LOWER BOUNDS FOR HEIGHTS IN CYCLOTOMIC EXTENSIONS AND RELATED PROBLEMS

by

MOHAMED ISMAIL MOHAMED ISHAK

M.Sc., Kansas State University, 2006

AN ABSTRACT OF A DISSERTATION

submitted in partial fulfillment of the requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Mathematics
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2009

Abstract

We define the Mahler measure $M(f)$ of a polynomial $f(x)$ to be the absolute value of the product of the leading coefficient and the roots outside the unit circle. For a non zero algebraic number α we define the Mahler measure of α denoted by $M(\alpha)$, to be the Mahler measure of an irreducible polynomial $F(x)$ with integer coefficients and $F(\alpha) = 0$. Then the absolute logarithmic Weil height, $h(\alpha)$ of α is given by

$$h(\alpha) = \frac{1}{[\mathbb{Q}(\alpha):\mathbb{Q}]} \log M(\alpha).$$

In 1933, D.H. Lehmer asked does there exist a positive constant $c > 0$ such that

$$h(\alpha) > \frac{c}{[\mathbb{Q}(\alpha):\mathbb{Q}]}$$

when α is not a root of unity?

For an algebraic number α which is not a root of unity but which lies in a cyclotomic extension Amoroso & Dvornicich have established an even stronger (i.e. degree independent) lower bound

$$h(\alpha) > \frac{1}{12} \log 5 = 0.134119 \ldots.$$

Here we improve this bound to show that the height of a nonzero algebraic number which is not a root of unity but which lies in a cyclotomic extension must satisfy $h(\alpha) > 0.155090 \ldots$. For certain cyclotomic extensions we obtain the best possible lower bound

$$h(\alpha) \geq \frac{1}{12} \log 7 = 0.162159 \ldots.$$

Further, we show that the height of a nonzero algebraic number α which is not a root of unity but is a zero of a polynomial of degree d with all odd coefficients must satisfy

$$h(\alpha) \geq \frac{0.4278}{d+1}.$$

More generally we obtain bounds when the coefficients are all congruent to 1 modulo m for some integer $m \geq 2$.

LOWER BOUNDS FOR HEIGHTS IN CYCLOTOMIC EXTENSIONS AND RELATED PROBLEMS

by

MOHAMED ISMAIL MOHAMED ISHAK

M.Sc., Kansas State University, 2006

A DISSERTATION

submitted in partial fulfillment of the requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Mathematics
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2009

Approved by:

Major Professor
Christopher Pinner

Copyright

Abstract

We define the Mahler measure $M(f)$ of a polynomial $f(x)$ to be the absolute value of the product of the leading coefficient and the roots outside the unit circle. For a non zero algebraic number α we define the Mahler measure of α denoted by $M(\alpha)$, to be the Mahler measure of an irreducible polynomial $F(x)$ with integer coefficients and $F(\alpha) = 0$. Then the absolute logarithmic Weil height, $h(\alpha)$ of α is given by

$$h(\alpha) = \frac{1}{[\mathbb{Q}(\alpha):\mathbb{Q}]} \log M(\alpha).$$

In 1933, D.H. Lehmer asked does there exist a positive constant $c > 0$ such that

$$h(\alpha) > \frac{c}{[\mathbb{Q}(\alpha):\mathbb{Q}]}$$

when α is not a root of unity?

For an algebraic number α which is not a root of unity but which lies in a cyclotomic extension Amoroso & Dvornicich have established an even stronger (i.e. degree independent) lower bound

$$h(\alpha) > \frac{1}{12} \log 5 = 0.134119 \ldots.$$

Here we improve this bound to show that the height of a nonzero algebraic number which is not a root of unity but which lies in a cyclotomic extension must satisfy $h(\alpha) > 0.155090 \ldots$. For certain cyclotomic extensions we obtain the best possible lower bound

$$h(\alpha) \geq \frac{1}{12} \log 7 = 0.162159 \ldots.$$

Further, we show that the height of a nonzero algebraic number α which is not a root of unity but is a zero of a polynomial of degree d with all odd coefficients must satisfy

$$h(\alpha) \geq \frac{0.4278}{d+1}.$$

More generally we obtain bounds when the coefficients are all congruent to 1 modulo m for some integer $m \geq 2$.

Table of Contents

List of Tables

Acknowledgements

Alhamdulillah, I would like to thank my supervisor, Christopher Pinner, first for his patience and time in educating me constantly in the subject throughout this project, then for his thoughtful directions, helpful instructions, keen insights, and precious advice.

I would like to thank all the members of my dissertation committee for their careful reading of the manuscript. I appreciate their valuable time, and the suggestions to improve the clarity and the accuracy.

I would like to thank John Garza for the helpful discussions on problems of heights of algebraic numbers and Mahler measure. Also I greatly appreciate his insights and suggestions. Thank also goes to Benjamin Wiles for his great work of computations and the ideas on computations. I would like to thank Todd Cochrane, G.T. Seneviratne, and A.A.S. Perera for encouraging me in the field of number theory. Also I thank my high school teachers M.N. Misba and M. Cader Ali for all their support given to me in the study of mathematics.

Next, I would like to express my gratitude to the Department of Mathematics, Kansas State University for their generous financial support and for all other assistance given to me throughout this long period of time. Also I am thankful to University of Peradeniya, Sri Lanka for providing study leave and financial support to pursue me graduate studies.

I would like to thank my wife, Fathima Rizana and my children Abdul Rahman, Abdul Azeez, and Abdul Malik for their patience and for their supports. Also I thank my friend Talal Altahtamouni for his continuous encouragement and motivation.

Finally, my special thanks goes to my mother, Ainul Fareeka and my father, Mohamed Ismail for their dedications, sacrifices, and truthfulness to give me a decent education.

MOHAMED ISMAILI MOHAMED ISHAK

The Kansas State University at Kansas

August, 2009.

CHAPTER 1 - **INTRODUCTION**

This thesis is about the absolute logarithmic Weil height of algebraic numbers and the Mahler measure of polynomials. We show here a lower bound for the height of a nonzero algebraic number which is not a root of unity but which is in a cyclotomic extension, and a lower bound for the height of an algebraic number which is a root of a polynomial with all odd coefficients. Also we will state some interesting research problems. We discuss the absolute values and valuations on a field k and state some preliminary theorems on algebraic number fields in Chapter 2.

Let $f(x)$ be a polynomial with complex coefficients. We define the Mahler measure of $f(x)$ denoted by $M(f)$ to be the absolute value of the product of the leading coefficient and the roots outside the unit circle. That is, if we write $f(x)$ as

$$f(x) = a\prod_{i=1}^{d}(x-\alpha_i)$$

where a is the leading coefficient and the α_i's are the roots of $f(x)$ then $M(f)$ is expressed as

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

Let α be an algebraic number and suppose that α is a root of an irreducible integer polynomial

$$f(x) = a\prod_{i=1}^{d}(x-\alpha_i)$$

then we define the Mahler measure of α to be $M(\alpha) = M(f)$ and the absolute logarithmic Weil height $h(\alpha)$ of α to be

$$h(\alpha) = \frac{1}{d}\log M(f) = \frac{1}{d}\log M(\alpha).$$

For $f(x) \in \mathbb{Z}[x]$ we have $M(f) \geq 1$. By the result of Kronecker (Theorem 3.1.3) we have $M(f) = 1$ if and only if $f(x)$ is a product of a power of x and cyclotomic polynomials. The smallest known Mahler measure greater than 1 is given by **Lehmer's Polynomial**,

$$l(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$$

which is $M(l) = 1.176280\ldots$, discovered by D.H. Lehmer.

In 1933, D.H. Lehmer [18] asked the following question.
Does there exist a sequence (P_n), of noncyclotomic polynomials with integer coefficients such that the Mahler measure of the polynomial P_n can made arbitrarily close to 1? It is widely believed that the answer to this is No. Equivalently, any irreducible noncyclotomic polynomial $f(x) \in \mathbb{Z}[x]$ with $f(0) \neq 0$ satisfies $M(f) > c$ for some constant $c > 1$. This is known as **Lehmer's Problem.** Lehmer's problem can be equivalently stated in terms of absolute logarithmic Weil height of an algebraic number as follows:

For a nonzero algebraic number α which is not a root of unity, does there exists a positive constant $c > 0$ such that

$$h(\alpha) > \frac{c}{[\mathbb{Q}(\alpha):\mathbb{Q}]}$$

where $d = [\mathbb{Q}(\alpha):\mathbb{Q}]$ is the degree of the minimal polynomial of α?
A number of special cases of Lehmer's problem have been proved (we will discuss these in Chapter 3). The most relevant to this thesis are the following three cases (a), (b) and (c). We will show how the result in (b) can be obtained in a straightforward manner in Chapter 3 and in Chapter 4 we will show how to obtain the results of (c). Both these results will be improved.

(a) If α lies in a Kroneckerian field (totally a real number field, or a totally quadratic extension of such a field) and $|\alpha| \neq 1$ then Schinzel [24] showed that

$$h(\alpha) \geq \frac{1}{2}\log\left(\frac{1+\sqrt{5}}{2}\right) = 0.240605\ldots.$$

J.Garza [11] made a generalization of this result. G. Höhn & N.P. Skoruppa [14] gave a one page proof for Schinzel's result in the case of totally real algebraic integers, and

then G. Höhn [15] gave a shorter proof for Garza's results for algebraic integers. In Chapter 3 Lemma 3.5.5 we show how the G. Höhn & N.P. Skoruppa method can be used without the need of the extra restrictions.

(b) If α lies in an abelian extension of the rationals (i.e. α lies in some cyclotomic extension, by the Kronecker-Weber Theorem) Amoroso and Dvornicich [1] proved the bound

$$h(\alpha) \geq \frac{1}{12}\log 5 = 0.134119 \ldots.$$

We give an improvement of this in Theorem 2 below and we discuss this more precisely in Theorem 3.7.2 of Chapter 3.

(c) For an integer $m \geq 2$, let $D_m = \left\{f(x) = \sum_{i=1}^{n} a_i x^i \in \mathbb{Z}[x] : a_i \equiv 1(\text{mod } m)\right\}$. If α is a zero of a polynomial $f(x)$ in D_m of degree n, but not a $2(n+1)$st root of unity, then

$$h(\alpha) \geq c_m\left(\frac{1}{n+1}\right),$$

with $c_2 = 0.402359 \ldots$, $c_2 = 0.402359 \ldots$, and $c_m = \log\left(\sqrt{m^2+1}/2\right)$ for $m \geq 3$,

This result is due to Borwein, Dobrowolski and Mossinghoff [4] and was improved in [9] with $c_2 = 0.402359 \ldots$, and for small $m \geq 3$

$$c_3 = 0.501026 \ldots, c_4 = 0.832461 \ldots, c_5 = 0.952869, c_6 = 1.165884,$$

$$c_7 = 1.271775, c_8 = 1.425369, c_9 = 1.515669, c_{10} = 1.634836,$$

$$c_{11} = 1.712539.$$

We also show improvements of this in Theorem 3 (we discuss more precise results in Chapter 4).

We make two main observations. First observe that results in (a) and (b) are significantly better than a Lehmer type bound since these two height bounds do not decrease with degree. The

second observation is that in (c) we get a Lehmer type bound if the polynomial is irreducible and a Lehmer type absolute lower bound for $M(f)$ if a certain proportion of the roots are noncyclotomic.

Recall that α is abelian if it lies in some cyclotomic extension extension $\mathbb{Q}(\zeta_m)$ (where ζ_m is the primitive mth root of unity). Amoroso & Dvornicich [1] observed that for a nonzero algebraic number α which is not a root of unity which lies in a cyclotomic extension $\mathbb{Q}(\zeta_m)$, the lower bound for the absolute logarithmic Weil height cannot be replaced by anything larger than

$$\frac{1}{12}\log 7 = 0.162159\ldots.$$

To be explicit by writing

$$\alpha_0 = \frac{(3u^2-5)}{\sqrt{7}i(1+\lambda_0)}, u = 2\cos(2\pi/7),$$

$$\lambda_0 = \frac{1}{14}(2-9u-3u^2) + \frac{1}{14}(5u^2+u-8)\sqrt{3}i$$

(λ_0 is a root of $x^{12}+\frac{13}{7}x^6+1$) we see that all the roots of $7x^{12}-13x^6+7$, namely $\pm\alpha_0^{\varepsilon}\zeta_3^j$ for $j = 0,1,2$ and $\varepsilon = \pm 1$, lie in $\mathbb{Q}(\zeta_{21})$. Thus we achieve the smallest know abelian height,

$$h(\alpha_0) = \frac{1}{12}\log 7 = 0.162159\ldots$$

in $\mathbb{Q}(\zeta_{21})$. Suppose that $2|m$ and that $\alpha\zeta_m^u \notin \mathbb{Q}(\zeta_{m/2})$ for any u, then Amoroso & Dvornicich obtain the stronger result that,

$$h(\alpha) \geq \frac{1}{4}\log 2 = 0.173286\ldots.$$

This bound is sharp as shown by the examples,

$$\alpha_1 = \frac{1}{4}(1+i)\left(1+\sqrt{-7}\right) \in \mathbb{Q}(\zeta_{28}),$$

$$\alpha_2 = \frac{1}{4}(1+i)\left(\sqrt{5}+\sqrt{-3}\right) \in \mathbb{Q}(\zeta_{60})$$

$$h(\alpha_1) = \frac{1}{4}\log 2 = 0.173286\ldots = h(\alpha_2).$$

For an algebraic number α in a cyclotomic extension $\mathbb{Q}(\zeta_m)$ (where ζ_m is the primitive mth root of unity) we may plainly assume that m is minimal. Moreover if $\alpha = \alpha_1\zeta$ for any root of unity ζ we get $h(\alpha) = h(\alpha_1)$. Therefore it often convenient to assume that:

Property (1.1.1): There does not exist a root of unity ζ such that $\zeta\alpha \in \mathbb{Q}(\zeta_{m'})$ with $m' < m$.

If the property (1.1.1) does not hold then we should work with $\zeta\alpha$ rather than α.

Thus from Amoroso & Dvornicich [1], if $\alpha \in \mathbb{Q}(\zeta_m)$ has height less than $\frac{1}{4}\log 2 = 0.173286\ldots$ and satisfies property (1.1.1) one must have $\gcd(2, m) = 1$. We show any height less than $\frac{1}{12}\log 7 = 0.162159\ldots$ and satisfying property (1.1.1) must have $\gcd(6, m) = 1$.

The main results of this thesis are summarized in the following three theorems.

Theorem 1

Let $\alpha \in \mathbb{Q}(\zeta_m)$, $\alpha \neq 0$, and α is not a root of unity. If $3|m$ and that $\alpha\zeta_m^u \notin \mathbb{Q}(\zeta_{m/3})$ for any integer u. Then

$$h(\alpha) \geq \frac{1}{12}\log 7 = 0.162159\ldots.$$

More precisely in Theorem 3.7.1 of Chapter 3, we will give refinements classifying the small heights when $2|m$ and $3|m$.

Amoroso & Dvornicich also showed that a height less than

$$\frac{1}{12}\log(11/2) = 0.1420662\ldots$$

must have $385|m$. We show in the next theorem that there is no height this small and further show that any height less than $\frac{1}{12}\log 7 = 0.162159\ldots$ must have $35|m$:

Theorem 2

Suppose that $\alpha \in \mathbb{Q}(\zeta_m)$, $\alpha \neq 0$, and α is not a root of unity then

$$h(\alpha) \geq 0.155090\ldots.$$

If $\alpha \in \mathbb{Q}(\zeta_m)$ has height

$$h(\alpha) \leq \frac{1}{12}\log 7 = 0.162159\ldots$$

then we must have $35|m$. If in addition property (1.1.1) holds then $\gcd(6, m) = 1$.

Theorem (3)

If α is a zero of a polynomial $f(x)$ in D_m of degree n and α is not an $2(n+1)st$ root of unity (not an $(n+1)st$ if $m \geq 3$), then result in (c) above holds with

$$c_2 = 0.427188,$$

and

$$c_m = \begin{cases} \frac{1}{2}\log\left(\frac{m^2+3}{4}\right) & \text{if } m \geq 3 \text{ odd,} \\ \frac{1}{2}\log\left(\frac{m^2+4}{4}\right) & \text{if } m \geq 4 \text{ even.} \end{cases}$$

For small $m \geq 3$ we obtain,

$$c_3 = 0.620362,\ c_4 = 0.855600,\ c_5 = 1.016628,\ c_6 = 1.179916,$$

$$c_7 = 1.307083,\ c_8 = 1.434141,\ c_9 = 1.538934,\ c_{10} = 1.640027,$$

$$c_{11} = 1.728890.$$

We give an asymptotically more precise bound on c_m in Theorem 4.1. In Theorem 4.2.1 we show the optimal c_2 is at most 0.481211….

CHAPTER 2 - **ABSOLUTE VALUES AND VALUATIONS**

2.1 Absolute Values

Definition 2.1

Let k be a field. We say the map $|.| : k \to \mathbb{R}^+ \cup \{0\}$ is an absolute value on k if the following three properties are satisfied.

(i) $|x| = 0$ if and only if $x = 0$

(ii) $|x.y| = |x|.|y|$ for all $x, y \in k$

(iii) $|x + y| \leq |x| + |y|$ for all $x, y \in k$

Immediately we get $|.|_0$ on k, defined by

$$|x|_0 = \begin{cases} 1 & x \neq 0 \\ 0 & x = 0 \end{cases}$$

is an absolute value on k, and is called the trivial absolute value on k. All the other absolute values defined on k are said to be nontrivial.

An absolute value $|.|$ on k defines a group homomorphism from the multiplicative group $(k^\times, \times)$ to $(\mathbb{R}^+, \times)$, the multiplicative group of positive real numbers. Since $|.|$ is a group homomorphism it follows that

(i) $|1| = |-1| = 1$ and more generally if $\zeta^n = 1$ for $\zeta \in k,\ n \in \mathbb{Z}$, where ζ a root of unity then $|\zeta| = 1$

(ii) $|x^{-1}| = |x|^{-1}$.

Definition 2.1.1

An absolute value, $|.|$ is said to be non-archimedean if for all $x, y \in k$ property (iii) can be strengthened to

$$|x + y| \leq \max\{|x|, |y|\}, \tag{2.1.2}$$

which is called the strong triangle inequality or ultrametric inequality. We say an absolute value is archimedean if there exists a pair $x, y \in k$ such that

$$|x + y| > \max\{|x|, |y|\}.$$

Since an absolute value $|.|$ induces a metric topology on k through the map

$$d : \quad k \times k \ \to [0, \infty)$$

defined by

$$d(x, y) = |x - y|$$

we say any two absolute values on k are equivalent if they induce the same metric topology on k. Let us denote the set of all non trivial absolute values on k by $\mathfrak{M}(k)$, then this defines an equivalent relation on $\mathfrak{M}(k)$ and an equivalence class of $\mathfrak{M}(k)$ is called a place. We denote the set of places (equivalence classes of $\mathfrak{M}(k)$) of k by V_k. If an absolute value is archimedean then all other absolute values which are in the same place (equivalent ones) are also archimedean and an archimedean place is also called an infinite place. If an absolute value is nonarchimedean then all the equivalent ones are also nonarchimedean and a nonarchimedean place is also called a finite place.

In k we define,

$$n = \begin{cases} \underbrace{1 + 1 + \cdots + 1}_{n-\text{times}} & \text{if } n > 0 \\ \underbrace{(-1) + (-1) + \cdots + (-1)}_{-n-\text{times}} & \text{if } n < 0 \end{cases}$$

The following theorems are the results of Propositions 1-3-1 and 1-3-3 of [30] which defines and characterizes nonarchimedean absolute values on a field k.

Theorem 2.1.3

Let $|.|$ *be an absolute value on* k*. Then* $|.|$ *is non-archimedean if and only if* $|n| \leq 1$ *for all* $n \in k$.

Theorem 2.1.4

If $|.|$ *be a non-archimedean absolute value on* k *and if* $|x| < |y|$ *for* $x, y \in k$*, then* $|x + y| = |y|$.

Theorem 2.1.4 gives the following immediate result.

Suppose $x_1, x_2, \dots, x_n \in k$ such that $|x_i| < |x_n|$ for $i = 1,2, \dots, n$, then

$$\left|\sum_{i=1}^{n} x_i\right| = |x_n|.$$

In order to characterize the equivalent absolute values we go for the following theorem which can be deduced from Theorem 1-1-4 of [30].

Theorem 2.1.5

If $|.|_1$ *and* $|.|_2$ *are two non-trivial absolute values on k, then the following are equivalent.*

(i) $|.|_1$ *and* $|.|_2$ *induce same equivalent metric topology on k*

(ii) *For all* $x \in k$ $\quad |x|_1 < 1 \Rightarrow |x|_2 < 1$

(iii) $\exists\ \lambda > 0$ *in* $\mathbb{R}$ *with* $|x|_1 = |x|_2^{\lambda} \quad \forall\ x \in k$.

The weak approximation theorem stated below, derived from Theorem 3.1 in Chapter 2 of [6], is one of the tools used in proving an important Theorem, (Theorem 2.4.8) in this Chapter.

Theorem 2.1.6 (The Weak Approximation Theorem)

Let $|.|_j$ *, for* $j = 1,2,\dots,J$ *be pairwise inequivalent absolute values on k. Let* $b_1, b_2, \dots, b_J \in k$ *be any arbitrary elements in k and let* $\varepsilon > 0$*. Then there exist an* $a \in k$ *such that simultaneously*

$$|a - b_j|_j < \varepsilon \quad for\ J = 1,2,\dots,J.$$

Theorem 2.1.6 is closely related to the "Chinese Remainder Theorem" of elementary number theory.

Suppose that P is a nonarchimedean place of k containing the absolute value $|.|$, now define

$$\mathcal{O}_P = \{a \in k : |a| \leq 1\}$$

$$\mathcal{P}_P = \{a \in k : |a| < 1\}$$

$$\mathcal{U}_P = \{a \in k : |a| = 1\}$$

From Theorem 2.1.5 it follows that the sets $\mathcal{O}_P, \mathcal{P}_P$, and $\mathcal{U}_P$ are independent of the choice of any absolute value $|.|$ in P, but only depend on P. By the properties of the nonarchimedean absolute value $|.|$, it is easy to see that $\mathcal{O}_P$ is an integral domain with 1; it is called the **valuation ring at** $\boldsymbol{P}$ or the **ring of integers at** $\boldsymbol{P}$. Also $\mathcal{P}_P$ is a prime ideal (and the unique maximal ideal) in $\mathcal{O}_P$; it is called the **prime ideal at** $\boldsymbol{P}$. Then clearly $\mathcal{U}_P$ is the multiplicative group of invertible elements (group of units) of $\mathcal{O}_P$; it is called the **group of units at** $\boldsymbol{P}$.

We note that

$$k = \mathcal{O}_P \cup \mathcal{O}_P^{-1}, \text{ where } \mathcal{O}_P^{-1} = \{a^{-1} : a \in \mathcal{O}_P, a \neq 0\},$$

$$\mathcal{U}_P = \mathcal{O}_P \cap \mathcal{O}_P^{-1},$$

$$\mathcal{O}_P = \mathcal{P}_P \cup \mathcal{U}_P,$$

$$\mathcal{P}_P \cap \mathcal{U}_P = \emptyset,$$

Since $\mathcal{P}_P$ is the unique maximal ideal in $\mathcal{O}_P$, we obtain

$$\mathbb{F}_P = \mathcal{O}_P/\mathcal{P}_P$$

is a field and it is called the **residue class field at *P*.**

Note that for an archimedean place P, the sets $\mathcal{O}_P, \mathcal{P}_P$, and $\mathcal{U}_P$ can be defined as the closed unit disk, the open unit disk and the unit circle respectively but we will not discuss the structures of these sets. In the next section we will set another way through **valuation** to look at the nonarchimedean places.

2.2 Valuations

Definition 2.2

Let k be a field. A valuation is a function

$$v : k \to \mathbb{R} \cup \{\infty\}$$

such that

(i) $v(a) = \infty$ if and only if $a = 0$,

(ii) $v(a \cdot b) = v(a) + v(b)$ for all $a, b \in k$,

(iii) $v(a + b) \geq \min\{v(a), v(b)\}$ for all $a, b \in k$.

Let P be a nonarchimedean place of k and let $|.| \in P$ a nonarchimedean absolute value on k. Define

$$v(a) = -\log|a| \text{ for } a \in k, \text{so that } |a| = e^{-v(a)}.$$

It is easy to see that this defines a valuation on k and there is a 1-1 correspondence between the set of nonarchimedean absolute values on k and the set of valuations on k.
Recall the equivalence relation defined on absolute values. Connecting with valuations we say two valuations v and v' are equivalent if and only if the corresponding absolute values e^{-v} and $e^{-v'}$ are equivalent. By Theorem 2.1.5, $v \sim v'$ if and only if $v = \lambda\, v'$ for some $\lambda > 0, \lambda \in \mathbb{R}$. Now without any confusion we write $v \in P$ when $|.| = e^{-v} \in P$ and $P = \{\lambda v : \lambda > 0\}$. In terms of valuations we rewrite the sets $\mathcal{O}_P, \mathcal{P}_P,$ and $\mathcal{U}_P$ as

$$\mathcal{O}_P = \{a \in k : v(a) \geq 0\}$$

$$\mathcal{P}_P = \{a \in k : v(a) > 0\}$$

$$\mathcal{U}_P = \{a \in k : v(a) = 0\}$$

and these are independent of the choice of $v \in P$.

