UNIVERSITÉ DE STRASBOURG

ÉCOLE DOCTORALE Mathématiques, Sciences de l'Information et de l'Ingénieur - ED 269

IRMA UMR 7501

THÈSE présentée par :

Tomislav PEJKOVIĆ

soutenue le : **20 janvier 2012**

pour obtenir le grade de : **Docteur de l'université de Strasbourg**

Discipline/ Spécialité : MATHÉMATIQUES

POLYNOMIAL ROOT SEPARATION AND APPLICATIONS

THÈSE dirigée par :

M. BUGEAUD Yann	Professeur, université de Strasbourg
M. DUJELLA Andrej	Professeur, université de Zagreb

RAPPORTEURS :

M. FUCHS Clemens	Privatdozent, ETH Zürich
M. TICHY Robert	Professeur, Graz University of Technology

AUTRES MEMBRES DU JURY :

Mme JADRIJEVIĆ Borka	Professeur, université de Split
M. MIGNOTTE Maurice	Professeur, université de Strasbourg

Contents

Introduction

For a polynomial with integer coefficients, we can look at how close two of its roots can be. This can be done when we look at roots in the field of real or complex numbers and also if we wish to study roots in the p-adic setting, i.e. in the fields $\mathbb{Q}_p$ or $\mathbb{C}_p$, where p is some prime number. Since we can always find polynomials with roots as close as desired, we need to introduce some measure of size for polynomials with which we can compare this minimal separation of roots. This is done by bounding the degree and most usually using the height, i.e. maximum of the absolute values of the coefficients of a polynomial.

For an integer polynomial $P(x)$ of degree $d \geq 2$, height $\mathrm{H}(P)$ and with distinct roots $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$, we set

$$\mathrm{sep}(P) := \min_{1 \leq i < j \leq d} |\alpha_i - \alpha_j|$$

and define $e(P)$ by

$$\mathrm{sep}(P) = \mathrm{H}(P)^{-e(P)}.$$

For an infinite set S of integer polynomials containing polynomials of arbitrary large height, we define

$$e(S) = \limsup_{P(X) \in S,\, \mathrm{H}(P) \to +\infty} e(P).$$

Mahler [22] proved in 1964 that if S contains only polynomials of degree d, then $e(S) \leq d - 1$. The lower bound on $e(S)$ for this class of polynomials has been successively improved with the best bound in the real/complex case now standing at $e(S) \geq \frac{d}{2} + \frac{d-2}{4(d-1)}$ for general d (see [8]). However, for the set of cubic polynomials it was shown [15, 32] that $e(S) \geq 2$ which is, of course, best possible. For other small d, better results than the general one we mentioned have been found. Another direction of research is to study particular subsets of all polynomials of degree d, for example, we can distinguish between irreducible and reducible polynomials or monic and nonmonic polynomials (see [9]).

Taking up a combination of these directions in the first chapter, we examine in detail the class of reducible monic polynomials of fourth degree. We give a complete description of this case showing that $e(S) \leq 2$ and constructing a family of polynomials which gives $e(S) \geq 2$. We also examine the case of families of polynomials which have polynomial and not exponential growth of coefficients. This line of study is important also for the p-adic case of root separation since we know how to transfer results with polynomial growth of coefficients from the real into p-adic setting, unlike those where exponential growth of coefficients appears.

Separation of roots in the p-adic setting has been much less studied (see [7, §9.3] and [24]). In the second chapter we give analogues of some auxiliary lemmas on polynomials which have been proved in the reals, cf. [7, §A]. The next chapter gives explicit families of integer polynomials of general degree with proofs of bounds for root separation. The quadratic and reducible cubic polynomials are completely understood, while in the irreducible cubic case, we give a family with the bound $e_p(S) \geq 25/14$ which is the best currently known.

The second part of this thesis is concerned with results on p-adic versions of Mahler's and Koksma's classifications of transcendental numbers. For a transcendental number $\xi \in \mathbb{Q}_p$, denote by $w_n(\xi)$ the upper limit of the real numbers w for which there exist infinitely many integer polynomials $P(X)$ of degree at most n satisfying $0 < |P(\xi)|_p \leq \mathrm{H}(P)^{-w-1}$. Also, denote by $w_n^*(\xi)$ the upper limit of the real numbers w for which there exist infinitely many algebraic numbers α in $\mathbb{Q}_p$ of degree at most n satisfying $0 < |\xi - \alpha|_p \leq \mathrm{H}(\alpha)^{-w-1}$. Let $w(\xi) = \limsup_{n\to\infty} \frac{w_n(\xi)}{n}$ and $w^*(\xi) = \limsup_{n\to\infty} \frac{w_n^*(\xi)}{n}$. Mahler used the functions w_n in order to classify transcendental numbers into three classes: S-numbers are those that have $w(\xi) < \infty$, T-numbers are those with $w(\xi) = \infty$ and $w_n(\xi) < \infty$ for any integer $n \geq 1$ and U-numbers have $w(\xi) = \infty$ and $w_n(\xi) = \infty$ for some integer $n \geq 1$. Koksma's classification into S^*-, T^*- and U^*- numbers is achieved in the same way, just using functions w_n^*, w^* in place of w_n, w. These two classifications coincide. See [7] for all references.

Almost all numbers (in the sense of Lebesgue measure for real and Haar measure for p-adic numbers) are S-numbers and U-numbers contain for example Liouville numbers. But, it was only in 1968 that Schmidt [29] proved the existence of T-numbers in $\mathbb{R}$. Schlickewei [28] adapted this result to the p-adic setting. While Schlickewei showed that p-adic T-numbers do exist, his proof only gave numbers ξ such that $w_n(\xi) = w_n^*(\xi)$ for all integers $n \geq 1$. Since for any p-adic transcendental number ξ we have

$$w_n^*(\xi) \leq w_n(\xi) \leq w_n^*(\xi) + n - 1,$$

it is natural to ask whether there exist p-adic numbers ξ such that $w_n(\xi) \neq w_n^*(\xi)$ for some integer n and how large can $w_n(\xi) - w_n^*(\xi)$ really be. Although the second question is, as in the more extensively studied real case, far from being resolved, the main result of chapter four gives a positive answer to the first question and goes some way in answering the second one.

Theorem 4.1. *Let $(w_n)_{n\geq 1}$ and $(w_n^*)_{n\geq 1}$ be two non-decreasing sequences in $[1, +\infty]$ such that*

$$w_n^* \leq w_n \leq w_n^* + (n-1)/n, \quad w_n > n^3 + 2n^2 + 5n + 2, \qquad \text{for any } n \geq 1.$$

Then there exists a p-adic transcendental number ξ such that

$$w_n^*(\xi) = w_n^* \quad \text{and} \quad w_n(\xi) = w_n, \qquad \text{for any } n \geq 1.$$

We also impose much milder growth requirements on the sequence $(w_n)_{n\geq 1}$ than Schlickewei and thus our theorem considerably improves the range of attainable values for w_n^* and w_n. The proof is quite involved and follows that of R. C. Baker's theorem in [1].

In chapter five we improve an aspect of Theorem 4.1 showing that for any $n \geq 3$, function $w_n - w_n^*$ contains the interval $[0, \frac{n}{4}]$. We achieve that using integer polynomials having two zeros very close to each other. Estimating the distance between algebraic numbers is done with the help of a lemma which unlike the lemma in the previous chapter has effective constants appearing in the lower bound. However, the drawback we have to endure in this method is a larger left endpoint of interval for w_n. More importantly, we can construct p-adic numbers ξ with prescribed values for $w_n^*(\xi)$ and $w_n(\xi)$ for only one (or, with a modification, finitely many) positive integer n at a time. This is in stark contrast to the situation in Theorem 4.1 where we succeeded in constructing p-adic numbers ξ with prescribed value for $w_n^*(\xi)$ and $w_n(\xi)$ for all positive integers $n \geq 2$.

At the end of this chapter, we briefly mention the case $n = 1$. We also examine the case $n = 2$, proving that the difference $w_2 - w_2^*$ can take any value from the interval $[0, 1[$ which is essentially best possible.

Mahler proved in [20] that his classification of real numbers has the property that every two algebraically dependent numbers belong to the same class. In order to prove this basic property he showed that if ξ and η are transcendental real numbers such that $P(\xi, \eta) = 0$ for an irreducible polynomial $P(x, y) \in \mathbb{Z}[x, y]$ of degree M in x and N in y, then the inequalities

$$w_n(\xi) + 1 \leq M(w_{nN}(\eta) + 1) \quad \text{and} \quad w_n(\eta) + 1 \leq N(w_{nM}(\xi) + 1)$$

are valid for every positive integer n. Schmidt [29] showed that these conditions also imply inequalities

$$w_n^*(\xi) + 1 \leq M(w_{nN}^*(\eta) + 1) \quad \text{and} \quad w_n^*(\eta) + 1 \leq N(w_{nM}^*(\xi) + 1),$$

i.e. the inequalities we get when Mahler's function w_k is replaced with Koksma's function w_k^*.

Mahler himself [21] proved the first two inequalities under analogous conditions in the p-adic setting. We establish in chapter six a p-adic version of the last two inequalities and show that in a very special, but nontrivial case these inequalities become equalities.

Basic notation, definitions and lemmas

Notation

In this chapter we will describe the notation used in this thesis. To simplify our exposition later on, we include here some basic definitions and well known lemmas.

For the real number r, we denote by $\lfloor r \rfloor$ the largest integer not greater than r.

We will be using the most natural measure for the size of a polynomial or an algebraic number. The notation $\mathrm{H}(P)$ stands for *naive height* of polynomial P, i.e. the maximum of the absolute values of its coefficients. The height $\mathrm{H}(\alpha)$ of a number α algebraic over $\mathbb{Q}$ is that of its minimal polynomial over $\mathbb{Z}$.

For a polynomial $P(X) \in \mathbb{Z}[X]$ of degree $d \geq 2$ and with distinct roots $\alpha_1, \ldots, \alpha_d$, we set

$$\mathrm{sep}(P) := \min_{1 \leq i < j \leq d} |\alpha_i - \alpha_j|$$

and we call this quantity *minimal separation of roots* of $P(X)$.

Now we fix our notation with respect to the p-adic analysis we will be using. Let p be a rational prime number. We denote by $\mathbb{Q}_p$ the completion of the field of rational numbers $\mathbb{Q}$ with respect to p-adic absolute value $|\cdot|_p$ which is normalised in such a way that $|p|_p = p^{-1}$. By $\mathbb{Z}_p$ we denote the ring of p-adic integers, i.e. set $\{x \in \mathbb{Q}_p : |x|_p \leq 1\}$. We also use $\mathbb{C}_p$ for the (metric) completion of an algebraic closure of $\mathbb{Q}_p$. The field $\mathbb{Q}_p$ of p-adic numbers is usually considered as an analogue of the field $\mathbb{R}$ of real numbers, while the field $\mathbb{C}_p$ is analogous to the field $\mathbb{C}$ of complex numbers. The function μ denotes the Haar measure which is defined on balls in $\mathbb{Q}_p$ by $\mu(\{x \in \mathbb{Q}_p : |x - a|_p \leq p^{-\lambda}\}) = p^{-\lambda}$ for $a \in \mathbb{Q}_p$ and $\lambda \in \mathbb{Z}$ and then extended in the usual fashion. Basic facts about p-adic theory will be tacitly used, interested reader can consult e.g. [16].

Symbols $\gg$ and $\ll$ are the Vinogradov symbols. For example $A \ll B$ means $A \leq cB$ where c is some constant. We will usually say what this constant depends upon in a particular case. When $A \ll B$ and $A \gg B$, we write $A \asymp B$.

Lemmas

First we give two versions of a result by Carl Friedrich Gauss. Recall that a polynomial with integer coefficients is called primitive if the greatest common divisor of its coefficients is 1.

Lemma 0.1 (Gauss's Lemma)**.** *(1) If $f(X) = g(X)h(X)$, where $f(X)$, $g(X) \in \mathbb{Z}[X]$, $h(X) \in \mathbb{Q}[X]$ and $g(X)$ is primitive, then $h(X) \in \mathbb{Z}[X]$ as well.*

(2) Let $\mathbf{A}$ be a unique factorization domain (factorial ring) and $\mathbf{F}$ its field of fractions. If a polynomial $P(X) \in \mathbf{A}[X]$ is reducible in $\mathbf{F}[X]$, then it is reducible in $\mathbf{A}[X]$.

Proof. See [19, Theorem 2.1, Corollary 2.2, §IV.2, p. 181]. ∎

The next lemma relates the height of a product of polynomials to the product of heights of these polynomials.

Lemma 0.2 (Gelfond's Lemma)**.** *Let $P_1(X_1, \dots, X_k)$,...,$P_r(X_1, \dots, X_k)$ be non-zero polynomials of total degree n_1,...,n_r, respectively, and set $n = n_1 + \cdots + n_r$. We then have*

$$2^{-n} \operatorname{H}(P_1) \cdots \operatorname{H}(P_r) \leq \operatorname{H}(P_1 \cdots P_r) \leq 2^n \operatorname{H}(P_1) \cdots \operatorname{H}(P_r).$$

Proof. See [7, Lemma A.3, p. 221] or [3, Lemma 1.6.11, p. 27]. ∎

The following lemma and its proof hold whether we take the algebraic number to be in $\mathbb{C}$ or in $\mathbb{C}_p$.

Lemma 0.3. *Let α be a non-zero algebraic number of degree n. Let a, b and c be integers with $c \neq 0$. We then have*

$$\operatorname{H}\left(\frac{a\alpha + b}{c}\right) \leq 2^{n+1} \operatorname{H}(\alpha) \max\{|a|, |b|, |c|\}^n.$$

Proof. (cf. [7, Lemma A.4, p. 222]) Let $P(X)$ and $Q(X)$ be minimal polynomials over $\mathbb{Z}$ of α and $\frac{a\alpha+b}{c}$, respectively. Since $Q(\frac{aX+b}{c})$ is a polynomial in $\mathbb{Q}[X]$ vanishing at α, we must have $\deg Q \geq \deg P$. Likewise, since $a^n P(\frac{cX-b}{a})$ is a polynomial in $\mathbb{Z}[X]$ vanishing at $\frac{a\alpha+b}{c}$, we must have $\deg Q \leq \deg P$. From the minimality of P and Q using Gauss's Lemma 0.1, we conclude that $a^n P(\frac{cX-b}{a}) = d \cdot Q(X)$, where d is an integer. Therefore,

$$\mathrm{H}\left(\frac{a\alpha+b}{c}\right) = \mathrm{H}(Q(X)) \leq \mathrm{H}\left(a^n P\Big(\frac{cX-b}{a}\Big)\right)$$
$$\leq \max_i \sum_{k=i}^{n} \binom{k}{i} \cdot \max\{|a|,|b|,|c|\}^n \cdot \mathrm{H}(P) < 2^{n+1} \max\{|a|,|b|,|c|\}^n \cdot \mathrm{H}(P),$$

because $\sum_{k=i}^{n} \binom{k}{i} = \binom{n+1}{i+1} < 2^{n+1}$. ∎

Standard tools to investigate questions of separation of roots are the notions of *resultant* and *discriminant*. We gather definitions and most important properties in the following lemma, for proofs and further results consult for example [14, 19, 23].

Lemma 0.4. *Let D be an integral domain contained in an algebraically closed field K. Let $P(X)$ and $Q(X)$ be two polynomials in $D[X]$, of degree m and n respectively. Write*

$$P(X) = a_m X^m + \cdots + a_1 X + a_0 = a_m(X-\alpha_1)\cdots(X-\alpha_m) \quad \textit{and}$$
$$Q(X) = b_n X^n + \cdots + b_1 X + b_0 = b_n(X-\beta_1)\cdots(X-\beta_n)$$

in $K[X]$. The resultant of two non-zero polynomials $P(X)$ and $Q(X)$ is the product

$$\mathrm{Res}(P,Q) = a_m^n b_n^m \prod_{\substack{1\leq i\leq m\\ 1\leq j\leq n}} (\alpha_i - \beta_j) = a_m^n \prod_{1\leq i\leq m} Q(\alpha_i) = (-1)^{mn} b_n^m \prod_{1\leq j\leq n} P(\beta_j).$$

If $P(X) \equiv 0$ or $Q(X) \equiv 0$, then $\mathrm{Res}(P,Q) = 0$. The resultant of two polynomials in $D[X]$ is zero if and only if the two polynomials have a common root in K. The resultant can also be written as

$$\mathrm{Res}(P,Q) = \begin{vmatrix} a_m & \cdots & a_0 & & \\ & \ddots & & \ddots & \\ & & a_m & \cdots & a_0 \\ b_n & \cdots & b_0 & & \\ & \ddots & & \ddots & \\ & & b_n & \cdots & b_0 \end{vmatrix}$$

where, more precisely, the coefficients of the $(m+n)\times(m+n)$ *matrix* $(c_{i,j})$ *associated to this determinant are given by*

$$\begin{aligned} c_{i,j} &= a_{m-j+i}, \qquad \text{for } 1 \le i \le n, \\ c_{n+i,j} &= b_{n-j+i}, \qquad \text{for } 1 \le i \le m \end{aligned}$$

and 0 *otherwise. Thus,* $\mathrm{Res}(P,Q)$ *is an element of* D.

The discriminant of the polynomial $P(X)$ *as above is given by*

$$\mathrm{Disc}(P) = a_m^{2m-2} \prod_{1\le i<j\le m} (\alpha_i - \alpha_j)^2 = (-1)^{m(m-1)/2} a_m^{-1} \mathrm{Res}(P, P').$$

The discriminant $\mathrm{Disc}(P)$ *can easily be written as a determinant, it is an element of* D *and it is non-zero if and only if* $P(X)$ *is separable.*

If we have polynomials in more than one variable, we will denote the variable with respect to which the resultant is to be computed. The other variables are taken as constants during this computation. For example, for polynomials $P(X,Y), Q(X,Y) \in \mathbb{Z}[X,Y]$, the resultant $\mathrm{Res}_X(P,Q)$ will be computed exactly as in the previous lemma looking at $P(X,Y)$ and $Q(X,Y)$ as polynomials in X with coefficients in $D = \mathbb{Z}[Y]$. The same lemma then insures that $\mathrm{Res}_X(P,Q) \in \mathbb{Z}[Y]$.

The following result, known as *Hensel's Lemma* is probably the most important algebraic property of p-adic numbers. It says that one can often decide quite easily whether a polynomial has roots in $\mathbb{Z}_p$. The test involves finding an "approximate" root of the polynomial and then verifying a condition on the (formal) derivative of the polynomial [16]. We bring two versions of this result. The first one is probably best known and the second one, while more general, also shows more clearly why this is actually a p-adic analogue of Newton's approximation method from the reals.

Lemma 0.5 (Hensel's Lemma)**.** *(1) Let* $f(X) \in \mathbb{Z}_p[X]$ *be a polynomial in one variable and let* $\alpha_0 \in \mathbb{Z}_p$ *be such that*

$$f(\alpha_0) \equiv 0 \pmod{p\mathbb{Z}_p} \qquad \text{and} \qquad f'(\alpha_0) \not\equiv 0 \pmod{p\mathbb{Z}_p},$$

where $f'(X)$ *denotes the formal derivative of* $f(X)$*. Then there exists a unique* p*-adic integer* $\alpha \in \mathbb{Z}_p$ *such that* $\alpha \equiv \alpha_0 \pmod{p\mathbb{Z}_p}$ *and* $f(\alpha) = 0$.

(2) Let $f(X) \in \mathbb{Z}_p[X]$ *be a polynomial in one variable and let* $\alpha_0 \in \mathbb{Z}_p$ *be such that*

$$|f(\alpha_0)|_p < |f'(\alpha_0)^2|_p.$$

Then the sequence

$$\alpha_{i+1} = \alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)}$$

converges to a root α of $f(X)$ in $\mathbb{Z}_p$, and we have

$$|\alpha - \alpha_0|_p \leq \left| \frac{f(\alpha_0)}{f'(\alpha_0)^2} \right|_p .$$

Moreover, there is only one root α of $f(X)$ in $\mathbb{Q}_p$ which satisfies the last inequality.

Proof. See [10, §4.3] or [19, Proposition 7.6, §XII.7, p. 493] for the proof of the general form of this lemma. Statement in (1) is an easy consequence of (2). ∎

Chapter 1

Separation of complex roots for integer polynomials of small degree

1.1 Introduction

For an integer polynomial $P(x)$ of degree $d \geq 2$ and with distinct roots $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$, we set

$$\mathrm{sep}(P) := \min_{1 \leq i < j \leq d} |\alpha_i - \alpha_j|$$

and define $e(P)$ by

$$\mathrm{sep}(P) = \mathrm{H}(P)^{-e(P)}.$$

For an infinite set S of integer polynomials containing polynomials of arbitrary large height, we define

$$e(S) = \limsup_{P(x) \in S, \mathrm{H}(P) \to +\infty} e(P).$$

In this chapter we will be concerned with reducible monic polynomials of degree four with integer coefficients. Therefore, we introduce the notation $\mathcal{RM}_d$ for the set of all reducible monic polynomials of degree d with integer coefficients.

First, we briefly summarize what is known about bounds on $e(S)$ if S is some class of integer polynomials. We start with a classical result of Mahler [22].

Lemma 1.1. *Let $P(x)$ be a separable, integer polynomial of degree $n \geq 2$. For any two distinct zeros α and β of $P(x)$ we have*

$$|\alpha - \beta| > \sqrt{3}(n+1)^{-(2n+1)/2} \max\{1, |\alpha|, |\beta|\} \, \mathrm{H}(P)^{-n+1}.$$

Proof. See [7, Theorem A.3, p. 226]. ∎

This immediately implies that if S contains only polynomials of degree d, then $e(S) \leq d - 1$.

We are interested here in classes of polynomials of relatively small degree ($d \leq 4$). Therefore, in the next table we merely give the lower bounds on $e(S)$ if S is a certain class of polynomials of degree $d \geq 5$. The exact constructions of polynomial families establishing these bounds can be found in the references ([8] for classes of general irreducible polynomials and monic irreducible polynomials of odd degree $d \geq 7$, [9] for everything else).

$d \geq 5$	general	monic
irreducible	$e \geq \frac{d}{2} + \frac{d-2}{4(d-1)}$	$e \geq \frac{7}{4}$ for $d = 5$, $e \geq \frac{d}{2} + \frac{d-2}{4(d-1)} - 1$ for odd $d \geq 7$ $e \geq \frac{d-1}{2}$ for even d
reducible	$e \geq \frac{d+1}{2}$ for odd d $e \geq \frac{d}{2}$ for even d	$e \geq \frac{d-1}{2}$ for odd d $e \geq \frac{d}{2}$ for even d

We go back to polynomials of small degree. For a quadratic polynomial $P(x) = ax^2 + bx + c$, we have

$$\mathrm{sep}(P) = \Big|\frac{-b + \sqrt{b^2 - 4ac}}{2a} - \frac{-b - \sqrt{b^2 - 4ac}}{2a}\Big| = \Big|\frac{\sqrt{b^2 - 4ac}}{a}\Big|,$$

which gives upper bounds $e(S) \leq 1$ and $e(S) \leq 0$ when S is the set of all quadratic polynomials and the set of all monic quadratic polynomials, respectively. Since this case is almost trivial, we only give four families of polynomials that prove these bounds are actually attained

$$(k^2 + k - 1)x^2 + (2k + 1)x + 1, \quad x^2 + (2k + 1)x + (k^2 + k - 1),$$
$$(kx - 1)\big((k + 1)x - 1\big), \quad (x - k)(x - k + 1).$$

The next table sums up the results for $d = 2$.

$d = 2$	general	monic
irreducible	$e = 1$	$e = 0$
reducible	$e = 1$	$e = 0$

For cubic polynomials, the case of general (i.e. nonmonic) polynomials was first solved by Evertse [15] and later Schönhage [32] gave an easier constructive proof. In the monic case Bugeaud and Mignotte [9] proved the lower bound $e(\mathcal{M}_3) \geq \frac{3}{2}$, where $\mathcal{M}_3$ is the set of monic cubic polynomials with integer coefficients. They also showed that $e(\mathcal{M}_3) = \frac{3}{2}$ is equivalent to Hall's conjecture which asserts that, for any positive real number ε, we have $|x^3 - y^2| > x^{1/2-\varepsilon}$, for any suficiently large positive integers x and y with $x^3 \neq y^2$. Hall's conjecture is one of the many consequences of the *abc*-conjecture (see [30]).

Proving that $e(\mathcal{RM}_3) = 1$ is not hard when we notice that a polynomial from this set is a product of a linear and a quadratic polynomial, both monic and with integer coefficients because of Gauss's Lemma 0.1. In the next table we summarize known results for $d = 3$:

$d = 3$	general	monic
irreducible	$e = 2$	$e \geq \frac{3}{2}$
reducible	$e = 2$	$e = 1$

Until now no exact values when $d = 4$ were known, just the lower bounds given in the following table:

$d = 4$	general	monic
irreducible	$e \geq \frac{13}{6}$	$e \geq \frac{3}{2}$
reducible	$e \geq \frac{7}{3}$	$e \geq 2$

The bound for the nonmonic irreducible case arises from a general construction by Bugeaud and Dujella [8] which gives $e((\overline{P}_{4,n}(x))_{n\in\mathbb{N}}) = \frac{13}{6}$ in this special case, where

$$\overline{P}_{4,n}(x) = (20n^4 - 2)x^4 + (16n^5 + 4n)x^3 + (16n^6 + 4n^2)x^2 + 8n^3x + 1.$$

For nonmonic reducible polynomials, a recent unpublished result by Bugeaud and Dujella, shows that the sequence

$$\widetilde{P}_{4,n}(x) = \big((2n+1)x^3 + (2n-1)x^2 + (n-1)x - 1\big)\big((n^2+3n+1)x - (n+2)\big)$$

gives $e \geq e((\widetilde{P}_{4,n}(x))_{n\in\mathbb{N}}) = \frac{7}{3}$. The bound for monic irreducible polynomials $e \geq \frac{3}{2}$ is deduced by looking at the sequence

$$\widehat{P}_{4,n}(x) = (x^2 - nx + 1)^2 - 2(nx - 1)^2, \quad n \in \mathbb{N}$$

(see Bugeaud and Mignotte [9]). Finally, for reducible monic polynomials, it follows from a general case discussed in [9] that $e(\mathcal{RM}_4) \geq 2$. While

the proof from [9] is nonconstructive, in Section 1.2 we establish the same inequality by exhibiting a set $S \subseteq \mathcal{RM}_4$ such that $e(S) = 2$. In Section 1.3 we prove that $e(\mathcal{RM}_4) \leq 2$. By putting together the results from Sections 1.2 and 1.3, we obtain the main result of this chapter, which gives the first exact value in the above table for $d = 4$.

