The Dissertation Committee for Paul Arthur Fili
certifies that this is the approved version of the following dissertation:

Orthogonal decompositions of the space of algebraic numbers modulo torsion

Committee:

Jeffrey D. Vaaler, Supervisor

Felipe Voloch

Mirela Ciperiani

David Helm

Clayton Petsche

Orthogonal decompositions of the space of algebraic numbers modulo torsion

by

Paul Arthur Fili, A.B.

DISSERTATION

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

THE UNIVERSITY OF TEXAS AT AUSTIN

May 2010

Acknowledgments

I first wish to thank my advisor, Jeffrey Vaaler, for countless hours of patient and enjoyable mathematical discussion and for introducing me to a wide variety of interesting questions. I wish to thank Clayton Petsche and Felipe Voloch for helpful comments on this thesis and my research in general. I thank my committee for taking the time to review this thesis. I thank Zac and Charles for their friendship and collaboration and Maggie and Tom for their support. Last but certainly not least, I thank my parents for always being so supportive of me and encouraging me in my studies.

Orthogonal decompositions of the space of algebraic numbers modulo torsion

Publication No. _____

Paul Arthur Fili, Ph.D.
The University of Texas at Austin, 2010

Supervisor: Jeffrey D. Vaaler

We introduce decompositions determined by Galois field and degree of the space of algebraic numbers modulo torsion and the space of algebraic points on an elliptic curve over a number field. These decompositions are orthogonal with respect to the natural inner product associated to the L^2 Weil height recently introduced by Allcock and Vaaler in the case of algebraic numbers and the inner product naturally associated to the Néron-Tate canonical height on an elliptic curve. Using these decompositions, we then introduce vector space norms associated to the Mahler measure. For algebraic numbers, we formulate L^p Lehmer conjectures involving lower bounds on these norms and prove that these new conjectures are equivalent to their classical counterparts, specifically, the classical Lehmer conjecture in the $p = 1$ case and the Schinzel-Zassenhaus conjecture in the $p = \infty$ case.

Table of Contents

Acknowledgments **iv**

Abstract **v**

Index of Notation and Terminology viii

Chapter 1. Introduction **1**

1.1 Background 1

1.2 Basic height constructions 4

1.3 The space of algebraic numbers modulo torsion $\mathcal{F}$ 7

1.4 Main results and conjectures 11

1.4.1 Algebraic numbers modulo torsion 11

1.4.2 Algebraic points modulo torsion on elliptic curves 17

Chapter 2. Orthogonal Decompositions **21**

2.1 Galois isometries 21

2.2 Subspaces associated to number fields 24

2.3 Orthogonal projections associated to number fields 27

2.4 Main decomposition theorem 34

2.5 Decomposition by Galois field and proof of Theorem 2 40

2.6 Decomposition by degree and proof of Theorems 3 and 4 . . . 43

Chapter 3. Reducing the Lehmer problem **49**

3.1 Lehmer irreducibility 49

3.2 Reduction to Lehmer irreducible numbers 55

3.3 Projection irreducibility 57

Chapter 4. The Mahler p-norm **59**
4.1 An L^p analogue of Northcott's theorem 59
4.2 The Mahler p-norms and proof of Theorem 6 62
4.3 Explicit values 69
4.3.1 Surds 69
4.3.2 Pisot and Salem numbers 69
4.4 The group Γ and proof of Theorem 7 72
4.5 The Mahler 2-norm and proof of Theorem 9 77

Chapter 5. Decompositions on Elliptic Curves **79**
5.1 Projection operators associated to number fields 79
5.2 Decomposition by Galois field and proof of Theorem 10 85
5.3 Decomposition by degree and proof of Theorems 11 and 12 . . 91
5.4 Open conjectures on elliptic curve constructions 95

Bibliography **99**

Vita **106**

Index of Notation and Terminology

d, minimal degree
  algebraic numbers, 49
  elliptic curves, 95
δ, orbital degree
  algebraic numbers, 43
  elliptic curves, 87

$\mathcal{F}$, space of algebraic numbers modulo torsion, 7

Γ, additive subgroup
  of $\mathcal{F}$, 72
  of V, 97

h, Weil height, 5
$\widehat{h}$, Néron-Tate height on an elliptic curve, 17

$\mathcal{K}$, set of number fields, 7, 80
  properties as a lattice, 24
$\mathcal{K}^G$, set of finite Galois extensions, 7, 80
  properties as a lattice, 24
K_f, minimal field of f, 25
K_ξ, minimal field of ξ on an elliptic curve, 86

$\mathcal{L}$, set of Lehmer irreducible elements
  algebraic numbers, 50
  elliptic curves, 95
L_σ, isometry associated to Galois automorphism σ
  algebraic numbers, 22
  elliptic curves, 80

m, Mahler measure, 5
m_p, L^p Mahler measure, 15
$\|\cdot\|_{m,p}$, Mahler p-norm, 63
$\|\cdot\|_m$, Mahler norm on an elliptic curve, 95

$\mathcal{P}$, projection irreducible elements
  algebraic numbers, 57
  elliptic curves, 97

torsion-free representative, 50

V, vector space of algebraic points of an elliptic curve E modulo torsion, 79

Y, space of algebraic places, 7

Chapter 1

Introduction

1.1 Background

Heights have played an important role in Diophantine geometry since Weil first introduced his height in order to generalize Mordell's theorem (see [BG06] or [HS00] for a general reference on heights and Diophantine geometry). Closely related to the Weil height is the Mahler measure of an algebraic number. Mahler measure is connected to a diverse range of topics, including special values of L-functions [Smy81, Vil99, Lal07], algebraic dynamics [EW99], hyperbolic manifolds [MR03], and growth rates for Coxeter groups and knot theory [GH01].

The central question regarding the Mahler measure is Lehmer's problem, posed by D.H. Lehmer in 1933 [Leh33], which asks if there exist numbers of arbitrarily small Mahler measure. Such numbers necessarily have small height, a subject of interest in itself (see e.g. [Bil97, Zha98, BP05]). It is widely believed that there do not exist numbers of arbitrarily small Mahler measure, and that the minimum value is attained by a particular number discovered by D.H. Lehmer in his 1933 paper [Leh33] (extensive computer searches have revealed no number smaller than Lehmer's number [MRW08, Mos]). Partial

results towards Lehmer's problem exist (major results include [Smy71, Dob79, BDM07]; see [Smy08] for a detailed survey), but the problem remains open. Lehmer's problem has also been extensively studied for algebraic points on elliptic curves defined over number fields using the Néron-Tate canonical height (see [HS90] for the best known current result).

Recently, Allcock and Vaaler [AV09] observed that the absolute logarithmic Weil height can in fact be viewed as the L^1 norm on a certain measure space (Y, λ). The points of Y are the places of $\overline{\mathbb{Q}}$ endowed with a topology which makes Y a totally disconnected locally compact Hausdorff space, and each equivalence class of the algebraic numbers modulo torsion gives rise to a unique, continuous, locally constant real-valued function on Y with compact support. Their work also introduces L^p analogues of the Weil height.

The aim of this thesis is to construct analogous function space norms in order to study the Mahler measure, both on algebraic numbers as well as on elliptic curves. These norms are constructed via the aid of new geometric structure within the space of algebraic numbers modulo torsion (geometry intimately associated to the L^2 norm and the pre-Hilbert space structure on the space of algebraic numbers modulo torsion). Once we have introduced our new norms, we will give a general L^p formulation of the Lehmer conjecture which is equivalent to the classical Lehmer conjecture for $p = 1$ and to the Schinzel-Zassenhaus conjecture [SZ65] for $p = \infty$.

The study of the Mahler measure on the vector space of algebraic numbers modulo torsion presents several difficulties absent for the Weil height,

first of which is that the Mahler measure, unlike the Weil height, is not well-defined modulo torsion. Recent attempts to find topologically better-behaved objects related to the Mahler measure include the introduction of the *metric Mahler measure*, a well-defined metric on $\mathcal{F}$, by Dubickas and Smyth [DS01], and later the introduction of the *ultrametric Mahler measure* by the author and Samuels [FS09] and the introduction of the vector space norms extremal to the Mahler measure by the author and Miner [FMa].

Both the metric and ultrametric Mahler measure induce the discrete topology on the space of algebraic numbers modulo torsion if and only if Lehmer's conjecture is true, so they bear an obvious relevance to the Lehmer problem. These constructions result in metrics that satisfy an extremal property but which are typically difficult to compute explicitly except on special classes of algebraic numbers such as the rational numbers, surds, and Pisot or Salem numbers (even in the case of the rational numbers, the computation of the metric Mahler measure is somewhat nontrivial).

The norms (which we term the "Mahler p-norms") introduced in this thesis, in contrast, induce a vector space topology and so the completions are, typically, Banach spaces, and so techniques from Banach space theory may be brought to bear on these problems. We establish in Theorem 7. p. 16, for example, the existence of an additive subgroup within the space of algebraic numbers modulo torsion which is closed in the Banach space determined by the Mahler p-norm if and only if the L^p Lehmer conjecture (Conjecture 5 below, p. 15) is true.

The Mahler p-norms are constructed with the aid of two new decompositions of the space of algebraic numbers modulo torsion which are orthogonal with respect to the L^2 geometry of the space. As a result, the norms introduced in this thesis tend to be somewhat easier to compute than the metric versions of the Mahler measure since these norms are essentially constructed with the aid of projections associated to certain subspaces. However, explicit computations for algebraic numbers of large degree remain difficult to achieve in the general case.

We note that portions of this thesis have been submitted for publication in a paper of the author and Miner [FMb].

Before we give precise statements of the results of this thesis in Section 1.4 below, we begin by reviewing the constructions and main conjectures surrounding Lehmer's problem and the space of algebraic numbers modulo torsion.

1.2 Basic height constructions

Let us begin by recalling the definition of the Weil height and the Mahler measure. Let K be a number field and let M_K denote the set of places of K (recall that a *place* of a field K is an equivalence class of a nontrivial absolute value, where two absolute values on K are considered equivalent if they induce the same topology on K). We say that a place v of K *lies over* the place p of $\mathbb{Q}$, denoted $v|p$, if there exists an absolute value in the equivalence class of v which restricts to $\mathbb{Q}$ to give an absolute value in the class of p. For

each $v \in M_K$ lying over the rational place p, let $\|\cdot\|_v$ be the particular absolute value on K extending the usual p-adic absolute value on $\mathbb{Q}$ if v is finite or the usual archimedean absolute value if v is infinite. Then for $\alpha \in K^\times$, the *absolute logarithmic Weil height* h is given by

$$h(\alpha) = \sum_{v \in M_K} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log^+ \|\alpha\|_v \tag{1.2.1}$$

where $\log^+ t = \max\{0, \log t\}$. By the degree extension formula, which tells us that for any finite extension L/K and place $v \in M_K$ we have

$$\sum_{\substack{w \in M_L \\ w|v}} \frac{[L_w : \mathbb{Q}_w]}{[L : \mathbb{Q}]} = \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]}, \tag{1.2.2}$$

we see that the expression on the right hand side of this equation does not depend on the choice of field K containing α. The Weil height h is thus a well-defined function mapping $\overline{\mathbb{Q}}^\times \to [0, \infty)$ which vanishes precisely on the roots of unity, $\mathrm{Tor}(\overline{\mathbb{Q}}^\times)$.

The *logarithmic Mahler measure* of an algebraic number α is defined to be

$$m(\alpha) = (\deg \alpha) \cdot h(\alpha) \tag{1.2.3}$$

where $\deg \alpha = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. The Mahler measure is often studied for polynomials $f \in \mathbb{C}[x]$, and is defined as

$$M(f) = \exp\left(\int_0^1 \log|f(e^{2\pi i t})| \, dt \right).$$

The Mahler measure is multiplicative, in the sense given $f, g \in \mathbb{C}[x]$, we have

$$M(fg) = M(f)M(g).$$

Thus, if we restrict our attention to polynomials with rational integral coefficients (the case typically of interest in applications to number theory), then it suffices to consider the value of the Mahler measure on irreducible polynomials $f \in \mathbb{Z}[x]$. Such a polynomial $f \in \mathbb{Z}[x]$ is therefore the minimal polynomial of an algebraic number α, and in fact, it is not difficult to show via Jensen's theorem that

$$\log M(f) = m(\alpha).$$

Thus, the study of bounding the Mahler measure of polynomials with rational integral coefficients is equivalent to bounding the Mahler measure of algebraic numbers.

Though related to the Weil height in a simple fashion, the Mahler measure exhibits rather more erratic and mysterious behavior because of its dependence on the degree of the number over the field of rationals. The question of the existence of algebraic numbers of arbitrarily small Mahler measure is called *Lehmer's problem*. The question was first posed in 1933 by D.H. Lehmer [Leh33] and since then the conjectured existence of an absolute lower bound away from zero has come to be known as *Lehmer's conjecture*:

Conjecture 1 (Lehmer's conjecture)**.** *There exists an absolute constant c such that*

$$m(\alpha) \geq c > 0 \quad \textit{for all} \quad \alpha \in \overline{\mathbb{Q}}^{\times} \setminus \mathrm{Tor}(\overline{\mathbb{Q}}^{\times}). \tag{1.2.4}$$

The current best known lower bound, due to Dobrowolski [Dob79], is of the

form

$$m(\alpha) \gg \left(\frac{\log\log\deg\alpha}{\log\deg\alpha}\right)^3 \quad \text{for all} \quad \alpha \in \overline{\mathbb{Q}}^\times \setminus \mathrm{Tor}(\overline{\mathbb{Q}}^\times)$$

where the implied constant is absolute.

1.3 The space of algebraic numbers modulo torsion $\mathcal{F}$

We will here recall the constructions of [AV09] which we will use throughout this thesis. For proofs of the assertions given here we refer the reader to [AV09]. We fix once and for all our algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and let $\mathcal{K}$ denote the set of finite extensions of $\mathbb{Q}$. Let $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group, and let

$$\mathcal{K}^G = \{K \in \mathcal{K} : \sigma K = K \text{ for all } \sigma \in G\}$$

denote the collection of finite Galois extensions of $\mathbb{Q}$.

Let Y denote the set of places of $\overline{\mathbb{Q}}$, that is, the set of nontrivial absolute values on $\overline{\mathbb{Q}}$ modulo equivalence. For any $K \in \mathcal{K}$, let M_K denote the set of places of K, endowed with the discrete topology. Observe that, as a set,

$$Y = \varprojlim_{K\in\mathcal{K}} M_K = \varprojlim_{K\in\mathcal{K}^G} M_K \tag{1.3.1}$$

where the second equality follows from the fact that the collection $\mathcal{K}^G$ is cofinal in the collection $\mathcal{K}$ as each $K \in \mathcal{K}$ is contained in its Galois closure, which is also a finite extension and thus in $\mathcal{K}^G$. We will take our limits over $\mathcal{K}^G$ in general as this allows us to keep track of the Galois action on places (we will discuss the action on places more explicitly at the start of Chapter 2). We

endow Y with the inverse limit topology and claim that Y is a locally compact Hausdorff space. Let $M_{K,p} = \{v \in M_K : v|p\}$ where p is a rational prime. Each $M_{K,p}$ is a finite set which we also endow with the discrete topology. Then we let

$$Y(\mathbb{Q}, p) = \varprojlim_{K \in \mathcal{K}^G} M_{K,p}. \tag{1.3.2}$$

be the usual profinite limit, and thus $Y(\mathbb{Q}, p)$ is a totally disconnected compact Hausdorff space which is a subspace of Y. In fact, it is not hard to see that the space Y is the disjoint union

$$Y = \bigcup_{p \in M_{\mathbb{Q}}} Y(\mathbb{Q}, p), \tag{1.3.3}$$

and in particular $Y(\mathbb{Q}, p)$ is a compact open set. Thus we have endowed the set Y of places of $\overline{\mathbb{Q}}$ with a topology which makes it a totally disconnected, locally compact, and Hausdorff space. A basis for the topology of Y is given by compact open sets of the form

$$Y(K, v) = \{y \in Y : y|v\}, \quad \text{where} \quad K \in \mathcal{K} \text{ and } v \in M_K. \tag{1.3.4}$$

In fact, the subcollection $\{Y(K, v) : K^G \in \mathcal{K} \text{ and } v \in M_K\}$ forms another basis for the topology of Y, as if $v \in M_K$ and $K \in \mathcal{K}$, then $K \subset L$ for some $L \in \mathcal{K}^G$, and

$$Y(K, v) = \bigcup_{\substack{w \in M_L \\ w|v}} Y(L, w)$$

as a disjoint union.

To each equivalence class α in $\overline{\mathbb{Q}}^\times / \operatorname{Tor}(\overline{\mathbb{Q}}^\times)$, we can uniquely associate the function $f_\alpha : Y \to \mathbb{R}$ (we will often drop the subscript α when convenient) given by

$$f_\alpha(y) = \log \|\alpha\|_y,$$

where the absolute value $\|\cdot\|_y$ is normalized as above. In the topology of Y, such a function has finite support and is locally constant and continuous. Let us denote the collection of continuous real-valued functions on Y with compact support by $C_c(Y)$. Then the map

$$\begin{aligned} \overline{\mathbb{Q}}^\times / \operatorname{Tor}(\overline{\mathbb{Q}}^\times) &\to C_c(Y) \\ \alpha \operatorname{Tor}(\overline{\mathbb{Q}}^\times) &\mapsto (f_\alpha : Y \to \mathbb{R}) \end{aligned}$$

is in fact a vector space isomorphism, that is:

1. $f_\alpha(y) + f_\beta(y) = f_{\alpha\beta}(y)$ for all $\alpha, \beta \in \overline{\mathbb{Q}}^\times / \operatorname{Tor}(\overline{\mathbb{Q}}^\times)$ and $y \in Y$,
2. $r f_\alpha(y) = f_{\alpha^r}(y)$ for all $r \in \mathbb{Q}$ and $\alpha \in \overline{\mathbb{Q}}^\times / \operatorname{Tor}(\overline{\mathbb{Q}}^\times)$, and
3. $f_\alpha(y) = 0$ for all $y \in Y$ if and only if $\alpha \in \operatorname{Tor}(\overline{\mathbb{Q}}^\times)$ (Kronecker's theorem).

We denote the image of this map, which we thereby identify with the space of algebraic numbers modulo torsion, by $\mathcal{F}$. Specifically,

$$\mathcal{F} = \{f_\alpha \in C_c(Y) : \alpha \in \overline{\mathbb{Q}}^\times / \operatorname{Tor}(\overline{\mathbb{Q}}^\times)\}. \tag{1.3.5}$$

Notice that, as was the case for $\overline{\mathbb{Q}}^\times / \operatorname{Tor}(\overline{\mathbb{Q}}^\times)$, the space $\mathcal{F}$ is a vector space over the rationals $\mathbb{Q}$.

Allcock and Vaaler [AV09, Theorem 4] prove the existence of a Borel measure λ on the space Y which satisfies

$$\lambda(Y(K,v)) = \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]}. \tag{1.3.6}$$

If $\alpha \in K^\times$, then the function $f_\alpha(y)$ is constant on the sets $Y(K,v) = \{y \in Y : y|v\}$ for $v \in M_K$ and takes the value $\log \|\alpha\|_v$. Therefore we have

$$\|f_\alpha\|_1 = \int_Y |f_\alpha(y)|\, d\lambda(y) = \sum_{v \in M_K} |\log \|\alpha\|_v| \, \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} = 2\, h(\alpha),$$

where the last equality follows from the general fact that if for some finite set of real numbers $\{a_n\}$ we have $\sum_n a_n = 0$, then $\sum_n |a_n| = 2 \sum_n \max\{a_n, 0\}$. In this formulation, the product formula now takes the form

$$\int_Y f_\alpha \, d\lambda = 0. \tag{1.3.7}$$

We also have a well-defined inner product on $\mathcal{F}$ given by

$$\langle f, g \rangle = \int_Y f(y) g(y)\, d\lambda(y)$$

which satisfies $\|f\|_2 = \langle f, f \rangle^{1/2}$. As we noted above, the geometry of the space $\mathcal{F}$ will play a significant role in our study.

Remark 1.3.1 (Note on the choice of base field). Before we continue let us remark that while we choose $\mathbb{Q}$ to be our base field because of its relevance to Lehmer's problem, any number field $k/\mathbb{Q}$ could serve just as well and the proofs would not change substantially as is discussed in [AV09]. When dealing with elliptic curves in Chapter 5, however, we shall work over a number field k.

1.4 Main results and conjectures

Our constructions and ideas can be applied to both the space of algebraic numbers modulo torsion as well as the space of algebraic points on an elliptic curve modulo torsion. We begin with the problem for algebraic numbers modulo torsion and then discuss our results on the generalization of these techniques to elliptic curves.

1.4.1 Algebraic numbers modulo torsion

In order to construct our norms related to the Mahler measure, we first construct an orthogonal decomposition of the space $\mathcal{F}$ of algebraic numbers modulo torsion. Let V_K denote the $\mathbb{Q}$-vector space span of the functions given by

$$V_K = \operatorname{span}_{\mathbb{Q}}\langle\{f_\alpha : \alpha \in K^\times / \operatorname{Tor}(K^\times)\}\rangle.$$

We first prove the following result which gives the orthogonal decomposition by Galois field:

Theorem 2. *There exist projection operators $T_K : \mathcal{F} \to \mathcal{F}$ for each $K \in \mathcal{K}^G$ such that $T_K(\mathcal{F}) \subset V_K$, $T_K(\mathcal{F}) \perp T_L(\mathcal{F})$ for all $K \neq L \in \mathcal{K}^G$ with respect to the inner product on $\mathcal{F}$, and*

$$\mathcal{F} = \bigoplus_{K \in \mathcal{K}^G} T_K(\mathcal{F}).$$

The notation $\mathcal{F} = \bigoplus_{K\in\mathcal{K}^G} T_K(\mathcal{F})$ indicates a direct sum in the usual $\mathbb{Q}$-vector space sense, specifically, that every element of the $\mathbb{Q}$-vector space $\mathcal{F}$ is uniquely

expressible as a finite sum of elements from the $\mathbb{Q}$-vector spaces $T_K(\mathcal{F})$ as K ranges over the set $\mathcal{K}^G$.

In particular, it follows from Theorem 2 that the projection operators T_K are orthogonal projections with respect to the inner product on $\mathcal{F}$, and thus in the completion with respect to the L^2 norm, this gives a Hilbert space decomposition in the usual sense of a Hilbert space direct sum (in which each element of the Hilbert space has a unique expansion as a series of vectors, one from each summand).

It is interesting to note what this decomposition implies, and why in particular we cannot have a decomposition along the set of all number fields $\mathcal{K}$ rather than all finite Galois extensions $\mathcal{K}^G$. Conjugate number fields exhibit a linear dependence which arises from the conjugacy of elements in those fields. Suppose for example that $\alpha \in \overline{\mathbb{Q}}^\times$ was a cubic algebraic unit with nonsquare discriminant, with conjugates β, γ. The fields $\mathbb{Q}(\alpha), \mathbb{Q}(\beta)$ and $\mathbb{Q}(\gamma)$ (and thus the corresponding vector spaces $V_{\mathbb{Q}(\alpha)}$, etc.) would all be distinct. However, the relation

$$\alpha\beta\gamma = \pm 1 \quad \text{implies that} \quad f_\alpha + f_\beta + f_\gamma = 0.$$

In fact, it is not hard to see (Remark 2.5.2, p. 42) that

$$V_{\mathbb{Q}(\alpha)} + V_{\mathbb{Q}(\beta)} = V_{\mathbb{Q}(\alpha)} + V_{\mathbb{Q}(\beta)} + V_{\mathbb{Q}(\gamma)}.$$

Thus any attempt to determine a unique orthogonal decomposition amongst these three subspaces, which assigns to an algebraic number modulo torsion

its unique component arising from each field, would be impossible. Our result above demonstrates that this is the *only* obstruction to such a decomposition.

