p-adic Methods for rationality

Tuan Dung Hoang and Léo Reverte

May 2025

Contents

1 Introduction

Borel's theorem gives us a condition on the convergence of a power series for being a rational function, whose coefficients are integers.

Theorem 1.1 (Borel)**.** *Let* $f(X) = \sum_{i=0}^{\infty} a_i X^i \in \mathbb{Z}[\![X]\!]$*. Suppose that* f *is meromorphic in a disc of radius* $R > 1$*. Then,* f *is a rational function.*

In this bachelor thesis, we will present improvements of this result based on p-adic analysis. We will first introduce p-adic numbers and $\mathbb{Q}_p$ and prove a first improvement of Borel's theorem, that is the Borel-Dwork's theorem. Then, this can still be improved by constructing $\mathbb{C}_p$ and the analytic elements, that are the p-adic equivalents of $\mathbb{C}$ and the holomorphic functions. On our way, we will also show main results about p-adic numbers.
The construction of the $\mathbb{Q}_p$ and $\mathbb{C}_p$ are mainly based on Gouvêa's introduction to p-adic numbers [Gou20], and Robert's book [Rob00]. The theorems of Borel-Dwork and Polya-Bertrandias are well presented by Amice in [Ami75].

2 The p-adic field $\mathbb{Q}_p$

2.1 Absolute Values

In order to construct the p-adic numbers, we need an introduction to absolute values, and more precisely to non-archimedean absolute values. Let us begin with a definition.

Definition 2.1. Let $\Bbbk$ be a field. An absolute value on $\Bbbk$ is a function $|\cdot| : \Bbbk \longrightarrow \mathbb{R}_+$ that satisfies the following conditions:

1. $|x| = 0$ if and only if $x = 0$.
2. $|xy| = |x||y|$ for all $x, y \in \Bbbk$.
3. $|x + y| \leqslant |x| + |y|$ for all $x, y \in \Bbbk$.

An absolute value is said non-archimedean if it satisfies: $|x + y| \leqslant \max(|x|, |y|)$ for all $x, y \in \Bbbk$; otherwise, the absolute value is archimedean.

We recall that for any prime number p, we can extend the p-adic valuation on $\mathbb{Q}$, by $v_p(\frac{x}{y}) = v_p(x) - v_p(y)$; which depends only on rational $\frac{x}{y}$.

Definition 2.2. For any non-zero rational x, we define the p-adic absolute value of x by:

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

We also define $|0|_p = 0$.

Proposition 2.3. *The p-adic absolute value on $\mathbb{Q}$ is indeed an absolute value, which is non-archimedean.*

2.2 Elementary Properties

We will now examine elementary properties on a non-archimedean absolute value and the topology it induce.
Let $\Bbbk$ be a field with an absolute value $|\cdot|$.

Definition 2.4. The metric induced by the absolute value on $\Bbbk$ is:

$$d(x, y) = |x - y|, \forall x, y \in \Bbbk.$$

The following proposition is important and will be used twice in this bachelor thesis, but we will skip the proof since it is not a central point of our subject. A proof can be found in the Gouvêa's book [Gou20] (correction of the 72-th exercice, p.305).

Proposition 2.5. *Let $|\cdot|_1$ and $|\cdot|_2$ be two absolute values on the field $\Bbbk$. The following statements are equivalents.*

- *The metrics induced by the two absolute value define the same topology.*
- *There exists a positive real number α, such that:*

$$\forall x \in \Bbbk, |x|_2 = |x|_1^{\alpha}.$$

We now assume that $|\cdot|$ is non-archimedean.

Proposition 2.6. *If $x, y \in \Bbbk$ with $|x| \neq |y|$:*

$$|x + y| = \max(|x|, |y|).$$

The essential fact about the ultrametric space is the following corrolary.

Corollary 2.7. *All triangles are isosceles in an ultrametric space.*

Proposition 2.8. *Let a be in $\Bbbk$ and r be a non-zero positive real number.*

- *Every point in the open ball $B(a,r)$ is a center of the ball; that is, $\forall b \in B(a,r), B(b,r) = B(a,r)$.*
- *Every point in the closed ball $\overline{B}(a,r)$ is a center of the ball.*
- *$B(a,r)$ and $\overline{B}(a,r)$ are open and closed.*

Proof. Let b be in $B(a,r)$. For all x in $B(a,r)$, we have:

$$d(x,b) \leqslant \max(d(x,a), d(a,b)) < r.$$

Then, $B(a,r) \subseteq B(b,r)$, and the symmetry between a and b gives us $B(a,r) = B(b,r)$.
The second point is similar to the first.
For the third point, let us take c in $\Bbbk$ such that $d(c,a) \geqslant r$.
Assuming we have $x \in B(a,r) \cap B(c,r)$, we have:

$$d(a,c) \leqslant \max(d(a,x), d(x,c)) < r.$$

It's impossible, so $B(a,r) \cap B(c,r) = \varnothing$, and $B(a,r)$ is closed.

□

We can deduce from the previous results the following result.

Proposition 2.9. *The field $\Bbbk$ is a totally disconnected space.*

Important Remark. On a field with a non-archimedean absolute value, we have all tools to define the derivative of a function and all what we can pretend to need to do analysis. However, this approach misses the point. Indeed, this fails since $\Bbbk$ is a totally disconnected space. For a function, being differentiable is not a strong enough property to have an interest.
Let us take for example the indicator function of a ball (closed or open). For every $x \in \Bbbk$, the function is constant on a neighborhood of x, so it is differentiable and its derivative is constant, equal to 0.
This simple example is probably sufficient to show that our classical results of real or complex analysis are no longer true with a non-archimedean absolute value. This is why we will later use power series and analytic elements, avoiding the notion of derivative.

Proposition 2.10. *The subset:*

$$\mathcal{O} = \overline{B}(0,1)$$

is subring of $\Bbbk$ and is called the valuation ring of $|\cdot|$.
$\mathfrak{p} = B(0,1)$ is the only maximal ideal of $\mathcal{O}$ and is called the valuation ideal of $|\cdot|$.
$\kappa = \Omega/\Pi$ is called the residue field of $|\cdot|$.

2.3 Construction of $\mathbb{Q}_p$

The Ostrowski's theorem gives a first justification of the study of p-adic absolute values. It will not be proven here.

Theorem 2.11 (Ostrowski)**.** *Two absolute values are said equivalent if the metrics their induce give the same topology.*
A non-trivial absolute value $|\cdot|$ on $\mathbb{Q}$ ($|x| \neq \nVdash_{x\neq 0}$) is either equivalent to the usual archimedean absolute value, or equivalent to $|\cdot|_p$ for p a prime number.

We now fix p, a prime number.

Definition 2.12. We denote $\mathbb{Q}_p$ the completion of $\mathbb{Q}$ for the metric induced by $|\cdot|_p$ on $\mathbb{Q}$.

Remark. We already have a metric on $\mathbb{Q}_p$, and we easily deduce an extension of $|\cdot|_p$ to $\mathbb{Q}_p$. If $(x_n) \in \mathbb{Q}^{\mathbb{N}}$ and $x = \lim_{n\to\infty} x_n \in \mathbb{Q}_p$, we define :

$$|x|_p = d_{\mathbb{Q}_p}(0, x) = lim_{n\to\infty}|x_n|_p.$$

The absolute value on $\mathbb{Q}_p$ is non-archimedean The image of $\mathbb{Q}\backslash\{0\}$ by the application $|\cdot|_p$ is $\{p^k, k \in \mathbb{Z}\}$, which is discrete. So, we have eventually that $|x_n|_p = |x|_p$. Then, $\mathbb{Q}$ and $\mathbb{Q}_p$ have the same image by $|\cdot|_p$.