Theorem 1.1. *It holds that* $e(\mathcal{RM}_4) = 2$.

Furthermore, in Section 1.4, we show that if the coefficients of polynomials in the sequence $S = (P_n(x))_{n\in\mathbb{N}} \subseteq \mathcal{RM}_4$ grow polynomially in n, we must have a strict inequality $e(S) < 2$. But we also show that we can choose such a sequence so that $e(S)$ is arbitrarily close to 2. More precisely, we prove the following theorem.

Theorem 1.2. *If* $S = (P_n(x))_{n\in\mathbb{N}} \subseteq \mathcal{RM}_4$ *is a sequence of polynomials whose coefficients are polynomials in* n*, then* $e(S) < 2$*. For any* $\varepsilon > 0$*, there is a sequence of polynomials* $S = (P_n(x))_{n\in\mathbb{N}} \subseteq \mathcal{RM}_4$ *whose coefficients are polynomials in* n *such that* $e(S) > 2 - \varepsilon$*.*

1.2 The constructive proof of $e(\mathcal{RM}_4) \geq 2$

We want to find a sequence of polynomials $S = (P_n(x))_{n\in\mathbb{N}} \subseteq \mathcal{RM}_4$ such that $e(S) = 2$. We look at integer polynomials of the type

$$P(x) = (x^2 + rx + s)(x^2 + ax + b),$$

where r and s are fixed while a and b depend on them and on n such that one root of the polynomial in the first bracket is very close to a root of the polynomial in the second bracket.

Choose r and s such that the roots λ_1, λ_2 of the polynomial $R(x) = x^2 + rx + s \in \mathbb{Z}[x]$ satisfy $\lambda = \lambda_1 > 1 > \lambda_2 > 0$. Also, let $(a_n)_{n\in\mathbb{N}}$ be an increasing sequence of positive integers that satisfies the recurrence $a_{n+2} + ra_{n+1} + sa_n = 0$ whose characteristic polynomial is $R(x)$. Hence,

$$a_n = c_1\lambda_1^n + c_2\lambda_2^n = c_1\lambda^n + c_2\frac{s}{\lambda^n},$$

for some constants c_1, c_2.

Assume that $\lambda + \varepsilon$ is a root of the polynomial $x^2 + ax + b \in \mathbb{Z}[x]$. Then we have

$$(\lambda + \varepsilon)^2 + a(\lambda + \varepsilon) + b = 0 \qquad \text{or}$$
$$\varepsilon^2 + (2\lambda + a)\varepsilon + (a - r)\lambda + (b - s) = 0.$$

Therefore $2\varepsilon = -(2\lambda+a) \pm \sqrt{(2\lambda+a)^2 - 4\big((a-r)\lambda+(b-s)\big)}$. If we have

$$2\lambda + a > 0 \qquad \text{and} \qquad |4\big((a-r)\lambda+(b-s)\big)| < (2\lambda+a)^2, \tag{1.1}$$

then we get a smaller $|\varepsilon|$ for the $+$ sign, so

$$\begin{aligned} |2\varepsilon| &= \left| \frac{4\big((a-r)\lambda+(b-s)\big)}{-(2\lambda+a) - \sqrt{(2\lambda+a)^2 - 4\big((a-r)\lambda+(b-s)\big)}} \right| \\ &\asymp \left| \frac{(a-r)\lambda+(b-s)}{2\lambda+a} \right| \end{aligned} \tag{1.2}$$

(here $M \asymp N$ stands for $M \ll N$ and $N \ll M$, where the implicit constants depend only on r and s). At this point we see that by choosing

$$a - r = a_n, \quad r \leq -1, \quad b - s = -a_{n+1}, \quad s = 1,$$

the conditions on λ_1, λ_2, $(a_n)_{n\in\mathbb{N}}$ and inequalities (1.1) are fulfilled, while from (1.2) we have

$$\begin{aligned} \operatorname{sep}(P_n) = |\varepsilon| \asymp \left| \frac{a_n\lambda - a_{n+1}}{2\lambda + a_n + r} \right| &= \left| \frac{c_1\lambda^{n+1} + \frac{c_2}{\lambda^{n-1}} - c_1\lambda^{n+1} - \frac{c_2}{\lambda^{n+1}}}{2\lambda + c_1\lambda^n + \frac{c_2}{\lambda^n} + r} \right| \\ &\asymp \frac{1}{\lambda^{2n}} \asymp \max\{1, |a|, |b|\}^{-2} \asymp \mathrm{H}(P_n)^{-2} \end{aligned}$$

and thus

$$e((P_n)_{n\in\mathbb{N}}) = 2,$$

where

$$P_n(x) = (x^2 + rx + 1)\big(x^2 + (r + a_n)x + (1 - a_{n+1})\big).$$

This shows that $e(\mathcal{RM}_4) \geq 2$.

Note that we could have taken $s = -1$ before and if we were trying to approach the smaller root i.e. λ_2, we would get a similar family of polynomials

$$P_n(x) = (x^2 + rx - 1)\big(x^2 + (r - a_{n+1})x - (a_n + 1)\big),$$

and after substitution $x \mapsto -x$, we would get

$$P_n(x) = (x^2 - rx - 1)\big(x^2 + (-r + a_{n+1})x - (a_n + 1)\big).$$

In case of $a_1 = 1$, $a_2 = 1$, $r = -1$, the above polynomial is

$$P_n(x) = (x^2 + x - 1)\big(x^2 + (1 + F_{n+1})x - (F_n + 1)\big)$$

where $(F_n)_{n\in\mathbb{N}}$ is the Fibonacci sequence. This last sequence of polynomials, which was first obtained by numerical experiments, was the motivating factor for this study.

1.3 The proof of $e(\mathcal{RM}_4) \le 2$

Let us prove that $e(\mathcal{RM}_4) \le 2$. In other words, the best separation of roots we can get in the case of a *reducible* separable monic quartic polynomial $P(x) \in \mathbb{Z}[x]$ is $\asymp \mathrm{H}(P)^{-2}$. (All the constants implied in $\asymp, \ll, \gg$ in this section are absolute.)

We have to look at two cases: when the polynomial has a cubic irreducible factor and when the polynomial has a quadratic irreducible factor. Because of Gauss's Lemma 0.1 all the monic divisors in $\mathbb{Q}[x]$ of $P(x)$ will actually be from $\mathbb{Z}[x]$. Therefore, the case when $P(x)$ is a product of linear factors is trivial.

If we have $P(x) = (x-k)(x^3+ax^2+bx+c)$, where $a,b,c,k \in \mathbb{Z}$, then by the result of Mahler we know that the roots of $Q(x) = x^3+ax^2+bx+c$ can be no closer than $\asymp (\max\{1,|a|,|b|,|c|\})^{-2}$. Because of Gelfond's Lemma 0.2, we have

$$\frac{1}{16}\max\{1,|k|\}\max\{1,|a|,|b|,|c|\} \le \mathrm{H}(P) \le 16\max\{1,|k|\}\max\{1,|a|,|b|,|c|\}, \quad (1.3)$$

so $\mathrm{sep}(Q) \gg \mathrm{H}(P)^{-2}$. There only remains to check whether we can have a root of $Q(x)$ close to k. Let us take $Q(k+\varepsilon) = (k+\varepsilon)^3+a(k+\varepsilon)^2+b(k+\varepsilon)+c = 0$ where without loss of generality we can suppose $|\varepsilon| < 1$. It is obvious that $|k+\varepsilon| < |a|+|b|+|c|+1$ must hold, otherwise we get a contradiction. Thus, from (1.3) we get $|k| \ll \mathrm{H}(P)^{1/2}$. Since $P(x)$ does not have multiple roots and $Q(x) \in \mathbb{Z}[x]$ we have

$$1 \le |Q(k)| = |Q(k+\varepsilon) - Q(k)| = |Q'(t)| \cdot |\varepsilon|,$$

where $t \in (k, k+\varepsilon) \subset (k-1, k+1)$. But, using (1.3) and $|k| \ll \mathrm{H}(P)^{1/2}$, we get

$$|Q'(t)| = |3t^2+2at+b| \le 3(|k|+1)^2 + 2|a|(|k|+1) + |b| \ll \mathrm{H}(P).$$

Finally, we arrive at $|\varepsilon| \ge 1/|Q'(t)| \gg \mathrm{H}(P)^{-1}$.

If $P(x) = Q_1(x)Q_2(x)$, where $Q_1(x), Q_2(x) \in \mathbb{Z}[x]$ are two quadratic polynomials, then we have from Gelfond's Lemma 0.2

$$\frac{1}{16}\mathrm{H}(Q_1)\,\mathrm{H}(Q_2) \le \mathrm{H}(P) \le 16\,\mathrm{H}(Q_1)\,\mathrm{H}(Q_2). \quad (1.4)$$

Since for quadratic polynomials we have $\mathrm{sep}(Q_i) \gg H(Q_i)^{-1}$, we only have to check the proximity of the roots α and β of $Q_1(x)$ and $Q_2(x)$, respectively.

Theorem A.1 from [7, p. 223] states that in our separable case

$$|\alpha - \beta| \geq 2^{-1}3^{-5/2} \cdot \mathrm{H}(Q_1)^{-2}\,\mathrm{H}(Q_2)^{-2} \cdot \max\{1, |\alpha|\}\max\{1, |\beta|\} \gg \mathrm{H}(P)^{-2}.$$

Hence, we proved that $e(\mathcal{RM}_4) \leq 2$, which concludes the proof of Theorem 1.1.

1.4 Polynomial growth of coefficients

In Section 1.2 we exhibited a family of reducible monic polynomials $P_n(x)$ whose coefficients grow exponentially in n such that $\mathrm{sep}(P_n) \asymp \mathrm{H}(P_n)^{-2}$.

We will show that this is not possible if the coefficients grow polynomially. More precisely, let $P_n(x) = P(n, x) \in \mathbb{Z}[n, x]$ be a polynomial which is monic of degree 4 in x and such that for every positive integer n', polynomial $P_{n'}(x) \in \mathbb{Z}[x]$ is reducible. This is the exact meaning of the conditions in the first statement of Theorem 1.2. Now we will need a quantitative version of Hilbert's Irreducibility Theorem. Hilbert's Irreducibility Theorem roughly asserts that for polynomials in several variables irreducible over the rational field, there always exist rational specializations of some of the variables which preserve irreducibility [34]. Stating precisely, we will use the following theorem proved by Dörge [12].

Theorem H-D. *If $f(x_1, \ldots, x_k, t)$ is an irreducible polynomial with integral coefficients and if $R(N)$ is the number of integers τ such that $|\tau| < N$ and $f(x_1, \ldots, x_k, \tau)$ is reducible, then $R(N) \leq CN^{1-\alpha}$ where α, C are certain positive constants.*

Note that an earlier result by Skolem [33] giving $\lim_{N\to\infty} R(N)/N = 0$ would be sufficient for our purposes. Together with our assumption on reducibility this easily implies that

$$P_n(x) = Q_{n,1}(x)Q_{n,2}(x),$$

where $Q_{n,1}(x)$ and $Q_{n,2}(x)$ are monic polynomials in x whose coefficients are integer polynomials in n. Note that because of the result in the previous section, the case of a reducible monic polynomial with a linear factor is not very interesting. Therefore, we will assume that $Q_{n,1}(x)$ and $Q_{n,2}(x)$ are irreducible quadratic polynomials in x without common roots, so we may write

$$Q_{n,1}(x) = x^2 + r(n)x + s(n), \quad Q_{n,2}(x) = x^2 + a(n)x + b(n),$$

where $r(n), s(n), a(n), b(n) \in \mathbb{Z}[n]$. For the sake of simplicity, we will usually omit n. As already mentioned, we can assume that the closest roots of P are a root of Q_1 and a root of Q_2. So, without loss of generality, let us take

$$2\,\mathrm{sep}(P) = 2\varepsilon = -r + \sqrt{r^2 - 4s} + a + \sqrt{a^2 - 4b}.$$

After some manipulation we get that ε satisfies the following equality

$$\begin{aligned}\varepsilon^4 - 2(a-r)\varepsilon^3 + (r^2 + a^2 - 3ra + 2s + 2b)\varepsilon^2 \\ - (a-r)(-ra + 2s + 2b)\varepsilon + (s^2 + b^2 - rsa - rab - 2bs + sa^2 + br^2) = 0.\end{aligned} \tag{1.5}$$

Notice that the last term is just the resultant $\mathrm{Res}_x(Q_1, Q_2)$ of the polynomials Q_1 and Q_2:

$$\mathrm{Res}(Q_1, Q_2) = \mathrm{Res}(Q_1, Q_2 - Q_1) = (b-s)^2 + (a-r)(as - br).$$

Let us suppose that $\varepsilon \ll \mathrm{H}^{-2}$, where by Gelfond's Lemma 0.2, $\mathrm{H} = \mathrm{H}(P) \asymp \mathrm{H}(Q_1)\,\mathrm{H}(Q_2)$. We mention here that all the constants in $\mathcal{O}$, $\ll$, $\gg$, $\asymp$ in the first part of this section depend at most on the coefficients of r, s, a, b. Since $P(x)$ is a separable integer polynomial, it follows that $\mathrm{Res}(Q_1, Q_2)$ is an integer polynomial in n and $|\,\mathrm{Res}(Q_1, Q_2)| \geq 1$. Now we get from (1.5) and (1.4) that

$$\mathrm{H}^{-2} \gg \varepsilon \gg \frac{|\,\mathrm{Res}(Q_1, Q_2)|}{|\underbrace{\varepsilon^3}_{\mathcal{O}(\mathrm{H}^{-6})} \underbrace{-2(a-r)\varepsilon^2}_{\mathcal{O}(\mathrm{H}^{-3})} + \underbrace{(\underbrace{r^2 + a^2}_{\mathcal{O}(\mathrm{H}^2)} \underbrace{- 3ra + 2s + 2b}_{\mathcal{O}(\mathrm{H})})\varepsilon - (a-r)(-ra + 2s + 2b)}_{\mathcal{O}(1)}|}$$

and

$$\mathrm{H}^{-2} \gg \varepsilon \gg \frac{|\,\mathrm{Res}(Q_1, Q_2)|}{|\mathcal{O}(1) - \underbrace{2as + 2rb}_{\mathcal{O}(\mathrm{H})} + ra^2 - r^2 a + 2rs - 2ab|}. \tag{1.6}$$

Because of Gelfond's Lemma 0.2, $|r|, |s|, |a|, |b| \ll \mathrm{H}$ and $|ar| \ll \mathrm{H}$ which implies that $|a| \ll \mathrm{H}^{1/2}$ or $|r| \ll \mathrm{H}^{1/2}$. Without loss of generality we can suppose that $|a| \ll \mathrm{H}^{1/2}$. Thus we get $|ra^2| = |ra| \cdot |a| \ll \mathrm{H}^{3/2}$ and $|ab| = |a| \cdot |b| \ll \mathrm{H}^{3/2}$. We also have $|-r^2 a + 2rs| = |r| \cdot |ra - 2s| = |r|\mathcal{O}(\mathrm{H})$ so the inequality (1.6) becomes

$$\mathrm{H}^{-2} \gg \varepsilon \gg \frac{1}{\max\{\mathcal{O}(\mathrm{H}^{3/2}), |r|\mathcal{O}(\mathrm{H})\}}.$$

It implies that $|r| \gg \mathrm{H}$, so from $|r| \ll \mathrm{H}$, we get $|r| \asymp \mathrm{H}$. Also, we obtain $|\operatorname{Res}(Q_1, Q_2)| = \mathcal{O}(1)$. Since r, s, a, b are polynomials in n and $|ra| \ll \mathrm{H}$, $|rb| \ll \mathrm{H}$, we conclude that a and b are constants.

If we now have $\deg_n s < \deg_n r$, then

$$\deg_n \operatorname{Res}(Q_1, Q_2) = \deg_n \big((b-s)^2 + (a-r)(as-br)\big) \geq \deg_n r + \deg_n s,$$

so $|\operatorname{Res}(Q_1, Q_2)| \gg \mathrm{H}$, which leads to a contradiction. Therefore, $\deg_n s = \deg_n r$ and hence $|s| \asymp |r| \asymp \mathrm{H} \to \infty$.

The leading coefficient of $\operatorname{Res}(Q_1, Q_2)$ as a polynomial in n, i.e. the coefficient that belongs to the monomial of degree $2\deg_n r = 2\deg_n s$, is the leading coefficient of $s^2 - ars + br^2$, i.e. $k_s^2 - ak_rk_s + bk_r^2$, where k_s, k_r are leading coefficients of s and r, respectively. If it were 0, then $-k_s/k_r \in \mathbb{Q}$ would be a root of $x^2 + ax + b$ which is impossible, since by our assumption this polynomial is irreducible. Thus $\deg_n \operatorname{Res}(Q_1, Q_2) = 2\deg_n r \geq 2$ and this is in contradiction with the condition $|\operatorname{Res}(Q_1, Q_2)| = \mathcal{O}(1)$.

We conclude that $\operatorname{sep}(P_n) \ll \mathrm{H}(P_n)^{-2}$ cannot hold in this case, and this proves the first statement of Theorem 1.2.

Although the previous result of this section shows that we cannot have a family of reducible monic quartic integer polynomials with polynomial growth of coefficients that has the best possible exponent for root separation in this case, i.e. -2, we can still construct families with the exponent as close to -2 as we like. The construction that follows is similar to the one in Section 1.2.

We look at the family of polynomials $P_{k,n}(x)$ indexed with $n \in \mathbb{N}$ in variable x. As before, we will usually omit n and write simply $P_k(x)$. We define

$$\begin{aligned} P_k(x) &= \underbrace{(x^2 + nx + 1)}_{Q_k(x)} \underbrace{(x^2 + nx + 1 + A_{k+1}x + A_k)}_{R_k(x)} \\ &= (x^2 + \underbrace{n}_{r} x + \underbrace{1}_{s})\big(x^2 + \underbrace{(A_{k+1} + n)}_{a} x + \underbrace{(A_k + 1)}_{b}\big), \end{aligned}$$

where $\big(A_k(n)\big)_{k \in \mathbb{N}_0}$ is defined recursively by

$$A_0(n) = 1,\ A_1(n) = n, \quad A_{k+1}(n) = nA_k(n) - A_{k-1}(n) \text{ for } n \geq 2.$$

It is easy to see that $\deg_n A_k = k$, so we get (implied constants are absolute from now on)

$$\mathrm{H}(P_k) \asymp n^{k+2}.$$

Let us look at the resultant:

$$\begin{aligned}\mathrm{Res}_x(Q_k,R_k) &= (b-s)^2 - r(b-s)(a-r) + s(a-r)^2\\ &= A_k^2 - nA_kA_{k+1} + A_{k+1}^2\\ &= A_k^2 + A_{k+1}(A_{k+1} - nA_k)\\ &= A_k^2 - A_{k+1}A_{k-1}\\ &= A_k^2 - (nA_k - A_{k-1})A_{k-1}\\ &= A_k(A_k - nA_{k-1}) + A_{k-1}^2\\ &= A_{k-1}^2 - A_kA_{k-2}\\ &= \ldots = A_1^2 - A_2A_0 = n^2 - (n^2-1)\cdot 1 = 1.\end{aligned} \tag{1.7}$$

The roots of $Q_k(x)$ are

$$\alpha_1 = \frac{-n-\sqrt{n^2-4}}{2}, \quad \alpha_2 = \frac{-n+\sqrt{n^2-4}}{2},$$

and the roots of $R_k(x)$ are

$$\begin{aligned}\beta_1 &= \frac{-(A_{k+1}+n) - \sqrt{(A_{k+1}+n)^2 - 4(A_k+1)}}{2},\\ \beta_2 &= \frac{-(A_{k+1}+n) + \sqrt{(A_{k+1}+n)^2 - 4(A_k+1)}}{2}.\end{aligned}$$

Therefore,

$$\alpha_1 \asymp -n, \quad \alpha_2 \asymp -\frac{1}{n}, \qquad \beta_1 \asymp -n^{k+1}, \quad \beta_2 = \frac{A_k+1}{\beta_1} \asymp \frac{-1}{n},$$

so we have

$$1 = \mathrm{Res}(Q_k,R_k) = 1^2 1^2 \underbrace{|\alpha_1-\beta_2|}_{\asymp n} \underbrace{|\alpha_1-\beta_1|}_{\asymp n^{k+1}} \underbrace{|\alpha_2-\beta_1|}_{\asymp n^{k+1}} \mathrm{sep}(P_k),$$

and it follows that

$$\mathrm{sep}(P_k) \asymp n^{-2k-3} = n^{-2(k+2)}n \asymp \mathrm{H}(P_k)^{-2+\frac{1}{k+2}}.$$

Hence, we proved the last statement of Theorem 1.2.

Chapter 2

General results on polynomials in the p-adic setting

This chapter brings together results of a general nature on polynomials in the p-adic setting. These are for the most part analogues of the results in the real and complex case. In this way we streamline the proof of our main results and avoid unnecessary repetition. However, some lemmas on polynomials which are specific to the subject of a particular chapter are left there.

The first two lemmas give bounds on the size of roots and products of roots of a polynomial.

Lemma 2.1. *If $\alpha \in \mathbb{C}_p$ is a root of the polynomial $P(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}_p[X]$, then $|a_0|_p \leq |\alpha|_p \leq 1/|a_n|_p$.*

Proof. If $\alpha = 0$, then both inequalities obviously hold. Therefore, we assume $\alpha \neq 0$. From $P(\alpha) = 0$ we get

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

If $|\alpha|_p \leq 1$ this implies $|a_0 \alpha^{-1}|_p \leq 1$. If $|\alpha|_p > 1$, $|a_0 \alpha^{-1}|_p \leq 1$ obviously holds. Either way, we get $|a_0|_p \leq |\alpha|_p$ and the other inequality follows from this one by noting that $1/\alpha$ is a root of the polynomial $X^n P(1/X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n$. ∎

Lemma 2.2. *Let $P(X) = a_n X^n + \cdots + a_1 X + a_0 = a_n (X - \alpha_1) \cdots (X - \alpha_n) \in \mathbb{C}_p[X]$. Then for any set $I \subseteq \{1, \ldots, n\}$, it holds*

$$\prod_{i \in I} |\alpha_i|_p \leq \frac{\max_{j \in \{0,1,\ldots,n\}} |a_j|_p}{|a_n|_p}.$$

Proof. This is shown in [24, p. 341]. ∎

As an analogue of Lemma 1.1 proved by Mahler for complex roots, we prove a lower bound on the distance of two roots in the p-adic case. Just as in the complex case, for a polynomial $P(x)$ of degree $d \geq 2$ and with distinct roots $\alpha_1, \ldots, \alpha_d \in \mathbb{C}_p$, we set

$$\operatorname{sep}_p(P) := \min_{1 \leq i < j \leq d} |\alpha_i - \alpha_j|_p.$$

Lemma 2.3. *Let $P(X)$ be a separable, integer polynomial of degree $n \geq 2$. For any two distinct zeros $\alpha, \beta \in \mathbb{C}_p$ of $P(X)$, we have*

$$|\alpha - \beta|_p \geq \operatorname{sep}_p(P) \geq n^{-\frac{3}{2}n} \operatorname{H}(P)^{-n+1}.$$

First proof. First part of this proof has been done by Morrison (cf. [24]). If no two roots of the polynomial

$$P(X) = a_n(X-\alpha_1)\cdots(X-\alpha_n) = a_nX^n+\cdots+a_1X+a_0, \quad \alpha_i \in \mathbb{C}_p\,(1 \leq i \leq n)$$

are equal we look at the polynomial

$$Q(X) = \prod_{1 \leq i < j \leq n} \big(X - (\alpha_i - \alpha_j)^2\big).$$

The coefficients of Q are symmetric polynomials with integer coefficients in $\alpha_1, \ldots, \alpha_n$ and therefore integer polynomials in elementary symmetric polynomials in $\alpha_1, \ldots, \alpha_n$, that is, by Viète's formulas, in $\frac{a_0}{a_n}, \ldots, \frac{a_{n-1}}{a_n}$ and it is easy to see that their degree in α_i is at most $2(n-1)$ and since each of $\frac{a_0}{a_n}, \ldots, \frac{a_{n-1}}{a_n}$ is of degree 1 in α_i, we get that

$$a_n^{2n-2}Q(X) \in \mathbb{Z}[a_0, \ldots, a_{n-1}, a_n][X] \subset \mathbb{Z}[X].$$

According to Lemma 2.1, we now know that

$$|(\alpha_i - \alpha_j)^2|_p \geq |\text{constant term of } a_n^{2n-2}Q(X)|_p$$

and since

$$|\text{constant term of } a_n^{2n-2}Q(X)| = |a_n^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2| = |\operatorname{Disc}(P)|$$

we are left to bound

$$
\begin{aligned}
|\operatorname{Disc}(P)| &= \left|\frac{1}{a_n}(-1)^{\frac{n(n-1)}{2}}\operatorname{Res}(P,P')\right| \\
&= \frac{1}{|a_n|}|\det\begin{bmatrix} a_n & \cdots & a_0 & & \\ & \ddots & & \ddots & \\ & & a_n & \cdots & a_0 \\ na_n & \cdots & a_1 & & \\ & \ddots & & \ddots & \\ & & na_n & \cdots & a_1 \end{bmatrix}| = |\det\begin{bmatrix} 1 & \cdots & a_0 & & \\ & \ddots & & \ddots & \\ & & a_n & \cdots & a_0 \\ n & \cdots & a_1 & & \\ & \ddots & & \ddots & \\ & & na_n & \cdots & a_1 \end{bmatrix}| \\
&\leq (n+1)^{n-1}n^n \cdot n^n \operatorname{H}(P)^{2n-2} \leq n^{3n}\operatorname{H}(P)^{2n-2}.
\end{aligned} \tag{2.1}
$$

Finally, it follows that, $\operatorname{sep}_p(P) \geq n^{-\frac{3}{2}n}\operatorname{H}(P)^{-n+1}$. ∎

Second proof. We briefly sketch an alternative proof of this lemma. Instead of using Morrison's construction of the polynomial $Q(X)$ from the first part of the proof we just showed, we use the procedure similar to what Mahler employed in his proof of the complex numbers analogue of this result (cf. [7, Theorem A.3]). Namely,

$$
\begin{aligned}
|\operatorname{Disc}(P)|_p &= |a_n^{2n-2}|_p \prod_{1\leq i<j\leq n} |\alpha_i - \alpha_j|_p^2 \\
&\leq |\alpha_1-\alpha_2|_p^2 |a_n|_p^{2n-2} \prod_{\substack{1\leq i<j\leq n \\ (i,j)\neq(1,2)}} \big(\max\{1,|\alpha_i|_p\}\max\{1,|\alpha_j|_p\}\big)^2 \\
&\leq |\alpha_1-\alpha_2|_p^2 \big(|a_n|_p \prod_{1\leq i\leq n}\max\{1,|\alpha_i|\}\big)^{2n-2} \\
&\leq |\alpha_1-\alpha_2|_p^2 \big(\max_{0\leq i\leq n}|a_i|_p\big)^{2n-2} \\
&\leq |\alpha_1-\alpha_2|_p^2,
\end{aligned}
$$

where we used Lemma 2.2 in order to get to the penultimate line.