Any $v \in P$ defines a group homomorphism

$$v : k^{\times} \to \mathbb{R}^{+}$$

from the multiplicative group $k^{\times}$ to the additive group of the real numbers. Thus the image

$$v(k^{\times}) = \{v(a) : a \in k^{\times}\}$$

is a subgroup of $\mathbb{R}^{+}$ and called the additive value group of v.
If $v' \in P$ then $v'(k^{\times}) = \lambda\, v(k^{\times})$ for some $\lambda > 0$ and

$$v'(k^{\times}) \cong v(k^{\times})$$

an order isomorphism. Any subgroup of $\mathbb{R}^{+}$ is either discrete or dense in $\mathbb{R}^{+}$ and any discrete subgroup is either trivial or infinite cyclic. Since this does not depend on v, P is said to be discrete or non-discrete according to $v(k^{\times})$ is discrete or non-discrete in $\mathbb{R}^{+}$. For a non trivial discrete place P there exist $v_P \in P$ a unique **normalized valuation** such that $v_P(k^{\times}) = \mathbb{Z}$.

Let $k = \mathbb{Q}$, then any $a \in \mathbb{Q}$ can be expressed as

$$a = \pm \prod_{\text{all prime, } p \in \mathbb{Z}} p^{r_p}$$

where r_p = the exponent of p in the factorization of a (called the ordinal of a at $p = \text{ord}_p(a)$).

Define the function

$$v_p : \mathbb{Q}^\times \to \mathbb{Z}$$

such that

$$v_p(a) = r_p = \text{ord}_p(a) \text{ and } \quad v_p(0) = \infty,$$

then

$$v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$$

is a normalized valuation on $\mathbb{Q}$ and $|.| = e^{-v_p}$ is a nonarchimedean absolute value on $\mathbb{Q}$. Thus for $a \in \mathbb{Q}$ define the **normalized $p-$adic absolute value** by

$$|a|_p = \left(\frac{1}{p}\right)^{v_{p(a)}} \text{ with } |.|_p = |.|^\lambda,$$

where $\lambda = \log_e p > 0$.

Observe that for two distinct primes p and q we have

$$|p|_p = \frac{1}{p} < 1 \text{ and } |p|_q = 1.$$

So each prime $p \in \mathbb{Z}$ we have $|.|_p$ a nonarchimedian absolute value on $\mathbb{Q}$ and gives a set of inequivalent nonarchimedian absolute values on $\mathbb{Q}$. The ordinary absolute value

$$|a|_\infty = |a| \text{ for all } a \in \mathbb{Q}$$

is an archimedean absolute value on $\mathbb{Q}$ and we denote the place which $|.|_\infty$ determines by ∞. By a theorem of Ostrowski we observe that these are all the inequivalent absolute values of $\mathbb{Q}$. Now

we record this result, the set of inequivalent nontrivial absolute values equivalently saying the set of places of $\mathbb{Q}$ in the following theorem deduced from Theorem 1-4-1 in [30].

Theorem 2.2.1

Let $V_{\mathbb{Q}}$ be the set of places of $\mathbb{Q}$, then

$$V_{\mathbb{Q}} = \{\infty, 2, 3, 5, 7, 11, \dots, p, \dots\}.$$

Let $|.|_p$ be the absolute value corresponding to each place $p \in V_{\mathbb{Q}}$. Then for any $a \neq 0 \in \mathbb{Q}$ we have $|a|_p = 1$ for almost all $p \in V_{\mathbb{Q}}$ and

$$\prod_{p \in V_{\mathbb{Q}}} |a|_p = 1.$$

This is called the product formula for $\mathbb{Q}$.

Now immediately from the product formula we get

$$|a|_\infty = \prod_{p \neq \infty, p \in V_{\mathbb{Q}}} |a|_p^{-1}$$

For each place $p \in V_{\mathbb{Q}}$ the sets $\mathcal{O}_p, \mathcal{P}_p$, and $\mathcal{U}_p$ are

$$\mathcal{O}_p = \left\{\frac{m}{n} \in \mathbb{Q} : m, n \in \mathbb{Z}, \quad (m, n) = 1, \quad (n, p) = 1\right\}$$

$$\mathcal{P}_p = \left\{\frac{m}{n} \in \mathbb{Q} : m, n \in \mathbb{Z}, \quad (m, n) = 1, \quad (n, p) = 1, \quad p|m\right\}$$

$$\mathcal{U}_p = \left\{\frac{m}{n} \in \mathbb{Q} : m, n \in \mathbb{Z}, \quad (m, n) = 1, \quad (m, p) = (n, p) = 1\right\}$$

and the residue class field

$$\mathbb{F}_p = \mathcal{O}_p/\mathcal{P}_p \cong \mathbb{Z}/p\mathbb{Z}.$$

2.3 Extensions and Completions of Absolute Values

In this section we would like to study the connection between absolute values of a field and its extension field.

Let k, K be fields and $k \subset K$ (K is an extension field of k). Let $|.|_W$ be an absolute value on K belonging to the place $W \in V_K$, then it is clear that the restriction of $|.|_W$ on k is an absolute value on k. Note that there exists a one to one correspondence between the absolute values W in V_K and the absolute values w in V_k. We say W is an extension of w to K or w is a restriction of W on k and we denote this correspondence by $W|w$ $(i.e.\ |.|_w = |.|_W|k)$. Since the place W leads to a full place w on k and the one to one correspondence between the set of places $\mathfrak{M}(K)$ of K to the set of places $\mathfrak{M}(k)$ of k, it is immediate that W is archimedean (nonarchimedean) if and only if w is archimedean (nonarchimedean). Again for the nonarchimedean case writing $\mathcal{O}_w$, $\mathcal{O}_W$, $\mathcal{P}_w$, $\mathcal{P}_W$, $\mathcal{U}_w$, and $\mathcal{U}_W$ we get the residue class fields

$$\mathbb{F}_w = \mathcal{O}_w/\mathcal{P}_w,$$

$$\mathbb{F}_W = \mathcal{O}_W/\mathcal{P}_W.$$

Therefore the canonical mapping

$$\bar{\varphi} : \mathbb{F}_w \to \mathbb{F}_W$$

given by

$$\bar{\varphi}(a + \mathcal{P}_w) = a + \mathcal{P}_W$$

is a monomorphism thus $\bar{\varphi}$ is an inclusion.
Now we define

$$f = f\left(\frac{W}{w}\right) = [\mathbb{F}_W : \mathbb{F}_w],$$

the **degree of W over w**, or the residue class degree of K over k at W, and

$$e = e\left(\frac{W}{w}\right) = [v_W(K^\times): v_w(k^\times)] = [v_W(K^\times): v_W(k^\times)]$$

which is called the **ramification index of W over w**.

Completion 2.3.1

We say that $(k, |.|)$ is complete if k is a complete metric space with respect to the metric topology induced by the absolute value $|.|$. Let K be a field and let $|.|_K$ be an absolute value define on K, then we say the pair $(K, |.|_K)$ is a completion of the pair $(k, |.|)$ if and only if

(i) K is complete with respect to $|.|_K$,

(ii) There exists an isometric isomorphism of k onto a dense subfield of K.

We ask the question for a given field k and an absolute value $|.|$ does there exist a completion? The following theorem derived from Theorem 1-7-1 of [30] gives the existence and the uniqueness of the completion of a pair $(k, |.|)$.

Theorem 2.3.1

Let k be a field with absolute value $|.|_k$. Then there exist a completion $(K, |.|_K)$ of $(k, |.|_k)$ and it is unique up to isomorphism. If $(K, |.|_K)$ and $(L, |.|_L)$ are both completions of $(k, |.|_k)$ with isomorphisms μ_K and μ_L, then there exists a unique isomorphism

$$\mu : K \to L$$

which is an extension of the identity map

$$i : k \to k \qquad \text{such that} \qquad \mu \circ \mu_K = \mu_L.$$

Immediately for the nonarchimedean case if $(K, |.|_W)$ is a completion of $(k, |.|_w)$ then k is dense in K and for any $b \in \mathcal{O}_W$ there exist $a \in k$ such that $|a - b|_W < 1$.

$$|a|_w = |a - b + b|_W \leq \max\{|a - b|_W, |b|_W\} \leq 1$$

implies that $a \in \mathcal{O}_w$ and $a - b \in \mathcal{P}_W$, which leads to the proof of the following Lemma obtained from Proposition 1-7-5 of [30].

Lemma 2.3.1

Let $(K, |.|_W)$ is a completion of $(k, |.|_w)$ with a nonarchimedean place $w \in V_k$, then

$$e = e\left(\frac{W}{w}\right) = f = f\left(\frac{W}{w}\right) = 1.$$

Thus from lemma 2.3.1 we get

$$\mathbb{F}_w = \mathcal{O}_w/\mathcal{P}_w \cong \mathbb{F}_W = \mathcal{O}_W/\mathcal{P}_W$$

and

$$v_W(K^\times) = v_w(k^\times) = v_W(k^\times).$$

Let $v = v_w \in w$ be a discrete valuation of k. Let $\pi \in k$ such that $v(\pi) = 1$ then π called as a prime element of k with respect to v or a local uniformizing parameter. We note that if $|.|_v \in w$ the corresponding nonarchimedean absolute value of v then

$$|\pi|_v = \sup\{|a|_v : a \in \mathcal{P}_w\},$$

and

$$\mathcal{P}_w = \pi\mathcal{O}_w = \{\pi a : a \in \mathcal{O}_w\}.$$

For each integer $r > 0$,

$$\mathcal{P}_w^r = (\pi\mathcal{O}_w)^r = \{\pi^r a : a \in \mathcal{O}_w\} = \{b \in k : v(b) \geq r\}$$

is an ideal of $\mathcal{O}_w$ and if $\mathcal{P}_w^r = a\mathcal{O}_w$ for some $a \in k$ then $v(a) = r$. In fact it is easy to show that $\mathcal{O}_w$ is a principal ideal domain and in particular is a unique factorization domain with π as its only prime element.

For the archimedean case the following theorem stated as Theorem 1-8-3 of [30], characterizes the completion.

Theorem 2.3.2 (Ostrowski)

Let k be a field which is complete with respect to an archimedean absolute value $|.|_w \in w$ and $w \in V_k$. Then there exist an isomorphism σ of k onto either $\mathbb{R}$ or $\mathbb{C}$ such that

$$\sigma^*(w_\infty) = w,$$

where w_∞ is the infinite place determined by the usual absolute value $|.|_\infty$.

In the case of rational number field $\mathbb{Q}$, for each place

$$p \in \mathrm{V}_{\mathbb{Q}} = \{\infty, 2,3,5,7, \dots, p, \dots\}$$

there exist a unique completion $\mathbb{Q}_p$ such that $\mathbb{Q}_p = \mathbb{R}$ when $p = \infty$ and when $p \neq \infty$, $\mathbb{Q}_p$ is called the set of $p-$ adic numbers or the $p-$ adic completion of $\mathbb{Q}$.

2.4 Absolute Values on an Algebraic Number Field

Definition 2.4

Let $\mathbb{K}$ be a field with an absolute value $|.|_{\mathbb{K}}$ and Let $\mathfrak{X}$ be a vector space over the field $\mathbb{K}$. Then the function $\|.\| : \mathfrak{X} \to [0, \infty)$ is a norm if the following three properties are satisfied.

(i) $\|\vec{x}\| = 0$ if and only if $\vec{x} = 0$

(ii) $\|\vec{x} + \vec{y}\| \leq \|\vec{x}\| + \|\vec{y}\|$ For all $\vec{x}, \vec{y} \in \mathfrak{X}$

(iii) $\|\lambda\vec{x}\| = |\lambda|_{\mathbb{K}}\|\vec{x}\|$ For any $\vec{x} \in \mathfrak{X}$ and $\lambda \in \mathbb{K}$

If $\|.\|$ is a norm on $\mathfrak{X}$, then $\mathfrak{X}$ is a metric space with respect to the norm given by

$$d(\vec{x},\vec{y}) = \|\vec{x}-\vec{y}\|$$

thus induces a metric topology. We say two norms are equivalent if they induce the same topology. If $\|.\|_1$ and $\|.\|_2$ are two equivalent norms on $\mathfrak{X}$ then there exist two positive constants c_1 and c_2 such that for all $\vec{x} \in \mathfrak{X}$,

$$c_1\|\vec{v}\|_2 \leq \|\vec{v}\|_1 \leq c_2\|\vec{v}\|_2.$$

Suppose $\mathfrak{X}$ is a finite dimensional vector space over $\mathbb{K}$ with basis $\overrightarrow{x_1}, \overrightarrow{x_2}, \dots, \overrightarrow{x_n}$ then we define the canonical norm or the sup norm, $\|.\|_\infty$ as

$$\left\|\vec{X}\right\|_\infty = \|a_1\vec{x}_1 + a_2\vec{x}_2 + \cdots + a_n\vec{x}_n\|_\infty = \max\{|a_1|_{\mathbb{K}}, |a_2|_{\mathbb{K}}, \dots, |a_n|_{\mathbb{K}}\}.$$

We note here suppose k is a field and let $|.|$ is a nonarchimedean absolute value on k. Then for $c > 0$, and for $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in k[x]$ define

$$\|f\| = \max_{1\leq i\leq n} c^i|a_i| \quad \text{and for } f, g \in k[x] \quad \left\|\frac{f}{g}\right\| = \frac{\|f\|}{\|g\|}.$$

Then $\|.\|$ is a nonarchimedean absolute value on $k(x)$ (coinciding with$|.|$ on k). In particular we can take $c = 1$.

Theorem 2.4.1

Let $\mathfrak{X}$ be a finite dimensional vector space over a field $\mathbb{K}$ and let $\mathbb{K}$ be complete with respect to an absolute value $|.|_{\mathbb{K}}$. Then any two norms $\|.\|_1$ and $\|.\|_2$ on $\mathfrak{X}$ are equivalent and $\mathfrak{X}$ is complete with respect to the metric induced by the norm.

Theorem 2.4.1 is stated as Lemma 2.1 in Chapter 7 of [6].

Suppose $\mathbb{L} \supset \mathbb{K}$ finite galois extension and $|.|_{\mathbb{K}}$ an absolute value on $\mathbb{K}$. By the above theorem there exist a unique extension $\|.\|$, of $|.|_{\mathbb{K}}$ to $\mathbb{L}$ and if $\sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$ then $\|.\|_\sigma$ defined by

$$\|\alpha\|_\sigma = \|\sigma(\alpha)\|$$

is also a an extension of $|.|_{\mathbb{K}}$ to $\mathbb{L}$. Thus $\|.\|_\sigma = \|.\|$ implies

$$\|\alpha\|_\sigma = \|\sigma(\alpha)\| = \|\alpha\| \quad \text{for all } \alpha \in \mathbb{L},$$

and for each $\sigma_i \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$ for $i = 1,2,\dots,n$,

$$\mathrm{Norm}_{\mathbb{L}/\mathbb{K}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) = \sigma_1(\alpha) \dots \sigma_n(\alpha).$$

Hence we get

$$\left|\mathrm{Norm}_{\mathbb{L}/\mathbb{K}}(\alpha)\right|_{\mathbb{K}} = \left\|\prod_{i=1}^{n} \sigma_i(\alpha)\right\| = \|\sigma_1(\alpha)\| \dots \|\sigma_n(\alpha)\|$$

$$= \|\alpha\|^n.$$

Now we need an understanding of how an absolute value can be extended in a finite extension of a complete field k. The following theorem, Theorem 1.1 of Chapter 7 in [6] tells us there is a unique way to extend an absolute value on a complete field.

Theorem 2.4.2

Let k be a complete field with respect to an absolute value $|.|_k$ and let K a finite extension of degree n (i.e $[K:k] = n$). Then there exists a unique absolute value $|.|_K$ on K, that extends $|.|_k$ on k. It is given by

$$|\xi|_K = \left|Norm_{K/k}(\xi)\right|_k^{1/n}$$

for all $\xi \in K$ and K is complete with respect to the metric topology induced by $|.|_K$.

We would like to take our discussion to algebraic number fields (a finite extension of the rational number field $\mathbb{Q}$) through a more general set up where $\mathbb{E}$ is a finite extension of $\mathbb{K}$. Then we want to know for any place $w \in V_{\mathbb{K}}$ do there exist extensions of w to $\mathbb{E}$? If so how many? Since our interest is on algebraic number fields we would like to answer these questions more carefully in the following section. We will make a significant use of this section in our main results. The following theorem is a careful use of some of the above results.

Theorem 2.4.3

Suppose $\mathbb{K}$ *is complete with respect to an absolute value* $|.|_{\mathbb{K}}$ *and suppose*

$$f_\alpha(x) = \prod_{i=1}^{n}(x - \alpha_i) \in \mathbb{K}[x]$$

is the minimal polynomial for α *over* $\mathbb{K}$*. Then for*

$$\xi = \sum_{i=1}^{n-1} a_i\, \alpha^i \in \mathbb{K}(\alpha) \text{ with } a_i \in \mathbb{K},$$

the unique extension of $|.|_{\mathbb{K}}$ *to* $\mathbb{K}(\alpha)$ *(say* $\|.\|$*) is given by*

$$\|\xi\| = \left|\prod_{j=1}^{n}\left(\sum_{i=1}^{n-1} a_i\, \alpha_j^i\right)\right|_{\mathbb{K}}^{1/n}.$$

Let k be a field with an absolute value $|.|_w$ corresponding to the place $w \in V_k$ and let $\mathbb{K} = k_w$ be the completion of k with respect to $|.|_w$. Let $\alpha \in \bar{k}$ the algebraic closure of k and let $f_\alpha(x) \in k[x]$ be the minimal polynomial of α over k of degree n. Let $K = k(\alpha)$ and let

$$f_\alpha(x) = \prod_{i=1}^{n}(x - \alpha_i)$$

be the factorization of the minimal polynomial of α over $\bar{k}_w = \overline{\mathbb{K}}$, the algebraic closure of $\mathbb{K}$. Now taking $\mathbb{L} = k_w(\alpha_1, \ldots, \alpha_n)$ where $\alpha_i \in \bar{k}_w$, we know that the absolute value $|.|_w$ can be uniquely extend to $\mathbb{L}$ (say $\|.\|$) as

$$\|\beta\| = \left|\mathrm{Norm}_{\mathbb{L}/\mathbb{K}}(\beta)\right|_w^{1/[\mathbb{L}:\mathbb{K}]} \quad \text{for } \beta \in \mathbb{L}.$$

Let

$$\varphi : k(\alpha) = K \to \mathbb{L}$$

be defined by

$$\varphi\left(\sum_{i=0}^{n-1} a_i\alpha^i\right) = \sum_{i=0}^{n-1} a_i\varphi(\alpha)^i$$

be an embedding of $k(\alpha) = K$ into $\mathbb{L}$.

Since $\varphi\big(f_\alpha(x)\big) = f_\alpha(x)$ we have $\varphi(\alpha)$ is also a zero of $f_\alpha(x)$. Thus we get exactly n different embeddings such that

$$\varphi_i(\alpha) = \alpha_i \quad \text{for } i = 1,2,\dots,n.$$

Now we can define absolute values on $k(\alpha) = K$ such that for $l = 1,2,\dots,n$

$$\left|\sum_{i=0}^{n-1} a_i\alpha^i\right|_l = \left\|\varphi_l\left(\sum_{i=0}^{n-1} a_i\alpha^i\right)\right\| = \left\|\sum_{i=0}^{n-1} a_i\varphi_l(\alpha)^i\right\|$$

$$= \left\|\sum_{i=0}^{n-1} a_i\alpha_l^i\right\|$$

$$= \left|\mathrm{Norm}_{\mathbb{L}/\mathbb{K}}\left(\sum_{i=0}^{n-1} a_i\alpha_l^i\right)\right|_w^{1/[\mathbb{L}:\mathbb{K}]}.$$

Suppose

$$f_\alpha(x) = \prod_{j=1}^{J} s_j(x)$$

factors into J irreducible factors in $k_W[x] = \mathbb{K}[x]$ and if α_1 and α_2 are zeros of the same irreducible factor then they generate the same absolute value. If α_1 and α_2 are zeros of different irreducible factors then they generate inequivalent absolute values. This means there are J ways

to extend the place w in $k_W(\alpha)$. We now state the theorems on $\mathbb{Q}$ which is our main interest of the section.

Let $\mathbb{K}$ be a algebraic number field of degree d over $\mathbb{Q}$. Let $W \in V_{\mathbb{K}}$ be a place of $\mathbb{K}$ and let w be the place of $\mathbb{Q}$ to which W is restricted. Then the local degree of W is defined as

$$d_W = [\mathbb{K}_W : \mathbb{Q}_w]$$

where $\mathbb{K}_W$ and $\mathbb{Q}_w$ are the completions of $\mathbb{K}$ and $\mathbb{Q}$ with respect to the places W and w . Then we have

$$\sum_{W \in V_{\mathbb{K}}, W|w} [\mathbb{K}_W : \mathbb{Q}_w] = \sum_{W \in V_{\mathbb{K}}, W|w} d_W = [\mathbb{K} : \mathbb{Q}] = d \qquad (2.4.4)$$

We examine the two absolute values within $\mathfrak{M}(\mathbb{K})$, which are the archimedean and the nonarchimedean. If W is archimedean then there exist a unique absolute value $\|.\|_W \in W$ that restricts to the usual absolute value $|.|_\infty$ on $\mathbb{Q}$. If W is nonarchimedean then there exist a prime $p \in \mathbb{Q}$ such that W restricts to the $p-$ adic place of $\mathbb{Q}$ and we let $\|.\|_W$ be the unique absolute value in W that restricts the $p-$ adic absolute value $|.|_p$ on $\mathbb{Q}$. We now define a second normalized equivalent absolute value $|.|_W$ for any place $W \in V_{\mathbb{K}}$ achimedean or nonarchimedean as,

$$|.|_W = \|.\|_W^{d_W/d}.$$

Suppose $\mathbb{K}, \mathbb{E}$ are algebraic number fields and $\mathbb{K} \subseteq \mathbb{E}$. For an archimedean (or nonarchimedean) place w of $\mathbb{K}$ and for an archimedean (or nonarchimedean) place W of $\mathbb{E}$ such that W restricts to w on $\mathbb{K}$, we would like to see the explicit relation between $\|.\|_W$ and $\|.\|_w$. The following theorem deduced from Lemma 2.1 in proving a more general Theorem (1.1) in Chapter 9 of [6] gives the characterization as a summarized result.

Theorem 2.4.4

Let $\mathbb{K} \subseteq \mathbb{E}$ *be an extension of algebraic number fields. Let* $\alpha \in \mathbb{E}$ *such that* $\mathbb{E} = \mathbb{K}(\alpha)$. *Let* w *be an archimedean (or nonarchimedean) place of* $\mathbb{K}$ *and* W *an archimedean (or nonarchimedean) place of* $\mathbb{E}$ *such that* W *restricts to* w *on* $\mathbb{K}$. *Let* $\mathbb{K}_w$ *be the completion of* $\mathbb{K}$ *with respect to* w *and let* $\widehat{\|.\|}_w$ *be the extension of* $\|.\|_w$ *on* $\mathbb{K}$ *to* $\mathbb{K}_w$.

Let

$$f_\alpha(x) = \prod_{j=1}^{J} s_j(x)$$

be the unique factorization of the minimal polynomial of α *over* $\mathbb{K}[x]$, *into distinct monic irreducibles* $s_j(x)$ *in* $\mathbb{K}_w[x]$. *For* α_j *a root of* $s_j(x)$ *let* $\mathbb{E}_j = \mathbb{K}_w(\alpha_j)$ *and let* $\widehat{\|.\|}_{W_j}$ *be the unique extension of* $\widehat{\|.\|}_w$ *to* $\mathbb{E}_j$. *Then* $\mathbb{E}$ *is embedded as a dense subfield of the complete field* $\mathbb{E}_j$ *by*

$$\mathbb{K}(\alpha) = \mathbb{E} \hookrightarrow \mathbb{E}_j = \mathbb{K}_w(\alpha_j) \quad with \quad \alpha \mapsto \alpha_j$$

which is an extension of $\mathbb{K} \hookrightarrow \mathbb{K}_w$. *The restriction* $\|.\|_{W_j}$ *of* $\widehat{\|.\|}_{W_j}$ *to* $\mathbb{E}$ *is an archimedean (or nonarchimedean) absolute value which is further restrict to* $\|.\|_w$ *on* $\mathbb{K}$. *The absolute values* $\|.\|_{W_j}$ *are distinct and every absolute value on* $\mathbb{E}$ *restricting to* $\|.\|_w$ *on* $\mathbb{K}$ *corresponds to one of these.*

In the archimedean case we look at $\mathbb{K}$ as a subfield of the complex field $\mathbb{C}$. Let r_1 be the number of real embeddings and r_2 the number of complex embeddings. Since the complex embeddings are of degree two we have $d = r_1 + 2r_2$. We state the following corollary to illustrate the Theorem 2.4.4 on the archimedean places.

Corollary 2.4.4

Let $|.|_\infty$ *be the usual archimedean absolute value on* $\mathbb{Q}$. *Let* $\mathbb{K}$ *be an algebraic number field of degree* d *over* $\mathbb{Q}$ *and let* $g_1, g_2, g_3, \dots, g_{r_1}$ *be the real isomorphisms and* $(g_{r_1+1}, g_{r_1+r_2+1}), \dots, (g_{r_1+r_2}, g_d)$ *the pairs of complex conjugate isomorphisms of* $\mathbb{K}$ *into* $\mathbb{C}$ *we then obtain all the extensions* $\|.\|_W$ *of* $|.|_\infty$ *to* $\mathbb{K}$ *by*

$$\|\alpha\|_W = \|g_i(\alpha)\|_\infty \text{ for } \alpha \in \mathbb{K}, i = 1,2, \dots, r_1 + r_2.$$

Let us look at the following example to see the explicit description of archimedean places on $\mathbb{K}$. We denote the usual absolute value on $\mathbb{C}$ by $\|.\|_\infty$.

