On the Inverse Problem for Mahler Measure

Matthew Staines

A Thesis submitted for the degree of Doctor of Philosophy

School of Mathematics

University of East Anglia

November 2012

Abstract

We investigate a number of aspects of the inverse problem for Mahler Measure. If β is an algebraic unit, we demonstrate how to determine if there are any reciprocal numbers with measure β. We also give a formula for the number of integer polynomials with measure β and given degree.

Contents

Definitions **1**

Introduction **5**

1 Background Material **7**

1.1 Permutation Groups 7

1.2 Number Fields and Valuations 9

1.3 $\mathbb{C}G$-modules and Representations 13

2 Introduction to Mahler Measure **19**

2.1 Mahler Measure 19

2.2 Lehmer-Pierce Sequences 27

2.3 Algebraic Numbers 32

3 Archimedean Equivalence **43**

3.1 Archimedean Equivalence 43

3.2 Condensed and Basal Polynomials 49

3.3 Calculating Maximal Mahler Sets 67

4 Mahler Sets **85**

4.1 Arbitrarily Large Mahler Sets 85

4.2 Mahler Sets of Condensed Numbers 98

Appendix **110**

Definitions

Definition	Page
action of G on Ω	7
degree of an action	7
permutation isomorphic actions	7
orbit of α under G	8
transitive group	8
block	8
trivial block	8
non-trivial block	8
system of blocks	8
minimally transitive	9
primitive polynomial	9
$Irr(\alpha)$	9
Pisot number	10
Salem number	10
valuation	11
$\lvert \cdot \rvert_v$ extends $\lvert \cdot \rvert_u$	11
equivalent valuations	12
trivial valuation	12
Archimedean valuation	12
non-Arcimedian valuation	12
$\mathbb{C}G$-module	13

Definition	Page
$\mathbb{C}G$-submodule	14
$\mathbb{C}G$-isomorphism	14
isomorphic $\mathbb{C}G$-modules	14
$V(K,\zeta,(\epsilon_1,\ldots,\epsilon_m))$	14
$\pi_\epsilon(x)$	14
representation of G over $\mathbb{C}$	15
equivalent representations	15
matrix of θ relative to $\mathscr{B}$, $[\theta]_{\mathscr{B}}$	16
irreducible $\mathbb{C}G$-submodule	17
irreducible representation	17
reducible $\mathbb{C}G$-submodule	17
reducible representation	17
Malher measure of a polynomial, $M(f)$	19
large algebraic number	19
length of a polynomial, $L(f)$	21
reciprocal of a polynomial	24
reciprocal polynomial	24
Mahler set of polynomials	25
degree and measure of a Mahler set of polynomials	25
maximal Mahler set	25
$\Delta_n(f)$	27
Mahler measure of an algebraic number	32
Mahler set of algebraic numbers	33
degree/measure of a Mahler set (numbers)	33
maximal Mahler set of algebraic numbers	33
$\mathcal{M}^*$	34
$\mathcal{M}$	35
measure	35
reciprocal number	36

Definition	Page
$\mathcal{R}$	38
$\mathcal{N}$	38
Perron numbers	39
$\mathbb{P}$	39
irreducible Perron number	41
Archimedian equivalent to α over K	43
Archimedian equivalent to α	44
A-equivalent, $\sim$	44
basal	50
basal irreducible	50
condensed polynomial	54
condensed algebraic number	54
$\Gamma(\alpha)$	54
$\Gamma^*(\alpha)$	54
$C(\alpha)$	54
$C^*(\alpha)$	54
DD-minimal	55
Archimedean standard form	70
$\tau(f)$	70
$T(\beta)$	70
$S_0(\beta, d)$	72
$S_1(\tau^*, \beta, d)$	72
$E(\alpha)$	72
basis for $\tau(\alpha)$	72
$S_2((\alpha_1, \ldots, \alpha_n), (i_1, \ldots, i_n), \beta, d)$	73
$S_2(\alpha, i)$	73
matches α	75
$N(\alpha, m)$	75
relative height on K, $H_K(\alpha)$	88

Definition	Page
quasi-reciprocal	93
Ω_n	98
$S(\alpha)$	98
Υ_n	98
c_n	98
Large Mahler Set	99
Φ_n	100
Ψ_n	100

Introduction

We investigate a number of aspects of the inverse problem for Mahler Measure. The first two chapters cover background material and introduce Mahler measure and the inverse problem. We also introduce Mahler sets, which are sets of integer polynomials or algebraic numbers with the same Mahler measure and degree.

In Chapter 3 we introduce Archimedean equivalence. Dixon and Dubickas [4] showed how to determine if an algebraic number is the Mahler measure of an integer polynomial or algebraic unit. Theorem 3.24 and Theorem 3.25 show how to do this using Archimedean equivalence. We introduce a third result of this format with Theorem 3.27. This shows how to determine if an algebraic number is the Mahler measure of a reciprocal algebraic unit. For an algebraic unit β, Section 3.3 describes the enumeration of integer polynomials of a given degree and Mahler measure β.

Chapter 4 focuses on Mahler sets of algebraic units. We investigate whether or not the unit group of the ring of integers of an algebraic number field contains arbitrarily large Mahler sets. We provide some sufficient conditions in Corollary 4.6, whilst Theorem 4.12 shows that this phenomenon cannot occur in number fields of prime degree. In Section 4.2

we define large Mahler sets. For large Mahler sets with degree less than or equal to 11, Theorem 4.21 gives restrictions on the Mahler measure of the Mahler set.

Chapter 1

Background Material

1.1 Permutation Groups

In this section we introduce permutation groups. This material is all covered in greater detail by Dixon and Mortimer in [5]. Let G be a group and let Ω be a non-empty set, and suppose that $(\alpha, x) \mapsto \alpha^x$ is a function of $\Omega \times G$ into Ω. We say this defines an *action* of G on Ω, or G *acts on* Ω, if the following holds.

- $\alpha^1 = \alpha$ for all $\alpha \in \Omega$, where 1 is the identity element in G.
- $(\alpha^x)^y = \alpha^{xy}$ for all $\alpha \in \Omega$ and all $x, y \in G$.

The *degree* of an action is defined to be the cardinalilty of Ω.

Let G and H be groups acting on Ω_G and Ω_H respectively. We say G and H are *permutation isomorphic* if there exists a bijection $\lambda : \Omega_G \to \Omega_H$

and a group isomorphism $\psi : G \to H$ such that

$$\lambda(\alpha^x) = \lambda(\alpha)^{\psi(x)} \text{ for all } \alpha \in \Omega_G \text{ and all } x \in G.$$

The *orbit* of α under G is the set

$$\alpha^G = \{\alpha^x \mid x \in G\}.$$

Orbits partition Ω into mutually disjoint subsets.

A group G acting on a set Ω is said to be *transitive* on Ω if $\alpha^G = \Omega$ for all $\alpha \in \Omega$. When a group G acts on Ω, it also acts on the subsets of Ω in a natural way. Define $\Gamma^x = \{\gamma^x \mid \gamma \in \Gamma\}$ for any $\Gamma \subset \Omega$. Let G be a group acting transitively on Ω. A nonempty subset Δ of Ω is called a *block* for G if, for each $x \in G$, either $\Delta^x = \Delta$ or $\Delta^x \cap \Delta = \emptyset$. For any group G acting transitively on a set Ω, then Ω and singleton sets $\{\alpha\}$, where $\alpha \in \Omega$, are blocks. These blocks are called *trivial blocks*, and all other blocks are called *non-trivial.* If G acts transitively on Ω, and Δ and Γ are blocks for G then either the two blocks are disjoint, or $\Delta \cap \Gamma$ is a block. Suppose G acts transitively on Ω and that Δ is a block for G. Then the sets contained in $\Sigma = \{\Delta^x \mid x \in G\}$ are all blocks and partition Ω. We call such a partition a *system of blocks.* If Σ is a system of blocks for a transitive group G, then the action of G on Σ is also transitive. The following lemma captures the relationship between a system of blocks and equivalence relations.

Lemma 1.1. *Let G be a group acting transitively on Ω. A G-congruence* *on Ω is an equivalence relation $\sim$ on Ω with the property that, for $\alpha, \beta \in \Omega$,*

$$\alpha \sim \beta \iff \alpha^x \sim \beta^x \text{ for all } x \in G.$$

If Σ is a system of blocks for G then Σ is the set of equivalence classes for some G-congruence. If $\sim$ is a G-congruence then the equivalence classes of $\sim$ form a system of blocks for G.

We say the action of a transitive group G on Ω is *minimally transitive* if the restriction of the action to $\Omega \times H$ is not transitive for any proper subgroup H of G.

1.2 Number Fields and Valuations

In this section we cover some fundamental results about number fields. We first mention that we require a number field to be a subset of $\mathbb{C}$, and not just an arbritrary finite extension of $\mathbb{Q}$. We begin with some defintions and highlighting some facts about number fields.

Definition 1.2. Let α be an algebraic number.

- We say an integer polynomial is *primitive* if ± 1 are the only integers are which divide every coefficient of the polynomial.
- We define $\operatorname{Irr}(\alpha)$ to be the unique non-zero, primitive, irreducible polynomial in $\mathbb{Z}[X]$ of smallest degree, with positive leading coefficient such that $\operatorname{Irr}(\alpha) = 0$.

- α is called a *Pisot* number if it is a real algebraic integer, with $\alpha > 1$ and if none of its other conjugates lie on or outside the unit circle.
- α is called a *Salem* number if it is a real algebraic unit with $\alpha > 1$, if none of its other conjugates lie outside the unit circle and if α has conjugates on the unit circle.

Lemma 1.3. *Let K be a number field of degree n.*

- *K contains at most $2n^2$ roots of unity. If n is odd, then ± 1 are the only roots of unity in K.*
- *Let α be an algebraic number, and let a_d be the leading coefficient of Irr(α). If $\{\alpha_1, \ldots, \alpha_m\}$ is a subset of the set of conjugates of α then $a_d\alpha_1 \ldots \alpha_m$ is an algebraic integer. Furthermore $k\alpha$ is an algebraic integer if and only if a_d divides k.*
- *If $K \subset \mathbb{R}$ and $n \geq 2$, then the unit group of $\mathcal{O}_K$ contains a Pisot number of degree n.*

Proof. The majority of these statements are proven in Chapter 13 of Alaca Williams [1]. The exception is the claim that $a_d\alpha_1 \ldots \alpha_m$ is an algebraic integer. This is a classical result found for example on page 91 in Hecke [12].

□

We now cover Dirichlet's unit theorem and the Archimedean valuations on a number field. Both of these will be very important. Dirichlet's unit theorem describes the structure of the unit group of a ring of integers. A proof can be found in Chapter 13 of Alaca and Williams [1].

Theorem 1.4. *Let K be a number field of degree n. Let r be the number of real embeddings of K and $2s$ the number of complex embeddings of K. Then $\mathcal{O}_K$ contains $r+s-1$ units $\epsilon_1, \dots, \epsilon_{r+s-1}$ such that each unit of $\mathcal{O}_K$ can be expressed uniquely in the form*

$$\rho \epsilon_1^{n_1} \cdots \epsilon_{r+s-1}^{n_{r+s-1}},$$

where ρ is a root of unity in $\mathcal{O}_K$ and $n_1, \dots, n_{r+s-1}$ are integers.

We begin describing the Archimedean valuations of a number field by defining the general notion of a valuation for a field. More information on valuations and the following results can be found in Chapter 2 of Janusz [14].

Definition 1.5. Let K be a field. An *valuation* on K is a map $a \mapsto |a|$ from K to $\mathbb{R}$ such that

1. $|a| \geq 0$ and $|a| = 0 \iff a = 0$,
2. $|ab| = |a||b|$,
3. $|a+b| \leq |a| + |b|$.

The following example describes an important set of valuations for $\mathbb{Q}$.

Example 1.6. *Let p be a prime. Then there exists a valuation $|\cdot|_p$ on $\mathbb{Q}$ defined as follows. Any non-zero $x \in \mathbb{Q}$ can be written as $x = p^i \frac{r}{s}$, where $r, s \in \mathbb{Z}$ and $p \nmid rs$. Then $|x|_p$ is defined to be $|x|_p = p^{-i}$. A separate valuation is the usual absolute value, sometimes denoted $|\cdot|_\infty$ to avoid confusion.*

Definition 1.7. Let K be a field and let $|\cdot|_v$ be a valuation on K. If L is a subfield of K, then the restriction of $|\cdot|_v$ to L is a valuation $|\cdot|_u$ on L. We say that $|\cdot|_v$ *extends* $|\cdot|_u$.

Definition 1.8. Let K be a field. For any valuation $|\cdot|$ on K, we can define a metric using $d(a, b) = |a - b|$. This metric then induces a topology on K. We say two valuations on K are *equivalent* if they induce the same topology on K.

There are three distinct types of valuation.

Definition 1.9. Let $|\cdot|$ be a valuation for a field K. The *trivial* valuation is defined as $|a| = 1$ for all non-zero $a \in K$, whilst $|0| = 0$. We say a non-trivial valuation $|\cdot|$ is *non-Archimedean* if it satisfies $|a + b| \leq \max\{|a|, |b|\}$ for all $a, b \in K$. A valuation $|\cdot|$ is *Archimedean* if it is neither of the previous two types.

Lemma 1.10. *Let $|\cdot|_1$ and $|\cdot|_2$ be valuations on a field K. The following are equivalent statements.*

1. *$|\cdot|_1$ is equivalent to $|\cdot|_2$*

2. *$|\cdot|_1 = |\cdot|_2^{\alpha}$ for some $\alpha > 0$.*

The trivial valuation is equivalent only to itself. Furthermore an Archimedean valuation on K can only be equivalent to an Archimedean valuation.

This allows us to describe the set of all valuations for $\mathbb{Q}$.

Example 1.11. *Let $|\cdot|$ be a non-trivial valuation for $\mathbb{Q}$. If $|\cdot|$ is Archimedean, then it is equivalent to $|\cdot|_\infty$. If $|\cdot|$ is non-Archimedean, then there is a unique prime p such that $|\cdot|$ is equivalent to $|\cdot|_p$.*

We now describe the Archimedean valuations for an algebraic number field.

Lemma 1.12. *Let K be a number field with r real embeddings $\sigma_1, \ldots, \sigma_r$ and $2s$ complex embeddings $\sigma_{r+1}, \ldots, \sigma_{r+2s}$ such that $\sigma_{r+i} = \overline{\sigma_{r+s+i}}$ for $1 \leq i \leq s$. Then there exist $r+s$ pairwise inequivalent Archimedean valuations $|x|_v = |\sigma_v(x)|$ for $1 \leq i \leq r+s$. Each of these valuations extends the usual absolute value on $\mathbb{Q}$ and every Archimedean valuation is equivalent to one of these $r+s$ valuations.*

1.3 $\mathbb{C}G$-modules and Representations

In this section we introduce $\mathbb{C}G$-modules and representations of groups. This material is covered in greater detail by James and Liebeck in [13]. We will also show a construction of $\mathbb{C}G$-modules from the unit group of a normal number field.

Let V be a vector space over $\mathbb{C}$ and let G be a group. We say V is a $\mathbb{C}G$-*module* if multiplication gv ($g \in G$,$v \in V$) is defined so as to satisfy the following properties:

- $gv \in V$ for all $g \in G$ and all $v \in V$,
- $g(hv) = (gh)v$ for all $g, h \in G$ and all $v \in V$,
- $1v = v$ for all $v \in V$ where 1 is the identity in G,
- $g(\lambda v) = \lambda(gv)$ for all $\lambda \in \mathbb{C}$, all $g \in G$ and all $v \in V$,
- $g(u+v) = gu + gv$ for all $g \in G$ and all $u, v \in V$.

A $\mathbb{C}G$-*submodule* of V is a subspace of V which is also a $\mathbb{C}G$-module. Let V and W be $\mathbb{C}G$-modules. We call a function $\theta : V \to W$ a $\mathbb{C}G$-*isomorphism* if θ is an invertible linear transformation and if

$$\theta(gv) = g\theta(v) \text{ for all } v \in V, g \in G.$$

We say two $\mathbb{C}G$-modules V and W are *isomorphic* if there exists a $\mathbb{C}G$-isomorphism from V to W. We denote this by $V \cong W$.

A $\mathbb{C}G$-module is often easier to work with if a basis is defined for the underlying vector space. It is also a convenient way to create a $\mathbb{C}G$-module from a vector space. If $\mathscr{B}$ is a basis for a vector space, it is sufficient to define multiplication for the elements of $\mathscr{B}$. The axioms listed above then extend the multiplication to all elements of the vector space to give a $\mathbb{C}G$-module. The following is an example of this.

Definition 1.13. Let K be an algebraic number field, normal over $\mathbb{Q}$, such that K is neither $\mathbb{Q}$ nor an imaginary quadratic field. Let r and $2s$ be the number of real and complex embeddings, respectively, and let $m = r + s - 1$. Let $\zeta \in K$ be a root of unity, and let $\epsilon_1, \dots, \epsilon_m$ be units such that the unit group of $\mathcal{O}_K$ is equal to $U = \langle \zeta, \epsilon_1, \dots, \epsilon_m \rangle$. Let $G = \mathrm{Gal}(K/\mathbb{Q})$. Let $e_i \in \mathbb{C}^m$ be the vector with the i-th entry equal to 1 and zeroes everywhere else. Then for any $e_i \in \{e_1, \dots, e_m\}$, ge_i is defined as the vector $(v_1, \dots, v_m)$ such that $g(\epsilon_i) = \zeta^{v_0}\epsilon_1^{v_1} \cdots \epsilon_m^{v_m}$ for some integer v_0. This defines a $\mathbb{C}G$-module of dimension m, which we denote $V(K, \zeta, (\epsilon_1, \dots, \epsilon_m))$.

Definition 1.14. Suppose $\epsilon_1, \dots, \epsilon_n$ are independent algebraic units, and that none of them are a root of unity. Suppose $a_1, \dots, a_n$ are integers and that ζ is a root of unity. Let

$$x = \zeta \epsilon_1^{a_1} \dots \epsilon_n^{a_n}.$$

and let $\epsilon = (\epsilon_1, \dots, \epsilon_n)$. Then $\pi_\epsilon(x)$ is defined to be $(a_1, \dots, a_n)$.

Example 1.15. *Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ which is a totally real quartic number field. Let $\epsilon_1 = 1 + \sqrt{2}$, $\epsilon_2 = \sqrt{2} + \sqrt{3}$ and $\epsilon_3 = \frac{1}{2}(\sqrt{2} + \sqrt{6})$. These are three independent units such that the unit group of the ring of integers of K is equal to $\langle -1, \epsilon_1, \epsilon_2, \epsilon_3 \rangle$. We label the four elements $\sigma_1, \dots, \sigma_4$ of $G = \mathrm{Gal}(K/\mathbb{Q})$ such that:*

$$\sigma_1 \textit{ is the identity, } \sigma_2 \textit{ fixes } \sqrt{2}, \sigma_3 \textit{ fixes } \sqrt{3} \textit{ and } \sigma_4 \textit{ fixes } \sqrt{6}.$$

Then $V(K, -1, (\epsilon_1, \epsilon_2, \epsilon_3))$ is a 3-dimensional $\mathbb{C}G$-module with multiplication defined as follows;

$$\begin{aligned} \sigma_1(v_1, v_2, v_3) &= (v_1, v_2, v_3), & \sigma_2(v_1, v_2, v_3) &= (v_1, -v_2, -v_3), \\ \sigma_3(v_1, v_2, v_3) &= (-v_1, -v_2, v_3), & \sigma_4(v_1, v_2, v_3) &= (-v_1, v_2, -v_3) \end{aligned}$$

The study of $\mathbb{C}G$-modules leads to studying representations of G over $\mathbb{C}$. We begin by defining representations.

Let $\mathrm{GL}(n, \mathbb{C})$ be the group of invertible $n \times n$ matrices with entries in $\mathbb{C}$. Let G be a group. A *representation of G over $\mathbb{C}$* of degree n is a homomorphism ρ from G to $\mathrm{GL}(n, \mathbb{C})$, where n is a positive integer. Two representations σ and ρ of the group G, are called *equivalent* if they have the same degree, say n, and there exists an invertible $n \times n$ matrix T such that, for all $g \in G$,

$$\sigma(g) = T^{-1}\rho(g)T.$$

It is straightforward to check that this relation is an equivalence relation.

Let V be a vector space over $\mathbb{C}$, and let θ be an endomorphism of V. Suppose $\mathscr{B} = \{v_1, \ldots, v_n\}$ is a basis for V. Then there exist scalars $a_{ij} \in \mathbb{C}$ where $1 \leq i, j \leq n$ such that for each i,

$$\theta(v_i) = a_{i1}v_1 + \cdots + a_{in}v_n.$$

We then define the matrix of θ *relative to the basis* $\mathscr{B}$ to be the $n \times n$ matrix (a_{ij}) and denote it $[\theta]_{\mathscr{B}}$. The following lemma explains the relationship between $\mathbb{C}G$-modules and representations of G over $\mathbb{C}$.

Lemma 1.16. *Suppose that V is a $\mathbb{C}G$-module with basis $\mathscr{B}$, and let ρ be the representation of G over $\mathbb{C}$ defined by*

$$\rho : g \to [g]_{\mathscr{B}} \quad (g \in G)$$

1. *If $\mathscr{B}'$ is also a basis of V, then the representation*

   $$\phi : g \to [g]_{\mathscr{B}'} \quad (g \in G)$$

   of G is equivalent to ρ.

2. *If σ is a representation of G, then there is a basis $\mathscr{B}'$ of V such that*

$$\sigma : g \to [g]_{\mathscr{B}'} \quad (g \in G).$$

3. *If W is another $\mathbb{C}G$-module with basis $\mathscr{B}'$, then $V \cong W$ if and only if the representation*

$$\sigma : g \to [g]_{\mathscr{B}'}$$

is equivalent to ρ.

Example 1.17. *Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and let $\epsilon_1, \epsilon_2, \epsilon_3$ and G be defined as in Example 1.15. Let $\mathscr{B}$ be the basis $\{(1,0,0),(0,1,0),(0,0,1)\}$ for $\mathbb{C}^3$. Then we can define a representation for G using $V(K, -1, (\epsilon_1, \epsilon_2, \epsilon_3))$ and Lemma 1.16 as follows:*

$$\rho(\sigma_1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \rho(\sigma_2) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$
$$\rho(\sigma_3) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \rho(\sigma_4) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

We now give an important result about the structure of $\mathbb{C}G$-modules. If V and W are two disjoint $\mathbb{C}G$-modules, then $V \oplus W$ is also a $\mathbb{C}G$-module. A $\mathbb{C}G$-submodule V is called *irreducible* if it is non-zero and it has no $\mathbb{C}G$-submodules apart from $\{0\}$ and V. A representation $\rho : G \to GL(n, \mathbb{C})$ is *irreducible* if the corresponding $\mathbb{C}G$-module $\mathbb{C}^n$ given by

$$gv = \rho(g)v \quad (v \in \mathbb{C}^n, g \in G)$$

is irreducible. A $\mathbb{C}G$-module or representation that is not irreducible is known as *reducible*.

Theorem 1.18. *Let G be a finite group and let V be a $\mathbb{C}G$-module. Then there exist irreducible $\mathbb{C}G$-modules $U_1, \ldots, U_m$ such that $V = U_1 \oplus \cdots \oplus U_m$. This decomposition is unique up to order and $\mathbb{C}G$-isomorphism of the factors.*

Lemma 1.19. *Let G be the cyclic group of n elements generated by g and let $\omega = e^{2\pi i/n}$. For each integer j with $0 \leq j \leq n-1$, let ρ_j be the representation of G over $\mathbb{C}$ such that*

$$\rho_j(g^k) = \left(\omega^{jk}\right)$$

for all integers k with $0 \leq k \leq n-1$. Then every irreducible representation of G over $\mathbb{C}$ is equal to one of the representations ρ_j.

Chapter 2

Introduction to Mahler Measure

In this chapter we introduce Mahler measure and the problem of studying polynomials with the same Mahler measure.

2.1 Mahler Measure

Mahler measure first appeared as an unnamed function in a paper of D.H. Lehmer from 1933 [15]. His work on factoring large numbers is discussed in Section 2.2. The following is a simple generalisation of Lehmer's definition.

Definition 2.1. For a non-zero polynomial

$$f = a_d \prod_{i=1}^{d} (X - \alpha_i) \in \mathbb{C}[X]$$

of degree d, the Mahler measure of f is defined to be

$$M(f) = |a_d| \prod_{i=1}^{d} \max(1, |\alpha_i|).$$

We say an algebraic number α is *large* if $|\alpha| > 1$.

Kurt Mahler proved a number of results about this function, and it now bears his name. His notation, $M(f)$, has also replaced Lehmer's as the standard notation. We begin by covering a number of classical results about Mahler measure. The first is that Mahler measure of polynomials is multiplicative. The existence, or otherwise, of a multiplicative structure is a recurrent theme in our work.

