An analog of the Lindemann-Weierstrass Theorem for the Weierstrass $\wp$-function

Martin Rivard-Cooke

Thesis submitted to the Faculty of Graduate and Postdoctoral Studies
in partial fulfillment of the requirements for the degree of Master of Science in
Mathematics [1]

Department of Mathematics and Statistics
Faculty of Science
University of Ottawa

© Martin Rivard-Cooke, Ottawa, Canada, 2014

[1] The M.Sc. program is a joint program with Carleton University, administered by the Ottawa-Carleton Institute of Mathematics and Statistics

Abstract

This thesis aims to prove the following statement, where the Weierstrass $\wp$-function has algebraic invariants and complex multiplication by $\mathbb{Q}(\alpha)$:

> "If $\beta_1, \ldots, \beta_n$ are algebraic numbers which are linearly independent over $\mathbb{Q}(\alpha)$, then $\wp(\beta_1), \ldots, \wp(\beta_n)$ are algebraically independent over $\mathbb{Q}$."

This was proven by Philippon in 1983, and the proof in this thesis follows his ideas. The difference lies in the strength of the tools used, allowing certain arguments to be simplified.

This thesis shows that the above result is equivalent to imposing the restriction

$$(\beta_1, \ldots, \beta_n) = (1, \beta, \ldots, \beta^{n-1}),$$

where $n = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)]$. The core of the proof consists of developing height estimates, constructing representations for morphisms between products of elliptic curves, and finding height and degree estimates on large families of polynomials which are small at a point in

$$\mathbb{Q}(\alpha, \beta, g_2, g_3)(\wp(1), \wp'(1), \ldots, \wp(\beta^{n-1}), \wp'(\beta^{n-1})).$$

An application of Philippon's zero estimate (1986) and his criterion of algebraic independence (1984) is then used to obtain the main result.

Contents

Introduction

The existence of transcendental numbers was first established by Liouville in 1844. He proved the existence of a non-empty class of numbers called *Liouville numbers*, which are, vaguely, real numbers that satisfy a certain strong rational approximation inequality that no algebraic number can satisfy. He also gave an explicit example in 1851, the so-called *Liouville constant*, namely

$$\sum_{n=1}^{\infty} 10^{-n!} = 0.1100010000000\ldots$$

However, Liouville's constant was constructed for the sake of proving the existence of transcendental numbers, and does not answer whether or not numbers which arise in more "natural" contexts can be transcendental. It was in 1873 that Charles Hermite answered this question affirmatively, proving that Euler's number, e, is transcendental. This naturally spurred greater interest in the theory of transcendental numbers, further promoted by Cantor's proof in 1874 that the set of transcendental numbers is in fact larger than the set of algebraic numbers. The methods in the proof by Hermite provided much of the basis with which several classes of numbers have historically been shown to be transcendental. Indeed, Hermite's methods formed the basis of the proof, given by Lindemann in 1882, that e^{β} is a transcendental number for each non-zero algebraic number β, which in particular implies the transcendence of π. In 1885, Weierstrass generalized this result by proving the Lindemann-Weierstrass Theorem, which states that if $\beta_1, \ldots, \beta_n$ are algebraic numbers which are linearly independent over $\mathbb{Q}$, then $e^{\beta_1}, \ldots, e^{\beta_n}$ are algebraically independent over $\mathbb{Q}$. Several more proofs of this theorem have appeared over the course of nearly a century, but they all relied on reducing the problem of algebraic independence to one of linear independence. It was not until a paper by Chudnovsky published in 1980 [13] that algebraic independence methods had managed to yield a partial result. The significance of this is that it allowed Chudnovsky in the same year to adapt his methods to prove an analogous result for Weierstrass $\wp$-functions which have complex multiplication and which are defined over the algebraic numbers, with the caveat that only six algebraic numbers could be considered. Nevertheless, it was his methods that ultimately led Philippon and Wüstholz to prove the complete result independently of each other in 1983. The result can be stated as follows, where the Weierstrass $\wp$-function is assumed to have algebraic invariants and complex multiplication by $\mathbb{Q}(\alpha)$:

> "If $\beta_1, \ldots, \beta_n$ are algebraic numbers which are linearly independent over $\mathbb{Q}(\alpha)$, then $\wp(\beta_1), \ldots, \wp(\beta_n)$ are algebraically independent over $\mathbb{Q}$."

The main goal of this thesis is to demonstrate this result, based on Philippon's methods. The main difference lies in the strength of the tools used, allowing several arguments to be simplified.

The first chapter consists of a brief exposition on Algebraic Geometry, establishing the notion of an elliptic curve, and stating a few results on morphisms between projective algebraic varieties. The second chapter establishes the notion of an elliptic function, and defines the related Weierstrass functions. The section on the Weierstrass $\wp$-function is of particular importance, as it presents many results which will be key in proving the main result. The rest of the thesis consists of proving the main result. The first step in doing so is to show that the statement of the main result is equivalent to a simpler one, stated as follows, where the Weierstrass $\wp$-function is assumed to have algebraic invariants and complex multiplication by $\mathbb{Q}(\alpha)$:

> "Let β be an algebraic integer, and let $d = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)]$. Then the numbers $\wp(1), \wp(\beta), \ldots, \wp(\beta^{d-1})$ are algebraically independent over $\mathbb{Q}$."

The proof of this statement relies heavily on the construction of an auxiliary function for each sufficiently large $L \in \mathbb{N}^+$. To make this more precise, let E be the elliptic curve induced by $\wp$, and let $\Phi : \mathbb{C} \to \mathbb{C}^3$ be a holomorphic representation of the exponential map on E, i.e. $\exp_E(z) = [\Phi(z)]$. Further, let $\rho : \mathbb{C}^q \to \mathbb{C}^{qd}$ be defined as $\rho(\mathbf{t}) = (\mathbf{t}, \mathbf{t}\beta, \ldots, \mathbf{t}\beta^{d-1})$, and let $\Psi : \mathbb{C}^{qd} \to (\mathbb{C}^3)^{qd}$ be defined as $\Psi(\mathbf{z}) = (\Phi(z_1), \ldots, \Phi(z_{qd}))$. The auxiliary function is then of the form

$$F(\mathbf{t}) = P(1, \mathbf{t}, \Psi \circ \rho(\mathbf{t})) \quad (\forall \mathbf{t} \in \mathbb{C}^q),$$

where $P \in \mathbb{Z}[\mathbf{Z}, \mathbf{X}_1, \ldots, \mathbf{X}_{qd}]$, with $\mathbf{X}_i = (X_{i,0}, X_{i,1}, X_{i,2}) \in \mathbb{C}^3$ for $1 \leqslant i \leqslant qd$, and with $\mathbf{Z} = (Z_0, \ldots, Z_q) \in \mathbb{C}^{q+1}$. The polynomial P satisfies

$$\deg_{\mathbf{Z}} P = L \quad \text{and} \quad \deg_{\mathbf{X}_i} = \lfloor (\log L)^{\epsilon} \rfloor + 1 \quad (1 \leqslant i \leqslant qd),$$

and is of height bounded by L, whereas F satisfies

$$\max_{|\sigma| \leqslant L} \max_{|\mathbf{t}| \leqslant \log L} |F^{(\sigma)}(\mathbf{t})| \leqslant \exp(-L(\log L)^{1+\epsilon/2})$$

where $\varepsilon > 0$ can be chosen arbitrarily small. This auxiliary function differs only slightly from the one constructed by Philippon in [8], in that Ψ is embedded in a large product of low-dimensional projective spaces, instead of a single high-dimensional projective space. Its construction also differs, in that it follows rather straightforwardly from a result of Waldschmidt in [7], combined with Cauchy's inequality in several variables. The usefulness of the auxiliary function lies in providing a link between the algebraic arguments and the analytic arguments inherent in attempting to prove the main result.

The proof will also require certain morphisms to be represented by families of polynomials whose degrees and heights are bounded, and so some useful results on heights of polynomials are demonstrated. In order to find these representations, a complete system of bidegree $(2, 2)$ for the group law on elliptic curves with complex multiplication is given, whose proof is attributed to [6], and the multiplication-by-2 map is shown to be represented by a single triple of polynomials. These representations allow several families of polynomials to be constructed, each such family representing one of several morphisms between products of elliptic curves with complex multiplication.

In order to adequately describe the ideas underlying how the auxiliary function and representations of morphisms are used in this thesis, the following notation is established. Let Λ denote the lattice associated to $\wp$, and define for each $j \in \{1, \ldots, d\}$,

$$u_j = \begin{cases} (1, \wp(\beta^{j-1}), \wp'(\beta^{j-1})) & \text{if } \beta^{j-1} \notin \Lambda; \\ (0, 0, 1) & \text{if } \beta^{j-1} \in \Lambda, \end{cases}$$

let $\mathbf{u} = (u_1, \ldots, u_d)$, and let $K = \mathbb{Q}(g_2, g_3, \alpha, \beta)$, where g_2, g_3 are the invariants of $\wp$. Though the details surrounding the use of the auxiliary function and the constructed representations of morphisms are technical, let it suffice to begin with the following.

For each sufficiently large $L \in \mathbb{N}^+$, the partial derivatives of F are shown to be small at points $\gamma = (\gamma_1, \ldots, \gamma_q)$, with $\gamma_i \in \mathbb{Z}[\alpha, \beta]$. These are normalized to yield elements of $K[\mathbf{u}]$ which have absolute values that are small. These elements are then shown to be the image at $\mathbf{u}$ of polynomials whose heights and degrees are bounded.

Denote by $\mathcal{F}_L$ the family consisting of the aforementioned polynomials. The completion of the proof is then reliant on an application of Philippon's zero estimate (1986) followed by an application of Philippon's criterion of algebraic independence (1984). The zero estimate shows that $\mathcal{F}_L$ has no common zeros in $E^d \subset (\mathbb{P}^2(\mathbb{C}))^d$. Adding to $\mathcal{F}_L$ the d polynomials which define E^d, a new family is constructed, denoted $\tilde{\mathcal{F}}_L$, which has no common zeros in $(\mathbb{P}^2(\mathbb{C}))^d$. The criterion of algebraic independence then uses the fact that $\tilde{\mathcal{F}}_L$ has no common zeros in $(\mathbb{P}^2(\mathbb{C}))^d$, as well as the estimates on the heights and degrees of the polynomials in $\tilde{\mathcal{F}}_L$ and the bound on the values they take at the point $\mathbf{u}$, to deduce that $K(u_1, \ldots, u_d)$ has transcendence degree d. Since the invariants are algebraic, the relation $\wp'^2 = 4\wp^3 - g_2\wp - g_3$ allows the deduction of the main result.

Chapter 1

Algebraic Geometry

This chapter provides the details concerning algebraic geometry which are relevant to this thesis. Its content is attributed to [1] and [2]. Throughout this chapter, fix a field k_0 of characteristic zero, and let $k \supseteq k_0$ be an algebraically closed field extension.

1.1 Algebraic Varieties

In what follows, notions related to both affine algebraic varieties and projective algebraic varieties will be treated simultaneously, due to similarities in their exposition.

Let $\mathbb{A}^n \coloneqq k^n$ denote the affine n-space over k, and let $\mathbb{P}^n \coloneqq \mathbb{P}^n(k)$ denote the projective n-space over k. Further, denote the equivalence classes of points in $\mathbb{P}^n$ by

$$[x_0, \ldots, x_n] = (x_0 : \cdots : x_n) = \{(\lambda x_0, \ldots, \lambda x_n) \mid \lambda \in k^\times\}.$$

Let $A = k[x_1, \ldots, x_n]$ be a polynomial ring in n variables. Given a subset $T \subseteq A$, denote by $Z(T)$ the set of common zeros of all polynomials in T, i.e.

$$Z(T) = \{\mathbf{a} \in \mathbb{A}^n \mid f(\mathbf{a}) = 0 \text{ for all } f \in T\}.$$

Let $S = k[x_0, \ldots, x_n]$ be a polynomial ring in $n + 1$ variables.

Definition. A polynomial $f \in S$ is *homogeneous of degree* d if

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n) \quad (\forall \lambda \in k).$$

Let S_d be the set of polynomials in S which are homogeneous of degree d, and denote the set of homogeneous polynomials by $S_H = \bigcup_{d=0}^{\infty} S_d$. Notice that while a homogeneous polynomials $f \in S_d$ is not a function of $\mathbb{P}^n$, it does make sense to ask whether or not f is zero at a point in $\mathbb{P}^n$. Indeed, if f is zero for some representative $(x_0, \ldots, x_n)$ of a point $\mathbf{p} \in \mathbb{P}^n$, then

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n) = 0 \quad (\forall \lambda \in k),$$

and so f is zero for every representative of $\mathbf{p}$. Thus, given a subset $T \subseteq S_H$, denote by $Z(T)$ the set of common zeros of all polynomials in T, i.e.

$$Z(T) = \{\mathbf{p} \in \mathbb{P}^n \mid f(\mathbf{p}) = 0 \text{ for all } f \in T\}.$$

Definition. A subset X of $\mathbb{A}^n$ (resp. $\mathbb{P}^n$) is said to be an *algebraic set* if there exists a subset T of A (resp. S_H) such that $X = Z(T)$. If T can be chosen such that the coefficients of the polynomials in T lie in k_0, then X is said to be *defined over* k_0.

Proposition 1.1.1. *Consider the following sets to be contained in* $\mathbb{A}^n$ *(resp.* $\mathbb{P}^n$*). Then,*

a) the union of two algebraic sets is an algebraic set;

b) the intersection of a family of algebraic sets is an algebraic set;

c) $\varnothing$ *and* $\mathbb{A}^n$ *(resp.* $\mathbb{P}^n$*) are algebraic sets.*

Definition. The *Zariski topology* on $\mathbb{A}^n$ (resp. $\mathbb{P}^n$) is defined by taking the open sets to be the complements of the algebraic sets in $\mathbb{A}^n$ (resp. $\mathbb{P}^n$).

Remark that, by the proposition above, this is indeed a topology.

Definition. A non-empty subset Y of a topological space X is said to be *irreducible* if it can not be written as the union of two proper subsets, Y_1 and Y_2, both of which are closed in Y.

Definition. An *affine* (resp. *projective*) *algebraic variety* is an algebraic set which is irreducible in the Zariski topology on $\mathbb{A}^n$ (resp. $\mathbb{P}^n$).

Proposition 1.1.2. *Each algebraic set can be uniquely written as a finite union of algebraic varieties, none containing another.*

Definition. Let X be a topological space. The *dimension* of X, denoted $\dim X$, is defined to be the supremum of all integers n such that there exists a chain $Z_0 \subset Z_1 \subset \cdots \subset Z_n$ of irreducible closed subsets of X. The *dimension* of an algebraic variety is its dimension as a topological space.

Definition. Let $X = Z(f_1, \ldots, f_s)$ be an algebraic variety in $\mathbb{A}^n$ (resp. $\mathbb{P}^n$); let $p \in X$. Then, X is *smooth* at p if the rank of the Jacobian is maximal, i.e.

$$\operatorname{rank}\left(\frac{\partial f_i}{\partial x_j}(p)\right) = n - \dim(X).$$

An algebraic variety is said to be *smooth* if it is smooth at every point.

1.2 Morphisms

Note that understanding morphisms between projective algebraic varieties will suffice for the scope of this thesis. As such, the following exposition will be simplified accordingly. For more details on morphisms, see [1].

Definition. Let $V \subseteq \mathbb{P}^n(\mathbb{C})$ and $W \subseteq \mathbb{P}^m(\mathbb{C})$ be algebraic varieties. Let $\Psi : V \to W$ be a map. If there exists a Zariski open cover $(U_i)_{i \in I}$ of V, such that

$$(\Psi_0^{(i)}(x), \ldots, \Psi_m^{(i)}(x)) \neq \mathbf{0} \quad (\forall i \in I; \forall x \in U_i);$$

$$\Psi(x) = [\Psi_0^{(i)}(x), \ldots, \Psi_m^{(i)}(x)]$$

for some family $(\Psi^{(i)})_{i \in I}$, where each $\Psi^{(i)} = (\Psi_0^{(i)}, \ldots, \Psi_m^{(i)})$, and where each $\Psi_j^{(i)}$ is a polynomial which is homogeneous of degree d_i, independent of j. Then, Ψ is said to be a *morphism*, and it is said to be *represented by* the family $(\Psi^{(i)})_{i \in I}$.

Note that the choice of a family which represents a morphism is not unique. Also, given morphisms $\phi : U \to V$, $\psi : V \to W$, the composition $\psi \circ \phi : U \to W$ is a morphism.

Proposition 1.2.1. *Let $\Psi : V \to W$ be a morphism. Then, the family $(\Psi^{(i)})_{i \in I}$ which represents Ψ can be chosen with a finite indexing set I. Furthermore, if $x \in V$ and $i \in I$ are such that*

$$(\Psi_0^{(i)}(x), \ldots, \Psi_m^{(i)}(x)) \neq \mathbf{0},$$

then

$$\Psi(x) = [\Psi_0^{(i)}(x), \ldots, \Psi_m^{(i)}(x)].$$

Definition. Let $\Psi : V \to W$ be a morphism which is represented by a finite family $(\Psi^{(i)})_{i \in I}$. Then, the family $(\Psi^{(i)})_{i \in I}$ is said to form a *complete system* for Ψ.

Reciprocally, if a finite family $(\Psi^{(i)})_{i \in I}$ is such that, for each $i, j \in I$,

$$(\Psi_0^{(i)}(x), \ldots, \Psi_m^{(i)}(x)) \neq \mathbf{0} \neq (\Psi_0^{(j)}(x), \ldots, \Psi_m^{(j)}(x))$$

implies that

$$[\Psi_0^{(i)}(x), \ldots, \Psi_m^{(i)}(x)] = [\Psi_0^{(j)}(x), \ldots, \Psi_m^{(j)}(x)],$$

then $(\Psi^{(i)})_{i \in I}$ forms a complete system for a unique morphism $\Psi : V \to W$.

1.3 Elliptic Curves

This section introduces the notion of algebraic groups, as well as that of elliptic curves defined over fields of characteristic zero. A few key results are also stated.

Definition. Let X be an algebraic set defined over k_0. Suppose that X possesses a group structure whose group operations can be given locally by polynomials whose coefficients lie in k_0. Then, X is said to be an *algebraic group*, and it is said to be *defined over* k_0.

For instance, the algebraic set $\mathbb{C}^n$ is an algebraic group defined over $\mathbb{Q}$ for each $n \in \mathbb{N}^+$, taking '+' as the group law.

Definition. An *elliptic curve* is a smooth projective algebraic variety of genus 1 [2], with a specified basepoint O. It is said to be *defined over* k_0 if the polynomials defining it can be chosen to have coefficients in k_0, and if there exists a representative of O whose coordinates are in k_0.

Proposition 1.3.1. *Let E be an elliptic curve defined over k_0. Then, it is isomorphic as an algebraic variety to an elliptic curve which is in* Weierstrass normal form*, i.e.*

$$E = Z(x_0x_2^2 - 4x_1^3 + g_2x_0^2x_1 + g_3x_0^3).$$

The quantities g_2 and g_3 are called the *invariants* of E, and are such that if E is defined over k_0, then $g_2, g_3 \in k_0$. Further, the smoothness condition on E requires that $g_2^3 - 27g_3^2 \neq 0$.

In order to show the following proposition, consider the following. Let E be an elliptic curve which is in Weierstrass normal form. One can consider the points of E which are *at infinity*, i.e. the points $[0, x_1, x_2] \in E$. Since E is in Weierstrass normal form, it follows that $[0, 0, 1]$ is the only point at infinity. Let $O = [0, 0, 1]$ be the specified basepoint of E. If L is a line in $\mathbb{P}^2$, then Bézout's theorem [2] yields that $L \cap E$ has exactly three points, counting multiplicities. It thus makes sense to define the composition law in the upcoming proposition.

Proposition 1.3.2 (Group Law)**.** *Let $P, Q \in E$. Let L be the line connecting P and Q (if $P = Q$, then L is the line tangent to E at P), and let R be the unique third* *point of intersection of L with E. Let L' be the line connecting R and O, and define $P \oplus Q$ to be the unique third point of intersection of L' with E. Then, the composition law given by $\oplus$ turns E into an abelian group with identity element O.*

Definition. Let X be an algebraic group which is also a projective algebraic variety. Then, X is said to be an *abelian variety.*

For example, an elliptic curve is an abelian variety of dimension 1, as the group law on E given above can be expressed locally by polynomials, as seen in [2]. However, all that will be needed throughout this thesis is its reformulation (Theorem 2.2.9) in terms of the Weierstrass $\wp$-function which is defined in the next chapter.

Definition. An *isogeny* is a basepoint preserving morphism between abelian varieties.

Proposition 1.3.3. *Aside from the zero isogeny, an isogeny is finite-to-one and onto.*

Definition. The *endomorphism ring of E*, denoted $\mathrm{End}(E)$ is defined by

$$\mathrm{End}(E) = \{\text{isogenies } \phi : E \to E\}.$$

Proposition 1.3.4. *Let E be an elliptic curve. Then,* $\mathrm{End}(E)$ *is either isomorphic to $\mathbb{Z}$ or to a quadratic imaginary extension of $\mathbb{Z}$.*

If the endomorphism ring of an elliptic curve E is not isomorphic to $\mathbb{Z}$, i.e. if $\mathrm{End}(E) \cong \mathbb{Z}[\alpha]$ for some quadratic imaginary integer α, then E is said to have *complex multiplication.*

Chapter 2

Weierstrass Functions

The aim of this chapter is to provide the reader with a foundation of the theory surrounding the Weierstrass $\wp$-function. Its content is standard, and some of it is presented for the sake of completion. Of particular noteworthiness are Theorem 2.1.1, Propositions 2.3.1 and 2.4.1, and the entire section devoted to the Weierstrass $\wp$-function. Further, it should be noted throughout this chapter that when a statement is lacking a proof or reference, it can be found in Chapter 6 from [2].

The following terminology will be useful. A *lattice* is defined to be a discrete subgroup of $\mathbb{C}$ which contains an $\mathbb{R}$-basis for $\mathbb{C}$. Throughout this chapter, fix a lattice $\Lambda \subset \mathbb{C}$. It should be noted that many of the definitions in this chapter depend on the choice of Λ.

2.1 Elliptic Functions

Definition. An *elliptic function* (*relative to* Λ) is a meromorphic function $f(z)$ on $\mathbb{C}$ satisfying

$$f(z+\omega) = f(z) \quad \text{for all } \omega \in \Lambda, z \in \mathbb{C}.$$

The set of all elliptic functions, relative to Λ, is denoted by $\mathbb{C}(\Lambda)$. The set $\mathbb{C}(\Lambda)$

is a field.

Definition. A *fundamental parallelogram* for Λ is a set of the form

$$\{a + t_1\omega_1 + t_2\omega_2 \,|\, 0 \leqslant t_1, t_2 < 1\},$$

where $a \in \mathbb{C}$ and where $\omega_1, \omega_2 \in \mathbb{C}$ are such that $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.

Definition. The *order* of an elliptic function is defined to be its number of poles, counting multiplicities, in any fundamental parallelogram.

The following notation will be used frequently. Let $g : \mathbb{C} \to \mathbb{C}$ be such that for each fundamental parallelogram D, $g|_D$ has finite support. If the value of $\sum_{w\in D} g(w)$ is independent of the choice of a fundamental parallelogram D, then define

$$\sum_{w\in\mathbb{C}/\Lambda} g(w) := \sum_{w\in D} g(w).$$

Theorem 2.1.1. *Let $f \in \mathbb{C}(\Lambda)$. Then,*

a) $\displaystyle\sum_{w\in\mathbb{C}/\Lambda} \operatorname{res}_w f = 0$

b) $\displaystyle\sum_{w\in\mathbb{C}/\Lambda} \operatorname{ord}_w f = 0$

c) $\displaystyle\sum_{w\in\mathbb{C}/\Lambda} w \cdot \operatorname{ord}_w f \in \Lambda$

Corollary 2.1.2. *A non-constant elliptic function has order at least two.*

Definition. The *divisor group* of $\mathbb{C}/\Lambda$, denoted by $\operatorname{Div}(\mathbb{C}/\Lambda)$, is the group of formal linear combinations

$$\sum_{w\in\mathbb{C}/\Lambda} n_w(w),$$

where $n_w \in \mathbb{Z}$, with $n_w \neq 0$ for only finitely many w. The *degree* of $D \in \operatorname{Div}(\mathbb{C}/\Lambda)$, with $D = \sum n_w(w)$, is defined by

$$\deg D = \sum n_w.$$

Further, define

$$\mathrm{Div}^0(\mathbb{C}/\Lambda) = \{D \in \mathrm{Div}(\mathbb{C}/\Lambda) \mid \deg D = 0\},$$

and define a group homomorphism $\mathrm{div} : \mathbb{C}(\Lambda)^\times \to \mathrm{Div}^0(\mathbb{C}/\Lambda)$ by

$$\mathrm{div}(f) = \sum_{w \in \mathbb{C}/\Lambda} (\mathrm{ord}_w f)(w).$$

Proposition 2.1.3. *If $f, g \in \mathbb{C}(\Lambda)^\times$ are such that $\mathrm{div}(f) = \mathrm{div}(g)$, then $f = cg$ for some $c \in \mathbb{C}^\times$, i.e.*

$$\ker(\mathrm{div}) \cong \mathbb{C}^\times.$$

2.2 The Weierstrass $\wp$-function

Definition. The *Weierstrass $\wp$-function* (*for* Λ) is defined by the series

$$\wp(z) := \wp(z; \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \backslash \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Theorem 2.2.1. *The series defining the Weierstrass $\wp$-function defines a meromorphic function on $\mathbb{C}$. It is an even function, and its poles are situated at each $z \in \Lambda$ and are all of order 2. Further, $\wp$ and $\wp'$ are elliptic functions, and the roots of $\wp'$ are precisely the elements of $\frac{1}{2}\Lambda\backslash\Lambda$, i.e.*

$$\wp'(z) = 0 \Leftrightarrow z \in \tfrac{1}{2}\Lambda\backslash\Lambda.$$

The following theorem provides insight into the significance of the Weierstrass $\wp$-function.

Theorem 2.2.2. *The elements of $\mathbb{C}(\Lambda)$ are precisely the rational functions of $\wp$ and $\wp'$, i.e.*

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp').$$

Proposition 2.2.3. *Let D_0 be a fundamental domain for $(\mathbb{C}/\Lambda)/\{\pm 1\}$. If $f \in \mathbb{C}(\Lambda)$ is even, then*

$$\operatorname{div}(f) = \sum_{n_w \in D_0} n_w[(w) + (-w)] \quad (\textit{for some } n_w \in \mathbb{Z});$$

$$f(z) = c \prod_{w \in D_0 \backslash \{0\}} [\wp(z) - \wp(w)]^{n_w} \quad (\textit{for some } c \in \mathbb{C}).$$

Definition. The *Eisenstein series of weight* $2k$ (*for* Λ) is the series

$$G_{2k} \coloneqq G_{2k}(\Lambda) = \sum_{\omega \in \Lambda \backslash \{0\}} \omega^{-2k}.$$

The series G_{2k} is absolutely convergent for each integer $k > 1$.

Theorem 2.2.4. *The Laurent series for $\wp(z)$ about $z = 0$ is given by*

$$\wp(z) = z^{-2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2} z^{2k}.$$

Definition. The *invariants* of Λ, denoted g_2, g_3, are defined as

$$g_2 \coloneqq g_2(\Lambda) = 60 G_4 \quad \text{and} \quad g_3 \coloneqq g_3(\Lambda) = 140 G_6.$$

According to [3], the Laurent series for $\wp(z)$ has coefficients in $\mathbb{Q}(g_2, g_3)$.

Theorem 2.2.5. *There is an algebraic relation between the meromorphic functions $\wp$ and $\wp'$, namely*

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3.$$

In particular, we also have that $\wp'' = 6\wp^2 - g_2/2$.

Proposition 2.2.6. *The polynomial $f(x) = 4x^3 - g_2 x - g_3$ has non-zero discriminant, denoted*

$$\Delta \coloneqq \Delta(\Lambda) = g_2^3 - 27 g_3^2.$$

In particular, $E = Z(x_0 x_2^2 - 4x_1^3 + g_2 x_0^2 x_1 + g_3 x_0^3)$ is an elliptic curve, and

$$[1, \wp(z), \wp'(z)] \in E,$$

for each $z \in \mathbb{C} \backslash \Lambda$.

The lattice Λ is said to *induce* the elliptic curve E. The following notion is linked to the endomorphism ring of an elliptic curve E.

