0:1:0)$ in which case φ is the identity morphism) and therefore isn't an endomorphism of groups. This example illustrates that, to have a well defined map f_φ making 26 commute, it is necessary that φ commutes with σ. If we choose P such that it is not the identity or of the form $(x:0:z)$ then φ does not commute with σ since there exist points Q such that $-(Q+P) \neq (-Q)+P$ (this equality only holds if $P=-P$ which we have excluded). In this case we would require that our function $f_\varphi(\pi(Q)) = f_\varphi(\pi(-Q)) = \pi(Q+P) = \pi(-Q+P)$ which is absurd. Thus no such f_φ can exist.

Let us consider the cases we excluded above where P is of the form $(x:0:z)$. Then $P=-P$ and φ commutes with σ thus there exists a map f_φ making 26 commute.
Take for example the curve $\mathcal{E}: y^2z = x^3 - xz^2$ and choose $P=(0:0:1)$. Due to the addition formulas of the elliptic curve we have that $P \mapsto \mathcal{O}$ and $\mathcal{O} \mapsto P$ which are the special points that map to and fro the point at infinity and cannot be described by a rational equation on the affine part. For the remaining points we have that

$$\begin{aligned}\varphi(X:Y:1) &= \left(\lambda^2 - X : \lambda(X-(\lambda^2-X)) - Y : 1\right)\\ &= \left(\frac{-1}{X} : \frac{Y}{X^2} : 1\right)\\ &= \left(-xz : yz : x^2\right)\end{aligned}$$

This suggests that $f_\varphi((x:z)) = (-z:x)$. Note that this also works for $\pi(P) = (0:1) \mapsto (1:0) = \pi(\mathcal{O}) = \pi(\varphi(P))$ and $\pi(\mathcal{O}) = (1:0) \mapsto (0:1) = \pi(P) = \pi(\varphi(\mathcal{O}))$. Thus this f_φ is the unique one making 26 commute with respect to φ given by addition of a point.

5 Lattès maps

Here we follow section 1.6.3 of [Sil07]. Fix $K=\mathbb{C}$, the maps that arise out of commutativity of 26 with the maps $[d]$ over $\mathbb{C}$ are called Lattès maps. As mentioned before, they are of historical importance to dynamics as they present the first examples of rational maps with empty Fatou set, which we here present. Unlike the previous examples where we make statements about $\mathcal{E}$ based on the dynamical properties of f_φ, in this example we use the algebraic structure of $\mathcal{E}$ (in particular its group structure) to make statements about the dynamics of the related rational map f_φ.

Theorem 5.1. *Let $\mathcal{E}$ be an elliptic curve over $\mathbb{C}$, then there exists a lattice $L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} \subseteq \mathbb{C}$ for some $\omega_i \in \mathbb{C}$ such that $\mathcal{E} \cong \mathbb{C}/L$ as groups. ([Sil09] sec VI.5)*

Thus replacing $\mathcal{E}$ with $\mathbb{C}/L$ in diagram 26 yields the commutative diagram

$$\begin{array}{ccc} \mathbb{C}/L & \xrightarrow{[d]} & \mathbb{C}/L \\ \wp\downarrow & & \downarrow\wp \\ \mathbb{P}^1 & \xrightarrow{f_\varphi} & \mathbb{P}^1 \end{array}, \tag{34}$$

where $\wp$ is a modified Weierstraß $\wp$-function ([Sil09] sec. VI.3) composed with the projection and is a meromorphic function[11]. Let $z \in \mathbb{C}/L$, by commutativity of the above we have that

$$f_{[d]} \circ \wp(z) = \wp(dz) \tag{35}$$

[11] Holomorphic everywhere except at a set of isolated points.

and by replacing $\mathcal{E}$ with $\mathbb{C}/L$ in proposition 4.4 we have that $f^n_{[d]} \circ \wp(z) = \wp(d^n z)$. Thus the points of period $m|n$ are exactly the fixed points of $f^n_{[d]} \circ \wp(z)$. Let us consider the fixed points of $f_{[d]}$[12] in the image of $\wp$, which we denote by $\wp(\zeta)$. By 35 these must satisfy $\wp(d\zeta) = \wp(\zeta)$ and since $\wp$ is an isomorphism on $\mathbb{C}/L$ composed with the projection, this gives that $d\zeta = \pm\zeta \mod L$.
By differentiating equation 35 with the chain rule, we obtain

$$f'_{[d]}(\wp(z)) \cdot \wp'(z) = d\wp'(dz). \tag{36}$$

Taking ζ to be a as above, we use that $d\zeta = \pm\zeta \mod L$ thus $\wp'(d\zeta) = \wp'(\pm\zeta) = \pm\wp'(\zeta)$ and $f'_{[d]}(\wp(\zeta)) \cdot \wp'(\zeta) = \pm d\wp'(\zeta)$. Assuming that $\wp(\zeta) \neq 0$ or ∞ we get the condition $f'_{[d]}(\wp(\zeta)) = \pm d$. Thus these fixed points have multipliers $\lambda_{f^n_{[d]}} = \pm d^n$ and therefore are all repelling points. We conclude that these points are all contained in the Julia set as in definition 2.10.

