AN ABSTRACT OF THE THESIS OF

Brian Christopher Dietel for the degree of Doctor of Philosophy in Mathematics
presented on April 28, 2009.
Title: Mahler's Order Functions and Algebraic Approximation of p-adic Numbers

Abstract approved: _____

Mary E. Flahive

If P is an integer polynomial denote the degree of P by $\partial(P)$ and let $H(P)$ be the maximum of the absolute value of the coefficients of P. Define $\Lambda(P) = 2^{\partial(P)}H(P)$ and for a fixed prime p let $\mathbb{C}_p$ denote the completion of the algebraic closure of the p-adic numbers. We generalize the order function of Mahler to the p-adic numbers by associating each $\theta \in \mathbb{C}_p$ to the function $O(u|\theta) = \max \log \frac{1}{|P(\theta)|}$, where $|*|$ denotes the p-adic absolute value and the maximum is taken over all $P(x) \in \mathbb{Z}[x]$ satisfying $\Lambda(P) \leq u$ and $P(\theta) \neq 0$. Similarly, define $O^*(u|\theta) = \max \log \frac{1}{|\theta-\alpha|}$ where the maximum is now taken over the set of all algebraic numbers $\alpha \neq \theta$ with minimal polynomial m satisfying $\Lambda(m) \leq u$. Placing a partial order $\gg$ and equivalence relation $\asymp$ on both O and O^* induces two corresponding partial orders and equivalence relations on $\mathbb{C}_p$.

In this thesis we demonstrate several results concerning O and O^*. In particular, it is proved that if θ is algebraic over $\mathbb{Q}_p$ then θ must satisfy $O^*(u|\theta) \gg \log u$ and if $\theta, \eta \in \mathbb{C}_p$ are algebraically dependent over $\mathbb{Q}$ then $O(u|\theta) \asymp O(u|\eta)$. Also, under certain conditions, given a function g we construct $\theta \in \mathbb{C}_p$ such that $g(c'(\log\log u)^{1/2}) \ll O^*(u|\theta)$ and $O^*(u|\theta) \ll g(c \log\log u)$, where c and c' are positive constants. The transcendence type considers the limiting behavior of O and O^* and will be used to prove that under certain conditions O and O^* behave similarly. Finally, given $\tau \geq (3+\sqrt{5})/2$ we demonstrate that it is possible to construct elements of $\mathbb{C}_p$ with transcendence type equal to τ.

Mahler's Order Functions and Algebraic Approximation of p-adic Numbers

by

Brian Christopher Dietel

A THESIS

submitted to

Oregon State University

in partial fulfillment of
the requirements for the
degree of

Doctor of Philosophy

Presented April 28, 2009
Commencement June 2009

Doctor of Philosophy thesis of Brian Christopher Dietel presented on April 28, 2009

APPROVED:

Major Professor, representing Mathematics

Chair of the Department of Mathematics

Dean of the Graduate School

I understand that my thesis will become part of the permanent collection of Oregon State University libraries. My signature below authorizes release of my thesis to any reader upon request.

Brian Christopher Dietel, Author

ACKNOWLEDGEMENTS

Academic

I am indebted to my advisor Mary Flahive for her commitment and dedication. I also thank my teachers and committee members, David Finch, Dennis Garity, Thomas Schmidt, Holly Swisher, and Todd Palmer.

Personal

I wish to thank my parents Sharon and Wallace Dietel, and my brother Kevin Dietel. I cannot express my gratitude for the love and support they have given me throughout my life. I also thank my grandparents, Ruby Bull, Richard Dietel, and Warna Dietel for their love and strength.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

Dedicated to the memory of Harlan Bull

MAHLER'S ORDER FUNCTIONS AND ALGEBRAIC APPROXIMATION OF P-ADIC NUMBERS

1 INTRODUCTION

When studying transcendental numbers a natural question is to consider how well a given transcendental number can be approximated by algebraic numbers, or if there exist integer polynomials which are close to zero when evaluated at a given transcendental number. The algebraic numbers are dense in $\mathbb{C}$ and therefore any element of $\mathbb{C}$ can be approximated with arbitrary precision by an element in the algebraic closure of $\mathbb{Q}$. Thus it is necessary to place a restriction on the set of polynomials or algebraic numbers which are being used to approximate. One method to measure a polynomial is to consider a function depending on the degree of the polynomial and the absolute value of the polynomial's coefficients. First let $|*|_\infty$ denote the standard absolute value on the complex numbers and suppose $Q(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$. Denote the degree of Q by $\partial(Q)$ and the length of Q by $L(Q) = |a_n|_\infty + \cdots + |a_0|_\infty$. Define $\Lambda'(Q) = 2^{\partial(Q)} L(Q)$. Moreover, if $\alpha \in \overline{\mathbb{Q}}$ let $M_\alpha(x) \in \mathbb{Q}[x]$ denote the minimal polynomial of α over $\mathbb{Q}$ and define $m_\alpha(x) \in \mathbb{Z}[x]$ to be $aM_\alpha(x)$, where a is the least common multiple of the denominators of the coefficients of M_α. Define $\partial(\alpha) = \partial(m_\alpha)$, $H(\alpha) = H(m_\alpha)$, and $\Lambda'(\alpha) = \Lambda'(m_\alpha)$. Note that given $u \in \mathbb{N}$ there exist only finitely many integer polynomials Q and algebraic numbers α which satisfy $\Lambda'(Q) \leq u$ and $\Lambda'(\alpha) \leq u$. In a 1971 paper Mahler [22] associated to each $\theta \in \mathbb{C}$ two "order functions" O_M and O_M^*, and then used the order functions to construct a classification of $\mathbb{C}$ based on algebraic approximation. Note that this classification is different from Mahler's [20] 1932 classification of $\mathbb{R}$ based on algebraic approximation in which he divided $\mathbb{R}$ into the A, S, T, and U numbers. An overview of the results on this

earlier classification can be found in Bugeaud [6].

Definition 1.1. *Let $\theta \in \mathbb{C}$. Define $O_M(*|\theta) : \mathbb{N} \to \mathbb{R}$ and $O_M^*(*|\theta) : \mathbb{N} \setminus \{1\} \to \mathbb{R}$ by*

$$O_M(u|\theta) = \max_{\substack{\Lambda'(P) \leq u \\ P(\theta) \neq 0}} \log \frac{1}{|P(\theta)|_\infty}$$

$$O_M^*(u|\theta) = \max_{\substack{\Lambda'(\alpha) \leq u \\ \alpha \neq \theta}} \log \frac{1}{|\alpha - \theta|_\infty}.$$

The function O_M measures polynomial approximations and O_M^* measures approximations by algebraic numbers. Thus elements of $\mathbb{C}$ for which O_M grows quickly have "good" polynomial approximations relative to Λ' and if O_M^* grows quickly for some $\theta \in \mathbb{C}$ then there are algebraic numbers that are "good" approximations of θ relative to Λ'. By placing a partial order on the set of order functions Mahler [22] constructed two classifications of the elements of $\mathbb{C}$.

Definition 1.2. *Let $a(u)$ and $b(u)$ be non-decreasing functions from $\mathbb{N}$ to $\mathbb{R}$ which are positive for sufficiently large u. Define the partial order $\gg$ by $a(u) \gg b(u)$ (or equivalently $b(u) \ll a(u)$) if there exist $c, u_0 \in \mathbb{N}$ and $\gamma \in \mathbb{R}^+$ such that $a(u^c) \geq \gamma b(u)$ for all $u \geq u_0$. Define the equivalence relation $\asymp$ by $a(u) \asymp b(u)$ if $a(u) \gg b(u)$ and $b(u) \gg a(u)$.*

Since $\Lambda'(1) = 1$ it follows that $O_M(u|\theta) \geq 0$ for all θ. It is possible for O_M^* to be negative, but it must be positive for all sufficiently large u because the algebraic numbers are dense in $\mathbb{C}$. Applying the partial order $\gg$ to O_M and O_M^* induces partial orders on $\theta, \eta \in \mathbb{C}$ given by $\theta \gg \eta$ if $O_M(u|\theta) \gg O_M(u|\eta)$ and $\theta \gg^* \eta$ if $O_M^*(u|\theta) \gg O_M^*(u|\eta)$. Likewise the equivalence relation $\asymp$ on $\mathbb{C}$ is defined by $\theta \asymp \eta$ if $O_M(u|\theta) \asymp O_M(u|\eta)$ and the equivalence relation $\asymp^*$ on $\mathbb{C}$ is defined by $\theta \asymp^* \eta$ if $O_M^*(u|\theta) \asymp O_M^*(u|\eta)$. Mahler [22] proved the following results on O_M.

Theorem 1.3.

(i) If $\theta \in \mathbb{C}$ is algebraic and θ is not an algebraic integer in an imaginary quadratic field then $O_M(u|\theta) \asymp \log u$.

(ii) If θ is transcendental then $O_M(u|\theta) \gg (\log u)^2$.

(iii) If θ and η are algebraically dependent and transcendental then $\theta \asymp \eta$.

Durand [10] gave different proofs of these results. In addition, Mahler [22] posed several questions concerning O_M. Durand [11] provided solutions to most of these questions and in doing so proved the following results on O_M and O_M^*.

Theorem 1.4.

(i) If θ is algebraic then $O_M^*(u|\theta) \asymp \log u$.

(ii) If $\asymp$ or $\asymp^*$ is used as an equivalence relation on $\mathbb{C}$ then there are uncountably many equivalence classes.

(iii) The partial orders $\gg$ and $\gg^*$ on $\mathbb{C}$ are not total orders.

(iv) With respect to Lebesgue measure $O_M(u|\theta) \asymp (\log u)^2$ for almost all $\theta \in \mathbb{C}$.

In proving these results Durand [11] also used results due to Fel'dman [13] to prove the following proposition.

Proposition 1.5. *If $\tau \geq 2$ and $\theta \in \mathbb{C}$ then*

$$\limsup_{u\to\infty} \frac{O_M^*(u|\theta)}{(\log u)^\tau} = \infty$$

if and only if

$$\limsup_{u\to\infty} \frac{O_M(u|\theta)}{(\log u)^\tau} = \infty.$$

For $\theta \in \mathbb{C}$ define

$$T(\theta) = \left\{\tau \geq 0 : \limsup_{u\to\infty} \frac{O_M(u|\theta)}{(\log u)^\tau} = \infty\right\}.$$

Define the transcendence type of θ by $\tau(\theta) = \sup\{\tau : \tau \in T(\theta)\}$. Given any $\tau \geq 3$, Durand [11] constructed $\theta \in \mathbb{C}$ such that $\tau(\theta) = \tau$. Amoroso [2] improved this result by

constructing $\theta \in \mathbb{C}$ for which $\tau(\theta) = \tau$ given any $\tau \geq 2$. Philippon [28] also studied the equivalence relation $\asymp$ on $\mathbb{C}$ by using nonstandard analysis.

Our goal is to investigate the p-adic analogues to O_M and O_M^*, which we denote by O and O^*. Although no previous work has been done on this specific problem there are numerous results concerning related problems in p-adic algebraic approximation. Mahler [21] constructed a p-adic version of his first classification. Escassut [12] studied an analogue to transcendence type when considering approximation by numbers algebraic over the p-adics. In the p-adics Adams [1] used algebraic approximation to study the transcendence of numbers of the form α^β where $\alpha, \beta \in \overline{\mathbb{Q}}$. Nesterenko [25, 26] also proved several results on p-adic algebraic approximation in polynomials with more than one variable. Beresnevich, Bernik, and Kovalevskaya [3] extended some metric results to the p-adics. Teulié [32] and Morrison [24] considered approximation of p-adic numbers by algebraic numbers of bounded degree. The results of Teulié were then extended by Zelo [35] who considered simultaneous algebraic approximation to sets containing real and p-adic numbers. Wang [34] studied algebraic approximations to values of p-adic functions satisfying a certain functional equation.

Denote the completion of the algebraic closure of the p-adic numbers by $\mathbb{C}_p$. In this thesis we first set up the necessary background on polynomials and p-adic numbers in Chapter 2. Chapter 3 then focuses on the basic properties of the p-adic order function O. In particular, the first main result is Corollary 3.9 which states that if $\theta, \eta \in \mathbb{C}_p$ are algebraically dependent over $\mathbb{Q}$ then $O(u|\theta) \asymp O(u|\eta)$. In Chapter 4, Theorem 4.2 demonstrates that if α is algebraic over the p-adic numbers then $O^*(u|\alpha) \gg \log u$, and Theorem 4.5 constructs $\theta \in \mathbb{C}_p$ for which $O^*(u|\theta)$ grows slowly. Using the same θ from Theorem 4.5 in Theorem 4.6 we construct a lower bound for $O^*(u|\theta)$. Chapter 5 studies transcendence type in the p-adic numbers and Theorem 5.9 is the p-adic analogue of Proposition 1.5. Our final main result is Theorem 5.11 which states that given any real number $\tau \geq (3+\sqrt{5})/2$ it is possible to construct elements of $\mathbb{Q}_p$ with transcendence type τ.

2 BACKGROUND

Before beginning our study of p-adic order functions it is first necessary to go over some background results. The primary goal of Section 2.1 is to state several definitions and lemmas concerning polynomials. Section 2.2 provides a brief introduction to the p-adic numbers and gives some results concerning algebraic numbers over the p-adics.

2.1 Polynomials

We first state several definitions and results from basic field theory. Then we consider results on polynomials in $\mathbb{Z}[x]$. For additional background and results see Bourbaki [5], Dummit and Foote [9], and Mignotte and Ştefănescu [23]

For proofs and further discussion on the following results concerning fields see Chapters 13 and 14 in Dummit and Foote [9]. Let F be a field and let K be an extension field of F. If $\alpha \in K$ is a root of a polynomial in $F[x]$ then α is *algebraic* over F. If α is not a root of any polynomial in $F[x]$ then α is *transcendental*. Every element of a finite extension field of F is algebraic over F. If α is algebraic over F then there exists a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ for which $m_{\alpha,F}(\alpha) = 0$. This will be referred to as the *minimal polynomial* of α over F. The *degree* of α over F is the degree of the minimal polynomial of α over F. In the particular case when $F = \mathbb{Q}$ the *minimal polynomial* of α over $\mathbb{Z}$ will be defined to be $am_{\alpha,\mathbb{Q}}(x) \in \mathbb{Z}[x]$ where $a \in \mathbb{N}$ is the least common multiple of the denominators of the coefficients of $m_{\alpha,\mathbb{Q}}$. The *degree* of a finite extension field K over F will be denoted by $[K : F]$. If $\alpha \in K$ it can be proved that the degree of α over F must divide $[K : F]$. If K is an extension of F and $\alpha, \beta \in K$ then β is *algebraic* over α if there exists a polynomial $P(x) \in F(\alpha)[x]$ such that $P(\beta) = 0$, where $F(\alpha)$ denotes the smallest field constaining both F and α. If β is algebraic over α and α is algebraic over β

then α and β are said to be *algebraically dependent* over F.

A field K is *algebraically closed* if for every $Q(x) \in K[x]$ there is $\alpha \in K$ for which $Q(\alpha) = 0$. In particular this implies that all polynomials factor completely in an algebraically closed field. It can be proved by Zorn's Lemma that for every field F there exists a field $\overline{F}$, unique up to isomorphism fixing F, consisting of elements algebraic over F such that for every $Q(x) \in F[x]$ there is $\alpha \in \overline{F}$ for which $Q(\alpha) = 0$. The field $\overline{F}$ is algebraically closed and is called the *algebraic closure* of F.

Given a field F and a finite extension field K let $\mathrm{Aut}(K/F)$ denote the group of field automorphisms on K which fix F. The field K is said to be a *Galois extension* field of F if the number of elements in $\mathrm{Aut}(K/F)$ is equal to $[K : F]$. Now suppose $\alpha \in K$ and K is a Galois extension field of F. The *conjugates* of α over F are defined to be $\{\sigma(\alpha) : \sigma \in \mathrm{Aut}(K/F)\}$. Provided K is Galois the set of conjugates is independent of the field K. If α is algebraic over a field F let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be the conjugates of α and define the *norm* of α over F by

$$\mathrm{Nm}(\alpha) = \prod_{1 \le i \le n} \alpha_i.$$

For all $\alpha, \beta \in \overline{F}$ it can be demonstrated that $\mathrm{Nm}(\alpha\beta) = \mathrm{Nm}(\alpha)\mathrm{Nm}(\beta)$ and $\mathrm{Nm}(\alpha) \in F$. Using these definitions and results we now turn our attention to polynomials.

Definition 2.1. *Let B be a ring. Let $P(x) = a_n x^n + \cdots + a_0$ and $Q(x) = b_q x^q + \cdots + b_0$ be polynomials with coefficients in B with a_n and b_q both nonzero. Define the Sylvester matrix $M_s(P, Q)$ to be the $n + q$ by $n + q$ matrix given by*

$$M_s(P(x), Q(x)) = \begin{pmatrix} a_n & & & & b_q & & & \\ a_{n-1} & a_n & & & b_{q-1} & b_q & & \\ \vdots & \vdots & \ddots & a_n & \vdots & \vdots & \ddots & b_q \\ a_0 & a_1 & & \vdots & b_0 & b_1 & & \vdots \\ & a_0 & & \vdots & & b_0 & & \vdots \\ & & \ddots & \vdots & & & \ddots & \vdots \\ & & & a_0 & & & & b_0 \end{pmatrix}$$

where the first q columns contain the coefficients of P and the final n columns contain the coefficients of Q with 0 in the remaining entries. The resultant *R is defined to be $R(P,Q) = \det(M_s(P,Q))$.*

When B is an algebraically closed field let $P(x) = a_n(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$ and $Q(x) = b_q(x-\beta_1)(x-\beta_2)\dots(x-\beta_q)$ be the unique factorizations of P and Q. It can be proved that (see Chapter 4 of Bourbaki [5])

$$R(P(x),Q(x)) = a_n^q \prod_{\substack{1\le j\le n\\ 1\le k\le q}} (\alpha_k - \beta_j).$$

From this equation it is clear that in an algebraically closed field $R(P(x),Q(x)) = 0$ if and only if P and Q share a root. Related to the resultant is the discriminant.

Definition 2.2. *Let B be a ring and let $P(x) = a_nx^n + \cdots + a_0 \in B[x]$. Define the* discriminant *of P by*

$$\operatorname{disc}(P) = (-1)^{n(n-1)/2} a_n^{-1} R(P,P')$$

where $P'(x) = na_nx^{n-1} + (n-1)x^{n-2} + \cdots + a_1 \in B[x]$ is the formal derivative of P.

If B is an algebraically closed field and $P(x) = a_n(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$ then it can be proved (again see see Chapter 4 of Bourbaki [5])

$$\operatorname{disc}(P) = a_n^{2n-2} \prod_{j=2}^{n} \prod_{k=1}^{j-1} (\alpha_k - \alpha_j)^2. \tag{2.1}$$

Let $P(x) = a_nx^n + \cdots + a_0 \in \mathbb{Z}[x]$. The following notation will be used throughout. Let $|*|_\infty$ denote the standard absolute value. Define $H(P) = \max\{|a_n|_\infty, \dots, |a_0|_\infty\}$ to be the *height* of P and $L(P) = |a_n|_\infty + \cdots + |a_0|_\infty$ to be the *length* of P. Let $\partial(P)$ denote the *degree* of P and define the *size* of P by $\Lambda(P) = 2^{\partial(P)}H(P)$. Likewise, if $\alpha \in \overline{\mathbb{Q}}$ let m_α to be the minimal polynomial of α over $\mathbb{Z}$ and define $H(\alpha) = H(m_\alpha)$, $L(\alpha) = L(m_\alpha)$, $\partial(\alpha) = \partial(m_\alpha)$, and $\Lambda(\alpha) = \Lambda(m_\alpha)$. Note that given $u \in \mathbb{N}$ there exist only finitely many polynomials $P(x) \in \mathbb{Z}[x]$ and $\alpha \in \overline{\mathbb{Q}}$ such that $\Lambda(P) \le u$ and $\Lambda(\alpha) \le u$.

The following proposition allows us to bound the resultant $R(P,Q)$ and discriminant $\operatorname{disc}(P)$ in terms of the height and degree.

Proposition 2.3. *Let $P, Q \in \mathbb{Z}[x]$. Then*

$$|R(P,Q)|_\infty \leq (\partial(P)+\partial(Q))!\, H(P)^{\partial(Q)} H(Q)^{\partial(P)}.$$

and

$$|\operatorname{disc}(P)|_\infty \leq (2\partial(P)-1)!\, H(P)^{2\partial(P)-1} \partial(P)^{\partial(P)}.$$

Proof. If M is an n by n matrix with entries $a_{i,j}$ recall the Leibniz formula for the determinant gives

$$\det(M) = \sum_{\sigma \in S_n} \left(\operatorname{sgn}(\sigma) \prod_{j=1}^{n} a_{\sigma(j),j} \right) \tag{2.2}$$

where S_n is the symmetric group on n elements. Let $P, Q \in \mathbb{Z}[x]$. The largest entry in each of the first $\partial(Q)$ columns of the Sylvester matrix $M_s(P,Q)$ is $H(P)$ and the largest entry in each of the last $\partial(P)$ columns of $M_s(P,Q)$ is $H(Q)$. Moreover, there are $(\partial(P)+\partial(Q))!$ elements of $S_{\partial(P)+\partial(Q)}$ and (2.2) implies

$$|R(P,Q)| = |\det(M_s(P,Q))| \leq (\partial(P)+\partial(Q))!\, H(P)^{\partial(Q)} H(Q)^{\partial(P)}.$$

Since $H(P') \leq \partial(P) H(P)$ and $\partial(P') = \partial(P) - 1$ it thus follows that

$$|\operatorname{disc}(P)|_\infty \leq (2\partial(P)-1)!\, H(P)^{2\partial(P)-1} \partial(P)^{\partial(P)}. \qquad \square$$

When considering the product of polynomials it will be useful to bound the height by the height of the individual factors. The next proposition will be used several times to bound the height of a product of polynomials. A proof is given in Appendix A of Bugeaud [6].