Definition. The *order* of Λ is defined as

$$\mathcal{O} \coloneqq \mathcal{O}(\Lambda) = \{\tau \in \mathbb{C} \mid \tau\Lambda \subseteq \Lambda\}.$$

Proposition 2.2.7. *Let E be the elliptic curve induced by Λ. Then,*

$$\mathcal{O} \cong \mathrm{End}(E).$$

In particular, if E does not have complex multiplication, then $\mathcal{O} = \mathbb{Z}$, and if E has complex multiplication, then $\mathcal{O} = \mathbb{Z}[\alpha]$ for some quadratic imaginary integer α. In order to provide insight into the isomorphism involved, some terminology is introduced. Given a Lie group G with tangent space $T_G(\mathbb{C})$, the *exponential map of* G is the unique map $\exp_G : T_G(\mathbb{C}) \to G$ satisfying

- $\exp(0) = 1_G$;
- $\frac{d}{dt}(\exp_G(tv)) = L_v(\exp_G(tv)) \quad (\forall v \in T_G(\mathbb{C}))$,

where $L_v(x) = m_x'(v)$, and where $m_x : G \to G$ is such that $m_x(g) = xg$. Then, the isomorphism is induced by the *exponential map of* E, $\exp_E : \mathbb{C} \to E$, defined as

$$\exp_E(z) = \begin{cases} [1, \wp(z), \wp'(z)] & \text{if } z \in \mathbb{C}\backslash\Lambda \\ [0, 0, 1] & \text{if } z \in \Lambda. \end{cases}$$

It is a complex analytic homomorphism of complex Lie groups.

Proposition 2.2.8. *Let $\tau \in \mathcal{O}$. The* multiplication-by-τ map *$[\tau] : E \to E$ defined by*

$$[\tau](p) = \exp_E(\tau \cdot \exp_E^{-1}(p)) \quad (\forall p \in E)$$

is an isogeny, i.e. $[\tau] \in \mathrm{End}(E)$. Further, every isogeny in End(E) *arises in this way.*

The following theorem is an amalgamation of results in [4].

Theorem 2.2.9 (Addition Law). *Let $z, y \in \mathbb{C}\backslash\Lambda$. Then the following holds:*
If $y \not\equiv \pm z \mod \Lambda$, then $\wp(z) \neq \wp(y)$ and

$$\wp(z+y) = \frac{1}{4}\left(\frac{\wp'(z)-\wp'(y)}{\wp(z)-\wp(y)}\right)^2 - \wp(z) - \wp(y);$$

$$\wp'(z+y) = \frac{\wp'(z)\wp(y) - \wp'(y)\wp(z) - \wp(z+y)(\wp'(z)-\wp'(y))}{\wp(z)-\wp(y)}.$$

If $y \equiv z \not\equiv -z \mod \Lambda$, then $\wp'(z) \neq 0$ and

$$\wp(z+y) = \wp(2z) = \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2 - 2\wp(z);$$

$$\wp'(z+y) = \wp'(2z) = \frac{\wp''(z)\wp(z) - \wp'(z)^2 - \wp(2z)\wp''(z)}{\wp'(z)}.$$

Recalling that $\wp'' = 6\wp^2 - g_2/2$ yields the following corollary.

Corollary 2.2.10. *Let $z, y \in \mathbb{C}\backslash\Lambda$. If $z+y \notin \Lambda$, then*

$$\wp(z+y), \wp'(z+y) \in \mathbb{Q}(g_2)(\wp(z), \wp(y), \wp'(z), \wp'(y)).$$

2.3 The Weierstrass ζ-function

Though the following function is not explicitly used in this thesis, it is used to define the η-function in Proposition 2.3.1. This η-function is noteworthy, as it figures in a useful result, namely Proposition 2.4.1.

Definition. The *Weierstrass ζ-function* (*for* Λ) is defined by the series

$$\zeta(z) \coloneqq \zeta(z;\Lambda) = \frac{1}{z} + \sum_{\omega\in\Lambda\backslash\{0\}}\left(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\right).$$

The Weierstrass ζ-function is an odd function which satisfies

$$\frac{d}{dz}\zeta(z) = -\wp(z).$$

Proposition 2.3.1. *Define* $\eta : \Lambda \to \mathbb{C}$ *by*

$$\eta(\omega) \coloneqq \eta(\omega; \Lambda) = 2\zeta(\omega/2; \Lambda).$$

Then, η *is an additive map satisfying, for each* $z \in \mathbb{C}\backslash\Lambda$ *and each* $\omega \in \Lambda$*, the equation*

$$\zeta(z + \omega) = \zeta(z) + \eta(\omega).$$

2.4 The Weierstrass σ-function

Definition. The *Weierstrass* σ*-function* (*for* Λ) is defined by the series

$$\sigma(z) \coloneqq \sigma(z; \Lambda) = z \prod_{\omega \in \Lambda\backslash\{0\}} \left(1 - \frac{z}{\omega}\right) e^{(z/\omega) + \frac{1}{2}(z/\omega)^2}.$$

The infinite product for $\sigma(z)$ defines a holomorphic function on all of $\mathbb{C}$. It has simple zeros at each $z \in \Lambda$, and no other zeros. The Weierstrass σ-function also satisfies

$$\frac{d}{dz} \log \sigma(z) = \zeta(z) \quad \text{and} \quad \frac{d^2}{dz^2} \log \sigma(z) = -\wp(z).$$

Proposition 2.4.1. *Let* $\omega \in \Lambda$ *and let* $z \in \mathbb{C}$*. Then*

$$\sigma(z + \omega) = \varepsilon e^{\eta(\omega)(z + \omega/2)} \sigma(z),$$

where $\varepsilon = 1$ *if* $\omega \in 2\Lambda$ *and* $\varepsilon = -1$ *if* $\omega \notin 2\Lambda$.

The following proposition provides a reciprocal to Theorem 2.1.1.

Proposition 2.4.2. *Let* $n_1, \ldots, n_r \in \mathbb{Z}$ *and let* $z_1, \ldots, z_r \in \mathbb{C}$ *be such that*

$$\sum_{i=1}^{r} n_i = 0 \quad \text{and} \quad \sum_{i=1}^{r} n_i z_i = \lambda \in \Lambda.$$

Then

$$f(z) = \frac{\sigma(z)}{\sigma(z - \lambda)} \prod_{i=1}^{r} \sigma(z - z_i)^{n_i}$$

belongs to $\mathbb{C}(\Lambda)$*. Furthermore, it satisfies*

$$\operatorname{div}(f) = \sum n_i(z_i).$$

Chapter 3

Equivalence Theorem

This chapter shows that the main theorem of this thesis is in fact equivalent to a statement which will be simpler to demonstrate. This problem reduction appears in Philippon's original proof, but its proof in this chapter is independent of Philippon's methods.

3.1 Preliminaries

Throughout this section, fix a field K of characteristic zero, a field extension $C \supseteq K$, and a subfield $k \subseteq \mathbb{C}$. The following lemma is a standard result [11]. Note that while it can be proven very quickly using the standard fact that any non-zero meromorphic function on an open connected subset of $\mathbb{C}$ has isolated zeros and poles, the proof provided below is more elementary.

Lemma 3.1.1. *Let D be an open connected subset of $\mathbb{C}$. If $f_1, f_2 : D \to \mathbb{C} \cup \{\infty\}$ are meromorphic functions such that $f_1 \cdot f_2 \equiv 0$, then either $f_1 \equiv 0$ or $f_2 \equiv 0$.*

Proof: Let f be a meromorphic function on D, and define the set

$$U_f = \{x \in D \,|\, \text{There exists } \varepsilon > 0 \text{ such that } f|_{B(x,\varepsilon)} = 0\}.$$

Clearly, U_f is open, but it can be shown that it is also closed.

Since $\varnothing$ is closed, assume without loss of generality that $U_f \neq \varnothing$. Let $a \in \overline{U_f}$, and so for all $n > 0$, there exists $b_n \in B(a, \frac{1}{n}) \cap U_f \neq \varnothing$. Since $b_n \in U_f$, then $f^{(j)}(b_n) = 0$ for $j \geqslant 0$. Since a is arbitrarily close to points for which $f^{(j)}$ is zero, we get that $f^{(j)}(a)$ is not infinity, and so $f^{(j)}$ must be continuous at the point a. Thus, $b_n \to a$ implies that $f^{(j)}(a) = 0$ for $j \geqslant 0$. Further, since f is differentiable at a, there exists $\varepsilon > 0$ such that f is represented by a Taylor series in $B(a, \varepsilon)$. Therefore,

$$f(x) = \sum_{j=0}^{\infty} \frac{1}{j!} f^{(j)}(a)(x-a)^n = 0$$

for all $x \in B(a, \varepsilon)$, and so $a \in U_f$. Hence, U_f is closed.

Since U_f is both open and closed, and since D is connected, then either $U_f = \varnothing$ or $U_f = D$. Thus, if $f : D \to \mathbb{C}$ is a meromorphic function, then

$$U_f \neq \varnothing \Rightarrow U_f = D.$$

Let f_1, f_2 be meromorphic functions on D such that $f_1 \cdot f_2 \equiv 0$. Assume without loss of generality that $f_2 \not\equiv 0$. Then, there exists $a \in D$ such that $f_2(a) \neq 0$, and so there exists $\varepsilon > 0$ such that $f_2 \neq 0$ on all of $B(a, \varepsilon)$. Thus, $f_1|_{B(a,\varepsilon)} = 0$, and so $a \in U_{f_1} \neq \varnothing \Rightarrow U_{f_1} = D$. Thus, $f_1 \equiv 0$, completing the proof. ∎

Before stating the following corollary, note that the binary relation $\leqslant$ will be used to denote the usual ordering on $\mathbb{Z}$ as well as the partial order over $\mathbb{Z} \times \mathbb{Z}$ defined by

$$(x_1, y_1) \leqslant (x_2, y_2) \Leftrightarrow x_1 \leqslant x_2 \quad \text{and} \quad y_1 \leqslant y_2.$$

Also define $(x_1, y_1) < (x_2, y_2) \Leftrightarrow (x_1, y_1) \leqslant (x_2, y_2)$ and either $x_1 < x_2$ or $y_1 < y_2$.

Corollary 3.1.2. *Let h_1, h_2 be meromorphic functions on $\mathbb{C}$. If there exists $H \in k[x,y]\backslash\{0\}$ such that $H(h_1, h_2) \equiv 0$, then there exists $G \in k[x,y]\backslash\{0\}$ which is irreducible and which satisfies $G(h_1, h_2) \equiv 0$.*

Proof: Suppose there exists H as described. Then, in particular, there exists $G \in k[x, y]\backslash\{0\}$ minimal in $(\deg_x G, \deg_y G)$ which satisfies $G(h_1, h_2) \equiv 0$. Suppose to the contrary that G is not irreducible. Then, there exists $g_1, g_2 \in k[x, y]\backslash\{0\}$ with $(\deg_x g_i, \deg_y g_i) < (\deg_x G, \deg_y G)$ such that $G = g_1 g_2$. Thus, the $f_i \coloneqq g_i(h_1, h_2)$ are meromorphic functions on $\mathbb{C}$ such that $f_1 f_2 \equiv 0$, and so Lemma 3.1.1 yields that f_1 or f_2 is zero, which contradicts the minimality for G. Thus, G is irreducible, as required. ▮

Throughout what follows, view $C(x)$ and $K((x^{-1}))$ as subfields of $C((x^{-1}))$. Thus, it makes sense to take their intersection.

Lemma 3.1.3. $C(x) \cap K((x^{-1})) = K(x)$

Proof: Since $K(x) \subseteq C(x) \cap K((x^{-1}))$, it suffices to show $C(x) \cap K((x^{-1})) \subseteq K(x)$. To this end, given $F \in C(x)\backslash\{0\}$, there exists $A, B \in C[x]$ such that $(A, B) = 1$ and $F = A/B$. Standard results in algebra yield the unicity of $\deg A + \deg B$ for $(A, B) = 1$, and so it makes sense to define a function $h : C(x) \to \mathbb{N}$ by

$$h(F) = \begin{cases} \deg A + \deg B & \text{if } F \neq 0; \\ 0 & \text{if } F = 0, \end{cases}$$

where A, B satisfy the aforementioned properties. The proof that

$$F \in C(x) \cap K((x^{-1})) \Rightarrow F \in K(x) \tag{3.1.1}$$

is done by induction on $h(F) \geqslant 0$:

The base case $h(F) = 0$ yields that $F(x) = c \in K((x))$ for some $c \in K$, and so $F \in K(x)$. Suppose now that (3.1.1) holds for $h(F) \in \{0, ..., n-1\}$. Then, let $F \in C(x) \cap K((x^{-1}))$ with $h(F) = n > 0$. Thus, there exists $A, B \in C[x]$ with $(A, B) = 1$ such that $F = A/B$. Notice that if $R \in C(x) \cap K((x^{-1}))\backslash\{0\}$, then $1/R \in C(x) \cap K((x^{-1}))$. Thus, since $h(1/F) = n$, assume without loss of generality that $\deg A \geqslant \deg B$. Furthermore, letting $r = \deg A$ and $s = \deg B$ yields that

$$A(x) = \sum_{i=0}^{r} a_i x^i \quad \text{(for some } a_i \in C\text{)};$$

$$B(x) = \sum_{j=0}^{s} b_j x^j \quad \text{(for some } b_j \in C\text{)}.$$

Thus, F satisfies

$$F(x) \equiv a_r b_s^{-1} \left(x^{-1}\right)^{s-r} \mod \left(x^{-1}\right)^{s-r+1} C[[x^{-1}]]$$

Since $F \in K((x^{-1}))$, it follows that $a_r b_s^{-1} \in K$, and so

$$G(x) \coloneqq F(x) - a_r b_s^{-1} x^{r-s} \in K((x^{-1})).$$

Since $r \geqslant s$, then

$$H(x) \coloneqq G(x)B(x) = A(x) - a_r b_s^{-1} x^{r-s} B(x) = \sum_{i=0}^{r-1} a_i x^i - a_r b_s^{-1} \sum_{j=r-s}^{r-1} b_{j+s-r} x^j,$$

is in fact a polynomial in $C[x]$. Suppose that $H = 0$, and so $G = 0$ which implies that $h(G) = 0 < n$. Suppose that $H \neq 0$. Then $\deg H \leqslant r - 1 < \deg A$, and so

$$G(x) = \frac{H(x)}{B(x)} \in C(x) \cap K((x^{-1}))$$

is such that $h(G) \leqslant \deg H + \deg B < h(F) = n$. The induction hypothesis then yields that $G(x) \in K(x)$. Thus,

$$F(x) = G(x) + a_r x^{r-s} \in K(x).$$

The desired result follows by induction. ∎

Corollary 3.1.4. $C(x) \cap K((x)) = K(x)$

Proof: By the previous lemma, $C(x^{-1}) \cap K((x)) = K(x^{-1})$. However, $C(x^{-1}) = C(x)$ and $K(x^{-1}) = K(x)$, thus completing the proof. ∎

In order to state the following lemma, the technical issue regarding composition in a given field of formal Laurent series over a field C needs to be treated (cf. [11]).

Definition. A family $\{g_n(x)\}_{n\in\mathbb{N}}$ of formal Laurent series in $\mathbb{C}((x))$ is called *summable* if for each integer k,

$$\mathrm{ord}_x g_n > k$$

for all but a finite number of g_n's.

Example. The family $\left\{ \sum_{k=n}^{\infty} x^n \right\}_{n\in\mathbb{N}}$ is a summable family of Laurent series.

Note in this context that ord_x operates on Laurent series, and that it is not to be confused with the order function introduce in Chapter 2 which operated on meromorphic functions.

If a family $\{g_n(x)\}_{n\in\mathbb{N}}$ is summable, then the sum of the family defines a Laurent series. Indeed, by letting $m = \min_n\{\mathrm{ord}_x g_n\} > -\infty$, the sum of the family can then be defined as

$$g(x) = \sum_{i=m}^{\infty} \left(\sum_{n=0}^{\infty} a_{n,i} \right) x^i,$$

where $g_n(x) = \sum_{n=\mathrm{ord}_x g_n}^{\infty} a_{n,i} x^i$. Since each sum $\sum_{n=0}^{\infty} a_{n,i}$ is in fact a finite sum, then $g \in C((x))$.

Proposition 3.1.5. *Let $f \in C((x))$, and let $g \in xC[[x]]$. Let $l = \mathrm{ord}_x f$, let $m = \mathrm{ord}_x g > 0$, and write*

$$f(x) = \sum_{n=l}^{\infty} a_n x^n \quad \textit{and} \quad g(x) = \sum_{n=m}^{\infty} b_n x^n \quad (\textit{for some } a_n, b_n \in C).$$

Then, the composition $f \circ g$ is defined and belongs to $C((x))$. Further, $\mathrm{ord}_x(f \circ g) = lm$, and the coefficient of $f \circ g$ in x^{lm} is $a_l b_m^l$.

Proof: Since $b_m \neq 0$, it makes sense to define functions r_n via the relation

$$\left(1 + \sum_{i=1}^{\infty} \frac{b_{i+m}}{b_m} x^i\right)^n = 1 + r_n(x) \quad (\forall n \in \mathbb{Z}).$$

Note that $r_n(x) \in xC[[x]]$ for each integer n. Since $g(x)^n = b_m^n x^{mn}(1 + r_n(x))$, then $\mathrm{ord}_x(g^n) = nm = n\mathrm{ord}_x g$, and so the sequence $(\mathrm{ord}_x(g^l), \mathrm{ord}_x(g^{l+1}), \dots)$ is strictly increasing. It follows that $\{a_n g^n(x)\}_{n \geqslant l}$ is a summable family, and so

$$f \circ g = \sum_{n=l}^{\infty} a_n g^n(x) \in C((x)).$$

In particular, $\mathrm{ord}_x(f \circ g) = lm$, and the coefficient of $f \circ g$ in x^{lm} is $a_l b_m^l$. ∎

Lemma 3.1.6. *Let $f \in C((x))$, and let $g \in xK[[x]]\backslash\{0\}$. If $f \circ g \in K((x))$, then $f \in K((x))$.*

Proof: Let f, g be as described above. If $f = 0$, then $f \in K((x))$. Thus, assume without loss of generality that $f \neq 0$. Let $l = \mathrm{ord}_x f$ and $m = \mathrm{ord}_x g$ for some $l, m \in \mathbb{Z}$. Thus,

$$f(x) = \sum_{n=l}^{\infty} a_n x^n \quad (\text{for some } a_n \in C);$$

$$g(x) = \sum_{n=m}^{\infty} b_n x^n \quad (\text{for some } b_n \in K).$$

Suppose to the contrary that $f \notin K((x))$. Then there exists a smallest integer p such that $a_p \notin K$. Thus, $f_p(x) := a_l x^l + \cdots + a_{p-1}x^{p-1} \in K((x))$, and so $h := f \circ g - f_p \circ g \in K((x))$. Then, $\mathrm{ord}_x h = pm$, and so $a_p b_m^p \in K$. Since $b_m \neq 0$, this implies that $a_p \in K$, which is a contradiction. Therefore, $f \in K((x))$ as required. ∎

Lemma 3.1.7. *Let $f \in C(x)$, and let $g \in xK[[x]]\backslash\{0\}$. If $f \circ g \in K((x))$, then $f \in K(x)$.*

Proof: Let f, g be as described above. Then, since $f \in C(x) \subseteq C((x))$, Lemma 3.1.6 yields that $f \in K((x))$. Thus, $f \in C(x) \cap K((x))$, and so $f \in K(x)$ by Corollary 3.1.4. ∎

3.2 Equivalence Theorem

Throughout this section, fix a lattice $\Lambda \subset \mathbb{C}$, and recall that $\mathcal{O} = \{\tau \in \mathbb{C} \mid \tau\Lambda \subseteq \Lambda\}$. Fix $K = \mathbb{Q}(g_2, g_3)$, and fix $k = \mathrm{Frac}(\mathcal{O})$, i.e. the fractional field of $\mathcal{O}$. The following notion will prove to be useful.

Definition. Let $x_1, \ldots, x_s \in \mathbb{C}$. The set $\{x_1, \ldots, x_s\}$ is said to be *irreducible (with respect to* Λ*)* if

$$\sum_{i \in I} x_i \not\equiv 0 \mod \Lambda,$$

for each non-empty subset $I \subseteq \{1, \ldots, s\}$.

Suppose that $x_1, \ldots, x_s \in \mathbb{C}$ are such that $x_1 + \cdots + x_s \notin \Lambda$. Then, there exists a non-empty subset $I \subseteq \{1, \ldots, s\}$ with minimal cardinality such that

$$\sum_{i \in I} x_i \equiv \sum_{i=1}^{s} x_i \mod \Lambda.$$

In this case, the set $(x_i)_{i \in I}$ is called a *reduction* of the $\{x_1, \ldots, x_s\}$. If it is not irreducible, then there exists a non-empty subset $J \subset I$ such that $\sum_{i \in J} x_i \in \Lambda$, but then $I \backslash J \neq \varnothing$ contradicts the minimality of I. Thus, any reduction must be irreducible.

Proposition 3.2.1. *Let* $\{x_1, \ldots, x_s\} \subset \mathbb{C}$ *be irreducible. Then*

$$\wp(x_1 + \cdots + x_s), \wp'(x_1 + \cdots + x_s) \in \mathbb{Q}(g_2)(\wp(x_1), \ldots, \wp(x_s), \wp'(x_1), \ldots, \wp'(x_s)).$$

Proof: The claim is proven by induction on $s \geqslant 1$. For the base case $s = 1$, $x_1 \notin \Lambda$, and so $\wp(x_1), \wp'(x_1) \in \mathbb{Q}(g_2)(\wp(x_1), \wp'(x_1))$ is trivially true. Suppose for $s = 1, \ldots, n-1$ that $\wp(x_1 + \cdots + x_s)$ and $\wp'(x_1 + \cdots + x_s)$ belong to

$$\mathbb{Q}(g_2)(\wp(x_1), \ldots, \wp(x_s), \wp'(x_1), \ldots, \wp'(x_s)).$$

Let $\{x_1, \ldots, x_n\}$ be irreducible and so $\{x_1, \ldots, x_{n-1}\}$ is irreducible. Thus, by induction hypothesis, $\wp(x_1 + \cdots + x_{n-1})$ and $\wp'(x_1 + \cdots + x_{n-1})$ belong to

$$\mathbb{Q}(g_2)(\wp(x_1), \ldots, \wp(x_{n-1}), \wp'(x_1), \ldots, \wp'(x_{n-1})).$$

Corollary 2.2.10 yields that $\wp(x_1 + \cdots + x_n)$ and $\wp'(x_1 + \cdots + x_n)$ belong to

$$\mathbb{Q}(g_2)(\wp(x_1 + \cdots + x_{n-1}), \wp(x_n), \wp'(x_1 + \cdots + x_{n-1}), \wp'(x_n)),$$

and so

$$\wp(x_1 + \cdots + x_n), \wp'(x_1 + \cdots + x_n) \in \mathbb{Q}(g_2)(\wp(x_1), \ldots, \wp(x_n), \wp'(x_1), \ldots, \wp'(x_n)).$$

The desired result follows by induction. ∎

Before stating the next lemma, define for each $c \in \mathbb{C}^\times$

$$\wp_c(z) = \wp(cz) \quad \text{and} \quad \wp'_c(z) = \wp'(cz) \quad (\forall z \in \mathbb{C}).$$

Remark that this is strictly notation, as $(\wp_c)' = c\wp'_c$.

Lemma 3.2.2. *Let $c \in k^\times = \mathrm{Frac}(\mathcal{O})^\times$. Then, $\wp_c$ and $\wp'_c$ belong to $\overline{K(\wp)}$.*

Proof: Remark that

$$(\wp'_c)^2 = 4(\wp_c)^3 - g_2\wp_c - g_3 \quad (\forall c \in \mathbb{C}^\times),$$

and so $\wp'_c \in \overline{K(\wp_c)}$. Thus, it suffices to show that $\wp_c$ is algebraic over $K(\wp)$. Let $D \in \mathbb{N}^+$ be such that $\gamma = Dc \in \mathcal{O}\backslash\{0\}$. The first step is to show that $\wp_\gamma$ is in $K(\wp)$.

Note that $\wp_\gamma \in \mathbb{C}(\Lambda)$ is an even function, and so there exists $f(x) \in \mathbb{C}(x)$ such that $\wp_\gamma = f(\wp^{-1})$. Since $\wp \in x^{-2}K[[x]]\backslash x^{-1}K[[x]]$, then $g := \wp^{-1} \in x^2K[[x]]\backslash\{0\}$. Since $\wp \in K((x))$ and $\gamma x \in xK[[x]]$, then the composition $\wp_\gamma$ belongs to $K((x))$. Hence,

$$f \circ g = f(\wp^{-1}) = \wp_\gamma \in K((x)).$$

Lemma 3.1.7 then yields that $f \in K(x)$, and so $\wp_\gamma$ is in $K(\wp)$. Similarly, $\wp_D \in K(\wp)$ since $D \in \mathbb{N}^+ \subseteq \mathcal{O}\backslash\{0\}$, and so there exists $G \in K[x,y]\backslash\{0\}$ such that $G(\wp, \wp_D) = 0$. Hence,

$$G(x,y) = \sum_{i=0}^{m} A_i(y)x^i,$$

for some $A_i(y) \in K[y]$, not all zero. Thus,

$$\sum_{i=0}^{m} A_i(\wp_D)\wp^i = 0,$$

from which it follows that

$$\sum_{i=0}^{m} A_i(\wp_\gamma)(\wp_{\gamma/D})^i = 0 \quad (\forall\gamma \in \mathbb{C}^\times).$$

Since a meromorphic function over $\mathbb{C}$ cannot be the root of a polynomial in constant coefficients without being a constant itself, then each non-zero A_i satisfies $A_i(\wp_\gamma) \neq 0$. Thus, $G(x, \wp_\gamma) \in K(\wp_\gamma)[x]\backslash\{0\}$, and it admits $\wp_{\gamma/D}$ as a root. Therefore, $\wp_c = \wp_{\gamma/D}$ is algebraic over $K(\wp_\gamma) \subseteq K(\wp)$. ∎

Corollary 3.2.3. *Let $z_0 \in \mathbb{C}\backslash\Lambda$, and let $c \in k^\times$ be such that $cz_0 \notin \Lambda$. Then $\wp(cz_0)$ and $\wp'(cz_0)$ are algebraic over $K(\wp(z_0))$.*

Proof: Since $\wp'(cz_0) \in \overline{K(\wp(cz_0))}$, it suffices to show that $\wp(cz_0) \in \overline{K(\wp(z_0))}$. By Lemma 3.2.2 and Corollary 3.1.2, there exists irreducible $G(x,y) \in K[x,y]\backslash\{0\}$, such that $G(\wp(cz), \wp(z)) = 0$ for all $z \in \mathbb{C}$. Hence,

$$G(x,y) = \sum_{i=0}^{m} A_i(y)x^i,$$

for some $A_i(y) \in K[y]$, not all zero. Thus,

$$\sum_{i=0}^{m} A_i(\wp(z))\wp(cz)^i = 0.$$

Suppose that $G(x, \wp(z_0)) \in K(\wp(z_0))[x]$ is the zero polynomial. Then each $A_i(\wp(z_0)) = 0$, and so $\wp(z_0)$ is algebraic over K. Thus, there exists a minimal polynomial $m \in K[y]$ with $\deg m \geqslant 1$ such that $m(\wp(z_0)) = 0$. It follows that $m(y)|A_i(y)$ for $0 \leqslant i \leqslant n$, and so $m(y)$ divides $G(x, y)$. Since G is irreducible, then $G = \alpha m$ for some $\alpha \in K$. Thus, $\alpha m(\wp(z)) = 0$ for all $z \in \mathbb{C}$, and so $\wp(z)$ has a finite image, which yields a contradiction. Therefore, $G(x, \wp(z_0)) \in K(\wp(z_0))[x]\backslash\{0\}$, and it admits $\wp(cz_0)$ as a root, which yields the desired conclusion. ∎

Theorem 3.2.4. *Suppose that $\Lambda \cap \overline{\mathbb{Q}} = \{0\}$. The following statements are equivalent.*

(A) If $\beta_1, \ldots, \beta_s \in \overline{\mathbb{Q}}$ are linearly independent over k, then $\wp(\beta_1), \ldots, \wp(\beta_s)$ are algebraically independent over $\mathbb{Q}$.

(B) Let β be a non-zero algebraic integer, and $d = [k(\beta) : k]$. Then, it follows that $\wp(1), \wp(\beta), ..., \wp(\beta^{d-1})$ are algebraically independent over $\mathbb{Q}$.

Proof: Suppose that (A) is true. Let β be a non-zero algebraic integer and let $d = [k(\beta) : k]$. Then $1, \beta, \ldots, \beta^{d-1} \in \overline{\mathbb{Q}}$ are linearly independent over k. Since (A) is true, then $\wp(1), \wp(\beta), \ldots, \wp(\beta^{d-1})$ are algebraically independent over $\mathbb{Q}$, and so (B) holds. Thus, (A) implies (B).

