P-adic analysis

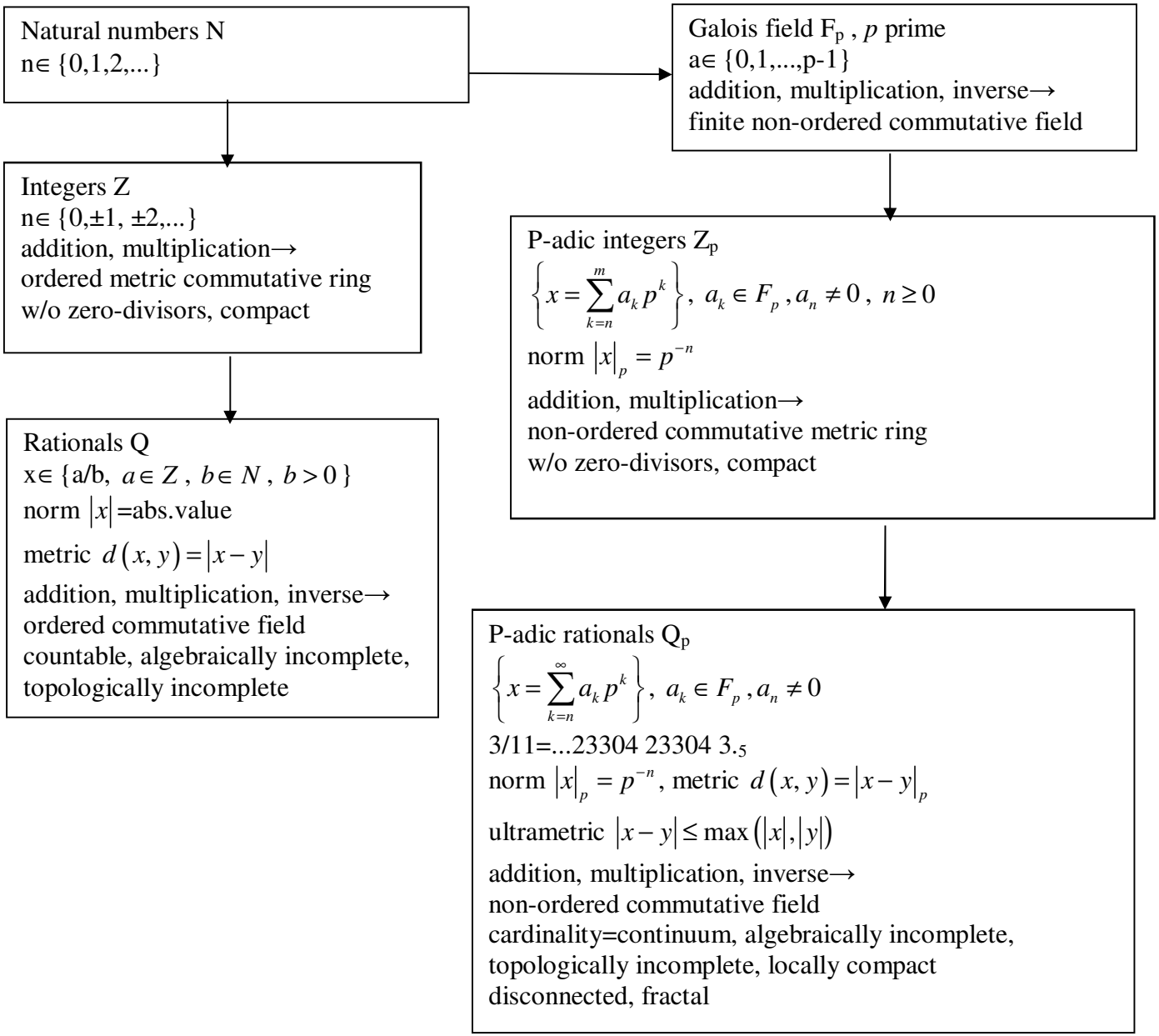
Jan Helm
Technical University Berlin
Email: jan.helm@alumni.tu-berlin.de

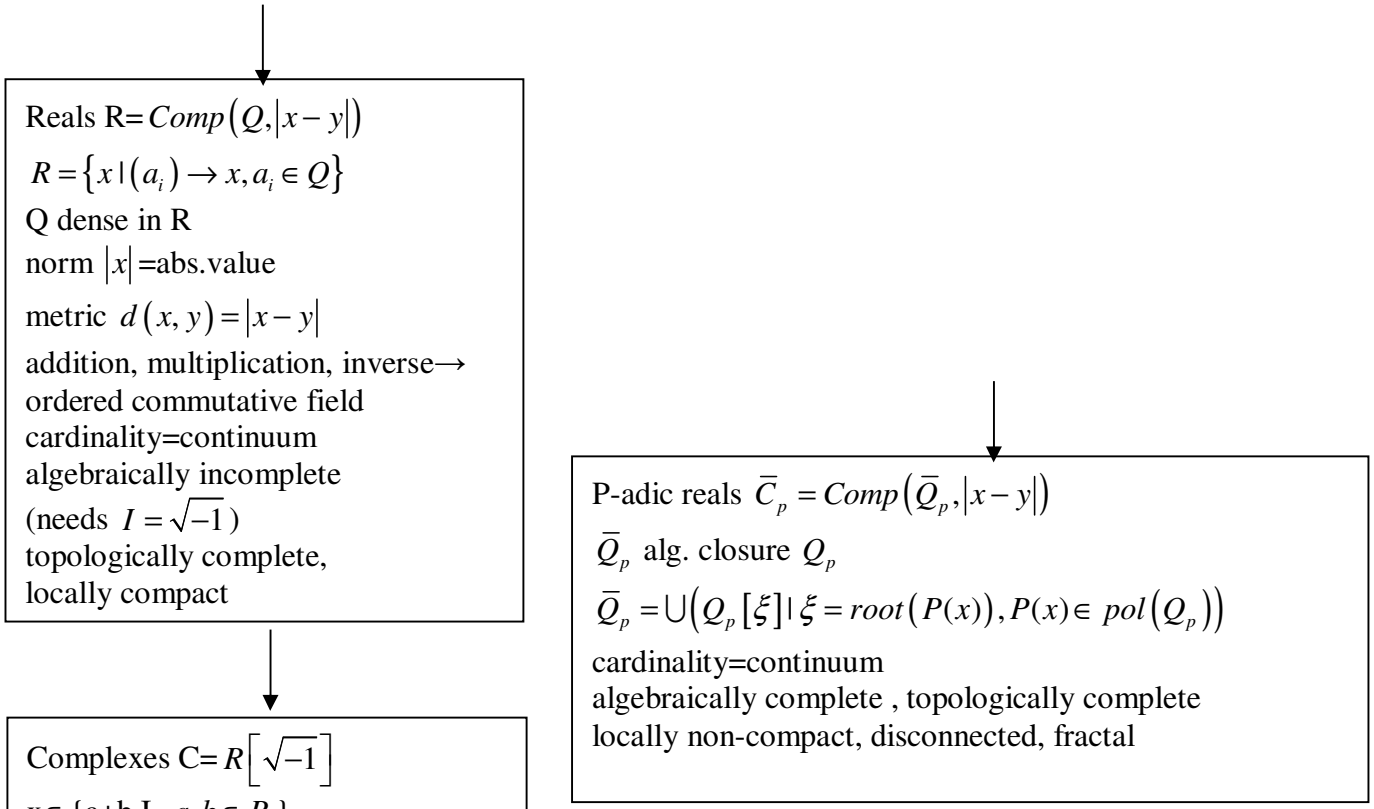
Abstract
Real and complex analysis is the most important part of the mathematical fundament of physics.
P-adic analysis based on p-adic numbers yields an alternative, which is similar in many respects, but has a completely different topology.
This paper is an introduction to p-adic number analysis in comparison with real and complex analysis, based on original papers, mathematical literature and on own calculations.