We now want to have a better understanding of the structure of $\mathbb{Q}_p$. We will first study the p-adic integers, which are defined in the following definition, and then give a simple representation for the elements of $\mathbb{Q}_p$. In our way, we will see how the algebraic and topological aspects of p-adic numbers are linked.

Definition 2.13. The valuation ring of $\mathbb{Q}_p$ is denoted by $\mathbb{Z}_p$ and its elements are called p-adic integers.

Since:

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p, |x|_p \leqslant 1\},$$

we have that:

$$\mathbb{Q} \cap \mathbb{Z}_p = \{\frac{a}{b} \in \mathbb{Q}, p \nmid b\},$$

and:

$$\mathbb{Z} \subset \mathbb{Z}_p.$$

Proposition 2.14. *The valuation ideal of* $\mathbb{Q}_p$ *is* $p\mathbb{Z}_p$.
Furthermore, the ideals of $\mathbb{Q}_p$ *are the* $p^n\mathbb{Z}_p = \{x \in \mathbb{Q}_p, |x|_p \leqslant p^{-n}\} = B(0, p^{-n})$, *with* $n \geqslant 0$.

We now want to give a more understandable expression for p-adic numbers. We start by showing that p-adic integers are limits of sequences of elements of $\mathbb{Z}$ with nice properties.

Theorem 2.15. *Let us fix a p-adic integer x. There exists a sequence of integers* $(x_n) \in \mathbb{Z}^{\mathbb{N}}$ *such that:*

- $x_n \equiv x \pmod{p^n}$;
- $0 \leqslant x_n \leqslant p^n - 1$.

Corollary 2.16. *For* $n \geqslant 1$, *we have:*

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}.$$

In particular, the residue field is:

$$\kappa = \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p.$$

Remark. A point to clarify is that :

$$a \equiv b \pmod{p^n}$$

in $\mathbb{Z}_p$ means:

$$a \equiv b \pmod{I},$$

with I the ideal generated by p^n in $\mathbb{Z}_p$, i.e. $p^n\mathbb{Z}_p$.
The important point is that this is equivalent to $|a - b| \leqslant p^{-n}$.

Remark. The Theorem 2.15 gives us a sequence $(x_n)_{n\in\mathbb{N}}$, such that: $x_n \longrightarrow x$.
So, $\mathbb{Z}$ is dense in the ring of p-adic integers.

Proof of the Theorem 2.15. $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, so, for a fixed $n \in \mathbb{N}$, there exists $\frac{a}{b} \in \mathbb{Q}$ such that $|\frac{a}{b} - x| \leqslant p^{-n}$. Then, $|\frac{a}{b}| \leqslant \max(|x|, |\frac{a}{b} - x|) \leqslant 1$. So we can assume that $p \nmid b$. Then, we have $k \in \mathbb{Z}$ such that $p^n | a - kb$, that is $|\frac{a}{b} - k| \leqslant p^{-n}$.
We have yet : $|k - x| \leqslant p^{-n}$.
We have x_n such that $0 \leqslant x_n \leqslant p^n - 1$ and $x_n \equiv k \pmod{p^n}$. Then x_n satisfies the two points of the theorem.

□

Remark. A such sequence is unique, with respect to x. We notice that for all $n \in \mathbb{N}$, $x_n \equiv x_{n+1} \pmod{p^n}$.

We can rewrite the sequence :

$$\begin{aligned} x_1 &= b_0 \\ x_2 &= b_0 + pb_1 \\ x_3 &= b_0 + pb_1 + p^2b_2 \\ x_4 &= b_0 + pb_1 + p^2b_2 + p^3b_3 \\ &\vdots \end{aligned}$$

with all b_i integers inferior to p, and unique.
We will then write : $x = b_0 + pb_1 + p^2b_2 + p^3b_3 + p^4b_4 \ldots$
This makes perfect sense since $p^k \xrightarrow[k\to\infty]{} 0$.

For every $y \in \mathbb{Q}_p$, there exists $k \in \mathbb{Z}$ such that: $|p^k y|_p \leqslant 1$, that is $p^k y \in \mathbb{Z}_p$. We deduce the following proposition.

Proposition 2.17. *Every $y \in \mathbb{Q}_p$ can be rewritten as:*

$$y = p^{-k}b_{-k} + \ldots + b_0 + pb_1 + p^2b_2 + p^3b_3 + \ldots$$

with $k \in \mathbb{N}$ and $b_i \in \{0, ..., p-1\}$, which are unique.

Example. Let us compute the expansion of $-\frac{1}{2}$ in $\mathbb{Q}_3$. In this situation, we compute coefficient by coefficient to find the b_i. Then, we will probably have a sequence of coefficient that repeat after a certain rank.
We have:

$$-\frac{1}{2} \equiv 1 \pmod 3, \tag{1}$$

and:

$$-\frac{1}{2} = 1 + 3 \cdot (-\frac{1}{2}). \tag{2}$$

From the equation 1, we have that $-\frac{1}{2} = 1 + b_1 \cdot 3 + b_2 \cdot 3^2 + \cdots$
But the equation 2 the recursive way of computing the b_i. So:

$$-\frac{1}{2} = 1 + 3 + 3^2 + 3^3 + \cdots$$

We can also compute with the expansions, for example, $-\frac{1}{2}$ is solution of $2x + 1 = 0$. Indeed:

$$\begin{aligned} 2 \cdot (1 + 3 + 3^2 + \cdots) + 1 &= (2 + 2 \cdot 3 + 2 \cdot 3^2 + \cdots) + 1 \\ &= 3 + 2 \cdot 3 + 2 \cdot 3^2 + \cdots \\ &= 3^2 + 2 \cdot 3^2 + \cdots \\ &= 0 \end{aligned}$$

Important Remark. This whole chapter shows the precise and deep relations between topological and arithmetical aspects of the p-adic numbers. This come from the arithmetical definition of the absolute value. It gives hopeful prospects to have algebraic results from analytic hypothesis.

2.4 Hensel's lemma

We follow construction in [Neu99] One of our chief concerns will be to study the finite extensions $L/\mathbb{Q}_p$. This means that we have to turn to the question of factoring algebraic equations:

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0.$$

We call a polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathcal{O}[x] = \mathbb{Z}_p[x]$ *primitive* if $f(x) \not\equiv 0 \mod p$, i.e., if:

$$|f| = \max\{|a_0|, \ldots, |a_n|\} = 1.$$

Theorem 2.18 (Hensel)**.** *Let us assume that a primitive polynomial $f(x) \in \mathcal{O}[x]$ admits modulo p a factorization:*

$$f(x) \equiv \overline{g}(x)\overline{h}(x) \pmod p$$

into relatively prime polynomials $\overline{g}, \overline{h} \in \kappa[x] = \mathbb{F}_p[x]$.
Then $f(x)$ admits a factorization:

$$f(x) = g(x)h(x)$$

into polynomials $g, h \in \mathcal{O}[x]$ such that $\deg(g) = \deg(\overline{g})$ *and:*

$$g(x) \equiv \overline{g}(x) \pmod p \quad \textit{and} \quad h(x) \equiv \overline{h}(x) \pmod p.$$