Combined with the upper bound (2.1) on $|\operatorname{Disc}(P)|$ from the first proof and inequality

$$\frac{1}{|\operatorname{Disc}(P)|} \leq |\operatorname{Disc}(P)|_p,$$

we get another proof of Lemma 2.3. ∎

The following lemma compares the value of an integer polynomial at some number with the distance of this number from the roots of the polynomial.

Lemma 2.4. *Let $P(X)$ be a non-constant, separable, integer polynomial of degree n. Let $\xi \in \mathbb{C}_p$ and α be a root of $P(X)$ in $\mathbb{C}_p$ such that $|\xi - \alpha|_p$ is minimal. Then*

$$n^{-3n/2}\,\mathrm{H}(P)^{-n+1}|\xi-\alpha|_p \le |P(\xi)|_p.$$

Proof. (cf. [7, Lemma A.8, p. 231]) Let $P(X) = a_nX^n + \cdots + a_1X + a_0 = a_n(X-\alpha_1)\cdots(X-\alpha_n) \in \mathbb{Z}[X]$, where we order the roots $\alpha_1, \ldots, \alpha_n \in \mathbb{C}_p$ in such a way that

$$\alpha = \alpha_1 \quad \text{and} \quad |\xi-\alpha_1|_p \le \cdots \le |\xi-\alpha_n|_p.$$

First we bound the discriminant of $P(X)$ as in (2.1)

$$|\operatorname{Disc}(P)| \le n^{3n}\,\mathrm{H}(P)^{2n-2}.$$

Now we have,

$$n^{-3n/2}\,\mathrm{H}(P)^{-n+1} \le \sqrt{|\operatorname{Disc}(P)|_p} = |a_n|_p|\alpha_1-\alpha_2|_p\cdots|\alpha_1-\alpha_n|_p\sqrt{|\operatorname{Disc}(Q)|_p},$$

where $Q(X) = a_n(X-\alpha_2)\cdots(X-\alpha_n)$. Applying Lemma 2.2 to the integer polynomial $P(X)$, we get the last bound below

$$\begin{aligned}\sqrt{|\operatorname{Disc}(Q)|_p} &= |a_n|_p^{n-2}\cdot\left|\begin{vmatrix}\alpha_2^0 & \cdots & \alpha_2^{n-2}\\ \vdots & \ddots & \vdots\\ \alpha_n^0 & \cdots & \alpha_n^{n-2}\end{vmatrix}\right|_p\\ &\le |a_n|_p^{n-2}\prod_{2\le i\le n}\max\{1,|\alpha_i|_p\}^{n-2} \le 1.\end{aligned}$$

Using $|\xi-\alpha_1|_p \le \cdots \le |\xi-\alpha_n|_p$, we get for $1 \le i < j \le n$

$$|\alpha_i-\alpha_j|_p \le \max\{|\xi-\alpha_i|_p, |\xi-\alpha_j|_p\} = |\xi-\alpha_j|_p$$

which combined with the previous bound gives

$$\begin{aligned}n^{-3n/2}\,\mathrm{H}(P)^{-n+1} &\le |a_n|_p|\xi-\alpha_2|_p\cdots|\xi-\alpha_n|_p,\\ n^{-3n/2}\,\mathrm{H}(P)^{-n+1}|\xi-\alpha|_p &\le |P(\xi)|_p.\end{aligned}$$

■

Next lemma gives a useful lower estimate for the distance between two distinct algebraic numbers.

Lemma 2.5. *Let α and β be distinct algebraic numbers in $\mathbb{C}_p$ of degree at most m and n, respectively. Then there exists a positive constant $c(m,n) < 1$, depending only on m and n, such that*

$$|\alpha-\beta|_p \ge c(m,n)\,\mathrm{H}(\alpha)^{-n}\,\mathrm{H}(\beta)^{-m}.$$

An admissible value for $c(m,n)$ is $(m+1)^{-n}(n+1)^{-m}$.

Proof. If α and β are conjugate over $\mathbb{Q}$, let their minimal polynomial over $\mathbb{Z}$ be $P(X) = a_k(X-\alpha_1)\cdots(X-\alpha_k)$, where $\alpha_1 = \alpha$, $\alpha_2 = \beta$. Thus, $\mathrm{H}(\alpha) = \mathrm{H}(\beta) = \mathrm{H}(P)$ and $k \le \min\{m,n\}$. We are now in the situation of Lemma 2.3 and so

$$|\alpha-\beta|_p \ge k^{-3k/2}\,\mathrm{H}(P)^{-k+1} \ge (m+1)^{-n}(n+1)^{-m}\,\mathrm{H}(\alpha)^{-n}\,\mathrm{H}(\beta)^{-m}.$$

Next, we assume that numbers α and β are not conjugate over $\mathbb{Q}$. Suppose that α and β are algebraic numbers of degree exactly m and n, respectively. Let

$$\begin{aligned} P(X) &= a_m(X-\alpha_1)\cdots(X-\alpha_m) = a_mX^m+\cdots+a_1X+a_0 \quad \text{and}\\ Q(X) &= b_n(X-\beta_1)\cdots(X-\beta_n) = b_nX^n+\cdots+b_1X+b_0 \end{aligned}$$

be the minimal polynomials of $\alpha=\alpha_1$ and $\beta=\beta_1$ over $\mathbb{Z}$. Then the resultant $\mathrm{Res}(P,Q)$ is a non-zero integer and it can be bounded from above:

$$\begin{aligned} |\,\mathrm{Res}(P,Q)| &= |\det \begin{bmatrix} a_m & \cdots & a_0 & & \\ & \ddots & & \ddots & \\ & & a_m & \cdots & a_0 \\ b_n & \cdots & b_0 & & \\ & \ddots & & \ddots & \\ & & b_n & \cdots & b_0 \end{bmatrix}| \\ &\le (m+1)^n(n+1)^m\,\mathrm{H}(P)^n\,\mathrm{H}(Q)^m \\ &= (m+1)^n(n+1)^m\,\mathrm{H}(\alpha)^n\,\mathrm{H}(\beta)^m. \end{aligned}$$

On the other hand, from the definition of $\mathrm{Res}(P,Q)$ we get

$$\begin{aligned} |\,\mathrm{Res}(P,Q)|_p &= |b_n|_p^m \prod_{1\le j\le n} |P(\beta_j)|_p \\ &\le |b_n|_p^m |P(\beta)|_p \prod_{2\le j\le n} \big(\max_{0\le i\le m} |a_i|_p (\max\{1,|\beta_j|_p\})^m\big) \\ &\le |b_n|_p^m |a_m|_p |\beta-\alpha|_p \prod_{2\le i\le m} |\beta-\alpha_i|_p \prod_{2\le j\le n} (\max\{1,|\beta_j|_p\})^m \\ &\le |b_n|_p^m |a_m|_p |\beta-\alpha|_p \prod_{2\le i\le m} (\max\{1,|\alpha_i|_p\}\max\{1,|\beta|_p\}) \prod_{2\le j\le n} (\max\{1,|\beta_j|_p\})^m \\ &\le |\beta-\alpha|_p\big(|a_m|_p \prod_{2\le i\le m} \max\{1,|\alpha_i|_p\}\big)\big(|b_n|_p \prod_{1\le j\le n} \max\{1,|\beta_j|_p\}\big)^m. \end{aligned}$$

Lemma 2.2 together with the already used fact that all the coefficients of the polynomials $P(X)$ and $Q(X)$ are integers implies that both brackets above are ≤ 1. Thus

$$|\beta-\alpha|_p \geq |\operatorname{Res}(P,Q)|_p \geq \frac{1}{|\operatorname{Res}(P,Q)|} \geq (m+1)^{-n}(n+1)^{-m}\,\mathrm{H}(\alpha)^{-n}\,\mathrm{H}(\beta)^{-m}.$$

We immediately see that if the degrees of α and β are smaller than m and n, the same inequality holds a fortiori.

After covering both cases, this lemma is proved. ∎

Chapter 3

On separation of roots in the p-adic case

3.1 General degree

Lemma 2.3 shows that for an integer polynomial $P(X)$ of degree $\leq n$, the distance between two of its roots in $\mathbb{C}_p$ is always $\gg \mathrm{H}(P)^{-n+1}$, where the implicit constant depends only on n. In the first part of this chapter we give explicit families of integer polynomials of general degree with close roots in $\mathbb{C}_p$. The second part deals with quadratic and especially cubic polynomials with close roots.

One usual idea for construction of such polynomials is to take an already known family $(P_k(X))_{k\geq 1}$ of polynomials whose coefficients are polynomials in the indexing variable k, substitute k with $1/p^k$ in $P_k(X)$ and then multiply this polynomial with a sufficiently high power of p^k so that the resulting polynomial has integer coefficients. While the starting polynomial had relatively small discriminant, we arrive at a polynomial whose discriminant is a rational integer divisible by a large power of p and from Lemma 0.4 we expect that such a polynomial has close roots in $\mathbb{C}_p$. In order to find out how small sep_p really is, we use the so called Newton polygons. We briefly explain some basic facts on this concept adopting the exposition from [16] while more properties together with proofs can be found e.g. in [16, §6.4] or [17, §IV.3].

Let $P(X) \in \mathbb{C}_p[X]$ be a polynomial. Since we are interested in understanding zeros of $P(X)$, we may factor out the highest power of X which divides $P(X)$. In other words, we may assume that $P(0) \neq 0$ and after dividing by $P(0)$, we may also assume that $P(0) = 1$. Thus, we take a

polynomial

$$P(X) = 1 + a_1X + a_2X^2 + \cdots + a_nX^n$$

with $a_i \in \mathbb{C}_p$. In the Cartesian coordinate plane we plot the points $(0, 0)$ and, for each i between 1 and n, $(i, v_p(a_i))$, where $v_p(x) = -\log_p(|x|_p)$ is the usual p-adic valuation. If $a_i = 0$ for some i, we take $v_p(a_i)$ to be $+\infty$ and think of the corresponding point as "infinitely high". In practice, we just ignore that value of i. The polygon we want to consider is the lower boundary of the convex hull of this set of points. We can also think of it this way:

i) Start with the vertical half-line which is the negative part of y-axis.

ii) Rotate that line counter-clockwise until it hits one of the points we have plotted.

iii) "Break" the line at that point, and continue rotating the remaining part until another point is hit.

iv) Continue until all the points have either been hit or lie strictly above a portion of the polygon. Cut off the polygon at its last vertex.

The resulting polygon is called *Newton polygon* of the polynomial $P(X)$ with respect to p. Since we always fix the prime p, we will usually not make a reference to it. We will be interested in the following information from this polygon:

i) the slopes of the line segments appearing in the polygon;

ii) the "length" of each slope, meaning the length of the projection of the corresponding segment on the x-axis;

iii) the "breaks", i.e. the values of i such that the point $(i, v_p(a_i))$ is a vertex of the polygon.

To illustrate these concepts, we take $p = 3$ and consider the polynomial

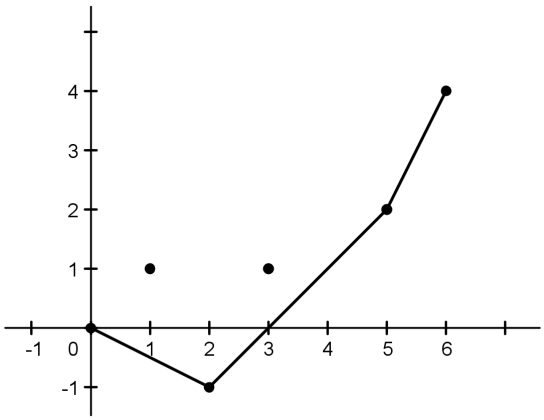
$$P(X) = 1 + 6X + \frac{1}{3}X^2 + 15X^3 + 63X^5 + 81X^6.$$

The points we work with are

$$(0, 0),\ (1, 1),\ (2, -1),\ (3, 1),\ (5, 2),\ (6, 4).$$

Plotting these points and applying the process with the rotating line gives the next figure.

Here are the properties of Newton polygon we will be using (cf. [16, Theorem 6.4.7]).



Lemma 3.1. *Let $P(X) = 1 + a_1X + a_2X^2 + \cdots + a_nX^n \in \mathbb{C}_p[X]$ be a polynomial, and let $m_1, m_2, \ldots, m_r$ be the slopes of its Newton polygon in increasing order. Let $i_1, i_2, \ldots, i_r$ be the corresponding lengths. Then, for each k, $1 \le k \le r$, $P(X)$ has exactly i_k roots in $\mathbb{C}_p$ (counting multiplicities) of p-adic absolute value p^{m_k}.*

Thus, the polynomial from our example above has in $\mathbb{C}_3$ two roots of absolute value $1/\sqrt{3}$, three roots of absolute value 3 and one root of absolute value 9.

Getting back to our subject, here are some examples of polynomials with small root separation. Note that the first two families are reducible, while the other two are irreducible according to Eisenstein's criterion.

If we take $P(X) = \begin{cases} (X-p^k)(X^{n-1}-X+p^k) \\ (X-p^k)(p^kX^{n-1}-X+p^k) \\ X^n - 2(X-p^k)^2 \\ p^{2k}X^n - 2(X-p^k)^2 \end{cases}$, $k \ge 1$,

we get $\mathrm{sep}_p(P) \ll \begin{cases} \mathrm{H}(P)^{-\frac{n-1}{2}} \\ \mathrm{H}(P)^{-\frac{n}{2}} \\ \mathrm{H}(P)^{-\frac{n}{4}} \\ \mathrm{H}(P)^{-\frac{n}{4}-\frac{1}{2}} \end{cases}$. Let us show how to arrive at these results.

$$\boxed{P(X) = (X-p^k)(X^{n-1}-X+p^k)}$$

One root of $P(X)$ is p^k, let another one, closest to p^k, be $p^k + \varepsilon \in \mathbb{C}_p$. Then

$$P(p^k+\varepsilon) = \varepsilon\big((p^k+\varepsilon)^{n-1} - (p^k+\varepsilon) + p^k\big) = 0,$$

and since $\varepsilon \neq 0$, we get $(p^k+\varepsilon)^{n-1} - \varepsilon = 0$. Let us look at the polynomial

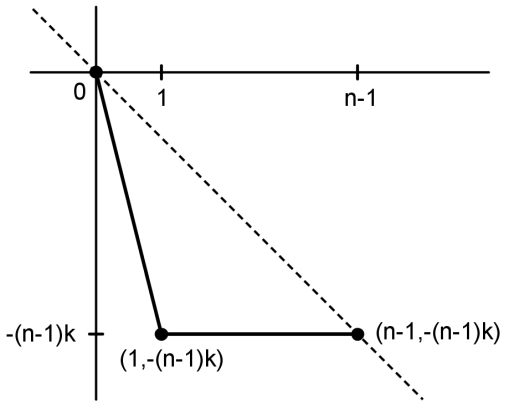
$$\begin{aligned} Q(X) &= \frac{(p^k+X)^{n-1} - X}{p^{(n-1)k}} \\ &= 1 + \frac{(n-1)p^{(n-2)k} - 1}{p^{(n-1)k}} X + \frac{(n-1)(n-2)}{2} \cdot \frac{1}{p^{2k}} X^2 + \cdots + \frac{1}{p^{(n-1)k}} X^{n-1} \\ &= 1 + \sum_{i=1}^{n-1} a_i X^i. \end{aligned}$$

If we now look at the Newton polygon of $Q(X)$, we are interested in the points

$$(0,0),\ (1, v_p(a_1)),\ (2, v_p(a_2)),\ \ldots,\ (n-1, v_p(a_{n-1})), \quad \text{i.e.}$$

$$(0,0),\ (1, v_p\Big(\frac{(n-1)p^{(n-2)k} - 1}{p^{(n-1)k}}\Big)),$$
$$(2, v_p\Big(\frac{(n-1)(n-2)}{2p^{2k}}\Big),\ \ldots,\ (n-1, v_p\Big(\frac{1}{p^{(n-1)k}}\Big)).$$

We see that $v_p(a_1) = -(n-1)k$, $v_p(a_i) \geq -ik$ for $i = 2, \ldots, n-2$ and $v_p(a_{n-1}) = -(n-1)k$. Therefore, the Newton polygon is as shown in the picture below.



From the properties of Newton polygons i.e. Lemma 3.1, as there is exactly one slope $\lambda = \frac{-(n-1)k-0}{1-0} = -(n-1)k$ of length 1 and the other slope $\lambda = 0$ is of length $n-2$, we conclude that exactly one root ξ of $Q(X)$ satisfies $|\xi|_p = p^{-(n-1)k}$ and all the other roots η of $Q(X)$ have $|\eta|_p = 1$. The choice of ε implies that $\varepsilon = \xi$ so

$$\mathrm{sep}_p(P) \leq |\varepsilon|_p = p^{-(n-1)k} = (p^{2k})^{-\frac{n-1}{2}} = \big(\mathrm{H}(P)\big)^{-\frac{n-1}{2}}.$$

The case of the polynomial $P(X) = (X - p^k)(p^k X^{n-1} - X + p^k)$ is done very similarly. We omit the details.

$$\boxed{P(X) = X^n - 2(X - p^k)^2}$$

The polynomial $P(X)$ is irreducible over $\mathbb{Q}$ because of Eisenstein's criterion.

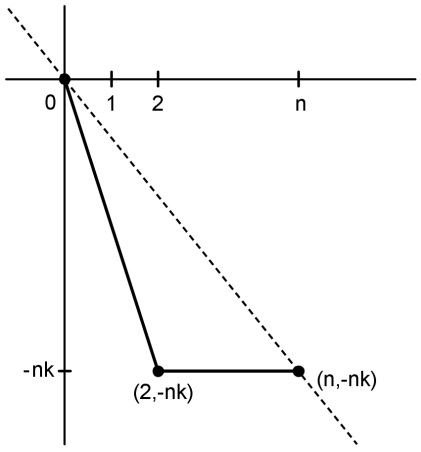
Let $p^k + \varepsilon$ be the root of $P(X)$ closest to p^k. Then

$$P(p^k + \varepsilon) = (p^k + \varepsilon)^n - 2\big((p^k + \varepsilon) - p^k\big)^2 = (p^k + \varepsilon)^n - 2\varepsilon^2 = 0.$$

For the polynomial

$$\begin{aligned} Q(X) &= \frac{1}{p^{nk}}\big((p^k + X)^n - 2X^2\big) \\ &= 1 + \frac{n}{p^k}X + \frac{\binom{n}{2}p^{(n-2)k} - 2}{p^{nk}}X^2 + \frac{\binom{n}{3}}{p^{3k}}X^3 + \cdots + \frac{1}{p^{nk}}X^n \\ &= 1 + \sum_{i=1}^{n} a_i X^i, \end{aligned}$$

we have $v_p(a_i) \geq -ik$, for $i = 1$ and $i = 3, \ldots, n-1$, and $v_p(a_2) = v_p(a_n) = -nk$. Therefore, the Newton polygon of $Q(X)$ is as shown below.



Since there are two slopes on it, $\lambda = -\frac{nk}{2}$ of length 2 and $\lambda = 0$ of length $n - 2$, we conclude that there are two roots of $Q(X)$ with p-adic absolute value $p^{-\frac{nk}{2}}$ and these have to be ε and $-\varepsilon$. Finally we get

$$\mathrm{sep}_p(P) \leq |(p^k+\varepsilon)-(p^k-\varepsilon)|_p = |2\varepsilon|_p = |\varepsilon|_p = p^{-\frac{nk}{2}} = (p^{2k})^{-\frac{n}{4}} \asymp \big(\mathrm{H}(P)\big)^{-\frac{n}{4}}.$$

Although we tacitly used that p is an odd prime, note that for $p = 2$ we can take $P(X) = X^n - 3(X - p^k)^2$ and all the conclusions remain the

same. Also, compare with Lemma 5.1 for a more detailed analysis of a similar polynomial.

The case of the polynomial $P(X) = p^{2k}X^n - 2(X - p^k)^2$ is done very similarly and we again leave the details to the interested reader.

3.2 Degrees two and three

Quadratic polynomials

Lemma 2.3 says that for a quadratic separable polynomial $P(X)$ with integer coefficients, we have $\operatorname{sep}_p(P) \geq \frac{1}{8}\operatorname{H}(P)^{-1}$. To show that the exponent -1 over $\operatorname{H}(P)$ really can be attained we can take the family of reducible polynomials

$$P_k(X) = X(X + p^k) = X^2 + p^k X, \quad k \geq 1$$

which gives $\operatorname{sep}_p(P_k) = p^{-k} = \operatorname{H}(P)^{-1}$. We can also look at the family of irreducible polynomials

$$P_k(X) = (-p^{2k} + p^k + 1)X^2 + (p^{2k} + 2p^k)X + p^{2k}, \quad k \geq 1$$

for which

$$\begin{aligned}\operatorname{sep}_p(P_k) &= \left|\frac{\sqrt{(p^{2k} + 2p^k)^2 - 4(-p^{2k} + p^k + 1)p^{2k}}}{-p^{2k} + p^k + 1}\right|_p \\ &= \left|\frac{\sqrt{5p^{4k}}}{-p^{2k} + p^k + 1}\right|_p = p^{-2k}\end{aligned}$$

if $p \neq 5$. Thus, here we have $\operatorname{sep}_p(P_k) \asymp \operatorname{H}(P_k)^{-1}$, where the implied constants are absolute. The last asymptotic relation obviously holds even if $p = 5$. For a family of monic irreducible quadratic polynomials $(P_k(X))_k$ with root separation $\operatorname{sep}_p(P_k) \asymp \operatorname{H}(P_k)^{-1}$, see Lemma 5.2.

Lemma 3.2. *Let $P(X)$ be a quadratic separable polynomial with integer coefficients. For every prime p, we have*

$$\operatorname{sep}_p(P) \geq \frac{1}{\operatorname{H}(P)\sqrt{5}}.$$

Equality is achieved if and only if $p = 5$ and $P(X) \in \{X^2 \pm X + 1, -X^2 \pm X - 1\}$.

Proof. For a separable quadratic polynomial $P(X) = aX^2 + bX + c$ with integer coefficients, the following sequence of inequalities holds

$$\begin{aligned}\operatorname{sep}_p(P) &= \left|\frac{\sqrt{b^2-4ac}}{a}\right|_p \\ &= \frac{|b^2-4ac|_p^{\frac{1}{2}}}{|a|_p} \overset{(i)}{\geq} \frac{1}{|b^2-4ac|^{\frac{1}{2}}} \overset{(ii)}{\geq} \frac{1}{\big(|b|^2+4|a||c|\big)^{\frac{1}{2}}} \overset{(iii)}{\geq} \frac{1}{\mathrm{H}(P)\sqrt{5}}.\end{aligned} \tag{3.1}$$

In (3.1.i) equality holds if and only if p does not divide a and $b^2 - 4ac = p^k$ for some nonnegative integer k. In (3.1.ii) equality is achieved if and only if $ac \leq 0$ while equality in (3.1.iii) is equivalent to $|a| = |b| = |c| = \mathrm{H}(P)$. Combining these conditions we arrive at the statement of the lemma. ∎

Reducible cubic case

We will exhibit a family of reducible cubic polynomials whose separation of roots is (up to an absolute constant) best possible.

We look at the polynomial $P(X) = (aX - b)(X^2 + rX + s) \in \mathbb{Z}[X]$. The roots of this polynomial are

$$\frac{b}{a} \quad \text{and} \quad \frac{-r \pm \sqrt{r^2-4s}}{2},$$

so in order to get the smallest separation of roots we only have to look at the distance of the root of the linear and of the quadratic factor of $P(X)$. Let

$$0 = P\big(\frac{b}{a} + \varepsilon\big) = \varepsilon\Big(\varepsilon^2 + \big(\frac{2b}{a} + r\big)\varepsilon + \big(\frac{b^2}{a^2} + \frac{rb}{a} + s\big)\Big).$$

Therefore, $\varepsilon \neq 0$ is a root of the polynomial

$$Q(X) = 1 + \frac{2ba + ra^2}{b^2 + rba + sa^2}X + \frac{a^2}{b^2 + rba + sa^2}X^2.$$

It is obvious that

$$\Big|\frac{2ba + ra^2}{b^2 + rba + sa^2}\Big|_p \leq |b^2 + rba + sa^2| \ll \mathrm{H}(P)^2,$$

where the implied constant in second inequality is absolute and follows from Gelfond's Lemma 0.2. The same bound holds for the leading coefficient of $Q(X)$ as well. We will construct a sequence of polynomials $\big(P_k(X)\big)_k$ such that the above bound becomes asymptotic equality. Then, using the Newton

polygons it will follow that $\operatorname{sep}(P_k) \asymp \mathrm{H}(P_k)^{-2}$ which is, of course, the best possible exponent.

To this end we will use the sequence $\big(A_k(n)\big)_{k\ge 0}$ of polynomials defined recursively

$$A_0(n) = 1,\ A_1(n) = n, \quad A_{k+1}(n) = nA_k(n) - A_{k-1}(n) \text{ for } n \ge 2.$$

We already used this sequence in the real case of reducible quartics. It is easy to see that $\deg_n A_k = k$, and it was shown in (1.7) that

$$A_k^2 - nA_kA_{k+1} + A_{k+1}^2 = 1.$$

Now we define new polynomials $\tilde{A}_k(n)$ by "reversion": $\tilde{A}_k(n) = n^k A_k\big(\frac{1}{n}\big)$. It is a recursive sequence

$$\tilde{A}_0(n) = 1,\ \tilde{A}_1(n) = n, \quad \tilde{A}_{k+1}(n) = \tilde{A}_k(n) - n^2\tilde{A}_{k-1}(n) \text{ for } n \ge 2$$

that satisfies

$$\tilde{A}_{k+1}^2 - \tilde{A}_{k+1}\tilde{A}_k + n^2\tilde{A}_k^2 = (n^{k+1})^2. \tag{3.2}$$

First few terms of the sequence $\tilde{A}_k(n)$ are

$$1, 1, -n^2+1, -2n^2+1, n^4-3n^2+1, 3n^4-4n^2+1, \dots$$

so we see that the constant term is always 1 and the degree is $\deg_n \tilde{A}_k = 2\big\lfloor \frac{k}{2} \big\rfloor$.