Contents

0 Flowcharts

Numbers


Natural numbers N
n∈ {0,1,2,...}
Galois field F_p , p prime
a∈ {0,1,...,p-1}
addition, multiplication, inverse→
finite non-ordered commutative field
Integers Z
n∈ {0,±1, ±2,...}
addition, multiplication→
ordered metric commutative ring
w/o zero-divisors, compact
P-adic integers Z_p
$\left\{x=\sum_{k=n}^{m} a_k p^k\right\},\ a_k \in F_p, a_n \neq 0,\ n \geq 0$
norm $|x|_p = p^{-n}$
addition, multiplication→
non-ordered commutative metric ring
w/o zero-divisors, compact
Rationals Q
x∈ {a/b, $a \in Z$, $b \in N$, $b>0$ }
norm $|x|$ =abs.value
metric $d(x,y)=|x-y|$
addition, multiplication, inverse→
ordered commutative field
countable, algebraically incomplete,
topologically incomplete
P-adic rationals Q_p
$\left\{x=\sum_{k=n}^{\infty} a_k p^k\right\},\ a_k \in F_p, a_n \neq 0$
3/11=...23304 23304 $3._5$
norm $|x|_p = p^{-n}$, metric $d(x,y)=|x-y|_p$
ultrametric $|x-y| \leq \max(|x|,|y|)$
addition, multiplication, inverse→
non-ordered commutative field
cardinality=continuum, algebraically incomplete,
topologically incomplete, locally compact
disconnected, fractal


Reals R= $Comp(Q,|x-y|)$
$R=\{x\,|\,(a_i)\to x, a_i\in Q\}$
Q dense in R
norm $|x|$ =abs.value
metric $d(x,y)=|x-y|$
addition, multiplication, inverse→
ordered commutative field
cardinality=continuum
algebraically incomplete
(needs $I=\sqrt{-1}$)
topologically complete,
locally compact
Complexes C= $R\left[\sqrt{-1}\right]$
x∈ {a+b I, $a,b\in R$ }
Q dense in R
norm $|x|=\sqrt{a^2+b^2}$ =abs.value
cardinality=continuum
algebraically complete
topologically complete
locally compact
P-adic reals $\bar{C}_p=Comp(\bar{Q}_p,|x-y|)$
$\bar{Q}_p$ alg. closure Q_p
$\bar{Q}_p=\cup\left(Q_p[\xi]\,|\,\xi=root(P(x)),P(x)\in pol(Q_p)\right)$
cardinality=continuum
algebraically complete , topologically complete
locally non-compact, disconnected, fractal

Polynomials and power series

sums in R: Cauchy convergence

$$\left(\sum_{i=0}^{\infty} a_i \mid a_i \in R\right) \to a \text{ iff}$$

$$\sum_{i=m}^{n} |a_i| < \varepsilon, \forall m,n$$

polynomials in Q: $P(x) \in Q[x]$

algebraically solvable in C

zeros: Newton-Raphson iteration

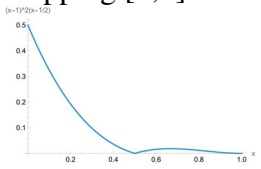
$$x_{n+1} = x_n - f(x_n) / f'(x_n)$$

error $\varepsilon_n = |\alpha - x_n|$, $\xi_n \in [x_n, \alpha]$

converges $|\varepsilon_{n+1}| = \varepsilon_n^{\,2} \dfrac{|f''(\xi_n)|}{2|f'(\xi_n)|}$

example $P(x) = (x-1)^2 (x-1/2)$

mapping [0,1]→R compact, connected



sums in Q_p: coefficients →0

$$\left(\sum_{i=0}^{\infty} a_i \mid a_i \in Q_p\right) \to a \text{ iff}$$

$$|a_i|_p \to 0$$

polynomials in Q_p: $P(x) \in Q_p[x]$

algebraically solvable in C_p

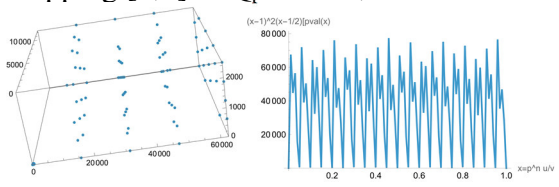
zeros: Hensel iteration

$$\hat{x}(x) = x - P(x) / P'(x)$$

converges if order $v(P'(x)) < n/2$

example $P(x) = (x-1)^2 (x-1/2)$

mapping [0,1]→ Q_p fractal, disconnected



polynomial approximation in R
Taylor series

$$f(x)=\sum_{i=0}^{k}\frac{f^{i}(a)}{i!}(x-a)^{i}+h_{k}(x)$$

$$h_{k}(x)=\frac{f^{k+1}(\xi)}{(k+1)!}(x-a)^{k+1}$$

Weierstraß approximation
f continuous $f:[a,b]\to R$

$$p_{n}(x)=\sum_{i=0}^{n}f\left(a+\frac{i}{n}(b-a)\right)B_{i,n}^{a,b}(x)$$

$p_{n}(x)\to f(x)$ uniform

$B_{i,n}^{a,b}(x)$ Bernstein polynomials

polynomial approximation in Q_p
Mahler series

$$f(x)=\sum_{x\geq k\geq 0}\nabla^{k}f(0)\binom{x}{k}$$ uniform conv.

$$\binom{x}{i}=\frac{x(x-1)...(x-i+1)}{i!}$$ binomial polynomials

forward difference operator $\nabla f(x)=f(x+1)-f(x)$

van-der-Putt approximation

$f:Z_{p}\to\bar{Q}_{p}$ continuous

$a_{0}=f(0)$, $a_{n}=f(n)-f(n\_)$, $n_{\_}=n-n_{v-1}p^{v-1}$

$\sum_{n}a_{n}\to f$ uniform

Functional analysis

functional norm in R[x]

$\|f\|_I = \sqrt{\int_{x\in I} f^2(x)\,dx}$ L_2 norm on interval I

differential $f'(a) = \lim_{x\to a} \frac{f(x)-f(a)}{x-a}$

differential operator $Df(x) = f'(x)$

mean value $f'(c) = \frac{f(b)-f(a)}{b-a}, c\in[a,b]$

fixed point $|f(x)-f(y)| \le q|x-y|$, q<1 $\rightarrow$

$\exists x_* : f(x_*) = x_*$

integral $\int_a^b f(x)\,dx = \lim_{n\to\infty} \sum_{i=1}^{n-1} f(x_i)(x_{i+1}-x_i)$

for $x_i \in [a,b]$

integral operator $(I_a f)(x) = \int_a^x f(t)\,dt$

fundamental theorem $D(I_a f)(x) = f(x)$

functional norm in Q_p[x]