Proof. Let $d = \deg(f)$, $m = \deg(\overline{g})$, hence $d - m \geqslant \deg(\overline{h})$. Let g_0, $h_0 \in \mathcal{O}[x]$ be polynomials such that

$$g_0 \equiv \overline{g} \mod p, \quad h_0 \equiv \overline{h} \mod p,$$

and $\deg(g_0) = m$, $\deg(h_0) \leqslant d - m$. Since $(\overline{g}, \overline{h}) = 1$, there exist polynomials $a(x), b(x) \in \mathcal{O}[x]$ satisfying

$$ag_0 + bh_0 \equiv 1 \mod p.$$

Among the coefficients of the two polynomials $f - g_0h_0$ and $ag_0 + bh_0 - 1 \in \mathfrak{p}[x] = p\mathbb{Z}_p[x]$ we pick one with minimum value and call it π.
Let us look for the polynomials g and h in the following form:

$$g = g_0 + p_1\pi + p_2\pi^2 + \cdots, \quad h = h_0 + q_1\pi + q_2\pi^2 + \cdots,$$

where $p_i, q_i \in \mathcal{O}[x]$ are polynomials of degree $< m$, resp. $\leqslant d - m$. We then determine successively the polynomials

$$g_n = g_0 + p_1\pi + \cdots + p_n\pi^n, \quad h_n = h_0 + q_1\pi + \cdots + q_n\pi^n,$$

in such a way that one has

$$f \equiv g_n h_n \mod \pi^{n+1}.$$

Passing to the limit as $n \to \infty$, we will finally obtain the identity $f = gh$. For $n = 1$ the congruence is satisfied in view of our choice of π. Let us assume that it is already established for some $n \geqslant 1$. Then, in view of the relation

$$g_n = g_{n-1} + p_n\pi^n, \quad h_n = h_{n-1} + q_n\pi^n,$$

the condition on g_n, h_n reduces to

$$f - g_{n-1}h_{n-1} \equiv (g_n - q_n + h_{n-1} - p_n)\pi^n \mod \pi^{n+1}.$$

Dividing by π^n, this means

$$g_n - q_n + h_{n-1} - p_n \equiv g_0q_n + h_0p_n = f_n \mod \pi,$$

where $f_n = \pi^{-n}(f - g_{n-1}h_{n-1}) \in \mathcal{O}[x]$. Since $g_0a + h_0b \equiv 1 \mod \pi$, one has

$$g_0af_n + h_0bf_n = f_n \mod \pi.$$

At this point we would like to put $q_n = af_n$ and $p_n = bf_n$, but the degrees might be too big. For this reason, we write

$$b(x)f_n(x) = q(x)g_0(x) + \pi p_n(x),$$

where $\deg(p_n) < \deg(g_0) = m$. Since $g_0 \equiv \bar{g} \mod \pi$ and $\deg(g_0) = \deg(\bar{g})$, the highest coefficient of g_0 is a unit; hence $q(x) \in \mathcal{O}[x]$ and we obtain the congruence

$$g_0(af_n + h_0 q) + h_0 p_n = f_n \mod \pi.$$

Omitting now from the polynomial $af_n + h_0 q$ all coefficients divisible by π, we get a polynomial q_n such that $g_0 q_n + h_0 p_n = f_n \mod \pi$ and which, in view of $\deg(f_n) \leqslant d$, $\deg(g_0) = m$ and $\deg(h_0 p_n) < (d-m) + m = d$, has degree $\leqslant d - m$ as required.

□

Example: The polynomial $x^{p-1} - 1 \in \mathbb{Z}_p[x]$ splits over the residue class field $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$ into distinct linear factors. Applying (repeatedly) Hensel's lemma, we see that it also splits into linear factors over $\mathbb{Z}_p$. We thus obtain the result that the field $\mathbb{Q}_p$ of p-adic numbers contains the $(p-1)$-th roots of unity. These, together with 0, even form a system of representatives for the residue class field, which is closed under multiplication.

3 $\mathbb{C}_p$, the p-adic equivalent of the complex field

3.1 Algebraic extensions of $\mathbb{Q}_p$

Our goal is now to construct a p-adic equivalent of $\mathbb{C}$, that is an algebraically closed and complete field. We begin by extending the p-adic absolute value to algebraic extensions of $\mathbb{Q}_p$, and to its algebraic closure. The following proposition states that if an extension of the absolute value exists, it is unique.

Proposition 3.1. *Let K be a field with an absolute value $|\cdot|$, and let L a finite extension of K. Then, there is at most one absolute value on L that extends $|\cdot|$.*

Proof. Let us assume there is two absolute values $|\cdot|_1$ and $|\cdot|_2$ on L that both extend $|\cdot|$. The two absolute values are also norms on the K-vector space L. Furthermore, L/K is a finite extension, so all norms are equivalent on L. That means that $|\cdot|_1$ and $|\cdot|_2$ define the same topology. By the Proposition 2.5, there exists a positive real number α, such that:

$$|\cdot|_1^\alpha = |\cdot|_2.$$

But the two absolute values are equal on K, so:

$$|\cdot|_1 = |\cdot|_2.$$

□

Definition 3.2. Let K/F be a finite field extension. If x lies in K, the multiplication by x is a linear automorphism of K, seen as a F-vector space. We define $N_{K/F}(x)$ as the determinant of this automorphism. The application:

$$N_{K/F} : K \longrightarrow F$$

is called the norm from F to K (even if it is not a norm in the sense of linear algebra).

Proposition 3.3. *Let us assume $K/\mathbb{Q}_p$ is a finite field extension, and $n = [K : \mathbb{Q}_p]$. The application:*

$$x \in K \longrightarrow \sqrt[n]{|N_{K/\mathbb{Q}_p}(x)|_p} \in \mathbb{R}_+$$

is a non-archimedean absolute value that extends the p-adic absolute value from $\mathbb{Q}_p$ to K, and it is the unique extension.

Before proving this, let us take a look at one important fact: the absolute value of an element x of a finite extension of $\mathbb{Q}_p$ does not depend on the extension chosen, as the next proposition states.

Proposition 3.4. *Let $\mathbb{Q}_p \subseteq L \subseteq K$ be a tower of finite extensions. Let $m = [L : \mathbb{Q}_p]$ and $n = [K : \mathbb{Q}_p]$. If $x \in L$, then:*

$$\sqrt[m]{|N_{L/\mathbb{Q}_p}(x)|_p} = \sqrt[n]{|N_{K/\mathbb{Q}_p}(x)|_p}.$$

Proof. We denote $k = n/m$.
Let $(a_1, \dots, a_k)$ be a L-basis of K.
Since x lies in L, the multiplication by x (a linear application on K) stabilizes all the one-dimensional vector spaces La_i. So its determinant is the product of all determinants of its restrictions to the one-dimensional vector spaces, and then:

$$N_{K/\mathbb{Q}_p}(x) = (N_{L/\mathbb{Q}_p}(x))^k.$$

We deduce the proposition from this formula. □

Proof of the Proposition 3.3. The uniqueness directly follows the Proposition 3.1.
The determinant $N_{K/\mathbb{Q}_p}(x)$ is zero, if and only if the multiplication by x is not invertible as a linear function, that is, $x = 0$.
Furthermore, our new application is multiplicative, since the determinant is multiplicative.
It also extend the p-adic absolute value, because if $x \in \mathbb{Q}_p$:

$$N_{K/\mathbb{Q}_p}(x) = x^{[K:\mathbb{Q}_p]}$$

We will now prove the non-archimedean property.
Let us denote $|x| = \sqrt[m]{|N_{L/\mathbb{Q}_p}(x)|_p}$.
We take $x \in K$, and by the Poposition 3.4, we can take $K = \mathbb{Q}_p(x)$. It is sufficient to prove that:

$$|x| \leqslant 1 \Rightarrow |x - 1| \leqslant 1$$

i.e.:

$$|N_{K/\mathbb{Q}_p}(x)|_p \leqslant 1 \Rightarrow |N_{K/\mathbb{Q}_p}(x - 1)|_p \leqslant 1$$

i.e.:

$$|N_{K/\mathbb{Q}_p}(x)|_p \in \mathbb{Z}_p \Rightarrow |N_{K/\mathbb{Q}_p}(x - 1)|_p \in \mathbb{Z}_p$$