Fixing any integer $k \ge 2$, we set

$$a_{k,l} = \tilde{A}_k(p^l),\ b_{k,l} = \tilde{A}_{k+1}(p^l),\ r_{k,l} = -1,\ s_{k,l} = p^{2l}, \quad \text{for } l \ge 1.$$

Denoting

$$\begin{aligned} P_{k,l}(X) &= (a_{k,l}X - b_{k,l})(X^2 + r_{k,l}X + s_{k,l}) \\ &= \big(\tilde{A}_k(p^l)X - \tilde{A}_{k+1}(p^l)\big)(X^2 - X + p^{2l}), \quad l \ge 1, \end{aligned}$$

we see that the quadratic factor is irreducible over $\mathbb{Q}$ and (dropping indices k and l)

$$v_p\Big(\frac{2ba + ra^2}{b^2 + rba + sa^2}\Big) = -2(k+1)l$$

since $a \equiv b \equiv 1 \pmod p$ and $b^2 + rba + sa^2 = p^{2(k+1)l}$ because of (3.2). Therefore, $|\varepsilon|_p = p^{-2(k+1)l}$ and since $|a| \asymp_k p^{2\lfloor k/2 \rfloor l}$ and $|b| \asymp_k p^{2\lfloor (k+1)/2 \rfloor l}$, we have

$$\mathrm{H}(P_k) \asymp_k p^{2(\lfloor (k+1)/2 \rfloor + 1)l},$$

which implies

$$\operatorname{sep}_p(P_{k,l}) \ll \mathrm{H}(P_{k,l})^{-2+\varepsilon_k}, \quad l \to \infty.$$

Here, $\varepsilon_k \to 0$ when $k \to \infty$. Hence, we can choose $P_k(X) = P_{k,l_k}(X)$ for some sequence $(l_k)_k$ which increases sufficiently fast so that

$$\operatorname{sep}_p(P_k) \asymp \mathrm{H}(P_k)^{-2}, \quad k \to \infty.$$

Irreducible cubic case

Let $P(X) = aX^3 + bX^2 + cX + d \in \mathbb{Z}[X]$ be an integer polynomial with distinct roots $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}_p$. In order to analyze $\mathrm{sep}_p(P)$, we first construct a polynomial whose roots are closely related to the distances between the roots of $P(X)$. Denoting by $Q(X) = \mathrm{Res}_Y\big(P(Y), P(X+Y)\big)$, Lemma 0.4 tells us that $Q(X)$ has integer coefficients and for $x_0 \in \mathbb{C}_p$:

$$\begin{aligned} Q(x_0) = 0 \quad &\Leftrightarrow \quad P(Y) \text{ and } P(x_0+Y) \text{ have a common root in } \mathbb{C}_p \\ &\Leftrightarrow \quad \exists y_0 \in \mathbb{C}_p \text{ such that } P(y_0) = P(x_0+y_0) = 0 \\ &\Leftrightarrow \quad \exists \alpha, \beta \in \mathbb{C}_p \text{ such that } P(\alpha) = P(\beta) = 0,\ x_0 = \alpha - \beta \end{aligned}$$

This shows that if we denote $\delta_1 = \alpha_1 - \alpha_2$, $\delta_2 = \alpha_2 - \alpha_3$, $\delta_3 = \alpha_3 - \alpha_1$, then

$$Q(X) = \tilde{a} \prod_{\substack{1 \le i \le 3 \\ 1 \le j \le 3}} \big(X - (\alpha_i - \alpha_j)\big) = \tilde{a}(X^2 - \delta_1^2)(X^2 - \delta_2^2)(X^2 - \delta_3^2)X^3.$$

Taking $R(X) = Q(X)/X^3 \in \mathbb{Z}[X]$ and then $S(X) = R(\sqrt{X})/R(0)$, we get that

$$S(X) = \frac{-1}{\delta_1^2\delta_2^2\delta_3^2}(X - \delta_1^2)(X - \delta_2^2)(X - \delta_3^2)$$

is a polynomial in $\mathbb{Q}[X]$ such that

$$S(0) = 1 \quad \text{and} \quad \mathrm{sep}_p(P) = \min\big\{|\delta|_p^{\frac{1}{2}} \,:\, \delta \in \mathbb{C}_p,\ S(\delta) = 0\big\}. \tag{3.3}$$

After some computation, we obtain

$$\begin{aligned} S(X) = 1 &- \frac{(b^2 - 3ac)^2\, X}{b^2c^2 - 4ac^3 - 4b^3d + 18abcd - 27a^2d^2} \\ &+ \frac{2a^2\,(b^2 - 3ac)\, X^2}{b^2c^2 - 4ac^3 - 4b^3d + 18abcd - 27a^2d^2} \\ &- \frac{a^4 X^3}{b^2c^2 - 4ac^3 - 4b^3d + 18abcd - 27a^2d^2}. \end{aligned} \tag{3.4}$$

Before announcing the family of polynomials with the best currently known upper bound for separation of roots, let us mention an example we get using the process described in the introduction of this chapter. Taking from [8] a family of polynomials $Q_k(X) = (8k^3 - 2)X^3 + (4k^4 + 4k)X^2 + 4k^2X + 1$, $k \ge 1$, with close roots in $\mathbb{R}$, substituting k with $1/p^k$ and multiplying by p^{4k} we procure the polynomial

$$P_k(X) = (-2p^{4k} + 8p^k)X^3 + (4p^{3k} + 4)X^2 + (4p^{2k})X + p^{4k}$$

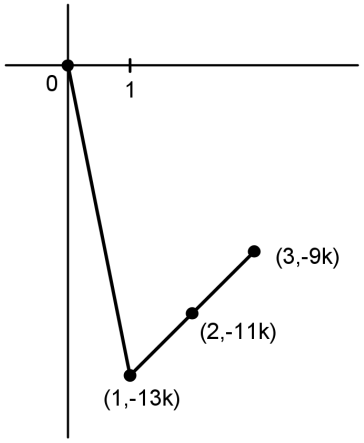
and insert its coefficients into (3.4). The coefficients of $S(X) = a_0 + a_1X + a_2X^2 + a_3X^3$ in the order a_0, a_1, a_2, a_3 are

$$1, \quad \frac{16p^{-13k}\left(2-8p^{3k}+5p^{6k}\right)^2}{-8+27p^{3k}}, \\ -\frac{16p^{-11k}\left(-4+p^{3k}\right)^2\left(2-8p^{3k}+5p^{6k}\right)}{-8+27p^{3k}}, \quad \frac{4p^{-9k}\left(-4+p^{3k}\right)^4}{-8+27p^{3k}},$$

which gives the following points we are interested in (for $p \neq 2$)

$$(0, v_p(a_0)),\ (1, v_p(a_1)),\ (2, v_p(a_2)),\ (3, v_p(a_3)) \\ =\ (0,0),\ (1,-13k),\ (2,-11k),\ (3,-9k).$$

Thus, the Newton polygon of $S(X)$ is as below (note that we have dropped the index k to ease the notation, but this is still a family of polynomials).



Lemma 3.1 and (3.3) show that $\mathrm{sep}_p(P_k) = p^{-13k/2} \asymp \mathrm{H}(P_k)^{-13/8}$ because $\mathrm{H}(P_k) \asymp p^{4k}$.

Finally, for a family of polynomials

$$P_k(X) = (-45056p^k - 17280p^{4k} - 243p^{7k})X^3 + (8192 + 1536p^{3k} - 378p^{6k})X^2 \\ + (512p^{2k} + 156p^{5k})X + 8p^{4k} + 2p^{7k},$$

coefficients of $S(X) = a_0 + a_1X + a_2X^2 + a_3X^3$ in the order a_0, a_1, a_2, a_3 are

$$1, \frac{256p^{-25k}\left(2097152 + 9p^{3k}\left(327680 + 99p^{3k}\left(1536 + 256p^{3k} + 9p^{6k}\right)\right)\right)^2}{19683\left(128 + 81p^{3k}\right)},$$
$$- \frac{16p^{-23k}\left(45056 + 27p^{3k}\left(640 + 9p^{3k}\right)\right)^2}{19683\left(128 + 81p^{3k}\right)}\cdot$$
$$\cdot \left(2097152 + 9p^{3k}\left(327680 + 99p^{3k}\left(1536 + 256p^{3k} + 9p^{6k}\right)\right)\right),$$
$$\frac{p^{-21k}\left(45056 + 27p^{3k}\left(640 + 9p^{3k}\right)\right)^4}{78732\left(128 + 81p^{3k}\right)},$$

which gives the following points we are interested in (for $p \neq 2$)

$$(0, v_p(a_0)),\ (1, v_p(a_1)),\ (2, v_p(a_2)),\ (3, v_p(a_3)) = (0,0),\ (1,-25k),\ (2,-23k),\ (3,-21k).$$

Lemma 3.1 and (3.3) show that $\mathrm{sep}_p(P_k) = p^{-25k/2} \asymp \mathrm{H}(P_k)^{-25/14}$ because $\mathrm{H}(P_k) \asymp p^{7k}$. Even if asymptotics does not change for $p = 2$, we are not certain that the polynomials $P_k(X)$ are irreducible in this case. For $p \neq 2$ this is guaranteed by Eisenstein's criterion.

Remark 3.1. This last family of polynomials was deduced from the family

$$(-45056n^6 - 17280n^3 - 243)X^3 + (8192n^7 + 1536n^4 - 378n)X^2 + (512n^5 + 156n^2)X + 8n^3 + 2, \quad n \geq 0$$

by the usual process. The original family of polynomials gives a separation of roots in the real case with the exponent $-25/14$ which is at present the best exponent for a family of irreducible cubic polynomials with polynomial growth of coefficients. Although Schönhage [32] proved that in the real case the best possible exponent -2 is attainable, his families of polynomials have exponential growth of coefficients. One of the main ingredients Schönhage used to construct these families is continued fraction expansion of real numbers. In the p-adic setting there are several types of continued fractions that have been proposed. None of them have all the good properties of the standard continued fractions and at the moment Schönhage's construction does not seem to translate easily to p-adic numbers. This is one of the reasons why we are interested in families of polynomials with polynomial growth of coefficients.

Chapter 4

p-adic T-numbers

4.1 Introduction

Mahler [20] introduced in 1932 a classification of complex transcendental numbers according to how small the value of an integer polynomial at the given number can be with regards to the the height and degree of this polynomial. In 1939 Koksma [18] devised another classification which looks at how closely the complex transcendental number can be approximated by algebraic numbers of bounded height and degree. Koksma proved that the two classifications are identical and thus we have three classes consisting of S-numbers or S^*-numbers, T-numbers or T^*-numbers and U-numbers or U^*-numbers. Here the nonstared letters refer to Mahler's classification whereas the stared ones refer to Koksma's. See [7] for all references.

While almost all numbers in the sense of Lebesgue measure are S-numbers and U-numbers contain for example Liouville numbers, it was only in 1968 that Schmidt [29] proved the existence of T-numbers.

Schlickewei [28] adapted this result to the p-adic setting. After this informal introduction, we give the necessary definitions in order to explain how the main result of this chapter improves Schlickewei's result. We take inspiration from a paper by R. C. Baker [1] on complex T-numbers in order to establish similar results for p-adic T-numbers.

In analogy with his classification of complex numbers, Mahler proposed a classification of p-adic numbers. Let $\xi \in \mathbb{Q}_p$ and given $n \geq 1$, $H \geq 1$, define the quantity

$$w_n(\xi, H) := \min\{|P(\xi)|_p \,:\, P(X) \in \mathbb{Z}[X],\, \deg(P) \leq n,\, \mathrm{H}(P) \leq H,\, P(\xi) \neq 0\}.$$

We set

$$w_n(\xi) := \limsup_{H\to\infty} \frac{-\log(Hw_n(\xi, H))}{\log H} \quad \text{and} \quad w(\xi) := \limsup_{n\to\infty} \frac{w_n(\xi)}{n},$$

and thus $w_n(\xi)$ is the upper limit of the real numbers w for which there exist infinitely many integer polynomials $P(X)$ of degree at most n satisfying

$$0 < |P(\xi)|_p \leq \mathrm{H}(P)^{-w-1}.$$

In analogy with Koksma's classification of complex numbers, for $\xi \in \mathbb{Q}_p$ and given $n \geq 1$, $H \geq 1$, we define the quantity

$$w_n^*(\xi, H) := \min\{|\xi - \alpha|_p \,:\, \alpha \text{ algebraic in } \mathbb{Q}_p,\ \deg(\alpha) \leq n,\ \mathrm{H}(\alpha) \leq H,\ \alpha \neq \xi\}.$$

We set

$$w_n^*(\xi) := \limsup_{H \to \infty} \frac{-\log(H w_n^*(\xi, H))}{\log H} \quad \text{and} \quad w^*(\xi) := \limsup_{n \to \infty} \frac{w_n^*(\xi)}{n},$$

and thus $w_n^*(\xi)$ is the upper limit of the real numbers w for which there exist infinitely many algebraic numbers α in $\mathbb{Q}_p$ of degree at most n satisfying

$$0 < |\xi - \alpha|_p \leq \mathrm{H}(\alpha)^{-w-1}.$$

We say that a transcendental number $\xi \in \mathbb{Q}_p$ is an

- *S-number* if $0 < w(\xi) < \infty$;
- *T-number* if $w(\xi) = \infty$ and $w_n(\xi) < \infty$ for any integer $n \geq 1$;
- *U-number* if $w(\xi) = \infty$ and $w_n(\xi) = \infty$ for some integer $n \geq 1$.

S^*-, T^*- and U^*- numbers are defined as above, using w_n^* in place of w_n.

Actually, the definition of the quantity $w_n(\xi)$ given here differs from the one used by Schlickewei [28]. Indeed, for him, the numerator of the defining fraction is $-\log(w_n(\xi, H))$ instead of $-\log(H w_n(\xi, H))$. This means that there is a shift by 1 in the value of the critical exponent, which however does not imply any change regarding the class of a given p-adic number. We have adopted the same notation as in [7] since then $w_n(\xi) = w_n^*(\xi) = n$ holds for almost all p-adic numbers ξ, with respect to the Haar measure on $\mathbb{Q}_p$.

Another possible issue is also settled, namely, as in the real case, if $w_n^*(\xi, H)$ is replaced by the minimum of $|\xi - \alpha|_p$ over *all* numbers $\alpha \neq \xi$ which are roots of integer polynomials of degree at most n and height at most H, the value of $w_n^*(\xi)$ does not change, see [7, §9.3]. So by replacing $\mathbb{Q}_p$ with an algebraic closure $\overline{\mathbb{Q}}_p$ in the definition of $w_n^*(\xi, H)$ we gain nothing new in respect to $w_n^*(\xi)$. See [7] for details and further results on the exponents w_n and w_n^*.

The central result of Schlickewei's paper [28] is his Theorem 2:

Theorem S. *Let $(B_n)_{n\geq 1}$ be a sequnce of real numbers such that*

$$B_1 > 9, \quad B_n > 3n^2 B_{n-1} \text{ for } n > 1.$$

There exist numbers $\xi \in \mathbb{Q}_p$ with

$$w_n^*(\xi) = B_n \text{ for any } n \geq 1.$$

While Schlickewei showed that p-adic T-numbers do exist, his proof only gave numbers ξ such that $w_n(\xi) = w_n^*(\xi)$ for all integers $n \geq 1$. Since for any p-adic transcendental number ξ we have

$$w_n^*(\xi) \leq w_n(\xi) \leq w_n^*(\xi) + n - 1 \tag{4.1}$$

(see Theorem 9.3 in [7]), it is natural to ask whether there exist p-adic numbers ξ such that $w_n(\xi) \neq w_n^*(\xi)$ for some integer n and how large $w_n(\xi) - w_n^*(\xi)$ can really be. Although the second question is, as in the more extensively studied real case, far from being resolved, our main result (cf. [1] or [7, Theorem 7.1, p. 140]) gives a positive answer to the first question and goes some way in answering the second one.

Theorem 4.1. *Let $(w_n)_{n\geq 1}$ and $(w_n^*)_{n\geq 1}$ be two non-decreasing sequences in $[1, +\infty]$ such that*

$$w_n^* \leq w_n \leq w_n^* + (n-1)/n, \quad w_n > n^3 + 2n^2 + 5n + 2, \qquad \text{for any } n \geq 1. \tag{4.2}$$

Then there exists a p-adic transcendental number ξ such that

$$w_n^*(\xi) = w_n^* \quad \text{and} \quad w_n(\xi) = w_n, \qquad \text{for any } n \geq 1.$$

It is also important to notice that we impose much milder growth requirements on the sequence $(w_n)_{n\geq 1}$ than in Theorem S. Thus our Theorem 4.1 considerably improves the range of attainable values for w_n^* and w_n.

The next section brings together necessary auxiliary results. In Section 4.3 we give the main proposition together with its proof and in the last section we use this proposition to prove our Theorem 4.1.

4.2 Auxiliary results

We will be using the following lemma by Schlickewei which is an immediate corollary of his p-adic version of Schmidt's Subspace Theorem.

Lemma 4.1. *Let ξ be an algebraic number in $\mathbb{Q}_p$ and n be a positive integer. Then, for any positive real number ε, there exists a positive (ineffective) constant $\kappa(\xi, n, \varepsilon)$ such that*

$$|\xi - \alpha|_p > \kappa(\xi, n, \varepsilon)\, \mathrm{H}(\alpha)^{-n-1-\varepsilon}$$

for any algebraic number α of degree at most n.

Proof. See [28, Theorem 3, p. 183]. ∎

In the next two lemmas we look at polynomials whose roots will be building blocks in the construction of numbers satisfying conditions of Theorem 4.1.

Lemma 4.2. *Let n be a positive integer.*
(a) Let p be an odd prime and d be the smallest prime in the arithmetic progression $p-1, 2p-1, 3p-1, \ldots$.

(i) If $p \nmid n$, the polynomial $X^n + d$ is irreducible over $\mathbb{Q}$ and has a root in $\mathbb{Q}_p$.

(ii) If $p|n$, the polynomial $X^n + dX^{n-1} - dX + d$ is irreducible over $\mathbb{Q}$ and has a root in $\mathbb{Q}_p$.
(b) Let $p = 2$.

(iii) If n is odd, the polynomial $X^n + 3$ is irreducible over $\mathbb{Q}$ and has a root in $\mathbb{Q}_2$.

(iv) If n is even, the polynomial $X^n + X + 2$ is irreducible over $\mathbb{Q}$ and has a root in $\mathbb{Q}_2$.
Moreover, in each of the four cases we can take the root to be in $1 + p\mathbb{Z}_p$.

Proof. A statement similar to this Lemma is given in [28, Lemma 1, p. 184]. Proof of irreducibility uses Eisenstein's criterion (see e.g. [27, Theorem 2.1.3, p. 50]) in cases (i), (ii) and (iii). For the irreducibility in case (iv) we use another result by Osada [25], see [27, Theorem 2.2.7, p. 58].

Hensel's Lemma 0.5 shows that each of the specified polynomials has a root in $1 + p\mathbb{Z}_p$. ∎

For the prime p and any positive integer n we denote by $\eta_n \in 1 + p\mathbb{Z}_p$ the root defined in the appropriate case of Lemma 4.2.

Lemma 4.3. *If η_n' is a conjugate of η_n over $\mathbb{Q}$ different from η_n itself, then $|\eta_n' - \eta_n|_p = 1$.*

Proof. Obviously, η_n and η_n' are both roots of a polynomial $P(X)$ mentioned in Lemma 4.2. We denote by $\delta = \eta_n' - \eta_n$ and then easily establish that it satisfies

$$0 = \frac{P(\eta_n') - P(\eta_n)}{\delta} = \sum_{k=1}^{n} \frac{P^{(k)}(\eta_n)}{k!} \delta^{k-1}$$

where $P^{(k)}(\eta_n)/k! \in \mathbb{Z}_p$ since $P(X) \in \mathbb{Z}[X]$ and $\eta_n \in \mathbb{Z}_p$. It follows from Lemma 2.1 that

$$|P'(\eta_n)|_p \leq |\delta|_p \leq \frac{1}{|P^{(n)}(\eta_n)/n!|_p}.$$

But with reference to Lemma 4.2,

$$\begin{aligned}
&P'(\eta_n) \equiv n \cdot 1 \not\equiv 0 \pmod{p} && \text{(case (i))},\\
&P'(\eta_n) \equiv n \cdot 1 - 1 \cdot (n-1) \cdot 1 + 1 \equiv 2 \not\equiv 0 \pmod{p} && \text{(case (ii))},\\
&P'(\eta_n) \equiv n \cdot 1 \equiv 1 \not\equiv 0 \pmod{p} && \text{(case (iii))},\\
&P'(\eta_n) \equiv n \cdot 1 + 1 \equiv 1 \not\equiv 0 \pmod{p} && \text{(case (iv))},
\end{aligned}$$

while $P^{(n)}(\eta_n)/n! = 1$ in all four cases. This shows that $|\delta|_p = 1$ which is what we wanted to prove. ∎

Remark 4.1. In order to minimize cumbersome repetition, we will be assuming that p is an odd prime which does not divide the degree n of the algebraic number η_n we defined earlier, in other words, the situation from case (i) of Lemma 4.2. Modifications which are needed to deal with the other three cases from this Lemma will be briefly mentioned at the appropriate places.

Later on, we will define $\xi_j = -c_j + v_j\eta_{m_j}$, where c_j, v_j are integers. If $\xi_j = \theta_{j,1}, \theta_{j,2}, \ldots, \theta_{j,m_j} \in \mathbb{C}_p$ are roots of the minimal polynomial of ξ_j over $\mathbb{Z}$, i.e. $P_j(X) = (X + c_j)^{m_j} + dv_j^{m_j}$, then we obviously have

$$\xi_j - \theta_{j,k} = (-c_j + v_j\eta_{m_j}) - (-c_j + v_j\eta'_{m_j}) = v_j(\eta_{m_j} - \eta'_{m_j}),$$

where we denoted by η'_{m_j} a conjugate of η_{m_j}. But Lemma 4.3 now implies $|\xi_j - \theta_{j,k}|_p = |v_j|_p$ for all $k = 2, \ldots, m_j$.

In our construction we will have $\xi = \lim_{j\to\infty} \xi_j$ and $|\xi_j - \theta_{j,k}|_p > |\xi_j - \xi|_p$, so $|\xi - \theta_{j,k}|_p = |\xi_j - \theta_{j,k}|_p = |v_j|_p$ which gives

$$|P_j(\xi)|_p = \prod_{k=1}^{m_j} |\xi - \theta_{j,k}|_p = |v_j|_p^{m_j-1} |\xi - \xi_j|_p. \tag{4.3}$$

(It is easily seen that the same equality holds in the other three cases from Lemma 4.2 as well.)

Remark 4.2. Let us consider what happens if we take $\xi_j = \frac{a_j}{b_j}\eta_{m_j}$ where $a_j, b_j \in \mathbb{Z}$ and $\gcd(a_j, b_j) = 1$. Schlickewei even has $|a_j|_p = |b_j|_p = 1$ in [28], but we do not take these additional assumptions. Now, because $\eta_{m_j}^{m_j} + d = 0$, where $d \equiv -1 \pmod{p}$, we have $|\eta_{m_j}|_p = 1$ and thus $|\xi_j|_p = |a_j|_p |b_j|_p^{-1}$. If $|a_j|_p$ is not bounded by a positive number from below, then $\gcd(a_j, b_j) =$

1 implies $|\xi_{j_k}|_p \to 0$ $(k \to \infty)$ for some subsequence $(\xi_{j_k})_{k\geq 1}$ which gives $\xi = 0$ and this is not possible. If $|b_j|_p$ is not bounded by a positive number from below, then $\gcd(a_j, b_j) = 1$ implies $|\xi_{j_k}|_p \to \infty$ $(k \to \infty)$ for some subsequence $(\xi_{j_k})_{k\geq 1}$ which gives $\xi = \infty$ and this is not possible either.

Therefore, $(|a_j|_p)_{j\geq 1}$ and $(|b_j|_p)_{j\geq 1}$ are both bounded from below by a positive number and since they are trivially bounded from above by 1, we conclude that for all positive integers n and for all j such that $m_j = n$, $|a_j|_p^{m_j-1}|b_j|_p$ is bounded so that an equality similar to (4.3) implies $|P_j(\xi)|_p \asymp |\xi - \xi_j|_p$. This gives (after an analysis we later give for the general case we study) $w_n(\xi) = w_n^*(\xi)$. That is why we have to construct ξ_j in a more complicated manner analogous to the real case.

4.3 Main proposition

We now follow the exposition of R. C. Baker's theorem as given in [7, §7.2, p. 141]. Some lines where the proof is identical to the real case will be briefly mentioned, while places where a modification is necessary will be more thoroughly explained.

Proposition 4.1. *(cf. [7, Proposition 7.1, p. 142]) Let $\nu_1, \nu_2, \ldots$ be real numbers > 1 and $\mu_1, \mu_2, \ldots$ be real numbers in $[0, 1]$. Let $m_1, m_2, \ldots$ be positive integers and $\chi_1, \chi_2, \ldots$ be real numbers satisfying $\chi_n > n^3 + 2n^2 + 4n + 3$ for any $n \geq 1$. Then, there exist positive real numbers $\lambda_1, \lambda_2, \ldots$, an increasing sequence of positive integers $g_1, g_2, \ldots$, and integers $c_1, c_2, \ldots$ such that the following conditions are satisfied.*
(I_j) $c_j \in [g_j/2, g_j]$, $v_j = p^{\lfloor \mu_j \log_p g_j \rfloor}$ $(j \geq 1)$.
(II_1) $\xi_1 = -c_1 + v_1\eta_{m_1}$.
(II_j) $\xi_j = -c_j + v_j\eta_{m_j}$ *belongs to the annulus $I_{j-1} \subseteq \mathbb{Q}_p$ defined by*

$$\frac{1}{2p} g_{j-1}^{-\nu_{j-1}} \leq |x - \xi_{j-1}|_p < g_{j-1}^{-\nu_{j-1}}.$$

(III_j) $|\xi_j - \alpha_n|_p \geq \lambda_n H(\alpha_n)^{-\chi_n}$ *for any algebraic number α_n of degree $n \leq j$ which is distinct from $\xi_1, \ldots, \xi_j$ $(j \geq 1)$.*

Proof. In what follows, we denote by α_n a p-adic algebraic number of degree exactly n. We fix a sequence $(\varepsilon_n)_{n\geq 1}$ in $]0, 1[$ such that, for any $n \geq 1$, we have

$$\chi_n > n^3 + 2n^2 + 4n + 3 + 20n^2\varepsilon_n. \tag{4.4}$$

We add four extra conditions $(IV_j), \ldots, (VII_j)$ to be satisfied by the numbers ξ_j.