Let us look at the points satisfying $dz = \pm z \mod L$ in more detail, take $z = a\omega_1 + b\omega_2$. In other words we require that $da\omega_1 + db\omega_2 = \pm a\omega_1 + \pm b\omega_2 + k\omega_1 + l\omega_2$ for $k, l \in \mathbb{Z}$. Since ω_1 and ω_2 are linearly independent over $\mathbb{Z}$ we find that $a = \frac{k}{d\mp 1}$ and $b = \frac{l}{d\mp 1}$. We pass to a fixed d, the set of points points such that $dz = \pm z \mod L$,

$$\{z \in \mathbb{C}/L \mid \exists n \in \mathbb{Z}_{\geq 1} \mid z = \pm d^n z \mod L\} = \left\{ \frac{k}{d^n \mp 1}\omega_1 + \frac{l}{d^n \mp 1}\omega_2 \mod L \mid l, k, n \in \mathbb{Z} \text{ and } n > 0 \right\},$$

is dense in $\mathbb{C}/L$. Since $\wp$ covers $\mathbb{P}^1$ thus the fixed points of $f_{[d]^n}$ or equivalently the periodic points of $f_{[d]}$ are dense in $\mathbb{P}^1$. However by the above argument all such points are contained in the Julia set of $f_{[d]}$ and since by definition the Julia set is closed, thus the closure of all periodic points must be contained in the Julia set. This, however, is all of $\mathbb{P}^1$ since those points are dense. Hence The Julia set is the entire space $\mathbb{P}^1$ and the Fatou set is empty.

Example 5.1. The map in example 4.4.1 is a Lattès map. In particular every rational map on $\mathbb{P}^1$ of the form

$$f(x:z) = \left(x^4 - 2az^2x^2 - 8bz^3x + a^2z^4 : 4(zx^3 + az^3x + bz^4)\right),$$

where $a, b \in \mathbb{C}$ satisfy $4a^3 + 27b^2 \neq 0$, has empty Fatou set.

5.1 A Generalization of Lattès maps

The construction of quotients leading to maps defined by commutativity of 26 is loosely referred to as a Lattès construction. In what follows we consider how it may be generalized. For this procedure let us remain with $K = \mathbb{C}$. As mentioned before the Lattès maps are rational maps making diagram 26, however it can occur that there exist other subgroups $\mathcal{G}$ of $\mathrm{Aut}(\mathcal{E})$ which yield $\mathcal{E}/\mathcal{G} \cong \mathbb{P}^1_K$. Then, replacing $\langle\sigma\rangle$ with $\mathcal{G}$, we can obtain another map f_φ making the diagram 26 commute with respect to $\pi : \mathcal{E} \longrightarrow \mathcal{E}/\mathcal{G} \xrightarrow{\cong} \mathbb{P}^1_K$. These are sometimes referred to as *reduced Lattès maps* though we will make no such distinction ([Sil07] ch. 6.6).

Example 5.2. Consider our example $\mathcal{E} : zy^2 = x^3 + z^3$ over K and note that this curve has complex multiplication. In what follows let us denote the third root of unity by ζ_3. We find that $(\zeta_3 x : y : z)$ is a point on $\mathcal{E}$ whenever $(x : y : z) \in \mathcal{E}$ hence $[\zeta_3] : \mathcal{E} \to \mathcal{E}$ defined by $(x : y : z) \mapsto (\zeta_3 x : y : z)$ is an endomorphism of $\mathcal{E}$. Moreover it is a bijective endomorphism with inverse $[\zeta_3^2] = [\zeta_3] \circ [\zeta_3]$ and hence an automorphism of order 3. Let us take $\mathcal{G} = \langle\zeta_3\rangle \leq \mathrm{Aut}(\mathcal{E})$ and the natural projection $\pi : \mathcal{E} \to \mathcal{E}/\mathcal{G}$. We begin by showing that the genus of $\mathcal{E}/\mathcal{G}$ is 0. Note

[12] Since d can be chosen arbitrarily it suffices to consider only the fixed point.

that π has degree 3, thus applying the Riemann-Hurwitz formula (analogously to lemma 4.1) we obtain

$$g(\mathcal{E}/\mathcal{G}) = 1 - \frac{R}{2\deg(\pi)} = 1 - \frac{R}{6}. \tag{37}$$

Since genera are non-negative integer quantities, it suffices to show that the ramification is not 0. To this end, consider the point at infinity, $\mathcal{O}$, which is fixed under the action of $\mathcal{G}$ and hence has ramification index 3. This is enough to conclude that R is not 0, thus $R = 1$ and $g(\mathcal{E}/\mathcal{G}) = 0$. The remaining ramification points are $(0 : \pm 1 : 1)$, the fixed points under the action of $\mathcal{G}$, each having multiplicity 3 thus indeed $R = \sum(e_P - 1) = 6$. Moreover $\mathcal{E}/\mathcal{G}(K)$ is nonempty since it contains at least $\pi(\mathcal{O})$, thus $\mathcal{E}/\mathcal{G} \cong \mathbb{P}^1_K$ ([Poo09] 34.13).

Together with $\langle\sigma\rangle$ discussed in section 4.1, this gives an example of a curve with two subgroups giving rise to Lattès examples. Curiously, This particular curve exhibits one more group with this property.