Let $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be the minimal polynomial for x.
By expressing the determinant of the multiplication by x in the base $(1, x, x^2, \dots, x^{n-1})$, we have that:

$$N_{K/\mathbb{Q}_p}(x) = (-1)^n a_0$$

Since the minimal polynomial of $x - 1$ is:

$$P(x + 1) = x^n + \cdots + (1 + a_{n-1} + \cdots + a_0),$$

we need:

$$a_0 \in \mathbb{Z}_p \Rightarrow (1 + a_{n-1} + \cdots + a_0) \in \mathbb{Z}_p.$$

In fact, we can prove that all a_i belong to $\mathbb{Z}_p$ (which is an even better result).
Let assume that there exists $a_i \notin \mathbb{Z}_p$. We then define $Q(x) = p^k P(x) = p^k x^n + b_{n-1}x^{n-1} + \cdots + b_0$, where k is the smaller integer, such that all b_i belong to $\mathbb{Z}_p$. Then, we take l the smaller integer, such that b_l is not divisible by p, and we have:

$$Q(x) \equiv (p^k x^{k-l} + \cdots + b_l)x^l \pmod{p}$$

The Hensel's Lemma (2.18), we have that $Q(x)$ is reducible, and therefore $P(x)$ is also reducible. That is a contradiction.
So, all a_i belong to $\mathbb{Z}_p$, and the non-archimedean property is proven. □

The Proposition 3.4 allows us to extend the p-adic absolute value to the algebraic closure of $\mathbb{Q}_p$, since the extended absolute value of an element does not depend on the field in which we consider this element.

Proposition 3.5. *The p-adic absolute value extends to $\overline{\mathbb{Q}}_p$, the algebraic closure of $\mathbb{Q}_p$. And this extension is unique.*

Maybe, one can think we are done with our goal of finding an equivalent of $\mathbb{C}$. But we really need completeness in order to do analysis, and unfortunately we do not have that yet.

Proposition 3.6. *$\overline{\mathbb{Q}}_p$ is not complete.*

Proof. We will use the Baire theorem. If we can prove that $\overline{\mathbb{Q}}_p$ is not a Baire space, then it cannot be complete.
We denote $Z_n = \{x \in \overline{\mathbb{Q}}_p, [\mathbb{Q}_p(x) : \mathbb{Q}_p] \leqslant n\}$, for $n \geqslant 1$.
We have: $\overline{\mathbb{Q}}_p = \bigcup_{n \geqslant 1} Z_n$.

First, the Z_n are closed. Let $(x_i) \in Z_n^{\mathbb{N}}$. For every $i \in \mathbb{N}$, we have $P_i \in \mathbb{Q}_p[x]$, with $\deg P_i \leqslant n$ and $P_i(x_i) = 0$. Multiplying if necessary the P_i, we can assume that their coefficients are bounded (they all lie in $\mathbb{Z}_p$, for example). Extracting if necessary, we can now assume $P_i \longrightarrow P \in \mathbb{Q}_p[x]$.
We denote $P_i(x) = \sum_{k \leqslant n} a_i^k x^k$ and $P(x) = \sum_{k \leqslant n} a^k x^k$. Then:

$$\begin{aligned} P(x_i) &= P(x_i) - P_i(x_i) \\ &\leqslant \max_{k \leqslant n} (a^k - a_i^k) x_i^k \\ &\xrightarrow[i \to \infty]{} 0, \end{aligned}$$

since $a_i^k \longrightarrow a^k$ and x_i^k is bounded.
Furthermore: $P(x_i) \longrightarrow P(x)$, by continuity.
So we have: $P(x) = 0$, and then $x \in Z_n$.

Second, Z_n have no interior point. Indeed, for every ball $B \subset \overline{\mathbb{Q}}_p$, we have $\mathbb{Q}_p.B = \overline{\mathbb{Q}}_p$. So, if there exists a ball $B \subseteq Z_n$, we have $\overline{\mathbb{Q}}_p = \mathbb{Q}_p.B \subseteq \mathbb{Q}_p.Z_n = Z_n$. That is impossible.

$\overline{\mathbb{Q}}_p$ is not a Baire space, and then it is not complete.

□

3.2 $\mathbb{C}_p$

We finally achieve our goal of constructing an algebraically closed and complete extension of $\mathbb{Q}_p$ by going through the completion again.

Definition 3.7. The result of the completion of $\overline{\mathbb{Q}}_p$ is denoted $\mathbb{C}_p$, considering that it is the p-adic equivalent of $\mathbb{C}$.

Proposition 3.8. *$\mathbb{C}_p$ is algebraically closed.*

Proof. We do not have a specific object that we need for this proof. Indeed, we will need an extension of the absolute value on the algebraic closure of $\mathbb{C}_p$ (we do not know yet that it is $\mathbb{C}_p$ itself). We will just admit that we can extend our absolute value. Robert gives a precise proof by constructing a universal p-adic field in [Rob00] (pages 137-142).

Let $P(x) = \sum_{n \leqslant d} a_n x^n \in \mathbb{C}_p[x]$ an irreducible polynomial. We assume $d \geqslant 2$ and that the zeros of $P(x)$, denoted $(a_1, \ldots, a_d)$, are not in $\mathbb{C}_p$. We also fix $b \in \overline{\mathbb{Q}}_p$ such that:

$$\forall i \in [\![2; d]\!], |b - a_1| < |b - a_i|.$$

We have at least one morphism $\sigma : \mathbb{C}_p(a_1) \longrightarrow \overline{\mathbb{C}}_p$, such that $\sigma(a_1) \neq a_1$ (a_1 is sent on one of its conjugates). But now, $|\sigma(\cdot)|$ is an absolute value. By uniqueness of the extension of the absolute value (Proposition 3.1), we have that:

$$|b - \sigma(a_1)| = |\sigma(b) - \sigma(a_1)| = |\sigma(b - a_1)| = |b - a|.$$

That is impossible by our choice of b. So $P(x)$ cannot have a degree greater than one, and $\mathbb{C}_p$ is algebraically closed. ☐

Proposition 3.9. *We can extend the* p*-adic absolute value to* $\mathbb{C}_p$*, and* $|\mathbb{C}_p|_p = \{p^{\alpha}, \alpha \in \mathbb{Q}\} \cup \{0\}$.

Proof. Since $|\cdot|_p$ is non-archimedean on $\overline{\mathbb{Q}}_p$, if (x_i) is a Cauchy sequence in $\overline{\mathbb{Q}}_p$, we have that $|x_i|_p$ is stationary. We then define: $|\lim x_i|_p = \lim |x_i|_p$.

Clearly, the image of $\mathbb{C}_p$ by $|\cdot|_p$ is the same as the image of $\overline{\mathbb{Q}}_p$.
Then, the proposition comes from the definition of the p-adic absolute value on $\overline{\mathbb{Q}}_p$. ☐

4 The Borel-Dwork theorem

4.1 Power series

We can now define power series on $\mathbb{Q}_p$ and on $\mathbb{C}_p$.

Remark. A power series $f(X) = \sum_{i=0}^{\infty} a_i X^i \in \mathbb{Q}_p[\![x]\!]$ converges on z if and only if $|a_i z^i|_p \longrightarrow 0$, because $|\cdot|_p$ is non-archimedean.

The criterion is simpler than in real and complex fields. It follows that the regions of convergence are also simpler.

