Analytic functions on p-adic fields

Laureando: Carlo Buccisano
Relatore: Prof. Maurizio Cailotto

Corso di laurea triennale
Dipartimento di Matematica "Tullio Levi-Civita"
Università degli Studi di Padova

5 luglio 2019
Anno Accademico 2018/2019

Plan of the presentation

Plan of the presentation

Plan of the presentation

1. Basic Concepts
2. Construction of $\mathbb{Q}_p$: analytic approach
3. Construction of $\mathbb{Q}_p$: algebraic approach
4. Finite field extensions of $\mathbb{Q}_p$
5. Construction of $\mathbb{C}_p$
6. p-adic power series
7. Newton polygon

Plan of the presentation

1. Basic Concepts
2. Construction of $\mathbb{Q}_p$: analytic approach
3. Construction of $\mathbb{Q}_p$: algebraic approach
4. Finite field extensions of $\mathbb{Q}_p$
5. Construction of $\mathbb{C}_p$
6. p-adic power series
7. Newton polygon

Plan of the presentation

Plan of the presentation

Plan of the presentation

Field norms

Definition

Let F be a field, a function $\| \ \| \colon F \to \mathbb{R}_{\geq 0}$ is a field norm if:

1. $\|x\| = 0 \iff x = 0$;
2. $\|x \cdot y\| = \|x\| \cdot \|y\|$;
3. $\|x + y\| \leq \|x\| + \|y\|$.

Definition

Let F be a field and $\| \ \|_1, \| \ \|_2$ two field norms. They are said to be equivalent if they have the same Cauchy sequences.

Example

The classic absolute value $| \ |_\infty$ is a field norm on $\mathbb{Q}$.

Field norms

Definition

Let F be a field, a function $\| \, \| \colon F \to \mathbb{R}_{\geq 0}$ is a field norm if:

1. $\|x\| = 0 \iff x = 0$;
2. $\|x \cdot y\| = \|x\| \cdot \|y\|$;
3. $\|x + y\| \leq \|x\| + \|y\|$.

Definition

Let F be a field and $\| \, \|_1, \| \, \|_2$ two field norms. They are said to be equivalent if they have the same Cauchy sequences.

Example

The classic absolute value $| \, |_\infty$ is a field norm on $\mathbb{Q}$.

Field norms

Definition

Let F be a field, a function $\| \ \| \colon F \to \mathbb{R}_{\geq 0}$ is a field norm if:

1. $\|x\| = 0 \iff x = 0$;
2. $\|x \cdot y\| = \|x\| \cdot \|y\|$;
3. $\|x + y\| \leq \|x\| + \|y\|$.

Definition

Let F be a field and $\| \ \|_1, \| \ \|_2$ two field norms. They are said to be equivalent if they have the same Cauchy sequences.

Example

The classic absolute value $| \ |_\infty$ is a field norm on $\mathbb{Q}$.

Non-Archimedean field norms

Definition

Let F be a field and $\| \ \|: F \to \mathbb{R}_{\geq 0}$ a field norm. We say that $\| \ \|$ is a non-Archimedean norm if, for every $x, y \in F$, we have

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

An immediate consequence is the following.

Proposition

With $(F, \| \ \|)$ as before, we have:

$$\|x\| \neq \|y\| \implies \|x + y\| = \max\{\|x\|, \|y\|\}.$$

It can be proved that every triangle in such a space is isosceles.

Definition

Let F be a field and $\| \ \| \colon F \to \mathbb{R}_{\geq 0}$ a field norm. We say that $\| \ \|$ is a non-Archimedean norm if, for every $x, y \in F$, we have

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

An immediate consequence is the following.

Proposition

With $(F, \| \ \|)$ as before, we have:

$$\|x\| \neq \|y\| \implies \|x + y\| = \max\{\|x\|, \|y\|\}.$$

It can be proved that every triangle in such a space is isosceles.

Let p be a fixed prime number.

Definition

Let's define a function $\operatorname{ord}_p : \mathbb{Z} \to \mathbb{N} \cup \{+\infty\}$ as follows:

$$\operatorname{ord}_p a := \begin{cases} +\infty, & \text{if } a = 0; \\ n, & \text{such that } p^n \mid a \text{ and } p^{n+1} \nmid a. \end{cases}.$$

We can extend it to $\mathbb{Q}$ setting $\operatorname{ord}_p \left(\frac{a}{b}\right) := \operatorname{ord}_p a - \operatorname{ord}_p b$.

Proposition

The function $\operatorname{ord}_p : \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$ is a discrete valuation.

Let p be a fixed prime number.

Definition

Let's define a function $\mathrm{ord}_p : \mathbb{Z} \to \mathbb{N} \cup \{+\infty\}$ as follows:

$$\mathrm{ord}_p\, a := \begin{cases} +\infty, & \text{if } a = 0; \\ n, & \text{such that } p^n \mid a \text{ and } p^{n+1} \nmid a. \end{cases}.$$

We can extend it to $\mathbb{Q}$ setting $\mathrm{ord}_p \left(\frac{a}{b}\right) := \mathrm{ord}_p\, a - \mathrm{ord}_p\, b$.

Proposition

The function $\mathrm{ord}_p \colon \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$ *is a discrete valuation.*

p-adic absolute value

Finally we can define the p-adic absolute value.

Definition

The function $|\ |_p \colon \mathbb{Q} \to \mathbb{Q}$ defined by

$$|x|_p := \begin{cases} p^{-\mathrm{ord}_p x}, & \text{if } x \neq 0; \\ 0, & \text{otherwise}; \end{cases}$$

is the p-adic absolute value on $\mathbb{Q}$.

Proposition

The p-adic absolute value is a non-Archimedean field norm on $\mathbb{Q}$.

Finally we can define the p-adic absolute value.

Definition

The function $|\ |_p \colon \mathbb{Q} \to \mathbb{Q}$ defined by

$$|x|_p := \begin{cases} p^{-\mathrm{ord}_p x}, & \text{if } x \neq 0; \\ 0, & \text{otherwise}; \end{cases}$$

is the p-adic absolute value on $\mathbb{Q}$.

Proposition

The p-adic absolute value is a non-Archimedean field norm on $\mathbb{Q}$.

Ostrowski theorem

Definition

The function $|\ |_0 \colon \mathbb{Q} \to \mathbb{R}_{\geq 0}$ defined by

$$|x|_0 := \begin{cases} 1, & \text{if } x \neq 0; \\ 0, & \text{otherwise.} \end{cases}$$

is the trivial norm.

Theorem (Ostrowski)

Every non-trivial norm on $\mathbb{Q}$ is equivalent to $|\ |_p$ where $p = \infty$ or is some prime number.

Definition

The function $|\ |_0 \colon \mathbb{Q} \to \mathbb{R}_{\geq 0}$ defined by

$$|x|_0 := \begin{cases} 1, & \text{if } x \neq 0; \\ 0, & \text{otherwise.} \end{cases}$$

is the trivial norm.

Theorem (Ostrowski)

Every non-trivial norm on $\mathbb{Q}$ is equivalent to $|\ |_p$ where $p = \infty$ or is some prime number.

It can be proved (using Hensel's lemma) that:

Proposition

The space $(\mathbb{Q}, |\ |_p)$ is not complete.

Definition

The completion of $(\mathbb{Q}, |\ |_p)$ is the space $(\mathbb{Q}_p, |\ |_p)$, obtained considering $\mathcal{S}$, the set of all the Cauchy sequences, and identifying $(a_n)_n$ and $(b_n)_n$ if $\lim_{n\to+\infty}|a_n - b_n|_p = 0$.

It can be proved that, with component-wise sum and product, $\mathbb{Q}_p$ is actually a field containing $\mathbb{Q}$.

Definition of $\mathbb{Q}_p$

It can be proved (using Hensel's lemma) that:

Proposition

The space $(\mathbb{Q}, |\ |_p)$ is not complete.