Lemma 2.2. *For non-zero polynomials $f, g \in \mathbb{C}[X]$, Mahler measure is multiplicative: $M(f \cdot g) = M(f) \cdot M(g)$.*

Proof. This follows immediately from the definition of Mahler measure. □

The next result was proven by Mahler, and can be used as an alternative definition for Mahler measure. It states that Mahler measure is equal to the geometric mean of $|f|$ around the unit circle. The result is an application of Jensen's formula and is given without proof. Further details are given by Everest and Ward in [10] on page 9.

Theorem 2.3. *For a non-zero polynomial $f \in \mathbb{C}[X]$,*

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

A number of applications for Mahler measure consider only integer polynomials. The following theorem gives an upper and lower bound for the Mahler measure of an integer polynomial.

Definition 2.4. For a non-zero integer polynomial $f = \sum_{i=0}^{n} a_i x^i$, let the *length* $L(f)$ *of* f be $L(f) = |a_0| + \cdots + |a_n|$.

Lemma 2.5. *Let f be a non-zero integer polynomial. Then*

$$2^{-n} L(f) \leq M(f) \leq L(f).$$

Proof. The upper bound is proven using Theorem 2.3. It is clear that $L(f)$ is an upper bound for the value of $|f(X)|$ on the unit circle, and so $M(f) \leq L(f)$. The lower bound is straightforward once it is observed that the coefficients a_i satisfy $|a_i| \leq \binom{d}{i} M(f)$. To see this, treat the coefficients of f as elementary symmetric functions in the roots $\alpha_1, \ldots, \alpha_n$ of f. Then

$$\begin{aligned} |a_i| = \left| a_d \sum_{1 \leq j_1 < \cdots < j_i \leq n} \alpha_{j_1} \cdots \alpha_{j_i} \right| &\leq a_d \sum_{1 \leq j_1 < \cdots < j_i \leq n} |\alpha_{j_1} \cdots \alpha_{j_i}| \\ \leq \sum_{1 \leq j_1 < \cdots < j_i \leq n} M(f) = \binom{d}{i} M(f). \end{aligned}$$

□

The inverse problem for Mahler measure is best considered in two parts, following Boyd in [2].

1. Given an algebraic number β, does there exist an integer polynomial with Mahler measure equal to β?

2. Assuming an affirmative answer to the first question, can you determine all integer polynomials with Mahler measure β?

An effective method for solving the first question was provided by Dixon and Dubickas in [4]. We develop the ideas of their paper in Chapter 3. It is often necessary, or of interest, to restrict the inverse problem to irreducible polynomials. This renders the first problem, in general, unresolved. The second question is almost completely unanswered. There are only two instances for which this question has been resolved. The first example we can solve is the equation $M(f) = 1$. This is clearly the minimum value of Mahler measure over the integer polynomials. To proceed we require the following classical result of Kronecker. The following proof is taken from [10].

Lemma 2.6 (Kronecker)**.** *Suppose that $\alpha \neq 0$ is an algebraic integer and the algebraic conjugates $\alpha_1 = \alpha, \ldots, \alpha_d$ of α all have modulus at most 1. Then α is a root of unity.*

Proof. Consider the polynomials

$$F_n = \prod_{i=1}^{d} (X - \alpha_i^n)$$

where n ranges over the positive integers. We see that $F_n \in \mathbb{Z}[X]$, since the coefficients are symmetric functions in $\alpha_1, \ldots, \alpha_d$. Since all roots of these polynomials have modulus at most 1, the coefficients are uniformly bounded. These ensures that F_n can take only finitely many values. Choose positive integers n, m such that $m > n$ and $F_n = F_m$. We then observe that

$$\{\alpha_1^n, \ldots, \alpha_d^n\} = \{\alpha_1^m, \ldots, \alpha_d^m\}.$$

We define a permutation τ on the set $\{1,\ldots,d\}$, where $\tau(i)$ satisfies

$$\alpha_i^n = \alpha_{\tau(i)}^m.$$

If r is the order of this permutation, then

$$\alpha_1^{n^r}\left(\alpha_1^{m^r-n^r}-1\right)=0,$$

and since $\alpha=\alpha_1\neq 0$, α must be a root of unity. Permutations of finite sets have finite order, so we can choose a positive integer r such that

$$\alpha^{n^r}(\alpha^{m^r-n^r}-1)=0.$$

Together with $\alpha\neq 0$, this implies that α is a root of unity. □

The following is the first complete solution for the inverse problem.

Theorem 2.7. *Let $f\in\mathbb{Z}[X]$ be a non-zero polynomial such that $f(0)\neq 0$. The following are equivalent.*

- *$M(f)=1$*
- *f is primitive, and every root of f is a root of unity.*

Proof. Write $f=a_0\prod_{i=1}^d(X-\alpha_i)$. f is primitive if and only if $a_0=\pm 1$. The result then follows by comparing the definition of Mahler measure with the result of Kronecker. □

The only other complete solution to the inverse problem is for the equation

$M(\alpha) = \theta_0$ where

$$\theta_0 = \left(\tfrac{1}{2} + \tfrac{1}{6}\sqrt{\tfrac{23}{3}}\right)^{1/3} + \left(\tfrac{1}{2} - \tfrac{1}{6}\sqrt{\tfrac{23}{3}}\right)^{1/3},$$

is the largest root of $X^3 - X - 1 = 0$. It was shown by Siegel in [20] that θ_0 is the smallest Pisot number. To discuss the result, we first require a definition.

Definition 2.8. The *reciprocal* f^* of a non-zero polynomial $f \in \mathbb{C}[X]$ of degree n is defined as $f^*(X) = X^n f(X^{-1})$. A polynomial f is called *reciprocal* if $f = f^*$.

The following theorem is the product of two results. From the work of Smyth [22], we can give all non-reciprocal solutions f to the equation $M(f) = \theta_0$. The result was completed by Dixon and Dubickas in [4], who showed that there are no reciprocal solutions. We develop the ideas of this final step with Theorem 3.27.

Theorem 2.9. *Let $f \in \mathbb{Z}[X]$ be a polynomial such that $f(0) \neq 0$ and such that no root of f is a root of unity. Then the following are equivalent:*

- *$M(f) = \theta_0$,*
- *f is equal to $\epsilon_1(X^{3n} - X^n - \epsilon_2)$ or $\epsilon_1(\epsilon_2 X^{3n} - X^{2n} + 1)$ where n is a positive integer, and $\epsilon_1, \epsilon_2 \in \{\pm 1\}$.*

The fact that only two complete solutions to the inverse problem are known demonstrates the difficulty of the problem. Restricting the search for solutions to polynomials of a given degree, however, transforms the problem. We call a family of polynomials with the same Mahler measure and degree a Mahler set.

Definition 2.10. We call $S \subset \mathbb{Z}[X]$ a *Mahler set* if it has the following three properties:

- S does not contain the zero polynomial,
- Every member of S has the same degree,
- Every member of S has the same Mahler measure.

The *degree* and *measure* of a Mahler set are defined to be the degree and Mahler measure of any of its elements.

The following theorem is a classical result, and an important property of Mahler measure in some applications. We however express it using the novel framework of Mahler sets.

Theorem 2.11. *If $S \subset \mathbb{Z}[X]$ is a Mahler set, then S is finite.*

Proof. If $f \in S$, then $L(f) \leq \beta 2^d$, where d is the degree of S and β is the measure of S. This is immediate from Lemma 2.5. Since there are only finitely many integer polynomials with bounded length and fixed degree, S cannot be infinite. □

This inspires the following definition.

Definition 2.12. We say a Mahler set $S \subset \mathbb{Z}[X]$ of degree d and measure β is a *maximal* Mahler set if it contains every polynomial in $\mathbb{Z}[X]$ of degree d and measure β.

Maximal Mahler sets can naturally be viewed as the fibres of Mahler measure ranging over integer polynomials of a given degree. The method demonstrated in Theorem 2.11 can be used to calculate maximal Mahler sets. Clearly the number of polynomials to be tested grows too rapidily in general for this to be a practical method. Because of the difficulty of calculating maximal Mahler sets, we often work with the more flexible notion of Mahler sets. In later chapters we explore the question of how and when maximal Mahler sets can be calculated without resorting to this approach. For now, we highlight the importance of the restriction to integer coefficients.

Lemma 2.13. *Suppose $f \in \mathbb{C}[X]$ is non-zero. Then there exists an uncountable set $S \subset \mathbb{C}[X]$ containing f, such that every element in S has the same degree and measure.*

Proof. Let ϵ be on the unit circle, and let $g_\epsilon(X) = \epsilon f(X)$. By Lemma 2.2, the two polynomials have the same Mahler measure and degree. Since the unit circle is uncountable, the result follows. □

We finish with some simple relationships between polynomials which ensure that they have the same Mahler measure.

Lemma 2.14. *Let $f \in \mathbb{C}[X]$ be a non-zero polynomial. Let $g(X) = f(-X)$, $h(X) = -f(X)$ and $j(X) = f(X^n)$ where n is a positive integer. Then $M(f) = M(f^*) = M(g) = M(h) = M(j)$. The cardinality of any maximal Mahler set is even and, if $f \in \mathbb{Z}[X]$, there are infinitely many other polynomials in $\mathbb{Z}[X]$ with the same Mahler measure.*

Proof. The fact that $M(f) = M(g) = M(h)$ follows directly from the definition of Mahler measure. Since f and $-f$ are distinct for all non-zero polynomials, maximal Mahler sets must have even cardinalities. The claim that $M(f) = M(f^*) = M(j)$ comes directly from Theorem 2.3. Letting n range over the positive integers gives the final claim if f has positive degree. If f is a constant polynomial, say $f = c$ for some positive integer c, then the polynomials $f_n(X) = X^n - c$ can be used instead. □

2.2 Lehmer-Pierce Sequences

Lehmer published many papers on prime numbers and factoring large numbers. This included works on primality testing [16], and the Mersenne numbers, $M_n = 2^n - 1$ [17]. He also studied the following generalisation of the Mersenne sequence, first described by Pierce [19]. Lehmer's results in this section were published in [15].

Definition 2.15 (Lehmer-Pierce Sequences)**.** Let $f \in \mathbb{Z}[X]$ be a monic polynomial, of degree d, where

$$f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_1 X + a_0 = \prod_{i=1}^{d}(X - \alpha_i).$$

To each polynomial f, we associate the sequence $\Delta_n(f)$ as follows

$$\Delta_n(f) = \prod_{i=1}^{d} |\alpha_i^n - 1|.$$

The Mersenne sequence is associated with the polynomial $X - 2$ since

$$\Delta_n(X-2) = 2^n - 1.$$

Since the functions Δ_n are symmetric in the roots of f, Lehmer-Pierce sequences are integer sequences. Lehmer was interested in being able to factorize the terms of these sequences. An attraction of being able to do this, was discovering novel, large prime numbers. The following lemma shows that we can focus on sequences associated to irreducible polynomials.

Lemma 2.16. *Let f and g be monic integer polynomials. Then for all positive integers n, $\Delta_n(f \cdot g) = \Delta_n(f) \cdot \Delta_n(g)$.*

Proof. This follows immediately from the definition of Δ_n. □

We call a prime a characteristic prime factor of $\Delta_n(f)$ if it divides no number of the form $\Delta_\delta(f)$, where δ divides n. Because of the following lemma, being able to calculate the characteristic prime factors of $\Delta_n(f)$ is sufficient to factor terms of Lehmer-Pierce sequences.

Lemma 2.17. *Let n and m be positive integers such that n divides m. Then $\Delta_n(f)$ divides $\Delta_m(f)$ for any monic integer polynomial f.*

Proof. Let α be any root of f and let $m = qn$. Then

$$\alpha^{qn} - 1 = (\alpha^n)(\alpha^{n(q-1)} + \alpha^{n(q-2)} + \cdots + \alpha^n + 1).$$

The result is then obvious. □

Clearly characteristic prime factors can be discovered using trial division. Lehmer's contribution was to prove modular relations which greatly reduce the number of trial attempts that must be made.

Theorem 2.18. *Suppose that $f \in \mathbb{Z}[X]$ is irreducible and of degree r. Let p^e be the highest power of a characteristic prime factor p of $\Delta_n(f)$. If ω is the exponent to which p belongs modulo n, then $\omega \leq r$ and ω divides e.*

This theorem is most effective at reducing the difficultly of factorisation of $\Delta_n(f)$ when $\Delta_n(f)$ is large compared to n. This led Lehmer to study the growth rate of $\Delta_n(f)$, and introduce the first definition of Mahler measure. The following theorem is the connection that Lehmer proved between the growth rate of Lehmer-Pierce sequences and Mahler measure.

Theorem 2.19. *Suppose that no root of $f \in \mathbb{Z}[X]$ lies on the unit circle. Then*

$$\lim_{n\to\infty} \frac{\Delta_{n+1}(f)}{\Delta_n(f)} = M(f).$$

Proof. This follows from the basic properties of limits. We treat each factor of $\Delta_n(f)$ separately. If α is a root of f, then

$$\lim_{n\to\infty} \frac{|\alpha^{n+1}-1|}{|\alpha^n - 1|} = \begin{cases} |\alpha| & \text{if } |\alpha| > 1 \\ 1 & \text{if } |\alpha| < 1 \end{cases}$$

and the result follows. □

When an integer polynomial has roots on the unit circle, this sequence does not converge. However, if f has no cyclotomic factors, we can still relate the growth rate of $\Delta_n(f)$ to $M(f)$. This result is proved using Baker's Theorem from transcendence theory. Further details are given by Everest and Ward in [10] on page 9.

Theorem 2.20. *Suppose that no root of $f \in \mathbb{Z}[X]$ is a root of unity. Then*

$$\lim_{n\to\infty} \frac{1}{n} \log|\Delta_n(f)| = \log M(f).$$

This motivates the use of polynomials with small Mahler measure. A second application of Kronecker's Theorem shows that we should choose polynomials with Mahler measure greater than 1.

Theorem 2.21. *Let $f \in \mathbb{Z}[X]$ be a monic, irreducible, non-zero polynomial. The following are equivalent.*

1. $M(f) = 1$

2. *$f(X) = \pm X$, or f is cyclotomic.*

3. *The sequence $\Delta_n(f)$ is periodic.*

4. *The sequence $\Delta_n(f)$ is bounded.*

Proof. (1.) and (2.) are equivalent by Lemma 2.6. It is trivial to see that (2.) $\implies$ (3.) $\implies$ (4.). If the sequence $\Delta_n(f)$ is bounded, then by Theorem 2.20, $\log(M(f)) = 0$. Hence (4.) implies (1.), which completes the proof. □

We return to the search for large primes amongst the factors of Lehmer-Pierce sequences. In order to reduce the effort needed we aim to find a sequence which grows as slowly as possible, without being bounded. This requires a polynomial with Mahler measure above one, but as small as possible. This gives rise to a question known as Lehmer's problem.

Question 2.22 (Lehmer's problem)**.** *Amongst monic polynomials in $\mathbb{Z}[X]$ with Mahler measure greater than 1, can polynomials be chosen with Mahler measure arbitrarily close to 1?*

The problem is still unresolved. Lehmer showed that

$$M(X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1) = 1.176\ldots,$$

which is still the smallest known value, greater than 1. The level of interest in Mersenne primes raises questions about primes in other Lehmer-Pierce Sequences. Theorem 2.18 was used by subsequent authors [9] to suggest that the terms of the seqeunce $\Delta_n(f)$ are more likely to be prime if $M(f)$ is small. They provide numerical evidence and heuristic arguments to support their conjectures. This encourages the use of polynomials with the same Mahler measure. The simplest technique we have for creating lots of polynomials with the same measure was given in Lemma 2.14. The following theorem shows that this is of no use when interested in prime number generation.

Theorem 2.23. *Let p be a prime number. Let $g(X) = f(X^p)$. For n divisible by p,*

$$\Delta_n(g) = \Delta_{n/p}(f)^p,$$

and for n co-prime to p,

$$\Delta_n(g) = \Delta_n(f).$$

Proof. Let $\alpha_1, \ldots, \alpha_m$ be the roots of f, where $m = \deg(f)$. For each root α_i we choose a solution to the equation $X^p - \alpha_i$ and denote it $\sqrt[p]{\alpha_i}$. Let ζ be a primitive p-th root of unity. Then the roots of g are

$$\zeta^0 \sqrt[p]{\alpha_1}, \zeta^1 \sqrt[p]{\alpha_1}, \ldots, \zeta^{p-1} \sqrt[p]{\alpha_1}, \ldots, \zeta^0 \sqrt[p]{\alpha_m}, \ldots, \zeta^{p-1} \sqrt[p]{\alpha_m},$$

listed with multiplicity. Then if p divides n, we see that

$$\begin{aligned}\Delta_n(g) &= \left|\prod_{i=1}^{m}\prod_{j=0}^{p-1}\left((\zeta^j \sqrt[p]{\alpha_i})^n - 1\right)\right| = \left|\prod_{i=1}^{m}\prod_{j=0}^{p-1}(\alpha_i^{n/p} - 1)\right| \\ &= \left|\prod_{i=1}^{m}(\alpha_m^{n/p} - 1)^p\right| = \left|\Delta_{n/p}(f)^p\right|.\end{aligned}$$

If n and p are co-prime then

$$\begin{aligned}\Delta_n(g) &= \left|\prod_{i=1}^{m}\prod_{j=0}^{p-1}\left(\zeta^{jn}(\sqrt[p]{\alpha_i})^n - 1\right)\right| \\ &= \left|\prod_{i=1}^{m}\prod_{j=0}^{p-1}\left(\zeta^{j}(\sqrt[p]{\alpha_i})^n - 1\right)\right| \\ &= \left|\prod_{i=1}^{m}\left(\left(\prod_{j=0}^{p-1}\zeta^j\right)\alpha_i{}^n + (-1)^p\right)\right|.\end{aligned}$$

The result then follows by considering the odd primes separately from 2. □

This theorem nicely motivates the study of polynomials having the same Mahler measure, where the relationship between them is non-trivial.

2.3 Algebraic Numbers

In this section we describe how Mahler measure is extended to algebraic numbers.

Definition 2.24. The Mahler measure of an algebraic number is defined to be $M(\text{Irr}(\alpha))$.

We extend the definition of a Mahler set to algebraic numbers.

Definition 2.25. We call $S \subset \overline{\mathbb{Q}}$ a *Mahler set* if every element has the same degree and Mahler measure. The *degree* and *measure* of a Mahler set are defined to be the degree and Mahler measure of any of its elements. We say a Mahler set $S \subset \overline{\mathbb{Q}}$ of degree d and measure β, is a *maximal* Mahler set if it contains every algebraic number in $\overline{\mathbb{Q}}$ of degree d and measure β.

The following useful lemma relates the norm of an algebraic number to the norm of its Mahler measure.

Lemma 2.26. *Let α be an non-zero algebraic number of degree d, and let a_d be the leading coefficient of $Irr(\alpha)$. Let $\alpha_1, \ldots, \alpha_m$ be the large conjugates of α and let ϵ be ± 1 such that $M(\alpha) = \epsilon a_d \alpha_1 \cdots \alpha_m$. Let K be the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ and let N be the norm with respect to K. Then*

$$N(M(\alpha)) = (\epsilon a_d)^n N(\alpha)^m$$

where n is the degree of K. Furthermore α is a unit if and only if $M(\alpha)$ is a unit.

Proof. The first claim is trivial since

$$N(M(\alpha)) = N(\epsilon a_d) N(\alpha_1) \ldots N(\alpha_m) = (\epsilon a_d)^n N(\alpha)^m.$$

We can see that if α is a unit, then ϵ,a_d and $N(\alpha)$ all belong to $\{\pm 1\}$. This implies that $N(M(\alpha)) = \pm 1$ and $M(\alpha)$ is a unit. To prove the converse, assume that $N(M(\alpha)) = \pm 1$. By considering the norm of the product of all conjugates of α we can see that

$$N(\alpha) = (a_0/a_d)^{n/d}$$

where a_0 is the last coefficient of $\mathrm{Irr}(\alpha)$. Hence

$$N(M(\alpha)) = \epsilon^n a_d^{n(1-m/d)} a_0^{nm/d}. \tag{2.1}$$

If $m = 0$, then $M(\alpha)$ is invariant under the action of $\mathrm{Gal}(K/\mathbb{Q})$, and so $M(\alpha) = \pm 1$. By Equation (2.1), $a_d = 1$, and so, by Lemma 2.6, α is a root of unity. If $m = d$, we can repeat this analysis for α^{-1}. This would show that α is a root of unity which is a contradiction, and so $m \neq d$. If $0 < m < d$, then all numbers dividing $a_d a_0$ will divide $N(M(\alpha))$, by Equation (2.1). Hence $a_d a_0 = \pm 1$ and so α is a unit. □

In Section 2.1, we stated the first half of the inverse problem is trying to determine if a number is the Mahler measure of a integer polynomial. We complete this section by discussing properties of such numbers.

Definition 2.27.

$$\mathcal{M}^* = \{M(f) \text{ such that } f \in \mathbb{Z}[X]\}$$

The simplest property of $\mathcal{M}^*$ is the following.

Theorem 2.28. *If $\beta \in \mathcal{M}^*$, then $\beta \geq 1$ and β is a real algebraic integer.*

Proof. Let f be an integer polynomial with Mahler measure β. We can assume f is irreducible, since Mahler measure is multiplicative. The fact that $\beta \geq 1$ follows immediately from the definition of Mahler measure. The complex conjugate of a large root of f is also large, which implies that β is real. Finally β is an algebraic integer by Lemma 1.3. □

The inverse problem naturally carries over to algebraic numbers. By analogy with $\mathcal{M}^*$, we study the set of algebraic integers which are the Mahler measure of an algebraic number.

Definition 2.29.

$$\mathcal{M} = \{M(\alpha) \text{ such that } \alpha \in \overline{\mathbb{Q}}\}$$

We call $\beta \in \overline{\mathbb{Q}}$ a *measure* if β belongs to $\mathcal{M}$.

The following theorem describes the relationship between $\mathcal{M}^*$ and $\mathcal{M}$. The non-trivial part, that $\mathcal{M}$ is not a monoid, was proven by Dixon and Dubickas in [4]. We cover their proof in Example 3.22.

Theorem 2.30. *The set $\mathcal{M}^*$ is a monoid under multiplication, generated by $\mathcal{M}$. However $\mathcal{M}$ is not a monoid under multiplication and therefore $\mathcal{M}^* \neq \mathcal{M}$.*

We now calculate some explicit maximal Mahler sets of algebraic numbers. The result is straightforward, but demonstrates an enumeration technique we use later. Corollary 4.13 gives a generalisation to Mahler sets of prime degree.

Lemma 2.31. *Let $S \subset \overline{\mathbb{Q}}$ be a maximal Mahler set of unit measure. If S has degree 2 and measure 1, then $|S| = 6$. If S has degree 2 and measure greater than 1, then $|S| = 4$. If S has degree 3 then $|S| = 12$.*

Proof. We know from Lemma 2.26 that S contains only units. By Kronecker's Theorem, the first claim simply restates the fact that there are exactly 6 quadratic roots of unity. For any quadratic unit x, not a root of unity, let S_x be the Mahler set $S_x = \{\pm x, \pm x^{-1}\}$. Notice that for any such quadratic units x and y, either $S_x = S_y$ or $S_x \cap S_y = \emptyset$. Each S_x contains a single Pisot number, and hence S_x must contain its own measure. The same method works for degree 3. For a cubic unit x let $x_1 = x, x_2$ and x_3 be the conjugates of x and let S_x be the set

$$S_x = \{\pm x_1, \pm x_1^{-1}, \pm x_2, \pm x_2^{-1}, \pm x_3, \pm x_3^{-1}\}.$$

Again we see that for two cubic units x,y, either $S_x = S_y$ or $S_x \cap S_y = \emptyset$ and that each S_x contains a single Pisot number, and hence its own measure. □

Although $\mathcal{M}$ is not a monoid under multiplication, there is still some multiplicative structure. The following theorem was proven by Dubickas [8]. We give a generalisation for unit measures in Chapter 3.

Theorem 2.32. *Let α be an algebraic number, and n a positive integer, then $M(\alpha)^n$ is a measure.*

An important class of numbers in the study of Mahler measure are the reciprocal numbers.

Definition 2.33. Let $\alpha \neq 0$ be an algebraic number. We say α is *reciprocal* if it is conjugate to its reciprocal α^{-1}.

A well known property of a reciprocal number $\alpha \neq 1$ is that $\mathrm{Irr}(\alpha)$ is palindromic.