Proposition 2.4. *Let $P, P_1, P_2, \ldots, P_l \in \mathbb{Z}[x]$ be polynomials such that $P = P_1 P_2 \ldots P_l$. Then*

$$2^{-\partial(P)} H(P_1) \ldots H(P_l) \leq H(P) \leq 2^{\partial(P)} H(P_1) \ldots H(P_l).$$

In particular, note that this implies

$$\Lambda(P_1)\Lambda(P_2)\dots\Lambda(P_l) = 2^{\partial(P)}H(P_1)H(P_2)\dots H(P_l) \leq 2^{\partial(P)}2^{\partial(P)}H(P) \leq (\Lambda(P))^2. \quad (2.3)$$

Occasionally this bound will not be sufficient and instead we will use the following bound for the height of the product of only two polynomials.

Proposition 2.5. *Let $P, Q \in \mathbb{Z}[x]$. Then*

$$H(PQ) \leq (\min\{\partial(P), \partial(Q)\} + 1)H(P)H(Q).$$

Proof. Suppose $P(x) = a_n x^n + \cdots + a_0$ and $Q(x) = b_m x^m + \cdots + b_0$ with a_n and b_m both nonzero. Assume without loss of generality $n \geq m$. The kth coefficient of PQ is $a_k b_0 + a_{k-1}b_1 + \cdots + a_{k-m}b_m$ where any coefficient with a negative subscript is defined to be 0. The standard absolute value of each of these summands in the kth coefficient is at most $H(P)H(Q)$ and since there are at most $m+1$ summands the kth coefficient can be at most $(m+1)H(P)H(Q)$. Thus $H(PQ) \leq (\min\{\partial(P), \partial(Q)\} + 1)H(P)H(Q)$. □

We will also require an upper bound on the height and degree of a polynomial obtained by taking the determinant of a matrix of polynomials. The following result is proved in Durand [10].

Proposition 2.6. *Let $\{P_{ij}(x)\}$ for $1 \leq i, j \leq n$ be polynomials in $\mathbb{Z}[x]$ and let M be the matrix*

$$M = \begin{pmatrix} P_{11} & P_{12} & \dots & P_{1n} \\ P_{21} & P_{22} & \dots & P_{2n} \\ \vdots & \vdots & & \vdots \\ P_{n1} & P_{n2} & \dots & P_{nn} \end{pmatrix}.$$

Then the determinant of M satisfies

$$\partial(\det(M)) \leq \sum_{j=1}^{n} \max_{1 \leq i \leq n} \partial(P_{ij}) \quad (2.4)$$

and

$$H(\det(M)) \leq \prod_{j=1}^{n} \left(\sum_{i=1}^{n} (1 + \partial(P_{ij}))H(P_{ij}) \right). \tag{2.5}$$

Proof. Both parts of the lemma are proved by induction on n. The base case is immediate for the first assertion. Assume that the first part of the lemma is true for any $(n-1)$ by $(n-1)$ matrix of integer polynomials. Then

$$\det(M) = \sum_{k=1}^{n} (-1)^{k-1} P_{1k} \det(M_k)$$

where M_k is the matrix obtained by deleting the first row and kth column of the original matrix. Thus

$$\begin{aligned} \partial(\det(M)) &\leq \max_{1 \leq j \leq n} \partial(P_{1j}) + \max_{1 \leq j \leq n} \partial(\det(M_j)) \\ &\leq \max_{1 \leq j \leq n} \partial(P_{1j}) + \sum_{i=2}^{n} \max_{1 \leq j \leq n} \partial(P_{ij}) \\ &= \sum_{i=1}^{n} \max_{1 \leq j \leq n} \partial(P_{ij}). \end{aligned}$$

The base case is likewise immediate for (2.5) also. Assume (2.5) is true for all $n-1$ by $n-1$ matrices. Using the notation from above it thus follows that

$$H(\det(M)) = H\left(\sum_{k=1}^{n} (-1)^{k-1} P_{1k} \det(M_k) \right) \leq \sum_{k=1}^{n} H(P_{1k} \det(M_k)).$$

Proposition 2.5 then implies

$$\begin{aligned} H(\det(M)) &\leq \sum_{k=1}^{n} (1 + \min\{\partial(P_{1k}), \partial(\det(M_k))\}) H(P_{1k}) H(\det(M_k)) \\ &\leq \sum_{k=1}^{n} (1 + \partial(P_{1k})) H(P_{1k}) H(\det(M_k)) \\ &\leq \max_{1 \leq k \leq n} \{H(\det(M_k))\} \sum_{k=1}^{n} (1 + \partial(P_{1k})) H(P_{1k}). \end{aligned}$$

Recall the induction hypothesis implies for $1 \leq k \leq n$

$$H(\det(M_k)) \leq \prod_{i=2}^{n} \sum_{\substack{j=1 \\ j \neq k}}^{n} (1 + \partial(P_{ij}))H(P_{ij}) \leq \prod_{i=2}^{n} \sum_{j=1}^{n} (1 + \partial(P_{ij}))H(P_{ij}).$$

Hence

$$H(\det(M)) \leq \left(\prod_{i=2}^{n}\sum_{j=1}^{n}(1+\partial(P_{ij}))H(P_{ij})\right)\left(\sum_{k=1}^{n}(1+\partial(P_{1k}))H(P_{1k})\right)$$
$$= \prod_{i=1}^{n}\sum_{j=1}^{n}(1+\partial(P_{ij}))H(P_{ij}). \qquad \square$$

Clearly $H(P+Q) \leq H(P)+H(Q)$. We will also require a bound on $H(\alpha+\beta)$ in terms of $H(\alpha)$ and $H(\beta)$. The next result is due to Dubickas and Smyth [8] and gives a bound for $L(\alpha+\beta)$ and thus can be used to obtain a bound for $H(\alpha+\beta)$. Note that a stronger inequality is given by Mignotte and Ştefănescu [23], but for our purposes it is sufficient to use this result on L and then express it in terms of H.

Proposition 2.7. *If $\alpha_1, \alpha_2, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ and $\partial(\alpha_1+\alpha_2+\cdots+\alpha_n) = d$ then*

$$L(\alpha_1+\alpha_2+\cdots+\alpha_n) \leq (L(\alpha_1)L(\alpha_2)\ldots L(\alpha_n))^d \tag{2.6}$$

and

$$H(\alpha_1+\alpha_2+\cdots+\alpha_n) \leq \left(\prod_{i=1}^{n}(1+\partial(\alpha_i))H(\alpha_i)\right)^d. \tag{2.7}$$

Proof. For the proof of (2.6) see Dubickas and Smyth [8]. In order to prove the inequality (2.7) note that $H(\alpha) \leq L(\alpha) \leq (1+\partial(\alpha))H(\alpha)$ for any $\alpha \in \overline{\mathbb{Q}}$. Thus (2.6) implies

$$\begin{aligned} H(\alpha_1+\alpha_2+\cdots+\alpha_n) &\leq L(\alpha_1+\alpha_2+\cdots+\alpha_n) \\ &\leq (L(\alpha_1)L(\alpha_2)\ldots L(\alpha_n))^d \\ &\leq \left(\prod_{i=1}^{n}(1+\partial(\alpha_i))H(\alpha_i)\right)^d. \end{aligned}$$ $\square$

To finish this section we now briefly give four additional results from algebra and number theory. The following theorem gives conditions which imply a polynomial is irreducible and will be used later in Chapter 4.

Theorem 2.8. *Eisenstein's Criterion. Let $P(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$. If there exists a prime $q \in \mathbb{N}$ such that q does not divide a_n, q divides $a_{n-1}, \ldots, a_0$, and q^2 does not divide a_0, then $P(x)$ is irreducible over $\mathbb{Q}$.*

Proof. The proof follows by way of contradiction. Let $P(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ and assume there exists a prime $q \in \mathbb{N}$ dividing $a_{n-1}, \ldots, a_0$ such that q does not divide a_n and q^2 does not divide a_0. Suppose that $P(x) = P_1(x)P_2(x)$ where $P_1(x), P_2(x) \in \mathbb{Z}[x]$ are two non-constant polynomials. Let $P_1(x) = b_m x^m + \cdots + b_0$ and $P_2(x) = c_k x^k + \cdots + c_0$. Then reducing modulo q gives $a_n x^n \equiv P_1(x)P_2(x) \mod q$. Since $a_n = b_m c_k$ is not divisible by q, both b_m and c_k are not divisible by q. Thus $P_1(x)$ and $P_2(x)$ are non-constant polynomials modulo q. It follows that x divides both $P_1(x)$ and $P_2(x)$ modulo q and hence $P_1(0) = b_0 \equiv 0 \mod q$ and $P_2(0) = c_0 \equiv 0 \mod q$. Since q divides both b_0 and c_0 it follows that q^2 divides $b_0 c_0 = a_0$, which is a contradiction. □

Since we will often be considering polynomials with integer coefficients we will require the following theorem which allows us to factor an integer polynomial into the product of integer polynomials if we can prove a factorization exists over the rationals. A proof can be found in Chapter 9 of Dummit and Foote [9].

Theorem 2.9. *Gauss's Lemma. If $Q(x) \in \mathbb{Z}[x]$ is reducible over $\mathbb{Q}$ then $Q(x)$ is reducible over $\mathbb{Z}$.*

The following theorem gives that any finite extension of a field of characteristic 0 can be generated by a single element. A proof is in Chapter 14 of Dummit and Foote.

Theorem 2.10. *If F is a field of characteristic 0 and K is a finite extension of F then there exists $\alpha \in K$ such that $K = F(\alpha)$.*

The final theorem of this section guarantees the existence of a prime number in certain intervals and will be used later in Chapter 4. A proof can be found in Niven, Zuckerman, and Montgomery [27].

Theorem 2.11. *Bertrand's Postulate. For every integer $n \geq 2$ there exists a prime $q \in \mathbb{N}$ that satisfies $n < q < 2n$.*

2.2 *p*-adic Numbers

We now turn our attention to the basic algebraic and topological properties of the p-adic numbers. The p-adic field is an extension of $\mathbb{Q}$ and was first introduced by Hensel [16]. Hensel sought an analogy between the theory of analytic functions and the rational numbers. Instead of constructing a Taylor series centered at a particular point to obtain local information about an analytic function at the particular point Hensel wrote rational numbers as a sum of powers of a prime number to obtain "local" information at the prime. Gouvêa [14] gives an elementary introduction to the p-adic numbers. Koblitz [17] and Robert [29] are also standard references on the p-adic numbers.

Definition 2.12. *Let F be a field. An* absolute value $|*| : F \to \mathbb{R}_{\geq 0}$ *on F is a function which satisfies $|a| = 0$ if and only if $a = 0$, and all $a, b \in F$ satisfy $|ab| = |a||b|$ and $|a + b| \leq |a| + |b|$.*

Let p be a fixed prime. We will use the notation log to denote the logarithm base p. If $a \in \mathbb{Z}\backslash\{0\}$ then there exist unique $m \in \mathbb{Z}$ with $\gcd(m, p) = 1$ and $n \in \mathbb{N}$, $n \geq 0$ such that $a = mp^n$. Define $v(a) = n$ and if $\frac{a}{b} \in \mathbb{Q} \setminus \{0\}$ with a, b integers then let $v(\frac{a}{b}) = v(a) - v(b)$. The *$p$-adic absolute value* on $\mathbb{Q}$ is defined by $|\frac{a}{b}|_p = p^{-v(a/b)}$ if $\frac{a}{b} \neq 0$ and $|0|_p = 0$. Since p is fixed in order to simplify notation we will usually write $|*| = |*|_p$. To prove $|*|$ is an absolute value on $\mathbb{Q}$ first note that $|a| = 0$ if and only if $a = 0$. Moreover, if $\frac{a}{b} = p^{n_1}(\frac{m_1}{k_1})$ and $\frac{c}{d} = p^{n_2}(\frac{m_2}{k_2})$ with $n_1, n_2, m_1, m_2, k_1, k_2 \in \mathbb{Z}$, $k_1, k_2 \neq 0$ and m_1, m_2, k_1, k_2 all relatively prime to p then

$$\left|\frac{a}{b}\frac{c}{d}\right| = \left|p^{n_1+n_2}\frac{m_1 m_2}{k_1 k_2}\right| = p^{-(n_1+n_2)} = |p^{n_1}|\,|p^{n_2}| = \left|p^{n_1}\frac{m_1}{k_1}\right|\left|p^{n_2}\frac{k_1}{k_2}\right| = \left|\frac{a}{b}\right|\left|\frac{c}{d}\right|.$$

Now assume without loss of generality $n_1 \leq n_2$. Then

$$\left|\frac{a}{b} + \frac{c}{d}\right| = \left|p^{n_1}\frac{m_1}{k_1} + p^{n_2}\frac{m_2}{k_2}\right| = \left|\frac{p^{n_1} m_1 k_2 + p^{n_2} m_2 k_1}{k_1 k_2}\right|$$

and since k_1 and k_2 are relatively prime to p

$$\left|\frac{a}{b} + \frac{c}{d}\right| = |p^{n_1} m_1 k_2 + p^{n_2} m_2 k_1| = |p^{n_1}||m_1 k_2 + p^{n_2 - n_1} m_2 k_1|.$$

Since $n_1 \leq n_2$ it follows that $n_2 - n_1 \geq 0$ and $m_1 k_2 + p^{n_2 - n_1} m_2 k_1$ is an integer. From the definition of $|*|$ any integer has p-adic absolute value at most 1. Thus

$$\left|\frac{a}{b} + \frac{c}{d}\right| \leq |p^{n_1}| = \max\left\{\left|\frac{a}{b}\right|, \left|\frac{c}{d}\right|\right\} \leq \left|\frac{a}{b}\right| + \left|\frac{c}{d}\right|$$

and $|*|$ is an absolute value on $\mathbb{Q}$. Note that $|*|$ satisfies a condition stronger than the standard triangle inequality. In particular, $|a+b| \leq \max\{|a|, |b|\}$ for all $a, b \in \mathbb{Q}$. An absolute value that satisfies this inequality is said to be *non-archimedean*. Moreover, $|a-b|$ defines a metric on $\mathbb{Q}$. A metric d defined on a space X is called an *ultrametric* if $d(a,b) \leq \max\{d(a,c), d(c,b)\}$ for all $a, b, c \in X$. It is clear that the metric induced by the p-adic absolute value is an ultrametric on $\mathbb{Q}$.

The *p-adic numbers* $\mathbb{Q}_p$ are constructed by taking the completion of $\mathbb{Q}$ with respect to the p-adic absolute value. If $\theta \in \mathbb{Q}_p$ then the p-adic absolute value on $\mathbb{Q}$ can be extended to $\mathbb{Q}_p$ be defining $|\theta| = \lim_{n\to\infty} |a_n|$ where $\{a_n\}$ is a Cauchy sequence in $\mathbb{Q}$ converging to θ. By considering the sequence $\{a_n\}$ converging to θ it can be proved that $|*|_p$ is a non-archimedean absolute value on $\mathbb{Q}_p$ (see Chapter 3 of Gouvêa [14]). Likewise define v on $\theta \in \mathbb{Q}_p$ by $v(\theta) = -\log|\theta|$. The *p-adic integers* are given by $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x| \leq 1\}$.

As with $\mathbb{R}$, the completion of $\mathbb{Q}$ with respect to $|*|_\infty$, the field $\mathbb{Q}_p$ is not algebraically closed. For example, $p^{1/2} \notin \mathbb{Q}_p$ because if it were then the properties of $|*|$ would imply $|p^{1/2}| = p^{-1/2}$, which is not an integer power of p. The algebraic closure of $\mathbb{Q}_p$ will be denoted by $\overline{\mathbb{Q}}_p$. Since $\mathbb{Q} \subset \mathbb{Q}_p$ the field $\overline{\mathbb{Q}}$ embeds in $\overline{\mathbb{Q}}_p$. The p-adic absolute value can be extended to all $\theta \in \overline{\mathbb{Q}}_p$ as follows. If $\theta \in \overline{\mathbb{Q}}_p$ has a minimal polynomial of degree n then define $|\theta| = |\operatorname{Nm}(\theta)|^{1/n}$ where $\operatorname{Nm}(\theta)$ is the norm of θ over the field $\mathbb{Q}_p$ given in the previous section. It is demonstrated that this extension of $|*|$ to $\overline{\mathbb{Q}}_p$ is a non-archimedean absolute value in Chapter 3 of Robert [29]. A direct consequence of the definition of Nm is that if $\alpha \in \overline{\mathbb{Q}}_p$ then the p-adic absolute value of α must equal the p-adic absolute value of every conjugate of α.

In the real case after taking the algebraic closure of $\mathbb{R}$ we obtain $\mathbb{C}$ which is algebraically closed and topologically complete. However, $\overline{\mathbb{Q}}_p$ is not complete. In fact the

sequence $\{\theta_n\} \subset \overline{\mathbb{Q}}_p$ which we will construct for Theorem 4.5 is an example of a Cauchy sequence in $\overline{\mathbb{Q}}_p$ that does not converge in $\overline{\mathbb{Q}}_p$. Define $\mathbb{C}_p$ to be the completion of $\overline{\mathbb{Q}}_p$ with respect to $|*|$. As when extending $|*|$ from $\mathbb{Q}$ to $\mathbb{Q}_p$ it is possible to extend $|*|$ from $\overline{\mathbb{Q}}_p$ to $\mathbb{C}_p$ to a non-archimedean absolute value by considering $|*|$ on Cauchy sequences converging to elements of $\mathbb{C}_p$. Likewise v can be extended to $\theta \in \mathbb{C}_p$ by defining $v(\theta) = -\log|\theta|$. The field $\mathbb{C}_p$ is topologically complete and algebraically closed (see Chapter 5 of Gouvêa [14] for a proof).

The following proposition gives several basic properties of the p-adic numbers.

Proposition 2.13.

(i) Suppose a is an nonzero integer. Then $1 \leq |a||a|_\infty$.

(ii) Let θ and η be elements of $\mathbb{C}_p$. If $|\theta| \neq |\eta|$ then $|\theta + \eta| = \max\{|\theta|, |\eta|\}$.

(iii) If $\{\theta_n\}$ is a convergent sequence in $\mathbb{C}_p$ that does not converge to 0 then the sequence $\{|\theta_n|\}$ is eventually constant.

(iv) Every nonzero $\theta \in \mathbb{Q}_p$ can be written uniquely in the form $a_n p^n + a_{n+1}p^{n+1} + \ldots$ where $n \in \mathbb{Z}$, $a_n \neq 0$, and $0 \leq a_i < p$ for all $i \geq n$.

Proof. Statement (i) follows easily from the definition of $|*|$. If a is a nonzero integer then there exist a unique nonzero $m \in \mathbb{Z}$ relatively prime to p and $n \in \mathbb{N}$ such that $a = mp^n$. Thus $|a||a|_\infty = p^{-n}p^n|m| = |m| \geq 1$.

To prove (ii) without loss of generality assume $|\eta| < |\theta|$. Then $|\theta + \eta| \leq |\theta|$ and

$$|\theta| = |(\theta + \eta) - \eta| \leq \max\{|\theta + \eta|, |\eta|\} = |\theta + \eta|.$$

Thus $|\theta + \eta| = |\theta| = \max\{|\theta|, |\eta|\}$.

To prove (iii) first assume $\{\theta_n\}$ is a sequence in $\mathbb{C}_p$ converging to $\theta \in \mathbb{C}_p$, $\theta \neq 0$. Then there exist $\epsilon > 0$ and $M_1 \in \mathbb{N}$ such that $|\theta_n| \geq \epsilon$ for all $n \geq M_1$. Moreover,

there also exists $M_2 \geq M_1$ for which $|\theta_n - \theta_m| < \epsilon$ for all $n, m \geq M_2$. The properties of the p-adic absolute value give $|\theta_n - \theta_m| \leq \max\{|\theta_n|, |\theta_m|\}$ for all $n, m \geq M_2$. Since $\max\{|\theta_n|, |\theta_m|\} \geq \epsilon$ this implies $|\theta_n - \theta_m| < \max\{|\theta_n|, |\theta_m|\}$ and by (ii) it thus follows that $|\theta_n| = |\theta_m|$ for all $n, m \geq M_2$.

The proof of (iv) requires a bit more work than the previous parts of the proposition. Our proof follows that of Koblitz [17]. We will first consider the case where $|\theta| = 1$. Note that if $\theta = a_0 + a_1 p + a_2 p^2 \cdots = b_0 + b_1 p + b_2 p^2 + \ldots$ has two distinct representations of this form then there exists $k \geq 0$ such that $a_k \neq b_k$ and $a_i = b_i$ for all $0 \leq i < k$. Then since $a_k - b_k \neq 0$ it follows from part (ii) of the proposition that

$$\begin{aligned} 0 &= |(a_0 + a_1 p + a_2 p^2 + \ldots) - (b_0 + b_1 p + b_2 p^2 \ldots)| \\ &= |(a_k - b_k)p^k + (a_{k+1} - b_{k-1})p^{k+1} + \ldots| \\ &= \max\{|(a_k - b_k)p^k|, |(a_{k+1} - b_{k-1})p^{k+1} + \ldots|\} \\ &= p^{-k}. \end{aligned}$$

This is a contradiction and thus $a_i = b_i$ for all $i \geq 0$. Hence if such a representation exists it must be unique.