Set

$$J_j := \{x \in I_j \,:\, |x-\alpha_n|_p \geq 2\lambda_n \,\mathrm{H}(\alpha_n)^{-\chi_n} \text{ for any algebraic} \\ \alpha_n \text{ of degree } n \leq j,\ \alpha_n \neq \xi_1, \dots, \xi_j, x,\ \mathrm{H}(\alpha_n) \geq (\lambda_n g_j^{\nu_j})^{1/\chi_n}\}.$$

The extra conditions are:
(IV_j) $\xi_j \in J_{j-1}$ $(j \geq 2)$.
(V_j) $|\xi_j - \alpha_j|_p \geq 2\lambda_j \,\mathrm{H}(\alpha_j)^{-\chi_j}$ for any $\alpha_j \neq \xi_j$ $(j \geq 1)$.
(VI_j) $n \leq j,\ \mathrm{H}(\alpha_n) \leq g_j^{1/(n+1+\varepsilon_n)} \ \Rightarrow\ |\xi_j - \alpha_n|_p \geq 1/g_j$ $(j \geq 1)$.
(VII_j) $\mu(J_j) \geq \mu(I_j)/2$ $(j \geq 1)$.
Here, μ denotes the Haar measure ($\mu(\{x \in \mathbb{Q}_p \,:\, |x-a|_p \leq p^{-\lambda}\}) = p^{-\lambda}$).

We construct the numbers $\xi_1, \lambda_1, \xi_2, \lambda_2, \dots$ by induction with description of steps the same as in [7, p. 144]. At the j-th stage, there are two steps. Step (A_j) consist in building an algebraic number

$$\xi_j = -c_j + v_j \eta_{m_j}$$

satisfying conditions (I_j) to (VI_j). In step (B_j), we show that the number ξ_j constructed in (A_j) satisfies (VII_j) as well, provided that g_j is chosen large enough in terms of

$$\nu_1, \dots, \nu_j, \mu_1, \dots, \mu_j, m_1, \dots, m_j, \chi_1, \dots, \chi_j, \\ \varepsilon_1, \dots, \varepsilon_j, \xi_1, \dots, \xi_{j-1}, \lambda_1, \dots, \lambda_{j-1}. \quad (4.5)$$

The symbols o, $\gg$ and $\ll$ used throughout steps (A_j) and (B_j) mean that the numerical implicit constants depend (at most) on the quantities displayed in (4.5). Furthermore, the symbol o implies 'as g_j tends to infinity'.

Note that we will have $v_j, c_j \in [g_j/2, g_j]$.

Step (A_1) is easy. There are $\gg g_1$ possible numbers $\xi_1 = -c_1 + v_1\eta_{m_1}$ and since $0 < c_1 \leq g_1$, the distance between such numbers is

$$|(-c_1' + v_1\eta_{m_1}) - (-c_1'' + v_1\eta_{m_1})|_p = |c_1' - c_1''|_p > \frac{1}{g_1}. \quad (4.6)$$

There are only $o(g_1)$ rational numbers α_1 satisfying $\mathrm{H}(\alpha_1) \leq g_1^{1/(2+\varepsilon_1)}$, so we are able to choose ξ_1 such that (VI_1) is verified. Moreover, by Lemma 4.1 with $n = 1$, there exist λ_1 in $]0,1[$ such that both (III_1) and (V_1) hold.

We continue exactly as in [7] making only the necessary and obvious changes. Let $j \geq 2$ be an integer and assume that $\xi_1, \dots, \xi_{j-1}$ have been constructed. Step (A_j) is much harder to verify, since we have no control on the set J_{j-1}. Thus, it is difficult to check that the condition (IV_j) holds, so we introduce a new set J_{j-1}' which contains J_{j-1}.

Set $\xi_j = -c_j + v_j\eta_{m_j}$ for some positive integers g_j and $c_j \in [g_j/2, g_j]$ with

$$g_j^{\nu_j} > 2g_{j-1}^{\nu_{j-1}}, \tag{4.7}$$

and denote by J'_{j-1} the set of p-adic numbers x in I_{j-1} satisfying $|x-\alpha_n|_p \geq 2\lambda_n \,\mathrm{H}(\alpha_n)^{-\chi_n}$ for any algebraic number α_n of degree $n \leq j-1$, distinct from $\xi_1, \ldots, \xi_{j-1}, x$ and whose height $\mathrm{H}(\alpha_n)$ satisfies the inequalities

$$(\lambda_n g_{j-1}^{\nu_{j-1}})^{1/\chi_n} \leq \mathrm{H}(\alpha_n) \leq (2\lambda_n g_j^{n^2+n+1+2n\varepsilon_n})^{1/(\chi_n-n-1-\varepsilon_n)}. \tag{4.8}$$

Since

$$\chi_n - n - 1 - \varepsilon_n > n^3+2n^2+2n+1+5n^2\varepsilon_n > (n+1)(n^2+n+1+2n\varepsilon_n), \tag{4.9}$$

the exponent of g_j in the right of (4.8) is strictly less than $1/(n+1)$. Thus, there are $o(g_j)$ algebraic numbers α_n satisfying (4.8). We will prove that for g_j large enough we have $\gg g_j$ suitable choices for c_j such that the conditions (I_j) to (V_j) are fulfilled.

Denote by $B(c,r)$ the ball $\{x \in \mathbb{Q}_p : |x-c|_p < r\}$. By introducing

$$\hat{B}_{j-1} = B(\xi_{j-1}, g_{j-1}^{-\nu_{j-1}}) \quad \text{and} \quad \check{B}_{j-1} = B\big(\xi_{j-1}, g_{j-1}^{-\nu_{j-1}}/(2p)\big),$$

we can write $I_{j-1} = \hat{B}_{j-1} \setminus \check{B}_{j-1}$.

Because in ultrametric space every two balls are either disjoint or one is a subset of the other, we can take a subfamily $\mathcal{F}$ of the balls defined by (4.8) and the text that immediately precedes it, i.e. a subfamily of

$$\{B(\alpha_n, 2\lambda_n \,\mathrm{H}(\alpha_n)^{-\chi_n}) : \alpha_n \text{ algebraic of degree } n \leq j-1, \\ \alpha_n \neq \xi_1, \ldots, \xi_{j-1}, x, \text{ and } \mathrm{H}(\alpha_n) \text{ satisfies (4.8)}\}$$

such that every two balls in $\mathcal{F}$ are disjoint, each of them is contained in $\hat{B}_{j-1}$, has nonempty intersection with I_{j-1} and $J'_{j-1} = I_{j-1} \setminus \bigcup_{B\in\mathcal{F}} B$. If $\check{B}_{j-1}$ is not already a subset of some ball in $\mathcal{F}$, then we add $\check{B}_{j-1}$ to the family $\mathcal{F}$ so that

$$J'_{j-1} = I_{j-1} \setminus \bigcup_{B\in\mathcal{F}} B = \hat{B}_j \setminus \bigcup_{B\in\mathcal{F}} B.$$

We look at the numbers from the set

$$S_j := \{\xi_j = -c_j + v_j\eta_{m_j} : c_j \in [g_j/2, g_j] \cap \mathbb{Z}\}.$$

For any ball $B = B(s,r) \in \mathcal{F}$, we have $r = p^{-k}$ for some $k \in \mathbb{Z}_{\geq 0}$ (depending on B) and we can take s to be the smallest nonnegative integer in B. Consider when $\xi_j \in B$:

$$|(-s + v_j\eta_{m_j}) - c_j|_p = |(-c_j + v_j\eta_{m_j}) - s|_p = |\xi_j - s|_p < r = p^{-k}.$$

Thus we see that all the associated c_j for such ξ_j are of the form $c_j = \tilde{s}+p^{k+1}l$, where $l = 0, 1, 2, \ldots$, also $\tilde{s}$ is an integer, $0 \le \tilde{s} < p^{k+1}$, and $c_j \in [g_j/2, g_j]$. The measure of B is obviously $\mu(B) = p^{-k-1}$ and if we define

$$N_j(B) := \#\{\xi_j : \xi_j \in S_j \cap B\},$$

it follows that

$$\frac{g_j}{2}\mu(B) - 1 = \frac{g_j/2}{p^{k+1}} - 1 \le N_j(B) \le \frac{g_j/2}{p^{k+1}} + 1 = \frac{g_j}{2}\mu(B) + 1,$$
$$\frac{g_j}{2}\mu\Big(\bigcup_{B\in\mathcal{F}} B\Big) - \#\mathcal{F} \le \sum_{B\in\mathcal{F}} N_j(B) \le \frac{g_j}{2}\mu\Big(\bigcup_{B\in\mathcal{F}} B\Big) + \#\mathcal{F}.$$

Analogously,

$$\frac{g_j}{2}\mu(\hat{B}_{j-1}) - 1 \le N_j(\hat{B}_{j-1}) \le \frac{g_j}{2}\mu(\hat{B}_{j-1}) + 1.$$

Using

$$N_j(J'_{j-1}) = N_j(\hat{B}_{j-1}) - \sum_{B\in\mathcal{F}} N_j(B) \quad \text{and} \quad \mu(J'_{j-1}) = \mu(\hat{B}_{j-1}) - \mu\Big(\bigcup_{B\in\mathcal{F}} B\Big),$$

we get

$$\mu(J'_{j-1}) - \frac{\#\mathcal{F}+1}{g_j/2} \le \frac{N_j(J'_{j-1})}{g_j/2} \le \mu(J'_{j-1}) + \frac{\#\mathcal{F}+1}{g_j/2}.$$

As was explained right after the equation (4.9), $\#\mathcal{F} = o(g_j)$. Since (VII_{j-1}) with $J'_{j-1} \supset J_{j-1}$ implies $\mu(J'_{j-1}) \gg 1$, we conclude

$$N_j(J'_{j-1}) \gg g_j.$$

We now have $\gg g_j$ possible numbers $\xi_j = -c_j + v_j\eta_{m_j} \in J'_{j-1}$ which means that they trivially satisfy (II_j). We will prove that they also satisfy (IV_j) for g_j large enough.

Let α_n be an algebraic number of degree n. By Lemma 4.1, there exists a positive constant $\kappa(m_j, n, \varepsilon_n)$ such that

$$\begin{aligned} |\xi_j - \alpha_n|_p &= |(-c_j + v_j\eta_{m_j}) - \alpha_n|_p = |v_j|_p\left|\eta_{m_j} - \left(\frac{\alpha_n + c_j}{v_j}\right)\right|_p \\ &\ge |v_j|_p\kappa(m_j, n, \varepsilon_n)\,\mathrm{H}\left(\frac{\alpha_n + c_j}{v_j}\right)^{-n-1-\varepsilon_n} \\ &\ge g_j^{-(n^2+n+1+2n\varepsilon_n)}\,\mathrm{H}(\alpha_n)^{-n-1-\varepsilon_n}, \end{aligned} \tag{4.10}$$

if g_j satisfies

$$g_j \geq \kappa(m_j, n, \varepsilon_n)^{-1/(n\varepsilon_n)} 2^{(n+1)(n+1+\varepsilon_n)/(n\varepsilon_n)}.$$

Here, we have used Lemma 0.3:

$$\mathrm{H}\left(\frac{\alpha_n + c_j}{v_j}\right) \leq 2^{n+1}\,\mathrm{H}(\alpha_n)\max\{1, |c_j|, |v_j|\}^n \leq 2^{n+1}\,\mathrm{H}(\alpha_n) g_j^n.$$

In particular, if g_j is large enough, we have

$$|\xi_j - \alpha_n|_p \geq 2\lambda_n\,\mathrm{H}(\alpha_n)^{-\chi_n} \tag{4.11}$$

as soon as

$$\mathrm{H}(\alpha_n)^{\chi_n - n - 1 - \varepsilon_n} \geq 2\lambda_n g_j^{n^2+n+1+2n\varepsilon_n}. \tag{4.12}$$

This together with the definition of J'_{j-1} shows that all our $\xi_j \in J'_{j-1}$ also belong to J_{j-1}. Therefore, the condition (IV_j) is verified. Note that the proofs of all the conditions from the proposition are obviously independent of the case from Lemma 4.2 we are in.

Conditions (VI_j), (V_j), (III_j) and the step (B_j) are done mutatis mutandis just like in [7]. We are left with $\gg g_j$ suitable algebraic numbers ξ_j, mutually distant by at least g_j^{-1} (compare (4.6)). Only $o(g_j)$ algebraic numbers α_n satisfy

$$\mathrm{H}(\alpha_n) \leq g_j^{1/(n+1+\varepsilon)}, \tag{4.13}$$

thus there are $\gg g_j$ algebraic numbers ξ_j such that $|\xi_j - \alpha_n|_p \geq 1/g_j$ for the numbers α_n verifying (4.13). Further, Lemma 4.1 ensures that there exists λ_j in $]0, 1[$ such that (V_j) is satisfied. Consequently, there are $\gg g_j$ algebraic numbers ξ_j satisfying $(I_j), (II_j), (IV_j), (V_j)$ and (VI_j).

It remains for us to show that such a ξ_j also satisfies (III_j). To this end, because of (IV_j) and (V_j), it suffices to prove that

$$|\xi_j - \alpha_n|_p \geq \lambda_n\,\mathrm{H}(\alpha_n)^{-\chi_n}$$

holds for any algebraic number α_n of degree $n < j$, which is different from $\xi_1, \ldots, \xi_j$ and whose height $\mathrm{H}(\alpha_n)$ satisfies

$$\mathrm{H}(\alpha_n) < (\lambda_n g_{j-1}^{\nu_{j-1}})^{1/\chi_n}.$$

Since by (4.7) the sequence $(g_t^{\nu_t})_{t\geq 1}$ is increasing, we either have

$$g_n^{-\nu_n} < \lambda_n\,\mathrm{H}(\alpha_n)^{-\chi_n}, \tag{4.14}$$

or there exists an integer t with $n < t < j$ such that

$$g_t^{-\nu_t} < \lambda_n \, \mathrm{H}(\alpha_n)^{-\chi_n} \le g_{t-1}^{-\nu_{t-1}}. \tag{4.15}$$

In the former case, we infer from (V_n), (4.7) and (4.14) that

$$|\xi_j - \alpha_n|_p \ge |\xi_n - \alpha_n|_p - |\xi_j - \xi_n|_p \ge 2\lambda_n \, \mathrm{H}(\alpha_n)^{-\chi_n} - g_n^{-\nu_n} > \lambda_n \, \mathrm{H}(\alpha_n)^{-\chi_n}.$$

In the latter case, (IV_t), (4.7) and (4.15) yield that

$$|\xi_j - \alpha_n|_p \ge |\xi_t - \alpha_n|_p - |\xi_j - \xi_t|_p \ge 2\lambda_n \, \mathrm{H}(\alpha_n)^{-\chi_n} - g_t^{-\nu_t} > \lambda_n \, \mathrm{H}(\alpha_n)^{-\chi_n}.$$

Thus condition (III_j) holds and the proof of step (A_j) is completed.

Before going on with the step (B_j), let us mention that the integer c_j is far from being uniquely determined. Indeed, at any step j we have $\gg g_j$ suitable choices for ξ_j which shows that the construction actually gives an uncountable set of T-numbers.

Let $j \ge 1$ be an integer. For the proof of step (B_j), we first establish that if g_j is large enough and if x lies in I_j, then we have

$$|x - \alpha_n|_p \ge 2\lambda_n \, \mathrm{H}(\alpha_n)^{-\chi_n} \tag{4.16}$$

for any algebraic number $\alpha_n \ne \xi_j$ of degree $n \le j$ such that

$$(\lambda_n g_j^{\nu_j})^{1/\chi_n} \le \mathrm{H}(\alpha_n) \le g_j^{\nu_j/(\chi_n - n - 1 - \varepsilon_n)}. \tag{4.17}$$

Let, then, $\alpha_n \ne \xi_j$ be an algebraic number satisfying (4.17) and let x be in I_j, that is, such that

$$\frac{1}{2p} g_j^{-\nu_j} \le |x - \xi_j|_p < g_j^{-\nu_j}. \tag{4.18}$$

If $\nu_j(n+1+\varepsilon_n) \le \chi_n - n - 1 - \varepsilon_n$, then $\mathrm{H}(\alpha_n) \le g_j^{1/(n+1+\varepsilon_n)}$ and it follows from (VI_j), (4.17), (4.18), and the assumption $\nu_j > 1$ that

$$|x - \alpha_n|_p \ge |\xi_j - \alpha_n|_p - |\xi_j - x|_p \ge g_j^{-1} - g_j^{-\nu_j} \ge 2g_j^{-\nu_j} \ge 2\lambda_n \, \mathrm{H}(\alpha_n)^{-\chi_n},$$

provided that g_j is large enough.

Otherwise, we have

$$\nu_j(n + 1 + \varepsilon_n) > \chi_n - n - 1 - \varepsilon_n, \tag{4.19}$$

and, by (4.10), we get

$$\begin{aligned} |x - \alpha_n|_p &\ge |\xi_j - \alpha_n|_p - |\xi_j - x|_p \\ &\ge g_j^{-(n^2+n+1+2n\varepsilon_n)} \, \mathrm{H}(\alpha_n)^{-n-1-\varepsilon_n} - g_j^{-\nu_j} \\ &\ge g_j^{-(n^2+n+1+2n\varepsilon_n)} \, \mathrm{H}(\alpha_n)^{-n-1-\varepsilon_n}/2. \end{aligned} \tag{4.20}$$

To check the last inequality, we have to verify that

$$2g_j^{-\nu_j} \le g_j^{-(n^2+n+1+2n\varepsilon_n)}\,\mathrm{H}(\alpha_n)^{-n-1-\varepsilon_n}. \tag{4.21}$$

In view of (4.17), inequality (4.21) is true as soon as

$$2g_j^{\nu_j(n+1+\varepsilon_n)/(\chi_n-n-1-\varepsilon_n)} \le g_j^{\nu_j} g_j^{-(n^2+n+1+2n\varepsilon_n)},$$

which, by (4.19), holds for g_j large enough when

$$\frac{n+1+\varepsilon_n}{\chi_n-n-1-\varepsilon_n} < 1-(n^2+n+1+2n\varepsilon_n)\frac{n+1+\varepsilon_n}{\chi_n-n-1-\varepsilon_n}, \tag{4.22}$$

and in particular when χ_n satisfies (4.4). Furthermore, we have

$$g_j^{-(n^2+n+1+2n\varepsilon_n)}\,\mathrm{H}(\alpha_n)^{-n-1-\varepsilon_n} \ge 4\lambda_n\,\mathrm{H}(\alpha_n)^{-\chi_n}. \tag{4.23}$$

Indeed, by (4.17), $\lambda_n < 1$, and (4.19), we get

$$\begin{aligned}\mathrm{H}(\alpha_n)^{-\chi_n-n-1-\varepsilon_n} &\ge (\lambda_n g_j^{\nu_j})^{(\chi_n-n-1-\varepsilon_n)/\chi_n} \ge \lambda_n g_j^{\nu_j(\chi_n-n-1-\varepsilon_n)/\chi_n}\\ &> \lambda_n g_j^{(\chi_n-n-1-\varepsilon_n)^2/(\chi_n(n+1+\varepsilon_n))} \ge 4\lambda_n g_j^{n^2+n+1+2n\varepsilon_n},\end{aligned}$$

since we infer from (4.4) that

$$(\chi_n-n-1-\varepsilon_n)^2 > \chi_n(n+1+\varepsilon_n)(n^2+n+1+2n\varepsilon_n). \tag{4.24}$$

Combining (4.20) and (4.23), we have checked that

$$|x-\alpha_n|_p \ge 2\lambda_n\,\mathrm{H}(\alpha_n)^{-\chi_n}$$

holds under assumption (4.19). By (4.19), this implies that (4.16) is true if α_n satisfies (4.17) and is not equal to ξ_j. Consequently, for g_j large enough, the complement J_j^c of J_j in I_j is contained in the union of the balls

$$B(\alpha_n, 2\lambda_n\,\mathrm{H}(\alpha_n)^{-\chi_n}),$$

where $\alpha_n \in \mathbb{Q}_p$ runs over the algebraic numbers of degree $n \le j$ and height greater than $g_j^{\nu_j/(\chi_n-n-1-\varepsilon_n)}$. The Haar measure of J_j^c is then

$$\ll \sum_{n=1}^{j} \sum_{H>g_j^{\nu_j/(\chi_n-n-1-\varepsilon_n)}} H^{n-\chi_n} = o(g_j^{-\nu_j}) = o(\mu(I_j)),$$

since for any positive integers H and n there are at most

$$(2H+1)^{n+1}-(2(H-1)+1)^{n+1} < (8H)^n$$

algebraic numbers of height H and degree n. Thus, we conclude that we can find g_j large enough such that $\mu(J_j) \ge \mu(I_j)/2$. This completes step (B_j) as well as proof of Proposition 4.1. ∎

At this point, we summarize where the condition $\chi_n > n^3 + 2n^2 + 4n + 3$ appears. There are three steps where it is needed, namely (4.9), (4.22) and (4.24). Asymptotically, these three inequalities reduce, respectively, to $\chi_n > (n+1)(n^2+n+2)$, $\chi_n > (n+1)(n^2+n+3)$, and $(\chi_n - n - 1)^2 > \chi_n(n+1)(n^2+n+1)$. The most restricting condition is given by (4.22), hence, our assumption on χ_n.

4.4 Proof of Theorem 4.1

Let $(w_n)_{n\geq 1}$ and $(w_n^*)_{n\geq 1}$ be two sequences fulfilling the conditions of Theorem 4.1. We will define numbers which are needed to apply Proposition 4.1.

Let $(m_j)_{j\geq 1}$ be a sequence of positive integers taking infinitely many times each value $1, 2, \ldots$ For $j \geq 1$, we set $\nu_j = m_j(w^*_{m_j} + 1)$ and define μ_j in $[0, 1]$ by

$$w^*_{m_j} + \frac{m_j - 1}{m_j}\mu_j = w_{m_j}.$$

Moreover, for any integer $n \geq 1$, we set $\chi_n = w_n - n + 1$ so that $\chi_n > n^3+2n^2+4n+3$. Let $\lambda_1, \lambda_2, \ldots, \xi_1, \xi_2, \ldots$ be as in Proposition 4.1 and denote by ξ the limit of the sequence $(\xi_j)_{j\geq 1}$. This sequence obviously converges since it is a Cauchy sequence and $\mathbb{Q}_p$ is complete.

We fix an integer $n \geq 1$. Observe that the minimal polynomial of ξ_j over $\mathbb{Z}$ is the polynomial

$$P_j(X) = (X + c_j)^{m_j} + dv_j^{m_j},$$

which is primitive since it is monic. Thus, recalling that $c_j, v_j \in [g_j/2, g_j]$, we get that $(g_j/2)^{m_j} \leq \mathrm{H}(\xi_j) \leq (dg_j)^{m_j}$. (We have completely analogous statements in the other three cases of Lemma 4.2.) Furthermore, for any $j \geq 1$ we have

$$|\xi - \xi_j|_p \in [\frac{1}{2p} g_j^{-\nu_j}, g_j^{-\nu_j}[$$

and the definition of ν_j implies that

$$|\xi - \xi_j|_p \in [\frac{1}{2p} 2^{-\nu_j}\, \mathrm{H}(\xi_j)^{-w^*_{m_j}-1}, d^{\nu_j}\, \mathrm{H}(\xi_j)^{-w^*_{m_j}-1}]. \tag{4.25}$$

Moreover, if α_m is an algebraic number of degree $m \leq n$, which is not equal to one of the ξ_j, then, by (III_j) we have

$$|\xi_j - \alpha_m|_p \geq \lambda_m\, \mathrm{H}(\alpha_m)^{-\chi_m},$$

hence, as j tends to infinity,

$$|\xi - \alpha_m|_p \geq \lambda_m \, \mathrm{H}(\alpha_m)^{-\chi_m} \geq \lambda_m \, \mathrm{H}(\alpha_m)^{-w_m^*-1}, \tag{4.26}$$

since $\chi_m = w_m - m + 1 \leq w_m^* + 1 - m + 1 \leq w_m^* + 1$. As $m_j = n$ for infinitely many integers j, it follows from (4.25), (4.26) and from the fact that the sequence $(w_m^*)_{m \geq 1}$ is increasing that

$$w_n^*(\xi) = w_n^*.$$

It remains for us to prove that $w_n(\xi) = w_n$. This is clear for $n = 1$, thus we assume $n \geq 2$. Until the end of this proof, we write $A \ll B$ when there is a positive constant $c(m_j)$, depending only on m_j, such that $|A| \leq c(m_j)|B|$, and we write $A \asymp B$ if both $A \ll B$ and $B \ll A$ hold. Since $\mathrm{H}(P_j) \asymp g_j^{m_j}$, we get from (4.3)

$$\begin{aligned} |P_j(\xi)|_p &= |v_j|_p^{m_j - 1} |\xi - \xi_j|_p \\ &\asymp g_j^{-\mu_j(m_j-1)} g_j^{-\nu_j} \asymp g_j^{-m_j(w_{m_j} - w_{m_j}^*)} g_j^{-m_j(w_{m_j}^*+1)} \\ &\asymp \mathrm{H}(P_j)^{-w_{m_j}-1}. \end{aligned} \tag{4.27}$$

Since $m_j = n$ for infinitely many j, we infer from (4.27) that $w_n(\xi) \geq w_n$. In order to show that we have equality, let $P(X)$ be an integer polynomial of degree at most n, which we write as

$$P(X) = a R_1(X) \cdots R_s(X) \cdot Q_1(X) \cdots Q_t(X),$$

where a is an integer and the polynomials $R_i(X)$ and $Q_j(X)$ are primitive and irreducible. We moreover assume that each $R_i(X)$ does not have a root equal to one of the ξ_ℓs, but that each $Q_j(X)$ has a root equal to some ξ_ℓ. If k denotes the degree of the polynomial $R_i(X)$, then, by Lemma 2.4, it has a root θ satisfying

$$\begin{aligned} |R_i(\xi)|_p &\gg \mathrm{H}(R_i)^{1-k} |\xi - \theta|_p \gg \lambda_n \, \mathrm{H}(R_i)^{-\chi_k - k + 1} \\ &= \lambda_n \, \mathrm{H}(R_i)^{-w_k} \gg \lambda_n \, \mathrm{H}(R_i)^{-w_n}. \end{aligned} \tag{4.28}$$

If ℓ denotes the degree of $Q_j(X)$, then (4.27) shows that

$$|Q_j(\xi)|_p \asymp \mathrm{H}(Q_j)^{-w_\ell - 1} \geq \mathrm{H}(Q_j)^{-w_n - 1}.$$

Together with (4.28) and Lemma 0.2, this gives

$$|P(\xi)|_p \gg \big(\mathrm{H}(R_1) \cdots \mathrm{H}(R_s) \, \mathrm{H}(Q_1) \cdots \mathrm{H}(Q_t) \big)^{-w_n - 1} \gg \mathrm{H}(P)^{-w_n - 1},$$

and we get $w_n(\xi) = w_n$, as claimed.