Lemma 2.34. *Let $\alpha \neq \pm 1$ be an algebraic number of degree n. Let $Irr(\alpha) = a_0 + \cdots + a_n X^n$. Then α is reciprocal if and only if n is even, $a_0 = a_n = 1$ and for $0 \leq i \leq n$, $a_i = a_{n-i}$.*

Proof. We first observe that if $a_0 = a_n = 1$, then

$$\mathrm{Irr}(\alpha^{-1}) = a_n + a_{n-1}X + \cdots + a_1 X^{n-1} + a_0 X^n.$$

This follows by treating the coefficients of $\mathrm{Irr}(\alpha)$ and $\mathrm{Irr}(\alpha^{-1})$ as symmetric functions in the conjugates of α and α^{-1} respectively.

($\Longrightarrow$) If σ is an embedding of $\mathbb{Q}(\alpha)$ then $\sigma(\alpha)\sigma(\alpha^{-1}) = 1$. This allows us to partition the conjugates of α into pairs, which implies n is even. The product of all n conjugates must be 1, which means $a_0 = a_n = 1$. The last condition follows by seeing that $\mathrm{Irr}(\alpha) = \mathrm{Irr}(\alpha^{-1})$.

($\Longleftarrow$) The last condition implies that $\mathrm{Irr}(\alpha) = \mathrm{Irr}(\alpha^{-1})$. Hence α and α^{-1} are conjugate as required. □

We introduced Lehmer's problem in Section 2.2 and θ_0 in Section 2.1 Whilst the original problem remains unsolved, a number of weaker results have been proven. The survey article of Smyth [23] gives a good overview of such results. The following result was proven by Dobrowolski in [6].

Theorem 2.35. *Let α be an algebraic integer of degree n, which is not a root of unity. Then*

$$M(\alpha) > 1 + \frac{1}{1200}\left(\frac{\log(\log(n))}{\log(n)}\right)^3.$$

Another interesting result was proven by Smyth in [21].

Theorem 2.36. *Let $\alpha \neq 0$ be an algebraic number whose Mahler measure is less than θ_0. Then α is a reciprocal number.*

An alternative to the inverse problem is to restrict attention to reciprocal numbers or to non-reciprocal numbers. Theorem 2.36 shows that there exist measures β such that the equation $M(\alpha) = \beta$ has no non-reciprocal solutions. Conversely Theorem 2.9 shows that $M(\alpha) = \theta_0$ has no reciprocal solutions. To continue exploring this problem, we define the following sets.

Definition 2.37. Let $\mathcal{R}$ be the following set.

$$\mathcal{R} = \{M(\alpha) \text{ such that } \alpha \text{ is a reciprocal unit}\}.$$

Let $\mathcal{N}$ be the following set.

$$\mathcal{N} = \{M(\alpha) \text{ such that } \alpha \text{ is a non-reciprocal unit}\}.$$

An open problem is to determine if there is a smallest element of $\mathcal{R} \cap \mathcal{N}$. The following example shows that $\mathcal{R} \cap \mathcal{N}$ is non-empty.

Lemma 2.38. *Let α be a real quadratic unit with $\alpha > 1$. Then $\alpha^2 \in \mathcal{R} \cap \mathcal{N}$.*

Proof. Clearly α^2 is quadratic with norm 1. Hence it is reciprocal, and $M(\alpha^2) = \alpha^2$, and so $\alpha^2 \in \mathcal{R}$. If α has norm 1, let ω be a primitive fourth root of unity. Alternatively if α has norm -1, let ω be a primitive third root of unity. Then $\omega\alpha$ is non-reciprocal, and $M(\omega\alpha) = \alpha^2$. Hence $\alpha^2 \in \mathcal{R} \cap \mathcal{N}$. □

We now describe Perron numbers and explain some connections to the inverse problem. Many of these results and more information about the arithmetic of Perron numbers are given by Lind in [18].

Definition 2.39. Let α be a real algebraic integer whose conjugates are $\alpha_1 = \alpha, \ldots, \alpha_n$. We say α is a *Perron* number if $\alpha > 1$ and, for all integers i with $2 \leq i \leq n$, $|\alpha_i| < \alpha$. Let $\mathbb{P}$ denote the set of all Perron numbers.

Like $\mathcal{M}^*$, the set $\mathbb{P}$ is closed under multiplication.

Lemma 2.40. *Suppose $\alpha, \beta \in \mathbb{P}$. Then $\alpha\beta \in \mathbb{P}$.*

Proof. Clearly $\alpha\beta$ is a real algebraic number with $\alpha\beta > 1$. Let the conjugates of α be $\alpha_1 = \alpha, \ldots, \alpha_n$ and the conjugates of β be $\beta_1, \ldots, \beta_m$. Then the conjugates of $\alpha\beta$ belong to the set $\{\alpha_i\beta_j | 1 \leq i \leq n, 1 \leq j \leq m\}$. For any element $\alpha_i\beta_j$ in this set, $|\alpha_i\beta_j| \leq |\alpha||\beta|$, where equality only holds if $i = j = 1$. Furthermore $\alpha\beta$ is a Perron number. □

Theorem 2.41. *Let $\beta \in \mathcal{M}$ be greater than 1 with conjugates $\beta_1 = \beta, \ldots, \beta_n$. Then for all integers i with $2 \leq i \leq n$, either $\beta^{-1} < |\beta_i| < \beta$ or $\beta_i = \pm\beta^{-1}$. Hence β is a Perron number.*

Proof. Theorem 2.28 shows that β is a real algebraic integer. Let α be an algebraic number with Mahler measure β, and degree d. Let the conjugates of α be $\alpha_1 = \alpha, \ldots, \alpha_d$. Let a_d be the leading coefficient of $\mathrm{Irr}(\alpha)$ and a_0 the constant coefficient. We can assume they are labelled such that

$$|\alpha_1| \geq |\alpha_2| \geq \cdots \geq |\alpha_k| > 1 \geq |\alpha_{k+1}| \geq \cdots \geq |\alpha_d|,$$

where k is the number of conjugates of α outside the unit circle. If $|a_d| > 1$ and $k = 0$, then $\beta = a_d$ and the theorem holds trivially. Hence we can assume $k \geq 1$ since $\beta > 1$, and see that

$$\beta = \pm a_d \alpha_1 \alpha_2 \cdots \alpha_k.$$

Let K be a normal extension of $\mathbb{Q}$ containing α. Then any automorphism σ of K permutes the conjugates of α, and hence the conjugates of β. We see that

$$\sigma(\beta) = \pm a_d \sigma(\alpha_1)\sigma(\alpha_2) \cdots \sigma(\alpha_k).$$

If σ permutes the roots outside the unit circle then $\sigma(\beta) = \beta$. If σ sends β to one of its conjugates, there must be $i \leq k$ and $j > k$ such that $\sigma(\alpha_i) = \alpha_j$. This ensures that $|\sigma(\beta)| < \beta$. We now use the fact that $\alpha_1 \cdots \alpha_d = \pm a_0/a_d$ to show that

$$|\sigma(\beta)| = |a_d \sigma(\alpha_1) \cdots \sigma(\alpha_k)| = \left| \frac{a_d a_0}{a_d \sigma(\alpha_{k+1}) \cdots \sigma(\alpha_d)} \right| \geq \frac{a_d |a_0|}{\beta}.$$

We can see that $|\sigma(\beta)| = |\beta^{-1}|$ if and only if $a_d = |a_0| = 1$ and

$$\{\alpha_1, \ldots, \alpha_k\} = \{\sigma(\alpha_{k+1}), \ldots, \sigma(\alpha_d)\}.$$

This can only happen if $d = 2k$ and for one conjugate of β, implying it must be a real conjugate as required. □

For future reference we record the following result, which was described in the previous proof.

Lemma 2.42. *Let α be an algebraic number and let K be a number field, which is normal over $\mathbb{Q}$ and contains α. Let S be the set of large conjugates* *of α. Then the following holds for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$;*

$$\sigma(M(\alpha)) = M(\alpha) \iff S = \sigma(S).$$

The elements of $\mathcal{M}$ can clearly be factorised into elements of $\mathcal{M}^*$. This corresponds to polynomials being expressed as a product of irreducible factors. We can use the properties of Perron numbers to understand these factorisations.

Theorem 2.43. *If $\lambda = \alpha\beta$ with $\alpha, \beta, \lambda \in \mathbb{P}$, then $\alpha, \beta \in \mathbb{Q}(\lambda)$.*

Proof. Let K be a number field, which is normal over $\mathbb{Q}$ and which contains λ, α and β. Observe that either $\alpha, \beta \in \mathbb{Q}(\lambda)$ or $\alpha, \beta \notin \mathbb{Q}(\lambda)$. For example if $\alpha \in \mathbb{Q}(\lambda)$, then $\beta = \lambda/\alpha \in \mathbb{Q}(\lambda)$. Assume $\alpha, \beta \notin \mathbb{Q}(\lambda)$. Then there will exist an automorphism σ of K which fixes λ, but not α or β. Since α and β are Perron numbers, this implies that $\sigma(\alpha\beta) < \alpha\beta$. This would imply that $\lambda < \lambda$, a contradiction. Hence α, $\beta \in \mathbb{Q}(\lambda)$. □

Definition 2.44. We call $\lambda \in \mathbb{P}$ *irreducible* if $\lambda > 1$ and λ cannot be written as $\lambda = \alpha\beta$ with $\alpha, \beta \in \mathbb{P}$ and $\alpha, \beta > 1$.

We can factorise Perron numbers into a product of irreducible Perron numbers, in the same way as integers are factorised into primes. We consider two factorisations to be the same if the terms of one can be rearranged to give the other.

Theorem 2.45. *Every Perron number greater than one can be factored into a finite number of irreducibles. There are only a finite number of such factorisations, but factorisations into irreducibles are not always unique.*

Proof. Let α be a Perron number and let λ be a Perron number, which appears in a factorisation of α into irreducible Perron numbers. By Theorem 2.43, this implies that λ belongs to the set $\mathbb{P} \cap \mathbb{Q}(\alpha) \cap (1, \alpha]$. Hence to prove the result, it is sufficient to prove that there are finitely many Perron numbers of a given degree d, and below a given bound M. Any such Perron number λ must have Mahler measure less than equal to M^d and hence by Lemma 2.5, $L(\mathrm{Irr}(\lambda)) \leq (2M)^d$. Since there are only finitely many polynomials of degree d with this property, the first claim holds.

The following example from [18] shows that such factorisations need not be unique. Let $\lambda = (1 + \sqrt{5})/2$. Then 5, λ and $\lambda + 2$ are all irreducible Perron numbers. The number $5\lambda^2 = (\lambda + 2)^2$ can therefore be factorised into irreducibles in two different ways. □

We finish the section with two results which compare $\mathbb{P}$ with $\mathcal{M}^*$. The first is due to Boyd [2], whilst the second is due to Dubickas [7].

Theorem 2.46. *Let $f_m = X^m - X - 1$ for any integer $m \geq 4$. Then f has one positive, real root, which is a Perron number, but not a measure.*

Chapter 3

Archimedean Equivalence

In this chapter we introduce an equivalence relation for algebraic numbers. This provides a novel framework for studying Mahler measure and we cover a number of applications. Some of the results in this chapter were first proved by Dixon and Dubickas in [4]. Our approach provides alternative proofs of their results, and generalises some of the ideas they presented.

3.1 Archimedean Equivalence

In this section we define Archimedean equivalence, and introduce some of its basic properties.

Definition 3.1. Let K be a number field and let $\alpha_1, \alpha_2 \in K$. We say α_1 *is Archimedean equivalent to* α_2 *over* K, if $|\alpha_1| > 1 \iff |\alpha_2| > 1$ holds for all Archimedean valuations $|\cdot|$ on K.

It is straightforward to see that this forms an equivalence relation on the elements of K. Using the following lemma, we can remove the dependence on a specific number field.

Lemma 3.2. *Let K and L be number fields which contain α_1 and α_2. Then α_1 is Archimedean equivalent to α_2 over K if and only if α_1 is Archimedean equivalent to α_2 over L.*

Proof. It is sufficient to prove the lemma for $L \subset K$ since the intersection of two number fields is always a number field. The result then follows by considering all valuations on K as extensions of valuations on L, as described by Definition 1.7. □

Definition 3.3. Let α_1 and α_2 be algebraic numbers. We say α_1 *is Archimedean equivalent to* α_2 if there exists a number field K, such that $\alpha_1, \alpha_2 \in K$, and α_1 is Archimedean equivalent to α_2 over K. We write this as $\alpha_1 \sim \alpha_2$ and use the abbreviation *A-equivalence.*

Archimedean equivalence is an equivalence relation, ranging over the set of all algebraic numbers. We use Lemma 3.2 to ensure that A-equivalence is transitive. If $\alpha_1 \sim \alpha_2$ and $\alpha_2 \sim \alpha_3$ then we can use $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ to show that $\alpha_1 \sim \alpha_3$. The following lemma records some of the basic properties of Archimedean equivalence.

Lemma 3.4. *Let α_1, α_2 be algebraic numbers. Let ζ be a root of unity. Then the following results hold;*

1. *Suppose $\alpha_1 \sim \alpha_2$. Then $\alpha_1 \sim \alpha_1\alpha_2 \sim \zeta\alpha_1$.*

2. *Suppose α is a non-zero algebraic integer. Then*

$$\alpha \textit{ is a root of unity} \iff \alpha \sim 1 \iff \alpha \sim \alpha^{-1}.$$

3. *Suppose α_1 and α_2 are non-zero algebraic numbers with no conjugates on the unit circle. Then $\alpha_1 \sim \alpha_2 \iff \alpha_1^{-1} \sim \alpha_2^{-1}$.*

4. *Archimedean equivalence divides any number field into a finite number of equivalence classes.*

Proof. (1) follows from valuations being multiplicative functions, and that any valuation of a root of unity equals 1.

To prove (2), observe that all three conditions imply that α has no conjugates outside the unit circle. For a non-zero algebraic integer this ensures α is a root of unity, by Lemma 2.6.

(3) follows directly from the definition of A-equivalence.

(4) follows from Lemma 1.12 which shows that there are only a finite number of inequivalent Archimedean valuations on any number field. □

Archimedean equivalence is best understood using Galois groups. The following theorem demonstrates how this is done.

Lemma 3.5. *Let K be a number field, normal over $\mathbb{Q}$ with Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. Let $\alpha_1, \alpha_2 \in K$ be algebraic numbers. Let $|\cdot|$ be the usual absolute norm on $\mathbb{C}$. Then the following are equivalent;*

1. *α_1 and α_2 are Archimedean equivalent.*

2. *$|\sigma(\alpha_1)| > 1$ if and only if $|\sigma(\alpha_2)| > 1$ for all $\sigma \in G$.*

Proof. Let $|\cdot|_v$ be an archimedean valuation on K, and $|\cdot|_u$ be the unique equivalent valuation on K which extends the absolute norm on $\mathbb{Q}$. By Lemma 1.12,

$$|\alpha|_u > 1 \iff |\alpha|_v > 1 \text{ for any } \alpha \in K.$$

Hence to test Archimedean equivalence, it is sufficient to test the valuations which extend the absolute value on $\mathbb{Q}$. These valuations can be expressed using the elements of G as shown in the result. □

In the following example we show how Archimedean equivalence fibres the unit group of an algebraic number field.

Example 3.6. *Let $K = \mathbb{Q}(\sqrt[4]{2})$. The unit group of $\mathcal{O}_K$ is $U = \langle -1, \epsilon_1, \epsilon_2 \rangle$, where $\epsilon_1 = 1 + \sqrt[4]{2}$ and $\epsilon_2 = 1 + \sqrt{2}$ are independent units. Let $\epsilon = (\epsilon_1, \epsilon_2)$. We can determine the equivalence class of a number x from the value of $\pi_\epsilon(x)$ since by Lemma 3.4*

$$\pi_\epsilon(x) = \pi_\epsilon(y) \implies x \sim y \textit{ for all } x, y \in U.$$

Considering π_ϵ as a surjection from U to $\mathbb{Z}^2$, we can consider each embedding of K as splitting $\mathbb{Z}^2$ in half. One half corresponds to elements of U mapped outside the unit circle, whilst its complement corresponds to those mapped inside or onto the unit circle. When all embeddings are considered, $\mathbb{Z}^2$ is split up according to the A-equivalence classes for U, by Lemma 3.5. This division of $\mathbb{Z}^2$ is shown in Figure 3.1. In total there are 7 A-equivalence classes represented in U. The first contains only the roots of unity, as described by Lemma 3.4, and is represented by the central point of Figure 3.1. The other equivalence classes correspond to the six regions displayed. These have been labelled with the embeddings which correspond to large roots.

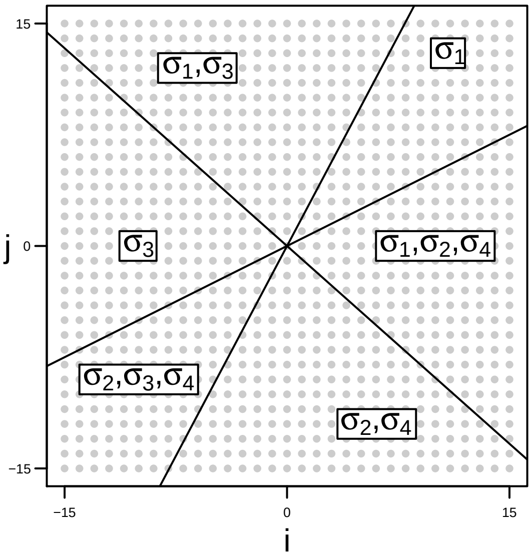

Figure 3.1: A-equivalence classes for $\pm\epsilon_1^i\epsilon_2^j$

We now describe the four embeddings of K. For $n = 1, \ldots, 4$, let σ_n be the embedding that sends $\sqrt[4]{2}$ to $i^{n-1}\sqrt[4]{2}$. Notice that $\sigma_1(x) = x$ and $\sigma_2(x) = \overline{\sigma_4(x)}$ for all $x \in K$. Observe that $1-\sqrt{2} = -\epsilon_2^{-1}$, $1-\sqrt[4]{2} = -\epsilon_1^{-1}\epsilon_2^{-1}$ and $(1+i\sqrt[4]{2})(1-i\sqrt[4]{2}) = \epsilon_2$. These facts allow us to describe when an embedding of a number in U is outside the unit circle;

$$|\sigma_1(x)| > 1 \iff \pi_\epsilon(x) = (i,j) \text{ where } j > -i\frac{\log(\epsilon_1)}{\log(\epsilon_2)},$$

$$|\sigma_2(x)| > 1 \iff |\sigma_4(x)| > 1 \iff \pi_\epsilon(x) = (i,j) \text{ where } j < \frac{i}{2},$$

$$|\sigma_3(x)| > 1 \iff \pi_\epsilon(x) = (i,j) \text{ where } j > i\left(1 + \frac{\log(\epsilon_1)}{\log(\epsilon_2)}\right).$$

We prove the last fact in order to demonstrate the general method. Let $x \in U$

be such that $|\sigma_3(x)| > 1$ *and* $\pi_\epsilon(x) = (i, j)$*. Then*

$$\begin{aligned}
|\sigma_3(x)| > 1 \iff |\sigma_3(\epsilon_1^i \epsilon_2^j) > 1| &\iff |-\epsilon_1^{-1}\epsilon_2^{-1}|^i |\epsilon_2|^j > 1 \\
&\iff -i(\log(\epsilon_1) + \log(\epsilon_2)) + j\log(\epsilon_2) > 0 \\
&\iff j > i\left(1 + \frac{\log(\epsilon_1)}{\log(\epsilon_2)}\right).
\end{aligned}$$

Repeating this method for $|\sigma_1|$ *and* $|\sigma_2\sigma_4|$ *completes the description of the* A*-equivalence classes.*

An important fact about Archimedean equivalence is that it is invariant under the action of Galois groups.

Theorem 3.7. *Let* K *be an algebraic number field normal over* $\mathbb{Q}$*. Let* $\alpha_1, \alpha_2 \in K$ *and* $\sigma \in G = Gal(K/\mathbb{Q})$*. Then* $\alpha_1 \sim \alpha_2 \iff \sigma(\alpha_1) \sim \sigma(\alpha_2)$*.*

Proof. ($\implies$)Assume that $\alpha_1 \sim \alpha_2$. For any $\sigma^* \in G$, $\sigma^*\sigma \in G$, hence

$$|\sigma^*(\sigma(\alpha_1))| > 1 \iff |\sigma^*(\sigma(\alpha_2))| > 1,$$

as required.

($\impliedby$) Let $\sigma^{-1} \in G$ be the inverse of σ. Then

$$\sigma(\alpha_1) \sim \sigma(\alpha_2) \implies \sigma^{-1}(\sigma(\alpha_1)) \sim \sigma^{-1}(\sigma(\alpha_2)) \implies \alpha_1 \sim \alpha_2,$$

using the first half of the proof. □

We finish the section by giving the first connection between Archimedean equivalence and Mahler measure.

Theorem 3.8. *Suppose $\alpha_1 \sim \alpha_2$. Then $\mathbb{Q}(M(\alpha_1)) = \mathbb{Q}(M(\alpha_2))$.*

Proof. Let K be a number field which is normal over $\mathbb{Q}$ and which contains α_1 and α_2. Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. We prove the result by showing that

$$\sigma(M(\alpha_1)) = M(\alpha_1) \text{ if and only if } \sigma(M(\alpha_2)) = M(\alpha_2). \tag{3.1}$$

For any $g \in \mathrm{Gal}(K/\mathbb{Q})$ and for $i = 1$ or 2, let

$$G_i^g = \left\{ \theta \in \mathrm{Gal}(K/\mathbb{Q}) \,\middle|\, |g(\theta(\alpha_i))| > 1 \right\}.$$

We can see from Lemma 2.42 that

$$\sigma(M(\alpha_1)) = M(\alpha_1) \text{ if and only if } G_1^\sigma = G_1^e$$

where e is the identity element of $\mathrm{Gal}(K/\mathbb{Q})$. We now notice that for any $g \in \mathrm{Gal}(K/\mathbb{Q})$, $G_1^g = G_2^g$. This is due to Theorem 3.7. This gives

$$\sigma(M(\alpha_1)) = M(\alpha_1) \text{ if and only if } G_2^\sigma = G_2^e$$

We use Lemma 2.42 again to give (3.1) as required. □

3.2 Condensed and Basal Polynomials

The concept of a basal polynomial was first introduced by Dixon and Dubickas in [4]. We use a simpler definition, by dropping a superfluous condition on the number of roots outside the unit circle. The results in [4] still hold with the new definition.

Definition 3.9. Let $f \in \mathbb{Z}[X]$. We say f is *basal* if no polynomial in $\mathbb{Z}[X]$ has smaller degree and the same Mahler measure. We say that f is *basal irreducible* if no irreducible polynomial in $\mathbb{Z}[X]$ has smaller degree and the same Mahler measure.

By Theorem 2.11, determining if a polynomial is basal can be considered to be a finite calculation, even if it is impractical and unenlightening. The following lemma can be used to create a simple, sufficient condition for being basal. It is a useful result, which was first published by Boyd in [3]. We follow the argument used by Boyd, but use a slightly different framework. We introduce the sets S_θ to show the relationship between the proof of this result and that of Theorem 3.12.

Lemma 3.10. *Let α be an algebraic number of degree d, with s roots outside the unit circle. Suppose $M(\alpha)$ has degree n. Then d divides sn.*

Proof. Let the conjugates of α be $\alpha_1 = \alpha, \ldots, \alpha_d$ and the conjugates of $M(\alpha)$ be $\beta_1 = M(\alpha), \ldots, \beta_n$. Let K be the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ and let $G = \mathrm{Gal}(K/\mathbb{Q})$. For each element of $\theta \in G$, let S_θ be the conjugates of α which are mapped outside the unit circle by θ. We wish to show that

$$\theta(M(\alpha)) = \sigma(M(\alpha)) = \beta_i \text{ implies } S_\theta = S_\sigma$$

for any β_i and any $\sigma, \theta \in G$. We proved this for the case $\beta_i = \beta_1$ in Theorem 2.41. Assume the statement $\theta(M(\alpha)) = \sigma(M(\alpha)) = \beta_i$ holds and let $\rho \in G$ send β_i to $M(\alpha)$. We then see $S_{\rho\theta} = S_{\rho\sigma}$. Applying ρ^{-1} to this set yields $S_\theta = S_\sigma$. Hence for any integer i with $1 \leq i \leq n$, we can unambiguously define the set A_i to be set S_θ where $\theta(M(\alpha)) = \beta_i$. We have two ways of evaluating the sum $\sum_{i=1}^n |A_i|$. The first answer is ns because each set A_i has size s. Alternatively let $\theta_1, \ldots, \theta_m$ be the list of elements of G. Then each conjugate of α appears equally often in the list $\theta_1(\alpha), \ldots, \theta_m(\alpha)$. This means there is a constant l such that each conjugate of α appears in exactly l of the sets A_i. Hence $\sum_{i=1}^n |A_i| = ld = ns$ and the result. □

Corollary 3.11. *Suppose α is an algebraic number of prime degree p, with roots inside and outside the unit circle. Then Irr(α) is basal.*

Proof. We can use Lemma 3.10 to show that p divides the degree of $M(\alpha)$, since p cannot divide the number of roots outside the unit circle. If Irr(α) is not basal, then there exists some $f \in \mathbb{Z}[X]$ with $M(f) = M(\alpha)$ and $\deg(f) < p$. By looking at the roots of f, there must exist an algebraic number α^* such that p divides $\deg(M(\alpha^*))$ with $\deg(\alpha^*) = n < p$. Let K be the Galois closure of $\mathbb{Q}(\alpha^*)$ over $\mathbb{Q}$. Then the group $\mathrm{Gal}(K/\mathbb{Q})$ must be isomorphic to a subgroup of S_n. Since p cannot divide $n!$, $M(\alpha^*)$ cannot belong to K. This is a contradiction, and hence Irr(α) is basal. □

A key technique of Dixon and Dubickas in [4] was to compare the splitting field of a polynomial f with the Galois closure of $\mathbb{Q}(M(f))$ over $\mathbb{Q}$. They showed that it is sufficient for f to be basal, or basal irreducible, for these two fields to be equal. We can go further and give a precise description of the relationship between the two fields.