In order to prove such a representation exists recall that we assumed $|\theta| = 1$ and $\theta \in \mathbb{Q}_p$. Let $\{b_i\}$ be a Cauchy sequence in $\mathbb{Q}$ converging to θ. Since θ is nonzero in part (iii) we proved there exists $M_2 \in \mathbb{N}$ such that $|b_i| = 1$ is constant for all $i \geq M_2$. Without loss of generality delete the first M_2 terms in the sequence $\{b_i\}$ and relabel such that b_{M_2+i} is now b_i. Since $\{b_i\}$ is Cauchy it is possible to define $N(k)$ such that for all $k \in \mathbb{N}$, $N(k) \geq k$ and for all $i, j \geq N(k)$,

$$|b_i - b_j| \leq p^{-k}. \tag{2.8}$$

Let $b_{N(i)} = \frac{c_i}{d_i}$ be in lowest terms. It follows that both c_i and d_i are relatively prime to p since $|b_i| = 1$. In particular there exist $h_i, l_i \in \mathbb{Z}$ satisfying $h_i d_i + l_i p^i = 1$. Let m_i be the integer such that $0 \leq h_i c_i + m_i p^i \leq p^i - 1$ and define $\alpha_i = h_i c_i + m_i p^i$. The sequence

$\{\alpha_i\}$ will provide us with the desired representation of θ. Now note

$$\left|\alpha_i - b_{N(i)}\right| = \left|\frac{c_i}{d_i}\right| \left|h_i d_i + \frac{d_i}{c_i} m_i p^i - 1\right| = \left|h_i d_i - 1 + \frac{d_i}{c_i} m_i p^i\right|$$

and recall that $h_i d_i + l_i p^i = 1$ so we have

$$\left|\alpha_i - b_{N(i)}\right| = \left|-l_i p^i + \frac{d_i}{c_i} m_i p^i\right| \leq p^{-i} \max\left\{\left|-l_i\right|, \left|\frac{d_i}{c_i} m_i\right|\right\}.$$

Since l_i, d_i and m_i are integers and c_i is relatively prime to p it follows that

$$|\alpha_i - b_{N(i)}| \leq p^{-i}. \tag{2.9}$$

We now prove $\alpha_{j+1} \equiv \alpha_j \mod p^j$ for all $j \geq 1$. Note that

$$|\alpha_{j+1} - \alpha_j| \leq \max\{|\alpha_{j+1} - b_{N(j+1)}|, |b_{N(j+1)} - b_{N(j)}|, |b_{N(j)} - \alpha_j|\}.$$

From (2.8) and (2.9) it thus follows that

$$|\alpha_{j+1} - \alpha_j| \leq \max\left\{p^{-(j+1)}, p^{-j}, p^{-j}\right\} = p^{-j}. \tag{2.10}$$

Since the α_i are integers the definition of the p-adic absolute value implies $\alpha_{j+1} = \alpha_j + a_j p^j$ for some $a_j \in \mathbb{Z}$. From the definition of each α_i recall that $0 \leq \alpha_i < p^i$. Thus $0 \leq a_j < p$. Letting $a_0 = \alpha_1$ it follows that

$$\alpha_{j+1} = \alpha_j + a_j p^j = \alpha_{j-1} + a_{j-1} p^{j-1} + a_j p^j = \cdots = a_0 + a_1 p + \cdots + a_{j-1} p^{j-1} + a_j p^j. \tag{2.11}$$

Thus $\lim_{j\to\infty} \alpha_j$ is of the desired form and all that remains to demonstrate is that $\lim_{j\to\infty} \alpha_j = \theta$. Note that if $i > j$ then

$$\begin{aligned} |\alpha_i - \alpha_j| &\leq \max\{|\alpha_i - \alpha_{i-1}|, |\alpha_{i-1} - \alpha_{i-2}|, \ldots, |\alpha_{j+1} - \alpha_j|\} \\ &\leq \max\left\{p^{-(i-1)}, p^{-(i-2)}, \ldots, p^{-(j+1)}, p^{-j}\right\} \\ &= p^{-j}. \end{aligned}$$

Since $\{b_j\}$ is a Cauchy sequence converging to θ it suffices to prove $\lim_{i\to\infty} |\alpha_i - b_i| = 0$. Apply the previous inequality and (2.9), (2.8) to obtain for any $i \geq N(j)$

$$|\alpha_i - b_i| \leq \max\{|\alpha_i - \alpha_j|, |\alpha_j - b_{N(j)}|, |b_i - b_{N(j)}|\} \leq \max\left\{p^{-j}, p^{-j}, p^{-j}\right\} = p^{-j}.$$

Thus $\{a_i\}$ converges to θ.

Recall that we assumed $|\theta| = 1$. In the case where $|\theta| = p^{-n}$ for some integer n then $p^{-n}\theta$ will satisfy $|p^{-n}\theta| = 1$ and thus have a unique representation of the form $a_0 + a_1 p + \ldots$ with $a_0 \neq 0$ and $0 \leq a_i < p$ for $i \geq 0$. It follows that $a_0 p^n + a_1 p^{n+1} + \ldots$ must be a unique representation of θ in the desired form. □

The topology of $\mathbb{C}_p$ is substantially different from the topology of $\mathbb{R}$ or $\mathbb{C}$. Proofs and discussion of the topological properties of $\mathbb{C}_p$ can be found in Robert [29] and Gouvêa [14]. The space $\mathbb{C}_p$ is totally disconnected and any ball of positive radius is both open and closed. Moreover, given any two open (or closed) balls in $\mathbb{C}_p$ one is contained in the other, or they are disjoint. Although $\mathbb{Q}_p$ and all finite extension fields of $\mathbb{Q}_p$ are locally compact both $\overline{\mathbb{Q}}_p$ and $\mathbb{C}_p$ are not. In particular, any nonempty closed bounded ball of positive radius in $\overline{\mathbb{Q}}_p$ and $\mathbb{C}_p$ is not compact. However, there is still a p-adic analogue of the maximum modulus principle (see Chapter 6 of Robert [29] for a proof).

Proposition 2.14. *Let $f(x)$ be a power series centered at 0 with coefficients in $\mathbb{C}_p$. If r is a rational power of p and $f(x)$ converges on the closed ball centered at 0 of radius r then*

$$\sup_{|x|\leq r} |f(x)| = \max_{|x|\leq r} |f(x)| = \sup_{|x|=r} |f(x)| = \max_{|x|=r} |f(x)|.$$

Now that the basic structure of the p-adic numbers has been given we state several more results on $\mathbb{Q}_p$. The following theorem is proved in Chapter 3 of Robert [29].

Theorem 2.15. *Given $n \in \mathbb{N}$ there are only finitely many extensions of $\mathbb{Q}_p$ of degree n in $\overline{\mathbb{Q}}_p$.*

Another important theorem that takes advantage of the properties of the p-adic numbers is Krasner's Lemma which states that if $\alpha, \beta \in \overline{\mathbb{Q}}_p$ and β is sufficiently close to α with respect to $|*|$ then the field generated by β contains the field generated by α.

Theorem 2.16. *Krasner's Lemma. Let K be a finite extension field of $\mathbb{Q}_p$ and $\alpha \in \overline{\mathbb{Q}}_p$. Let $\alpha = \alpha_1, \alpha_2, \ldots \alpha_n \in \overline{\mathbb{Q}}_p$ denote the conjugates of α over K. If $\beta \in \overline{\mathbb{Q}}_p$ satisfies $|\beta - \alpha| < |\alpha - \alpha_i|$ for all $2 \leq i \leq n$ then $K(\alpha) \subseteq K(\beta)$.*

Proof. The proof follows by contradiction. Assume $|\beta - \alpha| < |\alpha - \alpha_i|$ for all $2 \leq i \leq n$ and $\alpha \notin K(\beta)$. It follows that $[K(\beta, \alpha) : K(\beta)] \geq 2$. Let σ be a field homomorphism from $K(\beta, \alpha)$ to $\overline{\mathbb{Q}}_p$ such that $K(\beta)$ is fixed and $\sigma(\alpha) = \alpha_i$ for some $2 \leq i \leq n$. Recall from our definition of $|*|$ on $\overline{\mathbb{Q}}_p$ that $|\theta| = |\sigma(\theta)|$ for any $\theta \in K(\beta, \alpha)$. Thus

$$|\beta - \alpha| = |\sigma(\beta - \alpha)| = |\sigma(\beta) - \sigma(\alpha)| = |\beta - \sigma(\alpha)|.$$

It follows that $|\alpha - \sigma(\alpha)| \leq \max\{|\alpha - \beta|, |\beta - \sigma(\alpha)|\} = |\alpha - \beta|$, which contradicts the assumption $|\beta - \alpha| < |\alpha - \alpha_i|$ for $2 \leq i \leq n$. □

If $\alpha \in \overline{\mathbb{Q}}_p$ let $m_{\alpha,\mathbb{Q}_p}(x) \in \mathbb{Q}_p[x]$ be the minimal polynomial of α over $\mathbb{Q}_p$. From part (iv) of Proposition 2.13 each coefficient of $m_{\alpha,\mathbb{Q}_p}(x)$ can be uniquely written as a series in powers of p. Let k be the smallest power of p appearing in the expansions of the coefficients of $m_{\alpha,\mathbb{Q}_p}(x)$. The polynomial $p^{-k} m_{\alpha,\mathbb{Q}_p}(x)$ must have coefficients in $\mathbb{Z}_p = \{\theta \in \mathbb{Q}_p : |\theta| \leq 1\}$ and will be referred to as the *minimal polynomial* of α over $\mathbb{Z}_p$.

Now let $Q(x) = a_n x^n + \cdots + a_0$ be a polynomial with coefficients in $\mathbb{Q}_p$ and define $\|Q\|$ by $\|Q\| = \max\{|a_n|, \ldots, |a_0|\}$. If $P(x) \in \mathbb{Q}_p[x]$ then $\|P - Q\|$ defines a metric on $\mathbb{Q}_p[x]$. To prove this first note $\|P - Q\| = 0$ if and only if the coefficients of P equal the coefficients of Q. Thus $\|P - Q\| = 0$ if and only if $P = Q$. Since $|a| = |-a|$ for all $a \in \mathbb{Q}_p$ it is clear that $\|P - Q\| = \|Q - P\|$. Finally, if $P(x) = b_m x^m + \cdots + b_0$ and $m \geq n$ then the coefficients of $P - Q$ are of the form b_i if $n < i \leq m$, or $b_i - a_i$ if $0 \leq i \leq n$. Thus if $n < i \leq m$ then $|b_i| \leq \|P\| \leq \max\{\|P\|, \|Q\|\}$ and if $0 \leq i \leq n$ then $|b_i - a_i| \leq \max\{|b_i|, |a_i|\} \leq \max\{\|P\|, \|Q\|\}$. Hence the triangle inequality is satisfied and $\|*\|$ induces an ultrametric on $\mathbb{Q}_p[x]$. A sequence of polynomials $\{Q_m\}$ in $\mathbb{Q}_p[x]$ converging to Q with respect to $\|*\|$ must be such that the p-adic absolute value of the coefficients of $Q_m - Q$ tend to zero as m increases.

The following corollary to Krasner's Lemma demonstrates that if two polynomials are close with respect to $\|*\|$ then they must also have roots that are close with respect to $|*|$ and as a result the roots satisfy the hypotheses of Krasner's Lemma. This will be used in Chapter 4 and to prove $\overline{\mathbb{Q}}$ is dense in $\mathbb{C}_p$.

Corollary 2.17. *Let $\alpha \in \overline{\mathbb{Q}}_p$ and let $Q(x) \in \mathbb{Z}_p[x]$ be the minimal polynomial of α over $\mathbb{Z}_p$. Let n be the degree of Q and suppose $\{Q_m(x)\} \subset \mathbb{Z}_p[x]$ is a sequence that converges to $Q(x)$ with respect to $\|*\|$. Denote the degree of Q_m by n_m and suppose $n_m \leq n$ for all $m \in \mathbb{N}$. Then there exist $M \in \mathbb{N}$ and a sequence $\{\beta_m\} \subset \overline{\mathbb{Q}}_p$ such that for all $m \geq M$, we have $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta_m)$, $Q_m(\beta_m) = 0$, and*

$$|\alpha - \beta_m| \leq c\|Q - Q_m\|^{1/n} \tag{2.12}$$

for some constant c depending only on α.

Proof. Let α, Q, n, and $\{Q_m\}$ be as in the statement of the corollary and suppose that $Q_m(x) = b_{m,n}x^n + b_{m,n-1}x^{n-1} + \cdots + b_{m,0}$ and $Q(x) = a_n x^n + \cdots + a_0$ where it is possible $b_{m,n} = 0$. Since the sequence $\{Q_m\}$ converges to Q with respect to $\|*\|$ the sequence $\{b_{m,n}\}$ must converge to $a_n \neq 0$ and hence part (iii) of Proposition 2.13 implies there exists $M_1 \in \mathbb{N}$ such that $|b_{m,n}| = |a_n|$ for all $m \geq M_1$. It follows that the degree of Q_m is n for all $m \geq M_1$.

From now on we will assume $m \geq M_1$ and let $c = |a_n|$. Let $\beta_{m,1}, \beta_{m,2}, \ldots, \beta_{m,n} \subset \overline{\mathbb{Q}}_p$ be the (not necessarily distinct) roots of Q_m. Then

$$|Q(\alpha) - Q_m(\alpha)| = |Q_m(\alpha)| = |b_{m,n}| \prod_{i=1}^{n} |\alpha - \beta_{m,i}| \geq c \min_{1 \leq i \leq n} |\alpha - \beta_{m,i}|^n. \tag{2.13}$$

Let β_m be a root of Q_m for which the minimum is attained. Note that the p-adic triangle inequality implies

$$|Q(\alpha) - Q_m(\alpha)| = |(a_n - b_{m,n})\alpha^n + \cdots + (a_0 - b_{m,0})| \leq \|Q - Q_m\| \max\{1, |\alpha|^n\}$$

and the inequality (2.13) becomes

$$c|\alpha - \beta_m|^n \leq \|Q - Q_m\| \max\{1, |\alpha|^n\}.$$

Thus

$$|\alpha - \beta_m| \leq c^{-1/n} \max\{1, |\alpha|\} \|Q - Q_m\|^{1/n}.$$

The term $c^{-1/n} \max\{1, |\alpha|\}$ is a constant depending only on α and (2.12) follows.

It only remains to prove that $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta_m)$ for all m sufficiently large. Since $\{\|Q - Q_m\|\}$ converges to 0 there exists $M_2 \geq M_1$ such that for all $m \geq M_2$

$$|\alpha - \beta_m| \leq c^{-1/n} \max\{1, |\alpha|\} \|Q - Q_m\|^{1/n} \leq \min\{|\alpha - \alpha_i|\}$$

where the minimum is taken over all conjugates α_i of α not equal to α. Krasner's Lemma implies $\mathbb{Q}_p(\alpha) \subseteq \mathbb{Q}_p(\beta_m)$ for all $m \geq M_2$. Since β_m is a root of Q_m the degree of β_m over $\mathbb{Q}_p$ is less than or equal to n for all $m \geq M_2$. It follows that $\mathbb{Q}_p(\beta_m) = \mathbb{Q}_p(\alpha)$ for all $m \geq M_2$. □

Corollary 2.18. *The field $\overline{\mathbb{Q}}$ is dense in $\mathbb{C}_p$.*

Proof. Since $\mathbb{C}_p$ is the completion of $\overline{\mathbb{Q}}_p$ it suffices to prove $\overline{\mathbb{Q}}$ is dense in $\overline{\mathbb{Q}}_p$. Suppose $\alpha \in \overline{\mathbb{Q}}_p$. Let $Q(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}_p[x]$ be the minimal polynomial of α over $\mathbb{Z}_p$. Write each coefficient of Q in its base p expansion such that $a_i = a_{i,0} + a_{i,1}p + a_{i,2}p^2 + \ldots$ and define the sequence of polynomials $\{P_m(x)\} \subset \mathbb{Z}[x]$ by $P_m(x) = b_{m,n}x^n + \cdots + b_{m,0}$ where $b_{m,i} = a_{i,0} + a_{i,1}p + \cdots + a_{i,m}p^m$. The sequence $\{P_m\}$ converges to Q with respect to $\|*\|$ and the hypotheses of Corollary 2.17 are satisfied. Thus there exist $M \in \mathbb{N}$, a sequence $\{\beta_m\} \in \overline{\mathbb{Q}}_p$, and a constant c depending only on α such that for all $m \geq M$,

$$|\alpha - \beta_m| \leq c\|Q - Q_m\|^{1/n}$$

and $Q_m(\beta_m) = 0$. Since $Q_m(x) \in \mathbb{Z}[x]$ it follows that $\beta_m \in \overline{\mathbb{Q}}$ for all $m \geq M$. Thus $\{\beta_m\}$ is a sequence of algebraic numbers converging to α and the result follows. □

3 PROPERTIES OF O ON $\mathbb{C}_P$

Let p be a fixed prime and define log to be the logarithm to the base p. Denote the p-adic absolute value by $|*|$ and the standard absolute value by $|*|_\infty$. Recall that we denote the degree of an integer polynomial P by $\partial(P)$ and the maximum of the absolute value of the coefficients of P by $H(P)$. Define Λ by $\Lambda(P) = 2^{\partial(P)}H(P)$. Using Mahler's order functions as a template we define O on $\mathbb{C}_p$ as follows.

Definition 3.1. *Let $\theta \in \mathbb{C}_p$. Define $O(*|\theta) : \mathbb{N} \to \mathbb{R}$ by*

$$O(u|\theta) = \max_{\substack{\Lambda(P)\leq u \\ P(\theta)\neq 0}} \log \frac{1}{|P(\theta)|}$$

where the P are polynomials in $\mathbb{Z}[x]$.

The maximum can be used in this definition because for any $u \in \mathbb{N}$ there are only finitely many integer polynomials P satisfying $\Lambda(P) \leq u$ since a bound on Λ bounds both the degree and the height of a polynomial. Also note that when defining the complex order functions Mahler used $\Lambda'(P) = 2^{\partial(P)}L(P)$, where $L(P)$ is the sum of the absolute values of the coefficients of P, instead of $\Lambda(P) = 2^{\partial(P)}H(P)$. This change does not affect any of the results in the complex case or p-adic case since it can be shown that the terms introduced by applying the inequalities $H(P) \leq L(P) \leq (1 + \partial(P))H(P)$ when changing from Λ' to Λ are negligible. As with the complex case for a fixed $\theta \in \mathbb{C}_p$ the function $O(u|\theta)$ is a non-negative increasing function because $\Lambda(1) = 1$. We will use the same partial order Mahler defined on the complex order functions.

Definition 3.2. *Let $a(u)$ and $b(u)$ be non-decreasing functions from $\mathbb{N}$ to $\mathbb{R}$ which are positive for sufficiently large u. Define the partial order $\gg$ by $a(u) \gg b(u)$ (or equivalently $b(u) \ll a(u)$) if there exist $c, u_0 \in \mathbb{N}$ and $\gamma \in \mathbb{R}^+$ such that $a(u^c) \geq \gamma b(u)$ for all $u \geq u_0$. Define the equivalence relation $\asymp$ by $a(u) \asymp b(u)$ if $a(u) \gg b(u)$ and $b(u) \gg a(u)$.*

Define the partial order $\gg$ on $\mathbb{C}_p$ by $\theta \gg \eta$ if $O(u|\theta) \gg O(u|\eta)$ and define the equivalence relation $\asymp$ on $\mathbb{C}_p$ by $\theta \asymp \eta$ if $O(u|\theta) \asymp O(u|\eta)$.

In Section 3.1 we first prove $O(u|\theta) \gg \log u$ for all $\theta \in \mathbb{C}_p$ and then show a result of Escassut [12] implies there exist transcendental $\theta \in \mathbb{C}$ such that $O(u|\theta) \asymp \log u$. The main result of Section 3.2 is that if $\theta, \eta \in \mathbb{C}_p$ and η is algebraic over $\mathbb{Q}(\theta)$ then $O(u|\theta) \gg O(u|\eta)$. From this it will follow that $O(u|\alpha) \asymp \log u$ for all $\alpha \in \overline{\mathbb{Q}}$.

3.1 Preliminary Results

We first prove the following proposition which gives a lower bound on O.

