Delft University of Technology
Faculty of Electrical Engineering, Mathematics and Computer Science
Delft Institute of Applied Mathematics

Periodicity and a Problem of Powers
a P-adic Perspective

A thesis submitted to the
Delft Institute of Applied Mathematics
in partial fulfillment of the requirements

for the degree

MASTER OF SCIENCE
in
APPLIED MATHEMATICS

by

ROLF YPMA

Delft, the Netherlands
June 2009

MSc THESIS APPLIED MATHEMATICS

"Periodicity and a Problem of Powers a P-adic Perspective"

ROLF YPMA

Delft University of Technology

Daily supervisor

Dr. R.J. Fokkink

Responsible professor

Prof. dr. M. Dekking

Other thesis committee members

Dr. K. Dajani

Dr. R. Koekoek

June 2009

Delft, the Netherlands

Preface

Here I will give an overview of the structure of this thesis.

Chapter one will introduce a well-known problem, and give some existing results.

Chapter two will introduce β-expansions, and end with some more recent results which I managed to extend.

Chapter three will introduce p-adic numbers, and end with the generalization of a theorem from chapter two. This generalization has turned out to be the focal point of my thesis.

Chapter four will give a new interesting approach to the problem from the introduction, using notions from the previous two chapters.

If challenged for time, the reader may skip many of the more algebraic sections, and just take those (well-known) theorems for granted.

Contents

Chapter 1

Introduction

Take an integer. Any integer.

Now multiply by one and a half. Round upwards, i.e. if the integer was odd, add a half.

Repeat into infinity.

Questions

1. Can you start with an integer such that you never get an odd number?
2. Can you start with an integer such that you never get two odd numbers in a row?

Answers

1. No. Let's say you could find such a number. Then question 2 would be trivial. But question 2 has been posed. Therefore there cannot be such a number.
2. Probably not. But nobody knows for sure.

The above question actually lies at the heart of an apparently easy, but hard to solve problem.

1.1 Mahler's problem

In his paper [9] Mahler poses a problem on powers of $\frac{3}{2}$. Given any $x \in \mathbb{R}$, look at the points $x, \frac{3}{2}x, (\frac{3}{2})^2x, (\frac{3}{2})^3x, ...$, which we call the orbit of x, $orb(x)$, under multiplication by $\frac{3}{2}$. Mahler's question then is: is there an x for which every number in $orb(x)$ has fractional part lying in $[0, \frac{1}{2})$, i.e. does $\exists x \in \mathbb{R} \forall y \in orb(x) : y - \lfloor y \rfloor \in [0, \frac{1}{2})$ hold?

As of yet, this is an unsolved problem, although Mahler does deduce several characteristics for such a number, which he calls a 'Z-number', should it exist. Most notably he shows only countable many Z-numbers can exist. Furthermore, he gives un upper bound for the maximal frequency of Z-numbers that can occur. We will give a short review of these results, and some known improvements on them.

Let α be a Z-number, and write $(\frac{3}{2})^n\alpha = g_n + r_n$, with $g_n \in \mathbb{N}, r_n \in [0, \frac{1}{2})$. If we now define ϵ_n as 1 if g_n is odd, and ϵ_n as 0 if g_n is even, we get

$$r_{n+1} = \frac{3}{2}r_n - \frac{1}{2}\epsilon_n$$

$$g_{n+1} = \frac{3}{2}g_n + \frac{1}{2}\epsilon_n$$

From this recursion follows that

$$r_0 = \frac{1}{3}\left(\varepsilon_{n-1} + \frac{2}{3}\varepsilon_{n-2} + \ldots + \frac{2}{3}^{n-1}\varepsilon_0\right) + (\frac{2}{3})^n r_n$$

$$g_0 = -\frac{1}{3}\left(\varepsilon_{n-1} + \frac{2}{3}\varepsilon_{n-2} + \ldots + \frac{2}{3}^{n-1}\varepsilon_0\right) + (\frac{2}{3})^n g_n$$

This shows that the integer part of α, g_0, completely determines the sequence $\{\varepsilon_n\}_{n\in\mathbb{N}}$. Since the series $\frac{1}{3}\sum_{n=1}^{\infty}(\frac{2}{3})^n\varepsilon_n$ is convergent and the r_n are bounded, this uniquely determines the fractional part of α. So for any g_0, the r_0 is uniquely determined by the above equation. Thus there can only be one Z-number in each interval $[g, g+1)$, and this shows only countably many Z-numbers exist.

Mahler notes that both series above converge in the 2-adic sense. This observation is central to this thesis. In the following chapters we will introduce the notions of a general β-expansion and p-adic evaluations. In the last chapter we will view the g_0 above as a 2-adic number, and show that Mahler's result still holds. This will lift the problem into a more complicated, but in a sense more natural space, where some interesting extra properties hold, e.g. the existence of Z-numbers.

1.2 Further results

Assume we have two consecutive ones in the sequence $\{\varepsilon_n\}_{n\in\mathbb{N}}$, i.e. $\varepsilon_m = \varepsilon_{m-1} = 1$ for certain $m \in \mathbb{N}^+$. We then have, by the earlier recursion

$$r_0 = \frac{1}{3}\left(\varepsilon_{m-1} + \frac{2}{3}\varepsilon_{m-2} + \ldots + \frac{2}{3}^{m-1}\varepsilon_0\right) + \frac{2}{3}^m r_n$$

$$> \frac{1}{3}\left(\varepsilon_{m-1} + \frac{2}{3}\varepsilon_{m-2}\right) = \frac{1}{3} + \frac{2}{9} > \frac{1}{2}$$

But by assumption $r_0 < \frac{1}{2}$, hence no sequence $\{\varepsilon_n\}_{n\in\mathbb{N}}$ associated with a Z-number can ever contain two consecutive ones (this is where we find question 2 from the start of this chapter again). We call this finite sequence 11 a 'forbidden word'. This simple fact allowed Mahler to give an upper bound on the frequency of Z-numbers:

Theorem 1.2.1. *(Mahler) Let x be a sufficiently large integer. Then there exist no more than $x^{0.695}$ Z-numbers smaller than x.*

Proof. Denote by w_n a sequence of zeros and ones of length n not containing two adjacent 1's, and by W_n the set of all such sequences. Let $\#W_n$ be the number of distinct sequences. For each $w_{n+1} \in W_{n+1}$ we have either $w_{n+1} = 0w_n$ for some $w_n \in W_n$ or $w_{n+1} = 10w_{n-1}$ for some $w_{n-1} \in W_{n-1}$. This tells us $\#W_{n+1} = \#W_n + \#W_{n-1}$. Since $\#W_1 = 2, \#W_2 = 3$, we have that $\#W_n = F_{n+2}$, the $(n+2)$nd Fibonacci number.

By the above expansion in ε, each sequence of length n corresponds to a starting integer $g_0 \mod 2^n$, so the number of permissible residue classes for starting integers of Z-numbers is F_{n+2}. Since $F_{n+2} \sim \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+2}$, the fact that there can only be one Z-number per starting integer gives that the number of Z-numbers up to x is $O(x^{\log_2(\frac{1+\sqrt{5}}{2})}) = O(x^{0.695})$.

□

By the same method many more forbidden words can be found (in fact infinitely many). This allows Flatto [4] to improve the result, lowering the constant in the above theorem to $\log_2 \frac{2}{3}$.

The existence of Z-numbers is highly unlikely. For instance, Dubickas showed [2] that any Z-number, should it exist, is greater than 2^{57}.

A natural extension to the problem would be to consider multiplying by another number $b \neq \frac{3}{2}$. With an elegant proof, Tijdeman [14] proved that

Theorem 1.2.2. *Let $\mathbb{R} \ni \theta > 2$. Then there exists an $x \in \mathbb{R}$ such that the fractional parts of $\{\theta^n x\}_{n\in\mathbb{N}}$ lie in $(0, \frac{1}{\theta-1}]$.*

Proof. Let $\mathbb{R} \ni \theta > 2$ and define $a_0 = 1, a_{n+1} = \lfloor \theta a_n \rfloor + 1$. We then have $\theta a_n < a_{n+1} \leq \theta a_n + 1$. Let x_n be $\frac{a_n}{\theta^n}$. Then the sequence $\{x_n\}$ is monotone increasing by the left inequality, and bounded by the right inequality ($x_{n+1} \leq x_n + \frac{1}{\theta^n\theta}$). So it converges to a limit x. We now have

$$x\theta^n > x_n\theta^n = a_n$$

$$x\theta^n \leq (x_n + \sum_{i=n}^{\infty} \frac{1}{\theta^i \theta})\theta^n = (\frac{a_n}{\theta^n} + \frac{1}{\theta^n}\frac{1}{\theta}\frac{1}{1-\theta^{-1}})\theta^n = a_n + \frac{1}{\theta}\frac{\theta}{\theta-1} = a_n + \frac{1}{\theta-1}$$

And since the a_n are integers, this concludes the proof. □

On a final note, the next lemma by Dubickas [3], lemma 2.1, tells us we need not be concerned with the endpoints of our intervals.

Lemma 1.2.3. *Let $p > q > 1$ be two relatively prime integers. Then for every fixed pair of real numbers ξ, t, where $\xi \neq 0$ and $t \in [0, 1)$, there are at most finitely many integers n such that $\xi(p/q)^n - \lfloor \xi(p/q)^n \rfloor = t$.*

Chapter 2

β-expansions

Back in the old days, some people came up with this idea to denote spoken language by scribbling mysterious symbols on a piece of bark, which is a real help to those of us that find themselves in the middle of the supermarket frantically trying to remember whether their cookie jar was half full or half empty. Of course, when in said supermarket, it's a pretty good idea to not just be able to write 'cookies', but also '2 cookies'. For obvious reasons. In the beginning, this was done by just assigning a quantity to certain letters, e.g. I=1, V=5, and adding these up if your particular number didn't have a symbol. This went alright until some people got richer than others and decided they wanted something like 3333 cookies, a whopping 12 symbols, thus rapidly running out of bark to scribble on. Luckily some bright chap in India came up with the idea to write numbers in a finite power series to an integer base k with an equal number of digits, and since 10 seemed to be the predominant quantity for any of his bodily digits, he went decimal. Some time later computers were introduced and, lacking any of said digits, decided they wanted nothing to do with any of these odd numbers and have therefore been living in base 2. Thus when nowadays coming across 10.1 this can either mean $1 * 10^1 + 0 * 10^0 + 1 * 10^1 = 10.1$ or $1 * 2^1 + 0 * 2^0 + 1 * 2^1 = 2.5$ in common notation.

To expand a little on this point, we can take any integer greater than one as a base and express any number (almost) uniquely. In some cases however, it can be convenient to take a non-integer β as a base, taking digits in $\{0, 1, ..., \lfloor\beta\rfloor\}$. Now infinitely many representations may exist for any number, so usually one very special representation is taken, called the greedy β-expansion.

This chapter will first introduce β-expansions in general, and then some algebraic notions we will need later on. In the next section we will treat some questions on periodicity, and the chapter is concluded with the discussion of a different type of expansion, which yields some interesting results.

2.1 Working with non-integer base

Take $1 < \beta \in \mathbb{R}$. Our aim now is to find a way to construct a β-expansion for any real number. We start with any $x \in [0, 1)$. Define the operator T_β by

$$T_\beta(x) = \beta x - \lfloor \beta x \rfloor$$

$T_\beta(x)$ is again in $[0, 1)$, so we can iterate this process. Now let a_n be this integer part, i.e. $a_n = \lfloor \beta T_\beta^{n-1}(x) \rfloor$. We then have

$$x = \sum_{i=1}^{\infty} a_i \beta^{-i}$$

Now take any $y \geq 1$, then let k be the smallest integer such that $\beta^k > y$. By the above method we can write

$$y\beta^{-k} = \sum_{i=1}^{\infty} b_i \beta^{-i}$$

and

$$y = \sum_{i=-k+1}^{\infty} b_{i+k}\beta^{-i}$$

Finally, for $z < 0$, we can put

$$z = -|z| = -\sum_{i=N}^{\infty} c_i\beta^{-i}$$

This gives a possible expansion in base β for any real number, called the 'greedy expansion'.

2.2 Some algebra

When considering expansions in the usual integer base, we know that the set of numbers with (eventually) periodic expansion is exactly $\mathbb{Q}$. For a certain class of non-integer β, similar results are known. To understand these results, and give some new ones, we will now introduce some algebraic concepts related to β.

Definition 2.2.1. We call a set S a ring if you can add and multiply in it and

1. it is an abelian group under addition
2. $S\backslash\{0\}$ is a multiplicative semigroup (the inverse need not exist)
3. the actions are distributive, i.e. $\forall s, t, h \in S : s(t + h) = st + sh$
4. it has a 1-element, i.e. $\exists 1 \in S \forall s \in S : 1s = s$

Definition 2.2.2. We call a set F a field if it is a ring and $S\backslash\{0\}$ is a multiplicative group.

Definition 2.2.3. For any $\beta \in \mathbb{R}$, define $\mathbb{Q}(\beta)$ and $\mathbb{Z}[\beta]$ as the smallest field and ring containing β, respectively.

Definition 2.2.4. We call $\beta \in \mathbb{R}$ an algebraic number (of degree d) if it is the root of a non-divisible polynomial $a_d x^d + ... + a_1 x + a_0$ with coefficients $a_i \in \mathbb{Z}, a_d \neq 0$. If furthermore its minimum polynomial is monic, i.e. $a_d = 1$, we call β an algebraic integer.

Lemma 2.2.5. *Let $\mathbb{Q}[X]$ be the set of all polynomials over $\mathbb{Q}$. Let $F, G \in \mathbb{Q}[X]$, with F irreducible. Then there exist $H, J \in \mathbb{Q}[X]$ such that*

$$FH + GJ = 1$$

This is called the extended Euclidean algorithm. To see the analogy, think of polynomials as ordinary integers, and read 'prime' for 'irreducible'.

Proof. Denote by $deg(X)$ the degree of X.

First note that we can find $Q, R \in \mathbb{Q}[X]$ with

$$F = QG + R$$

where $deg(R) < deg(G)$ or $deg(R) = 0$. Why is this so? If $deg(G) > deg(F)$, take $R = F, Q = 0$. Otherwise, let Q be the polynomial of degree $v = deg(F) - deg(G)$ such that the highest $v + 1$ powers of QG are equal to those of F. Then choose R to be the difference, which has degree at most $deg(G) - v - 1$. By setting $F_2 = G$, $G_2 = R$, we can again find Q_2, R_2 such that

$$G = F_2 = Q_2 G_2 + R_2 = Q_2(F - QG) + R_2$$

and we can iterate

$$F_i = Q_i G_i + R_i = Q_i(F_{i-1} - Q_{i-1}G_{i-1}) + R_i = ...$$

This is just the Euclidean algorithm for polynomials. We eventually find a rest polynomial R_n of degree 0. Each F_i, G_i can be written in terms of F and G, thus we can rewrite to get

$$AF + BG = R_n = c$$

for some constant c, and some $A, B \in \mathbb{Q}[X]$. This constant cannot be 0, for then we would have found a common divisor of F and G. In other words, we could divide both by R_{n-1} (where $R_0 = G$), but by assumption F was irreducible. Thus by dividing A, B by c we have proved the lemma.