$\|f\|_s = \sup_{x\in Q_p} |f(x)|$ max-norm

$\|f\|_G = \sup_k |a_k|$, $f(x) = \sum_{k\ge 0} a_k x^k$ Gauss norm

strict differential $f'(a) = \lim_{(x,y)\to(a,a)} \frac{f(x)-f(y)}{x-y}$

differential operator $Df(x) = f'(x)$

forward diff.operator $\nabla f(x) = f(x+1) - f(x)$

$f'(y) = \sum_{k\ge 1} (-1)^{k-1} (\nabla^k f)(y) / k$

mean value $|f(x+h)-f(x)| \le |h| \|f'\|_G$

for $|x| \le 1$, $|h| \le r_p = |p|^{1/(p-1)}$

fixed point $\|f'\|_G < 1$, $\inf_{x\in B_{\le 1}} |f(x)-x| \le |p|^{1/(p-1)}$ $\rightarrow$

$\exists x_* \in B_{\le 1} : f(x_*) = x_*$

Volkenborn integral

$\int_{Z_p} f(x)\,dx = \lim_{n\to\infty} \frac{1}{p^n} \sum_{j=0}^{p^n} f(j) = (Sf)'(0)$

sum operator $Sf(x) = \sum_{0\le i\le x} f(i)$

integral operator $(If)(x) = \int_{Z_p} f(x+t)\,dt$

fundamental theorem

$(If)(x) = (DSf)(x)$

$(\nabla S)(x) = f(floor(x+1))$

$S\nabla f = \nabla S f - f(0)$

1 Galois fields

A Galois field, often denoted as F_q, is a finite commutative field containing a finite number of elements, where ($q = p^n$) is a power of a prime number *p*.
It is a set where addition, subtraction, multiplication, and division are defined and satisfy basic algebraic rules.
Galois fields are not ordered, i.e. there is no relation "<" .

Example:
F5, simple Galois field with elements {0,1,...,4}
Solution of x^2+1==0
$\sqrt{-1} = 2$, $\sqrt{-1} = 3$
Solution of x^2-1==0
$\sqrt{1} = 1$, $\sqrt{1} = 4$
Solution of x^2-2==0: no solution

Multiplication table F_5

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Addition table F_5

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

2 P-adic number analysis

[1]

P-adic numbers

P-adic numbers Q_p are an extension of the field of rationals Q such that congruences modulo powers of a fixed prime *p* are related to proximity in the p-adic metric.

Any rational number $x=\frac{a}{b}\in Q$ can be written uniquely in the form $p^n\frac{u}{v}$ where $p\nmid u \quad p\nmid v$ (*u* and *v* not divisible by *p*), where *p* is a prime number, *r* and *s* are integers not divisible by p .

The corresponding p-adic representation of *x* is then $x=\sum_{k=n}^{\infty}a_k p^k$, where $a_k\in\{0,1,...,p-1\}$, and $a_n\neq 0$.

The integer *n* is the order of the p-adic number (index of the lowest non-zero coefficient), *n* can be negative.

The coefficient a_k obey the arithmetic mod(p), i.e. they are elements of the underlying Galois field F_p , $a_k\in F_p$.

Then we define the *p*-adic norm of *x* by $|x|_p=p^{-n}$, also, $|0|_p=0$

For natural numbers $x\in N$ we have the finite sum representation $x=\sum_{k=n}^{m}a_k p^k$ with basis *p* analogous to the usual decimal representation.

For negative integers $x\in Z$, $x=-|x|$ we have the representation $x=\sum_{k=n}^{m}\tilde{a}_k p^k$, where the coefficients are the negative coefficients mod(p) $\tilde{a}_k+a_k=0\bmod(p)$ of the positive number representation $|x|=\sum_{k=n}^{m}a_k p^k$.

The p-adic integers Z_p obey multiplication and addition mod(p) with carry, and they have no zero-dividers , i.e. they allow multiplicative inverse, and can be extended to a field Q_p .

Rationals 1/q , $q\neq p^k$, k>0, are p-adic integers ${q^{-1}}_p\in Z_p$

Rationals 1/q , $q=p^k$, k>0, are proper p-adic fractures e.g. ${5^{-1}}_5=.1_5$

Arbitrary rationals $\frac{u}{v}$ (*u* and *v* not divisible by *p*) are formed by multiplication mod(p) $u*(1/v)\bmod(p)$

Valid identities are

$-1=\sum_{k=0}^{\infty}(p-1)p^k$, e.g. (p=5) $...4444444_5$

$\frac{1}{1-p}=\sum_{k=0}^{\infty}p^k$

p-adics are written as

- fractions, from right to left, where the point signifies the order (and is skipped, when at beginning, i.e. when order v=0), e.g. p=5

1/5=.1_5

1/11=... 42330423304233042331_5

- lists, from left to right, where the order is the first element of the list, e.g. p=5

1/5= {-1, {1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0}}

1/11= {0, {1, 3, 3, 2, 4, 0, 3, 3, 2, 4, 0, 3, 3, 2, 4, 0, 3, 3, 2, 4}}

The cardinality of Z_p (and of Q_p) is the cardinality of continuum like *R*, whereas *Q* is countable (cardinality of *N*).

The p-adics Q_p were first introduced by Hensel (1897) in a paper which was concerned with the development of algebraic numbers in power series, p-adic numbers were then generalized to valuations by Kűrschák in 1913.

Rationals as p-adic numbers

The p-adic valuation (=norm) $|x|_p$ on Q gives rise to the p-adic metric $d(x,y)=|x-y|_p$

which in turn gives rise to the p-adic topology.

It can be shown that the rationals Q, together with the p-adic metric, do not form a complete metric space.

The completion of this space is the set of complete p-adic numbers $\bar{Q}_p = Comp\left(Q_p, |x-y|_p\right)$.

The real numbers R are the completion of the rationals Q with respect to the usual absolute value $|x|$,

$R=\bar{Q}$ $R=Comp\left(Q,|x-y|\right)$ is the set of all convergent series in Q in the metric $d(x,y)=|x-y|$

A rational number with p-adic absolute value 1 has a purely periodic p-adic expansion if and only if it lies in the real interval $[-1,0)$.

A genuine fractional rational number with p-adic absolute value 1, outside the real interval $[-1,0)$ has a fixed initial expansion followed by a purely periodic p-adic expansion.

p-adic faculty *n!*

The p-adic faculty *n!* (without p-powers) has p-adic valuation

$|n!|_p = p^{-(n-A_p(n))/(p-1)}$

where the p-adic expansion of *n* is $n=a_0+a_1p^1+...+a_Lp^L$

and $A_p(n)=a_0+a_1+...a_L$

For sufficiently large *n* , $|n!|_p \le p^{-n/(2p-2)}$

p-adic metric

The p-adic metric is a non-Archimedean distance function where two numbers are close if their difference is highly divisible by a prime p.