Proposition 3.3. *Let $\theta \in \mathbb{C}_p$. Then $O(u|\theta) \gg \log u$.*

Proof. For any $u \in \mathbb{N}, u > p$ let $n \in \mathbb{N}$ be such that $p^n \leq u < p^{n+1}$. Let $Q_n(x)$ be the constant polynomial p^n. Then

$$\begin{aligned} O(u|\theta) &= \max_{\Lambda(P) \leq u} \log\left(\frac{1}{|P(\theta)|}\right) \\ &\geq \log\left(\frac{1}{|Q_n(\theta)|}\right) \\ &= \log(p^n) = n > \log u - 1 > c \log u \end{aligned}$$

where c is some positive constant. Thus $O(u|\theta) \gg \log u$. □

Recall that in the complex case all transcendental $\theta \in \mathbb{C}$ satisfy $O(u|\theta) \gg (\log u)^2$. This does not hold in the p-adics. The following theorem is due to Escassut [12] and will not be proved here. A direct consequence is that there exist transcendental $\theta \in \mathbb{C}_p$ for which $O(u|\theta) \asymp \log u$. Recall that $\|P\|$ denotes the maximum of the coefficients of $P(x) \in \mathbb{Q}_p[x]$ with respect to the p-adic absolute value.

Theorem 3.4. *There exist $\theta \in \mathbb{C}_p$ transcendental over $\mathbb{Q}_p$ such that for all $P(x) \in \mathbb{Q}_p[x]$, $\log \frac{1}{|P(\theta)|} \leq -\log\|P\| + c\partial(P)$ where c is some constant depending on θ.*

Corollary 3.5. *There exist $\theta \in \mathbb{C}_p$ transcendental over $\mathbb{Q}$ such that $O(u|\theta) \asymp \log u$.*

Proof of Corollary 3.5. Let θ be as in Theorem 3.4. If θ is transcendental over $\mathbb{Q}_p$ then θ is transcendental over $\mathbb{Q}$ because $\mathbb{Q}$ is contained in $\mathbb{Q}_p$. Given $u \in \mathbb{N}$ let $P(x) \in \mathbb{Z}[x]$ be such that $O(u|\theta) = \log \frac{1}{|P(\theta)|}$ and $\Lambda(P) \leq u$. Since all polynomials in $\mathbb{Z}[x]$ are also in $\mathbb{Q}_p[x]$ Theorem 3.4 implies that

$$O(u|\theta) = \log \frac{1}{|P(\theta)|} \leq \log \frac{1}{\|P\|} + c\partial(P) \tag{3.1}$$

where c is a constant depending only on θ. Note that $\|P\| = |a|$ where $a \in \mathbb{Z}$ is some coefficient of P. By part (i) of Proposition 2.13

$$\frac{1}{\|P\|} = \frac{1}{|a|} \leq |a|_\infty \leq H(P).$$

Since $\Lambda(P) = 2^{\partial(P)}H(P)$ it follows from (3.1) that

$$O(u|\theta) \leq \log H(P) + c\partial(P) \leq \log \Lambda(P) + c\frac{1}{\log 2}(\log \Lambda(P) - \log H(P)) \leq c' \log \Lambda(P)$$

where c' is a constant depending only on θ. Thus $O(u|\theta) \ll \log u$ and by Proposition 3.3 $O(u|\theta) \asymp \log u$. □

3.2 Equivalence of Order Functions

Recall that if θ and η are elements of $\mathbb{C}_p$ then θ and η are algebraically dependent over a subfield $K \subseteq \mathbb{C}_p$ if θ is algebraic over $K(\eta)$ and η is algebraic over $K(\theta)$. If we state two numbers are algebraically dependent without mentioning a base field it is implied they are algebraically dependent over $\mathbb{Q}$. Our main result for this section is the following theorem.

Theorem 3.6. *Let $\theta, \eta \in \mathbb{C}_p$ be nonzero and such that η is algebraic over $\mathbb{Q}(\theta)$. Then $O(u|\theta) \gg O(u|\eta)$.*

Before proving Theorem 3.6 we first demonstrate the following lemma.

Lemma 3.7. *Let $M = (a_{i,j})$ be an n by n matrix. Then*

$$|\det(M)| \leq \prod_{j=1}^{n} \max_{1 \leq i \leq n} \{|a_{i,j}|\}$$

Proof of Lemma 3.7. The Leibniz formula for the determinant states

$$\det(M) = \sum_{\sigma \in S_n} \left(\operatorname{sgn}(\sigma) \prod_{j=1}^{n} a_{\sigma(j),j} \right).$$

Taking the p-adic absolute value of this gives

$$|\det(M)| \leq \max_{\sigma \in S_n} \left\{ \left| \operatorname{sgn}(\sigma) \prod_{j=1}^{n} a_{\sigma(j),j} \right| \right\} \leq \prod_{j=1}^{n} \max_{1 \leq i \leq n} \{|a_{i,j}|\}. \qquad \square$$

In the complex case Mahler [22] originally proved the order functions of algebraically dependent elements are equivalent. Later Durand [10] presented an alternative proof. Our proof that algebraically dependent elements of $\mathbb{C}_p$ have equivalent order functions follows Durand's proof with only a few changes to take into account the p-adic absolute value and our different definition of Λ.

Proof of Theorem 3.6. If η is algebraic over $\mathbb{Q}(\theta)$ then there exists $P(x, y) \in \mathbb{Z}[x, y]$ such that $P(\theta, \eta) = 0$ and

$$P(x, y) = \sum_{i=0}^{n} a_i(x) y^i$$

with $a_i(x) \in \mathbb{Z}[x], a_n(\theta) \neq 0$. Fix $u \in \mathbb{N}$. Let $Q(y) \in \mathbb{Z}[y]$ be a polynomial that satisfies $O(u|\eta) = \log\left(\frac{1}{|Q(\eta)|}\right)$ and $\Lambda(Q) \leq u$. Let

$$Q(y) = \sum_{i=0}^{q} b_i y^j$$

with $b_q \neq 0$. Note that Q, q, and the b_i depend on u while P, n, and the $a_i(x)$ depend only on θ and η.

Consider $P(x, y)$ as a polynomial in y with coefficients in $\mathbb{Z}[x]$. Using the notation from Definition 2.1

$$M_s(P(x,y),Q(y)) = \begin{pmatrix} a_n(x) & & & & b_q & & & \\ a_{n-1}(x) & a_n(x) & & & b_{q-1} & b_q & & \\ \vdots & \vdots & \ddots & a_n(x) & \vdots & \vdots & \ddots & b_q \\ a_0(x) & a_1(x) & & \vdots & b_0 & b_1 & & \vdots \\ & a_0(x) & & \vdots & & b_0 & & \vdots \\ & & \ddots & \vdots & & & \ddots & \vdots \\ & & & a_0(x) & & & & b_0 \end{pmatrix}.$$

Also define the polynomial $T(x) \in \mathbb{Z}[x]$ to be $R(P(x, y), Q(y)) = \det(M_s(P(x, y), Q(y)))$, the resultant of $P(x, y)$ and $Q(y)$. Since the polynomials a_i depend only on η and θ and the b_i are constant polynomials in x applying Proposition 2.6 to $M_s(P(x, y), Q(y))$ implies there exists a constant $c_1 \geq 1$ depending only on η and θ such that

$$\partial(T) \leq \sum_{j=1}^{q} \max_{0 \leq i \leq n} \partial(a_i) \leq q \max_{0 \leq i \leq n} (\partial(a_i)) = c_1 q. \tag{3.2}$$

Proposition 2.6 also implies

$$H(T) \leq \left(\prod_{j=1}^{q} \sum_{i=0}^{n} (1 + \partial(a_i)) H(a_i) \right) \left(\prod_{j=q+1}^{n+q} \sum_{i=0}^{q} (1 + \partial(b_i)) H(b_i) \right)$$

where the first factor corresponds to the first q columns of $M_s(P(x, y), Q(y))$ and the second factor corresponds to the remaining n columns of $M_s(P(x, y), Q(y))$. Since the sums in both factors are independent of j it follows that

$$H(T) \leq \left(\sum_{i=0}^{n} (1 + \partial(a_i)) H(a_i) \right)^q \left(\sum_{i=0}^{q} H(b_i) \right)^n.$$

Note that the a_i and n depend only on η and θ, and that $H(b_i) = |b_i|_\infty \leq H(Q)$. Thus

$$H(T) \leq c_2^q ((q + 1) H(Q))^n \tag{3.3}$$

where $c_2 \geq 1$ is another constant depending only on η and θ. From the definition of Λ it follows from (3.2) and (3.3) that

$$\Lambda(T) = 2^{\partial(T)} H(T) \leq (2^{c_1} c_2)^q (q+1)^n H(Q)^n \leq (2^q)^{c'} (q+1)^n H(Q)^n.$$

for some constant c' depending only on θ and η. For q sufficiently large the term $(2^q)^{c'}$ will be greater than $(q+1)^n$ and thus there exists a constant $c \geq n$ depending only on θ and η such that

$$\Lambda(T) \leq (2^q)^c H(Q)^n \leq (\Lambda(Q))^c.$$

Hence

$$\log\left(\frac{1}{|T(\theta)|}\right) \leq \max_{\Lambda(P) \leq \Lambda(Q)^c} \log\left(\frac{1}{|P(\theta)|}\right) = O(\Lambda(Q)^c|\theta) \leq O(u^c|\theta).$$

Now that we have proved

$$\log\left(\frac{1}{|T(\theta)|}\right) \leq O(u^c|\theta) \tag{3.4}$$

the next step will be to find a lower bound on $\log\left(\frac{1}{|T(\theta)|}\right)$ in terms of $O(u|\eta)$. Consider the matrix

$$M = \begin{pmatrix}
a_n(\theta) & & & & b_q & & & \\
a_{n-1}(\theta) & a_n(\theta) & & & b_{q-1} & b_q & & \\
\vdots & \vdots & \ddots & a_n(\theta) & \vdots & \vdots & \ddots & b_q \\
a_0(\theta) & a_1(\theta) & & \vdots & b_0 & b_1 & & \vdots \\
 & a_0(\theta) & & \vdots & & b_0 & & \vdots \\
 & & \ddots & \vdots & & & \ddots & \vdots \\
 & & & a_0(\theta) & & & & b_0
\end{pmatrix}$$

and note $M = M_s(P(\theta, y), Q(y))$. By applying elementary row operations construct a new matrix M' as follows. For every $1 \leq i \leq n+q$ multiply the ith row of M by η^{n+q-i} and add it to the last row. Thus the lower left entry of M' becomes

$$a_n(\theta)\eta^{n+q-1} + a_{n-1}(\theta)\eta^{(n-1)+q-1} + \cdots + a_0(\theta)\eta^{q-1} = \eta^{q-1} P(\theta, \eta).$$

By simplifying the rest of the entries in this manner the bottom row of M' is equal to

$$\eta^{q-1}P(\theta,\eta), \eta^{q-2}P(\theta,\eta), \ldots, P(\theta,\eta), \eta^{n-1}Q(\eta), \eta^{n-2}Q(\eta), \ldots, Q(\eta).$$

Since $P(\theta, \eta) = 0$ the first q entries of the bottom row of M' are 0. Let M_i be the determinant of the minor obtained by deleting the bottom row and ith column of M'. Then expanding along the last row of M' gives

$$|\det(M)| = |\det(M')| = \left| \sum_{1 \le i \le n} (-1)^{n+q+q+i} \eta^{n-i} Q(\eta) M_{q+i} \right|$$
$$\le |Q(\eta)| \max\{|\eta^{n-1}|, 1\} \max_{1 \le i \le n} \{|M_{q+i}|\}.$$

Now apply Lemma 3.7 to the $|M_{q+i}|$. The b_i are integers and must satisfy $|b_i| \le 1$ for all i. Thus when applying Lemma 3.7 we only consider the first q columns. Hence

$$|\det(M)| \le |Q(\eta)| \max\{|\eta^{n-1}|, 1\} \left(\max_{0 \le i \le n} \{|a_i(\theta)|\} \right)^q. \tag{3.5}$$

To simplify notation let $\kappa = \max\{\partial(a_0), \ldots \partial(a_l)\}$, and note that κ depends only on η and θ because the a_i depend only on η and θ. The $a_i(\theta)$ are polynomials with integer coefficients in θ. Since the p-adic absolute value of any integer is at most 1 it follows $|a_i(\theta)| \le \max\{|\theta|^\kappa, 1\}$ for $0 \le i \le n$. Thus (3.5) becomes

$$|\det(M)| \le |Q(\eta)| \max\{|\eta^{n-1}|, 1\} \max\{|\theta|^{q\kappa}, 1\}.$$

Let c_3 and c_4 be constants depending only on θ and η such that $c_3 = \max\{1, |\eta|^{n-1}\}$ and if $|\theta| \ge 1$ then $|\theta|^\kappa = 2^{c_4}$ and $c_4 = 1$ otherwise. Substituting these constants into the last inequality gives

$$|T(\theta)| = |\det(M)| \le c_3 |Q(\eta)| (2^q)^{c_4}$$
$$\log |T(\theta)| \le \log c_3 + \log |Q(\eta)| + c_4 \log(2^q).$$

Having now obtained an upper bound for $\log |T(\theta)|$ recall that $2^q \le 2^q H(Q) = \Lambda(Q) \le u$ and apply (3.4) to obtain

$$O(u^c|\theta) \ge \log \left(\frac{1}{|T(\theta)|} \right) \ge \log \left(\frac{1}{|Q(\eta)|} \right) - \log c_3 - c_4 \log u.$$

Since Q was defined such that $\log \left(\frac{1}{|Q(\eta)|} \right) = O(u|\eta)$ it follows that

$$O(u^c|\theta) + c_4 \log u + \log c_3 \ge O(u|\eta).$$

By Proposition 3.3 there exists a positive constant c_5 depending on θ such that for all sufficiently large u, $O(u|\theta) \geq c_5 \log u$ and consequently there exists another positive constant c_6 depending only on θ and η such that

$$O(u|\eta) \leq O(u^c|\theta) + c_4 \log u + c_3 \leq c_6 O(u^c|\theta).$$

From the definition of the partial ordering it thus follows that $O(u|\theta) \gg O(u|\eta)$. □

Corollary 3.8. *If $\theta, \eta \in \mathbb{C}_p$ are algebraically dependent then $O(u|\theta) \asymp O(u|\eta)$.*

Proof. This follows directly from Theorem 3.6 by interchanging θ and η. □

Corollary 3.9. *If $\alpha \in \overline{\mathbb{Q}}$ then $O(u|\alpha) \asymp \log u$.*

Proof. By Corollary 3.8 it suffices to prove $O(u|1) \asymp \log u$. This is because $\mathbb{Q}(1) = \mathbb{Q}$ and hence 1 and α are algebraically dependent for any $\alpha \in \overline{\mathbb{Q}}$. From Lemma 3.3 $O(u|1) \gg \log u$ and thus it suffices to prove $O(u|1) \ll \log u$.

Fix $u \in \mathbb{N}$ and let n be such that $p^n \leq u < p^{n+1}$. Let $Q(x) = a_q x^q + \cdots + a_0 \in \mathbb{Z}[x]$ be a nonzero polynomial of degree q satisfying $\Lambda(Q) = 2^q H(Q) \leq u$. Then

$$|Q(1)|_\infty \leq |a_q|_\infty + \cdots + |a_0|_\infty \leq (q+1)H(Q) \leq \frac{q+1}{2^q} u < \frac{q+1}{2^q} p^{n+1} < p^{n+1}$$

and it follows that the largest power of p that can divide $Q(1)$ is p^n. Thus for all integer polynomials Q with $\Lambda(Q) \leq u$ and $Q(1) \neq 0$ we have $|Q(1)| \geq p^{-n}$. Moreover, the constant polynomial defined by $Q_n(x) = p^n$ satisfies $\Lambda(Q_n) \leq u$ and $|Q_n(1)| = p^{-n}$. Hence

$$O(u|1) = \log\left(\frac{1}{|p^n|}\right) = n \leq \log u.$$

and thus $O(u|1) << \log u$. □

With the exception of Corollary 3.5, which stated that there are transcendental $\theta \in \mathbb{C}_p$ for which $O(u|\theta) \asymp \log u$, all of our results in this chapter hold in the complex case. In particular, the results that every $\theta \in \mathbb{C}_p$ satisfies $O(u|\theta) \gg \log u$, algebraically dependent elements are equivalent under $\asymp$, and every $\alpha \in \overline{\mathbb{Q}}$ satisfies $O(u|\alpha) \asymp \log u$ were all proved in the complex case in the original paper on order functions by Mahler [22].

4 RESULTS ON O^*

Relatively little work has been done with O^*_M in the complex case. Most results are due to Durand [11]. Here we again use Mahler's order functions as motivation and define an analogue to the complex order function O^*_M on $\mathbb{C}_p$. If $\alpha \in \overline{\mathbb{Q}}$ recall that we defined the minimal polynomial of α over $\mathbb{Z}$ to be the minimal polynomial of α over $\mathbb{Q}$ multiplied by the least common multiple of the denominators of its coefficients. Also recall that if m is the minimal polynomial of α over $\mathbb{Z}$ then we defined $\Lambda(\alpha) = \Lambda(m)$.

Definition 4.1. *Let $\theta \in \mathbb{C}_p$. Define $O^*(*|\theta) : \mathbb{N} \setminus \{1\} \to \mathbb{R}$ by*

$$O^*(u|\theta) = \max_{\substack{\Lambda(\alpha)\leq u \\ \alpha\neq\theta}} \log \frac{1}{|\alpha - \theta|}$$

where $\alpha \in \overline{\mathbb{Q}}$.

As with O the maximum can be used in the definition because given any $u \in \mathbb{N}$ there are only finitely many $\alpha \in \overline{\mathbb{Q}}$ with minimal polynomial m over $\mathbb{Z}$ which satisfy $\Lambda(\alpha) = \Lambda(m) \leq u$. From Corollary 2.18, $\overline{\mathbb{Q}}$ is dense in $\mathbb{C}_p$ and hence $O^*(u|\theta)$ is a positive increasing function for sufficiently large u. Thus the partial order $\gg$ and equivalence relation $\asymp$ defined in Definition 3.2 can be used on the set of functions $\{O^*(u|\theta) : \theta \in \mathbb{C}_p\}$. Define the partial order $\gg^*$ on $\mathbb{C}_p$ by $\theta \gg^* \eta$ if $O^*(u|\theta) \gg O^*(u|\eta)$ and define the equivalence relation $\asymp^*$ on $\mathbb{C}_p$ by $\theta \asymp^* \eta$ if $O^*(u|\theta) \asymp O^*(u|\eta)$.

Since we will be considering extensions of both $\mathbb{Q}_p$ and $\mathbb{Q}$ in this chapter in order to avoid confusion when the field is not specified the term "degree" will always refer to the degree over $\mathbb{Q}$. The main result of Section 4.1 is that if $\alpha \in \overline{\mathbb{Q}}_p$ then $O^*(u|\alpha) \gg \log u$. In Section 4.2 we construct $\theta \in \mathbb{C}_p$ for which $O^*(u|\theta)$ grows slowly and in Theorem 4.6 we construct a lower bound for these θ under certain conditions. A particular case of this result will then allow us to construct $\theta \in \mathbb{C}_p$ which satisfy $O^*(u|\theta) \asymp \log^n u$, where $\log^n$ denotes the logarithm composed n times and $n \geq 3$.

4.1 A Lower Bound for O^* on Elements of $\overline{\mathbb{Q}}_p$

Given $\alpha \in \overline{\mathbb{Q}}_p$ Theorem 2.16 (Krasner's Lemma) will allow us to construct a sequence in $\overline{\mathbb{Q}}_p$ converging to α for which the terms in the sequence are roots of polynomials converging to the minimal polynomial of α. This idea will be used to bound O^* from below when considering elements of $\overline{\mathbb{Q}}_p$.

Theorem 4.2. *If $\alpha \in \overline{\mathbb{Q}}_p$ then $O^*(u|\alpha) \gg \log u$.*

Proof. Assume $\alpha \in \overline{\mathbb{Q}}_p$ and let $R(x) \in \mathbb{Q}_p[x]$ be the minimal polynomial of α over $\mathbb{Q}_p$. Recall that the minimal polynomial of α over $\mathbb{Z}_p = \{a \in \mathbb{Q}_p : |a| \leq 1\}$ is defined by multiplying R by the reciprocal of the least power of p appearing in the base p expansion of the coefficients of R. Let $Q(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}_p[x]$ be the minimal polynomial of α over $\mathbb{Z}_p$. Given $m \in \mathbb{N}$ let $0 \leq a_{i,m} \leq p^m - 1$ be the positive integers such that $a_{i,m} \equiv a_i \bmod p^m$. Define

$$Q_m(x) = (a_{n,m}x^n + \cdots + a_{0,m}) + p^m \in \mathbb{Z}[x].$$

Recall that for a polynomial $P(x) \in \mathbb{Q}_p[x]$ we defined $\|P\|$ to denote the maximum p-adic absolute value of the coefficients of P. By construction the sequence $\{Q_m\}$ converges to Q with respect to $\|*\|$ and $\partial(Q_m) \leq n$ for all $m \in \mathbb{N}$. Thus Corollary 2.17 implies there exist $M \in \mathbb{N}$ and a sequence $\{\beta_m\} \subset \overline{\mathbb{Q}}_p$ such that if $m \geq M$ then $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta_m)$, $Q_m(\beta_m) = 0$, and the inequality $|\alpha - \beta_m| \leq c_1\|Q - Q_m\|^{1/n}$ is satisfied for some positive constant c_1 depending on α. Since the Q_m are integer polynomials we have $\{\beta_m\} \subset \overline{\mathbb{Q}}$. It follows by the definition of the Q_m that

$$|\alpha - \beta_m| \leq c_1\|Q - Q_m\|^{1/n} \leq c_1|p^m|^{1/n} = c_1 p^{-m/n}. \tag{4.1}$$

Increase M as necessary such that taking the logarithm gives that for all $m \geq M$

$$\log \frac{1}{|\alpha - \beta_m|} \geq \frac{m}{n} - \log c_1 \geq c_2 m \tag{4.2}$$

where c_2 is another positive constant depending only on α.