Example 5.3. Take the same curve as in the above example 5.2 and consider the action of the group $\mathcal{G} = \langle \sigma, \zeta_3 \rangle \leq \mathrm{Aut}(\mathcal{E})$ (in fact this is the entire automorphism group[13] of $\mathcal{E}$, see [Sil09] thm. III.10.1). Take again the natural projection $\pi : \mathcal{E} \to \mathcal{E}/\mathcal{G}$, note that this time $\deg(\pi) = 6$ and applying the Riemann-Hurwitz formula as in equation 37 yields

$$g(\mathcal{E}/\mathcal{G}) = 1 - \frac{R}{12}.$$

Again, the ramification cannot be 0, since the point at infinity, $\mathcal{O}$, has multiplicity 6 (it is a fixed point for both σ and $[\zeta_3]$) and $\pi(\mathcal{O}) \in \mathcal{E}/\mathcal{G}(K)$. Thus $\mathcal{E}/\mathcal{G} \cong \mathbb{P}^1_K$ ([Poo09] 34.13). For this case, computing the ramification points explicitly yields, the point at infinity with multiplicity 6, the three fixed points of σ (excluding $\mathcal{O}$) of multiplicity 2 and the two fixed points of $[\zeta_3]$ of multiplicity 3 giving precisely $R = 12$.

In this case, quotients by all subgroups of $\mathrm{Aut}(\mathcal{E})$ yields a valid projection although to obtain a *Lattès* map f_φ corresponding to a morphism φ, we must require that φ is invariant under the action of $\mathcal{G}$.

Notation 5.1. Let $\mathcal{G} \leq \mathrm{Aut}(\mathcal{E})$, we denote the set of points that are invariant under the action of $\mathcal{G}$ by

$$S_P^{\mathcal{G}} := \{\mu(P) \mid \mu \in \mathcal{G}\}. \tag{38}$$

If it is apparent from the context we neglect the $\mathcal{G}$ in notation.

In this sense, to show that $\varphi : \mathcal{E} \to \mathcal{E}$ is invariant under the action of $\mathcal{G}$, it suffices to show that $\varphi(S_P^{\mathcal{G}}) \subseteq S_{\varphi(P)}^{\mathcal{G}}$. Note that this implies equality since the two sets $S_P^{\mathcal{G}}$ and $S_Q^{\mathcal{G}}$ are either disjoint or equal.

Lemma 5.2. *Let $K = \mathbb{C}$, $\mathcal{E}$ be an elliptic curve over K and $\mathcal{G} \leq Aut(\mathcal{E})$ be nontrivial, then $\mathcal{E}/\mathcal{G} \cong \mathbb{P}^1_K$.*

Proof. Take the natural projection $\pi : \mathcal{E} \to \mathcal{E}/\mathcal{G}$, we have that $\deg(\pi) = \#\mathcal{G} =: n$. Likewise $\#S_P^{\mathcal{G}} = n$ (since $S_P^{\mathcal{G}} = \pi^{-1}(\pi(P))$) for all but finitely many points $P \in \mathcal{E}(K)$, in particular $\#S_{\mathcal{O}}^{\mathcal{G}} = 1$ for all possible groups $\mathcal{G}$ (since they are group automorphisms by assumption). Applying the Riemann-Hurwitz formula as in equation 37 we obtain

$$g(\mathcal{E}/\mathcal{G}) = 1 - \frac{R}{2n},$$

and $R \neq 0$ since the ramification index of π at $\mathcal{O}$ is n. Furthermore $\pi(\mathcal{O}) \in \mathcal{E}/\mathcal{G}(K)$, by proposition 34.13 of [Poo09] we conclude that $\mathcal{E}/\mathcal{G} \cong \mathbb{P}^1_K$. ☐

[13] It is also cyclic and is generated by $[\zeta_6] = [\zeta_3^2] \circ \sigma$. To avoid confusion we keep the two generating elements σ and ζ_3.

This allows us to generalize the Lattès construction to quotients over other subgroups.

Proposition 5.3. *Let $K = \mathbb{C}$, $\mathcal{E}$ be an elliptic curve over K and $\mathcal{G} \leq Aut(\mathcal{E})$ be nontrivial, $\pi : \mathcal{E} \to \mathbb{P}^1_K$ a projection such that $\pi^{-1}(\pi(P)) = S_P^{\mathcal{G}}$ for all $P \in \mathcal{E}$ and $\varphi : \mathcal{E} \to \mathcal{E}$ a morphism such that $\varphi(S_P^{\mathcal{G}}) \subseteq S_{\varphi(P)}^{\mathcal{G}}$. Then there exists a unique map f_φ making the diagram*

$$\begin{array}{ccc} \mathcal{E} & \xrightarrow{\varphi} & \mathcal{E} \\ \pi \downarrow & & \downarrow \pi \\ \mathbb{P}^1_K & \xrightarrow{f_\varphi} & \mathbb{P}^1_K \end{array} \tag{39}$$

commute.

Proof. By assumption $\varphi(S_P^{\mathcal{G}}) \subseteq S_{\varphi(P)}^{\mathcal{G}}$, and since the sets are either disjoint or equal we have that $\varphi(Q) \in S_{\varphi(P)}^{\mathcal{G}}$ if and only if $Q \in S_P^{\mathcal{G}}$. Thus, analogously to proposition 4.2, we can define a unique map f_φ making diagram 39 commute by mapping $\alpha \in \mathbb{P}^1_K$ to the unique element in $\pi \circ \varphi \circ \pi^{-1}(\alpha) = \pi\left(S_{\varphi(P)}^{\mathcal{G}}\right)$ (for any $P \in \pi^{-1}(\alpha)$). □

Remark that the lemma is necessary for the existence of a projection with the property that $\pi^{-1}(\pi(P)) = S_P^{\mathcal{G}}$. Furthermore, such Lattès examples indeed exist; the endomorphisms $[d]$, for $d \in \mathbb{Z}$ non-zero, commute with all possible elements in $\mathrm{Aut}(\mathcal{E})$ giving rise to a family of rational maps $f_{[d]}$ for each π.