Let $\mathbb{K} = \mathbb{Q}$ and $\alpha = \sqrt[4]{3}$ then $\mathbb{E} = \mathbb{Q}(\alpha)$ and the minimal polynomial of $\sqrt[4]{3}$ over $\mathbb{Q}[x]$ is $f(x) = x^4 - 2$. Since $\mathbb{R} = \mathbb{Q}_\infty$ is completion of $\mathbb{Q}$ with respect to the usual absolute value $\|.\|_\infty$, we note $f(x) = x^4 - 3 = \left(x^2 + \sqrt{3}\right)\left(x - \sqrt[4]{3}\right)\left(x + \sqrt[4]{3}\right)$ is the factorization over $\mathbb{R}$. Therefore for each root we get an embedding from $\mathbb{Q}(\alpha)$ into $\mathbb{C}$ precisely by $\alpha \to \sqrt[4]{3}$, or $\alpha \to -\sqrt[4]{3}$, or $\alpha \to i\sqrt[4]{3}$, or $\alpha \to -i\sqrt[4]{3}$. Note the last two complex embeddings correspond to the same irreducible factor and thus give the same absolute value. Therefore we get three distinct archimedean absolute values on $\mathbb{Q}(\alpha)$ corresponding to those three irreducible factors, namely

$\|a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3\|_{W_1} = \|a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3\|_\infty$, as $\alpha \to \sqrt[4]{3}$ and $[\mathbb{R}(\alpha):\mathbb{R}] = 1$,

$\|a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3\|_{W_2} = \|a_0 - a_1\alpha + a_2\alpha^2 - a_3\alpha^3\|_\infty$, as $\alpha \to -\sqrt[4]{3}$, $[\mathbb{R}(\alpha):\mathbb{R}] = 1$,

$\|a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3\|_{W_3}$

$= \|(a_0 + a_1\alpha i - a_2\alpha^2 - a_3\alpha^3 i)(a_0 - a_1\alpha i - a_2\alpha^2 + a_3\alpha^3 i)\|_\infty^{\frac{1}{2}}$ as $\alpha \to i\sqrt[4]{3}$, $[\mathbb{R}(\alpha):\mathbb{R}] = 2$,

and the normalized archimedean absolute values

$$|a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3|_{W_1} = \|a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3\|_\infty^{1/4},$$
$$|a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3|_{W_2} = \|a_0 - a_1\alpha + a_2\alpha^2 - a_3\alpha^3\|_\infty^{1/4},$$
$$|a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3|_{W_3}$$
$$= \|(a_0 + a_1\alpha i - a_2\alpha^2 - a_3\alpha^3 i)(a_0 - a_1\alpha i - a_2\alpha^2 + a_3\alpha^3 i)\|_\infty^{\frac{1}{4}}$$

Let $\mathbb{K}$ be a number field and let p be any place on $\mathbb{Q}$ (i.e. $p \in \{\infty, 2,3,5, \dots, p, \dots\}$). Now let

$$\mathcal{A}(p) = \{W_1, W_2, \dots, W_l\}$$

denote the set of places of $\mathbb{K}$ restricting to the $p-$adic place on $\mathbb{Q}$. From equation (2.4.4) we have the following identity

$$\sum_{W \in \mathcal{A}(p)} d_W = d$$

For $\alpha \in \mathbb{K}$ we have

$$\text{Norm}_{\mathbb{K}/\mathbb{Q}}(\alpha) = \prod_{W \in \mathcal{A}(p)} \text{Norm}_{\mathbb{K}_W/\mathbb{Q}_p}(\alpha)$$

and by using Theorem (2.4.2) we have for $W \in \mathcal{A}(p)$,

$$\|\alpha\|_W = \left|\text{Norm}_{\mathbb{K}_W/\mathbb{Q}_p}(\alpha)\right|_p^{1/d_W}$$

and since

$$|\alpha|_W = \|\alpha\|_W^{d_W/d}$$

we have

$$|\alpha|_W = \|\alpha\|_W^{d_W/d} = \left|\text{Norm}_{\mathbb{K}_W/\mathbb{Q}_p}(\alpha)\right|_p^{1/d}$$

from this we obtain the identity

$$\left|\text{Norm}_{\mathbb{K}/\mathbb{Q}}(\alpha)\right|_p^{1/d} = \prod_{W \in \mathcal{A}(p)} |\alpha|_W$$

Let $\alpha \in \overline{\mathbb{Q}}^{\times}$, let $\mathbb{K}$ be an algebraic number field containing α, let $V_{\mathbb{K}}$ be the set of places of $\mathbb{K}$, let $V_{\mathbb{Q}}$ be the set of places of $\mathbb{Q}$ and for $p \in V_{\mathbb{Q}}$, let $\mathcal{A}(p)$ be the set of places of $\mathbb{K}$ that restrict to p on $\mathbb{Q}$. Then

$$\prod_{V_{\mathbb{K}}} |\alpha|_W = \prod_{p \in V_{\mathbb{Q}}} \left\{ \prod_{W \in \mathcal{A}(p), W|p} |\alpha|_W \right\}$$

$$= \left\{ \prod_{V_{\mathbb{K}}} \left| \mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(\alpha) \right|_p \right\}^{1/d}$$

$$= 1$$

This powerful result we record as the following theorem and refer to it as the product formula.

Theorem 2.4.5

Let $\mathbb{K}$ be an algebraic number field, $\alpha \in \mathbb{K}^{\times}$ and let $V_{\mathbb{K}}$ be the set of normalized places of $\mathbb{K}$. Then

$$\prod_{W \in V_{\mathbb{K}}} |\alpha|_W = 1.$$

Now we prove the following theorem (Theorem2.4.6) with the use of the weak approximation theorem (Theorem 2.1.6). This theorem becomes an essential tool in our main theorems in Chapter 3.

Theorem (2.4.6)

Suppose that α is a non zero element in an algebraic number field k and S a finite set of places on k. Then there exists an algebraic integer β in k such that $\alpha\beta$ is an algebraic integer and

$$|\beta|_v = \frac{1}{\max\{1, |\alpha|_v\}}$$

for each $v \in S$.

Proof.

Let P denote the set of primes p such that either $v|p$ for some v in S, or $v|p$ and $|\alpha|_v > 1$, and let S_0 denote the set of places w on k with $w|p$ for some $p \in P$ (in particular $S \subseteq S_0$ and $|\alpha|_v \leq 1$ for all $v \notin S_0$). By the weak Approximation Theorem (Theorem 2.1.6), there exists $\beta_0 \in k$ with

$$|\beta_0 - \alpha^{-1}|_w < |\alpha|_w^{-1} \text{ if } |\alpha|_w > 1$$

and

$$|\beta_0 - 1|_w < 1 \text{ if } |\alpha|_w \leq 1$$

for all w in S_0.

Note that

$$|\beta_0|_w = \frac{1}{\max\{1, |\alpha|_w\}}$$

and $|\alpha\beta_0|_w \leq 1$ for all $w \in S_0$. Let Q denote the primes q such that $|\beta_0|_w > 1$ for some $w|q$ (note $Q \cap S_0 = \emptyset$). By the Chinese Remainder Theorem, there is an integer n such that $n \equiv 0 (\text{mod } q^{\alpha_p})$ for $q \in Q$ and $n \equiv 1 (\text{mod } q^{\alpha_p})$ for $q \in P$, with the α_q chosen large enough so that

$$|q|_w^{\alpha_q} |\beta_0|_w < 1$$

for all $w|q$ and $q \in Q$, and

$$|q|_w^{\alpha_q} |\beta_0|_w < \frac{1}{\max\{1, |\alpha|_w\}}$$

for all $w|q$ and $q \in P$.

Now $\beta = n\beta_0$ will satisfy $|\beta|_w = |n|_w |\beta_0|_w \leq 1$ for $w|q$, $q \in Q$, $|\beta|_w \leq |\beta_0|_w \leq 1$ for $w|q$, $q \notin Q \cup S_0$, and

$$|\beta|_w = |(n-1)\beta_0 + \beta_0|_w = |\beta_0|_w = \frac{1}{\max\{1, |\alpha|_w\}}$$

for $w|q$, $q \in S_0$.

Thus $|\beta|_v \leq 1$ and $|\alpha\beta|_v \leq 1$ for all $v \nmid \infty$, and β and $\alpha\beta$ are algebraic integers, as claimed.

CHAPTER 3 - **MAHLER MEASURE AND ABSOLUTE WEIL HEIGHT**

3.1 The Mahler Measure

Definition 3.1

The Mahler measure of a non zero polynomial

$$f(x) = a\prod_{i=1}^{d}(x-\alpha_i) \in \mathbb{Z}[x]$$

denoted by $M(f)$ is defined as

$$M(f) = \exp\left(\int_0^1 \log\left\|f\left(e^{2\pi i\theta}\right)\right\|_\infty d\theta\right). \tag{3.1.1}$$

Here $\|.\|_\infty$ denotes the usual archimedean absolute value on $\mathbb{C}$.

The Mahler measure of the zero polynomial is zero, $M(0) = 0$. If

$$f(x) = ax^l\prod_{i=1}^{d}(x-\alpha_i) \in \mathbb{Z}[x],$$

then from the Jensen's formula we get

$$\int_0^1 \log\left\|f\left(e^{2\pi i\theta}\right)\right\|_\infty d\theta = \log\|a\|_\infty + \sum_{i=1}^{d}\log(\max\{\|\alpha_i\|_\infty, 1\}) \tag{3.1.2}$$

Thus (3.1.1) and (3.1.2) gives the following lemma.

Lemma 3.1 (Mahler [19])

Let

$$f(x) = a\prod_{i=1}^{d}(x-\alpha_i) \in \mathbb{Z}[x],$$

Then

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

We always get $M(f) \geq 1$ *and in particular if*

$$f(x) = \sum_{j=0}^{d} a_j x^j \in \mathbb{Z}[x] \text{ and } a_d, \text{ or } a_0 \neq \pm 1$$

then $M(f) \geq 2$.

Some Properties of Mahler Measure (see [25])

(i) If $f_1(x)$and $f_2(x)$ are two non zero integer polynomials then,

$$M\big(f_1(x).f_2(x)\big) = M\big(f_1(x)\big).M\big(f_2(x)\big)$$

(ii) $M\big(f(x^n)\big) = M\big(f(x)\big)$

(iii) For an integer polynomial $f(x)$ we define the reciprocal of $f(x)$ as

$x^d f\left(\frac{1}{x}\right)$. Then $M\left(x^d f\left(\frac{1}{x}\right)\right) = M\big(f(x)\big)$.

Let

$$f(x) = a_d\prod_{i=1}^{d}(x-\alpha_i) = \sum_{j=0}^{d} a_j x^j \in \mathbb{Z}[x].$$

We define the length and the height of the polynomial

$$\mathcal{L}(f) = \sum_{j=0}^{d} \|a_j\|_\infty,$$

and

$$\mathcal{H}(f) = \left\{ \sum_{j=0}^{d} \|a_j\|_\infty^2 \right\}^{1/2}.$$

Letting

$$\mathcal{V}(f) = \sup_{\|x\|_\infty = 1} \|f(x)\|_\infty,$$

we obtain the bounds

$$M(f) \leq \mathcal{H}(f) \leq \mathcal{V}(f) \leq \mathcal{L}(f) \leq 2^d M(f).$$

Thus we get the bounds for $M(f)$ as

$$2^{-d}\mathcal{V}(f) \leq M(f) \leq \mathcal{V}(f),$$

and

$$2^{-d}\mathcal{H}(f) \leq M(f) \leq \mathcal{H}(f).$$

It is not difficult to see that for a given C and D the set of polynomials in $\mathbb{Z}[x]$ with $M(f) < C$ and $\deg(f) \leq D$ is finite. Equivalently saying that the following set

$$\{f(x) \in \mathbb{Z}[x] : M(f) < C \text{ and } \deg(f) \leq D\} \text{ is finite.}$$

Definition 3.1.2

For an algebraic number $\alpha \in \overline{\mathbb{Q}}^\times$, suppose $f(x) \in \mathbb{Z}[x]$ is an irreducible polynomial with integer coefficients and $f(\alpha) = 0$. Then the Mahler measure of the algebraic number α denoted by $M(\alpha)$, is defined as, $M(\alpha) = M\big(f_\alpha(x)\big)$.

For an algebraic integer $\alpha \in \overline{\mathbb{Q}}^{\times}$, let $\alpha = \alpha_1, \alpha_2, \dots, \alpha_d$ be the conjugates of α and define

$$\overline{|\alpha|} = \max_{1 \le j \le d} \|\alpha_j\|_{\infty}.$$

Then we get for an algebraic integer $\alpha \neq 0$

$$\overline{|\alpha|} \le M(\alpha) \le \overline{|\alpha|}^d.$$

Theorem 3.1.3 (Kronecker's Theorem)

If $f(x) \in \mathbb{Z}[x]$ has $M(f) = 1$ then all the nonzero roots of $f(x)$ must be roots of unity.

Proof.

Let $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ be all the nonzero roots of $f(x)$. Since $M(f) = 1$ we have all the α_i's are algebraic integers and $\|\alpha_i\|_{\infty} \le 1$. For any $k \in \mathbb{N}$, consider the polynomial

$$F_k(x) = \prod_{i=1}^{n} \left(x - \alpha_i^k\right) \in \mathbb{Z}[x]$$

(note the coefficient a_j of $F_k(x)$ are symmetric rational functions of α_i's thus they are rational integers), then the coefficients a_j of $F_k(x)$ satisfy

$$\|a_j\|_{\infty} = \left\| \sum_{\text{product of } j \ \alpha_i^k\text{'s}} \alpha_{i_1}^k \alpha_{i_2}^k \dots \alpha_{i_j}^k \right\|_{\infty} \le \sum_{j \text{ chosen from } n} 1 = \binom{n}{j}.$$

Therefore the a_j's are bounded for all $k \in \mathbb{N}$ and thus $F_1(x), F_2(x), F_2(x), \dots$ can take on only finite number of different polynomials. In particular their roots α_i^k's comes from a finite set of values. Thus for any i we must have $\alpha_i^{k_1} = \alpha_i^{k_2}$ for some $k_1 \neq k_2 \in \mathbb{N}$. This implies that $\alpha_i^{k_1 - k_2} = 1$.

■

Note that if $\alpha = 0$ then $M(\alpha) = 1$. Thus we get from the above theorem if $\alpha \in \overline{\mathbb{Q}}^{\times}$, and α is not a root of unity then $M(\alpha) > 1$.

Definition 3.1.3

An integer polynomial $f(x) \in \mathbb{Z}[x]$ of degree d is said to be reciprocal if $f(x)$ is equal to its reciprocal, equivalently saying,

$$f(x) = x^d f\left(\frac{1}{x}\right).$$

3.2 Lehmer's Problem

D.H. Lehmer (in 1933) asked the following question.

For a given $\varepsilon > 0$ does there exist a polynomial $f(x) \in \mathbb{Z}[x]$ with integer coefficients such that

$$1 < M\big(f(x)\big) < 1 + \varepsilon\,?$$

This is known as **Lehmer's Problem**.

If $f(x) \in \mathbb{Z}[x], f(0) \neq 0$ is non-cyclotomic then Lehmer's problem can be reformulated as, Does there exist a positive constant c_0 such that

$$M(f) > 1 + c_0\,?$$

The Mahler measure of the Lehmer polynomial,

$$l(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$$

with $M(l) = 1.176280\ldots$ remains as the smallest known Mahler measure (other than 1) to date. It was first discovered by D.H. Lehmer.

Schinzel and Zassenhaus made the first progress in 1965, toward answering the Lehmer problem. If α is an algebraic number with conjugates $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_d$ then

$$\max_{1 \le i \le d} \|\alpha_i\|_\infty > 1 + 4^{-s-2},$$

where $2s$ is the number of complex conjugates of α. This implies that

$$M(\alpha) > 1 + c_1/2^d$$

for a positive constant c_1. Also they had the following conjecture.

Schinzel-Zassenhaus Conjecture

If α is an algebraic integer with conjugates $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_d$ then there exists a positive constant c such that

$$\max_{1 \le i \le d} \|\alpha_i\|_\infty > 1 + \frac{c}{d}.$$

3.3 Some Known Bounds on Mahler Measure

Theorem 3.3.1 (Dobrowolski 1979 [8])

Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible and non-cyclotomic polynomial of degree d with $f(0) \neq 0$. Then for each $\varepsilon > 0$ there exist a positive integer $d(\varepsilon)$ such that for all $d > d(\varepsilon)$,

$$M(f) \geq 1 + (1 - \varepsilon)\left(\frac{\log\log d}{\log d}\right)^3.$$

Moreover Dobrowolski claims that for $d \geq 2$,

$$M(f) \geq 1 + \frac{1}{1200}\left(\frac{\log\log d}{\log d}\right)^3.$$

Theorem 3.3.2 (Smyth 1971 [27])

If $f(x) \in \mathbb{Z}[x]$ is a nonreciprocal irreducible polynomial with $f(x) \neq x, x - 1$, then

$$M(f) \geq \theta_0$$

where $\theta_0 = 1.3247 \ldots = M(x^3 - x - 1)$.

J. Garza [13] proved in the following theorem that, $\theta_0 = 1.3247 \ldots = M(x^3 - x - 1)$ is the lower bound for some other class of polynomials.

Theorem 3.3.3 (J. Garza 2008 [13])

Amongst all polynomials in $\mathbb{Z}[x]$ *whose splitting fields are contained in a dihedral Galois extension of* $\mathbb{Q}$*, the lowest Mahler measure (other than 1) is attained by* $x^3 - x - 1$.

In the next section we bring our attention to absolute Weil heights of algebraic numbers and draw the connection between absolute Weil height and Mahler measure. This will allow us to restate the Lehmer Problem in a new direction which we will be referring to in the rest of our discussion.

3.4 Absolute Weil Height

Let k be an algebraic number field and let $\|.\|_w$ be an absolute value on k. Let

$$\vec{x} = (x_1, x_2, \dots, x_N) \in k^N.$$

Then we can extend the absolute value $\|.\|_w \in w$ to a norm on k^N such that

$$\|\vec{x}\|_w = \max_{1 \le i \le N} \|x_i\|_w \quad \text{for all } w \in V_k$$

and

$$|\vec{x}|_w = \|\vec{x}\|_w^{d_w/d}.$$

Now we define the homogeneous height of $\vec{x} \in k^N$ as

$$H_1(\vec{x}) = \prod_{w \in V_k} |\vec{x}|_w.$$

Since the homogeneous height is a well defined function on $\overline{\mathbb{Q}}^N$, regardless of the number field k which contains α, we have that the homogeneous height definition is independent of the field. This means if $\vec{x} = (x_1, x_2, \dots, x_N) \in k^N \subseteq K^N$ then we get

$$H_1(\vec{x}) = \prod_{w \in V_k} |\vec{x}|_w = \prod_{w \in V_k} \prod_{W \in V_K, W|w} |\vec{x}|_W = \prod_{W \in V_K} |\vec{x}|_W.$$

Then by the product formula $H_1(\lambda\vec{x}) = H_1(\vec{x})$ for any $\lambda \in k$. The inhomogeneous height is defined as

$$H(\vec{x}) = \prod_{w \in V_k} \max\{1, |\vec{x}|_w\} = H_1(x_1, x_2, \dots, x_N, 1)$$

and when $N = 1$ we define the **absolute Weil height** as,

$$H(\alpha) = \prod_{w \in V_k} \max\{1, |\alpha|_w\}.$$

Since the homogeneous height is independent of the field k containing α we also have the absolute Weil height is independent of the field chosen.

To see the relation between absolute Weil height of an algebraic number $\alpha \in \overline{\mathbb{Q}}^{\times}$ and the Mahler measure of the algebraic number α we state the following leaam.

Theorem 3.4

Let $\alpha \in \overline{\mathbb{Q}}^{\times}$ be an algebraic number and let $k = \mathbb{Q}(\alpha = \alpha_1, \alpha_2, \dots, \alpha_d)$ where the α_i's are the Galois conjugates. Then for the archimedean places we have

$$\prod_{w \in V_k, w|\infty} \max\{1, |\alpha|_w\} = \prod_{i=1}^{d} \max\{1, \|\alpha_i\|_{\infty}\}^{1/d},$$

while for a prime p we have

$$\prod_{w \in V_k, w|p} \max\{1, |\alpha|_w\} = \frac{1}{\|a_d\|_p^{1/d}},$$

where a_d is the leading coefficient of the integer minimal polynomial of α. Thus

$$H(\alpha) = M(\alpha)^{1/d}.$$

Proof.

let

$$f_\alpha(x) = a_d \prod_{i=1}^{d} (x - \alpha_i) \in \mathbb{Z}[x]$$

be an irreducible polynomial (a minimal polynomial with integer coefficients) and $f_\alpha(\alpha) = 0$. Recall that if $|.|_w$ is an absolute value on k and $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(k)$ then $|x|_{\sigma w} = |\sigma(x)|_w$ is also an absolute value. Now take $k = \mathbb{Q}(\alpha = \alpha_1, \alpha_2, \dots, \alpha_d)$ then by the definition of $H(\alpha)$ we have

$$H(\alpha) = \prod_{w \in V_k, w|\infty} \max\{1, |\alpha|_w\} \prod_{w \in V_k, w \nmid \infty} \max\{1, |\alpha|_w\}.$$

For the archimedean places $w|\infty$,

$$\prod_{w \in V_k, w|\infty} \max\{1, |\alpha|_w\} = \prod_{\alpha_i \text{ real}} \max\{1, |\alpha_i|_w\}^{1/d} \prod_{\alpha_i, \overline{\alpha}_i \text{ complex}} \max\{1, |\alpha_i|_w\}^{2/d}$$

$$= \prod_{i=1}^{d} \max\{1, \|\alpha_i\|_\infty\}^{1/d}.$$

For the nonarchimedean places $w \nmid \infty$, recall if $f(x) = a_0 + a_1 + \cdots + a_n x^n \in k[x]$ then

$$\|f(x)\|_w = \|a_0 + a_1 + \cdots + a_n x^n\|_w = \max_{1 \le i \le n} \{\|a_i\|_w\}$$

is an absolute value on $k[x]$. Thus

$$\prod_{w \in V_k, w|p} \max\{1, |\alpha|_w\}^d = \prod_{i=1}^{d} \prod_{w \in V_k, w|p} \max\{1, |\alpha_i|_w\} = \prod_{w \in V_k, w|p} \prod_{i=1}^{d} |x - \alpha_i|_w$$

$$= \prod_{w \in V_k, w|p} \left\| \prod_{i=1}^{d} (x - \alpha_i) \right\|_w^{d_w/d} = \prod_{w \in V_k, w|p} \left\| \frac{f(x)}{a_d} \right\|_p^{d_w/d} = \left\| \frac{f(x)}{a_d} \right\|_p^{\sum d_w/d}$$

$$= \left\| \frac{f(x)}{a_d} \right\|_p.$$

Since $f(x) \in \mathbb{Z}[x]$ we have $|a_i|_p \le 1$ and we cannot have all $|a_i|_p < 1$ as $f(x)$ is irreducible (otherwise p can be factored). Hence $\|f\|_p = 1$ and we get

$$\left\| \frac{f(x)}{a_d} \right\|_p = \frac{1}{|a_d|_p} = p^l \text{ where } p^l \parallel a_d.$$

Therefore running through all the primes we get,

$$\prod_{\text{all } p}\prod_{w\in V_k, w|p}\max\{1,|\alpha|_w\}^d = \prod_{p^l \| a_d} p^l = \|a_d\|_\infty.$$

Hence

$$H(\alpha)^d = \|a_d\|_\infty \prod_{i=1}^{d}\max\{1,\|\alpha_i\|_\infty\} = M(\alpha)$$

■

Thus from Lemma 3.1 we have a another representation for the Mahler measure as,

$$M(\alpha) = M(f_\alpha) = \prod_{v\in V_{\mathbb{Q}(\alpha)}}\max\{1,|\alpha|_v\}^d.$$

Now we record this result by the following theorem. The following theorem will now give us the relation between the Mahler measure and the absolute Weil height of an algebraic number α.

Now the **absolute logarithmic Weil height** $h(\alpha)$ is defined as,

$$h(\alpha) = \log H(\alpha) = \frac{1}{d}\log M(\alpha) \quad \text{or} \quad h(\alpha) = \log H(\alpha) = \sum_{w\in V_k}\log\max\{1,|\alpha|_w\}$$

and for our convenience we will be using these notations and the relations in our future discussions.

Properties of Logarithmic Absolute Weil Height

We state some elementary properties of the Weil height (see for example [25, pg 522-524]).

Lemma 3.4.1

For $\alpha,\beta \in \overline{\mathbb{Q}}^\times$ and let $\alpha,\beta \in k$, then

(i) $h(\alpha) = 0$ *if and only if α is a root of unity*

(ii) $h(\alpha_i) = h(\alpha_j)$, *whenever α_i and α_j are Galois conjugates*

(iii) $h(\alpha) = h(\alpha^{-1})$

(iv) $h(\alpha^m) = |m|h(\alpha)$ *for any* $m \in \mathbb{Z}$

(v) *If* $\alpha = \beta\zeta$ *for some root of unity* ζ, *then* $h(\alpha) = h(\beta)$

(vi) $h(\alpha\beta) \leq h(\alpha) + h(\beta)$

(vii) $h(\alpha + \beta) \leq h(\alpha) + h(\beta) + log\, 2$

3.5 Cyclotomic Extensions

We note most of the preliminary definitions and theorems in this section can be found in many of the text books on cyclotomic fields (see [29]).