Definition

The completion of $(\mathbb{Q}, |\ |_p)$ is the space $(\mathbb{Q}_p, |\ |_p)$, obtained considering $\mathcal{S}$, the set of all the Cauchy sequences, and identifying $(a_n)_n$ and $(b_n)_n$ if $\lim_{n\to+\infty} |a_n - b_n|_p = 0$.

It can be proved that, with component-wise sum and product, $\mathbb{Q}_p$ is actually a field containing $\mathbb{Q}$.

Structure of $\mathbb{Q}_p$

Proposition

The p-adic absolute value can be extended to $\mathbb{Q}_p$ setting

$$|a|_p := \lim_{n\to+\infty} |a_n|_p,$$

where $(a_n)_{n\in\mathbb{N}}$ is any representative of a.

Theorem

For every $a \in \mathbb{Q}_p$ there exists a unique representation as

$$a = \sum_{i=m}^{+\infty} a_i p^i, \qquad m \in \mathbb{Z}, a_i \in \{0, \dots, p-1\}.$$

Proposition

The p-adic absolute value can be extended to $\mathbb{Q}_p$ setting

$$|a|_p := \lim_{n \to +\infty} |a_n|_p,$$

where $(a_n)_{n \in \mathbb{N}}$ is any representative of a.

Theorem

For every $a \in \mathbb{Q}_p$ there exists a unique representation as

$$a = \sum_{i=m}^{+\infty} a_i p^i, \qquad m \in \mathbb{Z}, a_i \in \{0, \ldots, p-1\}.$$

Representation of $\mathbb{Q}$ in $\mathbb{Q}_p$

Clearly, if $a \in \mathbb{Q}_p^\times$, we have $|a|_p = p^{-\mathrm{ord}_p a}$, where $\mathrm{ord}_p a$ is the index of the first non-zero coefficient in a.

Proposition

Given $a = \sum_{i=m}^{+\infty} a_i p^i \in \mathbb{Q}_p$ *we have*

$$a \in \mathbb{Q} \iff \exists r, N \in \mathbb{N} : a_i = a_{i+r} \, \forall i > N$$

It's then easy to note that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.

Example

The p-adic number $\alpha := \sum_{i=0}^{+\infty} p^{2^i}$ hasn't a periodic expansion so $\alpha \in \mathbb{Q}_p \setminus \mathbb{Q}$.

Representation of $\mathbb{Q}$ in $\mathbb{Q}_p$

Clearly, if $a \in \mathbb{Q}_p^\times$, we have $|a|_p = p^{-\mathrm{ord}_p a}$, where $\mathrm{ord}_p a$ is the index of the first non-zero coefficient in a.

Proposition

Given $a = \sum_{i=m}^{+\infty} a_i p^i \in \mathbb{Q}_p$ we have

$$a \in \mathbb{Q} \iff \exists r, N \in \mathbb{N} : a_i = a_{i+r} \, \forall i > N$$

It's then easy to note that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.

Example

The p-adic number $\alpha := \sum_{i=0}^{+\infty} p^{2^i}$ hasn't a periodic expansion so $\alpha \in \mathbb{Q}_p \setminus \mathbb{Q}$.

Definition of $\mathbb{Z}_p$

We can obtain $\mathbb{Q}_p$ using a more algebraic construction, which will highlight some other important properties.

Definition

A p-adic integer is a formal series $\sum_{i=0}^{+\infty} a_i p^i$, with integer coefficients $0 \leq a_i \leq p-1$. The set containing all the p-adic integers is called $\mathbb{Z}_p$.

Proposition

The set $\mathbb{Z}_p$ equipped with a component-wise sum and a Cauchy product (both with carry) is a characteristic 0 integral domain.

Definition of $\mathbb{Z}_p$

We can obtain $\mathbb{Q}_p$ using a more algebraic construction, which will highlight some other important properties.

Definition

A p-adic integer is a formal series $\sum_{i=0}^{+\infty} a_i p^i$, with integer coefficients $0 \leq a_i \leq p-1$. The set containing all the p-adic integers is called $\mathbb{Z}_p$.

Proposition

The set $\mathbb{Z}_p$ equipped with a component-wise sum and a Cauchy product (both with carry) is a characteristic 0 *integral domain.*

Properties of $\mathbb{Z}_p$

It's immediate that the invertible elements of $\mathbb{Z}_p$ are exactly the ones with a non-zero constant term.

Proposition

$\mathbb{Z}_p$ is a topological ring (sum and multiplication are continuous) and a principal ideal domain, whose ideals are $\{0\}$ and $p^k\mathbb{Z}_p$, with $k \in \mathbb{N}$.

Proposition

$\mathbb{Z}_p$ is a compact space and is exactly the completion of $(\mathbb{Z}, | \ |_p)$.

Properties of $\mathbb{Z}_p$

It's immediate that the invertible elements of $\mathbb{Z}_p$ are exactly the ones with a non-zero constant term.

Proposition

$\mathbb{Z}_p$ is a topological ring (sum and multiplication are continuous) and a principal ideal domain, whose ideals are $\{0\}$ and $p^k\mathbb{Z}_p$, with $k \in \mathbb{N}$.

Proposition

$\mathbb{Z}_p$ is a compact space and is exactly the completion of $(\mathbb{Z}, |\ |_p)$.

Projective limits

Definition

A sequence $(E_n, \varphi_n)_{n\in\mathbb{N}}$ of sets and maps $\varphi_n \colon E_{n+1} \to E_n$ is called a projective system. A set E equipped with maps $\psi_n \colon E \to E_n$ such that $\psi_n = \varphi_n \circ \psi_{n+1}$, is called a projective limit of the system if every compatible set of maps can be factorized through it. It can be proved that E is unique, up to bijections, and it's often called $\varprojlim E_n$.

Theorem

Let's consider the projective system $(\mathbb{Z}/p^n\mathbb{Z}, \pi_n)$ where $\pi_n \colon \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ is the classical projection and let $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ be its projective limit. Then $\mathbb{Z}_p$ and $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ are two isomorphic topological rings.

Definition

A sequence $(E_n, \varphi_n)_{n\in\mathbb{N}}$ of sets and maps $\varphi_n \colon E_{n+1} \to E_n$ is called a projective system. A set E equipped with maps $\psi_n \colon E \to E_n$ such that $\psi_n = \varphi_n \circ \psi_{n+1}$, is called a projective limit of the system if every compatible set of maps can be factorized through it. It can be proved that E is unique, up to bijections, and it's often called $\varprojlim E_n$.

Theorem

Let's consider the projective system $(\mathbb{Z}/p^n\mathbb{Z}, \pi_n)$ where $\pi_n \colon \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ is the classical projection and let $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ be its projective limit. Then $\mathbb{Z}_p$ and $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ are two isomorphic topological rings.

The universal factorization property is the following: for every compatible sequence of maps $(f_n)_n$, i.e. $f_n \colon X \to E_n$ and $f_n = \varphi_n \circ f_{n+1}$, there exists $f \colon X \to \varprojlim E_n$ such that $f_n = \psi_n \circ f$.

$$
\begin{tikzcd}
& & & & \varprojlim E_n \arrow[dlll, "\psi_n"'] \arrow[dll, "\psi_{n+1}"] \\
\cdots & E_n \arrow[l] & E_{n+1} \arrow[l, "\varphi_n"'] & \cdots \arrow[l] & \\
& & & & X \arrow[ulll, "f_n"] \arrow[ull, "f_{n+1}"'] \arrow[uu, dashed, "f"]
\end{tikzcd}
$$

Another definition of $\mathbb{Q}_p$

Proposition

The field $\mathbb{Q}_p$ is exactly the field of fractions of $\mathbb{Z}_p$.

Let's observe that, with this construction, the structure of $\mathbb{Q}_p$ is immediate.