Any rational number $x=\frac{a}{b}\in Q$ can be written uniquely in the form $p^n\frac{u}{v}$ where $p\nmid u$ $p\nmid v$ (*u* and *v* not divisible by *p*).

The p-adic norm is then $|x|_p = p^{-n}$, the metric is $d(x,y) = |x-y|_p$

The metric is non-archimedean (ultrametric), it obeys the strong triangle inequality $|x-y| \le \max(|x|,|y|)$

instead of the simple (archimedean) triangle inequality $|x-y| \le |x| + |y|$.

p-adic half-metric

The p-adic metric yields a distance function sufficient for convergence criteria, but it is little sensitive near zero, therefore not well-suited for numerical calculations.

A better metric function is $f_{rat}(x_p, n, L)$ used for recovering rational numbers from the p-adic numbers.

$|x_p|_{hp} = |f_{rat}(x_p, n, L)|$, where period start position *n=1* and period length *L=N-1, N*=precision.

$|x_p|_{hp}$ is a half-norm, because it is not symmetric $|x_p|_{hp} \neq |-x_p|_{hp}$, and neither is the distance $|x_p - y_p|_{hp}$, but it satisfies the triangle relation

$|x_p - y_p|_{hp} \le |x_p|_{hp} + |y_p|_{hp}$.

Examples

p-adic numbers p=5, 10 or 20 digits

p-adic fraction form (right to left), below: list form (left to right)

$1=1_5$

{0, {1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0}}

finite

$-1=4444444444444444444_5$

{0, {4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4}}

period 4

$1/5=.1_5$

{-1, {1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0}}

here order v=-1, norm $|\ |_5 = 1/5$, all others have v=0, $|\ |_5 = 1$

$11=21_5$

{0, {1, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0}}

finite

$1/11=42330423304233042331_5$

{0, {1, 3, 3, 2, 4, 0, 3, 3, 2, 4, 0, 3, 3, 2, 4, 0, 3, 3, 2, 4}}
fixed=1 , period 04233

3/11=233042330423304233043_5
{0, {3, 4, 0, 3, 3, 2, 4, 0, 3, 3, 2, 4, 0, 3, 3, 2, 4, 0, 3, 3}}
fixed=3 , period 23304

-3/11= $42330423304233042323114021140211402114021402_5$
{0, {2, 0, 4, 1, 1, 2, 0, 4, 1, 1, 2, 0, 4, 1, 1, 2, 0, 4, 1, 1}}
period 11402

12/11=$204233042330423304233 2_5$
{0, {2, 3, 3, 2, 4, 0, 3, 3, 2, 4, 0, 3, 3, 2, 4, 0, 3, 3, 2, 4}}
fixed=2 , period 04233

Non-archimedean (ultra-metric) distance
p-adic distance is $d_p(x,y)=|x-y|_p$

A non-Archimedean distance, or ultrametric, is a distance metric d(x,y) that satisfies a strict form of the triangle inequality:
$|x-y| \le \max(|x|,|y|)$, whereas Euclidean distance obeys the simple triangle inequality $|x-y| \le |x|+|y|$.

Unlike Euclidean distance, it implies distances do not "add up" or accumulate, often resulting in topologies that are totally disconnected, where all balls are clopen (both open and closed).

- Strong triangle inequality $|x-y| \le \max(|x|,|y|)$, weaker in general $|x-y| \le |x|+|y|$
- Strong multiplicativity $|x*y|=|x|*|y|$, weaker in general $|x*y| \le |x|*|y|$
- Isosceles Triangles: All triangles are isosceles, with the two larger sides equal.
- Ball Structure: Two balls $B_{x.r}=\{x \mid |x|<r\}$ either are disjoint or one is contained within the other.
- Center Property: Any point within a ball can be considered its center.
- Topology: The resulting topology is totally disconnected, where all balls are clopen (open and close)
- Smallness: Numbers that are large in the real sense (like 5^{100}) are small in the p-adic sense mod5, while small numbers (like $1/5^{100}$ mod5) are large.
- **Ostrowski's Theorem**: This theorem states that any non-trivial absolute value on the rational numbers Q is equivalent to either the usual real absolute value or a p-adic absolute value.

Mapping Qp->R

There is **no canonical embedding** (a natural, structure-preserving map) from the p-adic numbers Qp into the real numbers R.

Here is a breakdown of why this is the case based on number theory principles:

- **Different Completions:** Both Qp and R are completions of the field of rational numbers Q, but they are completed with respect to completely different, non-equivalent metrics (absolute values).
- **Topological Incompatibility:** R is a connected, archimedean field, while Q_p is totally disconnected and non-archimedean. There is no continuous field homomorphism between them.
- **Algebraic Closure:** R is not algebraically closed (its algebraic closure is C), whereas Q_p is also not algebraically closed (its algebraic closure is Q_p^a).

Mapping Q->Q_p

- **Definition:** The map is defined by $\iota_p : Q \to Q_p$, where $\iota_p(x) = x$
- **Completeness:** The p-adic field Q_p is defined as the completion of Q with respect to the p-adic absolute value $|\ |_p$

Therefore, Q acts as a dense subfield of Qp

- **Dense Subset:** The image $\iota_p(Q)$ is dense in Q_p, meaning any p-adic number can be approximated by a sequence of rational numbers using the p-adic norm.
- **Field Structure:** This mapping is a injective ring homomorphism, preserving both addition and multiplication.
- **p-adic expansion**

Any rational number $\frac{a}{b} \in Q$ can be written uniquely in the form $p^n \frac{u}{v}$ where $p \nmid u \quad p \nmid v$

The canonical embedding is then $\iota : p^n \frac{u}{v} \to \sum_{k=n}^{\infty} a_k p^k$, $Q \to Q_p$, with $a_k \in \{0,1,\ldots p-1\}$

Extensions of Qp

mathoverflow.net

- The elements of Q_p are exactly those represented by series of the form $\sum_{r \in S} a_r p^r$, where S is a bounded-below subset of the integers and each a_r is a multiplicative lift (i.e., a "Teichmüller lift") of an element of F_p.
- The Teichmüller character is a homomorphism (lift) of multiplicative groups: $\omega : F_p^x \to Z_p^x$, such that $\omega(a)$ is the unique (p−1)-th root of unity in Z_p which is congruent to a modulo p
- The elements of Q_{nrp} (the maximal unramified extension of Q_p) are exactly represented by series of the form $\sum_{r \in S} a_r p^r$, where S is again a bounded-below subset of the integers, but the a_r can now be lifts of any element of F_q, where $q=p^n$ is a fixed power of p.
- The elements of $\bar{Q}_p$ and its completion C_p are represented by certain series of the form $\sum_{r \in S} a_r p^r$, where the a_r are again lifts of elements of F_q , but now S can be a more general well-ordered subset of Q.