□

Lemma 2.2.6. *Let β be an algebraic number of degree d, and let*

$$X = \{q_0 + q_1\beta + ... + q_{d-1}\beta^{d-1}, 0 \leq i < d : q_i \in \mathbb{Q}\}$$

Then $\mathbb{Q}(\beta) = X$, and all these elements are distinct.

In other words, we can view $\mathbb{Q}(\beta)$ as a vector space over $\mathbb{Q}$ with basis $\{1, ..., \beta^{d-1}\}$.

Proof. Obviously, $X \subset \mathbb{Q}(\beta)$. The elements of X are distinct since $1, \beta, ..., \beta^{d-1}$ are linearly independent over $\mathbb{Q}$ (since β is of degree d).

We will show that X is indeed a field. Note that it is closed under addition and multiplication since

$$\beta^d = \frac{1}{a_d}\left(a_0 + a_1\beta + ... + a_{d-1}\beta^{d-1}\right)$$

Now to show X is closed under division. Take any $0 \neq q = l_0 + l_1\beta + ... + l_{d-1}\beta^{d-1} \in X$, let $Q(x) = l_0 + l_1x + ... + l_{d-1}x^{d-1}$ be its corresponding polynomial and $F(x)$ the minimum polynomial of β. Since $F(x)$ is a minimum polynomial, by 2.2.5 we can find polynomials $G(x)$ and $H(x)$ over $\mathbb{Q}$ such that

$$F(x)G(x) + Q(x)H(x) = 1$$

By definition, $F(\beta) = 0$, so

$$F(\beta)G(\beta) + Q(\beta)H(\beta) = Q(\beta)H(\beta) = 1$$

ergo

$$\mathbb{Q}(\beta) \ni H(\beta) = \frac{1}{Q(\beta)} = \frac{1}{q}$$

This shows any element in X has an inverse, and if $x, y \in X$ then $\frac{x}{y} \in X$.

□

Lemma 2.2.7. *Let β be an algebraic number with minimum polynomial $a_dx^d + ... + a_1x + a_0$. Let*

$$Y = \{\frac{n_0}{a_d^{k_0}} + \frac{n_1}{a_d^{k_1}}\beta + ... + \frac{n_{d-1}}{a_d^{k_{d-1}}}\beta^{d-1}, 0 \leq i < d : n_i, k_i \in \mathbb{Z}\}$$

Then $\mathbb{Z}[\beta] \subset Y$.

Proof. Again, $1, \beta \in \mathbb{Z}[\beta]$, and the same holds for other powers of β. Since

$$\beta^d = \frac{1}{a_d}\left(a_0 + a_1\beta + ... + a_{d-1}\beta^{d-1}\right)$$

the first $d-1$ powers are in $\mathbb{Z}[\beta]$, with coefficients in $\frac{1}{a_d^n}\mathbb{Z}$ for some $n \in \mathbb{N}$.

□

Note that when β is an algebraic integer all the denominators are 1.

2.3 A mapping to $\mathbb{R}^d$

From now on, β will denote an algebraic number unless otherwise stated.

This section is devoted to constructing a mapping from the algebraic structures above to $\mathbb{R}^d$, and exploring its properties. The most important of these is that $\mathbb{Z}[\beta]$ forms a lattice in $\mathbb{R}^d$ when β is an algebraic integer.

A minimum polynomial of degree d has d distinct roots in $\mathbb{C}$, denote these by $\beta_1, \beta_2, ..., \beta_d$. All the above works for any of these roots, in an algebraic sense they are all the same. This allows us to extend $\mathbb{Q}(\beta)$ to $\mathbb{C}^d$, we will show its embedding is dense in a subspace of $\mathbb{C}^d$ which we can associate with $\mathbb{R}^d$.

Define the mapping

$$\varphi : \mathbb{Q}(\beta) \to \mathbb{C}^d$$

$$q_0 + q_1\beta + ... + q_{d-1}\beta^{d-1} \mapsto \begin{pmatrix} q_0 + q_1\beta_1 + ... + q_{d-1}\beta_1^{d-1} \\ q_0 + q_1\beta_2 + ... + q_{d-1}\beta_2^{d-1} \\ \vdots \\ q_0 + q_1\beta_d + ... + q_{d-1}\beta_d^{d-1} \end{pmatrix}$$

In other words, β^i is mapped to $(\beta_1^i, \beta_2^i, ..., \beta_d^i)^T$ for $0 \leq i < d$, so we can view $Im(\mathbb{Q}(\beta))$ as a vector space over $\mathbb{Q}$. To show this vector space has dimension d, we need to show that these vectors are linearly independent. This is equivalent with saying that the so-called 'Vandermonde' matrix V, built up of these vectors, has determinant unequal to 0. This is the matrix of φ with respect to $1, \beta, ..., \beta^{d-1}$, the standard basis of $\mathbb{Q}(\beta)$:

$$V = \begin{pmatrix} 1 & \beta_1 & \dots & \beta_1^{d-1} \\ 1 & \ddots & & \beta_2^{d-1} \\ \vdots & & \ddots & \vdots \\ 1 & \beta_d & \dots & \beta_d^{d-1} \end{pmatrix}$$

Lemma 2.3.1. *Take V as defined above. Then* $\det(V) = \prod_{d \geq i > j > 0}(\beta_i - \beta_j)$.

Proof. This is an easy exercise in linear algebra. First note for $d = 2$

$$\det(V) = \det \begin{pmatrix} 1 & \beta_1 \\ 1 & \beta_2 \end{pmatrix} = \beta_2 - \beta_1$$

Now assume the lemma holds for all β with degree lesser or equal to some $n \in \mathbb{N}$, then for $d = n + 1$

$$\det(V) = \begin{vmatrix} 1 & \beta_1 & \dots & \beta_1^{d-1} \\ 1 & \ddots & & \beta_2^{d-1} \\ \vdots & & \ddots & \vdots \\ 1 & \beta_d & \dots & \beta_d^{d-1} \end{vmatrix}$$

$$= \begin{vmatrix} 1 & \beta_1 & \dots & \beta_1^{d-1} \\ 0 & \beta_2 - \beta_1 & & \beta_2^{d-1} - \beta_1^{d-1} \\ \vdots & & \ddots & \vdots \\ 0 & \beta_d - \beta_1 & \dots & \beta_d^{d-1} - \beta_1^{d-1} \end{vmatrix} = \begin{vmatrix} \beta_2 - \beta_1 & \dots & \beta_2^{d-1} - \beta_1^{d-1} \\ \vdots & \ddots & \vdots \\ \beta_d - \beta_1 & \dots & \beta_d^{d-1} - \beta_1^{d-1} \end{vmatrix}$$

by subtracting the first row. Now divide every row by its first coefficient to get

$$\prod_{k=2}^{d}(\beta_k - \beta_1) \begin{vmatrix} 1 & \beta_2 + \beta_1 & \dots & \sum_{i=0}^{d} \beta_2^{d-2-i}\beta_1^i \\ 1 & \ddots & & \sum_{i=0}^{d} \beta_3^{d-2-i}\beta_1^i \\ \vdots & & \ddots & \vdots \\ 1 & \beta_d + \beta_1 & \dots & \sum_{i=0}^{d} \beta_d^{d-2-i}\beta_1^i \end{vmatrix}$$

Finally, for each column but the first, subtract the β_1 multiple of the previous column to get

$$\prod_{k=2}^{d}(\beta_k - \beta_1) \begin{vmatrix} 1 & \beta_2 & \dots & \beta_2^{d-1} \\ 1 & \ddots & & \beta_3^{d-1} \\ \vdots & & \ddots & \vdots \\ 1 & \beta_d & \dots & \beta_d^{d-1} \end{vmatrix}$$

Now, by hypothesis, this is equal to

$$\prod_{k=2}^{d}(\beta_k - \beta_1) \prod_{d\geq i>j>1}(\beta_i - \beta_j) = \prod_{d\geq i>j>0}(\beta_i - \beta_j)$$

This is unequal to 0 exactly if all the $\beta_i, 0 < i \leq d$ are distinct. This is exactly the case, since if any $\beta_i = \beta_j, i \neq j$ then β_i would also be a root of the derivative of the minimum polynomial, which is of lower degree than the minimum polynomial itself!

□

This shows the vectors $\{(\beta_1^i, \beta_2^i, ..., \beta_d^i)\}_{0\leq i<d}^T$ are linearly independent. Thus $Im(\mathbb{Q}(\beta))$ is a d-dimensional vector space over Q. By taking the closure of this space, we get a d-dimensional vector space over $\mathbb{R}$, which we will just consider $\mathbb{R}^d$.

For every complex root of the minimum polynomial, the conjugate is also a root. Let d_1 be the number of real roots and d_2 the number of pairs of complex roots, so $d = d_1 + 2d_2$. Then every element $x \in Im(\mathbb{Q}(\beta)) \subset \mathbb{C}^d$ has d_1 real elements, and d_2 pairs of conjugate elements.

Lemma 2.3.2. *The image of $\mathbb{Q}(\beta)$ under φ is dense in $\mathbb{R}^d$.*

Proof. The image of $\mathbb{Q}(\beta)$ under φ is exactly

$$Span_{\mathbb{Q}}\left(\begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}, \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_{d-1} \end{pmatrix}, ..., \begin{pmatrix} \beta_1^{d-1} \\ \beta_2^{d-1} \\ \vdots \\ \beta_{d-1}^{d-1} \end{pmatrix}\right)$$

□

Lemma 2.3.3. *The image of $\mathbb{Z}[\beta]$ under φ forms a lattice in $\mathbb{R}^d$ if β is an algebraic integer.*

Proof. Let β be an algebraic integer. By 2.2.7, the image of $\mathbb{Z}[\beta]$ under φ is exactly

$$Span_{\mathbb{Z}}\left(\begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}, \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_{d-1} \end{pmatrix}, ..., \begin{pmatrix} \beta_1^{d-1} \\ \beta_2^{d-1} \\ \vdots \\ \beta_{d-1}^{d-1} \end{pmatrix}\right)$$

Furthermore there exists a bijective continuous transformation from this basis to the standard basis of $\mathbb{R}^d$, and the standard embedding of $\mathbb{Z}^d$ lies discrete in $\mathbb{R}^d$. By means of this transformation we can go from this standard imbedding to $Im(\mathbb{Z}[\beta])$, which shows, by continuity, that $Im(\mathbb{Z}[\beta])$ also lies discrete.
□

An important invariant for $\mathbb{Q}(\beta)$ is the so-called discriminant which is defined as the square of the determinant of the Vandermonde matrix, which by 2.3.1 is equal to $\prod_{d\geq i>j>0}(\beta_i - \beta_j)$. Our first task is to show this is actually an integer.

This will require some deeper notions.

Definition 2.3.4. The splitting field of a polynomial $P(X)$ over a given field F is defined as a field extension K of F, over which P factorizes into linear factors $X - a_i$, and such that the a_i generate K over F.

In other words, K is exactly the extension of F by adjoining all the roots of a certain polynomial. Of course, $\mathbb{Q}(\beta_1, ..., \beta_d)$ is obtained from $\mathbb{Q}$ in exactly this way.

Definition 2.3.5. A finite extension K of F is a Galois extension if it's a splitting field over F for some polynomial.

This is not the usual definition, but by [8] it's equivalent.

Definition 2.3.6. An automorphism on a field K is a mapping f from K to itself which is bijective and for any $a, b \in K$

1. f(a+b)=f(a)+f(b)
2. f(ab)=f(a)f(b)
3. f(1)=1

Definition 2.3.7. The fixed field of a group of automorphisms on K is defined as the subset of K that is invariant under all of these automorphisms

Definition 2.3.8. A field F is said to have characteristic 0 if $1, 1+1, 1+1+1, ...$ are all distinct elements of F.

We will state without proof the following result, see for instance [8], theorem 4.1.

Theorem 2.3.9. *Let K be a Galois extension of a field F of characteristic 0. Let G be the group of automorphisms of K over F. Then F is the fixed field of G.*

We will use this theorem by taking $\mathbb{Q}$ for F, and the finite extension $\mathbb{Q}(\beta_1, ..., \beta_d)$ for K. Since $\mathbb{Q}$ has characteristic 0 we can apply the theorem, which tells us that the only elements in $\mathbb{Q}(\beta_1, ..., \beta_d)$ that are invariant under all automorphisms are the rationals.

Lemma 2.3.10. *Let β be an algebraic integer. Then the discriminant of $\mathbb{Q}(\beta)$ is an integer.*

Proof. First we will show the discriminant is an algebraic integer. The discriminant is equal to $\det(V)^2 = \prod_{d \geq i > j > 0} (\beta_i - \beta_j)^2$. Since -1 and all the conjugates of β are algebraic integers, this is a product of sums of (products of) algebraic integers, and thus itself an algebraic integer.

Furthermore we note that by 2.3.9 $\det(V)^2 \in \mathbb{Q}$ if it is invariant under all automorphisms on $\mathbb{Q}(\beta_1, ..., \beta_d)$. Let σ be such an automorphism. Let P be the minimum polynomial of β, then $P(\sigma(\beta_i)) = \sigma(P(\beta_i)) = \sigma(0) = 0$. This shows the image under σ of any of the roots of P is again a root of P. σ is an automorphism, so must be a permutation of the roots. Since $\det(V)^2 = \prod_{i \geq j} (\beta_i - \beta_j)^2$ is a polynomial in the roots which is invariant under permutations of these roots, it is invariant under automorphisms, and thus in $\mathbb{Q}$.

The only algebraic integers in $\mathbb{Q}$ are the integers, which proves the lemma.

□

We now introduce another concept of field extensions, that of the 'norm' of an element. This is not the same as the norm in the sense of a normed vector space, but closely related, so has wisely been given the same name. We will denote this 'norm' on a field K by N_K.

Since every element of $\mathbb{Q}(\beta)$ can be written as $q_0 + q_1\beta + ... + q_{d-1}\beta^{d-1}$, we can view $\mathbb{Q}(\beta)$ as a d-dimensional vector space over $\mathbb{Q}$. Then for any $\gamma \in \mathbb{Q}(\beta)$, multiplication by γ is a linear transformation of $\mathbb{Q}(\beta)$ that we can denote by A_γ.