Chapter 5

On the difference $w_n - w_n^*$

5.1 Introduction and auxiliary results

In this chapter we improve an aspect of Theorem 4.1 showing that for any $n \geq 3$, the range of the function $w_n - w_n^*$ contains the interval $[0, \frac{n}{4}]$. We achieve that using integer polynomials from Lemma 5.1 having two zeros very close to each other instead of polynomials from Lemma 4.2. Estimating the distance between algebraic numbers is done with the help of Lemma 2.5 which unlike Lemma 4.1 has effective constants appearing in the lower bound. However, the drawback we have to endure in this method is a larger left endpoint of interval for w_n. More importantly, we can construct p-adic numbers ξ with prescribed values for $w_n^*(\xi)$ and $w_n(\xi)$ for only one (or, with a modification, finitely many) positive integer n at a time. This is in stark contrast to the situation in Theorem 4.1 where we succeeded in constructing p-adic numbers ξ with prescribed value for $w_n^*(\xi)$ and $w_n(\xi)$ for all positive integers $n \geq 3$.

Following [4], we give full proof of Theorem 5.1 although it has many lines similar to the proof of Theorem 4.1 we did in the previous chapter.

At the end of this chapter, we briefly mention the case $n = 1$. We also examine the case $n = 2$, proving that the difference $w_2 - w_2^*$ can take any value from the interval $[0, 1[$ which is essentially best possible.

Lemma 5.1. *Let $n \geq 3$ and $a \geq 1$ be integers. If p is an odd prime, then let d be the smallest prime in the arithmetic progression $p-1, 2p-1, 3p-1, \ldots$. If $p = 2$, we set $d = 15$. The polynomial*

$$P_{n,a}(X) := X^n + d(X - p^{2a})^2$$

is irreducible and has two roots $\delta_1(n,a), \delta_2(n,a) \in \mathbb{Q}_p$ which are very close to

each other, namely

$$\begin{aligned}|\delta_1(n,a)-\delta_2(n,a)|_p &= |\delta_1(n,a)-p^{2a}|_p = |\delta_2(n,a)-p^{2a}|_p \\ &= \begin{cases} p^{-na} & \text{if } p \neq 2 \\ 2^{-na-1} & \text{if } p = 2 \end{cases} \\ &\asymp_p \mathrm{H}(P_{n,a})^{-\frac{n}{4}}.\end{aligned}$$

Every other root $\delta \in \mathbb{C}_p$ *of* $P_{n,a}(X)$ *satisfies*

$$|\delta|_p = |\delta - p^{2a}|_p = 1.$$

Remark 5.1. We do not explicitly note the dependence of the polynomial $P_{n,a}(X)$ on d, since it is uniquely determined by p and we presuppose that the prime number p is fixed from the start.

Proof. The polynomial $P_{n,a}(X)$ is irreducible over $\mathbb{Q}$ because of Eisenstein's criterion. We write $P(X)$ instead of $P_{n,a}(X)$ for convenience.

By introducing the substitution $Y = (X - p^{2a})/p^{na}$ or $X = p^{na}Y + p^{2a}$ and letting $Q(Y) = P(X)/p^{2na}$, we get

$$Q(Y) = \frac{1}{p^{2na}}P(p^{na}Y + p^{2a}) = (p^{(n-2)a}Y + 1)^n + dY^2.$$

Hence, we have $Q(Y) \in \mathbb{Z}[Y]$ and

$$Q'(Y) = np^{(n-2)a}(p^{(n-2)a}Y + 1)^{n-1} + 2dY.$$

First we deal with the situation when p is an odd prime. Then $Q(\pm 1) \equiv 1 - 1 \equiv 0 \pmod{p}$ while $Q'(\pm 1) \equiv 2d(\pm 1) \equiv \mp 2 \not\equiv 0 \pmod{p}$. Hensel's Lemma 0.5 now shows that $Q(Y)$ has two roots $\tilde{\delta}_1(n,a) \in -1 + p\mathbb{Z}_p$ and $\tilde{\delta}_2(n,a) \in 1 + p\mathbb{Z}_p$. Therefore, $P(X)$ has roots $\delta_i(n,a) = p^{na}\tilde{\delta}_i(n,a) + p^{2a} \in \mathbb{Q}_p$ $(i = 1, 2)$ which obviously satisfy the assertions of this lemma.

If $p = 2$, then

$$\begin{aligned}Q(Y) &= (2^{(n-2)a}Y + 1)^n + 15Y^2, \\ Q'(Y) &= n2^{(n-2)a}(2^{(n-2)a}Y + 1)^{n-1} + 30Y.\end{aligned}$$

It is manifest that we have to use the general form of Hensel's Lemma 0.5. So putting $\alpha_0 = 1$ and $\beta_0 = 15$, we calculate

$$\begin{aligned}|Q(\alpha_0)|_2 = |Q(1)|_2 = |16|_2 &= \frac{1}{16}, \\ |Q'(\alpha_0)^2|_2 = |Q'(1)|_2^2 = |30|_2^2 &= \frac{1}{4} > |Q(1)|_2, \\ |Q(\beta_0)|_2 = |Q(15)|_2 = |1 + 15^3|_2 = |3376|_2 &= \frac{1}{16}, \\ |Q'(\beta_0)^2|_2 = |Q'(15)|_2^2 = |30 \cdot 15|_2^2 &= \frac{1}{4} > |Q(15)|_2.\end{aligned}$$

Now, Lemma 0.5 implies that there exist $\alpha, \beta \in \mathbb{Z}_2$ such that

$$|\alpha - \alpha_0|_2 \leq \left|\frac{Q(\alpha_0)}{Q'(\alpha_0)^2}\right|_2 \quad \Leftrightarrow \quad |\alpha - 1|_2 \leq \frac{1}{4} \qquad \text{and}$$
$$|\beta - \beta_0|_2 \leq \left|\frac{Q(\beta_0)}{Q'(\beta_0)^2}\right|_2 \quad \Leftrightarrow \quad |\beta - 15|_2 \leq \frac{1}{4}$$

Therefore,

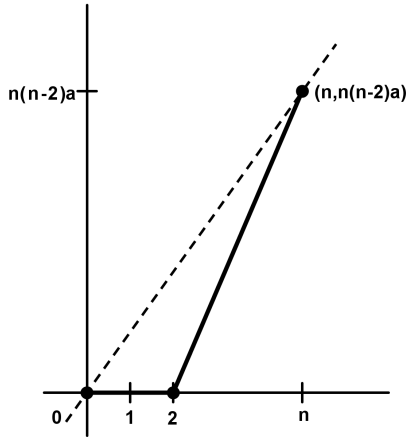
$$|\alpha - \beta|_2 \leq \max\{\underbrace{|\alpha - 1|_2}_{\leq \frac{1}{4}}, \underbrace{|\beta - 15|_2}_{\leq \frac{1}{4}}, \underbrace{|1 - 15|_2}_{= \frac{1}{2}}\} \quad \Rightarrow \quad |\alpha - \beta|_2 = \frac{1}{2},$$

which shows that $Q(Y)$ has two roots $\tilde{\delta}_1(n,a) = \alpha$ and $\tilde{\delta}_2(n,a) = \beta$, both in $1 + 2\mathbb{Z}_2$, with $|\tilde{\delta}_1(n,a) - \tilde{\delta}_2(n,a)|_2 = \frac{1}{2}$. Thus, $P(X)$ has roots $\delta_i(n,a) = 2^{na}\tilde{\delta}_i(n,a) + 2^{2a} \in \mathbb{Q}_2$ $(i = 1, 2)$ which satisfy the assertions of this lemma.

We continue the proof without having to distinguish primes p any more. To show that the other roots of $P(X)$ are "far enough" apart, we look at the Newton polygon of $Q(Y)$. For the polynomial

$$\begin{aligned} Q(Y) &= (p^{(n-2)a}Y + 1)^n + dY^2 \\ &= 1 + np^{(n-2)a}Y + (\binom{n}{2}p^{2(n-2)a} + d)Y^2 + \binom{n}{3}p^{3(n-2)a}Y^3 + \cdots + p^{n(n-2)a}Y^n \\ &= 1 + \sum_{i=1}^{n} a_i Y^i, \end{aligned}$$

we have $v_p(a_i) \geq i(n-2)a$ for $i \neq 2$ and $v_p(a_2) = 0$, so the Newton polygon of $Q(Y)$ is as shown below.



Since there are two different slopes on it, $\lambda = 0$ of length 2 and $\lambda = na$ of length $n-2$, we conclude that there are two roots of $Q(Y)$ with p-adic absolute value 1. These are exactly $\tilde{\delta}_1(n,a)$ and $\tilde{\delta}_2(n,a)$, while if $\tilde{\delta}$ is any of the other $n-2$ roots, we have $|\tilde{\delta}|_p = p^{na}$. Substituting back, we get that for every root δ of $P(X)$ different from $\delta_1(n,a)$ and $\delta_2(n,a)$ it holds

$$|\delta|_p = |p^{na}\tilde{\delta} + p^{2a}|_p = 1 \quad \text{and likewise} \quad |\delta - p^{2a}|_p = 1. \qquad \blacksquare$$

5.2 Main theorem and central part of its proof

Theorem 5.1 asserts the existence of p-adic numbers with special properties.

Theorem 5.1. *Let $n \geq 3$ be an integer and set $F(n) = 2n^3 + 2n^2 + 3n$. Let w_n and w_n^* be real numbers such that*

$$w_n^* \leq w_n \leq w_n^* + \frac{n}{4}, \quad w_n > F(n). \tag{5.1}$$

Then there exist $\xi \in \mathbb{Q}_p$ such that

$$w_n^*(\xi) = w_n^* \quad \textit{and} \quad w_n(\xi) = w_n.$$

Proposition 5.1 below gives an explicit inductive construction of sequences $(\xi_j)_{j\geq 1}$ of p-adic algebraic numbers of degree n. It will later be proved that such carefully selected sequences converge to p-adic numbers having the properties stated in Theorem 5.1. We use in the next proposition the same notation as in Lemma 5.1, namely we denote by $\delta_1(n,a)$ the root of the polynomial defined in that lemma.

Proposition 5.1. *Let $n \geq 3$ be an integer and let μ, ν be real numbers with $0 \leq \mu \leq n/4$ and $\nu > 1$. Set $H(n) = 2n^3 + 2n^2 + 2n + 1$ and let $\chi > H(n)$ be a real number.*

Then there exist a positive number $\lambda < 1/2$, an increasing sequence of integers $g_1 \geq 5, g_2, \ldots$, and a sequence of integers $c_1, c_2, \ldots$ such that the following conditions are satisfied, where we have set $\gamma_j := \delta_1(n, \lfloor \mu \log_p g_j \rfloor)$ for any integer $j \geq 1$:

(I_j) $\quad c_j \in [g_j/2, g_j]$.

(II_1) $\quad \xi_1 = -c_1 + \gamma_1$.

(II_j) $\quad \xi_j = -c_j + \gamma_j$ *belongs to the annulus $I_{j-1} \subseteq \mathbb{Q}_p$ defined by*

$$\frac{1}{2p} g_{j-1}^{-\nu} \leq |x - \xi_{j-1}|_p < g_{j-1}^{-\nu}.$$

(III_1) $|\xi_1 - \alpha|_p \geq 2\lambda H(\alpha)^{-\chi}$ *for any algebraic number* $\alpha \neq \xi_1$ *of degree* $\leq n$.
(III_j) $|\xi_j - \alpha|_p \geq \lambda H(\alpha)^{-\chi}$ *for any algebraic number* $\alpha \notin \{\xi_1, \ldots, \xi_j\}$ *of degree* $\leq n$ $(j \geq 2)$.

Proof. To simplify the notation, in what follows, we denote by α an algebraic number of degree $\leq n$. Let ε be a positive number such that

$$\chi > 2n^3 + 2n^2 + 2n + 1 + 2n^2\varepsilon. \tag{5.2}$$

In order to prove this proposition, we add three extra conditions (IV_j), (V_j) and (VI_j) which should be satisfied by the numbers ξ_j.

Set

$$J_j := \{x \in I_j \,:\, |x - \alpha|_p \geq 2\lambda\, \mathrm{H}(\alpha)^{-\chi} \quad \text{for any algebraic } \alpha \\ \text{of degree } \leq n,\ \alpha \neq \xi_1, \ldots, \xi_j, x,\ \mathrm{H}(\alpha) \geq (\lambda g_j^{\nu})^{1/\chi}\}.$$

The extra conditions are:
(IV_j) $\xi_j \in J_{j-1}$ $(j \geq 2)$.
(V_j) $\mathrm{H}(\alpha) \leq g_j^{1/(n+1+\varepsilon)} \ \Rightarrow\ |\xi_j - \alpha|_p \geq 1/g_j$ $(j \geq 1)$.
(VI_j) $\mu(J_j) \geq \mu(I_j)/2$ $(j \geq 1)$.
Here as before, μ denotes the Haar measure.

We construct the numbers $\xi_1, \xi_2, \ldots$ by induction with description of steps the same as before (cf. [4, 7]). At the j-th stage, there are two steps. Step (A_j) consist in building an algebraic number

$$\xi_j = -c_j + \gamma_j$$

satisfying conditions (I_j) to (V_j). In step (B_j), we show that the number ξ_j constructed in (A_j) satisfies (VI_j) as well, provided that g_j is chosen large enough in terms of

$$n, \mu, \nu, \chi, \varepsilon, \lambda, \xi_1, \ldots, \xi_{j-1}. \tag{5.3}$$

The symbols o, $\gg$ and $\ll$ used throughout steps (A_j) and (B_j) mean that the numerical implicit constants depend (at most) on quantities (5.3). Furthermore, the symbol o implies 'as g_j tends to infinity'.

Note that we will have $c_j \in [g_j/2, g_j]$.

Step (A_1) is easy. There are $\gg g_1$ possible numbers $\xi_1 = -c_1 + \gamma_1$ and since $0 < c_1 \leq g_1$, the distance between such numbers is

$$|(-c_1' + \gamma_1) - (-c_1'' + \gamma_1)|_p = |c_1' - c_1''|_p > \frac{1}{g_1}. \tag{5.4}$$

There are only $o(g_1)$ algebraic numbers α of degree at most n satisfying $\mathrm{H}(\alpha) \le g_1^{1/(n+1+\varepsilon)}$, so we are able to choose ξ_1 such that (V_1) is satisfied. Moreover, by Lemma 2.5, we have

$$|\xi_1 - \alpha|_p \ge 2\lambda\,\mathrm{H}(\alpha)^{-n}$$

with $\lambda = c(n,n)\,\mathrm{H}(\xi_1)^{-n}/2$, for any algebraic number $\alpha \ne \xi_1$ of degree at most n. Thus (I_1), (II_1), (III_1) and (V_1) are satisfied.

Let $j \ge 2$ be an integer and assume that $\xi_1, \dots, \xi_{j-1}$ have been constructed. Step (A_j) is much harder to verify, since we have no control on the set J_{j-1}. Thus, it is difficult to check that the condition (IV_j) holds, so we introduce a new set J'_{j-1} which contains J_{j-1}.

Set $\xi_j = -c_j + \gamma_j$ for some positive integers $g_j > g_{j-1}$ and $c_j \in [g_j/2, g_j]$ and denote by J'_{j-1} the set of p-adic numbers x in I_{j-1} satisfying $|x - \alpha|_p \ge 2\lambda\,\mathrm{H}(\alpha)^{-\chi}$ for any algebraic number α of degree $\le n$, distinct from $\xi_1, \dots, \xi_{j-1}, x$ and whose height $\mathrm{H}(\alpha)$ satisfies the inequalities

$$(\lambda g_{j-1}^{\nu})^{1/\chi} \le \mathrm{H}(\alpha) \le \left(c(n)^{-1} g_j^{2n^2}\right)^{1/(\chi-n)}, \tag{5.5}$$

where $c(n)$ is a constant depending only on n which will be defined in a moment. Since, by (5.2), we have

$$\chi - n > 2n^2(n+1), \tag{5.6}$$

the exponent of g_j in the right of (5.5) is strictly less than $1/(n+1)$. Thus, there are $o(g_j)$ algebraic numbers α satisfying (5.5). We will prove that for g_j large enough we have $\gg g_j$ suitable choices for c_j such that the conditions (I_j) to (IV_j) are fulfilled.

Exactly the same argument as in the proof of Proposition 4.1 is applied to show that $\mu(J'_{j-1}) \gg 1$ (which is a consequence of $J'_{j-1} \supset J_{j-1}$ and (VI_{j-1})) implies that there are $\gg g_j$ possible numbers $\xi_j = -c_j + \gamma_j \in J'_{j-1}$. These numbers trivially satisfy (II_j) and we will prove that they also satisfy (IV_j) for g_j large enough.

Let α be an algebraic number of degree $\le n$. We have

$$\mathrm{H}(\gamma_j) = \mathrm{H}\left(\delta_1(n, \lfloor \mu \log_p g_j \rfloor)\right) = d p^{4\lfloor \mu \log_p g_j \rfloor} \le d g_j^n$$

and Lemma 0.3 gives

$$\mathrm{H}(\xi_j) = \mathrm{H}(-c_j + \gamma_j) \le 2^{n+1}\,\mathrm{H}(\gamma_j)\max\{1, |c_j|\}^n \le 2^{n+1}\,\mathrm{H}(\gamma_j) g_j^n \le 2^{n+1} d g_j^{2n}.$$

We infer from Lemma 2.5 that there exist positive constants $\tilde{c}(n)$ and $c(n)$ such that

$$|\xi_j - \alpha|_p \ge \tilde{c}(n)\,\mathrm{H}(\xi_j)^{-n}\,\mathrm{H}(\alpha)^{-n} \ge c(n) g_j^{-2n^2}\,\mathrm{H}(\alpha)^{-n}. \tag{5.7}$$

In particular, using $2\lambda < 1$, we have

$$|\xi_j - \alpha|_p \geq 2\lambda \, \mathrm{H}(\alpha)^{-\chi} \tag{5.8}$$

as soon as

$$\mathrm{H}(\alpha)^{\chi - n} \geq c(n)^{-1} g_j^{2n^2}. \tag{5.9}$$

This together with the definition of J'_{j-1} shows that all our $\xi_j \in J'_{j-1}$ also belong to J_{j-1}. Therefore, the condition (IV_j) is verified.

We are left with $\gg g_j$ suitable algebraic numbers ξ_j, mutually distant by at least g_j^{-1} (compare with (5.4)). Only $o(g_j)$ algebraic numbers α of degree at most n satisfy

$$\mathrm{H}(\alpha) \leq g_j^{1/(n+1+\varepsilon)}, \tag{5.10}$$

thus there are $\gg g_j$ algebraic numbers ξ_j such that $|\xi_j - \alpha|_p \geq 1/g_j$ for the numbers α verifying (5.10). Consequently, there are $\gg g_j$ algebraic numbers ξ_j satisfying (I_j), (II_j), (IV_j) and (V_j).

We still have to prove that such a ξ_j also satisfies (III_j). To this end, because of (IV_j), it suffices to show that

$$|\xi_j - \alpha|_p \geq \lambda \, \mathrm{H}(\alpha)^{-\chi}$$

holds for any algebraic number α of degree $\leq n$, which is different from $\xi_1, \ldots, \xi_j$ and whose height $\mathrm{H}(\alpha)$ satisfies

$$\mathrm{H}(\alpha) < (\lambda g_{j-1}^{\nu})^{1/\chi}.$$

Since the sequence $(g_t)_{t \geq 1}$ is increasing, we either have

$$g_1^{-\nu} < \lambda \, \mathrm{H}(\alpha)^{-\chi}, \tag{5.11}$$

or there exists an integer t with $2 \leq t < j$ such that

$$g_t^{-\nu} < \lambda \, \mathrm{H}(\alpha)^{-\chi} \leq g_{t-1}^{-\nu}. \tag{5.12}$$

In the former case, we infer from (III_1) and (5.11) that

$$|\xi_j - \alpha|_p \geq |\xi_1 - \alpha|_p - |\xi_j - \xi_1|_p \geq 2\lambda \, \mathrm{H}(\alpha)^{-\chi} - g_1^{-\nu} > \lambda \, \mathrm{H}(\alpha)^{-\chi}.$$

In the latter case, (IV_t) and (5.12) yield that

$$|\xi_j - \alpha|_p \geq |\xi_t - \alpha|_p - |\xi_j - \xi_t|_p \geq 2\lambda \, \mathrm{H}(\alpha)^{-\chi} - g_t^{-\nu} > \lambda \, \mathrm{H}(\alpha)^{-\chi}.$$

Thus condition (III_j) holds and the proof of step (A_j) is completed.

Before going on with the step (B_j), let us mention that the integer c_j is far from being uniquely determined. Indeed, at any step j we have $\gg g_j$ suitable choices for ξ_j which shows that the construction actually gives an uncountable set of numbers.

Let $j \geq 1$ be an integer. For the proof of step (B_j), we first establish that if g_j is large enough and if x lies in I_j, then we have

$$|x - \alpha|_p \geq 2\lambda \, \mathrm{H}(\alpha)^{-\chi} \tag{5.13}$$

for any algebraic number $\alpha \neq \xi_j$ of degree $\leq n$ such that

$$(\lambda g_j^{\nu})^{1/\chi} \leq \mathrm{H}(\alpha) \leq g_j^{\nu/(\chi-n-1-\varepsilon)}. \tag{5.14}$$

Let, then, $\alpha \neq \xi_j$ be an algebraic number of degree $\leq n$ satisfying (5.14) and let x be in I_j, that is, such that

$$\frac{1}{2p} g_j^{-\nu} \leq |x - \xi_j|_p < g_j^{-\nu}. \tag{5.15}$$

If $\nu(n+1+\varepsilon_n) \leq \chi - n - 1 - \varepsilon$, then $\mathrm{H}(\alpha) \leq g_j^{1/(n+1+\varepsilon)}$ and it follows from (V_j), (5.14), (5.15) and the assumption $\nu > 1$ that

$$|x - \alpha|_p \geq |\xi_j - \alpha|_p - |\xi_j - x|_p \geq g_j^{-1} - g_j^{-\nu} \geq 2g_j^{-\nu} \geq 2\lambda \, \mathrm{H}(\alpha)^{-\chi}, \tag{5.16}$$

provided that g_j is large enough.

Otherwise, we have

$$\nu(n+1+\varepsilon) > \chi - n - 1 - \varepsilon, \tag{5.17}$$

and, by (5.7), we get

$$\begin{aligned} |x - \alpha|_p &\geq |\xi_j - \alpha|_p - |\xi_j - x|_p \\ &\geq c(n) g_j^{-2n^2} \, \mathrm{H}(\alpha)^{-n} - g_j^{-\nu} \\ &\geq c(n) g_j^{-2n^2} \, \mathrm{H}(\alpha)^{-n}/2. \end{aligned} \tag{5.18}$$

The last inequality holds if

$$2g_j^{-\nu} \leq c(n) g_j^{-2n^2} \, \mathrm{H}(\alpha)^{-n}. \tag{5.19}$$

In view of (5.14), inequality (5.19) is true as soon as

$$2g_j^{n\nu/(\chi-n-1-\varepsilon)} \leq c(n) g_j^{\nu} g_j^{-2n^2},$$

which, by (5.17), holds for g_j large enough when

$$\frac{n}{\chi - n - 1 - \varepsilon} < 1 - 2n^2 \frac{n + 1 + \varepsilon}{\chi - n - 1 - \varepsilon}, \tag{5.20}$$

and in particular when χ satisfies (5.2). Furthermore, we have

$$c(n) g_j^{-2n^2} \, \mathrm{H}(\alpha)^{-n} \geq 4\lambda \, \mathrm{H}(\alpha)^{-\chi}. \tag{5.21}$$

Indeed, by (5.14), $\lambda < 1$, and (5.17), we get

$$\begin{aligned} \mathrm{H}(\alpha)^{\chi - n} &\geq (\lambda g_j^{\nu})^{(\chi - n)/\chi} \geq \lambda g_j^{(\chi - n)(\chi - n - 1 - \varepsilon)/(\chi n + \chi + \chi\varepsilon)} \\ &\geq 4\lambda c(n)^{-1} g_j^{2n^2}, \end{aligned}$$

since we infer from (5.2) that

$$(\chi - n)(\chi - n - 1 - \varepsilon) > 2\chi n^2 (n + 1 + \varepsilon). \tag{5.22}$$

Combining (5.18) and (5.21), we have verified that

$$|x - \alpha|_p \geq 2\lambda \, \mathrm{H}(\alpha)^{-\chi}$$

holds under assumption (5.17). By (5.16), this implies that (5.13) is true if α satisfies (5.14) and is not equal to ξ_j. Consequently, for g_j large enough, the complement J_j^c of J_j in I_j is contained in the union of the balls

$$B(\alpha, 2\lambda \, \mathrm{H}(\alpha)^{-\chi}),$$

where $\alpha \in \mathbb{Q}_p$ runs over the algebraic numbers of degree $\leq n$ and height greater than $g_j^{\nu/(\chi - n - 1 - \varepsilon)}$. The Haar measure of J_j^c is then

$$\ll \sum_{H > g_j^{\nu/(\chi - n - 1 - \varepsilon)}} H^{n - \chi} = o(g_j^{-\nu}) = o(\mu(I_j)).$$

Thus, we conclude that we can find g_j large enough such that $\mu(J_j) \geq \mu(I_j)/2$. This completes step (B_j) as well as proof of Proposition 5.1. ∎

At this moment, we can recap where the condition $\chi > 2n^3 + 2n^2 + 2n + 1$ was used. There are three steps where it was needed, namely (5.6), (5.20) and (5.22). Asymptotically, these three inequalities reduce, respectively, to $\chi - n > 2n^2(n + 1)$, $\chi - n - 1 > 2n^2(n + 1) + n$, and $(\chi - n)(\chi - n - 1) > 2\chi n^2(n + 1)$. The most restricting condition is given by (5.20), hence, our assumption on χ.