Proposition 4.1. *Consider a power series* $f(x) = \sum_{i=0}^{\infty} a_i x^i$*. The radius of convergence of* $f(x)$ *is:*

$$\rho = \frac{1}{\limsup_{i\to\infty} \sqrt[i]{|a_i|}}$$

More precisely:

- *if* $|a_i|_p \rho^i \longrightarrow 0$ *(i.e.,* $f(\rho)$ *converges), then* $f(z)$ *converges if and only if* $|z| \leqslant \rho$.
- *if* $(|a_i|_p \rho^i)_{i\in\mathbb{N}}$ *does not tend to 0, then* $f(z)$ *converges if and only if* $|z| < \rho$.

4.2 The Theorem

This is a first improvement of Borel's theorem. It is a distinctive feature of the p-adic approach: we use analytic properties to prove an algebraic result.
We follow the proof of Cassels in [Cas86].

Theorem 4.2 (Borel-Dwork)**.** *Let*

$$f(X) = f_0 + f_1 X + \cdots + f_n X^n + \cdots \tag{3}$$

be a formal power series, where $f_n \in \mathbb{Q}$*. Suppose that there is a finite set* S *of prime numbers such that:*

(i) $|f_n|_p \leqslant 1$ *for all* $p \notin S$ *and all* n.

(ii) f *defines a function meromorphic on a disk* $B(0, R)$ *in* $\mathbb{C}$.

(iii) For each $p \in S$ *there is a polynomial*

$$g_p(X) = 1 + g_{1,p}X + \cdots + g_{m,p}X^m \in \mathbb{Q}_p[X]$$

such that the series $g_p(X)f(X)$*, considered as a series with coefficients in* k_p*, has radius of convergence* R_p *in* $\mathbb{Q}_p$*.*

$$R \cdot \prod_{p \in S} R_p > 1.$$

Then $f(X)$ *is the expansion of an element of* $k(X)$*.*

We will need some lemmas in order to prove the theorem. We begin by proving the classic lemma 4.5

Lemma 4.3. *Let* A *be the determinant of the matrix*

$$\begin{pmatrix} a_{00} & a_{01} & \cdots & a_{0s} \\ a_{10} & a_{11} & \cdots & a_{1s} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s0} & a_{s1} & \cdots & a_{ss} \end{pmatrix},$$

let A_{ij} *be the elements of the adjoint matrix (*A_{ij} *is the cofactor of* a_{ji}*), and let* a *be the determinant of the* $(s-1) \times (s-1)$ *matrix obtained by deleting the first and last row and column. Then*

$$A_{00}A_{ss} - A_{0s}A_{s0} = Aa.$$

Remark. This is a special case of "Jacobi's Theorem on the minors of the adjugate".

Proof. Follows by taking determinants in the matrix identity

$$\begin{pmatrix} A_{00} & A_{01} & \cdots & A_{0,s-1} & A_{0s} \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & 1 & 0 \\ A_{s0} & A_{s1} & \cdots & A_{s,s-1} & A_{ss} \end{pmatrix} \begin{pmatrix} a_{00} & a_{01} & \cdots & a_{0,s-1} & a_{0s} \\ a_{10} & a_{11} & \cdots & a_{1,s-1} & a_{1s} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{s-1,0} & a_{s-1,1} & \cdots & a_{s-1,s-1} & a_{s-1,s} \\ a_{s0} & a_{s1} & \cdots & a_{s,s-1} & a_{ss} \end{pmatrix} =$$

$$\begin{pmatrix} A & 0 & \cdots & 0 & 0 \\ a_{10} & a_{11} & \cdots & a_{1,s-1} & a_{1s} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{s-1,0} & a_{s-1,1} & \cdots & a_{s-1,s-1} & a_{s-1,s} \\ 0 & 0 & \cdots & 0 & A \end{pmatrix}$$

Here the first matrix has 1 on the diagonal, 0 elsewhere, except in the first and last rows.

□

We shall be concerned with the Hankel determinant:

$$F(n,s) = \det(a_{ij})$$

for which

$$a_{ij} = f_{n+i+j} \quad (0 \leqslant i \leqslant s, \quad 0 \leqslant j \leqslant s)$$

and the f_n are the coefficients in the equation 3.

Corollary 4.4. *For every* $n \geqslant 0$ *and* $s \geqslant 1$*:*

$$F(n,s-1)F(n+2,s-1) - (F(n+1,s-1))^2 = F(n,s)F(n+2,s-2). \tag{4}$$

Lemma 4.5. *Suppose that there is an s such that $F(n,s) = 0$ for all sufficiently large n. Then $f(X)$ is the expansion of a rational function.*

Proof. Without loss of generality, s is minimal. There is thus some n_0 such that

$$F(n,s) = 0 \quad (\text{all } n \geqslant n_0) \tag{5}$$

$$F(n_0+1, s-1) \neq 0. \tag{6}$$

By the equation 5 the right-hand side of the equation 4 is 0 for all $n \geqslant n_0$. It now follows from the equation 6 by induction on n that

$$F(n, s-1) \neq 0 \quad (\text{all } n \geqslant n_0 + 1). \tag{7}$$

By the equations 5 and 7, for any $n \geqslant n_0 + 1$ there are unique $c_r = c_r(n)$ such that

$$f_{l+s} + c_1 f_{l+s-1} + \cdots + c_s f_l = 0 \quad (n \leqslant l \leqslant n+s). \tag{8}$$

On comparing the equation 8 for n and $n+1$ and using the equation 7, we readily deduce that $c_r(n+1) = c_r(n)$; that is, the c_r are independent of n. Hence

$$(1 + c_1 X + \cdots + c_s X^s) f(X)$$

is a polynomial in X, as required.

□

Lemma 4.6. *(i) Let A be the determinant of the matrix $(a_{ij})_{0 \leqslant i,j \leqslant s}$, where $a_{ij} \in \mathbb{Q}$, and let*

$$\alpha_i = \max_{0 \leqslant j \leqslant s} |a_{ij}| \qquad (0 \leqslant i \leqslant s).$$

Then:

$$|A|_p \leqslant \prod_{0 \leqslant i \leqslant s} \alpha_i$$

where $M(p,s)$ depends only on p and s.

(ii) With the usual absolute value on $\mathbb{Q}$, let

$$\alpha_i = \max_{0 \leqslant j \leqslant s} |a_{ij}|_p \qquad (0 \leqslant i \leqslant s).$$

Then:

$$|A| \leqslant (s+1)! \prod_{0 \leqslant i \leqslant s} \alpha_i$$

Proof. The result is due to this expression of the determinant:

$$A = \sum_j \sigma(j) a_{0,j(0)} a_{1,j(1)} \cdots a_{s,j(s)}$$

where j runs through the permutations of $\{0, \dots, s\}$, and $\sigma(j)$ is its signature.

□

Proof of the Theorem 4.2. By the hypothesis of the theorem,we can choose T such that $TR > 1$ and for $p \in S$, we can choose T_p such that

$$T_p R_p > 1 \quad \text{and} \quad T \cdot \prod_{p \in S} T_p < 1.$$

Then the coefficients of

$$h_p(X) = g_p(X) f(X) = h_0 + h_1 X + \dots \tag{9}$$

satisfy

$$|h_n|_p \leqslant T_p^n$$

for all sufficiently large n.
The formal expansion of $g_p^{-1}(X)$ as a power series clearly converges in some neighborhood of the origin. Hence $f(X)$, considered as a power series with coefficients in $\mathbb{Q}_p$, converges in some neighborhood of the origin. There is thus some $t_p > 0$ such that

$$|f_n|_p \leqslant t_p^n$$

for all sufficiently large n. We now estimate p-adically for $p \in S$ the determinants F(n,s). If s > m, which we suppose, we can use the recurrence relations furnished by the equation 9 to replace the f_{n+i+j} for $i \geqslant m$ by h_{n+i+j}. That means $F(n,s) = \det(b_{ij})$, where:

$$b_{ij} = \begin{cases} f_{n+i+j} & \text{for } 0 \leqslant i < m, \\ h_{n+i+j} & \text{for } m \leqslant i \leqslant s. \end{cases}$$

On using our estimates in the preceding lemma we readily obtain

$$|F(n,s)|_p \leqslant L_p \cdot t_p^{nm} \cdot T_p^{n(s-m)}$$

for all sufficiently large n, where $L_p = L_p(s)$ is independent of n.