Lemma 2.3.11. *The following definitions are equivalent.*

Definition 2.3.12. We define the 'norm' of β in $\mathbb{Q}(\beta)$ as

1. $N_{\mathbb{Q}(\beta)}(\beta) = \det(A_\beta)$
2. $N_{\mathbb{Q}(\beta)}(\beta) = (-1)^d \frac{a_0}{a_d}$
3. $N_{\mathbb{Q}(\beta)}(\beta) = \prod_{i=1}^{d} \beta_i$ (where the β_i are the conjugates of β)

Proof. First $1 \Leftrightarrow 2$. Let $a_0 + a_1\beta + ... + a_d\beta^d$ be the minimum polynomial of β. Then

$$A_\beta = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ -\frac{a_0}{a_d} & -\frac{a_1}{a_d} & \cdots & -\frac{a_{d-2}}{a_d} & -\frac{a_{d-1}}{a_d} \end{pmatrix}$$

which has determinant $(-1)^d \frac{a_0}{a_d}$. Furthermore, $2 \Leftrightarrow 3$ since $a_0 + a_1\beta + ... + a_d\beta^d = \prod_{i=1}^{d}(x - \beta_i)$. □

Now to define the 'norm' on $\mathbb{Q}(\beta)$ for any element.

Lemma 2.3.13. *The following definitions are equivalent.*

Definition 2.3.14. The 'norm' of $\gamma \in \mathbb{Q}(\beta)$ is defined as

1. $N_{\mathbb{Q}(\beta)}(\gamma) = \det(A_\gamma)$
2. $N_{\mathbb{Q}(\beta)}(\gamma) = (N_{\mathbb{Q}(\gamma)}(\gamma))^{(\mathbb{Q}(\beta):\mathbb{Q}(\gamma))}$, where $(\mathbb{Q}(\beta) : \mathbb{Q}(\gamma))$ is the dimension of $\mathbb{Q}(\beta)$ over $\mathbb{Q}(\gamma)$.

Proof. We can take a basis $\{g_1, ..., g_n\}$ of $\mathbb{Q}(\gamma)$ as a vector space over $\mathbb{Q}$, and a basis $\{h_1, ..., h_m\}$ of $\mathbb{Q}(\beta)$ as a vector space over $\mathbb{Q}(\gamma)$. We then find a basis of $\mathbb{Q}(\beta)$ over $\mathbb{Q}$ by taking the products of an element in the first basis with an element in the second basis, i.e. $\{g_1h_1, ..., g_nh_1, ..., g_1h_m, ..., g_nh_m, \}$. But then the matrix of multiplication by γ in $\mathbb{Q}(\beta)$ is of the block form

$$A_\gamma = \begin{pmatrix} B_\gamma & 0 & & \\ 0 & B_\gamma & & \\ & & \ddots & \\ & & & B_\gamma \end{pmatrix}$$

where B_γ is the matrix of multiplication by γ in $\mathbb{Q}(\gamma)$. Of course, $\det(A_\gamma) = \det(B_\gamma)^{(\mathbb{Q}(\beta):\mathbb{Q}(\gamma))}$, since the number of blocks is equal to $(\mathbb{Q}(\beta) : \mathbb{Q}(\gamma))$.

□

Remark For $\alpha, \gamma \in \mathbb{Q}(\beta)$, $N_{\mathbb{Q}(\beta)}(\alpha\gamma) = N_{\mathbb{Q}(\beta)}(\alpha)N_{\mathbb{Q}(\beta)}(\gamma)$, since the product of the determinant of two matrices is the determinant of the product.

2.4 Periodicity in base β

Definition 2.4.1. $Per(\beta)$ is the set of numbers whose (greedy) expansion in base β is eventually periodic.

In usual expansions with integer base N $Per(N)$ is equal to $\mathbb{Q}$. One inclusion holds for any real number as base.

Lemma 2.4.2. *Take* $1 < \beta \in \mathbb{R}$. *Then* $Per(\beta) \subset \mathbb{Q}(\beta)$.

Proof. For $x \in [0, 1)$, define the operator T_β as before by $T_\beta(x) = \beta x \mod 1$. Then $T_\beta^n(x) = \beta^n(x - \sum_{i=1}^{n} a_i(x)\beta^{-i})$, with $a_i \in \{0, 1, ..., \lfloor\beta\rfloor\}$. $x \in Per(\beta)$ means $\exists k, m \in \mathbb{N} : T_\beta^k(x) = T_\beta^m(x), k \neq m$. So $\beta^k x = \beta^m k \mod \mathbb{Z}[\beta]$. But this means $(\beta^k - \beta^m)x \in \mathbb{Z}[\beta]$ which implies $x \in \mathbb{Q}(\beta)$. This of course also holds for $y \in \mathbb{R}$ not in the unit interval, since by multiplication by β^k (shifting the expansion) and/or adding a minus sign we can get $x \in [0, 1)$. □

Schmidt [13] characterized $Per(\beta)$ for β algebraic integer[1]

Definition 2.4.3. An algebraic number β is called a Pisot number if it is an algebraic integer, $\beta > 1$ and $|\beta'| < 1$ for all conjugate roots β'.

[1]His definition of $Per(\beta)$ is that T_β is periodic. This is (almost) equivalent to our definition.

Definition 2.4.4. An algebraic number β is called a Salem number if it is an algebraic integer, $\beta > 1$ and $|\beta'| \leq 1$ for all conjugate roots β', with equality for at least one of these.

Theorem (Schmidt) 2.4.1. *Let $\beta \in \mathbb{R}$ be an algebraic integer. We then have*

1. *$\mathbb{Q}(\beta) \subset Per(\beta) \Rightarrow \beta$ is a Pisot- or Salemnumber*
2. *β is a Pisot number $\Rightarrow Per(\beta) = \mathbb{Q}(\beta)$*

We will give a proof in a few steps.

To prove the first part, assume all rationals are in $Per(\beta)$, and let $x \in \mathbb{Q}$, $\beta \in \mathbb{R}$ any algebraic integer, and η be a conjugate root of β with $|\eta| > 1$. Since $x \in Per(\beta) \Leftrightarrow x\beta \in Per(\beta)$, without loss of generality we can assume $x \in [0, 1)$. Then

$$T_\beta^n(x) = \beta^n(x - \sum_{i=1}^{n} a_i\beta^{-i}) = \frac{1}{N}\sum_{i=1}^{d} p_i\beta^i$$

with $a_i \in \{0, 1, ..., \lfloor\beta\rfloor\}, p_i, N \in \mathbb{N}$. But then also

$$\eta^n(x - \sum_{i=1}^{n} a_i\eta^{-i}) = \frac{1}{N}\sum_{i=1}^{d} p_i\eta^i$$

But since $x \in Per(\beta)$, the right hand side of both equations is bounded. Dividing by β^n and η^n respectively and letting n go to infinity, we get

$$\sum_{i=1}^{\infty} a_i\beta^{-i} = x = \sum_{i=1}^{\infty} a_i\eta^{-i}$$

Let $\gamma = \max\{\beta^{-1}, |\eta^{-1}|\}, \delta = |\beta^1 - \eta^{-1}|$ and $m > 2$ such that $\lfloor\beta\rfloor\gamma^m(1-\gamma)^{-1} < 3^{-1}\delta$. Since the above formula holds for all rationals, take α such that

$$\alpha = \frac{1}{\beta} + \sum_{i=m}^{\infty} b_i\beta^{-i} = \frac{1}{\eta} + \sum_{i=m}^{\infty} b_i\eta^{-i}$$

Then

$$\delta = |\frac{1}{\beta} - \frac{1}{\eta}| \leq \sum_{i=m}^{\infty} b_i|\eta^{-i} - \beta^{-i}|$$

$$\leq 2\sum_{i=m}^{\infty} b_i\gamma^k \leq 2\gamma^m\frac{\lfloor\beta\rfloor}{1-\gamma} \leq \frac{2}{3}\delta$$

A contradiction, so $\eta = \beta$.

For the second part, take $\beta \in \mathbb{R}$ any algebraic integer, let its order be d. Take $x \in \mathbb{Q}(\beta)$. Then, by dividing out the denominators in 2.2.6, $x = \frac{1}{N}(n_0 + n_1\beta + ... + n_{d-1}\beta^{d-1}) \in \frac{1}{N}\mathbb{Z}[\beta]$ for some $N, n_0, ..., n_{d-1} \in \mathbb{N}$. But since $\mathbb{Z}[\beta]$ is closed under multiplication and addition, and all integers and β are in $\mathbb{Z}[\beta]$,

$$T_\beta(x) = \beta x - \lfloor\beta x\rfloor \in \frac{1}{N}\mathbb{Z}[\beta]$$

Now by 2.3.3 we have a mapping φ from $\mathbb{Q}(\beta)$ to $\mathbb{R}^d$, and $\varphi(\mathbb{Z}[\beta])$ lies discrete in $\mathbb{R}^d$. Obviously, the same holds for $\frac{1}{N}\mathbb{Z}[\beta]$. Now, since β is real

$$\varphi(T_\beta^n(x)) = \varphi\left(\beta^n(x - \sum_{i=1}^{n} a_i\beta^{-i})\right)$$

$$= \begin{pmatrix} \gamma_1^n(x - \sum_{i=1}^{n} a_i\gamma_1^{-i}) \\ \gamma_2^n(x - \sum_{i=1}^{n} a_i\gamma_2^{-i}) \\ \vdots \\ \gamma_d^n(x - \sum_{i=1}^{n} a_i\gamma_d^{-i}) \end{pmatrix}$$

$$= \begin{pmatrix} \beta^n(x - \sum_{i=1}^{n} a_i \beta^{-i}) \\ \gamma_2^n x - \sum_{i=0}^{n-1} a_i \gamma_2^i \\ \vdots \\ \gamma_d^n x - \sum_{i=0}^{n-1} a_i \gamma_d^i \end{pmatrix}$$

where the $\gamma_i : 1 < i \leq d$ are conjugate roots of β. By construction of T_β, the above vector is bounded in the first coordinate. And because β is Pisot, $|\gamma_i| < 1$ for all $1 < i \leq d$, so it is bounded in all coordinates for all $n \in \mathbb{N}$. Because $T_\beta^n(x) \in \frac{1}{N}\mathbb{Z}[\beta]$, and this is a lattice in $\mathbb{R}^d$, $\varphi(T_\beta^n(x))$ can only take finitely many values. Because φ is obviously injective (it maps its argument to the first coordinate), $T_\beta^n(x)$ can only take finitely many values, and must therefore be periodic. This proves the second assertion.

2.5 Another expansion

Let Y be a subset of $[0, 1)$, and a $Z_{\frac{p}{q}}(Y)$-number be a number ξ such that the fractional part of $\xi(\frac{p}{q})^n$ lies in Y for every $n \in \mathbb{N}$. In this notation Mahler's Z-numbers would be $Z_{\frac{3}{2}}([0, \frac{1}{2}))$. Here and throughout this thesis, when we take any $\frac{p}{q} \in \mathbb{Q}$, we assume p and q to be coprime. A recent result by Akiyama, Frougny and Sakarovitch in [1], based on an adjusted expansion, states that for any rational $\frac{p}{q} \in \mathbb{Q}$ such that $p \geq 2q - 1$ there exists a union of intervals $Y_{\frac{p}{q}}$ in $[0, 1)$ with Lebesgue measure $\frac{q}{p}$ such that $Z_{\frac{p}{q}}(Y_{\frac{p}{q}})$ is countable infinite. $Y_{\frac{2}{3}}$ is given by $[0, \frac{1}{3}) \bigcup [\frac{2}{3}, 1)$.

In this section we will give a simpler proof of this, and then give some new results obtained by iterating the arguments in a clever way.

Theorem 2.5.1. *In the above notation, there exists a subset $L_{\frac{p}{q}}$ of $[0, 1)$ of Lebesgue measure $\min\{\frac{q-1}{p-q}\frac{q}{p}, 1\}$ such that $Z_{\frac{p}{q}}(L_{\frac{p}{q}})$ is countable infinite.*

The key to this theorem is a new expansion in rational base proposed in [1]. The idea of this expansion is to use 'digits' $a_i \in \{0, \frac{1}{q}, \frac{2}{q}, ..., \frac{p-1}{q}\}$, and then only allow those expansions $\sum_{i=1}^{\infty} a_i \frac{p}{q}^{-i}$ such that $\sum_{i=-k}^{0} a_{i+k+1}(\frac{p}{q})^{-i}$ is an integer for every $k \in \mathbb{N}$. In this way, the authors prove there is some constant $w_{\frac{p}{q}}$ such that every real in $[0, w_{\frac{p}{q}})$ can be represented, but every expansion apart from that of 0 is infinite and aperiodic. Furthermore, the algorithm to compute the expansion for a certain real computes the digits from least to most significant. A problem when there are an infinite amount of them. This is overcome by the definition of a computable companion expansion, which is heavily used in the (partial) proof of their theorem. We use a different approach.

Lemma 2.5.2. *Take any nonnegative integer s, then there exists a sequence of digits $a_i \in \{0, \frac{1}{q}, \frac{2}{q}, ..., \frac{p-1}{q}\}$ such that $s = \sum_{i=-k}^{0} a_{i+k+1}(\frac{p}{q})^{-i}$. We will denote this by $s =< a_i >_{1 \leq i \leq k+1}$.*

Proof. Let $N_0 = s$, and for $i > 1$

$$qN_i = pN_{i+1} + b_i$$

where the b_i is the remainder of division of qN by p. Since the N_i are integers and $N_{i+1} < N_i$ if $N_i > 0$, this algorithm terminates for some k when $N_{k+1} = 0$, and $b_i \in \{0, 1, ..., p - 1\}$. We then have that

$$s = N_0 = \frac{pN_1 + b_0}{q} = \frac{p}{q}(\frac{pN_2 + b_1}{q}) + \frac{b_0}{q} = (\frac{p}{q})^k N_{k+1} + \sum_{i=0}^{k} \frac{b_i}{q}(\frac{p}{q})^i$$

which proves the lemma.

□

This series is even unique. An easy way to see this is to note that the p-adic expansion of qs is $\frac{p}{q}$ is unique, and in the finite case always coincides with the archimedean expansion. More on this in the next chapter.

We now turn to the proof of our theorem.

Proof. Let y and z be positive integers. Then, conventionally, $y \mod z \in \{0, ..., z-1\}$. However, any set of representatives of these equivalence classes can be taken. In this proof, for convenience, we will let $y \mod z$ take values in $\{1, ..., z\}$.

Take any $0 < s =< a_i >_{1 \leq i \leq N} \in \mathbb{N}$. Let $l = ps \mod q$. Define

$$f(s) = \frac{p}{q}s + \frac{(q-l)}{q}$$

We want to prove that this is still an integer. Obviously, $f^0(s) = s$ is an integer with an expansion of length N. Assume $f^n(s)$ is an integer with an expansion of length $N+n$ for some $n \in N$, then

$$f^{n+1}(s) = f(f^n(s)) = f(< c_i >_{1 \leq i \leq N+n}) =< b_i >_{1 \leq i \leq N+n+1}$$

where $b_1 = \frac{q-l}{q}$ and $b_i = c_{i-1}$ for $1 < i \leq N+n+1$ is again an integer, whose expansion has length $N+n+1$.

Note that we could have obtained another sequence of integers by adding an integer k to b_1 whenever $\frac{q-l}{q} \leq \frac{p-1}{q} - k$. So applying f to an integer is nothing more than shifting its expansion, and then adding the *smallest* digit such that $f(s)$ is again an integer. This construction gives what is called the 'minimum word' in [1].