5.3 Proof of Theorem 5.1

Let w_n and w_n^* be two real numbers fulfilling the conditions of Theorem 5.1. We will define numbers which are needed to apply Proposition 5.1. Set $\mu = w_n - w_n^* \in [0, n/4]$, $\nu = n(w_n^* + 1)$ and finally, set $\chi = w_n - n + 1$, so that $\chi > H(n) = 2n^3 + 2n^2 + 2n + 1$.

Let λ and $\xi_1, \xi_2, \dots$ be as in Proposition 5.1 and denote by $\xi \in \mathbb{Q}_p$ the limit of the Cauchy sequence $(\xi_j)_{j\geq 1}$.

The constants implied in $\gg$ and $\asymp$ of this section depend at most on p and n. Our choice of γ_j implies that the minimal polynomial of ξ_j over $\mathbb{Z}$ is

$$Q_j(X) := (X + c_j)^n + d\big((X + c_j) - p^{2\lfloor \mu \log_p g_j \rfloor}\big)^2.$$

This polynomial is indeed primitive and irreducible by the first statement of Lemma 5.1.

Since $c_j \in [g_j/2, g_j]$ and $\mu \leq n/4$, we have $\mathrm{H}(\xi_j) = \mathrm{H}(Q_j) \asymp g_j^n$. Moreover, for any $j \geq 1$

$$|\xi - \xi_j|_p \in [\frac{1}{2p} g_j^{-\nu}, g_j^{-\nu}[$$

and we deduce that

$$|\xi - \xi_j|_p \asymp \mathrm{H}(\xi_j)^{-\nu/n} \asymp \mathrm{H}(\xi_j)^{-w_n^*-1}. \tag{5.23}$$

Further, if α is of degree $\leq n$ and is not one of the ξ_j's, then $|\xi - \alpha|_p \geq \lambda\, \mathrm{H}(\alpha)^{-\chi}$, whence

$$|\xi - \alpha|_p \geq \mathrm{H}(\alpha)^{-w_n^*-1} \tag{5.24}$$

since $\chi \leq w_n^* + 1$. It follows from (5.23), (5.24) and our remarks on the definition of $w_n^*(\xi)$ from §4.1 that $w_n^*(\xi) = w_n^*$.

It now remains to prove that $w_n(\xi) = w_n$. Denote by $\xi_j = \beta_{j1}, \dots, \beta_{jn}$ the roots of $Q_j(X)$, numbered in such a way that β_{j2} is closest to ξ_j. Denote by $\delta_3, \dots, \delta_k$ the roots of $P_{n,\lfloor \mu \log_p g_j \rfloor}(X)$ other than $\delta_i(n, \lfloor \mu \log_p g_j \rfloor)$, $i = 1, 2$. Then using Lemma 5.1, we get

$$\begin{aligned} |\xi_j - \beta_{j2}|_p &= |(-c_j + \gamma_j) - (-c_j + \delta_2(n, \lfloor \mu \log_p g_j \rfloor))|_p \\ &= |\delta_1(n, \lfloor \mu \log_p g_j \rfloor) - \delta_2(n, \lfloor \mu \log_p g_j \rfloor)|_p \\ &= p^{-n\lfloor \mu \log_p g_j \rfloor} \asymp g_j^{-n\mu} \end{aligned}$$

and

$$|\xi_j - \beta_{jk}|_p = |\gamma_j - \delta_k|_p = 1, \quad \text{for } k \geq 3.$$

Keeping in mind that $|\xi-\beta_{j2}|_p=|\xi_j-\beta_{j2}|_p$ since $|\xi_j-\beta_{j2}|_p>|\xi-\xi_j|_p$, we arrive at

$$\begin{aligned}|Q_j(\xi)|_p&=|\xi-\xi_j|_p|\xi-\beta_{j2}|_p\prod_{3\le k\le n}|\xi-\beta_{jk}|_p\\&\asymp \mathrm{H}(\xi_j)^{-w_n^*-1}g_j^{-n\mu}\\&\asymp \mathrm{H}(Q_j)^{-w_n^*-\mu-1}.\end{aligned}$$

We see that

$$w_n(\xi)\ge w_n^*+\mu. \tag{5.25}$$

Now we will show that (5.25) is indeed an equality. Let $P(X)$ be an integer polynomial of degree $\le n$ which is not a multiple of some $Q_j(X)$. Write

$$P(X)=aR_1(X)\cdots R_s(X),$$

where a is an integer and the polynomials $R_i(X)$ are primitive and irreducible. Since $R_i(\xi)\neq 0$, if k denotes the degree of the polynomial $R_i(X)$, then by Lemma 2.4, this polynomial has a root θ satisfying

$$|R_i(\xi)|_p\gg \mathrm{H}(R_i)^{1-k}|\xi-\theta|_p\gg \lambda\,\mathrm{H}(R_i)^{-\chi-k+1}\gg \lambda\,\mathrm{H}(R_i)^{-w_n}. \tag{5.26}$$

Consequently, it follows from (5.26) and Gelfond's Lemma 0.2 that

$$|P(\xi)|_p\gg \big(\mathrm{H}(R_1)\cdots\mathrm{H}(R_s)\big)^{-w_n}\gg \mathrm{H}(P)^{-w_n}$$

and we get $w_n(\xi)=w_n$ as claimed.

5.4 The case $n=1$

Solely for completeness, we include the following proposition which deals with the case $n=1$.

Proposition 5.2. *For every $\xi\in\mathbb{Q}_p\setminus\mathbb{Q}$ we have $w_1(\xi)=w_1^*(\xi)\ge 1$. Moreover, for every $w\in[1,+\infty]$, there are uncountably many $\xi\in\mathbb{Q}_p$ such that $w_1(\xi)=w_1^*(\xi)=w$.*

Proof. The lower bound $w_1(\xi)\ge 1$ follows from the general case proved by Mahler [21] and is basically a consequence of Dirichlet's pigeonhole principle.

The equality $w_1(\xi)=w_1^*(\xi)$ is obtained from the inequality $w_1(\xi)\ge w_1^*(\xi)$, which is trivial in this case, and the reversed inequality, which becomes obvious if we notice that for a reduced fraction $a/b\in\mathbb{Q}$ such that $|\xi-a/b|_p<|\xi|_p$, we have $|a/b|_p=|\xi|_p$ and therefore $\min\{|a|_p,|b|_p\}\ge\min\{|\xi|_p,1/|\xi|_p\}$.

The second part of this proposition is deduced for example during computation of Hausdorff dimension of sets $\{\xi\in\mathbb{Q}_p : w_n(\xi)=w\}$, $w\ge n$, see [7, Theorem 9.6] or [2, §6]. ∎

If $w > \frac{1+\sqrt{5}}{2}$, we can give a simple construction of $\xi \in \mathbb{Q}_p$ such that $w_1^*(\xi) = w$.

Proposition 5.3. *Let $w > \frac{1+\sqrt{5}}{2}$ and*

$$\xi = \sum_{i=1}^{\infty} a_i p^{\lfloor (w+1)^i \rfloor} \in \mathbb{Q}_p,$$

where $a_i \in \{1, \dots, p-1\}$ for all $i \geq 1$. Then $w_1(\xi) = w_1^*(\xi) = w$.

Proof. Take any $w > \frac{1+\sqrt{5}}{2}$ and let $\xi_k = \sum_{i=1}^{k} a_i p^{\lfloor (w+1)^i \rfloor}$. All the implicit constants in $\ll$ and $\asymp$ in this proof depend at most on p. Since

$$|\xi - \xi_k|_p = p^{-\lfloor (w+1)^{k+1} \rfloor} \asymp \xi_k^{-w-1}$$

for any $k \geq 1$, we have $w_1^*(\xi) \geq w$.

For a reduced fraction $a/b \in \mathbb{Q}$ whose height is large enough, let $l \geq 1$ be such that

$$\xi_l \leq \mathrm{H}(a/b) < \xi_{l+1}.$$

Suppose that

$$\Big|\xi - \frac{a}{b}\Big|_p = \mathrm{H}\left(\frac{a}{b}\right)^{-\nu},$$

where $\nu > w + 1$. We have

$$\begin{aligned} |\xi - \xi_l|_p = |\xi_{l+1} - \xi_l|_p = p^{-\lfloor (w+1)^{l+1} \rfloor} &\asymp \xi_l^{-w-1}, \\ |\xi - \xi_{l+1}|_p = p^{-\lfloor (w+1)^{l+2} \rfloor} &\asymp \xi_{l+1}^{-w-1} \asymp \xi_l^{-(w+1)^2}. \end{aligned}$$

Therefore,

$$\begin{aligned} \frac{1}{|b|\xi_l + |a|} \leq \Big|\frac{b\xi_l - a}{b}\Big|_p = \Big|\xi_l - \frac{a}{b}\Big|_p &\leq \max\{|\xi - \xi_l|_p, \Big|\xi - \frac{a}{b}\Big|_p\} \qquad (5.27) \\ &\ll \max\{\xi_l^{-w-1}, \mathrm{H}(a/b)^{-\nu}\} = \xi_l^{-w-1} \quad \text{and} \\ \frac{1}{|b|\xi_{l+1} + |a|} \leq \Big|\xi_{l+1} - \frac{a}{b}\Big|_p &\leq \max\{|\xi - \xi_{l+1}|_p, \Big|\xi - \frac{a}{b}\Big|_p\} \qquad (5.28) \\ &\ll \max\{\xi_{l+1}^{-w-1}, \mathrm{H}(a/b)^{-\nu}\}. \end{aligned}$$

From (5.27) we get

$$\xi_l^{w+1} \ll |b|\xi_l + |a| \ll \mathrm{H}(a/b)(\xi_l + 1) \ll \mathrm{H}(a/b)\xi_l, \qquad \text{i.e.}$$

$$\xi_l^{w} \ll \mathrm{H}(a/b). \qquad (5.29)$$

From (5.28) we get

$$\min\{\xi_{l+1}^{w+1}, \mathrm{H}(a/b)^{\nu}\} \ll |b|\xi_{l+1} + |a| \ll \mathrm{H}(a/b)\xi_{l+1}.$$

Since $\xi_{l+1}^{w} \ll \mathrm{H}(a/b)$ does not hold, we must have

$$\mathrm{H}(a/b)^{\nu} \ll \mathrm{H}(a/b)\xi_{l+1}, \qquad \text{i.e.}$$

$$\mathrm{H}(a/b) \ll \xi_{l+1}^{\frac{1}{\nu-1}} \ll \xi_{l+1}^{\frac{1}{w}} \ll \xi_{l}^{\frac{w+1}{w}}. \tag{5.30}$$

If there is an infinite sequence $\frac{a_k}{b_k} \in \mathbb{Q}$ such that

$$\limsup_{k\to\infty} \frac{-\log|\xi - \frac{a_k}{b_k}|_p}{\log \mathrm{H}(a_k/b_k)} > w,$$

then $\mathrm{H}(a_k/b_k) \to \infty$ when $k \to \infty$ and we conclude from (5.29) and (5.30) that $w \le \frac{w+1}{w}$ which implies $w \le \frac{1+\sqrt{5}}{2}$, contrary to our choice of w.

Hence, it must hold that $w_1^*(\xi) = w$. ∎

5.5 On $w_2 - w_2^*$

Lemma 5.2. *There exists a family of irreducible integer polynomials*

$$P_m(X) = X^2 + a_m X + b_m, \quad m \ge 1$$

with roots in $\mathbb{Q}_p$ such that $a_m + 1 \ge |b_m|$, $a_m \asymp p^m$ and

$$\mathrm{sep}_p(P_m) \asymp \mathrm{H}(P_m)^{-1},$$

where the implicit constants depend only on p.

Proof. We first examine the case $p \neq 2$. Let g be the smallest prime such that $g \equiv 1 \pmod{4p}$. Its existence is guaranteed by Dirichlet's theorem on primes in arithmetic progressions.

Let

$$l_m = \Big\lfloor \frac{p^m\sqrt{g}}{2} + \frac{1}{2} \Big\rfloor.$$

Then it is easy to see that

$$(2l_m - 1)^2 \le p^{2m} g < (2l_m + 1)^2$$

and we put $a_m = 2l_m - 1$ if $p^{2m}g \le \frac{1}{2}\big((2l_m-1)^2 + (2l_m+1)^2\big) = 4l_m^2 + 1$. Otherwise, we put $a_m = 2l_m + 1$. Since $(2l_m+1)^2 - (2l_m-1)^2 = 8l_m$, if we

now set $b_m = \frac{1}{4}(a_m^2 - p^{2m}g)$, it must be $|b_m| \leq \frac{1}{4}8l_m = 2l_m \leq a_m + 1$, while $b_m \in \mathbb{Z}$ is assured by $a_m^2 \equiv (2l_m \pm 1)^2 \equiv 1 \pmod 4$ and $p^{2m}g \equiv (\pm 1)^{2m}1 \equiv 1 \pmod 4$.

Hensel's Lemma 0.5 ensures that the polynomial $Q(X) = X^2 - g$ has roots $\delta \in 1 + p\mathbb{Z}_p$ and $-\delta \in -1 + p\mathbb{Z}_p$. Thus the polynomial

$$P_m(X) = X^2 + a_m X + b_m = \frac{1}{4}\big((2X + a_m)^2 - p^{2m}g\big) = \frac{p^{2m}}{4}Q\Big(\frac{2X + a_m}{p^m}\Big)$$

has roots $\frac{-a_m \pm p^m\delta}{2}$, which are in $\mathbb{Q}_p$ and their distance is

$$\mathrm{sep}_p(P_m) = |p^m\delta|_p = p^{-m} \asymp a_m^{-1} \asymp \mathrm{H}(P_m)^{-1}.$$

If $p = 2$, we take $l_m = \lfloor 2^m\sqrt{17}\rfloor$, and put either $a_m = 2l_m$ or $a_m = 2l_m + 2$ depending for which choice a_m^2 is closer to $2^{2(m+1)}17$. Taking $b_m^2 = \frac{a_m^2}{4} - 2^{2m}17$, it can easily be checked that all the claims of this lemma are fulfilled. ∎

We will prove the next theorem which is analogous to a result for the real numbers from [6].

Theorem 5.2. *The set of values taken by the function $w_2 - w_2^*$ contains the interval $[0, 1[$.*

In view of (4.1), Theorem 5.2 is essentially best possible. Unfortunately, our method of proof does not enable us to deduce whether there exist $\xi \in \mathbb{Q}_p$ such that $w_2(\xi) = w_2^*(\xi) + 1$.

The proof of Theorem 5.2 basically follows that of Theorems 4.1 and 5.1. The key point is the existence of a family of quadratic integer polynomials from Lemma 5.2 having two p-adic roots very close to each other. We will not give a full proof of this theorem, but merely explain which lines from the Proposition 5.1, Theorem 5.1 and their proofs need to be modified beyond the simple substitution $n = 2$.

Proposition 5.4. *Let μ, ν, χ be real numbers such that $\mu \in]1/2, 1[$, $\nu > 1$ and χ is sufficiently large with respect to μ, for example $\chi > 12(2 + \frac{\mu}{1-\mu})$.*

Then there exist a positive number $\lambda < 1/2$, an increasing sequence of integers $g_1, g_2, \ldots$, and a sequence of integers $c_1, c_2, \ldots$ such that the following conditions are satisfied for any integer $j \geq 1$:

(I_j) $c_j \in [g_j/2, g_j]$ and γ_j is one root of polynomial $P_{m_j}(X) = X^2 + a_{m_j}X + b_{m_j}$ from Lemma 5.2 where m_j is such that $a_{m_j} \asymp g_j^{\frac{\mu}{1-\mu}}$.

(II_1) $\xi_1 = -c_1 + \gamma_1$.

(II_j) $\xi_j = -c_j + \gamma_j$ belongs to the annulus $I_{j-1} \subseteq \mathbb{Q}_p$ defined by

$$\frac{1}{2p}g_{j-1}^{-\nu} \leq |x - \xi_{j-1}|_p < g_{j-1}^{-\nu}.$$

(III_1) $|\xi_1 - \alpha|_p \geq 2\lambda H(\alpha)^{-\chi}$ *for any algebraic number* $\alpha \neq \xi_1$ *of degree* ≤ 2.
(III_j) $|\xi_j - \alpha|_p \geq \lambda H(\alpha)^{-\chi}$ *for any algebraic number* $\alpha \notin \{\xi_1, \ldots, \xi_j\}$ *of degree* ≤ 2 $(j \geq 2)$.

Proof (sketch). For ease of writing, denote $\tau = 2 + \frac{\mu}{1-\mu}$. The main difference from the proof of Proposition 5.1 is that inequalities (5.9) no longer hold. Therefore, we need to make the following modifications:

$$(\lambda g_{j-1}^{\nu})^{1/\chi} \leq \mathrm{H}(\alpha) \leq \big(c(\mu)^{-1} g_j^{2\tau}\big)^{1/(\chi-2)} \tag{5.5'}$$

$$\chi - 2 > 6\tau \tag{5.6'}$$

$$\mathrm{H}(\xi_j) \leq 8\,\mathrm{H}(\gamma_j) g_j^2 < \hat{c}(\mu) g_j^{\tau}$$

$$|\xi_j - \alpha|_p \geq \tilde{c}\,\mathrm{H}(\xi_j)^{-2}\,\mathrm{H}(\alpha)^{-2} \geq c(\mu) g_j^{-2\tau}\,\mathrm{H}(\alpha)^{-2} \tag{5.7'}$$

$$\mathrm{H}(\alpha)^{\chi-2} \geq c(\mu)^{-1} g_j^{2\tau} \tag{5.9'}$$

$$|x - \alpha|_p \geq c(\mu) g_j^{-2\tau}\,\mathrm{H}(\alpha)^{-2}/2 \tag{5.18'}$$

$$2 g_j^{-\nu} \leq c(\mu) g_j^{-2\tau}\,\mathrm{H}(\alpha)^{-2} \tag{5.19'}$$

$$\frac{2}{\chi - 3 - \varepsilon} < 1 - 2\tau \frac{3 + \varepsilon}{\chi - 3 - \varepsilon} \tag{5.20'}$$

$$c(\mu) g_j^{-2\tau}\,\mathrm{H}(\alpha)^{-2} \geq 4\lambda\,\mathrm{H}(\alpha)^{-\chi} \tag{5.21'}$$

$$(\chi - 2)(\chi - 3 - \varepsilon) > 2\tau\chi(3 + \varepsilon) \tag{5.22'}$$

We see that for example $\chi > 12\tau = 12(2 + \frac{\mu}{1-\mu})$ satisfies all the conditions (5.6') (5.20'), (5.22') for ε small enough, say $0 < \varepsilon < 1$. ∎

Proof of Theorem 5.2 (sketch). The function $w_2 - w_2^*$ certainly takes all values from $[0, 1/2]$ according to Theorem 4.1, so we are only concerned with the interval $]1/2, 1[$. Pick μ from that interval, χ large enough, $w_2 \geq \chi + 1$, $w_2^* = w_2 - \mu$ and $\nu = \frac{1}{1-\mu}(w_2^* + 1)$. Apply Proposition 5.4 and set $\xi = \lim_{j\to\infty} \xi_j \in \mathbb{Q}_p$.

The minimal polynomial of ξ_j over $\mathbb{Z}$ is

$$Q_j(X) := P_{m_j}(X + c_j) = (X + c_j)^2 + a_{m_j}(X + c_j) + b_{m_j}.$$

Noting that we employ the usual notation for algebraic conjugates and that the implicit constants in $\asymp$ depend only on p and μ, it holds

$$\mathrm{H}(\xi_j) = \mathrm{H}(Q_j) \asymp c_j \max\{a_{m_j}, c_j\} \asymp c_j a_{m_j} \asymp g_j^{\frac{1}{1-\mu}}$$

since $a_{m_j} \asymp g_j^{\frac{\mu}{1-\mu}}$, $c_j \asymp g_j$ and $\mu \in]1/2, 1[$. Also,

$$
\begin{aligned}
&|\xi - \xi_j|_p \asymp g_j^{-\nu} \asymp \mathrm{H}(\xi_j)^{-w_2^*-1},\\
&|\xi - \xi_j'|_p = |\xi_j - \xi_j'|_p = |\gamma_j - \gamma_j'|_p = \mathrm{sep}_p(P_{m_j}) \asymp a_{m_j}^{-1},\\
&|Q_j(\xi)|_p = |\xi - \xi_j|_p |\xi - \xi_j'|_p \asymp \mathrm{H}(\xi_j)^{-w_2^*-1} a_{m_j}^{-1} \asymp \mathrm{H}(Q_j)^{-w_2^*-\mu-1}.
\end{aligned}
$$

Therefore, $w_2(\xi) \geq w_2^* + \mu = w_2$ and the rest of the proof, just like all the details, is the same as the proof of Theorem 5.1. ■

Chapter 6

Some results on w_n^*

Mahler proved in [20] that his classification of real numbers has the property that every two algebraically dependent numbers belong to the same class. In order to prove this basic property he showed that if ξ and η are transcendental real numbers such that $P(\xi, \eta) = 0$ for an irreducible polynomial $P(x, y) \in \mathbb{Z}[x, y]$ of degree M in x and N in y, then the inequalities

$$w_n(\xi) + 1 \leq M(w_{nN}(\eta) + 1) \quad \text{and} \quad w_n(\eta) + 1 \leq N(w_{nM}(\xi) + 1) \tag{6.1}$$

are valid for every positive integer n. Schmidt [29, (4), p. 276] showed that these conditions also imply inequalities

$$w_n^*(\xi) + 1 \leq M(w_{nN}^*(\eta) + 1) \quad \text{and} \quad w_n^*(\eta) + 1 \leq N(w_{nM}^*(\xi) + 1), \tag{6.2}$$

i.e. the analogous inequalities we get when Mahler's function w_k is replaced with Koksma's function w_k^*.

Mahler himself [21] proved the inequalities (6.1) under analogous conditions in the p-adic setting. We will establish in this chapter a p-adic version of (6.2). Let us mention that our proof is in different fashion from what Mahler did in [21] and is more in vein with [29].

Our first lemma is valid for every algebraic number, whether we take it from $\mathbb{C}$ or $\mathbb{C}_p$.

Lemma 6.1. *Let α be an algebraic number of degree n and let*

$$P(x) = a_n x^n + \cdots + a_0 = a_n(x - \alpha)(x - \alpha_2) \cdots (x - \alpha_n)$$

be its minimal polynomial over $\mathbb{Z}$. Then if $k_1, \ldots, k_t$ are distinct numbers among $1, \ldots, n$, the number $a_n \alpha_{k_1} \cdots \alpha_{k_t}$ is an algebraic integer.

Proof. See [31, Hilfssatz 17, p. 77]. ∎

The second lemma deals with the standard representation of symmetric polynomials through elementary symmetric polynomials but with an important observation that will later be required.

Lemma 6.2. *Let $P(t_1, \dots, t_k) \in \mathbb{Z}[t_1, \dots, t_k]$ be a homogeneous symmetric polynomial. Denote*

$$\deg_{t_1} P = \cdots = \deg_{t_k} P = d.$$

There exists a unique polynomial $Q(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ such that

$$P(t_1, \dots, t_k) = Q(s_1, \dots, s_k),$$

where $s_i = s_i(t_1, \dots, t_k)$ $(1 \leq i \leq k)$ are elementary symmetric polynomials of $t_1, \dots, t_k$. For every monomial $s_1^{i_1} \cdots s_k^{i_k}$ in $Q(s_1, \dots, s_k)$, we have $i_1 + \cdots + i_k \leq d$.

Proof. See [19, Theorem 6.1, §IV.6, p. 191], [14, Theorem 3.3.1, p. 25], [11, Exercise 13, §7.1, p. 326]. ∎

Now we prove the announced result.

Theorem 6.1. *Let $\xi, \eta \in \mathbb{Q}_p$ be two transcendental numbers which are algebraically dependent. Suppose $P(x, y) \in \mathbb{Z}[x, y]$ is a non-zero polynomial irreducible over $\mathbb{Q}$, of degree M in x and degree N in y such that $P(\xi, \eta) = 0$. Then for every positive integer n, it holds*

$$w_n^*(\xi) + 1 \leq M(w_{nN}^*(\eta) + 1) \quad \textit{and} \quad w_n^*(\eta) + 1 \leq N(w_{nM}^*(\xi) + 1).$$

Proof. Of course, it is enough to prove only the first inequality since the second follows by interchanging ξ and η.

Fix a positive integer n. It is not hard to see from Lemma 0.3 that for any integer $l \neq 0$ we have $w_n^*(\xi) = w_n^*(l\xi)$ and $w_n^*(\eta) = w_n^*(l\eta)$. Hence, by taking l to be a large power of p and multiplying the polynomial $P(x, y)$ by the appropriate power of p, we see that without loss of generality we can suppose $\xi, \eta \in \mathbb{Z}_p$.

The partial derivatives of $P(x, y)$ do not vanish at (ξ, η). Suppose to the contrary that $\frac{\partial}{\partial y} P(x, y)$ vanishes at (ξ, η). By considering $P(\xi, y)$ as a polynomial in y with coefficients in $\mathbb{Q}(\xi)$, one sees that $P(\xi, y) = P_1^*(\xi, y) P_2^*(\xi, y)$, where $P_1^*(\xi, y)$, $P_2^*(\xi, y)$ are polynomials of positive degree in y, with coefficients in $\mathbb{Q}(\xi)$. Since ξ is transcendental, $\mathbb{Q}(\xi)$ is isomorphic to $\mathbb{Q}(x)$, so in fact we have $P(x, y) = P_1^*(x, y) P_2^*(x, y)$, where $P_1^*(x, y), P_2^*(x, y) \in \mathbb{Q}(x)[y]$. But $\mathbb{Q}(x)$ is the fraction field of $Q[x]$, so by Gauss's Lemma 0.1 we can

find polynomials $P_1(x,y), P_2(x,y) \in \mathbb{Q}[x,y]$ of positive degree in y and with $P(x,y) = P_1(x,y)P_2(x,y)$. This contradicts the irreducibility of $P(x,y)$.