Example (Geometric series)

Let's consider $\sum_{i=0}^{+\infty} p^i \in \mathbb{Z}_p$. This series doesn't converge in $(\mathbb{Q}, |\ |_\infty)$ but, in $(\mathbb{Q}, |\ |_p)$, we have $\lim_{i\to+\infty} p^i = 0$ so it converges and we have

$$\sum_{i=0}^{+\infty} p^i = \frac{1}{1-p} \implies \left(\sum_{i=0}^{+\infty} p^i\right)^{-1} = 1 - p.$$

Another definition of $\mathbb{Q}_p$

Proposition

The field $\mathbb{Q}_p$ is exactly the field of fractions of $\mathbb{Z}_p$.

Let's observe that, with this construction, the structure of $\mathbb{Q}_p$ is immediate.

Example (Geometric series)

Let's consider $\sum_{i=0}^{+\infty} p^i \in \mathbb{Z}_p$. This series doesn't converge in $(\mathbb{Q}, |\ |_\infty)$ but, in $(\mathbb{Q}, |\ |_p)$, we have $\lim_{i\to+\infty} p^i = 0$ so it converges and we have

$$\sum_{i=0}^{+\infty} p^i = \frac{1}{1-p} \implies \left(\sum_{i=0}^{+\infty} p^i\right)^{-1} = 1 - p.$$

Theorem (Hensel's lemma)

Let $P(X) \in \mathbb{Z}_p[X]$ and $x \in \mathbb{Z}_p$ such that $P(x) \equiv 0 \mod p^n$. If $k := \operatorname{ord}_p(P'(x)) < n/2$ then there exists a unique $\xi \in \mathbb{Z}_p$ such that $\xi \equiv x \mod p^{n-k}$ and $P(\xi) = 0$.

Using this powerful tool we can prove the aforementioned non-completeness of $(\mathbb{Q}, |\ |_p)$.

Example

We just need to find a suitable polynomial with no roots in $\mathbb{Q}$ but a root in $\mathbb{Z}/p\mathbb{Z}$.

- For $p = 2$: $P(X) = X^3 - 7$.
- For $p = 3$: $P(X) = X^2 - 7$.
- For $p \equiv 1 \mod 4$: $P(X) = X^2 - (p+1)$.
- For $p \equiv 3 \mod 4$: $P(X) = X^2 - t$, where $4t \equiv 1 \mod p$.

Hensel's lemma

Theorem (Hensel's lemma)

Let $P(X) \in \mathbb{Z}_p[X]$ *and* $x \in \mathbb{Z}_p$ *such that* $P(x) \equiv 0 \mod p^n$*. If* $k := \mathrm{ord}_p(P'(x)) < n/2$ *then there exists a unique* $\xi \in \mathbb{Z}_p$ *such that* $\xi \equiv x \mod p^{n-k}$ *and* $P(\xi) = 0$*.*

Using this powerful tool we can prove the aforementioned non-completeness of $(\mathbb{Q}, |\ |_p)$.

Example

We just need to find a suitable polynomial with no roots in $\mathbb{Q}$ but a root in $\mathbb{Z}/p\mathbb{Z}$.

- For $p = 2$: $P(X) = X^3 - 7$.
- For $p = 3$: $P(X) = X^2 - 7$.
- For $p \equiv 1 \mod 4$: $P(X) = X^2 - (p+1)$.
- For $p \equiv 3 \mod 4$: $P(X) = X^2 - t$, where $4t \equiv 1 \mod p$.

Extension of the p-adic absolute value

Proposition

Let V be a finite dimensional $\mathbb{Q}_p$-vector space. Then all norms on V are equivalent.

It's then easy to prove that if $K/\mathbb{Q}_p$ is a finite degree field extension then there can be at most one field norm on K extending the p-adic one.

Theorem

Let $K/\mathbb{Q}_p$ be a field extension of degree $d < +\infty$. Then there is a unique extension of the p-adic absolute value to K and is obtained setting

$$|x|_p := |\det \ell_x|_p^{1/d},$$

where $\ell_x : K \to K$ is the linear map $y \to xy$.

Proposition

Let V be a finite dimensional $\mathbb{Q}_p$-vector space. Then all norms on V are equivalent.

It's then easy to prove that if $K/\mathbb{Q}_p$ is a finite degree field extension then there can be at most one field norm on K extending the p-adic one.

Theorem

Let $K/\mathbb{Q}_p$ be a field extension of degree $d < +\infty$. Then there is a unique extension of the p-adic absolute value to K and is obtained setting

$$|x|_p := |\det \ell_x|_p^{1/d},$$

where $\ell_x \colon K \to K$ is the linear map $y \to xy$.

Residue degree and index of ramification

Proposition

Let $K/\mathbb{Q}_p$ be a finite field extension and let's define

$$A := \left\{x \in K : |x|_p \leq 1\right\}, \quad M := \left\{x \in K : |x|_p < 1\right\}.$$

Then A is the integral closure of $\mathbb{Z}_p$ in K, M is its maximal ideal and $k := A/M$, the residue field, is an extension of $\mathbb{F}_p$ of degree at most $[K : \mathbb{Q}_p]$.

Definition

With the same notations used above, we say that $f := [k : \mathbb{F}_p]$ is the residue degree and $e := (|K^\times|_p : |\mathbb{Q}_p^\times|_p)$ is the ramification index. It can be proved that $[K : \mathbb{Q}_p] = e \cdot f$.

Residue degree and index of ramification

Proposition

Let $K/\mathbb{Q}_p$ be a finite field extension and let's define

$$A := \left\{x \in K : |x|_p \leq 1\right\}, \quad M := \left\{x \in K : |x|_p < 1\right\}.$$

Then A is the integral closure of $\mathbb{Z}_p$ in K, M is its maximal ideal and $k := A/M$, the residue field, is an extension of $\mathbb{F}_p$ of degree at most $[K : \mathbb{Q}_p]$.

Definition

With the same notations used above, we say that $f := [k : \mathbb{F}_p]$ is the residue degree and $e := \left(|K^\times|_p : \left|\mathbb{Q}_p^\times\right|_p\right)$ is the ramification index. It can be proved that $[K : \mathbb{Q}_p] = e \cdot f$.

Structure of a finite extension

Proposition

Let $K/\mathbb{Q}_p$ be a field extension of degree $n = e \cdot f$. Then $K = K_f^{\text{unram}}(\pi)$, where K_f^{unram} is the only totally unramified extension of $\mathbb{Q}_p$ of degree f and π is a root of an Eisenstein polynomial in $K_f^{\text{unram}}[X]$.

Theorem

Let $K/\mathbb{Q}_p$ a finite field extension of degree $n = e \cdot f$ and let $\pi \in K$ such that $\operatorname{ord}_p \pi = 1/e$. Then for every $a \in K$ there is a unique representation as

$$a = \sum_{i=m}^{+\infty} a_i \pi^i,$$

where $m = e \cdot \operatorname{ord}_p \alpha \in \mathbb{Z}$ and $a_i \in K$ is such that $a_i^{p^f} = a_i$.

Structure of a finite extension

Proposition

Let $K/\mathbb{Q}_p$ be a field extension of degree $n = e \cdot f$. Then $K = K_f^{\text{unram}}(\pi)$, where K_f^{unram} is the only totally unramified extension of $\mathbb{Q}_p$ of degree f and π is a root of an Eisenstein polynomial in $K_f^{\text{unram}}[X]$.

Theorem

Let $K/\mathbb{Q}_p$ a finite field extension of degree $n = e \cdot f$ and let $\pi \in K$ such that $\operatorname{ord}_p \pi = 1/e$. Then for every $a \in K$ there is a unique representation as

$$a = \sum_{i=m}^{+\infty} a_i \pi^i,$$

where $m = e \cdot \operatorname{ord}_p \alpha \in \mathbb{Z}$ and $a_i \in K$ is such that $a_i^{p^f} = a_i$.

Definition

Let $f(X) \in \mathbb{Z}_p[X]$ be a monic polynomial of degree n such that

$$f(X) \equiv X^n \mod p, \quad f(0) \not\equiv 0 \mod p^2.$$

Then $f(X)$ is called an Eisenstein polynomial.