Suppose that (B) is true, and let $\beta_1, \ldots, \beta_s \in \overline{\mathbb{Q}}$ be linearly independent over k. By the primitive element theorem, there exists $\gamma \in \overline{\mathbb{Q}}\backslash\{0\}$ such that $k(\gamma) = k(\beta_1, \ldots, \beta_s)$. Since γ is an algebraic number, there exists $D \in \mathbb{N}^+$ such that $\alpha = D\gamma$ is an algebraic integer. Letting $d = [k(\alpha) : k]$ and viewing $k(\alpha)$ as a k-vector space, then, since $\{\beta_1, \ldots, \beta_s\} \subseteq k(\gamma) = k(D\gamma) = k(\alpha)$ is a linearly independent subset over

k, there exists an extension $\mathfrak{B} = \{\beta_1, \ldots, \beta_d\}$ such that $\mathfrak{B}$ is a k-vector space basis of $k(\alpha)$. Thus,

$$\alpha^j = \sum_{i=1}^{d} c_{ij}\beta_i \quad (\text{for some } c_{ij} \in k; 0 \leqslant j < d).$$

Notice that $\alpha^j \in \overline{\mathbb{Q}}\backslash\{0\}$ for $0 \leqslant j < d$. It follows from the hypotheses of the theorem that

$$\alpha^j = \sum_{i=1}^{d} c_{ij}\beta_i \notin \Lambda \quad (0 \leqslant j < d).$$

Further, there exists I_j such that $(c_{ij})_{i \in I_j}$ is a reduction of $\{c_{1j}\beta_1, \ldots, c_{dj}\beta_d\}$, i.e.

$$\alpha^j \equiv \sum_{i \in I_j} c_{ij}\beta_i \mod \Lambda,$$

and each subsum of the above sum is not in Λ. Thus, Proposition 3.2.1 yields that

$$\mathbb{Q}(\wp(1), \wp(\alpha), \ldots, \wp(\alpha^{d-1})) \subseteq \overline{\mathbb{Q}}(\{\wp(c_{ij}\beta_i), \wp'(c_{ij}\beta_i) \,|\, 0 \leqslant j < d; (i,j) \in I_j \times \{j\}\}) =: \mathfrak{N}.$$

Then, under the hypothesis that (B) is true, it follows that $\wp(1), \wp(\alpha), \ldots, \wp(\alpha^{d-1})$ are algebraically independent over $\mathbb{Q}$, and so in particular, $\text{tr.deg}_{\mathbb{Q}}(\mathfrak{N}) \geqslant d$. Corollary 3.2.3 yields that $\mathfrak{N}$ is algebraic over $\overline{\mathbb{Q}}(\wp(\beta_1), \ldots, \wp(\beta_d))$, and so

$$\text{tr.deg}_{\mathbb{Q}}(\overline{\mathbb{Q}}(\wp(\beta_1), \ldots, \wp(\beta_d))) \geqslant \text{tr.deg}_{\mathbb{Q}}(\mathfrak{N}) \geqslant d.$$

Thus, $\wp(\beta_1), \ldots, \wp(\beta_d)$ are algebraically independent over $\overline{\mathbb{Q}}$, and so over $\mathbb{Q}$ as well. In particular, $\wp(\beta_1), \ldots, \wp(\beta_s)$ are algebraically independent over $\mathbb{Q}$. Thus, (B) implies (A). ∎

Chapter 4

Analytic Estimates

The goal of this chapter is to demonstrate three theorems. The first provides an estimate on the exponential map for some fixed elliptic curve. This estimate is based on an estimate in Philippon's original proof, but is obtained independently. The second is a generalization of Cauchy's inequality in several variables. Finally, the third theorem will deal with the construction of an auxiliary function, due to Philippon, but proven independently by using a result of Waldschmidt. Throughout this chapter, fix a lattice $\Lambda \subset \mathbb{C}$, let E be the induced elliptic curve, and define

$$\Phi = (\phi_0, \phi_1, \phi_2) = (\sigma^3, \sigma^3 \wp, \sigma^3 \wp').$$

Proposition 4.0.5. *The meromorphic functions ϕ_0, ϕ_1 and ϕ_2 are holomorphic on $\mathbb{C}$. Furthermore,*

$$\exp_E(z) = [\Phi(z)] \quad (\forall z \in \mathbb{C}).$$

Proof: Since σ is entire, it is clear that ϕ_0 is entire. Remark that the poles of $\wp$ are of order 2 and are situated on Λ, and that the poles of $\wp'$ are of order 3 and are situated on Λ. Thus, since σ^3 is entire with zeros of order 3 at each point of Λ, then ϕ_1 and ϕ_2 are entire functions. To show that $\exp_E = [\Phi]$, consider the following two cases. If $z \notin \Lambda$, then $\sigma^3(z) \neq 0$ and so

$$\exp_E(z) = [1, \wp(z), \wp'(z)] = [\Phi(z)] \quad (\forall z \in \mathbb{C} \backslash \Lambda).$$

If $z \in \Lambda$, then $\sigma^3(z) = \sigma^3(z)\wp(z) = 0$, and $\sigma^3(z)\wp'(z) \neq 0$. Thus,

$$\exp_E(z) = [0, 0, 1] = [\Phi(z)] \quad (\forall z \in \Lambda).$$

Thus, $\exp_E(z) = [\Phi(z)]$ for each $z \in \mathbb{C}$, as required. ▮

4.1 Estimates for Φ

This section is devoted to finding estimates on the functions ϕ_0, ϕ_1 and ϕ_2. Recall that $\eta : \Lambda \to \mathbb{C}$ is the unique additive map such that

$$\sigma(z + \omega) = \varepsilon e^{\eta(\omega)(z+\omega/2)}\sigma(z) \quad (\forall \omega \in \Lambda; \forall z \in \mathbb{C}),$$

where $\varepsilon = 1$ if $\omega \in 2\Lambda$ and $\varepsilon = -1$ if $\omega \notin 2\Lambda$.

Lemma 4.1.1. *Let $i \in \{0, 1, 2\}$. Then,*

$$\phi_i(z + \omega) = \varepsilon e^{3\eta(\omega)(z+\omega/2)}\phi_i(z) \quad (\forall \omega \in \Lambda; \forall z \in \mathbb{C}),$$

where $\varepsilon = 1$ if $\omega \in 2\Lambda$ and $\varepsilon = -1$ if $\omega \notin 2\Lambda$.

Proof: Since 1, $\wp$, and $\wp'$ are all periodic functions with respect to Λ, the formula for σ shows that the equation above is valid so long as $z \notin \Lambda$. Suppose then that $z \in \Lambda$. Since ϕ_i is continuous, then

$$\phi_i(z + \omega) = \lim_{t \to z} \phi_i(t + \omega) = \varepsilon \lim_{t \to z} e^{3\eta(\omega)(t+\omega/2)}\phi_i(t) = \varepsilon e^{3\eta(\omega)(z+\omega/2)}\phi_i(z),$$

for all $\omega \in \Lambda$, thus proving the claim. ▮

Before stating the following lemma, write $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, and let D be the fundamental parallelogram associated to $\{\omega_1, \omega_2\}$ which is centered at the origin. For each $z \in \mathbb{C}$, there exists a unique choice $a_z \in D$ and $\omega_z \in \Lambda$ such that $z = a_z + \omega_z$. This defines functions

$$a_z : \mathbb{C} \to D \quad \text{and} \quad \omega_z : \mathbb{C} \to \Lambda.$$

Accordingly, it makes sense to define

$$g(z) = 3\eta(\omega_z)(a_z + \omega_z/2) \quad (\forall z \in \mathbb{C}).$$

Lemma 4.1.2. *There exists $c_1 > 0$ such that $|g(z)| \leqslant c_1|z|^2$ for all $z \in \mathbb{C}$.*

Proof: Let $z \in \mathbb{C}$, and let $r, R > 0$ be such that $\overline{B(0;r)} \subset D \subset \overline{B(0;R)}$. Suppose that $|z| \leqslant r$, and so in particular $z \in D$. Thus, $a_z = z$ and $\omega_z = 0$, which implies that

$$|a_z|, |\omega_z| \leqslant |z|.$$

Suppose now that $|z| > r$, and note that $|a_z| \leqslant R$, and that $|\omega_z| \leqslant |z| + |a_z| \leqslant |z| + R$. Thus,

$$|a_z|, |\omega_z| \leqslant c'|z| \qquad (c' = 1 + R/r).$$

Since $c' \geqslant 1$, the above equation holds for all $z \in \mathbb{C}$. A bound for $\eta(\omega_z)$ can be obtained as follows.

Since $\{\omega_1, \omega_2\}$ is a $\mathbb{Z}$-basis for Λ, then $\omega_z = m_z\omega_1 + n_z\omega_2$ for a unique choice of $m_z, n_z \in \mathbb{Z}$. This defines functions $m_z, n_z : \mathbb{C} \to \mathbb{Z}$. In order to find estimates for m_z and n_z, let P be the parallelogram in the complex plane whose vertices are located at $\omega_1, \omega_2, -\omega_1$ and $-\omega_2$. Since ω_1 and ω_2 are linearly independent over $\mathbb{R}$, then

$$b_1\omega_1 + b_2\omega_2 \in P \Rightarrow |b_i| \leqslant 1 \quad (\forall b_1, b_2 \in \mathbb{R}).$$

Let $r_0 > 0$ be such that $\overline{B(0;r_0)} \subset P$, and so

$$m_z\omega_1 + n_z\omega_2 \in \overline{B(0;|\omega_z|)} \subset (|\omega_z|/r_0)P.$$

Thus, $|m_z|, |n_z| \leqslant |\omega_z|/r_0 \leqslant (c'/r_0)|z|$. Since η is additive, then

$$|\eta(\omega_z)| \leqslant |m_z||\eta(\omega_1)| + |n_z||\eta(\omega_2)| \leqslant (c'/r_0)(|\eta(\omega_1)| + |\eta(\omega_2)|)|z|.$$

Thus, letting $c'' = (c'/r_0)(|\eta(\omega_1)| + |\eta(\omega_2)|)$ yields that $\eta(\omega_z) \leqslant c''|z|$.

Let $c_1 = 6c'c''$, and so

$$|g(z)| = 3|\eta(\omega_z)(a_z + \omega_z/2)| \leqslant c_1|z|^2,$$

from which the conclusion follows. ∎

Corollary 4.1.3. *Let $c_1 > 0$ be as in the previous lemma, let $i \in \{0, 1, 2\}$, and let $z \in \mathbb{C}$. Then*

$$|\phi_i(a_z)|e^{-c_1|z|^2} \leqslant |\phi_i(z)| \leqslant |\phi_i(a_z)|e^{c_1|z|^2}.$$

Proof: By Lemma 4.1.1, it follows that

$$|\phi_i(z)| = e^{\mathrm{Re}(g(z))}|\phi_i(a_z)|,$$

and Lemma 4.1.2 yields that

$$-c_1|z|^2 \leqslant \mathrm{Re}(g(z)) \leqslant c_1|z|^2,$$

from which the claim follows. ∎

Corollary 4.1.4. *Let $i \in \{0, 1, 2\}$, and let $R \geqslant 1$. There exists $c_2 > 0$ depending only on Λ, such that*

$$|\phi_i(z)| \leqslant e^{c_2R^2} \quad (\forall |z| \leqslant R).$$

Proof: By Corollary 4.1.3, there exists $c_1 > 0$ such that

$$|\phi_i(z)| \leqslant |\phi_i(a_z)|e^{c_1R^2} \quad (\forall |z| \leqslant R).$$

Since ϕ_i is entire and D is bounded, there exists $M_i > 0$ such that $|\phi_i(z)| \leqslant M_i$ for all $z \in D$. Let $M = \max_i M_i$, let $N = \log \max\{1, M\}$, and let $c_2 = N + c_1$. Thus

$$|\phi_i(z)| \leqslant Me^{c_1 R^2} \leqslant e^{N+c_1 R^2} \leqslant e^{(N+c_1)R^2} = e^{c_2 R^2}$$

for all $|z| \leqslant R$, thus proving the claim. ∎

In order to state the following theorem, define the smallest vector length

$$\Omega := \Omega(\Lambda) = \min_{\omega \in \Lambda \backslash \{0\}} |\omega|,$$

and denote by C_0 the set of all points which are closer to $\frac{1}{2}\Lambda \backslash \Lambda$ than to Λ, i.e.

$$C_0 = \{z \in \mathbb{C} \mid \text{there exists } \omega \in \frac{1}{2}\Lambda \backslash \Lambda \text{ such that } |z - \omega| \leqslant |z - \lambda| \text{ for all } \lambda \in \Lambda\}.$$

Denote the complement of C_0 by C_2, i.e. $C_2 = \mathbb{C} \backslash C_0$.

Theorem 4.1.5. *There exists $c_3 > 0$ satisfying the following. Let $R \geqslant \max\{1, \Omega/4\}$, let $|z_0| \leqslant R$, and let $k \in \{0, 2\}$ be such that $z_0 \in C_k$. Then,*

$$e^{-c_3 R^2} \leqslant |\phi_k(z)|$$

for all $z \in B(z_0; \Omega/4)$.

Proof: From Corollary 4.1.3, there exists $c_1 > 0$ such that

$$|\phi_k(a_z)|e^{-c_1|z|^2} \leqslant |\phi_k(z)| \quad (\forall z \in \mathbb{C}).$$

Let B be the closed set defined by

$$B = \{z \in \mathbb{C} \,|\, \text{There exists } c \in \overline{C_k} \text{ such that } |z - c| \leqslant \Omega/4\}.$$

Notice that each point in C_k is at least $\Omega/2$ away from all zeros of ϕ_k. Thus, each point in the set B is at least at a distance of $\Omega/4$ from any zero of ϕ_k. Also note that C_k is invariant under translation by elements of Λ, and so B is as well. Let

$A = B \cap \overline{D}$, and so A is compact. Thus, since ϕ_k is entire and non-zero on A, there exists $M > 0$ such that $M \leqslant \phi_k(z)$ for all $z \in A$. Let $z \in B(z_0; \Omega/4)$, and so $|z| \leqslant 2R$, and $z = a_z + \omega_z \in B$. Thus,

$$a_z \in (B - \omega_z) \cap D = B \cap D = A,$$

and so $M \leqslant \phi_k(a_z)$. Let $N = \log \min\{1, M\}$, and let $c_3 = |N| + 4c_1$. Thus,

$$e^{-c_3 R^2} \leqslant e^{-(|N|+4c_1 R^2)} \leqslant M e^{-c_1 (2R)^2} \leqslant |\phi_k(z)|,$$

as required. ∎

4.2 Cauchy's Inequality

This section proves a generalization of Cauchy's inequality. Throughout this section, fix an integer $n \in \mathbb{N}^+$. For a complex continuous function $F : \mathbb{C}^n \to \mathbb{C}$ and a real number $r \geqslant 0$, define

$$|F|_r = \sup\{|F(\mathbf{z})|\,;\, \mathbf{z} \in B(\mathbf{0}, r)\}.$$

Theorem 4.2.1 (Cauchy's inequality)**.** *Let $r \in \mathbb{R}^+$, let $q \in \mathbb{N}^+$, and let $\mathbf{a} \in \mathbb{C}^q$. Suppose that F is a holomorphic function on $B(\mathbf{a}; r) \subset \mathbb{C}^q$, and that it is continuous on its closure. Then,*

$$|F^{(\sigma)}(\mathbf{a})| \leqslant \frac{\sigma!}{r^{|\sigma|}} |F(\mathbf{a} + \mathbf{z})|_r \quad (\forall \sigma \in \mathbb{N}^q).$$

Furthermore, if $r \geqslant 1$, then

$$|F^{(\sigma)}(\mathbf{a} + \mathbf{z})|_{r-1} \leqslant \sigma! |F(\mathbf{a} + \mathbf{z})|_r \quad (\forall \sigma \in \mathbb{N}^q).$$

Proof: Cauchy's integral formula in several variables yields

$$\left.\frac{\partial^{|\sigma|}}{\partial \mathbf{z}^\sigma} F(\mathbf{z})\right|_{\mathbf{z}=\mathbf{a}} = \frac{\sigma!}{(2\pi i)^q} \int_{|z_1|=r} \cdots \int_{|z_q|=r} \frac{F(\mathbf{a} + \mathbf{z})}{z_1^{\sigma_1+1} \cdots z_q^{\sigma_q+q}} dz_1 \cdots dz_q,$$

and so

$$\begin{aligned}|F^{(\sigma)}(\mathbf{a})| &\leqslant \frac{\sigma!}{(2\pi)^q}\frac{|F(\mathbf{a}+\mathbf{z})|_r}{r^{|\sigma|+q}}\int_{|z_1|=r}\cdots\int_{|z_q|=r} dz_1\cdots dz_q\\ &= \frac{\sigma!}{(2\pi)^q}\frac{|F(\mathbf{a}+\mathbf{z})|_r}{r^{|\sigma|+q}}(2\pi r)^q,\end{aligned}$$

thus proving the first inequality. For the second inequality, let $z_0 \in \mathbb{C}^q$ be such that $|z_0| \leqslant r-1$, and so F is holomorphic on $B(\mathbf{a}+z_0;1)$ and continuous on its closure. Thus,

$$|F^{(\sigma)}(\mathbf{a}+z_0)| \leqslant \sigma!|F(\mathbf{a}+\mathbf{z})|_r,$$

and so

$$|F^{(\sigma)}(\mathbf{a}+\mathbf{z})|_{r-1} \leqslant \sigma!|F(\mathbf{a}+\mathbf{z})|_r,$$

as required. ∎

4.3 Auxiliary Function

In order to construct an auxiliary function, the following result which is due to Waldschmidt [7] will be used.

Lemma 4.3.1. *Let $M, n \in \mathbb{N}^+$, let $S, U, R, r \in \mathbb{R}^+$, and let $\varphi_1, \ldots, \varphi_M$ be continuous functions on $B(\mathbf{0}, R) = \{z \in \mathbb{C}^n; |z| \leqslant R\}$, which are analytic inside. If*

$$3 \leqslant U, S \leqslant U, e \leqslant R/r \leqslant e^U, \sum_{\lambda=1}^{M} |\varphi_\lambda|_R \leqslant e^U,$$

and

$$(8U)^{n+1} \leqslant MS\left(\log\frac{R}{r}\right)^n,$$

then, there exists $p_1, \ldots, p_M \in \mathbb{Z}$ with

$$0 < \max_{1\leqslant\lambda\leqslant M} |p_\lambda| \leqslant e^S,$$

such that the function

$$F = \sum_{\lambda=1}^{M} p_\lambda \varphi_\lambda$$

satisfies

$$|F|_r \leqslant e^{-U}.$$

In order to prove the following theorem, which is in essence a simplified construction of Philippon's auxiliary function found in Lemma 4.1 of [8], define $\rho : \mathbb{C}^q \to \mathbb{C}^{qd}$ by

$$\rho(\mathbf{t}) = (\mathbf{t}, \mathbf{t}\beta, \ldots, \mathbf{t}\beta^{d-1}),$$

and define $\Psi : \mathbb{C}^{qd} \to (\mathbb{C}^3)^{qd}$ by

$$\Psi(\mathbf{z}) = (\Phi(z_1), \ldots, \Phi(z_{qd})).$$

Also note the following notation and definition.

- $f(L) \ll g(L)$ signifies that there exists $c > 0$ such that $0 < f(L) \leqslant cg(L)$ for sufficiently large L.
- $f(L) \asymp g(L)$ signifies that $f(L) \ll g(L)$ and $g(L) \ll f(L)$.

Definition. A polynomial $P(\mathbf{z}_1, \ldots, \mathbf{z}_n)$ is said to be *multihomogeneous* of *multidegree* $(d_1, \ldots, d_n)$ if it is homogeneous of degree d_i in $\mathbf{z}_i$ for each $i \in \{1, \ldots, n\}$.

Theorem 4.3.2. *Fix $d \in \mathbb{N}^+$. Let $\epsilon \in \mathbb{R}^+$ be arbitrarily small, and fix $q \in \mathbb{N}$ such that $q > (2+\epsilon)/(\epsilon(2d-1))$. Then, for each sufficiently large $L \in \mathbb{N}^+$, there exists a non-zero multihomogeneous polynomial*

$$P \in \mathbb{Z}[\mathbf{Z}, \mathbf{X}_1, \ldots, \mathbf{X}_{qd}]$$

of degree L in $\mathbf{Z} = (Z_0, \ldots, Z_q)$ and of degree $D = \lfloor (\log L)^\epsilon \rfloor + 1$ in each $\mathbf{X}_i = (X_{i,0}, X_{i,1}, X_{i,2})$ with $\deg_{X_{i,2}} P \leqslant 1$, and with $\mathrm{h}(P) \leqslant L$ such that the function,

$$F(\mathbf{t}) = P(1, \mathbf{t}, \Psi \circ \rho(\mathbf{t})),$$

satisfies

$$\max_{|\sigma|\leqslant L}|F^{(\sigma)}|_{\log L}\leqslant\exp(-2L(\log L)^{1+\epsilon/2}).$$

The following commutative diagram illustrates the relation between F and P.

$$\begin{tikzcd}
\mathbb{C}^q \arrow[d, "{(1,\mathrm{id}_{\mathbb{C}^q},\Psi\circ\rho)}"'] \arrow[dr, "F"] & \\
\mathbb{C}^{q+1}\times(\mathbb{C}^3)^{qd} \arrow[r, "P"'] & \mathbb{C}
\end{tikzcd}$$

Proof: Note that q and d are fixed parameters, so any constant appearing in this proof might implicitly depend on the choice of q and d. Let $M=\binom{L+q}{q}(2D+1)^{qd}$, $n=q$, $S=L$, $R=\sqrt{L}$, $r=\log(L)+1$, $U=3L(\log L)^{1+\epsilon/2}$, and let $\varphi_1,\ldots,\varphi_M$ cover the monomials

$$\mathbf{t}^j\Phi(t_1)^{e_1}\cdots\Phi(t_q\beta^{d-1})^{e_{qd}}$$

with $|j|\leqslant L, |e_i|=D$ and $e_{i,2}\leqslant 1$. By Corollary 4.1.4, there exists $c>0$ such that

$$\begin{aligned}|\varphi_\lambda|_{R_0}&\leqslant R_0^L\exp\left(cR_0^2(|e_1|+\cdots+|e_{qd}|)\right)\\&=R_0^L\exp\left(cR_0^2qdD\right)\\&=\exp\left(L\log R_0+cR_0^2qdD\right)\end{aligned}$$

for each $\lambda\in\{1,\ldots,M\}$ and for each $R_0\geqslant 1$. Then,

$$\begin{aligned}\sum_{\lambda=1}^{M}|\varphi_\lambda|_R&\leqslant M\exp\left(L\log R+cR^2qdD\right)\\&=\binom{L+q}{q}(2D+1)^{qd}\exp\left(L\log R+cR^2qdD\right)\\&\ll 2^{L+q+qd}(\log L)^{\epsilon qd}\exp\left(L\log L+\tilde{c}L(\log L)^{\epsilon}\right)\\&\ll\exp\left(L+L\log L+\tilde{c}L(\log L)^{\epsilon}\right)\end{aligned}$$

This last expression is of order strictly less than $\exp\left(3L(\log L)^{1+\epsilon/2}\right)$, and so

$$\sum_{\lambda=1}^{M}|\varphi_\lambda|_R\leqslant\exp\left(3L(\log L)^{1+\epsilon/2}\right)=\exp U$$

for sufficiently large L. Further, for sufficiently large L, it follows that

$$er = e(\log(L) + 1) \leqslant \sqrt{L} = R \leqslant (\log(L) + 1) \cdot e^U = re^U.$$

Since $q > (2 + \epsilon)/(\epsilon(2d - 1))$, then

$$\begin{aligned} 1/q &< (d\epsilon - \epsilon/2)/(1 + \epsilon/2) \\ 1/q &< (1 + d\epsilon)/(1 + \epsilon/2) - 1 \\ (1 + q)/q &< (1 + d\epsilon)/(1 + \epsilon/2) \\ (1 + q)(1 + \epsilon/2) &< q(1 + d\epsilon). \end{aligned}$$

Note that $(8U)^{q+1} \asymp (L(\log L)^{1+\epsilon/2})^{1+q} = L^{1+q}(\log L)^{(1+q)(1+\epsilon/2)}$, and that

$$\begin{aligned} L^{1+q}(\log L)^{q+qd\epsilon} &= LL^q((\log L)^\epsilon)^{qd}(\log L)^q \\ &\asymp L\tbinom{L+q}{q}(2((\log L)^\epsilon + 1) + 1)^{qd}\left(\log\left(\frac{\sqrt{L}}{\log(L) + 1}\right)\right)^q \\ &= SM\left(\log\frac{R}{r}\right)^q. \end{aligned}$$

Thus, since $(1 + q)(1 + \epsilon/2) < q + qd\epsilon$, it follows that

$$(8U)^{n+1} \leqslant MS(\log(R/r))^n$$

for sufficiently large L. It is also easy to see that $S \leqslant U$ and that $U \geqslant 3$ for sufficiently large L. Thus, for sufficiently large L, Lemma 4.3.1 provides integers $p_1, \ldots, p_M$ such that

$$0 < \max_{1 \leqslant \lambda \leqslant M} |p_\lambda| \leqslant e^S,$$

and such that

$$F = \sum_{\lambda=1}^{M} p_\lambda \varphi_\lambda$$

satisfies

$$|F^{(\mathbf{0})}|_{\log L} \leqslant |F|_r \leqslant e^{-U}.$$

This induces the polynomial in the statement of the lemma, namely

$$P(\mathbf{Z}, \mathbf{X}_{11}, \ldots, \mathbf{X}_{qd}) = \sum_{\lambda=1}^{M} p_\lambda(\mathbf{Z}, \mathbf{X}_{11}, \ldots, \mathbf{X}_{qd})^{\mathbf{e}_\lambda} \quad (\text{where } \mathbf{e}_\lambda \in \mathbb{N}^{q+1} \times (\mathbb{N}^3)^{qd}),$$

with $\deg_{\mathbf{Z}} P = L$, each $\deg_{\mathbf{X}_{ij}} = D$, and each $\deg_{\mathbf{X}_{ij,2}} \leqslant 1$. Furthermore,

$$\mathrm{h}(P) \leqslant \mathrm{h}(1, \ldots, \lfloor e^S \rfloor) \leqslant S.$$

Finally, if $1 \leqslant |\sigma| \leqslant L$, then Cauchy's inequality yields

$$\begin{aligned} |F^{(\sigma)}|_{\log L} &\leqslant |\sigma|!|F|_r \\ &\leqslant L^L \exp(-U) \\ &= \exp\left(L \log L - 3L(\log L)^{1+\epsilon/2}\right) \\ &\leqslant \exp\left(-2L(\log L)^{1+\epsilon/2}\right), \end{aligned}$$

which is the desired result. ∎

Chapter 5

Heights

This chapter introduces the notion of the height of an algebraic number. The main goal, however, is to find estimates for the simultaneous height of several algebraic numbers, for instance the height of the set of coefficients of some polynomial. These results are obtained independently, and will ultimately be used to bound the heights of several families of polynomials so that Philippon's criterion for algebraic independence may be applied. Throughout this chapter, fix a number field $K \subset \mathbb{C}$, let $D = [K : \mathbb{Q}]$, and fix $n \in \mathbb{N}^+$.

5.1 Preliminaries

Definition. An absolute value on an integral domain R, denoted $|\cdot|_v$, is said to be *ultrametric* if

$$|x + y|_v \leqslant \max\{|x|_v, |y|_v\} \quad (\forall x, y \in R).$$

Otherwise, it is said to be *Archimedean.*

By Ostrowski's theorem, every non-trivial absolute value on K restricted to $\mathbb{Q}$ is equivalent (i.e. they yield the same topology) either to the usual absolute value on $\mathbb{Q}$ (in which case the absolute value is *Archimedean*), or to a p-adic absolute value (in which case the absolute value is *ultrametric*). Given an absolute value v, let $v|\infty$ denote that v is Archimedean, and let $v|p$ if v extends the p-adic valuation of $\mathbb{Q}$. For each equivalence class v, choose the following representative, denoted $|\cdot|_v$, and said to be normalized by

$$\begin{cases} |x|_v = x & \text{if } x \in \mathbb{Q},\ x > 0, \text{ and } v|\infty, \\ |p|_v = \frac{1}{p} & \text{if } v|p. \end{cases}$$

Denote the set of normalized absolute values by $\mathfrak{M}_K$, and define the local degree of K at $v \in \mathfrak{M}_K$ to be $D_v := [K_v : \mathbb{Q}_v]$, where K_v is the completion of K by v, and where $\mathbb{Q}_v$ is the completion of $\mathbb{Q}$ by $v|_{\mathbb{Q}}$. One fact that will be used frequently is that

$$\frac{1}{D}\sum_{v|\infty} D_v = 1.$$

For $v \nmid \infty$, the only fact concerning D_v that will be used in this thesis is that $D_v \in \mathbb{N}^+$. For a more detailed exposition on the absolute values which arise over a number field K, see [5].

Definition. Let $(\alpha_1, \ldots, \alpha_n) \in K^n$. The *height* of $(\alpha_1, \ldots, \alpha_n)$ is defined to be

$$\mathrm{h}(\alpha_1, \ldots, \alpha_n) = \frac{1}{D}\sum_{v \in \mathfrak{M}_K} D_v \log \max\{1, |\alpha_1|_v, \ldots, |\alpha_n|_v\}.$$

Notice that for $\alpha \in K$, $\mathrm{h}(\alpha)$ is equal to the Weil absolute logarithmic height [5]. Remark also that permuting the coordinates of the vector does not change the height, and so it makes sense to extend the height to finite sets, i.e.

$$\mathrm{h}((\alpha_i)_{1 \leqslant i \leqslant n}) = \mathrm{h}(\alpha_1, \ldots, \alpha_n).$$

Thus, this height can further be extended to a height for polynomials

$$P = \sum_{\mathbf{k}} c_{\mathbf{k}} \mathbf{x}^{\mathbf{k}} \in K[x_1, \ldots, x_n] \quad (\text{where } n \in \mathbb{N})$$

by defining

$$\mathrm{h}(P) = \frac{1}{D} \sum_{v \in \mathfrak{M}_K} D_v \log \max\{1, \|P\|_v\},$$

where

$$\|P\|_v = \max_{\mathbf{k}} |c_{\mathbf{k}}|_v.$$

The following lemma relates the height of a polynomial to its coefficients.