Theorem 3.12. *Let $f \in \mathbb{Z}[X]$ and suppose J is the splitting field of f. Let K be the Galois closure of $\mathbb{Q}(M(f))$ over $\mathbb{Q}$ and let $\sigma \in \mathrm{Gal}(J/\mathbb{Q})$.*

Then $\sigma \in \mathrm{Gal}(J/K)$ if and only if $\sigma(x) \sim x$ for all roots x of f.

Proof. We first prove the result for $f = \mathrm{Irr}(\alpha)$, where α is an algebraic number. Let $\alpha_1 = \alpha, \ldots, \alpha_n$ and $\beta_1 = M(\alpha), \ldots, \beta_m$ be the conjugates of α and $M(\alpha)$ respectively. Let a be the leading coefficient of f. As in the proof of Lemma 3.10, for all $\theta \in \mathrm{Gal}(J/\mathbb{Q})$, let S_θ be the following set of conjugates of α:

$$S_\theta = \{\alpha_k \,||\theta(\alpha_k)| > 1\}\,.$$

We first show that

$$\sigma \in \mathrm{Gal}(J/K) \iff S_{\sigma\theta} = S_\theta \text{ for all } \theta \in \mathrm{Gal}(J/\mathbb{Q}).$$

($\Longrightarrow$) It was shown during the proof of Lemma 3.10 that if $\theta \in \mathrm{Gal}(J/\mathbb{Q})$, then

$$\sigma(\theta(M(\alpha))) = \theta(M(\alpha)) \implies S_{\sigma\theta} = S_\theta.$$

Since σ fixes every conjugate of $M(\alpha)$, we must have $S_{\sigma\theta} = S_\theta$ for all θ as required.

($\Longleftarrow$) For any $\theta \in \mathrm{Gal}(J/\mathbb{Q})$, we can see that

$$\theta^{-1}(M(\alpha)) = \pm a \prod_{x \in S_\theta} x$$

by applying θ. Hence

$$\sigma(\theta^{-1}(M(\alpha))) = \pm a \prod_{x \in S_\theta} \sigma(x) = \pm a \prod_{x \in S_{\sigma\theta}} x = \pm a \prod_{x \in S_\theta} x = \theta^{-1}(M(\alpha))$$

for any $\theta \in \mathrm{Gal}(J/\mathbb{Q})$. Therefore σ fixes every conjugate of $M(\alpha)$ as required.

($\implies$) We now show that

$$S_{\sigma\theta} = S_\theta \text{ for all } \theta \in \mathrm{Gal}(J/\mathbb{Q}) \iff \sigma(\alpha_k) \sim \alpha_k \text{ for all } \alpha_k.$$

From the definition of S_θ, we see that $S_{\sigma\theta} = S_\theta$ for all $\theta \in \mathrm{Gal}(J/\mathbb{Q})$ is equivalent to

$$|\sigma(\theta(\alpha_k))| > 1 \iff |\theta(\alpha_k)| > 1 \text{ for all } \alpha_k \text{ and all } \theta \in \mathrm{Gal}(J/\mathbb{Q}).$$

This implies that

$$\sigma(\alpha_k) \sim \alpha_k \text{ for all } \alpha_k$$

since θ simply permutes the α_k.

($\impliedby$) This is clear from the definition of S_θ and A-equivalence. This completes the proof of the theorem for $f = \mathrm{Irr}(\alpha)$.

We now let $f = a\mathrm{Irr}(\theta_1)\cdots\mathrm{Irr}(\theta_d)$ for some integer a and algebraic numbers $\theta_1, \ldots, \theta_d$. We wish to show that

$$\sigma \in \mathrm{Gal}(J/K) \iff \sigma(x) \sim x \text{ for all roots } x \text{ of } f.$$

($\implies$) We recall from Theorem 2.41 that $M(f) = |a|M(\theta_1)\cdots M(\theta_d)$ gives a factorisation of $M(f)$ into Perron numbers. Since σ fixes every element of K, by Theorem 2.43, σ fixes every conjugate of the numbers $\theta_1, \ldots, \theta_d$. We now apply the first half of the proof to the polynomials $\mathrm{Irr}(\theta_1), \ldots, \mathrm{Irr}(\theta_d)$ which shows that $\sigma(x) \sim x$ for roots of f.

($\Longleftarrow$) We again use the first half of the proof to see that σ must fix every conjugate of the numbers $M(\theta_1), \ldots, M(\theta_d)$. Hence σ must also fix every conjugate of $M(f)$, and hence $\sigma \in \mathrm{Gal}(J/K)$ as required. □

The Galois closure J of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ will be equal to the Galois closure K of $\mathbb{Q}(M(\alpha))$ over $\mathbb{Q}$ if and only if the Galois group $\mathrm{Gal}(J/K)$ is trivial. The simplest instance of this is when no two conjugates of α are Archimedean equivalent. This inspires the following definition.

Definition 3.13. We say a polynomial $f \in \mathbb{Z}[X]$ is *condensed* if no root of f is Archimedean equivalent to any other. We say an algebraic number α is *condensed* if no two distinct conjugates of α are Archimedean equivalent.

An advantage of Archimedean equivalence is that it provides a useful partition of the conjugates of an algebraic numbers.

Definition 3.14. Let α be an algebraic number. Define $\Gamma(\alpha)$ to be the set of conjugates of α that are Archimedean equivalent to α. Define $\Gamma^*(\alpha)$ to be

$$\Gamma^*(\alpha) = \{\Gamma(\alpha_i) \text{ where } \alpha_i \text{ is conjugate to } \alpha\}.$$

Define the condensation of α, denoted $C(\alpha)$, to be the product of all numbers in $\Gamma(\alpha)$. Define $C^*(\alpha)$ to be

$$C^*(\alpha) = \{C(\alpha_i) \text{ where } \alpha_i \text{ is conjugate to } \alpha\}.$$

We can show that $\Gamma^*(\alpha)$ is an explicit description for the block systems defined by Dixon and Dubickas in [4].

Definition 3.15. Let α be an algebraic number. Let K be the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ and let $G = \mathrm{Gal}(K/\mathbb{Q})$. Suppose $\Sigma = \{\Delta_1, \ldots, \Delta_m\}$ is a system of blocks for the action of G on the set of conjugates of α. We say Σ is *DD-minimal* if the following conditions hold:

- For each $\Delta_i \in \Sigma$, Δ_i contains either only large numbers, or no large numbers.
- Further, the size m of the block system is as small as possible, with respect to the previous condition.

Theorem 3.16. *Let α be an algebraic number. Let K be the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ and let $G = Gal(K/\mathbb{Q})$. Suppose $\Sigma = \{\Delta_1, \ldots, \Delta_m\}$ is a system of blocks for the action of G on the set of conjugates of α. Then Σ is DD-minimal if and only if $\Sigma = \Gamma^*(\alpha)$.*

Proof. We assume Σ is DD-minimal and let $\Delta \in \Sigma$. If $x, y \in \Delta$ then by Lemma 3.5, x and y are A-equivalent. Hence every member of Σ is a subset of a member of $\Gamma^*(\alpha)$. This implies that $|\Gamma^*(\alpha)| \leq \Sigma$ where equality only holds if $\Gamma^*(\alpha) = \Sigma$. Since Σ is DD-minimal, it cannot be larger than $\Gamma^*(\alpha)$ and so the result holds. □

We intend to show that the condensation of an algebraic number α belongs to the Galois closure of $\mathbb{Q}(M(\alpha))$ over $\mathbb{Q}$. This is part of a more general fact about $\Gamma(\alpha)$.

Theorem 3.17. *Let α be an algebraic number, with $\Gamma(\alpha) = \{\alpha_1, \ldots, \alpha_m\}$ and let K be the Galois closure of $\mathbb{Q}(M(\alpha))$ over $\mathbb{Q}$. If f is a symmetric polynomial in m variables with coefficients in $\mathbb{Q}$, then $f(\alpha_1, \ldots, \alpha_m) \in K$.*

Proof. Let J be the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ and let $\sigma \in \mathrm{Gal}(J/K)$. Then $\sigma(f(\alpha_1, \ldots, \alpha_m)) = f(\sigma(\alpha_1), \ldots, \sigma(\alpha_m) = f(\alpha_1, \ldots, \alpha_m)$. The first equality is straight forward since σ is a homomorphism. For the second equality notice that by Theorem 3.12, σ permutes the elements of $\Gamma(\alpha)$. The equality then holds, since f is symmetric. Since $f(\alpha_1, \ldots, \alpha_m)$ is fixed by any element of $\mathrm{Gal}(J/K)$, it must belong to K as required. □

We can now summarise the relationship between an algebraic number α, $C(\alpha)$ and $M(\alpha)$.

Theorem 3.18. *Let α be an algebraic number. Let K be the Galois closure of $\mathbb{Q}(M(\alpha))$ over $\mathbb{Q}$ and suppose Irr$(\alpha) = a_nX^n + \cdots + a_0$. Then*

1. *$C(\alpha) \in K$.*

2. *$C(\alpha) \sim \alpha$.*

3. *$C(C(\alpha)) = C(\alpha)$.*

4. *There exists an integer c such that $cM(C(\alpha)) = M(\alpha)$.*

5. *If $\gcd(a_n, a_0) = 1$, then $M(\alpha) = M(C(\alpha))$.*

Proof. (1) is a special case of Theorem 3.17 using $f(x_1, \ldots, x_m) = x_1 \cdots x_m$ where $m = |\Gamma(\alpha)|$. (2) is a corollary of Lemma 3.4. To prove (3), we look at the conjugates of $C(\alpha)$. These are all of the form $C(\alpha^*)$, where α^* is a conjugate of α. If $C(\alpha^*) \sim C(\alpha)$ then $\alpha^* \sim \alpha$ by (2). This implies $\alpha^* \in \Gamma(\alpha)$ and so $C(\alpha^*) = C(\alpha)$. Hence $C(\alpha)$ is condensed. The proof of (4) and (5) are very similar. Let S be the set of large conjugates of α and let $\Gamma_1, \ldots, \Gamma_m$ be the members of $\Gamma^*(\alpha)$ which consist of large conjugates. Notice that

$S = \Gamma_1 \cup \cdots \cup \Gamma_m$. Let a be the leading coefficient of $\mathrm{Irr}(\alpha)$ and let a_c be the leading coefficient of $\mathrm{Irr}(C(\alpha))$. Then

$$M(\alpha) = a_n \prod_{x \in S} |x| = a \prod_{i=1}^{m} \prod_{y \in \Gamma_i} |y| = \frac{a}{a_c} M(C(\alpha)).$$

Hence (4) will hold if we can show that a_c divides a. This follows from using the second part of Lemma 1.3. Finally to prove (5), observe that $N(\alpha) = a_0/a_n = N(C(\alpha))$. This ensures that $a_n = a_c$ as required. □

Theorem 3.19. *If α_1 and α_2 are algebraic numbers that are Archimedean equivalent, then the following hold: s*

1. $\mathbb{Q}(C(\alpha_1)) = \mathbb{Q}(C(\alpha_2))$.
2. $C(\alpha_1) = \alpha_1 \iff \alpha_1 \in \mathbb{Q}(C(\alpha_2))$.
3. *If $C(\alpha_1) = \alpha_1$ and $C(\alpha_2) = \alpha_2$, then $C(\alpha_1\alpha_2) = \alpha_1\alpha_2$.*

Proof. (1) Let K be the Galois closure of $\mathbb{Q}(\alpha_1, \alpha_2)$ over $\mathbb{Q}$ and let $G = \mathrm{Gal}(K/\mathbb{Q})$. We need to show that

$$\sigma(C(\alpha_1)) = C(\alpha_1) \iff \sigma(C(\alpha_2)) = C(\alpha_2)$$

for all $\sigma \in G$. Let $\sigma \in G$. Then

$$\begin{aligned} \sigma(C(\alpha_1)) = C(\alpha_1) &\iff \sigma(\alpha_1) \sim \alpha_1 \\ &\iff \sigma(\alpha_2) \sim \alpha_2 \qquad \text{by Theorem 3.7} \\ &\iff \sigma(C(\alpha_2)) = C(\alpha_2). \end{aligned}$$

(2) Proving ($\implies$) follows from (1). To prove the converse direction, notice that

$$\sigma(\alpha_1) \sim \alpha_1 \implies \sigma(C(\alpha_2)) \sim C(\alpha_2) \implies \sigma(C(\alpha_2)) = C(\alpha_2)$$

for all $\sigma \in G$. If σ fixes $C(\alpha_2)$ it must fix all elements of $\mathbb{Q}(C(\alpha_2))$. Hence if $\alpha_1 \in \mathbb{Q}(C(\alpha_2))$, then

$$\sigma(\alpha_1) \sim \alpha_1 \implies \sigma(\alpha_1) = \alpha_1$$

for all $\sigma \in G$ as required.

(3) This follows immediately from (2) since $\alpha_1\alpha_2 \sim \alpha_1$, by Lemma 3.4, and $\alpha_1\alpha_2 \in Q(C(\alpha_1))$. □

Theorem 3.20. *Let f be a basal polynomial. Then f is condensed.*

Proof. Any polynomial $f \in \mathbb{Z}[X]$ can be written as

$$f = a\prod_{i=1}^{m} \mathrm{Irr}(\alpha_i),$$

where $a \neq 0$ is an integer, and $\alpha_1, \cdots, \alpha_m$ is a list of algebraic numbers. These numbers need not be distinct. We first show that each factor $\mathrm{Irr}(\alpha_i)$ must be condensed. Assume some $\mathrm{Irr}(\alpha_i)$ is not condensed. Then

$$g = a\prod_{i=1}^{m} M(\alpha_i)M(C(\alpha_i))^{-1}\mathrm{Irr}(C(\alpha_i)),$$

has smaller degree than f. Further

$$M(g) = a\prod_{i=1}^{m} M(\alpha_i)M(C(\alpha_i))^{-1}M(\mathrm{Irr}(C(\alpha_i))) = a\prod_{i=1}^{m} M(\alpha_i) = M(f),$$

since $M(\alpha_i)M(C(\alpha_i))^{-1}$ is a positive integer by Theorem 3.18. This fact also implies that $g \in \mathbb{Z}[X]$. This contradicts f being basal. Hence if f is basal and not condensed we can assume $\alpha_1 \sim \alpha_2$ without loss of generality. Since $\mathrm{Irr}(\alpha_1)$ and $\mathrm{Irr}(\alpha_2)$ are condensed, we know that they and $\mathrm{Irr}(\alpha_1\alpha_2)$ all have the same degree. This means $\mathrm{Irr}(\alpha_1\alpha_2)$ has smaller degree than $\mathrm{Irr}(\alpha_1)\mathrm{Irr}(\alpha_2)$. Let a_1 and a_2 be the leading coefficients of $\mathrm{Irr}(\alpha_1)$ and $\mathrm{Irr}(\alpha_2)$. Let $\sigma_1, \ldots, \sigma_d$ be the embeddings of $\mathbb{Q}(\alpha_1)$. Then

$$\begin{aligned} M(\mathrm{Irr}(\alpha_1)\mathrm{Irr}(\alpha_2)) &= a_1a_2\prod_{i=1}^{d} \max(1, |\sigma_i(\alpha_1)|)\max(1, |\sigma_i(\alpha_2)|) \\ &= a_1a_2\prod_{i=1}^{d} \max(1, |\sigma_i(\alpha_1\alpha_2)|) \\ &= cM(\mathrm{Irr}(\alpha_1\alpha_2)) \end{aligned}$$

for some integer c. This integer exists since the leading coefficient of $\mathrm{Irr}(\alpha_1\alpha_2)$ must divide a_1a_2. This again allows us to find a second polynomial g, with smaller degree than f, but with the same Mahler measure. This contradicts f being basal, so f must be condensed. □

Theorem 3.21. *Let $f = a_nX^n + \ldots + a_0$ be a basal irreducible polynomial. Suppose* $\gcd(a_n, a_0) = 1$. *Then f is condensed.*

Proof. The proof is identical to the first half of the proof of Theorem 3.20. The exception is that we must ensure that g is irreducible. By Theorem 3.18, the condition that $\gcd(a_n, a_0) = 1$ will ensure this. $\square$

The following example is proof that $\mathcal{M}$ is not closed under multiplication. This result was discussed in Section 2.3. It was originally proven by Dixon and Dubickas in [4]. The beginning of the proof is taken from Dixon and Dubickas. Our proof is longer, since we give a description of the unit group of the ring of integers.

Example 3.22. *Let β_1 and β_2 be quadratic unit measures such that $\mathbb{Q}(\beta_1) \neq \mathbb{Q}(\beta_2)$. Then $\beta_1\beta_2 \notin \mathcal{M}$.*

Proof. Let β_1^* and β_2^* be the conjugates of β_1 and β_2 respectively. The other three conjugates of $\beta_1\beta_2$ are $\beta_1\beta_2^*$, $\beta_1^*\beta_2$ and $\beta_1^*\beta_2^*$. Since

$$|\beta_1^*| = \beta_1^{-1} \neq \beta_2^{-1} = |\beta_2^*|$$

we can see that $\beta_1\beta_2$ has exactly two conjugates outside the unit circle. Suppose α is an algebraic unit such that $M(\alpha) = \beta_1\beta_2$. We can assume $\alpha \in \mathbb{Q}(\beta_1\beta_2)$ by Theorem 3.18(5). Obviously if α has 0, 1 or 3 conjugates outside the unit circle, $M(\alpha)$ is either 1 or a Pisot number. Hence α must have two conjugates outside the unit circle. Let K_1, K_2 and K_3 be the following number fields;

$$K_1 = \mathbb{Q}(\beta_1) = \mathbb{Q}(\sqrt{n_1}), K_2 = \mathbb{Q}(\beta_2) = \mathbb{Q}(\sqrt{n_2}), K_3 = \mathbb{Q}(\sqrt{n_1 n_2}).$$

For $i = 1, 2, 3$ let η_i be the unique number such that $\eta_i > 1$ and the unit group of the ring of integers of K_i is equal to $\langle, -1, \eta_1\rangle$. Further let ϵ_i be $\sqrt{\eta_i}$ if $\sqrt{\eta_i} \in \mathbb{Q}(\beta_1\beta_2)$, and η_i otherwise. We claim that the unit group of the ring of integers of $\mathbb{Q}(\beta_1\beta_2)$ is equal to $\langle -1, \epsilon_1, \epsilon_2, \epsilon_3\rangle$. Since $\mathbb{Q}(\beta_1\beta_2)$ is a real quartic number field, we require a system of 3 fundamental units. Further the numbers ϵ_1,ϵ_2 and ϵ_3 are independent, because the number fields K_1, K_2 and K_3 are distinct. If $\langle -1, \epsilon_1, \epsilon_2, \epsilon_3\rangle$ is not the complete unit group, then there must be some unit $x \in \mathbb{Q}(\beta_1\beta_2)$ which does not belong to $\langle -1, \epsilon_1, \epsilon_2, \epsilon_3\rangle$. We can assume that $x^n = \epsilon_i$ for some positive integer n and $i \in \{1, 2, 3\}$. However for $m \geq 3$, $\sqrt[m]{\eta_i}$ has a complex conjugate, and so cannot belong to $\mathbb{Q}(\beta_1\beta_2)$. Hence $\langle -1, \epsilon_1, \epsilon_2, \epsilon_3\rangle$ is the unit group as required.

The four conjugates of α are

$$\zeta_1\epsilon_1^i\epsilon_2^j\epsilon_3^k, \qquad \zeta_2\epsilon_1^i\epsilon_2^{-j}\epsilon_3^{-k}, \qquad \zeta_3\epsilon_1^{-i}\epsilon_2^j\epsilon_3^{-k} \text{ and } \zeta_4\epsilon_1^{-i}\epsilon_2^{-j}\epsilon_3^k$$

for some $i, j, k \in \mathbb{Z}$ and $\zeta_1, \ldots, \zeta_4 \in \{\pm 1\}$. The product of any of these two conjugates is quadratic, which contradicts $M(\alpha)$ having degree 4. Hence $\beta_1\beta_2 \notin \mathcal{M}$. □

Theorem 3.23. *Suppose $f \in \mathbb{Z}[X]$ has Mahler measure of degree d.*

- *If f is condensed, then the degree of f is less than or equal to 2^d.*
- *If f is condensed and irreducible, then the degree of f is less than or equal to $\binom{d}{\lfloor d/2 \rfloor}$.*
- *If f is basal, then the degree of f is less than or equal to $\sum_{1 \leq r \leq d/2} \binom{d}{r}$.*

Proof. Let K be a splitting field for f, and $G = \mathrm{Gal}(K/\mathbb{Q})$. For each root ϵ of f, let

$$\Gamma_\epsilon = \{\sigma(M(f)) \mid \sigma \in G \text{ and } |\sigma(\epsilon)| > 1\}.$$

For two roots x, y of f, we can see that $\Gamma_x = \Gamma_y \iff x \sim y$. Hence if f is condensed, the set of roots of f is smaller than the set of subsets of roots of $\mathrm{Irr}(M(f))$. Hence the degree of f is less than or equal to 2^d.

If f is irreducible, each set Γ_ϵ must have the same size. This gives the second result.

If f is basal, we choose another basal polynomial, g with the same Mahler measure. If $f = a\prod_{i=1}^m f_i$, let $g = a\prod_{i=1}^m g_i$, where $g_i = f_i$ if f_i has at most half of its roots lying outside the unit circle, and f_i^* otherwise. Then for each root ϵ of g, $|\Gamma_\epsilon| < \frac{d}{2}$. Further no Γ_ϵ is empty, since we could replace the factor $\mathrm{Irr}(\epsilon)$ by the integer $M(\epsilon)$ to reduce the degree of g, without changing the Mahler measure. □

We now give two important results from [4], showing how to prove them using the ideas we have introduced. In Section 2.1, we considered the inverse problem for Mahler measure as two related problems. The first problem was to determine for a given algebraic number β, if there exists an integer polynomial with Mahler measure β. We now explain how to construct such a polynomial if possible, or show that such polynomials do not exist. Giving an upper bound for the degree of basal polynomials is the key step. We recall from Lemma 2.5, that if f is an integer polynomial with Mahler measure β, then

$$L(f) \leq 2^n M(f).$$

This gives an upper bound for the length and degree of a basal polynomial of degree β. It is clearly straightforward to construct a list of all integer polynomials which satisfy this bound on their length and degree. We then search this list for polynomials of degree β. This will determine if a basal polynomial exists with Mahler measure β and give a specific example if it does. If no basal polynomial of Mahler measure β exists, then no polynomial of Mahler measure β can exist.

Theorem 3.24. *Let $\beta \in \mathcal{M}^*$ and let d be the degree of β. Let K be the Galois closure of $\mathbb{Q}(\beta)$ over $\mathbb{Q}$. Then there exists a polynomial $f \in \mathbb{Z}[X]$ such that $M(f) = \beta$ and every root of f belongs to K. Further, the degree of f is at most $\sum_{1 \leq r \leq d/2} \binom{d}{r}$.*

Proof. Since $\beta \in \mathcal{M}^*$, let f be a basal polynomial with Mahler measure β and let J be the splitting field of f. Suppose $\sigma \in \mathrm{Gal}(J/\mathbb{Q})$. Then by Theorem 3.12, we have

$$\sigma \in \mathrm{Gal}(J/K) \iff \sigma(x) \sim x \text{ for all roots } x \text{ of } f.$$

By Theorem 3.20, f is a condensed polynomial. Therefore

$$\sigma \in \mathrm{Gal}(J/K) \iff \sigma(x) = x \text{ for all roots } x \text{ of } f.$$

Since J is the splitting field of f,

$$\sigma \in \mathrm{Gal}(J/K) \iff \sigma(x) = x \text{ for all } x \in J.$$

Hence $J = K$ as required, whilst Theorem 3.23 gives the bound on the size of f to complete the result. □

Dixon and Dubickas also proved a parallel result for algebraic units. We can use the process outlined prior to Theorem 3.24, to determine whether or not a given algebraic unit belongs to $\mathcal{M}$. We would again test the integer polynomials whose degree and length are below given bounds. The search however is conducted only amongst irreducible polynomials whose first and last coefficients are ±1. We can also use a lower bound on the degree of the polynomials to be tested.