By iterating f, we get an infinite sequence $\{a_n\}_{n \in \mathbb{N}}$, where $a_n \in \{0, \frac{1}{q}, ..., \frac{q-1}{q}\}$ for all $n > N$. Let $\xi = \frac{1}{q}(\sum_{i=1}^{\infty} a_i (\frac{p}{q})^{-i})$, and $N \leq k \in \mathbb{N}$. Then

$$(\frac{p}{q})^k \xi = \frac{1}{q}\left(\sum_{i=-k+1}^{0} a_{i+k} (\frac{p}{q})^{-i} + a_{k+1}\frac{q}{p} + \sum_{i=2}^{\infty} a_{i+k} (\frac{p}{q})^{-i} \right)$$

Note that for the last term holds

$$\frac{1}{q}\sum_{i=2}^{\infty} a_{i+k} (\frac{p}{q})^{-i} < \frac{1}{q}\frac{q-1}{q}\sum_{i=2}^{\infty} (\frac{p}{q})^{-i} = \frac{q-1}{q^2}(\frac{q}{p})^2 \frac{1}{1-\frac{p}{q}} = \frac{q-1}{(p-q)p}$$

The first term $\frac{1}{q}\sum_{i=-k+1}^{0} a_{i+k}(\frac{p}{q})^{-i}$ is equal to some integer n plus a $c \in \{0, 1, ..., q-1\}$. Let $l = pc \mod q$, then

$$\frac{1}{q} a_{k+1} \frac{q}{p} = \frac{1}{q}\frac{q-l}{q}\frac{q}{p}$$

Now, because $cp \leq (q-1)p$, we have that $cp - l$ is a multiple of q smaller than $pq - q$, and thus

$$\frac{c}{q} + \frac{1}{q}\frac{q-l}{q}\frac{q}{p} = \frac{cp - l + q}{pq} = \frac{n_c}{p}$$

where n_c is a nonnegative integer smaller than p. There are q possible values of c, each giving a unique n_c.

The above shows $\forall k \geq N, k \in \mathbb{N} : \exists n \in \mathbb{N}, r \in \mathbb{R}, 0 < r < \frac{q-1}{(p-q)p}$ such that

$$(\frac{p}{q})^k \xi = n + \frac{n_c}{p} + r$$

If we now take

$$L_{\frac{p}{q}} = \bigcup_{0 \leq c < q} [\frac{n_c}{p}, \left(\frac{n_c}{p} + \frac{q-1}{(p-q)p} \right) \mod 1)$$

we see that ξ is a $Z_{\frac{p}{q}}(L_{\frac{p}{q}})$-number. Since we could have started on any positive integer s, there are an infinite number of distinct numbers with this property.

□

So we have an expansion in base $\frac{p}{q}$, with the special property that the part in front of the comma is an integer, even if we shift our expansion to the left by an arbitrary amount. We can construct such a sequence for any integer. If we allow only coefficients smaller than 1 in this construction, the expansion

is unique. The crux of the above theorem is that the starting integer s completely determines the whole expansion, and dividing by q yields that the part in front of the comma plus the first term after the comma are of the form $\frac{n}{p}$, with n one of q possible integers. We can extend this idea by dividing by q^m, in which case the part in front of the comma plus the first m terms after the comma will be of the form $\frac{n}{p^m}$, with n one of q^m possible integers.

Theorem 2.5.3. *Take any $\varepsilon > 0$. Then for any integers $p > q$ relatively prime, there exists a finite union of intervals in $[0,1)$, $L_{\frac{p}{q}}$, of Lebesgue measure smaller than ε such that $Z_{\frac{p}{q}}(L_{\frac{p}{q}})$ is countable infinite.*

Proof. Take any $s \in \mathbb{N}$ and let $s = \sum_{i=-N}^{0} a_i(\frac{p}{q})^{-i}$ be its expansion with the coefficients $a_i \in \{0, \frac{1}{q}, ..., \frac{p-1}{q}\}$. Now extend this expansion to the right such that $\xi = \sum_{i=-N}^{\infty} a_i(\frac{p}{q})^{-i}$, $a_i \in \{0, \frac{1}{q}, ..., \frac{q-1}{q}\}$ for $i > 0$, and $\frac{p}{q}^l \sum_{i=-N}^{l} a_i(\frac{p}{q})^{-i}$ is an integer for any $l \in \mathbb{N}$. This is exactly the expansion constructed by the function f from the proof of the previous theorem. Now take m the smallest integer such that $(\frac{q}{p})^m \frac{q-1}{p-q} < \varepsilon$. Obviously, this m exists, and this is precisely the reason we don't need the restriction $p \geq 2q-1$ anymore. Then

$$\frac{\xi}{q^m} = \frac{1}{q^m} \sum_{i=-N}^{0} a_i(\frac{p}{q})^{-i} + \frac{1}{q^m} \sum_{i=1}^{m} a_i(\frac{p}{q})^{-i} + \frac{1}{q^m} \sum_{i=m+1}^{\infty} a_i(\frac{p}{q})^{-i} \tag{2.1}$$

where the first term is equal to some integer plus $\frac{s \mod q^m}{q^m}$ and the second term is completely determined by $s \mod q^m$. Since we know

$$\frac{p^m}{q^m} \left(\sum_{i=-N}^{0} a_i(\frac{p}{q})^{-i} + \sum_{i=1}^{m} a_i(\frac{p}{q})^{-i} \right)$$

is an integer, it follows that the sum of the first two terms in 2.1 is equal to $\frac{M}{p^m}$, for some nonnegative integer M smaller than p^m. The last term is smaller than $\frac{1}{q^m}(\frac{q}{p})^{m+1} \frac{q-1}{q} \frac{1}{1-\frac{q}{p}} = \frac{1}{p^m} \frac{q-1}{p-q}$. The same holds for the k-th iterate

$$\frac{\xi(\frac{p}{q})^k}{q^m} = \frac{1}{q^m} \sum_{i=-N-k}^{0} a_{i+k}(\frac{p}{q})^{-i} + \frac{1}{q^m} \sum_{i=1}^{m} a_{i+k}(\frac{p}{q})^{-i} + \frac{1}{q^m} \sum_{i=m+1}^{\infty} a_{i+k}(\frac{p}{q})^{-i}$$

the sum of the first two terms is equal to $\frac{M}{p^M}$ and the last term is smaller than $\frac{1}{q^m}(\frac{q}{p})^{m+1} \frac{q-1}{q} \frac{1}{1-\frac{q}{p}} = \frac{1}{p^m} \frac{q-1}{p-q}$. Since there are q^m equivalence classes modulo q^m, and the second term is completely determined by the first term modulo q^m, there are only q^m different possible values for M. This shows all the iterates of $\frac{\xi}{q^m}$ are contained in q^m intervals of length $\frac{1}{p^m} \frac{q-1}{p-q}$, the union of which has measure $(\frac{q}{p})^m \frac{q-1}{p-q} < \varepsilon$. □

To illustrate our proof we would like to give an example. A picture says more than a thousand words, and we have quite enough of those, so here you see the fractional parts of the first 40 iterates, with $s = 1, p = 3, q = 2, m = 2$.

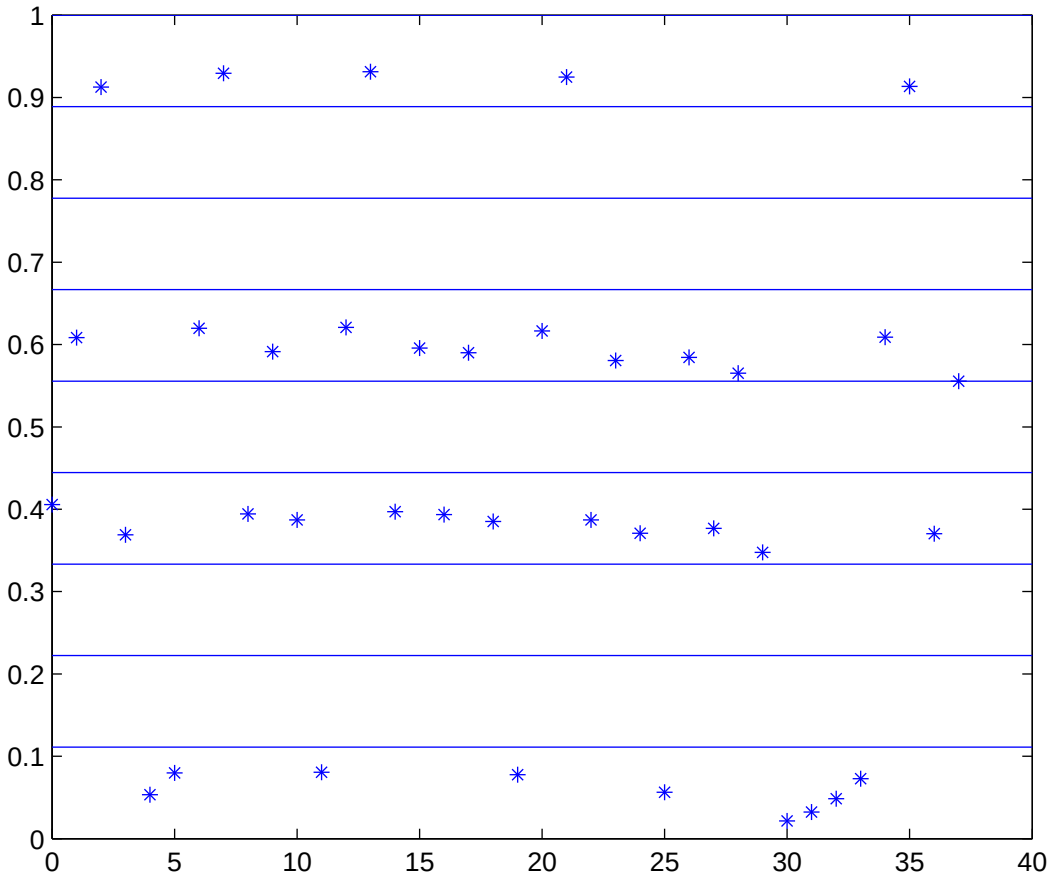

Figure 2.1: The fractional parts are contained in four intervals of length $\frac{1}{9}$

Chapter 3

p-adic numbers

In this chapter we will introduce p-adic valuations and numbers. We will then look at β-expansions in p-adic valuation.

3.1 Valuations

These first two sections are meant as an introduction. We refer the interested reader to [10] or the more understandable [7].

Definition 3.1.1. Define a norm or valuation φ on a commutative ring F as a mapping $F \to \mathbb{R}^+$, where $\mathbb{R}^+$ denotes the set of nonnegative real numbers, such that for all $x, y \in F$

1. $\varphi(x) = 0$ if and only if $x = 0$
2. $\varphi(xy) = \varphi(x)\varphi(y)$
3. $\varphi(x + y) \leq \varphi(x) + \varphi(y)$

if 2 holds in the weaker sense

$$\varphi(xy) \leq \varphi(x)\varphi(y)$$

we call φ a pseudo-valuation. If condition 3 holds in the stronger form

$$\varphi(x + y) \leq \max\{\varphi(x), \varphi(y)\}$$

we call the (pseudo-)valuation a non-archimedian (pseudo-)valuation.

Take $F = \mathbb{Q}$. The most obvious valuation is then the absolute value, denoted by $|.|$. The completion of $\mathbb{Q}$ with respect to the metric induced by this norm is of course $\mathbb{R}$. Another class of valuations on $\mathbb{Q}$ are the p-adic valuations, denoted by $|.|_p$.

Definition 3.1.2. Take $0 \neq \frac{a}{b} \in \mathbb{Q}$, and any prime p. Define $|0|_p = 0, |\frac{a}{b}|_p = p^n$, such that $\frac{a}{b}p^n = \frac{r}{s} \in \mathbb{Q}$ and $p \nmid r$, $p \nmid s$.

It is easily seen that this n exists and is unique.

Lemma 3.1.3. *The mapping defined above is a non-archimedean valuation for any prime p.*

Proof. Property 1 is trivial, property 2 is easy to check. We prove property 3. For any non-zero integer n, define $ord_p(n)$ as the greatest m such that p^m divides n. Note that $ord_p(n_1 n_2) = ord_p(n_1) + ord_p(n_2)$. For any $x = \frac{a}{b} \in \mathbb{Q}$, define $ord_p(x) = ord_p(a) - ord_p(b)$. Note that this definition only depends on x, i.e. if $x = \frac{ac}{bc}$, then still $ord_p(x) = ord_p(ac) - ord_p(cb)$. Now the definition of $|.|_p$ can be written as $|x|_p = 0$ if $x = 0$, otherwise

$$|x|_p = p^{-ord_p(x)}$$

Take $x, y \in \mathbb{Q}$ in their reduced form $x = \frac{a}{b}, y = \frac{c}{d}$, where $\gcd(a,b) = \gcd(c,d) = 1$. If $x = 0, y = 0$ or $x + y = 0$, property 3 is trivial, so assume they are nonzero. We now have $ord_p(x+y) = ord_p(ad+bc) - ord_p(b) - ord_p(d)$. If a power of p divides two numbers, than it also divides their sum. Therefore

$$\begin{aligned} ord_p(x+y) &\geq \min\{ord_p(ad), ord_p(bc)\} - ord_p(b) - ord_p(d) \\ &= \min\{ord_p(a) + ord_p(d), ord_p(b) + ord_p(c)\} - ord_p(b) - ord_p(d) \\ &= \min\{ord_p(a) - ord_p(b), ord_p(c) - ord_p(d)\} \\ &= \min\{ord_p(x), ord_p(y)\} \end{aligned}$$

This shows that

$$|x+y|_p = p^{-ord_p(x+y)} \leq \max\{p^{-ord_p(x)}, p^{-ord_p(y)}\} = \max\{|x|_p, |y|_p\}$$

hence property 3 is fulfilled in the strong form.

□

We can construct a similar mapping for non-primes, but then we lose property 2.

Definition 3.1.4. Take $0 \neq \frac{a}{b} \in \mathbb{Q}$, and any non-prime $g > 1$. Define $|0|_g = 0, |\frac{a}{b}|_g = g^n$, where n is the smallest integer such that $\frac{a}{b} g^n = \frac{r}{s} \in \mathbb{Q}$ and $\gcd\{r,s\} = \gcd\{g,s\} = 1$.

Such an n exists and is unique, see for example [6]. However, we lose the strong form of the multiplicative property, e.g.

$$|\frac{1}{6}|_6 = 6 < 6^2 = |\frac{1}{3}|_6 \cdot |\frac{1}{2}|_6$$

$|.|_g$ can be shown to be a non-archimedean pseudo-valuation, see for example [10].

On a final note, we would like to mention a well-known theorem by Ostrowski [11] which states that any non-trivial norm on $\mathbb{Q}$ is equivalent with the absolute value or a p-adic valuation.