Lemma 5.1.1. *Let $Q \in K[x_1, \ldots, x_n]$, and write*

$$Q(\mathbf{x}) = \sum_{\mathbf{k}} a_{\mathbf{k}} \mathbf{x}^{\mathbf{k}} \quad (\textit{for some } a_{\mathbf{k}} \in K).$$

Then

$$|a_{\mathbf{k}}|_v \leqslant e^{D\mathrm{h}(Q)} \quad (\forall \mathbf{k} \in \mathbb{N}^n; \forall v \in \mathfrak{M}_K).$$

Proof: Let $v \in \mathfrak{M}_K$. Since the claim holds trivially for $a_{\mathbf{i}} = 0$, assume without loss of generality that $a_{\mathbf{i}} \neq 0$. Thus, $\log |a_{\mathbf{i}}|_v \leqslant \log \max_{\mathbf{i}}\{1, |a_{\mathbf{i}}|_v\}$. Thus,

$$\log \max_{\mathbf{i}}\{1, |a_{\mathbf{i}}|_v\} \leqslant \sum_{v' \in \mathfrak{M}_K} D_{v'} \log \max_{\mathbf{i}}\{1, |a_{\mathbf{i}}|_{v'}\} = [K : \mathbb{Q}]\mathrm{h}(Q),$$

and so $|a_{\mathbf{i}}|_v \leqslant e^{[K:\mathbb{Q}]\mathrm{h}(Q)}$. ∎

Further still, for an m-tuplet of polynomials $(P_1, \ldots, P_m)$, each P_i with coefficients in K, define the height of $(P_1, \ldots, P_m)$ by

$$\mathrm{h}(P_1, \ldots, P_m) = \frac{1}{D} \sum_{v \in \mathfrak{M}_K} D_v \log \max_{1 \leqslant i \leqslant m}\{1, \|P_i\|_v\}.$$

It follows trivially that

$$\mathrm{h}(P_1, \ldots, P_m) \leqslant \mathrm{h}(P_1) + \cdots + \mathrm{h}(P_m).$$

However, something stronger will typically be required.

5.2 Height inequalities for polynomials

The following two lemmas provide a foundation with which the estimation of the height of a polynomial with unknown height can potentially be reduced to an expression which can be understood in terms of the heights of polynomials whose heights are known. In order to state these lemmas, define for each $v \in \mathfrak{M}_K$ the map $\{\cdot\}_v : \mathbb{N}^+ \to \mathbb{N}^+$ by

$$\{m\}_v = \begin{cases} m & v|\infty, \\ 1 & v \nmid \infty. \end{cases}$$

Notice that this map is multiplicative. Its use primarily arises in concisely capturing the fact that

$$|a_1 + \cdots + a_m|_v \leqslant \{m\}_v \max_i |a_i|_v \quad (\forall a_i \in K; \forall v \in \mathfrak{M}_K).$$

The reader should note that the results in this chapter will ultimately be used to estimate the heights of polynomials which represent morphisms between projective algebraic varieties, and will thus focus on estimating the heights of homogeneous polynomials.

Lemma 5.2.1. *Let $m \in \mathbb{N}$; $s \in \mathbb{N}^+$, and let $\mathbf{x}$ be a multivariable over $\mathbb{C}^{m+1}$. Let $\alpha_1, \dots, \alpha_s \in K$, and let $P_1, \dots, P_s \in K[\mathbf{x}]$ be homogeneous of respective degrees $p_1, \dots, p_s$. Then, for all $v \in \mathfrak{M}_K$,*

$$\|\alpha_1 P_1 + \cdots + \alpha_s P_s\|_v \leqslant \{s\}_v \max_i |\alpha_i|_v \max_i \|P_i\|_v; \tag{5.2.1}$$

$$\|P_1 \cdots P_s\|_v \leqslant \left\{\tbinom{p+m}{p}\right\}_v^{s-1} \|P_1\|_v \cdots \|P_s\|_v, \tag{5.2.2}$$

where $p = \max\{p_1, \dots, p_s\}$.

Proof: Write $P_i = \sum_{|\mathbf{k}| \leqslant p} a_{i,\mathbf{k}} \mathbf{x}^{\mathbf{k}}$. Thus,

$$\|\alpha_1 P_1 + \cdots + \alpha_s P_s\|_v = \max_{\mathbf{k}} |\alpha_1 a_{1,\mathbf{k}} + \cdots + \alpha_s a_{s,\mathbf{k}}|_v$$

$$\begin{aligned}&\leqslant \max_{\mathbf{k}}(\{s\}_v \max_i |\alpha_i a_{i,\mathbf{k}}|_v)\\ &\leqslant \{s\}_v \max_i |\alpha_i|_v \max_i \|P_i\|_v,\end{aligned}$$

which proves the first inequality. The second inequality is proven by induction, whose base case $s = 1$ holds trivially. Suppose the inequality holds for $s \in \{1, \ldots, r-1\}$. Let $p = \max\{p_1, \ldots, p_r\}$ and write

$$P_1 \cdots P_{r-1} = \sum_{|\mathbf{i}|=p_1+\cdots+p_{r-1}} a_{\mathbf{i}} \mathbf{x}^{\mathbf{i}} \quad (\text{for some } a_{\mathbf{i}} \in K; \text{where } \mathbf{i} \in \mathbb{N}^{m+1});$$

$$P_r = \sum_{|\mathbf{j}|=p_r} b_{\mathbf{j}} \mathbf{x}^{\mathbf{j}} \quad (\text{for some } b_{\mathbf{j}} \in K; \text{where } \mathbf{j} \in \mathbb{N}^{m+1}),$$

so that

$$P_1 \cdots P_r = \sum_{|\mathbf{k}|=p_1+\cdots+p_r} \Big(\sum_{\mathbf{i}+\mathbf{j}=\mathbf{k}} a_{\mathbf{i}} b_{\mathbf{j}}\Big) \mathbf{x}^{\mathbf{k}} \quad (\text{where } \mathbf{k} \in \mathbb{N}^{m+1}).$$

Since each sum $\sum a_{\mathbf{i}} b_{\mathbf{j}}$ has at most $\binom{p+m}{m}$ terms, the induction hypothesis yields that

$$\begin{aligned}\|P_1 \cdots P_r\|_v &= \max_{\mathbf{k}} \Bigg|\sum_{\mathbf{i}+\mathbf{j}=\mathbf{k}} a_{\mathbf{i}} b_{\mathbf{j}}\Bigg|_v\\ &\leqslant \left\{\tbinom{p+m}{m}\right\}_v \cdot \max_{\mathbf{i}} |a_{\mathbf{i}}|_v \cdot \max_{\mathbf{j}} |b_{\mathbf{j}}|_v\\ &= \left\{\tbinom{p+m}{m}\right\}_v \|P_1 \cdots P_{r-1}\|_v \|P_r\|_v\\ &\leqslant \left\{\tbinom{p+m}{m}\right\}_v \left\{\tbinom{p+m}{m}\right\}_v^{r-2} \cdot \|P_1\|_v \cdots \|P_r\|_v.\end{aligned}$$

The second inequality follows by induction. ∎

Lemma 5.2.2. *Let $P_1, \ldots, P_s$ be polynomials with coefficients in K, and, for each $j \in \{1, \ldots, r\}$, let $Q_{j,1}, \ldots, Q_{j,s_j}$ be polynomials with coefficients in K. Suppose for each $v \in \mathfrak{M}_K$ and for some integer $N \geqslant 1$ that*

$$\max_{1 \leqslant i \leqslant s} \|P_i\|_v \leqslant \{N\}_v \max_{1 \leqslant k \leqslant s_1} \|Q_{1,k}\|_v \cdots \max_{1 \leqslant k \leqslant s_r} \|Q_{r,k}\|_v,$$

Then

$$\mathrm{h}((P_i)_i) \leqslant \log N + \sum_{j=1}^{r} \mathrm{h}((Q_{j,k})_k).$$

Proof: Indeed, this follows immediately by

$$\begin{aligned}\mathrm{h}((P_i)_i) &= \frac{1}{D} \sum_{v \in \mathfrak{M}_K} D_v \log \max_{1 \leqslant i \leqslant s} \{1, \|P_i\|_v\} \\ &\leqslant \frac{1}{D} \sum_{v \in \mathfrak{M}_K} D_v \log[\{N\}_v \prod_{j=1}^{r} \max_{1 \leqslant k \leqslant s_1} \{1, \|Q_{j,k}\|_v\}] \\ &= \log N + \sum_{j=1}^{r} \mathrm{h}((Q_{j,k})_k).\end{aligned}$$

∎

As trivial as the previous result may seem, its use lies in both guiding one to seek such bounds, and primarily to compactify arguments. Throughout, note that a *multivariable* over $\mathbb{C}^n$ is taken to signify an n-tuplet of indeterminates over $\mathbb{C}$.

Lemma 5.2.3. *Let* $\mathbf{z}$ *be a multivariable over* $\mathbb{C}^{n+1}$*, and let* $\mathbf{z}'$ *be a multivariable over* $\mathbb{C}^{n'+1}$*. Let* $\Psi' : \mathbb{C}^{n'+1} \to \mathbb{C}^{n+1}$ *and* $\Psi : \mathbb{C}^{n+1} \to \mathbb{C}^{n''+1}$ *be such that*

$$\Psi'(\mathbf{z}') = (\Psi'_0(\mathbf{z}'), \ldots, \Psi'_n(\mathbf{z}')) \quad \textit{and} \quad \Psi(\mathbf{z}) = (\Psi_0(\mathbf{z}), \ldots, \Psi_{n''}(\mathbf{z})),$$

where each $\Psi'_i \in K[\mathbf{z}']$ *and each* $\Psi_i \in K[\mathbf{z}]$ *are homogeneous polynomials. Let*

$$d' = \max_{0 \leqslant i \leqslant n} \deg_{\mathbf{z}'} \Psi'_i \quad \textit{and} \quad d = \max_{0 \leqslant i \leqslant n''} \deg_{\mathbf{z}} \Psi_i.$$

Then

$$\mathrm{h}(\Psi \circ \Psi') \leqslant \log \binom{d+n}{n} + (d-1) \log \binom{d'+n'}{n'} + \mathrm{h}(\Psi) + d\mathrm{h}(\Psi').$$

Proof: Remark that each Ψ_j consists of at most $\binom{d+n}{n}$ monomials, and so by applying Lemma 5.2.1, it follows for each $v \in \mathfrak{M}_K$ that

$$\max_{1 \leqslant j \leqslant n''} \|\Psi_j(\Psi'_0, \ldots, \Psi'_n)\|_v \leqslant \left\{\binom{d+n}{n}\right\}_v \max_{1 \leqslant j \leqslant n''} \|\Psi_j\|_v \cdot \max_{|\mathbf{i}| \leqslant d} \|(\Psi'_0)^{i_1} \cdots (\Psi'_n)^{i_n}\|_v$$

$$\begin{aligned}
&\leqslant \left\{\tbinom{d+n}{n}\right\}_v \max_{1\leqslant j\leqslant n''} \|\Psi_j\|_v \left\{\tbinom{d'+n'}{n'}\right\}_v^{d-1} \max_{|\mathbf{i}|\leqslant d} \|\Psi'_0\|_v^{i_1}\cdots\|\Psi'_n\|_v^{i_n}\\
&\leqslant \left\{\tbinom{d+n}{n}\tbinom{d'+n'}{n'}^{d-1}\right\}_v \max_{1\leqslant j\leqslant n''}\|\Psi_j\|_v\cdot\max_{0\leqslant i\leqslant n}\|\Psi'_i\|_v^{d}.
\end{aligned}$$

Since $(\Psi\circ\Psi')_j = \Psi_j(\Psi'_0,\ldots,\Psi'_n)$ for $1\leqslant j\leqslant n''$, Lemma 5.2.2 yields the result. ∎

In order to state the following proposition, define iteratively for a set S and a map $\Psi : S \to S$,

$$\Psi^{[m]} = \Psi^{[m-1]}\circ\Psi \quad\text{and}\quad \Psi^{[0]} = \mathrm{id}_S \quad (\forall m\in\mathbb{N}^+).$$

Proposition 5.2.4. *Let $\mathbf{z}$ be a multivariable over $\mathbb{C}^{n+1}$. Let $\Psi : \mathbb{C}^{n+1}\to\mathbb{C}^{n+1}$ be such that*

$$\Psi(\mathbf{z}) = (\Psi_0(\mathbf{z}),\ldots,\Psi_n(\mathbf{z})),$$

where each $\Psi_i\in K[\mathbf{z}]$ is a homogeneous polynomial. Let $d=\max_i \deg_{\mathbf{z}}\Psi_i$. Then

$$\mathrm{h}(\Psi^{[m]}) \leqslant [\mathrm{h}(\Psi)+\log\tbinom{d+n}{n}]\sum_{i=0}^{m-1} d^i + mn\log 2 + m^2 n\log d.$$

Proof: Let $B:\mathbb{N}^+\to\mathbb{R}$ be the function defined by

$$B(i) = \log\tbinom{d^i+n}{n} + (d^i-1)\log\tbinom{d+n}{n} + d^i\mathrm{h}(\Psi),$$

so that Lemma 5.2.3 yields

$$\mathrm{h}(\Psi^{[i+1]}) = \mathrm{h}(\Psi^{[i]}\circ\Psi) \leqslant B(i)+\mathrm{h}(\Psi^{[i]}) \quad (\forall i\in\mathbb{N}^+).$$

Thus, for all $m\in\mathbb{N}^+$ with $m>1$, it follows that

$$\begin{aligned}
\mathrm{h}(\Psi^{[m]}) &\leqslant \mathrm{h}(\Psi) + \sum_{i=1}^{m-1} B(i)\\
&= \mathrm{h}(\Psi)\sum_{i=0}^{m-1} d^i + \log\tbinom{d+n}{n}\sum_{i=1}^{m-1}(d^i-1) + \sum_{i=1}^{m-1}\log\tbinom{d^i+n}{n}.
\end{aligned}$$

Notice that $\binom{d+n}{n}\leqslant (d+1)^n$, and so

$$\log\tbinom{d^i+n}{n} \leqslant n\log(d^i+1) \leqslant n\log(2d^i) = n\log 2 + ni\log d.$$

Thus, it follows that

$$\begin{aligned}
\mathrm{h}(\Psi^{[m]}) &\leqslant \mathrm{h}(\Psi)\sum_{i=0}^{m-1} d^i + \log\tbinom{d+n}{n}\sum_{i=1}^{m-1}(d^i-1) + (m-1)n\log 2 + \tbinom{m}{2}n\log d \\
&= \left[\mathrm{h}(\Psi) + \log\tbinom{d+n}{n}\right]\sum_{i=0}^{m-1} d^i - m\log\tbinom{d+n}{n} + (m-1)n\log 2 + \tbinom{m}{2}n\log d \\
&\leqslant \left[\mathrm{h}(\Psi) + \log\tbinom{d+n}{n}\right]\sum_{i=0}^{m-1} d^i + mn\log 2 + m^2 n\log d,
\end{aligned}$$

as required. ∎

The following proposition, which is a generalization of Lemma 5.2.3, is the main result of this chapter, and will be used repeatedly throughout this thesis.

Proposition 5.2.5. *Let $(\mathbf{z}'_1,\dots,\mathbf{z}'_{\nu'})$ be a ν'-tuplet of multivariables over $\mathbb{C}^{n'+1}$, and let $(\mathbf{z}_1,\dots,\mathbf{z}_\nu)$ be a ν-tuplet of multivariables over $\mathbb{C}^{n+1}$. Let Ψ and Ψ' be such that*

$$\Psi' : (\mathbb{C}^{n'+1})^{\nu'} \to (\mathbb{C}^{n+1})^{\nu} \quad \textit{and} \quad \Psi : (\mathbb{C}^{n+1})^{\nu} \to \mathbb{C}^{n''+1}$$

with

$$\Psi(\mathbf{z}_1,\dots,\mathbf{z}_\nu) = (\Psi_0(\mathbf{z}_1,\dots,\mathbf{z}_\nu),\dots,\Psi_{n''}(\mathbf{z}_1,\dots,\mathbf{z}_\nu));$$

$$\Psi'(\mathbf{z}'_1,\dots,\mathbf{z}'_{\nu'}) = (\Psi'_1(\mathbf{z}'_1,\dots,\mathbf{z}'_{\nu'}),\dots,\Psi'_\nu(\mathbf{z}'_1,\dots,\mathbf{z}'_{\nu'}));$$

$$\Psi'_j(\mathbf{z}'_1,\dots,\mathbf{z}'_{\nu'}) = (\Psi'_{j,0}(\mathbf{z}'_1,\dots,\mathbf{z}'_{\nu'}),\dots,\Psi'_{j,n}(\mathbf{z}'_1,\dots,\mathbf{z}'_{\nu'})),$$

where for $1 \leqslant j \leqslant \nu$, $0 \leqslant i' \leqslant n$ and $0 \leqslant i \leqslant n''$, the maps

$$\Psi'_{j,i'} : \mathbb{C}^{n'+1} \to \mathbb{C} \quad \textit{and} \quad \Psi_i : \mathbb{C}^{n+1} \to \mathbb{C}$$

are polynomials satisfying

- *$\Psi'_{j,i'}$ is homogeneous of degree d'_j $\quad(1 \leqslant j \leqslant \nu; 0 \leqslant i' \leqslant n)$;*
- *Ψ_i is homogeneous of degree d_j in $\mathbf{z}_j$ $\quad(1 \leqslant j \leqslant \nu; 0 \leqslant i \leqslant n'')$.*

Then,

$$\mathrm{h}(\Psi \circ \Psi') \leqslant \sum_{i=1}^{\nu} \log \tbinom{d_i+n}{n} + (d-1) \log \tbinom{d'+(n'+1)\nu-1}{(n'+1)\nu-1} + \mathrm{h}(\Psi) + \sum_{i=1}^{\nu} d_i \mathrm{h}(\Psi'_i),$$

where $d' = \max_j |d'_j|$, *and* $d = d_1 + \cdots + d_\nu$.

Proof: Remark that Ψ_j consists of at most $\prod_{i=1}^{\nu} \tbinom{d_i+n}{n}$ monomials. Thus, for each $v \in \mathfrak{M}_K$, it follows by Lemma 5.2.1 that

$$\begin{aligned}
&\max_{0\leqslant j\leqslant n''} \|\Psi_j(\Psi'_1, \dots, \Psi'_\nu)\|_v \\
&\leqslant \left\{\prod_{i=1}^{\nu} \tbinom{d_i+n}{n}\right\}_v \max_{0\leqslant j\leqslant n''} \|\Psi_j\|_v \max_{|\mathbf{i}_k|\leqslant d_k} \|(\Psi'_1)^{\mathbf{i}_1} \cdots (\Psi'_\nu)^{\mathbf{i}_\nu}\|_v \\
&= \left\{\prod_{i=1}^{\nu} \tbinom{d_i+n}{n}\right\}_v \max_{0\leqslant j\leqslant n''} \|\Psi_j\|_v \max_{|\mathbf{i}_k|\leqslant d_k} \|(\Psi'_{1,0})^{i_{1,0}} \cdots (\Psi'_{1,n})^{i_{1,n}} \cdots (\Psi'_{\nu,0})^{i_{\nu,0}} \cdots (\Psi'_{\nu,n})^{i_{\nu,n}}\|_v.
\end{aligned}$$

Note that the above product consists of d factors of the form $\Psi'_{j,i}$, and that each of these is a polynomial in $(n'+1)\nu'$ variables with degree bounded by d'. Thus, it follows by Lemma 5.2.1 that

$$\begin{aligned}
&\max_{0\leqslant j\leqslant n''} \|\Psi_j(\Psi'_1, \dots, \Psi'_\nu)\|_v \\
&\leqslant \left\{\prod_{i=1}^{\nu} \tbinom{d_i+n}{n}\right\}_v \max_{0\leqslant j\leqslant n''} \|\Psi_j\|_v \left\{\tbinom{d'+(n'+1)\nu'-1}{(n'+1)\nu'-1}\right\}_v^{d-1} \max_{|\mathbf{i}_k|\leqslant d_k} \left(\prod_{l=0}^{n} \|\Psi'_{1,l}\|_v^{i_{1,l}} \cdots \prod_{l=0}^{n} \|\Psi'_{\nu,l}\|_v^{i_{\nu,l}}\right) \\
&\leqslant \left\{\prod_{i=1}^{\nu} \tbinom{d_i+n}{n}\right\}_v \left\{\tbinom{d'+(n'+1)\nu'-1}{(n'+1)\nu'-1}\right\}_v^{d-1} \max_{0\leqslant j\leqslant n''} \|\Psi_j\|_v \max_{0\leqslant l\leqslant n} \|\Psi'_{1,l}\|_v^{d_1} \cdots \max_{0\leqslant l\leqslant n} \|\Psi'_{\nu,l}\|_v^{d_\nu}.
\end{aligned}$$

Since $(\Psi \circ \Psi')_j = \Psi_j(\Psi'_1, \dots, \Psi'_\nu)$ for $0 \leqslant j \leqslant n''$, then Lemma 5.2.2 yields the result. ∎

Chapter 6

Representations of maps

The goal of this chapter is to construct polynomial representations for morphisms between products of elliptic curves. These polynomials are shown to have heights and degrees controlled. Philippon's original proof requires such representations, but the constructions and estimates in this thesis are independent of his methods. Throughout this chapter, fix a lattice Λ, fix $K = \mathbb{Q}(g_2, g_3)$, and fix $E = Z(h)$, where

$$h(x_0, x_1, x_2) = x_0 x_2^2 - 4x_1^3 + g_2 x_0^2 x_1 + g_3 x_0^3.$$

Note that E is an elliptic curve which is in Weierstrass normal form. Denote by $\sigma_2 : E \times E \to E$, the map representing the group law on E, and let $\mathbf{x} = (x_0, x_1, x_2)$ and $\mathbf{y} = (y_0, y_1, y_2)$ be triples of indeterminates over $E \subseteq \mathbb{C}^3$. By definition, the multiplication-by-2 map satisfies

$$[2](x_0 : x_1 : x_2) = \sigma_2((x_0 : x_1 : x_2), (x_0 : x_1 : x_2)).$$

6.1 Group law of bidegree $(2, 2)$ for an elliptic curve

According to [6], the following three addition laws form a complete system for σ_2 which is of bidegree $(2, 2)$. Lange and Ruppert denote

$$(z_0 : z_1 : z_2) = \sigma_2((x_0 : x_1 : x_2), (y_0 : y_1 : y_2)),$$

and use the abbreviations $p_{ij} = x_iy_j + x_jy_i$, and $q_{ij} = x_iy_j - x_jy_i$. Further writing abbreviations

$$p_{ijkl} = x_ix_jy_ky_l + x_kx_ly_iy_j \quad \text{and} \quad q_{ijkl} = x_ix_jy_ky_l - x_kx_ly_iy_j,$$

allows the complete system of bidegree (2,2) to be written as

$$\begin{aligned}
\text{I}\quad z_0 &= p_{20}q_{20} + (12x_1y_1 - g_2x_0y_0)q_{01}\\
z_1 &= q_{2201} + g_2p_{01}q_{01} + (2x_2y_2 + 3g_3x_0y_0)q_{01}\\
z_2 &= x_2y_2q_{20} + g_2q_{1200} + (2g_2x_0y_0 - 12x_1y_1)q_{21} + 3g_3x_0y_0q_{20}
\end{aligned}$$

$$\begin{aligned}
\text{II}\quad z_0 &= 4q_{2201} + 4g_2p_{01}q_{01} + (12g_3x_0y_0 - 8x_2y_2)q_{01}\\
z_1 &= 4p_{21}q_{21} + (4g_2x_1y_1 + g_2^2x_0y_0)q_{10} + 12g_3p_{10}q_{10}\\
z_2 &= (g_2^2x_0y_0 + 8g_2x_1y_1)q_{02} + (24g_3x_0y_0 - 4x_2y_2)q_{12} + 4g_2q_{1102} + 12g_3q_{0012}
\end{aligned}$$

$$\begin{aligned}
\text{III}\quad z_0 &= (4x_2y_2 - 12g_3x_0y_0)p_{02} + (48x_1y_1 - 8g_2x_0y_0)p_{12} - 4g_2p_{1200}\\
z_1 &= (4x_2y_2 + 24g_3x_0y_0)p_{12} + (8g_2x_1y_1 + g_2^2x_0y_0)p_{02} + 12g_3p_{1200} + 4g_2p_{0211}\\
z_2 &= 4x_2^2y_2^2 - 48g_2x_1^2y_1^2 + (g_2^3 - 36g_3^2)x_0^2y_0^2 - 4g_2^2p_{01}^2 - 8g_2^2x_0x_1y_0y_1\\
&\quad - (144g_3x_1y_1 + 12g_2g_3x_0y_0)p_{01}
\end{aligned}$$

Note that all q terms are antisymmetric in $(\mathbf{x}, \mathbf{y})$, and so are zero when $\mathbf{x} = \mathbf{y}$. Thus, laws I and II have $\mathbf{z} = \mathbf{0}$ whenever $\mathbf{x} = \mathbf{y}$. Since the above system is complete, it follows that law III represents $\sigma(\mathbf{x}, \mathbf{y})$ whenever $\mathbf{x} = \mathbf{y}$. Therefore, the isogeny [2] is represented by a single triplet of homogeneous polynomials, induced by III. Moreover, noting that z_0 of law III can be written as

$$z_0 = 96x_1^3x_2 + 8x_0x_2^3 - 24g_2x_0^2x_1x_2 - 24g_3x_0^3x_2 = 24x_2(4x_1^3 - g_2x_0^2x_1 - g_3x_0^3) + 8x_0x_2^3,$$

then $z_0 = 32x_0x_2^3$. Thus, [2] can be represented by

$$R_2 = (R_{2,0}, R_{2,1}, R_{2,2}) \in (K[\mathbf{x}])^3,$$

where

$$R_{2,0}(x_0 : x_1 : x_2) = 32x_0x_2^3;$$

$$R_{2,1}(x_0 : x_1 : x_2) = 8x_1x_2^3 + 24g_2x_0x_1^2x_2 + 72g_3x_0^2x_1x_2 + 2g_2^2x_0^3x_2;$$

$$R_{2,2}(x_0 : x_1 : x_2) = 4x_2^4 - 48g_2x_1^4 - 288g_3x_0x_1^3 - 24g_2^2x_0^2x_1^2 - 24g_2g_3x_0^3x_1 + (g_2^3 - 36g_3^2)x_0^4.$$

6.2 Multiplication by 2

The goal of this section is to prove that the isogeny [2] is represented by a single triplet of polynomials of degree 4, independently of the result of Lange and Ruppert. In order to do so, note that multiplication-by-2 on E can be reduced to the following three cases.

$$[2](1 : \wp(z) : \wp'(z)) = (1 : \wp(2z) : \wp'(2z)) \quad (\forall z \notin \tfrac{1}{2}\Lambda); \tag{6.2.1}$$

$$[2](1 : \wp(\omega/2) : 0) = (0 : 0 : 1) \quad (\forall \omega \in \Lambda\backslash 2\Lambda); \tag{6.2.2}$$

$$[2](0 : 0 : 1) = (0 : 0 : 1). \tag{6.2.3}$$

To show that R_2 represents the first case, let $z \notin \frac{1}{2}\Lambda$, and write $x = \wp(z)$ and $y = \wp'(z)$. Thus,

$$\wp(2z) = \frac{(12x^2 - g_2)^2 - 32xy^2}{16y^2};$$
$$\wp'(2z) = \frac{(12x^2 - g_2)(48xy^2 - (12x^2 - g_2)^2) - 32y^4}{32y^3},$$

and so (6.2.1) can be rewritten as

$$[2](1 : x : y) = (f_0(1, x, y) : f_1(1, x, y) : f_2(1, x, y)),$$

where

$$f_0(x_0, x_1, x_2) = 32x_0^3x_2^3$$
$$f_1(x_0, x_1, x_2) = 2x_0x_2[(12x_1^2 - g_2x_0^2)^2 - 32x_0x_1x_2^2]$$
$$f_2(x_0, x_1, x_2) = (12x_1^2 - g_2x_0^2)[48x_0x_1x_2^2 - (12x_1^2 - g_2x_0^2)^2] - 32x_0^2x_2^4.$$

Recall throughout that

$$4x^3 = y^2 + g_2x + g_3.$$

Thus,

$$\begin{aligned}(12x^2 - g_2)^2 &= 36x(y^2 + g_2x + g_3) - 24g_2x^2 + g_2^2\\ &= 12x(3y^2 + g_2x + 3g_3) + g_2^2,\end{aligned}$$

and so

$$f_1(1, x, y) = 4xy^3 + 24g_2x^2y + 72g_3xy + g_2^2y,$$

and

$$\begin{aligned}f_2(1, x, y) &= (12x^2 - g_2)[12x(y^2 - 3g_3 - g_2x) - g_2^2] - 32y^4\\ &= 12(12x^3 - g_2x)(y^2 - 3g_3 - g_2x) - g_2^2(12x^2 - g_2) - 32y^4\\ &= 12(3y^2 + 2g_2x + 3g_3)(y^2 - g_2x - 3g_3) - g_2^2(12x^2 - g_2) - 32y^4\\ &= 4y^4 - 36g_2^2x^2 + (g_2^3 - 108g_3^2) - 12(g_2xy^2 + 6g_3y^2 + 9g_2g_3x).\end{aligned}$$

Alternatively, noting that

$$(g_2x + 6g_3)y^2 = 4g_2x^4 + 24g_3x^3 - g_2^2x^2 - 7g_2g_3x - 6g_3^2$$

yields

$$\begin{aligned}f_2(1, x, y) &= 4y^4 - 36g_2^2x^2 + (g_2^3 - 108g_3^2) - 12(g_2xy^2 + 6g_3y^2 + 9g_2g_3x)\\ &= 4y^4 - 24g_2^2x^2 + (g_2^3 - 36g_3^2) - 48g_2x^4 - 288g_3x^3 - 24g_2g_3x.\end{aligned}$$

Evaluating at $(x_0, x_1, x_2) = (1, x, y)$ immediately yields

$$R_2(1, x, y) = (f_0(1, x, y), f_1(1, x, y), f_2(1, x, y)),$$

thus showing that R_2 indeed represents (6.2.1). Remark that

$$x_0^2R_{2,2}(x_0, x_1, x_2) \equiv f_2(x_0, x_1, x_2) \mod (h).$$

To show that R_2 represents the second case, let $w \in \Lambda\backslash 2\Lambda$, and write $x = \wp(\omega/2)$. Thus,

$$R_{2,0}(1, x, 0) = R_{2,1}(1, x, 0) = 0,$$

and so representation by R_2 requires that $R_{2,2}(1, x, 0) \neq 0$. For the sake of attaining a contradiction, suppose that $R_{2,2}(1, x, 0) = 0$. Thus, $f_2(1, x, 0) = 0$, and so $12x^2 = g_2$, which in particular implies that

$$(2x)^2 = g_2/3.$$

Since $h(1, x, 0) = 0$, then

$$4x^3 = g_2x + g_3,$$

and so

$$12x^2 = g_2 \Rightarrow 12x^3 = g_2x \Rightarrow 8x^3 = -g_3 \Rightarrow (2x)^3 = -g_3.$$

Thus,

$$(g_2/3)^3 = g_3^2 \Rightarrow g_2^3 - 27g_3^2 = 0,$$

and so $\Delta(\Lambda) = g_2^3 - 27g_3^2 = 0$, which is impossible. Thus, $R_{2,2}(1, x, 0) \neq 0$ and so

$$[2](1 : \wp(\omega/2) : 0) = (0 : 0 : 1) = (R_{2,0}(1, x, 0) : R_{2,1}(1, x, 0) : R_{2,2}(1, x, 0)),$$

from which it follows that (6.2.2) is represented by R_2. Finally, $R_2(0, 0, 1) = (0, 0, 4)$, and so

$$[2](0 : 0 : 1) = (0 : 0 : R_{2,2}(0, 0, 1)) = (R_{2,0}(0, 0, 1) : R_{2,1}(0, 0, 1) : R_{2,2}(0, 0, 1)),$$

and so R_2 represents (6.2.3). Thus, R_2 is a complete system for the isogeny [2], as required.