Since $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta_m)$ for all $m \geq M$ the degree of the minimal polynomial of β_m over $\mathbb{Q}_p$ must be n. Moreover, the field $\mathbb{Q}$ is contained in $\mathbb{Q}_p$ and thus $n \leq \partial(\beta_m)$. Since β_m is a root of the integer polynomial Q_m and $\partial(Q_m) \leq n$ it follows that $\partial(\beta_m) = n$. Thus Q_m must be a rational integer multiple of the minimal polynomial of β_m over $\mathbb{Z}$ for all $m \geq M$. From the definition of Q_m the coefficients of Q_m are between 0 and $p^m - 1$ except for the constant coefficient which must be between p^m and $p^m - 1 + p^m = 2p^m - 1$. It follows that the height of Q_m is the standard absolute value of the constant coefficient and consequently

$$p^m \leq |a_{0,m} + p^m|_\infty = H(Q_m) < 2p^m.$$

Thus for all $m \geq M$

$$2^n p^m \leq \Lambda(Q_m) = 2^n H(Q_m) < 2^n(2p^m) = 2^{n+1}p^m. \tag{4.3}$$

In particular the sequence $\{\Lambda(Q_m)\}$ is strictly increasing because

$$\Lambda(Q_m) < 2^{n+1}p^m \leq 2^n p^{m+1} \leq \Lambda(Q_{m+1}).$$

Hence given $u \geq \Lambda(Q_M)$ there exists a unique $m \geq M$ such that $\Lambda(Q_m) \leq u < \Lambda(Q_{m+1})$. Take the logarithm and apply (4.3) to obtain

$$\log u < \log \Lambda(Q_{m+1}) < \log(2^{n+1}p^{m+1}) = (n+1)\log 2 + m + 1 \leq c_3 m$$

where c_3 is a positive constant depending only on α. Combining this with (4.2) implies there exists a positive constant c depending only on α which satisfies

$$\log \frac{1}{|\alpha - \beta_m|} > c \log u.$$

Since $m \geq M$ and Q_m is an integer multiple of the minimal polynomial of β_m over $\mathbb{Z}$ it follows that $\Lambda(\beta_m) \leq \Lambda(Q_m) \leq u$. Thus the definition of O^* gives that for all $u \geq \Lambda(Q_M)$,

$$O^*(u|\alpha) \geq \log \frac{1}{|\alpha - \beta_m|} > c \log u. \qquad \square$$

In the next chapter we will prove $O^*(u|\theta) \ll O(u|\theta)$ for all $\theta \in \mathbb{C}_p$. Corollary 3.9 states $O(u|\alpha) \asymp \log u$ for all $\alpha \in \overline{\mathbb{Q}}$ and thus Theorem 4.2 will imply $O^*(u|\alpha) \asymp \log u$ for all $\alpha \in \overline{\mathbb{Q}}$.

4.2 Elements of $\mathbb{C}_p$ for Which O^* Grows Slowly

Recall that the fields $\overline{\mathbb{Q}}_p$ and $\mathbb{C}_p$ are not locally compact. Consequently given any finite extension field K of $\mathbb{Q}_p$ there are always elements of $\overline{\mathbb{Q}}_p$ that cannot be approximated to arbitrary precision by elements of K. For example, if $\theta \in \overline{\mathbb{Q}}_p$ with $1 < |\theta| < p$ then for any nonzero $\gamma \in \mathbb{Q}_p$, $|\gamma - \theta| = \max\{|\theta|, |\gamma|\}$ because $v(\gamma) \in \mathbb{Z}$. Applying this idea will allow us to construct elements of $\mathbb{C}_p$ for which O^* grows slowly. We first prove the following two lemmas.

Lemma 4.3. *Let $n \in \mathbb{N}$ and define K_n to be the extension field of $\mathbb{Q}_p$ generated by adjoining the roots of all polynomials in $\mathbb{Q}_p[x]$ with degree less than or equal to n. If $q \in \mathbb{N}$ is any prime greater than n and $f \in \mathbb{Z}$ is not divisible by q then there does not exist $\alpha \in K_n$ satisfying $|\alpha| = p^{f/q}$.*

Proof. From Theorem 2.15 there are only finitely many extensions of $\mathbb{Q}_p$ of a given finite degree. By Theorem 2.10 there exist $\alpha_1, \ldots \alpha_m \in \overline{\mathbb{Q}}_p$ such that $\mathbb{Q}_p(\alpha_1), \ldots, \mathbb{Q}_p(\alpha_m)$ is every extension of $\mathbb{Q}_p$ of degree less than or equal to n. It follows that

$$K_n = \mathbb{Q}_p(\alpha_1, \ldots, \alpha_m).$$

For all $1 \leq i \leq m$ we have

$$[\mathbb{Q}_p(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i) : \mathbb{Q}_p(\alpha_1, \ldots, \alpha_{i-1})] \leq [\mathbb{Q}_p(\alpha_i) : \mathbb{Q}_p] \leq n \tag{4.4}$$

and hence

$$[K_n : \mathbb{Q}_p] = [\mathbb{Q}_p(\alpha_1, \ldots, \alpha_m) : \mathbb{Q}_p] = \prod_{i=1}^{m} [\mathbb{Q}_p(\alpha_1, \ldots, \alpha_i) : \mathbb{Q}_p(\alpha_1, \ldots, \alpha_{i-1})],$$

where we define the $i = 1$ term to be $[\mathbb{Q}_p(\alpha_1) : \mathbb{Q}_p]$. From (4.4) it follows that each of the terms in the product are less than or equal to n and therefore

$$[K_n : \mathbb{Q}_p] = \prod_{i=2}^{n} i^{b_i}$$

where each $b_i \geq 0$ is an integer. Since every element of K_n must have degree over $\mathbb{Q}_p$ dividing $[K_n : \mathbb{Q}_p]$ it follows that if $\alpha \in K_n$ then the degree of α over $\mathbb{Q}_p$ is of the form

$$d = \prod_{i=2}^{n} i^{d_i}$$

where each $d_i \geq 0$ is an integer. In particular, d is not divisible by any prime greater than n. From the definition of the p-adic absolute value on $\overline{\mathbb{Q}}_p$ it follows that

$$|\alpha| = (p^a)^{1/d} = p^{a/d}$$

for some $a \in \mathbb{Z}$. Thus $|\alpha|$ cannot be of the form $p^{f/q}$ where $q \in \mathbb{N}$ is a prime greater than n and $f \in \mathbb{Z}$ is not divisible by q. □

Lemma 4.4. *If $f, q \in \mathbb{N}$ with q prime and f not a multiple of q then the minimal polynomial of $p^{f/q}$ over $\mathbb{Q}$ is $x^q - p^f$.*

Proof. Since f and q are relatively prime there exist $a, b \in \mathbb{Z}$ such that $af + bq = 1$. In particular, $\frac{af}{q} + b = \frac{1}{q}$. Thus

$$p^{1/q} = (p^{f/q})^a p^b \in \mathbb{Q}(p^{f/q})$$

and hence $\mathbb{Q}(p^{1/q}) \subseteq \mathbb{Q}(p^{f/q})$. Since $(p^{1/q})^f = p^{f/q}$ it follows that $\mathbb{Q}(p^{1/q}) = \mathbb{Q}(p^{f/q})$ and thus $\partial(p^{1/q}) = \partial(p^{f/q})$. The polynomial $x^q - p$ has $p^{1/q}$ as a root and $x^q - p$ satisfies Theorem 2.8 (Eisenstein's Criterion). Thus $x^q - p$ is irreducible and must be the minimal polynomial of $p^{1/q}$ over $\mathbb{Q}$. It follows that $\partial(p^{1/q}) = \partial(p^{f/q}) = q$ and hence the minimal polynomial of $p^{f/q}$ over $\mathbb{Q}$ is $x^q - p^f$. □

Let $M_0 \in \mathbb{R}^+$. Suppose $g : [M_0, \infty) \to \mathbb{R}^+$ is an unbounded increasing function for which there exist positive integers s, m, and $M \geq M_0$ such that

$$g(sk + s) - g(sk) \geq \frac{3}{m^k} \tag{4.5}$$

for all positive integers $k \geq M$. Without loss of generality assume $m \geq 3$. Theorem 2.11 (Bertrand's Postulate) states that for all $k \geq 1$ there exists a prime number q_k which satisfies

$$m^k < q_k < 2m^k < m^{k+1}. \tag{4.6}$$

Since $g(sk+s) - g(sk) \geq \frac{3}{m^k} > \frac{3}{q_k}$ there exist three consecutive positive integers f_k, f_k+1, and f_k+2 which satisfy

$$g(sk) \leq \frac{f_k}{q_k} < \frac{f_k+1}{q_k} < \frac{f_k+2}{q_k} \leq g(sk+s). \tag{4.7}$$

Let A_k be the intersection of $\{f_k, f_k+1, f_k+2\}$ with the set of integers relatively prime to q_k and note that A_k must contain at least two elements since q_k is a prime greater than or equal to 5. Now let B be an infinite binary sequence and define f_k^* as follows. If the kth term of B is 0 let f_k^* be the smallest element of A_k and otherwise define f_k^* to be the largest element of A_k. Let $h_k = \frac{f_k^*}{q_k}$ and define

$$\theta_{g,B} = \sum_{k=M}^{\infty} p^{h_k} \tag{4.8}$$

where M is given in the definition of g. Since $h_k \geq g(sk)$ the sum defining $\theta_{g,B}$ converges with respect to the p-adic absolute value because $g(sk)$ is increasing and unbounded.

The conditions on g are very general since a function which satisfies equality in (4.5) for all k must be a geometric series and thus bounded. In fact we will prove later that for any finite number of compositions of logarithms the function $\log\log\cdots\log(x)$ satisfies the conditions for g. Our first main result in this section is $O^*(u|\theta_{g,B}) \ll g(c\log\log u)$ for some constant c depending only on g. Define

$$\theta_l = \sum_{k=M}^{l} p^{h_k} \tag{4.9}$$

where $l \geq M$ and M is from the definition of g. We are now prepared to prove our first result on $\theta_{g,B}$.

Theorem 4.5. *Let g be an unbounded positive increasing function satisfying (4.5) and let B be an infinite binary sequence. If $\theta_{g,B} \in \mathbb{C}_p$ is defined as in (4.8) then there exists a constant c depending only on g such that $O^*(u|\theta_{g,B}) \ll g(c\log\log u)$.*

Proof. Let g be a function as in the statement of the theorem and let B be an infinite binary sequence. To simplify notation we fix g and B and write $\theta = \theta_{g,B}$. Recall that

$$\theta = \theta_{g,B} = \sum_{k=M}^{\infty} p^{h_k}$$

where M is from the definition of g and $h_k = \frac{f_k^*}{q_k}$, with f_k^* depending on B. Also recall that the integers f_k^* were defined such that $\frac{f_k^*}{q_k}$ is in lowest terms and $g(sk) \leq \frac{f_k^*}{q_k} \leq g(sk+s)$. Let $u \in \mathbb{N}$, $u \geq 2$ and let $\gamma \in \overline{\mathbb{Q}}$ be such that $O^*(u|\theta) = \log \frac{1}{|\theta-\gamma|}$ and $\Lambda(\gamma) \leq u$. Now let n be the unique positive integer satisfying

$$2^{m^{n-1}} \leq \Lambda(\gamma) < 2^{m^n}, \tag{4.10}$$

where m is from the definition of g in (4.5). Since $\Lambda(\gamma)$ increases as u increases fix $u \in \mathbb{N}$ sufficiently large so that $n > M$. From (4.10) and the definition of Λ it follows that the degree of the minimal polynomial of γ over $\mathbb{Z}$ is at most $m^n - 1$. Define K_{m^n} again to be the field obtained by adjoining the roots of all polynomials of degree less than or equal to m^n over $\mathbb{Q}_p$. Recall from Lemma 4.3 that it is impossible for an element of K_{m^n} to have p-adic absolute value $p^{-h_n} = p^{-f_n^*/q_n}$ because q_n is prime and $q_n > m^n$ by (4.6). We now use this to prove $|\theta - \gamma| \geq p^{-h_n}$ by way of contradiction. Assume $|\theta - \gamma| < p^{-h_n}$ and recall that for every $l \geq M$ we defined θ_l by

$$\theta_l = \sum_{k=M}^{l} p^{h_k}$$

where M is from the definition of g. From Lemma 4.4 and (4.6) it follows that if $k < n$ then $\partial(p^{h_k}) = q_k < 2m^k < m^n$. Since the degree of p^{h_k} over $\mathbb{Q}_p$ must be less than or equal to $\partial(p^{h_k})$ we have $p^{h_k} \in K_{m^n}$ for $M \leq k \leq n-1$. In particular this implies $\theta_{n-1} \in K_{m^n}$. Since the degree of γ over $\mathbb{Q}_p$ is less than or equal to $\partial(\gamma) < m^n$ it also follows that $\gamma \in K_{m^n}$ and hence $\gamma - \theta_{n-1} \in K_{m^n}$. Moreover, note that from the definition of θ_l we have $|\theta - \theta_{n-1}| = p^{-h_n} > |\theta - \gamma|$ and it follows that

$$|\gamma - \theta_{n-1}| = \max\{|\gamma - \theta|, |\theta - \theta_{n-1}|\} = |\theta - \theta_{n-1}| = p^{-h_n} = p^{-f_n^*/q_n}.$$

This is a contradiction to Lemma 4.3 because $\gamma - \theta_{n-1} \in K_{m^n}$ and $q_n > m^n$ is prime.

Since we just proved $|\theta-\gamma| \geq p^{-h_n}$ it follows that $p^{h_n} \geq \frac{1}{|\gamma-\theta|}$. Recall γ was defined such that $\log \frac{1}{|\gamma-\theta|} = O^*(u|\theta)$. It thus follows that

$$O^*(u|\theta) \leq h_n. \tag{4.11}$$

Our goal is to prove h_n is bounded above by $g(c \log\log u)$ for some constant c depending only on θ. Take the logarithm of the left side of (4.10) twice to obtain

$$(n-1)\log m + \log\log 2 \leq \log\log \Lambda(\gamma) \leq \log\log u \tag{4.12}$$

since $\Lambda(\gamma) \leq u$. Recall s from the definition of g in (4.5). Since s and m are constants depending only on g and g is independent of B, by (4.12) there exists a positive constant c depending only on g such that

$$sn + s \leq c \log\log u.$$

Since g is increasing, (4.7) and (4.11) thus imply

$$O^*(u|\theta) \leq h_n = \frac{f_n^*}{q_n} \leq g(sn+s) \leq g(c\log\log u). \tag{4.13}$$

Recall that $\theta = \theta_{g,B}$ where B is an infinite binary sequence. Since (4.13) is independent of the choice of B it follows that $O^*(u|\theta) \ll g(c\log\log u)$ for uncountably many $\theta \in \mathbb{C}_p$. $\square$

In the next result we obtain a lower bound for $O^*(u|\theta_{g,B})$ when $g(x) \leq p^{cx^2}$ for some positive constant c depending only on g.

Theorem 4.6. *Suppose g satisfies (4.5) and assume there exists a positive constant c depending only on g such that $g(x) \leq p^{cx^2}$ for all sufficiently large $x \in \mathbb{R}^+$. If $\theta = \theta_{g,B} \in \mathbb{C}_p$ is defined as in (4.8) then there exists a positive constant c' depending only on g such that*

$$O^*(u|\theta) \gg g\left(c'(\log\log u)^{1/2}\right).$$

Proof. Let $g(x)$ be defined as in (4.5) and assume there exists positive constants c and x_0 depending only on g such that $g(x) \leq p^{cx^2}$ for all $x \geq x_0$. Recall that we defined

$$\theta = \sum_{k=M}^{\infty} p^{h_k}$$

and

$$\theta_l = \sum_{k=M}^{l} p^{h_k}$$

where $h_k = \frac{f_k^*}{q_k}$ is such that

$$g(sk) \leq h_k = \frac{f_k^*}{q_k} \leq g(sk+s). \tag{4.14}$$

Moreover, q_k satisfies $m^k < q_k < 2m^k < m^{k+1}$ where m is also defined in (4.5).

To simplify notation define $a_n = 2^n m^{n(n+1)/2}$ for $n \in \mathbb{N}$. Let $u \in \mathbb{N}$ be sufficiently large such that there exists a unique $n \in \mathbb{N}$, $n \geq \max\{M, \frac{x_0}{s} - 2\}$ satisfying

$$2^{a_n} \left((1+2m^n)p^{2m^n g(sn+s)}\right)^{na_n} \leq u \tag{4.15}$$

and

$$u < 2^{a_{n+1}} \left((1+2m^{n+1})p^{2m^{n+1} g(sn+2s)}\right)^{(n+1)a_{n+1}}. \tag{4.16}$$

Recall from Lemma 4.4 that $\partial(p^{h_k}) = q_k$. Since $\theta_n \in \mathbb{Q}(p^{h_M}, p^{h_{M+1}} \ldots, p^{h_n})$ it follows that $\partial(\theta_n) \leq q_M q_{M+1} \ldots q_n$ and hence

$$\partial(\theta_n) \leq \prod_{k=M}^{n} q_k < \prod_{k=1}^{n} 2m^k = 2^n m^{(n+1)n/2} = a_n. \tag{4.17}$$

In order to bound the height of θ_n apply Proposition 2.7 to obtain

$$H(\theta_n) \leq \left(\prod_{k=M}^{n} (1+\partial(p^{h_k}))H(p^{h_k})\right)^{\partial(\theta_n)}. \tag{4.18}$$

By Lemma 4.4 the minimal polynomial of $p^{h_k} = p^{f_k^*/q_k}$ over $\mathbb{Q}$ is $x^{q_k} - p^{f_k^*}$. Hence $H(p^{h_k}) = p^{f_k^*}$. Multiplying by q_k in (4.14) implies $f_k^* \leq q_k g(sk+s)$ and thus

$$H(p^{h_k}) = p^{f_k^*} \leq p^{q_k g(sk+s)}.$$

The inequality (4.18) then becomes

$$H(\theta_n) < \left(\prod_{k=M}^{n} (1+q_k)p^{q_k g(sk+s)}\right)^{a_n} \leq \left((1+q_n)p^{q_n g(sn+s)}\right)^{na_n}$$

because $\partial(p^{h_k}) = q_k$ and $\partial(\theta_n) \leq a_n$ by (4.17). Now that the height is bounded it is possible to bound $\Lambda(\theta_n)$

$$\Lambda(\theta_n) = 2^{\partial(\theta_n)} H(\theta_n) < 2^{a_n} \left((1+q_n)p^{q_n g(sn+s)}\right)^{na_n}. \tag{4.19}$$

Recall from (4.5) that we defined the q_n to be such that $q_n < 2m^n$. Thus (4.19) and (4.15) imply

$$\Lambda(\theta_n) < 2^{a_n} \left((1+2m^n)p^{2m^n g(sn+s)}\right)^{na_n} \leq u. \tag{4.20}$$

Hence $O^*(u|\theta) = \max_{\Lambda(\alpha)\leq u} \log \frac{1}{|\theta-\alpha|} \geq \log \frac{1}{|\theta-\theta_n|}$. From the definitions of θ and θ_n it follows that

$$|\theta - \theta_n| = \left|\sum_{k=1}^{\infty} p^{h_k} - \sum_{k=1}^{n} p^{h_k}\right| = \left|\sum_{k=n+1}^{\infty} p^{h_k}\right| = p^{-h_{n+1}}$$

and thus by (4.14) and (4.20)

$$O^*(u|\theta) \geq \log \frac{1}{|\theta-\theta_n|} = \log p^{h_{n+1}} = h_{n+1} \geq g(sn+s) > g(sn). \tag{4.21}$$

Now take the logarithm of (4.16) to obtain

$$\log u < a_{n+1} \log 2 + (n+1)a_{n+1}\left(\log(1+2m^{n+1}) + 2m^{n+1} g(sn+2s)\right). \tag{4.22}$$

Recall that we defined $a_{n+1} = 2^{n+1}m^{(n+1)(n+2)/2}$ and note that $\frac{1}{2}(n^2+3n+2) \leq 3n^2$ for all $n \in \mathbb{N}$. Thus (4.22) becomes

$$\log u < 2^{n+1}m^{3n^2} \log 2 + (n+1)2^{n+1}m^{3n^2}\left(\log(1+2m^{n+1}) + 2m^{n+1} g(sn+2s)\right)$$

Also recall that $g(x) \leq p^{cx^2}$ for all $x \geq x_0$, where c is a constant depending only on g. Since we assumed $n \geq \frac{x_0}{s} - 2$ it follows that $sn + 2s \geq x_0$. Thus $g(sn+2s) \leq p^{c(sn+2s)^2}$ and hence

$$\begin{aligned}\log u &< 2^{n+1}m^{3n^2} \log 2 + (n+1)2^{n+1}m^{3n^2}\left(\log(1+2m^{n+1}) + 2m^{n+1}p^{c(sn+2s)^2}\right) \\ &\leq c_1 n 2^{n+2} m^{3n^2+n+1} p^{c(sn+2s)^2}\end{aligned}$$

where c_1 is some positive constant independent of n. Taking the logarithm again gives

$$\log\log u < \log c_1 + \log n + (n+2)\log 2 + (3n^2+n+1)\log m + c(sn+2s)^2 < c_2 n^2 \tag{4.23}$$

where c_2 is a positive constant independent of n. It follows that $n > (\frac{1}{c_2}\log\log u)^{1/2}$. Recall that (4.15) gave a lower bound for u in terms of n and allowed us to obtain (4.21). Since g is strictly increasing applying (4.21) to (4.23) implies

$$O^*(u|\theta) \geq g(sn) > g\left(\frac{s}{\sqrt{c_2}}(\log\log u)^{1/2}\right)$$

and the result follows. □

Now that we have an upper bound and lower bound on $O^*(u|\theta_{g,B})$ when $g(x) \leq p^{cx^2}$ for a positive constant c it is possible to obtain equality is some cases.