A decomposition by Galois field alone, however, does not give enough information about the degree of a specific number in order to bound the Mahler measure of the number, as in general a number of degree n may lie in a Galois field of degree $n!$. We therefore define the vector subspace

$$V^{(n)} = \sum_{\substack{K \in \mathcal{K} \\ [K:\mathbb{Q}] \leq n}} V_K$$

(where the sum indicates a usual sum of $\mathbb{Q}$-vector spaces) and determine the following decomposition:

Theorem 3. *There exist projections $T^{(n)} : \mathcal{F} \to \mathcal{F}$ for each $n \in \mathbb{N}$ such that $T^{(n)}(\mathcal{F}) \subset V^{(n)}$, $T^{(m)}(\mathcal{F}) \perp T^{(n)}(\mathcal{F})$ for all $m \neq n$, and*

$$\mathcal{F} = \bigoplus_{n=1}^{\infty} T^{(n)}(\mathcal{F}).$$

These decompositions are independent of each other in the following sense:

Theorem 4. *The projections T_K and $T^{(n)}$ commute with each other for each $K \in \mathcal{K}^G$ and $n \in \mathbb{N}$.*

In particular, as a result of commutativity, we can form projections $T_K^{(n)} = T_K T^{(n)}$ and so we have an orthogonal decomposition

$$\mathcal{F} = \bigoplus_{n=1}^{\infty} \bigoplus_{K \in \mathcal{K}^G} T_K^{(n)}(\mathcal{F}).$$

Again, when we pass to the completion in the L^2 norm, the projections extend by continuity and the above decomposition extends to the respective closures and the direct sum becomes a direct sum in the usual Hilbert space sense.

This geometric structure within the algebraic numbers allows us to define linear operators, for all L^p norms with $1 \leq p \leq \infty$, which capture the contribution of the degree to the Mahler measure in such a way that we can define our Mahler norms. Specifically, we define the operator

$$\begin{aligned} M : \mathcal{F} &\to \mathcal{F} \\ f &\mapsto \sum_{n=1}^{\infty} n\, T^{(n)} f. \end{aligned}$$

The sum is finite for each $f \in \mathcal{F}$. M is a well-defined, unbounded (in any L^p norm, $1 \leq p \leq \infty$), invertible linear map defined on the incomplete vector space $\mathcal{F}$. We define the *Mahler p-norm* on $\mathcal{F}$ for $1 \leq p \leq \infty$ to be

$$\|f\|_{m,p} = \|Mf\|_p$$

where $\|\cdot\|_p$ denotes the usual L^p norm on the incomplete vector space $\mathcal{F}$. The Mahler p-norm is, in fact, a well-defined vector space norm on $\mathcal{F}$, and hence the completion $\mathcal{F}_{m,p}$ with respect to $\|\cdot\|_{m,p}$ is a Banach space.

In order to see that these norms form a suitable generalization of the Mahler measure of algebraic numbers, we will show that the Lehmer conjecture can be reformulated in terms of these norms. First, let us address what form the Lehmer conjecture takes inside $\mathcal{F}$. For any $\alpha \in \overline{\mathbb{Q}}^{\times}$, let $h_p(\alpha) = \|f_\alpha\|_p$. We formulate:

Conjecture 5 (L^p Lehmer conjectures)**.** *For $1 \leq p \leq \infty$, there exists an absolute constant c_p such that the L^p Mahler measure m_p satisfies the following equation:*

$$m_p(\alpha) = (\deg \alpha) \cdot h_p(\alpha) \geq c_p > 0 \quad \textit{for all} \quad \alpha \in \overline{\mathbb{Q}}^\times \setminus \mathrm{Tor}(\overline{\mathbb{Q}}^\times). \qquad (*_p)$$

From the fact that $h_1(\alpha) = 2h(\alpha)$ it is clear that when $p = 1$ this statement is equivalent to the Lehmer conjecture. For $p = \infty$, we will show in Proposition 4.2.4, p. 68 below that the statement is equivalent to the Schinzel-Zassenhaus conjecture.

In order to translate the Lehmer conjecture into a bound on function space norms which, unlike the metric Mahler measure, cannot possibly be discrete, it is necessary to reduce the Lehmer problem to a sufficiently small set of numbers which we can expect to be bounded away from zero in norm. This requires the introduction in Chapter 3 of two classes of algebraic numbers modulo torsion in $\mathcal{F}$, the *Lehmer irreducible* elements $\mathcal{L}$ and the *projection irreducible elements* $\mathcal{P}$. Let $\mathcal{U} \subset \mathcal{F}$ denote the subspace of algebraic units. Then we prove the following theorem:

Theorem 6. *For each $1 \leq p \leq \infty$, equation $(*_p)$ holds if and only if*

$$\|f\|_{m,p} \geq c_p > 0 \quad \textit{for all} \quad 0 \neq f \in \mathcal{L} \cap \mathcal{P} \cap \mathcal{U} \qquad (**_p)$$

where $\mathcal{L}$ denotes the set of Lehmer irreducible elements, $\mathcal{P}$ the set of projection irreducible elements, and $\mathcal{U}$ the subspace of algebraic units. Further, for $1 \leq p \leq q \leq \infty$, if $(**_p)$ holds then $(**_q)$ holds as well.

The last statement of the theorem, which is proven by reducing to a place of measure 1 and applying the usual inequality for the L^p and L^q norms on a probability space, generalizes the well-known fact that Lehmer's conjecture implies the conjecture of Schinzel-Zassenhaus.

Let $\mathcal{U}_{m,p}$ denote the Banach space which is the completion of the vector space $\mathcal{U}$ of units with respect to the Mahler p-norm $\|\cdot\|_{m,p}$. The set $\mathcal{L} \cap \mathcal{P} \cap \mathcal{U}$ has another useful property which we will prove, namely, that the additive subgroup it generates contains a subgroup $\Gamma = \Gamma_p$,

$$\Gamma \leq \langle \mathcal{L} \cap \mathcal{P} \cap \mathcal{U} \rangle,$$

which is also a set of equivalence for the Lehmer conjecture, that is, we will show that the L^p Lehmer conjecture $(*_p)$ is equivalent to the condition that Γ be a discrete subgroup in $\mathcal{U}_{m,p}$. Specifically, we prove:

Theorem 7. *Equation $(*_p)$ holds if and only if the additive subgroup $\Gamma \subset \mathcal{U}_{m,p}$ is closed.*

This leads us to a new conjecture, equivalent to $(*_p)$ for each $1 \leq p \leq \infty$:

Conjecture 8. *The additive subgroup $\Gamma \subset \mathcal{U}_{m,p}$ is closed for each $1 \leq p \leq \infty$.*

Lastly, the presence of orthogonal decompositions raises a particular interest in the study of the L^2 norm. In this case, the norm associated to the Mahler measure has a particularly simple form which is in sympathy with the geometry of L^2.

Theorem 9. *The Mahler 2-norm satisfies*

$$\|f\|_{m,2}^2 = \sum_{n=1}^{\infty} n^2 \, \|T^{(n)}(f)\|_2^2 = \sum_{K \in \mathcal{K}^G} \sum_{n=1}^{\infty} n^2 \, \|T_K^{(n)}(f)\|_2^2.$$

Further, the Mahler 2-norm arises from the inner product

$$\langle f, g \rangle_m = \langle Mf, Mg \rangle = \sum_{n=1}^{\infty} n^2 \, \langle T^{(n)} f, T^{(n)} g \rangle = \sum_{K \in \mathcal{K}^G} \sum_{n=1}^{\infty} n^2 \, \langle T_K^{(n)} f, T_K^{(n)} g \rangle$$

where $\langle f, g \rangle = \int_Y fg \, d\lambda$ *denotes the usual inner product in* $L^2(Y)$*, and therefore the completion* $\mathcal{F}_{m,2}$ *of* $\mathcal{F}$ *with respect to the Mahler 2-norm is a Hilbert space.*

1.4.2 Algebraic points modulo torsion on elliptic curves

Let us consider now the case of an elliptic curve E defined over a number field k. Let $\widehat{h} : E(\overline{k}) \to [0, \infty)$ denote the canonical Néron-Tate height on E, which is well-known to be a positive definite quadratic form on the finitely generated abelian group $E(K)/E_{\mathrm{tor}}(K)$ for all finite extensions K/k. Observe further that the abelian group

$$V = E(\overline{k})/E_{\mathrm{tor}}(\overline{k})$$

is divisible and torsion-free, and so V is in fact a vector space over the rational numbers $\mathbb{Q}$, and $\widehat{h}$ is a positive definite quadratic form on V. Since $\widehat{h}$ is a positive-definite quadratic form on V it defines an inner product $\langle \cdot, \cdot \rangle : E \to [0, \infty)$ and thus a vector space norm $\|\xi\| = \langle \xi, \xi \rangle^{1/2} = \sqrt{\widehat{h}(\xi)}$ on V. Let $G = \mathrm{Gal}(\overline{k}/k)$ and recall that G has a well-defined action $G \times V \to V$, which we will denote by $(\sigma, \xi) \mapsto \sigma(\xi)$ for $\xi \in V$ and $\sigma \in G$.

We now think of V as a pre-Hilbert space with norm $\|\cdot\|$. Let $\mathcal{K}$ denote the set (in fact, the lattice) of algebraic extensions of k, partially ordered by inclusion. Let $\mathcal{K}^G$ denote the sublattice of $\mathcal{K}$ given by finite normal extensions of k. For each $K \in \mathcal{K}$ we have a natural subspace

$$V_K = \mathrm{span}_{\mathbb{Q}}\langle E(K)/E_{\mathrm{tor}}(K)\rangle = E(K)/E_{\mathrm{tor}}(K) \otimes \mathbb{Q} \subset V.$$

Our main theorems regarding the space of algebraic points modulo torsion on an elliptic curve are the following:

Theorem 10. *For each $K \in \mathcal{K}^G$ there exists a continuous projection $T_K : V \to V$ such that the space V has an orthogonal direct sum decomposition into vector subspaces*

$$V = \bigoplus_{K \in \mathcal{K}^G} T_K(V)$$

and $T_K(V) \subset V_K$ for each K.

Again, as the decomposition by Galois degree is not quite fine enough, we define a decomposition using the "degree n" subspaces

$$V^{(n)} = \sum_{\substack{K \in \mathcal{K} \\ [K:k] \leq n}} V_K.$$

Theorem 11. *For each $n \in \mathbb{N}$ there exists a continuous projection $T^{(n)} : V \to V$ such that the space V has an orthogonal direct sum decomposition into vector subspaces*

$$V = \bigoplus_{n=1}^{\infty} T^{(n)}(V)$$

and $T^{(n)}(V) \subset V^{(n)}$ for each n.

Exactly as before, the points of the subspaces $T^{(n)}(V)$ consist of points which can be written as a sum of elements all arising from subspace V_K with K precisely a degree n extension of k and no lower. These decompositions are again compatible in the sense that:

Theorem 12. *The projections T_K and $T^{(n)}$ commute with each other for each $K \in \mathcal{K}^G$ and $n \in \mathbb{N}$.*

In particular, as a result of commutativity, we can form projections $T_K^{(n)} = T_K T^{(n)}$ and so we have an orthogonal decomposition

$$V = \bigoplus_{n=1}^{\infty} \bigoplus_{K \in \mathcal{K}^G} T_K^{(n)}(V).$$

This allows us to define a "degree decomposition" and therefore a Mahler norm $\| \cdot \|_m : V \to [0, \infty)$ on the vector space V via:

$$\|\xi\|_m = \|M\xi\| \quad \text{where} \quad M = \sum_{n=1}^{\infty} \sqrt{n} \cdot T^{(n)}.$$

We now recall Lehmer's conjecture for elliptic curves:

Conjecture 13 (Lehmer conjecture for Elliptic Curves)**.** *Given an elliptic curve E/k there exists a constant $C > 0$ such that*

$$\|P\|^2 = \widehat{h}(P) \geq \frac{C}{D(P)} \quad \textit{for all} \quad P \in E(\overline{k}) \setminus E_{\mathrm{tor}}(\overline{k}), \tag{1.4.1}$$

where $D(P) = [k(P) : k]$ is the degree of P.

The Lehmer conjecture for elliptic curves remains open (a survey of best known results can be found in [Sil07, §3.4]). In Chapter 5 we construct a

subgroup $\Gamma = \Gamma_E \leq \langle \mathcal{L} \cap \mathcal{P} \rangle$, where $\mathcal{L}$ denotes the Lehmer irreducible elements and $\mathcal{P}$ the projection irreducible elements of V, in analogy with Theorem 7 above. This leads to a new conjecture regarding the subgroup Γ within the completion of V with respect to the norm $\|\cdot\|_m$, which we will denote V_m:

Conjecture 14. *Let E/k be an elliptic curve defined over a number field k and let $V = E(\overline{k})/E_{\text{tor}}$ and V_m its completion with respect to $\|\cdot\|_m$, as above. Then the subgroup Γ from Conjecture 13 is closed in the Hilbert space V_m.*

We expect that the above conjecture and the Lehmer conjecture for E/k are equivalent, however, as we will discuss in Chapter 5, there are several questions which prove more difficult for elliptic curves than for algebraic numbers.

The layout of this thesis is as follows. In Chapter 2 we introduce the basic operators and subspaces of our study, namely, those arising naturally from number fields and Galois isomorphisms. The proofs of Theorems 2, 3 and 4 regarding the orthogonal decompositions of the space $\mathcal{F}$ with respect to Galois field and degree will then be carried out in Sections 2.4, 2.5, and 2.6. In Chapter 3 we prove our results regarding the reduction of the classical Lehmer problem and introduce the relevant classes of algebraic numbers which are essential to our theorems. In Chapter 4 we introduce the Mahler p-norms and prove Theorems 6, 7, and 9. In Chapter 5 we apply our constructions to elliptic curves and prove Theorems 10, 11, and 12.

Chapter 2

Orthogonal Decompositions

2.1 Galois isometries

Let $\mathcal{F}_p$ denote the completion of $\mathcal{F}$ with respect to the L^p norm. By [AV09, Theorems 1-3],

$$\mathcal{F}_p = \begin{cases} \{f \in L^1(Y,\lambda) : \int_Y f\, d\lambda = 0\} & \text{if } p = 1 \\ L^p(Y,\lambda) & \text{if } 1 < p < \infty \\ C_0(Y,\lambda) & \text{if } p = \infty. \end{cases}$$

We begin by introducing our first class of operators, the isometries arising from Galois automorphisms. Let us recall how the Galois group acts on the places of an arbitrary Galois extension K. Suppose $\alpha \in K$, $v \in M_K$ is a place of K, and $\sigma \in G$. We define σv to be the place of K given by $\|\alpha\|_{\sigma v} = \|\sigma^{-1}\alpha\|_v$, or in other words, $\|\sigma\alpha\|_v = \|\alpha\|_{\sigma^{-1}v}$.

Lemma 2.1.1. *Each $\sigma \in G$ is a measure-preserving homeomorphism of the measure space (Y, λ).*

Proof. That the map $\sigma : Y \to Y$ is a well-defined bijection follows from the fact that G gives a well-defined group action. Continuity of σ and σ^{-1} follow from [AV09, Lemma 3]. It remains to show that σ is measure-preserving, but this follows immediately from [AV09, (4.6)]. □

In accordance with the action on places, we define for $\sigma \in G$ the operator

$$L_\sigma : \mathcal{F}_p \to \mathcal{F}_p$$

given by

$$(L_\sigma f)(y) = f(\sigma^{-1} y). \tag{2.1.1}$$

Thus for $f_\alpha \in \mathcal{F}$, we have $L_\sigma f_\alpha = f_{\sigma\alpha}$, and in particular $L_\sigma(\mathcal{F}) \subseteq \mathcal{F}$ for all $\sigma \in G$. Further, by our definition of the action on places, we have $L_\sigma L_\tau = L_{\sigma\tau}$.

Let $\mathcal{B}(\mathcal{F}_p)$ denote the bounded linear maps from $\mathcal{F}_p$ to itself, and let $\mathcal{I}(\mathcal{F}_p) \subset \mathcal{B}(\mathcal{F}_p)$ denote the subgroup of isometries of $\mathcal{F}_p$. By the construction of λ, each $\sigma \in G$ is a measure-preserving topological homeomorphism of the space of places Y, so it follows immediately that L_σ is an isometry for all $1 \leq p \leq \infty$, that is, $\|L_\sigma f\|_p = \|f\|_p$ for all $\sigma \in G$. Thus we have a natural map

$$\rho : G \to \mathcal{I}(\mathcal{F}_p)$$

$$\sigma \mapsto L_\sigma$$

where $(L_\sigma f)(y) = f(\sigma^{-1} y)$. We will show that ρ gives an injective infinite-dimensional representation of the absolute Galois group (which is unitary in the case of L^2) and furthermore that the map ρ is continuous if G is endowed with its natural profinite topology and $\mathcal{I}$ is endowed with the strong operator topology inherited from $\mathcal{B}(\mathcal{F}_p)$. Recall that the strong operator topology, which is weaker than the norm topology, is the weakest topology such that the evaluation maps $A \mapsto \|Af\|_p$ are continuous for every $f \in L^p$.

Proposition 2.1.2. *The map $\rho : G \to \mathcal{I}$ is injective, and it is continuous if $\mathcal{I}$ is endowed with the strong operator topology and G has the usual profinite topology.*

Proof. First we will observe that the image $\rho(G)$ is discrete in the norm topology so that ρ is injective. To see this, fix $\sigma \neq \tau \in G$, so that there exists some finite Galois extension K and an element $\alpha \in K^\times$ such that $\sigma\alpha \neq \tau\alpha$. By [Dub05, Theorem 3], we can find a rational integer n such that $\beta = n + \alpha$ is torsion-free, that is, if $\beta/\beta' \neq 1$ then $\beta/\beta' \notin \mathrm{Tor}(\overline{\mathbb{Q}}^\times)$ for any conjugate β' of β, and in particular, the conjugates of β give rise to distinct functions in $\mathcal{F}$. Thus $L_\sigma f_\beta \neq L_\tau f_\beta$, so there exists some place v of K such that $\sigma(Y(K,v)) \neq \tau(Y(K,v))$ and are therefore disjoint sets. Choose a Galois extension L/K with distinct places $w_1, w_2 | v$. Since L/K is Galois, the local degrees agree and so $\lambda(Y(L,w_1)) = \lambda(Y(L,w_2))$ by [AV09, Theorem 5]. Define

$$f(y) = \begin{cases} 1 & \text{if } y \in Y(L,w_1) \\ -1 & \text{if } y \in Y(L,w_2) \\ 0 & \text{otherwise.} \end{cases}$$

Clearly $f \in \mathcal{F}_p$ for all $1 \leq p \leq \infty$ and $L_\sigma f$ and $L_\tau f$ have disjoint support. Thus,

$$\|(L_\sigma - L_\tau)f\|_p = \left(\|L_\sigma f\|_p^p + \|L_\tau f\|_p^p\right)^{1/p} = 2^{1/p}\|f\|_p$$

(where we let $2^{1/p} = 1$ when $p = \infty$). But this implies that $1 \leq 2^{1/p} \leq \|L_\sigma - L_\tau\|$ for all $\sigma \neq \tau \in G$, and thus the image $\rho(G)$ is discrete in the norm topology of $\mathcal{I}$, and ρ is injective.

Let us now prove continuity. Recall that a basis for the strong operator topology on $\mathcal{I}$ is given by sets of the form

$$U = \{A \in \mathcal{I} : \|(A - B)f_i\| < \epsilon \text{ for all } 1 \leq i \leq k\}$$

where $B \in \mathcal{I}$, $f_1, \ldots, f_k$ is a finite set of functions in $\mathcal{F}_p$, and $\epsilon > 0$. Fix such an open set U for a given $B = L_\sigma$ for some $\sigma \in G$. Approximate each f_i by an element $g_i \in \mathcal{F}$ such that $\|f_i - g_i\|_p < \epsilon/2^{1/p}$. Let V_K be a subspace of $\mathcal{F}$ containing $g_1, \ldots, g_k$. Let

$$N = \{\tau \in G : \sigma|_K = \tau|_K\}.$$

Then N is an open subset of G in the profinite topology. We claim that $\rho(N) \subseteq U$, and thus that ρ is continuous. To see this, observe that for $\tau \in N$,

$$\begin{aligned}\|(L_\tau - L_\sigma)f_i\|_p &\leq \|(L_\tau - L_\sigma)g_i\|_p + \|(L_\tau - L_\sigma)(f_i - g_i)\|_p \\ &< \|(L_\tau - L_\sigma)g_i\|_p + 2^{1/p} \cdot \epsilon/2^{1/p} = \epsilon\end{aligned}$$

where $\|(L_\tau - L_\sigma)g_i\|_p = 0$ because $g_i \in V_K$, and thus is locally constant on the sets $Y(K, v)$ for v a place of K, and $\tau \in N$ implies that σ and τ agree on K, so $L_\tau g_i = L_\sigma g_i$. □

2.2 Subspaces associated to number fields

We will now prove some lemmas regarding the relationship between the spaces V_K and the Galois group. As in the introduction, let us define

$$\mathcal{K} = \{K/\mathbb{Q} : [K : \mathbb{Q}] < \infty\} \quad \text{and} \quad \mathcal{K}^G = \{K \in \mathcal{K} : \sigma K = K \ \forall \sigma \in G\}.$$

As we shall have occasion to use them, let us recall the combinatorial properties of the sets $\mathcal{K}$ and $\mathcal{K}^G$ partially ordered by inclusion. Recall that $\mathcal{K}$ and $\mathcal{K}^G$ are *lattices*, that is, partially ordered sets for which any two elements have a unique greatest lower bound called the *meet* and a unique least upper bound called the *join*. Specfically, for any two fields K, L, the meet $K \wedge L$ is given by $K \cap L$ and the join $K \vee L$ is given by KL. If K, L are Galois then both the meet (the intersection) and the join (the compositum) are Galois as well, thus $\mathcal{K}^G$ is a lattice as well. Both lattices have a minimal element, namely $\mathbb{Q}$, and are *locally finite*, that is, between any two fixed elements we have a finite number of intermediate elements.

For each $K \in \mathcal{K}$, let

$$V_K = \mathrm{span}_{\mathbb{Q}}\langle\{f_\alpha : \alpha \in K^\times / \operatorname{Tor}(K^\times)\}\rangle. \tag{2.2.1}$$

Then V_K is the subspace of $\mathcal{F}$ spanned by the functions arising from numbers of K. Suppose we fix a class of an algebraic number modulo torsion $f \in \mathcal{F}$. Then the set

$$\{K \in \mathcal{K} : f \in V_K\}$$

forms a sublattice of $\mathcal{K}$, and by the finiteness properties of $\mathcal{K}$ this set must contain a unique minimal element.

Definition 2.2.1. For any $f \in \mathcal{F}$, the *minimal field* is defined to be the minimal element of the set $\{K \in \mathcal{K} : f \in V_K\}$. We denote the minimal field of f by K_f.

Lemma 2.2.2. *For any $f \in \mathcal{F}$, we have* $\mathrm{Stab}_G(f) = \mathrm{Gal}(\overline{\mathbb{Q}}/K_f) \leq G$.

Notation 2.2.3. By $\mathrm{Stab}_G(f)$ we mean the $\sigma \in G$ such that $L_\sigma f = f$. As this tacit identification is convenient we shall use it throughout without further comment.

Proof. Let $f = f_\alpha$. Then clearly $\mathrm{Gal}(\overline{\mathbb{Q}}/K_f) \leq \mathrm{Stab}_G(f)$, as $\alpha^\ell \in K_f$ for some $\ell \in \mathbb{N}$ by definition of V_{K_f}. To see the reverse implication, merely observe that $K_f = \mathbb{Q}(\alpha^\ell)$ for some $\ell \in \mathbb{N}$, as otherwise, there would be a proper subfield of K_f which contains a power of α, contradicting the definition of K_f. □

Remark 2.2.4. The minimal such exponent ℓ used above can in fact be uniquely associated to $f \in \mathcal{F}$ and this will be vital to the concept of Lehmer irreducibility developed in Chapter 3.