Theorem [Kedlaya] (Huang, Rayner, Stefanescu). Let L be the set of generalized power series of the form $f = \sum_{i \in S} x_i t^i$, where the set S⊂Q (which depends on f) has the following properties:
1. Every nonempty subset of S has a least element (i.e. S is well-ordered).
2. There exists a natural number *m* such that every element of m*S has denominator a power of *p*.
Then L is an algebraically closed field

- The elements of Ω_p, the *spherical completion* of C_p, are represented exactly by series of the form $\sum_{r \in S} a_r p^r$, where the a_r are as before, but now S can be *any* well-ordered subset of Q (with no other restrictions).

And this is in some sense as far as we can go, since Ω_p is maximally complete: we can't extend it any further without adding geometry, in the sense that it's the unique largest field of characteristic zero (sum of 1's is always ≠0) with value group Q and residue field the algebraic closure of F_p.

Visualization
[2]

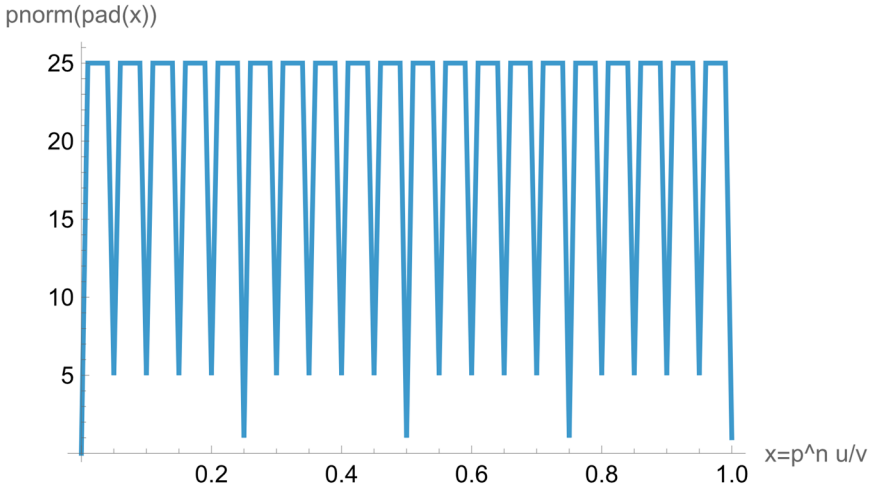
The canonical mapping is $\iota : p^n \frac{u}{v} \to \sum_{k=n}^{\infty} a_k p^k$, $Q \to Q_p$, with $a_k \in \{0,1,...p-1\}$

The canonical p-adic scalar valuation is $v_c : \left(\sum_{k=n}^{\infty} a_k p^k \right)_p \to \left(p^{-n} \sum_{k=n}^{\infty} a_k p^{k-n} \right)$, $Q_p \to Q$

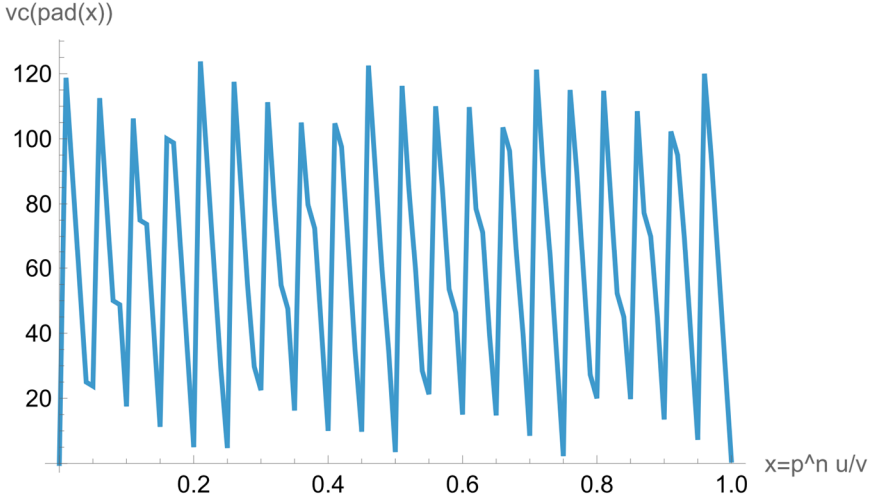
The canonical p-adic vector valuation length n_c is $v_v : \left(\sum_{k=n}^{\infty} a_k p^k \right)_p \to p^{-n} \left\{ a_k p^{k-n} \right\}_{k=n}^{n+n_c-1}$, $Q_p \to Q^{n_c}$

Example 1 p-adic norm , prime base p_0=5
npts=100 number grid points
dint=1 interval [0,1]
p0=5 base prime p=5
Ndigits=100 number of elements in series expansion

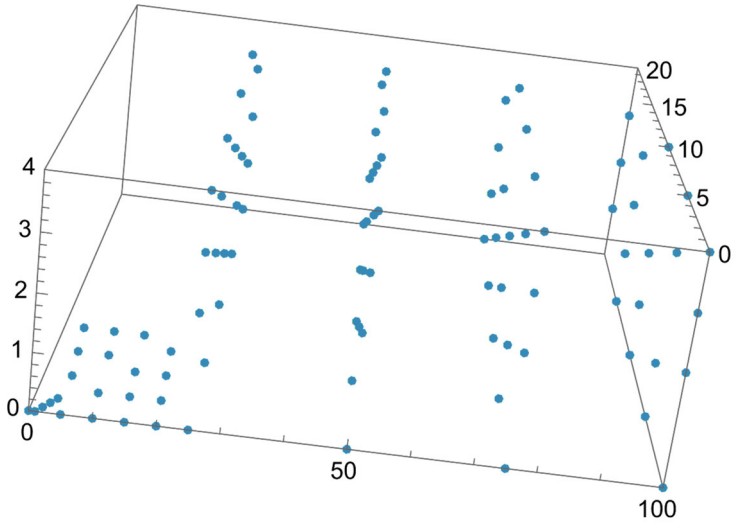
p-adic norm $|x|_p$



canonical scalar valuation v_c in Q



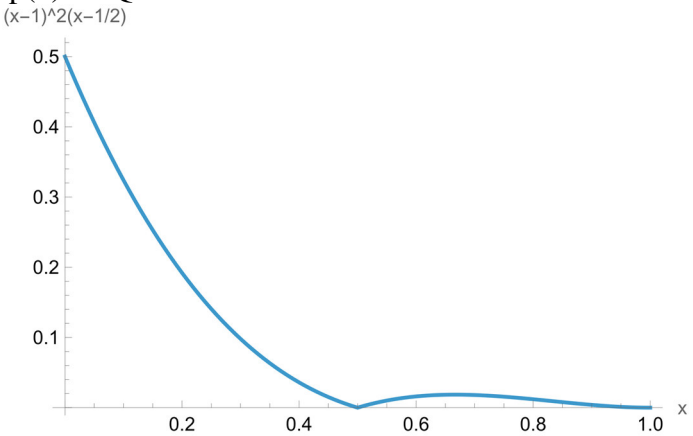
canonical vector valuation v_v with length 3 in Q^3