Theorem

If $f(X) \in \mathbb{Z}_p[X]$ is an Eisenstein polynomial then it is irreducible in $\mathbb{Z}_p[X]$ (and in $\mathbb{Q}_p[X]$).

The theorem can be easily generalized: if $K/\mathbb{Q}_p$ is a finite extension of degree $n = e \cdot f$ then we can use π in place of p (where $\operatorname{ord}_p \pi = 1/e$), A in place of $\mathbb{Z}_p$ and K in place of $\mathbb{Q}_p$.

Definition

Let $f(X) \in \mathbb{Z}_p[X]$ be a monic polynomial of degree n such that

$$f(X) \equiv X^n \mod p, \quad f(0) \not\equiv 0 \mod p^2.$$

Then $f(X)$ is called an Eisenstein polynomial.

Theorem

If $f(X) \in \mathbb{Z}_p[X]$ is an Eisenstein polynomial then it is irreducible in $\mathbb{Z}_p[X]$ (and in $\mathbb{Q}_p[X]$).

The theorem can be easily generalized: if $K/\mathbb{Q}_p$ is a finite extension of degree $n = e \cdot f$ then we can use π in place of p (where $\mathrm{ord}_p \pi = 1/e$), A in place of $\mathbb{Z}_p$ and K in place of $\mathbb{Q}_p$.

The algebraic closure of $\mathbb{Q}_p$

Definition

The algebraic closure of $\mathbb{Q}_p$ is $\mathbb{Q}_p^{\text{alg cl}}$.

Example

Let's consider the polynomial $P_n(X) := X^n - p \in \mathbb{Z}_p[X]$. It's an Eisenstein's polynomial so it is irreducible in $\mathbb{Q}_p[X]$. Then $\mathbb{Q}_p$ is not algebraically closed and $[\mathbb{Q}_p^{\text{alg cl}} : \mathbb{Q}_p] = +\infty$.

It's clear that there is a (unique) extension of the p-adic absolute value to $\mathbb{Q}_p^{\text{alg cl}}$.

The algebraic closure of $\mathbb{Q}_p$

Definition

The algebraic closure of $\mathbb{Q}_p$ is $\mathbb{Q}_p^{\text{alg cl}}$.

Example

Let's consider the polynomial $P_n(X) := X^n - p \in \mathbb{Z}_p[X]$. It's an Eisenstein's polynomial so it is irreducible in $\mathbb{Q}_p[X]$. Then $\mathbb{Q}_p$ is not algebraically closed and $[\mathbb{Q}_p^{\text{alg cl}} : \mathbb{Q}_p] = +\infty$.

It's clear that there is a (unique) extension of the p-adic absolute value to $\mathbb{Q}_p^{\text{alg cl}}$.

Definition of $\mathbb{C}_p$

Theorem

$(\mathbb{Q}_p^{\text{alg cl}}, |\ |_p)$ *is not complete.*

We can then complete it in a standard way (considering all the Cauchy sequences and identifying the ones whose difference tends to zero).

Definition

The completion of $\mathbb{Q}_p^{\text{alg cl}}$ is called $\mathbb{C}_p$.

Properties of $\mathbb{C}_p$

Proposition

$\mathbb{C}_p$ is a field and there is a unique extension of the p-adic absolute value, obtained by setting

$$|x|_p = \lim_{n \to +\infty} |x_n|_p,$$

where $(x_n)_n$ is a Cauchy sequence in $\mathbb{Q}_p^{\text{alg cl}}$ and a representative of $x \in \mathbb{C}_p$.

Theorem

$\mathbb{C}_p$ is a complete and algebraically closed field.

Properties of $\mathbb{C}_p$

Proposition

$\mathbb{C}_p$ is a field and there is a unique extension of the p-adic absolute value, obtained by setting

$$|x|_p = \lim_{n \to +\infty} |x_n|_p,$$

where $(x_n)_n$ is a Cauchy sequence in $\mathbb{Q}_p^{\text{alg cl}}$ and a representative of $x \in \mathbb{C}_p$.

Theorem

$\mathbb{C}_p$ is a complete and algebraically closed field.

Structure of $\mathbb{C}_p$

Definition

Let $r = a/b \in \mathbb{Q}$ with $a \in \mathbb{Z}, b \in \mathbb{N}^\times$ and $P(X) = X^b - p^a \in \mathbb{Q}_p[X]$. Any root of $P(X)$ in $\mathbb{Q}_p^{\text{alg cl}}$ is called a fractional power and is denoted by p^r.

Theorem

Any non-zero element of $\mathbb{C}_p$ can be written (although not in a unique way) as a product of a fractional power, a root of 1 and an element in $D_1(1) = \left\{x \in \mathbb{C}_p : |x-1|_p < 1\right\}$.

Definition

Let $r = a/b \in \mathbb{Q}$ with $a \in \mathbb{Z}, b \in \mathbb{N}^\times$ and $P(X) = X^b - p^a \in \mathbb{Q}_p[X]$. Any root of $P(X)$ in $\mathbb{Q}_p^{\text{alg cl}}$ is called a fractional power and is denoted by p^r.

Theorem

Any non-zero element of $\mathbb{C}_p$ can be written (although not in a unique way) as a product of a fractional power, a root of 1 and an element in $D_1(1) = \left\{x \in \mathbb{C}_p : |x-1|_p < 1\right\}$.

Other properties of $\mathbb{C}_p$

Proposition

We have the following properties:

- $|\mathbb{C}_p|_p = \left|\mathbb{Q}_p^{\text{alg cl}}\right|_p = p^{\mathbb{Q}} \cup \{0\}$;
- $\text{card}(\mathbb{C}_p) = \text{card}(\mathbb{R})$;
- *there exists a (non-canonical) field isomorphism between* $\mathbb{C}$ *and* $\mathbb{C}_p$.

Other properties of $\mathbb{C}_p$

Proposition

We have the following properties:

- $|\mathbb{C}_p|_p = \left|\mathbb{Q}_p^{\text{alg cl}}\right|_p = p^{\mathbb{Q}} \cup \{0\}$;
- $\text{card}(\mathbb{C}_p) = \text{card}(\mathbb{R})$;
- *there exists a (non-canonical) field isomorphism between $\mathbb{C}$ and $\mathbb{C}_p$.*

Proposition

We have the following properties:

- $|\mathbb{C}_p|_p = \left|\mathbb{Q}_p^{\text{alg cl}}\right|_p = p^{\mathbb{Q}} \cup \{0\}$;
- $\operatorname{card}(\mathbb{C}_p) = \operatorname{card}(\mathbb{R})$;
- *there exists a (non-canonical) field isomorphism between $\mathbb{C}$ and $\mathbb{C}_p$.*

A comparison with the classical case

The following diagram shows the differences between the construction of $\mathbb{C}$ and $\mathbb{C}_p$ (in-fact they are simply the smallest complete and algebraically closed fields containing $\mathbb{Q}$ with respect to $|\ |_\infty$ and $|\ |_p$, respectively).

$$\begin{tikzcd}
 & \mathbb{R} \arrow[r, "\text{alg cl}"] & \mathbb{C} & \\
\mathbb{Q} \arrow[ur, "|\ |_\infty"] \arrow[dr, "|\ |_p"'] & & & \\
 & \mathbb{Q}_p \arrow[r, "\text{alg cl}"] & \mathbb{Q}_p^{\text{alg cl}} \arrow[r, "|\ |_p"] & \mathbb{C}_p
\end{tikzcd}$$

From the previous diagram, it seems that the p-adic case is much more complicated than the classic one. Actually, we could have gotten to $\mathbb{C}$ (and $\mathbb{C}_p$) with the same number of steps:

$$\begin{tikzcd}
 & & \mathbb{C} \\
\mathbb{Q} \arrow[r, "\text{alg cl}"] & \mathbb{Q}^{\text{alg cl}} \arrow[ur, "| \ |_\infty"] \arrow[dr, "| \ |_p"'] & \\
 & & \mathbb{C}_p
\end{tikzcd}$$

but the problem is that $\mathbb{Q}^{\text{alg cl}}$ is a very difficult field to study.