Theorem 3.25. *Let $\beta \in \mathcal{M}$ be an algebraic unit of degree d. Let K be the Galois closure of $\mathbb{Q}(\beta)$ over $\mathbb{Q}$. Then there exists an algebraic unit α in K such that $M(\alpha) = \beta$. Further, the degree of α is at most $\binom{d}{\lfloor d/2 \rfloor}$.*

Proof. The proof is nearly identical to that of Theorem 3.24. The main change is that we choose a basal irreducible polynomial f with measure β instead of a basal one. We now must use Theorem 3.21 to show that f is condensed. The last change needed is to use the second part of Theorem 3.23 to give the improved bound on the degree of f. □

We now show that these ideas can be adapted to determining whether or not a given algebraic unit belongs to $\mathcal{R}$. Again the key step is finding an upper bound on the degree of reciprocal polynomials to be tested. We begin with the following straightforward result.

Theorem 3.26. *Let α be a reciprocal algebraic unit with no conjugates on the unit circle. Then $C(\alpha)$ is also reciprocal.*

Proof. Since α is not a root of unity, by Lemma 3.4, $\Gamma(\alpha) \neq \Gamma(\alpha^{-1})$. Then for each $\gamma \in \Gamma(\alpha)$, Lemma 3.4 shows that $\gamma^{-1} \in \Gamma(\alpha^{-1})$. It then follows that $C(\alpha^{-1}) = C(\alpha)^{-1}$. □

The fact that $C(\alpha)$ is reciprocal does not imply that α is reciprocal. The non-reciprocal numbers used in Lemma 2.38 are proof of this. The restriction that α has no conjugates on the unit circle is also important. For example if α is a number with $\mathrm{Irr}(\alpha) = X^6 + X^5 + 2X^4 + 3X^3 + 2X^2 + X + 1$, then $\mathrm{Irr}(C(\alpha)) = X^3 - X^2 - X - 1$. We can however adapt Theorem 3.26 to solve the general problem of determining when an algebraic unit belongs to $\mathcal{R}$. This result was proven for cubic unit measures in [4]. This provided the final step in the proof of Theorem 2.9.

Theorem 3.27. *Let β be a measure that is the measure of a reciprocal unit. Let K be the Galois closure of $\mathbb{Q}(\beta)$ over $\mathbb{Q}$. Then there exists a reciprocal unit $\alpha^* \in K$ such that $M(\alpha^*) = \beta$. Further, the degree of α^* is at most $\binom{d}{\lfloor d/2 \rfloor}\left[\binom{d}{\lfloor d/2 \rfloor} - 1\right]$.*

Proof. Let α be a reciprocal unit with $M(\alpha) = \beta$. Let $\Gamma^*(\alpha) = \{\Gamma_1, \ldots, \Gamma_n\}$. Let $\Gamma_i^{-1} = \{\epsilon^{-1} | \epsilon \in \Gamma_i\}$. Let $\Delta_{ij} = \Gamma_i \cap \Gamma_j^{-1}$. These sets can alternatively be generated by a new equivalence relation. If α_1 and α_2 are conjugates of α then they belong to the same Δ_{ij} if and only if $\alpha_i \sim \alpha_j$ and $\alpha_i^{-1} \sim \alpha_j^{-1}$. The rest of the proof can be understood as the condensation with respect to this new equivalence relation. Lemma 3.4 show us that unless a number has a conjugate on the unit circle, this will agree with the usual condensation.

We now prove a few results about the sets Δ_{ij}. Let J be the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ and let $G = \mathrm{Gal}(J/\mathbb{Q})$. Since the sets Γ_i and Γ_j^{-1} are blocks for the action of G, so are the intersections Δ_{ij} where non-empty. The action of G on the sets Δ_{ij} is easy to describe. Suppose $\sigma \in G$, and $\sigma(\Gamma_k) = \Gamma_l$. Then $\sigma(\Gamma_k^{-1}) = \Gamma_l^{-1}$. Suppose $\sigma \in \mathrm{Gal}(J/K)$. Then by

Theorem 3.12, $\sigma(\Gamma_i) = \Gamma_i$ for all i. Hence $\sigma(\Delta_{ij}) = \Delta_{ij}$ for all i and j. Choose a non-empty Δ_{ij}, and let α^* be the product of elements in Δ_{ij}. It is clear that the conjugates of α^* are the products of elements in any non-empty Δ_{ij}. Further if $\delta \in \Delta_{ij}$ then $\delta^{-1} \in \Delta_{ji}$, and so the reciprocal of α^* is the product of elements in Δ_{ji}.

The upper bound for the degree of α^* is found by enumerating the non-empty sets Δ_{ij}. As seen in Theorem 3.23, $\Gamma^*(\alpha)$ has cardinality at most $\binom{d}{\lfloor d/2 \rfloor}$. The bound then follows from the fact that $\Gamma_i \cap \Gamma_i^{-1} = \varnothing$. □

We finish by comparing $\mathcal{R}$ and $\mathcal{N}$, which reveals an interesting dichotomy. We can use Lemma 2.38 to show that the analogous version of Theorem 3.27 for $\mathcal{N}$ does not hold. If $\alpha > 1$ is a quadratic unit, Lemma 2.38 shows that $\alpha^2 \in \mathcal{R} \cup \mathcal{N}$. However the only elements in $\mathbb{Q}(\alpha)$ with Mahler measure α^2 are $\pm\alpha^2$ and $\pm\alpha^{-2}$. These are all reciprocal, and $\mathbb{Q}(\alpha)$ is normal over $\mathbb{Q}$.

We finish with a couple of results about the multiplicative structure of $\mathcal{M}$. If restricted to algebraic integers, Theorem 2.32 can be generalised as follows. The original result is recovered by assuming $\alpha_1 = \alpha_2 = \ldots = \alpha_m$. This shows that $\mathcal{M}$ still has some multiplicative structure, despite Theorem 3.22.

Theorem 3.28. *Let $\alpha_1, \ldots, \alpha_m$ be a list of algebraic integers, not necessarily distinct, which are archimedean equivalent. Then $\prod_{i=1}^{m} M(\alpha_i) \in \mathcal{M}$.*

Proof. Let $K = \mathbb{Q}(C(\alpha_1))$. Notice that K contains $C(\alpha_2), \ldots, C(\alpha_m)$ and the product $C(\alpha_1) \cdots C(\alpha_m)$ by Lemma 3.19. Let $\theta_1, \ldots, \theta_n$ be the embeddings of K which map $C(\alpha_1)$ outside the unit circle. By A-equivalence these are the embeddings that map any of $C(\alpha_2), \ldots, C(\alpha_m)$ and $C(\alpha_1) \cdots C(\alpha_m)$ outside the unit circle. Hence

$$M\left(\prod_{i=1}^{m} C(\alpha_i)\right) = \prod_{j=1}^{n} \left|\theta_j\left(\prod_{i=1}^{m} C(\alpha_i)\right)\right| = \prod_{i=1}^{m}\prod_{j=1}^{n} |\theta_j(C(\alpha_i))| = \prod_{i=1}^{m} M(\alpha_i)$$

as required. □

Whilst $\mathcal{M}$ is not a monoid under multiplication, we can still give a weak form of multiplicative structure to the units in $\mathcal{M}$.

Theorem 3.29. *Let K be a normal algebraic number field of degree d. Let $S \subset K \cap \mathcal{M}$ be a set of units with cardinality at least 2^{d-1}. Then there exist $x, y \in S$ such that $xy \in \mathcal{M}$.*

Proof. We can assume $1 \notin S$ since this case is trivial. Let $\beta_1, \dots, \beta_m$ be the elements of S, and let $\alpha_1, \dots, \alpha_m$ be units in K such that $M(\alpha_i) = \beta_i$. These can be chosen so that each α_i is outside the unit circle and must always exist by Lemma 2.6. By the pigeonhole principle we can choose two which are A-equivalent, and apply Theorem 3.28 to obtain the result. □

3.3 Calculating Maximal Mahler Sets

It was shown during the proof of Theorem 2.11 that we can calculate maximal Mahler sets in an inefficient manner. In this section we develop alternative methods for calculating these sets. The simplest situation is when a maximal Mahler set $S \subset \overline{\mathbb{Q}}$ is known to contain only condensed numbers. For example, if β is a unit measure we can use the maximal Mahler set $S \subset \overline{\mathbb{Q}}$ with measure β and smallest possible degree by Theorem 3.20. This special case is convenient because by Theorem 3.18, we know that $S \subset K$, where K is the Galois closure of $\mathbb{Q}(\beta)$ over $\mathbb{Q}$. Having reduced the inverse problem to searching within a single, known number field, we can use Dirichlet's Unit Theorem. Being able to operate inside a finitely generated group, with a unique description for each unit makes it straightforward to calculate S. The first step is to divide the unit group into equivalence classes generated by archimedean equivalence, as demonstrated in Example 3.6. We then study each equivalence class in turn. The examples in this section work with units of degree 4, which requires the following fact to be checked.

Lemma 3.30. *Suppose $f \in \mathbb{Z}[X]$ is irreducible, has degree 4 and the measure of f is a unit of degree at least 4. Then f is basal irreducible.*

Proof. All polynomials of degree at most three, have Mahler measure whose degree is at most three. Hence no such polynomial can have the same degree as f. □

The following example demonstrates a general principle for calculating maximal Mahler sets that contain only condensed numbers.

Example 3.31. *Let β be a unit and a measure such that the Galois closure of $\mathbb{Q}(\beta)$ over $\mathbb{Q}$ is equal to $\mathbb{Q}(i, \sqrt[4]{2})$. Then the maximal Mahler set $S \subset \overline{\mathbb{Q}}$ of degree 4 and measure β has cardinality 16.*

Proof. There are 5 quartic subfields of $\mathbb{Q}(i, \sqrt[4]{2})$. These are

$$K_1 = \mathbb{Q}(\sqrt[4]{2}), K_2 = \mathbb{Q}(i\sqrt[4]{2}), K_3 = \mathbb{Q}((1+i)\sqrt[4]{2}),$$
$$K_4 = \mathbb{Q}((1-i)\sqrt[4]{2}) \text{ and } K_5 = \mathbb{Q}(\sqrt{2}, i).$$

To calculate $|S|$, it is sufficient to study only K_1 and K_3. This is because K_1 and K_2 are conjugate fields, so $|S \cap K_1| = |S \cap K_2|$. Further since K_1, K_2 and S all have degree 4, $K_1 \cap K_2 \cap S = \varnothing$. The same argument applies to the conjugate fields K_3 and K_4. The last field K_5 is itself normal over $\mathbb{Q}$, so the Mahler measure of any number in K_5 will belong to K_5, implying $K_5 \cap S = \varnothing$. Hence $|S| = 2(|S \cap K_1| + |S \cap K_3|)$. Notice that β must belong to K_1, since it is the only real quartic subfield of $\mathbb{Q}(i, \sqrt[4]{2})$.

We begin with $K_1 = \mathbb{Q}(\sqrt[4]{2})$, which was studied in Example 3.6. We saw that Archimedean equivalence divides the unit group of K_1 into 7 classes. There are 4 classes which consist of numbers with quartic Mahler measure. These are also the 4 classes which have exactly 1 or 3 large conjugates. Keeping the notation of Example 3.6, let σ_3 be the embedding of K_1 which sends $\sqrt[4]{2}$ to $-\sqrt[4]{2}$. For $\alpha \in S \cap K_1$, let S_α be the set

$$S_\alpha = \{\pm\alpha, \pm\alpha^{-1}, \pm\sigma_3(\alpha), \pm\sigma_3(\alpha)^{-1}\}.$$

Notice that S_α is a Mahler set, contained in K_1, and that exactly one element of S_α is a Pisot or Salem number. Hence if $S \cap K_1 \neq \emptyset$, then $S \cap K_1 = S_\beta$, and β must be a Pisot or Salem number. If β is a Pisot number, we can check that the 8 numbers described above are distinct, and so $|S_\beta| = 8$. If β is a Salem number then β must be a positive power of $(1 + \sqrt[4]{2})^2(1 + \sqrt{2})$. Then $\beta^{-1} = \sigma(\beta)$, but $\pm\beta$ and $\pm\beta^{-1}$ are all distinct numbers, and so $|S_\beta| = 4$.

We now turn to $K_3 = \mathbb{Q}((1 + i)\sqrt[4]{2})$. The unit group of K_3 is equal to $\langle -1, \epsilon \rangle$ where $\epsilon = (1 + \sqrt[4]{2}) + (\sqrt{2} + \sqrt[4]{2})i$. If n is a non-zero integer, then $\pm\epsilon^n$ has degree 4 and Mahler measure $(1 + \sqrt[4]{2})^{2|n|}(1 + \sqrt{2})^{|n|}$. Hence if $S \cap K_3 \neq \emptyset$ then $|S \cap K_3| = |S \cap K_1| = 4$, completing the result. □

We now present a novel framework for approaching the calculation of maximal Mahler sets of integer polynomials. There are two main ideas involved. The first is to repeatedly break the sets down into useful disjoint subsets, whilst the second idea is to group the non-zero roots of a polynomial by Archimedean equivalence. We begin with defining when an integer polynomial is in Archimedean standard form.

Definition 3.32. Let $f \in \mathbb{Z}[X]$. We say f is in Archimedean standard form when the following conditions hold;

- $f = aX^n \prod_{i=1}^{m} f_i$ where $a, n \in \mathbb{Z}$, $n \geq 0$ and the non-zero roots of f fall into exactly m A-equivalence classes.
- Each factor f_i is monic, has positive degree, and all of its roots are non-zero and A-equivalent.

We define $\tau(f)$ to be the set of constant coefficients of the factors f_i. For any $\beta \in \mathcal{M}^*$, define $T(\beta)$ to be

$$T(\beta) = \{\tau(f) | f \in \mathbb{Z}[X] \text{ and } M(f) = \beta\}.$$

Lemma 3.33. *Let f and g be integer polynomials and let $\beta \in \mathcal{M}^*$. The following hold:*

1. *If f and g have the same leading coefficient and if $\tau(g) = \tau(f)$ then $M(f) = M(g)$.*
2. *The set $\tau(f)$ contains only condensed numbers.*

3. The set $T(\beta)$ is finite.

Proof. (1.) We can calculate $M(f)$ from just the leading coefficient a of f and $\tau(f)$. Large algebraic numbers can only be A-equivalent to large algebraic numbers, by the definition of A-equivalence. Hence the large elements of $\tau(f)$ are the product of only large roots of f. Similarly the non-large elements of $\tau(f)$ are the product of only non-large roots of f. Hence $M(f)$ is equal to a multiplied by the product of the large elements of $\tau(f)$. This gives the result, as we obviously get the same Mahler measure working with g.

(2.) Let f_i be a factor that appears in the Archimedean standard form of f. The set of roots of f_i is equal to $\Gamma(\alpha_1) \cup \cdots \cup \Gamma(\alpha_n)$ for some algebraic numbers $\alpha_1, \ldots, \alpha_n$ which are all A-equivalent. Then the constant coefficient of f_i is equal to $C(\alpha_1) \cdots C(\alpha_n)$. Then by Theorem 3.19(3), this is a condensed number.

(3.) For any $t \in T(\beta)$, let

$$f_t = a_t \prod_{\alpha \in t} (X - \alpha)$$

where a_t is the positive integer such that $M(f_t) = \beta$. This integer exists by the definition of $T(\beta)$. Let $F(\beta)$ be the set of all such f_t. Clearly $f_s = f_t \iff s = t$ and so $|F(\beta)| = |T(\beta)|$. For a positive integer i, let F_i be the polynomials in $F(\beta)$ of degree i. Notice that these are Mahler sets and so are finite. We notice that $\tau(f_t) = t$ and so that f_t is condensed. Then by Theorem 3.23 $\deg(f_t) \leq 2^d$ where $d = \deg(\beta)$ and so if $i > 2^d$

then $F_i(\beta) = \varnothing$. Hence

$$|T(\beta)| = |F(\beta)| = |F_1(\beta)| + \cdots + |F_{2^d}(\beta)| < \infty.$$

□

Definition 3.34. Let $\beta \in \mathcal{M}^*$ and let d be a positive integer. Let $S_0(\beta, d)$ be the maximal Mahler set of integer polynomials of degree d and measure β. For any $\tau^* \in T(\beta)$, let $S_1(\tau^*, \beta, d)$ be the set

$$S_1(\tau^*, \beta, d) = \{f \in S_0(\beta, d) | \tau(f) = \tau^*\}.$$

Lemma 3.35. *Let $\beta \in \mathcal{M}^*$ and let d be a positive integer. Then*

$$S_0(\beta, d) = \bigcup_{\tau^* \in T(\beta)} S_1(\tau^*, \beta, d),$$

and

$$|S_0(\beta, d)| = \sum_{\tau^* \in T(\beta)} |S_1(\tau^*, \beta, d)|.$$

Proof. The first claim comes directly from the definition of $S_0(\beta, d)$ and $S_1(\tau^*, \beta, d)$. The second claim requires that our decomposition of $S_0(\beta, d)$ consists of pairwise disjoint sets. This is also true, since τ is a single-valued function. □

Definition 3.36. For an algebraic number α, we define $E(\alpha)$ to be the set of conjugates of α. Let f be an integer polynomial. We say a vector $(\alpha_1, \ldots, \alpha_n)$ of algebraic numbers is a *basis for* $\tau(f)$ if the following conditions hold:

- $\tau(f) = E(\alpha_1) \cup \cdots \cup E(\alpha_n)$

- For any integers $1 \leq i < j \leq n$, no conjugate of α_i is Archimedean equivalent to any conjugate of α_j.

Definition 3.37. Let $\beta \in \mathcal{M}^*$, and let $\tau^* \in T(\beta)$. Let d be a positive integer and let $(\alpha_1, \ldots, \alpha_n)$ be a basis for τ^*. Then $S_2((\alpha_1, \ldots, \alpha_n), (i_1, \ldots, i_n), \beta, d)$ is defined to be the set

$$\{f \in S_1(\tau^*, \beta, d) | f \text{ has } i_j \text{ non-zero roots A-equivalent to } \alpha_j\}.$$

For an algebraic number α, define $S_2(\alpha, i)$ to be $S_2(\{\alpha\}, (i), M(\alpha), \deg(\alpha)i)$.

Lemma 3.38. *Let $\beta \in \mathcal{M}^*$ and let $\tau^* \in T(\beta)$. Let d be a positive integer, and let $(\alpha_1, \ldots, \alpha_m)$ be a basis for τ^*. Then*

$$S_1(\tau^*, \beta, d) = \bigcup_{\substack{d_1,\ldots,d_m \geq 1, \qquad d_1,\ldots,d_m \in \mathbb{Z} \\ \deg(\alpha_1)d_1 + \cdots + \deg(\alpha_m)d_m \leq d}} S_2((\alpha_1, \ldots, \alpha_m), (d_1, \ldots, d_m), \beta, d)$$

and

$$|S_1(\tau^*, \beta, d)| = \sum_{\substack{d_1,\ldots,d_m \geq 1, \qquad d_1,\ldots,d_m \in \mathbb{Z} \\ \deg(\alpha_1)d_1 + \cdots + \deg(\alpha_m)d_m \leq d}} |S_2((\alpha_1, \ldots, \alpha_m), (d_1, \ldots, d_m), \beta, d)|\,.$$

Proof. From the appropriate definitions, it is clear that

$$S_1(\tau^*, \beta, d) = \bigcup_{\substack{d_1,\ldots,d_m \geq 1, \\ d_1,\ldots,d_m \in \mathbb{Z}}} S_2((\alpha_1, \ldots, \alpha_m), (d_1, \ldots, d_m), \beta, d).$$

This infinite union can be replaced by the finite union given in the theorem.

Suppose $f \in S_2((\alpha_1, \ldots, \alpha_m), (d_1, \ldots, d_m), \beta, d)$. The number of non-zero roots of f, counted with multiplicity, is $\deg(\alpha_1)d_1 + \cdots + \deg(\alpha_m)d_m$. This must be less than the degree of f. Hence if $\deg(\alpha_1)d_1 + \cdots + \deg(\alpha_m)d_m > d$, then $S_2((\alpha_1, \ldots, \alpha_m), (d_1, \ldots, d_m), \beta, d)$ is empty. The second claim requires that our decomposition of $S_1(\tau^*, \beta, d)$ consists of pairwise disjoint sets. This again follows from the appropriate definitions. □

Lemma 3.39. *Let $\beta \in \mathcal{M}^*$ be a unit and let $\tau^* \in T(\beta)$. Let d be a positive integer, and let $(\alpha_1, \ldots, \alpha_m)$ be a basis for τ^*. Then*

$$S_2((\alpha_1, \ldots, \alpha_m), (i_1, \ldots, i_m), \beta, d) = \{X^q f_1 \cdots f_m | f_j \in S_2(\alpha_j, i_j)\}$$

where $q = d - \deg(\alpha_1)i_1 - \cdots - \deg(\alpha_m)i_m$. Furthermore:

$$|S_2((\alpha_1, \ldots, \alpha_m), (i_1, \ldots, i_m), d)| = 2^{1-m} \prod_{j=1}^{m} |S_2(\alpha_j, i_j)|.$$

Proof. It follows from the appropriate definitions that

$$\{X^q f_1 \cdots f_m | f_j \in S_2(\alpha_j, i_j)\} \subset S_2((\alpha_1, \ldots, \alpha_m), (i_1, \ldots, i_m), \beta, d).$$

Suppose $f \in S_2((\alpha_1, \ldots, \alpha_m), (i_1, \ldots, i_m), \beta, d)$ and let the Archimedean standard form of f be

$$f = aX^t \prod_{k=1}^{n} g_k$$

where $a \neq 0$, $t \geq 0$ and $n \geq 1$ are integers. Looking at the degree of f shows that $t = q$;

$$\deg(f) = t + \sum_{k=1}^{n} \deg(g_k) = t + \sum_{j=1}^{m} \deg(\alpha_j) i_j = q + \sum_{j=1}^{m} \deg(\alpha_j) i_j.$$

We also know that $a = \pm 1$ because $M(f) = \beta$ is a unit. For $i \in \{1, \ldots, m\}$ let f_i be the product of the polynomials g_k which have a constant term which is a conjugate of α_i. Then f_j and $-f_j$ belong to $S_2(\alpha_j, i_j)$. Hence

$$f = X^q (af_1) f_2 \cdots f_m \in \{X^q f_1 \cdots f_m | f_j \in S_2(\alpha_j, i_j)\}.$$

This completes the proof of the first claim. For the second claim, we must take into account the number of ways a polynomial can be factorised in this way. Up to ordering, the roots of each factor are determined by f. The leading coefficient of each factor f_j can be chosen to be ± 1. The only restriction is that the product of all such leading coefficients is equal to the leading coefficient of f. There are 2^{m-1} ways of doing this, giving the result. □

We aim to give a formula for the size of maximal Mahler sets with unit measure. The following definition allows us to describe the possible coefficients for a factor of a polynomial in standard form with unit measure.

Definition 3.40. Let α be a condensed unit and let K be the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Let $c = (c_1, \ldots, c_m)$ be a vector of algebraic integers in $\mathbb{Q}(\alpha)$. We say c matches α if for every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ the roots of $X^{m+1} + \sum_{i=1}^{m} \sigma(c_i) X^i + \sigma(\alpha)$ are all A-equivalent to $\sigma(\alpha)$. We also say that the vector of length zero matches with any condensed unit. Let $N(\alpha, m)$ be the number of distinct vectors of length $m-1$ which match α where m is a positive integer.

Lemma 3.41. *Let α be a condensed unit and let i be a positive integer. Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of $\mathbb{Q}(\alpha)$. Then for any $f \in \mathbb{Z}[X]$, the following are equivalent:*

1. *$f \in S_2(\alpha, i)$,*
2. *The Archimedean standard form of f is equal to*

$$f = a \prod_{j=1}^{n} \left(X^i + \left(\sum_{k=1}^{i-1} \sigma_j(c_k) X^k \right) + \sigma_j(\alpha) \right),$$

where $a = \pm 1$, and $(c_1, \ldots, c_{i-1}) \in \mathcal{O}_{\mathcal{Q}(\alpha)}^{i-1}$ matches α.