Lemma 2.2.5. *For a given $f \in \mathcal{F}$, we have $f \in V_K$ if and only if $L_\sigma f = f$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$.*

Proof. Necessity is obvious. To see that the condition is sufficient, observe that by definition of K_f, we have $f \in V_K$ if and only $K_f \subseteq K$, which is equivalent to $\mathrm{Gal}(\overline{\mathbb{Q}}/K) \leq \mathrm{Gal}(\overline{\mathbb{Q}}/K_f)$ under the Galois correspondence. But by the above lemma, $\mathrm{Gal}(\overline{\mathbb{Q}}/K_f) = \mathrm{Stab}_G(f)$. □

Proposition 2.2.6. *If $E, F \in \mathcal{K}$, then we have $E \neq F$ if and only if $V_E \neq V_F$.*

Proof. Suppose $E \neq F$ but $V_E = V_F$. Let $E = \mathbb{Q}(\alpha)$. By [Dub05, Theorem 3] we can find a rational integer n such that $\beta = n + \alpha$ is torsion-free, that is, if

$\beta/\beta' \neq 1$ then $\beta/\beta' \notin \mathrm{Tor}(\overline{\mathbb{Q}}^\times)$ for any conjugate β' of β, and in particular, the conjugates of β give rise to distinct functions in $\mathcal{F}$. Observe therefore that $E = \mathbb{Q}(\beta)$ and $\mathrm{Stab}_G(f_\beta) = \mathrm{Gal}(\overline{\mathbb{Q}}/E)$. By the above if $f_\beta \in V_F$ then we must have $\mathrm{Gal}(\overline{\mathbb{Q}}/F) \leq \mathrm{Gal}(\overline{\mathbb{Q}}/E)$, or $E \subseteq F$. Repeating the same argument for a generator of F, we find that $F \subseteq E$ so $E = F$, a contradiction. The reverse implication is obvious. □

Remark 2.2.7. The above proposition is no longer true if we restrict our attention to the space of units $\mathcal{U} \subset \mathcal{F}$. This follows from the well known fact that CM extensions (totally imaginary quadratic extensions of totally real fields) have the same unit group modulo torsion as their base fields, the simplest example being $\mathbb{Q}(i)/\mathbb{Q}$.

2.3 Orthogonal projections associated to number fields

For $K \in \mathcal{K}$, define the map $P_K : \mathcal{F} \to V_K$ via

$$(P_K f)(y) = \int_{H_K} (L_\sigma f)(y) d\nu(\sigma)$$

where $H_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and ν is the normalized (measure 1) Haar measure of H_K. (Observe that, like G, H_K is profinite and thus compact and possesses a Haar measure.) Let us prove that the map is well-defined. Since $f \in \mathcal{F}$, it has a finite Galois orbit and thus a finite orbit under H_K. Let us partition H_K into the $k = [H_K : \mathrm{Stab}_{H_K}(f)]$ cosets of equal measure by the translation invariance of the Haar measure. Denote these cosets by $\mathrm{Stab}_{H_K}(f)\sigma_1, \ldots, \mathrm{Stab}_{H_K}(f)\sigma_k$.

Then

$$P_K(f) = \frac{1}{k}\left(L_{\sigma_1} f + \cdots + L_{\sigma_k} f\right).$$

But each $L_{\sigma_i} f \in \mathcal{F}$ since $\mathcal{F}$ is closed under the action of the Galois isometries. Thus if $f = f_\alpha$, we have $L_{\sigma_i} f = f_{\sigma_i \alpha}$. Since $\mathcal{F}$ is a $\mathbb{Q}$-vector space, $P_K(f) \in \mathcal{F}$ as well. Further, it is stable under the action of H_K, and thus, by Lemma 2.2.5, we have $P_K(f) \in V_K$. The map P_K is in fact nothing more than the familiar algebraic norm down to K, subject to an appropriate normalization, that is, if $f_\beta = P_K f_\alpha$, then we have

$$\beta \equiv \left(\mathrm{Norm}_K^{K(\alpha)}\, \alpha\right)^{1/[K(\alpha):K]} \mod \mathrm{Tor}(\overline{\mathbb{Q}}^\times). \tag{2.3.1}$$

(We note in passing that the norm map $\mathrm{Norm}_K^{K(\alpha)} : K(\alpha)^\times \to K^\times$, as a homomorphism, necessarily maps torsion elements to other torsion elements and thus descends to a well-defined map modulo torsion.)

The following alternative formulation will also be helpful:

Lemma 2.3.1. *Let $K \in \mathcal{K}$ and let M_K denote the places of K. For each $v \in M_K$, let $\chi_v(y)$ be the characteristic function of the set $Y(K, v)$. Then*

$$P_K f(y) = \sum_{v \in M_K} \left(\frac{1}{\lambda(Y(K,v))} \int_{Y(K,v)} f(z)\, d\lambda(z) \right) \chi_v(y).$$

In other words, P_K is essentially the conditional expectation with respect to the Borel σ-algebra generated by the set $\{Y(K, v) : v \in M_K\}$. Of course, Y has infinite measure so this is not a conditional expectation in the usual sense from probability theory, although it shares many of the same properties. If we

restrict to the space of units, that is, functions supported on the measure one space $Y(\mathbb{Q}, \infty)$, then the restriction of P_K to this space is indeed a conditional expectation.

Proof. Fix a value $y \in Y$. Then there exists a unique $v \in M_K$ such that $y \in Y(K, v)$ since $Y = \bigcup_{v \in M_K} Y(K, v)$ is a disjoint union. The claim will be proven if we can show that for this value of y,

$$P_K f(y) = \frac{1}{\lambda(Y(K, v))} \int_{Y(K,v)} f(z)\, d\lambda(z).$$

Now,

$$P_K f(y) = \int_{H_K} f(\sigma^{-1} y)\, d\nu(\sigma)$$

where H_K, ν are as above. By the construction of λ (see (4.1) and surrounding remarks in [AV09]), for any $y \in Y(K, v)$,

$$\frac{1}{\lambda(Y(K, v))} \int_{Y(K,v)} f(z)\, d\lambda(z) = \int_{H_K} f(\sigma^{-1} y)\, d\nu(\sigma)$$

(where we need the normalization factor $1/\lambda(Y(K, v))$ since (4.1) assumes $\lambda(K, v) = 1$) and so the proof is complete. □

Proposition 2.3.2. *Let $K \subset \overline{\mathbb{Q}}$ be a field of arbitrary degree. Then P_K is a projection onto V_K of norm one with respect to the L^p norms for $1 \leq p \leq \infty$.*

Proof. We first prove that $P_K^2 = P_K$. Let $H = H_K$ as above and ν the normalized Haar measure on H. Suppose that $\tau \in H$. Observe that

$$P_K(f)(\tau^{-1} y) = \int_H f(\sigma^{-1} \tau^{-1} y) d\nu(\sigma) = \int_{\tau H} f(\sigma^{-1} y) d\nu(\sigma) = P_K(f)(y)$$

since $\tau H = H$ for $\tau \in H$. Thus,

$$({P_K}^2 f)(y) = \int_H P_K f(\sigma^{-1} y) d\nu(\sigma) = \int_H P_K f(y) d\nu(\sigma) = P_K f(y),$$

or more succinctly, ${P_K}^2 = P_K$. Since linearity is clear we will now prove that the operator norm $\|P_K\| = 1$ in the L^p norm in order to conclude that P_K is a projection. If $p = \infty$, this is immediate, so let us assume that $1 \leq p < \infty$. Let $f \in L^p(Y)$. Then first observe that since $\nu(H) = 1$, Jensen's inequality implies

$$\int_H |f(\sigma^{-1} y)| \, d\nu(\sigma) \leq \left(\int_H |f(\sigma^{-1} y)|^p \, d\nu(\sigma) \right)^{1/p}.$$

Now let us consider the L^p norm of $P_K f$:

$$\begin{aligned} \|P_K f\|_p &= \left(\int_Y |P_K(f)(y)|^p d\lambda(y) \right)^{1/p} = \left(\int_Y \left| \int_H f(\sigma^{-1} y) d\nu(\sigma) \right|^p d\lambda(y) \right)^{1/p} \\ &\leq \left(\int_Y \int_H \left| f(\sigma^{-1} y) \right|^p d\nu(\sigma) d\lambda(y) \right)^{1/p} = \left(\int_H \int_Y \left| f(\sigma^{-1} y) \right|^p d\lambda(y) d\mu(\sigma) \right)^{1/p} \\ &= \left(\int_H \|L_\sigma f\|_p^p d\mu(\sigma) \right)^{1/p} = \left(\int_H \|f\|_p^p d\mu(\sigma) \right)^{1/p} = \|f\|_p. \end{aligned}$$

where we have made use of the fact that L_σ is an isometry, and the application of Fubini's theorem is justified by the integrability of $|f|^p$. This proves that $\|P_K\| \leq 1$, and to see that the operator norm is not in fact less than 1, observe that the subspace $V_{\mathbb{Q}}$ is fixed for every P_K. □

As a corollary, if we extend P_K by continuity to the completion $\mathcal{F}_p$ of $\mathcal{F}$ under the L^p norm, we obtain:

Corollary 2.3.3. *The subspace $\overline{V_K} \subset \mathcal{F}_p$ is complemented in $\mathcal{F}_p$ for all $1 \leq p \leq \infty$.*

As $\mathcal{F}_2 = L^2(Y, \lambda)$ is a Hilbert space, in fact, we can show that P_K is an *orthogonal projection*. Specifically, we say P is an orthogonal projection on a Hilbert space H if P is idempotent, continuous, and if $P(H) \perp (I - P)(H)$, where I denotes the identity operator. Equivalently, P is orthogonal if $\|f\|^2 = \|Pf\|^2 + \|(I - P)f\|^2$ for all $f \in H$. Let us recall some basic facts about orthogonality from Hilbert space theory:

Lemma 2.3.4. *Let H be a real Hilbert space with norm $\|\cdot\|$ and inner product $\langle \cdot, \cdot \rangle$, and let $f, g \in H$. Then $\|f\| \leq \|f + \lambda g\|$ for all $\lambda \in \mathbb{R}$ if and only if $f \perp g$.*

We have assumed for simplicity that H is a real Hilbert space, although it is not difficult to see that the result is true in the complex case if we take $\lambda \in \mathbb{C}$ in our hypothesis.

Proof. Observe that the hypothesis can be equivalently written $\|f\|^2 \leq \|f + \lambda g\|^2$, or expanding in terms of the inner product,

$$\langle f, f \rangle \leq \langle f, f \rangle + 2\lambda \langle f, g \rangle + \lambda^2 \langle g, g \rangle,$$

equivalently,

$$0 \leq 2\lambda \langle f, g \rangle + \lambda^2 \langle g, g \rangle.$$

But this holds for all $\lambda \in \mathbb{R}$ if and only if $\langle f, g \rangle = 0$, which is the desired condition. □

Lemma 2.3.5. *If P is a norm one idempotent projection on a Hilbert space H, then P is an orthogonal projection.*

Proof. Let $Q = I - P$, where I denotes the identity operator. Then we wish to show that $P(H) \perp Q(H)$. Let $f \in H$ and observe that $PQ = P - P^2 = 0$ by assumption, so $P(Pf + \lambda Qf) = Pf$ for all $\lambda \in \mathbb{R}$. Then observe that

$$\|Pf\| = \|P(Pf + \lambda Qf)\| \leq \|Pf + \lambda Qf\| \quad \text{for all} \quad \lambda \in \mathbb{R}.$$

Thus, by the preceding lemma, we see that $Pf \perp Qf$. Since we can choose f so that $Pf = g$ and $Qf = h$ for any arbitrary $g \in P(H), h \in Q(H)$, we have the desired result. □

Proposition 2.3.6. *For each $K \in \mathcal{K}$, P_K is the orthogonal projection onto the subspace $\overline{V_K} \subset L^2(Y)$.*

Proof. It suffices to observe that P_K is idempotent and has operator norm $\|P_K\| = 1$ with respect to the L^2 norm, and any such projection in a Hilbert space is orthogonal by the preceding lemma. □

We now explore the relationship between the Galois isometries and the projection operators P_K for $K \in \mathcal{K}$.

Lemma 2.3.7. *For any field $K \subset \overline{\mathbb{Q}}$ of arbitrary degree and any $\sigma \in G$,*

$$L_\sigma P_K = P_{\sigma K} L_\sigma.$$

Equivalently, $P_K L_\sigma = L_\sigma P_{\sigma^{-1} K}$.

Proof. We prove the first form, the second obviously being equivalent. By definition of P_K, letting $H = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and ν be the normalized Haar measure

on H such that $\nu(H) = 1$,

$$\begin{aligned}(L_\sigma P_K f)(y) = (P_K f)(\sigma^{-1}y) &= \int_H f(\tau^{-1}\sigma^{-1}y)\, d\nu(\tau) \\ &= \int_H f(\sigma^{-1}\sigma\tau^{-1}\sigma^{-1}y)\, d\nu(\tau) \\ &= \int_H f(\sigma^{-1}(\sigma\tau\sigma^{-1})^{-1}y)\, d\nu(\tau) \\ &= \int_H (L_\sigma f)((\sigma\tau\sigma^{-1})^{-1}y)\, d\nu(\tau) \\ &= \int_{\sigma H\sigma^{-1}} (L_\sigma f)(\tau^{-1}y)\, d\nu(\tau) \\ &= P_{\sigma K}(L_\sigma f)(y). \qquad \square\end{aligned}$$

We will be particularly interested in the case where the projections P_K, P_L commute with each other (and thus $P_K P_L$ is a projection to the intersection of their ranges). To that end, let us determine the intersection of two distinguished subspaces:

Lemma 2.3.8. *Let $K, L \subset \overline{\mathbb{Q}}$ be fields of arbitrary degree. Then the intersection $V_K \cap V_L = V_{K\cap L}$.*

Proof. Observe that $f_\alpha \in V_K$ if and only if $\alpha^n \in K$ for some $n \in \mathbb{N}$, and likewise, since $f_\alpha \in V_L$, we have $\alpha^m \in L$ for some $m \in \mathbb{N}$. Then $\alpha^{nm} \in K \cap L$, so $f_\alpha \in V_{K\cap L}$. The reverse inclusion is obvious. $\square$

Lemma 2.3.9. *Suppose $K \in \mathcal{K}$ and $L \in \mathcal{K}^G$. Then P_K and P_L commute, that is,*

$$P_K P_L = P_{K\cap L} = P_L P_K.$$

In particular, the family of operators $\{P_K : K \in \mathcal{K}^G\}$ is commuting.

Proof. It suffices to prove $P_K(V_L) \subset V_L$, as this will imply that $P_K(V_L) \subset V_K \cap V_L = V_{K\cap L}$ by the above lemma, and thus that $P_K P_L$ is itself a projection onto $V_{K\cap L}$. It is norm one as both P_K and P_L are norm one, and therefore it is orthogonal, and thus $P_K P_L = P_{K\cap L}$ as the orthogonal projection is unique. Since $P_{K\cap L}$ is an orthogonal projection, it is equal to its adjoint (see e.g. [Yos80, Theorem III.2]), and so by taking the adjoints of both sides of the equation we find that

$$P_K P_L = P_{K\cap L} = P^*_{K\cap L} = P^*_L P^*_K = P_L P_K$$

as well. To prove that $P_K(V_L) \subset V_L$, observe that for $f \in V_L$,

$$P_K(f) = \frac{1}{k}(L_{\sigma_1} f + \cdots L_{\sigma_k} f)$$

where the σ_i are right coset representatives of $\mathrm{Gal}(\overline{\mathbb{Q}}/L)\cap\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ in $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$. However, $L_\sigma(V_L) = V_L$ for $\sigma \in G$ since L is Galois, and thus, $P_K(f) \in V_L$ as well. But $P_K(f) \in V_K$ by construction and the proof is complete. □

2.4 Main decomposition theorem

We will now begin the proof of Theorems 2 and 3, which state that we can orthogonally decompose the space $\mathcal{F}$ of algebraic numbers modulo torsion by their Galois field and by their degree. These results will be derived from the following general decomposition theorem, which we will apply to $\mathcal{F}$ in the next two sections.

Theorem 15. *Let V be a vector space over $\mathbb{Q}$ with an inner product $\langle \cdot, \cdot \rangle$ and suppose we have a family of subspaces $V_i \subset V$ together with projections P_i indexed by a partially ordered set I such that:*

1. *The index set I has a unique minimal element, denoted $0 \in I$, and I is locally finite, that is, any interval $[i, j] = \{k \in I : i \leq k \leq j\}$ is of finite cardinality.*

2. *Any pair of elements $i, j \in I$ has a unique greatest lower bound, called the meet of i and j, and denoted $i \wedge j$. (Such a poset I is called a meet-semilattice.)*

3. *$V_i \subseteq V_j$ if $i \leq j \in I$.*

4. *The projection map $P_i : V \to V_i$ is orthogonal with respect to the inner product of V for all $i \in I$.*

5. *For $i, j \in I$, $P_i P_j = P_j P_i = P_{i \wedge j}$, where $i \wedge j$ is the meet of i and j.*

6. *$V = \sum_{i \in I} V_i$ (the sum is in the usual $\mathbb{Q}$-vector space sense).*

Then there exist mutually orthogonal projections $T_i \leq P_i$ (that is, satisfying $T_i(V) \subseteq V_i$ and $T_i(V) \perp T_j(V)$ for $i \neq j$) which form an orthogonal decomposition of V:

$$V = \bigoplus_{i \in I} T_i(V), \quad \text{and} \quad T_i(V) \perp T_j(V) \text{ for all } i \neq j \in I.$$

(The notation $V = \bigoplus_{i \in I} T_i(V)$ indicates a direct sum in the $\mathbb{Q}$-vector space sense, that is, that each vector $v \in V$ has a unique expression as a finite sum of vectors, one from each summand.)

We call T_i the *essential projection* associated to the space V_i, as it gives the subspace of V_i which is unique to V_i and no other subspace V_j in the given family.

Remark 2.4.1. Theorem 15 can be stated and proven almost identically if V is a real Hilbert space rather than an incomplete vector space over $\mathbb{Q}$, the only changes being that condition (6) is replaced with the condition that the closure of $\sum_{i \in I} V_i$ is V, the direct sum is then understood in the usual Hilbert space sense, and the expansion of each f into $\sum_{i \in I} T_i f$ is to be understood as a unique series expansion rather than a finite sum. The construction of the T_i operators and the orthogonality are proven in exactly the same manner, and indeed, we will make use of the fact that if we complete V, the decomposition extends by continuity to the completion in the usual Hilbert space sense. The theorem as stated here and as applied to $\mathcal{F}$ is in fact a strictly stronger result than the statement it implies for the decomposition of $L^2(Y)$ as not only must such projections and such a decomposition exist, but this decomposition must also respect the underlying $\mathbb{Q}$-vector space of algebraic numbers $\mathcal{F}$ and map algebraic numbers to algebraic numbers.

Let us begin by recalling the background necessary to define our T_i projections. Since I is locally finite, it is a basic theorem in combinatorics that there exists a Möbius function $\mu : I \times I \to \mathbb{Z}$, defined inductively by the

requirements that $\mu(i,i) = 1$ for all $i \in I$, $\mu(i,j) = 0$ for all $i \not\leq j \in I$, and $\sum_{i \leq j \leq k} \mu(i,j) = 0$ for all $i < k \in I$ (the sums are finite by the assumption that I is locally finite). Since our set I has a minimal element 0 and is locally finite, we can sum over $i \leq j$ as well. The most basic result concerning the Möbius function is *Möbius inversion*, which (in one of the several possible formulations) tells us that given two functions f, g on I,

$$f(j) = \sum_{i \leq j} g(i) \quad \text{if and only if} \quad g(j) = \sum_{i \leq j} \mu(i,j)\, f(i).$$

In order that our T_i capture the unique contribution of each subfield V_i, we would like our T_i projections to satisfy the condition that:

$$P_j = \sum_{i \leq j} T_i.$$

Möbius inversion leads us to define the T_i operators via the equation:

$$T_j = \sum_{i \leq j} \mu(i,j) P_i. \tag{2.4.1}$$

Since each of the above sums is finite and μ takes values in $\mathbb{Z}$, we see that $T_j : V \to V_j$ is well-defined. We will prove that T_j is the desired family of projections.

Lemma 2.4.2. *Let the projections P_i for $i \in I$ satisfy the conditions of Theorem 15 and let T_i be defined as above. Then for all $i, j \in I$, $P_i T_j = T_j P_i$, and*

$$P_j T_i = \begin{cases} T_j & \text{if } i \leq j \\ 0 & \text{otherwise.} \end{cases}$$

Proof. The first claim follows immediately from equation (2.4.1) and condition (5) of the theorem statement. To prove the second claim, we proceed by induction. Observe that the statement is trivial for $T_0 = P_0$. Now given $j \in I$, suppose the theorem is true for all $i < j$. Observe that from (2.4.1) we get

$$T_j = P_j - \sum_{i<j} T_i. \tag{2.4.2}$$

Then, if $i < j$, we have

$$P_j T_i = P_j P_i - \sum_{k<i} P_j T_k = P_i - \sum_{k<i} T_k = T_i,$$

applying the induction hypothesis at the second equality.

Now suppose $i \not< j$, so that $i \wedge j \neq i$. Then

$$\begin{aligned} P_j T_i = P_j P_i - \sum_{k<i} P_j T_k = P_{i\wedge j} - \sum_{k\leq i\wedge j} P_j T_k - \sum_{\substack{k<i \\ k\not\leq i\wedge j}} P_j T_k \\ = P_{i\wedge j} - \sum_{k\leq i\wedge j} T_k - 0 = P_{i\wedge j} - P_{i\wedge j} = 0 \end{aligned}$$

by two applications of the induction hypothesis at the third equality. □

Lemma 2.4.3. *Let the T_i be as above and let $i \neq j$ for $i, j \in I$. Then $T_i T_j = T_j T_i = 0$.*

Proof. By Lemma 2.4.2, $T_i = T_i P_i$ and $T_j = P_j T_j$. Thus,

$$T_i T_j = (T_i P_i)(P_j T_j) = T_i (P_i P_j) T_j = T_i P_{i\wedge j} T_j = 0$$

since $i \neq j$ implies that $i \wedge j < i$ or $i \wedge j < j$, so either $T_i P_{i\wedge j} = 0$ or $P_{i\wedge j} T_j = 0$ by Lemma 2.4.2. □

We are now ready to prove the theorem statement.

Proof of Theorem 15. Let the operators T_i for $i \in I$ be constructed as above. Let us first show that each T_i is a projection, a continuous linear operator such that ${T_i}^2 = T_i$. The fact the T_i is a continuous linear operator follows from the same fact for the P_i operators, since each T_i is a finite linear combination of P_i projections.

Let us now show that T_i is idempotent. The base case $T_0 = P_0$ is trivial. Assume the lemma is true for all $i < j$. Using equation (2.4.2), we have

$$\begin{aligned} {T_j}^2 = \left(P_j - \sum_{i<j} T_i\right)^2 &= {P_j}^2 - \sum_{i<j} P_j T_i - \sum_{i<j} T_i P_j + \left(\sum_{i<j} T_i\right)^2 \\ &= P_j - \sum_{i<j} T_i - \sum_{i<j} T_i + \sum_{i<j} T_i = P_j - \sum_{i<j} T_i = T_j \end{aligned}$$

where we have used Lemmas 2.4.2 and 2.4.3 to simplify the middle and last terms.