Remark 5.1. The possible automorphism groups of elliptic curves over fields of characteristic not 2 or 3 (as can be found in [Sil09] cor. III.10.2) are exactly $\langle\sigma\rangle$, $\langle[i]\rangle$ and $\langle[\zeta_6]\rangle = \langle\sigma, [\zeta_3]\rangle$. The groups other than $\langle\sigma\rangle$ arise on curves with complex multiplication. Note that all the automorphism groups contain $\langle\sigma\rangle$ as a subgroup. Thus the only possible subgroups giving rise to $\mathbb{P}^1$ in the quotient are $\langle\sigma\rangle$, $\langle[i]\rangle$, $\langle[\zeta_3]\rangle$ and $\langle[\zeta_6]\rangle$.

6 The Surface Given by two Elliptic Curves and Generalized Lattès maps

A natural way in which one may generalize Lattès maps to abelian varieties A of dimension n is to define them as maps commuting with a morphism $\varphi : A \to A$. In other words, we call a map f_φ Lattès if it makes the diagram

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & A \\ \pi \downarrow & & \downarrow \pi \\ \mathbb{P}^n & \xrightarrow{f_\varphi} & \mathbb{P}^n \end{array} \tag{40}$$

commute. The issue is that, in general, it is rare for the quotient $A/\mathcal{G}$, where $\mathcal{G} \leq \mathrm{Aut}(A)$, to be isomorphic to $\mathbb{P}^n$ ([DeM23] sec. 1.2). Nevertheless it can be done for the product of two elliptic curves.

6.1 Two Elliptic Curves

Given two elliptic curves $\mathcal{E}_1$ and $\mathcal{E}_2$ over K, we can consider the surface given by $\mathcal{E}_1 \times \mathcal{E}_2$ in $\mathbb{P}^2_K \times \mathbb{P}^2_K$. Let us restrict to the case $K = \mathbb{C}$, the projection maps described in section 4.1 allow us to define a component-wise projection from the surface $\mathcal{E}_1 \times \mathcal{E}_2$ to the ruled surface $\mathbb{P}^1 \times \mathbb{P}^1$.

Proposition 6.1. *Let $\mathcal{E}_1$ and $\mathcal{E}_2$ be elliptic curves over $\mathbb{C}$, $\mathcal{E}_1 \times \mathcal{E}_2$ the corresponding surface, σ_i the involution on $\mathcal{E}_i$ as in 4.2 and $\pi : \mathcal{E}_1 \times \mathcal{E}_2 \to \mathbb{P}^1 \times \mathbb{P}^1$ the component-wise projection. Set $\mathcal{G} = \langle (\sigma_1, id), (id, \sigma_2) \rangle$. If $\varphi : \mathcal{E}_1 \times \mathcal{E}_2 \to \mathcal{E}_1 \times \mathcal{E}_2$ is a morphism such that $S_P^{\mathcal{G}} \subseteq S_{\varphi(P)}^{\mathcal{G}}$, then there exists a unique map f_φ making the diagram*

$$\begin{array}{ccc} \mathcal{E}_1 \times \mathcal{E}_2 & \xrightarrow{\quad \varphi \quad} & \mathcal{E}_1 \times \mathcal{E}_2 \\ \Big\downarrow{\scriptstyle \pi} & & \Big\downarrow{\scriptstyle \pi} \\ \mathbb{P}^1 \times \mathbb{P}^1 & \xrightarrow{\quad f_\varphi \quad} & \mathbb{P}^1 \times \mathbb{P}^1 \end{array} \tag{41}$$

commute.

Proof. Consider the set

$$S_{(P,Q)} := \{\mu(P,Q) \mid \mu \in \mathcal{G}\} = \{(P,Q), (-P,Q), (P,-Q), (-P,-Q)\}.$$

Note that $\pi(S_{(P,Q)}) = \{\pi(P,Q)\}$; in other words, for all $\alpha \in \mathbb{P}^1 \times \mathbb{P}^1$, $\pi^{-1}(\alpha) = S_{(P,Q)}$ for some $(P,Q) \in \mathcal{E}_1 \times \mathcal{E}_2$. Again we see that two such sets, at (P_1,Q_1) and (P_2,Q_2), are either disjoint or equal. By assumption $\varphi(\mu(P,Q)) = \mu'(\varphi(P,Q))$, therefore $\varphi(S_{(P,Q)}) = S_{\varphi(P,Q)}$. Hence we can define a unique $f_\varphi : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1 \times \mathbb{P}^1$ by taking any representative of $\pi^{-1}(\alpha)$ and applying $\pi \circ \varphi$. □

This procedure can be extended inductively to a product of n-many elliptic curve. The aim, however, is to generalize the example in 39 and produce a map making diagram 40 commute. That is, to obtain a self maps of $\mathbb{P}^2$ commuting with the chosen morphisms of the elliptic curve (recall that $\mathbb{P}^2 \ncong \mathbb{P}^1 \times \mathbb{P}^1$). We will restrict to the case where $\mathcal{E}_1 = \mathcal{E}_2 = \mathcal{E}$ and consider the surface $\mathcal{E} \times \mathcal{E} = \mathcal{E}^2$. Our approach to the Lattès maps on this surface is to use the result in proposition 6.1 and project further down onto $\mathbb{P}^2$. To that end we consider how $\mathbb{P}^2$ and $\mathbb{P}^1 \times \mathbb{P}^1$ can be related.