Let's recall some basic properties of ultrametric complete spaces (we state them for $\mathbb{C}_p$ but they can be generalized).

Proposition

- *A sequence* $(x_n)_{n\in\mathbb{N}} \subset \mathbb{C}_p$ *is Cauchy if and only if* $\lim_{n\to+\infty}|x_{n+1} - x_n|_p = 0$.
- *A series* $\sum_{i=0}^{+\infty} c_i$ *converges in* $\mathbb{C}_p$ *if and only if* $\lim_{i\to+\infty} c_i = 0$.
- *If* $\sum_{n=0}^{+\infty} a_n$ *converges then its terms can be re-arranged in any way.*
- *If* $a_1 + a_2 + \cdots + a_n = 0$ *then there exists* $i \neq j$ *such that* $|a_i|_p = |a_j|_p = \max_{1\leq h\leq n}|a_h|_p$.

Let's recall some basic properties of ultrametric complete spaces (we state them for $\mathbb{C}_p$ but they can be generalized).

Proposition

- *A sequence* $(x_n)_{n\in\mathbb{N}} \subset \mathbb{C}_p$ *is Cauchy if and only if* $\lim_{n\to+\infty}|x_{n+1} - x_n|_p = 0$.
- *A series* $\sum_{i=0}^{+\infty} c_i$ *converges in* $\mathbb{C}_p$ *if and only if* $\lim_{i\to+\infty} c_i = 0$.
- *If* $\sum_{n=0}^{+\infty} a_n$ *converges then its terms can be re-arranged in any way.*
- *If* $a_1 + a_2 + \cdots + a_n = 0$ *then there exists* $i \neq j$ *such that* $|a_i|_p = |a_j|_p = \max_{1\leq h\leq n}|a_h|_p$.

Basic properties

Let's recall some basic properties of ultrametric complete spaces (we state them for $\mathbb{C}_p$ but they can be generalized).

Proposition

- *A sequence* $(x_n)_{n\in\mathbb{N}} \subset \mathbb{C}_p$ *is Cauchy if and only if* $\lim_{n\to+\infty} |x_{n+1} - x_n|_p = 0$.
- *A series* $\sum_{i=0}^{+\infty} c_i$ *converges in* $\mathbb{C}_p$ *if and only if* $\lim_{i\to+\infty} c_i = 0$.
- *If* $\sum_{n=0}^{+\infty} a_n$ *converges then its terms can be re-arranged in any way.*
- *If* $a_1 + a_2 + \cdots + a_n = 0$ *then there exists* $i \neq j$ *such that* $|a_i|_p = |a_j|_p = \max_{1\leq h\leq n} |a_h|_p$.

Basic properties

Let's recall some basic properties of ultrametric complete spaces (we state them for $\mathbb{C}_p$ but they can be generalized).

Proposition

- *A sequence* $(x_n)_{n\in\mathbb{N}} \subset \mathbb{C}_p$ *is Cauchy if and only if* $\lim_{n\to+\infty}|x_{n+1} - x_n|_p = 0$.
- *A series* $\sum_{i=0}^{+\infty} c_i$ *converges in* $\mathbb{C}_p$ *if and only if* $\lim_{i\to+\infty} c_i = 0$.
- *If* $\sum_{n=0}^{+\infty} a_n$ *converges then its terms can be re-arranged in any way.*
- *If* $a_1 + a_2 + \cdots + a_n = 0$ *then there exists* $i \neq j$ *such that* $|a_i|_p = |a_j|_p = \max_{1\leq h\leq n}|a_h|_p$.

The main idea used to prove the next propositions on analytic function is this:

Theorem

Let $f(X_1, \dots, X_n) \in \mathbb{C}[\![X_1, \dots, X_n]\!]$ be a power series, absolutely convergent on $[-\varepsilon, \varepsilon]^n \subset \mathbb{R}^n$ for some $\varepsilon > 0$. If for every $x_1, \dots, x_n \in [-\varepsilon, \varepsilon]$ we have $f(x_1, \dots, x_n) = 0$ then f is identically zero.

Analytic functions

Definition

A (partial) function $f : \mathbb{C}_p \to \mathbb{C}_p$ is an analytic function if

$$f(X) := \sum_{n=0}^{+\infty} a_n X^n, \quad a_i \in \mathbb{C}_p.$$

Proposition

Using the same notations, the radius of convergence of f is given by:

$$r = \frac{1}{\limsup |a_n|_p^{1/n}}.$$

Analytic functions

Definition

A (partial) function $f : \mathbb{C}_p \to \mathbb{C}_p$ is an analytic function if

$$f(X) := \sum_{n=0}^{+\infty} a_n X^n, \quad a_i \in \mathbb{C}_p.$$

Proposition

Using the same notations, the radius of convergence of f is given by:

$$r = \frac{1}{\limsup |a_n|_p^{1/n}}.$$

Clearly if $|x|_p < r$ then f converges, if $|x|_p > r$ then f diverges. The behaviour when $|x|_p = r$ depends on f: f can either converge or diverge on the whole border.

Proposition

If $f(X) = \sum_{n=0}^{+\infty} a_n X^n$ converges on some disc D, then f is continuous on D.

Proposition

Every $f(X) \in \mathbb{Z}_p[\![X]\!]$ converges on $D(1^-) := \left\{x \in \mathbb{C}_p : |x|_p < 1\right\}$.

Clearly if $|x|_p < r$ then f converges, if $|x|_p > r$ then f diverges. The behaviour when $|x|_p = r$ depends on f: f can either converge or diverge on the whole border.

Proposition

If $f(X) = \sum_{n=0}^{+\infty} a_n X^n$ converges on some disc D, then f is continuous on D.

Proposition

Every $f(X) \in \mathbb{Z}_p[\![X]\!]$ converges on $D(1^-) := \left\{x \in \mathbb{C}_p : |x|_p < 1\right\}$.

p-adic logarithm

Definition

The function defined by

$$\log_p(X) := \sum_{n=1}^{+\infty} (-1)^{n+1} \frac{(X-1)^n}{n}$$

is called the p-adic logarithm. It can be proved that it converges on $D_1(1^-)$ and diverges elsewhere.

Proposition

We have

$$\log_p(x \cdot y) = \log_p(x) + \log_p(y), \quad \forall x, y \in D_1(1^-).$$

Definition

The function defined by

$$\log_p(X) := \sum_{n=1}^{+\infty} (-1)^{n+1} \frac{(X-1)^n}{n}$$

is called the p-adic logarithm. It can be proved that it converges on $D_1(1^-)$ and diverges elsewhere.

Proposition

We have

$$\log_p(x \cdot y) = \log_p(x) + \log_p(y), \quad \forall x, y \in D_1(1^-).$$

Definition

The function defined by

$$\exp_p(X) := \sum_{n=0}^{+\infty} \frac{X^n}{n!}$$

is called the p-adic exponential. It can be proved that it converges on $D(r_p^-)$ and diverges elsewhere, where $r_p := p^{-1/(p-1)} < 1$.

Proposition

We have

$$\exp_p(x+y) = \exp_p(x) \cdot \exp_p(y), \quad \forall x, y \in D(r_p^-).$$

Definition

The function defined by

$$\exp_p(X) := \sum_{n=0}^{+\infty} \frac{X^n}{n!}$$

is called the *p-adic exponential*. It can be proved that it converges on $D(r_p^-)$ and diverges elsewhere, where $r_p := p^{-1/(p-1)} < 1$.