Now, let us show that the T_i decompose V. To see this, observe that each element $f \in V$ by condition (6) lies in some $V_{i_1} + \ldots + V_{i_n}$. Let $I' = \bigcup_{m=1}^{n} [0, i_m] \subset I$, and then observe that $\sum_{k \in I'} T_k$ is the projection onto $V_{i_1} + \ldots + V_{i_n}$ and I' is finite by construction, so $f = \sum_{k \in I'} T_k f$. In fact, observe that we can write $f = \sum_{k \in I} T_k f$ as a formally infinite sum, and all terms except those satisfying $k \leq i$ are zero by Lemma 2.4.2. Thus we can write

$$V = \bigoplus_{i \in I} T_i(V).$$

That the T_i are orthogonal projections now follows from the fact that a continuous operator is an orthogonal projection if and only if it is idempotent and self-adjoint [Yos80, Theorem III.2], for, since the P_i are assumed to be orthogonal, they are self-adjoint and thus the T_i operators are self-adjoint as well as an integral linear combination of the P_i operators, and we have demonstrated that they are continuous and idempotent. □

2.5 Decomposition by Galois field and proof of Theorem 2

We will now apply Theorem 15 to $\mathcal{F}$. Recall that $\mathcal{K}^G$ is simply the set of finite Galois extensions of $\mathbb{Q}$. As remarked above, it is well known that both $\mathcal{K}$ and $\mathcal{K}^G$ satisfy all of the axioms of a lattice, that is, for any two fields K, L, there is a unique meet $K \wedge L$ given by $K \cap L$ and a unique *join* $K \vee L$ given by KL. If K, L are Galois then both the meet (the intersection) and the join (the compositum) are Galois as well, thus $\mathcal{K}^G$ is a lattice as well. Further, both $\mathcal{K}$ and $\mathcal{K}^G$ are locally finite posets and possess a minimal element, namely, $\mathbb{Q}$.

Our decomposition will be along $\mathcal{K}^G$ and the associated family of subspaces V_K with their canonical projections P_K. Since $\mathcal{K}^G$ is a locally finite lattice, conditions (1) and (2) of Theorem 15 are satisfied. Clearly the subspaces V_K for $K \in \mathcal{K}^G$ satisfy the containment condition (3). By Proposition 2.3.6, the projections are orthogonal and satisfy condition (4). By Lemma 2.3.9, the maps $\{P_K : K \in \mathcal{K}^G\}$ form a commuting family and satisfy condition (5). Lastly, since any $f = f_\alpha$ belongs to $V_{K_f} \subset V_K$ where $K \in \mathcal{K}^G$ is the

Galois closure of the minimal field K_f, we find that condition (6) is satisfied as well. Thus Theorem 15 gives us an orthgonal decomposition

$$\mathcal{F} = \bigoplus_{K \in \mathcal{K}^G} T_K(\mathcal{F}) \tag{2.5.1}$$

The relationship between the P_K and T_K operators is given by:

$$P_K = \sum_{\substack{F \in \mathcal{K}^G \\ F \subseteq K}} T_F, \quad \text{and} \quad T_K = \sum_{\substack{F \in \mathcal{K}^G \\ F \subseteq K}} \mu(F, K) P_F \tag{2.5.2}$$

where $\mu : \mathcal{K}^G \times \mathcal{K}^G \to \mathbb{Z}$ is the Möbius function associated to $\mathcal{K}^G$.

If K is the Galois closure of the minimal field K_f where $f = f_\alpha$, then $P_K(f) = f$, and so (2.5.2) gives us a unique representation modulo torsion of the algebraic number α which we call the *M-factorization* of α, or the *M-expansion* of f_α in functional notation.

Example 2.5.1. *Let $\alpha = 2 + \sqrt{2}$ and let $f = f_\alpha$. Then $K_f = \mathbb{Q}(\sqrt{2})$. Since $K \in \mathcal{K}^G$, $[K : \mathbb{Q}] = 2$ and it is easy to see that the interval $[\mathbb{Q}, K] = \{\mathbb{Q}, K\} \subset \mathcal{K}^G$, and so $\mu(\mathbb{Q}, K) = -1$, and thus*

$$T_K = P_K - P_{\mathbb{Q}}, \quad T_{\mathbb{Q}} = P_{\mathbb{Q}}.$$

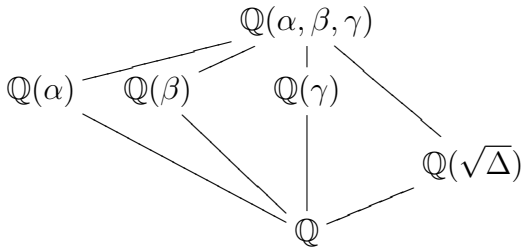
Thus

$$T_K(f_\alpha) = f_{1+\sqrt{2}}, \quad T_{\mathbb{Q}}(f_\alpha) = f_{\sqrt{2}},$$

and the M-factorization of α has the form $2 + \sqrt{2} = \sqrt{2} \cdot (1 + \sqrt{2})$, or in functional notation,

$$f_{2+\sqrt{2}} = f_{\sqrt{2}} + f_{1+\sqrt{2}}, \quad \textit{and} \quad f_{\sqrt{2}} \perp f_{1+\sqrt{2}}.$$

Remark 2.5.2. We end this section with a remark on why we decompose along $\mathcal{K}^G$ but not $\mathcal{K}$. It is not difficult to see that the P_K projections for $K \in \mathcal{K}$ do not form a commuting family. To see this, suppose α is a cubic algebraic unit with conjugates β, γ and nonsquare discriminant Δ. Then we have the following fields:



But the projections associated to the fields $\mathbb{Q}(\alpha)$ and its conjugates do not commute. Specifically, we may compute:

$$P_{\mathbb{Q}(\beta)} f_\alpha = -\frac{1}{2} f_\beta, \quad \text{and} \quad P_{\mathbb{Q}(\alpha)} f_\beta = -\frac{1}{2} f_\alpha$$

which shows that $P_{\mathbb{Q}(\alpha)} P_{\mathbb{Q}(\beta)} \neq P_{\mathbb{Q}(\beta)} P_{\mathbb{Q}(\alpha)}$. This noncommutativity is present precisely because there is a linear dependence among the vector space $V_{\mathbb{Q}(\alpha)}$ and its conjugates, e.g., $f_\alpha + f_\beta + f_\gamma = 0$ (since we assumed α was an algebraic unit). In particular, we have

$$V_{\mathbb{Q}(\alpha)} + V_{\mathbb{Q}(\beta)} = V_{\mathbb{Q}(\alpha)} + V_{\mathbb{Q}(\beta)} + V_{\mathbb{Q}(\gamma)},$$

as the projection map down to $\mathbb{Q}$ to gives us, for any $f \in V_{\mathbb{Q}(\gamma)}$, an expresion $g = P_{\mathbb{Q}} f = (f + L_\sigma f + L_\tau f)/3$ where $L_\sigma f \in V_{\mathbb{Q}(\alpha)}$ and $L_\tau f \in V_{\mathbb{Q}(\beta)}$, and thus $f = 3g - L_\sigma f + L_\tau f \in V_{\mathbb{Q}(\alpha)} + V_{\mathbb{Q}(\beta)}$ (since $V_{\mathbb{Q}}$ is in common to both subspaces). Clearly such a dependence would make it impossible to associate

a unique component T_K to each of the three fields. However, the commutavity of the P_K for $K \in \mathcal{K}^G$ implies that there is no such barrier to decomposition amongst the Galois fields.

2.6 Decomposition by degree and proof of Theorems 3 and 4

In order to associate a notion of degree to a subspace in a meaningful fashion so that we can define our Mahler p-norms we will determine a second decomposition of $\mathcal{F}$. Let us define the orbital degree function $\delta : \mathcal{F} \to \mathbb{N}$ by

$$\delta(f) = \#\{L_\sigma f : \sigma \in G\} = [G : \mathrm{Stab}_G(f)] \tag{2.6.1}$$

to be the size of the orbit of f under the action of the Galois isometries. Observe that by Lemma 2.2.2, we have $\mathrm{Stab}_G(f) = \mathrm{Gal}(\overline{\mathbb{Q}}/K_f)$ where K_f is the minimal field of f, and so we also have

$$\delta(f) = [K_f : \mathbb{Q}]. \tag{2.6.2}$$

Let

$$V^{(n)} = \sum_{\substack{K \in \mathcal{K} \\ [K:\mathbb{Q}] \leq n}} V_K \tag{2.6.3}$$

be the vector space spanned by all elements with orbit in $\mathcal{F}$ under G of size at most n. Let $P^{(n)}$ denote the unique orthogonal projection of the Hilbert space $L^2(Y)$ onto the closure $\overline{V^{(n)}}$ of the $\mathbb{Q}$-vector space $V^{(n)}$ inside $L^2(Y)$. We wish to show that the restriction of this orthogonal projection defined on the Hilbert space $L^2(Y)$ preserves the $\mathbb{Q}$-vector space $\mathcal{F}$ of equivalence classes

of algebraic numbers modulo torsion, that is, that $P^{(n)}(\mathcal{F}) \subset \mathcal{F}$, so that the map

$$P^{(n)} : \mathcal{F} \to V^{(n)}$$

is well-defined. Once this has been demonstrated, we can apply Theorem 15 to obtain projections $T^{(n)} : \mathcal{F} \to V^{(n)}$ which will give us the orthogonal decomposition of $\mathcal{F}$ into a subspace spanned by elements whose orbit under G is of order at most n. We begin by first showing that the projections $P^{(n)}$ and P_K for $n \in \mathbb{N}$ and $K \in \mathcal{K}^G$ commute.

Lemma 2.6.1. *If $K \in \mathcal{K}^G$, then $\delta(P_K f) \leq \delta(f)$ for all $f \in \mathcal{F}$.*

Proof. Let $F = K_f$. Since $K \in \mathcal{K}^G$, we have by Lemma 2.3.9 that $P_K f = P_K(P_F f) = P_{K \cap F} f$. Thus, $P_K f \in V_{K \cap F}$, and so by (2.6.2) above, we have $\delta(P_K f) \leq [K \cap F : \mathbb{Q}] \leq [F : \mathbb{Q}] = \delta(f)$. □

Proposition 2.6.2. *Let $n \in \mathbb{N}$ and $K \in \mathcal{K}^G$. Then the orthogonal projections $P^{(n)} : L^2(Y) \to \overline{V^{(n)}}$ and $P_K : L^2(Y) \to \overline{V_K}$ commute (where the closures are taken in L^2), and thus T_K and $P^{(n)}$ commute as well.*

Proof. Since $\delta(P_K f) \leq \delta(f)$ for all $f \in \mathcal{F}$ by Lemma 2.6.1 above, we have $P_K(V^{(n)}) \subset V^{(n)}$, and thus by continuity $P_K(\overline{V^{(n)}}) \subset \overline{V^{(n)}}$, so $P_K(\overline{V^{(n)}}) \subset \overline{V^{(n)}} \cap \overline{V_K}$ and $P_K P^{(n)}$ is a projection. Therefore they commute. The last part of the claim now follows from the definition of T_K in (2.4.1). □

Let $W_K = T_K(\mathcal{F}) \subset V_K$ for $K \in \mathcal{K}^G$. By the above proposition, we see that if we can show that $P^{(n)}(W_K) \subseteq W_K$, then we will have the desired result

since

$$P^{(n)}(\mathcal{F}) = \bigoplus_{K \in \mathcal{K}^G} P^{(n)}(W_K)$$

by the commutativity of $P^{(n)}$ and T_K. Since we will prove this result by reducing to finite dimensional S-unit subspaces, let us first prove an easy lemma regarding finite dimensional vector spaces over $\mathbb{Q}$.

Lemma 2.6.3. *Suppose we have a finite dimensional vector space A over $\mathbb{Q}$, and suppose that*

$$A = V_1 \oplus V_1' = V_2 \oplus V_2' = \cdots = V_n \oplus V_n'$$

for some subspaces V_i, V_i', $1 \leq i \leq n$. Then

$$A = (V_1 + \cdots + V_n) \oplus (V_1' \cap \cdots \cap V_n').$$

Proof. It suffices to prove the lemma in the case $n = 2$ as the remaining cases follow by induction, so suppose $A = V_1 \oplus V_1' = V_2 \oplus V_2'$. It is an easy exercise that

$$\dim_{\mathbb{Q}} V_1 + \dim_{\mathbb{Q}} V_2 = \dim_{\mathbb{Q}}(V_1 + V_2) + \dim_{\mathbb{Q}}(V_1 \cap V_2),$$

and likewise,

$$\dim_{\mathbb{Q}} V_1' + \dim_{\mathbb{Q}} V_2' = \dim_{\mathbb{Q}}(V_1' + V_2') + \dim_{\mathbb{Q}}(V_1' \cap V_2').$$

Now,

$$\begin{aligned} 2\dim_{\mathbb{Q}} A &= \dim_{\mathbb{Q}} V_1 + \dim_{\mathbb{Q}} V_1' + \dim_{\mathbb{Q}} V_2 + \dim_{\mathbb{Q}} V_2' \\ &= \dim_{\mathbb{Q}}(V_1 + V_2) + \dim_{\mathbb{Q}}(V_1 \cap V_2) + \dim_{\mathbb{Q}}(V_1' + V_2') + \dim_{\mathbb{Q}}(V_1' \cap V_2'). \end{aligned} \tag{2.6.4}$$

Notice that $(V_1 + V_2) \oplus (V_1' \cap V_2') \subseteq A$ and $(V_1' + V_2') \oplus (V_1 \cap V_2) \subseteq A$, so we must have

$$b = \dim_{\mathbb{Q}}(V_1 + V_2) + \dim_{\mathbb{Q}}(V_1' \cap V_2') \leq \dim_{\mathbb{Q}} A$$
$$c = \dim_{\mathbb{Q}}(V_1' + V_2') + \dim_{\mathbb{Q}}(V_1 \cap V_2) \leq \dim_{\mathbb{Q}} A.$$

But by (2.6.4), we have $b + c = 2\dim_{\mathbb{Q}} A$, so we must have $b = c = \dim_{\mathbb{Q}} A$, and in particular $b = \dim_{\mathbb{Q}} A$ proves the claim. □

Proposition 2.6.4. *With $W_K = T_K(\mathcal{F})$ as above, $P^{(n)}(W_K) \subseteq W_K$ for every $n \in \mathbb{N}$ and $K \in \mathcal{K}^G$, and thus $P^{(n)}(\mathcal{F}) \subset \mathcal{F}$.*

Proof. Let $f \in W_K$, and let $S \subset M_{\mathbb{Q}}$ be a finite set of rational primes, containing the infinite prime, such that

$$\mathrm{supp}_Y(f) \subset \bigcup_{p \in S} Y(\mathbb{Q}, p).$$

Let $V_{K,S} \subset V_K$ denote the subspace spanned by the S-units of K. By Dirichlet's S-unit theorem, $V_{K,S}$ is finite dimensional over $\mathbb{Q}$. Let $W_{K,S} = T_K(V_{K,S})$. Notice that $W_{K,S} \subset V_{K,S}$ since each P_F projection will preserve the support of f over each set $Y(\mathbb{Q}, p)$ for $p \in M_{\mathbb{Q}}$ by Lemma 2.3.1.

For all fields $F \in \mathcal{K}$ such that $F \subset K$, let

$$Z_{F,S} = P_F(W_{K,S}) \quad \text{and} \quad Z'_{F,S} = Q_F(W_{K,S}),$$

where $Q_F = I - P_F$ is the complementary orthogonal projection. Observe that for each such F, we have

$$W_{K,S} = Z_{F,S} \oplus Z'_{F,S}.$$

Then by Lemma 2.6.3, we have

$$W_{K,S} = \left(\sum_{\substack{F \subseteq K \\ [F:\overline{\mathbb{Q}}] \leq n}} Z_{F,S} \right) \oplus \left(\bigcap_{\substack{F \subseteq K \\ [F:\overline{\mathbb{Q}}] \leq n}} Z'_{F,S} \right). \tag{2.6.5}$$

This gives us a decomposition $f = f_n + f'_n$ where

$$f_n \in \sum_{\substack{F \subseteq K \\ [F:\overline{\mathbb{Q}}] \leq n}} Z_{F,S} = V^{(n)} \cap W_{K,S},$$

and

$$f'_n \in \bigcap_{\substack{F \subseteq K \\ [F:\overline{\mathbb{Q}}] \leq n}} Z'_{F,S} = (V^{(n)})^{\perp} \cap W_{K,S},$$

But then $f_n \in V^{(n)}$ and $f'_n \in (V^{(n)})^{\perp}$, so by the uniqueness of the orthogonal decomposition, we must in fact have $f_n = P^{(n)} f$ and $f'_n = Q^{(n)} f = (I - P^{(n)}) f$. Since this proof works for any $f \in \mathcal{F}$, we have established the desired claim. $\square$

Now we observe that the subspaces $V^{(n)}$ with their associated projections $P^{(n)}$, indexed by $\mathbb{N}$ with the usual partial order $\leq$, satisfy the conditions of Theorem 15, and thus we have orthogonal projections $T^{(n)}$ and an orthogonal decomposition

$$\mathcal{F} = \bigoplus_{n=1}^{\infty} T^{(n)}(\mathcal{F}). \tag{2.6.6}$$

The operators $T^{(n)}$ have a particularly simple form in terms of the $P^{(n)}$ projections. The Möbius function for $\mathbb{N}$ under the partial order $\leq$ is well-known and is merely

$$\mu_{\mathbb{N}}(m,n) = \begin{cases} 1 & \text{if } m = n, \\ -1 & \text{if } m = n-1, \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

Thus, $T^{(1)} = P^{(1)} = P_{\mathbb{Q}}$ and

$$T^{(n)} = P^{(n)} - P^{(n-1)} \quad \text{for all} \quad n > 1.$$

We call $T^{(n)}f$ the *degree n component of f*. The following proposition is now obvious from the above constructions:

Proposition 2.6.5. *Each $f \in \mathcal{F}$ has a unique finite expansion into its degree n components, $f^{(n)} = T^{(n)}f \in \mathcal{F}$*

$$f = \sum_{n \in \mathbb{N}} f^{(n)}.$$

Each $f^{(n)}$ term can be written as a finite sum $f^{(n)} = \sum_i f_i^{(n)}$ where $f_i^{(n)} \in \mathcal{F}$ and $\delta(f_i^{(n)}) = n$ for each i, and $f^{(n)}$ cannot be expressed as a finite sum $\sum_j f_j^{(n)}$ with $\delta(f_j^{(n)}) \leq n$ for each j and $\delta(f_j^{(n)}) < n$ for some j.

This completes the proof of Theorem 3. It remains to prove Theorem 4.

Proof of Theorem 4. From Proposition 2.6.2, we see that the operators T_K and $P^{(n)}$ commute for $K \in \mathcal{K}^G$ and $n \in \mathbb{N}$. But $T^{(n)} = P^{(n)} - P^{(n-1)}$ for $n > 1$ and $T^{(1)} = P^{(1)}$, so by the commutativity of T_K with $P^{(n)}$ we have the desired result. In particular, the map $T_K^{(n)} = T^{(n)}T_K : \mathcal{F} \to \mathcal{F}$ is also a projection, and thus we can combine equations (2.5.1) and (2.6.6) to obtain the orthogonal decomposition

$$\mathcal{F} = \bigoplus_{n=1}^{\infty} \bigoplus_{K \in \mathcal{K}^G} T_K^{(n)}(\mathcal{F}). \tag{2.6.7}$$

□

Chapter 3

Reducing the Lehmer problem

3.1 Lehmer irreducibility

Let us recall that we defined in Section 2.6 the orbital degree function $\delta : \mathcal{F} \to \mathbb{N}$ by

$$\delta(f) = \#\{L_\sigma f : \sigma \in G\} = [G : \mathrm{Stab}_G(f)] = [K_f : \mathbb{Q}].$$

Observe that since nonzero scaling of f does not affect its $\mathbb{Q}$-vector space span or the minimal field K_f that the function δ is invariant under nonzero scaling in $\mathcal{F}$, that is,

$$\delta(rf) = \delta(f) \quad \text{for all} \quad f \in \mathcal{F} \text{ and } 0 \neq r \in \mathbb{Q}. \tag{3.1.1}$$

In order to better understand the relationship between our functions in $\mathcal{F}$ and the algebraic numbers from which they arise, we need to understand when a function $f_\alpha \in V_K$ has a representative $\alpha \in K^\times$ or is merely an nth root of an element of $K^\times$ for some $n > 1$. Naturally, the choice of coset representative modulo torsion affects this question, and we would like to avoid such considerations. Therefore we define the function $d : \mathcal{F} \to \mathbb{N}$ by

$$d(f_\alpha) = \min\{\deg(\zeta\alpha) : \zeta \in \mathrm{Tor}(\overline{\mathbb{Q}}^\times)\}. \tag{3.1.2}$$

Notice that the minimum is invariant by construction under the choice of coset representative $\alpha \in \overline{\mathbb{Q}}^\times$ for $f_\alpha \in \mathcal{F}$. In other words, for a given function $f \in \mathcal{F}$, which is an equivalence class of an algebraic number modulo torsion, $d(f)$ gives us the minimum degree amongst all of the algebraic numbers which are coset representatives of the class of f modulo the torsion subgroup.

Notice that a function $f \in \mathcal{F}$ can then be written as $f = f_\alpha$ with $\alpha \in K_f^\times$ if and only if $d(f) = \delta(f)$. We therefore make the following definition:

Definition 3.1.1. We define the set of *Lehmer irreducible* elements of $\mathcal{F}$ to be the set

$$\mathcal{L} = \{f \in \mathcal{F} : \delta(f) = d(f)\}. \tag{3.1.3}$$

The set $\mathcal{L}$ consists precisely of the functions f such that $f = f_\alpha$ for some α of degree equal to the degree of the minimal field of definition K_f of f.

We recall the terminology from [Dub05] that a number $\alpha \in \overline{\mathbb{Q}}^\times$ is *torsion-free* if $\alpha/\sigma\alpha \notin \mathrm{Tor}(\overline{\mathbb{Q}}^\times)$ for all distinct Galois conjugates $\sigma\alpha$. As we observed above in the proof of Proposition 2.2.6, torsion-free numbers give rise to distinct functions $f_{\sigma\alpha} = L_\sigma f_\alpha$ for each distinct Galois conjugate $\sigma\alpha$ of α.

The goal of this section is to prove the following result relating δ and d:

Proposition 3.1.2. *Let $0 \neq f \in \mathcal{F}$ and $r, s \in \mathbb{Z}$ with $(r, s) = 1$. Then the set $R(f) = \{q \in \mathbb{Q} : qf \in \mathcal{L}\}$ satisfies*

$$R(f) = \frac{\ell}{n}\mathbb{Z}$$

where $\ell, n \in \mathbb{N}$, $(\ell, n) = 1$, *and*

$$d((r/s)f) = \frac{\ell s}{(\ell, r)(n, s)}\delta(f). \tag{3.1.4}$$

In particular, $d(f) = \ell \cdot \delta(f)$.

The proof of Proposition 3.1.2 consists of showing that $R(f)$ is a fractional ideal of $\mathbb{Q}$ which scales according to $R(qf) = (1/q)R(f)$, and that when f is scaled so that $R(f) = \mathbb{Z}$ we have $d((r/s)f) = s\delta(f)$. We establish these results in a series of lemmas below. We begin by demonstrating the most basic results concerning Lehmer irreducibility:

Lemma 3.1.3. *We have the following results:*

1. *For each* $f \in \mathcal{F}$, *there is a unique minimal exponent* $\ell = \ell(f) \in \mathbb{N}$ *such that* $\ell f \in \mathcal{L}$.
2. *For any* $\alpha \in \overline{\mathbb{Q}}^\times$, *we have* $\delta(f_\alpha) | \deg \alpha$.
3. $f \in \mathcal{L}$ *if and only if it has a representative in* $\overline{\mathbb{Q}}^\times$ *which is torsion-free.*
4. *Every torsion-free representative of* $f \in \mathcal{L}$ *lies in the same field* K_f, *the minimal field of* f.