6.3 Multiplication by $\tau \in \mathcal{O}$

Throughout this section, suppose that $\mathcal{O} = \mathbb{Z}[\alpha]$ where α is an imaginary quadratic integer. In the previous section, a representation which forms a complete system for the multiplication-by-2 map has been fixed. In what follows, whenever a new morphism is introduced, either a representation will be fixed in tandem, or a fixed representation will be chosen to be induced by the new morphism's relation to morphisms whose representations have already been fixed. Notice that if a morphism has already been given a representation, then re-identifying it via a new relation may, a priori, lead to a conflict in the chosen representation. Thus, it will be important to eliminate such cases when treating classes of morphisms which contain at least one morphism whose representation has already been fixed.

The first step to acquiring representations for the isogenies $[\tau]$ with $\tau \in \mathcal{O}$ is to note that it suffices to fix representations for the isogenies [0], [1], [2], [−1], and $[\alpha]$, so that a representation for $[\tau]$ can be inferred by iterating via the representation for σ_2 provided by Lange and Ruppert. The case $m = 2^k$ can be treated as follows. For each $k > 2$, the multiplication-by-2^k map is given by $[2^k] = [2^{k-1}] \circ [2]$, where $[2^1] = [2]$, is a morphism requiring a single law. Indeed, the map $[2^k]$ is represented by the triplet of homogeneous polynomials, denoted

$$R_{2^k} = (R_{2^k,0}, R_{2^k,1}, R_{2^k,2}),$$

where each $R_{2^k,i} = R_{2^{k-1}} \circ R_{2,i} = (R_2^{[k]})_i \in K[\mathbf{x}]$. Further, define $[2^0] = [1] = \mathrm{id}_E$, with representation $R_1(\mathbf{x}) = \mathbf{x}$, and let

$$R^{\zeta}_{\sigma_2} = (R^{\zeta}_{\sigma_2,0}, R^{\zeta}_{\sigma_2,1}, R^{\zeta}_{\sigma_2,2})$$

be the polynomials in $(\mathbf{x}, \mathbf{y})$ such that $R^{\zeta}_{\sigma_2,i} = z_i$ for law $\zeta \in \{\text{I, II, III}\}$ of σ_2. The task of fixing a representation for $[m]$ with $m \in \mathbb{N}$ and $m > 2$ can be induced by iterating via the representation for σ_2 and representations for $[2^k]$ where $k \in \mathbb{N}$. Let $m \in \mathbb{N}^+$, with m not a power of 2. From the binary expansion of m, it follows that $m = 2^k + m'$ with $0 < m' < 2^k$ for unique $k, m' \in \mathbb{N}^+$. Thus, iterating via the relation

$$[m] = \sigma_2\left([2^k], [m']\right)$$

induces a family of triplets of homogeneous polynomials in $K[\mathbf{x}]$ which represent $[m]$, denoted

$$R_m^\zeta = (R_{m,0}^\zeta, R_{m,1}^\zeta, R_{m,2}^\zeta),$$

for a finite set of indices ζ. Note also that the zero isogeny is represented by

$$R_0(\mathbf{x}) = (R_{0,0}(\mathbf{x}), R_{0,1}(\mathbf{x}), R_{0,2}(\mathbf{x})) = (0, 0, 1).$$

Finally, for each $m \in \mathbb{N}^+$, the map $[-m]$ is represented by

$$R_{-m}^\zeta = (R_{-m,0}^\zeta, R_{-m,1}^\zeta, R_{-m,2}^\zeta) = (R_{m,0}^\zeta, R_{m,1}^\zeta, -R_{m,2}^\zeta),$$

thus fixing representations $(R_m^\zeta)_\zeta$ for all maps $[m]$ with $m \in \mathbb{Z}$.

Since $[\alpha]$ is an isogeny, there exists a family of triplets of homogeneous polynomials in $K[\mathbf{x}]$ which represents $[\alpha]$, denoted

$$R_\alpha^\zeta = (R_{\alpha,0}^\zeta, R_{\alpha,1}^\zeta, R_{\alpha,2}^\zeta),$$

for a finite set of indices ζ. Thus, for each $\tau = m + n\alpha \in \mathcal{O}\backslash(\mathbb{Z} \cup \{\alpha\})$, the relation

$$[\tau] = \sigma_2([m], [\alpha] \circ [n])$$

induces a family of triplets of homogeneous polynomials in $K[\mathbf{x}]$ which represent $[\tau]$, denoted

$$R_\tau^\zeta = (R_{\tau,0}^\zeta, R_{\tau,1}^\zeta, R_{\tau,2}^\zeta)$$

for a finite set of indices ζ.

In order to state the results which follow in this section, take note of the following notation. Given a morphism Ψ and a fixed representation by a family of $(n+1)$-tuples of homogeneous polynomials, denoted

$$R_\Psi^\zeta = (R_{\Psi,0}^\zeta, \dots, R_{\Psi,n}^\zeta),$$

for a finite set of indices ζ, define

$$\deg_{\mathbf{x}}(\Psi) = \max_{\zeta,i} \deg_{\mathbf{x}}(R_{\Psi,i}^\zeta);$$

$$\mathrm{h}(\Psi) = \max_{\zeta} \mathrm{h}(R^{\zeta}_{\Psi,0}, \ldots, R^{\zeta}_{\Psi,n}).$$

Note that this definition is contingent on the choice of representation for Ψ, which is why it is crucial that many of the morphisms which will arise in this thesis have fixed representations.

Since the representation for $[2^k]$ is fixed by $R_{2^k} = (R_2)^{[k]}$, then

$$\deg_{\mathbf{x}}[2^k] = (\deg_{\mathbf{x}}[2])^k = 4^k = (2^k)^2. \tag{6.3.1}$$

Further, given that

$$y \leqslant 2x \Leftrightarrow y^2 \leqslant 2xy \Leftrightarrow x^2 + 2y^2 \leqslant (x+y)^2 \quad (\forall x, y \geqslant 0), \tag{6.3.2}$$

then the following two lemmas can be shown.

Lemma 6.3.1. *Let* $m \in \mathbb{Z}$. *Then,* $\deg_{\mathbf{x}}[m] \leqslant 2m^2$.

Proof: First note that $\deg_{\mathbf{x}}[0] = 0$, which verifies the claim for $m = 0$. Also, if the claim holds for $m > 0$, then the representation for $[-m]$ shows that

$$\deg_{\mathbf{x}}[-m] = \deg_{\mathbf{x}}[m] \leqslant 2m^2 = 2(-m)^2,$$

and so assume without loss of generality that $m > 0$. The proof is by induction, for which the base case $m = 1$ holds, since $\deg_{\mathbf{x}}[1] = 1$. Suppose that $\deg_{\mathbf{x}}[s] \leqslant 2s^2$ for $s = 1, \ldots, m-1$. Then,

$$m = 2^k + m' \quad (\text{for some } k, m' \in \mathbb{N}; m' < 2^k \leqslant m).$$

If $m' = 0$, then $m = 2^k$, so $\deg_{\mathbf{x}}[m] = m^2 \leqslant 2m^2$. If $m' > 0$, then $[m] = \sigma_2([2^k], [m'])$, and so

$$\deg_{\mathbf{x}}[m] = 2\deg_{\mathbf{x}}[2^k] + 2\deg_{\mathbf{x}}[m'],$$

since $(R^{\zeta}_{\sigma_2})_{\zeta}$ is of bidegree $(2, 2)$. By induction hypothesis and by (6.3.1),

$$\deg_{\mathbf{x}}[m] \leqslant 2 \cdot 4^k + 2 \cdot 2m'^2 = 2((2^k)^2 + 2m'^2),$$

and so by (6.3.2), it follows that $\deg_{\mathbf{x}}[m] \leqslant 2m^2$. Induction yields the desired result. ∎

In order to prove results concerning the heights of the maps $[m]$, note the following. Since $R_{2^k} = R_2^{[k]}$, then Lemma 5.2.3 yields that

$$\mathrm{h}([2^k]) \leqslant [\mathrm{h}([2]) + \log 15]\frac{4^k-1}{3} + (2\log 2)k + (2\log 4)k^2 \leqslant c''(2^k)^2 \qquad (6.3.3)$$

for some $c'' \in \mathbb{R}^+$.

Lemma 6.3.2. *There exists $c' \in \mathbb{R}^+$ such that $\mathrm{h}([m]) \leqslant c'm^2$ for all $m \in \mathbb{Z}\backslash\{0\}$.*

Proof: Given $m \in \mathbb{N}^+$, it is clear from the representations that $\mathrm{h}([-m]) = \mathrm{h}([m])$, and so it suffices to verify the claim for $m > 0$. In this case, write $m = 2^k + m'$ with $m' < 2^k$, for some $k, m' \in \mathbb{N}$. Let $\Psi = \sigma_2$ and let $\Psi' = ([2^k], [m'])$, so that $[m] = \Psi \circ \Psi'$. Let

$$d' = \max\{4^k, \deg_{\mathbf{x}}[m']\} \leqslant \max\{4^k, 2m'^2\} \leqslant \max\{4^k, 2(2^k-1)^2\},$$

and so $d'+1 \leqslant 2 \cdot 4^k$. Since $\deg_{\mathbf{x},\mathbf{y}} \Psi = (2,2)$, then Proposition 5.2.5 and (6.3.3) yield that

$$\begin{aligned}
\mathrm{h}([m]) &\leqslant 2\log 6 + 3\log\tbinom{d'+2}{2} + \mathrm{h}(\Psi) + 2\mathrm{h}([2^k]) + 2\mathrm{h}([m']) \\
&\leqslant 2\log 6 + 6\log(d'+1) + \mathrm{h}(\Psi) + 2c''4^k + 2\mathrm{h}([m']) \\
&\leqslant 2\log 6 + 6(2k+1)\log 2 + \mathrm{h}(\Psi) + 2c''4^k + 2\mathrm{h}([m']).
\end{aligned}$$

Define $L : \mathbb{N} \to \mathbb{R}$ by

$$L(k) = 2\log 6 + 6(2k+1)\log 2 + \mathrm{h}(\Psi).$$

Choose $c''' \in \mathbb{R}^+$ such that $L(k) \leqslant c'''4^k$. Then, let $c' = c''' + 2c''$, and so

$$\mathrm{h}([m]) \leqslant c'4^k + 2\mathrm{h}([m']).$$

The rest of the proof is by induction. The base case $m = 1$ holds, since $\mathrm{h}([1]) \leqslant c'' \leqslant c'$. Suppose that $\mathrm{h}([s]) \leqslant c's^2$ for $s = 1, \ldots, m-1$. Since $m = 2^k + m'$ has $m' < 2^k \leqslant m$, then the induction hypothesis and (6.3.2) yield that

$$\mathrm{h}([m]) \leqslant c'4^k + 2c'm'^2 = c'((2^k)^2 + 2m'^2) \leqslant c'm^2.$$

The conclusion follows by induction. ∎

In order to get estimates for the map $[\tau]$ for $\tau \in \mathcal{O}$, define for each $S \in \mathbb{R}$ the set

$$\mathcal{O}_S = \{m + n\alpha \mid m, n \in \mathbb{Z}, |m|, |n| \leqslant S\} \subseteq \mathrm{End}(E).$$

Proposition 6.3.3. *There exists $C_1 \in \mathbb{R}^+$ such that if $\tau = m + n\alpha \in \mathcal{O}_S$, with $S \geqslant 1$, then*

$$\deg_{\mathbf{x}}[\tau] \leqslant C_1 S^2 \quad \textit{and} \quad \mathrm{h}([\tau]) \leqslant C_1 S^2.$$

Proof: From the representation for $[\tau]$ and σ_2, it follows that

$$\begin{aligned}\deg_{\mathbf{x}}[\tau] &\leqslant 2\deg_{\mathbf{x}}[m] + 2\deg_{\mathbf{x}}[\alpha]\deg_{\mathbf{x}}[n] \\ &\leqslant 4m^2 + 4\deg_{\mathbf{x}}[\alpha]n^2 \\ &\leqslant c_1 S^2,\end{aligned}$$

where $c_1 = 4(1 + \deg_{\mathbf{x}}[\alpha])$. Applying Proposition 5.2.5 with $\Psi = [\alpha]$ and $\Psi' = [n]$ yields

$$\begin{aligned}\mathrm{h}([\alpha] \circ [n]) &\leqslant \log\tbinom{\deg_{\mathbf{x}}[\alpha]+2}{2} + (\deg_{\mathbf{x}}[\alpha] - 1)\log\tbinom{\deg_{\mathbf{x}}[n]+2}{2} + \mathrm{h}([\alpha]) + \deg_{\mathbf{x}}[\alpha]\mathrm{h}([n]) \\ &\leqslant c_2 + c_3\log((c'S^2+2)(c'S^2+1)/2) + \deg_{\mathbf{x}}[\alpha]c'S^2 \\ &\leqslant c_4 S^2,\end{aligned}$$

for some $c_4 \in \mathbb{R}^+$. Using the same result for $\Psi = \sigma_2$ and $\Psi' = ([m], [\alpha] \circ [n])$, it follows that

$$\mathrm{h}([\tau]) \leqslant 2\log\tbinom{4}{2} + 3\log\tbinom{c_1 S^2+2}{2} + \mathrm{h}([\sigma_2]) + 2\mathrm{h}([m]) + 2\mathrm{h}([\alpha] \circ [n])$$

$$
\begin{aligned}
&\leqslant c_5 + 3\log((c_1S^2+2)(c_1S^2+1)/2) + 2c'S^2 + 2c_4S^2 \\
&\leqslant c_6S^2,
\end{aligned}
$$

for some $c_6 \in \mathbb{R}^+$. Letting $C_1 = \max\{c_1, c_6\}$ yields the desired result. ∎

6.4 Multiplication by $(\tau_1, \ldots, \tau_n) \in \mathcal{O}^n$

In order to state the main result of this section, define the n-sum maps, denoted $\sigma_n : E^n \to E$, by

$$\sigma_n = \sigma_2(\mathrm{id}_E, \sigma_{n-1}) \quad (\forall n > 2).$$

This relation induces, iteratively, a fixed representation for σ_n by a family of triplets of homogeneous polynomials in $K(\mathbf{x}_1, \ldots, \mathbf{x}_n)$, denoted

$$R^{\zeta}_{\sigma_n} = (R^{\zeta}_{\sigma_n,0}, R^{\zeta}_{\sigma_n,1}, R^{\zeta}_{\sigma_n,2})$$

for a finite set of indices ζ. Consider for $n \geqslant 2$ the multiplication-by-$\underline{\tau}$ map, denoted $[\underline{\tau}]$, for vectors $\underline{\tau} = (\tau_1, \ldots, \tau_n) \in \mathcal{O}^n$, i.e.

$$[\underline{\tau}](\mathbf{z}_1, \ldots, \mathbf{z}_n) = \sigma_n \circ ([\tau_1] \times \cdots \times [\tau_n])(\mathbf{z}_1, \ldots, \mathbf{z}_n) = \sigma_n([\tau_1](\mathbf{z}_1), \ldots, [\tau_n](\mathbf{z}_n)).$$

This fixes a representation of $[\underline{\tau}]$ by a family of triplets of multi-homogeneous polynomials in $K(\mathbf{x}_1, \ldots, \mathbf{x}_n)$, denoted

$$R^{\zeta}_{\underline{\tau}} = (R^{\zeta}_{\underline{\tau},0}, R^{\zeta}_{\underline{\tau},0}, R^{\zeta}_{\underline{\tau},0}),$$

for a finite set of indices ζ.

Proposition 6.4.1. *Let $n \in \mathbb{N}^+$. There exists $C_2 \in \mathbb{R}^+$ depending only on n such that if $\underline{\tau} \in (\mathcal{O}_S)^n$, with $S \geqslant 1$, then*

$$\deg_{\mathbf{x}_i}[\underline{\tau}] \leqslant C_2S^2 \quad \textit{and} \quad \mathrm{h}([\underline{\tau}]) \leqslant C_2S^2 \quad (1 \leqslant i \leqslant n).$$

Proof: Let $(d'_1, \ldots, d'_n)$ be an upper bound for the multidegrees of $(R^{\zeta}_{\sigma_n})_{\zeta}$. Then,

$$\deg_{\mathbf{x}_i}[\underline{\tau}] \leqslant d'_i \deg_{\mathbf{x}}[\tau_i] \leqslant d'_i C_1 S^2.$$

By Proposition 5.2.5, with $\Psi = \sigma_n$ and $\Psi' = [\tau_1] \times \cdots \times [\tau_n]$, it follows that

$$\begin{aligned} \mathrm{h}([\underline{\tau}]) &\leqslant \sum_{i=1}^{n} \log\tbinom{d'_i+2}{2} + (d'_1 + \cdots + d'_n) \log\tbinom{C_1S^2+3n-1}{3n-1} + \mathrm{h}(\sigma_n) + \sum_{i=1}^{n} d'_i \mathrm{h}([\tau_i]) \\ &\leqslant c_7 + c_8(3n-1)\log(C_1S^2+1) + n(\max_i d'_i)C_1S^2 \\ &\leqslant c_9 S^2, \end{aligned}$$

for some $c_9 \in \mathbb{R}^+$ which depends only on n. Thus, let $C_2 = \max\{(\max_i d'_i C_1), c_9\}$. ∎

For the sake of completion, define $[(\tau_{ij})] : E^n \to E^n$ by

$$[(\tau_{ij})](\mathbf{z}_1, \ldots, \mathbf{z}_n) = ([\underline{\tau}_1](\mathbf{z}_1, \ldots, \mathbf{z}_n), \ldots, [\underline{\tau}_n](\mathbf{z}_1, \ldots, \mathbf{z}_n)) \quad (\forall (\tau_{ij}) \in \mathrm{Mat}_{n\times n}(\mathcal{O})),$$

where each $\underline{\tau}_i = (\tau_{i,1}, \ldots, \tau_{i,d})$. Then fix

$$R^{\zeta}_{(\tau_{ij})} = (R^{\zeta}_{[\underline{\tau}_1]}, \ldots, R^{\zeta}_{[\underline{\tau}_n]}),$$

for a finite set of indices ζ, as the representation of $[(\tau_{ij})]$.

Proposition 6.4.2. *Let $n \in \mathbb{N}^+$. There exists $c \in \mathbb{R}^+$ such that if $(\tau_{ij}) \in \mathrm{Mat}_{n\times n}(\mathcal{O}_S)$, with $S \geqslant 1$, then*

$$\deg_{\mathbf{x}_i}[(\tau_{ij})] \leqslant cS^2 \quad \textit{and} \quad \mathrm{h}([(\tau_{ij})]) \leqslant cS^2.$$

Proof: It is easy to see that

$$\deg_{\mathbf{x}_i}[(\tau_{ij})] = \max_j \deg_{\mathbf{x}_i}[\underline{\tau}_j] \leqslant C_2 S^2;$$

$$\mathrm{h}[(\tau_{ij})] \leqslant \sum_{j=1}^{n} \mathrm{h}([\underline{\tau}_j]) \leqslant nC_2S^2.$$

Thus, by letting $c = nC_2$, the result follows. ∎

Chapter 7

Estimates on the derivatives of the auxiliary function

The main goal of this chapter is to provide estimates on the derivatives of the auxiliary function. This is in line with Philippon's original proof, but the work in this chapter remains independent of his methods. Throughout this chapter and the remainder of the thesis, fix a lattice $\Lambda \subset \mathbb{C}$, and suppose that the induced elliptic curve E has complex multiplication, and that E is defined over $\overline{\mathbb{Q}}$. Thus, there exists a quadratic integer α such that $\mathcal{O} = \mathbb{Z}[\alpha] = \mathbb{Z} \bigoplus \mathbb{Z}\alpha$. Remark then that there exists $a, b \in \mathbb{Z}$ such that $\alpha^2 = a\alpha + b$. Further, fix β, an integral element over $\mathcal{O}$, fix $d = [\mathcal{O}[\beta] : \mathcal{O}]$, and fix $K = \mathbb{Q}(\alpha, \beta, g_2, g_3)$.

7.1 Preliminaries

Remark that $\{1, \beta, \ldots, \beta^{d-1}\}$ is an $\mathcal{O}$-basis for $\mathcal{O}[\beta]$, and so, for each $\gamma \in \mathcal{O}[\beta]$, there exists a unique matrix $B_\gamma \in \mathrm{Mat}_{d\times d}(\mathcal{O})$ such that

$$\gamma(1, \beta, \ldots, \beta^{d-1})^T = B_\gamma(1, \beta, \ldots, \beta^{d-1})^T.$$

Define

$$\Gamma = \{\tau_1 + \tau_2\beta + \cdots + \tau_d\beta^{d-1} \mid \tau_1, \ldots, \tau_d \in \mathcal{O}\} = \mathcal{O}[\beta],$$

and

$$\Gamma_S = \{\tau_1 + \tau_2\beta + \cdots + \tau_d\beta^{d-1} \mid \tau_1, \ldots, \tau_d \in \mathcal{O}_S\} \quad (\forall S \in \mathbb{N}).$$

Given an $S \geqslant 1$, and $\gamma \in \Gamma_S$, it will be useful to have an estimate on the height of γ as well as an estimate on the entries of B_γ, such as those provided in the upcoming propositions.

Proposition 7.1.1. *Let* $(\underline{\gamma}) = (\gamma_1, \ldots, \gamma_q) \in \Gamma_S^q$. *Then*

$$h(\underline{\gamma}) \leqslant \log(2dS) + \mathrm{h}(\alpha) + (d-1)\mathrm{h}(\beta).$$

Proof: Write

$$\gamma_i = \sum_{k=1}^{d}(m_{i,k} + n_{i,k}\alpha)\beta^{k-1} \quad (\text{for some } m_{i,k}, n_{i,k} \in \mathbb{Z})$$

with each $|m_{i,k}|, |n_{i,k}| \leqslant S$. Then, for each $v \in \mathfrak{M}_K$,

$$\begin{aligned}\max_{1\leqslant i\leqslant q} |\gamma_i|_v &= \max_{1\leqslant i\leqslant q} \left|\sum_{k=1}^{d}(m_{i,k} + n_{i,k}\alpha)\beta^{k-1}\right|_v \\ &\leqslant \max_{1\leqslant i\leqslant q} \{2d\}_v \max_{1\leqslant k\leqslant d}\{|m_{i,k}|_v, |n_{i,k}|_v |\alpha|_v\} \left|\beta^{k-1}\right|_v \\ &\leqslant \{2dS\}_v \max\{1, |\alpha|_v\} \max\{1, |\beta|_v\}^{d-1}.\end{aligned}$$

Remark that $\mathrm{h}(1, \delta) = \mathrm{h}(\delta)$ for each $\delta \in K$. Thus, by viewing elements of K as constant polynomials, Lemma 5.2.2 yields the result. ∎

To prove the second estimate, the following lemma will be used.

Lemma 7.1.2. *There exists* $c \in \mathbb{N}^+$ *depending only on* $\mathcal{O}(\Lambda)$ *such that for each* $S, S' \in \mathbb{N}$,

1. $\mathcal{O}_S + \mathcal{O}_{S'} \subseteq \mathcal{O}_{S+S'}$
2. $\mathcal{O}_S\mathcal{O}_{S'} \subseteq \mathcal{O}_{cSS'}$

Proof: Let $m_1 + m_2\alpha \in \mathcal{O}_S$ and let $n_1 + n_2\alpha \in \mathcal{O}_{S'}$. Then $|m_i + n_i| \leqslant S + S'$ for $i \in \{1, 2\}$. Thus,

$$(m_1 + m_2\alpha) + (n_1 + n_2\alpha) = (m_1 + n_1) + (m_2 + n_2)\alpha \in \mathcal{O}_{S+S'},$$

which proves (1). To prove the second claim, let $c = \max\{2 + |a|, 1 + |b|\}$. Then, it follows that

$$|m_1n_1 + m_2n_2b| \leqslant SS' + |b|SS' = (1 + |b|)SS' \leqslant cSS';$$

$$|m_1n_2 + m_2n_1 + m_2n_2a| \leqslant 2SS' + |a|SS' = (2 + |a|)SS' \leqslant cSS'.$$

Therefore,

$$(m_1 + m_2\alpha)(n_1 + n_2\alpha) = (m_1n_1 + m_2n_2b) + (m_1n_2 + m_2n_1 + m_2n_2a)\alpha \in \mathcal{O}_{cSS'},$$

which completes the proof of the lemma. ∎

Proposition 7.1.3. *There exists $c' \in \mathbb{N}^+$ satisfying*

$$\gamma \in \Gamma_S \Rightarrow B_\gamma \in \mathrm{Mat}_{d\times d}(\mathcal{O}_{c'S}) \quad (\forall S \in \mathbb{N}).$$

Proof: For each $i \in \mathbb{N}$, there exists $c_i \in \mathbb{N}^+$ such that

$$\beta^{d+i} = \sum_{j=1}^{d} a_{i,j}\beta^{d-j} \quad \text{(for some } a_{i,j} \in \mathcal{O}_{c_i}\text{)}.$$

Let $c'' = \max\{c_0, \ldots, c_{d-2}\} \in \mathbb{N}^+$, let c be as in Lemma 7.1.2, and let $c' = dcc''$. To show that c' has the desired property, let

$$\gamma = \tau_1 + \tau_2\beta + \cdots + \tau_d\beta^{d-1} \quad \text{(for some } \tau_i \in \mathcal{O}_S\text{)},$$

and write $B_\gamma = (\tau_{ij})_{1\leqslant i,j\leqslant d}$. For each $i \in \{0, \ldots, d-2\}$, write

$$\tau_{i1} + \cdots + \tau_{id}\beta^{d-1} = (\tau_1 + \cdots + \tau_d\beta^{d-1})\beta^{i-1}$$

$$
\begin{aligned}
&= \tau_1\beta^{i-1} + \cdots + \tau_{d+2-i}\beta^{d} + \cdots + \tau_d\beta^{d+i-2} \\
&= \tau_1\beta^{i-1} + \cdots + \tau_{d+2-i}\left(\sum_{j=1}^{d} a_{0,j}\beta^{d-j}\right) + \cdots + \tau_d\left(\sum_{j=1}^{d} a_{i-2,j}\beta^{d-j}\right).
\end{aligned}
$$

Thus, it follows by Lemma 7.1.2 that

$$\tau_{ij} \in \mathcal{O}_S\mathcal{O}_{c''} + \cdots + \mathcal{O}_S\mathcal{O}_{c''} \subseteq \mathcal{O}_{c'S} \quad (1 \leqslant i, j \leqslant d)$$

where the sum consists of d copies of $\mathcal{O}_S\mathcal{O}_{c''}$. Therefore, B_γ is in $\mathrm{Mat}_{d\times d}(\mathcal{O}_{c'S})$, as desired. ∎

7.1.1 Length inequalities for polynomials

This subsection introduces the notion of the length of a polynomial, and provides a few related estimates.