Furthermore $|S_2(\alpha, i)|$ is equal to

$$2 \left| \left\{ (c_1, \ldots, c_{i-1}) \in \mathcal{O}_{\mathcal{Q}(\alpha)}^{i-1} | (c_1, \ldots, c_{i-1}) \text{ matches } \alpha \right\} \right|.$$

Proof. (1) $\implies$ (2) By definition of $S_2(\alpha, i)$, we know that $M(f) = M(\alpha)$, $\deg(f) = in$ and $\tau(f) = \{\sigma_1(\alpha), \ldots, \sigma_n(\alpha)\}$. Let the Archimedean standard form of f be

$$f = aX^m \prod_{j=1}^{d} f_j$$

for some integers $a \neq 0$, $m > 0$ and $d > 0$. We first observe that $d = n$ since $d = |\tau(f)|$. We can therefore assume that the constant coefficient of f_j

is $\sigma_j(\alpha)$. Looking at the Mahler measure of f, we can see that $a = \pm 1$ since

$$\begin{aligned} M(f) = M(aX^m)\prod_{j=1}^{n} M(f_j) &= |a|\prod_{j=1}^{n} \max\left(\sigma_j(\alpha), 1\right) \\ &= |a|M(\alpha) = |a|M(f). \end{aligned}$$

Each f_i will have degree i, so $\deg(f) = m + ni$ and hence $m = 0$. We define the vector $(c_1, \ldots, c_{i-1}) \in \mathbb{C}^{i-1}$ to such that

$$f_1 = X^i + \sum_{k=1}^{i-1} c_k X^k + \alpha.$$

Since each root of f_1 is an algebraic integer, the coefficients $c_1, \ldots, c_{i-1}$ are also algebraic integers. Let K be the splitting field of f. We need to show that $(c_1, \ldots, c_{i-1}) \in \mathbb{Q}(\alpha)$. We will do this by showing that for any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ and any $c \in \{c_1, \ldots, c_{i-1}\}$, $\sigma(\alpha) = \alpha \implies \sigma(c) = c$. We recall that the roots of f_1 are A-equivalent to α, and are the only roots of f A-equivalent to α. Then by Theorem 3.7, $\sigma(\alpha) = \alpha$ implies that σ permutes the roots of f_1. Considering c as a symmetric function in the roots of f_1, this implies that $\sigma(c) = c$ as required. Finally we must check that $(c_1, \ldots, c_{i-1})$ matches α. By definition, this would imply that for $1 \leq j \leq n$, the roots of f_j are all A-equivalent to $\sigma_j(\alpha)$. Since f is in standard form, the roots of each f_j are A-equivalent to each other. Then by Lemma 3.4(1), $\sigma_j(\alpha)$ which is the constant term of f_j, is A-equivalent to the roots of f_j as required.

(2) $\implies$ (1) It is straightforward to check that $f \in S_2(\alpha, i)$.

The final claim is also straightforward, since every integer polynomial has exactly one standard form, up to the order of the factors. □

We are now ready to give an example of our explicit description of maximal Mahler sets. We first require the following lemma.

Lemma 3.42. *Let a and b be real numbers. Then the following hold:*

$$\begin{aligned} X^2+aX+b=0 \textit{ has two large roots } &\iff b<-|a|-1 \\ &\qquad \textit{or } b>\mathit{max}(1,|a|-1), \\ X^2+aX+b=0 \textit{ has no large roots } &\iff 1\geq b\geq |a|-1. \end{aligned}$$

Proof. Let $f=X^2+aX+b$. Notice that f has complex roots if and only if $a^2<4b$, and these roots both have modulus $\sqrt{b}$. We first show that the theorem holds when f has complex roots. In order to do this, we simplify the theorem using the fact that $a^2/4\geq |a|-1$ holds for all real a, and so $b>|a|-1$ holds if f has complex roots. A second simplification uses the fact that if $4b>a^2$ then $b>0>-|a|-1$. The theorem then reduces to f has 2 large roots if $b>1$ and no large roots otherwise. This is clear since the roots have modulus $\sqrt{b}$.

We can now assume $a^2\geq 4b$ and let θ_1,θ_2 be the roots of f, where

$$\theta_1=\frac{-a+\sqrt{a^2-4b}}{2} \text{ and } \theta_2=\frac{-a-\sqrt{a^2-4b}}{2}.$$

We look at the cases $\theta_1 > 1$, $\theta_1 < -1$, $\theta_2 > 1$ and $\theta_2 < -1$ independently.

$$\begin{aligned}
\theta_1 > 1 &\iff \sqrt{a^2-4b} > a+2 \iff \big(a < -2 \text{ or } a^2-4b > a^2+4a+4\big) \\
&\iff (a < -2 \text{ or } b < -a-1) \\
\theta_1 < -1 &\iff \sqrt{a^2-4b} < a-2 \iff \big(a > 2 \text{ and } a^2-4b < a^2-4a+4\big) \\
&\iff (a > 2 \text{ and } b > a-1) \\
\theta_2 > 1 &\iff \sqrt{a^2-4b} < -(a+2) \\
&\iff \big(a < -2 \text{ and } a^2-4b < a^2+4a+4\big) \\
&\iff (a < -2 \text{ and } b > -a-1) \\
\theta_2 < -1 &\iff \sqrt{a^2-4b} > 2-a \iff \big(a > 2 \text{ or } a^2-4b > a^2-4a+4\big) \\
&\iff (a > 2 \text{ or } b < a-1)
\end{aligned}$$

We first prove the result about f having large roots, if b is negative. Notice that $a^2 > 0 > 4b$, and so f must have real roots. Since $\theta_1 < -1$ and $\theta_2 > 1$ cannot happen simultaneously, f has two large roots if and only if $\theta_1 > 1$ and $\theta_2 < -1$.

$$\begin{aligned}
\theta_1 > 1 \text{ and } \theta_2 < -1 &\iff (a < -2 \text{ or } b < -a-1) \text{ and } (a > 2 \text{ or } b < a-1) \\
&\iff (b < -a-1 \text{ and } b < a-1) \iff b < |a|-1
\end{aligned}$$

This proves the result for f having two large roots when b is negative. We now look at when f has two large roots for $b \geq 0$.

$$\begin{aligned}(\theta_1, \theta_2 > 1) \text{ or } (\theta_1, \theta_2 < -1) &\iff (a < -2 \text{ and } b < -a - 1)\\ &\qquad \text{or } (a > 2 \text{ and } b > a - 1)\\ &\iff (|a| > 2 \text{ and } b > |a| - 1)\\ &\iff (b > 1 \text{ and } b > |a| - 1)\\ &\iff b > \max(1, |a| - 1)\end{aligned}$$

The non-obvious implication here is that if f has real roots and $b > 1$ then $|a| > 2$. This follows from using $a^2 \geq 4b$. This completes the proof of the first half of the theorem. The proof for f having no large roots, when the roots are real, is very similar.

$$\begin{aligned}|\theta_1|, |\theta_2| < 1 &\iff (|a| \leq 2 \text{ and } b \geq a - 1 \text{ and } b \geq -a - 1)\\ &\iff (|a| \leq 2 \text{ and } b \geq |a| - 1) \iff 1 \geq b \geq |a| - 1\end{aligned}$$

Again the non-obvious step is that if f has real roots and $|a| \leq 2$ then $b \leq 1$. This follows since $|a| \leq 2 \implies a^2 \leq 4 \implies b \leq 1$ using $a^2 \geq 4b$. This completes the proof of the second half of the theorem. □

Theorem 3.43. *Let $S \subset \mathbb{Z}[X]$ be a maximal Mahler set with degree 4. Suppose the measure β of S is a quadratic unit and suppose that $\mathrm{Gal}(\mathbb{Q}(\beta)/\mathbb{Q})$ is generated by σ. Then*

$$|S| = 2\,|N(\beta)| + 2\,|N(-\beta)| + 36$$

where

$$N(\beta) = \left\{x \in \mathcal{O}_K \,\middle|\, |x| < \beta \text{ and } |\sigma(x)| \leq 1 + \sigma(\beta)\right\}$$

and

$$N(-\beta) = \left\{x \in \mathcal{O}_K \,\middle|\, |x| < \beta \text{ and } |\sigma(x)| \leq 1 - \sigma(\beta)\right\}.$$

Proof. Let $\beta_1 = \beta$ and let β_2 be its conjugate. Let $K = \mathbb{Q}(\beta)$ and let

$$T_1 = \{\beta_1, \beta_2\}, \quad T_2 = \{-\beta_1, -\beta_2\}, \quad T_3 = \{1, \beta_1, \beta_2\}$$
$$T_4 = \{1, -\beta_1, -\beta_2\}, \quad T_5 = \{-1, \beta_1, \beta_2\} \text{ and } T_6 = \{-1, -\beta_1, -\beta_2\}.$$

We first claim that $T(\beta_1) = \{T_1, \ldots, T_6\}$. We can now use Lemma 3.35 to give

$$|S| = \sum_{i=1}^{6} |S_1(T_i, \beta_1, 4)|.$$

The next step is to use Lemma 3.38 on each term on the right hand side. We start with $S_1(T_1, \beta_1, 4)$ to give

$$|S_1(T_1, \beta_1, 4)| = |S_2(\beta_1, 2)| + |S_2((\beta_1), (1), \beta_1, 4)| = |S_2(\beta_1, 2)| + 2$$

Here we use the fact that $S_2((\beta_1), (1), \beta_1, (4)) = \{\pm X^2(X - \beta_1)(X - \beta_2)\}$. Repeating this analysis for $S_1(T_2, \beta_1, 4)$ to give

$$|S_1(T_2, \beta_1, 4)| = |S_2(-\beta_1, 2)| + |S_2((-\beta_1), (1), \beta_1, 4)| = |S_2(-\beta_1, 2)| + 2$$

We use the fact that $S_2((-\beta_1), (1), \beta_1, (4)) = \{\pm X^2(X + \beta_1)(X + \beta_2)\}$.

Moving on to $S_1(T_3, \beta_1, 4)$, we obtain

$$|S_1(T_3, \beta_1, 4)| = |S_2((1, \beta_1), (2, 1), \beta_1, 4)| + |S_2((1, \beta_1), (1, 1), \beta_1, 4)| = 12$$

Here we use Lemma 3.39 to give

$$\begin{aligned} S_2((1, \beta_1), (2, 1), \beta_1, 4) &= \frac{1}{2} \left|S_2(1, 2)\right| \left|S_2(\beta_1, 1)\right|, \\ S_2((1, \beta_1), (1, 1), \beta_1, 4) &= \frac{1}{2} \left|S_2(1, 1)\right| \left|S_2(\beta_1, 1)\right|. \end{aligned}$$

We then use the followings facts;

$$\begin{aligned} S_2(1, 1) &= \{\pm(X - 1)\}, \\ S_2((\beta_1), (1), \beta_1, 4) &= \{\pm X^2(X - \beta_1)(X - \beta_2)\}, \\ S_2(1, 2) &= \{\pm(X^2 + aX + 1) | a \in \{\pm 2, \pm 1, 0\}\}. \end{aligned}$$

The proof that $|S_2(T_4, \beta_1, 4)| = 12$ and $|S_2(T_5, \beta_1, 4)| = |S_2(T_6, \beta_1, 4)| = 4$ is almost identical. The followings facts are required for these cases;

$$\begin{aligned} S_2(-1, 1) &= \{\pm(X + 1)\}, \\ S_2((-\beta_1), (1), \beta_1, 4) &= \{\pm X^2(X + \beta_1)(X + \beta_2)\}, \\ S_2(1, 2) &= \{\pm(X^2 - 1)\}. \end{aligned}$$

We combine these results to give

$$|S| = |S_2(\beta_1, 2)| + |S_2(-\beta_1, 2)| + 36.$$

We now use Lemma 3.41 to calcuate $|S_2(\beta_1, 2)|$.

$$\begin{aligned}
|S_2(\beta_1,2)| &= 2|\{x \in \mathcal{O}_K | (x) \text{ agrees with } \beta_1\}| \\
&= 2\left|\left\{ x \in \mathcal{O}_K \;\middle|\; \begin{array}{c} X^2 + xX + \beta_1 \text{ has two large roots,} \\ X^2 + \sigma(x)X + \beta_2 \text{ has no large roots.} \end{array} \right\}\right| \\
&= 2\left|\left\{ x \in \mathcal{O}_K \;\middle|\; \begin{array}{c} \beta_1 < -|x| - 1 \text{ or } \beta_1 > \max(1, |x| - 1) \\ 1 \geq \beta_2 \geq |\sigma(x)| - 1 \end{array} \right\}\right| \\
&= 2\left|\left\{ x \in \mathcal{O}_K \;\middle|\; \beta_1 > |x| - 1 \text{ and } \beta_2 \geq |\sigma(x)| - 1 \right\}\right| \\
&= 2\left|\left\{ x \in \mathcal{O}_K \;\middle|\; |x| < \beta_1 + 1 \text{ and } |\sigma(x)| \leq \beta_2 + 1 \right\}\right| = 2\,|N(\beta)|
\end{aligned}$$

Repeating this method for $S_2(-\beta_1, 2)$ gives the required result.

$$\begin{aligned}
|S_2(-\beta_1,2)| &= 2|\{x \in \mathcal{O}_K | (x) \text{ agrees with } -\beta_1\}| \\
&= 2\left|\left\{ x \in \mathcal{O}_K \;\middle|\; \begin{array}{c} X^2 + xX - \beta_1 \text{ has two large roots,} \\ X^2 + \sigma(x)X - \beta_2 \text{ has no large roots.} \end{array} \right\}\right| \\
&= 2\left|\left\{ x \in \mathcal{O}_K \;\middle|\; \begin{array}{c} \beta_1 > |x| + 1 \text{ or } -\beta_1 > \max(1, |x| - 1) \\ 1 \geq -\beta_2 \geq |\sigma(x)| - 1 \end{array} \right\}\right| \\
&= 2\left|\left\{ x \in \mathcal{O}_K \;\middle|\; -\beta_1 < -|x| - 1 \text{ and } -\beta_2 \geq |\sigma(x)| - 1 \right\}\right| \\
&= 2\left|\left\{ x \in \mathcal{O}_K \;\middle|\; |x| < \beta_1 - 1 \text{ and } |\sigma(x)| \leq 1 - \beta_2 \right\}\right| = 2\,|N(-\beta)|
\end{aligned}$$

□

Corollary 3.44. *Let $S \subset \mathbb{Z}[X]$ be a maximal Mahler set of degree 4 with Mahler measure β. If β is a quadratic unit then $|S| \geq 40$ with equality if and only if $\beta = \phi = \frac{1+\sqrt{5}}{2}$.*

Proof. Let $K = \mathbb{Q}(\beta)$ and let σ generate $\mathrm{Gal}(K/\mathbb{Q})$. Let $\beta_1 = \beta$ and let β_2 be its conjugate. Let $N(\beta)$ and $N(-\beta)$ be defined as in Theorem 3.43, which states that $|S| = 2|N(\beta)| + 2|N(-\beta)| + 36$. Observe that since $\beta_1 > 1$ and $|\beta_2| < 1$, it is trivial that 0 belongs to both $N(\beta)$ and $(-\beta)$. This implies that $|S| \geq 40$.

If $\beta_2 = \beta^{-1}$, then 1 belongs to $N(\beta)$ and so $|S| \geq 42$. This is clear since $1 < 1 + \beta_2 < 1 + \beta$. If $\beta_2 = -\beta^{-1}$, and $\beta_2 > 2$ then 1 belongs to $N(-\beta)$ and so $|S| \geq 42$. This is clear since $1 < \beta - 1$ and $1 < 1 - \beta^* = 1 + \beta^{-1}$. Hence if $|S| = 40$, we know that $\beta_2 = -\beta^{-1} < 2$. The only quadratic unit β, greater than 1, for which this holds is $\beta = \phi$. We demonstrate that $N(\phi) = \{0\}$, the argument that $N(-\phi) = \{0\}$ is identical. Assume $x \in N(\phi)$. Then there exist integers a,b such that $x = a + b\phi$ and that

$$|a + b\phi| < \phi + 1 \qquad\qquad |a - b\phi^{-1}| \leq 1 - \phi^{-1}.$$

We need to show that $a = b = 0$. The above equations imply that

$$a+b\phi < \phi+1, \quad -a+b\phi^{-1} \leq 1-\phi^{-1}, \quad a-b\phi^{-1} \leq 1-\phi^{-1}, \quad -a-b\phi < \phi+1.$$

Combining the first two inequalities shows that $b(\phi + \phi^{-1}) < 3$ whilst combining the other inequalities give $-b(\phi + \phi^{-1}) < 3$. Hence we know that $|b| \leq 1$. These cases can tested one by one. It is then straightforward to see that $a = b = 0$ as required. □

Chapter 4

Mahler Sets

In this chapter we explore questions related to the size of Mahler sets.

4.1 Arbitrarily Large Mahler Sets

We begin by showing that the unit group of an algebraic number field can contain arbitrarily large Mahler sets.

Example 4.1. *Let n be a positive integer. Let $S \subset \overline{\mathbb{Q}}$ be the maximal Mahler set of degree 4 and measure $(1+\sqrt{2})^n$. Then*

$$\left| S \cap \mathbb{Q}(\sqrt[4]{2}) \right| = 8\lfloor n\theta \rfloor$$

where $\theta = \left(1 + \frac{2\log(1+\sqrt[4]{2})}{\log(1+\sqrt{2})}\right)^{-1}$.

Proof. We use the notation and ideas of Example 3.6, which described the

A-equivalence classes of the unit group of $\mathbb{Q}(\sqrt[4]{2})$. Let S_α be the Mahler set

$$S_\alpha = \{\pm\alpha, \pm\alpha^{-1}, \pm\sigma_3(\alpha), \pm\sigma_3(\alpha)^{-1}\}$$

for any $\alpha \in S$, and let T be the set

$$T = \left\{ \epsilon_1^i \epsilon_2^j \middle| j > i\left(1 + \frac{\log(\epsilon_1)}{\log(\epsilon_2)}\right), i > 0 \right\}.$$

Then for any $\alpha \in S$, $|S_\alpha \cap T| = 1$, which implies $|S \cap \mathbb{Q}(\sqrt[4]{2})| = 8|S \cap T|$. If $\alpha = \epsilon_1^i \epsilon_2^j \in T$, then $M(\alpha) = \epsilon_2^{2j-i}$. Hence

$$S \cap T = \left\{ \epsilon_1^i \epsilon_2^{(i+n)/2} \middle| (i+n)/2 > i\left(1 + \frac{\log(\epsilon_1)}{\log(\epsilon_2)}\right), i > 0 \right\}.$$

These conditions can be rearranged to give

$$S \cap T = \{\epsilon_1^i \epsilon_2^{(n+i)/2} | 0 < i < n\theta\},$$

from which the result is clear. □

We can then combine this result with Example 3.6 to compare all Mahler sets S in the unit group of $\mathbb{Q}(\sqrt[4]{2})$. This reveals a threshold on the size of S, beyond which S must be of a restricted form.

Example 4.2. *Let $S \subset \mathbb{Q}(\sqrt[4]{2})$ be a Mahler set of degree 4 with unit measure. Suppose $|S| \geq 9$. Then the measure of S is of the form $(1+\sqrt{2})^n$ for some positive integer n. Further there exist $x, y \in S$ such that x/y is a Salem number.*

Proof. We recall from Example 3.6 that the unit group of $\mathbb{Q}(\sqrt[4]{2})$ contains seven A-equivalence classes. One contains only ± 1, two contain only elements with quadratic measure, and four contain only elements which have quartic measure. During Example 3.31, we described the maximal Mahler sets with quartic unit measure in $\mathbb{Q}(\sqrt[4]{2}, i)$. These all have exactly 8 elements in $\mathbb{Q}(\sqrt[4]{2})$ and so the measure of S is not quartic since $|S| \geq 9$. This leaves only the units which are A-equivalent to $1+\sqrt{2}$ or $(1+\sqrt{2})^{-1}$, which have Mahler measure $(1+\sqrt{2})^n$ for some positive integer n. We then look at the condensed units with Mahler measure $(1+\sqrt{2})^n$ for a given n, which are $\pm(1+\sqrt{2})^n$ and $\pm(1+\sqrt{2})^{-n}$. By the pigeonhole principle principle we can choose α_1, $\alpha_2 \in S$ such that $C(\alpha_1) = C(\alpha_2)$. We will also assume that $\alpha_1 \sim \alpha_2 \sim 1+\sqrt{2}$. The argument for $(1+\sqrt{2})^{-1}$ is identical. For any $\alpha = \zeta\epsilon_1^i\epsilon_2^j \sim 1+\sqrt{2}$ where $\zeta = \pm 1$, $C(\alpha) = \zeta(-1)^i\epsilon_2^{2j-i}$. Hence we can assume

$$\alpha_1 = \zeta\epsilon_1^k\epsilon_2^{(n+k)/2} \text{ and } \alpha_2 = \zeta\epsilon_1^l\epsilon_2^{(n+l)/2}$$

where $\zeta \in \{\pm 1\}$, n, k, l are integers such that $n \equiv k \equiv l \pmod 2$, $n > 0$ and $k > l$. Then $\alpha_1/\alpha_2 = (\epsilon_1^2\epsilon_2)^{k-l}$ which is a Salem number as required. □

We will continue to explore such thresholds in Section 4.2. We now turn to the following question;

Question 4.3. *Given a number field K, does the unit group of $\mathcal{O}_K$ contain arbitrarily large Mahler sets?*

We have already seen that the answer is affirmative for $\mathbb{Q}(\sqrt[4]{2})$ whilst by Lemma 2.31 it is negative for any quadratic or cubic number field. The principles used in Example 4.2 can be repeated for an arbitrary number field.

Theorem 4.4. *Let K be a number field of degree d and let U be the unit group of $\mathcal{O}_K$. The following are equivalent*

1. *U contains arbitrarily large Mahler sets.*

2. *U contains a Mahler set of size $2^{d+1}d^2 + 1$.*

3. *U contains x, y such that $x \sim y$, $M(x) = M(y)$, x and y have the same degree, and x/y is not a root of unity.*

Proof. We prove this by showing that (1) $\implies$ (2) $\implies$ (3) $\implies$ (1), where the first implication is trivial. We use the pigeonhole principle to show that (2) $\implies$ (3). Let $S \subset U$ be a Mahler set of size $2^{d+1}d^2 + 1$. Archimedean equivalence divides K into at most 2^d equivalence classes. By the pigeonhole principle, there must be $2d^2 + 1$ elements in S which are A-equivalent. There are at most $2d^2$ roots of unity in K, and so by the pigeonhole principle again, the implication holds. To prove that (3) $\implies$ (1) we introduce relative height on K. Let $H_K : \mathcal{O}_K \to [1, \infty)$ be the map

$$H_K(\alpha) = \prod_{i=1}^{d} \max(1, |\sigma_i(\alpha)|)$$

where $\sigma_1, \ldots, \sigma_d$ are the d embeddings of K. Notice that if x and y are A-equivalent algebraic units, then

$$H_K(x)H_K(y) = H_K(xy).$$

Further if two algebraic units have the same degree and relative height on K, then they have the same Mahler measure. Under the conditions of statement

(3), let S_n be the set

$$S_n = \{x^i y^{n-i} \mid 0 \leq i \leq n\}$$

where n is a positive integer. In general, S_n need not be a Mahler set but every element will have the same relative height on K. Hence any subset of S_n whose elements have the same degree, will be a Mahler set. Further since x/y is not a root of unity, $|S_n| = n + 1$. The degree of elements in S_n must divide the degree of K so let m be the number of divisors of d. By the pigeonhole principle, S_{lm} must contain a Mahler set of size l, completing the proof. □

We now give two methods for constructing arbitrarily large Mahler sets inside a number field.

Theorem 4.5. *Suppose α is an algebraic integer such that $C(\alpha) \neq \alpha$ and deg(α^k) = deg(α) for all positive integers k. Let $m = |\Gamma(\alpha)|$ and let S_n be the set*

$$S_n = \left\{C(\alpha)^{n-j}\alpha^{mj} \middle| j \in \mathbb{Z}, 0 < j \leq n\right\}$$

for some positive integer n. Then S_n is a Mahler set, with degree $\deg(\alpha)$, *measure $M(\alpha)^{mn}$ and cardinality n.*

Proof. Suppose $\Gamma(\alpha) = \{\alpha_1, \ldots, \alpha_m\}$. Then for $x = C(\alpha)^{n-j}\alpha_1^{mj} \in S_n$, we see that

$$\Gamma(x) = \{C(\alpha)^{n-j}\alpha_1^{mj}, \ldots, C(\alpha)^{n-j}\alpha_m^{mj}\}.$$

We can see that $|\Gamma(x)| = m$, since else there exist α_k, $\alpha_l \in \Gamma(\alpha)$ with

$\alpha_k^{n-j} = \alpha_l^{n-j}$, contradicting our assumption that $\deg(\alpha^{n-j}) = \deg(\alpha)$. This also ensures the elements of S_n all have the same degree as α. To calculate the Mahler measure of the elements of S_n, we first calculate their condensation:

$$C\left(C(\alpha)^{n-j}\alpha^{mj}\right) = C(\alpha)^{m(n-j)}\alpha_1^{mj}\dots\alpha_m^{mj} = C(\alpha)^{mn-mj+mj} = C(\alpha)^{mn}.$$

By Theorem 3.19, $C(\alpha)$ and $C(\alpha)^{mn}$ have the same degree, whilst α and $C(\alpha)$ have the same Mahler measure by Theorem 3.18. This ensures every element of S_n has Mahler measure $M(\alpha)^{mn}$. We now show $|S_n| = n$. If $|S_n| < n$, then there exists $0 < k < l \leq n$ such that $C(\alpha)^{n-k}\alpha^{mk} = C(\alpha)^{n-l}\alpha^{ml}$. Re-arranging we get that $C(\alpha)^{l-k}\alpha^{m(k-l)} = 1$. This cannot happen since by our assumptions and Theorem 3.19,

$$\deg(C(\alpha)^{l-k}) = \deg(C(\alpha)) \neq \deg(\alpha) = \deg(\alpha^{m(k-l)}).$$

□

We can now answer Question 4.3 for many number fields that contain a proper subfield.