20
15
10
5
0
4
3
2
1
0
0
50
100

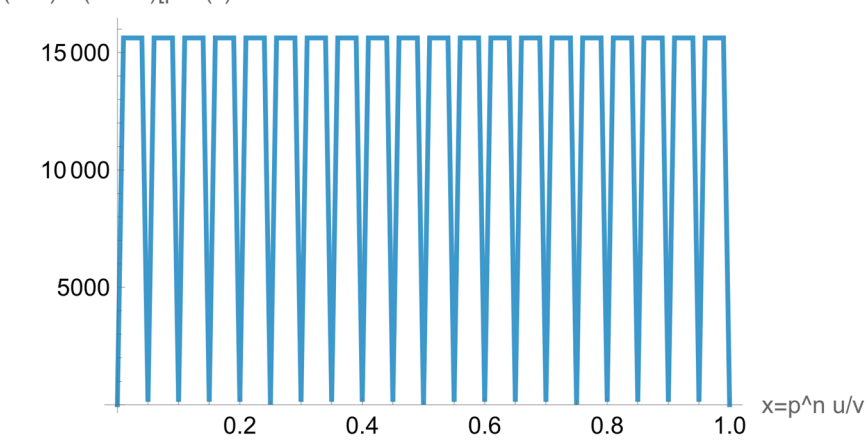
Example 2 polynomial p(x)=(x−1)^2 (x−12), prime base p_0=5

npts=100 number grid points
dint=1 interval [0,1]
p_0=5 base prime
Ndigits=100 number of elements in series expansion
pnorm=p-adic norm $|x|_p$
pval=p-adic scalar valuation v_c
vpval vector valuation v_v with length 3 in Q^3

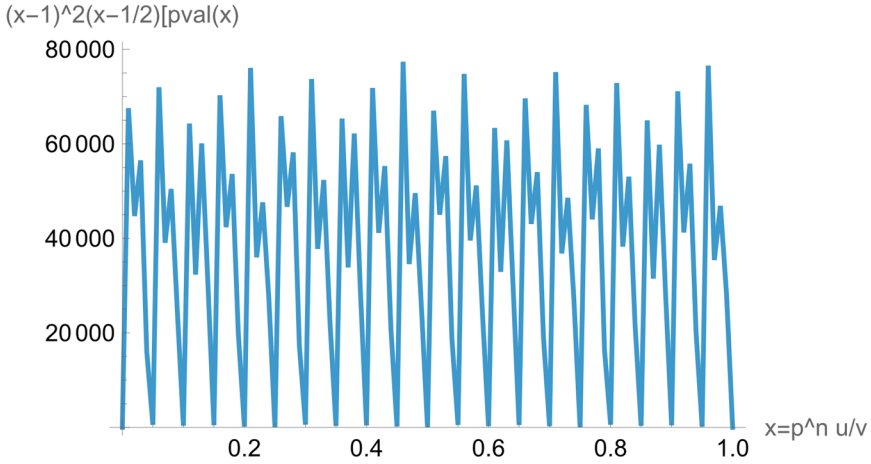
|p(x)| in Q



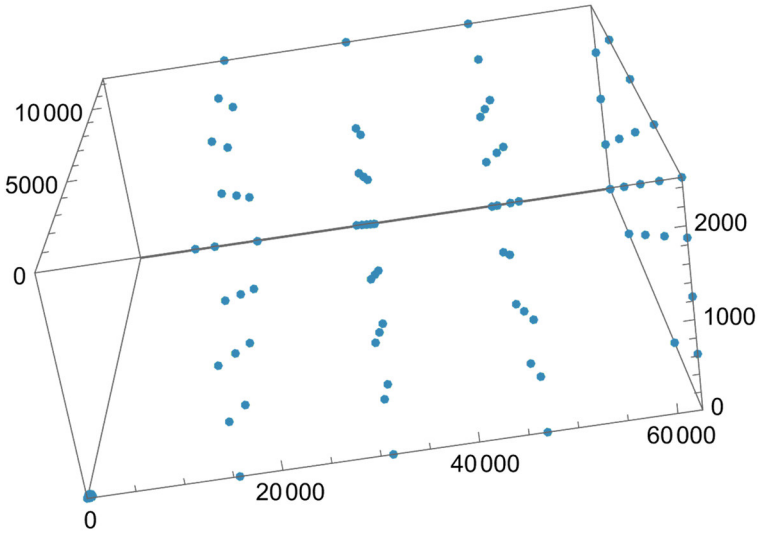
pnorm(p(x),p) in Qp



scalar valuation pval(p(x),p) in Qp



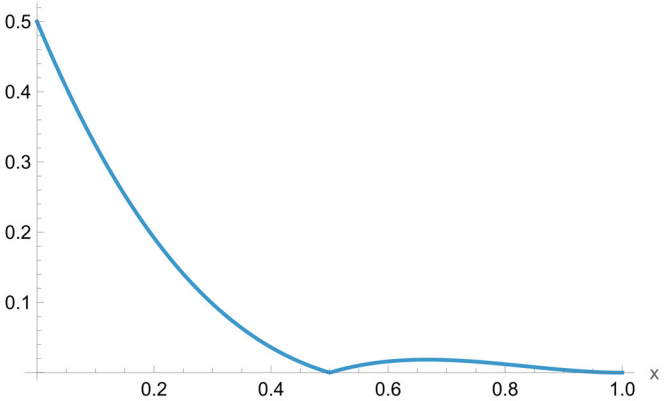
vpval vector valuation v_v with length 3 in Q^3



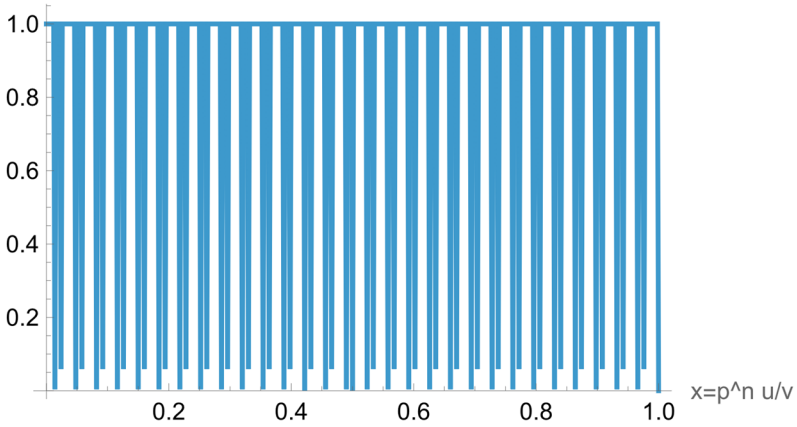
Example 3 polynomial p(x)=(x−1)^2 (x−12), prime base p_0=17

npts=100 number grid points
dint=1 interval [0,1]
p_0=17 base prime
Ndigits=500 number of elements in series expansion
pnorm=p-adic norm $|x|_p$
pval=p-adic scalar valuation v_c
vpval vector valuation v_v with length 3 in Q^3