We do this as follows, take a smooth and irreducible projective conic such as $C : x^2 = y^2 + z^2$ in $\mathbb{P}^2$, to be consistent with the explicit map used in [Ued93] we pick this particular conic. Since this is a plane curve, we can apply the formula in 5 to find that it has genus 0. Moreover it has a rational point, namely $(1 : 0 : 1)$, thus by [Poo09] 34.13 we have that $C \cong \mathbb{P}^1$. If we pick a point in the plane that is not on C, then there exist precisely two distinct tangent lines to C intersecting at P. This can be seen as follows, take the family of lines through P, $\{L_t | t \in \mathbb{P}^1\}$ where t represents the slope of the line in a chosen affine patch. This family is in bijection with $\mathbb{P}^1$ by $L_t \mapsto t$. Note that in the projective plane over $\mathbb{C}$ every line through P intersects the conic twice (since it has degree 2) except finitely many. Thus the morphism $f : C \to \mathbb{P}^1$ given by $Q \mapsto t$ where t is the slope of the line through $Q \in C$ and P, is a 2-1 map. Thus we apply the Riemann-Hurwitz formula with $g(C) = g(\mathbb{P}^1) = 0$ and $\deg(f) = 2$ to find that

$$\sum_{Q \in C} (e_Q - 1) = 2.$$

and since this is a degree 2 map $e_Q \neq 3$. This implies that there are exactly two points Q and Q' such that $e_Q = e_{Q'} = 2$, i.e. precisely two distinct points such that the line through P and Q (Q' respectively) does not intersect C at any other point. It follows that these are the tangent lines $T_Q C$ and $T_{Q'} C$. Since lines in the plane intersect at precisely one point we have that $T_Q C \cap T_{Q'} C = \{P\}$.

On the other hand if the point P lies on C then there is exactly one such tangent line, the one through P itself. This follows by an analogous argument where we again take the family of lines through P and and construct the same map, this time of degree 1, and find that there are no ramification points.

Thus we can define a map $C \times C \to \mathbb{P}^2$ by taking (Q, Q') to the unique point in $T_Q C \cap T_{Q'} C$ if $Q \neq Q'$ and to Q if $Q = Q'$, see the figure below[14]. From this description it is clear that the map is symmetric and 2-1 except at the diagonal in $C \times C$. Since $C \cong \mathbb{P}^1$ this gives a map $\mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^2$ that it is a double cover of $\mathbb{P}^2$ except at the conic C.

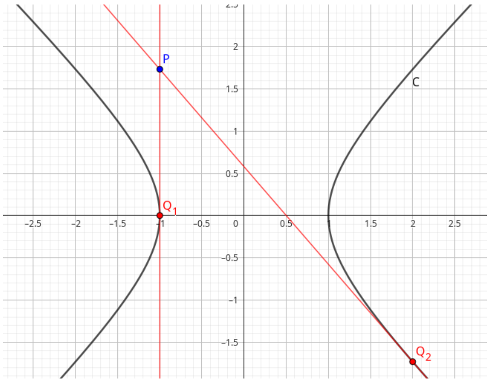

Figure 7: Two tangents to C intersecting at P.

The explicit equations of a map $\pi : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^2$ as above can be given by

$$((u : v), (w : r)) \longmapsto (uw + vr : uw - vr : ur + vw) \,. \tag{42}$$

([Ued93] sec. 4)

With this we can construct an appropriate map $\pi : \mathcal{E} \times \mathcal{E} \to \mathbb{P}^2$ that will have similar properties to the one dimensional Lattès map. We first construct it as a map commuting with a function on $\mathbb{P}^1 \times \mathbb{P}^1$. Let us denote the self-morphism acting on $\mathbb{P}^1 \times \mathbb{P}^1$ by $(P, Q) \mapsto (Q, P)$ as j to keep the notation of [Ued93].

Proposition 6.2. *Given that f is a self morphism of $\mathbb{P}^1 \times \mathbb{P}^1$ commuting with j defined above and that $\pi : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^2$ is as in 42, then there exists a unique map F making the diagram*

$$\begin{array}{ccc} \mathbb{P}^1 \times \mathbb{P}^1 & \xrightarrow{\ f\ } & \mathbb{P}^1 \times \mathbb{P}^1 \\ {\scriptstyle \pi}\downarrow & & \downarrow{\scriptstyle \pi} \\ \mathbb{P}^2 & \xrightarrow{\ F\ } & \mathbb{P}^2 \end{array} \tag{43}$$

commute.

Proof. The proof is very similar to that of proposition 6.1. By assumption the map π is surjective thus for all $\alpha \in \mathbb{P}^2$ we have a unique set $S_{(P,Q)} := \{(P, Q), (Q, P)\}$ such that $\pi(S_{(P,Q)}) = \{\pi(P, Q)\}$ and since f commutes with j we have that $f(S_{(P,Q)}) = S_{f(P,Q)}$ which uniquely defines an element in $\mathbb{P}^2$ since $\pi(S_{f(P,Q)})$ is a singleton set. Thus we can define F by mapping the pre-image of each point under π with $\pi \circ f$. □

Remark 6.1. By the explicit equations in 42 and properties of morphisms, if f is a rational map, then F must also be rational.

Combining this with the projection in 6.1 we have

[14] The image over $\mathbb{R}$ is meant as a reference. It does not fully convey the projective nature of the map nor the fact that we work over an algebraically closed field.