Everything was express with a p-adic absolute value but we can apply the same proof to $\mathbb{C}$ and the classic absolute value. We find the same domination: $|F(n,s)| \leqslant L \cdot t^{nm} \cdot T^{n(s-m)}$.

By the hypothesis of the Theorem and by the preceding lemma, for all $p \notin S$ and all n and s we have:

$$|F(n,s)|_p \leqslant 1$$

Then:

$$\prod_{\text{all } p} |F(n,s)|_p \leqslant A \cdot B^{nm} \cdot C^{n(s-m)} \tag{10}$$

for all sufficiently large n, where

$$A = A(s) = L \cdot \prod_{p \in S} L_p, \qquad B = t \cdot \prod_{p \in S} t_p, \qquad C = T \cdot \prod_{p \in S} T_p < 1,$$

by hypothesis on the T_p.

Then, we can choose s so that:

$$D = B^m C^{s-m} < 1$$

and then, by the equation 10,

$$|F(n,s)| \cdot \prod_{\text{all } p} |F(n,s)|_p \leqslant AD^n < 1$$

for all sufficiently large n.
But for any $x \in \mathbb{Q} \backslash \{0\}$, we have:

$$|x| \cdot \prod_p |x|_p = 1$$

So, for all sufficiently large n: $F(n,s) = 0$.
The result now follows the Lemma 4.5.

□

5 Analytic elements and Polya-Bertrandias Theorem

5.1 Analytic elements

We follow construction in [Rob00] and [Ami75]
Since analytic continuation cannot be achieved by means of Taylor expansions in p-adic analysis, another procedure has to be devised. It was Krasner's idea to mimic the Runge theorem of complex analysis: A holomorphic function f defined in a domain D of the complex plane $\mathbb{C}$ can be uniformly approximated using rational functions .
More precisely, for each compact subset $C \in D$, choose $A = \{a_i\}_{i \in I}$ with one point in each connected component of the complement of C in the Riemann sphere. Then f can be uniformly approximated on C by rational functions having all their poles in the set A.
We denote
$\|f\|_D$ is the sup norm of f on D
let $R(D)$ denote the ring of rational functions having no pole in D:

$$R(D) = \left\{ f = \frac{g}{h} : g, h \in \mathbb{C}_p[X],\ h \text{ having no zero in } D \right\}.$$

Definition. Let D be a closed subset of $\mathbb{C}_p$. A function $f : D \to \mathbb{C}_p$ is an analytic element if it is a uniform limit of a sequence of rational functions $f_n \in R(D)$.

The analytic elements on D make up a vector space $H(D)$, which is a uniform completion of $R(D)$. However, note that in general an $f \in R(D)$ can be an unbounded function on D, so that $R(D)$ is not a metric space. Let us start with the important case where it is a metric space (in (4.3) we shall show how to treat the other case).

Proposition When $D \subset \mathbb{C}_p$ is a closed and bounded subset, each $f \in R(D)$ is bounded on D, and $H(D)$ is the closure of $R(D)$ in the Banach algebra $C_b(D)$ for the sup norm. [Rob00]
To be able to speak of analytic elements on the complement of a ball (which is unbounded) we now approach the case of **unbounded domains** D, and hence $R(D)$ is not a metric space. Let us introduce the vector subspaces

$$R_b(D) := \{f \in R(D) : f \text{ bounded on } D\},$$

consisting of the rational functions $f = g/h$, $\deg g \leqslant \deg h$, having no pole in D,

$$R_0(D) := \{f \in R(D) : f \to 0 \text{ as } |x| \to \infty\} \subset R_b(D)$$

consisting of the rational functions $f = g/h$, $\deg g < \deg h$, having no pole in D.

The Euclidean division algorithm shows more precisely that

$$\begin{aligned} R(D) &= R_0(D) \oplus \mathbb{C}_p[x] \\ &= \underbrace{R_0(D) \oplus \mathbb{C}_p}_{=R_b(D)} \oplus x\mathbb{C}_p[x]. \end{aligned}$$

A fundamental system of neighborhoods of an f_0 in $R(D)$ is given by

$$V_\varepsilon(f_0) = \left\{ f \in R(D) : \sup_{x \in D} |f(x) - f_0(x)| < \varepsilon \right\} \quad (\varepsilon > 0).$$

In particular, if f_0 is bounded, then $V_\varepsilon(f_0) \subset R_b(D)$, namely:

$$V_\varepsilon(f_0) \cap x\mathbb{C}_p[x] = \{0\}.$$

This proves that the topology induced by uniform convergence on $x\mathbb{C}_p[x]$ is the discrete one:

$$R(D) = \underbrace{R_b(D)}_{\text{normed space}} \oplus \underbrace{x\mathbb{C}_p[x]}_{\text{uniformly discrete}} \quad .$$

By completion we get:

$$H(D) = \underbrace{H_b(D)}_{\text{Banach space}} \oplus \underbrace{x\mathbb{C}_p[x]}_{\text{uniformly discrete}} \quad .$$

We can also write

$$H(D) = H_0(D) \oplus \mathbb{C}_p \oplus x\mathbb{C}_p[x]$$

and group the last two factors

$$H(D) = H_0(D) \oplus \mathbb{C}_p[x],$$

but the uniform structure on the last factor is not the discrete one.

When D is unbounded, we shall only use bounded analytic elements and thus work in the Banach algebra $H_b(D) = H_0(D) \oplus \mathbb{C}_p$.

We note that $H_0(D)$ is a (maximal) ideal in this algebra with quotient

$$H_b(D)/H_0(D) \cong \mathbb{C}_p \quad \text{(a field)}.$$

5.2 Lescaminate

Let P be a monic, non-constant polynomial of degree q, and let $M > 0$. Then the **lemniscate** defined by P and M is the set:

$$B = B(P, M) = \{x \in K \mid |P(x)| \leqslant M\}.$$

It is clear that B is closed and bounded.
Let P be a monic polynomial of degree $q > 1$, and let us define the following sets:

$$B'(P, M) = \{x \in \mathbb{P}_1(K) \mid |P(x)| > M\},$$

$$C(P, M) = B(P, M) \cap B'(P, M).$$

We finish this paragraph with a remark that will be useful in Chapter 7. Let $f = Q + g$, Q be a polynomial and $g \in H_0(B')$. We define $a_1(f)$ as the residue of f at infinity, that is:

$$\lim_{x \to \infty} xg(x),$$

where $D(B)$ designates the diameter of B, so that:

$$|a_1(f)| \leqslant \|f\|_B D(B)$$

Suppose $0 \in B$ (which we can assume, as $a_1(f)$ is clearly translation invariant), then from

$$|a_1(f)| \leqslant \|fx\|_C \leqslant \|f\|_C / \mathrm{diam}(B).$$

Estimate on residue[Ami75] Let $f \in H_0(B')$. Then there exists a constant $M(f)$ such that, for any polynomial Q:

$$|a_1(fQ)| \leqslant M(f)\|Q\|_C.$$

5.3 Lemniscates in the Complex Plane

Let $P \in \mathbb{C}[X]$ be a monic polynomial of degree $q \geqslant 1$, and let $M > 0$. We define:

$$B(P,M) = \{z \in \mathbb{C} \mid |P(z)| \leqslant M\},$$
$$B^0(P,M) = \{z \in \mathbb{C} \mid |P(z)| < M\},$$
$$B'(P,M) = \{z \in \mathbb{C} \mid |P(z)| \geqslant M\},$$

and

$$C(P,M) = B(P,M) \cap B'(P,M).$$

When no confusion arises, we will denote these sets by B, B^0, B', C.