Let $\overline{\mathbb{Q}}$ be the algebraic closure of the rational number field $\mathbb{Q}$. Consider the polynomial

$$f(x) = x^m - 1.$$

Let

$$\xi_1, \xi_2, \cdots, \xi_m$$

be the roots of $f(x)$, the m distinct mth roots of unity in $\overline{\mathbb{Q}}$. We view $\overline{\mathbb{Q}}$ as a subfield of the complex numbers $\mathbb{C}$. These roots form a multiplicative subgroup of $\mathbb{C}$ which is itself a cyclic group. An element ζ in this cyclic group is called a primitive mth root of unity if ζ generates the whole group and is denoted by ζ_m. Thus ζ_m^i is a primitive mth root of unity if and only if $(i, m) = 1$. This implies there are $\phi(m)$ primitive mth roots of unity. Now the mth **cyclotomic field** is defined as $\mathbb{K}_m = \mathbb{Q}(\zeta_m)$ and the mth **cyclotomic polynomial** is defined as

$$\prod_{(i,m)=1} \left(x - \zeta_m^i\right)$$

and denoted by $\Phi_m(x)$. Since the case $m = 2$ is obvious we assume $m > 2$ unless otherwise stated. We can show that

$$\Phi_m(x) = \prod_{(i,m)=1} \left(x - \zeta_m^i\right)$$

is the minimal polynomial of ζ_m over $\mathbb{Q}$ and the primitive mth roots of unity are the conjugates of ζ_m.

An algebraic extension $\mathbb{E}$ of $\mathbb{Q}$ is called an **abelian extension** if the Galois group $\mathrm{Gal}(\mathbb{E}/\mathbb{Q})$ is an abelian group.

Theorem 3.5.1

The cyclotomic extension $\mathbb{K}_m = \mathbb{Q}(\zeta_m)$ is an abelian extension of degree $\phi(m)$ and the Galois group $Gal(\mathbb{K}_m/\mathbb{Q})$ is isomorphic to $\mathbb{Z}_m^*$, the multiplicative group of integers mod m.

Since we have,

$$\Phi_m(x) = \prod_{(i,m)=1} \left(x - \zeta_m^i\right)$$

we can write

$$x^m - 1 = \prod_{d|m} \Phi_d(x)$$

and

$$\Phi_m(x) = \prod_{d|m} \left(x^{m/d} - 1\right)^{\mu(d)}$$

where $\mu(d)$ is the möbius function.

Let

$$m = \prod_i p_i^{s_i}$$

be the prime factorization of the integer m, then looking at the group structure of $\mathbb{Z}_m^*$ we get

$$\mathrm{Gal}(\mathbb{K}_m/\mathbb{Q}) \cong \prod_i \mathrm{Gal}\left(\mathbb{K}_{p_i^{s_i}}/\mathbb{Q}\right).$$

We also note that $\mathbb{Z}[\zeta_m]$ is the ring of algebraic integers in the cyclotomic field $\mathbb{K}_m = \mathbb{Q}(\zeta_m)$.

Theorem 3.5.2 (Kronecker-Weber [29])

Let K be an abelian extension of $\mathbb{Q}$. Then K is contained in a cyclotomic field.

Now we restate **Lehmer's Problem** as for a nonzero algebraic number α, not a root of unity with degree $d = [\mathbb{Q}(\alpha): \mathbb{Q}]$ does there exist a positive constant $c > 0$ such that

$$h(\alpha) \geq \frac{c}{d}.$$

Lemma 3.5.3 (Gauss Sum Lemma)

For any prime p the classical Gauss sum can be defined as,

$$g = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) e^{\frac{2\pi i a}{p}} = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4, \\ \sqrt{p}i & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

where $\left(\frac{a}{p}\right) = 1$ if a is a square modulo p and -1 otherwise.

(This lemma can be found in many analytic number theory books, see Theorem 3.3 of [16])

Let ζ_p be the primitive pth root of unity $e^{\frac{2\pi i}{p}}$, then we get

$$\sqrt{(-1)^{(p-1)/2}p} = \sum_{i=0}^{p-1} \zeta_p^{i^2},$$

concluding that $\sqrt{(-1)^{(p-1)/2}p} \in \mathbb{Q}(\zeta_p)$. For an example let us look at the cases $p = 5$ and $p = 7$. When $p = 5,\ 5 \equiv 1 \pmod 4$, and $\mathbb{Q}(g) = \mathbb{Q}\left(\sqrt{(-1)^{(5-1)/2}5}\right) = \mathbb{Q}(\sqrt{5})$ is the unique quadratic subfield with $g = \sqrt{5} = 1 + 2(\zeta_5 + \zeta_5^4)$. When $p = 7,\ 7 \equiv 3 \pmod 4$, and $\mathbb{Q}(g) = \mathbb{Q}\left(\sqrt{(-1)^{(7-1)/2}7}\right) = \mathbb{Q}(\sqrt{-7})$ is the unique quadratic subfield with $g = \sqrt{-7} = 1 + 2(\zeta_7 + \zeta_7^2 + \zeta_7^4)$.

Definition 3.5.4

A number field K is said to be Kroneckerian if it is a totally real number field or a totally complex quadratic extension of a totally real number field. Equivalently a number field K is Kroneckerian if and only if for every $\alpha \in K$ we have $\bar{\alpha} \in K$ and for every embedding σ of K into $\mathbb{C}$ we have $\overline{\sigma(\alpha)} = \sigma(\bar{\alpha})$ (complex conjugation commutes with every σ).

Since any cyclotomic field $\mathbb{Q}(\zeta_m)$ is of degree $\phi(m)$ and $\gamma = \zeta_m + \zeta_m^{-1}$ is totally real number in $\mathbb{Q}(\zeta_m)$, we get $\mathbb{Q}(\gamma)$ is a totally real subfield of $\mathbb{Q}(\zeta_m)$ (in fact the maximal real subfield of $\mathbb{Q}(\zeta_m)$) and $[\mathbb{Q}(\zeta_m): \mathbb{Q}(\gamma)] = 2$. Thus $\mathbb{Q}(\zeta_m)$ is a totally complex quadratic extension of a totally real number field $\mathbb{Q}(\gamma)$. We note here that cyclotomic fields (abelian extensions) are examples of Kroneckerian fields as they are clearly a complex quadratic extension of a totally real number field. It follows from the Kronecker-Weber theorem that if an algebraic number α lies in an abelian extension then α lies in a Kroneckerian subfield.

Lemma 3.5.5

Suppose $\alpha \in \overline{\mathbb{Q}}^{\times}$, $|\alpha| \neq 1$ *and all the embeddings* τ *of* $\mathbb{Q}(\alpha)$ *into* $\mathbb{C}$ *commute with complex conjugation. Then*

$$h(\alpha) \geq \frac{1}{2}\log\left(\frac{1+\sqrt{5}}{2}\right).$$

Proof.

Let

$$A = \left(\alpha - \frac{1}{\bar{\alpha}}\right)$$

where $\bar{\alpha}$ is the complex conjugate of α, and let $\overline{\mathbb{Q}}(\alpha)$ be the galois closure of $\mathbb{Q}(\alpha)$. Since $|\alpha| \neq 1$ we get $A \neq 0$. Therefore by the product formula we have

$$\prod_{v \in V_{\overline{\mathbb{Q}}(\alpha)}} |A|_v^a = 1,$$

for any positive a.

Now for any finite place $v \nmid \infty$, and $a \leq 1/2$ we have

$$|A|_v^a = \left|\alpha - \frac{1}{\bar{\alpha}}\right|_v^a \leq \max\{1, |\alpha|_v\}^a \max\{1, |\bar{\alpha}|_v^{-1}\}^a \leq \max\{1, |\alpha|_v\}^{1/2} \max\{1, |\bar{\alpha}^{-1}|_v\}^{1/2}.$$

For the infinite places $v|\infty$, let d_v denote the common local degree and $|.|$ denote the absolute value on $\mathbb{Q}$. For any infinite place $v \in V_{\overline{\mathbb{Q}}(\alpha)}$ there exists $\sigma \in \mathrm{Aut}(\overline{\mathbb{Q}}(\alpha)/\mathbb{Q})$ such that $|.|_v = |.|_\sigma$ and write $|\beta|_v = |\beta|_\sigma = |\sigma(\beta)|^{d_v/d}$ for all $\beta \in \overline{\mathbb{Q}}(\alpha)$, where $d = [\overline{\mathbb{Q}}(\alpha): \mathbb{Q}]$. Since $\sigma \in \mathrm{Aut}(\overline{\mathbb{Q}}(\alpha)/\mathbb{Q})$ commutes with the complex conjugation, therefore we have

$$\sigma(A) = \left(\sigma(\alpha) - \frac{1}{\sigma(\bar{\alpha})}\right) = \left(\sigma(\alpha) - \frac{1}{\overline{\sigma(\alpha)}}\right)$$

and for the infinite places $\left(\text{since } \left|x - \frac{1}{\bar{x}}\right| = \left|\frac{|x|^2 - 1}{x}\right| = \left||x| - \frac{1}{|x|}\right|\right)$,

$$|A|_v^a = |A|_\sigma^a = \left|\sigma(\alpha) - \frac{1}{\overline{\sigma(\alpha)}}\right|^{ad_v/d} = \left||\sigma(\alpha)| - \frac{1}{|\sigma(\alpha)|}\right|^{ad_v/d}$$

$$= (f(|\sigma(\alpha)|_\infty))^{d_v/d} \max\{1, |\alpha|_v\}^{1/2} \max\{1, |\bar{\alpha}|_v^{-1}\}^{1/2},$$

where $f(x) = \dfrac{|x - x^{-1}|^a}{\max\{1, |x|\}^{1/2} \max\{1, |x|^{-1}\}^{1/2}}$.

Note by the symmetry of $f(x)$ we may assume that $x > 1$ (if $x < 1$ then put $y = \frac{1}{x} > 1$ yields the same function as $x > 1$ replaced by y). When $x > 1$ then $f(x) = x^{-1/2}(x - x^{-1})^a$ attains its global maximum at $x = \frac{\sqrt{1+2a}}{\sqrt{1-2a}}$ and the minimum of the global maximum is $x_0^{-1/2}$ where $x_0 = \left(1 + \sqrt{5}\right)/2$ achieved when $a = 1/2\sqrt{5}$. Hence when $v|\infty$ we have

$$|A|_v^a = \left|\alpha - \frac{1}{\bar{\alpha}}\right|_v^a \leq \left(x_0^{-1/2}\right)^{d_v/d} \max\{1, |\alpha|_v\}^{1/2} \max\{1, |\bar{\alpha}^{-1}|_v\}^{1/2},$$

which implies that

$$1 = \prod_{v \in V_{\overline{\mathbb{Q}}(\alpha)}} |A|_v^a \leq \prod_{v|\infty} \left(x_0^{-1/2}\right)^{d_v/d} \prod_v \max\{1, |\alpha|_v\}^{1/2} \max\{1, |\bar{\alpha}^{-1}|_v\}^{1/2}$$

$$= x_0^{-1/2} H(\alpha)^{\frac{1}{2}} H(\bar{\alpha}^{-1})^{\frac{1}{2}}.$$

We note that from Lemma 3.4.1 (ii) and (iii), $h(\alpha) = h(\bar{\alpha}^{-1})$ and so $H(\alpha) = H(\bar{\alpha}^{-1})$. Thus we get $H(\alpha) \geq \sqrt{x_0}$, that is,

$$h(\alpha) \geq \log\left(x_0^{1/2}\right) = \frac{1}{2}\log\left(\frac{1+\sqrt{5}}{2}\right).$$

■

From Theorem 3.5.1 and Theorem 3.5.2 we get K is an abelian extension if and only if $K \subseteq \mathbb{K}_m = \mathbb{Q}(\zeta_m)$ for some positive integer m. This becomes a useful result to us when finding lower bounds for abelian heights. In the following Section 3.6 we will state some known results on absolute height which give some significant results on Lehmer's Problem in some special classes. In section 3.7 we present our results on heights in cyclotomic extensions as an improvement of some of the results in section 3.6.

3.6 Some Known bounds on the Absolute Logarithmic Weil Height

Theorem 3.6.1 (Schinzel 1973 [24])

Suppose α lies in a Kroneckerian field (a totally real number field, or a quadratic extension of such a field) and $|\alpha| \neq 1$. *Then,*

$$h(\alpha) \geq \frac{1}{2}\log\left(\frac{\sqrt{5}+1}{2}\right).$$

Note that this bound holds for an algebraic number α with $|\alpha| \neq 1$ which lies in an abelian extension by Lemma 3.5.5.

Theorem 3.6.2 (P. Borwein, E. Dobrowolski, M.J. Mossinghoff 1991[4])

Suppose $f(x) \in D_m$ *with degree n, where*

$$D_m = \left\{ f(x) = \sum_{i=1}^{n} a_i x^i \in \mathbb{Z}[x] : a_i \equiv 1 (mod\, m) \right\},$$

and suppose $F \in \mathbb{Z}[x]$ *satisfies* $gcd\left(f(x), F(x^{n+1})\right) = 1$. *Then*

$$\log M(f) \geq \begin{cases} \dfrac{v(F)\log 2 - \log\|F\|_\infty}{\deg F}\left(\dfrac{n}{n+1}\right), & \text{if } m = 2, \\ \dfrac{v_0(F)\log m - \log\|F\|_\infty}{\deg F}\left(\dfrac{n}{n+1}\right), & \text{if } m > 2. \end{cases}$$

Here $v_k(g)$ denote the multiplicity of the cyclotomic polynomial $\Phi_{2^k}(x)$ in $g(x)$, and

$$v(g) = \sum_{k\geq 0} v_k(g).$$

We immediately get the following results from this theorem.

If $f(x)$ has all odd coefficients and no cyclotomic factors, then we get

$$\log M(f) \geq \frac{\log 2}{2}\left(\frac{n}{n+1}\right),$$

by taking $F(x) = x^2 - 1$.

For $m > 2$, if $f(x) \in D_m$ with no cyclotomic factors, yields

$$\log M(f) \geq \log(m/2)\left(\frac{n}{n+1}\right),$$

by using $F(x) = x - 1$.

Also the following two corollaries from the above theorem give us some improved results.

Corollary 3.6.3 (P. Borwein, E. Dobrowolski, M.J. Mossinghoff 1991[4]).

Let $f(x)$ be a polynomial with degree n having all odd coefficients and no cyclotomic factors. Then

$$\log M(f) \geq \frac{\log 5}{4}\left(\frac{n}{n+1}\right),$$

with equality if and only if $f(x) = \pm 1$.

Using $F(x) = (1 + x^2)(1 - x^2)^4$ we get the result.

Corollary 3.6.4 (P. Borwein, E. Dobrowolski, M.J. Mossinghoff 1991[4]).

Let $f(x) \in D_m$ be a polynomial with degree n and no cyclotomic factors. Then

$$\log M(f) \geq \log\left(\frac{\sqrt{m^2+1}}{2}\right)\ \left(\frac{n}{n+1}\right),$$

with equality if and only if $f(x) = \pm 1$.

Using $F(x) = (1+x)\,(1-x)^{m^2}$ we get the result.

Theorem 3.6.5 (F. Amoroso & R. Dvornicich1998 [1])

Let $\alpha \neq 0 \in \mathbb{Q}(\zeta_m)$. Then

1. *If α is not a root of unity,*

$$h(\alpha) \geq\ c(m)$$

where

$$c(m) = \begin{cases} \frac{1}{8}\log(7/2) = 0.156595\ldots & \text{if } 7 \nmid m\,; \\ \frac{1}{6}\log(5/2) = 0.152715\ldots & \text{if } 7 \mid m \text{ and } 5 \nmid m\,; \\ \frac{1}{12}\log(11/2) = 0.1420662\ldots & \text{if } 35 \mid m \text{ and } 11 \nmid m\,; \\ \frac{1}{12}\log(5) = 0.134119\ldots & \text{if } 385 \mid m\,. \end{cases}$$

2. *If $4 \mid m$ and there is no root of unity $\zeta \in \mathbb{Q}(\zeta_m)$ such that $\alpha\zeta$ is contained in a proper cyclotomic subextension of $\mathbb{Q}(\zeta_m)$, we have the stronger lower bound*

$$h(\alpha) \geq\ \frac{1}{4}\log 2 = 0.173286\ldots.$$

Corollary 3.6.6 (F. Amoroso & R. Dvornicich 1998 [1])

Let $\mathbb{L}/\mathbb{Q}$ be an abelian extension and let $\alpha \in \mathbb{L}^*$, α not a root of unity. Then

$$h(\alpha) \geq\ \frac{1}{12}\log 5 = 0.134119\ldots.$$

They also observed that this lower bound cannot be replaced by any number $> (\log 7)/12$. Recently Amoroso & Zannier [2] have shown more generally that if k is a number field, $k(\alpha)$ is an abelian extension of k, and $m = [k : \mathbb{Q}]$, then

$$h(\alpha) \geq 3^{-m^2-2m-6}.$$

In particular, if $\alpha \neq 0$ lies in a dihedral extension of the rationals, then using $m = 2$ we see that

$$h(\alpha) \geq 3^{-14}.$$

Garza [13] had previously obtained the bound

$$h(\alpha) \geq \frac{1}{d}\log M(x^3 - x - 1) = \frac{1}{d}(0.281186\ldots)$$

in this situation, which is optimal with respect to **Lehmer's Problem**.

Theorem 3.6.7 (Garza 2008 [11])

Let α be an algebraic number such that $\alpha \neq 0$ and is not a root of unity. Let $\mathbb{K}$ be the galois closure of $\mathbb{Q}(\alpha)$. Let $\eta: \mathbb{K} \hookrightarrow \mathbb{C}$ be an embedding. Let Λ be the set of galois conjugates of α that are real with respect to η. Suppose that $|\Lambda| \neq 0$(non empty). Let $d = [\mathbb{Q}(\alpha): \mathbb{Q}]$ and $R_\alpha \equiv |\Lambda|/d$. Let $\beta = 1 - 1/R_\alpha$. Then

$$h(\alpha) \geq \log\left(\frac{2^\beta + \sqrt{4^\beta + 4}}{2}\right)^{R_\alpha/2}.$$

This Theorem (3.6.7) by J. Garza is a generalization of the Theorem (3.6.1) by Schinzel. For the case of algebraic integers G. Höhn [15] gave a shorter proof of this theorem.

3.7 Lower Bounds for Heights in Cyclotomic Extensions

Here we show that the height of a nonzero algebraic number α that lies in an abelian extension of the rationals and is not a root of unity must satisfy

$$h(\alpha) > 0.155090,$$

which is an improvement of the Amoroso & Dvornicich bound in Theorem (3.6.6). Suppose α lies in an algebraic number field k of degree d, let V_k be the complete set of places of k such that the normalization ensures that $|x|_v = \|x\|_v^{d_v/d}$ for all $v \in V_k$. Here $d = [k\colon \mathbb{Q}]$ the degree of the extension, $d_v = [k_v\colon \mathbb{Q}_v]$ the local degree, and $\|x\|_v = |x|_p$ on $\mathbb{Q}$ with $p \in V_{\mathbb{Q}} = \{\infty, 2,3,5,7, \dots\}$. Throughout this section we will assume that the algebraic number α lies in a cyclotomic extension $\mathbb{Q}(\zeta_m)$, where ζ_m is a primitive mth root of unity, and that $\alpha \neq 0$ is not a root of unity.

Property (3.7): For a rational prime p, if $p \nmid m$ then let $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ be defined by $\sigma_p(\zeta_m) = \zeta_m^p$. If $p|m$ then let σ_p be a generator of the cyclic galois group $\mathrm{Gal}\left(\mathbb{Q}(\zeta_m)/\mathbb{Q}\left(\zeta_{m/p}\right)\right)$ which is of order p or $p-1$ depending on whether $p^2|m$ or not, thus we have $\sigma_p(\zeta_m) = \zeta_p\zeta_m$ for an appropriate pth root of unity ζ_p.

Since we have the Schinzel bound

$$h(\alpha) \geq \frac{1}{2}\log\left(\frac{1+\sqrt{5}}{2}\right) = 0.240605\ldots,$$

if α lies in a Kroneckerian field (a totally real number field, or a quadratic extension of such a field) and $|\alpha| \neq 1$, we also assume $|\alpha|_v = 1$ for all $v|\infty$ (α lies in an abelian extension implies that α lies in a Kroneckerian field). From Amoroso & Dvornicich [1] we observe that lower bound of height of α in an abelian extension cannot be greater than

$$\frac{1}{12}\log 7 = 0.162159\ldots.$$

Now recall the relation

$$h(\alpha) = \frac{1}{d}\log M(f),$$

where

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

When $|\alpha| = 1$ with all its conjugates also lying in the unit circle, is a root of an irreducible integer polynomial

$$f(x) = a\prod_{i=1}^{d}(x - \alpha_i),$$

then we get simply

$$h(\alpha) = \frac{1}{d}\log M(f) = \frac{1}{d}\log|a|.$$

Note that the following algebraic numbers α_0, α_1, α_2, and α_3 are examples of the algebraic numbers on the unit circle with all its conjugates lying on the unit circle. Which provide examples for the later bounds to be sharp and we will discuss this in theorem 3.7.1.

When α_0 is a root of $7x^{12} - 13x^6 + 7$ then we obtain the smallest known non zero abelian height (note the root of $7x^{12} - 13x^6 + 7$ are the all 6^{th} roots of the quadratic polynomial $7x^2 - 13x + 7$ and the roots of the quadratic polynomial lie on the unit circle. Thus α_0 and its conjugates lie on the unit circle)

$$h(\alpha_0) = \frac{1}{12}\log 7 = 0.162159\ldots,$$

by writing explicitly one of the roots of this polynomial $7x^{12} - 13x^6 + 7$ in the form

$$\alpha_0 := \frac{(3u^2-5)}{i\sqrt{7}(1+\lambda_0)}, \qquad u := 2\cos(2\pi/7) \tag{3.7.1}$$

where

$$\lambda_0 := \frac{1}{14}(2-9u-3u^2) + \frac{1}{14}(-8+u+5u^2)\sqrt{3}i$$

is a zero of

$$x^6 + \frac{13}{7}x^3 + 1.$$

Thus the roots $\pm\alpha_0^{\varepsilon}\zeta_3^j$, $\varepsilon = \pm 1$, $j = 0,1,2$ of $7x^{12} - 13x^6 + 7$ plainly lie in $\mathbb{Q}(\zeta_{21})$. We will show in Theorem 3.7.1 that the height

$$\frac{1}{12}\log 7 = 0.162159\ldots$$

is sharp when $3|m$ and $\alpha\zeta_m^u \notin \mathbb{Q}(\zeta_{m/3})$ for any integer u.

When $2|m$ and $\alpha\zeta_m^u \notin \mathbb{Q}(\zeta_{m/2})$ for any integer u, the sharpness of the stronger lower bound

$$h(\alpha) \geq \frac{1}{4}\log 2 = 0.173286\ldots$$

obtained by Amoroso & Dvornicich can be achieved from the following examples.

First by using

$$\alpha_1 := \frac{1}{4}(1+i)\left(1+\sqrt{-7}\right) \in \mathbb{Q}(\zeta_{28}), \tag{3.7.2}$$

which has minimal polynomial

$$x^4 - x^3 + \frac{1}{2}x^2 - x + 1,$$

or by using

$$\alpha_2 := \frac{1}{4}(1+i)\left(\sqrt{5}+\sqrt{-3}\right) \in \mathbb{Q}(\zeta_{60}), \tag{3.7.3}$$

which has minimal polynomial

$$x^8 - \frac{7}{4}x^4 + 1.$$

(Notice that $\left(\sqrt{5}+\sqrt{-3}\right) \in \mathbb{Q}(\zeta_{15})$, and also that $\alpha_2 = \zeta_8\beta_2$ where

$$\beta_2 = \frac{1}{4}\left(\sqrt{10}+\sqrt{-6}\right) \in \mathbb{Q}(\zeta_{120})$$

has lower degree with minimal polynomial

$$x^4 - \frac{1}{2}x^2 + 1,$$

but of course the same height). We will show in theorem 3.7.1 that α_1 and α_2 shows the necessity of the conditions to obtain the bounds (3.7.9) and (3.7.7) respectively.

In the case of $2|m$ in Theorem 3.7.1, we also obtain the sharp lower bound

$$h(\alpha_3) = \frac{1}{8}\log 5 = 0.201179\ldots$$

with some restrictions on the form of α with low height. For that we take the value

$$\alpha_3 = \sqrt{\frac{5+\sqrt{5}}{10}} + \sqrt{\frac{5-\sqrt{5}}{10}}\,i \tag{3.7.4}$$

$$= \left(\frac{2}{\sqrt{5}}\right)\sin\left(\frac{2\pi}{5}\right) + \frac{1}{2\sin\left(\frac{2\pi}{5}\right)}\,i \in \mathbb{Q}(\zeta_{20})$$

which has minimal polynomial

$$x^8 + \frac{6}{5}x^4 + 1.$$

We go through the following lemmas to establish our main theorems.