Proof. Choose a representative $\alpha \in \overline{\mathbb{Q}}^\times$ such that $f = f_\alpha$ and let

$$\ell = \operatorname{lcm}\{\operatorname{ord}(\alpha/\sigma\alpha) : \sigma \in G \text{ and } \alpha/\sigma\alpha \in \operatorname{Tor}(\overline{\mathbb{Q}}^\times)\}$$

where $\operatorname{ord}(\zeta)$ denotes the order of an element $\zeta \in \operatorname{Tor}(\overline{\mathbb{Q}}^\times)$. Then observe that α^ℓ is torsion-free. Clearly, $\mathbb{Q}(\alpha^\ell) \subset \mathbb{Q}(\alpha)$ so $[\mathbb{Q}(\alpha^\ell) : \mathbb{Q}] | [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Now if

a number $\beta \in \overline{\mathbb{Q}}^\times$ is torsion-free, then since each distinct conjugate $\sigma\beta$ gives rise to a distinct function in $\mathcal{F}$, we have

$$\deg \beta = [G : \mathrm{Stab}_G(f_\beta)] = [K_{f_\beta} : \mathbb{Q}] = \delta(f_\beta).$$

Thus $\deg \alpha^\ell = \delta(f_\alpha)$ and we have proven existence in the first claim. The existence of a minimum value follows since $\mathbb{N}$ is discrete. To prove the second claim it now suffices to observe that since δ is invariant under scaling, with the choice of ℓ as above, we have $\delta(f_\alpha) = \delta(f_\alpha^\ell)|\deg \alpha$ for all $\alpha \in \overline{\mathbb{Q}}^\times$. The third claim now follows immediately. Lastly, since any representative of f differs by a root of unity, each representative has some power which lies in (and generates) the minimal field, and thus each torsion-free representative generates the minimal field. □

We note the following easy corollary for its independent interest:

Corollary 3.1.4. *Let $\alpha \in \overline{\mathbb{Q}}^\times$ have minimal polynomial $F(x) \in \mathbb{Z}[x]$. Let $G(x) \in \mathbb{Z}[x]$ be an irreducible polynomial of smallest degree in $\mathbb{Z}[x]$ such that there exists some $k \in \mathbb{N}$ with $F(x)|G(x^k)$. Then $\delta(f_\alpha) = \deg G$.*

(We observe in passing that $\delta(f) = 1$ if and only if $f \in V_\mathbb{Q}$, in which case, $f = f_\alpha$ where $\alpha^n \in \mathbb{Q}^\times$ and so f represents a *surd*, that is, a root of a rational number.)

Lemma 3.1.5. *If $0 \neq f \in \mathcal{F}$, then $R(f) = \{r \in \mathbb{Q} : rf \in \mathcal{L}\}$ is a fractional ideal of $\mathbb{Q}$, that is, $R(f) = r\mathbb{Z}$ for some $r \in \mathbb{Q}$.*

Proof. We can assume $\delta(f) > 1$, otherwise f arises from a surd and the proof is trivial. First we show that $R(f)$ is a $\mathbb{Z}$-module. It is trivial that if $r \in R(f)$ then $-r \in R(f)$ as inversion does not affect degree. Suppose now that we have $r, s \in R(f)$ and choose torsion-free representatives $\beta \in \overline{\mathbb{Q}}^\times$ of rf and $\gamma \in \overline{\mathbb{Q}}^\times$ of sf. If $r + s = 0$ the result is trivial, so suppose not. By Lemma 3.1.3 (4), we have $\beta, \gamma \in K_f$. But then $\beta\gamma \in K_f$ as well, and hence is a representative of $f_{\beta\gamma} = f_\beta + f_\gamma = rf + sf = (r + s)f$ of degree $[K_f : \mathbb{Q}] = \delta(f)$, and thus we have $r + s \in R(f)$ as well.

If we can now show that $R(f)$ is finitely generated the proof will be complete, as it is easy to check that any finitely generated $\mathbb{Z}$-submodule of $\mathbb{Q}$ is indeed a fractional ideal. But were it to require an infinite number of generators, we would have to have elements of arbitrarily large denominator. Further, we could fix an N sufficiently large so that for a sequence of $n_i \to \infty$, we would have some $r_i/n_i \in R(f)$ and $|r_i/n_i| \leq N$. (For example, given r_1/n_1, we can take $N = r_1/n_1$ by appropriately subtracting off multiples of r_1/n_1 from any other r_i/n_i.) But then we would have torsion-free representatives α^{r_i/n_i} satisfying $h(\alpha^{r_i/n_i}) \leq N\, h(\alpha)$, and as Lehmer irreducible representatives, each representative has the same degree $\delta(f)$, and thus we have an infinite number of algebraic numbers with bounded height and degree, contradicting Northcott's theorem. □

Lemma 3.1.6. *Let $0 \neq q \in \mathbb{Q}$. Then $R(qf) = \frac{1}{q}R(f)$.*

Proof. This is clear from the definition. □

Lemma 3.1.7. *Let $f \in \mathcal{L}$ with $R(f) = \mathbb{Z}$ and let $m, n \in \mathbb{Z}$ where $(m, n) = 1$ and $n > 0$. Let α be a torsion-free representative of f and denote by $\alpha^{m/n}$ any representative of the class of $f_{\alpha^{m/n}} = (m/n)f$ modulo torsion of minimal degree. Then $\deg \alpha^{m/n} = n \deg \alpha$. In particular, we have*

$$d((m/n)f) = n\, d(f) = n\, \delta(f) \quad \text{if} \quad R(f) = \mathbb{Z}. \tag{3.1.5}$$

Proof. Since $R(f) = \mathbb{Z}$, our choice of torsion-free representative β in $\overline{\mathbb{Q}}^{\times}$ has degree $\delta(f)$. Clearly, we can say that $d((m/n)f) \leq n \deg \alpha = n\, \delta(f)$ because any root of $x^n - \alpha^m$ over $\mathbb{Q}(\alpha)$ will be a representative of the class of $(m/n)f$. Observe that the minimal field $K_f = \mathbb{Q}(\alpha)$ is, as we observed above, unique, and thus the choice of α differs at most by some torsion element of $\mathbb{Q}(\alpha)^{\times}$. Further, any choice of representative $\beta \in \overline{\mathbb{Q}}^{\times}$ of $(m/n)f$ will satisfy $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\beta)$ since some power of β will make it torsion-free and therefore it will be a power of α.

Let us show that the degree of β cannot satisfy $\deg \beta < n \deg \alpha$ if $R(f) = \mathbb{Z}$. Suppose it did, so that $k = [\mathbb{Q}(\beta) : \mathbb{Q}(\alpha)] < n$. Then observe that by taking the algebraic norm down to $\mathbb{Q}(\alpha)$, we have

$$\mathrm{Norm}_{\mathbb{Q}(\alpha)}^{\mathbb{Q}(\beta)}(\beta) = \zeta \alpha^{km/n} \in \mathbb{Q}(\alpha)$$

where ζ is a root of unity. As $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \delta(f)$ the existence of the representative $\zeta \alpha^{km/n}$ would imply that $km/n \in R(f)$, but since $(m, n) = 1$ and $k < n$, we have $km/n \notin \mathbb{Z}$. This contradicts our assumption that $R(f) = \mathbb{Z}$. $\square$

Combining the above lemmas, we now see that we have proven Proposition 3.1.2.

3.2 Reduction to Lehmer irreducible numbers

We will now show that we can reduce questions related to lower bounds for the L^p Mahler measure to the set of Lehmer irreducible elements. We begin with two lemmas regarding the relationship between the projection operators P_K and the degree functions d and δ which will be used below:

Lemma 3.2.1. *If $f \in \mathcal{F}$ and $K \subset K_f$, then $d(P_K f) \leq d(f)$.*

Proof. Let $f = f_\alpha$ and let $\alpha \in \overline{\mathbb{Q}}^\times$ be a minimal degree representative of f, and choose $\ell \in \mathbb{N}$ such that α^ℓ is torsion-free. Then $\mathbb{Q}(\alpha^\ell) = K_f$, so in particular, we see that

$$K \subseteq K_f \subseteq \mathbb{Q}(\alpha).$$

Observe that the norm $N_K^{K(\alpha)}$, as a group homomorphism from $K(\alpha)^\times$ to $K^\times$, is necessarily well-defined modulo torsion. Taking some $1/[K(\alpha) : K]$th root, we have $(N_K^{K(\alpha)}\alpha)^{1/[K(\alpha):K]}$ is a representative of $P_K f_\alpha$ modulo torsion, and it follows from the fact that $N_K^{K(\alpha)}\alpha \in K$ that

$$\begin{aligned} d(P_K f) \leq \deg(N_K^{K(\alpha)}\alpha)^{1/[K(\alpha):K]} &\leq [K(\alpha) : K] \cdot [K : \mathbb{Q}] \\ &= [\mathbb{Q}(\alpha) : \mathbb{Q}] = d(f). \quad \square \end{aligned}$$

Lemma 3.2.2. *If $K \in \mathcal{K}$ and $K \subset K_f$ for $f \in \mathcal{F}$, we have $\delta(P_K f) \leq \delta(f)$.*

Proof. Since we can rescale f without affecting either δ value, we can assume $f \in \mathcal{L}$ so $d(f) = \delta(f)$. Let $F = K_f$. Then by Lemma 3.2.1 above, we have

$$\delta(P_K f) \leq d(P_K f) \leq d(f) = \delta(f). \qquad \square$$

From the construction of d above, it is easy to see that:

Proposition 3.2.3. *Let $m_p : \mathcal{F} \to [0, \infty)$ be given by $m_p(f) = d(f) \cdot \|f\|_p$. Fix $0 \neq f \in \mathcal{F}$. Then*

$$m_p(f) = \min\{(\deg \alpha) \cdot h_p(\alpha) : \alpha \in \overline{\mathbb{Q}}^\times, f_\alpha = f\}.$$

The right hand side of this equation is the minimum of the L^p analogue of the usual logarithmic Mahler measure on $\overline{\mathbb{Q}}^\times$ taken over all representatives of f modulo torsion.

We now prove the reduction to $\mathcal{L} \subset \mathcal{F}$:

Proposition 3.2.4. *Let $m_p(f) = d(f) \cdot \|f\|_p$. Then $m_p(\mathcal{F}) = m_p(\mathcal{L})$, so in particular,* $\inf m_p(\mathcal{F} \setminus \{0\}) > 0$ *if and only if* $\inf m_p(\mathcal{L} \setminus \{0\}) > 0$.

Proof. Let $f \in \mathcal{F}$ and $\ell = \ell(f)$. Then by Proposition 3.1.2 we have $\delta(f) = d(\ell f)$ and $\ell\, \delta(f) = d(f)$, and thus

$$m_p(\ell f) = \delta(f) \cdot \|\ell f\|_p = \ell\, \delta(f) \|f\|_p = d(f) \cdot \|f\|_p = m_p(f). \qquad \square$$

Remark 3.2.5. Proposition 3.2.4, which will be used below in the proof of Theorem 6, is a key step in constructing equivalent statements of Lehmer's

conjecture for heights which scale, such as $\delta\, h_p$ and particularly for the norms we will construct. Consider for example that if $\alpha = 2^{1/n}$ then $\delta(f_\alpha) = 1$ for all $n \in \mathbb{N}$ and $h_1(2^{1/n}) = (2\log 2)/n \to 0$.

3.3 Projection irreducibility

In this section we introduce the last criterion which we will require to reduce the Lehmer conjectures to a small enough set of algebraic numbers to prove our main results.

Definition 3.3.1. We say $f \in \mathcal{F}$ is *projection irreducible* if $P_K(f) = 0$ for all proper subfields K of the minimal field K_f. We denote the collection of projection irreducible elements by $\mathcal{P} \subset \mathcal{F}$.

Remark 3.3.2. Notice that we cannot in general require that $P_K(f) = 0$ for all $K \neq K_f$, as an element with a minimal field which is not Galois will typically have nontrivial projections to the conjugates of its minimal fields. See Remark 2.5.2 above for more details.

We now prove that we can reduce questions about lower bounds on the Mahler measure m_p to elements of $\mathcal{P}$:

Proposition 3.3.3. *We have*

$$\inf_{f\in\mathcal{F}\setminus\{0\}} m_p(f) > 0 \quad \Longleftrightarrow \quad \inf_{f\in\mathcal{P}\setminus\{0\}} m_p(f) > 0.$$

Proof. Let $f \in \mathcal{F}$. Notice that for any $K \in \mathcal{K}$ that by Lemma 3.2.1 we have $d(P_K f) \leq d(f)$ and by Lemma 2.3.2 we have $h_p(P_K f) \leq h_p(f)$, so $m_p(P_K \alpha) \leq$

$m_p(f)$. Let $\mathrm{supp}_{\mathcal{K}}(f) = \{K \in \mathcal{K} : P_K f \neq 0\}$. Notice that if $K \subset L$ and $K \in \mathrm{supp}_{\mathcal{K}}(f)$, then $L \in \mathrm{supp}_{\mathcal{K}}(f)$. Let E denote the Galois closure of K_f, and observe that $P_K f = P_K(P_E f) = P_{K\cap E} f$ by Lemma 2.3.9, so since we have only a finite number of subfields of E, we can write $\mathrm{supp}_{\mathcal{K}}(f) = \bigcup_{i=1}^{n} [K_i, \ )$ where $[K_i, \ ) = \{L \in \mathcal{K} : K_i \subseteq L\}$, and each $K_i \subseteq E$ is minimal in the sense that $[K_i, \ ) \not\subseteq [K_j, \ )$ for all $i \neq j$. Thus, for each i, $P_F f = 0$ for all $F \subsetneq K_i$, and so $P_{K_i} f \in \mathcal{P} \setminus \{0\}$. Then $0 < m_p(P_{K_i} f) \leq m_p(f)$, and so we have shown $\inf_{f\in\mathcal{P}\setminus\{0\}} m_p(f) \leq \inf_{f\in\mathcal{F}\setminus\{0\}} m_p(f)$. The reverse inequality is trivial. $\square$

Chapter 4

The Mahler p-norm

4.1 An L^p analogue of Northcott's theorem

We begin by proving an analogue of Northcott's theorem for the L^p Weil heights which we will make use of in this chapter. We begin with some easy lemmas which relate the L^p height to the L^1 height.

Lemma 4.1.1. *Let $f \in \mathcal{F}$ and suppose $\mathrm{supp}(f) \subseteq Y(\mathbb{Q}, \pi)$ for some rational prime π (possibly infinity). Then for $1 < p \leq \infty$, we have*

$$\|f\|_1 \leq \|f\|_p \leq \delta(f)^{1-1/p}\|f\|_1.$$

(We follow the usual convention for exponents and let $1/p = 0$ when $p = \infty$ for convenience.)

Proof. The first inequality in fact is a well-known fact of L^p norms on measure one spaces, however, we will give another proof in this case as it is useful to do so. Let $K = K_f$ be the minimal field, so in particular, $[K : \mathbb{Q}] = \delta(f)$. Let $n = \delta(f)$ denote this common value. Then $Y(\mathbb{Q}, \pi)$ can be partitioned into a disjoint union of the sets $Y(K, v)$ for $v|\pi$. Notice that $\lambda(Y(K, v)) = d_v/n$ for each v, where $d_v = [K_v : \mathbb{Q}_v]$ is the local degree. Enumerate the set of v lying over π as $v_1, \ldots, v_n$, counting each place d_v times, so that if, for example,

$d_v = 3$, then there will be three places v_k, v_{k+1}, v_{k+2} corresponding to v (for some number k). Let c_i denote the value of $f(y)$ on $Y(K, v_i)$. Let q be the usual conjugate exponent determined by $1/p + 1/q = 1$. Then observe that:

$$\|f\|_1 = \frac{1}{n}\sum_{i=1}^{n}|c_i| \leq \frac{1}{n}\cdot n^{1/q}\bigg(\sum_{i=1}^{n}|c_i|^p\bigg)^{1/p} = \frac{1}{n^{1/p}}\bigg(\sum_{i=1}^{n}|c_i|^p\bigg)^{1/p} = \|f\|_p.$$

where we have applied Hölder's inequality. For the upper bound, we compute

$$\|f\|_p = \frac{1}{n^{1/p}}\bigg(\sum_{i=1}^{n}|c_i|^p\bigg)^{1/p} \leq \frac{1}{n^{1/p}}\sum_{i=1}^{n}|c_i| = n^{1-1/p}\cdot\frac{1}{n}\sum_{i=1}^{n}|c_i| = n^{1-1/p}\|f\|_1$$

from which the result now follows. □

We now bound our heights without assuming that f is supported on a single prime:

Proposition 4.1.2. *Let $f \in \mathcal{F}$ and $1 < p \leq \infty$. Then we have the following inequalities:*

$$\|f\|_1 \leq \lambda(\operatorname{supp} f)^{1-1/p}\,\|f\|_p \quad \textit{and} \quad \|f\|_p \leq \delta(f)^{1-1/p}\|f\|_1. \tag{4.1.1}$$

Proof. Let q be given by $1/p + 1/q = 1$ as usual. Then the first inequality is just the usual application of Hölder's inequality:

$$\|f\|_1 = \int_{\operatorname{supp} f}|f(y)|\,d\lambda(y) \leq \bigg(\int_{\operatorname{supp} f}1^q\,d\lambda(y)\bigg)^{1/q}\bigg(\int_{\operatorname{supp} f}|f(y)|^p\,d\lambda(y)\bigg)^{1/p} = \lambda(\operatorname{supp} f)^{1/q}\|f\|_p.$$

For the second inequality, let us write $f|_\pi$ for the restriction of f to the set $Y(\mathbb{Q}, \pi)$. Then $f|_\pi$ is a function on a measure one space, so locally we can

make use of the above lemma at each place π:

$$\|f\|_p = \Big(\sum_{\pi \in M_{\mathbb{Q}}} \|f|_\pi\|_p^p \Big)^{1/p} \leq \Big(\sum_{\pi \in M_{\mathbb{Q}}} \delta(f)^{p/q} \|f|_\pi\|_1^p \Big)^{1/p}$$
$$= \delta(f)^{1/q} \Big(\sum_{\pi \in M_{\mathbb{Q}}} \|f|_\pi\|_1^p \Big)^{1/p} \leq \delta(f)^{1/q} \sum_{\pi \in M_{\mathbb{Q}}} \|f|_\pi\|_1 = \delta(f)^{1-1/p} \|f\|_1. \quad \square$$

where we make use of the general fact that for any sequence $x \in \ell^p(\mathbb{N})$, we have $\|x\|_{\ell^p} \leq \|x\|_{\ell^1}$. (In fact, each $f \in \mathcal{F}$ is supported on a finite number of rational primes, so there is no issue of convergence here.)

The classical Northcott theorem tells us that any set of algebraic numbers of bounded height and degree is finite. As $2h(\alpha) = \|f_\alpha\|_1$, this translates to a bound on the L^1 height. Naturally, as we are working in $\mathcal{F}$, we count modulo torsion, but even so we must be careful about the choice of our notion of degree (indeed, it is easy to see that the number of elements of $\mathcal{F}$ with bounded δ and L^p norm is not finite).

Theorem 16 (L^p Northcott)**.** *For any $C, D > 0$, we have*

$$\#\{f \in \mathcal{L} : \|f\|_p \leq C \text{ and } \delta(f) \leq D\} < \infty, \tag{4.1.2}$$

and

$$\#\{f \in \mathcal{F} : \|f\|_p \leq C \text{ and } d(f) \leq D\} < \infty. \tag{4.1.3}$$

Proof. Notice that $f \in \mathcal{L}$ implies that $d(f) = \delta(f)$ by definition, so that the first set is a subset of the second. Thus, it suffices to show that the second set is finite. Each element f_α of the second set gives rise to a representative

$\alpha \in \overline{\mathbb{Q}}^{\times}$ with degree $d(f_\alpha)$, so if we can show that $h(\alpha)$ is bounded, then Northcott's theorem will give us the desired result. Notice that if $f \in \mathcal{F}$ has nontrivial support at a rational prime π, then

$$\|f\|_p \geq \|f|_{Y(\mathbb{Q},\pi)}\|_p \geq \|f|_{Y(\mathbb{Q},\pi)}\|_1 \geq \frac{\log \pi}{d(f)} \geq \frac{\log \pi}{D}.$$

As we assume that $\|f\|_p \leq C$, this tells us that $\log \pi \leq CD$. This places a limit on the possible support of f on nonarchimedean places. In particular, since the measure λ assigns measure 1 to any rational prime, we see that

$$\lambda(\mathrm{supp}(f)) \leq 1 + \pi(\exp(CD))$$

where $\pi(x)$ is the usual prime counting function. Thus, by Proposition 4.1.2, we see that

$$\|f\|_1 \leq \lambda(\mathrm{supp}(f))^{1-1/p} \|f\|_p \leq (1 + \pi(\exp(CD)))^{1-1/p}\, C. \tag{4.1.4}$$

As $2h(\alpha) = \|f_\alpha\|_1$, this gives a bound on the classical Weil height for any representative of an element of our set. Northcott's theorem then applies and gives us the desired result, as we find we have a finite number of possible coset representatives and therefore a finite number of elements of $\mathcal{F}$. □

4.2 The Mahler p-norms and proof of Theorem 6

We will now make use of our orthogonal decomposition (2.6.6) to define one of the main operators of our study. Let

$$\begin{aligned} M : \mathcal{F} &\to \mathcal{F} \\ f &\mapsto \sum_{n=1}^{\infty} n\, T^{(n)} f. \end{aligned} \tag{4.2.1}$$

The M operator serves the purpose of allowing us to scale a function in $\mathcal{F}$ by its appropriate degree while still being linear. As each element of $\mathcal{F}$ has a finite expansion in terms of $T^{(n)}$ components, the above map is well-defined. Further, it is easily seen to be linear by the linearity of the $T^{(n)}$, and it is also a bijection. However, it is not a bounded operator (and thus, in particular, M is not well-defined on the space $L^p(Y)$):

Proposition 4.2.1. *The linear operator $M : \mathcal{F} \to \mathcal{F}$ is unbounded in any L^p norm.*

Proof. Below in Propositions 4.3.1, 4.3.2, and 4.2.3 we will prove that every Salem number $\tau > 1$ is Lehmer irreducible, projection irreducible, and therefore, an eigenvector of the M operator of eigenvalue $\delta(f_\tau)$, that is, $f_\tau \in \mathcal{L} \cap \mathcal{P}$, $K_\tau = \mathbb{Q}(\tau)$, and $Mf_\tau = \delta(f_\tau) \cdot f_\tau = d(f_\tau) \cdot f_\tau$. As there exist Salem numbers of arbitrarily large degree, M has eigenvectors of arbitrarily large eigenvalue and we obtain the desired result. □

We define the Mahler p-norm on $\mathcal{F}$ to be

$$\|f\|_{m,p} = \|Mf\|_p \tag{4.2.2}$$

where $\|\cdot\|_p$ denotes the usual L^p norm as defined above.