Corollary [Ami75] — Let f be an analytic function on B' vanishing at infinity. Then there exists a constant $M(f)$ such that, for every polynomial Q,

$$|a_1(Qf)| \leqslant M(f)\,\|Q\|_C.$$

5.4 Transfinite Diameter

Let E be a metric space, $B \subseteq E$, and for $n \geqslant 2$, we define:

$$D_n(B) = \sup\left\{\prod_{i\neq j} d(x_i,x_j) \;\middle|\; x=(x_1,\dots,x_n)\in B^n\right\}$$

and

$$d_n(B) = (D_n(B))^{1/n(n-1)}.$$

Then, $\lim_{n\to\infty} d_n(B)$ exists. We denote this limit as $d(B)$, and we call it the **transfinite diameter** of B.
Note that if B is not bounded, then $D_n(B) = +\infty$, and we agree that in such cases $d(B) = \infty$, but from now on we will only be concerned with bounded subsets of E.
If B is bounded, let $D(B)$ denote its diameter:

$$D(B) = \sup\left\{d(x,y) \mid (x,y) \in B^2\right\},$$

then $D_2(B) = (D(B))^2$, and it is immediate that for $n \geqslant 2$,

$$d_n(B) \leqslant D(B)^{2n} \quad \Rightarrow \quad d(B) \leqslant D(B).$$

We also note that if the distance d is replaced by a proportional distance

$$d'(x,y) = r \cdot d(x,y), \quad r > 0,$$

then all quantities scale accordingly. Let $d'_n(B)$ be the quantity corresponding to a scaled distance $d'(x,y) = rd(x,y)$, then $d'_n(B) = rd_n(B)$. Hence, we may assume without loss of generality that $D(B) \leqslant 1$.
Define

$$g_n(x_1,\dots,x_n) = \prod_{i\neq j} d(x_i,x_j) = g_n(x), \quad x=(x_1,\dots,x_n)\in B^n,$$

then

$$g_{n+1}(x_1,\dots,x_{n+1})^n = h_1\cdots h_{n+1},$$

where

$$h_j = g_n(x^j), \quad x^j = (x_1,\dots,\hat{x_j},\dots,x_{n+1}) \in B^n.$$

Therefore,

$$(D_{n+1}(B))^n \leqslant D_n(B)^{n+1}, \quad \Rightarrow \quad d_{n+1}(B) \leqslant (d_n(B))^{1+1/n} \leqslant d_n(B)(D(B))^{1/n}.$$

If $D(B) < 1$, then the sequence $d_n(B)$ is decreasing and bounded below, hence convergent.
We can verify that if B is a disk in $\mathbb{C}$ or a valued non-archimedean field with infinite residue field, then $d(B)$ is the radius of B.

Some Immediate Properties:

(i) If $A \subseteq B$, then $d(A) \leqslant d(B)$;

(ii) If $A \subseteq B$ and A is dense in B, then $d(A) = d(B)$;

(iii) If B is a finite set, then $d(B) = 0$;

(iv) If B is finite and A is bounded, then $d(A \cup B) = d(A)$.

In the case where the metric space E is a valued field K, the transfinite diameter admits a definition equivalent to the previous, which we shall now use.

Lemma Let B be a bounded subset of the valued field K. Let $\mathcal{P}_n$ be the set of monic polynomials of degree n with coefficients in K, and define:

$$S_n(B) = \inf \left\{ \sup_{x \in B} |P(x)| \;\middle|\; P \in \mathcal{P}_n \right\}, \quad s_n(B) = (S_n(B))^{1/n^2}.$$

Then

$$s_n(B) \to d(B), \quad \text{as } n \to \infty.$$

Moreover, if f is a function defined on B with values in K (or in $\mathbb{R}$), we write $\|f\|_B = \sup\{|f(x)| \mid x \in B\}$. Then

$$S_n(B) = \inf\{\|P\|_B \mid P \in \mathcal{P}_n\}.$$

Choose

$$y = (y_1, \ldots, y_n) \in B^n,$$

and let

$$P_y(x) = (x - y_1)(x - y_2) \cdots (x - y_n),$$

then

$$g_n(x_1, \ldots, x_n) = P_y(x_1) \cdots P_y(x_n) = g_n(y_1, \ldots, y_n).$$

Given $\varepsilon > 0$, we can choose y such that $g_n(y) > D_n(B)(1 - \varepsilon)$. Then for any such choice of y, we have:

$$D_n(B)(1 - \varepsilon) \leqslant \|P_y\|_B^2 \leqslant D_{n+1}(B).$$

For each $\varepsilon > 0$, we can associate $P_y \in \mathcal{P}_n$ satisfying this inequality, hence:

$$S_n(B) \leqslant (D_{n+1}(B)/D_n(B))^{1/2}.$$

Now, as $n \to \infty$, $(D_{n+1}(B)/D_n(B))^{1/n} \to d(B)^2$. Therefore,

$$\limsup s_n(B) \leqslant d(B).$$

Moreover, note that:

$$g_n(x_1, \ldots, x_n) = |V(x_1, \ldots, x_n)|^2,$$

where $V(x_1, \ldots, x_n)$ is the Vandermonde determinant associated to $x_1, \ldots, x_n$, and

$$V = [v_{ij}], \quad v_{ij} = x_j^{i-1}, \quad 1 \leqslant i \leqslant n, \; 1 \leqslant j \leqslant n.$$

Let $P \in \mathcal{P}_{n-1}$. Then $V(x_1, \dots, x_n)$ is also the determinant obtained by replacing, in the last column of V, x_n^{i-1} by $P(x_i)$. Expanding this last column in terms of its entries, we get:

$$V(x_1, \dots, x_n) = \sum V_i P(x_i),$$

where V_i is the Vandermonde determinant of $(x_1, \dots, \hat{x}_i, \dots, x_n)$.
Choose $s = (x_1, \dots, x_n)$ such that

$$g_n(s) \geqslant D_n(B)(1-\varepsilon),$$

and set

$$D_n(B)(1-\varepsilon) \leqslant \|P\|_B |V(x_1, \dots, x_n)|, \quad \forall P \in \mathcal{P}_{n-1}.$$

Hence, we conclude (taking supremum and infimum):

$$S_{n-1}(B) \geqslant \frac{D_n(B)}{D_{n-1}(B)},$$

and thus:

$$\liminf s_n(B) \geqslant d(B),$$

which completes the proof.
Corollary — Let B be a bounded subset of K, $d(B)$ its transfinite diameter, $\varepsilon > 0$, and $r > 1$; there exists an integer n and a polynomial $P \in \mathcal{P}_n$ such that:

$$B \subseteq \{x \in K \mid |P(x)| \leqslant (d(B)+\varepsilon)^n \cdot r\}.$$

Indeed, for sufficiently large n, $s_n(B) \leqslant d(B)+\varepsilon$, and $S_n(B) \leqslant (d(B)+\varepsilon)^n$; by choosing such an n, there exists $P \in \mathcal{P}_n$ such that $\|P\|_B \leqslant r S_n(B)$.