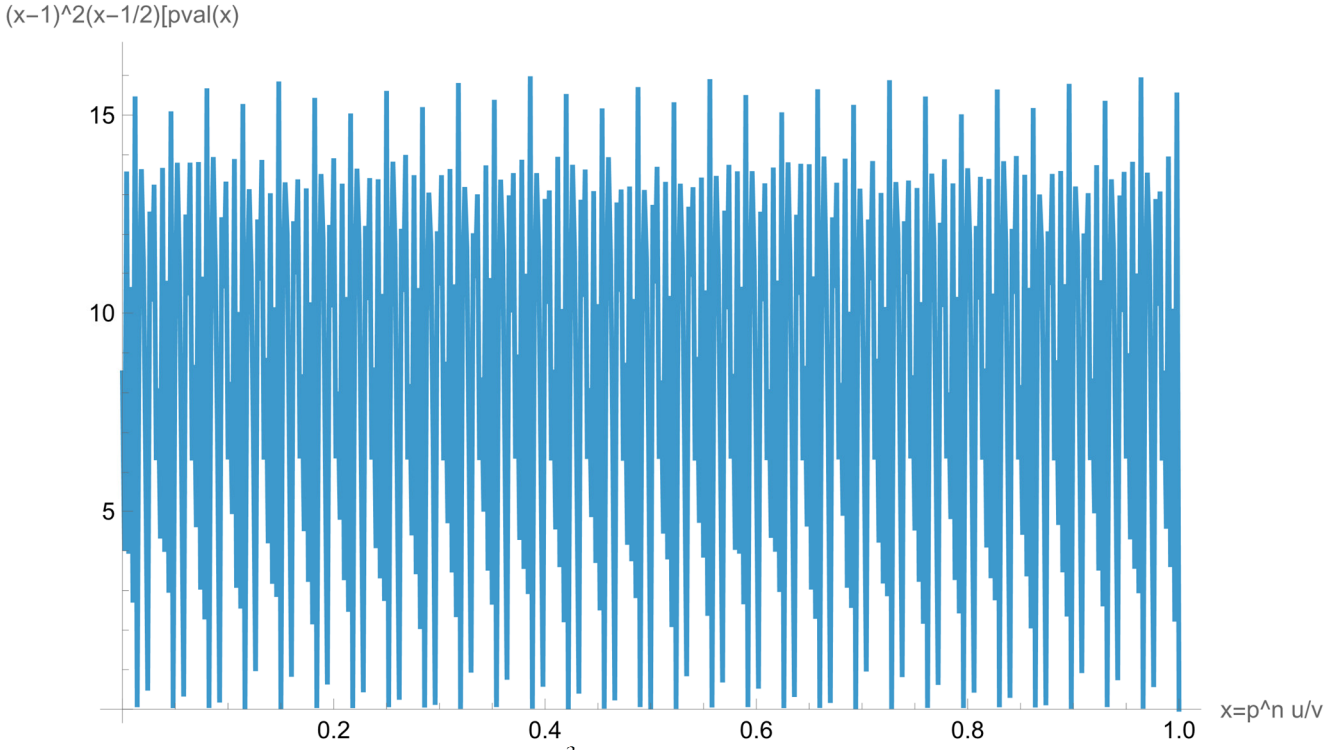
|p(x)| in Q
(x−1)^2(x−1/2)



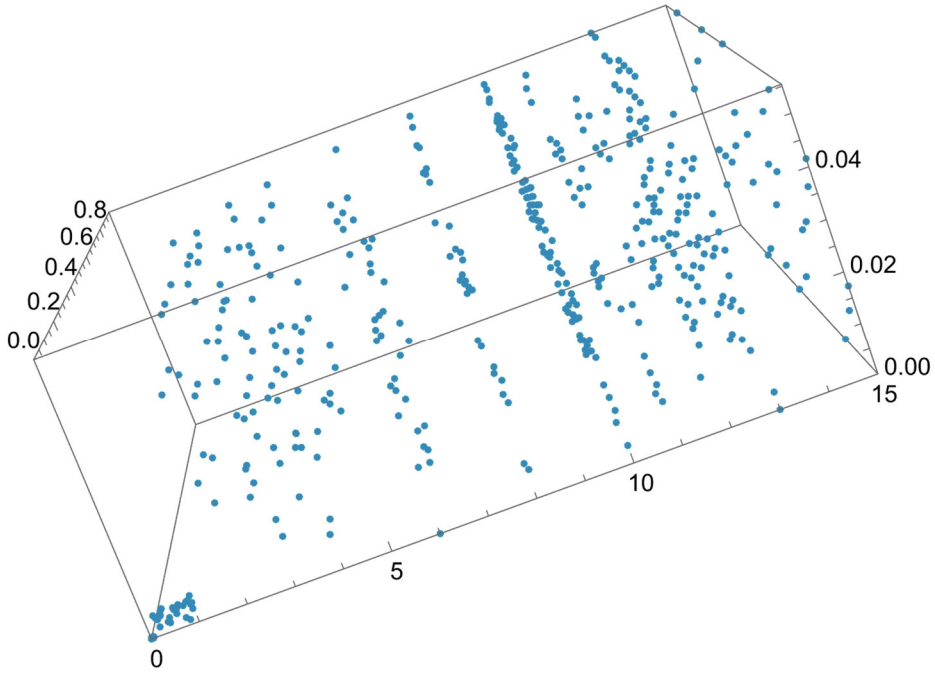
pnorm(p(x),p) in Qp
(x−1)^2(x−1/2)[pad(x)



scalar valuation pval(p(x),p) in Qp



vpval vector valuation v_v with length 3 in Q^3



P-adic analysis in brief

In mathematics, p-adic analysis is a branch of number theory that studies functions of p-adic numbers. Along with the more classical fields of real and complex analysis, which deal, respectively, with functions on the real and complex numbers, it belongs to the discipline of mathematical analysis.

The theory of complex-valued numerical functions on the p-adic numbers is part of the theory of locally compact groups (abstract harmonic analysis). The usual meaning taken for p-adic analysis is the theory of p-adic-valued functions on spaces of interest.

Applications of p-adic analysis have mainly been in number theory, where it has a significant role in diophantine geometry and diophantine approximation. Some applications have required the development of p-adic functional analysis and spectral theory. In many ways p-adic analysis is less subtle than classical analysis, since the ultrametric inequality means, for example, that convergence of infinite series of p-adic numbers is much simpler. Topological vector spaces over p-adic fields show distinctive features; for example aspects relating to convexity and the Hahn–Banach theorem are different.

Ostrowski's theorem

Ostrowski's theorem, (1916), states that every non-trivial absolute value on the rational numbers Q is equivalent to either the usual real absolute value or a p-adic absolute value.

Mahler's theorem

expresses continuous *p*-adic functions in terms of polynomials.

In any field of characteristic 0 , one has the following result.
In mathematics, the characteristic of a ring R, often denoted char(R), is defined to be the smallest positive number of copies of the ring's multiplicative identity (1) that will sum to the additive identity (0). If no such number exists, the ring is said to have characteristic zero.
Let $(\nabla f)(x) = f(x+1) - f(x)$ be the forward difference operator. Then for polynomial functions f we have the Newton series:

$$f(x) = \sum_{k=0}^{\infty} (\nabla^k f)(0) \binom{x}{k}$$

where $\binom{x}{k} = \frac{x(x-1)\ldots(x-k+1)}{k!}$

is the k-th binomial coefficient polynomial.
Over the field of real numbers, the assumption that the function f is a polynomial can be weakened, but it cannot be weakened all the way down to mere continuity.
Mahler's theorem: If f is a continuous p-adic-valued function on the p-adic integers then the Newton series identity holds.