Definition. Let $F \in \mathbb{C}[x_1, \ldots, x_n]$. Thus,

$$F(x_1, \ldots, x_n) = \sum_{\mathbf{i}\in\mathbb{N}^n} c_{\mathbf{i}}x^{\mathbf{i}} \quad \text{(for some } c_{\mathbf{i}} \in \mathbb{C}\text{)},$$

for a unique choice of $(c_{\mathbf{i}})_{\mathbf{i}\in\mathbb{N}^n}$. By definition, only finitely many of the coefficients $c_{\mathbf{i}}$ are not equal to zero. Thus, it makes sense to define the *length* of the polynomial F, denoted $\mathrm{L}(F)$, by

$$\mathrm{L}(F) = \sum_{\mathbf{i}\in I} |c_{\mathbf{i}}|.$$

Proposition 7.1.4. *Let $F, G \in \mathbb{C}[x_1, \ldots, x_n]$. Then, the following holds.*

$$\mathrm{L}(F+G) \leqslant \mathrm{L}(F) + \mathrm{L}(G) \tag{7.1.1}$$

$$\mathrm{L}(\partial F/\partial x_j) \leqslant \deg_{x_j}(F)\mathrm{L}(F) \tag{7.1.2}$$

$$\mathrm{L}(FG) \leqslant \mathrm{L}(F)\mathrm{L}(G) \tag{7.1.3}$$

Proof: Write

$$F(x_1, \ldots, x_n) = \sum_{\mathbf{i} \in \mathbb{N}^n} c_{\mathbf{i}} x^{\mathbf{i}} \quad (\text{for some } c_{\mathbf{i}} \in \mathbb{C});$$

$$G(x_1, \ldots, x_n) = \sum_{\mathbf{i} \in \mathbb{N}^n} d_{\mathbf{i}} x^{\mathbf{i}} \quad (\text{for some } d_{\mathbf{i}} \in \mathbb{C}).$$

Then, it follows that

$$\mathrm{L}(F + G) = \sum_{\mathbf{i} \in \mathbb{N}^n} |c_{\mathbf{i}} + d_{\mathbf{i}}| \leqslant \sum_{\mathbf{i} \in \mathbb{N}^n} |c_{\mathbf{i}}| + \sum_{\mathbf{i} \in \mathbb{N}^n} |d_{\mathbf{i}}| = \mathrm{L}(F) + \mathrm{L}(G);$$

$$\mathrm{L}(\partial F/\partial x_j) = \sum_{\mathbf{i} \in \mathbb{N}^n} |i_j c_{\mathbf{i}}| \leqslant \deg_{x_j}(F) \sum_{\mathbf{i} \in \mathbb{N}^n} |c_{\mathbf{i}}| = \deg_{x_j}(F) \mathrm{L}(F);$$

$$\mathrm{L}(FG) = \sum_{\mathbf{k} \in \mathbb{N}^n} \left| \sum_{\mathbf{i}+\mathbf{j}=\mathbf{k}} c_{\mathbf{i}} d_{\mathbf{j}} \right| \leqslant \sum_{\mathbf{k} \in \mathbb{N}^n} \sum_{\mathbf{i}+\mathbf{j}=\mathbf{k}} |c_{\mathbf{i}}||d_{\mathbf{j}}| = \sum_{\mathbf{i} \in \mathbb{N}^n} \sum_{\mathbf{j} \in \mathbb{N}^n} |c_{\mathbf{i}}||d_{\mathbf{j}}| = \mathrm{L}(F)\mathrm{L}(G),$$

thus completing the proof. ∎

Proposition 7.1.5. *Let k be a number field. Let $(\alpha_1, \ldots, \alpha_m) \in k^m$, let $\mathbf{x}$ be a multivariable over $\mathbb{C}^m$, and let $F \in \mathbb{Z}[\mathbf{x}]$ with $\deg_{\mathbf{x}} F = n$. Then*

$$|F(\alpha_1 \ldots, \alpha_m)|_v \leqslant \{\mathrm{L}(F)\}_v \max\{1, |\alpha_1|_v, \ldots, |\alpha_m|_v\}^n \quad (\forall v \in \mathfrak{M}_k),$$

recalling that

$$\{m\}_v = m \text{ if } v|\infty \quad \text{and} \quad \{m\}_v = 1 \text{ if } v \nmid \infty \quad (\forall m \in \mathbb{Z}\backslash\{0\}).$$

Proof: Write

$$F(\mathbf{x}) = \sum_{\mathbf{i} \in \mathbb{N}^m} c_{\mathbf{i}} x^{\mathbf{i}} \quad (\text{for some } c_{\mathbf{i}} \in \mathbb{Z}),$$

from which it follows that

$$\begin{aligned} |F(\alpha_1, \ldots, \alpha_m)|_v &= \left| \sum_{\mathbf{i} \in \mathbb{N}^m} c_{\mathbf{i}} \alpha_1^{\mathbf{i}_1} \cdots \alpha_m^{\mathbf{i}_m} \right|_v \\ &\leqslant \{\mathrm{L}(F)\}_v \max_{|\mathbf{i}| \leqslant n} \{ |\alpha_1^{\mathbf{i}_1} \cdots \alpha_m^{\mathbf{i}_m}|_v \} \end{aligned}$$

$$\leqslant \{\mathrm{L}(F)\}_v \max\{1, |\alpha_1|_v, \ldots, |\alpha_m|_v\}^n,$$

as required. ∎

Applying Lemma 5.2.2 to the above proposition immediately yields the following.

Corollary 7.1.6. *Following the same notation as in Proposition* 7.1.5*, then*

$$\mathrm{h}(F(\alpha_1, \ldots, \alpha_m)) \leqslant \log \mathrm{L}(F) + (\deg_{\mathbf{x}} F)\mathrm{h}(\alpha_1, \ldots, \alpha_m).$$

7.1.2 Holomorphic representation of Φ around 0

This subsection will provide a function that represents points on the elliptic curve around its origin, which will be useful in finding the derivatives of the auxiliary function. The core goal of this subsection is to establish estimates on this function.

Notice that there exists $\varepsilon > 0$ such that the functions $\wp/\wp'$ and $1/\wp'$ are holomorphic on $B(0;\varepsilon)$. Thus, the function

$$\Phi_0 : z \in B(0,\varepsilon) \mapsto \left(\frac{1}{\wp'(z)}, \frac{\wp(z)}{\wp'(z)}, 1\right)$$

is a triplet of holomorphic functions. Notice that its equivalence class in projective space is such that

$$[\Phi_0(z)] = \exp_E(z) = [\Phi(z)]$$

for all $z \in B(0;\varepsilon) \subseteq \mathbb{C}$. The derivatives of the auxiliary function will involve the derivatives of the coordinates of the function Φ_0. Define functions $f, h : B(0;\varepsilon) \to E$ via

$$f(z) = \frac{1}{\wp'(z)} = -\frac{z^3}{2} + \cdots;$$
$$h(z) = \frac{\wp(z)}{\wp'(z)} = -\frac{z}{2} + \cdots.$$

Recall that $\wp'^2 = 4\wp^3 - g_2\wp - g_3$, and that $\wp'' = 6\wp^2 - g_2/2$. Thus, it follows that

$$f' = -\frac{\wp''}{\wp'^2}$$

$$= -6\left(\frac{\wp}{\wp'}\right)^2 + \frac{g_2}{2\wp'^2}$$
$$= -6h^2 + g_2 f^2/2,$$

and that

$$\begin{aligned} h' &= \frac{\wp'^2 - \wp''\wp}{\wp'^2} \\ &= 1 - 6\frac{\wp^3}{\wp'^2} + \frac{g_2\wp}{2\wp'^2} \\ &= 1 - \frac{3}{2}\left(\frac{\wp'^2 + g_2\wp + g_3}{\wp'^2}\right) + \frac{g_2\wp}{2\wp'^2} \\ &= -\frac{1}{2} - g_2\frac{\wp}{\wp'^2} - \frac{3g_3}{2\wp'^2} \\ &= -1/2 - g_2 fh - 3g_3 f^2/2. \end{aligned}$$

Thus, $f^{(k)}$ and $h^{(k)}$ are both polynomials in (g_2, g_3, f, h) for each $k \in \mathbb{N}$. In order to see this, let $\mathbf{x} = (x_1, x_2)$ and $\mathbf{y} = (y_1, y_2)$ be multivariables over $\mathbb{C}^2$, and define recursively

$$F_{n+1}(\mathbf{x},\mathbf{y}) = \frac{\partial F_n}{\partial y_1}(\mathbf{x},\mathbf{y})\cdot(-12y_2^2 + x_1y_1^2) + \frac{\partial F_n}{\partial y_2}(\mathbf{x},\mathbf{y})\cdot(-1 - 2x_1y_1y_2 - 3x_2y_1^2); \quad (7.1.4)$$

$$H_{n+1}(\mathbf{x},\mathbf{y}) = \frac{\partial H_n}{\partial y_1}(\mathbf{x},\mathbf{y})\cdot(-12y_2^2 + x_1y_1^2) + \frac{\partial H_n}{\partial y_2}(\mathbf{x},\mathbf{y})\cdot(-1 - 2x_1y_1y_2 - 3x_2y_1^2); \quad (7.1.5)$$

$$F_0(\mathbf{x},\mathbf{y}) = y_1 \quad \text{and} \quad H_0(\mathbf{x},\mathbf{y}) = y_2. \quad (7.1.6)$$

Proposition 7.1.7. *Let $k \in \mathbb{N}$. Then, it follows for each $z \in B(0;\varepsilon)$ that*

$$2^k f^{(k)}(z) = F_k(g_2, g_3, f(z), h(z)) \quad \text{and} \quad 2^k h^{(k)}(z) = H_k(g_2, g_3, f(z), h(z)).$$

Proof: Equations (7.1.4) and (7.1.5) yield

$$F_{n+1}(g_2, g_3, f, h) = 2(F_n(g_2, g_3, f, h))' = 2^{n+1}(F_0(g_2, g_3, f, h))^{(n+1)};$$

$$H_{n+1}(g_2, g_3, f, h) = 2(H_n(g_2, g_3, f, h))' = 2^{n+1}(H_0(g_2, g_3, f, h))^{(n+1)}.$$

Equation (7.1.6) yields that $F_0(g_2, g_3, f, h) = f$ and that $H_0(g_2, g_3, f, h) = h$. ∎

Proposition 7.1.8. *Let $k \in \mathbb{N}$. Then*

$$\begin{aligned} F_k, H_k &\in \mathbb{Z}[\mathbf{x}, \mathbf{y}]; \\ \deg_{\mathbf{x}} F_k, \deg_{\mathbf{x}} H_k &\leqslant k; \\ \deg_{\mathbf{y}} F_k, \deg_{\mathbf{y}} H_k &\leqslant k+1; \\ \mathrm{L}(F_k), \mathrm{L}(H_k) &\leqslant k! 19^k. \end{aligned}$$

Proof: The proof is by induction on $k \geqslant 0$, whose base cases $F_0 = y_1$ and $H_0 = y_2$ clearly hold. Now, suppose that the claim holds for $k = 0, \ldots, n$. Since $\mathbb{Z}[\mathbf{x}, \mathbf{y}]$ is closed under the operators $\partial/\partial y_1$ and $\partial/\partial y_2$, it follows by (7.1.4) and (7.1.5) that $F_{n+1}, H_{n+1} \in \mathbb{Z}[\mathbf{x}, \mathbf{y}]$. Thus, by induction, it follows for each $k \in \mathbb{N}$ that $F_k, H_k \in \mathbb{Z}[\mathbf{x}, \mathbf{y}]$. It also follows by induction hypothesis that

$$\begin{aligned} \deg_{\mathbf{x}} F_{n+1} &\leqslant \max_{1 \leqslant i \leqslant 2} \deg_{\mathbf{x}} \frac{\partial F_n}{\partial y_i} + \max\{\deg_{\mathbf{x}}(-12y_2^2 + x_1 y_1^2), \deg_{\mathbf{x}}(-1 - 2x_1 y_1 y_2 - 3x_2 y_1^2)\} \\ &\leqslant n+1, \end{aligned}$$

and that

$$\begin{aligned} \deg_{\mathbf{y}} F_{n+1} &\leqslant \max_{1 \leqslant i \leqslant 2} \deg_{\mathbf{y}} \frac{\partial F_n}{\partial y_i} + \max\{\deg_{\mathbf{y}}(-12y_2^2 + x_1 y_1^2), \deg_{\mathbf{y}}(-1 - 2x_1 y_1 y_2 - 3x_2 y_1^2)\} \\ &\leqslant ((n+1) - 1) + 2 = n+2. \end{aligned}$$

Letting F_{n+1}, F_n in the above computations go to H_{n+1}, H_n, respectively, it follows that

$$\begin{aligned} \deg_{\mathbf{x}} H_{n+1} &\leqslant n+1; \\ \deg_{\mathbf{y}} H_{n+1} &\leqslant n+2. \end{aligned}$$

Thus, for each $k \in \mathbb{N}$, it follows that

$$\deg_{\mathbf{x}} F_k, \deg_{\mathbf{x}} H_k \leqslant k;$$

$$\deg_{\mathbf{y}} F_k, \deg_{\mathbf{y}} H_k \leqslant k+1.$$

Finally, Proposition 7.1.4 yields that

$$L(F_{n+1}) \leqslant 19(n+1)L(F_n) \leqslant 19^{n+1}(n+1)!;$$

$$L(H_{n+1}) \leqslant 19(n+1)L(H_n) \leqslant 19^{n+1}(n+1)!,$$

from which induction yields the desired result. ∎

Corollary 7.1.9. *Let $N \in \mathbb{N}$. Then*

$$\mathrm{h}(f^{(0)}(0), h^{(0)}(0), \ldots, f^{(N)}(0), h^{(N)}(0)) \leqslant N \log N + N\big(\mathrm{h}(g_2, g_3) + \log 38\big).$$

Proof: Write $\tilde{F}_n(\mathbf{x}) = F_n(\mathbf{x}, \mathbf{0})$, and write $\tilde{H}_n(\mathbf{x}) = H_n(\mathbf{x}, \mathbf{0})$. By noting that $f(0) = h(0) = 0$, it follows that

$$f^{(n)}(0) = 2^{-n}\tilde{F}_n(g_2, g_3) \quad (0 \leqslant n \leqslant N);$$

$$h^{(n)}(0) = 2^{-n}\tilde{H}_n(g_2, g_3) \quad (0 \leqslant n \leqslant N).$$

Thus, for each $v \in \mathfrak{M}_K$,

$$\begin{aligned}\max_{0\leqslant n\leqslant N}\{\left|f^{(n)}(0)\right|_v, \left|h^{(n)}(0)\right|_v\} &= \max_{0\leqslant n\leqslant N}\{|2^{-n}\tilde{F}_n(g_2, g_3)|_v, |2^{-n}\tilde{H}_n(g_2, g_3)|_v\} \\ &\leqslant \max\{1, \left|2^{-1}\right|_v\}^N \max_{0\leqslant n\leqslant N}\{|\tilde{F}_n(g_2, g_3)|_v, |\tilde{H}_n(g_2, g_3)|_v\}\end{aligned}$$

By Proposition 7.1.5 and Proposition 7.1.8, it follows that

$$\max_{0\leqslant n\leqslant N}\{\left|f^{(n)}(0)\right|_v, \left|h^{(n)}(0)\right|_v\} \leqslant \max\{1, \left|2^{-1}\right|_v\}^N \left\{N^N 19^N\right\}_v \max\{1, \left|g_2\right|_v, \left|g_3\right|_v\}^N.$$

Therefore, Lemma 5.2.2 yields that

$$\mathrm{h}(f^{(0)}(0), h^{(0)}(0), \ldots, f^{(N)}(0), h^{(N)}(0)) \leqslant N \log N + N\big(\mathrm{h}(g_2, g_3) + \mathrm{h}(2^{-1}) + \log 19\big),$$

as required. ∎

7.2 Estimates on the derivatives of the auxiliary function

The aim of this section is to show that the derivatives of the auxiliary function are of bounded degree and height, and are small at the point $(u_1, \ldots, u_d)$, where each u_j is defined by

$$u_j = \begin{cases} (1, \wp(\beta^{j-1}), \wp'(\beta^{j-1})) & \text{if } \beta^{j-1} \notin \Lambda; \\ (0, 0, 1) & \text{if } \beta^{j-1} \in \Lambda. \end{cases}$$

This will in turn allow the use of Philippon's zero lemma and independence criterion, from which the main theorem of this thesis will follow.

Let $\gamma \in \Gamma$, and note that $B_\gamma \in \mathrm{Mat}_{d\times d}(\mathcal{O})$ is such that

$$[B_\gamma]([\Phi(t)], [\Phi(t\beta)], \ldots, [\Phi(t\beta^{d-1})]) = ([\Phi(\gamma t)], [\Phi(\gamma t\beta)], \ldots, [\Phi(\gamma t\beta^{d-1})]).$$

Define

$$\mathbf{b}_{\gamma,j} = (b_{\gamma,j,1}, \ldots, b_{\gamma,j,d}) = \text{“}j^{th} \text{ row vector of } B_\gamma\text{”} \quad (1 \leqslant j \leqslant d).$$

Following an idea by Baker-Coates-Anderson [12], the following map helps to simplify the task of estimating the derivatives of the auxiliary function at specific points. Specifically, define the map $q_{\gamma,j} : E^{d+1} \to E$ by

$$q_{\gamma,j} = \sigma_2 \circ ([\mathbf{b}_{\gamma,j}] \times \mathrm{id}_E) \quad (1 \leqslant j \leqslant d).$$

Then, use the representations for σ_2, $[\mathbf{b}_{\gamma,j}]$ and id_E to induce a family of triplets of homogeneous polynomials in $K(\mathbf{x}_1, \ldots, \mathbf{x}_d, \mathbf{y})$, denoted

$$Q^\zeta_{\gamma,j} = (Q^\zeta_{\gamma,j,0}, Q^\zeta_{\gamma,j,1}, Q^\zeta_{\gamma,j,2}),$$

where $\zeta \in Z_{\gamma,j}$, and $Z_{\gamma,j}$ is a finite indexing set. Further denote

$$Z_{\underline{\gamma}} = \{(\zeta_{ij})_{ij} \mid \zeta_{ij} \in Z_{\gamma_i,j} \text{ for } 1 \leqslant i \leqslant q; 1 \leqslant j \leqslant d\} \quad (\forall \underline{\gamma} = (\gamma_1, \ldots, \gamma_q) \in \Gamma^q).$$

Proposition 7.2.1. *There exists $C \in \mathbb{R}^+$ such that if $S \geqslant 1$ and $\gamma \in \Gamma_S$, then*

$$\deg_{\mathbf{x}_k} q_{\gamma,j} \leqslant CS^2 \quad \textit{and} \quad \mathrm{h}(q_{\gamma,j}) \leqslant CS^2 \quad (\forall k \in \{1, \dots, d\}).$$

Furthermore, the representation for $q_{\gamma,j}$ satisfies $\deg_{\mathbf{y}} q_{\gamma,j} = 2$.

Proof: Since $(R^{\zeta}_{\sigma_2})_\zeta$ is of bidegree $(2,2)$, then

$$\deg_{\mathbf{x}_k} q_{\gamma,j} = 2\deg_{\mathbf{x}_k}[\mathbf{b}_{\gamma,j}] + 2\deg_{\mathbf{x}_k} \mathrm{id}_E = 2\deg_{\mathbf{x}_k}[\mathbf{b}_{\gamma,j}];$$

$$\deg_{\mathbf{y}} q_{\gamma,j} = 2\deg_{\mathbf{y}}[\mathbf{b}_{\gamma,j}] + 2\deg_{\mathbf{y}} \mathrm{id}_E = 2\deg_{\mathbf{y}} \mathrm{id}_E = 2.$$

By Proposition 7.1.3, there exists $c_1 \in \mathbb{R}^+$ such that $\mathbf{b}_{\gamma,j} \in (\mathcal{O}_{c_1 S})^d$. Thus, Proposition 6.4.1 yields

$$\deg_{\mathbf{x}_k} q_{\gamma,j} \leqslant 2C_2(c_1 S)^2.$$

By Proposition 5.2.5, with $\Psi = \sigma_2$ and $\Psi' = [\mathbf{b}_{\gamma,j}] \times \mathrm{id}_E$, it follows that

$$\begin{aligned}\mathrm{h}(q_{\gamma,j}) &\leqslant 2\log\left(\tfrac{4}{2}\right) + 3\log\left(\tfrac{2C_2c_1^2S^2+3d+2}{3d+2}\right) + \mathrm{h}(\sigma_2) + 2\mathrm{h}([\mathbf{b}_{\gamma,j}]) + 2\mathrm{h}(\mathrm{id}_E)\\ &\leqslant c_2 + 3(3d+2)\log(2C_2c_1^2S^2+1) + 2C_2(c_1S)^2\\ &\leqslant c_3S^2,\end{aligned}$$

for some $c_3 \in \mathbb{R}^+$. Thus, letting $C = \max\{2C_2c_1^2, c_3\}$ yields the desired result. ▮

Write $\mathbf{u} = (u_1, \dots, u_d)$, and recall that

$$u_j = \begin{cases} (1, \wp(\beta^{j-1}), \wp'(\beta^{j-1})) & \text{if } \beta^{j-1} \notin \Lambda; \\ (0,0,1) & \text{if } \beta^{j-1} \in \Lambda, \end{cases}$$

and so $u_j \propto \Phi(\beta^{j-1})$ for each $j \in \{1, \dots, d\}$. Adopt the following notation. Let $\mathbf{f}, \mathbf{g} : \mathbb{C}^n \to \mathbb{C}^m$ be functions in a variable $\mathbf{x}$. If there exists a function $\rho : \mathbb{C}^n \to \mathbb{C}$ such that

$$\mathbf{f}(\mathbf{x}) = \rho(\mathbf{x})\mathbf{g}(\mathbf{x}),$$

then write

$$\mathbf{f}(\mathbf{x}) \propto_{\mathbf{x}} \mathbf{g}(\mathbf{x}).$$

Remark that while this binary operator is not symmetric, it is in fact transitive, which will be used in the proof of the following lemma.

Lemma 7.2.2. *Let $\gamma \in \Gamma$, and let $w \in \mathbb{C}$ be a variable. Let $1 \leqslant j \leqslant d$, and let $\zeta \in Z_{\gamma,j}$. Then*

$$Q^{\zeta}_{\gamma,j}(\mathbf{u}, \Phi_0(w\beta^{j-1})) \propto_w \Phi((\gamma + w)\beta^{j-1})$$

for $|w| < \varepsilon/c_\beta$, where $c_\beta = \max\{1, |\beta|^{d-1}\}$.

Proof: Remark that

$$u_j \propto \Phi(\beta^{j-1}) \quad (1 \leqslant j \leqslant d);$$

$$\Phi_0(w\beta^{j-1}) \propto_w \Phi(w\beta^{j-1}) \quad (\forall w \in B(0; \varepsilon/c_\beta)).$$

Since $Q_{\gamma,j}$ is homogeneous in each $\mathbf{x}_k$ and in $\mathbf{y}$, then

$$Q^{\zeta}_{\gamma,j}(\mathbf{u}, \Phi_0(w\beta^{j-1})) \propto_w Q^{\zeta}_{\gamma,j}(\Phi(1), \ldots, \Phi(\beta^{d-1}), \Phi(w\beta^{j-1}))$$

for $|w| < \varepsilon/c_\beta$. Notice that $(0, 0, 0)$ trivially satisfies

$$(0, 0, 0) \propto_w \Phi((\gamma + w)\beta^{j-1}).$$

Thus, assume without loss of generality that $|w| < \varepsilon/c_\beta$ is such that

$$Q^{\zeta}_{\gamma,j}(\mathbf{u}, \Phi_0(w\beta^{j-1})) \neq (0, 0, 0).$$

Thus,

$$Q^{\zeta}_{\gamma,j}(\Phi(1), \ldots, \Phi(\beta^{d-1}), \Phi(w\beta^{j-1})) \neq (0, 0, 0),$$

and so by Proposition 1.2.1, it follows that

$$[Q^{\zeta}_{\gamma,j}(\Phi(1), \ldots, \Phi(\beta^{d-1}), \Phi(w\beta^{j-1}))] = q_{\gamma,j}([\Phi(1)], \ldots, [\Phi(\beta^{d-1})], [\Phi(w\beta^{j-1})])$$

$$\begin{aligned} &= [\Phi(\mathbf{b}_{\gamma,j} \cdot (1, \ldots, \beta^{d-1}) + w\beta^{j-1})] \\ &= [\Phi(\gamma\beta^{j-1} + w\beta^{j-1})] \\ &= [\Phi((\gamma + w)\beta^{j-1})]. \end{aligned}$$

Therefore, $Q^{\zeta}_{\gamma,j}(\Phi(1), \ldots, \Phi(\beta^{d-1}), \Phi(w\beta^{j-1})) \propto_w \Phi((\gamma + w)\beta^{j-1})$, from which transitivity yields that $Q^{\zeta}_{\gamma,j}(\mathbf{u}, \Phi_0(w\beta^{j-1})) \propto_w \Phi((\gamma + w)\beta^{j-1})$. ▮

In finding estimates on the proportionality function implied in the result of the above lemma, define for each $\gamma \in \Gamma$, for each $j \in \{1, \ldots, d\}$, and for each $\zeta \in Z_{\gamma,j}$, the functions

$$\delta_{\gamma,j}(w) = \phi_k((\gamma + w)\beta^{j-1});$$

$$\Delta^{\zeta}_{\gamma,j}(w) = Q^{\zeta}_{\gamma,j,k}(\mathbf{u}, \Phi_0(w\beta^{j-1})),$$

where $k \in \{0, 2\}$ is such that $\gamma\beta^{j-1} \in C_k$. Recall that $\Omega = \min_{\omega \in \Lambda \setminus \{0\}} |\omega|$, and let $c_\alpha = 1 + |\alpha|$.

Lemma 7.2.3. *There exists $c_1 \in \mathbb{R}^+$ such that if $S \geqslant 1$ and $\gamma \in \Gamma_S$, then*

$$|\delta_{\gamma,j}(w)| \geqslant e^{-c_1 S^2} \quad (1 \leqslant j \leqslant d)$$

for $|w| \leqslant \Omega/(4c_\beta)$.