3.2 p-adic numbers

From now on, unless otherwise stated, we mean by p a prime, by g a non-prime integer greater than 1, and by l any integer greater than 1. l-adic (pseudo-)valuations induce metrics, by $d(x,y) = |x-y|_l$. Therefore we can define $\mathbb{Q}_l$, the set of l-adic numbers, as the completion of $\mathbb{Q}$ with respect to the associated metric. $\mathbb{Q}_p$ is a field, while $\mathbb{Q}_g$ is only a ring. It turns out that these numbers can be written in a power series. The following lemma taken from [7] asserts that in a certain way, power series are easier in the l-adic than in the archimedean case.

Lemma 3.2.1. *Every infinite series in $\mathbb{Q}_l$ converges if and only if its terms form a null sequence, i.e. $\sum_{i=0}^{\infty} a_n$ converges if and only if $\lim a_n = 0$.*

This lemma states that something like the harmonic series $(1 + \frac{1}{2} + \frac{1}{3} + ...)$, i.e. a series that diverges even though its terms go to zero, cannot occur in $\mathbb{Q}_l$.

Proof. If the terms of the series aren't a null sequence, then obviously the series cannot converge.

Now consider the partial sums $S_n = a_1 + a_2 + \ldots + a_n$, with $\{a_n\}$ a null sequence. These converge in $\mathbb{Q}_l$, since $|S_M - S_N|_l = |a_{n+1} + a_{n+2} + \ldots + a_M|_l \leq \max\{|a_{n+1}|_l, |a_{n+2}|_l, \ldots, |a_M|_l\}$ which goes to 0 for $M, N \to \infty$.

□

Any l-adic number $x \in \mathbb{Q}_l$, for any $1 < l \in \mathbb{Z}$, can be uniquely written as a power series in l, i.e.

$$x = a_k l^k + a_{k+1} l^{k+1} + ... = \sum_{n=k}^{\infty} a_n l^k$$

for some $k \in \mathbb{Z}$, and the digits $a_i \in \{0, 1, ..., l-1\}$. A thorough but understandable proof for this can be found in [7], p 11. To see that it is true, take any $x \in \mathbb{Q}$, and let $l^k = |x|_l$. Without loss of generality,

since we can always multiply by l^{-k}, we can assume $k = 0$. Now let $a_0 = x \mod l$, $a_1 = l^{-1}(x - a_0) \mod l$, $a_n = l^{-n}(x - \sum_{i=0}^{n-1} a_i l^{-i}) \mod l$. This algorithm exactly gives you the digits needed, since $a_n \in \{0, 1, ..., l-1\}$ for all n.

Another interesting property is that we actually have equality in 3 if the two terms have different valuations.

Lemma 3.2.2. *Take $a, b \in \mathbb{Q}_l, |a|_l > |b|_l$. Then $|a + b|_l = \max\{|a|_l, |b|_l\} = |a|_l$*

Proof. Assume the lemma doesn't hold. Then there exist $x, y \in \mathbb{Q}_l, |x|_l > |y|_l$ with $|x+y|_l < \max\{|x|_l, |y|_l\}$. Dividing by x shows this holds if and only if there exists $z \in \mathbb{Q}_l$, with $|z| < 1, |1 + z| < 1$. Let ε_N be 1 if N is even, -1 if N is odd. Then

$$\frac{1 + \varepsilon_N z^{N+1}}{1 + z} = \sum_{i=0}^{N} z^i (-1)^i$$

Again by property 3 we have that $\forall N : |\sum_{i=0}^{N} z^i|_l \leq 1$, taking limits yields $|\frac{1}{1+z}|_l \leq 1$, which is a direct contradiction of the assumption that $|1 + z|_l < 1$.

□

3.3 β-expansion in l-adic valuation

Take $1 < d \in \mathbb{Z}$ such that $gcd(l, d) = 1$. Then $\{(\frac{l}{d})^n\}_{n\in\mathbb{N}}$ is a l-adic null sequence, and by 3.2.1 $r = \sum_{n=k}^{\infty} a_n \frac{l}{d}^k$ exists, where the a_n are again digits in $\{0, 1, ..., l-1\}$.

Lemma 3.3.1. *Take any $\zeta \in \mathbb{Q}_l$ and $d \in \mathbb{N} : gcd(d, l) = 1$. Then ζ can be written uniquely in power series in $\frac{l}{d}$, i.e. $\zeta = \sum_{i=K}^{\infty} b_i (\frac{l}{d})^i$.*

Note the striking difference with the archimedean case, where for a non-integer rational β in general infinitely many expansions exist.

Proof. The property is trivial for zero, so let's assume $\zeta \neq 0$. First note that $\zeta = \sum_{i=M}^{\infty} a_i l^i$ has such a unique expansion if and only if $\zeta(\frac{l}{d})^{-M}$ has one, so without loss of generality we can assume $M = 0$. Since ζ has a l-adic expansion, there exists a unique a_0 in $\{0, 1, ..., l-1\}$ such that $|\zeta - a_0|_l < 1$. Now to find the normal l-adic expansion you would subtract this number, divide by l, and repeat the procedure. To find the l-adic expansion to base $\frac{l}{d}$, subtract, divide by $\frac{l}{d}$, and repeat. The fact that $gcd(d, l) = 1$ assures that indeed $|(\frac{d}{l})^n(\zeta - \sum_{i=0}^{n-1} b_i(\frac{l}{d})^i)|_l \leq 1$ for all n. □

3.4 A field extension

The usual closure of $\mathbb{Q}$, i.e. $\mathbb{R}$, still has one major shortcoming: there exist polynomials over $\mathbb{R}$ that do not have a solution in $\mathbb{R}$. In other words, the space is not algebraically closed. This of course prompted the fabrication of $\mathbb{C}$, which is nothing more than $\mathbb{R}(i)$, where $i^2 = -1$. And here we are done, since $\mathbb{C}$ is algebraically closed, and still complete. The first is usually called the fundamental theorem of algebra. Both facts are not trivial, as the following will show.

Like $\mathbb{R}$, $\mathbb{Q}_p$ is not algebraically closed. The unsolvable polynomials are not the same as those in $\mathbb{R}$, for example, $X^2 = p$ doesn't have a solution in $\mathbb{Q}_p$, but of course has one in $\mathbb{R}$. $\mathbb{Q}_p$ does have an algebraic closure, but it has infinite dimension as a $\mathbb{Q}_p$ space. The construction of this space, which we will call Ω_p, is complicated. We just assert that it is algebraically closed and complete under the p-adic valuation, which can indeed be extended to the whole space. We refer to [7] for the details.

3.5 Some more algebra

Our goal now is to generalize theorem 2.4.1 to algebraic numbers. Therefore we need an equivalent of 2.3.3, which turns out to be related to p-adic numbers. This section is devoted to constructing the algebraic tools needed, the next section will give the results found.

The next lemma is a form of 'Hensel's lemma'.

Lemma 3.5.1. *Let $f(X) \in \mathbb{Z}_p[X]$, a polynomial with coefficients in $\mathbb{Z}_p$, the p-adic numbers with p-adic valuation smaller than or equal to 1, and assume there exist $g_1(X), h_1(X) \in \mathbb{Z}_p[X]$ such that*

1. *$g_1(X)$ is monic*
2. *$g_1(X)$ and $h_1(X)$ are relatively prime modulo p*
3. *$f(X) = g_1(X)h_1(X) \mod p$*

then there exist $g(X), h(X) \in \mathbb{Z}_p[X]$ such that

1. *$g(X)$ is monic*
2. *$g(X) = g_1(X) \mod p$ and $h(X) = h_1(X) \mod p$*
3. *$f(X) = g(X)h(X)$*

where we take the congruences coefficient-wise.

Proof. We want to construct two sequences of polynomials $g_n(X)$ and $h_n(X)$ such that

1. each $g_n(X)$ is monic and its degree is equal to the degree of g_1
2. $g_{n+1}(X) = g_n(X) \mod p^n$ and $h_{n+1}(X) = h_n(X) \mod p^n$
3. $f(X) = g_n(X)h_n(X) \mod p^n$

then clearly, taking the limit would give the desired polynomials $g(X)$ and $h(X)$.

Since $g_1(X)$ and $h_1(X)$ are relatively prime, we can find $a(X), b(X) \in \mathbb{Z}_p[X]$ such that

$$a(X)g_1(X) + b(X)h_1(X) = 1 \mod p$$

Since $f(X) = g_1(X)h_1(X) \mod p$, we find $pk(X) = f(X) - g_1(X)h_1(X)$, for some $k(X) \in \mathbb{Z}_p[X]$. Divide $b(X)k(X)$ by $g_1(X)$ to get

$$b(X)k(X) = q(X)g_1(X) + r(X)$$

where the degree of $r(X)$ is smaller than that of $g_1(X)$.

Now set $g_2(X) = g_1(X) + pr(X), h_2(X) = h_1(X) + p(a(X)k(X) + h_1(X)q(X))$, we see 1 is satisfied, because the degree of $r(X)$ is smaller than that of $g(X)$, and 2 is satisfied. We can check

$$g_2(X)h_2(X) = (g_1(X) + pr(X))(h_1(X) + p(a(X)k(X) + h_1(X)q(X)))$$

$$= g_1(X)h_1(X) + p(r(X)h_1(X) + (a(X)k(X) + h_1(X)q(X))g_1(X)) + p^2r(X)(a(X)k(X) + h_1(X)q(X))$$

$$= g_1(X)h_1(X) + p((b(X)k(X) - q(X)g_1(X))h_1(X) + (a(X)k(X) + h_1(X)q(X))g_1(X))$$

$$= g_1(X)h_1(X) + pk(X)(b(X)h_1(X) + a(X)g_1(X))$$

$$= g_1(X)h_1(X) + (f(X) - g_1(X)h_1(X)) = f(X) \mod p^2$$

Since by congruence $g_2(X)$ and $h_2(X)$ are again relatively prime modulo p, we can iterate this procedure, proving the lemma. □

Lemma 3.5.2. *Let β be an algebraic number with minimum polynomial $f(X) = a_0 + a_1X + ... + a_dX^d$ over $\mathbb{Z}$. Let H be the set of elements in Ω_p that are roots of this polynomial. Then $\exists \eta \in H : |\eta|_p > 1$ if and only if $p|a_d$.*

Proof. Take $\eta \in H$ with $|\eta|_p > 1$. Then

$$|\eta^d|_p = |\frac{a_0}{a_d} + \frac{a_1}{a_d}\eta + ... + \frac{a_{d-1}}{a_d}\eta^{d-1}|_p$$

$$\leq \max\{|\frac{a_0}{a_d}|_p, |\frac{a_1}{a_d}\eta|_p, ..., |\frac{a_{d-1}}{a_d}\eta^{d-1}|_p\}$$

Since $|\eta^d|_p > |\eta^i|_p, 0 \leq i < d$, this can only happen if $p|a_d$.

Now assume $p|a_d$. If p doesn't divide a_0, then $|\prod_{\eta\in H}\eta|_p = |\frac{a_0}{a_d}|_p > 1$, so at least one of these has valuation greater than 1. So assume $p|a_0$. But then $f(X) = Xh(X) \mod p$, for some polynomial h of degree $d-1$. By Hensel's lemma 3.5.1 we can write $f(X) = (X-\alpha)g(X)$, with g a polynomial with coefficients in $\mathbb{Z}_p$, and α a root of f with $|\alpha|_p < 1$, since $(X-\alpha) = X \mod p$.

Let $g(X) = b_0 + ... + b_{d-1}X^{d-1}$. If $|b_0|_p = 1$, then by the above reasoning g, and thus f, has a root which has a valuation greater than 1. If not, we can iterate this procedure to find a polynomial that does. For if we couldn't do this, we could write $f(X) = a_n(X-\eta_1)...(X-\eta_d)$, and $|\eta_i|_p < 1$ for $1 \le i \le d$. But then all the coefficients in f would be strictly smaller than 1 in valuation, which cannot happen since f is a minimum polynomial. □

Definition 3.5.3. A polynomial over $\mathbb{Z}$ is called primitive if the greatest common divisor of its coefficients is 1.

The following lemma is known as Gauss's lemma [5].

Lemma 3.5.4. *If $g, h \in \mathbb{Z}[X]$ are both primitive, then $f = g \cdot h$ is also primitive.*

Proof. Assume f is not primitive, then we can find a prime p that divides the greatest common divisor of its coefficients. By assumption p cannot divide all the coefficients of g or h, so let b_n and c_m be the first coefficients of g and h that are not a multiple of p, respectively. The coefficient of f of the term X^{n+m} must be of the form

$$b_nc_m + b_{n+1}c_{m-1} + b_{n+2}c_{m-2} + ... + b_{n-1}c_{m+1} + b_{n-2}c_{m+2} + ...$$

But the first term here is not divisible by p, and all the others are, so the coefficient cannot be divisible by p. A contradiction. □

Lemma 3.5.5. *Let $\mathbb{R} \ni \beta > 1$ be an algebraic number. If $\frac{1}{n}$ has a periodic β-expansion for each $n \in \mathbb{N}$, β is an algebraic integer.*

Proof. By assumption, we have

$$\frac{1}{n} = b_1\beta^{-1} + b_2\beta^{-2} + ... + b_m\beta^{-m} + \beta^{-m-1}\frac{c_0 + c_1\beta^{-1} + ... + c_s\beta^{-s+1}}{1-\beta^{-s}}$$

for some $m, s \in \mathbb{N}$, since the expansion of $\frac{1}{n}, n \in \mathbb{N}$ consists of some leading polynomial in β^{-1}, and then a periodic part. Multiply by $n(1-\beta^{-s})$, and bring everything to the left hand side to get $F(\beta^{-1}) = 0$ for some polynomial F with constant term 1. By multiplying by β^k, where k is the degree of F, we get $P(\beta) = 0$ for a monic polynomial P over $\mathbb{Z}$. Of course, we can write P as the product $\prod_{j=0}^{g} Q_j(X)$ of a finite number of irreducible polynomials over $\mathbb{Q}$ such that we can multiply each of these Q_j by an integer c_j such that c_jQ_j is a primitive polynomial over $\mathbb{Z}$. But then by Gauss's lemma 3.5.4 $\prod_{j=0}^{g} c_jQ_j(X) = P(X)\prod_{j=0}^{g} c_j$ is primitive, which shows us all the c_j are 1, thus the Q_j are actually polynomials over $\mathbb{Z}$. But these must be monic since P is monic. Since β is a root of at least one of these, it is an algebraic integer. □

Definition 3.5.6. Two valuations $|.|$ and $||.||$ on a field are called topologically equivalent if and only if $|x| > 1 \Leftrightarrow ||x|| > 1$.

The next theorem is known as Artin's approximation theorem.

Theorem 3.5.7. *If $|.|_1, ..., |.|_n$ are n topologically distinct valuations on a field K, then for each n elements $x_1, ..., x_n \in K$ and $\varepsilon > 0$ there is an $w \in K$ such that* $\max_{1\le i\le n}\{|x-x_i|_i\} < \varepsilon$

Proof. For any two distinct valuations $|.|_\alpha, |.|_\beta$ we can find $a, b \in K$ such that $|a|_\alpha > 1, |a|_\beta \le 1$, and $|b|_\beta > 1, |b|_\alpha \le 1$. Let $y = \frac{a}{b}$, we then have $|y|_\alpha > 1$ and $|y|_\beta < 1$. We will now prove by induction that there exists a $z \in K$ such that $|z|_1 > 1, |z|_j < 1$ for $2 \le j \le n$.