Example — Suppose K is non-archimedean and algebraically closed. The lemniscate $B = B(P, M)$ is defined by a monic polynomial P of degree $q \geqslant 1$ and a constant M, with transfinite diameter $d(B) = M^{1/q}$. Indeed, $\|P^k\|_B = M^k \Rightarrow S_n(B) \geqslant M^k$, thus $d(B) \leqslant M^{1/q}$.
On the other hand, if Q is a monic polynomial of degree kq, write:

$$Q = Q_1 P + \dots + Q_k P^k,$$

where each $\deg Q_i < q$, then:

$$\|Q\|_B \leqslant \max\left(\|Q_i\|_B \cdot \|P^i\|_B\right) \leqslant \max\left(\|Q_i\|_B\right) \cdot M^k = M^k,$$

so $S_n(B) = M^k$ and $d(B) = M^{1/q}$.

5.5 The Polya-Bertrandias theorem

Theorem 5.1 (Polya-Bertrandias). *Let $f(X) = \sum_{n \geqslant 1} \frac{a_n}{X^n}$ be a Laurent series with $a_k \in \mathbb{Q}$. We suppose there exists a finite set P of prime numbers such that:*

- *For every prime number $p \notin P$ and $n \geqslant 1$, $|a_n|_p \leqslant 1$;*
- *f defines in $\mathbb{C}$ a function extendable to a connected domain B_0, whose supplement is bounded and has a transfinite diameter d_0;*
- *For every prime number $p \in P$, f defines in $\mathbb{C}_p$ a function extendable into an analytic element on a part B_p of $\mathbb{C}_p$, whose supplement is bounded and has a transfinite diameter d_p;*
- *The product $d = d_0 \times \prod_{p \in P} d_p$ satisfies $d < 1$;*

then f is a rational function.

Remark: The Borel–Dwork theorem is a corollary of this one, for if

$$f(X) = \sum_{n \geqslant 0} a_n X^n$$

satisfies the hypotheses of the Borel–Dwork theorem, it is easy to verify that

$$g(X) = f(1/X) - a_0$$

satisfies hypotheses 4.1

5.6 Lemma

Let $\mathscr{K}$ be a field complete with respect to an absolute value and algebraically closed (for example, $\mathscr{K} = \mathbb{C}$ or $\mathscr{K} = \mathbb{C}_p$) and let

$$f(X) = \sum_{n \geqslant 0} a_n X^n \in \mathscr{K}[[X]].$$

Let $P \in \mathscr{K}[X]$, $\deg(P) > 1$, and let $B' = \{x \in \mathscr{K} \mid |P(x)| \geqslant d^{\deg(P)}\}$.
If f extends to a function in $\mathscr{H}_0(B')$, then

$$\limsup_{k \to \infty} |D_1^k(f)|^{2/k^2} \leqslant d.$$

Let $\Gamma = \{x \in \mathscr{K} \mid |P(x)| = d^{\deg(P)}\}$. It is known that there exists a constant $M(f)$ such that, for any polynomial Q,

$$|a_\ell(fQ)| \leqslant M(f) \|Q\|_\Gamma.$$

Let $P_1, \ldots, P_k$ be monic polynomials, $P_k \in \mathscr{P}_{k-1}$. By definition, $D_1^k = [a_{ij}]$ where $a_{ij} = a_{i+j-1}$ for $i = 1, \ldots, k$, $j = 1, \ldots, k$. By linear combination of the columns of D_1^k, we see that if

$$P_j(X) = X^{r-1} + p_{j1} X^{r-2} + \cdots + p_{j,r-1},$$

and

$$P_j f = \sum_{k \geqslant 0} b_{jk} X^k,$$

then we also have $D_1^k = [b_{ij}]$ for $i = 1, \ldots, k$, $j = 1, \ldots, k$. Performing an analogous combination on the rows of D_1^k, we find that $D_1^k(P_1 f, \ldots, P_k f) = D_1^k(f)$. Let

$$\|P_j\|_\Gamma = \sum |p_{j\ell}|,$$

then there exists a constant $M(f)$ such that

$$|a_\ell(P_j f)| \leqslant M(f) \|P_j\|_\Gamma.$$

Let $S_k = \max(\|P_1\|_\Gamma, \ldots, \|P_k\|_\Gamma)$. If $\mathscr{K}$ is non-Archimedean, set $S_k = (|p_{ij}| + \cdots + 1) = \mathbb{C} = \mathbb{C}$. Applying Hadamard's inequality, we obtain

$$|D_1^k(f)| \leqslant M(f)^k p_1 \cdots p_k S_k^k.$$

Choose $P_1, \ldots, P_k$ such that $p_k \leqslant (d + \varepsilon)^k$ for k sufficiently large
Assume first $d < 1$, and let L be a constant (not necessarily the same across all inequalities). Then, by choosing ε small enough so that $d + \varepsilon < 1$, we have:

$$S_k \leqslant kL, \quad p_1 \cdots p_k \leqslant L(d + \varepsilon)^{k(k-1)/2},$$

and hence:

$$\frac{2}{k^2} \log |D_1^k(f)| \leqslant \frac{L}{k} + \log(d + \varepsilon) + \frac{\log k}{k} + L.$$

As $k \to \infty$, we deduce that:

$$\lim_{k\to\infty} |D_1^k(f)|^{2/k^2} \leqslant d.$$

If $d < 1$, the lemma is proved. Otherwise, let $\lambda \in \mathbb{K}$, and let:

$$f_\lambda(X) = f(\lambda X).$$

Then f_λ can be extended to an element of $\mathscr{H}_0\left(\frac{1}{\lambda}B'\right)$, where $\frac{1}{\lambda}B'$ is the image of B' under the homothety centered at 0 with ratio $1/\lambda$.
Clearly:

$$D_1^k(f_\lambda) = \lambda^{-k^2} D_1^k(f), \quad \text{and} \quad d\left(\frac{1}{\lambda}B'\right) = \frac{1}{|\lambda|}d.$$

Hence, if the lemma is true for $d < 1$, then it is true for all $d > 0$.

5.7 Proof of Theorem 8.1

For $x \in \mathbb{Q}$, denote

$$\|x\| = |x| \times \prod_{p\in P} |x|_p,$$

the product of all normalized absolute values of x.
Let d be the product of the transfinite diameters appearing in condition (iv). If $p \notin P$, then

$$|D_1^k(f)|_p \leqslant 1.$$

Let:

$$N = 1 + \mathrm{Card}(P).$$

Choose $\varepsilon > 0$ so that $d(1+\varepsilon)^N < 1$.
Then there exist integers k_0 and k_p for $p \in P$ such that for $k \geqslant k_0$ (resp $k \geqslant k_p$), we have:

$$|D_1^k(f)| \leqslant (d(1+\varepsilon))^k, \quad |D_1^k(f)|_p \leqslant (d_p(1+\varepsilon))^k.$$

Let K be the maximum of k_0 and k_p. Then for $k \geqslant K$ we have:

$$\|D_1^k(f)\| < (d(1+\varepsilon)^N)^k < 1.$$

Thus, for such k, we get $D_1^k(f) = 0$, and from Lemma 4.4 , it follows that f is rational.

References

[Ami75] Yvette Amice. *Les nombres p-adiques*. PUF, 1975. ISBN: 9782130335283.

[Cas86] J. W. S. Cassels. *Local Fields*. CUP, 1986. ISBN: 9780521315258.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. Springer, 1999. ISBN: 9783540653998.

[Rob00] Alain M. Robert. *A Course in p-adic Analysis*. Springer, 2000. ISBN: 9781475732542.

[Gou20] Fernando Q. Gouvêa. *p-adic Numbers*. Springer, 2020. ISBN: 9783030472948.