Corollary 4.7. *For $n \in \mathbb{N}$ let $\log^n(x)$ denote the function $\log\log\cdots\log(x)$ where the logarithm is composed n times. If $n \geq 3$ then there exist uncountably many $\theta \in \mathbb{C}_p$ which satisfy $O^*(u|\theta) \asymp \log^n(u)$.*

Proof. Fix $n \in \mathbb{N}$. Our goal is to prove that $\log^n$ satisfies the conditions on g in Theorem 4.5 and Theorem 4.6. The function $\log^n(x)$ is positive for sufficiently large x, increasing, and unbounded. In order to prove $\log^n$ satisfies (4.5) first note that induction on n implies

$$\int_k^{k+1} \frac{dx}{x(\log x)(\log^2 x)\dots(\log^{n-1} x)} = \log^n(k+1) - \log^n k.$$

Moreover, for k sufficiently large

$$\begin{aligned}\int_k^{k+1} \frac{dx}{x(\log x)(\log^2 x)\dots(\log^{n-1} x)} &\geq \left((k+1)(\log(k+1))\dots(\log^{n-1}(k+1))\right)^{-1} \\ &\geq \frac{1}{(k+1)^n} \\ &\geq \frac{3}{3^k}.\end{aligned}$$

Hence (4.5) is satisfied for all $n \in \mathbb{N}$ with $s = 1$. Since $\log^n(x)$ is bounded above by p^{x^2} the function $g(x) = \log^n(x)$ satisfies the conditions for Theorem 4.5 and Theorem 4.6. Thus for all $n \in \mathbb{N}$ there exist uncountably many $\theta \in C_p$ and positive constants c and c' depending only on on n such that for all sufficiently large u

$$O^*(u|\theta) > \log^n\left(c'(\log\log u)^{1/2}\right) = \log^{n-1}\left(\log c' + \frac{1}{2}\log\log\log u\right) > c_1\log^{n+2} u$$

and

$$O^*(u|\theta) \leq \log^n(c\log(\log u)) \leq c_2 \log^{n+2} u,$$

where c_1 and c_2 are constants independent of u. It thus follows that for a fixed $n \in \mathbb{N}$ there exist uncountably many $\theta \in \mathbb{C}_p$ satisfying $O^*(u|\theta) \asymp \log^{n+2} u$. $\square$

Although not much work has been done with O^*_M in the complex case the properties of $\mathbb{C}_p$ allowed us to prove several results on O^*. In this chapter we proved that if $\alpha \in \overline{\mathbb{Q}}_p$ then $O^*(u|\alpha) \gg \log u$. In Theorem 4.5 we constructed elements of $\mathbb{C}_p$ for which O^* grows slowly and in Theorem 4.6 we gave a lower bound for these elements provided the function $g(x)$ is bounded by p^{cx^2} for some positive constant c. Finally, in Corollary 4.7 we used these results to construct $\theta \in \mathbb{C}_p$ which satisfy $O^*(u|\theta) \asymp \log^n u$ for all integers $n \geq 3$.

5 TRANSCENDENCE TYPE

In the complex case the main tool Durand [11] used to prove his results on O_M and O_M^* was transcendence type. Our definition of p-adic transcendence type is as follows.

Definition 5.1. *For $\theta \in \mathbb{C}_p$ the* transcendence type *of θ is defined by $\tau(\theta) = \sup T(\theta)$ where*

$$T(\theta) = \left\{ \tau \geq 0 : \limsup_{u \to \infty} \frac{O(u|\theta)}{(\log u)^\tau} = \infty \right\}.$$

Because of the $\limsup$ in the definition the set $T(\theta)$ considers $u \in \mathbb{N}$ for which $O(u|\theta)$ is large. Thus the function $\tau(\theta)$ provides us with a method of measuring the rate of the best polynomial approximations of θ relative to a power of $\log u$. It is also possible to construct an analogue of transcendence type corresponding to the function O^*. Define $\tau^*(\theta) = \sup T^*(\theta)$ where

$$T^*(\theta) = \left\{ \tau \geq 0 : \limsup_{u \to \infty} \frac{O^*(u|\theta)}{(\log u)^\tau} = \infty \right\}.$$

In Section 5.1 we will demonstrate that if $\tau^*(\theta) \geq 2$ or $\tau(\theta) > 2$ then $\tau^*(\theta) = \tau(\theta)$. In doing this we will also prove that for all $\theta \in \mathbb{C}_p$, $O^*(u|\theta) \ll O(u|\theta)$. Given any real number $\tau \geq (3 + \sqrt{5})/2$ in Section 5.2 we construct $\theta \in \mathbb{Q}_p$ that satisfy $\tau(\theta) = \tau^*(\theta) = \tau$, which will then imply there are uncountably many equivalence classes in $\mathbb{C}_p$ under the equivalence relations $\asymp$ and $\asymp^*$.

Before proceeding we first give an equivalent definition of the set $T(\theta)$ in the next lemma, which will be used later to prove Theorem 5.11.

Lemma 5.2. *Let $\theta \in \mathbb{C}_p$ and let $T'(\theta)$ be the set of all $\tau \geq 0$ for which there exists a sequence of polynomials $\{P_n\} \subset \mathbb{Z}[x]$ such that $P_n(\theta) \neq 0$, $\Lambda(P_{n+1}) > \Lambda(P_n)$, and*

$$\log\left(\frac{1}{|P_n(\theta)|}\right) \geq n(\log \Lambda(P_n))^\tau$$

for all $n \in \mathbb{N}$. Then $T(\theta) = T'(\theta)$, and hence $\tau(\theta) = \sup T'(\theta)$.

Proof. Suppose $\tau \in T(\theta)$. Then there is an increasing sequence of integers $\{u_n\}$ such that

$$\lim_{n\to\infty} \frac{O(u_n|\theta)}{(\log u_n)^\tau} = \infty.$$

Deleting elements as necessary allows us to assume that for all $n \in \mathbb{N}$,

$$\frac{O(u_n|\theta)}{(\log u_n)^\tau} \geq n.$$

For each n define $P_n(x) \in \mathbb{Z}[x]$ to be a polynomial satisfying $\log\left(\frac{1}{|P_n(\theta)|}\right) = O(u_n|\theta)$ and $\Lambda(P_n) \leq u_n$. If necessary redefine the u_n such that $\Lambda(P_n) = u_n$ for each n. It follows that

$$\log\left(\frac{1}{|P_n(\theta)|}\right) = O(\Lambda(P_n)|\theta) \geq n(\log \Lambda(P_n))^\tau$$

and $\tau \in T'(\theta)$.

Now assume $\tau \in T'(\theta)$ and let $u_n = \Lambda(P_n)$ where $\{P_n\}$ is the sequence of polynomials from the definition of $T'(\theta)$. By the definitions of O and $T'(\theta)$ it follows that

$$\frac{O(u_n|\theta)}{(\log u_n)^\tau} \geq \frac{\log\left(\frac{1}{|P_n(\theta)|}\right)}{(\log \Lambda(P_n))^\tau} \geq n.$$

Since this is true for every $n \in \mathbb{N}$,

$$\limsup_{u\to\infty} \frac{O(u|\theta)}{(\log u)^\tau} \geq \lim_{n\to\infty} \frac{O(u_n|\theta)}{(\log u_n)^\tau} = \infty$$

and $\tau \in T(\theta)$. □

5.1 Comparing τ and τ^*

Our goal for this section will be to prove Theorem 5.9, which states that if $\tau^*(\theta) \geq 2$ then $\tau(\theta) = \tau^*(\theta)$. This was first done in the complex case by Durand [11] using results proved by Fel'dman [13]. If F is a field, a polynomial with coefficients in F is *separable* if it has no repeated roots in the algebraic closure of F. Given $\theta \in \mathbb{C}_p$ and a polynomial $P(x) \in \mathbb{Z}[x]$ in Proposition 5.4 we obtain an upper bound for $|P(\theta)|$ in terms of the roots

of P, and in Proposition 5.7 we obtain a corresponding lower bound when P is separable. These bounds are due to Fel'dman in the complex case. We then take the lim sup of these bounds to obtain the desired result. Although our bounds are different from those obtained by Fel'dman, our proof in the p-adic case will follow the same outline as Durand and Fel'dman in the complex case. The following lemma provides us with an upper bound on the product of roots of P.

Lemma 5.3. *Let $P(x) \in \mathbb{Z}[x]$ be a polynomial of degree n. Let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ be the roots of P, including repetitions due to multiplicity. Then for any set $\{i_1, i_2, \ldots, i_k\}$ contained in $\{1, 2, \ldots, n\}$ we have $|\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k}| \leq H(P)$.*

Proof. Suppose $P(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ and let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ be the roots of P, including repetitions due to multiplicity. If the roots of P all have p-adic absolute value less than 1 then the result follows. Without loss of generality we can order the roots of P such that $|\alpha_i| \leq |\alpha_j|$ if $i \leq j$. If $|\alpha_1| < 1$ define m such that $|\alpha_m| < 1 \leq |\alpha_{m+1}|$ and if $|\alpha_1| \geq 1$ let $m = 0$. By Proposition 2.14 there exists $x_0 \in \mathbb{C}_p$ with $|x_0| = 1$ such that

$$\sup_{|x|=1} |P(x)| = |P(x_0)| = |a_n x_0^n + \cdots + a_0| \leq \max_{0 \leq i \leq n} \{|a_i x_0^i|\} \leq 1. \tag{5.1}$$

Let

$$Q(x) = \prod_{i=m+1}^{n} (x - \alpha_i)$$

and note $Q(0) = \pm\alpha_{m+1}\alpha_{m+2}\ldots\alpha_n$. Moreover, applying the p-adic maximum modulus theorem (Proposition 2.14) again gives there exists $x_1 \in \mathbb{C}_p$ satisfying $|x_1| = 1$ and

$$|Q(0)| \leq \sup_{|x|\leq 1} |Q(x)| = \sup_{|x|=1} |Q(x)| = |Q(x_1)| = \frac{1}{|a_n|}|P(x_1)| \prod_{i=1}^{m} |x_1 - \alpha_i|^{-1} \tag{5.2}$$

where if $m = 0$ the empty product is assumed to equal 1. The inequality (5.1) implies $|P(x_1)| \leq 1$. If $i \leq m$ then $|\alpha_i| < 1$ and from part (ii) of Proposition 2.13 it follows that $|x_1 - \alpha_i| = |x_1| = 1$. Thus (5.2) becomes $|Q(0)| \leq \frac{1}{|a_n|}$. Part (i) of Proposition 2.13 implies $\frac{1}{|a_n|} \leq |a_n|_\infty \leq H(P)$ and since the largest product of roots of P is

$$|\alpha_{m+1}\alpha_{m+2}\ldots\alpha_n| = |Q(0)|$$

the result follows. □

Proposition 5.4. *Let $P(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ be a polynomial of degree n with roots $\alpha_1, \ldots, \alpha_n$. Then for any $\theta \in \mathbb{C}_p$*

$$|P(\theta)| \leq \min_{1 \leq i \leq n} |\theta - \alpha_i| \max\{1, |\theta|^{n-1}\} H(P).$$

Proof. The result is trivial if $P(\theta) = 0$. Thus we assume $P(\theta) \neq 0$. First note that $|P(\theta)| = |a_n| \prod_{i=1}^{n} |\theta - \alpha_i|$ and let

$$Q(x) = \left(a_n \min_{1 \leq i \leq n} |\theta - \alpha_i| \right)^{-1} P(x). \tag{5.3}$$

Then $Q(\theta) = \beta_{n-1}\theta^{n-1} + \cdots + \beta_0 \in \mathbb{C}_p$ where each β_i is a sum of products of the form $\alpha_{1,i}\alpha_{2,i} \ldots \alpha_{n-i,i}$ where the subscripts are distinct. The p-adic triangle inequality and Lemma 5.3 thus imply $|\beta_i| \leq H(P)$ for $0 \leq i \leq n-1$. Apply this to equation (5.3) to obtain

$$\begin{aligned} |Q(\theta)| &= |\beta_{n-1}\theta^{n-1} + \cdots + \beta_0| \\ &\leq \max\{|\beta_{n-1}|, \ldots, |\beta_0|\} \max\{|\theta|^{n-1}, 1\} \\ &\leq H(P) \max\{|\theta|^{n-1}, 1\}. \end{aligned}$$

Hence

$$|P(\theta)| = |a_n| \min_{1 \leq i \leq n} |\theta - \alpha_i| \, |Q(\theta)| \leq \min_{1 \leq i \leq n} |\theta - \alpha_i| \, H(P) \, \max\{1, |\theta|^{n-1}\}. \qquad \square$$

Corollary 5.5. *Let $\theta \in \mathbb{C}_p$. Then $O^*(u|\theta) \ll O(u|\theta)$.*

Proof. Given $u \in \mathbb{N}$ and $\theta \in \mathbb{C}_p$ let α be such that $O^*(u|\theta) = \log \frac{1}{|\theta - \alpha|}$ and $\Lambda(\alpha) \leq u$. Let $P(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α over $\mathbb{Z}$ and let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ be the roots of P. By Proposition 5.4

$$\begin{aligned} O^*(u|\theta) &= \log \frac{1}{\min_{1 \leq i \leq n} |\theta - \alpha_i|} \\ &\leq \log \frac{1}{|P(\theta)|} + \log H(P) + \log(\max\{|\theta|^{n-1}, 1\}) \\ &\leq O(u|\theta) + \log \Lambda(P) + \max\{0, (n-1)\log|\theta|\}. \end{aligned}$$

Note that $\log \Lambda(\alpha) = \log \Lambda(P) = n \log 2 + \log H(P) \leq \log u$ and $n \leq \frac{1}{\log 2} \log u$. Thus since Theorem 3.3 gives $\log u \ll O(u|\theta)$ there exists a positive constant c depending only on θ which satisfies $O^*(u|\theta) \leq c\, O(u|\theta)$. □

Corollary 5.6. *If $\alpha \in \overline{\mathbb{Q}}$ then $O^*(u|\alpha) \asymp \log u$.*

Proof. Suppose $\alpha \in \overline{\mathbb{Q}}$. Corollary 3.9 implies $O(u|\alpha) \asymp \log u$ and Theorem 4.2 gives $O^*(u|\alpha) \gg \log u$. Apply Corollary 5.5 to obtain $\log u \ll O^*(u|\alpha) \ll O(u|\alpha) \asymp \log u$. □

Proposition 5.4 gives an upper bound on the size of $|P(\theta)|$. Obtaining a lower bound on $|P(\theta)|$ in the next proposition will allow us to relate τ and τ^*.

Proposition 5.7. *Let $P(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ be a separable polynomial of degree n with height H and distinct roots $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$. Then for all $\theta \in \mathbb{C}_p$,*

$$|P(\theta)| \geq \min_{1 \leq i \leq n} |\theta - \alpha_i| |a_n|^{-n+2} H^{-2n} n^{-n/2} ((2n-1)!)^{-1/2}.$$

Proof. Let P be as given. Without loss of generality let α_1 be such that $|\theta - \alpha_1| \leq |\theta - \alpha_i|$ for $2 \leq i \leq n$. Relabel the other α_i such that $|\alpha_i - \alpha_1| \leq |\alpha_j - \alpha_1|$ for all $2 \leq i \leq j$ and to simplify notation define $\delta = |\theta - \alpha_1|$. The theorem follows directly when $n = 1$ because then $|P(\theta)| = |a_1\theta + a_0| = |a_1|\delta$. We thus assume $n \geq 2$.

Let m be such that $|\alpha_i - \alpha_1| \leq \delta$ for $1 \leq i \leq m$ and $|\alpha_i - \alpha_1| > \delta$ for $m+1 \leq i \leq n$. Then

$$|P(\theta)| = |a_n| \prod_{i=1}^{n} |\theta - \alpha_i| \geq |a_n| \delta^m \prod_{i=m+1}^{n} |(\theta - \alpha_1) - (\alpha_i - \alpha_1)|. \tag{5.4}$$

Since $|\alpha_i - \alpha_1| > |\theta - \alpha_1| = \delta$ for all $m+1 \leq i \leq n$ part (ii) of Proposition 2.13 implies

$$|(\theta - \alpha_1) - (\alpha_i - \alpha_1)| = \max\{|\alpha_i - \alpha_1|, |\theta - \alpha_1|\} = |\alpha_i - \alpha_1|.$$

Thus (5.4) becomes

$$\begin{aligned}|P(\theta)| &\geq |a_n|\delta\delta^{m-1}\prod_{i=m+1}^{n}|\alpha_i-\alpha_1| \\ &= |a_n|\delta\left(\prod_{i=2}^{m}\delta\right)\left(\prod_{i=m+1}^{n}|\alpha_i-\alpha_1|\right) \\ &\geq |a_n|\delta\left(\prod_{i=2}^{m}|\alpha_i-\alpha_1|\right)\left(\prod_{i=m+1}^{n}|\alpha_i-\alpha_1|\right).\end{aligned}$$

Defining $D=\prod_{j=2}^{n}|\alpha_1-\alpha_j|$ then gives

$$|P(\theta)| \geq |a_n|\delta D. \tag{5.5}$$

In order to estimate the right hand side of (5.5) in terms of n and H first recall from (2.1) that the discriminant of P is equal to

$$\Delta = \operatorname{disc}(P) = a_n^{2n-2}\prod_{j=2}^{n}\prod_{k=1}^{j-1}(\alpha_k-\alpha_j)^2.$$

Since P has distinct roots, Δ is a nonzero integer. Let $\Gamma=(2n-1)!H^{2n-1}n^n$ and applying Proposition 2.3 gives $|\Delta|_\infty \leq \Gamma$. Combining this with part (i) of Proposition 2.13 then implies that $\frac{1}{\Gamma}\leq\frac{1}{|\Delta|_\infty}\leq|\Delta|$ and consequently

$$\frac{1}{\Gamma}\leq|\Delta|=|a_n|^{2n-2}\prod_{j=2}^{n}\prod_{k=1}^{j-1}|\alpha_k-\alpha_j|^2=|a_n|^{2n-2}D^2\prod_{j=3}^{n}\prod_{k=2}^{j-1}|\alpha_k-\alpha_j|^2.$$

Thus we obtain the following upper bound for $\frac{1}{D^2}$

$$\frac{1}{D^2}\leq\Gamma|a_n|^{2n-2}\prod_{j=3}^{n}\prod_{k=2}^{j-1}|\alpha_k-\alpha_j|^2. \tag{5.6}$$

Keeping α_1 fixed relabel the other α_i such that $|\alpha_2|\leq\cdots\leq|\alpha_n|$. Note (5.6) is still satisfied with the relabeled α_i. Moreover, $|\alpha_j-\alpha_i|\leq|\alpha_i|$ for all $2\leq j\leq i$ and applying this to (5.6) implies

$$\frac{1}{D^2}\leq\Gamma|a_n|^{2n-2}\prod_{j=3}^{n}\prod_{k=2}^{j-1}|\alpha_k-\alpha_j|^2\leq\Gamma|a_n|^{2n-2}\prod_{j=3}^{n}|\alpha_j|^{2n}.$$

By Lemma 5.3 the p-adic absolute value of the product of distinct roots must be less than the height. Thus

$$\frac{1}{D^2} \leq \Gamma |a_n|^{2n-2} H^{2n}$$

and hence

$$D \geq \left(|a_n|^{2n-2} H^{2n} \Gamma\right)^{-1/2} = |a_n|^{-n+1} H^{-n} \Gamma^{-1/2}.$$

Finally use this in (5.5) and apply the definition of Γ to obtain

$$\begin{aligned} |P(\theta)| &\geq \delta |a_n|^{-n+2} H^{-n} \Gamma^{-1/2} \\ &\geq \delta |a_n|^{-n+2} H^{-n} ((2n-1)! H^{2n-1} n^n)^{-1/2} \\ &\geq \min_{1 \leq i \leq n} |\theta - \alpha_i| |a_n|^{-n+2} H^{-2n} n^{-n/2} \left((2n-1)!\right)^{-1/2}. \end{aligned}$$

□

One more lemma is still required before using Propositions 5.4 and 5.7 to prove Theorem 5.9. In the complex case this result can be found in Chapter 6 of Lang [18]. The proof of Lang transfers to the p-adic case.