Lemma (3.7.1)

Let p be a prime and σ_p be as defined in property (3.7). Suppose that γ is algebraic integer in $\mathbb{Q}(\zeta_m)$, $\alpha \in \mathbb{Q}(\zeta_m)$, and $v \nmid \infty$.

(i) *If $p \nmid m$ then* $p \mid \left(\gamma^p - \sigma_p(\gamma)\right)$

(ii) *If $p \mid m$ then* $(1-\zeta_m)^p \mid \left(\gamma^p - \sigma_p(\gamma)^p\right)$

(iii) *If* $p \nmid m$ *then* $\left|\alpha^p - \sigma_p(\alpha)\right|_v \leq |p|_v \max\{1, |\alpha|_v\}^p \max\left\{1, \left|\sigma_p(\alpha)\right|_v\right\}$

(iv) *If $p \mid m$ then* $\left|\alpha^p - \sigma_p(\alpha)^p\right|_v \leq |p|_v^{\frac{p}{p-1}} \max\{1, |\alpha|_v\}^p \max\left\{1, \left|\sigma_p(\alpha)\right|_v\right\}^p$

Proof.

For (i) (see [1, Lemma 2]), if $p \nmid m$ then let $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ be defined by $\sigma_p(\zeta_m) = \zeta_m^p$. Now for any algebraic integer $\gamma \in \mathbb{Q}(\zeta_m)$ we can write $\gamma = f(\zeta_m)$ for some $f(x) \in \mathbb{Z}[x]$ (since $\mathbb{Z}[\zeta_m]$ is the ring of integers of $\mathbb{Q}(\zeta_m)$). Therefore we get

$$\gamma^p \equiv f\left(\zeta_m^p\right) \equiv f\left(\sigma_p(\zeta_m)\right) \equiv \sigma_p(\gamma) \pmod{p}.$$

Thus we have $p \mid \left(\gamma^p - \sigma_p(\gamma)\right)$. For (ii), write

$$\gamma = \sum_{i=0}^{p-1} \left(\sum_{j \equiv i \pmod p} a_j \zeta_m^j \right) = \sum_{i=0}^{p-1} A_i \zeta_m^i,$$

with $A_i = \sum_{j \equiv i \pmod p} a_j \in \mathbb{Q}\left(\zeta_{m/p}\right)$.

Hence, since $\sigma_p(\zeta_m) = \zeta_p \zeta_m$,

$$\sigma_p(\gamma) = \sum_{i=0}^{p-1} A_i \zeta_m^i \zeta_p^i,$$

and for each $k = 0,1, \dots, p-1$, we have that

$$\sigma_p(\gamma) - \zeta_p^k \gamma = \sum_{i=0}^{p-1} A_i \zeta_m^i \left(\zeta_p^i - \zeta_p^k\right)$$

is divisible by $\left(1 - \zeta_p\right)$.

For $v \nmid p$, statements (iii) and (iv) are trivial. From Theorem (2.4.6), there must exist an algebraic integer β such that $\alpha\beta$ is an algebraic integer, but

$$|\beta|_v = \frac{1}{\max\{1, |\alpha|_v\}}$$

for all places $v|p$. Hence when $p \nmid m$ and $v|p$ by (i) we have

$$\max\left\{\left|(\alpha\beta)^p - \sigma_p(\alpha\beta)\right|_v, \left|\beta^p - \sigma_p(\beta)\right|_v\right\} \leq |p|_v,$$

and

$$\left|\alpha^p - \sigma_p(\alpha)\right|_v \leq \max\{1, |\alpha|_v\}^p \left|(\alpha\beta)^p - \sigma_p(\alpha\beta) + \sigma_p(\alpha)\left(\sigma_p(\beta) - \beta^p\right)\right|_v$$

$$\leq |p|_v \ \max\{1, |\alpha|_v\}^p \max\left\{1, \left|\sigma_p(\alpha)\right|_v\right\}.$$

Similarly, when $p|m$ and $v|p$, by (ii) we have

$$\max\left\{\left|(\alpha\beta)^p - \sigma_p(\alpha\beta)^p\right|_v, \left|\beta^p - \sigma_p(\beta)^p\right|_v\right\} \leq |p|_v^{\frac{p}{p-1}}$$

and

$$\left|\alpha^p - \sigma_p(\alpha)^p\right|_v \leq \max\{1, |\alpha|_v\}^p \ \left|(\alpha\beta)^p - \sigma_p(\alpha\beta)^p + \sigma_p(\alpha)^p\left(\sigma_p(\beta)^p - \beta^p\right)\right|_v$$

$$\leq |p|_v^{\frac{p}{p-1}} \max\{1, |\alpha|_v\}^p \max\left\{1, \left|\sigma_p(\alpha)\right|_v\right\}^p.$$

■

The following lemma will be needed to describe cases when certain factors of the product A used in the proof of Theorem 3.7.1 vanish.

Lemma (3.7.2)

Let p be a prime and σ_p be as defined in property (3.7). Suppose that $\alpha \in \mathbb{Q}(\zeta_m)$ and $\alpha \neq 0$.

(i) *If $p|m$ and $\sigma_p(\alpha)^p = \alpha^p$ then $\alpha/\zeta_m^u \in \mathbb{Q}(\zeta_{m/p})$ for some integer u.*

(ii) *Suppose that $2|m$ and $\sigma_2(\alpha) = \lambda\alpha$. If $\lambda = \pm i$ then $m = 4l$ with l odd, and $(1+\lambda)\alpha \in \mathbb{Q}(\zeta_l)$. If $5\lambda^4 + 6\lambda^2 + 5 = 0$ then $m = 20l$ with l odd, $\lambda = -\alpha_3^{-2\varepsilon}(-1)^j$ for some $\varepsilon = \pm 1$, $j = 0$ or 1, and $\alpha/\alpha_3^{\varepsilon} i^j \in \mathbb{Q}(\zeta_{5l})$.*

(iii) *Suppose that $3|m$ and $\sigma_3(\alpha) = \lambda\alpha$. If $7\lambda^6 + 13\lambda^3 + 7 = 0$ then $m = 21l$ with $3 \nmid l$, $\lambda = -\alpha_0^{-2\varepsilon}\zeta_3^j$ for some $\varepsilon = \pm 1$, $0 \leq j \leq 2$, and $\alpha/\alpha_0^{\varepsilon}\zeta_3^j \in \mathbb{Q}(\zeta_{7l})$. If $8\lambda^6 + 11\lambda^3 + 8 = 0$ then $m = 15l$, $3 \nmid l$, with*

$$\lambda = \left(\frac{1-\sqrt{-15}}{4}\right)\zeta_3^j$$

for some $\varepsilon = \pm 1$, $0 \leq j \leq 2$, and $\alpha/\left(\sqrt{5}+\sqrt{-3}\right)^{\varepsilon}\zeta_3^j \in \mathbb{Q}(\zeta_{5l})$.

Statement (i) is a classical result of Amoroso & Dvornicich (see [1, Lemma 2]).

Proof.

For (i), note that the Galois group $\mathrm{Gal}\left(\mathbb{Q}(\zeta_m)/\mathbb{Q}\left(\zeta_{m/p}\right)\right)$ is cyclic of order p or $(p-1)$ depending on whether $p^2|m$ or not. Suppose $\sigma_p \in \mathrm{Gal}\left(\mathbb{Q}(\zeta_m)/\mathbb{Q}\left(\zeta_{m/p}\right)\right)$ is a generator then $\sigma_p(\zeta_m) = \zeta_p\zeta_m$ for some primitive pth root of unity ζ_p. Suppose that $\sigma_p(\alpha)^p = \alpha^p$, then

$\sigma_p(\alpha) = \zeta_p^k \alpha$ for some integer k. Now it follows that $\sigma_p(\alpha/\zeta_m^k) = \zeta_p^k \alpha/(\zeta_p\zeta_m)^k = \alpha/\zeta_m^k$, hence α/ζ_m^k belongs to the fixed field $\mathbb{Q}(\zeta_{m/p})$.

For (ii), suppose that $p = 2$, $4|m$, $\alpha \neq 0$ and $\sigma_2(\alpha) = \lambda\alpha$ with $\lambda = \pm i$. Then writing

$$\alpha = A_0 + \zeta_m A_1, \text{ with } A_i \in \mathbb{Q}(\zeta_{m/2}),$$

we get that

$$\sigma_2(\zeta_m) = -\zeta_m \quad \text{and} \quad \sigma_2(\alpha) = A_0 - \zeta_m A_1 = \lambda A_0 + \lambda\zeta_m A_1.$$

If $8|m$, then $\lambda \in \mathbb{Q}(\zeta_{m/2})$ with $[\mathbb{Q}(\zeta_m): \mathbb{Q}(\zeta_{m/2})] = 2$,

which forces us to get the relations

$$A_0 = \lambda A_0 \quad \text{and} \quad A_1 = -\lambda A_1, \text{ so that } \alpha = 0.$$

Thus $8 \nmid m$ and $m = 4l$ with l odd and $A_i \in \mathbb{Q}(\zeta_l)$. Since we assume that $\lambda = \mp i$, we get

$$\zeta_m = i\zeta_l \quad \text{and} \quad [\mathbb{Q}(\zeta_m): \mathbb{Q}(\zeta_l)] = 2,$$

which now produces $\zeta_m A_1 = \pm i A_0$ and $\alpha = (1 \pm i)A_0$, with $A_0 \in \mathbb{Q}(\zeta_l)$.

Suppose now that λ is a root of $5x^4 + 6x^2 + 5$. Recall that

$$\alpha_3 = \sqrt{\frac{5+\sqrt{5}}{10}} + \sqrt{\frac{5-\sqrt{5}}{10}}\, i \in \mathbb{Q}(\zeta_{20}),$$

and that α_3 has minimal polynomial

$$x^8 + \frac{6}{5}x^4 + 1.$$

Since $\alpha_3^2 = (1+2i)/\sqrt{5}$ we get that $\lambda = -\alpha_3^{-2\varepsilon}(-1)^j$ for some $\varepsilon = \pm 1$, $j = 0$ or 1.
As $\lambda = \sigma_2(\alpha)/\alpha \in \mathbb{Q}(\zeta_m)$ to get α_3^2 in $\mathbb{Q}(\zeta_m)$ we must have $5|m$. Similarly as above if $8|m$ then we can write

$$\alpha = A_0 + \zeta_m A_1, \text{ with } A_i \in \mathbb{Q}(\zeta_{m/2}), \text{ and}$$

$$\sigma_2(\zeta_m) = -\zeta_m \text{ and } \sigma_2(\alpha) = A_0 - \zeta_m A_1 = \lambda A_0 + \lambda\zeta_m A_1.$$

Then $\lambda \in \mathbb{Q}\left(\zeta_{m/2}\right)$ with $\left[\mathbb{Q}(\zeta_m): \mathbb{Q}\left(\zeta_{m/2}\right)\right] = 2$, forcing $A_0 = \lambda A_0$, $A_1 = -\lambda A_1$, and $\alpha = 0$. Thus we have $m = 20l$ with l odd and $A_i \in \mathbb{Q}(\zeta_{5l})$. Since $\lambda = -\alpha_3^{-2\varepsilon}(-1)^j$, $\sigma_2(\zeta_5) = \zeta_5$, and $\sigma_2(i) = -i$, by writing explicitly

$$\cos\left(\frac{2\pi}{5}\right) = \frac{-1+\sqrt{5}}{4} \quad \text{and} \quad \sin\left(\frac{2\pi}{5}\right) = \frac{\sqrt{10+2\sqrt{5}}}{4},$$

we obtain that

$$\sigma_2(\zeta_5) = \zeta_5 = \cos\left(\frac{2\pi}{5}\right) + \sin\left(\frac{2\pi}{5}\right)i = \sigma_2\left(\frac{-1+\sqrt{5}}{4}\right) + \sigma_2\left(\frac{\sqrt{10+2\sqrt{5}}}{4}\right)\sigma_2(i), \text{ and}$$

$$\sigma_2(\zeta_5^2) = \zeta_5^2 = \cos\left(\frac{4\pi}{5}\right) + \sin\left(\frac{4\pi}{5}\right)i = \sigma_2\left(\frac{-1-\sqrt{5}}{4}\right) + \sigma_2\left(\frac{\sqrt{10-2\sqrt{5}}}{4}\right)\sigma_2(i).$$

Thus $\sigma_2\left(\sqrt{5}\right) = \sqrt{5}$, $\sigma_2\left(\sqrt{2\sqrt{5}+10}/4\right) = -\sqrt{2\sqrt{5}+10}/4$, and $\sigma_2\left(\sqrt{2\sqrt{5}-10}/4\right) = -\sqrt{2\sqrt{5}-10}/4$. Writing

$$\sqrt{\frac{5+\sqrt{5}}{10}} = \left(\frac{2}{\sqrt{5}}\right)\frac{\sqrt{2\sqrt{5}+10}}{4} \text{ and } \sqrt{\frac{5-\sqrt{5}}{10}} = \left(\frac{2}{\sqrt{5}}\right)\frac{\sqrt{2\sqrt{5}-10}}{4}$$

implies that

$$\sigma_2(\alpha_3) = -\overline{\alpha}_3 = -1/\alpha_3.$$

Now we see that $\sigma_2\left(\alpha/\alpha_3^{\varepsilon}i^j\right) = \lambda\alpha\left(-\alpha_3^{\varepsilon}(-i)^{-j}\right) = -\alpha_3^{-2\varepsilon}(-1)^j(\alpha)\left(-\alpha_3^{\varepsilon}(-i)^{-j}\right) = \alpha/\alpha_3^{\varepsilon}i^j$. Thus $\alpha/\alpha_3^{\varepsilon}i^j$ is fixed by σ_2 and hence lies in $\mathbb{Q}(\zeta_{5l})$.

For (iii) suppose that $3|m$ and $\sigma_3(\alpha) = \lambda\alpha$. If $7\lambda^6 + 13\lambda^3 + 7 = 0$, then we clearly see that λ^3 is a root of $7x^2 + 13x + 7$, so that $\lambda = -\alpha_0^{-2\varepsilon}\zeta_3^j$ for some $\varepsilon = \pm 1$, $0 \le j \le 2$. Since $\lambda \in \mathbb{Q}(\cos(2\pi/7), \zeta_3) - \mathbb{Q}(\zeta_3)$, we must have $7|m$.

Now writing

$$\sigma_3(\zeta_m) = \zeta_m\omega$$

for an appropriate primitive cube root of unity ω and suppose if $3^2|m$, then λ and ω are both in $\mathbb{Q}(\zeta_{m/3})$ and $\left[\mathbb{Q}(\zeta_m):\mathbb{Q}\left(\zeta_{m/3}\right)\right] = 3$.

Hence, writing

$$\alpha = A_0 + \zeta_m A_1 + \zeta_m^2 A_2,$$

where

$$A_i = \sum_{j \equiv i \bmod 3} a_j \zeta_m^{j-i} \in \mathbb{Q}\left(\zeta_{m/3}\right),$$

we have

$$\sigma_3(\alpha) = A_0 + \omega\zeta_m A_1 + \omega^2 \zeta_m^2 A_2.$$

Since we have $\sigma_3(\alpha) = \lambda\alpha$ this forces $A_0 = \lambda A_0$, $A_1\omega = \lambda A_1$, and $A_2\omega^2 = \lambda A_2$, which cannot occur if $\alpha \neq 0$. So we get $3^2 \nmid m$ and $m = 21l$.

For $m = 21l$ with $3 \nmid l$, we have $\sigma_3(\zeta_3) = \zeta_3^{-1}$ and $\sigma_3(\zeta_7) = \zeta_7$, thus we get $\sigma_3(u) = u$ where $2\cos(2\pi/7) = u$. Also we have from Lemma 3.5.3 that, $\sqrt{7}i \in \mathbb{Q}(\zeta_7)$ and $\sqrt{7}i$ is the classical Gauss sum. Therefore we can write $\sqrt{7}i = 1 + 2(\zeta_7 + \zeta_7^2 + \zeta_7^4)$ and this implies that $\sqrt{7}i$ is fixed by σ_3, as $\sigma_3\left(\sqrt{7}i\right) = 1 + 2\sigma_3(\zeta_7 + \zeta_7^2 + \zeta_7^4) = 1 + 2(\zeta_7 + \zeta_7^2 + \zeta_7^4) = \sqrt{7}i$. Now explicitly writing

$$\alpha_0 := \frac{(3u^2 - 5)}{i\sqrt{7}(1 + \lambda_0)}, \qquad \text{where } \lambda_0 := \frac{1}{14}(2 - 9u - 3u^2) + \frac{1}{14}(-8 + u + 5u^2)\sqrt{3}i$$

we can clearly see $\sigma_3(1 + \lambda_0) = 1 + \bar{\lambda}_0$ thus we have

$$\sigma_3(\alpha_0) = -\overline{\alpha}_0 = -1/\alpha_0.$$

Hence we get $\sigma_3\left(\alpha/\alpha_0^{\varepsilon}\zeta_3^j\right) = \lambda\alpha\left(-\alpha_0^{\varepsilon}\zeta_3^j\right) = \left(-\alpha_0^{-2\varepsilon}\zeta_3^j\right)\alpha\left(-\alpha_0^{\varepsilon}\zeta_3^j\right) = \alpha/\alpha_0^{\varepsilon}\zeta_3^j$. Thus $\alpha/\alpha_0^{\varepsilon}\zeta_3^j$ is fixed by σ_3, so it is in $\mathbb{Q}(\zeta_{7l})$.

Suppose now that λ^3 is a zero of $8x^2 + 11x + 8$, so that

$$\lambda = \left(\frac{1-\sqrt{-15}}{4}\right)^{\varepsilon} \zeta_3^j$$

for some $\varepsilon = \pm 1$, $0 \leq j \leq 2$. Note that $\lambda^3 = \left(-11 \pm 3\sqrt{-15}\right)/16$. Since $\lambda \in \mathbb{Q}\left(\sqrt{5}, \zeta_3\right)/\mathbb{Q}(\zeta_3)$, we must have $5|m$. Again writing

$$\sigma_3(\zeta_m) = \zeta_m \omega$$

for an appropriate primitive cube root of unity ω. If $3^2|m$, then λ and ω are in $\mathbb{Q}(\zeta_{m/3})$ and $\left[\mathbb{Q}(\zeta_m) : \mathbb{Q}\left(\zeta_{m/3}\right)\right] = 3$. Hence, writing

$$\alpha = A_0 + \zeta_m A_1 + \zeta_m^2 A_2 \ ,$$

with

$$A_i = \sum_{j \equiv i \bmod 3} a_j \zeta_m^{j-i} \in \mathbb{Q}\left(\zeta_{m/3}\right),$$

we have

$$\sigma_3(\alpha) = A_0 + \omega \zeta_m A_1 + \omega^2 \zeta_m^2 A_2,$$

and $\sigma_3(\alpha) = \lambda\alpha$ forces $A_0 = \lambda A_0$, $A_1\omega = \lambda A_1$, and $A_2\omega^2 = \lambda A_2$, which implies $\alpha = 0$. Thus $3^2 \nmid m$ and $m = 15l$.

Similarly, when $m = 15l$ and $3 \nmid l$, since $\sigma_3\left(\sqrt{5}\right) = \sqrt{5}$ and $\sigma_3\left(\sqrt{-3}\right) = -\sqrt{-3}$ we have

$$\sigma_3\left(\sqrt{5} + \sqrt{-3}\right) = \sqrt{5} - \sqrt{-3} = \left(\frac{1-\sqrt{-15}}{4}\right)\left(\sqrt{5} + \sqrt{-3}\right),$$

and $\alpha/\left(\sqrt{5} + \sqrt{-3}\right)^{\varepsilon} \zeta_3^j$ is fixed by σ_3.

■

The following lemma provides the necessary conditions to assume that the constructed element A in the proof of Theorem 3.7.2 does not vanish.

Lemma (3.7.3)

Suppose that $\alpha \in \mathbb{Q}(\zeta_m)$ *and* $\alpha \neq 0$, $p \nmid m$, *and* $\sigma_p(\alpha) = \lambda\alpha^p$. *Let* $\alpha_0, \alpha_1, \alpha_2$ *and* α_3 *be as in equations (3.7.1), (3.7.2), (3.7.3), (3.7.4).*

(i) *If* $\sigma_p(\alpha) = \alpha^p$ *then* α *is a root of unity.*

(ii) *If* $p = 3$ *and* $5\lambda^2 + 8\lambda + 5 = 0$ *then* $\alpha = \alpha_3^{\varepsilon}\zeta$ *for some root of unity* ζ, $\varepsilon = \pm 1$, *and*

$$h(\alpha) = \frac{1}{8}\log 5 = 0.201179 \ldots.$$

(iii) *If* $p = 3$ *and* $11\lambda^4 + 19\lambda^3 + 21\lambda^2 + 19\lambda + 11 = 0$ *then*

$$h(\alpha) = \frac{1}{10}\log 11 = 0.239789 \ldots.$$

(iv) *If* $p = 5$ *and* $7\lambda^2 + 11\lambda + 7 = 0$ *then* $\alpha = \alpha_0^{\varepsilon}\zeta$ *for some root of unity* ζ, $\varepsilon = \pm 1$, *and*

$$h(\alpha) = \frac{1}{12}\log 7 = 0.162159 \ldots.$$

(v) *If* $p = 5$ *and* $8\lambda^2 + 9\lambda + 8 = 0$ *then* $\alpha = \alpha_1^{\varepsilon}\zeta$ *for some root of unity* ζ, $\varepsilon = \pm 1$, *and*

$$h(\alpha) = \frac{1}{4}\log 2 = 0.173286 \ldots.$$

(vi) *If* $p = 5$ *and* $61\lambda^4 + 156\lambda^3 + 191\lambda^2 + 156\lambda + 61 = 0$ *then*

$$h(\alpha) = \frac{1}{16}\log 61 = 0.256929 \ldots.$$

(vii) *If* $p = 7$ *and* $13\lambda^2 + 23\lambda + 13 = 0$ *then*

$$h(\alpha) = \frac{1}{12}\log 13 = 0.213745 \ldots.$$

(viii) *If* $p = 7$ *and* $181\lambda^4 + 599\lambda^3 + 841\lambda^2 + 599\lambda + 181 = 0$ *then*

$$h(\alpha) = \frac{1}{25}\log 181 = 0.20794 \ldots.$$

(ix) *If* $p = 7$ *and* $193\lambda^4 + 600\lambda^3 + 815\lambda^2 + 600\lambda + 193 = 0$ *then*

$$h(\alpha) = \frac{1}{24}\log 193 = 0.219279 \ldots.$$

Statement (i) is a classical result of Dobrowolski (see [8, Lemma 2.1]).

Proof.

For statement (i), for an algebraic number α if $\sigma_p(\alpha) = \alpha^p$, then let r be the order of σ_p in $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. Then we get $\sigma_p^r(\alpha) = \alpha = \alpha^{p^r}$ thus $\alpha^{p^r-1} = 1$ and α is a root of unity.