Proposition

We have

$$\exp_p(x+y) = \exp_p(x) \cdot \exp_p(y), \quad \forall x, y \in D(r_p^-).$$

Theorem

The restrictions $\log_p \colon D_1(r_p^-) \to D(r_p^-)$ *and* $\exp_p \colon D(r_p^-) \to D_1(r_p^-)$ *are two mutually inverse isomorphisms between the multiplicative group* $(D_1(r_p^-), \cdot)$ *and the additive group* $(D(r_p^-), +)$*.*

p-adic binomial expansion

Definition

Fixed $a \in \mathbb{C}_p$, the function defined by

$$B_{a,\,p}(X) := \sum_{n=0}^{+\infty} \binom{a}{n} X^n = 1 + \sum_{n=1}^{+\infty} \frac{a(a-1)\cdots(a-n+1)}{n!} X^n$$

is called the *p-adic binomial expansion*.

Proposition

If $|a|_p > 1$ then the region of convergence of $B_{a,\,p}(X)$ is $D((r_p/|a|_p)^-)$. If $|a|_p \leq 1$ then $B_{a,\,p}(X)$ converges on $D(r_p^-)$. Finally, if $a \in \mathbb{Z}_p$ then $B_{a,\,p}(X) \in \mathbb{Z}_p[\![X]\!]$.

p-adic binomial expansion

Definition

Fixed $a \in \mathbb{C}_p$, the function defined by

$$B_{a,\,p}(X) := \sum_{n=0}^{+\infty} \binom{a}{n} X^n = 1 + \sum_{n=1}^{+\infty} \frac{a(a-1)\cdots(a-n+1)}{n!} X^n$$

is called the p-adic binomial expansion.

Proposition

If $|a|_p > 1$ then the region of convergence of $B_{a,\,p}(X)$ is $D((r_p/|a|_p)^-)$. If $|a|_p \leq 1$ then $B_{a,\,p}(X)$ converges on $D(r_p^-)$. Finally, if $a \in \mathbb{Z}_p$ then $B_{a,\,p}(X) \in \mathbb{Z}_p[\![X]\!]$.

In the classic case, if $|x| < 1$ then $B_a(x)$ is the MacLaurin series of $(1+x)^a$. There is an analogue in p-adic environment.

Theorem

If $a \in \mathbb{Q}^\times$ and $x \in \mathbb{C}_p$ is in the region of convergence of $B_{a,\,p}(X)$, then

$$\left(B_{a,\,p}(x)\right)^{1/a} = 1 + x.$$

In this case we'll sometimes use the shorthand $B_{a,\,p}(X) = (1+X)^a$.

Achtung!

Remark

The same series in $\mathbb{Q}[\![X]\!]$ can converge to different numbers in $\mathbb{C}$ and in $\mathbb{C}_p$.

Let's consider the following example.

Example

$$B_{1/2}\left(\frac{7}{9}\right) = \frac{4}{3}, \quad B_{1/2,7}\left(\frac{7}{9}\right) = -\frac{4}{3}$$

In-fact the only square root of $16/9$ which is congruent to $1 \mod 7$ is $-4/3$.

Achtung!

Remark

The same series in $\mathbb{Q}[\![X]\!]$ can converge to different numbers in $\mathbb{C}$ and in $\mathbb{C}_p$.

Let's consider the following example.

Example

$$B_{1/2}\left(\frac{7}{9}\right) = \frac{4}{3}, \quad B_{1/2,7}\left(\frac{7}{9}\right) = -\frac{4}{3}$$

In-fact the only square root of $16/9$ which is congruent to $1 \mod 7$ is $-4/3$.

Differentiation

Definition

Let $X \subseteq \mathbb{C}_p$ be a set with no isolated points. A function $f : X \to \mathbb{C}_p$ is differentiable at $a \in \mathbb{C}_p$ is

$$\exists \lim_{X \ni x \to a} \frac{f(x) - f(a)}{x - a} := f'(a) \in \mathbb{C}_p.$$

Definition

With the same notations used above, let's define this function:

$$\Phi f(x, y) := \frac{f(x) - f(y)}{x - y}.$$

We say that f is strictly differentiable at $a \in X$ (and we write $f \in S^1(a)$) if

$$\Phi f(x, y) \to f'(a)$$

as $(x, y) \to (a, a)$ and $(x, y) \notin \Delta_{X \times X}$.

Differentiation

Definition

Let $X \subseteq \mathbb{C}_p$ be a set with no isolated points. A function $f : X \to \mathbb{C}_p$ is differentiable at $a \in \mathbb{C}_p$ is

$$\exists \lim_{X \ni x \to a} \frac{f(x) - f(a)}{x - a} := f'(a) \in \mathbb{C}_p.$$

Definition

With the same notations used above, let's define this function:

$$\Phi f(x, y) := \frac{f(x) - f(y)}{x - y}.$$

We say that f is strictly differentiable at $a \in X$ (and we write $f \in S^1(a)$) if

$$\Phi f(x, y) \to f'(a)$$

as $(x, y) \to (a, a)$ and $(x, y) \notin \Delta_{X \times X}$.

Example of differentiation

Theorem

Let $f(X) = \sum_{n=0}^{+\infty} a_n X^n$ be an analytic function convergent on some open disc D. Then f is strictly differentiable on D and

$$f'(X) = \sum_{n=1}^{+\infty} n a_n X^{n-1}.$$

Example

$$\frac{\mathrm{d}}{\mathrm{d}x} \exp_p(x) = \frac{\mathrm{d}}{\mathrm{d}x} \left(\sum_{n=0}^{+\infty} \frac{x^n}{n!} \right) = \sum_{n=1}^{+\infty} \frac{x^{n-1}}{(n-1)!} = \exp_p(x).$$

Example of differentiation

Theorem

Let $f(X) = \sum_{n=0}^{+\infty} a_n X^n$ be an analytic function convergent on some open disc D. Then f is strictly differentiable on D and

$$f'(X) = \sum_{n=1}^{+\infty} n a_n X^{n-1}.$$

Example

$$\frac{\mathrm{d}}{\mathrm{d}x} \exp_p(x) = \frac{\mathrm{d}}{\mathrm{d}x} \left(\sum_{n=0}^{+\infty} \frac{x^n}{n!} \right) = \sum_{n=1}^{+\infty} \frac{x^{n-1}}{(n-1)!} = \exp_p(x).$$

Proposition

There exists a unique function $\mathrm{Log}_p \colon \mathbb{C}_p^\times \to \mathbb{C}_p$ *such that:*

- $\mathrm{Log}_p(x) = \log_p(x)$ *if* $x \in D_1(1^-)$*;*
- $\mathrm{Log}_p(x \cdot y) = \mathrm{Log}_p(x) + \mathrm{Log}_p(y)$ *for any* $x, y \in \mathbb{C}_p^\times$*;*
- $\mathrm{Log}_p(p) = 0$.

This is called the Iwasawa logarithm.

Proposition

$\mathrm{Log}_p(X)$ *is a locally analytic function with derivative* $x \mapsto 1/x$.

Proposition

There exists a unique function $\mathrm{Log}_p\colon \mathbb{C}_p^\times \to \mathbb{C}_p$ *such that:*

- $\mathrm{Log}_p(x) = \log_p(x)$ *if* $x \in D_1(1^-)$*;*
- $\mathrm{Log}_p(x \cdot y) = \mathrm{Log}_p(x) + \mathrm{Log}_p(y)$ *for any* $x, y \in \mathbb{C}_p^\times$*;*
- $\mathrm{Log}_p(p) = 0$.

This is called the Iwasawa logarithm.

Proposition

$\mathrm{Log}_p(X)$ *is a locally analytic function with derivative* $x \mapsto 1/x$.

Definition

The function $\mu\colon \mathbb{N}^\times \to \mathbb{N}$ defined by

$$\mu(n) := \begin{cases} 0, & \text{if } n \text{ is not square-free;} \\ (-1)^k, & \text{if } n \text{ is a product of } k \text{ distinct primes;} \end{cases}$$

is the Möbius function.