Proof: Let $\gamma \in \Gamma_S$, and let $j \in \{1, \ldots, d\}$. Then,

$$|\gamma| = \left| \sum_{k=1}^{d} \tau_k \beta^{k-1} \right| \leqslant \sum_{k=1}^{d} |\tau_k||\beta|^{k-1} \quad (\text{for some } \tau_k \in \mathcal{O}_S).$$

Since $|\tau_k| \leqslant c_\alpha S$, and $|\beta|^{k-1} \leqslant c_\beta$, then

$$|\gamma| \leqslant dc_\alpha c_\beta S,$$

and so $|\gamma\beta^{j-1}| \leqslant dc_\alpha c_\beta^2 S$. Note that

$$\delta_{\gamma,j}(w) = \phi_k((\gamma + w)\beta^{j-1}) = \phi_k(\gamma\beta^{j-1} + w\beta^{j-1}),$$

where $\gamma\beta^{j-1} \in C_k$. If $|w| \leqslant \Omega/(4c_\beta)$, then $|w\beta^{j-1}| \leqslant \Omega/4$, and so by Theorem 4.1.5, it follows that

$$|\phi_k(\gamma\beta^{j-1} + w\beta^{j-1})| \geqslant e^{-cR^2},$$

for some $c \in \mathbb{R}^+$ which does not depend on R, and where $R = dc_\alpha c_\beta^2 S$. Let $c_1 = c(dc_\alpha c_\beta^2)^2 > 0$, so that

$$|\delta_{\gamma,j}(w)| \geqslant e^{-c_1 S^2}. \qquad \blacksquare$$

Lemma 7.2.4. *There exists $c_2 \in \mathbb{R}^+$ such that if $S \geqslant 1$ and $\gamma \in \Gamma_S$, then*

$$|Q^\zeta_{\gamma,j,k}(\mathbf{u}, \Phi_0(w\beta^{j-1}))| \leqslant \exp(c_2 S^2) \quad (1 \leqslant j \leqslant d; 0 \leqslant k \leqslant 2; \forall\zeta \in Z_{\gamma,j}),$$

for $|w| \leqslant \varepsilon/(2c_\beta)$. In particular,

$$|\Delta^\zeta_{\gamma,j}(w)| \leqslant \exp(c_2 S^2) \quad (1 \leqslant j \leqslant d; \forall\zeta \in Z_{\gamma,j}).$$

Proof: Write

$$Q^\zeta_{\gamma,j,k} = \sum_{|\mathbf{e}_l| = \deg_{\mathbf{x}_l} Q^\zeta_{\gamma,j,k}} a_{\mathbf{e}_1,\ldots,\mathbf{e}_{d+1}} \mathbf{x}_1^{\mathbf{e}_1} \cdots \mathbf{x}_{d+1}^{\mathbf{e}_{d+1}}.$$

Let $m_l = \max_r\{|u_{l,r}|\}$ for $1 \leqslant l \leqslant d$. The functions $f, h, 1$ are entire on $\overline{B(0;\varepsilon/2)}$ which is compact, and so let M be an upper bound for $|f|, |h|, 1$ on $\overline{B(0;\varepsilon/2)}$. Since $|w\beta^{j-1}| \leqslant \varepsilon/2$, then Proposition 7.2.1 and Lemma 5.1.1 yield that

$$\begin{aligned}
|Q^\zeta_{\gamma,j,k}(\mathbf{u}, \Phi_0(w\beta^{j-1}))| &\leqslant \sum_{|\mathbf{e}_l| = \deg_{\mathbf{x}_l} Q^\zeta_{\gamma,j,k}} |a_{\mathbf{e}_1,\ldots,\mathbf{e}_{d+1}}| m_1^{CS^2} \cdots m_d^{CS^2} M^2 \\
&\leqslant \sum_{|\mathbf{e}_l| = \deg_{\mathbf{x}_l} Q^\zeta_{\gamma,j,k}} e^{[K:\mathbb{Q}]CS^2} m_1^{CS^2} \cdots m_d^{CS^2} M^2 \\
&\leqslant ((CS^2+2)(CS^2+1)/2)^{d+1} e^{[K:\mathbb{Q}]CS^2} m_1^{CS^2} \cdots m_d^{CS^2} M^2,
\end{aligned}$$

since $Q^{\zeta}_{\gamma,j,k}$ consists of at most $((CS^2+2)(CS^2+1)/2)^{d+1}$ monomials. Thus, there exists constants $c', c'', c''' > 0$ such that

$$|Q^{\zeta}_{\gamma,j,k}(\mathbf{u}, \Phi_0(w\beta^{j-1}))| \leqslant e^{c'S^2+c''\log S+c'''}.$$

Finally, there exists $c_2 > 0$ such that $c'S^2 + c''\log S + c''' \leqslant c_2 S^2$. ∎

The following proposition and theorem justify the reasoning behind Lemma 7.2.2, 7.2.3 and 7.2.4, and illustrate the usefulness of the aforementioned idea by Baker-Coates-Anderson. Recall that P denotes the polynomial for the auxiliary function F constructed in Theorem 4.3.2.

Proposition 7.2.5. *Let* $\underline{\gamma} = (\gamma_1, \ldots, \gamma_q) \in \Gamma^q$, *and let* $\underline{\zeta} \in Z_{\underline{\gamma}}$. *Then,*

$$P(1, \underline{\gamma}+\mathbf{w}, \ldots, Q^{\zeta_{ij}}_{\gamma_i,j}(\mathbf{u}, \Phi_0(w_i\beta^{j-1})), \ldots) = \left(\prod_{i,j} \frac{\Delta^{\zeta_{ij}}_{\gamma_i,j}(w_i)}{\delta_{\gamma_i,j}(w_i)}\right)^D F(\underline{\gamma}+\mathbf{w}),$$

for $\mathbf{w} \in B(0; \varepsilon/c_\beta)$.

Proof: Let $i \in \{1, \ldots, q\}$, and let $j \in \{1, \ldots, d\}$. Then, Lemma 7.2.2 implies the existence of a function $\rho^{\zeta_{ij}}_{\gamma_i,j} : \mathbb{C} \to \mathbb{C}$ such that

$$Q^{\zeta_{ij}}_{\gamma_i,j}(\mathbf{u}, \Phi_0(w_i\beta^{j-1})) = \rho^{\zeta_{ij}}_{\gamma_i,j}(w_i)\Phi((\gamma_i+w_i)\beta^{j-1}) \quad (\forall w_i \in B(0; \varepsilon/c_\beta)).$$

Since Theorem 4.1.5 implies that $\delta_{\gamma_i,j}(w_i) \neq 0$, then

$$\rho^{\zeta_{ij}}_{\gamma_i,j}(w_i) = \frac{\Delta^{\zeta_{ij}}_{\gamma_i,j}(w_i)}{\delta_{\gamma_i,j}(w_i)} \quad (\forall w_i \in B(0; \varepsilon/c_\beta)).$$

Since $P(1, \mathbf{z}, \mathbf{x}_{1,1}, \ldots, \mathbf{x}_{q,d})$ is homogeneous of degree D in each $\mathbf{x}_{i,j}$, then

$$\begin{aligned}\left(\prod_{i,j} \frac{\Delta^{\zeta_{ij}}_{\gamma_i,j}(w_i)}{\delta_{\gamma_i,j}(w_i)}\right)^D F(\underline{\gamma}+\mathbf{w}) =& \left(\prod_{i,j} \rho^{\zeta_{ij}}_{\gamma_i,j}(w_i)\right)^D P(1, \underline{\gamma}+\mathbf{w}, \ldots, \Phi((\gamma_i+w_i)\beta^{j-1}), \ldots) \\ =& P(1, \underline{\gamma}+\mathbf{w}, \ldots, \rho^{\zeta_{ij}}_{\gamma_i,j}(w_i)\Phi((\gamma_i+w_i)\beta^{j-1}), \ldots)\end{aligned}$$

$$=P(1,\underline{\gamma}+\mathbf{w},\dots,Q^{\zeta_{ij}}_{\gamma_i,j}(\mathbf{u},\Phi_0(w_i\beta^{j-1})),\dots),$$

as required. ∎

For the sake of compactness, define the polynomial

$$p^{\sigma}_{\underline{\gamma},\underline{\zeta}}(\mathbf{x})=\frac{\partial^{|\sigma|}}{\partial\mathbf{w}^{\sigma}}P(1,\underline{\gamma}+\mathbf{w},\dots,Q^{\zeta_{ij}}_{\gamma_i,j}(\mathbf{x},\Phi_0(w_i\beta^{j-1})),\dots)\bigg|_{\mathbf{w}=\mathbf{0}},$$

where $\mathbf{x}$ is a multivariable over $(\mathbb{C}^3)^d$. Let $\eta=\min\{\Omega/(4c_\beta),\varepsilon/(2c_\beta),1\}$. Throughout the remainder of this thesis, fix $S\coloneqq S(L)$ such that it satisfies

$$q^{1/2}dc_\alpha c_\beta S+\eta=(\log L)^{\varsigma}\quad(\forall L\in\mathbb{N}^+),$$

where $\varsigma=1/(2d-1)\leqslant 1$.

Theorem 7.2.6. *Let $\underline{\gamma}=(\gamma_1,\dots,\gamma_q)\in\Gamma^q_S$, and let $\underline{\zeta}\in Z_{\underline{\gamma}}$. If L is sufficiently large, then*

$$|p^{\sigma}_{\underline{\gamma},\underline{\zeta}}(\mathbf{u})|\leqslant e^{-L(\log L)^{1+\epsilon/2}}\quad(\forall|\sigma|\leqslant L).$$

Proof: Since $\underline{\gamma}\in\Gamma^q_S$, then

$$|\underline{\gamma}+\mathbf{w}|\leqslant|\underline{\gamma}|+\eta\leqslant q^{1/2}dc_\alpha c_\beta S+\eta\leqslant\log L\quad(\forall|\mathbf{w}|\leqslant\eta).$$

Then, Theorem 4.3.2 yields

$$|F(\underline{\gamma}+\mathbf{w})|_{\eta}\leqslant e^{-2L(\log L)^{1+\varepsilon/2}}.$$

Then, from Lemma 7.2.3 and Lemma 7.2.4, it follows that

$$\left|\left(\prod_{i,j}\frac{\Delta^{\zeta_{ij}}_{\gamma_i,j}(w_i)}{\delta_{\gamma_i,j}(w_i)}\right)^{D}F(\underline{\gamma}+\mathbf{w})\right|_{|\mathbf{w}|\leqslant\eta}\leqslant e^{(c_1+c_2)S^2qdD-2L(\log L)^{1+\epsilon/2}}.$$

Remark that $(\delta_{\gamma_i,j}(w))^{-1}$ is holomorphic for $|\mathbf{w}|\leqslant\eta$. Thus, Cauchy's inequality yields

$$\left|\frac{\partial^{|\sigma|}}{\partial\mathbf{w}^{\sigma}}\left(\prod_{i,j}\frac{\Delta^{\zeta_{ij}}_{\gamma_i,j}(w_i)}{\delta_{\gamma_i,j}(w_i)}\right)^{D}F(\underline{\gamma}+\mathbf{w})\right|_{\mathbf{w}=0}\leqslant\frac{|\sigma|!}{\eta^{|\sigma|}}e^{(c_1+c_2)S^2qdD-2L(\log L)^{1+\epsilon/2}}\quad(\forall\sigma\in\mathbb{N}^q).$$

Thus, if $|\sigma| \leqslant L$, then

$$\frac{|\sigma|!}{\eta^{|\sigma|}} e^{(c_1+c_2)S^2qdD-2L(\log L)^{1+\epsilon/2}} \leqslant e^{L\log L - L\log\eta+(c_1+c_2)S^2qdD-2L(\log L)^{1+\epsilon/2}} \leqslant e^{-L(\log L)^{1+\epsilon/2}},$$

for sufficiently large L. Proposition 7.2.5 yields the conclusion. ∎

Theorem 7.2.7. *Let $\underline{\gamma} = (\gamma_1, \ldots, \gamma_q) \in \Gamma_S^q$, and let $\underline{\zeta} \in Z_{\underline{\gamma}}$. Then, for all sufficiently large L,*

$$\deg_{\mathbf{x}} p^{\sigma}_{\underline{\gamma},\underline{\zeta}}(\mathbf{x}) \leqslant d^2CqDS^2;$$

$$\mathrm{h}(p^{\sigma}_{\underline{\gamma},\underline{\zeta}}) \leqslant 3L(\log L)^{\epsilon} \quad (\forall |\sigma| \leqslant M),$$

where $M = L/\log L$.

Proof: Let $\sigma \in \mathbb{N}^q$ with $|\sigma| \leqslant M$. Differentiating by $\mathbf{w}$ does not affect the degree in $\mathbf{x}$ of

$$P(1, \underline{\gamma} + \mathbf{w}, \ldots, Q^{\zeta_{ij}}_{\gamma_i,j}(\mathbf{x}, \Phi_0(w_i\beta^{j-1})), \ldots),$$

which has degree in $\mathbf{x}$ bounded by $qd \cdot D \cdot dCS^2$. Thus, it follows that

$$\deg_{\mathbf{x}} p^{\sigma}_{\underline{\gamma},\underline{\zeta}}(\mathbf{x}) \leqslant d^2CqDS^2.$$

Define

$$\mathrm{D}_i^{\sigma_i} = \frac{\partial^{\sigma_i}}{\partial {w_i}^{\sigma_i}},$$

and write $\mathrm{D} = (\mathrm{D}_1, \ldots, \mathrm{D}_q)$ so that $\mathrm{D}^{\sigma} = \mathrm{D}_1^{\sigma_1} \cdots \mathrm{D}_q^{\sigma_q}$, and so

$$p^{\sigma}_{\underline{\gamma},\underline{\zeta}}(\mathbf{x}) = \mathrm{D}^{\sigma} P(1, \underline{\gamma} + \mathbf{w}, \ldots, Q^{\zeta_{ij}}_{\gamma_i,j}(\mathbf{x}, \Phi_0(w_i\beta^{j-1})), \ldots)|_{\mathbf{w}=\mathbf{0}}.$$

Define

$$A_i = \gamma_i + w_i \quad \text{and} \quad B_{ijk} = Q^{\zeta_{ij}}_{\gamma_i,j,k}(\mathbf{x}, \Phi_0(w_i\beta^{j-1})),$$

and write

$$\mathbf{B}_{ij} = (B_{ij0}, B_{ij1}, B_{ij2}) \quad \text{and} \quad \mathbf{B}_i = (\mathbf{B}_{i1}, \ldots, \mathbf{B}_{id}).$$

By writing

$$P = \sum_{|\mathbf{k}|=L} \sum_{|\mathbf{e}_{ij}|=D} c_{\mathbf{k},\mathbf{e}} z_0^{k_0} \prod_{i=1}^{q} (z_i^{k_i} \prod_{j=1}^{d} \mathbf{x}_{ij}^{\mathbf{e}_{ij}}) \quad (\text{for some } c_{\mathbf{k},\mathbf{e}} \in \mathbb{Z}),$$

then

$$P(1, \underline{\gamma} + \mathbf{w}, \dots, Q^{\zeta_{ij}}_{\gamma_i,j}(\mathbf{x}, \Phi_0(w_i\beta^{j-1})), \dots) = \sum_{|\mathbf{k}|=L} \sum_{|\mathbf{e}_{ij}|=D} c_{\mathbf{k},\mathbf{e}} \prod_{i=1}^{q} (A_i^{k_i} \prod_{j=1}^{d} \mathbf{B}_{ij}^{\mathbf{e}_{ij}}).$$

Since each w_i only appears in the A_i and $\mathbf{B}_{ij}$ terms, it follows that

$$\mathrm{D}^{\sigma} P(1, \underline{\gamma} + \mathbf{w}, \dots, Q^{\zeta_{ij}}_{\gamma_i,j}(\mathbf{x}, \Phi_0(w_i\beta^{j-1})), \dots) = \sum_{|\mathbf{k}|=L} \sum_{|\mathbf{e}_{ij}|=D} c_{\mathbf{k},\mathbf{e}} \prod_{i=1}^{q} \mathrm{D}_i^{\sigma_i}(A_i^{k_i} \mathbf{B}_i^{\mathbf{e}_i}).$$

Define

$$T_{i\mathbf{ke}} \coloneqq \mathrm{D}_i^{\sigma_i}(A_i^{k_i} \mathbf{B}_i^{\mathbf{e}_i})|_{\mathbf{w}=\mathbf{0}}. \tag{7.2.1}$$

Since the sum above has at most $M_1 = \binom{L+q}{L}(2D+1)^{qd}$ terms, and $\deg_{\mathbf{x}} T_{i\mathbf{ke}} \leqslant M_2 = d^2DCS^2$, then Lemma 5.2.1 yields that

$$\left\| p^{\sigma}_{\underline{\gamma},\underline{\zeta}} \right\|_v \leqslant \left\{ M_1 \binom{M_2+3d-1}{M_2}^{q-1} \right\}_v \|P\|_v \max_{i\mathbf{ke}} \|T_{i\mathbf{ke}}\|_v^q \quad (\forall v \in \mathfrak{M}_K). \tag{7.2.2}$$

Note that if $i \in \{1, \dots, q\}$, then

$$\mathrm{D}_i^{\sigma_i}(A_i^{k_i} \mathbf{B}_i^{\mathbf{e}_i}) = \sum_{l=0}^{\min\{\sigma_i,k_i\}} \binom{\sigma_i}{l} \frac{k_i!}{(k_i-l)!} A_i^{k_i-l} \mathrm{D}_i^{\sigma_i-l}(\mathbf{B}_i^{\mathbf{e}_i}).$$

Define

$$U_{il\mathbf{e}} \coloneqq \mathrm{D}_i^{\sigma_i-l}(\mathbf{B}_i^{\mathbf{e}_i})|_{\mathbf{w}=\mathbf{0}}, \tag{7.2.3}$$

and so

$$T_{i\mathbf{ke}} = \sum_{l=0}^{\min\{\sigma_i,k_i\}} \binom{\sigma_i}{l} \frac{k_i!}{(k_i-l)!} \gamma_i^{k_i-l} U_{il\mathbf{e}}.$$

Since $l, \sigma_i \leqslant M$, and $k_i \leqslant L$, then Lemma 5.2.1 yields that

$$\max_{i\mathbf{ke}} \|T_{i\mathbf{ke}}\|_v \leqslant \left\{ M \cdot 2^M \cdot L^M \right\}_v \max_i \{1, |\gamma_i|_v\}^L \max_{il\mathbf{e}} \|U_{il\mathbf{e}}\|_v \quad (\forall v \in \mathfrak{M}_K). \tag{7.2.4}$$

Note that if $i \in \{1, \ldots, q\}$, then

$$\mathrm{D}_i^{\sigma_i - l}(\mathbf{B}_i^{\mathbf{e}_i}) = \sum_{\sum_{j,k} s_{ijk} = \sigma_i - l} \binom{\sigma_i - l}{s_{i11} \cdots s_{id3}} \prod_{j,k} \mathrm{D}_i^{s_{ijk}} B_{ijk}^{e_{ijk}}.$$

Define

$$V_{ijk}^{s,e} \coloneqq \mathrm{D}_i^s B_{ijk}^e|_{\mathbf{w}=\mathbf{0}}, \tag{7.2.5}$$

and so

$$U_{il\mathbf{e}} = \sum_{\sum_{j,k} s_{ijk} = \sigma_i - l} \binom{\sigma_i - l}{s_{i11} \cdots s_{id3}} \prod_{j,k} V_{ijk}^{s_{ijk}, e_{ijk}}.$$

The sum above has at most $M_3 = \binom{M+3d-1}{M}$ terms, $\deg_{\mathbf{x}} V_{ijk}^{s_{ijk}, e_{ijk}} \leqslant M_4 = dDCS^2$, and $\binom{\sigma_i - l}{s_{i11} \cdots s_{id3}} \leqslant (3d)^M$. Thus, Lemma 5.2.1 yields for each $v \in \mathfrak{M}_K$ that

$$\max_{il\mathbf{e}} \|U_{il\mathbf{e}}\|_v \leqslant \left\{ M_3 (3d)^M \binom{M_4 + 3d - 1}{M_4}^{3d-1} \right\}_v \max_{ijk} \max_{s \leqslant M} \max_{e \leqslant D} \left\| V_{ijk}^{s,e} \right\|_v^{3d}. \tag{7.2.6}$$

Note that if $i \in \{1, \ldots, q\}$, then

$$\mathrm{D}_i^s B_{ijk}^e = \mathrm{D}_i^s (Q_{\gamma_i, j, k}^{\zeta_{ij}}(\mathbf{x}, \Phi_0(w_i \beta^{j-1})))^e = \sum_{s_1 + \cdots + s_e = s} \binom{s}{s_1 \cdots s_e} \prod_{l=0}^{e} \mathrm{D}_i^{s_l} Q_{\gamma_i, j, k}^{\zeta_{ij}}(\mathbf{x}, \Phi_0(w_i \beta^{j-1})).$$

By writing

$$Q_{\gamma_i, j, k}^{\zeta_{ij}}(\mathbf{x}, \mathbf{y}) = \sum_{\underline{\delta}} \sum_{|\underline{\epsilon}| = 2} b_{\underline{\delta}, \underline{\epsilon}}^{i,j,k} \mathbf{x}^{\underline{\delta}} \mathbf{y}^{\underline{\epsilon}} \quad (\text{for some } b_{\underline{\delta}, \underline{\epsilon}}^{i,j,k} \in K),$$

then

$$\mathrm{D}_i^s B_{ijk}^e = \sum_{s_1 + \cdots + s_e = s} \binom{s}{s_1 \cdots s_e} \prod_{l=1}^{e} \sum_{\underline{\delta}} \left(\sum_{|\underline{\epsilon}| = 2} b_{\underline{\delta}, \underline{\epsilon}}^{i,j,k} \mathrm{D}_i^{s_l} (\Phi_0(w_i \beta^{j-1}))^{\underline{\epsilon}} \right) \mathbf{x}^{\underline{\delta}}.$$

Since $\Phi_0 = (f, h, 1)$, then it is possible to write for each $|\underline{\epsilon}| = 2$ that

$$\Phi_0(w_i \beta^{j-1})^{\underline{\epsilon}} = \chi_{1, \underline{\epsilon}}(w_i \beta^{j-1}) \chi_{2, \underline{\epsilon}}(w_i \beta^{j-1}) \quad (1 \leqslant i \leqslant q; 1 \leqslant j \leqslant d),$$

for some $\chi_{1, \underline{\epsilon}}, \chi_{2, \underline{\epsilon}} \in \{f, h, 1\}$. Notice then that

$$\mathrm{D}_i^n (\chi_{\lambda, \underline{\epsilon}}(w_i \beta^{j-1}))|_{\mathbf{w}=\mathbf{0}} = \chi_{\lambda, \underline{\epsilon}}^{(n)}(0) \beta^{n(j-1)} \quad (\forall \lambda \in \{1, 2\}; \forall n \in \mathbb{N}),$$

and so

$$\mathrm{D}_i^{s_l} (\Phi_0(w_i \beta^{j-1}))^{\underline{\epsilon}}|_{\mathbf{w}=\mathbf{0}} = \sum_{\lambda=0}^{s_l} \binom{s_l}{\lambda} \beta^{s_l (j-1)} \chi_{1, \underline{\epsilon}}^{(\lambda)}(0) \chi_{2, \underline{\epsilon}}^{(s_l - \lambda)}(0). \tag{7.2.7}$$

Thus, it follows

$$\begin{aligned} V_{ijk}^{s,e} &= \sum_{s_1+\cdots+s_e=s} \binom{s}{s_1\cdots s_e} \prod_{l=1}^{e} \left(\sum_{\underline{\delta}} \left(\sum_{|\underline{\epsilon}|=2} b_{\underline{\delta},\underline{\epsilon}}^{i,j,k} \sum_{\lambda=0}^{s_l} \binom{s_l}{\lambda} \beta^{s_l(j-1)} \chi_{1,\underline{\epsilon}}^{(\lambda)}(0) \chi_{2,\underline{\epsilon}}^{(s_l-\lambda)}(0) \right) \mathbf{x}^{\underline{\delta}} \right) \\ &= \sum_{s_1+\cdots+s_e=s} \binom{s}{s_1\cdots s_e} \beta^{s(j-1)} \prod_{l=1}^{e} \left(\sum_{\underline{\delta}} \left(\sum_{|\underline{\epsilon}|=2} b_{\underline{\delta},\underline{\epsilon}}^{i,j,k} \sum_{\lambda=0}^{s_l} \binom{s_l}{\lambda} \chi_{1,\underline{\epsilon}}^{(\lambda)}(0) \chi_{2,\underline{\epsilon}}^{(s_l-\lambda)}(0) \right) \mathbf{x}^{\underline{\delta}} \right). \end{aligned}$$

Since $s \leqslant M$, $e \leqslant D$, and $\underline{\delta} = (\underline{\delta}_1, \ldots, \underline{\delta}_d)$ has each $|\underline{\delta}_l| \leqslant CS^2$, then $\sum \binom{s}{s_1\cdots s_e} \leqslant D^M$, and each polynomial in the product of polynomials has degree in $\mathbf{x}$ bounded by $M_5 = dCS^2$. Then, Lemma 5.2.1 yields for each $v \in \mathfrak{M}_K$ that

$$\begin{aligned} &\max_{ijkse} \left\| V_{ijk}^{se} \right\|_v \\ &\leqslant \{D\}_v^M \max\{1, |\beta|_v^{(d-1)M}\} \left\{ \binom{M_5+3d-1}{M_5} \right\}_v^{D-1} \max_{ijkl\underline{\delta}} \left| \sum_{|\underline{\epsilon}|=2} b_{\underline{\delta},\underline{\epsilon}}^{i,j,k} \sum_{\lambda=0}^{s_l} \binom{s_l}{\lambda} \chi_{1,\underline{\epsilon}}^{(\lambda)}(0) \chi_{2,\underline{\epsilon}}^{(s_l-\lambda)}(0) \right|_v^D \\ &\leqslant \{D\}_v^M \max\{1, |\beta|_v^{dM}\} \left(\left\{ M_5^{3d} \cdot 6 \cdot 2^M \right\}_v \max_{ijkl\lambda\underline{\varepsilon}} \left\| Q_{\gamma_i,j,k}^{\zeta_{ij}} \right\|_v \left| \chi_{1,\underline{\epsilon}}^{(\lambda)}(0) \chi_{2,\underline{\epsilon}}^{(s_l-\lambda)}(0) \right|_v \right)^D. \end{aligned}$$

By letting $M_6 = D^M (M_5^{3d} \cdot 6 \cdot 2^M)^D$, it follows for each $v \in \mathfrak{M}_K$ that

$$\begin{aligned} &\max_{ijkse} \left\| V_{ijk}^{se} \right\|_v \\ &\leqslant \{M_6\}_v \max_{ijk} \left\| Q_{\gamma_i,j,k}^{\zeta_{ij}} \right\|_v^D \max\{1, |\beta|_v^{dM}\} \max_{0 \leqslant \lambda \leqslant M} \{1, \left|f^{(\lambda)}(0)\right|_v, \left|h^{(\lambda)}(0)\right|_v\}^{2D}. \end{aligned} \tag{7.2.8}$$

Let

$$M_7 = M_1 \binom{M_2+3d-1}{M_2}^{q-1} \left(M(6dL)^M M_3 \binom{M_4+3d-1}{M_4}^{3d-1} \right)^q M_6^{3qd},$$

and note that Proposition 7.2.1 yields that

$$\mathrm{h}((Q_{\gamma_i,j,k}^{\zeta_{ij}})_{ijk}) \leqslant qdCS^2.$$

Thus, Lemma 5.2.2 and equations (7.2.2), (7.2.4), (7.2.6), and (7.2.8) yield that

$$\begin{aligned} \mathrm{h}(p_{\underline{\gamma},\underline{\zeta}}^{\sigma}) \leqslant{}& \log M_7 + \mathrm{h}(P) + qL\mathrm{h}(\underline{\gamma}) + 3qdDCS^2 \\ &+ 3qd^2M\mathrm{h}(\beta) + 6qdD\mathrm{h}((f^{(n)}(0), h^{(n)}(0))_{0 \leqslant n \leqslant M}). \end{aligned}$$

By Theorem 4.3.2, Proposition 7.1.1, and Corollary 7.1.9, this last expression, with the $\log M_7$ term omitted, is thus bounded by

$$\begin{aligned}&L + qL(\log(2dS) + \mathrm{h}(\alpha) + d\mathrm{h}(\beta))\\&\quad + 3qd(DCS^2 + dM\mathrm{h}(\beta) + 2DM(\log M + \mathrm{h}(g_2, g_3) + \log 38))\\&\quad \leqslant 2DM \log L = 2DL,\end{aligned}$$

for sufficiently large L. Since all of the $\log M_i$ terms for $i \in \{1, \ldots, 6\}$ have order less than $M \log L$, it follows that

$$\log M_7 \leqslant \tilde{c} M \log L = \tilde{c} L,$$

for some $\tilde{c} \in \mathbb{R}^+$, and sufficiently large L. Therefore,

$$\mathrm{h}(p^{\sigma}_{\underline{\gamma},\underline{\varsigma}}) \leqslant 2DL + \tilde{c}L \leqslant 2((\log L)^{\epsilon} + 1)L + \tilde{c}L \leqslant 3L(\log L)^{\epsilon},$$

for sufficiently large L, as required. ∎

Chapter 8

Zero Estimate

The main result of this chapter will use Philippon's zero lemma, stated as Theorem 8.2.1, and whose proof is in [9]. Before doing so, some notation and terminology will be established.

8.1 Preliminaries

Let $G = \mathbb{C}^n \times E^m$, and note that it is an algebraic group. The *exponential map on* G, denoted $\exp_G : \mathbb{C}^n \times \mathbb{C}^m \to G$ is defined by

$$\exp_G(\mathbf{t}, z_1, \ldots, z_m) = (\mathbf{t}, \exp_E(z_1), \ldots, \exp_E(z_m)).$$

The following notion will be quite relevant as well.

Definition. An *algebraic subgroup* is an algebraic set which is a subgroup of an algebraic group.

Let $H \leqslant G$ be a connected algebraic subgroup. The *tangent space of* H, denoted $T_H(\mathbb{C})$, is defined as the connected component of the preimage of $\exp_G$ at H which contains $\mathbf{0} \in \mathbb{C}^{n+m}$. In fact, there exists a subspace $U \subseteq \mathbb{C}^n$ and a subspace $V \subseteq \mathbb{C}^m$ defined over $\mathbb{Q}(\alpha)$ such that

$$T_H(\mathbb{C}) = U \times V.$$

In particular, letting $k = \dim_{\mathbb{C}}(U)$ and $l = \dim_{\mathbb{C}}(V)$, it follows that $H \cong \mathbb{C}^k \times E^l$.