For (ii), if $p = 3$ and $5\lambda^2 + 8\lambda + 5 = 0$ then $\lambda = (-4 \pm 3i)/5$ and $\sigma_3(\lambda) = 1/\lambda$. Hence σ_3 has order $2d$. Since we have $\sigma_3(\alpha) = \lambda\alpha^3$, we get

$$\sigma_3^2(\alpha) = \sigma_3(\lambda\alpha^3) = \lambda^{-1}\lambda^3\alpha^{3^2}$$

$$\sigma_3^3(\alpha) = \sigma_3^2(\lambda\alpha^3) = \sigma_3\left(\lambda^{-1}\lambda^3\alpha^{3^3}\right) = \lambda\,\lambda^{-3}\,\lambda^{3^2}\,\alpha^{3^3}$$

$$\sigma_3^4(\alpha) = \sigma_3^3(\lambda\alpha^3) = \sigma_3\left(\lambda\,\lambda^{-3}\,\lambda^{3^2}\,\alpha^{3^3}\right) = \lambda^{-1}\,\lambda^3\,\lambda^{-3^2}\,\lambda^{3^3}\alpha^{3^4}$$

$$\sigma_3^{2d}(\alpha) = \alpha = \lambda^{-1+3-3^2+\cdots+3^{2d-1}}\,\alpha^{3^{2d}}$$

which gives the relation

$$\alpha^{1-3^{2d}} = (\lambda^{-1})^{\frac{1-3^{2d}}{4}} \quad \Rightarrow \quad \alpha^{4(3^{2d}-1)} = (\lambda^{-1})^{(3^{2d}-1)}.$$

We also get

$$\lambda = \frac{(-4 \pm 3i)}{5} = (i\alpha_3^4)^{\pm} \Rightarrow \alpha = (\alpha_3)^{\pm}\,\zeta \text{ for some root of unity } \zeta.$$

Since λ has the minimal polynomial $5x^2 + 8\mathrm{x} + 5$ we get

$$h(\alpha) = \frac{1}{4}h(\lambda^{-1}) = \frac{1}{4}\left(\frac{1}{2}\log 5\right) = \frac{1}{8}\log 5 = 0.201179\ldots$$

Thus

$$h(\alpha) = \frac{1}{8}\log 5 = 0.201179\ldots.$$

For (iii), we first note that

$$\cos\left(\frac{2\pi}{5}\right) = \frac{-1+\sqrt{5}}{4} \quad \text{and} \quad \sin\left(\frac{2\pi}{5}\right) = \frac{\sqrt{10+2\sqrt{5}}}{4}.$$

Using these identities observe that the roots of $11x^4 + 19x^3 + 21x^2 + 19x + 11$ are in $\mathbb{Q}(\zeta_5)$ and take the form

$$\lambda_1 = -\frac{19}{44} + \frac{9}{44}\sqrt{5} + \frac{3}{22}\sin\left(\frac{2\pi}{5}\right)(1+3\sqrt{5})i,$$

$$\lambda_2 = \sigma_3(\lambda_0) = -\frac{19}{44} - \frac{9}{44}\sqrt{5} + \frac{3}{22}\sin\left(\frac{6\pi}{5}\right)(1-3\sqrt{5})i,$$

$$\sigma_3^2(\lambda_1) = 1/\lambda_1, \text{ and } \sigma_3^3(\lambda_1) = 1/\lambda_2.$$

Hence if σ_3 has order $k = 4d$ and $\sigma_3(\alpha) = \lambda\alpha^3$, then

$$\alpha = \sigma_3^k(\alpha) = \lambda^{3^{k-1}}\,\sigma_3\left(\lambda^{3^{k-2}}\right)\,\sigma_3^2\left(\lambda^{3^{k-3}}\right)\ldots\,\sigma_3^{k-1}(\lambda)\left(\alpha^{3^k}\right)$$

$$= \lambda^{3^{k-1}-3^{k-3}+3^{k-5}-\ldots-3}\;\sigma_3(\lambda)^{3^{k-2}-3^{k-4}+3^{k-6}-\ldots-1}\;\alpha^{3^k}$$

$$= \left(\lambda^3\,\sigma_3(\lambda)\right)^{(3^k-1)/10}\;\alpha^{3^k},$$

where $\lambda^3\sigma_3(\lambda)$ has minimal polynomial $11^4\,x^4 - 44209\,x^3 + 59541\,x^2 - 44209\,x + 11^4$. Thus

$$h(\alpha) = \frac{1}{10} h\left(\left(\lambda^3\, \sigma_3(\lambda)\right)^{-1}\right) = \frac{1}{10}\log 11.$$

For (iv) and (v), observe that if

$$\lambda = \frac{1}{14}\left(-11 \pm 5\sqrt{3}i\right) = (\zeta_3 \alpha_0^6)^{\pm 1}, \qquad \zeta_3 = \frac{1}{2}\left(-1 + \sqrt{3}i\right),$$

or

$$\lambda = \frac{1}{16}\left(-9 \mp 5\sqrt{7}i\right) = (-i\, \alpha_1^6)^{\pm 1}.$$

Since $\sigma_5(\zeta_3) = \zeta_3^5 = \zeta_3^{-1}$ and $\sigma_5(\zeta_7) = \zeta_7^5$, again by Lemma 3.5.3 writing Gauss sum of $\sqrt{7}i$, we get $\sqrt{7}i = 1 + 2(\zeta_7 + \zeta_7^2 + \zeta_7^4)$. Therefore we get $\sigma_5\left(\sqrt{7}i\right) = 1 + 2(\zeta_7^5 + \zeta_7^3 + \zeta_7^6)$ which is the conjugate of $1 + 2(\zeta_7 + \zeta_7^2 + \zeta_7^4)$, gives us $\sigma_5\left(\sqrt{7}i\right) = -\sqrt{7}i$. Thus $\sigma_5(\lambda) = \lambda^{-1}$. Hence if σ_5 has order $2d$ and $\sigma_5(\alpha) = \lambda\alpha^5$ then

$$\alpha = \sigma_5^{2d}(\alpha) = \lambda^{-1+5-5^2+\ \ldots +5^{2d-1}}\ \left(\alpha^{5^{2d}}\right),$$

producing

$$\alpha^{6\left(5^{2d}-1\right)} = (\lambda^{-1})^{5^{2d}-1},$$

and

$$h(\alpha) = \frac{1}{6} h(\lambda^{-1}) = \frac{1}{12}\log 7 \text{ or } \frac{1}{12}\log 8,$$

and $\alpha = \alpha_0^{\pm 1}\zeta$ or $\alpha = \alpha_1^{\pm 1}\zeta$ for some root of unity ζ.

For (vi), observe that the zeros of $61x^4 + 156x^3 + 191x^2 + 156x + 61$ take the form

$$\lambda_1 = \frac{1}{122}(-78 + 25\sqrt{3} + 5(13 + 6\sqrt{3})i),$$

$$\sigma_5(\lambda_1) = \frac{1}{122}(-78 - 25\sqrt{3} + 5(13 - 6\sqrt{3})i),$$

$$\lambda_1^{-1} \text{ and } \sigma_5(\lambda_1)^{-1}.$$

Hence if σ_5 has order $2d$ and $\sigma_5(\alpha) = \lambda\alpha^5$, then

$$\alpha = \sigma_5^{2d}(\alpha) = \sigma_5(\lambda)^{1+5^2+\cdots+5^{2d-2}}\ \lambda^{5+5^3+\ \ldots+5^{2d-1}}\ \left(\alpha^{5^{2d}}\right),$$

yielding

$$\alpha^{24(5^{2d}-1)} = ((\lambda^5\sigma_5(\lambda))^{-1})^{5^{2d}-1},$$

where $(\lambda^5\ \sigma_5(\lambda))^{-1}$ has the minimal polynomial

$$61^6x^4 - 74995263794x^3 + 54052054491x^2 - 74995263794x + 61^6,$$

and

$$h(\alpha) = \frac{1}{24}\left(\frac{1}{4}\log 61^6\right).$$

For (vii), if $p = 7$ and $\lambda = \left(-23 \pm 7\sqrt{3}i\right)/26$ then $\sigma_7(\lambda) = \lambda$.
Hence $\sigma_7(\alpha) = \lambda\alpha^7$and σ_7 has order, then

$$\alpha = \lambda^{1+7+\cdots+7^{d-1}}\ \alpha^{7^d}$$

and

$$h(\alpha) = \frac{1}{6}h(\lambda^{-1}) = \frac{1}{12}\log 13.$$

For (viii), observe that the roots of $181x^4 + 599x^3 + 841x^2 + 599x + 181$ are in $\mathbb{Q}(\zeta_5)$ and take the form

$$\lambda_1 = -\frac{599}{724} + \frac{49}{724}\sqrt{5} + \frac{7}{362}\sin\left(\frac{2\pi}{5}\right)(11 + 13\sqrt{5})i,$$

$$\lambda_2 = \sigma_7(\lambda_1) = -\frac{599}{724} - \frac{49}{724}\sqrt{5} + \frac{7}{362}\sin\left(\frac{4\pi}{5}\right)(11 - 13\sqrt{5})i,$$

$$\sigma_7^2(\lambda_1) = 1/\lambda_1, \text{ and } \sigma_7^3(\lambda_1) = 1/\lambda_2.$$

Hence if σ_7 has order $k = 4d$ and $\sigma_7(\alpha) = \lambda\alpha^7$, then

$$\alpha = \sigma_7^k(\alpha) = \lambda^{7^{k-1}}\, \sigma_7\left(\lambda^{7^{k-2}}\right)\, \sigma_7^2\left(\lambda^{7^{k-3}}\right) \ldots\, \sigma_7^{k-1}(\lambda)\left(\alpha^{7^k}\right)$$

$$= \lambda^{7^{k-1}-7^{k-3}+7^{k-5}-\ldots-7}\ \sigma_7(\lambda)^{7^{k-2}-7^{k-4}+7^{k-6}-\ldots-1}\ \alpha^{7^k}$$

$$= \left(\lambda^7\, \sigma_7(\lambda)\right)^{(7^k-1)/50}\ \alpha^{7^k},$$

where $\lambda^7\sigma_7(\lambda)$ has minimal polynomial $181^8\, x^4 - \mathrm{M}\, x^3 + \mathrm{N}\, x^2 - \mathrm{M}\, x + 181^8$ with $\mathrm{M} = 281682528266569259$ and $\mathrm{N} = 975592782269041.$

Thus

$$h(\alpha) = \frac{1}{50}h\left(\left(\lambda^7\, \sigma_7(\lambda)\right)^{-1}\right) = \frac{1}{50}(\frac{1}{4}\log(181^8) = \frac{1}{25}\log 181 = 0.207939\ldots.$$

For (ix), observe that the zeros of $193x^4 + 600x^3 + 815x^2 + 600x + 193$ take the form

$$\lambda_1 = \frac{1}{386}(-300 + 49\sqrt{3} + 7(25 + 12\sqrt{3})i),$$

$$\sigma_7(\lambda_1) = \frac{1}{386}(-300 - 49\sqrt{3} - 7(25 - 12\sqrt{3})i),$$

$$\lambda_1^{-1} \text{ and } \sigma_7(\lambda_1)^{-1}.$$

Hence if σ_7 has order $2d$ and $\sigma_7(\alpha) = \lambda\alpha^7$, then

$$\alpha = \sigma_7^{2d}(\alpha) = \sigma_7(\lambda)^{1+7^2+\cdots+7^{2d-2}}\ \lambda^{7+7^3+\ldots+7^{2d-1}}\ \left(\alpha^{7^{2d}}\right),$$

yielding

$$\alpha^{48(7^{2d}-1)} = ((\lambda^7\sigma_7(\lambda))^{-1})^{7^{2d}-1},$$

where $(\lambda^7\,\sigma_7(\lambda))^{-1}$ has the minimal polynomial $193^8x^4 - \mathrm{M}x^3 + \mathrm{N}x^2 - \mathrm{M}x + 193^8$, with $\mathrm{M} = 6860085418082952770$ and $\mathrm{N} = 9960501621392740227$ and we get

$$h(\alpha) = \frac{1}{48}\left(\frac{1}{4}\log(193^8)\right) = \frac{1}{24}\log 193 = 0.219278\ldots.$$

■

Lemma (3.7.4)

If $t = 1$ or $t > 1$ and $k \le 4t/(t-1)^2$, then

$$\sup_{|z|=1}|(z-1)^k(z+t)| = \frac{(t+1)^{k+1}}{(k+1)^{\frac{1}{2}(k+1)}}\left(\frac{k}{t}\right)^{\frac{1}{2}k},$$

achieved at

$$z = \frac{\left((t^2+1)k - 2t\right)}{2t(k+1)} \pm \frac{(t+1)\sqrt{k(4t-(t-1)^2k)}}{2t(k+1)}\,i.$$

If $t > 1$ and $k \ge 4t/(t-1)^2$, then the supremum is $2^k(t-1)$ achieved at $z = -1$.

Proof.

Writing $z = e^{i\theta}$, $u = \cos\theta$, it is readily checked that

$$|(z-1)^k(z+t)|^2 = 2^k(1-u)^k\left((t^2+1) + 2tu\right)$$

is maximized for $-1 \le u \le 1$ at

$$u = -\frac{\left((t^2+1)k - 2t\right)}{2t(k+1)}$$

provided $k \le 4t/(t-1)^2$, and at $u = -1$ when $k \ge 4t/(t-1)^2$.

■

Theorem (3.7.1)

Suppose that $\alpha \in \mathbb{Q}(\zeta_m)$, $\alpha \neq 0$, *and* α *is not a root of unity*

(i) Suppose that $3|m$ *and that* $\alpha\zeta_m^u \notin \mathbb{Q}\left(\zeta_{m/3}\right)$ *for any* u. *Then*

$$h(\alpha) \geq \frac{1}{12}\log 7 = 0.162159\ldots. \tag{3.7.5}$$

If $7 \nmid m$, *or* $m = 21l$ *with* $3 \nmid l$ *and* $\frac{\alpha}{\alpha_0^{\varepsilon}\zeta_3^j} \notin \mathbb{Q}(\zeta_{7l})$, *for any* $\varepsilon = \pm 1, j = 0,1,2$, *where* α_0 *is a root of* $7x^{12} - 13x^6 + 7$, *then*

$$h(\alpha) \geq \frac{1}{4}\log 2 = 0.173286\ldots. \tag{3.7.6}$$

If further $5 \nmid m$ *or* $m = 15l$ *with* $3 \nmid l$ *and* $\frac{\alpha}{(\sqrt{5}+\sqrt{-3})^{\varepsilon}\zeta_3^j} \notin \mathbb{Q}(\zeta_{5l})$ *for any* $\varepsilon = \pm 1$, $j = 0,1,2, or\ if\ 9|m, then$

$$h(\alpha) \geq 0.174878. \tag{3.7.7}$$

(ii) Suppose that $2|m$ *and that* $\alpha\zeta_m^u \notin \mathbb{Q}(\zeta_{m/2})$ *for any* u. *Then*

$$h(\alpha) \geq \frac{1}{4}\log 2 = 0.173286\ldots. \tag{3.7.8}$$

If $m = 4l$ *with* l *odd, and* $(1 \pm i)\alpha \notin \mathbb{Q}(\zeta_l)$ *then*

$$h(\alpha) \geq \frac{1}{8}\log 5 = 0.201179\ldots. \tag{3.7.9}$$

If further $5 \nmid m$, *or* $m = 20l$ *with* l *odd, and* $\frac{\alpha}{\alpha_3^{\varepsilon} i^j} \notin \mathbb{Q}(\zeta_{5l})$, $for\ any\ \varepsilon = \pm 1$, $j = 0,1,2,3, where\ \alpha_3 = \sqrt{\frac{5+\sqrt{5}}{10}} + \sqrt{\frac{5-\sqrt{5}}{10}}\, i\ \in \mathbb{Q}(\zeta_{20})$, *or if* $8|m$, *then*

$$h(\alpha) \geq 0.210291. \tag{3.7.10}$$

Proof.

Suppose that $3|m$. From Lemma 3.7.1 we have

$$|\alpha^3 - \sigma_3(\alpha)^3|_v \leq |3|_v^{3/2} \max\{1, |\alpha|_v\}^3 \max\{1, |\sigma_3(\alpha)|_v\}^3.$$

Similarly,

$$|\alpha^3 + 2\sigma_3(\alpha)^3|_v = |\alpha^3 - \sigma_3(\alpha)^3 + 3\sigma_3(\alpha)^3|_v$$

$$\leq |3|_v \max\{1, |\alpha|_v\}^3 \max\{1, |\sigma_3(\alpha)|_v\}^3 \ ,$$

$$|7\alpha^6 + 13\alpha^3\sigma_3(\alpha)^3 + 7\sigma_3(\alpha)^6|_v = |\ 7(\alpha^3 - \sigma_3(\alpha)^3)^2 + 27\ \alpha^3\ \sigma_3(\alpha)^3|_v$$

$$\leq |3|_v^3\ \max\{1, |\alpha|_v\}^6 \max\{1, |\sigma_3(\alpha)|_v\}^6,$$

and

$$|8\alpha^6 + 11\alpha^3\sigma_3(\alpha)^3 + 8\sigma_3(\alpha)^6|_v = |\ 8(\alpha^3 - \sigma_3(\alpha)^3)^2 + 27\ \alpha^3\ \sigma_3(\alpha)^3|_v$$

$$\leq |3|_v^3\ \max\{1, |\alpha|_v\}^6 \max\{1, |\sigma_3(\alpha)|_v\}^6$$

for finite places v.

We consider the quantity

$$A = \ (\alpha^3 - \sigma_3(\alpha)^3)^k\ \ (\alpha^3 + 2\sigma_3(\alpha)^3)^l\ \ (\ 7\alpha^6 + 13\alpha^3\sigma_3(\alpha)^3 + 7\sigma_3(\alpha)^6)^t$$

$$(8\alpha^6 + 11\alpha^3\sigma_3(\alpha)^3 + 8\sigma_3(\alpha)^6)^s.$$

Setting $\beta = \alpha^3/\sigma_3(\alpha)^3$, then as long as $\beta \neq 1$ when $k > 0$, β is not a zero of $7x^2 + 13x + 7$ when $t > 0$, and β is not a zero of $8x^2 + 11x + 8$ when $s > 0$, we have $A \neq 0$. Thus, writing

$$h(\alpha) = \log H(\alpha),$$

where

$$H(\alpha) = \prod_{v \nmid \infty} \max\{1, |\alpha|_v\},$$

the product formula produces

$$1 = \prod_{v\nmid\infty} |A|_v \prod_{v|\infty} |A|_v.$$

Since $|\alpha|_v = 1$ for all $v|\infty$, we have

$$\prod_{v\nmid\infty} |A|_v \le \prod_{v\nmid\infty} |3|_v^{3k/2+l+3t+3s} \left(\prod_{v\nmid\infty} \max\{1, |\alpha|_v\} \max\{1, |\sigma_3(\alpha)|_v\} \right)^{3k+3l+6t+6s}$$

$$= 3^{-(1.5k+l+3t+3s)} H(\alpha)^{6(k+l+2t+2s)},$$

and

$$\prod_{v|\infty} |A|_v = \prod_{v|\infty} |(\beta-1)^k (\beta+2)^l (7\beta^2+13\beta+7)^t (8\beta^2+11\beta+8)^s|_v$$

$$\le \prod_{v|\infty} \sup_{|z|=1} |(z-1)^k (z+2)^l (7z^2+13z+7)^t (8z^2+11z+8)^s|^{d_v/d}$$

$$= \sqrt{M},$$

where

$$M = \sup_{|z|=1} |(z-1)^k (z+2)^l (7z^2+13z+7)^t (8z^2+11z+8)^s|^2$$

$$= \sup_{-1\le u\le 1} 2^k (1-u)^k (5+4u)^l (14u+13)^{2t} (16u+11)^{2l}.$$

Hence

$$h(\alpha) \ge \frac{\log\left(3^{1.5k+l+3t+3s}/\sqrt{M}\right)}{6(k+l+2t+2s)}.$$

When $\beta \ne 1$, by taking $s = t = 0, k = 6,$ and $l = 1$, we have $M = 3^{20}/7^7$, achieved at $u = -13/14$, producing

$$h(\alpha) \geq \frac{1}{12}\log 7.$$

When $\beta \neq 1$ and β is not a root of $7x^2 + 13x + 7$, taking $s = 0, k = 14$, and $l = 0$, and $t = 1$, we have $M = (3/2)^{48}$, achieved at $u = -11/16$, giving

$$h(\alpha) \geq \frac{1}{4}\log 2.$$

When $\beta \neq 1$ and β is not a root of $7x^2 + 13x + 7$ or $8x^2 + 11x + 8$, then choosing $k = 303$, and $l = 0, t = 37$ and $s = 17$, yields

$$h(\alpha) \geq 0.174878.$$

The restrictions on α (corresponding to the restrictions on β) needed for these bounds follow from Lemma (3.7.2), parts (i) and (iii).

For $2|m$, we assume $\beta = \alpha^2/\sigma_2(\alpha)^2 \neq 1$, and take

$$A = (\alpha^2 - \sigma_2(\alpha)^2)^k \ (\alpha^2 + \sigma_2(\alpha)^2)^l \ (5\alpha^4 + 6\alpha^2\sigma_2(\alpha)^2 + 5\sigma_2(\alpha)^4)^t,$$

where for $v \nmid \infty$

$$|\alpha^2 - \sigma_3(\alpha)^2|_v \leq |2|_v^2 \max\{1, |\alpha|_v\}^2 \max\left\{1, \left|\sigma_p(\alpha)\right|_v\right\}^2,$$

$$|\alpha^2 + \sigma_3(\alpha)^2|_v = |(\alpha^2 - \sigma_3(\alpha)^2) + 2\sigma_3(\alpha)^2|_v$$

$$\leq |2|_v \max\{1, |\alpha|_v\}^2 \max\left\{1, \left|\sigma_p(\alpha)\right|_v\right\}^2,$$

and

$$|5\alpha^4 + 6\alpha^2\sigma_2(\alpha)^2 + 5\sigma_2(\alpha)^4|_v = |5(\alpha^2 - \sigma_2(\alpha)^2)^2 + 2^4\,\alpha^2\,\sigma_2(\alpha)^2|_v$$

$$\leq |2|_v^4 \ \max\{1, |\alpha|_v\}^4 \ \max\left\{1, \left|\sigma_p(\alpha)\right|_v\right\}^4.$$

Hence, as long as $A \neq 0$, we have

$$h(\alpha) \geq \frac{\log\left(2^{2k+l+4t}/\sqrt{M}\right)}{4(k+l+2t)},$$

where

$$M = \sup_{|z|=1} |(z-1)^k (z+1)^l (5z^2+6z+5)^t|^2$$

$$= \sup_{-1 \leq u \leq 1} 2^{k+l+2t} (1-u)^k (1+u)^l (5u+3)^{2t}.$$

If $k = 1$ and $l = t = 0$, then $M = 4$, achieved at $u = -1$, which yields the Amoroso & Dvornicich bound,

$$h(\alpha) \geq \frac{1}{4}\log 2.$$

If $\beta \neq -1$, then choosing $k = 4$ and $l = 1$ produces $M = 2^{18}/5^5$, achieved at $u = -3/5$, from which one calculates

$$h(\alpha) \geq \frac{1}{8}\log 5.$$

Finally, when $\beta \neq -1$ and β is not a zero of $5x^2 + 6x + 5$, taking $k = 181$, $l = 37$, and $t = 17$, and calculating M numerically, we find the bound

$$h(\alpha) \geq 0.210291.$$

The conditions on α (for the various restrictions on β) follow from Lemma (3.7.2) parts (i) and (ii).

■

The bounds (3.7.7) and (3.7.10) can probably be improved, but the examples α_i with $0 \leq i \leq 3$ shows that the other bonds are sharp, as well as the necessity of the restrictions on the form of any α having smaller height.

From **Theorem (3.7.1)**, plainly any abelian α of height below

$$\frac{1}{12}\log 7 = 0.162159\ldots$$

must (if it exist, and after dividing by a root of unity as necessary) have $\gcd(6, m) = 1$. Amoroso & Dvornicich also obtained the bounds

$$h(\alpha) \geq \begin{cases} \frac{1}{6}\log(5/2) = 0.152715\ldots & \text{if } 5 \nmid m, \\ \frac{1}{8}\log(7/2) = 0.156595\ldots & \text{if } 7 \nmid m, \\ \frac{1}{12}\log(11/2) = 0.1420662\ldots & \text{if } 11 \nmid m. \end{cases}$$

We improved these bounds in the following theorem to deduce that an abelian α with height below

$$\frac{1}{12}\log 7 = 0.162159\ldots$$

must in fact have $35|m$.

Theorem (3.7.2)

Suppose that $\alpha \in \mathbb{Q}(\zeta_m)$, $\alpha \neq 0$, *and* α *is not a root of unity*

(i) *If* $3 \nmid m$ *then* $h(\alpha) \geq 0.155090\ldots$

(ii) *If* $5 \nmid m$ *then* $h(\alpha) \geq 0.169438\ldots$ *unless* $\alpha = \alpha_0^{\varepsilon}\zeta$ *with* $\varepsilon = \pm 1$ *and* ζ *a root of unity, whence*

$$h(\alpha) = \frac{1}{12}\log 7 = 0.162159\ldots$$

(iii) *If* $7 \nmid m$ *then* $h(\alpha) \geq 0.16338541\ldots$

Proof.

The proof is similar to the proof of Theorem 3.7.1. When $p \nmid m$ (we take $p = 3, 5,$ or 7) we consider

$$A = A_1^k A_2^l \prod_{i=1}^{I} A_{3,i}^{t_i} \prod_{j=1}^{J} A_{4,j}^{s_j},$$

where

$$A_1 = \alpha^p - \sigma_p(\alpha),$$

$$A_2 = \tfrac{1}{2}(p-1)\alpha^p + \tfrac{1}{2}(p+1)\sigma_p(\alpha),$$

and for i and j,

$$A_{3,i} = D_i\big(\alpha^p - \sigma_p(\alpha)\big)^2 + \mathrm{E_i}\, p^2\alpha^p\sigma_p(\alpha)\,,$$

$$A_{4,i} = C_j\big(\alpha^p - \sigma_p(\alpha)\big)^4 + B_j\, p^2\alpha^p\sigma_p(\alpha)\left(\alpha^p - \sigma_p(\alpha)\right)^2 + p^4\alpha^{2p}\,\sigma_p(\alpha)^2$$

for integers $B_j, C_j,$ and D_j, with $D_1 = (p^2+3)/4$, $E_1 = 1$.