Proposition 4.2.2. *The map $\|\cdot\|_{m,p} : \mathcal{F} \to [0, \infty)$ is a vector space norm on $\mathcal{F}$.*

Proof. This follows easily from the fact that M is an invertible linear operator on $\mathcal{F}$. Specifically, we have for all $f, g \in \mathcal{F}$ and $r \in \mathbb{Q}$,

$$\|f\|_{m,p} = \|Mf\|_p = 0 \iff Mf = 0 \iff f = 0$$

because M is invertible and $\|\cdot\|_p$ is a norm on $\mathcal{F}$, and

$$\|f+g\|_{m,p} = \|M(f+g)\|_p = \|Mf+Mg\|_p \leq \|Mf\|_p+\|Mg\|_p = \|f\|_{m,p}+\|g\|_{m,p},$$

and

$$\|rf\|_{m,p} = \|M(rf)\|_p = \|rMf\|_p = |r| \cdot \|Mf\|_p = |r| \cdot \|f\|_{m,p}$$

by the linearity of M. □

The following proposition, interesting in its own right, will be useful to us below:

Proposition 4.2.3. *If $f \in \mathcal{P}$, then $T^{(\delta(f))}f = f$, and in particular f is an eigenvector of the M operator with eigenvalue $\delta(f)$.*

Proof. Let $n = \delta(f)$ and $K = K_f$ be the minimal field of f. Obviously, as $f \in V_K$ and $[K_f : \mathbb{Q}] = \delta(f) = n$, we have $P^{(n)}f = f$. Since

$$P^{(n)} = \sum_{k=1}^{n} T^{(k)},$$

we can find a minimal value $1 \leq m \leq n$ such that $T^{(m)}f \neq 0$. Then $T^{(m)}f = P^{(m)}f$ for this value. We claim that if $m < n$, then f is not projection irreducible. To see this, observe that from the proof of Proposition 2.6.4, p. 46, we found equation (2.6.5), which, together with the commutativity of $P^{(m)}$

and the T_K operators and expanding the set of primes S appropriately (every element of V_K is an S-unit for a large enough set of primes S of K) tells us that in fact, the $P^{(m)}$ projection corresponds to the $\mathbb{Q}$-vector space direct sum decomposition:

$$V_K = P^{(m)}(V_K) \oplus Q^{(m)}(V_K) = \Bigg(\sum_{\substack{F \subseteq K \\ [F:\mathbb{Q}] \leq m}} P_F(V_K) \Bigg) \oplus \Bigg(\bigcap_{\substack{F \subseteq K \\ [F:\mathbb{Q}] \leq m}} Q_F(V_K) \Bigg), \tag{4.2.3}$$

where $Q^{(m)} = I - P^{(m)}$ and $Q_F = I - P_F$ are the complementary projections. (Technically, we should replace K with its Galois closure to match the construction in the proof of Proposition 2.6.4, but observe that we can repeat the construction starting with $V_{K,S}$ for K any number field instead of using $T_K(V_{K,S})$ for K Galois; the results are the same, as it is only the finite dimensionality of the S-unit space $V_{K,S}$ that is essential to the construction). If $P_F(f) = 0$ then $Q_F(f) = f$, so if f had no nontrivial projections to any proper subfields of f, it would also have decomposition $f = 0 \oplus f$ and thus $P^{(m)}f = 0$. Thus if $P^{(m)}f \neq 0$ then $P_F(f) \neq 0$ for some $F \subsetneq K$, but this is a contradiction to the projection irreducibility of f. Hence we must have had $T^{(n)}f = f$. □

We can complete $\mathcal{F}$ with respect to $\| \cdot \|_{m,p}$ to obtain a real Banach space which we denote $\mathcal{F}_{m,p}$. We are now ready to prove Theorem 6, which we restate for the reader's convenience. First, we recall the L^p analogue of the Lehmer conjecture (Conjecture 5) from above:

$$m_p(\alpha) = (\deg \alpha) \cdot h_p(\alpha) \geq c_p > 0 \quad \text{for all} \quad \alpha \in \overline{\mathbb{Q}}^\times \setminus \mathrm{Tor}(\overline{\mathbb{Q}}^\times). \tag{$*_p$}$$

Theorem 6. *For each $1 \leq p \leq \infty$, equation $(*_p)$ holds if and only if*

$$\|f\|_{m,p} \geq c_p > 0 \quad \textit{for all} \quad 0 \neq f \in \mathcal{L} \cap \mathcal{P} \cap \mathcal{U} \tag{$**_p$}$$

where $\mathcal{L}$ denotes the set of Lehmer irreducible elements, $\mathcal{P}$ the set of projection irreducible elements, and $\mathcal{U}$ the subspace of algebraic units. Further, for $1 \leq p \leq q \leq \infty$, if equation $(*_p)$ holds for p then equation $(*_p)$ holds for q as well.

Proof of Theorem 6. First let us show that it suffices to bound $m_p(f)$ away from zero for $f \in \mathcal{L} \cap \mathcal{P} \cap \mathcal{U}$. Let $f \in \mathcal{F}$. We begin by reducing to the vector space $\mathcal{U} = \{f \in \mathcal{F} : \mathrm{supp}_Y(f) \subseteq Y(\mathbb{Q}, \infty)\}$. If $1 \leq p < \infty$, observe that

$$h_p(f) = \|f\|_p = \left(\sum_{\pi \in M_{\mathbb{Q}}} \|f|_{Y(\mathbb{Q},\pi)}\|_p^p \right)^{1/p} \geq \|f|_{Y(\mathbb{Q},\pi)}\|_p \geq \|f|_{Y(\mathbb{Q},\pi)}\|_1,$$

since $Y(\mathbb{Q}, \pi)$ is a space of measure 1. Likewise, it is easy to see that

$$h_\infty(f) = \max_{\pi \in M_{\mathbb{Q}}} \|f|_{Y(\mathbb{Q},\pi)}\|_\infty \geq \|f|_{Y(\mathbb{Q},\pi)}\|_\infty \geq \|f|_{Y(\mathbb{Q},\pi)}\|_1$$

for a specific rational prime π, so we can let $p = \infty$ as well. Let the rational prime π be chosen above so that the norm of the restriction to $Y(\mathbb{Q}, \pi)$ is nonzero, which we can do if $f \notin \mathcal{U}$. Let $\alpha \in \overline{\mathbb{Q}}^\times$ be a representative of minimal degree $d(f)$ for f. Then α has a nontrivial valuation over π, and since the product of α over all of its conjugates must be in $\mathbb{Q}$, we know that we must have $\|f|_{Y(\mathbb{Q},p)}\|_1 \geq (\log \pi)/d(f)$. Thus $h_p(f) \geq (\log 2)/d(f)$, so $m_p(f) \geq \log 2$ for $1 \leq p \leq \infty$ if $f \notin \mathcal{U}$. Now it remains to show that we can reduce to the consideration of $\mathcal{P}$ as well, but this now follows immediately from the technique of the proof in Proposition 3.3.3, p. 57 above, specifically, by projecting to a

minimal field F in the $\mathcal{K}$-support of f to ensure projection irreducibility, and observing that by Lemma 2.3.1, p. 28, $P_F(f) \in \mathcal{U}$ if $f \in \mathcal{U}$. Now observe that if $f \in \mathcal{U} \cap \mathcal{P}$, then upon scaling f it remains in $\mathcal{U} \cap \mathcal{P}$, so we are free to replace f by $\ell(f)f$ as in the proof of Proposition 3.2.4, p. 56 without changing the value of $m_p(f)$, and thus we can assume $f \in \mathcal{L} \cap \mathcal{P} \cap \mathcal{U}$, as claimed.

Now let $f \in \mathcal{L} \cap \mathcal{P} \cap \mathcal{U}$, and we will show that $m_p(f) = \|f\|_{m,p}$, completing the proof of the equivalence. Observe that for such an element, by Proposition 4.2.3 projection irreducibility, we must have $T^{(n)}f = f$ where $n = \delta(f) = [K_f : \mathbb{Q}]$ for K_f the minimal field of f, and in particular, $Mf = nf$. Thus

$$\|f\|_{m,p} = \|Mf\|_p = [K_f : \mathbb{Q}] \cdot \|f\|_p = \delta(f)h_p(f) = d(f)h_p(f) = m_p(f)$$

where the second equality follows from the fact that $f \in \mathcal{P}$ and the fourth from the fact that $f \in \mathcal{L}$. This completes the equivalence of the bounds.

To show that for $1 \leq p \leq q \leq \infty$ the result for p implies the result for q, we observe that having reduced the problem to the study of algebraic units $\mathcal{U} = \{f \in \mathcal{F} : \mathrm{supp}(f) \subseteq Y(\mathbb{Q}, \infty)\}$, and since $\lambda(Y(\mathbb{Q}, \infty)) = 1$, we are reduced to the consideration of measurable functions on a probability space $(Y(\mathbb{Q}, \infty), \lambda)$. But on such a space one has the usual inequality $\|f\|_p \leq \|f\|_q$ (see also Proposition 4.1.2 above) and thus $\|f\|_{m,p} = \|Mf\|_p \leq \|Mf\|_q = \|f\|_{m,q}$. □

Lastly, we note for its own interest:

Proposition 4.2.4. *Equation* $(*_p)$ *for* $p = 1$ *is equivalent to the Lehmer conjecture, and for* $p = \infty$, $(*_p)$ *is equivalent to the Schinzel-Zassenhaus conjecture.*

Proof. Since $h = 2h_1$ it is obvious that $m_1 = 2m$ so we exactly have the statement of the Lehmer conjecture when $p = 1$. Let us now show that when $p = \infty$, equation $(*_p)$ is equivalent to the Schinzel-Zassenhaus conjecture. Recall that the house $\overline{|\alpha|} = \max\{|\sigma\alpha| : \sigma : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}\}$ where $|\cdot|$ denotes the usual Euclidean absolute on $\mathbb{C}$. The Schinzel-Zassenhaus conjecture [SZ65] states that for an algebraic integer α, $(\deg \alpha) \cdot \log \overline{|\alpha|}$ is bounded away from zero by an absolute constant. Observe that by Smyth's well-known theorem [Smy71], we have $m_1(\alpha) \geq c > 0$ for an absolute constant c if α is not reciprocal. Since $\|f\|_{m,\infty} \geq \|f\|_{m,1} = m_1(f)$ for the numbers under consideration, we see that if α is not reciprocal, then there is nothing more to show by the previous theorem. If α is reciprocal, then observe that α and α^{-1} are conjugate, and so $\overline{|\alpha|} = \max\{\overline{|\alpha|}, \overline{|\alpha^{-1}|}\}$, where $\max\{\overline{|\alpha|}, \overline{|\alpha^{-1}|}\}$ is called the *symmetric house*. Now, it is easy to see that $h_\infty(\alpha) = \log \max\{\overline{|\alpha|}, \overline{|\alpha^{-1}|}\}$ is the logarithmic symmetric house of α for $f_\alpha \in \mathcal{U}$, so we do indeed recover the Schinzel-Zassenhaus conjecture when $p = \infty$.[1] □

[1] We remark in passing that while h_∞ agrees with the logarithmic symmetric house on $\mathcal{U}$, h_∞ seems to be a better choice for non-integers as well, as, for example, $h_\infty(3/2) = \log 3$ while the logarithmic symmetric house of $3/2$ is $\log(3/2)$.

4.3 Explicit values

We now evaluate the Mahler p-norms for two classes of algebraic numbers, surds and Salem numbers. Salem numbers are conjectured to be of minimal Mahler measure for the classical Lehmer conjecture. This is in part due to the fact that the minimal value for the Mahler measure known, dating back to Lehmer's original 1933 paper [Leh33], is that of the Salem number called Lehmer's $\tau > 1$, the larger positive real root of the irreducible polynomial $x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$. Here we show that, in fact, Salem numbers belong to the set $\mathcal{L} \cap \mathcal{P} \cap \mathcal{U}$.

4.3.1 Surds

Recall that a *surd* is an algebraic number which is a root of a rational number. In particular, if $\alpha \in \overline{\mathbb{Q}}^\times$ is a surd, then $\alpha^n \in \mathbb{Q}^\times$ for some n. Therefore, an element $f \in \mathcal{F}$ is represented by a surd if and only if $f \in V_\mathbb{Q}$, or equivalently $\delta(f) = 1$. As $\mathbb{Q}$ has no proper subfields, all surds are trivially projection irreducible. Thus, for a surd f,

$$\|f\|_{m,p} = \delta(f)\|f\|_p = \|f\|_p = h_p(f).$$

4.3.2 Pisot and Salem numbers

We say that $f_\tau \in \mathcal{F}$ is Pisot or Salem number if it has a representative $\tau \in \overline{\mathbb{Q}}^\times$ which is a Pisot or Salem number, respectively. Recall that $\tau > 1$ is said to be a Pisot number if τ is an algebraic integer whose conjugates in the complex plane all lie strictly within the unit circle, and that $\tau > 1$ is a Salem

number if τ is algebraic unit which is reciprocal and has all conjugates except τ and τ^{-1} on the unit circle in the complex plane (with at least one pair of conjugates on the circle).

Proposition 4.3.1. *Every Pisot or Salem number f_τ is Lehmer irreducible, that is, $f_\tau \in \mathcal{L}$.*

Proof. Observe that for a Pisot or Salem number f_τ and its given representative $\tau > 1, \overline{\tau} = \tau$ and all other Galois conjugates τ' have $|\tau'| < |\tau|$. Therefore τ is Lehmer irreducible, since if $\delta(f_\tau) < \deg \tau$, then each equivalence class modulo torsion would have more than one member, and in particular the real root $\tau > 1$ would not uniquely possess the largest modulus, as $\zeta\tau$ would be a conjugate for some $1 \neq \zeta \in \mathrm{Tor}(\overline{\mathbb{Q}}^\times)$ which would have the same modulus, a contradiction. Since f_τ has a representative of degree $\delta(f_\tau)$, we have by definition $f_\tau \in \mathcal{L}$. □

Proposition 4.3.2. *Every Salem number τ is projection irreducible and an algebraic unit, and therefore $f_\tau \in \mathcal{L} \cap \mathcal{U} \cap \mathcal{P}$.*

Proof. That τ is a unit is well-known and follows immediately from being a reciprocal algebraic integer. Suppose f_τ has its distinguished representative $\tau \in K^\times$, where $K = K_f = \mathbb{Q}(\tau)$. Then there are precisely two real places of K, call them $v_1, v_2 | \infty$, where τ has nontrivial valuation, and the remaining archimedean places are complex. By the definition of projection irreducibility, we need to show that $P_F(f_\tau) = 0$ for all $F \subsetneq K$. Now, since

$\lambda(Y(K,v_1)) = \lambda(Y(K,v_2)) = 1/[K:\mathbb{Q}]$, we know that for our subfield $F \subsetneqq K$, either $Y(K,v_1) \cup Y(K,v_2) \subseteq Y(F,w)$ for some place w of F, in which case $P_F(f_\tau) = 0$ because the two valuations sum to zero by the product formula, or else v_1 and v_2 lie over distinct places of F, call them w_1 and w_2. Then the algebraic norm $\beta = \mathrm{N}_F^K \tau$ has nontrivial valuations at precisely the two archimedean places w_1, w_2. Observe that w_1, w_2 must be real, as the completions are $\mathbb{Q}_\infty = \mathbb{R} \subset F_{w_i} \subset K_{v_i} = \mathbb{R}$ for $i = 1, 2$. Thus β must be a nontrivial Salem number or a quadratic unit. In either case, if we assume without loss of generality that $\log \|\beta\|_{w_1} > 0$, observe that

$$\beta = \|\beta\|_{w_1}$$

But it is easy to see that

$$\log \|\beta\|_{w_1} = \frac{1}{[K:F]} \log \|\tau\|_{v_1}$$

and thus $\beta^{[K:F]} = \tau$. But this is a contradiction, as then the minimal field of f_β must also be K, but $\beta \in F \subsetneqq K$. That it is also in $\mathcal{L} \cap \mathcal{U}$ follows from the preceding proposition. □

Corollary 4.3.3. *Every Salem number $\tau > 1$ gives rise to an eigenvector f_τ of the M operator with eigenvalue $\delta(f_\tau) = [\mathbb{Q}(\tau) : \mathbb{Q}]$.*

Proof. This now follows from the above results and Proposition 4.2.3. □

Thus, if $\tau > 1$ is a Salem number, we have $f_\tau \in \mathcal{L} \cap \mathcal{P} \cap \mathcal{U}$, so we can compute explicitly:

$$\|f_\tau\|_{m,p} = \delta(f_\tau)\|f_\tau\|_p = \delta(f_\tau)^{1-1/p} 2^{1/p} |\log \tau|. \tag{4.3.1}$$

When $p = 1$ this is, of course, twice the classical logarithmic Mahler measure of τ, and when $p = \infty$, this is precisely the degree times the logarithmic house of τ.

4.4 The group Γ and proof of Theorem 7

We now construct an additive subgroup $\Gamma \leq \langle \mathcal{L} \cap \mathcal{P} \cap \mathcal{U} \rangle$ which is bounded away from 0 if and only if the L^p Lehmer conjecture is true and thus establish Theorem 7. For $K \in \mathcal{K}^G$, let $W_K = T_K(\mathcal{U}) \cap \mathcal{P} \cap \mathcal{L}$. Notice first W_K is not empty if $T_K(\mathcal{U})$ is not empty, as any element $f \in T_K(\mathcal{U})$ can be projected to a minimal element of its $\mathcal{K}$-support $\{F \in \mathcal{K} : P_F(f) \neq 0\}$, and that by construction such a projected element $P_F(f)$ will be an element of $T_K(\mathcal{U}) \cap \mathcal{P}$, and since $T_K(\mathcal{U})$ and $\mathcal{P}$ are both closed under scaling, we can ensure such an element is Lehmer irreducible. (We remark in passing that we may in fact have $T_K(\mathcal{U}) = \{0\}$, for example, when $K = \mathbb{Q}(i)$ where $i^2 = -1$; see Remark 2.2.7, p. 27.) By our L^p Northcott analogue Theorem 16, p. 61, we see that the set $\{f \in W_K : \|f\|_p \leq C\}$ is finite (notice that $f \in W_K \implies \delta(f) = [K_f : \mathbb{Q}] \leq [K : \mathbb{Q}]$) for any $C > 0$. As $W_K \subset \mathcal{P}$ we have $\|f\|_{m,p} = \delta(f) \cdot \|f\|_p$ (see Proposition 4.2.3 above), so we may choose an element $f_K \in W_K$ of minimal Mahler p-norm for each $K \in \mathcal{K}^G$, letting $f_K = 0$ if $T_K(\mathcal{U}) = \{0\}$. Notice that

$$m_p(f_K) = \|f_K\|_{m,p}$$

by construction (this follows from the usual argument following Proposition 4.2.3 and using $\mathcal{L} = \{d = \delta\}$). We let $\Gamma = \Gamma_p$ be the additive subgroup

generated by these elements (notice that our choices may depend on p):

$$\Gamma = \langle \{ f_K : K \in \mathcal{K}^G \} \rangle \leq \mathcal{L} \cap \mathcal{P} \cap \mathcal{U}. \tag{4.4.1}$$

Notice that Γ is, by construction, clearly a free group, as by Theorem 2, p. 11, we have the direct sum $\Gamma = \bigoplus_{K \in \mathcal{K}^G} \mathbb{Z} \cdot f_K$.

Let $\mathcal{U}_{m,p}$ denote the completion of $\mathcal{U}$ with respect to the Mahler p-norm $\| \cdot \|_{m,p}$. Our goal is now to prove Theorem 7, which we recall here:

Theorem 7. *Equation $(*_p)$ holds if and only if the additive subgroup $\Gamma \subset \mathcal{U}_{m,p}$ is closed.*

We begin by proving a basic result about additive subgroups of Banach spaces, following the remarks and proofs in [Ban91, Remark 5.6] and [Sid77, Theorem 2 et seq.]. (We only need the second part of this lemma for our theorem, however, we prove both directions for their own interest.)

Lemma 4.4.1. *Let Λ be a countable additive subgroup of a Banach space $\mathcal{B}$. If Λ is discrete, then it is closed and free abelian. If Λ is closed, then it is discrete.*

Proof. We restrict our attention to real Banach spaces, as this is the case that interests us, but note that the result continues to be true in the complex setting under suitable assumptions (see the discussion in [Sid77]).

We will first show that if $\Lambda \subset \mathcal{B}$ is countable and discrete then it is also closed and free. That it is closed is trivial, so let us show that it is free

by exhibiting a basis as a $\mathbb{Z}$-module. Let $\{v_i\}_{i=1}^{\infty}$ be an enumeration of the non-zero elements of Λ. Choose $b_1 = tv_1$ where $t > 0$ is the smallest number such that $tv_1 \in \Lambda$; clearly such a choice exists, else Λ would not be discrete. Let $B_1 = \{b_1\}$ and let $X_1 = \operatorname{span}_{\mathbb{R}} B_1$. Then B_1 is a basis for $\Lambda \cap X_1$. Suppose now we have chosen basis vectors $B_n = \{b_1, \ldots, b_n\}$ such that B_n is a basis for $\Lambda \cap X_n$ where $X_n = \operatorname{span}_{\mathbb{R}} B_n$. If $\Lambda \subset X_n$, then Λ has finite rank and we are done, so suppose $\Lambda \not\subset X_n$. Let $v = v_k$ be the first element of the enumeration $\{v_i\}$ which is not in $\Lambda \cap X_n$, so that $v_i \in \Lambda \cap X_n$ for all $i < k$. Let $X_{n+1} = \operatorname{span}_{\mathbb{R}}(B_n \cup \{v\})$. Observe that the set

$$T = \{t \in \mathbb{R} : tv \in X_n + \Lambda\}$$

is an additive subgroup of $\mathbb{R}$, and further, there must exist a minimal element $t_0 > 0$, as otherwise, we could find a sequence $t_n \to 0$ such that $0 < t_n < 1$, $x_n + t_n v \in \Lambda$, and $x_n = \sum_{i=1}^{n} r_i b_i \in X_n$ where $r_i \in [0, 1)$ for each $1 \leq i \leq n$ by adding appropriate elements of $\Lambda \cap X_n$ to x_n. But then

$$\|x_n + t_n v\| \leq \max_{r \in [0,1]^n} \left\| \sum_{i=1}^{n} r_i b_i \right\| + \|v\|$$

so the vectors $x_n + t_n v$ give an infinite subset of $\Lambda \cap X_{n+1}$ of bounded norm in the finite dimensional vector space X_{n+1} (with the norm from $\mathcal{B}$) and this contradicts the fact that $\Lambda \cap X_{n+1}$ is discrete (which follows from the fact that Λ is discrete). Thus, there must exist a minimal positive element $t_0 \in T$ such that $T = \mathbb{Z}t_0$. Let $b_{n+1} = x_0 + t_0 v$ where $x_0 = \sum_{i=1}^{n} r_i b_i \in X_n$ for some $r_i \in [0, 1)$. We claim that $B_{n+1} = \{b_1, \ldots, b_{n+1}\}$ is a basis for $\Lambda \cap X_{n+1}$ such that $v = v_k \in \Lambda \cap X_{n+1}$. To see this, observe that by our construction of the

set T, every $\lambda \in \Lambda \cap X_{n+1}$ has the form $\lambda = x + m_{n+1}t_0 v$ for some $m_{n+1} \in \mathbb{Z}$. Then

$$\lambda - m_{n+1}b_{n+1} = x - m_{n+1}x_0 \in \Lambda \cap X_n \implies \lambda - m_{n+1}b_{n+1} = \sum_{i=1}^{n} m_i b_i \quad (m_i \in \mathbb{Z}).$$

But then $\lambda = \sum_{i=1}^{n+1} m_i b_i$ and so B_{n+1} is indeed a basis for $\Lambda \cap X_{n+1}$. Now, either this process continues indefinitely and each nonzero element v_k of Λ is contained in some B_n, in which case $\bigcup_n B_n$ is a basis for Λ, or else $\Lambda \subset X_n$ for some n, in which case Λ has a basis B_n. In either case, we have constructed a basis for Λ as a $\mathbb{Z}$-module, and thus Λ is free.