Let $H > 1$ and suppose $\beta \in \mathbb{Q}_p$ is an algebraic number with $\deg(\beta) \leq n$, $\mathrm{H}(\beta) \leq H$ such that $w_n^*(\xi, H) = |\xi - \beta|_p$. Obviously, if H is large enough, $w_n^*(\xi, H)$ becomes as small as we want, and since $\xi \in \mathbb{Z}_p$, we can assume $\beta \in \mathbb{Z}_p$ as well. Since $P(x,y)$ and $\frac{\partial}{\partial y}P(x,y)$ are polynomials, there exist ε, c_1, c_2 all positive real numbers depending only on $P(x,y)$ (in other words, only on ξ and η) such that for any $u \in \mathbb{Q}_p$

$$|u-\xi|_p < \varepsilon \;\Rightarrow \begin{cases} |P(u,\eta)|_p = |P(u,\eta) - P(\xi,\eta)|_p < c_1|u-\xi|_p, \\ \left|\dfrac{\partial}{\partial y}P(u,\eta) - \dfrac{\partial}{\partial y}P(\xi,\eta)\right|_p < \dfrac{1}{2}\left|\dfrac{\partial}{\partial y}P(\xi,\eta)\right|_p = c_2 > 0. \end{cases}$$

If we take H large enough, we get

$$|\xi - \beta|_p < \min\left\{\varepsilon, \frac{c_2^2}{2c_1}\right\},$$

which implies

$$|P(\beta,\eta)|_p < c_1|\beta-\xi|_p < \frac{c_2^2}{2} \qquad \text{and} \qquad \left|\frac{\partial}{\partial y}P(\beta,\eta)\right|_p > c_2.$$

Therefore,

$$\left|\frac{P(\beta,\eta)}{\left(\frac{\partial}{\partial y}P(\beta,\eta)\right)^2}\right|_p < \frac{1}{2}$$

and if we look at $P(\beta,y)$ as a polynomial in y, we see that the conditions of Lemma 0.5 are fulfilled. This lemma implies there is a $\beta' \in \mathbb{Z}_p$ such that $P(\beta,\beta') = 0$ and

$$|\beta' - \eta|_p \leq \left|\frac{P(\beta,\eta)}{\left(\frac{\partial}{\partial y}P(\beta,\eta)\right)^2}\right|_p < \frac{c_1}{c_2^2}|\beta-\xi|_p \ll |\beta-\xi|_p = w_n^*(\xi,H),$$

where the implied constants in $\ll$ and $\gg$ everywhere they appear in this proof depend at most on ξ, η and n.

Let $Q(x) = a_k(x-\beta_1)\cdots(x-\beta_k)$ $(k \leq n)$ be the minimal polynomial of $\beta = \beta_1$ over $\mathbb{Z}$. The number β' is a root of the polynomial $P(\beta,y)$ in y, hence a root of the polynomial

$$R(y) = a_k^M P(\beta_1,y)P(\beta_2,y)\cdots P(\beta_k,y).$$

The polynomial $P(\beta, y)$ is not identically zero, since $P(x, y)$ would otherwise be divisible by the minimal polynomial of β. Thus $R(y)$ is not identically zero. The coefficients of $R(y)$ are linear combinations with rational integer coefficients of terms of the type

$$a_k^M \sum_\sigma \beta_{\sigma(1)}^{i_1} \cdots \beta_{\sigma(k)}^{i_k},$$

where the sum is taken over all permutations σ of $\{1, \dots, k\}$ while $0 \le i_j \le M$ for $1 \le j \le k$. But, because of Lemma 6.2 and Vietè's formulas for the polynomial $Q(x)$, such terms are rational integers themselves and $\ll \mathrm{H}(Q)^M \le H^M$. Therefore, $R(y) \in \mathbb{Z}[y]$ and $\mathrm{H}(R) \ll H^M$. Since $R(\beta') = 0$, we see that β' is algebraic and its minimal polynomial over $\mathbb{Z}$ is a factor of $R(y)$. Using Gauss's Lemma 0.1 and Gelfond's Lemma 0.2, we get that this minimal polynomial also has coefficients $\ll H^M$. Hence $\mathrm{H}(\beta') \ll H^M$, say $\mathrm{H}(\beta') \le cH^M$. Thus

$$\begin{aligned} w_{nN}^*(\eta, cH^M) \le w_{kN}^*(\eta, cH^M) \le |\eta - \beta'|_p \ll w_n^*(\xi, H) \Rightarrow \\ w_{nN}^*(\xi) + 1 = \limsup_{H\to\infty} \frac{-\log(w_{nN}^*(\xi, cH^M))}{\log(cH^M)} \\ \ge \frac{1}{M} \limsup_{H\to\infty} \frac{-\log(w_n^*(\xi, H))}{\log H} = \frac{1}{M}(w_n^*(\xi) + 1). \end{aligned}$$

■

We are able to show that the inequalities in (6.2) are sharp at least in a very special situation.

Proposition 6.1. *Let $k \ge 1$ be an integer, w be a real number such that*

$$w > -1 + k + \frac{k^2 + k\sqrt{k^2 + 4k}}{2}$$

and

$$\xi = a_0 + \sum_{i=1}^{\infty} a_i p^{\lfloor (w+1)^i \rfloor} \in \mathbb{Q}_p,$$

where $a_i \in \{1, \dots, p-1\}$ for all $i \ge 0$. Then $w_1^*(\xi) = w$ and $w_1^*(\xi^k) = \frac{w+1}{k} - 1$.

Proof. It has been shown in Proposition 5.3 that $w_1^*(\xi) = w$. We claim that $w_1^*(\xi^k) = \frac{w+1}{k} - 1$ and, thus,

$$w_1^*(\xi) + 1 = k\big(w_1^*(\xi^k) + 1\big),$$

so that inequality (6.2.i) becomes an equality for this special choice of $\eta = \xi^k$ and $n = 1$.

Using similar notation as in Proposition 5.3, we have

$$\begin{aligned} |\xi^k - \xi_l^k|_p &= |(\xi_l + \rho_l p^{\lfloor (w+1)^{l+1} \rfloor})^k - \xi_l^k|_p \\ &\asymp p^{-\lfloor (w+1)^{l+1} \rfloor} \\ &\asymp \xi_l^{-(w+1)} \asymp (\xi_l^k)^{-\frac{w+1}{k}}, \end{aligned}$$

with ρ_l being some element in $\mathbb{Z}_p \setminus p\mathbb{Z}_p$ and constants in $\asymp$ depending only on p and k. Hence,

$$w_1^*(\xi^k) \geq \frac{w+1}{k} - 1.$$

In order to show that the last inequality is actually an equality, we proceed just like in the proof of Proposition 5.3. Let $a/b \in \mathbb{Q}$ be a reduced fraction such that

$$\xi_l^k \leq \mathrm{H}(a/b) < \xi_{l+1}^k$$

and

$$\left|\xi - \frac{a}{b}\right|_p = \mathrm{H}\left(\frac{a}{b}\right)^{-\nu},$$

where $\nu > \frac{w+1}{k}$.

Instead of (5.29), we now have

$$(\xi_l^k)^{\frac{w+1}{k}-1} \leq \mathrm{H}(a/b)$$

and instead of (5.30),

$$\mathrm{H}(a/b) \leq (\xi_l^k)^{\frac{k(w+1)}{w+1-k}}$$

where we used the fact that $w + 1 > 2k$ which obviously holds if w satisfies the conditions of this proposition.

If we had $w_1^*(\xi^k) > \frac{w+1}{k} - 1$, we could conclude that

$$\frac{w+1}{k} - 1 \leq \frac{k(w+1)}{w+1-k}$$

which contradicts the lower bound on w imposed in the statement of this proposition. ∎

Remark 6.1. Set

$$\xi = a_0 + \sum_{i=1}^{\infty} a_i 10^{-\lfloor (w+1)^i \rfloor} \in \mathbb{R},$$

where $a_i \in \{1, 2, \ldots, 9\}$ for all $i \geq 0$ and the same condition on w as in Proposition 6.1. Proceeding completely analogously as in the proof of Proposition 6.1, we get a new example in the real numbers for which equality in (6.2.i) holds. See also [7, §3.7,§7.7].

Bibliography

[1] R. C. Baker, *On approximation with algebraic numbers of bounded degree*, Mathematika **23** (1976), no. 1, 18–31.

[2] V. I. Bernik and M. M. Dodson, Metric Diophantine approximation on manifolds. Cambridge Tracts in Mathematics, 137. Cambridge University Press, Cambridge, 1999.

[3] E. Bombieri and W. Gubler, Heights in Diophantine geometry. New Mathematical Monographs, 4. Cambridge University Press, Cambridge, 2006.

[4] Y. Bugeaud, *Mahler's classification of numbers compared with Koksma's*, Acta Arith. **110** (2003), 89–105.

[5] Y. Bugeaud, *Mahler's classification of numbers compared with Koksma's, II*, In: Diophantine approximation. Festschrift for Wolfgang Schmidt. Ed. H.-P. Schlickewei, K. Schmidt and R. F. Tichy, Developments in Mathematics 16, pp. 107–121 (2008), Springer Wien.

[6] Y. Bugeaud, *Mahler's classification of numbers compared with Koksma's, III*, Publ. Math. Debrecen **65** (2004), 305–316.

[7] Y. Bugeaud, Approximation by algebraic numbers. Cambridge Tracts in Mathematics, Cambridge, 2004.

[8] Y. Bugeaud and A. Dujella, *Root separation for irreducible integer polynomials*, Bull. Lond. Math. Soc., to appear.

[9] Y. Bugeaud and M. Mignotte, *Polynomial root separation*, Intern. J. Number Theory **6** (2010), 587–602.

[10] J. W. S. Cassels, Local fields. London Mathematical Society Student Texts, 3. Cambridge University Press, Cambridge, 1986.

[11] D. Cox, J. Little, and D. O'Shea, Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra. Third edition. Undergraduate Texts in Mathematics. Springer, New York, 2007.

[12] K. Dörge, *Über die Seltenheit der reduziblen Polynome und der Normalgleichungen*, Math. Ann. **95** (1926), no. 1, 247256.

[13] A. Dujella and T. Pejković, *Root separation for reducible monic quartics*, Rend. Semin. Mat. Univ. Padova, to appear.

[14] J.-P. Escofier, Théorie de Galois. Cours avec exercices corrigés. Enseignement des Mathématiques. Masson, Paris, 1997.

[15] J.-H. Evertse, *Distances between the conjugates of an algebraic number*, Publ. Math. Debrecen **65** (2004), 323–340.

[16] F. Q. Gouvêa, p-adic numbers. An introduction. Second edition. Universitext. Springer-Verlag, Berlin, 1997.

[17] N. Koblitz, p-adic numbers, p-adic analysis, and zeta-functions. Second edition. Graduate Texts in Mathematics, 58. Springer-Verlag, New York, 1984.

[18] J. F. Koksma, *Über die Mahlersche Klasseneinteilung der transzendenten Zahlen und die Approximation komplexer Zahlen durch algebraische Zahlen*, Monatsh. Math. Phys. **48**, (1939), 176–189.

[19] S. Lang, Algebra. Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002.

[20] K. Mahler, *Zur Approximation der Exponentialfunktion und des Logarithmus. I, II*, J. Reine Angew. Math. **166** (1932), 118–150.

[21] K. Mahler, *Über eine Klassen-Einteilung der p-adischen Zahlen*, Mathematica Leiden **3** (1935), 177–185.

[22] K. Mahler, *An inequality for the discriminant of a polynomial*, Michigan Math. J. **11** (1964), 257–262.

[23] M. Mignotte, Mathematics for computer algebra. Springer-Verlag, New York, 1992.

[24] J. F. Morrison, *Approximation of p-adic numbers by algebraic numbers of bounded degree*, J. Number Theory **10** (1978), no. 3, 334–350.

[25] H. Osada, *The Galois groups of the polynomials* X^n+aX^l+b, J. Number Theory **25** (1987), no. 2, 230–238.

[26] T. Pejković, *On p-adic T-numbers*, preprint.

[27] V. V. Prasolov, Polynomials. Algorithms and Computation in Mathematics, 11. Springer-Verlag, Berlin, 2004.

[28] H. P. Schlickewei, *p-adic T-numbers do exist*, Acta Arith. **39** (1981), no. 2, 181–191.

[29] W. M. Schmidt, *Mahler's T-numbers*, 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), pp. 275–286. Amer. Math. Soc., Providence, R.I., 1971.

[30] W. M. Schmidt, Diophantine Approximations and Diophantine Equations. Lecture Notes in Math. 1467, Springer, Berlin, 1991.

[31] T. Schneider, Einführung in die transzendenten Zahlen. Springer-Verlag, Berlin-Göttingen-Heidelberg, 1957.

[32] A. Schönhage, *Polynomial root separation examples*, J. Symbolic Comput. **41** (2006), 1080–1090.

[33] Th. Skolem, *Untersuchungen über die möglichen Verteilungen ganzzahliger Lösungen gewisser Gleichungen*, Videnskapsselskapets Skr. I (1921), Nr. 17, 57 S.

[34] U. Zannier, *On the Hilbert irreducibility theorem*, Rend. Semin. Mat. Univ. Politec. Torino **67** (2009), no. 1, 1–14.

Acknowledgements

I was a member of the European Doctoral College of the University of Strasbourg during the preparation of my PhD, from 2007 to 2011, class name Marco Polo. I have benefited from specific financial supports offered by the College and, along with my mainstream research, have followed a special course on topics of general European interests presented by international experts. This PhD research project has been led with the collaboration of two universities: University of Zagreb, Croatia and the University of Strasbourg, France.

I am grateful to my supervisors, professor Yann Bugeaud at the University of Strasbourg and professor Andrej Dujella at the University of Zagreb, for their commitment and direction of my research.

I wish to thank my parents Radoslav and Ana, and my brothers Branimir and Marko, for their love and support. I also thank my aunt Ruža for her encouragement.

Summary

Polynomial root separation and applications

In this thesis we study bounds on the distances of roots of integer polynomials and applications of such results. Denote by $\mathrm{sep}(P)$ the minimal distance of roots of the separable integer polynomial $P(X)$ and by $\mathrm{H}(P)$ maximum of the absolute values of its coefficients.

In the first chapter which looks at polynomial roots in the set of complex numbers, we first summarize results on quadratic and cubic polynomials. The bulk of this chapter is dedicated to quartic polynomials and especially reducible monic integer polynomials of fourth degree. We show that for such polynomials $\mathrm{sep}(P) \gg \mathrm{H}(P)^{-2}$ but also construct families $(P_k(X))$ of such polynomials that have $\mathrm{sep}(P) \asymp \mathrm{H}(P)^{-2}$. The case when coefficients of $P_k(X)$ are polynomials in k is studied more thoroughly.

In the second chapter different lemmas on roots of polynomials in the p-adic setting are proved. These lemmas are mostly analogues of the results in the real and complex case and are used later in the thesis.

In the third chapter explicit families of polynomials of general degree n are given which bound the exponent above $\mathrm{H}(P)$ from the other side than $\mathrm{sep}_p(P) \gg \mathrm{H}(P)^{-n+1}$. Results are proved using Newton polygons. Then the case of quadratic and reducible cubic polynomials in the p-adic setting is completely solved which shows that the bound above is really attained in those classes of polynomials. For irreducible cubic polynomials a bound with a new, better exponent is exhibited.

The rest of the thesis is concerned with results on p-adic versions of Mahler's and Koksma's functions w_n and w_n^* and the related classifications of transcendental numbers in $\mathbb{C}_p$.

In the fourth chapter the main result is a construction of numbers such that the two functions w_n and w_n^* differ on them for every n. We can even require $w_n - w_n^*$ to be a chosen number in some small interval. The proof is quite involved and follows R. C. Baker's proof in the real case.

In the fifth chapter the interval of possible values for $w_n - w_n^*$ is expanded using an effective estimate for the distance of algebraic numbers and a family of polynomials with very close roots. The main proof in this chapter follows the one in the previous chapter, but is a little easier since we restrict ourselves to one or finitely many n. Special attention is given to cases $n = 1$ and $n = 2$.

In the last chapter inequalities linking values of Koksma's functions for algebraically dependent numbers are proved.

Résumé

Séparation des racines des polynômes et applications

Dans cette thèse, nous étudions les bornes sur les distances des racines des polynômes entiers et les applications de ces résultats. Notons par $\mathrm{sep}(P)$ la distance minimale des racines du polynôme entier séparable $P(X)$ et par $\mathrm{H}(P)$ le maximum des valeurs absolues de ses coefficients.

Dans le premier chapitre, qui examine les racines des polynômes dans l'ensemble des nombres complexes, nous avons d'abord résumé les résultats sur les polynômes quadratiques et cubiques. L'essentiel de ce chapitre est consacré aux polynômes quartiques et surtout aux polynômes réductibles normalisés de quatrième degré à coefficients entiers. Nous avons montré que pour de tels polynômes $\mathrm{sep}(P) \gg \mathrm{H}(P)^{-2}$, mais aussi construit des familles $(P_k(X))$ de tels polynômes qui ont $\mathrm{sep}(P) \asymp \mathrm{H}(P)^{-2}$. Le cas où les coefficients de $P_k(X)$ sont polynômes en k est étudié plus à fond.

Dans le deuxième chapitre différents lemmes sur les racines des polynômes en nombres p-adiques sont prouvés. Ces lemmes sont pour la plupart analogues aux résultats dans le cas réel et complexe et sont utilisés plus tard dans la thèse.

Dans le troisième chapitre sont données les familles explicites de polynômes de degré n qui bornent l'exposant de $\mathrm{H}(P)$ de l'autre côté que $\mathrm{sep}_p(P) \gg \mathrm{H}(P)^{-n+1}$. Les résultats sont prouvés en utilisant des polygones de Newton. Ensuite, le cas des polynômes quadratiques et des polynômes cubiques réductibles dans les p-adiques est résolu complètement, ce qui montre que la limite présentée ci-dessus est vraiment atteinte dans ces classes de polynômes. Pour les polynômes cubiques irréductibles une borne avec un nouveau et meilleur exposant est fournie.

Le reste de la thèse est dédié aux résultats liés aux versions p-adiques des fonctions de Mahler et de Koksma w_n et w_n^*, ainsi qu'aux classifications correspondantes des nombres transcendants dans $\mathbb{C}_p$.

Dans le quatrième chapitre le résultat principal est une construction des nombres pour lesquelles les deux fonctions w_n et w_n^* sont différentes pour tous les n. Nous pouvons même exiger que $w_n - w_n^*$ prenne une valeur choisie dans un certain intervalle de petite taille. La preuve en est assez complexe et suit celle de R. C. Baker dans le cas réel.

Dans le cinquième chapitre l'intervalle de valeurs possibles pour $w_n - w_n^*$ est élargi en utilisant une estimation efficace pour la distance de nombres algébriques et une famille de polynômes à racines très proches. La principale preuve dans ce chapitre suit celle du chapitre précédent, mais est quelque peu plus simple car elle est limitée à un seul, ou à un nombre fini de n. Une attention particulière est accordée aux cas $n = 1$ et $n = 2$.

Dans le dernier chapitre sont prouvées les inégalités reliant les valeurs des fonctions de Koksma en nombres algébriquement dépendants.

Sažetak

Separacija korijena polinoma i primjene

U ovoj disertaciji se proučavaju ograde na udaljenosti korijena cjelobrojnih polinoma i primjene takvih rezultata. Označimo sa $\mathrm{sep}(P)$ minimalnu udaljenost korijena separabilnog cjelobrojnog polinoma $P(X)$, a s $\mathrm{H}(P)$ maksimum apsolutnih vrijednosti njegovih koeficijenata.

U prvom poglavlju promatraju se korijeni polinoma u skupu kompleksnih brojeva. Ukratko se donose rezultati o kvadratnim i kubnim polinomima, a glavnina poglavlja posvećena je polinomima četvrtog stupnja, posebice klasi reducibilnih normiranih polinoma četvrtog stupnja. Pokazuje se da za takve polinome vrijedi $\mathrm{sep}(P) \gg \mathrm{H}(P)^{-2}$, ali se i konstruira familija $(P_k(X))$ takvih polinoma za koju je $\mathrm{sep}(P) \asymp \mathrm{H}(P)^{-2}$. Detaljnije je proučen slučaj kada su koeficijeniti od $P_k(X)$ polinomi u k.

U drugom poglavlju dokazane su različite leme o korijenima polinoma u p-adskom slučaju. Ove su leme većinom analogoni rezultata u realnom i kompleksnom slučaju, a koriste se kasnije u disertaciji.

U trećem poglavlju dane su eksplicitne familije polinoma općeg stupnja n koje eksponent iznad $\mathrm{H}(P)$ ograđuju s druge strane od $\mathrm{sep}_p(P) \gg \mathrm{H}(P)^{-n+1}$. Rezultate se dokazuje korištenjem Newtonovih poligona. Zatim je potpuno riješen slučaj kvadratnih i reducibilnih kubnih polinoma s korijenima u skupu p-adskih brojeva. Pokazuje se da se za te klase polinoma gornje ograde zaista postižu. Dana je i nova ograda s boljim eksponentom za ireducibilne kubne polinome.

Drugi dio disertacije bavi se rezultatima vezanim uz p-adsku verziju Mahlerovih i Koksminih funkcija w_n i w_n^* te s njima povezanim klasifikacijama transcendentnih brojeva u $\mathbb{C}_p$.

U četvrtom poglavlju glavni je rezultat konstrukcija brojeva za koje se funkcije w_n i w_n^* razlikuju za svaki prirodan broj n. Može se zahtijevati i da vrijednost $w_n - w_n^*$ bude odabrani broj u nekom malom intervalu. Podulji dokaz slijedi dokaz koji je u realnom slučaju dao R. C. Baker.

U petom poglavlju interval mogućih vrijednosti od $w_n - w_n^*$ je povećan korištenjem efektivne ocjene za udaljenost algebarskih brojeva i familija polinoma s vrlo bliskim korijenima. Glavni dokaz u ovom poglavlju slijedi onaj iz prethodnog, ali je nešto jednostavniji jer se ograničuje na samo jedan ili konačno mnogo brojeva n. Posebna pozornost dana je slučajevima $n = 1$ te $n = 2$.

U posljednjem poglavlju dokazane su nejednakosti koje povezuju vrijednosti Koksminih funkcija za algebarski zavisne brojeve.

Biography

Tomislav Pejković was born in Zagreb, Republic of Croatia on 25 September 1981. He was educated at *Petar Preradović* elementary school and *V. gimnazija* high school in Zagreb. In September 2000 he enrolled into University of Zagreb where he studied mathematics and graduated in November 2005 with the thesis entitled *Roth's theorem* written under direction of professor Andrej Dujella.

During this time he took part in different national and international mathematical competitions and won various awards such as bronze medals at 1999 and 2000 International Mathematical Olympiads in Romania and South Korea. Among the scholarships that he received were the multi-annual City of Zagreb scholarship and *Top Scholarship for Top Student* for the year 2004/05. He worked as an undergraduate teaching assistant and directed a math group at his old high school with his students achieving success at competitions and olympiads. He wrote a short book *Irrational numbers* which was published in 2001 and several articles for Croatian journal for young mathematicians *Matka*. Two of his papers on inequalities with academician Josip Pečarić have been published in a scientific journal.

In 2005/06 he started PhD studies at the Department of Mathematics, University of Zagreb. The same year he was hired as teaching and research assistant at this department working within A. Dujella's projects *Diophantine equations* (until 2007) and *Diophantine equations and elliptic curves*. He completed all undergraduate and graduate exams with the best possible grade. The paper *Root separation for reducible monic quartics* which he coauthored with A. Dujella has been accepted for publication in Rend. Semin. Mat. Univ. Padova in 2010.

From 2007 until 2011 he was a member of the Executive Committee of Croatian Mathematical Society and since 2007 he is a member of state Committee for mathematical competitions. In 2010 he was the leader of the Croatian team at the International Mathematical Olympiad in Kazakhstan.

From the academic year 2007/08 he is enrolled in the PhD programme at the University of Strasbourg under the cotutelle agreement of the two universities with thesis directors Yann Bugeaud at the University of Strasbourg and Andrej Dujella at the University of Zagreb. He is the recipient of a grant by French government for two months in 2007 and starting in the same year he became a member of the European Doctoral College in Strasbourg for the duration of four years.

Tomislav Pejković participated in the following summer and winter schools: Combinatorics, Automata and Number Theory (Liège, Belgium, 2006), Solvability of Diophantine Equations (Leiden, Netherlands, 2007), Summer School in Analytic Number Theory and Diophantine Approximation (Ottawa, Canada, 2008), Winter School on Explicit Methods in Number Theory (Debrecen, Hungary, 2009).

Tomislav PEJKOVIĆ

POLYNOMIAL ROOT SEPARATION AND APPLICATIONS

Résumé

Nous étudions les bornes sur les distances des racines des polynômes entiers et les applications de ces résultats. La séparation des racines complexes pour les polynômes réductibles normalisés de quatrième degré à coefficients entiers est examinée plus à fond. Différents lemmes sur les racines des polynômes en nombres p-adiques sont prouvés. Sont fournies les familles explicites de polynômes de degré général, ainsi que les familles dans certaines classes de polynômes quadratiques et cubiques avec une très bon separation des racins dans le cadre p-adique. Le reste de la thèse est dédié aux résultats liés aux versions p-adiques des fonctions de Mahler et de Koksma w_n et w^*_n , ainsi qu'aux classifications correspondantes des nombres transcendants dans $\mathbf{C}_p$. Le résultat principal est une construction des nombres pour lesquelles les deux fonctions w_n et w^*_n sont différentes pour tous les n et puis l'intervalle de valeurs possibles pour w_n-w^*_n est élargi. Les inégalités reliant les valeurs des fonctions de Koksma en nombres algébriquement dépendants sont prouvées.

polynômes entiers – séparation des racines – nombres p-adiques – nombres transcendants – classification de Mahler – classification de Koksma

Résumé en anglais

We study bounds on the distances of roots of integer polynomials and applications of such results. The separation of complex roots for reducible monic integer polynomials of fourth degree is thoroughly explained. Lemmas on roots of polynomials in the p-adic setting are proved. Explicit families of polynomials of general degree as well as families in some classes of quadratic and cubic polynomials with very good separation of roots in the same setting are exhibited. The second part of the thesis is concerned with results on p-adic versions of Mahler's and Koksma's functions w_n and w^*_n and the related classifications of transcendental numbers in $\mathbf{C}_p$. The main result is a construction of numbers such that the two functions w_n and w^*_n differ on them for every n and later on expanding the interval of possible values for w_n-w^*_n. The inequalities linking values of Koksma's functions for algebraically dependent numbers are proved.

integer polynomials – root separation – p-adic numbers – transcendental numbers – Mahler's classification – Koksma's classification