Corollary 4.6. *Let α be a condensed algebraic unit with no conjugates on the unit circle. Let K be a proper extension of $\mathbb{Q}(\alpha)$ which is not totally complex if both $[K : \mathbb{Q}(\alpha)] = 2$ and $\mathbb{Q}(\alpha)$ is totally real. Then the unit group of $\mathcal{O}_K$ contains arbitrarily large Mahler sets.*

Proof. Let r_α and r_K be the number of real embeddings of $\mathbb{Q}(\alpha)$ and K respectively, and let s_α and s_K be the same for complex embeddings. We first show that under our assumptions

$$r_K + s_K/2 - 1 > r_\alpha + s_\alpha/2 - 1. \tag{4.1}$$

Notice that each complex embedding of $\mathbb{Q}(\alpha)$ contributes $1/2$ to the right hand side of (4.1) and $[K : \mathbb{Q}(\alpha)]/2$ to the left hand side. This is because there will be $[K : \mathbb{Q}(\alpha)]$ complex embeddings of K which extend each complex embedding of $\mathbb{Q}(\alpha)$. For each real embedding σ, let n_σ be the number of real embeddings of K which extend σ. Then σ contributes 1 to the right hand side of (4.1), and

$$n_\sigma + \frac{([K : \mathbb{Q}(\alpha)] - n_\sigma)}{2} = n_\sigma/2 + [K : \mathbb{Q}(\alpha)]/2 \tag{4.2}$$

to the left hand side. We observe that no embedding can contribute more to the right hand side of (4.1) than the left hand side. Hence we have

$$r_K + s_K/2 - 1 \geq r_\alpha + s_\alpha/2 - 1.$$

We now determine when equality holds. Since $[K : \mathbb{Q}(\alpha)] > 1$, equality cannot hold if $\mathbb{Q}(\alpha)$ has any complex embeddings. We also notice that the quantity in (4.2) is larger than 1 if $n_\sigma > 1$ or if $[K : \mathbb{Q}(\alpha)] > 2$. Thus equality will hold if and only if $\mathbb{Q}(\alpha)$ is totally real, K is totally complex and $[K : \mathbb{Q}(\alpha)] = 2$. Hence (4.1) holds under our assumptions.

Let $a = r_\alpha + s_\alpha/2 - 1$ and let $\epsilon_1^\alpha, \ldots, \epsilon_a^\alpha$ be a system of fundamental units for $\mathbb{Q}(\alpha)$. Let $b = r_K + s_K/2 - 1$ and let $\epsilon_1^K, \ldots, \epsilon_b^K$ be a system of fundamental units for K. We can assume that for $1 \leq i \leq a$, ϵ_i^α is some power of ϵ_i^K. If $x = \epsilon_b^K$, then no power of x is contained in $\mathbb{Q}(\alpha)$. Since α has no roots on the unit circle we can choose an integer n such that $y = \alpha^n x \sim \alpha$. Notice that no power of y is in $\mathbb{Q}(\alpha)$. Since the sequence $\deg(y^i)$ is cyclic, we can choose a second positive integer m such that $\deg((y)^{im}) = \deg(y^m)$ for all positive integers i. Then y^m satisfies the conditions of Theorem 4.5 and the result follows. □

Corollary 4.7. *Let $K \subset \mathbb{R}$ be a number field which is a proper extension of some number field $J \neq \mathbb{Q}$. Then the unit group of $\mathcal{O}_K$ contains arbitrarily large Mahler sets.*

Proof. We first check that J contains a condensed algebraic unit with no conjugates on the unit circle. This follows from Lemma 1.3, since J contains a Pisot number. The result then follows from Corollary 4.6. □

We can also construct arbitrarily large Mahler sets using condensed numbers.

Theorem 4.8. *Suppose α_1 and α_2 are condensed algebraic units that are A-equivalent and have the same Mahler measure. Let S_n be the set*

$$S_n = \left\{ \alpha_1^i \alpha_2^{n-i} \middle| i \in \mathbb{Z}, 0 \leq i \leq n \right\}.$$

Then S_n is a Mahler set, with degree $\deg(\alpha_1)$ and measure $M(\alpha_1)^n$. Further, if $\frac{\alpha_1}{\alpha_2}$ is not a root of unity, then $|S_n| = n + 1$.

Proof. The fact that S_n is a Mahler set with the given degree and measure follows immediately from Theorem 3.19. Now assume α_1/α_2 is not a root of unity and suppose $|S_n| < n+1$. Then there exist $0 \leq i < j \leq n$ such that $\alpha_1^i \alpha_2^{n-i} = \alpha_1^j \alpha_2^{n-j}$. This implies $\alpha_1^{i-j}\alpha_2^{j-i} = 1$ which is impossible, and hence $|S_n| = n+1$. □

We can also show that for many number fields the answer to Question 4.3 is negative. To do this we introduce quasi-reciprocal numbers, which are defined in a similar way to reciprocal numbers.

Definition 4.9. Let α be an algebraic number of degree d. We say α is *quasi-reciprocal* if there exists a set S of conjugates of α, with $1 < |S| < d$ and $\prod_{s \in S} s = \pm 1$.

It is important to note, and trivial to prove, that reciprocal numbers are quasi-reciprocal if and only if they have degree greater than 2. Hence Pisot numbers are never quasi-reciprocal whilst Salem numbers are always quasi-reciprocal. The following lemma shows that quasi-reciprocal numbers appear naturally when studying Mahler sets. Example 4.2 was an example of this appearance, since all Salem numbers are quasi-reciprocal.

Lemma 4.10. *Let α_1 and α_2 be algebraic units with the same Mahler measure and such that the relationships $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2)$ and $\alpha_1 \sim \alpha_2$ hold. Then α_1/α_2 either belongs to a proper subfield of $\mathbb{Q}(\alpha_1)$, or is a root of unity, or is quasi-reciprocal.*

Proof. Let $\theta = \alpha_1/\alpha_2$. It is clear that $\theta \in \mathbb{Q}(\alpha)$. We assume that $\theta \in \mathbb{Q}(\alpha_1)$ and that θ is not a root of unity. Note that this implies that α_1 and α_2 are not roots of unity. If one of α_1 or α_2 is a root of unity, the other must also be, since they have the same Mahler measure, by Theorem 2.7. This would then imply θ is a root of unity. We prove the result by showing that θ is quasi-reciprocal.

Let $\sigma_1, \ldots, \sigma_m$ be the set of embeddings of $\mathbb{Q}(\alpha_1)$ into $\mathbb{C}$ for which $|\sigma_i(\alpha_1)| > 1$. Then

$$\prod_{i=1}^{m} \sigma_i(\theta) = \prod_{i=1}^{m} \frac{\sigma_i(\alpha_1)}{\sigma_i(\alpha_2)} = \frac{\epsilon_1 M(\alpha_1)}{\epsilon_2 M(\alpha_2)} = \pm 1$$

where $\epsilon_1, \epsilon_2 \in \{\pm 1\}$. Since α_1 is not a root of unity, $1 < m < \deg(\theta)$ and θ is quasi-reciprocal as required. □

Lemma 4.11. *Let K be an algebraic number field which is normal over $\mathbb{Q}$ and let $g_1, \ldots, g_n$ be elements of $G = \mathrm{Gal}(K/\mathbb{Q})$. Suppose α is an algebraic unit in K which is not a root of unity and such that $g_1(\alpha) \cdots g_n(\alpha)$ is a root of unity. Let H be a subgroup of G which contains $\langle g_1, \ldots, g_n \rangle$. Then there exists an irreducible representation ρ of H over $\mathbb{C}$ such that*

$$\det\left(\rho(g_1) + \cdots + \rho(g_n)\right) = 0.$$

Proof. Let r and $2s$ be the number of real and complex embeddings of K respectively, and let $m = r+s/2-1$. Let $\epsilon_1, \ldots, \epsilon_m$ be independent units in K, and ζ a root of unity such that the unit group of K is $\langle \zeta, \epsilon_1, \ldots, \epsilon_m \rangle$. Let V be the $\mathbb{C}H$-module formed by restricting the $\mathbb{C}G$-module $V(K, \zeta, (\epsilon_1, \ldots, \epsilon_m))$ to H. Let $\mathscr{B}' = \{e_1, \ldots, e_m\}$ be the basis of elementary vectors. Then

$$([g_1]_{\mathscr{B}'} + \ldots + [g_n]_{\mathscr{B}'})\, \pi_\epsilon(\alpha) = \pi_\epsilon(g_1(\alpha) \cdots g_n(\alpha)) = 0$$

where $\epsilon = (\epsilon_1, \ldots, \epsilon_m)$. Hence $\pi_\epsilon(\alpha)$ is a non-zero vector in the null space of the matrix $[g_1]_{\mathscr{B}'} + \cdots + [g_n]_{\mathscr{B}'}$. Hence

$$\det\left([g_1]_{\mathscr{B}'} + \cdots + [g_n]_{\mathscr{B}'}\right) = 0.$$

Let $V_1, \ldots, V_d$ be irreducible $\mathbb{C}H$-modules such that $V = V_1 \oplus \cdots \oplus V_d$. Let $\mathscr{B}_1, \ldots, \mathscr{B}_d$ be bases of $V_1, \ldots, V_d$ respectively. We can amalgamate the bases $\mathscr{B}_1, \ldots, \mathscr{B}_d$ to obtain a basis $\mathscr{B}$ of V, such that

$$[g]_{\mathscr{B}} = \begin{pmatrix} [g]_{\mathscr{B}_1} & & 0 \\ & \ddots & \\ 0 & & [g]_{\mathscr{B}_d} \end{pmatrix}$$

for all $g \in G$. Let T be the change of basis matrix from $\mathscr{B}$ to $\mathscr{B}'$. Hence

$$\begin{aligned} \det\left([g_1]_{\mathscr{B}} + \cdots + [g_n]_{\mathscr{B}}\right) &= \det\left(T^{-1}[g_1]_{\mathscr{B}'}T + \cdots + T^{-1}[g_n]_{\mathscr{B}'}T\right) \\ &= \det(T^{-1})\det\left([g_1]_{\mathscr{B}'} + \cdots + [g_n]_{\mathscr{B}'}\right)\det(T) = 0. \end{aligned}$$

We can then see that

$$\det\left([g_1]_{\mathscr{B}} + \cdots + [g_n]_{\mathscr{B}}\right) = \prod_{i=1}^{d} \det\left([g_1]_{\mathscr{B}_i} + \cdots + [g_n]_{\mathscr{B}_i}\right) = 0.$$

Therefore we can choose some i such that the function

$$g \to [g]_{\mathscr{B}_i} (g \in H)$$

is a representation of H over $\mathbb{C}$ with the required property. □

We can now show that no number field of prime degree contains arbitrarily large Mahler sets.

Theorem 4.12. *Let K be an algebraic number field of prime degree p. Let $S \subset K$ be a Mahler set with unit measure. Then $|S| \leq 2(2^p - 2)$.*

Proof. We first handle the case where K contains non-real roots of unity. This can only happen when the degree of K is even, and hence the only possibilities are $K = \mathbb{Q}(i)$ and $K = \mathbb{Q}(\sqrt{3}i)$. The unit group of $\mathbb{Q}(i)$ is $\{\pm 1, \pm i\}$ and $\mathbb{Q}(\sqrt{3}i)$ has unit group $\{\pm 1, \pm(-1+\sqrt{3}i)/2, \pm(1+\sqrt{3})i/2\}$. In either case, the result holds.

We now assume the only roots of unity in K are ± 1. We assume $|S| > 2(2^p - 2)$, and proceed to find a contradiction. By the pigeonhole principle we can find $\alpha_1, \alpha_2 \in S$ which are A-equivalent but such that $\alpha_1/\alpha_2 \neq \pm 1$. The argument is identical to that used in Theorem 4.4, except that we know there are only 2 roots of unity in K. We can now consider K as being $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2)$ since $\alpha_1 \neq \pm 1$ and the only proper subfield of K is $\mathbb{Q}$. Let J be the Galois closure of K over $\mathbb{Q}$ and let $G = \mathrm{Gal}(J/\mathbb{Q})$. Let $g \in G$ be an element of order p. This can always be done since p, the degree of G divides the order of G, which allows the use of Cauchy's theorem. We now claim that g does not fix α_1 or α_2. If it did, p would divide both $|K|$ and $[J : K]$ ensuring p^2 divides G. This is impossible since G is isomorphic to a subgroup of the symmetric group S_p which has order $p!$. Hence the group $\langle g \rangle$ when restricted to K gives a complete set of embeddings for K. Let $g_1, \ldots, g_m$ be the elements of $\langle g \rangle$ which map α_1 and α_2 outside the unit circle. We can then see that

$$\prod_{i=1}^{m} g_i\left(\frac{\alpha_1}{\alpha_2}\right) = \pm\frac{M(\alpha_1)}{M(\alpha_2)} = \pm 1.$$

Then by Lemma 4.11, there exists an irreducible representation for $\langle g\rangle$ such that

$$\det\left(\rho(g_1) + \cdots + \rho(g_m)\right) = 0. \tag{4.3}$$

Since $\langle g\rangle$ is cyclic of order p, we know that $\rho(g) = (\mu)$ for some p-th root of unity μ by Lemma 1.19. It is clear that Equation (4.3) cannot hold if $\mu = 1$, so we can assume μ is a primitive p-th root of unity. Let q be an integer such that the q-th power of g maps α_1 inside the unit circle and $0 \leq q < p$. Equation (4.3) then implies that the numbers $\mu^{p-q}\rho(g_1), \ldots, \mu^{p-q}\rho(g_m)$ are not linearly independent over $\mathbb{Q}$. However these numbers form a subset of $\{\mu, \ldots, \mu^{p-1}\}$ which is an integral basis for $\mathbb{Q}(\mu)$. This contradiction proves that our assumption $|S| > 2(2^p - 2)$ is false, as required. □

A very similar result is the generalisation of Lemma 2.31.

Corollary 4.13. *Let p be a prime. There exists a finite, uniform upper bound on all Mahler sets of degree p and unit measure.*

Proof. Let S be a maximal Mahler set of degree p and unit measure β. Let K be the Galois closure of $\mathbb{Q}(\beta)$ over $\mathbb{Q}$. The case $p = 2$ is covered by Lemma 2.31. Hence we can assume p is an odd prime. Let α be a unit of degree p. Since there are no roots of unity of degree p, α has conjugates inside and outside the unit circle and so $|\Gamma| < p$. Because $|\Gamma^*(\alpha)|$ is a block system, we know that $|\Gamma|$ divides p. This implies $|\Gamma(\alpha)| = 1$ and so α is condensed. Hence S is contained inside K by Theorem 3.18. Since $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to a subgroup of S_p, there is a uniform upper bound on the number of subfields of K with degree p. We can then use Theorem 4.12 to give the result. □

4.2 Mahler Sets of Condensed Numbers

In this chapter we consider Mahler sets of condensed algebraic units. We wish to explore the relationship between the degree, measure and size of such Mahler sets. We begin by defining some important notation.

Definition 4.14. Let $n \geq 2$ be a integer and let Ω_n be the set of condensed units of degree n. For $\alpha \in \Omega_n$ let $S(\alpha)$ be the set

$$S(\alpha) = \left\{\alpha^* \in \Omega_n \middle| \alpha^* \sim \alpha, M(\alpha^*) = M(\alpha)\right\}.$$

Let Υ_n be the set

$$\Upsilon_n = \left\{\alpha \in \Omega_n \middle| x, y \in S(\alpha) \implies x/y \text{ is a root of unity}\right\},$$

and let $c_n = \sup(|S|)$ where S runs over all Mahler sets contained in Υ_n.

The following lemma gives basic facts about Ω_n, Υ_n and c_n.

Lemma 4.15. *Let $n \geq 2$ be an integer. Then*

1. *Ω_n contains no roots of unity.*

2. *If α belongs to Ω_n, then so do all conjugates of α. Further, if α belongs to Υ_n, then so do all conjugates of α.*

3. If α is a Pisot or Salem number of degree n, then $\alpha \in \Upsilon_n$.

4. If p is a prime number, then $\Omega_p = \Upsilon_p$.

5. We have $c_n < \infty$.

Proof. Lemma 3.4 shows that the only condensed roots of unity are ±1, which proves (1). For a condensed algebraic unit α, let K be the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. We know that the elements of $G = \mathrm{Gal}(K/\mathbb{Q})$ preserve the property of being condensed. This gives the first claim of (2). Using Theorem 3.7 we can then see that $S(\sigma(\alpha)) = \{\sigma(x) | x \in S(\alpha)\}$ for all $\sigma \in G$. This completes the proof of (2). To prove (3), we assume α is a Pisot or Salem number, and let $\alpha^* \in S(\alpha)$. Since α and α^* are A-equivalent and condensed, we know that $\mathbb{Q}(\alpha^*) = \mathbb{Q}(\alpha)$. Using this fact, and the fact that α and α^* are A-equivalent, shows that the only large conjugate of α^* is α^*. Then $\alpha^* = \pm\alpha$ since $M(\alpha) = M(\alpha^*)$. This implies $S(\alpha) = \{\pm\alpha\}$ as required. A proof of (4) was contained within the proof of Theorem 4.12. The proof of (5) is very similar to that used in Corollary 4.13. Let $S \subset \Upsilon_n$ be a Mahler set with measure β, and let K be the Galois closure of $\mathbb{Q}(\beta)$ over $\mathbb{Q}$. Since S contains only condensed numbers, $S \subset K$ by Theorem 3.18. Since $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to a subset of the symmetric group S_n, there are at most $2^{n!}$ A-equivalence classes in K. Further we know that $|S(\alpha)|$ is at most $2n^2$ for any $\alpha \in S$ by Lemma 1.3. Hence $c_n \leq 2^{n!+1}n^2$, proving (5). □

Having determined that the constants c_n are finite, we can make the following definition.

Definition 4.16. A Mahler set $S \subset \Omega_n$ is called *large* if $|S| > c_n$.

The remainder of this section is spent trying to describe the constraints placed upon the measure of a Mahler set $S \subset \Omega_n$ if S is known to be large. Any such large Mahler set must contain elements outside Υ_n. By studying such elements we can study the measure of large Mahler sets. The following lemmas explain how we prove our main results in this section.

Definition 4.17. Let Φ_n and Ψ_n be the sets

$$\Phi_n = \left\{\alpha \in \Omega_n \middle| \deg(M(\alpha)) < n\right\};$$
$$\Psi_n = \left\{\alpha \in \Omega_n \middle| M(\alpha) \text{ is quasi-reciprocal}\right\}.$$

Lemma 4.18. *Let α be an algebraic unit and let $A = \{\alpha_1 = \alpha, \dots, \alpha_n\}$ be the set of conjugates of α. Let K be the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ and let $G = Gal(K/\mathbb{Q})$. Let H be a subgroup of S_n and let λ be an appropriate bijection $\lambda : A \to [1, \dots, n]$ so that G and H are permutation isomorphic. Let Γ be the image under λ of the large roots in A and let $\Sigma = \{\Gamma^x | x \in H\}$. Let $\rho_1, \dots, \rho_m$ be a set of irreducible representations for H over $\mathbb{C}$ such that every irreducible representation of H over $\mathbb{C}$ is equivalent to one of them. Then*

1. *If $\{\{1\}, \dots, \{n\}\}$ is the only block system such that Γ is a union of blocks, then $\alpha \in \Omega_n$.*

2. *If $\alpha \in \Omega_n$ and if there exists a subset $J \subset H$ such that $|J| = |\Gamma|$, $\Gamma = \{1^x | x \in J\}$ and $\det\left(\sum_{j\in J} \rho_i(j)\right) \neq 0$ for all $1 \leq i \leq m$, then $\alpha \in \Upsilon_n$.*

3. *If $\alpha \in \Omega_n$ and $|\Sigma| < n$ then $\alpha \in \Phi_n$.*

4. If $\alpha \in \Omega_n$ and there exists $\Sigma^{'} \subset \Sigma$ such that $1 < |\Sigma^{'}| < |\Sigma|$ and each integer $1 \leq i \leq n$ appears in exactly k elements of $\Sigma^{'}$, then $\alpha \in \Psi_n$.

Proof. (1) The image under λ of $\Gamma^*(\alpha)$ will be block system for H. If this block system is $\{\{1\}, \ldots, \{n\}\}$, then $\Gamma^*(\alpha) = \{\{\alpha_n\}, \ldots, \{\alpha_n\}\}$ since λ is a bijection.

(2) Assume $\alpha \in \Omega_n$ but that $\alpha \notin \Upsilon_n$. Then there exists $\alpha^* \in S(\alpha)$ such that α/α^* is not a root of unity. Let this ratio be θ and let $g_1, \ldots, g_{|\Gamma|}$ be the embeddings of $\mathbb{Q}(\alpha)$ which map α outside the unit circle. Then

$$\prod_{i=1}^{|\Gamma|} g_i(\theta) = \prod_{i=1}^{|\Gamma|} \frac{g_i(\alpha)}{g_i(\alpha^*)} = \frac{M(\alpha)}{M(\alpha^*)} = \pm 1.$$

We can use the permutation isomorphism between G and H and the set J to find $\sigma_1, \ldots, \sigma_{|\Gamma|} \in G$ which meet the requirements of Lemma 4.11. We can then use Lemma 4.11 to show there exists an irreducible representation ρ such that

$$\det\big(\rho(\sigma_1) + \cdots + \rho(\sigma_{|\Gamma|})\big) = 0. \tag{4.4}$$

We know that ρ must be equivalent to one of the representations ρ_i. We recall from the proof of Lemma 4.11 that the value of the left hand side of (4.4) depends only on the equivalence class of the representation. Hence we have a contradiction and so $\alpha \in \Upsilon_n$.

(3) Let $\beta_1 = M(\alpha)$ and let $B = \{\beta_1, \ldots, \beta_d\}$ be the set of conjugates of $M(\alpha)$. The action of G on A defines an action on B, whilst H acting on $[1, \ldots, n]$ defines an action on Σ. These two new actions are permutation isomorphic and $|B| = \deg(M(\alpha)) = |\Sigma|$. Hence if $|\Sigma| < n$,

then $\deg(M(\alpha)) < n$ as required.

(4) Let $\theta : G \to H$ be a bijection such that

$$\lambda(\alpha_i^g) = (\lambda(\alpha_i))^{\theta(g)}$$

for all $\alpha_i \in A$ and all $g \in G$. This exists since the actions of G and H are permutation isomorphic. Let $\Sigma^{'} = \{\Sigma_1^{'}, \ldots, \Sigma_m^{'}\}$ and let $h_1, \ldots, h_m$ be such that $\Gamma^{h_i} = \Sigma_i^{'}$. For each h_i let $g_i = \theta^{-1}(h_i)$. Since θ is a permutation isomorphism, $g_i(M(\alpha)) \neq g_j(M(\alpha))$ for any $i \neq j$. It then follows that $\{g_1(M(\alpha)), \ldots, g_m(M(\alpha))\}$ is a proper subset of the conjugates of $M(\alpha)$. To show that $M(\alpha)$ is quasi-reciprocal, we show that the product of these conjugates is ± 1. Let S be the set of large conjugates of α, and let $\epsilon \in \{\pm 1\}$ be such that $M(\alpha) = \epsilon \prod_{a \in S} a$. Then

$$\prod_{i=1}^{m} g_i\left(M(\alpha)\right) = \prod_{i=1}^{m} g_i(\epsilon) \prod_{a \in S} g_i(a) = \epsilon^m \prod_{i=1}^{m} \prod_{a \in S} \lambda^{-1}\left(\lambda\left(a^{g_i}\right)\right).$$

We now use the permutation isomorphism relation to give

$$\prod_{i=1}^{m} g_i\left(M(\alpha)\right) = \epsilon^m \prod_{i=1}^{m} \prod_{a \in S} \lambda^{-1}\left(\lambda\left(a\right)^{h_i}\right).$$

We complete the proof by using the fact that each integer from 1 to n appears in k elements of $\Sigma^{'}$.

$$\prod_{i=1}^{m} g_i\left(M(\alpha)\right) = \epsilon^m \prod_{i=1}^{m} \prod_{x \in \Sigma_i} \lambda^{-1}\left(x\right) = \epsilon^m \prod_{j=1}^{n} \lambda(j)^k = \epsilon^m \left(\prod_{a \in A} a\right)^k = \pm 1.$$

□

Lemma 4.19. *Let α be an algebraic unit of degree $n \geq 2$.*

1. $\alpha \in \Omega_n \iff \alpha^{-1} \in \Omega_n^{-1}$.