Let $\Theta : \mathbb{C}^n \to \mathbb{C}^n \times \mathbb{C}^m$ be a $\mathbb{C}$-linear map, and let $W = \mathrm{Im}(\Theta)$ be its image. Let

$$\mathbf{Z} = (Z_0, \ldots, Z_n) \quad \text{and} \quad \mathbf{X}_i = (X_{i,0}, X_{i,1}, X_{i,2}) \quad (1 \leqslant i \leqslant m)$$

be indeterminates over $\mathbb{C}$, and let $P(\mathbf{Z}, \mathbf{X}_1, \ldots, \mathbf{X}_m)$ be multihomogeneous with

$$\deg_{\mathbf{Z}}(P) = L \quad \text{and} \quad \deg_{\mathbf{X}_i}(P) = D \quad (1 \leqslant i \leqslant m). \tag{8.1.1}$$

Let $T \in \mathbb{N}$. The polynomial P is said to vanish at a point $\exp_G(\mathbf{u}) \in G$ at an order $> T$ along W if

$$0 = \frac{\partial^{|\sigma|}}{\partial \mathbf{w}^{\sigma}} P(1, \exp_G(\mathbf{u} + \Theta(\mathbf{w})))|_{\mathbf{w}=\mathbf{0}} \quad (\forall |\sigma| \leqslant T).$$

Finally, define, for a finite set $\Sigma \subseteq G$ and an integer $N \geqslant 1$, the set

$$\Sigma(N) = \{x_1 + \cdots + x_N \,|\, \text{each } x_i \in \Sigma\}.$$

8.2 Zero Estimate

The following theorem is due to Philippon, and specialized to the above context.

Theorem 8.2.1 (Philippon, 1986)**.** *Let Σ be a finite subset of $G = \mathbb{C}^n \times E^m$ which contains the origin. Suppose that P satisfies* (8.1.1) *and vanishes at each point of $\Sigma(n+m)$ at an order $> T$ along W. Then, there exists a connected algebraic subgroup*

$$H \leqslant G, \quad H \cong \mathbb{C}^k \times E^l,$$

such that H is contained in a translate of $G \cap Z(P)$, and such that

$$\left| \frac{\Sigma + H}{H} \right| \cdot T^{\dim_{\mathbb{C}}(W/(W \cap T_H))} \ll L^{n-k} D^{m-l}.$$

This theorem plays a crucial role in the proof of the following proposition.

Proposition 8.2.2. *Let the notation be as in Theorem* 7.2.7*, and let* $K = \mathbb{Q}(\alpha, \beta)$*. Recall that* $d = [K : \mathbb{Q}(\alpha)]$*,* $\varsigma = 1/(2d-1)$*,* $S \asymp (\log L)^{\varsigma}$*,* $\epsilon > 0$ *is a real parameter that can be chosen to be arbitrarily small, and that* $q \in \mathbb{N}^{+}$ *is a parameter satisfying* $q > (2+\epsilon)/(\epsilon(2d-1))$*. Let* $T = L/\log L$*. Then, the polynomials in*

$$\mathcal{F}_L \coloneqq \{p^{\sigma}_{\underline{\gamma},\underline{\zeta}} \,|\, \sigma \in \mathbb{N}^q, \text{ with } |\sigma| \leqslant T;\ \underline{\gamma} = (\gamma_1, \ldots, \gamma_q) \in \Gamma^q_S;\ \underline{\zeta} \in Z_{\underline{\gamma}}\}$$

have no common zeros in $E^d \subseteq \mathbb{C}^{3d}$ *for all sufficiently large* L*.*

Proof: Take $n = q$ and $m = qd$, so that $G = \mathbb{C}^q \times E^{qd}$. Recall that P denotes the polynomial constructed in Theorem 4.3.2 which satisfies (8.1.1) with $D = \lfloor \log(L)+1 \rfloor^{\epsilon}$. Suppose that $\mathbf{a} \in E^d \subseteq \mathbb{C}^{3d}$ is a common zero for the polynomials in $\mathcal{F}_L$. Then, there exists $\mathbf{z} \in \mathbb{C}^d$ such that $\mathbf{a} = \exp_{E^d}(\mathbf{z})$. Thus, since

$$p^{\sigma}_{\underline{\gamma},\underline{\zeta}}(\mathbf{a}) = 0 \quad (\forall |\sigma| \leqslant T; \forall \underline{\gamma} \in \Gamma^q_S, \forall \underline{\zeta} \in Z_{\underline{\gamma}}),$$

it follows that

$$0 = \frac{\partial^{|\sigma|}}{\partial \mathbf{w}^{\sigma}} P(1, \exp_G(\underline{\gamma} + \mathbf{w}, \ldots, B_{\gamma_i}(\mathbf{z})^T + w_i \underline{\beta}^T, \ldots))|_{\mathbf{w}=\mathbf{0}} \tag{8.2.1}$$

for all $|\sigma| \leqslant T$, and for all $\underline{\gamma} \in \Gamma^q_S$. For what follows, identify $\mathbb{C}^{qd}$ with $\mathbb{C}^q \otimes \mathbb{C}^d$, and let $e_i \otimes e_j \in \mathbb{C}^q \otimes \mathbb{C}^d$ identify with the vector in $\mathbb{C}^{qd}$ whose entries are all zero except for a 1 in the j^{th} position of the i^{th} bloc which consists of d coordinates. Let $\{e_1, \ldots, e_q\}$ be the canonical basis for $\mathbb{C}^q$, and write $\underline{\beta} = (1, \beta, \ldots, \beta^{d-1})$. Define

$$\omega_i = (e_i, e_i \otimes \underline{\beta}) \in \mathbb{C}^q \times (\mathbb{C}^q \otimes \mathbb{C}^d) \quad (1 \leqslant i \leqslant q),$$

and let $\Theta : \mathbb{C}^q \to \mathbb{C}^q \times (\mathbb{C}^q \otimes \mathbb{C}^d)$ be the $\mathbb{C}$-linear map for which

$$\Theta(e_i) = \omega_i \quad (1 \leqslant i \leqslant q).$$

Define $W = \Theta(\mathbb{C}^q) = \langle \omega_1, \ldots, \omega_q \rangle_{\mathbb{C}}$. Let

$$\mathbf{v}_{ij} = (\beta^{j-1} e_i, e_i \otimes (B_{\beta^{j-1}}(\mathbf{z})^T)) \in \mathbb{C}^q \times (\mathbb{C}^q \otimes \mathbb{C}^d) \quad (1 \leqslant i \leqslant q; 1 \leqslant j \leqslant d).$$

Let $c = q + qd$, and let $N = \lfloor S/c \rfloor$. Define

$$Z_N = \left\{ \sum_{i=1}^{q} \sum_{j=1}^{d} \tau_{ij} \mathbf{v}_{ij} \,\middle|\, \tau_{ij} \in \mathcal{O}_N \right\} \quad (\forall N \in \mathbb{N});$$

$$\Sigma_N = \exp_G(Z_N) \quad (\forall N \in \mathbb{N}).$$

Notice that since $cN \leqslant S$, then for each point $u \in Z_{cN}$, there exists $\underline{\gamma} \in \Gamma_S^q$ such that

$$u = (\underline{\gamma}, \dots, B_{\gamma_i}(\mathbf{z})^T, \dots).$$

Thus, by remarking that $\Sigma_{cN} = \Sigma_N(c)$, we get by (8.2.1) that P vanishes at each point of $\Sigma_N(c)$ at an order $> T$ along W. Thus, by Theorem 8.2.1, there exists a connected algebraic subgroup

$$H \leqslant G, \quad H \cong \mathbb{C}^k \times E^l,$$

such that H is contained in a translate of $G \cap Z(P)$, and such that

$$\left| \frac{\Sigma_N + H}{H} \right| \cdot (L/\log L)^{\dim_{\mathbb{C}}(W/(W \cap T_H))} \ll L^{q-k} D^{qd-l}. \tag{8.2.2}$$

The next step is to show that (8.2.2) is impossible. Note that

$$1 \leqslant |(\Sigma_N + H)/H|,$$

and so by comparing powers of L in (8.2.2), it follows that

$$\begin{aligned} \dim_{\mathbb{C}}(W/(W \cap T_H))) + k &\leqslant q \\ q - \dim_{\mathbb{C}}(W \cap T_H) &\leqslant q - k \\ k &\leqslant \dim_{\mathbb{C}}(W \cap T_H). \end{aligned} \tag{8.2.3}$$

Define the projections

$$\pi_1 : \mathbb{C}^q \times (\mathbb{C}^q \otimes \mathbb{C}^d) \to \mathbb{C}^q \quad \text{and} \quad \pi_2 : \mathbb{C}^q \times (\mathbb{C}^q \otimes \mathbb{C}^d) \to (\mathbb{C}^q \otimes \mathbb{C}^d)$$

by

$$\pi_1(x,t) = x \quad \text{and} \quad \pi_2(x,t) = t \quad (\forall x \in \mathbb{C}^q; \forall t \in \mathbb{C}^q \otimes \mathbb{C}^d).$$

In order to obtain an upper bound for $\dim_{\mathbb{C}}(W \cap T_H)$, write

$$T_H = \pi_1(T_H) \times \pi_2(T_H) = U \times V,$$

for some subspace $U \subseteq \mathbb{C}^q$ and some subspace $V \subseteq \mathbb{C}^q \otimes \mathbb{C}^d$ defined over $\mathbb{Q}(\alpha)$, satisfying

$$\dim_{\mathbb{C}}(U) = k \quad \text{and} \quad \dim_{\mathbb{C}}(V) = l.$$

Then, since $\pi_1|_W : W \to \mathbb{C}^q$ is a bijection, it follows that

$$\dim_{\mathbb{C}}(W \cap T_H) = \dim_{\mathbb{C}} \pi_1(W \cap T_H) \leqslant \dim_{\mathbb{C}} \pi_1(T_H) = \dim_{\mathbb{C}}(U) \leqslant k,$$

and so, recalling (8.2.3),

$$\dim_{\mathbb{C}}(W \cap T_H) = k.$$

Thus, (8.2.2) yields

$$\left| \frac{\Sigma_N + H}{H} \right| \ll D^{qd-l} \log(L)^{q-k} \asymp \log(L)^{q-k+\epsilon(qd-l)}. \tag{8.2.4}$$

Further, a lower bound for $l = \dim_{\mathbb{C}}(V)$ can be deduced. Since

$$\dim_{\mathbb{C}} \pi_1(W \cap T_H) = \dim_{\mathbb{C}} \pi_1(T_H) \quad \text{and} \quad \pi_1(W \cap T_H) \subseteq \pi_1(T_H),$$

then $\pi_1(W \cap T_H) = \pi_1(T_H)$. Thus, remarking that

$$(\pi_1|_W)^{-1}(z) = \Theta(z) \quad (\forall z \in \mathbb{C}^q),$$

yields that

$$\begin{aligned} U &= \pi_1(T_H) = \pi_1(W \cap T_H) = (\pi_1|_W)(W \cap T_H) \\ \Theta(U) &= W \cap T_H \subseteq T_H \\ \pi_2(\Theta(U)) &\subseteq \pi_2(T_H) = V. \end{aligned}$$

By letting

$$\kappa = \dim_K(K^q \cap U) \leqslant k,$$

it is claimed that $l \geqslant \kappa d$. Remark that the smallest subspace defined over $\mathbb{Q}(\alpha)$ which contains $\pi_2(\Theta(U))$ is $R_1^{\perp}$ where

$$R_1 = \left\{ \sum a_{ij} e_i \otimes e_j \in \mathbb{Q}(\alpha)^q \otimes \mathbb{Q}(\alpha)^d \,\middle|\, \langle \sum_{ij} a_{ij} e_i \otimes e_j, \mathbf{x} \otimes \underline{\beta} \rangle = 0 \text{ for all } \mathbf{x} \in U \right\},$$

using the scalar product

$$\langle \sum_{ij} a_{ij} e_i \otimes e_j, \sum_{ij} b_{ij} e_i \otimes e_j \rangle = \sum_{ij} a_{ij} b_{ij}.$$

Note that,

$$\dim_{\mathbb{C}}(V) = \dim_{\mathbb{Q}(\alpha)}(V \cap \mathbb{Q}(\alpha)^q \otimes \mathbb{Q}(\alpha)^d) \geqslant \dim_{\mathbb{Q}(\alpha)}(R_1^{\perp}) = qd - \dim_{\mathbb{Q}(\alpha)}(R_1).$$

Now, define

$$R_2 = \left\{ (b_1, \ldots, b_q) \in K^q \,\middle|\, \sum_{i=1}^{q} b_i x_i = 0 \text{ for all } \mathbf{x} = (x_1, \ldots, x_q) \in U \right\},$$

and notice that $R_2 = K^q \cap U^{\perp} \subseteq (K^q \cap U)^{\perp}$. Then, since $\{1, \beta, \ldots, \beta^{d-1}\}$ are linearly independent over $\mathbb{Q}(\alpha)$, the following is a bijection.

$$\begin{aligned} R_1 &\cong R_2 \\ \Sigma_{ij} a_{ij} e_i \otimes e_j &\mapsto (\Sigma_{j=1}^d a_{1j} \beta^{j-1}, \ldots, \Sigma_{j=1}^d a_{qj} \beta^{j-1}), \end{aligned}$$

which is a $\mathbb{Q}(\alpha)$-linear map. Thus,

$$\dim_{\mathbb{Q}(\alpha)}(R_1) = d \dim_K(R_2) \leqslant d(q - \dim_K(K^q \cap U)) = d(q - \kappa),$$

and so

$$\dim_{\mathbb{C}}(V) \geqslant qd - \dim_{\mathbb{Q}(\alpha)}(R_1) \geqslant d\kappa,$$

which proves the claim. Notice then that

$$-k \leqslant -\kappa \quad \text{and} \quad -l \leqslant -d\kappa,$$

and so

$$q - k + \epsilon(qd - l) \leqslant (q - \kappa)(1 + \epsilon d).$$

Thus, it follows by (8.2.4) that

$$\left| \frac{\Sigma_N + H}{H} \right| \ll \log(L)^{(q-\kappa)(1+\epsilon d)}. \tag{8.2.5}$$

In order to find the desired contradiction, a lower bound for the cardinality of the set

$$\left| \frac{\Sigma_N + H}{H} \right|$$

will be required. Since $\ker(\exp_G) = \{0\}^q \times \Lambda^{qd}$ and $\exp_G(T_H) = H$, the following is a bijection:

$$T_G/(\{0\}^q \times \Lambda^{qd} + T_H) \cong G/H$$
$$(x + \{0\}^q \times \Lambda^{qd}) + T_H \mapsto \exp_G(x) + H.$$

Thus, it follows that

$$\left| \frac{\Sigma_N + H}{H} \right| = \left| \frac{Z_N + T_H + \{0\}^q \times \Lambda^{qd}}{T_H + \{0\}^q \times \Lambda^{qd}} \right|.$$

Since $\pi_1(Z_N) = \Gamma_N^q$, $\pi_1(T_H) = U$ and $\pi_1(\{0\}^q \times \Lambda^{qd}) = \{0\}^q$, then the following is a surjection:

$$\frac{Z_N + T_H + \{0\}^q \times \Lambda^{qd}}{T_H + \{0\}^q \times \Lambda^{qd}} \to \frac{\Gamma_N^q + U}{U}$$
$$x + T_H + \{0\}^q \times \Lambda^{qd} \mapsto \pi_1(x) + U,$$

and so

$$\left| \frac{Z_N + T_H + \{0\}^q \times \Lambda^{qd}}{T_H + \{0\}^q \times \Lambda^{qd}} \right| \geqslant \left| \frac{\Gamma_N^q + U}{U} \right|.$$

Since $\Gamma_N^q \subset K^q$, it follows that

$$\left| \frac{\Gamma_N^q + U}{U} \right| \geqslant |\Gamma_N|^{q - \dim_K(K^q \cap U)}.$$

Since $\{\alpha^i\beta^j \mid 0 \leqslant i < 2, 0 \leqslant j < d\}$ is a $\mathbb{Z}$-basis for Γ, then $|\Gamma_N| = (2N+1)^{2d}$, and so

$$(2N+1)^{2d(q-\kappa)} \leqslant \left|\frac{\Sigma_N + H}{H}\right|.$$

Therefore, it follows from (8.2.5) that $(\log L)^{\varsigma \cdot 2d(q-\kappa)} \ll \log(L)^{(q-\kappa)(1+\epsilon d)}$, and so

$$\varsigma \cdot 2d(q-\kappa) \leqslant (q-\kappa)(1+\epsilon d). \tag{8.2.6}$$

Suppose that $q \neq \kappa$, then $q - \kappa > 0$. Thus, since $\varsigma = 1/(2d-1)$, it follows that

$$\begin{aligned} 2d/(2d-1) &\leqslant 1 + \epsilon d \\ 1 + 1/(2d-1) &\leqslant 1 + \epsilon d \\ (d(2d-1))^{-1} &\leqslant \epsilon, \end{aligned}$$

which is a contradiction, if ϵ is chosen small enough, and so $q = \kappa$. Note that this could not have been deduced if E did not have complex multiplication. Specifically, if E did not have complex multiplication, then $|\Gamma_N| = (2N+1)^d$, so that the above inequalities would yield $d/(2d-1) \leqslant 1 + \epsilon d$ which does not yield a contradiction for any choice of ϵ and d. Since $q = \kappa$, it follows that $qd \geqslant l \geqslant \kappa d$, and so $l = qd$. Therefore, it follows that $T_H = U \times V = \mathbb{C}^q \times (\mathbb{C}^q \otimes \mathbb{C}^d)$, and so $H = G$. Since $G = H$ is contained in a translate of $G \cap Z(P)$, then $G = Z(P)$, and so

$$P(1, \mathbf{z}, \mathbf{x}_{11}, \ldots, \mathbf{x}_{1d}, \ldots, \mathbf{x}_{q1}, \ldots, \mathbf{x}_{qd}) = 0 \quad (\forall \mathbf{z} \in \mathbb{C}^q; \forall \mathbf{x}_{ij} \in E \subset \mathbb{C}^3).$$

In particular, by letting $\mathbf{x} = (\mathbf{x}_{11}, \ldots, \mathbf{x}_{1d}, \ldots, \mathbf{x}_{q1}, \ldots, \mathbf{x}_{qd})$, and by defining

$$h_{ij}(\mathbf{x}) = x_{ij,0}x_{ij,2}^2 - 4x_{ij,1}^3 + g_2 x_{ij,0}^2 x_{ij,1} + g_3 x_{ij,0}^3,$$

it follows that

$$P \in (h_{ij}(\mathbf{x}), \ldots, h_{qd}(\mathbf{x})).$$

Since $P \neq 0$, and since each distinct generating polynomial in the above ideal has distinct indeterminates, it follows for some $i \in \{1, \ldots, q\}$ and some $j \in \{1, \ldots, d\}$ that

$$\deg_{\mathbf{x}_{ij,2}} P \geqslant 2.$$

However, Theorem 4.3.2 guarantees that $\deg_{\mathbf{x}_{ij,2}} P \leqslant 1$, yielding a contradiction. Thus, the family $\mathcal{F}_L$ has no common zeros in $E^d \subseteq \mathbb{C}^{3d}$, as required. ∎

Chapter 9

Independence Criterion

In order to prove the main theorem, Philippon's criterion for algebraic independence from [10] will be given, specialized to the case where the families of polynomials have no common zeros.

Theorem 9.0.3 (Philippon, 1984)**.** *Let $k \in \mathbb{N}$ and let $\theta = (\underline{\theta}_1, \dots, \underline{\theta}_d) \in (\mathbb{C}^{n+1})^d$. Let $N_0 \in \mathbb{N}$, and let δ, τ, and V be increasing functions on $\{N_0, N_0 + 1, \dots\} \to [1, \infty)$ such that $\delta(N) \leqslant \tau(N)$ for all $N \geqslant N_0$, and such that*

$$\lim_{N\to\infty} \tau(N) = \infty, \quad \lim_{N\to\infty} \frac{\tau(N+1)}{\tau(N)} = \lim_{N\to\infty} \frac{\delta(N+1)}{\delta(N)} = 1 \quad \textit{and} \quad \lim_{N\to\infty} V(N) = \infty.$$

Suppose for each N sufficiently large that there exists a family of polynomials $\mathcal{F}$ which has no common zeros in $(\mathbb{P}^n)^d$, and is such that

$$\mathrm{h}(p) \leqslant \tau(N), \quad \deg_{\mathbf{x}}(p) \leqslant \delta(N) \quad (\forall p \in \mathcal{F});$$

$$\max_{p\in\mathcal{F}} |p(\theta)| \leqslant \exp(-V(N)\tau(N)\delta(N)^k).$$

Then

$$\mathrm{tr.deg}_{\mathbb{Q}}(\mathbb{Q}(\underline{\theta}_1, \dots, \underline{\theta}_d)) > k.$$

By taking the family of polynomials from Proposition 8.2.2, and by applying the estimates from Theorem 7.2.6 and Theorem 7.2.7, an application of Theorem 9.0.3 can be used to deduce the following theorem.

Theorem 9.0.4. *Let $\Lambda \subset \mathbb{C}$ be a lattice such that the corresponding elliptic curve has complex multiplication, and such that $g_2(\Lambda), g_3(\Lambda) \in \overline{\mathbb{Q}}$. Let β be a non-zero algebraic integer with $d = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)]$. Then, by defining*

$$u_j = \begin{cases} (1, \wp(\beta^{j-1}), \wp'(\beta^{j-1})) & \text{if } \beta^{j-1} \notin \Lambda; \\ (0, 0, 1) & \text{if } \beta^{j-1} \in \Lambda, \end{cases}$$

it follows that $\text{tr.deg}_{\mathbb{Q}}(\mathbb{Q}(u_1, \ldots, u_d)) = d$. *In particular,* $\{1, \beta, \ldots, \beta^{d-1}\} \cap \Lambda = \varnothing$.

Proof: Following the notation in Theorem 9.0.3, let $k = d - 1$, $N = L$, and $\theta = (u_1, \ldots, u_d)$. Further, define the functions

$$\tau(L) = 3L(\log L)^{\epsilon}, \quad \delta(L) = d^2 CqDS^2 \quad \text{and} \quad V(L) = L(\log L)^{1+\epsilon/2}/(\tau(L)\delta(L)^k),$$

where $D = \lfloor \log(L) + 1 \rfloor^{\epsilon}$ and $S \asymp (\log L)^{\varsigma}$ with $\varsigma = 1/(2d-1)$. Notice that

$$\begin{aligned} V(L) &\asymp (\log L)^{1+\epsilon/2} / \big((\log L)^{\epsilon} (\log(L)^{\epsilon} \log(L)^{2\varsigma})^k\big) \\ &= (\log L)^{1-\epsilon/2-k\epsilon-2k\varsigma}. \end{aligned}$$

Since $1 - 2k\varsigma = 1 - 2(d-1)/(2d-1) = 1/(2d-1) = \varsigma$, then

$$V \asymp (\log L)^{\varsigma-(1+2k)\epsilon/2}.$$

By choosing $\epsilon > 0$ such that $\varsigma > (1+2k)\epsilon/2$, then

$$\lim_{L\to\infty} V(L) \to \infty.$$

Define

$$h_i(\mathbf{x}) = x_{i,0}x_{i,2}^2 - 4x_{i,1}^3 + g_2 x_{i,0}^2 x_{i,1} + g_3 x_{i,0}^3 \quad (1 \leqslant i \leqslant d),$$

and define for each L the family of polynomials

$$\tilde{\mathcal{F}}_L = \mathcal{F}_L \cup \{h_1, \ldots, h_d\}.$$

Since $Z(h_1, \ldots, h_d) = E^d \subseteq (\mathbb{P}^2)^d$, Proposition 8.2.2 yields for sufficiently large L that $\tilde{\mathcal{F}}_L$ has no common zeros in $(\mathbb{P}^2)^d$. Note that

$$h_i(\theta) = 0 \quad (1 \leqslant i \leqslant q; 1 \leqslant j \leqslant d),$$

and so Theorem 7.2.6 yields for sufficiently large L that

$$\max_{p \in \tilde{\mathcal{F}}_L} |p(\theta)| \leqslant \exp(-V(N)\tau(N)\delta(N)^k).$$

Further, since each h_i is of bounded height and degree, Theorem 7.2.7 yields

$$\mathrm{h}(p) \leqslant \tau(L), \quad \deg_{\mathbf{x}}(p) \leqslant \delta(L) \quad (\forall p \in \tilde{\mathcal{F}}_L)$$

for sufficiently large L. Thus, Theorem 9.0.3 yields

$$\mathrm{tr.deg}_{\mathbb{Q}}(\mathbb{Q}(u_1, \ldots, u_d)) \geqslant d.$$

Since g_2, g_3 are algebraic over $\mathbb{Q}$, then $\wp'(z)$ is algebraic over $K(\wp(z))$. Thus,

$$\mathrm{tr.deg}_{\mathbb{Q}}(\mathbb{Q}(u_1, \ldots, u_d)) \leqslant d,$$

and so

$$\mathrm{tr.deg}_{\mathbb{Q}}(\mathbb{Q}(u_1, \ldots, u_d)) = d.$$

In particular, $\{1, \beta, \ldots, \beta^{d-1}\} \cap \Lambda = \varnothing$, or else $\mathrm{tr.deg}_{\mathbb{Q}}(\mathbb{Q}(u_1, \ldots, u_d)) < d$. ∎

Corollary 9.0.5. *Let $\Lambda \subset \mathbb{C}$ be a lattice such that the corresponding elliptic curve has complex multiplication, and such that $g_2(\Lambda), g_3(\Lambda) \in \overline{\mathbb{Q}}$. Then,*

$$\overline{\mathbb{Q}} \cap \Lambda = \{0\}.$$

Proof: Let β be an algebraic integer not in $\mathbb{Z}$. Thus, Theorem 9.0.4 gives that $\beta \notin \Lambda$. Furthermore, it gives that $1 \notin \Lambda$. Now, suppose that $n \in \Lambda$ for some

$n \in \mathbb{Z} \backslash \{1, 0\}$. Then, it follows that $1 \in n^{-1}\Lambda$. To show that this is impossible, note that $\wp(z; n^{-1}\Lambda)$ has invariants

$$g_2(n^{-1}\Lambda) = n^4 g_2 \in \overline{\mathbb{Q}} \quad \text{and} \quad g_3(n^{-1}\Lambda) = n^6 g_3 \in \overline{\mathbb{Q}}.$$

Since $\mathcal{O} \cdot n^{-1}\Lambda \subseteq n^{-1}\Lambda$, then the associated elliptic curve must have complex multiplication. Thus, by Theorem 9.0.4, it follows that $1 \notin n^{-1}\Lambda$, which is a contradiction. Thus, every non-zero algebraic integer is not in Λ. Finally, letting $q \in \overline{\mathbb{Q}}^{\times}$, there exists $D \in \mathbb{N}^{+}$ such that Dq is a non-zero algebraic integer. Thus, $qD \notin \Lambda$ which implies that $q \notin D^{-1}\Lambda \supseteq \Lambda$. Thus, $q \notin \Lambda$. ∎

The main result thus follows immediately from Theorem 9.0.4 and Theorem 3.2.4.

Theorem 9.0.6. *Let $k = \mathbb{Q}(\alpha)$, and let $\beta_1, \ldots, \beta_s \in \overline{\mathbb{Q}}$ be linearly independent over k. Then $\wp(\beta_1), \ldots, \wp(\beta_s)$ are algebraically independent over $\mathbb{Q}$.*

Bibliography

[1] Hartshorne, R. *Algebraic Geometry*, Springer-Verlag, New York, 1997, xxi+496 pp.

[2] Silverman, J. *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986, xii+400 pp.

[3] Abramowitz, M. and Stegun, I. A. *Handbook of Mathematical Functions: with Formulas, Graphs, and Mathematical Tables*, Dover Publications, 1965, 1046 pp.

[4] Koblitz, N. *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, New York, 1984, viii+248 pp.

[5] Waldschmidt, M. *Diophantine Approximation on Linear Algebraic Groups*, Grundlehren 326, Springer-Verlag, 2000, xxiii+633 pp.

[6] Lange, H., Ruppert, W. *Complete systems of addition laws on abelian varieties*, Invent. Math. **79** (1985), 603–610.

[7] Waldschmidt, M. *Transcendance et exponentielles en plusieurs variables*, Invent. Math. **63** (1981), 97–127.

[8] Philippon, P. *Variétés abéliennes et indépendence algébrique II: Un analogue abélien du théorème de Lindemann-Weierstraß*, Invent. Math. **72** (1983), 389–405.

[9] Philippon, P. *Lemmes de zéros dans les groupes algébriques commutatifs*, Bulletin de la S. M. F. **114** (1986), 355–383.

[10] Philippon, P. *Critères pour l'indépendance algébrique*, Centre Mathématique de l'Ecole Polytechnique (1984).

[11] Cartan, H. *Elementary Theory of Analytic Functions of One or Several Complex Variables*, Dover Publications, New York, 1995, 240 pp.

[12] Waldschmidt, M. *Transcendence Methods*, Queen's Papers in Pure and Applied Mathematics **52** (2001), 6.1–6.14.

[13] Chudnovsky, G. *Algebraic Independence of the Values of Elliptic Function at Algebraic Points: Elliptic Analogue of the Lindemann-Weierstrass Theorem* Invent. Math. **61** (1980), 267–290.

[14] Samuel, P. *Algebraic Theory of Numbers*, Dover Publications, New York, 2008, 112 pp.

[15] Baker, A. *Transcendental Number Theory*, Cambridge University Press, New York, 1975, x+147 pp.

[16] Bump, D. *Lie Groups*, Springer Science+Business Media, Inc., New York, 2004, xii+451 pp.