From Lemma (3.7.1) for $v \nmid \infty$, we have

$$|A_1|_v \le |p|_v \max\{1, |\alpha|_v\}^p \ \max\left\{1, \left|\sigma_p(\alpha)\right|_v\right\},$$

$$|A_2|_v = \left|\frac{1}{2}(p-1)\big(\alpha^p - \sigma_p(\alpha)\big) + \ p\ \sigma_p(\alpha)\right|_v$$

$$\le |p|_v \max\{1, |\alpha|_v\}^p \ \max\left\{1, \left|\sigma_p(\alpha)\right|_v\right\},$$

$$\left|A_{3,i}\right|_v \le |p|_v^2 \max\{1, |\alpha|_v\}^{2p} \ \max\left\{1, \left|\sigma_p(\alpha)\right|_v\right\}^2,$$

for each i, and

$$\left|A_{4,j}\right|_v \le |p|_v^4 \max\{1, |\alpha|_v\}^{4p} \max\left\{1, \left|\sigma_p(\alpha)\right|_v\right\}^4$$

for each j. Hence, as long as $A \neq 0$, we find from the product formula,

$$1 \le p^{-\left(k+l+2\sum_i t_i+4\sum_j s_j\right)} H(\alpha)^{(p+1)\left(k+l+2\sum_i t_i+4\sum_j s_j\right)} M^{\frac{1}{2}},$$

where

$$M = \sup_{|z|=1} \left| \begin{array}{c} (1-z)^k \left(\frac{1}{2}(p-1)z + \frac{1}{2}(p+1)\right)^l \prod_{i=1}^{I} (D_i(z-1)^2 + p^2 z)^{t_i} \\ \prod_{j=1}^{J} \left(C_j(z-1)^4 + B_j\, p^2\, z(z-1)^2 + p^4 z^2\right)^{s_j} \end{array} \right|^2$$

$$= \sup_{u\in[-1,1]} \left\{ \begin{array}{c} 2^k(1-u)^k \left(\frac{1}{2}(p^2+1) + \frac{1}{2}(p^2-1)u\right)^l \prod_{i=1}^{I} (2D_i(u-1) + p^2)^{2t_i} \\ \prod_{j=1}^{J} \left(4C_j(u-1)^2 + 2B_j\, p^2\, (u-1) + p^4\right)^{2s_j} \end{array} \right\}.$$

Since $\lambda = \sigma_p(\alpha)/\alpha^p$ is not 1 (as α is not a root of unity) or $-(p-1)/(p+1)$ (as $|\lambda| = 1$, we know that $A_1 A_2 \neq 0$. For $l = 1$, and all the $t_i, s_j = 0$, the optimal k is readily determined: By Lemma (3.7.4), with $t = (p+1)/(p-1)$, the maximum for $k \le p^2 - 1$ occurs at

$$u = -\left((p^2+1)k - (p^2-1)\right)/(p^2-1)(k+1),$$

leading to the bound

$$h(\alpha) \ge \frac{\log\left(\left(\frac{p^2-1}{4k}\right)^{\frac{1}{2}k} (k+1)^{\frac{1}{2}(k+1)}\right)}{(p+1)(k+1)}.$$

This is readily seen to be maximized by taking $k = (p^2 - 1)/4$, with corresponding value of $u = -(p^2 - 3)/(p^2 + 3)$, producing the lower bound

$$h(\alpha) \geq \frac{\log\left(\frac{p^2+3}{4}\right)}{2(p+1)}.$$

When $p \leq 13$ this improves upon Amoroso & Dvornicich's bounds. For $p > 13$ we are already below their unconditional lower bound (note that when p increases such bounds weaken rapidly). For our bounds we will use only $p = 3, 5, 7$.

In particular, with $p = 5$ we recover the bound

$$h(\alpha) \geq \frac{1}{12}\log 7 = 0.162159\ldots$$

when $5 \nmid m$, with equality only possible when $7\lambda^2 + 11\lambda + 7 = 0$.

When $p = 3$, we clearly have

$$\lambda \neq -\frac{p^2-3}{p^2+3} \pm \frac{2p}{p^2+3}\sqrt{3}\,i$$

and $A_{3,1} \neq 0$.

From Lemma (3.7.3), part (iv) and (vii), we may assume this also for $p = 5$ and 7. For $p = 7$, the choice $k = 218, l = 14, t_1 = 7$ and $J = 0$ yields the lower bound

$$\log H(\alpha) \geq 0.1623680562\ldots.$$

For $p = 3$, we take $(D_2, E_2) = (5,2)$, $(C_1, B_1) = (11,7)$ and $(C_2, B_2) = (13,8)$. From Lemma (3.7.3), part (ii) and (iii), we can assume $A_{3,2} \neq 0$ and $A_{4,1} \neq 0$. Since the zeros of $13x^4 + 20x^3 + 15x^2 + 20x + 13$ are

$$\left(-\frac{5}{26}(2 - 3i) \pm \frac{3}{26}\sqrt{3}(3 + 2i)\right)^{\pm 1}$$

and we are assuming that $3 \nmid m$, we may also assume that $A_{4,2} \neq 0$. We carry out our numerical computations by programming in Mathematica and Maple. Using a hill- climbing strategy, we

find that for the choice $k = 823, l = 178, t_1 = 183, t_2 = 7, s_1 = 48,$ and $s_2 = 53$ produces the bound

$$h(\alpha) \geq 0.155090 \ldots.$$

For $p = 5$, we take $(D_1, E_1) = (7,1), (D_2, E_2) = (8,1)$ and $(C_1, B_1) = (55, 15)$, $(C_2, B_2) = (61,16)$. From Lemma (3.7.3), part (iv), (v) and (vi), we may assume that $A_{3,1}\, A_{3,2} \neq 0$ and $A_{4,2} \neq 0$. We can also assume $A_{4,1} \neq 0$, since the zeros of $5(11x^4 + 31x^3 + 41x^2 + 31x + 11)$ are given by

$$\left(-\frac{31}{44} + \frac{5\sqrt{5}}{44} \pm \frac{1}{22}\sin\left(\frac{2\pi}{5}\right)(5 + 7\sqrt{5})\mathrm{i}\right)^{\pm 1}$$

and we are assuming that $5 \nmid m$.

Taking $k = 340,\ l = 10,\ t_1 = 29,\ t_2 = 1,\ s_1 = 10,$ and $s_2 = 8$, we obtain

$$\log H(\alpha) \geq 0.169438 \ldots.$$

For $p = 7$, we take $(D_2, E_2) = (14,1)$, $(C_1, B_1) = (181,27)$ and $(C_2, B_2) = (193,28)$. From Lemma (3.7.3), part (viii) and (ix), we can assume $A_{4,1} \neq 0$ and $A_{4,2} \neq 0$. Since the zeros of $7(2x^2 + 3x + 2)$ are of the form

$$\left(\frac{1}{4}(-3 \pm i\sqrt{7}\right)$$

and we are assuming that $7 \nmid m$, thus we may also assume that $A_{3,2} \neq 0$. We find that the choice $k = 309,\ l = 16,\ t_1 = 9,\ t_2 = 2,\ s_1 = 4,$ and $s_2 = 1$ gives the bound

$$h(\alpha) \geq 0.16338541 \ldots.$$

■

Note that when $2 \nmid m$, taking

$$A = (\alpha^4 - \sigma_2(\alpha)^2)^4 \, (\alpha^4 + \sigma_2(\alpha)^2)$$

yields

$$1 \leq 2^{-9} \, H(\alpha)^{30} \left(2^9 / 5^{5/2}\right),$$

recovering the Amoroso & Dvornicich bound $H(\alpha) \geq 5^{1/12}$ without the need for their Lemma 4 inequality, similar to the simplification in [14] of the proof of Schinzel's theorem. Constructing additional auxiliary polynomials as in [9] would produce something marginally better and could be used in a similar way to improve the bound in (i) slightly.

CHAPTER 4 - **HEIGHTS OF ROOTS OF POLYNOMIALS WITH ODD COEFFICIENTS**

4.1 Heights of Polynomials in D_m

Here we will show that the height of a non-zero non root of unity α which is a zero of a polynomial with all odd coefficients of degree n satisfies

$$h(\alpha) \geq \frac{0.4278}{n+1}.$$

More generally we obtain bounds when the coefficients are all congruent to 1 modulo m for some $m \geq 2$.

For an integer $m \geq 2$, let D_m denote the set of integer polynomials $f(x)$ whose coefficients a_i all satisfy $a_i \equiv 1 \pmod{m}$, i.e.

$$D_m = \left\{ \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[x] : a_i \equiv 1 \pmod{m}, 0 \leq i \leq d \right\}.$$

A Littlewood polynomial is a class of polynomials which has all its coefficients equal to ± 1. It is clear that D_2 contains the class of Littlewood polynomials. For the class of nonreciprocal polynomials with all odd coefficients, P. Borwein, G. Hare and J. Mossinghoff [5] showed that

$$M(f) \geq M(x^2 - x - 1) = \frac{1+\sqrt{5}}{2}.$$

Note that there is no better bound even if we restrict to the subclass of nonreciprocal Littlewood polynomials, since $x^2 - x - 1$ is a nonreciprocal Littlewood polynomial. Now for a polynomial of degree n in D_m with no cyclotomic factors Borwein, Dobrowolski & Mossinghoff [4] proved that

$$\log M(f) \geq c_m \frac{n}{n+1}$$

with

$$c_2 = \frac{1}{4}\log 5 = 0.402359\ldots, c_3 = 0.459003 \text{ and } c_m = \log\left(\frac{\sqrt{m^2+1}}{2}\right) \text{ for } m > 3.$$

These constants were improved in [9] to obtain $c_2 = 0.416230\ldots$, general bounds of strength

$$c_m = \begin{cases} \log\left(\frac{m}{2}\right) + \frac{(3-\log 3)}{2m^2} + O\left(\frac{1}{m^4}\right) & \text{if } m \geq 3 \text{ odd,} \\ \log\left(\frac{m}{2}\right) + \frac{(4-\log 4)}{m^2} + O\left(\frac{1}{m^4}\right) & \text{if } m \geq 4 \text{ even,} \end{cases}$$

and particular values

$$c_3 = 0.501026\ldots, c_4 = 0.832461\ldots, c_5 = 0.952869, c_6 = 1.165884,$$

$$c_7 = 1.271775, c_8 = 1.425369, c_9 = 1.515669, c_{10} = 1.634836,$$

$$c_{11} = 1.712539.$$

In this section we will give a more straightforward proof to obtain bounds of the form

$$h(\alpha) \geq c_m \frac{1}{n+1} \tag{4.1.1}$$

when α is a zero of a polynomial $f(x)$ in D_m of degree n, but not a $2(n+1)$st root of unity. Suppose if $f(x)$ in D_m has d noncyclotomic roots $\alpha_1, \alpha_2, \ldots, \alpha_d$, then from $\log M(f) \geq h(\alpha_1) + h(\alpha_2) + \cdots + h(\alpha_d)$ and (4.1.1) we get

$$\log M(f) \geq c_m \frac{d}{n+1}$$

where d is the degree of the non-cyclotomic part of $f(x)$ (the type of bound obtained in Theorem (2.2) of [9]). In particular when f has no cyclotomic factors or the degree of the noncyclotomic part is a positive proportion of the degree of f then we get a Lehmer type constant lower bound for $M(f)$. Of course we would prefer to get a constant bound for any factor of $f(x)$ (but this seems to be a much harder problem).

The following theorem called Capelli's Theorem will be used as a tool in the proofs of the Lemma 4.1.

Capelli's Theorem

Let k be a field. The binomial $x^N - a$ is reducible over k if and only if either of the following holds.

(i) *There exist a prime $p|N$ such that $a = \lambda^p$ for some $\lambda \in k$, or*

(ii) $4|N$ *and* $a = -4\mu^4$ *for some* $\mu \in k$.

Lemma 4.1

Let m be a positive integer and define the polynomials

$$g_1(z) = \frac{1}{2}(m-\delta)z + \frac{1}{2}(m+\delta) \qquad \textit{and}$$

$$g_2(z) = \frac{1}{4}\left(m^2 + (4-\delta)\right)z^2 + \frac{1}{2}\left(m^2 - (4-\delta)\right)z + \frac{1}{4}\left(m^2 + (4-\delta)\right),$$

where $\delta = \begin{cases} 1 & \text{if } m \text{ odd,} \\ 0 & \text{if } m \text{ even.} \end{cases}$

Then the polynomial $F_1(z) = g_1(z^N)$ is irreducible over $\mathbb{Q}$ when m is odd and the polynomial $F_2(z) = g_2(z^N)$ is irreducible over $\mathbb{Q}$ when $4|m$ with m even or $3 \nmid m$ with m odd for any positive integer N.

Proof of Lemma 4.1

We first consider $F_1(z) = g_1(z^N)$ with $m = 2k+1$, m odd. By Capelli's Theorem $(k)z^N + (k+1) = 0$ is reducible if and only if $-(k+1)/(k)$ is a nontrivial prime power of a rational number (i.e when is p odd, $-(k+1)/(k) = -(a/b)^p$ for some positive $a, b \in \mathbb{Z}$ with $\gcd(a,b) = 1$ which leads to the equation $a^p - b^p = 1$; when $p = 2$, $(k+1)/(k) = 4(a/b)^4$ for some positive $a, b \in \mathbb{Z}$ which leads to the equation $4a^4 - b^4 = (2a^2 - b^2)(2a^2 + b^2) = 1$). Observe that these differences cannot be 1, thus $(k+1)/(k)$ cannot be a rational power. Therefore $F_1(z) = g_1(z^N)$ is irreducible.

Now suppose $F_2(z)$ is reducible over $\mathbb{Q}$ for both cases when $4|m$ with $m = 2l$ (l even) or when $3 \nmid m$ with $m = 2l + 1$ (m odd). Then any factor of $F_2(z) = g_2(z^N)$ must have degree $2d < 2N$ since the roots of $F_2(z)$ are all complex and also lie in the unit circle. We see that when $m = 2l$ (l even) then we get

$$(l^2 + 1)\alpha^{2N} + 2(l^2 - 1)\alpha^N + (l^2 + 1) = 0$$

which implies

$$\alpha^N = -\left(\frac{l+i}{l-i}\right) \text{ or } -\left(\frac{l-i}{l+i}\right).$$

When $m = 2l + 1$, odd case we have

$$(m^2 + 3)\alpha^{2N} + 2(m^2 - 3)\alpha^N + (m^2 + 3) = 0$$

implies that

$$\alpha^N = \frac{-(m+\sqrt{3}i)/2}{(m-\sqrt{3}i)/2} \text{ or } \frac{-(m-\sqrt{3}i)/2}{(m+\sqrt{3}i)/2}.$$

Now set

$$A = \frac{1}{4}\left(m^2 + (4 - \delta)\right)$$

and let θ be any root of a factor of $F_2(z)$ of degree $2d$ with leading coefficient B. By the definition of height $nh(\theta) = \log M(f)$, we get $2dh(\theta) = \log(B)$, $\log A = 2Nh(\theta)$. Thus $B^{1/2d} = A^{1/2N}$. This implies A must be a $N/(N,d)$th power of B. Therefore when $4|m$, m even we get $l^2 + 1 = y^p$ for some integer $y > 1$ and prime $p|(N/(N,d))$. But the equation

$$l^2 + 1 = y^p$$

is a special case of Catalan's conjecture and does not have solutions (see [16]). Thus when $4|m$, m even $F_2(z)$ is irreducible. Now when $3 \nmid m$, m odd we get $l^2 + l + 1 = y^p$ for some integer $y > 1$ and prime $p|(N/(N,d))$. But the equation

$$(l^2 + l + 1) = y^p$$

has no solutions for $p \neq 3$ (see [21]). The only solution to the equation $(l^2 + l + 1) = y^p$ is when $p = 3,\ y = 7,\ l = 18$ (see [18]) which gives us $m = 37$. Thus for any $m \neq 37,\ m$ odd $F_2(z) = g_2(z^N)$ is irreducible.

When $m = 37$ we have

$$F_2(z) = g_2(z^N) = 7^3 z^{2N} + 683 z^N + 7^3 = 7^3 (z^N - \alpha)(z^N - \alpha^{-1}).$$

Now by Capelli's Theorem $F_2(z)$ is reducible only if any root α (or α^{-1}) of $g_2(z)$ is a prime power in $\mathbb{Q}(\sqrt{3}i)$ or $-4\mu^4$ for some $\mu \in \mathbb{Q}(\sqrt{3}i)$, i.e.

$$\alpha = -\frac{(683 + 37\sqrt{3}i)}{2(7^3)} = \lambda^p \text{ or } -4\mu^4 \text{ for some } \lambda, \mu \in \mathbb{Q}(\sqrt{3}i).$$

Since

$$\alpha = -\frac{(683 + 37\sqrt{3}i)}{2(7^3)} = \left(\frac{1 - \sqrt{3}i}{2}\right)\left(\frac{1 + 4\sqrt{3}i}{7}\right)^3 = \left(\frac{1 - \sqrt{3}i}{2}\right)\left(\frac{(2 + \sqrt{3}i)^2}{(2 + \sqrt{3}i)(2 - \sqrt{3}i)}\right)^3$$

$$= \left(\frac{1 - \sqrt{3}i}{2}\right)\left(\frac{(2 + \sqrt{3}i)}{(2 - \sqrt{3}i)}\right)^3,$$

and considering the prime factorization of any integer in $\mathbb{Q}(\sqrt{3}i)$ (any integer in $\mathbb{Q}(\sqrt{3}i)$ factors in to product of two primes or square of a prime or remains as a prime in $\mathbb{Q}(\sqrt{3}i)$) we only get the possibility $p = 3$. But this cannot happen since we know $\alpha = \zeta_6\, \lambda^3$ for some $\lambda \in \mathbb{Q}(\sqrt{3}i)$ where ζ_6 the sixth root of unity as

$$\alpha = \left(\frac{1 - \sqrt{3}i}{2}\right)\left(\frac{(2 + \sqrt{3}i)}{(2 - \sqrt{3}i)}\right)^3.$$

Since ζ_6 is not a cube root in $\mathbb{Q}(\sqrt{3}i)$ (i.e. $\zeta_{18} \notin \mathbb{Q}(\sqrt{3}i)$) we have $F_2(z) = g_2(z^N)$ is irreducible.

■

Theorem 4.1

If α is a zero of a polynomial $f(x)$ in D_m of degree n and α is not an $2(n+1)$st root of unity (not an $(n+1)$st if $m \geq 3$), then (4.1.1) holds with

$$c_2 = 0.427800,$$

and

$$c_m = \log\left(\frac{m}{2}\right) + \frac{2.947486 - \frac{1}{2}\delta}{m^2} + O\left(\frac{1}{m^4}\right), \text{where } \delta = \begin{cases} 1 & \text{if } m \geq 3 \text{ odd,} \\ 0 & \text{if } m \geq 4 \text{ even.} \end{cases}$$

For small $m \geq 3$ we show the following improvements:

$$c_3 = 0.620362,\ c_4 = 0.855600,\ c_5 = 1.016628,\ c_6 = 1.179916,$$

$$c_7 = 1.307083,\ c_8 = 1.434141,\ c_9 = 1.538934,\ c_{10} = 1.640027,$$

$$c_{11} = 1.728890.$$

We note here an asymptotically less precise bound

$$c_m = \begin{cases} \frac{1}{2}\log\left(\frac{m^2+3}{4}\right) & \text{if } m \geq 3 \text{ odd,} \\ \frac{1}{2}\log\left(\frac{m^2+4}{4}\right) & \text{if } m \geq 4 \text{ even,} \end{cases} \tag{4.1.2}$$

can be easily obtained (the even case had already been showed and improved in [9]). We remark that the optimal c_m in (4.1.1) certainly satisfies (upper bound on c_m can be seen in Theorem 4.2)

$$c_m = \log m + O(1).$$

Proof of Theorem 4.1

Suppose α is a zero of a polynomial $f(x)$ in D_m of degree n then

$$f(x) = \frac{x^{n+1} - 1}{x - 1} + m\, r(x)$$

for some $r(x)$ of degree at most n in $\mathbb{Z}[x]$.

Now writing $\beta = \alpha^{n+1}$, we get

$$f(\alpha) = 0 = \frac{\alpha^{n+1} - 1}{\alpha - 1} + m\, r(\alpha) \;\Rightarrow\; (\beta - 1) = -\big(m(\alpha - 1)\, r(\alpha)\big).$$

Hence for all finite places $v \nmid \infty$ we have

$$|\beta - 1|_v = |m(\alpha - 1)\, r(\alpha)|_v \leq |m|_v \max\{1, |\beta|_v\}. \tag{4.1.3}$$

For $m = 2$ we take

$$g(z) = (z-1)^k\,(z+1)^l\,(5z^2 + 6z + 5)^t\,(29z^4 + 60z^3 + 78z^2 + 60z + 29)^w$$

$$(3z^2 + 2z + 3)^c (33z^4 + 60z^3 + 70z^2 + 60z + 33)^e$$

$$(169z^6 + 490z^5 + 871z^4 + 1036z^3 + 871z^2 + 490z + 169)^s.$$

Thus for $v \nmid \infty$

$$|\beta - 1|_v \leq |2|_v \max\{1, |\beta|_v\},$$

$$|\beta + 1|_v = |\beta - 1 + 2|_v \leq |2|_v \max\{1, |\beta|_v\},$$

and

$$|\beta^2 - 1|_v \leq |2|_v^2 \max\{1, |\beta|_v\}^2 \tag{4.1.4}$$

giving

$$|\beta^2 + 1|_v = |\beta^2 - 1 + 2|_v \leq |2|_v \max\{1, |\beta|_v\}^2,$$

$$|5\beta^4 + 6\beta^2 + 5|_v = |5(\beta^2 - 1)^2 + 16\beta^2|_v \leq |2|_v^4 \max\{1, |\beta|_v\}^4,$$

$$|3\beta^4 + 2\beta^2 + 3|_v = |3(\beta^2 - 1)^2 + 8\beta^2|_v \leq |2|_v^3 \max\{1, |\beta|_v\}^4.$$

For integers A, B, C, D (the quartic factors in $g(z)$ correspond to $(A, B, C) = (29, 11, 1)$ and $(33, 12, 1)$, and the sextic to $(A, B, C, D) = (169, 94, 17, 1)$, we thus have

$$|A(\beta^2 - 1)^4 + B\ 2^4\beta^2(\beta^2 - 1)^2 + C\ 2^8\beta^4|_v \leq |2|_v^8 \max\{1, |\beta|_v\}^8,$$

$$|A(\beta^2 - 1)^6 + B\ 2^4\beta^2(\beta^2 - 1)^4 + C\ 2^8\beta^4(\beta^2 - 1)^2 + D\ 2^{12}\beta^6|_v \leq |2|_v^{12} \max\{1, |\beta|_v\}^{12}.$$

Hence we have

$$|g(\beta^2)|_v \leq |2|_2^{2k+l+4t+8w+3c+8e+12s} \max\{1, |\beta|_v\}^{2 \deg g}, \text{ for } v \nmid \infty.$$

Now For $v|\infty$ and $|\beta|_v > 1$ we observe that

$$|g(\beta^2)|_v = |\beta|_v^{2 \deg g} |g(\beta^{-2})|_v$$

with $|\beta^{-2}|_v < 1$.
Hence for $v|\infty$

$$|g(\beta^2)|_v \leq \max\{1, |\beta|_v\}^{2 \deg g} \left(\sup_{|z| \leq 1} |g(z)| \right)^{d_v/d} = \max\{1, |\beta|_v\}^{2 \deg g} \left(\sqrt{M}\right)^{d_v/d},$$

where writing $z = e^{it}$ and $u = \cos t$,

$$M = \sup_{|z|=1} |g(z)|^2 = 2^{k+l+2t+4w+2c+4e+6s} L$$

with

$$L = \sup_{-1 \leq u \leq 1} \left\{ \begin{matrix} (1-u)^k (1+u)^l (5u+3)^{2t} (29u^2 + 30u + 5)^{2w} (3u+1)^{2c} \\ (33u^2 + 30u + 1)^{2e} (169u^3 + 245u^2 + 91u + 7)^{2s} \end{matrix} \right\}.$$

We want to apply the product formula to our constructed element $g(\beta^2)$. Thus we need to justify that $g(\beta^2) \neq 0$. By the assumption that α is not an $2(n+1)$st root of unity we have $\beta^2 \neq 1$, and from (4.1.4) we observe that clearly $\beta^2 \neq -1$.

We also observe that the factors

$$5z^{4(n+1)} + 6z^{2(n+1)} + 5,$$

$$3z^{4(n+1)} + 2z^{2(n+1)} + 3,$$

$$29\, z^{8(n+1)} + 60\, z^{6(n+1)} + 78\, z^{4(n+1)} + 60\, z^{2(n+1)} + 29,$$

$$33\, z^{8(n+1)} + 60\, z^{6(n+1)} + 70\, z^{4(n+1)} + 60\, z^{2(n+1)} + 33,$$

and

$$13\, z^{6(n+1)} + 2\, z^{5(n+1)} + 19\, z^{4(n+1)} - 4\, z^{3(n+1)} + 19\, z^{2(n+1)} + 2\, z^{(n+1)} + 13\,,$$

$$13\, z^{6(n+1)} - 2\, z^{5(n+1)} + 19\, z^{4(n+1)} + 4\, z^{3(n+1)} + 19\, z^{2(n+1)} - 2\, z^{(n+1)} + 13$$

(the factors of $169\, z^{12(n+1)} + 490\, z^{10(n+1)} + 871\, z^{8(n+1)} + 1036\, z^{6(n+1)} + 871\, z^{4(n+1)} + 490\, z^{2(n+1)} + 169$) are all irreducible of degree more than $2(n+1)$. To see this, observe that each of their roots lie on the unit circle having the same non-trivial height. So the lead coefficients of each factor would need to contain all the primes in the original lead coefficient. Since α has degree at most n, α cannot be a zero of any of these factors and thus these remaining factors cannot vanish.