Now, let us show that if Λ is countable and closed then it must be discrete. If Λ were not discrete, then we could choose a sequence of vectors $v_n \to 0$ such that $\|v_{n+1}\| \leq \frac{1}{3}\|v_n\|$ for all $n \in \mathbb{N}$. To every subset $S \subset \mathbb{N}$ we associate the vector $v_S = \sum_{n \in S} v_n$. Notice that each v_S is an absolutely convergent series, and belongs to Λ since Λ is closed. We claim that the elements v_S are distinct for distinct subsets of $\mathbb{N}$. To see this, observe that for $S \neq T \subset \mathbb{N}$,

$$v_S - v_T = \sum_{n \in S \setminus T} v_n - \sum_{m \in T \setminus S} v_m = \sum_{n=1}^{\infty} \epsilon_n v_n$$

where $\epsilon_n \in \{-1, 0, +1\}$, and for at least one n we have $\epsilon_n \neq 0$. Let k be the first such number. Then if $v_S - v_T = 0$ we must have $-\epsilon_k v_k = \sum_{n=k+1}^{\infty} \epsilon_n v_n$, but

$$\left\| \sum_{n=k+1}^{\infty} \epsilon_n v_n \right\| \leq \left(\sum_{n=1}^{\infty} \frac{1}{3^n} \right) \|v_k\| = \frac{\|v_k\|}{2} < \|v_k\| = \|\epsilon_k v_k\|,$$

which is impossible. Thus each v_S is uniquely associated to S, but this gives an uncountable number of elements of Λ, a contradiction. $\square$

We remark that countability is essential in the above lemma, as the uncountable subgroup $\{f : [0,1] \to \mathbb{Z} : \|f\|_\infty < \infty\} \subset L^\infty[0,1]$ is discrete and closed but not free.

We are now prepared to prove Theorem 7:

Proof of Theorem 7. By Proposition 3.2.4 and Theorem 6, we know that $(*_p)$ holds if and only if there exists a constant c_p such that $m_p(f) \geq c_p > 0$ for all $f \in \mathcal{L} \cap \mathcal{U} \cap \mathcal{P}$. Given any $f \in \mathcal{L} \cap \mathcal{U} \cap \mathcal{P}$, let $A(f) = \{K \in \mathcal{K}^G : P_K(f) \neq 0\}$. $A(f)$ clearly contains a minimal element K which satisfies $F \subsetneqq K, F \in \mathcal{K}^G \implies P_F(f) = 0$. Let K be any such minimal element. Then observe that $P_K(f) = T_K(f)$, as

$$P_K(f) = \sum_{\substack{F \subseteq K \\ F \in \mathcal{K}^G}} T_F(f),$$

but $P_F(f) = 0 \implies T_F(f) = 0$ for all $F \subsetneqq K, F \in \mathcal{K}^G$. Observe that $m_p(P_K f) \leq m_p(f)$ by Proposition 2.3.2 and Lemma 3.2.1. But then, by construction of Γ, $\|f_K\|_{m,p} = m_p(f_K) \leq m_p(P_K f)$ since $P_K f = T_K f \in T_K(\mathcal{U}) \cap \cap \mathcal{P}$. Thus, if Γ is discrete, we gain $(**_p)$ and by Theorem 6 we gain the L^p Lehmer conjecture $(*_p)$.

Likewise, supposing $(**_p)$, we can repeat the same procedure as above given an arbitrary element $f \in \Gamma$ to obtain $P_K(f) = f_K$ for some minimal K in $A(f)$. Now, by the fact that P_K is a norm one projection with respect to the L^p norm (Propositon 2.3.2), and the fact that it commutes with the $T^{(n)}$ operators (Proposition 2.6.2), we see that it commutes with the M operator

well, and therefore, by the definition of the Mahler norm,

$$\|P_K f\|_{m,p} = \|MP_K f\|_p = \|P_K(Mf)\|_p \leq \|Mf\|_p = \|f\|_{m,p}.$$

Since $f_K \in \mathcal{L} \cap \mathcal{U} \cap \mathcal{P}$, we see that $(**_p)$ implies that $\|P_K f\|_{m,p} \geq c_p > 0$ and thus Γ is discrete.

Finally, observe that as a countable (free abelian) additive subgroup of the Banach space $\mathcal{U}_{m,p}$, by Lemma 4.4.1 above, Γ is discrete if and only it is closed. □

4.5 The Mahler 2-norm and proof of Theorem 9

Recall that we define the Mahler 2-norm for $f \in \mathcal{F}$ to be:

$$\|f\|_{m,2} = \|Tf\|_2 = \left\| \sum_{n=1}^{\infty} n\, T^{(n)} f \right\|_2.$$

The goal of this section is to prove Theorem 9, which we recall here for the convenience of the reader:

Theorem 9. *The Mahler 2-norm satisfies*

$$\|f\|_{m,2}^2 = \sum_{n=1}^{\infty} n^2 \, \|T^{(n)}(f)\|_2^2 = \sum_{K \in \mathcal{K}^G} \sum_{n=1}^{\infty} n^2 \, \|T_K^{(n)}(f)\|_2^2.$$

Further, the Mahler 2-norm arises from the inner product

$$\langle f, g \rangle_m = \langle Mf, Mg \rangle = \sum_{n=1}^{\infty} n^2 \, \langle T^{(n)} f, T^{(n)} g \rangle = \sum_{K \in \mathcal{K}^G} \sum_{n=1}^{\infty} n^2 \, \langle T_K^{(n)} f, T_K^{(n)} g \rangle$$

where $\langle f, g \rangle = \int_Y fg \, d\lambda$ denotes the usual inner product in $L^2(Y)$, and therefore the completion $\mathcal{F}_{m,2}$ of $\mathcal{F}$ with respect to the Mahler 2-norm is a Hilbert space.

Proof of Theorem 9. The first part of the theorem follows easily from the fact that the $T_K^{(n)}$ form an orthogonal decomposition of $\mathcal{F}$. Indeed, for $f \in \mathcal{F}$, we have:

$$\|f\|_{m,2}^2 = \left\| \sum_{K \in \mathcal{K}^G} \sum_{n=1}^{\infty} n\, T_K^{(n)}(f) \right\|_2^2 = \sum_{K \in \mathcal{K}^G} \sum_{n=1}^{\infty} n^2 \, \|T_K^{(n)}(f)\|_2^2.$$

The above sums are, of course, finite for each $f \in \mathcal{F}$. That the specified inner product $\langle f, g \rangle_m$ defines this norm is then likewise immediate. Therefore, the completion of $\mathcal{F}$ with respect to the norm $\| \cdot \|_{m,2}$ is a Hilbert space, as claimed. $\square$

Chapter 5

Decompositions on Elliptic Curves

5.1 Projection operators associated to number fields

Most of the constructions in this section mirror those of Chapter 2 and Chapter 3, with some minor differences necessitated by our lack of a function space structure for V. Foremost amongst these differences, we shall define P_K in general as a Bochner integral as, lacking a function space structure, we cannot define it explicitly as a function of any places itself. Most of the proofs, however, follow the pattern of those in Chapter 2.

As above we fix a number field k and let E/k be an elliptic curve with canonical Néron-Tate height $\widehat{h} : E \to [0, \infty)$. Let

$$V = E(\overline{k})/E_{\mathrm{tor}}(\overline{k}),$$

so V is in fact a vector space over the rational numbers $\mathbb{Q}$. We have an inner product $\langle \cdot, \cdot \rangle : E \to [0, \infty)$ given by

$$2\langle \xi, \eta \rangle = \widehat{h}(\xi + \eta) - \widehat{h}(\xi) - \widehat{h}(\eta).$$

where $\xi, \eta \in V$. Since $\widehat{h}$ is a positive-definite quadratic form on V,

$$\|\xi\| = \langle \xi, \xi \rangle^{1/2} = \sqrt{\widehat{h}(\xi)}$$

defines a vector space norm on V. Let $G = \mathrm{Gal}(\overline{k}/k)$ and recall that G has a well-defined action $G \times V \to V$, which we will denote by $(\sigma, \xi) \mapsto \sigma(\xi)$ for $\xi \in V$ and $\sigma \in G$. Recall that the canonical height is invariant under G, that is, that $\widehat{h}(\sigma(\xi)) = \widehat{h}(\xi)$ for all $\xi \in V, \sigma \in G$. Therefore,

$$\|\sigma(\xi)\| = \|\xi\| \quad \text{for all} \quad \xi \in V, \sigma \in G. \tag{5.1.1}$$

Since σ is linear and bounded, it extends by continuity to a well-defined continuous operator (in fact, an isometry)

$$L_\sigma : \overline{V} \to \overline{V} \tag{5.1.2}$$

which satisfies $L_\sigma(V) = V$.

We now think of V as a pre-Hilbert space with norm $\|\cdot\|$. Let $\mathcal{K}$ denote the set of algebraic extensions of k, partially ordered by inclusion. Let $\mathcal{K}^G$ denote the collection of finite Galois extensions of k. For a field K/k with $K \subset \overline{k}$, let

$$H = H_K = \mathrm{Gal}(\overline{k}/K) \leq G = \mathrm{Gal}(\overline{k}/k). \tag{5.1.3}$$

Recall that H is a compact profinite group with a normalized Haar measure ν such that $\nu(H) = 1$. Define the map

$$\begin{aligned} P_K : \overline{V} &\to \overline{V} \\ \xi &\mapsto \int_H L_\sigma(\xi)\, d\nu(\sigma) \end{aligned} \tag{5.1.4}$$

where the integral on the right is a *Bochner integral*. We recall here the definition of a Bochner integral (for a detailed treatment of Bochner integration we refer the reader to [Yos80, §V.5]):

Definition 5.1.1 (Bochner integral)**.** Suppose (Ω, μ) is a measure space and $(B, \|\cdot\|)$ is a Banach space. We say a function $s : \Omega \to B$ is *simple* if $s(x) = \sum_{i=1}^{n} \chi_{A_i}(x) b_i$ for some measurable sets $A_i \subseteq \Omega$ of finite measure and $b_i \in B$. We define

$$\int_\Omega s \, d\mu = \sum_{i=1}^{n} \mu(A_i) b_i.$$

We say a function $F : \Omega \to B$ is *Bochner integrable* if there exists a sequence of simple functions $s_n : \Omega \to B$ such that

$$\int_\Omega \|F(x) - s_n(x)\| \, d\mu(x) \to 0. \tag{5.1.5}$$

In this case we define

$$\int_\Omega F(x) \, d\mu(x) = \lim_{n\to\infty} \int_\Omega s_n(x) \, d\mu(x) \in B.$$

It is easy to see (using simple functions) that the Bochner integral satisfies

$$\left\| \int_\Omega F(x) \, d\mu(x) \right\| \leq \int_\Omega \|F(x)\| \, d\mu(x). \tag{5.1.6}$$

Further, notice that the assumption (5.1.5) together with (5.1.6) implies in fact that the vectors $v_i = \int_\Omega s_i \, d\mu$ form a Cauchy sequence in the Banach space B, so convergence is assured by the fact that B is a Banach space and the Bochner integral is well-defined.

Lemma 5.1.2. *The function $H = H_K \to \overline{V}$ given by $\sigma \mapsto L_\sigma(\xi)$ for a given $\xi \in \overline{V}$ is Bochner integrable, and thus $P_K : \overline{V} \to \overline{V}$ is well-defined.*

Proof. Let $\xi_n \in V$ be a sequence of vectors such that $\|\xi - \xi_n\| \to 0$. We associate to each ξ_n the simple function $s : H \to V$ given by

$$s_n(\sigma) = L_\sigma(\xi_n) = \sum_{i=1}^{N} \chi_{A_i}(\sigma) L_{\sigma_i}(\xi_n). \tag{5.1.7}$$

where $N = [H : \mathrm{Stab}_H(\xi)]$ and the A_i are the right cosets of $\mathrm{Stab}_H(\xi_n)$ in H and the σ_i is a right coset representative of A_i for each i. We wish to show that the function $\sigma \mapsto L_\sigma(\xi)$ is approximated by $s_n(\sigma)$ in the sense of (5.1.5). Since L_σ is an isometry, we compute that

$$\begin{aligned}\int_H \|L_\sigma(\xi) - s_n(\sigma)\|\, d\nu(\sigma) &= \int_H \|L_\sigma(\xi) - L_\sigma(\xi_n)\|\, d\nu(\sigma) \\ &= \int_H \|L_\sigma(\xi - \xi_n)\|\, d\nu(\sigma) = \int_H \|\xi - \xi_n\|\, d\nu(\sigma) = \|\xi - \xi_n\| \to 0.\end{aligned}$$

which completes the proof. □

From equation (5.1.7) of the proof of the above lemma, we also see that if $\xi \in V$, then the function $\sigma \mapsto L_\sigma(\xi)$ is simple and in particular that

$$P_K(\xi) = \int_H L_\sigma(\xi)\, d\nu(\sigma) = \frac{1}{N} \sum_{i=1}^{N} L_{\sigma_i}(\xi) \quad \text{for} \quad \xi \in V. \tag{5.1.8}$$

where $N = [H : \mathrm{Stab}_H(\xi)]$ and the σ_i form a system of a right coset representatives for $\mathrm{Stab}_H(\xi)$ in H.

We now prove the following lemma regarding Bochner integration which will be helpful to us below (see also [Yos80, Corollary V.2]):

Lemma 5.1.3. *Suppose (Ω, μ) is a measure space and $(B, \|\cdot\|)$ is a Banach space. Let L be a continuous linear operator from B to itself. Then L commutes with Bochner integration on Ω, that is,*

$$L\bigg(\int_\Omega F(x)\,d\mu(x)\bigg) = \int_\Omega L(F(x))\,d\mu(x). \tag{5.1.9}$$

In particular, if F is Bochner integrable then so is $L \circ F$.

Proof. Recall that from equation (5.1.5) above that F is Bochner integrable if there exists a sequence of simple functions $s_n : \Omega \to B$ such that

$$\int_\Omega \|F(x) - s_n(x)\|\,d\mu(x) \to 0,$$

and that in this case we defined

$$\int_\Omega F(x)\,d\mu(x) = \lim_{n\to\infty} \int_\Omega s_n(x)\,d\mu(x) \in B.$$

Now, let the simple function $s_n(x) = \sum_{i=1}^N \chi_{A_i}(x) b_i$, where the sets $A_i \subseteq \Omega$ of measurable and of finite measure and $b_i \in B$. Then

$$L\bigg(\int_\Omega s_n\,d\mu\bigg) = L\bigg(\sum_{i=1}^N \mu(A_i) b_i\bigg) = \sum_{i=1}^N \mu(A_i) L(b_i) = \int_\Omega L \circ s_n\,d\mu.$$

since $L \circ s_n(x) = \sum_{i=1}^N \chi_{A_i}(x) L(b_i)$ is clearly simple as well. Now observe that $L \circ F$ is approximated by $L \circ s_n$:

$$\begin{aligned}\int_\Omega \|L \circ F(x) - L \circ s_n(x)\|\,d\mu(x) &= \int_\Omega \|L(F(x) - s_n(x))\|\,d\mu(x) \\ &\leq \|L\| \cdot \int_\Omega \|F(x) - s_n(x)\|\,d\mu(x) \to 0.\end{aligned}$$

But then we have, using the continuity of L to exchange it with the limit,

$$\int_\Omega L \circ F(x)\, d\mu(x) = \lim_{n\to\infty} \int_\Omega L \circ s_n(x)\, d\mu(x) = \lim_{n\to\infty} L\bigg(\int_\Omega s_n(x)\, d\mu(x) \bigg)$$
$$= L\bigg(\lim_{n\to\infty} \int_\Omega s_n(x)\, d\mu(x) \bigg) = L\bigg(\int_\Omega F(x)\, d\mu(x) \bigg)$$

and the proof is complete. □

Lemma 5.1.4. *For each field $k \subseteq K \subseteq \overline{k}$, the map P_K is a norm one projection.*

Proof. We first prove that $P_K^2 = P_K$. Let $H = H_K$ as above and ν the normalized Haar measure on H. Suppose that $\tau \in H$. Observe that for any $\xi \in \overline{V}$, by applying Lemma 5.1.3,

$$L_\tau(P_K(\xi)) = L_\tau\bigg(\int_H L_\sigma(\xi)\, d\nu(\sigma) \bigg) = \int_H L_\tau(L_\sigma \xi)\, d\nu(\sigma)$$
$$= \int_H L_{\tau\sigma}(\xi)\, d\nu(\sigma) = \int_{\tau H} L_\sigma(\xi) d\nu(\sigma) = P_K(\xi)$$

since $\tau H = H$ for $\tau \in H$. Thus,

$$P_K{}^2(\xi) = \int_H L_\sigma(P_K(\xi))\, d\nu(\sigma) = \int_H P_K(\xi) d\nu(\sigma) = P_K(\xi),$$

proving the first claim. To see that $\|P_K\| = 1$, we combine the inequality (5.1.6) with the fact that L_σ is an isometry:

$$\bigg\| \int_H L_\sigma(\xi)\, d\nu(\sigma) \bigg\| \leq \int_H \|L_\sigma(\xi)\|\, d\nu(\sigma) = \int_H \|\xi\|\, d\nu(\sigma) = \|\xi\|. \qquad \square$$

Corollary 5.1.5. *The projection P_K is orthogonal, that is, $P_K(\overline{V}) \perp (I - P_K)(\overline{V})$ where I is the identity operator.*

Proof. This now follows from Lemmas 5.1.4 and 5.2.6 above, and the fact that for a Hilbert space, a norm one projection is orthogonal onto its range (see Lemma 2.3.5, p. 31). □

5.2 Decomposition by Galois field and proof of Theorem 10

As we did for algebraic numbers modulo torsion in the case of the multiplicative group of a number field modulo torsion $K^\times/\operatorname{Tor}(K^\times)$, we associate to each group $E(K)/E_{\text{tor}}$ its vector space span:

$$V_K = \operatorname{span}_{\mathbb{Q}} E(K)/E_{\text{tor}} = E(K)/E_{\text{tor}} \otimes \mathbb{Q} \subset V. \tag{5.2.1}$$

By the Mordell-Weil theorem, $\dim_{\mathbb{Q}} V_K < \infty$ for all $K \in \mathcal{K}$. For $N \in \mathbb{Z}$, we let $[N] : E \to E$ denote the multiplication-by-N endomorphism on E.

Lemma 5.2.1. *Let $K, L \in \mathcal{K}$. Then $V_K \cap V_L = V_{K \cap L}$.*

Proof. We take a representative of P of ξ such that $[N]P \in E(K)$ and $[M]P \in E(L)$. Then $[NM]P \in E(K) \cap E(L) = E(K \cap L)$. The reverse inclusion is clear. □

As above, if we fix some $\xi \in V$ then the set

$$\{K \in \mathcal{K} : \xi \in V_K\}$$

forms a sublattice of $\mathcal{K}$ by the above lemma, and by the finiteness properties of $\mathcal{K}$ this set must contain a unique minimal element.

Definition 5.2.2. For any $\xi \in V$, the *minimal field* is defined to be the minimal element of the sublattice $\{K \in \mathcal{K} : \xi \in V_K\}$. We denote the minimal field of ξ by K_ξ.

Remark 5.2.3. We already have a notion of *minimal field of definition* $k(P)$ for a point $P \in E(K)$ (cf. e.g. [Sil92, §I.2]). Let us emphasize that the minimal field of definition $k(P)$ typically differs amongst the representatives P of ξ in $E(K)$, as each can differ by a torsion point of arbitrarily large degree, and that the minimal field we have defined here, K_ξ, may be distinct from all of the fields $k(P)$ for the representatives P of ξ. One can easily see, however, that

$$K_\xi = \bigcap_{N \in \mathbb{N}} k([N]P)$$

for any representative P. Notice that the minimal field of definition of a point P is the fixed field of all of the elements of the absolute Galois group which fix P, and while we will soon prove a similar result for ξ and its minimal field, we must keep in mind that Galois automorphisms which fix ξ may not fix a particular representative P as we are working modulo torsion (and thus, the stabilizer groups will sometimes be different).

Lemma 5.2.4. *For any $\xi \in V$, we have* $\mathrm{Stab}_G(\xi) = \mathrm{Gal}(\overline{k}/K_\xi) \leq G$.

Proof. Let ξ have a representative $P \in E(\overline{k})$. Clearly $\mathrm{Gal}(\overline{\mathbb{Q}}/K_\xi) \leq \mathrm{Stab}_G(\xi)$, as $[N]P \in K_\xi$ for some $N \in \mathbb{N}$ by definition of V_{K_ξ}. To see the reverse implication, observe that $K_\xi = k([N]P)$ for some $N \in \mathbb{N}$, as otherwise, there would

be a proper subfield of K_ξ which contains some multiple of ξ, contradicting the definition of K_ξ. $\square$

We now define, as we had for algebraic numbers modulo torsion, the orbital degree function $\delta : V \to \mathbb{N}$ by

$$\delta(\xi) = \#\{L_\sigma \xi : \sigma \in G\} = [G : \mathrm{Stab}_G(f)] = [K_\xi : k] \tag{5.2.2}$$

to be the size of the orbit of ξ under the action of the Galois isometries, and where the last equality follows from the above lemma.

Lemma 5.2.5. *Let $\xi \in V$. Then the following are equivalent:*

1. $\xi \in V_K$.
2. $L_\sigma(\xi) = \xi$ *for each* $\sigma \in H_K = \mathrm{Gal}(\overline{k}/K)$.
3. $P_K(\xi) = \xi$.

Proof. Observe that $\xi \in V_K$ if and only if $H_K = \mathrm{Gal}(\overline{k}/K)$ fixes ξ by applying Lemma 5.2.4 and noting that $\xi \in V_K$ if and only if $K_\xi \subset K$ by construction of K_ξ. This is clearly equivalent to ξ having a representative P such that $[N]P \in E(K)$ for some $N \in \mathbb{N}$, but we claim that $L_\sigma(\xi) = \xi$ for all $\sigma \in H_K$ if and only if $P_K(\xi) = \xi$. The forward implication is clear, so let us show the reverse; suppose $P_K(\xi) = \xi$, and then

$$L_\sigma(\xi) = L_\sigma\left(\int_{H_K} L_\tau(\xi)\, d\nu(\tau)\right) = \int_{H_K} L_\sigma L_\tau(\xi)\, d\nu(\tau),$$

where we see that we can bring L_σ into the integrand by Lemma 5.1.3 above, and

$$\int_{H_K} L_\sigma L_\tau(\xi)\, d\nu(\tau) = \int_{\sigma H_K} L_\tau(\xi)\, d\nu(\tau) = \int_{H_K} L_\tau(\xi)\, d\nu(\tau)$$

since $\sigma H_K = H_K$ for $\sigma \in H_K$. We have then established that

$$L_\sigma(\xi) = \int_{H_K} L_\tau(\xi)\, d\nu(\tau) = P_K(\xi) = \xi$$

where the last equality follows by assumption, and the proof is complete. □

Lemma 5.2.6. *For $K \in \mathcal{K}$, we have $P_K(V) = V_K$ and $P_K(\overline{V}) = \overline{V_K}$.*

Proof. The first claim, that $P_K(V) = V_K$, follows immediately from the idempotency of P_K, namely, that $P_K^2 = P_K$, and the preceding lemma. The second now follows by the continuity of P_K established above. □

Lemma 5.2.7. *For any field $K \subset \overline{\mathbb{Q}}$ of arbitrary degree and any $\sigma \in G$,*

$$L_\sigma P_K = P_{\sigma K}\, L_\sigma.$$

Equivalently, $P_K\, L_\sigma = L_\sigma P_{\sigma^{-1} K}$.

Proof. We prove the first form, the second obviously being equivalent. As before, let $H = \mathrm{Gal}(\overline{k}/K)$ and ν be the normalized Haar measure on H. Then we have

$$L_\sigma P_K(\xi) = L_\sigma\bigg(\int_{H_K} L_\tau(\xi)\, d\nu(\tau)\bigg) = \int_{H_K} L_\sigma L_\tau(\xi)\, d\nu(\tau),$$

where, as above, we see that we can bring L_σ into the integrand by Lemma 5.1.3, and then

$$\int_{H_K} L_\sigma L_\tau(\xi)\, d\nu(\tau) = \int_{H_K} L_\sigma L_\tau L_{\sigma^{-1}} L_\sigma(\xi)\, d\nu(\tau)$$
$$= \int_{\sigma H_K \sigma^{-1}} L_\tau(L_\sigma(\xi))\, d\nu(\tau) = P_{\sigma K} L_\sigma(\xi). \quad \square$$

As above, we are interested in the case where the projections P_K, P_L commute with each other (and thus $P_K P_L$ is a projection to the intersection of their ranges).