Corollary 6.3. *Given that $\mathcal{E}^2$ is a 2-copy of an elliptic curve over $\mathbb{C}$ and $\varphi : \mathcal{E}^2 \to \mathcal{E}^2$ a self-morphism then there exists a unique map F_φ such that the diagram*

$$\begin{array}{ccc} \mathcal{E}^2 & \xrightarrow{\varphi} & \mathcal{E}^2 \\ \pi \downarrow & & \downarrow \pi \\ \mathbb{P}^2 & \xrightarrow{F_\varphi} & \mathbb{P}^2 \end{array} \tag{44}$$

commutes.

Proof. Let $\mathcal{E}_1 = \mathcal{E}_2 =: \mathcal{E}$, then by proposition 6.1 there exists a unique f_φ making diagram 41 commute giving half a diagram. By proposition 6.2 there exists a unique F_φ making the diagram 43 commute with f_φ, this gives the second half of the diagram concluding the proof. □

Example 6.1. Consider the elliptic curve $\mathcal{E} : zy^2 = x^3 + xz^2$ as in example 4.4.2 with complex multiplication by $[i]$. As discussed there, this gives a rational map $f_i(u : v) = (-u : v)$. Then the endomorphism φ on $\mathcal{E} \times \mathcal{E}$ defined by $\varphi = ([i], [i])$ descends to the map $f_\varphi : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1 \times \mathbb{P}^1$ given by $((u : v), (w : r)) \mapsto ((-u : v), (-w : r))$, by proposition 6.1. This map further descends to a map $F_\varphi : \mathbb{P}^2 \to \mathbb{P}^2$ (by proposition 6.2) which is characterized by

$$\begin{aligned} F_\varphi(x : y : z) &= \pi \circ f_\varphi((u : v), (w : r)) \\ &= \pi((-u : v), (-w : r)) \\ &= (uw + vr : uw - vr : -ur - wv) \\ &= (x : y : -z) \end{aligned}$$

where $(x : y : z) = (uw + vr : uw - vr : ur + vw)$ and π is as in 42. Giving us the Lattès example $F_\varphi(x : y : z) = (x : y : -z)$ in $\mathbb{P}^2$.

Let us return to the projection of $\mathbb{P}^1 \times \mathbb{P}^1$ onto $\mathbb{P}^2$ and discuss the necessary condition that f commutes with j in proposition 6.2. Consider the action of j on the points of $\mathbb{P}^1 \times \mathbb{P}^1$, by $(P, Q) \mapsto (Q, P)$, and note that it is an involution. Thus the group of automorphisms generated by j, $\langle j \rangle$, has order 2. The natural projection $\pi : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1 \times \mathbb{P}^1 / \langle j \rangle$ is therefore a 2-to-1 map except at the fixed points of j, which are the points on the diagonal of $\mathbb{P}^1 \times \mathbb{P}^1$. This is analogous to the projection we discussed in section 4.1; we indeed find that $\mathbb{P}^1 \times \mathbb{P}^1 / \langle j \rangle \cong \mathbb{P}^2$ since taking the intersection point of two tangents is an isomorphism on the equivalence classes induced by j ([Ued93] sec. 4). This approach, however, allows us to backtrack and determine a subgroup $\mathcal{G} \leq \mathrm{Aut}(\mathcal{E}^2)$ such that $\mathcal{E}^2 / \mathcal{G} \cong \mathbb{P}^2$. Since the initial projection in proposition 6.1 is performed component-wise, the action of j on $\mathbb{P}^1 \times \mathbb{P}^1$ can be lifted to an action of $\hat{j} \in \mathrm{Aut}(\mathcal{E}^2)$ acting by $(P, Q) \mapsto (Q, P)$, where $Q, P \in \mathcal{E}$. Note that this is only well defined if $\mathcal{E}_1 = \mathcal{E}_2 = \mathcal{E}$ in proposition 6.1.

Proposition 6.4. *Given the surface $\mathcal{E}^2$, let $\sigma_1 = (\sigma, id)$, $\sigma_2 = (id, \sigma)$ and $\hat{j}$ be as above, then $\mathcal{G} := \left\langle \sigma_1, \sigma_2, \hat{j} \right\rangle \leq Aut(\mathcal{E}^2)$ is such that $\mathcal{E}^2 / \mathcal{G} \cong \mathbb{P}^2$.*

Proof. Note that $\left\langle \hat{j} \right\rangle$ is a normal subgroup of $\mathcal{G}$, thus the statement follows from the fact that $\mathcal{E}^2 / \langle \sigma_1, \sigma_2 \rangle \cong \mathbb{P}^1 \times \mathbb{P}^1$, and $\mathbb{P}^1 \times \mathbb{P}^1 / \langle j \rangle \cong \mathbb{P}^2$ and $j \circ \pi = \pi \circ \hat{j}$, where π is the projection onto $\mathbb{P}^1 \times \mathbb{P}^1$. □

6.2 Quotients by Different Groups

Similarly to the one dimensional case, there exist other subgroups of $\mathrm{Aut}(\mathcal{E} \times \mathcal{E})$ which yield a projection to $\mathbb{P}^2$. The first four of these are direct extensions of the one dimensional case and each one arises from the possible groups given in 5.1. The quotient corresponding to

$\langle\sigma\rangle$ is discussed above, as for the other groups $\mathcal{G}$ we can take the component wise projection $\pi : \mathcal{E} \times \mathcal{E} \longrightarrow \mathcal{E}/\mathcal{G} \times \mathcal{E}/\mathcal{G} \xrightarrow{\cong} \mathbb{P}^1 \times \mathbb{P}^1$. Here the projecting will have degree $(\#\mathcal{G})^2 =: n^2$. We projecting further $\mathbb{P}^1 \times \mathbb{P}^1$ to $\mathbb{P}^2$ by taking the quotient of the action of $\langle j\rangle$ giving us the desired diagram.