Lemma 5.8. *Let $\theta \in \mathbb{C}_p$. Suppose $\tau \geq 1$ is a constant and $P(x) \in \mathbb{Z}[x]$ is a polynomial with $P(\theta) \neq 0$ satisfying*

$$\log\left(\frac{1}{|P(\theta)|}\right) \geq c \left(\log \Lambda(P)\right)^{\tau}$$

for some positive constant c. Then there exists an irreducible polynomial $Q(x) \in \mathbb{Z}[x]$ dividing P such that

$$\log\left(\frac{1}{|Q(\theta)|}\right) \geq \frac{c}{2^{\tau}} (\log \Lambda(Q))^{\tau}.$$

Proof. The proof follows by contraposition. Let $\theta \in \mathbb{C}_p$. Suppose $P(x) \in \mathbb{Z}[x]$ is such that $P = P_1 P_2 \dots P_l$ where $P_1(x), \dots, P_l \in \mathbb{Z}[x]$ are (not necessarily distinct) irreducible polynomials and $P(\theta) \neq 0$. Assume there exists a positive constant c such that

$$\log\left(\frac{1}{|P_i(\theta)|}\right) < \frac{c}{2^{\tau}} (\log \Lambda(P_i))^{\tau}$$

for every $1 \leq i \leq l$. Then since $\tau \geq 1$

$$\begin{aligned}
\log\left(\frac{1}{|P(\theta)|}\right) &= \sum_{i=1}^{l} \log\left(\frac{1}{|P_i(\theta)|}\right) \\
&< \frac{c}{2^\tau} \sum_{i=1}^{l} (\log \Lambda(P_i))^\tau \\
&\leq \frac{c}{2^\tau} \left(\sum_{i=1}^{l} \log(\Lambda(P_i))\right)^\tau \\
&= \frac{c}{2^\tau} \left(\log(\Lambda(P_1) \dots \Lambda(P_l))\right)^\tau .
\end{aligned}$$

Now apply Proposition 2.4 to obtain

$$\log\left(\frac{1}{|P(\theta)|}\right) < \frac{c}{2^\tau} \left(\log\left(2^{\partial(P)}\Lambda(P)\right)\right)^\tau \leq \frac{c}{2^\tau} \left(\log\left(\Lambda\left(P\right)\right)^2\right)^\tau = c\left(\log \Lambda(P)\right)^\tau.$$

This completes the proof. □

We can now prove our main result comparing τ and τ^*.

Theorem 5.9. *Suppose $\theta \in \mathbb{C}_p$. If $\tau^*(\theta) \geq 2$ or $\tau(\theta) > 2$ then $\tau(\theta) = \tau^*(\theta)$.*

Proof. Suppose $\tau \geq 0$. Given $\theta \in \mathbb{C}_p$ from Corollary 5.5 we have $O^*(u|\theta) \ll O(u|\theta)$, and there exist constants c and u_0 such that $O^*(u|\theta) \leq c\, O(u|\theta)$ for all $u \geq u_0$. Dividing by $(\log u)^\tau$ implies

$$\limsup_{u\to\infty} \frac{O^*(u|\theta)}{(\log u)^\tau} \leq \limsup_{u\to\infty} \frac{c\, O(u|\theta)}{(\log u)^\tau}$$

and by the definition of transcendence type it follows that $\tau^*(\theta) \leq \tau(\theta)$.

It now suffices to prove that if $\tau(\theta) > 2$ then $\tau(\theta) \leq \tau^*(\theta)$. This is because if $\tau^*(\theta) > 2$ then $\tau(\theta) > 2$ and if $\tau^*(\theta) = 2$ then either $\tau(\theta) = 2$, in which case we are done, or $\tau(\theta) > 2$, which would then lead to a contradiction. In order to demonstrate $\tau(\theta) \leq \tau^*(\theta)$ when $\tau(\theta) > 2$ it suffices to prove for fixed $\tau \geq 2$, if

$$\limsup_{u\to\infty} \frac{O(u|\theta)}{(\log u)^\tau} = \infty \tag{5.7}$$

then

$$\limsup_{u\to\infty} \frac{O^*(u|\theta)}{(\log u)^\tau} = \infty. \tag{5.8}$$

Assume equation (5.7) is satisfied for some fixed $\tau \geq 2$. Then there exists a sequence of polynomials $\{P_l(x)\} \subset \mathbb{Z}[x]$ such that for every $l \in \mathbb{N}$

$$\log \frac{1}{|P_l(\theta)|}(\log \Lambda(P_l))^{-\tau} = \frac{O(\Lambda(P_l)|\theta)}{(\log \Lambda(P_l))^\tau} \geq l.$$

By Lemma 5.8 for every l there exists an irreducible $Q_l(x) \in \mathbb{Z}[x]$ dividing $P_l(x)$ such that

$$\log\left(\frac{1}{|Q_l(\theta)|}\right) \geq \frac{l}{2^\tau}(\log \Lambda(Q_l))^\tau. \tag{5.9}$$

Although it is possible the sequence $\{Q_l\}$ contains repetitions there must be an infinite number of distinct Q_l because $\frac{l}{2^\tau}$ can be arbitrarily large. Since only a finite number of polynomials can have a given size it is thus possible to pick a subsequence and relabel the Q_l such that $\Lambda(Q_l) < \Lambda(Q_{l+1})$ for all l.

For a fixed l, let $n = \partial(Q_l)$, $H = H(Q_l)$, and a_n be the leading coefficient of Q_l. It can be proved that all irreducible polynomials with coefficients in $\mathbb{Q}$ are separable with roots in $\overline{\mathbb{Q}}$ (see Chapter 13 of Dummit and Foote [9]), and since Q_l is irreducible, Q_l must be separable. Define $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ to be the distinct roots of Q_l. Without loss of generality let $\alpha = \alpha_1$ be such that $|\theta - \alpha| = \min_{1\leq i\leq n} |\theta - \alpha_i|$. From Proposition 5.7

$$\log\left(\frac{1}{|Q_l(\theta)|}\right) \leq \log\left(|\theta-\alpha|^{-1}|a_n|^{n-2}H^{2n}n^{n/2}((2n-1)!)^{1/2}\right),$$

where the logarithm on the right hand side can be written as the sum

$$\log\frac{1}{|\theta-\alpha|} + (n-2)\log|a_n| + 2n\log H + \frac{1}{2}n\log n + \frac{1}{2}\log((2n-1)!). \tag{5.10}$$

First note that $\log\frac{1}{|\theta-\alpha|} \leq O^*(\Lambda(Q_l)|\theta)$ because $\Lambda(\alpha) = \Lambda(Q_l)$. We claim the remaining terms of (5.10) are less than or equal to a constant multiple of $(\log \Lambda(Q_l))^2$. If $n \geq 2$ in the second term then $(n-2)\log|a_n|$ is not positive because $|a_n| \leq 1$. If $n = 1$ then by part (ii) of Proposition 2.13, $|a_n|^{-1} \leq |a_n|_\infty \leq H(Q_l)$ and consequently

$$(n-2)\log|a_n| = \log|a_n|^{-1} \leq \log H(Q_l) \leq \log \Lambda(Q_l).$$

To simplify notation let $c = (\log 2)^{-1}$ and recall that from the definition of Λ

$$\log \Lambda(Q_l) = nc^{-1} + \log H.$$

In particular, $\log H \leq \log \Lambda(Q_l)$ and

$$n \leq c \log \Lambda(Q_l) - c \log H \leq c \log \Lambda(Q_l). \tag{5.11}$$

Thus the third term of (5.10) satisfies

$$2n \log H \leq 2c(\log \Lambda(Q_l))^2$$

and similarly the fourth term of the sum is bounded above by

$$\frac{1}{2} n \log n \leq \frac{1}{2} c(\log \Lambda(Q_l))(\log(c \log \Lambda(Q_l)).$$

For the final term of (5.10)

$$\frac{1}{2} \log((2n-1)!) \leq \frac{1}{2} \log\left((2n-1)^{2n-1}\right) = \left(n - \frac{1}{2}\right) \log(2n-1).$$

Now apply (5.11) to obtain

$$\frac{1}{2} \log((2n-1)!) \leq c(\log \Lambda(Q_l))(\log(2c \log \Lambda(Q_l)).$$

Thus we have proved the first term in (5.10) is less than or equal to $O^*(\Lambda(Q_l)|\theta)$ and the sum of the remaining terms is less than or equal to $c_1(\log \Lambda(Q_l))^2$ for some constant c_1. From (5.9) it thus follows that

$$l \leq 2^\tau (\log \Lambda(Q_l))^{-\tau} \log\left(\frac{1}{|Q_l(\theta)|}\right) \leq 2^\tau \left(\frac{O^*(\Lambda(Q_l)|\theta)}{(\log \Lambda(Q_l))^\tau} + c_1 \frac{(\log \Lambda(Q_l))^2}{(\log \Lambda(Q_l))^\tau}\right). \tag{5.12}$$

Since it was assumed that $\tau \geq 2$, then

$$0 \leq \lim_{l \to \infty} c_1 \frac{(\log \Lambda(Q_l))^2}{(\log \Lambda(Q_l))^\tau} \leq c_1$$

and thus (5.12) implies

$$\begin{aligned}
\lim_{l \to \infty} \frac{l}{2^\tau} &= \lim_{l \to \infty} \left(\frac{O^*(\Lambda(Q_l)|\theta)}{(\log \Lambda(Q_l))^\tau} + c_1 \frac{(\log \Lambda(Q_l))^2}{(\log \Lambda(Q_l))^\tau}\right) \\
&= \lim_{l \to \infty} \frac{O^*(\Lambda(Q_l)|\theta)}{(\log \Lambda(Q_l))^\tau} \\
&\leq \limsup_{u \to \infty} \frac{O^*(u|\theta)}{(\log u)^\tau}.
\end{aligned}$$

Hence we have demonstrated (5.7) implies (5.8) and the result follows. □

Under the given conditions this result relates O and O^* when considering the best approximations relative to a power of $\log u$. In particular, if $\theta \in \mathbb{C}_p$ is such that the largest values of $O(u|\theta)$ or $O^*(u|\theta)$ grow faster than $(\log u)^2$ then from this perspective approximation by algebraic numbers is the same as approximation by polynomials.

5.2 Constructing Numbers With a Given Transcendence Type

Theorem 5.11 will allow us to construct elements of $\mathbb{Q}_p$ with transcendence type τ for any real number $\tau \geq \frac{3+\sqrt{5}}{2} \approx 2.618$. In the complex case Durand [11] constructed numbers with transcendence type τ for all $\tau \geq 3$. This result was then improved by Amoroso [2] when he constructed real numbers with transcendence type τ for all $\tau \geq 2$. Our construction is similar to that of Durand and Amoroso. The following lemma gives a lower bound on the p-adic absolute value of a polynomial evaluated at a positive integer and will be used in our construction in Theorem 5.11.

Lemma 5.10. *Let $\alpha \in \mathbb{N}$ and let $\alpha = \alpha_0 + \alpha_1 p + \cdots + \alpha_n p^n$ be the base p expansion of α where $\alpha_n \neq 0$. Let $Q(x) \in \mathbb{Z}[x]$ be a polynomial of degree d. If $Q(\alpha) \neq 0$ then*

$$|Q(\alpha)| > H(Q)^{-1} 2^{-(d+1)} \alpha_n^{-d} p^{-nd}.$$

Proof. First consider the case when $\alpha = 1$. It follows that $|Q(1)|_\infty \leq H(Q)(d+1)$ and then part (i) of Proposition 2.13 implies

$$|Q(1)| \geq \frac{1}{|Q(1)|_\infty} \geq H(Q)^{-1}(d+1)^{-1}.$$

Thus the result follows because $d + 1 \leq 2^{d+1} p^{nd}$ for all $d \in \mathbb{N}$. Now suppose $\alpha \neq 1$. It therefore follows from the geometric series formula that

$$|Q(\alpha)|_\infty \leq H(Q) \sum_{i=0}^{d} \alpha^i = H(Q) \left(\alpha^d + \frac{\alpha^d - 1}{\alpha - 1} \right) \leq H(Q) 2\alpha^d$$

and from the definition of α we have

$$|Q(\alpha)|_\infty \leq 2H(Q)(\alpha_0 + \cdots + \alpha_n p^n)^d < 2H(Q)(2\alpha_n p^n)^d = H(Q)2^{d+1}\alpha_n^d p^{nd}.$$

By part (i) of Proposition 2.13, $1 \leq |Q(\alpha)||Q(\alpha)|_\infty$. Thus $1 < H(Q)2^{d+1}\alpha_n^d p^{nd}|Q(\alpha)|$ and hence

$$|Q(\alpha)| > H(Q)^{-1}2^{-(d+1)}\alpha_n^{-d}p^{-nd}. \qquad \square$$

Given $\tau \geq \frac{3+\sqrt{5}}{2}$ we are now prepared to construct $\alpha \in \mathbb{Q}_p$ satisfying $\tau(\alpha) = \tau$. From Theorem 5.9 this also gives that $\tau^*(\alpha) = \tau$. The notation $\lfloor * \rfloor$ will be used to denote the greatest integer function.

Theorem 5.11. *Let $f : \mathbb{N} \to \{0, 1\}$ be an arbitrary function and let $a \geq 2$. For any real number $\tau \geq \frac{3+\sqrt{5}}{2}$ let*

$$\alpha_n = 1 + \sum_{i=1}^{n} p^{\lfloor a^{\tau^i} \rfloor - f(i)} \tag{5.13}$$

and $\alpha = \lim_{n\to\infty} \alpha_n \in \mathbb{Q}_p$. Then the transcendence type of α is τ.

Proof. For any $a \geq 2$ and $\tau \geq \frac{3+\sqrt{5}}{2}$ let $\{\alpha_n\}$ and α be defined as in (5.13). Then $\alpha \in \mathbb{Q}_p$ because $\alpha = \lim_{n\to\infty} \alpha_n$ since $\lfloor a^{\tau^i} \rfloor - f(i)$ monotonically increases without bound as i approaches infinity and $\mathbb{Q}_p$ is complete with respect to $|*|$. Our proof that $\tau(\alpha) = \tau$ will consist of two parts. Recall Lemma 5.2 states that if $t > 0$ and there exists a sequence of integer polynomials $\{Q_n\}$ with monotone increasing $\Lambda(Q_n)$ which satisfies

$$\log\left(\frac{1}{|Q_n(\alpha)|}\right) \geq n(\log \Lambda(Q_n))^t \tag{5.14}$$

for every integer $n \geq 1$ then $t \in T(\alpha)$. Given $0 < \epsilon < \tau$ our first step will be to construct a sequence of integer polynomials $\{Q_n\}$ which satisfies (5.14) for $t = \tau - \epsilon$. Since this implies $\tau - \epsilon \in T(\alpha)$ for all $0 < \epsilon < \tau$ it will then follow that $\tau \leq \sup T(\alpha) = \tau(\alpha)$. The second step is to prove $\tau \geq \tau(\alpha)$. To do this we prove there exists a constant c' depending only on a and τ such that every polynomial $Q(x) \in \mathbb{Z}[x]$ satisfies

$$\log\left(\frac{1}{|Q(\alpha)|}\right) \leq c'(\log \Lambda(Q))^\tau. \tag{5.15}$$

If this holds then for any $u \in \mathbb{N}$ define the polynomial $Q(x) \in \mathbb{Z}[x]$ to be such that $O(u|\alpha) = \log\left(\frac{1}{|Q(\alpha)|}\right)$ and $\Lambda(Q) = u$. Then (5.15) implies

$$\frac{O(u|\alpha)}{(\log u)^\tau} = \frac{\log(\frac{1}{|Q(\alpha)|})}{(\log u)^\tau} \leq c'$$

and by Definition 5.1, $\tau \geq \tau(\alpha)$.

Before proving the first step we first note that since $f(n) \in \{0, 1\}$, (5.13) implies

$$\alpha_{n-1} \leq p^{\lfloor a^{\tau^n} \rfloor - f(n)} \leq p^{a^{\tau^n}}$$

and

$$p^{-2}p^{a^{\tau^n}} \leq p^{\lfloor a^{\tau^n} \rfloor - f(n)} \leq \alpha_n = p^{\lfloor a^{\tau^n} \rfloor - f(n)} + \alpha_{n-1} \leq 2p^{a^{\tau^n}}.$$

For $P_n(x) = x - \alpha_n \in \mathbb{Z}[x]$, we obtain the following rough upper and lower bounds on $\Lambda(P_n)$ in terms of a, τ and n

$$2p^{-2}p^{a^{\tau^n}} \leq 2\alpha_n = 2H(P_n) = \Lambda(P_n) \leq 4p^{a^{\tau^n}}. \tag{5.16}$$

The proof of the first step follows by first taking the logarithm of the right inequality in (5.16)

$$(\log \Lambda(P_n))^\tau \leq (\log 4 + a^{\tau^n})^\tau.$$

Then there exists a constant $c_1 > 0$ depending only on τ and a such that

$$\begin{aligned}
(\log 4 + a^{\tau^n})^\tau &\leq 2^\tau a^{\tau^{n+1}} \\
&\leq 2^\tau((\lfloor a^{\tau^{n+1}} \rfloor + 1) + (1 - f(n+1))) \\
&\leq 2^\tau(\lfloor a^{\tau^{n+1}} \rfloor - f(n+1) + 2) \\
&\leq c_1(\lfloor a^{\tau^{n+1}} \rfloor - f(n+1))
\end{aligned}$$

and hence

$$(\log \Lambda(P_n))^\tau \leq c_1(\lfloor a^{\tau^{n+1}} \rfloor - f(n+1)). \tag{5.17}$$

Part (ii) of Proposition 2.13 implies

$$\begin{aligned} |\alpha - \alpha_n| &= \left| \sum_{i=n+1}^{\infty} p^{\lfloor a^{\tau^i} \rfloor - f(i)} \right| \\ &= \max \left\{ \left| p^{\lfloor a^{\tau^{n+1}} \rfloor - f(n+1)} \right|, \left| \sum_{i=n+2}^{\infty} p^{\lfloor a^{\tau^i} \rfloor - f(i)} \right| \right\} \\ &= \left| p^{\lfloor a^{\tau^{n+1}} \rfloor - f(n+1)} \right| \end{aligned}$$

and since $P_n(\alpha) = \alpha - \alpha_n$ it follows that

$$\log \left(\frac{1}{|P_n(\alpha)|} \right) = \lfloor a^{\tau^{n+1}} \rfloor - f(n+1). \tag{5.18}$$

Up to the positive factor of c_1 this is equal to the right hand side of (5.17) and hence

$$(\log \Lambda(P_n))^{\tau} \leq c_1 \log \left(\frac{1}{|P_n(\alpha)|} \right).$$

Therefore, for any $\epsilon > 0$

$$\frac{1}{c_1} (\log \Lambda(P_n))^{\epsilon} (\log \Lambda(P_n))^{\tau - \epsilon} \leq \log \left(\frac{1}{|P_n(\alpha)|} \right).$$

The sequence $\{\Lambda(P_n)\}$ increases monotonically without bound by (5.16) and consequently for fixed $\epsilon > 0$ the sequence $\{(\log \Lambda(P_n))^{\epsilon}\}$ must also be increasing and unbounded. Thus there exists a subsequence $\{Q_n\}$ of $\{P_n\}$ such that for all $n \in \mathbb{N}$, $n \leq \frac{1}{c_1} (\log \Lambda(Q_n))^{\epsilon}$ and hence

$$n (\log \Lambda(Q_n))^{\tau - \epsilon} \leq \log \left(\frac{1}{|Q_n(\alpha)|} \right).$$

Thus for every $\epsilon > 0$ we have found a sequence of integer polynomials with monotone increasing size satisfying (5.14) with $t = \tau - \epsilon$ and $t \in T(\alpha)$. Hence $\tau \leq \tau(\alpha)$ and the proof of the first step is complete.

We now prove the second step by demonstrating (5.15). We proceed by proving (5.15) first for $P_n(x) = x - \alpha_n$. From (5.18), $\log \left(\frac{1}{|P_n(\alpha)|} \right) \leq (a^{\tau^n})^{\tau}$. Take the logarithm of the left side of (5.16) to obtain

$$(a^{\tau^n})^{\tau} \leq \left(\log \left(\frac{p^2}{2} \Lambda(P_n) \right) \right)^{\tau} \leq c_2 (\log \Lambda(P_n))^{\tau}$$

where c_2 is a constant depending only on τ. Hence

$$\log\left(\frac{1}{|P_n(\alpha)|}\right) \leq c_2(\log \Lambda(P_n))^\tau \tag{5.19}$$

which proves (5.15) when $Q(x) = P_n(x) = x - \alpha_n$ for all $n \in \mathbb{N}$.

Now suppose $Q(x) \in \mathbb{Z}[x]$ is arbitrary. To simplify notation define $\exp(x)$ to denote p^x. Let $N_0 \in \mathbb{N}$ be such that if $\Lambda(Q) \geq N_0$ then there exists a positive integer n such that

$$\exp\left((c+1)^{-1}a^{\tau^n - \tau^{n-1}}\right) \leq \Lambda(Q) < \exp\left((c+1)^{-1}a^{\tau^{n+1} - \tau^n}\right). \tag{5.20}$$

where $c = \frac{1}{\log 2}$.