For only two valuations we are done by the above. Assume we have an x such that $|x|_1 > 1$ and $|x|_j < 1$ for $2 \le j \le s-1$. We want to find a number such that $|x|_1 > 1$ and $|x|_j < 1$ for $2 \le j \le s$. Let

y be such that $|y|_1 > 1, |y|_s < 1$. If $|x|_s \leq 1$ then by taking m large enough $x^m y$ is the number we seek. If $|x|_s > 1$ then

$$|t_n|_i = |\frac{x^n}{1+x^n}|_i$$

goes to 1 for $i \in \{1, s\}$ for n to infinity, and to 0 for $i \in \{2, ..., s-1\}$. Thus for large enough n $t_n y$ satisfies our demand.

Now take such an element z_i we have constructed, large in the ith valuation but small in the others. Then by using the same trick, i.e. letting n be very large in

$$\frac{z_i^n}{1+z_i^n}$$

we find elements w_i in K that are arbitrarily close to 1 in the ith valuation but arbitrarily close to 0 in the others. Thus $w = x_1 w_1 + ... + x_n w_n$ is the element of K wanted for the proof. □

Lemma 3.5.8. *Let β be an algebraic number. Then there are only a finite amount of non-archimedean valuations $|.|$ with $|\beta'| > 1$, where β' is a root of the minimum polynomial of β.*

Proof. Let $a_0 + ... + a_d \beta^d$ be the minimum polynomial of β, then $\alpha = a_d \beta'$ is an algebraic integer. By 3.5.2 there are no non-archimedean valuations $|.|$ for which $|a_d \beta'| > 1$, so there can only be finitely many for which $|\beta'| > 1$, since $|a_d| \neq 1$ for finitely many non-archimedean valuations.

□

Definition 3.5.9. Let β be an algebraic number, then $\mathbb{Q}_p(\beta)$ is defined as the p-adic closure of the smallest field in Ω_p containing β.

The idea is now to generalize 2.3.3 by enlarging the space $\mathbb{R}^d$. Let β be an algebraic number, and let $p_1, ..., p_n$ be the p-adic valuations for which $|a_d|_p < 1$. By 3.5.2 there is at least one root $\eta_{p_i} \in \Omega_{p_i}$ of the minimum polynomial of β with $|\eta|_{p_i} > 1$. Now define the mapping φ^* from $\mathbb{Q}(\beta)$ to $\mathbb{R}^d \times \mathbb{Q}_{p_1}(\eta_{p_1}) \times ... \times \mathbb{Q}_{p_n}(\eta_{p_n})$ in the following way. On the first d coordinates it is defined as identical to φ from the last chapter. On the last n coordinates we just let $b_0 + ... + b_{d-1}\beta^{d-1} \mapsto b_0 + ... + b_{d-1}\eta_{p_i}^{d-1}$. In a slight abuse of notation, we will write β for each of the η_{p_i}. Notice that β is now just a root of the minimum polynomial which is greater than 1 in the current valuation.

Theorem 3.5.10. *The image of $\mathbb{Q}(\beta)$ under φ^* is dense in $\mathbb{R}^d \times \mathbb{Q}_{p_1}(\beta) \times ... \times \mathbb{Q}_{p_n}(\beta)$, the image of $\mathbb{Z}[\beta]$ lies discrete, i.e. each point of the image has a neighborhood that contains no other points in the image.*

Proof. The image of $\mathbb{Q}(\beta)$ is dense due to 2.3.2 together with 3.5.7.

First note that $a_d\beta$ is an algebraic integer, so $\varphi^*(\mathbb{Z}[a_d\beta])$ is a lattice by 2.3.3 (the property isn't lost in a larger space). Now consider $\mathbb{Z}[\frac{1}{a_d}, a_d\beta]$, the smallest ring containing $\frac{1}{a_d}$ and $a_d\beta$. Obviously, $\mathbb{Z}[\beta] \subset \mathbb{Z}[\frac{1}{a_d}, a_d\beta]$, so it is sufficient to prove that $\varphi^*(\mathbb{Z}[\frac{1}{a_d}, a_d\beta])$ forms a lattice. We have

$$\mathbb{Z}[\frac{1}{a_d}, a_d\beta] = \bigcup_{n\in\mathbb{N}} (\frac{1}{a_d})^n \mathbb{Z}[a_d\beta]$$

We know that $\exists\varepsilon\forall x \in \varphi^*((\frac{1}{a_d})^0\mathbb{Z}[\beta]) : |x| > \varepsilon$, for any norm on $\mathbb{R}^d \times \mathbb{Q}_{p_1}(\beta) \times ... \times \mathbb{Q}_{p_n}(\beta)$. If we take the Euclidean norm on $\mathbb{R}^d$ and then the multiplication norm, we get for $x \in \varphi^*((\frac{1}{a_d})^n\mathbb{Z}[\beta])$

$$|\frac{1}{a_d}x| = |\frac{1}{a_d}x|_{\mathbb{R}^d}|\frac{1}{a_d}x|_{\mathbb{Q}_{p_1}(\beta)\times...\times\mathbb{Q}_{p_n}(\beta)} = \frac{1}{a_d}|x|_{\mathbb{R}^d} \cdot a_d|x|_{\mathbb{Q}_{p_1}(\beta)\times...\times\mathbb{Q}_{p_n}(\beta)} = |x|$$

since the product of all the p-adic valuations of an integer n is exactly $\frac{1}{n}$. So if no point in $\varphi^*((\frac{1}{a_d})^n\mathbb{Z}[\beta])$ comes close to 0, then no point in $\varphi^*((\frac{1}{a_d})^{n+1}\mathbb{Z}[\beta])$ does either. This proves $\varphi^*(\mathbb{Z}[\frac{1}{a_d}, a_d\beta])$, and hence $\varphi^*(\mathbb{Z}[\beta])$ lies discrete in $\mathbb{R}^d \times \mathbb{Q}_{p_1}(\beta) \times ... \times \mathbb{Q}_{p_n}(\beta)$.

□

3.6 Periodicity in base β

Definition 3.6.1. Let $Per_l(\beta)$ denote the set of numbers with eventually periodic l-adic expansions in base β. Let $Per_\infty(\beta) \equiv Per(\beta)$, the set of numbers with eventually periodic expansions in base β under the normal archimedean valuation.

It is well known that $Per(\beta) = \mathbb{Q}$ for any $\beta \in \mathbb{Z}$. Schmidt [13] proved that for any algebraic integer $\gamma \in \mathbb{R}$, $Per(\gamma) = \mathbb{Q}(\gamma)$ if γ is a Pisot-number, this is theorem 2.4.1. We will extend this theorem, first for the simple case $\beta \in \mathbb{Q}$.

Take $\alpha \in \mathbb{Q}$ and let $\sum_{j=K}^{\infty} r_j \beta^{-j}$ be its β-expansion in l-adic valuation. Since $\alpha \in Per_l(\beta)$ if and only if $\beta^K \alpha \in Per_l(\beta)$, we can assume $K = 0$. Define the operator lT_β by

$$lT_\beta(\alpha) = lT_\beta(\sum_{j=0}^{\infty} r_j \beta^{-j}) = \sum_{j=0}^{\infty} r_{j+1} \beta^{-j} = \beta\alpha - r_0$$

Theorem 3.6.2. *Let $0 \neq \beta = \frac{k}{l} \in \mathbb{Q}, gcd(k,l) = 1, k < l$. We than have $Per_l(\beta) = \mathbb{Q}(\beta) = \mathbb{Q}$.*

Proof. It can be easily seen that $Per_l(\beta) \subset \mathbb{Q}$, since $\sum_{n=0}^{\infty} t^n = \frac{1}{1-t}$ holds l-adically for any t with $|t|_l < 1$. Note that any power series with periodic digits can be written in this form multiplied by a constant, hence we have for any $x \in Per_l(\beta)$ with period d, that $\exists y \in \mathbb{Q} : x = \frac{y}{1-\beta^{-d}}$ which is in $\mathbb{Q}$.

To see $\mathbb{Q} \subset Per_l(\beta)$, take any $\alpha = \frac{p}{q} \in \mathbb{Q}$, w.l.o.g. we can assume its l-adic expansion starts at 0. Since $|\beta| < 1$, $\exists M \in \mathbb{N}, \forall n : |lT_\beta(\alpha)| < M$. Furthermore, $lT_\beta(\alpha) \in \mathbb{Q}$ so by writing

$$lT_\beta^n(\alpha) = \frac{qk^n}{ql^n}(\frac{pl^n}{ql^n} - \sum_{j=0}^{n} r_j \frac{qk^{-j}}{ql^{-j}})$$

we see the denominator of $lT_\beta(\alpha)$ is a divisor of ql^n. But because by definition of the expansion $|lT_\beta(\alpha)|_l \leq 1$, we have that the denominator is actually a divisor of q. Therefore the denominator can only take finitely many values, and then by boundedness of lT_β in $\mathbb{R}$, the numerator can only take finitely many values. So $\exists n, m : n \neq m, lT_\beta^m(\alpha) = lT_\beta^n(\alpha)$, and periodicity follows. Of course, periodicity of lT_β implies periodicity of the expansion of α. □

In fact, this is a special version of the following theorem, which generalizes 2.4.1. We first introduce Pisot and Salem numbers in a broader sense.

Definition 3.6.3. Let P denote the set of primes, and $P^+ = P \cup \{\infty\}$.

Definition 3.6.4. Let β be an algebraic number of degree d. Consider the following valuations on β

1. The d absolute values of each of its conjugate roots
2. The p-adic valuations on all the roots $\eta_i \in \Omega_p$ of its minimum polynomial

We call β an ∞-Pisot (∞-Salem) number if $|\beta| > 1$, each of the other d first above valuations are strictly smaller than 1 (smaller than or equal to 1, with at least one equality) and $\forall p \in P : |\eta_i|_p \leq 1$.

We call β a p-Pisot (p-Salem) number if $|\eta_i|_p > 1$ for some i, each of the d other above valuations are strictly smaller than 1 (smaller than or equal to 1) and $\forall p' \in P \backslash \{p\} : |\eta_i|_{p'} \leq 1$.

Notice that the usual definition of a Pisot number requires β to be an algebraic integer. We have an extension of this definition, since the condition on its p-adic valuations is equivalent with β being an algebraic integer by 3.5.2.

Theorem 3.6.5. *Let $0 < \beta \in \mathbb{R}$ be an algebraic number. If β is a p^+-Pisot number, $p^+ \in P^+$, then*

$$Per_{p^+}(\beta) = \mathbb{Q}(\beta)$$

Conversely, if

$$Per_{p^+}(\beta) = \mathbb{Q}(\beta)$$

for some $p^+ \in P^+$, then β is a p^+-Pisot number or a p^+-Salem number.

Proof. Let β be a p^+-Pisot number for some $p^+ \in P^+$. Then by 3.5.10 the image of $\mathbb{Z}[\beta]$ under the constructed φ^* forms a lattice in $\mathbb{R}^d \times \mathbb{Q}_{p^+}(\beta)$ (where we define $\mathbb{Q}_\infty$ as a singleton). There is only one coordinate in this space where multiplication by β is not a contraction. So, for any $x \in \mathbb{Q}(\beta)$, $\{p^+ T_\beta^n(x)\}_{n\in\mathbb{N}}$ is bounded in this space. These two facts show p^+T_β is periodic, and thus $Per_{p^+}(\beta) = \mathbb{Q}(\beta)$.

To prove the second part, take $\beta > 0$ an algebraic number, and assume $Per_{p^+}(\beta) = \mathbb{Q}(\beta)$ for some $p^+ \in P^+$. Then obviously, since we can form expansions at all, $|\beta|_{p^+} > 1$. First consider the case $p^+ = \infty$. By the same argument as in the proof of 2.4.1, all the conjugate roots of β are smaller than or equal to 1 in absolute value. Furthermore, β is an algebraic integer by 3.5.5, thus all the p-adic valuations cannot be greater than 1 by 3.5.2.

Now consider the case p^+ is some prime p. Assume $|\beta| > 1$ for some archimedean valuation. Then every series in β^{-1} with bounded coefficients converges in archimedean valuation, and if it is (eventually) periodic it converges to the same limit as in the p-adic case. Thus $Per_\infty(\beta) = \mathbb{Q}(\beta)$. But then by the above argument $|\beta|_p \leq 1$, a contradiction. Now to show p is the only prime with $|\beta|_p > 1$. Assume there exists another prime p' with this property, then take any $x \in \mathbb{Q}(\beta)$ with $|x|_{p'} > |x|_p = 1$. Now

$$|pT_\beta(x)|_{p'} = |\beta x - a_i\beta|_{p'} = \max\{|\beta x|_{p'}, |a_i\beta|_{p'}\} = |\beta x|_{p'} > |x|_{p'}$$

where the second equality holds by 3.2.2 because the valuation of the two terms is not equal, since a_i is an integer. But then $\{pT_\beta^n(x)\}_{n\in\mathbb{N}}$ takes an infinite amount of values, and thus cannot be periodic. Which is a contradiction, since we assumed $Per_p(\beta) = \mathbb{Q}(\beta)$. □

Remark For $|\beta| < 1$ an algebraic number with $|\beta|_{p_i}| > 1$ for several primes p_i, we could even consider expansions in the l-adic pseudo-valuation, where $l = \prod_i p_i$. Then again $Per_l(\beta) = \mathbb{Q}(\beta)$.

Chapter 4

A compact approach

We now have the machinery needed to look again at Mahler's problem introduced in the first chapter. We will look at numbers in this problem by using their β-expansion, with $\beta = \frac{3}{2}$, which is more or less done by Mahler. We will look at the related problem on the locally compact space $\mathfrak{X} \equiv \mathbb{R} \times \mathbb{Q}_2 \times \mathbb{Q}_3$, made compact by taking the quotient space $\mathfrak{X}/\mathbb{Z}[\frac{1}{6}]$. In this space it will even make sense to look at multiplication by $\frac{2}{3}$, enabling us to look at Z-numbers under both forward and backward iteration.

4.1 Forbidden words

Definition 4.1.1. An alphabet A is a finite set of symbols $\{a_1, ..., a_n\}$.

Definition 4.1.2. A word w over an alphabet A is a finite sequence of symbols in A. A sentence s over an alphabet A is an infinite sequence $b_1 b_2 b_3 ...$ of symbols in A.

Definition 4.1.3. A word w is said to be contained in a sentence s if $s = w_1 w s_1$ for some word w_1 and some sentence s_1.

Definition 4.1.4. Let $\pi_{\frac{a}{b}}$ be the mapping from the set of all words over the alphabet $\{0, 1\}$ given by $a_1 a_2 ... a_n \mapsto \sum_{i=1}^{n} a_i (\frac{a}{b})^i$.