Lemma 6.5. *Let $\mathcal{G} \leq Aut(\mathcal{E})$, $h_{\mathcal{G}} := \{\mu = (\eta, \theta) \in Aut(\mathcal{E} \times \mathcal{E}) \mid \eta, \theta \in \mathcal{G}\}$ and take $\hat{j} \in Aut(\mathcal{E} \times \mathcal{E})$ to be the automorphism defined by $(P, Q) \mapsto (Q, P)$, then for all $\mu \in h_{\mathcal{G}}$ there exists an element $\tau \in h_{\mathcal{G}}$ such that $\hat{j} \circ \mu = \tau \circ \hat{j}$.*

Proof. Let $\mu = (\mu_1, \mu_2)$, by assumption $\mu_1, \mu_1 \in \mathcal{G}$. Then $\hat{j} \circ \mu(P, Q) = \hat{j}(\mu_1(P), \mu_2(Q)) = (\mu_2(Q), \mu_1(P))$. Since $\mu_1, \mu_2 \in \mathcal{G}$ we have that $\tau := (\mu_2, \mu_1) \in h_{\mathcal{G}}$, therefore $(\mu_2(Q), \mu_1(P)) = \tau(Q, P) = \tau \circ \hat{j}(P, Q)$. We conclude that $\hat{j} \circ \mu(P, Q) = \tau \circ \hat{j}(P, Q)$ for all $(P, Q) \in \mathcal{E} \times \mathcal{E}$ and since μ was arbitrary this concludes the proof. □

Lemma 6.6. *Let $\mathcal{G} \leq Aut(\mathcal{E})$, $h_{\mathcal{G}}$ and $\hat{j}$ be as above. Take $j : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1 \times \mathbb{P}^1$ by $(\bar{P}, \bar{Q}) \mapsto (\bar{Q}, \bar{P})$ and $\pi : \mathcal{E} \times \mathcal{E} \to \mathbb{P}^1 \times \mathbb{P}^1$ the component wise projection with respect to $\mathcal{G}$, then $\pi \circ \hat{j} = j \circ \pi$.*

Proof. This follows immediately by computation. Let $(P, Q) \in \mathcal{E} \times \mathcal{E}$ and $(\bar{P}, \bar{Q}) = \pi(P, Q) \in \mathbb{P}^1 \times \mathbb{P}^1$, then $\pi \circ \hat{j}(P, Q) = \pi(Q, P) = (\bar{Q}, \bar{P}) = j(\bar{P}, \bar{Q}) = j \circ \pi(P, Q)$. □

Given a fixed $\mathcal{G}$ as above, let $H_{\mathcal{G}} := \left\langle h_{\mathcal{G}} \cup \{\hat{j}\} \right\rangle$. It follows that $(\mathcal{E} \times \mathcal{E})/H_{\mathcal{G}} \cong (\mathbb{P}^1 \times \mathbb{P}^1)/\langle j\rangle \cong \mathbb{P}^2$. This gives rise to the following possible quotients

Proposition 6.7. *Let $\mathcal{E}$ be an elliptic curve over $\mathbb{C}$ and let $\mathcal{G} \leq Aut(\mathcal{E})$, then*

$$(\mathcal{E} \times \mathcal{E})/H_{\mathcal{G}} \cong \mathbb{P}^2. \tag{45}$$

Where

1. *$H_{\langle\sigma\rangle}$ is valid for all elliptic curves.*
2. *$H_{\langle[i]\rangle}$ is valid on curves with automorphism group $\langle[i]\rangle$ (j-invariant 1728).*
3. *$H_{\langle[\zeta_3]\rangle}$ is valid on curves with automorphism group $\langle\zeta_6\rangle$ (j-invariant 0).*
4. *$H_{\langle[\zeta_6]\rangle}$ is valid on curves with automorphism group $\langle\zeta_6\rangle$ (j-invariant 0).*

Proof. This follows directly from the discussion above. □

Note that the groups $H_{\mathcal{G}}$ have $2n^2$ many elements (where $n = \#\mathcal{G}$) and thus the projections onto $\mathbb{P}^2$ have degree $2n^2$. These are the first 4 surfaces listed in [Dup01] sec. 5.1.

Example 6.1 gives a map arising out of the quotient of $\mathcal{E} \times \mathcal{E}$, where $\mathcal{E} : y^2z = x^3 + z^3$, with $H_{\langle\sigma\rangle}$. The explicit computations for more complicated maps quickly become convoluted as their degree increases. The doubling map itself is already challenging to write down.

7 Concluding Remarks

Above we have the first four examples listed in [Dup01], the remaining two require more results that could not be introduced here. Let us describe one of these without giving any proofs. Recall that $\mathcal{E}$ has an End($\mathcal{E}$)-module structure, thus $\mathcal{E}^2$ can also be seen as an End($\mathcal{E}$)-module. With this, the endomorphisms on $\mathcal{E}^2$ can be represented as matrices with entries in End($\mathcal{E}$). Note that the above groups act only by multiplication on each component and permuting the components, thus their representations are diagonal and anti-diagonal matrices. Allowing the components to also act on one another we find that for all surfaces $\mathcal{E}^2$, there exists the additional group of automorphisms given by

$$H = \left\langle \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle$$

such that $\mathcal{E}^2/H \cong \mathbb{P}^2$. For the proof of this we refer the reader to [KTY82] section 4. For the final example in the table given in section 5 of [Dup01], we refer the reader to [KTY82] section 2.