Now assume $\Lambda(Q) \geq N_0$ and $Q(\alpha_n) \neq 0$. We will consider the other cases at the end of the proof. Let $d = \partial(Q)$. The last term in the base p expansion of α_n is $p^{\lfloor a^{\tau^n} \rfloor - f(n)}$ with a coefficient of 1. Since $\alpha_n \in \mathbb{N}$, Lemma 5.10 implies

$$(H(Q))^{-1}2^{-(d+1)}p^{-d\lfloor a^{\tau^n} \rfloor + df(n)} \leq |Q(\alpha_n)| \leq \max\{|Q(\alpha) - Q(\alpha_n)|, |Q(\alpha)|\}.$$

Define $\alpha^* = p^{\lfloor a^{\tau^n} \rfloor - f(n)}$ to simplify notation. To proceed we show

$$\max\{|Q(\alpha) - Q(\alpha_n)|, |Q(\alpha)|\} = |Q(\alpha)| \tag{5.21}$$

by demonstrating

$$|Q(\alpha) - Q(\alpha_n)| < (H(Q))^{-1}2^{-(d+1)}(\alpha^*)^{-d}. \tag{5.22}$$

The ultrametric triangle inequality implies

$$\begin{aligned} |Q(\alpha) - Q(\alpha_n)| &= \left|\sum_{i=1}^{d} a_i(\alpha^i - \alpha_n^i)\right| \\ &\leq \max_{1\leq i\leq d}\{|a_i|\} \max_{1\leq i\leq d}\{|\alpha^i - \alpha_n^i|\} \\ &\leq \max_{1\leq i\leq d}\{|\alpha^i - \alpha_n^i|\}. \end{aligned}$$

Note that $\alpha^i = (\alpha_n + (\alpha - \alpha_n))^i = \alpha_n^i + (\alpha - \alpha_n)\rho$ where ρ is simply the remaining terms obtained from expanding. Moreover, $|\rho| \leq 1$ and hence

$$|\alpha^i - \alpha_n^i| = |\alpha - \alpha_n||\rho| \leq |\alpha - \alpha_n|.$$

It follows that

$$\max_{1\leq i\leq d}\{|\alpha^i-\alpha_n^i|\}\leq|\alpha-\alpha_n|=p^{-\lfloor a^{\tau^{n+1}}\rfloor+f(n+1)}\leq p^{-a^{\tau^{n+1}}+2}$$

and consequently

$$|Q(\alpha)-Q(\alpha_n)|\leq p^{-a^{\tau^{n+1}}+2}. \tag{5.23}$$

Recall we defined $c=\frac{1}{\log 2}$ and by the change of base formula for logarithms we have

$$\begin{aligned}(H(Q))^{-1}2^{-(d+1)}(\alpha^*)^{-d} &= \frac{1}{2}(H(Q))^{-1}2^{-d}2^{-cd\log\alpha^*}\\ &= \frac{1}{2}(\Lambda(Q))^{-1}2^{-cd(\lfloor a^{\tau^n}\rfloor-f(n))}\\ &\geq \frac{1}{2}(\Lambda(Q))^{-1}(2^d)^{-ca^{\tau^n}}\\ &\geq \frac{1}{2}(\Lambda(Q))^{-1}(2^dH(Q))^{-ca^{\tau^n}}\\ &= \frac{1}{2}(\Lambda(Q))^{-ca^{\tau^n}-1}.\end{aligned}$$

Thus

$$(H(Q))^{-1}2^{-(d+1)}(\alpha^*)^{-d}\geq\frac{1}{2}(\Lambda(Q))^{-ca^{\tau^n}-1}. \tag{5.24}$$

Recall that $\exp(x)$ denotes p^x. Now apply (5.20) to obtain

$$\begin{aligned}\frac{1}{2}(\Lambda(Q))^{-ca^{\tau^n}-1} &\geq \frac{1}{2}\exp\left(\left(\frac{1}{c+1}a^{\tau^{n+1}-\tau^n}\right)\left(-ca^{\tau^n}-1\right)\right)\\ &= \frac{1}{2}\exp\left(\frac{-c}{c+1}a^{\tau^{n+1}}-\frac{1}{c+1}a^{\tau^{n+1}-\tau^n}\right)\end{aligned}$$

and thus (5.24) implies

$$(H(Q))^{-1}2^{-(d+1)}(\alpha^*)^{-d}>\frac{1}{2}\exp\left(\frac{-c}{c+1}a^{\tau^{n+1}}-\frac{1}{c+1}a^{\tau^{n+1}-\tau^n}\right). \tag{5.25}$$

If we assume by way of contradiction to (5.22) that

$$(H(Q))^{-1}2^{-(d+1)}(\alpha^*)^{-d}\leq|Q(\alpha)-Q(\alpha_n)| \tag{5.26}$$

then taking the logarithm of (5.23) and (5.25) gives

$$\log\frac{1}{2}-\frac{c}{c+1}a^{\tau^{n+1}}-\frac{1}{c+1}a^{\tau^{n+1}-\tau^n}\leq-a^{\tau^{n+1}}+2.$$

Now multiply by $-a^{-\tau^{n+1}} < 0$ to obtain

$$-a^{-\tau^{n+1}} \log \frac{1}{2} + \frac{c}{c+1} + \frac{1}{c+1} a^{-\tau^n} \geq 1 - 2a^{-\tau^{n+1}}. \tag{5.27}$$

Since n, as defined in (5.20), is an unbounded increasing function of $\Lambda(Q)$, and $\Lambda(Q)$ can be arbitrarily large, (5.27) must hold for arbitrarily large positive integers n. However, if we let n increase without bound taking the limit gives $\frac{c}{c+1} \geq 1$, which is impossible. Thus (5.26) can only hold for finitely many n and there exists a positive integer $N_1 \geq N_0$ for which all $Q(x) \in \mathbb{Z}[x]$ with $\Lambda(Q) \geq N_1$ and $Q(\alpha_n) \neq 0$ cannot satisfy (5.27) and therefore satisfy (5.21). Consequently $(H(Q))^{-1} 2^{-(d+1)} (\alpha^*)^{-d} \leq |Q(\alpha)|$ and hence

$$\log \frac{1}{|Q(\alpha)|} \leq \log \left(H(Q) 2^{d+1} (\alpha^*)^d \right). \tag{5.28}$$

We can now use our previous results to bound the right hand side of (5.28) in terms of $\Lambda(Q)$. The inequality (5.24) gives

$$\begin{aligned} \log \left(H(Q) 2^{d+1} (\alpha^*)^d \right) &\leq \log \left(2\Lambda(Q)^{ca^{\tau^n}+1} \right) \\ &= \log 2 + (ca^{\tau^n} + 1) \log \Lambda(Q) \\ &\leq 2ca^{\tau^n} \log \Lambda(Q) \end{aligned}$$

and thus

$$\log \frac{1}{|Q(\alpha)|} \leq 2ca^{\tau^n} \log \Lambda(Q). \tag{5.29}$$

Now note $(\tau^n - \tau^{n-1}) \frac{\tau}{\tau - 1} = \tau^n$. To simplify notation let $\gamma = \frac{\tau}{\tau - 1}$. By (5.20) it follows that

$$(c+1)^\gamma (\log \Lambda(Q))^\gamma \geq \left(a^{(\tau^n - \tau^{n-1})} \right)^\gamma = a^{\tau^n}.$$

Using this in (5.29) and defining $c_3 = 2c(1+c)^\gamma$ gives

$$\log \frac{1}{|Q(\alpha)|} \leq c_3 (\log \Lambda(Q))^{1+\gamma}.$$

Recall that we assumed $\tau \geq \frac{3+\sqrt{5}}{2}$. Thus it follows that

$$1 + \gamma = 1 + \frac{\tau}{\tau - 1} \leq 1 + \frac{3+\sqrt{5}}{1+\sqrt{5}} = \frac{3+\sqrt{5}}{2} \leq \tau$$

and hence

$$\log \frac{1}{|Q(\alpha)|} \leq c_3(\log \Lambda(Q))^\tau. \tag{5.30}$$

This is true for all integer polynomials Q such that $Q(\alpha_n) \neq 0$ and $\Lambda(Q) \geq N_1$. Moreover, there are only finitely many polynomials Q with $\Lambda(Q) < N_1$ and thus there exists a constant c_4 such that if $\Lambda(Q) < N_1$ then

$$\log \left(\frac{1}{|Q(\alpha)|} \right) \leq c_4(\log \Lambda(Q))^\tau. \tag{5.31}$$

It remains to consider when α_n is a root of Q (where n is still defined as it was in (5.20)). Recall that $P_n(x) = x - \alpha_n$ is the minimal polynomial of α_n over $\mathbb{Q}$ and P_n must divide any integer polynomial that has α_n as a root. Thus if $Q(\alpha_n) = 0$ then $Q = P_n^l R$ for some $l \in \mathbb{N}$ and $R(x) \in \mathbb{Q}[x]$ with $R(\alpha_n) \neq 0$. By Theorem 2.9 (Gauss's Lemma) $R(x) \in \mathbb{Z}[x]$. From Theorem 2.4, and in particular (2.3) it follows that $(\Lambda(P_n))^l \leq (\Lambda(Q))^2$ and $\Lambda(R) \leq (\Lambda(Q))^2$. Recall by (5.19)

$$\log \left(\frac{1}{|P_n(\alpha)|} \right) \leq c_2(\log \Lambda(P_n))^\tau$$

where c_2 depends only on α and τ. Since $R(\alpha_n) \neq 0$, (5.30) and (5.31) imply

$$\log \left(\frac{1}{|R(\alpha)|} \right) \leq c_5(\log \Lambda(R))^\tau.$$

where $c_5 = \max\{c_3, c_4\}$ depends only on a and τ. Applying these inequalities gives

$$\begin{aligned}
\log \left(\frac{1}{|Q(\alpha)|} \right) &= l \log \left(\frac{1}{|P_n(\alpha)|} \right) + \log \left(\frac{1}{|R(\alpha)|} \right) \\
&< c_2 l^\tau (\log \Lambda(P_n))^\tau + c_5(\log \Lambda(R))^\tau \\
&\leq c_2(\log(\Lambda(P_n))^l)^\tau + c_5(\log \Lambda(R))^\tau \\
&\leq c_2(\log(\Lambda(Q))^2)^\tau + c_5(\log(\Lambda(Q)^2))^\tau \\
&= (2^\tau c_2 + 2^\tau c_5)(\log \Lambda(Q))^\tau.
\end{aligned}$$

Hence when $Q(\alpha_n) = 0$

$$\log \left(\frac{1}{|Q(\alpha)|} \right) \leq (2^\tau c_2 + 2^\tau c_5)(\log \Lambda(Q))^\tau. \tag{5.32}$$

If we let $c' = 2^\tau c_2 + 2^\tau c_5$ and note $c' \geq \max\{c_2, c_5\}$ is a constant depending only on α and τ it thus follows from (5.19), (5.30), (5.31), and (5.32) that

$$\log\left(\frac{1}{|Q(\alpha)|}\right) \leq c'(\log \Lambda(Q))^\tau$$

for all polynomials Q. Hence the second step of the proof is complete and $\tau \geq \tau(\alpha)$. Thus the transcendence type of α must equal τ. □

Corollary 5.12. *There are uncountably many different equivalence classes on $\mathbb{C}_p$ under the equivalence relation $\asymp$ defined by $\theta \asymp \eta$ if $O(u|\theta) \asymp O(u|\eta)$. The same holds for the equivalence classes on $\mathbb{C}_p$ under the equivalence relation $\asymp^*$ defined by $\theta \asymp^* \eta$ if $O^*(u|\theta) \asymp O^*(u|\eta)$.*

Proof. Given any $\tau \geq \frac{3+\sqrt{5}}{2}$ Theorem 5.11 gives that there exists $\theta \in \mathbb{C}_p$ with transcendence type τ. Thus the result on $\asymp$ will follow if we can prove that if $\theta, \eta \in \mathbb{C}_p$ are such that $\tau(\theta) \neq \tau(\eta)$ then $O(u|\theta)$ and $O(u|\eta)$ are not equivalent.

Let $\theta, \eta \in \mathbb{C}_p$ and suppose $O(u|\eta) \gg O(u|\theta)$. Then there exist $u_0, c \in \mathbb{N}$ and positive $\gamma \in \mathbb{R}$ such that $O(u^c|\eta) \geq \gamma O(u|\theta)$ for all $u \geq u_0$. It follows that for all $\tau > 0$

$$\limsup_{u\to\infty} \frac{\gamma O(u|\theta)}{(\log u)^\tau} \leq \limsup_{u\to\infty} \frac{O(u^c|\eta)}{(\log u)^\tau} = c^\tau \limsup_{u\to\infty} \frac{O(u^c|\eta)}{(\log u^c)^\tau} \leq c^\tau \limsup_{u\to\infty} \frac{O(u|\eta)}{(\log u)^\tau}$$

and thus $\tau(\theta) \leq \tau(\eta)$. In particular, if $\tau(\theta) > \tau(\eta)$ then $O(u|\eta) \gg O(u|\theta)$ cannot hold and hence θ and η do not satisfy $O(u|\theta) \asymp O(u|\eta)$. Thus it follows that any two elements of $\mathbb{C}_p$ with different transcendece types must be in different equivalence classes under the equivalence relation $\asymp$. Since Theorem 5.11 gives that there are uncountably many possible values for the transcendence type of elements of $\mathbb{C}_p$ the result follows. The proof for $\asymp^*$ is identical since if $\tau \geq \frac{3+\sqrt{5}}{2} > 2$ then Theorem 5.9 implies that $\tau^*(\theta) = \tau$. □

All of our results in this chapter are also true in the complex case. The proof that $O^*(u|\theta) \ll O(u|\theta)$ and the equality of $\tau(\theta)$ and $\tau^*(\theta)$ when $\tau^*(\theta) \geq 2$ or $\tau(\theta) > 2$ are analogous to the results of Fel'dman [13] and Durand [11]. Given $\tau \geq (3+\sqrt{5})/2$ the construction of $\theta \in \mathbb{Q}_p$ with $\tau(\theta) = \tau$ is similar to results of Durand [11] and Amoroso [2].

6 CONCLUSION

Our initial goal was to consider the results on complex order functions due to Mahler [22] and Durand [11] in the p-adics. Several of our results are analogous to those in the complex case. Theorem 3.6 established that the order functions $O(u|\theta)$ and $O(u|\eta)$ are equivalent when $\theta, \eta \in \mathbb{C}_p$ are algebraically dependent. Given $\tau \geq \frac{3+\sqrt{5}}{2}$, Theorem 5.11 constructs $\theta \in \mathbb{Q}_p$ such that $\tau(\theta) = \tau$ and Theorem 5.9 demonstrates if $\theta \in \mathbb{C}_p$ is such that $\tau^*(\theta) \geq 2$ or $\tau(\theta) > 2$ then $\tau^*(\theta) = \tau(\theta)$. Further study revealed that the properties of the p-adics could be used to obtain results different from those proved in the complex case. For instance, Corollary 3.5 is a direct result of work done by Escassut [12] and states that there are transcendental $\theta \in \mathbb{C}_p$ for which $O(u|\theta) \asymp \log u$. Also, Theorem 4.2 gives that if $\alpha \in \overline{\mathbb{Q}}_p$ then $O^*(u|\alpha) \gg \log u$. Theorem 4.5 gave $\theta \in \mathbb{C}_p$ for which $O^*(u|\theta)$ grows slowly, and under certain conditions a lower bound for $O^*(u|\theta)$ then could be obtained from Theorem 4.6. Corollary 4.7 then used these results to demonstrate that if $n \geq 3$ then there exist uncountably many $\theta \in \mathbb{C}_p$ which satisfy $\log^n u \asymp O^*(u|\theta)$.

There are many open questions concerning both the complex and p-adic order functions. A likely subject for further study would be a proof or counterexample that $O^*(u|\theta) \asymp O^*(u|\eta)$ when θ and η are algebraically dependent elements of $\mathbb{C}_p$. Given $\tau \geq 2$ Amoroso [2] was able to construct $\theta \in \mathbb{C}$ such that $\tau(\theta) = \tau$ and thus it seems likely that Theorem 5.11 could be extended in this manner. A more difficult question would be to consider the existence of $\theta \in \mathbb{C}_p$ for which $1 < \tau(\theta) < 2$. This is impossible in the complex case because $O(u|\theta) \gg (\log u)^2$ for all transcendental $\theta \in \mathbb{C}$. However, Corollary 3.5 implies there exist transcendental $\theta \in \mathbb{C}_p$ for which $\tau(\theta) = 1$ and therefore it is certainly possible there are $\theta \in \mathbb{C}_p$ with $\tau(\theta)$ between 1 and 2. Another open problem is to determine for which functions $a : \mathbb{R}^+ \to \mathbb{R}^+$ there exist $\theta \in \mathbb{C}_p$ for which $O(u|\theta) \asymp a(u)$ or $O^*(u|\theta) \asymp a(u)$. In the complex case this problem was posed by Mahler [22] and remains open.

BIBLIOGRAPHY

1. W. Adams. Transcendental numbers in the p-adic domain. *Amer. J. Math.*, 88:279–308, 1966.

2. F. Amoroso. On the distribution of complex numbers according to their transcendence types. *Ann. Mat. Pura Appl. (4)*, 151:359–368, 1988.

3. V. Beresnevich, V. Bernik, and E. Kovalevskaya. On approximation of p-adic numbers by p-adic algebraic numbers. *J. Number Theory*, 111:33–56, 2005.

4. V. Bernik and M. Dodson. *Metric Diophantine Approximation on Manifolds*. Cambridge University Press, Cambridge, 1999.

5. N. Bourbaki. *Algebra. II. Chapters 4–7*. Springer-Verlag, Berlin, 1990. Translated from the French by P. M. Cohn and J. Howie.

6. Y. Bugeaud. *Approximation by Algebraic Numbers*. Cambridge University Press, Cambridge, 2004.

7. P. Cijsouw. *Transcendence Measures*. PhD thesis, Amsterdam University, 1972.

8. A. Dubickas and C. Smyth. Length of the sum and product of algebraic numbers. *Math. Notes*, 77:854–860, 2004.

9. D. Dummit and R. Foote. *Abstract Algebra*. John Wiley and Sons, Hoboken, NJ, third edition, 2004.

10. A. Durand. Une nouvelle classification des nombres complexes, selon K. Mahler. In *Séminaire Delange-Pisot-Poitou (Groupe d'étude de Théorie des nombres)*, pages G17.01–G17.06. 1973/74.

11. A. Durand. Quatre problèmes de Mahler sur la fonction ordre d'un nombre transcendant. *Bull. Soc. Math. France*, 102:365–377, 1974.

12. A. Escassut. Transcendence order over $\mathbb{Q}_p$ in $\mathbb{C}_p$. *J. Number Theory*, 16:395–402, 1983. Correction in *J. Number Theory*, 19:451, 1984.

13. N. Fel'dman. The approximation of certain transcendental numbers. I. Approximation of logarithms of algebraic numbers. *Izvestiya Akad. Nauk SSSR. Ser. Mat*, 15:53–74, 1951. (in Russian). English transl. in *Amer. Math. Soc. Transl. Series 2*, 59:224-245, 1966.

14. F. Gouvêa. *p-adic Numbers: An Introduction*. Springer-Verlag, New York, second edition, 1997.

15. R. Güting. Approximation of algebraic numbers by algebraic numbers. *Michigan Math. J.*, 8:149–159, 1961.

16. K. Hensel. *Zahlentheorie*. Göschen, Berlin, 1913.

17. N. Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta Functions*. Springer-Verlag, New York, second edition, 1984.

18. S. Lang. *Introduction to Transcendental Numbers*. Addison-Wesley Pub. Co., Reading, MA, 1966.

19. É. Lutz. *Sur les Approximations Diophantiennes Linéaires p-adiques*. Hermann, Paris, 1955.

20. K. Mahler. Über Approximation der Exponentialfunktionen und des Logarithmus, I,II. *J. Reine Angew. Math.*, 166:118–150, 1932.

21. K. Mahler. Über eine Klassen-Einteilung der p-adischen Zahlen. *Compositio Math.*, 2:259–275, 1935.

22. K. Mahler. On the order function of a transcendental number. *Acta Arith.*, 18:63–76, 1971.

23. M. Mignotte and D. Ştefănescu. *Polynomials: An Algorithmic Approach*. Springer-Verlag, Singapore, 1999.

24. J. Morrison. Approximation of p-adic numbers by algebraic numbers of bounded degree. *J. Number Theory*, 10:334–350, 1978.

25. Y. Nesterenko. Diophantine approximation in the field of p-adic numbers. *Mat. Zametki*, 35:653–662, 1984. (in Russian). English transl. in *Math. Notes*, 35:342-347, 1984.

26. Y. Nesterenko. Measure of algebraic independence for almost all pairs of p-adic numbers. *Mat. Zametki*, 36:295–304, 1984. (in Russian). English transl. in *Math. Notes*, 36:642-647, 1984.

27. I. Niven, H. Zuckerman, and H. Montgomery. *An Introduction to the Theory of Numbers*. John Wiley and Sons, New York, fifth edition, 1991.

28. P. Philippon. Classification de Mahler et distances locales. *Bull. Austral. Math. Soc.*, 49:219–238, 1994.

29. A. Robert. *A Course in p-adic Analysis*. Springer-Verlag, New York, 2000.

30. T. Schneider. *Einführung in die Transzendenten Zahlen*. Springer-Verlag, Berlin, 1957.

31. J. Serre. *Local Fields*. Springer-Verlag, New York, 1979.

32. O. Teulié. Approximation d'un nombre p-adique par des nombres algébriques. *Acta Arith.*, 102:137–155, 2002.

33. M. Waldschmidt. *Nombres Transcendants*. Springer-Verlag, New York, 1973.

34. T. Wang. p-adic transcendence and p-adic transcendence measures for the values of Mahler type functions. *Acta Math. Sin. (Engl. Ser.)*, 22:187–194, 2006.

35. D. Zelo. *Simultaneous Approximation to Real and p-adic Numbers*. PhD thesis, University of Ottawa, 2008.