Therefore by the product formula

$$1 = \prod_{\text{all } v} |g(\beta^2)|_v = \prod_{v\nmid\infty} |g(\beta^2)|_v \prod_{v\mid\infty} |g(\beta^2)|_v$$

$$\leq \prod_{v\nmid\infty} |2|_2^{2k+l+4t+8w+3c+8e+12s} \max\{1, |\beta|_v\}^{2\deg g} \prod_{v\mid\infty} \max\{1, |\beta|_v\}^{2\deg g} \left(\sqrt{M}\right)^{d_v/d}.$$

Now we recall that

$$h(\beta) = \log H(\beta) \text{ and } H(\beta) = \prod_{v\in V_k} \max\{1, |\beta|_v\},$$

which gives us

$$1 \le H(\beta)^{2\deg g}\, 2^{-(2k+l+4t+8w+3c+8e+12s)}\, \sqrt{M}\,.$$

Since $M = 2^{k+l+2t+4w+2c+4e+6s}\, L$, we get

$$1 \le H(\beta)^{2\deg g}\, 2^{-(3k+l+6t+12w+4c+12e+18s)/2}\, \sqrt{L},$$

and therefore

$$h(\beta) \ge \frac{\log(2^{3k+l+6t+12w+4c+12e+18s}/L)}{4(k+l+2t+4w+2c+4e+6s)}.$$

The choice $(k,l,t,w,c,e,s) = (3977{,}780{,}328, 96, 24, 16, 16)$ and numerical computation of L gives the lower bound

$$h(\beta) \ge 0.4278003111\ldots \text{ as desired.}$$

For $m = 4$ taking $g(\beta)$ in place of $g(\beta^2)$ immediately gives

$$h(\beta) \ge 2\,(0.4278003111\ldots) = 0.8556006223\ldots.$$

For general $m \ge 3$ we take

$$g(z) = \prod_{i=0}^{I} g_i(z)^{s_i} \quad \text{with } I = 2,$$

$$g_0(z) = (z-1),$$

$$g_1(z) = \frac{1}{2}(m-\delta)z + \frac{1}{2}(m+\delta), \qquad \delta = \begin{cases} 1 & \text{if } m \text{ odd}, \\ 0 & \text{if } m \text{ even}. \end{cases}$$

and

$$g_2(z) = \frac{1}{4}\big(m^2 + (4-\delta)\big)z^2 + \frac{1}{2}\big(m^2 - (4-\delta)\big)z + \frac{1}{4}\big(m^2 + (4-\delta)\big).$$

For all finite places $v \nmid \infty$ we have

$$|g_1(\beta)|_v = \left|\frac{1}{2}(m-\delta)(\beta-1)+m)\right|_v \leq |m|_v \max\{1,|\beta|_v\}$$

$$|g_2(\beta)|_v = \left|\frac{1}{4}\big(m^2+(4-\delta)\big)(\beta-1)^2+m^2\beta)\right|_v \leq |m|_v^2 \max\{1,|\beta|_v\}^2,$$

and

$$|g(\beta)|_v \leq \max\{1,|\beta|_v\}^{\deg g} |m|_v^{\deg g}.$$

For $v|\infty$ and $|\beta|_v > 1$ writing $|g(\beta)|_v = |\beta|_v^{\deg g} |g^*(\beta^{-1})|_v$, where $g^*(x)$ is the reciprocal of $g(x)$, we have

$$|g(\beta)|_v \leq \max\{1,|\beta|_v\}^{\deg g} \left(\sup_{|z|\leq 1} \max\{|g(z)|,|g^*(z)|\}\right)^{d_v/d}$$

$$= \max\{1,|\beta|_v\}^{\deg g} \sup_{|z|=1} |g(z)|^{d_v/d}.$$

Again to apply the product formula we assume that $g(\beta) \neq 0$ then we get

$$1 = \prod_{v\in V_k} |g(\beta)|_v = \prod_{v\nmid\infty} |g(\beta)|_v \prod_{v|\infty} |g(\beta)|_v \leq H(\beta)^{\deg g}\, m^{-\deg g} \sup_{|z|=1} |g(z)|,$$

and

$$h(\beta) \geq \log(m) - \frac{\log(\sqrt{M})}{\deg g}, \quad M \coloneqq \sup_{|z|=1} |g(z)|^2. \tag{4.1.5}$$

Now we must show that $g(\beta) \neq 0$. First we will show $g_1(\beta) \neq 0$. When m is even from our assumption $\beta \neq 1$ and

$$\prod_{\text{all } v} |1-\beta|_v = 1 \;\Rightarrow\; \prod_{v|\infty} |1-\beta|_v = \prod_{v\nmid\infty} |1-\beta|_v^{-1},$$

from (4.1.3) we know that

$$\prod_{v|\infty}|1-\beta|_v \geq m \prod_{v\nmid\infty}\max\{1,|\beta|_v\}^{-1}. \tag{4.1.6}$$

Hence for $m > 2$ we must have $\beta \neq -1$, otherwise from (4.1.6) we get $2 \geq m$. Thus $g_1(\beta) \neq 0$, for m even. For m odd $g_1(x^{n+1})$ is irreducible by Lemma 4.1, so cannot vanish at α (which has degree at most n). Therefore in both cases we have $g_1(\beta) \neq 0$. Since we have $g_1(\beta) \neq 0$, we recall Lemma 3.7.4 with

$$t = \frac{m+\delta}{m-\delta} > 1 \text{ when } m \text{ is odd and equal 1 when } m \text{ is even.}$$

Therefore when m is odd and

$$s_0 \leq \frac{4(m+\delta)/(m-\delta)}{((m+\delta)/(m-\delta)-1)^2} = m^2 - 1,$$

then

$$\sup_{|z|=1}\left|(z-1)^{s_0}\left(z+\frac{m+\delta}{m-\delta}\right)\right| = \frac{\left(\frac{m+\delta}{m-\delta}+1\right)^{s_0+1}}{(s_0+1)^{\frac{1}{2}(s_0+1)}}\left(\frac{s_0}{\frac{m+\delta}{m-\delta}}\right)^{\frac{1}{2}s_0},$$

achieved at

$$z = \frac{\left(\left(\left(\frac{m+\delta}{m-\delta}\right)^2+1\right)s_0 - 2\left(\frac{m+\delta}{m-\delta}\right)\right)}{2\left(\frac{m+\delta}{m-\delta}\right)(s_0+1)}$$
$$\pm \frac{\left(\left(\frac{m+\delta}{m-\delta}\right)+1\right)\sqrt{s_0\left(4\left(\frac{m+\delta}{m-\delta}\right)-\left(\frac{m+\delta}{m-\delta}-1\right)^2 s_0\right)}}{2\left(\frac{m+\delta}{m-\delta}\right)(s_0+1)}\, i.$$

Thus when $s_2 = 0, s_1 = 1$ (and $s_0 \leq m^2 - 1$ when m is odd) we get

$$\sqrt{M} = \sup_{|z|=1} \left|(m-\delta)(z-1)^{s_0}\left(z+\frac{m+\delta}{m-\delta}\right)\right| = \frac{m^{s_0+1}}{(s_0+1)^{\frac{1}{2}(s_0+1)}}\left(\frac{4s_0}{m^2-\delta}\right)^{\frac{1}{2}s_0},$$

and

$$H(\beta)^{s_0+1} \geq (s_0+1)^{\frac{1}{2}(s_0+1)}\left(\frac{m^2-\delta}{4s_0}\right)^{\frac{1}{2}s_0}.$$

Now optimally taking $s_0 = (m^2-\delta)/4$ it follows that,

$$c_m = \begin{cases} \frac{1}{2}\log\left(\frac{m^2+3}{4}\right) & \text{if } m \geq 3 \text{ odd,} \\ \frac{1}{2}\log\left(\frac{m^2+4}{4}\right) & \text{if } m \geq 4 \text{ even.} \end{cases}$$

Now we will show $g_2(\beta) \neq 0$. First if $3|m$ or $2 \parallel m$ then $g_2(\beta) \neq 0$, otherwise $g_2(\beta) = 0$ will imply that

$$h(\beta) \leq \begin{cases} \frac{1}{2}\log\left(\frac{m^2+3}{12}\right) & \text{when } 3|m, \\ \frac{1}{2}\log\left(\frac{m^2+4}{8}\right) & \text{when } 2 \parallel m. \end{cases}$$

which will contradict the above bound. Thus we have $g_2(\beta) \neq 0$ for $3|m$ or $2 \parallel m$. We need to show that $g_2(\beta) \neq 0$ when $3 \nmid m$ for m odd or $4|m$ for m even. Now we also have from Lemma 4.1 that $F_2(z)$ is irreducible, which leads to $g_2(\beta) \neq 0$.

By converting to cosines we have

$$M := \sup_{|z|=1} |g(z)|^2 = \sup_{u\in[-1,1]} \prod_{i=0}^{I} f_i(u)^{s_i}$$

with

$$f_0 = 2(1-u),$$

$$f_1(u) = \frac{1}{2}(m^2 - \delta)u + \frac{1}{2}(m^2 + \delta),$$

and

$$f_2(z) = \left(\frac{1}{2}\big(m^2 + (4-\delta)\big)u + \frac{1}{2}\big(m^2 - (4-\delta)\big)\right)^2,$$

where plainly M will be achieved at $u = -1$ or at zero of

$$\sum_{i=0}^{I} s_i \frac{f_i'(u)}{f_i(u)} = 0.$$

For example, after numerical computation and experimentation, the choices

$$(m; s_0, s_1, s_2) = (3; 107, 48, 17), (5; 198, 26, 13), (6; 246, 21, 11), (7; 225, 14, 8),$$

$$(8; 151, 7, 4), (9; 326, 12, 7), (10; 106,3,2), (11; 206, 5, 3)$$

give us

$$c_3 = 0.599206,\ c_5 = 1.001086,\ c_6 = 1.172140,\ c_7 = 1.298988, c_8 = 1.429512,$$

$$c_9 = 1.532875,\ c_{10} = 1.637694,\ c_{11} = 1.724309.$$

For the asymptotic bound we take a sequence of s_0, s_1, s_2 with

$$s_0/s_1 \to Am^2\ , \qquad s_1/s_2 \to 2C\ ,$$

for constants A, C which will be chosen optimally below. Hence M must be achieved at

$$u = \frac{-Am^6 + m^2\big((4-\delta)(2C - A\delta) - 2\delta\big) - 2\delta(4-\delta)(C+1) \pm 2m^2\sqrt{D_1}}{(m^2-\delta)(m^2+4-\delta)(Am^2+2C+2)}$$

where

$$D_1 = m^4((2A+1+C)^2 - 8AC) + m^2\left((2A+1+C)\big(8-2\delta(C+1)\big) + 8AC\delta\right) + \big(4-\delta(1+C)\big)^2,$$

or at $u = -1$ when m is odd. Writing

$$u = -1 + \frac{2}{Am^2}\big(2A+1+C-A\delta \pm \sqrt{D}\big) + O\left(\frac{1}{m^4}\right),$$

where $D = (2A+1+C)^2 - 8AC$, leads to

$$c_m \geq \log\left(\frac{m}{2}\right) + \frac{1}{2Am^2} \min_{\pm} \log\left(\frac{\exp\big(2A+1+C-A\delta \pm \sqrt{D}\big)}{\left(\frac{2A+1+C\pm\sqrt{D}}{4A}\right)^{2C}\left(\frac{-2A+1+C\pm D}{4A}\right)^2}\right) + O\left(\frac{1}{m^4}\right),$$

or

$$\log(m/2) + \frac{1}{Am^2}\log\big(2^{2(1+C)}/3\big) + O(m^{-4})$$

if this is smaller when m is odd. For a given choice of C we can choose A to make these $\pm$ quantities equal. Choosing (after numerical experimentation) $2C = 1.5799148239$ and calculating $A = 0.5569260220\ldots$ gives the desired asymptotic bound.

To obtain the improved values for $m = 3$ to 11 stated in the theorem we take

$$g(z) = \prod_{i=0}^{I} g_i(z)^{s_i}$$

with $I = 4$ or 5 and the auxiliary factors $g_i(z)$, and choice of exponents s_i given in Table 1. For these $g_j(x)$ we have

$$\big|g_j(\beta)\big|_v \leq |m|_v^{\deg g_j} \max\{1, |\beta|_v\}^{\deg g_j}$$

for $v \nmid \infty$ and (4.1.5) holds as before (as long as $g(\beta) \neq 0$).

We can argue as above that $g(\beta) \neq 0$ by irreducibility (and for $m = 8$ that $\frac{1}{2}\log 9 = 1.0986\ldots < 1.4295\ldots$ the previous lower bound and $m = 5$ and $m = 11$ that $\frac{1}{2}\log 8 > 1.016628$ and $\frac{1}{2}\log 32 > 1.728890$).

Additional factors could probably be added to the auxiliary polynomial $g(x)$ in the style of [dub2] for further improvements. The choices

$$g(x) = (x^2 - 1)^4(x^2 + 1) \quad \text{and} \quad g(x) = (x - 1)^{m^2}(x + 1)$$

similarly recover the values

$$c_2 = \frac{1}{4}\log 5 \quad \text{and} \quad c_m = \log\left(\sqrt{m^2 + 1}/2\right)$$

for $m > 2$ respectively (and using the auxiliary polynomials of [9] for $g(x)$ gives the improved values stated there).

■

4.2 Finding upper bounds on the constant c_m

Definition 4.2 (Salem Numbers & PV Numbers)

A real algebraic number $\alpha > 1$ is said to be a Salem number if all the conjugates of α lie in the unit disk with at least one on the unit circle. Suppose $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ are the conjugates, so that $|\alpha_i| \leq 1$ for all $i = 2, \ldots, n$ and $|\alpha_i| = 1$ for some i. Then they take the form α, α^{-1} and all the other $|\alpha_i| = 1$ giving $M(\alpha) = \alpha$. If all the conjugates of α, lie inside the unit disk then α is called a PV-number (Pisot-Vijayaraghavan number). That is $|\alpha_i| < 1$ for all $i \neq 1$. The smallest known Salem number is given by the Mahler measure of the Lehmer polynomial $l(x)$ with $M(l) = 1.17628\ldots$. The smallest PV (Pisot-Vijayaraghavan number) number is given by $M(x^3 - x - 1) = 1.32471\ldots$ (see [26]). The smallest Littlewood PV-number is the golden ratio. It is well known that every PV-number is a two-side limit point of Salem numbers. Borwein et al. (Theorem 6.2 of [4]) showed, the smallest Littlewood PV-number is a limit point from both sides, of Littlewood Salem numbers.

Theorem 4.2.1

If (4.1.1) holds for any non root of unity α that is a zero of a polynomial $f(x)$ in D_m of degree n, then

$$c_2 \le \log\left(\frac{1+\sqrt{5}}{2}\right) = 0.481211\ldots, \tag{4.2.1}$$

(even if we further restrict to Littlewood Polynomials),

$$c_3 \le \log(2) = 0.693147\ldots,$$

$$c_4 \le \log\left(1+\sqrt{2}\right) = 0.881373\ldots, \tag{4.2.2}$$

$$c_6 \le \log\left(\frac{3+\sqrt{13}}{2}\right) = 1.194763\ldots. \tag{4.2.3}$$

For general $m \ge 3$

$$c_m \le \log(m-1). \tag{4.2.4}$$

Remark: It is not clear what should be the optimal constant C_1 in a bound of the form

$$c_m = \log m - C_1 + o(1).$$

Proof of Theorem 4.2.1

Since as shown in (Theorem 6.2 of [4]) the golden ratio is a limit point of Salem numbers with Littlewood minimal polynomials

$$f_n(x) = x^{6n} + (1 - x - x^2)\sum_{i=0}^{2n-1} x^{3i},$$

we note that the optimal c_2 certainly satisfies (4.2.1).

Suppose that $m \ge 3$. For (4.2.4) we take $n \ge 2$ and

$$f_n(x) = x^{2n} + \sum_{i=0}^{n-1} x^{2i} - (m-1)x^{2i+1} = \frac{x^{n+1}}{x^2-1}F_n(x),$$

with

$$F_n(x) = \left(x^{n+1} - x^{-(n+1)}\right) - (m-1)\,(x^n - x^{-n}).$$

Since

$$f_n\left(\frac{1}{m-1}\right) > 0, f_n\left(\frac{1}{m-1}\left(1 + \left(\frac{2}{m-1}\right)^n\right)\right) < 0$$

it is clear that the $f_n(x)$ have real roots $\alpha_n,\ \alpha_n^{-1}$ with $\alpha_n \to (m-1)$ as $n \to \infty$. Notice that $f_n(x)$ does not vanish at ± 1 or any $(2n+1)$st root of unity (so by the theorem can have no cyclotomic factors). Since

$$\frac{1}{2i}F_n\left(e^{2\pi it}\right) = \sin(2\pi(n+1)t) - (m-1)\sin(2\pi nt)$$

changes sign it must have a zero t_j in each interval

$$\left[\frac{2j-1}{4n}, \frac{2j+1}{4n}\right], j = 1, 2, 3, \ldots, 2n-1$$

and the remaining $(2n-2)$ zeros $e^{2\pi i t_j}, t_j \neq 1/2$ of $f_n(x)$ all lie on the unit circle. Since $f_n(x)$ has no monic factors with all roots on the unit circle these $f_n(x)$ are irreducible with

$$(\deg f_n + 1)h(\alpha_n) = \left(\frac{2n+1}{2n}\right)\log\alpha_n \to \log(m-1) \ \text{ as } n \to \infty.$$

For (4.2.2) we similarly consider

$$f_{n,4}(x) = \sum_{i=0}^{4n+2} x^i - 4x \sum_{i=0}^{n} x^{4i} = (1-x)(1-2x-x^2)\sum_{i=0}^{n} x^{4i} - x^{4n+3}$$

with real roots $\alpha_n, \alpha_n^{-1} \to \sqrt{2}-1, \sqrt{2}+1$ and no roots at the $(4n+3)$st roots of unity. Writing $F_{n,4}(x) = (x^4-1)\,f_{n,4}(x)\,x^{-(2n+3)}$ and observing that

$$\frac{1}{4i}F_{n,4}\left(e^{2\pi it}\right) = (\cos(3\pi t) + \cos(\pi t))\sin\left((4n+3)\,\pi t\right) - 2\sin(4(n+1)\,\pi t)$$

has sign changes in each of the intervals

$$[(2j+1)/8(n+1), (2j+3)/8(n+1)]\,, \quad j = 0,1,\dots,4n+2,$$

(and removing the introduced 4th roots of unity) the remaining $4n$ zeros of $f_{n,4}(x)$ all lie on the unit circle.

For (4.2.3) we take

$$f_{n,6}(x) = \sum_{i=0}^{6n+4} x^i - 6x\,(1-x+x^2) \sum_{i=0}^{n} x^{6i}$$

$$= (1-x)(1-x+x^2)(1-3x-x^2) \sum_{i=0}^{n} x^{6i} - x^{6n+5}$$

with real roots $\alpha_n,\ \alpha_n^{-1} \to \frac{1}{2}\left(\sqrt{13}-3\right),\ \frac{1}{2}\left(\sqrt{13}+3\right)$ and no roots at the $(6n+5)$st roots of unity. Writing

$$F_{n,6}(x) = \frac{(x^6-1)}{x^2-x+1}\, f_{n,6}(x)\, x^{-(3n+4)}$$

and observing that

$$\frac{1}{4i} F_{n,6}\left(e^{2\pi i t}\right) = (\cos(3\pi t) + 2\cos(\pi t))\sin\left((6n+5)\,\pi t\right) - 3\sin(6(n+1)\,\pi t)$$

has sign changes in each of the intervals

$$[(2j+1)/12(n+1), (2j+3)/12(n+1)]\,, \quad j = 0,1,\dots,6n+4,$$

(and removing the introduced 6th roots of unity) the remaining $6n+2$ zeros of $f_{n,6}(x)$ all lie on the unit circle.

■

Table 4.1.1 Auxiliary factors and exponents

m	Auxiliary factors $g_3(z), g_4(z), \ldots$	$(s_0, s_1, s_2, s_3, \ldots)$
3	$g_3 = 11(z-1)^4 + 7.3^2\, z(z-1)^2 + 3^4 z^2$	(823,178,183,48,53,7)
	$g_4 = 13(z-1)^4 + 8.3^2\, z(z-1)^2 + 3^4 z^2$	
	$g_5 = 5(z-1)^2 + 2.3^2 z$	
5	$g_3 = 8(z-1)^2 + 5^2 z$	(340,10,29,1,8,10)
	$g_4 = 61(z-1)^4 + 16.5^2\, z(z-1)^2 + 5^4 z^2$	
	$g_5 = 5(11(z-1)^4 + 3.5^2\, z(z-1)^2 + 5^3 z^2)$	
6	$g_3 = 109(z-1)^4 + 21.6^2\, z(z-1)^2 + 6^4 z^2$	(222680,19000,8000,2793,2064,1000)
	$g_4 = 11(z-1)^2 + 6^2 z$	
	$g_5 = 2(59(z-1)^4 + 11.6^2\, z(z-1)^2 + 3.6^3 z^2)$	
7	$g_3 = 181(z-1)^4 + 27.7^2\, z(z-1)^2 + 7^4 z^2$	(309,16,9,4,1,2)
	$g_4 = 193(z-1)^4 + 28.7^2\, z(z-1)^2 + 7^4 z^2$	
	$g_5 = 7(2z^2 + 3z + 2)$	
8	$g_3 = 2(9(z-1)^2 + 2^5 z)$	(944,45,20,5,5,2)
	$g_4 = 305(z-1)^4 + 35.8^2\, z(z-1)^2 + 8^4 z^2$	
	$g_5 = 321(z-1)^4 + 36.8^2\, z(z-1)^2 + 8^4 z^2$	
9	$g_3 = 461(z-1)^4 + 43.9^2\, z(z-1)^2 + 9^4 z^2$	(44277,0,1256,538,273)
	$g_4 = 481(z-1)^4 + 44.9^2\, z(z-1)^2 + 9^4 z^2$	
10	$g_3 = 701(z-1)^4 + 53.10^2\, z(z-1)^2 + 10^4 z^2$	(1029,25,10,5,3)
	$g_4 = 1351(z-1)^4 + 104.10^2\, z(z-1)^2 + 2.10^4 z^2$	
11	$g_3 = 32(z-1)^2 + 11^2 z$	(827,6,12,2,6,3)
	$g_4 = 991(z-1)^4 + 63.11^2\, z(z-1)^2 + 11^4 z^2$	
	$g_{54} = 1021(z-1)^4 + 64.11^2\, z(z-1)^2 + 11^4 z^2$	

Bibliography

[1] F. Amoroso & R. Dvornicich, *A lower bound for the height in abelian extensions*, J. Number Theory 80 (2000), 260-262.

[2] F. Amoroso & U. Zannier, *A uniform relative Dobrowolski's lower bound over abelian extensions*, Preprint.

[3] P. Borwein and Kwok-Kwong Stephen Choi, *On cyclotomic polynomials with* ± 1 *coefficents*, Experiment. Math. Volume 8, Issue 4 (1999), 399-407.

[4] P. Borwein, E. Dobrowolski & M.J. Mossinghoff, *Lehmer's problem for polynomials with odd coefficients*, Ann. of Math. (2) 166 (2007), no. 2, 347-366.

[5] P. Borwein, K.G. Hare and M.J. Mossinghoff, *The Mahler measure of Littlewood polynomials*, Lond. Math Soc, DOI: 10.1112.

[6] J.W.S. Cassels, *Local fields*, Cambridge Univ. Press, 1986.

[7] T. Cochrane, *Topics in Number Theory*, Spring 2006, Kansas State University

[8] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. 34 (1979), 391-401.

[9] A. Dubickas & M.J. Mossinghoff, *Auxiliary polynomials for some problems regarding Mahler's measure*, Acta Arith. 119 (2005), no. 1, 65-79.

[10] D.S. Dummit and R.M. Foote, *Abstract Algebra*, Second edition, John Wiley and Sons Inc., 1999.

[11] J. Garza, *On the height of algebraic numbers with real conjugates*, Acta Arith. 128 (2007), 385-389.

[12] J. Garza, *The Lehmer strength bounds for total ramification*, Acta Arith. 137 (2009), 171-176.

[13] J. Garza, *The Mahler measure of dihedral extensions*, Acta Arith. 131 (2008), no. 3, 201-215.

[14] G. Höhn & N.P. Skoruppa, *Un résultat de Schinzel*, J. Théor. Nombres Bordeaux 5 (1993), 185.

[15] G. Höhn, *On a theorem of Garza regarding algebraic integers with real conjugates*, Preprint 2008.

[16] H. Iwaniec & E. Kowalski, *Analytic Number Theory*, Colloquium Publications, Vol. 53, AMS (2004).

[17] V. A. Lebesgue, *Sur l'impossibilité en nombres entiers de l'équation* $x^m = y^2 + 1$, Nouv. Ann. Math., 9, (1850) 178-181.

[18] D.H. Lehmer, *Factorization of certain cyclotomic functions*, Annals of Math. 34 (1933), 461-479

[19] W. Ljunggren, *Einige Bemerrkungen über die Darstellung ganzer Zahlen durch binäre kubische Formen mit positiver Diskriminante*, Acta. Math 75 (1942), pp. 1-21.

[20] K. Mahler, *An application of Jensen's formula to polynomials*, Mathematika 7 (1960), 98-100.

[21] J. McKee and C. Smyth, *Number Theory and Polynomials*, Lond. Math Soc.352, Cambridge Press 2008, 322-349.

[22] T. Nagell, *Des équations indéterminées* $x^2 + x + 1 = y^n$ *et* $x^2 + x + 1 = 3y^2$, Nordsk. Mat. Forenings Skr. Ser. 1, No. 2 (1921), 14 pages.

[23] C. Pinner, *Topics in Number Theory*, Spring 2007, Kansas State University.

[24] A. Schinzel, *On the product of the conjugates outside the unit circle of an algebraic number*, Acta Arith. 24 (1973), 385-399; Addendum ibid. 26 (1973), 329-361.

[25] A. Schinzel, *Polynomials with Special Regard to Reducibility*, Cambridge Press, 2000.

[26] C.L. Siegel, *Algebraic integers whose conjugates lie on the unit circle*, Duke Math. J**.** 11 (1944), 597-602.

[27] C.J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. Lond. Math Soc. 3 (1971), 169-175.

[28] P. Voutier, *An effective lower bound for the height of algebraic numbers*, Acta Arith. 74 (1996), 81-95.

[29] L.C. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, 1982.

[30] E. Weiss, *Algebraic Number Theory*, Dover Publications, Inc. Mineola, New York, 1998.