Proposition

We have the following identity in $\mathbb{Q}[\![X]\!]$:

$$\exp(X) = \prod_{n=1}^{+\infty} B_{-\mu(n)/n}(-X^n) = \prod_{n=1}^{+\infty} (1 - X^n)^{-\frac{\mu(n)}{n}}.$$

Definition

The function $\mu\colon \mathbb{N}^\times \to \mathbb{N}$ defined by

$$\mu(n) := \begin{cases} 0, & \text{if } n \text{ is not square-free;} \\ (-1)^k, & \text{if } n \text{ is a product of } k \text{ distinct primes;} \end{cases}$$

is the Möbius function.

Proposition

We have the following identity in $\mathbb{Q}[\![X]\!]$:

$$\exp(X) = \prod_{n=1}^{+\infty} B_{-\mu(n)/n}(-X^n) = \prod_{n=1}^{+\infty} (1 - X^n)^{-\frac{\mu(n)}{n}}.$$

Definition

The function defined by

$$\mathrm{E}_p(X) := \prod_{\substack{n=1 \\ p \nmid n}}^{+\infty} B_{-\mu(n)/n,\, p}(-X^n) = \prod_{\substack{n=1 \\ p \nmid n}}^{+\infty} (1 - X^n)^{-\frac{\mu(n)}{n}}$$

is called the Artin-Hasse exponential.

Let's note that we simply removed some terms from the product expression of $\exp_p(X)$. This operation will make $\mathrm{E}_p(X)$ converge on a much bigger disc than $D(r_p^-)$.

Proposition

We have the following identity in $\mathbb{Q}[\![X]\!]$:

$$\mathrm{E}_p(X) = \exp_p\left(\sum_{i=0}^{+\infty} \frac{X^{p^i}}{p^i}\right).$$

Theorem

$\mathrm{E}_p(X) \in \mathbb{Z}_p[\![X]\!]$ *so it converges on* $D(1^-)$.

Proposition

We have the following identity in $\mathbb{Q}[\![X]\!]$:

$$\mathrm{E}_p(X) = \exp_p\left(\sum_{i=0}^{+\infty} \frac{X^{p^i}}{p^i}\right).$$

Theorem

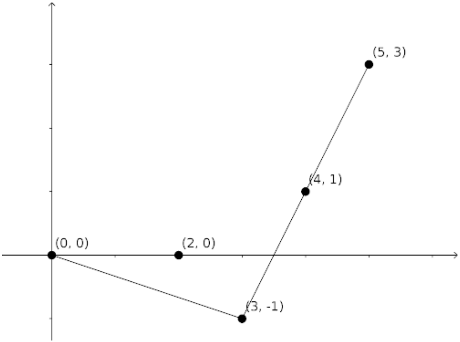
$\mathrm{E}_p(X) \in \mathbb{Z}_p[\![X]\!]$ *so it converges on* $D(1^-)$.

Definition

Let $f(X) = 1 + \sum_{i=1}^{n} a_i X^i \in 1 + X\mathbb{C}_p[X]$ be a polynomial of degree n. Let's define the set

$$\Gamma := \{(0,0)\} \cup \{(i, \operatorname{ord}_p a_i) : a_i \neq 0, i \in \{1, \dots, n\}\} \subset \mathbb{R}^2.$$

The inferior convex hull of Γ in $\mathbb{R}^2$ is the Newton polygon of $f(X)$.



The Newton polygon of

$f(X) = 1 + X^2 + \frac{1}{3}X^3 + 3X^4 + 54X^5$

in $\mathbb{Q}_3[X]$.

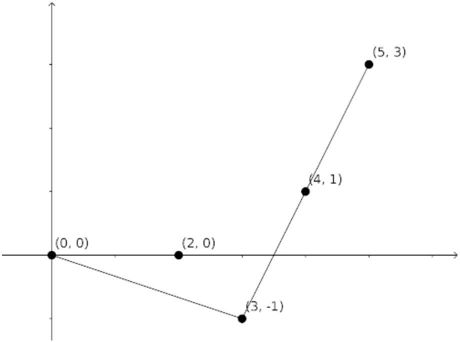
Newton polygon for polynomials

Definition

Let $f(X) = 1 + \sum_{i=1}^{n} a_i X^i \in 1 + X\mathbb{C}_p[X]$ be a polynomial of degree n. Let's define the set

$$\Gamma := \{(0,0)\} \cup \{(i, \operatorname{ord}_p a_i) : a_i \neq 0, i \in \{1, \ldots, n\}\} \subset \mathbb{R}^2.$$

The inferior convex hull of Γ in $\mathbb{R}^2$ is the Newton polygon of $f(X)$.



The Newton polygon of

$f(X) = 1 + X^2 + \frac{1}{3}X^3 + 3X^4 + 54X^5$

in $\mathbb{Q}_3[X]$.

Definition

The vertices of the Newton polygon are the points $(j, \mathrm{ord}_p\, a_j)$ where the slope changes, while the segments are the traits joining every vertex to the next one. The length of a segment is the length of its horizontal projection.

Theorem

Let $f(X) \in 1 + X\mathbb{C}_p[X]$ be a polynomial of degree n and let $\alpha_1, \ldots, \alpha_n$ be all of its roots and $\lambda_i := \mathrm{ord}_p\,(1/\alpha_i)$. If λ is a slope of the Newton polygon of length l then precisely l of the λ_i are equal to λ.

In other words, this theorem says that the slopes of the Newton polygon of $f(X)$ are counting, with multiplicity, the p-adic order of the reciprocal roots of $f(X)$.

Definition

The vertices of the Newton polygon are the points $(j, \mathrm{ord}_p\, a_j)$ where the slope changes, while the segments are the traits joining every vertex to the next one. The length of a segment is the length of its horizontal projection.

Theorem

Let $f(X) \in 1 + X\mathbb{C}_p[X]$ be a polynomial of degree n and let $\alpha_1, \dots, \alpha_n$ be all of its roots and $\lambda_i := \mathrm{ord}_p(1/\alpha_i)$. If λ is a slope of the Newton polygon of length l then precisely l of the λ_i are equal to λ.

In other words, this theorem says that the slopes of the Newton polygon of $f(X)$ are counting, with multiplicity, the p-adic order of the reciprocal roots of $f(X)$.

We can use the same definition of the Newton polygon when $f(X) \in 1 + X\mathbb{C}_p[\![X]\!]$, which we'll sometimes call $\mathfrak{N}(f)$. We can have three different types of polygons.

1. We get infinitely many segments of finite length.
2. At some point the line we're rotating hits simultaneously infinite points. In this case the Newton polygon has only a finite number of segments, the last one being infinitely long.
3. At some point the line we're rotating has not hit any point yet but it cannot rotate any farther without passing above some points. In this case the last segment has slope equal to the least upper bound of all possible slopes for which the line passes on or bellow all the points.

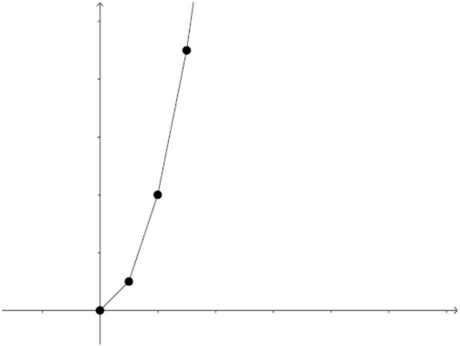
We can use the same definition of the Newton polygon when $f(X) \in 1 + X\mathbb{C}_p[\![X]\!]$, which we'll sometimes call $\mathfrak{N}(f)$. We can have three different types of polygons.

1. We get infinitely many segments of finite length.
2. At some point the line we're rotating hits simultaneously infinite points. In this case the Newton polygon has only a finite number of segments, the last one being infinitely long.
3. At some point the line we're rotating has not hit any point yet but it cannot rotate any farther without passing above some points. In this case the last segment has slope equal to the least upper bound of all possible slopes for which the line passes on or bellow all the points.