Lemma 5.2.8. *Suppose $K \in \mathcal{K}$ and $L \in \mathcal{K}^G$. Then P_K and P_L commute, that is,*

$$P_K P_L = P_{K \cap L} = P_L P_K.$$

In particular, the family of operators $\{P_K : K \in \mathcal{K}^G\}$ is commuting.

Proof. Notice that if $L \in \mathcal{K}^G$ (i.e., is a finite Galois extension of k), then $L_\sigma(V_L) = V_L$ for all $\sigma \in G$. Let $H = H_K$ as before denote the absolute Galois group over K with normalized Haar measure ν, and suppose $\xi \in V_K$. If we can show that $P_L(\xi) \in V_K$ for $\xi \in V_K$, then the proof will be complete, as then $P_L P_K$ will project onto $V_K \cap V_L = V_{K \cap L}$ and therefore must be $P_{K \cap L}$, as it is also norm one (as the composition of norm one operators) and would be idempotent, and therefore the orthogonal projection onto its range. Commutativity then follows by general principles for Hilbert spaces (specifically, that an orthogonal projection is equal to its adjoint [Yos80, Theorem III.2],

so by taking adjoints of both sides of the equation $P_L P_K = P_{K \cap L}$ we obtain commutativity). Thus let us assume $\xi \in V_K$. Let $\tau \in H_K = \mathrm{Gal}(\overline{k}/K)$. If we can show $L_\tau(P_L \xi) = P_L(\xi)$, the proof will be complete by Lemma 5.2.5, as $P_L(\xi)$ will be fixed for each $\tau \in H_K$. But then, using Lemma 5.2.7, we have

$$L_\tau P_L(\xi) = P_{\tau L} L_\tau(\xi) = P_L L_\tau(\xi) = P_L(\xi)$$

where $L_\tau(\xi) = \xi$ since $\tau \in H_K$ and $\xi \in V_K$ by assumption, and the proof is complete. □

We now recall the statement of Theorem 10 for the convenience of the reader:

Theorem 10. *For each $K \in \mathcal{K}^G$ there exists a continuous projection $T_K : V \to V$ such that the space V has an orthogonal direct sum decomposition into vector subspaces*

$$V = \bigoplus_{K \in \mathcal{K}^G} T_K(V) \tag{5.2.3}$$

and $T_K(V) \subset V_K$ for each K.

Proof. We apply our main decomposition result, Theorem 15 (p. 34). Let our index set be $\mathcal{K}^G = \{K/k : [K : k] < \infty \text{ and } \sigma K = K \ \forall \sigma \in G\}$. This poset and the associated vector spaces V_K clearly match criteria (1) - (3) by 5.2.6. Criterion (4) is precisely from Lemma 5.1.5. Criterion (5) follows from Lemma 5.2.8. Criterion (6) follows from the fact that $\xi \in V \implies \xi \in V_K$ for some K (for example, the minimal field K_ξ constructed above). The result now follows from Theorem 15. □

Let μ be the Möbius function associated to $\mathcal{K}^G$. Then by Theorem 15 the operators $T_K : \overline{V} \to \overline{V}$ are given by

$$T_K = \sum_{\substack{F \subseteq K \\ F \in \mathcal{K}^G}} \mu(F, P) P_F. \tag{5.2.4}$$

5.3 Decomposition by degree and proof of Theorems 11 and 12

We define, exactly analogous to the construction in Chapter 2, Section 2.6 above the subspace of elements generated by "degree n" points (compare (2.6.3) above):

$$V^{(n)} = \sum_{\substack{K \in \mathcal{K} \\ [K:k] \leq n}} V_K. \tag{5.3.1}$$

The goal of this section is to prove Theorem 11, which we recall here:

Theorem 11. *For each $n \in \mathbb{N}$ there exists a continuous projection $T^{(n)} : V \to V$ such that the space V has an orthogonal direct sum decomposition into vector subspaces*

$$V = \bigoplus_{n=1}^{\infty} T^{(n)}(V)$$

and $T^{(n)}(V) \subset V^{(n)}$ for each n.

Let $P^{(n)}$ be the (unique) orthogonal projection from the Hilbert space $\overline{V}$ to the closed subspace $\overline{V^{(n)}}$.

Lemma 5.3.1. *Let $K \in \mathcal{K}^G$ and $\xi \in V$. Then $\delta(P_K \xi) \leq \delta(\xi)$.*

Proof. Let $F = K_\xi$. Since $K \in \mathcal{K}^G$, we have by Lemma 5.2.8 that $P_K f = P_K(P_F f) = P_{K\cap F} f$. Thus, $P_K f \in V_{K\cap F}$, and so by equation (5.2.2) above, we have $\delta(P_K f) \leq [K \cap F : k] \leq [F : k] = \delta(f)$. □

Lemma 5.3.2. *The projections $P^{(n)}$ and P_K for $K \in \mathcal{K}^G$ commute, and thus T_K and $P^{(n)}$ commute as well.*

Proof. Since $\delta(P_K\xi) \leq \delta(\xi)$ for all $\xi \in V$ by Lemma 5.3.1 above, we have $P_K(V^{(n)}) \subset V^{(n)}$, and thus by continuity $P_K(\overline{V^{(n)}}) \subset \overline{V^{(n)}}$, so $P_K(\overline{V^{(n)}}) \subset \overline{V^{(n)}} \cap \overline{V_K}$ and $P_K P^{(n)}$ is a projection by the usual Hilbert space arguments. Therefore $P^{(n)}$ and P_K commute. The last part of the claim now follows from the definition of T_K in (5.2.4). □

Proposition 5.3.3. *The orthogonal projection $P^{(n)}$ takes the underlying $\mathbb{Q}$-vector space V to itself, that is, $P^{(n)}(V) \subset V$.*

Proof. Let $W_K = T_K(V) \subset V_K$ for $K \in \mathcal{K}^G$. We know that by commutativity of $P^{(n)}$ and T_K, we have the decomposition

$$P^{(n)}(V) = \bigoplus_{K\in\mathcal{K}^G} P^{(n)}(W_K)$$

and thus if we can show that $P^{(n)}(W_K) \subseteq W_K$, then we will have the desired result. But by the Mordell-Weil theorem we know the subspaces V_K have finite dimension over $\mathbb{Q}$, and thus so do the subspaces W_K. As above in the proof of Proposition 2.6.4, p. 46, we define for all fields $F \in \mathcal{K}$ such that $F \subset K$ the subspace

$$Z_F = P_F(W_K) \quad \text{and} \quad Z'_F = Q_F(W_K),$$

where $Q_F = I - P_F$ is the complementary orthogonal projection. Observe that for each such F, we have

$$W_K = Z_F \oplus Z'_F.$$

Then by Lemma 2.6.3, p. 45, we have

$$W_K = \Big(\sum_{\substack{F \subseteq K \\ [F:\overline{k}] \leq n}} Z_F \Big) \oplus \Big(\bigcap_{\substack{F \subseteq K \\ [F:\overline{k}] \leq n}} Z'_F \Big).$$

This gives us for any $\xi \in W_K$ a decomposition $\xi = \xi_n + \xi'_n$ where

$$\xi_n \in \sum_{\substack{F \subseteq K \\ [F:\overline{k}] \leq n}} Z_F = V^{(n)} \cap W_K,$$

and

$$\xi'_n \in \bigcap_{\substack{F \subseteq K \\ [F:\overline{k}] \leq n}} Z'_F = (V^{(n)})^{\perp} \cap W_K,$$

But then $\xi_n \in V^{(n)}$ and $\xi'_n \in (V^{(n)})^{\perp}$, so by the uniqueness of the orthogonal decomposition, we must in fact have $\xi_n = P^{(n)}\xi$ and $\xi'_n = Q^{(n)}\xi$. Therefore all $\xi \in V$ have projection $P^{(n)}(\xi) \in V$ and the proof is complete. □

Now we observe that the subspaces $V^{(n)}$ with their associated projections $P^{(n)}$, indexed by $\mathbb{N}$ with the usual partial order $\leq$, satisfy the conditions of Theorem 15, and thus we have orthogonal projections $T^{(n)}$ and an orthogonal decomposition

$$V = \bigoplus_{n=1}^{\infty} T^{(n)}(V). \tag{5.3.2}$$

As above in Proposition 2.6.5, p. 48, we note what this decomposition by degree tells us:

Proposition 5.3.4. *Each $\xi \in V$ has a unique finite expansion into its degree n components, $\xi^{(n)} = T^{(n)}\xi \in V$:*

$$\xi = \sum_{n\in\mathbb{N}} \xi^{(n)}.$$

Each $\xi^{(n)}$ term can be written as a finite sum $\xi^{(n)} = \sum_i \xi_i^{(n)}$ where $\xi_i^{(n)} \in V$ and $\delta(\xi_i^{(n)}) = n$ for each i, and $\xi^{(n)}$ cannot be expressed as a finite sum $\sum_j \xi_j^{(n)}$ with $\delta(\xi_j^{(n)}) \leq n$ for each j and $\delta(\xi_j^{(n)}) < n$ for some j.

It now remains to prove Theorem 12.

Theorem 12. *The projections T_K and $T^{(n)}$ commute with each other for each $K \in \mathcal{K}^G$ and $n \in \mathbb{N}$.*

Proof of Theorem 12. From Proposition 5.3.2, we see that the operators T_K and $P^{(n)}$ commute for $K \in \mathcal{K}^G$ and $n \in \mathbb{N}$. But $T^{(n)} = P^{(n)} - P^{(n-1)}$ for $n > 1$ and $T^{(1)} = P^{(1)}$, so by the commutativity of T_K with $P^{(n)}$ we have the desired result. In particular, the map $T_K^{(n)} = T^{(n)}T_K : V \to V$ is also a projection. □

Thus we can combine equations (5.2.3) and (5.3.2) to obtain the orthogonal decomposition

$$V = \bigoplus_{n=1}^{\infty} \bigoplus_{K\in\mathcal{K}^G} T_K^{(n)}(V). \tag{5.3.3}$$

5.4 Open conjectures on elliptic curve constructions

At this point we have established our orthogonal decompositions, and thus we could define our Mahler operator $M : V \to V$ via

$$M(\xi) = \sum_{n=1}^{\infty} \sqrt{n} \cdot T^{(n)}\xi. \tag{5.4.1}$$

and our Mahler norm $\| \cdot \|_m : V \to V$ via

$$\|\xi\|_m = \|M\xi\|. \tag{5.4.2}$$

We will now discuss briefly what constructions from Chapters 3 and 4 above easily follow in the elliptic curve setting and which ones remain open. It is easy to verify, exactly analogously to verifications for the Mahler p-norm defined in Section 4.2 above, that M is an invertible linear operator on V and thus that $\| \cdot \|_m$ is a well-defined vector space norm, and that we can complete our space V with respect to $\| \cdot \|_m$ to obtain a Hilbert space V_m. Likewise, we can define the *minimal degree* of ξ to be

$$d(\xi) = \min_{\substack{P \in V \\ P + E_{\text{tor}} = \xi}} [k(P) : k] \tag{5.4.3}$$

and our *Lehmer irreducible* elements of V to be

$$\mathcal{L} = \{\xi \in V : \delta(\xi) = d(\xi)\}. \tag{5.4.4}$$

Lehmer's conjecture for elliptic curves, Conjecture 13, p. 19 above, which we formulated as $[k(P) : k]\widehat{h}(P) \geq c$ for all non-torsion $P \in E(\overline{k})$, now takes the equivalent form:

Conjecture 17 (Reformulation of Lehmer's conjecture for E/k)**.** *There exists a constant $c > 0$ such that*

$$d(\xi)\widehat{h}(\xi) = d(\xi)\|\xi\|^2 \geq c \quad \textit{for all} \quad 0 \neq \xi \in V. \tag{5.4.5}$$

It is as yet an open question if we can restrict to $\xi \in \mathcal{L}$. We conjecture that we can do so, and in fact, the following analogue of Proposition 3.1.2, p. 50 should be true:

Conjecture 18. *Let $\xi \in V$. Then*

$$d\big(\tfrac{r}{s}\xi\big) = \left(\frac{\ell s}{(\ell, r)(n, s)}\right)^2 \delta(\xi).$$

where $R(\xi) = \{q \in \mathbb{Q} : q\xi \in \mathcal{L}\} = \frac{\ell}{n}\mathbb{Z}$ is a fractional ideal of $\mathbb{Q}$.

Let us explain for a moment why our scaling factor here is squared, whereas it is not for algebraic numbers modulo torsion. This proposition states that, when suitable scaling has occurred so that P "generates" its additive subgroup over $k(P)$ and no other multiples of P may be defined over $k(P)$, then an "nth root" Q such that $[n]Q = P$ should have $[k(Q) : k(P)]$ of maximum degree. As the multiplication by n map is a morphism of degree n^2, we expect generically the degree of this extension to be n^2 (when torsion being present in $k(P)$ is not an issue). Thus, when $R(\xi) = \mathbb{Z}$, we expect that

$$d((r/s)\xi) = s^2\delta(\xi) = s^2\, d(\xi).$$

For algebraic numbers, the proof of Proposition 3.1.2 consisted primarily of showing that an nth root $\alpha^{1/n}$ had to have degree at least n over $\mathbb{Q}(\alpha)$ in

the analogous setting, when α was a torsion-free representative of f and f satisfied $R(f) = \mathbb{Z}$. It is not difficult to see that analogues of Lemma 3.1.3, p. 51 and Lemma 3.1.5, p. 52 are true, and thus $R(\xi)$ is a well-defined fractional ideal, as claimed. Showing that the minimal degree scales in the same fashion, however, remains an open question.

As we did for algebraic numbers modulo torsion, we can define the *projection irreducible* elements $\mathcal{P}$ to be the set of $\xi \in V$ such that $P_K \xi = 0$ for all $K \in \mathcal{K}, K \subsetneqq K_\xi$. As we did in Section 4.4, we can choose for each $K \in \mathcal{K}^G$ from the finite dimensional subspace $T_K(V) \cap \mathcal{L} \cap \mathcal{P}$ an element ξ_K of minimal norm $\|\xi_K\|_m$ (notice that here we can use the classical Northcott theorem for elliptic curves and have no need to prove a new L^p analogue as we did in Chapter 4). Then we can define $\Gamma = \Gamma_E = \langle \{\xi_K : K \in \mathcal{K}^G\} \rangle \subset V$ to be the additive subgroup generated by the minimal elements in each $T_K(V)$ subspace which are both Lehmer and projection irreducible. We expect that Conjecture 17 can be shown to be equivalent to the group Γ being closed, and so we make the following conjecture, which is equivalent to Conjecture 14, p. 20 by Lemma 4.4.1, p. 73:

Conjecture 19. *There exists a constant $c > 0$ such that*

$$\|\xi\|_m \geq c \quad \textit{for all} \quad 0 \neq \xi \in \Gamma. \tag{5.4.6}$$

It is easy to see that all of our projections, being orthogonal, are norm one operators with respect to the norm $\|\cdot\|$, and thus the remaining difficulties

in establishing this conjecture primarily lie in showing that the minimal degree d and the orbital degree δ behave appropriately.

Bibliography

[AV09] Daniel Allcock and Jeffrey D. Vaaler, *A Banach space determined by the Weil height*, Acta Arith. **136** (2009), no. 3, 279–298. MR MR2475695 (2009j:11115)

[Ban91] Wojciech Banaszczyk, *Additive subgroups of topological vector spaces*, Lecture Notes in Mathematics, vol. 1466, Springer-Verlag, Berlin, 1991. MR MR1119302 (93b:46005)

[BDM07] Peter Borwein, Edward Dobrowolski, and Michael J. Mossinghoff, *Lehmer's problem for polynomials with odd coefficients*, Ann. of Math. (2) **166** (2007), no. 2, 347–366. MR MR2373144 (2008j:11153)

[BG06] Enrico Bombieri and Walter Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006. MR MR2216774 (2007a:11092)

[Bil97] Yuri Bilu, *Limit distribution of small points on algebraic tori*, Duke Math. J. **89** (1997), no. 3, 465–476. MR MR1470340 (98m:11067)

[BM] Anne-Marie Bergé and Jacques Martinet, *Minorations de hauteurs et petits régulateurs relatifs*, Séminaire de Théorie des Nombres, 1987–1988 (Talence, 1987–1988), Univ. Bordeaux I, Talence, pp. Exp. No. 11, 28. MR MR993110 (90e:11161)

[BM89] ———, *Notions relatives de régulateurs et de hauteurs*, Acta Arith. **54** (1989), no. 2, 155–170. MR MR1024424 (90m:11167)

[BP05] Matthew Baker and Clayton Petsche, *Global discrepancy and small points on elliptic curves*, Int. Math. Res. Not. (2005), no. 61, 3791–3834. MR MR2205235 (2007k:11103)

[dlMF08] Ana Cecilia de la Maza and Eduardo Friedman, *Heights of algebraic numbers modulo multiplicative group actions*, J. Number Theory **128** (2008), no. 8, 2199–2213. MR MR2394816 (2009c:11096)

[Dob79] Edward Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), no. 4, 391–401. MR MR543210 (80i:10040)

[DS01] Artūras Dubickas and Christopher J. Smyth, *On the metric Mahler measure*, J. Number Theory **86** (2001), no. 2, 368–387. MR MR1813119 (2002h:11103)

[DS03] ———, *On metric heights*, Period. Math. Hungar. **46** (2003), no. 2, 135–155. MR MR2004669 (2005a:11160)

[Dub05] Artūras Dubickas, *Two exercises concerning the degree of the product of algebraic numbers*, Publ. Inst. Math. (Beograd) (N.S.) **77(91)** (2005), 67–70. MR MR2213512 (2006m:11150)

[EW99] Graham Everest and Thomas Ward, *Heights of polynomials and entropy in algebraic dynamics*, Universitext, Springer-Verlag London Ltd., London, 1999. MR MR1700272 (2000e:11087)

[FMa] Paul Fili and Zachary Miner, *Norms extremal with respect to the metric Mahler measure*, in preparation.

[FMb] ———, *Orthogonal decomposition of the space of algebraic numbers and Lehmer's problem*, submitted.

[FS09] Paul Fili and Charles L. Samuels, *On the non-Archimedean metric Mahler measure*, J. Number Theory **129** (2009), no. 7, 1698–1708. MR MR2524190

[GH01] Eknath Ghate and Eriko Hironaka, *The arithmetic and geometry of Salem numbers*, Bull. Amer. Math. Soc. (N.S.) **38** (2001), no. 3, 293–314 (electronic). MR MR1824892 (2002c:11137)

[HS90] Marc Hindry and Joseph H. Silverman, *On Lehmer's conjecture for elliptic curves*, Séminaire de Théorie des Nombres, Paris 1988–1989, Progr. Math., vol. 91, Birkhäuser Boston, Boston, MA, 1990, pp. 103–116. MR MR1104702 (92e:11062)

[HS00] ———, *Diophantine geometry*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000, An introduction. MR MR1745599 (2001e:11058)

[KMR40] M. Krein, D. Milman, and M. Rutman, *A note on basis in Banach space*, Comm. Inst. Sci. Math. Méc. Univ. Kharkoff [Zapiski Inst. Mat. Mech.] (4) **16** (1940), 106–110. MR MR0004709 (3,49d)

[Lal07] Matilde N. Lalín, *An algebraic integration for Mahler measure*, Duke Math. J. **138** (2007), no. 3, 391–422. MR MR2322682 (2008i:11094)

[Leh33] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. (2) **34** (1933), no. 3, 461–479. MR MR1503118

[Mos] Michael J. Mossinghoff, *Lehmer's problem*, `http://www.cecm.sfu.ca/~mjm/Lehmer/`.

[MR03] Colin Maclachlan and Alan W. Reid, *The arithmetic of hyperbolic 3-manifolds*, Graduate Texts in Mathematics, vol. 219, Springer-Verlag, New York, 2003. MR MR1937957 (2004i:57021)

[MRW08] Michael J. Mossinghoff, Georges Rhin, and Qiang Wu, *Minimal Mahler measures*, Experiment. Math. **17** (2008), no. 4, 451–458. MR MR2484429 (2009k:11211)

[MS82] Gerald Myerson and Christopher J. Smyth, *Corrigendum: "On measures of polynomials in several variables" [Bull. Austral. Math. Soc.* **23** *(1981), no. 1, 49–63; MR 82k:10074] by Smyth*, Bull. Austral. Math. Soc. **26** (1982), no. 2, 317–319. MR MR683659 (84g:10088)

[Sal45] R. Salem, *Power series with integral coefficients*, Duke Math. J. **12** (1945), 153–172. MR MR0011720 (6,206b)

[Sama] Charles L. Samuels, *The finiteness of computing the ultrametric Mahler measure*, Int. J. Number Theory.

[Samb] ———, *The infimum in the metric Mahler measure*, Canad. Math. Bull.

[Sid77] S. J. Sidney, *Weakly dense subgroups of Banach spaces*, Indiana Univ. Math. J. **26** (1977), no. 6, 981–986. MR MR0458134 (56 #16337)

[Sil92] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original. MR MR1329092 (95m:11054)

[Sil07] ———, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics, vol. 241, Springer, New York, 2007. MR MR2316407 (2008c:11002)

[Smy71] Christopher J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. London Math. Soc. **3** (1971), 169–175. MR MR0289451 (44 #6641)

[Smy81] ———, *On measures of polynomials in several variables*, Bull. Austral. Math. Soc. **23** (1981), no. 1, 49–63, Corrigendum with Gerald

Myerson, Bull. Austral. Math. Soc. **26** (1982), no. 2, 317–319. MR MR615132 (82k:10074)

[Smy08] Chris Smyth, *The Mahler measure of algebraic numbers: a survey*, Number theory and polynomials, London Math. Soc. Lecture Note Ser., vol. 352, Cambridge Univ. Press, Cambridge, 2008, pp. 322–349. MR MR2428530 (2009j:11172)

[SUZ97] L. Szpiro, E. Ullmo, and S. Zhang, *Équirépartition des petits points*, Invent. Math. **127** (1997), no. 2, 337–347. MR MR1427622 (98i:14027)

[SZ65] A. Schinzel and H. Zassenhaus, *A refinement of two theorems of Kronecker*, Michigan Math. J. **12** (1965), 81–85. MR MR0175882 (31 #158)

[Vil99] Fernando Rodriguez Villegas, *Modular Mahler measures. I*, Topics in number theory (University Park, PA, 1997), Math. Appl., vol. 467, Kluwer Acad. Publ., Dordrecht, 1999, pp. 17–48. MR MR1691309 (2000e:11085)

[Yos80] Kôsaku Yosida, *Functional analysis*, sixth ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 123, Springer-Verlag, Berlin, 1980. MR MR617913 (82i:46002)

[Zha98] Shou-Wu Zhang, *Equidistribution of small points on abelian varieties*, Ann. of Math. (2) **147** (1998), no. 1, 159–165. MR

MR1609518 (99e:14032)

Vita

Paul Arthur Fili was born in Boston, Massachusetts on October 12, 1982, the son of Arthur A. Fili and Victoria Pappas Fili. He received his Bachelor of Arts degree in Mathematics and Physics *cum laude* with a citation in Classical Greek from Harvard College in 2004. He began his graduate studies at the University of Texas at Austin in the Fall of 2004. Paul has a younger brother Thomas.

Permanent address: 234 Brook Rd.
Milton, Massachusetts 02186

This dissertation was typeset with LaTeX[†] by the author.

[†]LaTeX is a document preparation system developed by Leslie Lamport as a special version of Donald Knuth's TeX Program.