2. *If more than half the conjugates of α lie outside the unit circle, then* $\alpha^{-1} \in \Upsilon_n \implies \alpha \in \Upsilon_n$.

3. $\alpha \in \Phi_n \iff \alpha^{-1} \in \Phi_n^{-1}$.

4. $\alpha \in \Psi_n \iff \alpha^{-1} \in \Psi_n^{-1}$.

Proof. (1) Clearly if α is a unit of degree n, so is α^{-1}. If α has no conjugates on the unit circle, then we can use Lemma 3.4 to see that α is condensed if and only if α^{-1} is condensed. If α has conjugates on the unit circle, then α and α^{-1} are conjugates and the result again holds.

(2) If $\alpha \in \Omega_n$ has more than half of its conjugates outside the unit circle, we can show that

$$x \in S(\alpha) \implies x^{-1} \in S(\alpha^{-1}).$$

Notice that if $x \in S(\alpha)$, then x has more than half its roots outside the unit circle. Hence x and α have no roots on the unit circle and the above fact follows from Lemma 3.4. The set of ratios of elements in $S(\alpha)$ is therefore a subset of the set of ratios of elements in $S(\alpha^{-1})$. This completes the second result.

(3) and (4) both follow from (1) and the fact that α and α^{-1} have the same Mahler measure. □

The following theorem shows how Lemma 4.18 and Lemma 4.19 can be used.

Theorem 4.20. *Let α be an algebraic unit of degree 6 and let K be the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. If $G = Gal(K/\mathbb{Q}) \cong A_4$ then*

$$\alpha \in \Omega_6 \implies \alpha \in \Upsilon_6 \cup \Phi_6 \cup \Psi_6.$$

Proof. We assume that α has at most 3 large conjugates. This will be sufficient to prove the result, by Lemma 4.19. If α were a root of unity, G would be an abelian group so we know that α has exactly one, two or three large conjugates. We use the transitive group library provided by the GAP system [11]. Every transitive group of degree 6 is permutation isomorphic to exactly one group in the library. Using the transitive group library shows that G is permutation isomorphic to $H = \langle(1,3,5)(2,4,6),(1,4)(3,6)\rangle$. Let γ be a permutation isomorphism $\gamma : G \to H$ and let λ be the associated map between the conjugates of α and $[1,\ldots,6]$. Let Γ be the image of the set of large conjugates of α under λ and let $\Sigma = \{\Gamma^x | x \in H\}$. Then Σ is equal to one of the following sets;

$$\begin{aligned}
\Sigma_1 &= \big\{\{1\},\{2\},\{3\},\{4\},\{5\},\{6\}\big\}\,,\\
\Sigma_2 &= \big\{\{1,4\},\{2,5\},\{3,6\}\big\}\,,\\
\Sigma_3 &= \big\{\{1,2\},\{1,3\},\{1,5\},\{1,6\},\{2,3\},\{2,4\},\{2,6\},\\
&\qquad\qquad\qquad\{3,4\},\{3,5\},\{4,5\},\{4,6\},\{5,6\}\big\}\,,\\
\Sigma_4 &= \big\{\{1,2,3\},\{3,4,5\},\{1,5,6\},\{2,4,6\}\big\}\,,\\
\Sigma_5 &= \big\{\{1,2,4\},\{1,4,5\},\{2,5,6\},\{2,3,5\},\{3,4,6\},\{1,3,6\}\big\}\,,\\
\Sigma_6 &= \big\{\{1,2,5\},\{2,4,5\},\{3,5,6\},\{2,3,6\},\{1,3,4\},\{1,4,6\}\big\}\,,\\
\Sigma_7 &= \big\{\{1,2,6\},\{4,5,6\},\{2,3,4\},\{1,3,5\}\big\}\,.
\end{aligned}$$

We see that Σ_2 is the only non-trivial block system for H, and so if $\Sigma = \Sigma_2$ then $\alpha \notin \Omega_6$. On the other hand, none of the other possibilities allow Γ to be a disjoint union of elements of Σ_2 and so if $\Sigma \in \{\Sigma_1, \Sigma_3, \ldots, \Sigma_7\}$ then $\alpha \in \Omega_6$.

We consider the other possibilities one by one. If $\Sigma = \Sigma_1$, then α has exactly one large conjugate, which must be equal to $\pm\alpha^*$ for some Pisot or Salem number. By Lemma 4.15(2), we can assume $\alpha = \pm\alpha^*$. We observe that $S(\alpha) = S(\alpha^*)$, and so $\alpha \in \Upsilon_6$ since $\alpha^* \in \Upsilon_6$ by Lemma 4.15(3). If $\Sigma \in \{\Sigma_4, \Sigma_7\}$ then $\alpha \in \Phi_6$ by Lemma 4.18(3), since $|\Sigma_4|, |\Sigma_7| < 6$. If $\Sigma = \Sigma_3$, we let $\Sigma' = \{\{1,2\},\{3,4\},\{5,6\}\}$ and use Lemma 4.18(4) to see that $\alpha \in \Psi_6$. This leaves the cases of Σ_5 and Σ_6, which we claim both imply that $\alpha \in \Upsilon_6$. In order to use Lemma 4.18(5), we must first describe the irreducible representations of H up to equivalence. In the table below, we list the elements of H together with 3 non-trivial irreducible representations ρ_1, ρ_2 and ρ_3. Every non-trivial irreducible representation of H is equivalent to exactly one of them. In the table, and the calculations that follow, ω is a primitive cube root of unity.

By Lemma 4.15(2), we can assume Γ is equal to $\{1, 2, 4\}$ or $\{1, 2, 5\}$. If $\Gamma = \{1, 2, 4\}$ let $J = \{h_1, h_3, h_7\}$, whilst if $\Gamma = \{1, 2, 5\}$ let $J = \{h_1, h_3, h_9\}$. Then the set J has the properties as required by Lemma 4.18(2). Verifying the required calculations then completes the proof;

$$\det(\rho_1(h_1) + \rho_1(h_3) + \rho_1(h_7)) = \det(1 + \omega^2 + 1) = 2 + \omega^2,$$

$$\det(\rho_2(h_1) + \rho_2(h_3) + \rho_2(h_7)) = \det(1 + \omega + 1) = 2 + \omega,$$

$$\det(\rho_3(h_1) + \rho_3(h_3) + \rho_3(h_7)) =$$

$$\det\left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{pmatrix} + \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right) = 1,$$

$$\det(\rho_1(h_1) + \rho_1(h_3) + \rho_1(h_9)) = \det(1 + \omega^2 + 1) = 1 + 2\omega^2,$$

$$\det(\rho_2(h_1) + \rho_2(h_3) + \rho_2(h_9)) = \det(1 + \omega + 1) = 1 + 2\omega,$$

$$\det(\rho_3(h_1) + \rho_3(h_3) + \rho_3(h_9)) =$$

$$\det\left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix}\right) = 1.$$

□

h	$h_1 = ()$	$h_2 = (2,5)(3,6)$	$h_3 = (1,2,3)(4,5,6)$
ρ_1	1	1	ω^2
ρ_2	1	1	ω
ρ_3	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{pmatrix}$
h	$h_4 = (1,2,6)(3,4,5)$	$h_5 = (1,3,5)(2,4,6)$	$h_6 = (1,3,2)(4,6,5)$
ρ_1	ω^2	ω	ω
ρ_2	ω	ω^2	ω^2
ρ_3	$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & -1 \\ -1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$
h	$h_7 = (1,4)(2,5)$	$h_8 = (1,4)(3,6)$	$h_9 = (1,5,3)(2,6,4)$
ρ_1	1	1	ω^2
ρ_2	1	1	ω
ρ_3	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix}$
h	$h_{10} = (1,5,6)(2,3,4)$	$h_{11} = (1,6,2)(3,5,4)$	$h_{12} = (1,6,5)(2,4,3)$
ρ_1	ω^2	ω	ω^2
ρ_2	ω	ω	ω^2
ρ_3	$\begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$

Theorem 4.21. *Let n be an integer such that $2 \leq n \leq 11$ or n is prime. Then*

$$\Omega_n = \Upsilon_n \cup \Phi_n \cup \Psi_n.$$

If $S \subset \Omega_n$ is a large Mahler set with measure β, then either β is quasi-reciprocal or $\deg(\beta) < n$.

Proof. We will assume n is composite, since the Theorem holds for prime n by Lemma 4.15. Assume $n \in \{4, 6, 8, 9, 10\}$. The result then follows by repeating the analysis of Theorem 4.20 for all transitive groups in the library of degree n. This analysis can be performed using the GAP system and the code listed in the appendix. The number of groups to be tested is reduced significantly by considering only those which are minimally transitive. We complete our discussion of this proof by explaining why.

Let α be a unit in Ω_n, and let K be the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Let $G = \mathrm{Gal}(K/\mathbb{Q})$ be permutation isomorphic to H_1 a subgroup of the symmetric group S_n. Let λ be the associated map between the conjugates of α and $[1, \ldots, n]$. Let H_2 be a transitive subgroup of H_1.

If $J \subset H_2$ has the properties required in Lemma 4.18(2), then it will also be suitable as a subset of H_1. This stems from the fact that every $\mathbb{C}H_1$-module is a direct sum of irreducible $\mathbb{C}H_2$-modules. We can then repeat the process used in Lemma 4.11 to show that if ρ is a representation of H_1 over $\mathbb{C}$, then

$$\det\left(\sum_{j \in J} \rho(j)\right) = \prod_{i=1}^{m} \det\left(\sum_{j \in J} \rho_i(j)\right)$$

for some irreducible representations $\rho_1, \ldots, \rho_m$ of H_2 over $\mathbb{C}$.

We now turn to parts (3) and (4) of Lemma 4.18. Let Γ be the image under λ of the large conjugates of α. Let $\Gamma_1^* = \{\Gamma^x | x \in H_1\}$ and $\Gamma_2^* = \{\Gamma^x | x \in H_2\}$. Notice that Γ_2^* must be a subset of Γ_1^*. If they are equal, then we can determine if α belongs to Φ_n or Ψ_n using only H_2. If they are not equal, we can use Γ_2^* and Lemma 4.18(4) to show that $\alpha \in \Psi_n$. $\square$

It is interesting to compare this result with some calculations performed by Boyd [2]. Boyd showed that if α is a reciprocal number of degree 6 then $M(\alpha)$ is either reciprocal or has degree less than 6. We can view Theorem 4.21 as a parallel result where the assumption that α is reciprocal is dropped.

Appendix

The following code was used to prove Theorem 4.21. All but the last function are auxillary functions. The last function ReturnGroupData replicates the analysis of Theorem 4.20. The three inputs are the group, the degree of the action, and a positive integer. This positive integer is the number of attempts made to find some group elements which are suitable for Lemma 4.18(2). We found setting this to be 25 to always be sufficient. The output is a list of useful information about the problem. The last element lists orbits which we cannot show to correspond to elements of Υ_n,Φ_n or Ψ_n. Hence if it is empty, the analogue of Theorem 4.20 holds, for the chosen group and degree.

```
#A function that gives the result of a permutation on a set of points
OnManyPoints:=function(Points,Permutation)
  local Answer, RepeatedPermutation;
  RepeatedPermutation:=ListWithIdenticalEntries(Size(Points),Permutation);
  Answer:=ListN(Points,RepeatedPermutation,OnPoints);
  return Answer;
end;
ReturnOrbitList:=function(Degree,GroupList)
  local ListOfCombinations, iiter, jiter, TempCombinations, RepeatedOnes,
   RepeatedPointsToActOn, SortingPermutations, InOrbitListFlag,
   OrbitListWithRepeats, OrbitList;
  ListOfCombinations:=[];
  for iiter in [1..(Int(Degree/2)-1)] do
    TempCombinations:=Combinations([2..Degree],iiter);
    RepeatedOnes:=ListWithIdenticalEntries(Size(TempCombinations),[1]);
    TempCombinations:=ListN(RepeatedOnes,TempCombinations,Concatenation);
    ListOfCombinations:=Concatenation(ListOfCombinations,
      TempCombinations);
  od;
  OrbitListWithRepeats:=[];
  for iiter in [1..Size(ListOfCombinations)] do
    RepeatedPointsToActOn:=ListWithIdenticalEntries(Size(GroupList),
      ListOfCombinations[iiter]);
    OrbitListWithRepeats[iiter]:=ListN(RepeatedPointsToActOn,GroupList,
      OnManyPoints);
    SortingPermutations:=ListN(OrbitListWithRepeats[iiter],SortingPerm);
    OrbitListWithRepeats[iiter]:=ListN(OrbitListWithRepeats[iiter],
      SortingPermutations,Permuted);
  od;
  #We filter out repeated orbits and repeats inside orbits.
  OrbitList:=[Unique(OrbitListWithRepeats[1])];
  for iiter in [2..Size(OrbitListWithRepeats)] do
    InOrbitListFlag:=true;
    for jiter in [1..(iiter-1)] do
      if OrbitListWithRepeats[jiter][1] in OrbitListWithRepeats[iiter]
        then InOrbitListFlag:=false; fi;
    od;
    if InOrbitListFlag then OrbitList:=Concatenation(OrbitList,
      [Unique(OrbitListWithRepeats[iiter])]); fi;
  od;
  return OrbitList;
end;
```

```
CalculateSearchTerm:=function(InputSet,Degree,NumRepeats)
  local Answer, iiter;
  Answer:=[];
  for iiter in [1..Degree] do
    if Size(Positions(InputSet,iiter))<NumRepeats then
    Add(Answer,iiter); fi;
  od;
  return Answer;
end;
QRSearch:=function(Orbit,NumberOfRoots,Degree)
  local SearchTerms, ListOfCombinations, NewSearchTerm, Temp,
  iiter, isQRflag;
  SearchTerms:=[];
  if NumberOfRoots=2 then
    SearchTerms:=[CalculateSearchTerm(Orbit[1],Degree,
      2*Size(Orbit[1])/Degree)];
  else
    if [Size(Orbit),NumberOfRoots] in [[6,3],[8,4],[9,3],[10,4],[10,5],
      [12,3],[12,4],[12,6],[14,2],[14,7],[15,3],[15,5],[16,4],[16,8],
      [20,10],[24,3],[24,4],[24,6],[25,5],[30,3],[30,5],[32,4],[32,8],
      [45,5],[48,3],[48,4],[75,5],[81,3],[135,5]] then
      ListOfCombinations:=Combinations([2..Size(Orbit)],NumberOfRoots-2);
      for iiter in [1..Size(ListOfCombinations)] do
        Temp:=Orbit{ListOfCombinations[iiter]};
        Temp:=Concatenation(Temp);
        Temp:=Concatenation(Temp,Orbit[1]);
        NewSearchTerm:=CalculateSearchTerm(Temp,Degree,
          NumberOfRoots*Size(Orbit[1])/Degree);
SearchTerms:=Concatenation(SearchTerms,[NewSearchTerm]);
      od;
    fi;
  fi;
  isQRflag:=false;
  for iiter in [1..Size(SearchTerms)] do
    if SearchTerms[iiter] in Orbit then isQRflag:=true; fi;
  od;
  return isQRflag;
end;


ReturnGroupData:=function(MyGroup,Degree, NumberAttempts)
  local   GroupData, ListMyGroup, MyGroupIrr, RepeatedMyGroup,
    MyGroupReps, OrbitList, NewGroupDataEntry, iiter, CurrentOrbit,
    MinQRNumber, NumberOfRootsToUse, isQRflag, EmbeddingsList,
    CurrentEmbeddings, RandomEmbeddings, Temp, Temp2, jiter, kiter;
  #Entry number 1: The group
  #Entry number 2: Degree of the action
  GroupData:=[MyGroup,Degree];
  #Entry number 3: list of elements of the group
  ListMyGroup:=List(MyGroup);
  GroupData:=Concatenation(GroupData,[ListMyGroup]);
  #Entry number 4: Irreducible characters for the group
  #Entry number 5: number of such characters.
  MyGroupIrr:=Irr(MyGroup);
  GroupData:=Concatenation(GroupData,[MyGroupIrr,Size(MyGroupIrr)]);
  #Entry number 6: Representations
  RepeatedMyGroup:=ListWithIdenticalEntries(Size(MyGroupIrr),MyGroup);
  MyGroupReps:=ListN(RepeatedMyGroup,MyGroupIrr,
    IrreducibleRepresentationsDixon);
  GroupData:=Concatenation(GroupData,[MyGroupReps]);
  #Entry number 7: Orbits
```

```
#Entry number 8: Number of Orbits
NewGroupDataEntry:=ReturnOrbitList(Degree,ListMyGroup);
GroupData:=Concatenation(GroupData,
  [NewGroupDataEntry,Size(NewGroupDataEntry)]);
#Entry number 9: Orbits with size >= Degree
#Entry number 10: Number of such orbits.
NewGroupDataEntry:=[];
for iiter in [1..GroupData[8]] do
  if Size(GroupData[7][iiter]) >= Degree then
    NewGroupDataEntry:=Concatenation(NewGroupDataEntry,
      [GroupData[7][iiter]]);
  fi;
od;
GroupData:=Concatenation(GroupData,
  [NewGroupDataEntry,Size(NewGroupDataEntry)]);
#Entry number 11: Orbits we cannot show are "quasi-reciprocal".
#Entry number 12: Number of such orbits.
NewGroupDataEntry:=[];
for iiter in [1..GroupData[10]] do
  CurrentOrbit:=GroupData[9][iiter];
  # Number roots used in QR * Number Large Roots Original =
  # Degree Original * Number of repeats
  # MinQRNumber:=Minimum number roots of M(alpha) needed
  # to get each root of original number repeated equally.
  MinQRNumber:=Lcm(Size(CurrentOrbit[1]),Degree)/Size(CurrentOrbit[1]);
  if MinQRNumber = Size(CurrentOrbit) then
    NewGroupDataEntry:=Concatenation(NewGroupDataEntry,[CurrentOrbit]);
  else
    #Produce a list of number of roots to use in QR.
    # require: < size(CurrentOrbit), divisible by MinQRNumber
  NumberOfRootsToUse:=MinQRNumber*Filtered(
   DivisorsInt(Size(CurrentOrbit)/MinQRNumber),
   n-> n <>Size(CurrentOrbit)/MinQRNumber);
  # And an exception to that previous rule.
  if (Degree=10 and Size(CurrentOrbit)=10 and Size(CurrentOrbit[1])=5)
   then NumberOfRootsToUse:=Concatenation(NumberOfRootsToUse,[4]);
  fi;
  isQRflag:=false;
  for jiter in [1..Size(NumberOfRootsToUse)] do
   if QRSearch(CurrentOrbit,NumberOfRootsToUse[jiter],Degree)=true
    then isQRflag:=true;break;
   fi;
  od;
  if isQRflag=false then Add(NewGroupDataEntry,CurrentOrbit); fi;
 fi;
od;
GroupData:=Concatenation(GroupData,
 [NewGroupDataEntry,Size(NewGroupDataEntry)]);
#Entry number 13: One entry for each orbit in GroupData[11].
# contains either: false or
# A list of group elements for Lemma 5.18 such that number in Upsilon_n
NewGroupDataEntry:=[];
#Partitions G, according to the value of 1^x
EmbeddingsList:=[];
for iiter in [1..Degree] do
 Add(EmbeddingsList,Filtered(ListMyGroup,x->1^x=iiter));
od;
for iiter in [1..GroupData[12]] do
 CurrentOrbit:=GroupData[11][iiter];
 CurrentEmbeddings:=EmbeddingsList{CurrentOrbit[1]};
```

```
    for jiter in [1..NumberAttempts] do
      RandomEmbeddings:=List(CurrentEmbeddings,Random);
      Temp:=[];
      for kiter in [1..GroupData[5]]  do
        Temp2:=ListWithIdenticalEntries(Size(CurrentOrbit[1]),
          MyGroupReps[kiter]);
        if Determinant(Sum(ListN(Temp2,RandomEmbeddings,Image)))=0 then
          Temp:=false; break;
        fi;
      od;

      if Temp=[] then
        Add(NewGroupDataEntry,RandomEmbeddings); break;
      fi;
      if (jiter=NumberAttempts and Temp=false) then
        Add(NewGroupDataEntry,Temp);
      fi;
    od;
  od;
  Add(GroupData,NewGroupDataEntry);
  #Entry number 14: Orbits we cannot place in Phi_n,Psi_n or Upsilon_n.
  #If empty for all minimally transitive groups of degree n,
  #Then Theorem 5.21 holds for degree n
  Add(GroupData, GroupData[11]{Positions(GroupData[13],false)});
  return GroupData;;
end;
```

Bibliography

[1] Şaban Alaca and Kenneth S. Williams. *Introductory algebraic number theory.* Cambridge University Press, Cambridge, 2004.

[2] David W. Boyd. Inverse problems for Mahler's measure. In *Diophantine analysis (Kensington, 1985)*, volume 109 of *London Math. Soc. Lecture Note Ser.*, pages 147–158. Cambridge Univ. Press, Cambridge, 1986.

[3] David W. Boyd. Perron units which are not Mahler measures. *Ergodic Theory Dynam. Systems*, 6(4):485–488, 1986.

[4] John D. Dixon and Artūras Dubickas. The values of Mahler measures. *Mathematika*, 51(1-2):131–148, 2004.

[5] John D. Dixon and Brian Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1996.

[6] E. Dobrowolski. On a question of Lehmer and the number of irreducible factors of a polynomial. *Acta Arith.*, 34:391–401, 1979.

[7] Artūras Dubickas. On numbers which are Mahler measures. *Monatsh. Math.*, 141(2):119–126, 2004.

[8] Artūras Dubickas. Mahler measures in a cubic field. *Czechoslovak Math. J.*, 56(131)(3):949–956, 2006.

[9] Manfred Einsiedler, Graham Everest, and Thomas Ward. Primes in sequences associated to polynomials (after Lehmer). *LMS Journal of Computation and Mathematics*, 3:125–139, 2000.

[10] Graham Everest and Thomas Ward. *Heights of polynomials and entropy in algebraic dynamics.* Universitext. Springer-Verlag London Ltd., London, 1999.

[11] The GAP Group, www.gap-system.org. *GAP – Groups, Algorithms, and Programming, Version 4.5.5*, 2012.

[12] E. Hecke. *Vorlesungen über die Theorie der algebraischen Zahlen.* Akad. Verlag. M.B.H., Leipzig, 1923 (reprinted, Chelsea, New York, 1948).

[13] Gordon James and Martin Liebeck. *Representations and characters of groups.* Cambridge University Press, New York, second edition, 2001.

[14] Gerald J Janusz. *Algebraic number theory*, volume 7 of *Graduate Studies in Mathematics.* American Mathematics Studies, Providence, RI, second edition, 1996.

[15] D. H. Lehmer. Factorization of certain cyclotomic functions. *The Annals of Mathematics*, 34(3):pp. 461–479, 1933.

[16] D. H. Lehmer. A factorization theorem applied to a test for primality. *Bull. Amer. Math. Soc.*, 45(2):132–137, 1939.

[17] D. H. Lehmer. On the factors of $2^n \pm 1$. *Bull. Amer. Math. Soc.*, 53:164–167, 1947.

[18] D. A. Lind. The entropies of topological Markov shifts and a related class of algebraic integers. *Ergodic Theory Dynam. Systems*, 4(2):283–300, 1984.

[19] Tracy A. Pierce. The numerical factors of the arithmetic forms $\sum_{i=1}^{n}(1 \pm \alpha_i^m)$. *Ann. of Math. (2)*, 18(2):53–64, 1916.

[20] Carl Ludwig Siegel. Algebraic integers whose conjugates lie in the unit circle. *Duke Math. J.*, 11:597–602, 1944.

[21] C. J. Smyth. On the product of the conjugates outside the unit circle of an algebraic integer. *Bull. London Math. Soc.*, 3:169–175, 1971.

[22] C. J. Smyth. Topics in the theory of numbers, Ph.D. Thesis, University of Cambridge, 1972.

[23] C. J. Smyth. Mahler measure of algebraic numbers: a survey. In *Number Theory and Polynomials*, volume 352 of *London Math. Soc. Lecture Note Ser.*, pages 322–349. Cambridge Univ. Press, Cambridge, 2008.