Definition 4.1.5. A word w is called a forbidden word if $\pi_{\frac{2}{3}}(w) > 1$.

We can now derive a first simple lemma.

Lemma 4.1.6. *The following two statements are equivalent*

1. $\{a_i\} \in \{0, 1\}^{\mathbb{N}^+}$ *does not contain any forbidden word.*
2. $\forall m \in \mathbb{N} : \sum_{i=1}^{\infty} a_{i+m} \frac{2}{3}^i \leq 1$.

Proof. Define $\mathfrak{W}$ as the set of all forbidden words. If any of these words would be contained in a sequence $\{b_i\}$ on say, the k-th position, then $\sum_{i=1}^{\infty} a_{i+k} \frac{2}{3}^i > 1$. So if a sequence fulfills the above condition 2, it cannot contain a word in $\mathfrak{W}$.

Now take any $\{c_i\} \in \{0, 1\}^{\mathbb{N}^+}$ that does not contain a word in $\mathfrak{W}$. Assume there exists an $m \in \mathbb{N}$ such that $\sum_{i=1}^{\infty} c_{i+m} \frac{2}{3}^i > 1$. The strict inequality here implies this must also hold for some finite sequence, i.e. there is a $s \in \mathbb{N}$ such that $\sum_{i=1}^{s} c_{i+m} \frac{2}{3}^i > 1$. Then by definition of $\mathfrak{W}$, $\{c_{i+m}\}$, and thus $\{c_i\}$, would contain a word from $\mathfrak{W}$. □

4.2 The space $\mathfrak{X}$

In this section we will look more closely at the space $\mathfrak{X} = \mathbb{R} \times \mathbb{Q}_2 \times \mathbb{Q}_3$. Let ψ be the mapping that maps any number to the (anti-)diagonal in $\mathfrak{X}$:

$$\begin{aligned} \psi : \mathbb{Q} &\to \mathfrak{X} \\ x &\mapsto (-x, x, x) \end{aligned}$$

Theorem 4.2.1. *$\psi(\mathbb{Q})$ lies dense in $\mathfrak{X}$.*

Proof. Let $x = (r, a, b) \in \mathfrak{X}, \varepsilon > 0$. We need to find $q \in \mathbb{Q}$ such that

$$\max\{|r - q|, |a - q|_2, |b - q|_3\} < \varepsilon$$

Since $\mathbb{Q}$ is dense in $\mathbb{Q}_2$ and $\mathbb{Q}_3$ we can choose $q_1 \in \mathbb{Q}$ such that $|a - q_1|_2 < \frac{1}{3}\varepsilon$, and $d, e \in \mathbb{Z}, \gcd(d, e) = 1$ such that $|b - q_1 - \frac{d}{e}|_3 < \frac{1}{3}\varepsilon$. Now take $q_2 = \frac{c_1 2^{k_1}}{e}$, with $k_1 = \min\{k \in \mathbb{N} : |\frac{2^k}{e}|_2 < \frac{1}{3}\varepsilon\}$ and $c_1 \in \mathbb{Z}$ such that $|\frac{d - c_1 2^{k_1}}{e}|_3 < \frac{1}{3}\varepsilon$.

Since $\mathbb{Q}$ is also dense in $\mathbb{R}$ we can choose $f, g \in \mathbb{Z}, \gcd(f, g) = 1$ such that $|r - q_1 - q_2 - \frac{f}{g}| < \frac{1}{2}\varepsilon$. Choose $q_3 = \frac{c_2 6^{k_3}}{g 7^{k_4}}$, where $k_3 = \min\{k \in \mathbb{N} : \max\{|\frac{6^k}{g}|_2, |\frac{6^k}{g}|_3\} < \frac{1}{3}\varepsilon\}$, $k_4 = \min\{k \in \mathbb{N} : |\frac{6^{k_3}}{g 7^k}|\} < \frac{1}{2}\varepsilon$, and $c_2 \in \mathbb{Z}$ such that $7^{k_4} f - c_2 6^{k_3} < 6^{k_3}$.

Then $q = q_1 + q_2 + q_3$ is the required number, since:

$$|r - q| = |r - q_1 - q_2 - \frac{f}{g} + \frac{f}{g} - q_3| \leq |r - q_1 - q_2 - \frac{f}{g}| + |\frac{f}{g} - q_3| < \frac{1}{2}\varepsilon + |\frac{f}{g} - \frac{c_2 6^{k_3}}{g 7^{k_4}}|$$
$$= \frac{1}{2}\varepsilon + |\frac{7^{k_4} f - c_2 6^{k_3}}{g 7^{k_4}}| < \frac{1}{2}\varepsilon + |\frac{6^{k_3}}{g 7^{k_4}}| < \frac{1}{2}\varepsilon + \frac{1}{2}\varepsilon = \varepsilon$$

$$|a - q|_2 = |a - q_1 - q_2 - q_3|_2 \leq |a - q_1|_2 + |q_2|_2 + |q_3|_2 < \frac{1}{3}\varepsilon + \frac{1}{3}\varepsilon + \frac{1}{3}\varepsilon = \varepsilon$$

$$|b - q|_3 = |b - q_1 - \frac{d}{e} + \frac{d}{e} - q_2 - q_3|_3 \leq |b - q_1 - \frac{d}{e}|_3 + |\frac{d}{e} - q_2|_3 + |q_3|_3$$
$$< \frac{1}{3}\varepsilon + |\frac{d - c_1 2^{k_1}}{e}|_3 + \frac{1}{3}\varepsilon < \frac{1}{3}\varepsilon + \frac{1}{3}\varepsilon + \frac{1}{3}\varepsilon = \varepsilon$$

Or just invoke 3.5.7.

□

The most important result is the following.

Theorem 4.2.2. *$\psi(\mathbb{Z}[\frac{1}{6}])$ lies discrete in $\mathfrak{X}$.*

Proof. By definition, $\mathbb{Z}[\frac{1}{6}]$ is closed under subtraction, so we just need to show that $\exists \varepsilon > 0 \forall 0 \neq x \in \mathfrak{X} : x \geq \varepsilon$. By 2.2.7 all elements of $\mathbb{Z}[\frac{1}{6}]$ are of the form $\frac{a}{6^k}, a \in \mathbb{Z}, k \in \mathbb{N}, 6 \nmid a$. If we now equip $\mathfrak{X}$ with the maximumnorm, we can just take $\varepsilon = 1$. For if $k = 0$ we have $|x| = |a| \geq 1$, and for $k \neq 0$ we have $|x|_2 > 1$ and/or $|x|_3 > 1$.

□

Define the quotient space $\mathfrak{Y} = \mathfrak{X}/\psi(\mathbb{Z}[\frac{1}{6}])$.

Lemma 4.2.3. *$[0, 1) \times \mathbb{Z}_2 \times \mathbb{Z}_3$ is a fundamental domain for $\mathfrak{Y}$. I.e. we can shift every element in $\mathfrak{X}$ over $\psi(\mathbb{Z}[\frac{1}{6}])$ to get an element in $[0, 1) \times \mathbb{Z}_2 \times \mathbb{Z}_3$ in a unique way.*

Proof. Let (r, d, e) in $\mathfrak{X}$, we have to find a z in $\mathbb{Z}[\frac{1}{6}]$ such that $(r + z, d - z, e - z)$ is in $[0, 1) \times \mathbb{Z}_2 \times \mathbb{Z}_3$. We know we can write $d = \sum_k^\infty a_i 2^i, e = \sum_k^\infty b_i 3^i$ in a unique way. Let d_0, e_0 be the sums of the negative powers in these two series respectively. Then d_0 and e_0 are elements of $\mathbb{Z}[\frac{1}{6}]$. Furthermore, $d_0 \in \mathbb{Z}_3$ and $e_0 \in \mathbb{Z}_2$. So $d - d_0 - e_0$ is in $\mathbb{Z}_2$ and $e - d_0 - e_0$ is in $\mathbb{Z}_3$. Now take the unique integer n such that $r + d_0 + e_0 + n$ is in $[0, 1)$. Then $z = d_0 + e_0 + n$ has the required properties. We still have to show that it is unique. Observe that an element of $\mathbb{Z}[\frac{1}{6}]$ is a rational number whose denominator contains primes 2 and 3 only. If such an element is in the fundamental domain, then it is necessarily equal to 0. Now suppose z' would be another element that translates (r, d, e) into the fundamental domain. Then either $z' - z$ or $z - z'$ would be in the fundamental domain and in $\psi(\mathbb{Z}[\frac{1}{6}])$. Hence it would be zero. □

Remark This shows $\mathfrak{Y}$ is compact.

We now lift Mahler's problem to the space $\mathfrak{Y}$. Here we can define Z-numbers in a more general way.

Definition 4.2.4. We call $y \in \mathfrak{Y}$ a Z-number if $\forall n \in \mathbb{Z} : (\frac{2}{3})^n y \in [0, \frac{1}{2}) \times \mathbb{Z}_2 \times \mathbb{Z}_3$.

Multiplication by $\frac{3}{2}$ expands the first and second coordinate, and contracts the third. Multiplication by $\frac{2}{3}$ obviously does exactly the opposite. For this reason we will now look at backward and forward iterations. First we show that these multiplications are just forward and backward shifts on an infinite sequence.

Lemma 4.2.5. *Let $\{a_i\} \in \{0,1\}^{\mathbb{Z}}$, and define $x = \chi(\{a_i\}) = (\frac{1}{2}\sum_{i=1}^{\infty} a_i \frac{2}{3}^i, -\frac{1}{2}\sum_{i=1}^{\infty} a_i \frac{2}{3}^i, \frac{1}{2}\sum_{i=-\infty}^{0} a_i \frac{2}{3}^i)$. We then have*

$$\frac{3}{2}x = \chi(\{a_{i+1}\})$$
$$\frac{2}{3}x = \chi(\{a_{i-1}\})$$

Proof. We have

$$\frac{3}{2}x = (\frac{1}{2}a_1 + \frac{1}{2}\sum_{i=1}^{\infty} a_{i+1}\frac{2}{3}^i, -\frac{1}{2}a_1 - \frac{1}{2}\sum_{i=1}^{\infty} a_{i+1}\frac{2}{3}^i, \frac{1}{2}\sum_{i=-\infty}^{-1} a_{i+1}\frac{2}{3}^i)$$
$$= (\frac{1}{2}\sum_{i=1}^{\infty} a_{i+1}\frac{2}{3}^i, -\frac{1}{2}\sum_{i=1}^{\infty} a_{i+1}\frac{2}{3}^i, \frac{1}{2}\sum_{i=-\infty}^{0} a_{i+1}\frac{2}{3}^i)$$

and

$$\frac{2}{3}x = (\frac{1}{2}\sum_{i=2}^{\infty} a_{i-1}\frac{2}{3}^i, -\frac{1}{2}\sum_{i=2}^{\infty} a_{i-1}\frac{2}{3}^i, \frac{1}{3}a_0 + \frac{1}{2}\sum_{i=-\infty}^{0} a_{i-1}\frac{2}{3}^i)$$
$$= (\frac{1}{2}\sum_{i=1}^{\infty} a_{i-1}\frac{2}{3}^i, -\frac{1}{2}\sum_{i=1}^{\infty} a_{i-1}\frac{2}{3}^i, \frac{1}{2}\sum_{i=-\infty}^{0} a_{i-1}\frac{2}{3}^i)$$

□

Theorem 4.2.6. *Take $\{a_i\} \in \{0,1\}^{\mathbb{Z}}$, then the following statements are equivalent*

1. *$\{a_i\}$ does not contain any forbidden word.*
2. *the point $(\frac{1}{2}\sum_{i=1}^{\infty} a_i \frac{2}{3}^i, -\frac{1}{2}\sum_{i=1}^{\infty} a_i \frac{2}{3}^i, \frac{1}{2}\sum_{i=-\infty}^{0} a_i \frac{2}{3}^i)$ is a Z-number.*

Proof. By 4.2.5 and the definition of a Z-number, (2) is equivalent with saying that $\frac{1}{2}\sum_{i=1}^{\infty} a_{i+m}\frac{2}{3}^i$ is smaller than $\frac{1}{2}$ for all $m \in \mathbb{Z}$. The theorem follows directly from 4.1.6. □

The following figures give a picture of how our Z-numbers lie in the space $\mathfrak{Y}$.

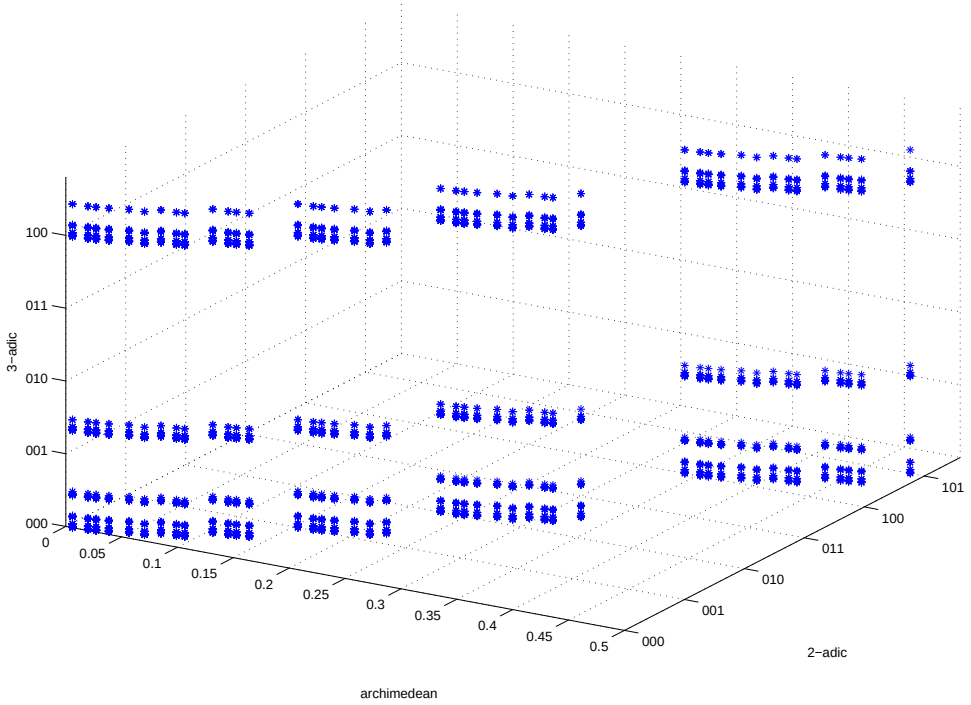

Figure 4.1: Z-numbers in the space $\mathfrak{Y}$

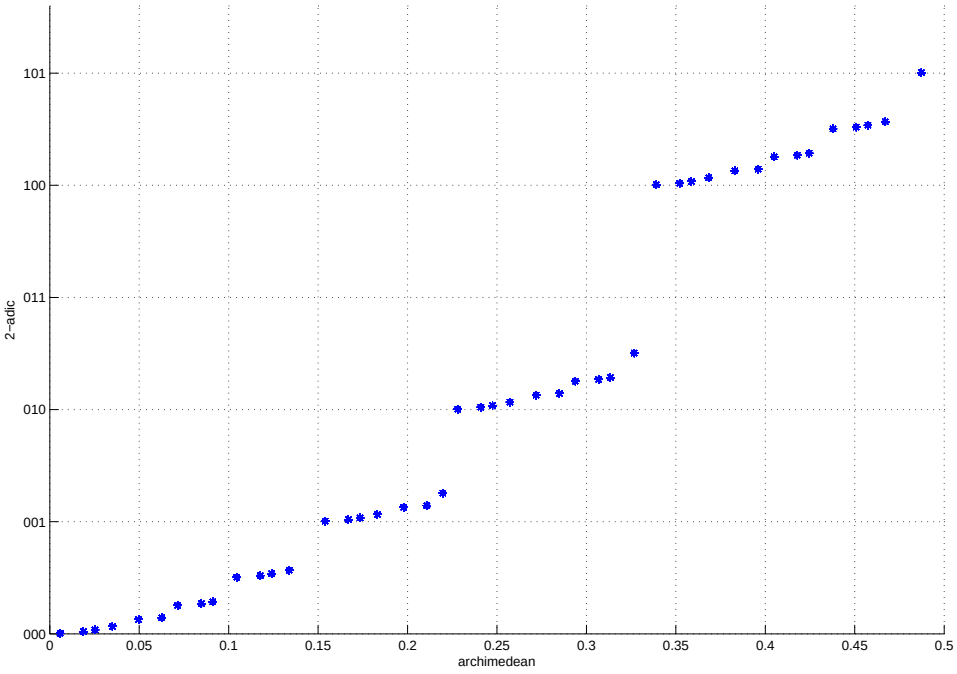

Figure 4.2: The same Z-numbers projected onto $\mathbb{R} \times \mathbb{Z}_2$

4.3 A generalization

We can generalize the above results to a broader context. Take any $1 < \frac{p}{q} \in \mathbb{Q}$ such that p, q prime, $q^2 \geq p$, and an interval $[c, d) \subset [0, 1)$ such that $\frac{p}{q}d \leq 1$. Let a_i be digits from $\{0, 1, ..., q-1\}$. The general sense of a forbidden word then becomes