The specific maps arising out of commutativity with $[d] \in \mathrm{End}(\mathcal{E}^2)$ have the same dynamical property as the Lattès maps in section 5, namely their Julia set is the entire projective plane $\mathbb{P}^2$ ([Ued93] prop. 4.1). This is a direct extension of the Lattès example and since the projection (with $\langle \sigma_1, \sigma_2 \rangle$) is a cover of $\mathbb{P}^2$, the denseness argument still holds as in 5 and the Julia set is indeed $\mathbb{P}^2$. Moreover we should note that that the map $[d] : A \to A$ (for $d \in \mathbb{Z}_{\geq 1}$) defined by d-fold addition of a point on an abelian variety A, has as its preperiodic points the torsion points. This suggests that if it is possible that $A/G \cong \mathbb{P}^n$, then the map commuting with $[d]$ may give insight into the torsion points. We saw that this is the case for $A = \mathcal{E}$.

We have considered the Lattès construction mainly over $\mathbb{C}$ in the two dimensional case, although its generalization to $\bar{\mathbb{Q}}$ is straightforward, it is not immediately clear what to do over $\bar{\mathbb{F}}_p$. In particular the automorphism groups of an elliptic curve over a finite field of characteristic 2 and 3 can have more elements then those we've discussed for $\mathbb{C}$ and it is unknown to myself if proposition 5.3 holds for fields of characteristic 2 and 3.

Recall that in example 4.3 we found an upper bound for the odd torsion of a point on that specific curve through reduction. It may be interesting to consider the explicit Lattès maps commuting with $[p]$, where p is prime, and investigate the bounds on the exact period of their periodic points through good reduction (by 3.4). Recall that the periodic points of $[p]$ are are precisely the torsion points of order coprime to p (remark 4.2) thus it suffices to consider primes and if a general statement is possible for all primes, it would give a bound on the maximal torsion. Furthermore the periodic points of $[p]$ coincide with the periodic points of $f_{[p]}$ although their exact period can differ by a factor of two (for the projection with $\mathcal{G} = \langle \sigma \rangle$).

Lattès maps on abelian varieties of dimension 2 other then $\mathcal{E} \times \mathcal{E}$ and dimension larger than 2 are largely undiscussed although Dupont remarks that examples exist in any dimension ([Dup01] rmk. 5.1). The field of arithmetic dynamics is, as mentioned in the introduction, a relatively new field and there is much which could not be said in the present text, we refer the interested reader to [Sil07].

References

[DeM23] Laura DeMarco. *Aithmetic Dynamics and Intersection Problems AWS 2023*. 2023.

[Dup01] Christophe Dupont. "Exemples de Lattes et domaines faiblement spheriques de $\mathbb{C}^n$". In: *manuscripta mathematica* 111 (Nov. 2001). DOI: 10.1007/s00229-003-0378-0.

[Ful08] William Fulton. "Algebraic curves". In: *An Introduction to Algebraic Geom* 54 (2008).

[Gat21] Andreas Gathmann. *Algebraic Geometry*. Vol. class notes 21/22. RPTU Kaiserslautern, 2021.

[Gat23] Andreas Gathmann. *Plane Algebraic Curves*. Vol. class notes. RPTU Kaiserslautern, 2023.

[Har77] Robin Hartshorne. *Algebraic Geometry*. Vol. Graduate Texts in Mathematics 52. Springer, 1977.

[KTY82] Jyoichi Kaneko, Syoshi Tokunaga, and Masaaki Yoshida. "Complex crystallographic groups II". In: *Journal of The Mathematical Society of Japan* 34 (1982), pp. 581–593. URL: https://api.semanticscholar.org/CorpusID:123420467.

[Mil04] John W Milnor. "On Lattès Maps". In: *arXiv preprint math/0402147* (2004).

[Mil08] James S. Milne. *Abelian Varieties (v2.00)*. Available at www.jmilne.org/math/. 2008.

[Poo09] Bjorn Poonen. *Introduction to Arithmetic Geometry*. notes from 18.782. 2009.

[Sch04] Alexander B Schwartz. "Elliptic Curves, Group Schemes, and Mazur's Theorem". PhD thesis. Harvard University, 2004.

[Sil07] Joseph H Silverman. *The arithmetic of dynamical systems*. Vol. 241. Springer Science & Business Media, 2007.

[Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*. Vol. 106. Springer, 2009.

[Sil10] Joseph H Silverman. "Lecture Notes on Arithmetic Dynamics Arizona Winter School March 13–17, 2010". In: (2010).

[Sil22] Joseph H Silverman. "Survey lecture on arithmetic dynamics". In: *Proc. Int. Cong. Math.* Vol. 3. 2022, pp. 1682–1710.

[Sil91] Joseph H Silverman. "Rational points on K3 surfaces: a new canonical height". In: *Inventiones mathematicae* 105.1 (1991), pp. 347–373.

[ST92] Joseph H Silverman and John Torrence Tate. *Rational points on elliptic curves*. Vol. 9. Springer, 1992.

[Ued93] Tetsuo Ueda. "Complex dynamical systems on projective spaces". In: *Chaotic Dynamical Systems - Proceedings Of The Rims Conference*. 1993, pp. 120–138.