We can use the same definition of the Newton polygon when $f(X) \in 1 + X\mathbb{C}_p[\![X]\!]$, which we'll sometimes call $\mathfrak{N}(f)$. We can have three different types of polygons.

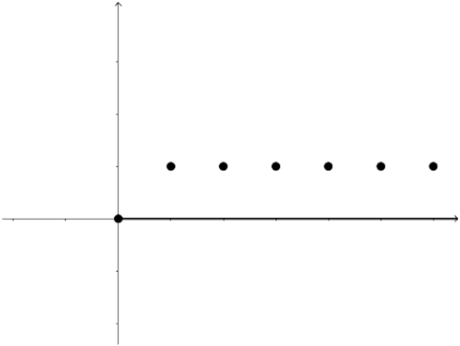
1. We get infinitely many segments of finite length.
2. At some point the line we're rotating hits simultaneously infinite points. In this case the Newton polygon has only a finite number of segments, the last one being infinitely long.
3. At some point the line we're rotating has not hit any point yet but it cannot rotate any farther without passing above some points. In this case the last segment has slope equal to the least upper bound of all possible slopes for which the line passes on or bellow all the points.

Examples



A type (1) Newton polygon, of

$$f(X) = 1 + \sum_{i=1}^{+\infty} p^{i^2} X^i.$$

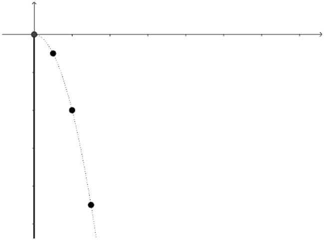


A type (3) Newton polygon, of

$$f(X) = 1 + \sum_{i=1}^{+\infty} p X^i.$$

A degenerate case

There is a degenerate case of type (3): when the line cannot rotate from the beginning. In this case it can be proved that the radius of convergence is always 0. For example, here's the Newton polygon of $f(X) = \sum_{i=0}^{+\infty} \frac{X^i}{p^{i^2}}$.



Radius of convergence

Theorem

Let $f(X) = 1 + \sum_{i=1}^{+\infty} a_i X^i \in 1 + X\mathbb{C}_p[\![X]\!]$ be a power series and let b be the least upper bound of all slopes of $\mathfrak{N}(f)$. Then the radius of convergence of $f(X)$ is $r = p^b$ (if $b = +\infty$ then $f(X)$ converges everywhere).

Proposition

With the same notations used above, $f(X)$ converges on the whole disc $D(p^b)$ if and only if $\mathfrak{N}(f)$ is of type (3) and $\lim_{i\to+\infty} d_i = +\infty$, where d_i is the distance between $(i, \mathrm{ord}_p\, a_i)$ and the last line of $\mathfrak{N}(f)$.

Radius of convergence

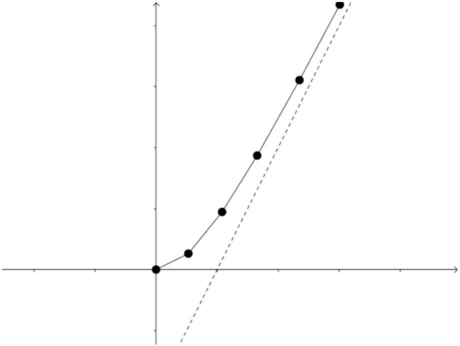
Theorem

Let $f(X) = 1 + \sum_{i=1}^{+\infty} a_i X^i \in 1 + X\mathbb{C}_p[\![X]\!]$ be a power series and let b be the least upper bound of all slopes of $\mathfrak{N}(f)$. Then the radius of convergence of $f(X)$ is $r = p^b$ (if $b = +\infty$ then $f(X)$ converges everywhere).

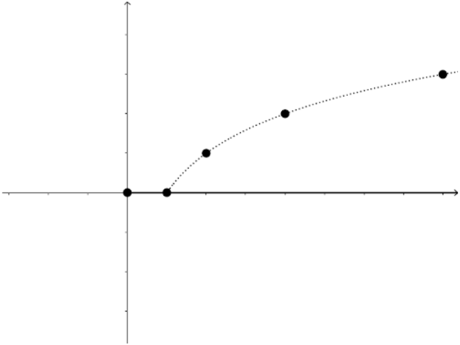
Proposition

With the same notations used above, $f(X)$ converges on the whole disc $D(p^b)$ if and only if $\mathfrak{N}(f)$ is of type (3) and $\lim_{i\to+\infty} d_i = +\infty$, where d_i is the distance between $(i, \mathrm{ord}_p\, a_i)$ and the last line of $\mathfrak{N}(f)$.

Other examples



There is no convergence at the border.



There is convergence at the border.

Theorem (*p*-adic Weierstrass preparation theorem)

Let $f(X) = 1 + \sum_{i=1}^{+\infty} a_i X^i$ *converge on* $D(p^\lambda)$. *Let* N *be the total horizontal length of all segments in* $\mathfrak{N}(f)$ *with slope less or equal to* λ, *if such number is finite, otherwise let* N *be the greatest index* i *such that* $(i, \operatorname{ord}_p a_i)$ *lies on the final segment. Then there exists a polynomial* $h(X) \in 1 + X\mathbb{C}_p[X]$ *of degree* N *and a power series* $g(X) \in 1 + X\mathbb{C}_p[\![X]\!]$, *which converges and is non-zero on* $D(p^\lambda)$, *such that*

$$h(X) = f(X) \cdot g(X).$$

The polynomial $h(X)$ *is uniquely determined by these properties and* $\mathfrak{N}(h)$ *coincides with* $\mathfrak{N}(f)$ *up to* $x = N$.

From the previous theorem the following proposition is immediate.

Proposition

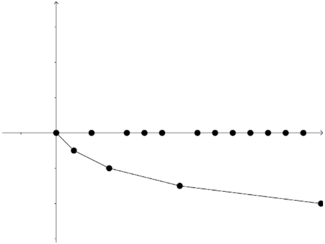
If a segment of $\mathfrak{N}(f)$ has finite length N and slope λ, then there are exactly N values of x (counting multiplicity) for which $f(x) = 0$ and $\mathrm{ord}_p\, x = -\lambda$.

Clearly every zero of $f(X)$ is obtained in this way. This is the exact power series analogue of the theorem about the zeroes of a polynomial and its Newton polygon.

We can use the Newton polygon to show that the exact region of convergence of $\mathrm{E}_p(X)$ is $D(1^-)$. We know that

$$\mathrm{E}_p(X) = \exp_p\left(X \cdot f(X)\right),$$

where $f(X) = \sum_{i=0}^{+\infty} \frac{X^{p^i-1}}{p^i}$. The Newton polygon of $f(X)$, using $p = 2$, is



and it's evident that $r = 1$ and we can't have convergence at border, since $\mathfrak{N}(f)$ is of type (1).

Theorem

Let $f(X) = 1 + \sum_{i=1}^{+\infty} a_i X^i$ be a proper power series (i.e. not a polynomial) everywhere convergent. Then, the set of its zeroes is countable infinite, let it be $(r_n)_{n\geq 1}$, and we have

$$f(X) = \prod_{i=1}^{+\infty} \left(1 - \frac{X}{r_i}\right).$$

This theorem implies, in particular, that every non-zero everywhere convergent power series must be a constant. Thus, an exponential like the classic one cannot exist in a p-adic environment.

Weierstrass product

Theorem

Let $f(X) = 1 + \sum_{i=1}^{+\infty} a_i X^i$ *be a proper power series (i.e. not a polynomial) everywhere convergent. Then, the set of its zeroes is countable infinite, let it be* $(r_n)_{n\geq 1}$*, and we have*

$$f(X) = \prod_{i=1}^{+\infty} \left(1 - \frac{X}{r_i}\right).$$

This theorem implies, in particular, that every non-zero everywhere convergent power series must be a constant. Thus, an exponential like the classic one cannot exist in a p-adic environment.