Definition 4.3.1. A word w is called a forbidden word if $\pi_{\frac{p}{q}}(w) > \frac{q(q-1)}{p-q}d$ or $\pi_{\frac{p}{q}}(w) < \frac{q(q-1)}{p-q}(c - (\frac{q}{p})^k)$, where k is the length of w.

Theorem 4.3.2. *Take $\{a_i\}$ in $\{0, 1, ..., q-1\}^{\mathbb{Z}}$. Then the following are equivalent*

1. *$\{a_i\}$ does not contain forbidden words*
2. *The point $x = \frac{p-q}{q(q-1)}(\sum_{i=1}^{\infty} a_i(\frac{p}{q})^{-i}, -\sum_{i=1}^{\infty} a_i(\frac{p}{q})^{-i}, \sum_{i=-\infty}^{0} a_i(\frac{p}{q})^{-i}) \in (\mathbb{R} \times \mathbb{Q}_q \times \mathbb{Q}_p)/\psi(\mathbb{Z}[\frac{1}{pq}])$ is a Z-number, i.e. $(\frac{p}{q})^z x$ has first coordinate in $[c, d)$ for all $z \in \mathbb{Z}$*

Proof. First note that $|\sum_{i=1}^{\infty} a_i(\frac{p}{q})^{-i}| \in [0, \frac{q(q-1)}{p-q}]$. Thus the first coordinate of x lies in $[0, 1]$, and for any $y \in [0, 1]$ there is a $\{a_i\}$ such that $y = \frac{p-q}{q(q-1)}\sum_{i=1}^{\infty} a_i(\frac{p}{q})^{-i}$. Since $\gcd(p, q) = 1$, $|\frac{p-q}{q(q-1)}|_q = q$ and $|\frac{p-q}{q(q-1)}|_p = 1$. Hence the second and third coordinate of x are exactly $\mathbb{Z}_q$ and $\mathbb{Z}_p$. We now have

$$\frac{p}{q}x$$

$$= \frac{p-q}{q(q-1)}\left((\sum_{i=1}^{\infty} a_{i+1}(\frac{p}{q})^{-i}, -\sum_{i=1}^{\infty} a_{i+1}(\frac{p}{q})^{-i}, \sum_{i=-\infty}^{0} a_i(\frac{p}{q})^{-i+1}) + (a_1, -a_1, 0)\right)$$

$$= \frac{p-q}{q(q-1)}(\sum_{i=1}^{\infty} a_{i+1}(\frac{p}{q})^{-i}, -\sum_{i=1}^{\infty} a_{i+1}(\frac{p}{q})^{-i}, \sum_{i=-\infty}^{0} a_{i+1}(\frac{p}{q})^{-i})$$

So again, we have that multiplication by $\frac{p}{q}$ is just shifting of the sequence of digits. Dividing is a backward shift, as can be shown by almost the same calculation. Now assume $\{a_i\}$ contains a forbidden word, at say a_{i+m}. Then for the first coordinate of $(\frac{p}{q})^m x$ we have either

$$\frac{p-q}{q(q-1)}\sum_{i=1}^{\infty} a_{i+m}(\frac{p}{q})^{-i} \geq \frac{p-q}{q(q-1)}\sum_{i=1}^{k} a_{i+m}(\frac{p}{q})^{-i}$$

$$> \frac{p-q}{q(q-1)}\frac{q(q-1)}{p-q}d = d$$

or

$$\frac{p-q}{q(q-1)}\sum_{i=1}^{\infty} a_{i+m}(\frac{p}{q})^{-i} \leq \frac{p-q}{q(q-1)}(\sum_{i=1}^{k} a_{i+m}(\frac{p}{q})^{-i} + \frac{q}{p}^k\frac{q(q-1)}{p-q})$$

$$< \frac{p-q}{q(q-1)}\left(\frac{q(q-1)}{p-q}(c - (\frac{q}{p})^k)\right) + (\frac{q}{p})^k = c$$

Now assume property 2 does not hold. Then there exists an $m \in \mathbb{Z}$ such that

$$\frac{p-q}{q(q-1)}\sum_{i=1}^{\infty} a_{i+m}(\frac{p}{q})^{-i} > d$$

or

$$\frac{p-q}{q(q-1)}\sum_{i=1}^{\infty} a_{i+m}(\frac{p}{q})^{-i} < c$$

But then the same must hold for the finite sequence $\frac{p-q}{q(q-1)}\sum_{i=1}^{k} a_{i+m}(\frac{p}{q})^{-i}$ for some $k \in \mathbb{N}$, implying $\{a_i\}$ contains a forbidden word.

□

4.4 Some remarks

This master's thesis started out with the study of the space $\mathfrak{X}$. To be more precise, with the study of a conjecture.

Conjecture 4.4.1. *We say that a sequence $\{a_i\}$ is admissible if it does not contain any forbidden words. Consider the embedding of the sequence $\{a_i\}$ into $\mathbb{R} \times \mathbb{Q}_q \times \mathbb{Q}_p$ defined as in theorem 4.3.2. Then the projection onto $\mathbb{R} \times \mathbb{Q}_q$ of the image of this map is a fundamental domain with respect to the lattice $\mathbb{Z}[\frac{1}{q}]$.*

This is a p-adic analogue of a well-known conjecture in numeration systems, known as the Pisot conjecture. The most famous example where this holds is due to Rauzy in [12]. The fundamental domain here is the beautiful 'Rauzy fractal'. As happens often, the subject of the thesis moved over time to a study of Schmidt's work on Pisot numbers and the conjecture on the embedding into $\mathbb{R} \times \mathbb{Q}_q \times \mathbb{Q}_p$ remains open.

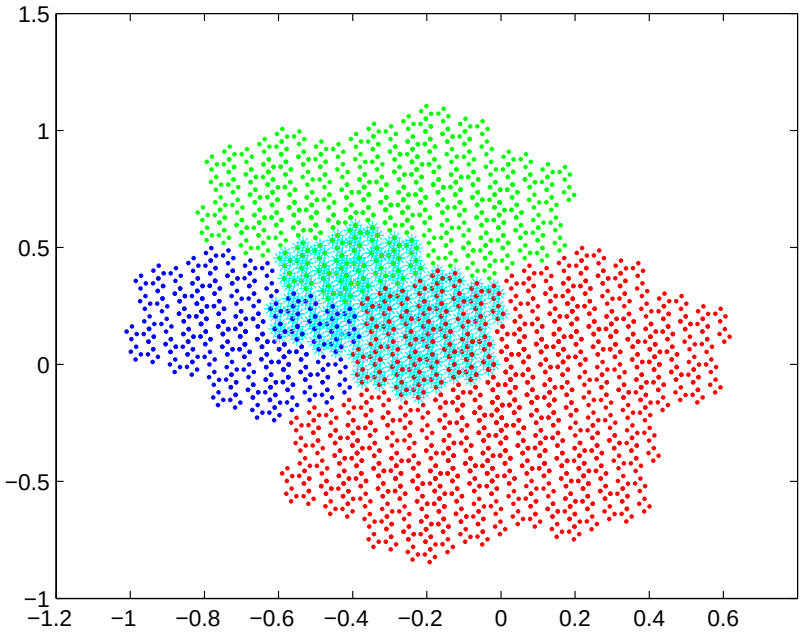

Figure 4.3: The original Rauzy fractal in $\mathbb{R}^2$

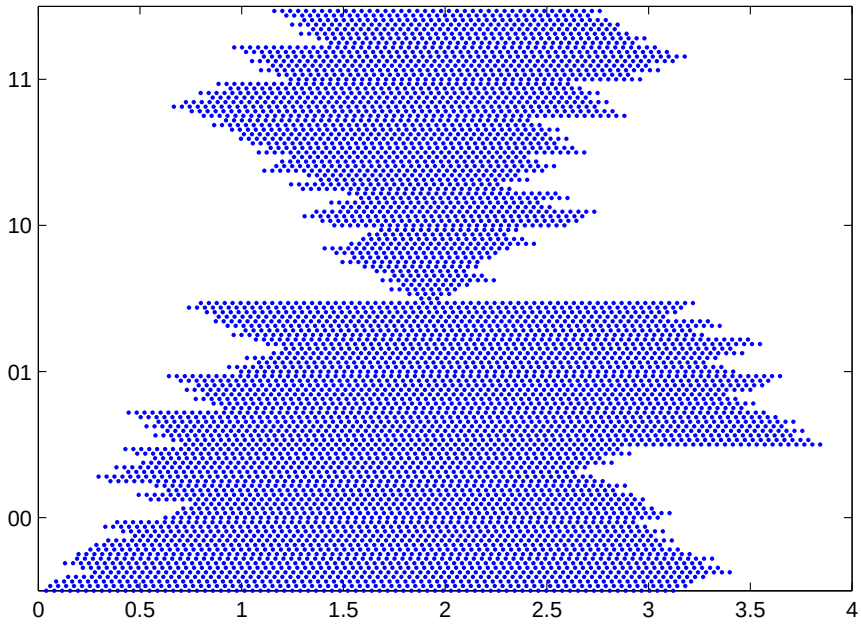

Figure 4.4: Our 'fractal' in $\mathbb{R} \times \mathbb{Q}_2$

Chapter 5

Conclusion

We have introduced a new perspective on Mahler's problem. Although no startling new breakthroughs have been found, lifting the problem to the space $\mathfrak{Y}$ is in itself very interesting. Also, we would like to note again the new results found as described at the end of chapter 2, which are very much related to the same problem.

Schmidt's theorem on periodicity has been generalized in an elegant way, by looking at the material on a higher level, i.e. as a lattice on $\mathbb{R}^d \times \mathbb{Q}_p(\beta)$. However, there is still room for some improvement, e.g. by looking at random expansions, not just the greedy one. Parts of the current proof are then still applicable, other parts have to be looked at. Also the remark on l-adic expansions following the proof could be made more explicit.

A very much related issue is that the proof now starts with some $1 < \beta \in \mathbb{R}$, it should be possible to find a more general and symmetric proof by just taking any minimum polynomial and considering its roots in various valuations.

Afterword

My research of the last few months has been initiated by an idea of dr Fokkink, to whom I owe a lot. By looking at an intriguing number theoretical problem from a more abstract perspective he hoped to find some new insights. He first ventured to make this a four-year PhD research, but when denied funding on the grounds of the project being too hard, he decided to hand it to me as material for a Master's thesis. For this, I am grateful.

During the last few months, my research has taken me through whole new fields of mathematics, looking at a range of related papers, theorems and the theory behind them. Although rarely rewarding and often frustrating, the project has always been challenging, I feel I have learned a lot. Not just about mathematics, but also about scientific research and what it entails.

In this report you have found those parts of my research I deemed worthy to write down (or could remember), as well as quite some mathematical theory behind the theorems. Most of the proofs are from my hand, on which my supervisor insisted. For this, I am less grateful.

Bibliography

[1] Shigeki Akiyama, Christiane Frougny, Jacques Sakarovitch, *On the Representation of Numbers in a Rational Base*, Proceedings of Words 2005, (S. Brlek et Ch. Reutenauer, eds.), Monographies du LaCIM 36 UQaM, Montréal, Canada, 47-64 (2005)

[2] Arturas Dubickas, Micheal J Mossinghoff, *Lower bounds for Z-numbers*, Mathematics of Computation (2009), published electronically

[3] Arturas Dubickas. *On the powers of 3/2 and other rational numbers*, Math. Nachr. 281, No. 7, 951-958 (2008)

[4] Leopold Flatto, *Z-numbers and β-transformations*, Symbolic Dynamics and its applications, American Mathematical Society, 181-201 (1992)

[5] Carl Friedrich Gauss, *Disquisitiones Arithmeticae*, article 42 (1801)

[6] Svetlana Katok, *p-adic Analysis compared with Real*, American Mathematical Society Bookstore (2007)

[7] Neal Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, 2nd edition, Springer-Verlag (1984)

[8] Serge Lang, *Undergraduate Algebra*, 3rd edition, New York: Springer (2005)

[9] K. Mahler *An unsolved problem on the powers of 3/2*, J. Austral. Math. Soc. 8, 313-321 (1968)

[10] K.Mahler, *p-adic numbers and their functions*, Cambridge University Press (1973)

[11] A. Ostrowski, *Über sogennante perfekte Körper.*, J. reine angew. Math. 147, 191-204 (1917).

[12] G. Rauzy, *Nombres Algébriques et substitutions*, Bull. Soc. math. France 110, 147-178 (1982)

[13] K. Schmidt, *On periodic expansions of Pisot numbers and Salem numbers*, Bull. London Math. Soc. 12, 269-278 (1980)

[14] R. Tijdeman, *Note on Mahler's $\frac{3}{2}$ problem*, K. norske Vidensk. Selsk. Skr. 16, 1-4 (1972)

[15] Rolf Ypma, *Muntjes en kettingbreuken*, 4, (2007)