Hensel's lemma

Hensel's lemma, also known as Hensel's lifting lemma, named after Kurt Hensel, is a result in modular arithmetic, stating that
if a polynomial equation has a simple root modulo a prime number p, then this root corresponds to a unique root of the same equation modulo any higher power of p,
which can be found by iteratively "lifting" the solution modulo successive powers of p. More generally it is used as a generic name for analogues for complete commutative rings (including p-adic fields in particular) of the Newton method for solving equations.
Since p-adic analysis is in some ways simpler than real analysis, there are relatively easy criteria guaranteeing a root of a polynomial.
To state the result, let $f(x)$ be a polynomial with integer (or p-adic integer) coefficients, and let m,k be positive integers such that $m \leq k$.
If r is an integer such that

$$f(r) = 0 \bmod p^k \text{ and } f'(r) \neq 0 \bmod p$$

then there exists an integer s such that

$$f(s) = 0 \bmod p^{k+m} \text{ and } r = s \bmod p^k$$

Furthermore, this s is unique modulo p^{k+m}, and can be computed explicitly as

$$s = r + t\,p^k \text{ where } t = -\frac{f(r)}{p^k f'(r)}$$

Hasse principle

Helmut Hasse's local–global principle, also known as the Hasse principle, is the idea that one can find an integer solution to an equation by using the Chinese remainder theorem to piece together solutions modulo powers of each different prime number. This is handled by examining the equation in the completions of the rational numbers: the real numbers and the p-adic numbers. A more formal version of the Hasse principle states that certain types of equations have a rational solution if and only if they have a solution in the real numbers and in the p-adic numbers for each prime p.
In mathematics, the *Chinese remainder* theorem states that if one knows the remainders of the Euclidean division of an integer n by several integers, then one can determine uniquely the remainder of the division of n by the product of these integers, under the condition that the divisors are pairwise coprime (no two divisors share a common factor other than 1).

***p*-adic exponential function**

In mathematics, particularly p-adic analysis, the p-adic exponential function is a p-adic analogue of the usual exponential function on the complex numbers. As in the complex case, it has an inverse function, named the p-adic logarithm.
The usual exponential function on C is defined by the infinite series

$$\exp(z)=\sum_{n=0}^{\infty}\frac{z^n}{n!}$$

Entirely analogously, one defines the exponential function on C_p, the completion of the algebraic closure of Q_p, by

$$\exp_p(z)=\sum_{n=0}^{\infty}\frac{z^n}{n!}$$

However, unlike exp which converges on all of C, $\exp_p$ only converges on the disc

$$|z|_p < p^{-1/(p-1)}$$

It follows from Legendre's formula that if $|z|_p < p^{-1/(p-1)}$ then $\left|\frac{z^n}{n!}\right|_p \to 0$, p-adically.

Legendre formula

For any prime number p and any positive integer n, let $v_p(n)$ be the exponent of the largest power of p that divides n (that is, the p-adic valuation of n).
Then

$$v_p(n!)=\sum_{i=1}^{\infty}\left\lfloor\frac{n}{p^i}\right\rfloor$$

where ⌊x⌋ is the floor function.

Calculus over p-adic numbers in brief

Calculus over p-adic numbers (Q_p) is a branch of analysis that operates on a field constructed from rational numbers using a non-Archimedean metric, where numbers are considered close if their difference is divisible by a high power of a prime p . Unlike real calculus, p-adic calculus uses an ultrametric, where convergence of series is much simpler, and the concept of "derivative" does not necessarily imply constant behavior for zero-derivative functions.

Fundamental Concepts in p-adic Calculus

Derivative

derivative of p-adic polynomial $f(x)\in Q_p[x]$, $f(x)=\sum_{k=0}^{n}a_k x^k$

is $f'(x)=\sum_{k=1}^{n}k\,a_k x^{k-1}$

The derivative is computed by taking the limit

$\lim_{h\to 0}\frac{f(x+h)-f(x)}{h}$ for $h\to 0$, i.e. $h(n)=\sum_{i\geq n}p^i$

forward-difference operator ∇ on the binomial functions:

$(\nabla f) = f(x+1) - f(x)$

$\nabla \binom{x}{0} = 0$, $\nabla \binom{x}{i} = \binom{x}{i-1}$ $i \geq 1$

compare: the **differential operator** D on x-powers $x^i / i!$

$D(x^0) = 0$, $D\left(\frac{x^i}{i!}\right) = \frac{x^{i-1}}{(i-1)!}$ $i \geq 1$

Mahler series

Theorem (Mahler)

Let $f : Q_p \to Q_p$, then there is a unique sequence $(m_i)_{i \geq 0}$, such that

$f(x) = \sum_{i=0}^{x} m_i \binom{x}{i}$, $m_i = (\nabla^i f)(0)$

With Pochhammer symbol $(x)_0 = 1$, $(x)_i = x(x-1)...(x-i+1)$ $i \geq 1$

binomial polynomes are $\nabla (x)_i = i (x)_{i-1}$, $\binom{x}{i} = \frac{(x)_i}{i!}$

Mahler series becomes $f(x) = \sum_{i=0}^{x} \frac{(\nabla^i f)(0)}{i!} (x)_i$, $(\nabla^k f)(0) = \sum_{i \leq k} (-1)^{k-i} \binom{k}{i} f(i)$

compare: classical analysis Taylor series $f(x) = \sum_{i=0}^{\infty} \frac{f^{(i)}(0)}{i!} x^i$

Unlike real analysis, the p-adic derivative of a non-constant function can be zero.

However, for a polynomial $f(x) \in Q_p[x]$, the formal derivative *f*‘ is not zero, unless *f*=const.

Integration

sum operator $Sf(x) = F(x)$, $F(n) = \sum_{0 \leq i \leq n} f(i)$ is the inverse of in comparison to the integration operator $\int f(x) dx$

p**-adic Metric:** The p-adic absolute value, $|x|_p$ is defined by factoring out the highest power of a prime *p* from a number.

The distance between two numbers is $|x - y|_p$

Convergence: A p-adic series $\sum_i a_i$, $a_i \in Q_p$ converges if and only if $\lim_{i \to \infty} |a_i|_p = 0$

This is a major simplification compared to real analysis, as convergence is only determined by the size of the terms, not their alternating sign.

Ultrametric Inequality: p-adic numbers satisfy a stronger triangle inequality:

$|x+y|_p \le \max\left(|x|_p, |y|_p\right)$ instead of $|x+y| \le |x|+|y|$

Compactness: The space of p-adic integers Z_p is a compact ring, which makes it a natural domain for integration.

Derivatives in Q_p

Definition: A function $f : Q_p \to Q_p$ is differentiable at x_0

if a p-adic linear map exists representing the local behavior of the function, similar to the real-valued case.

*f i*s strictly differentiable at a point $a \in X$ if the difference quotient

$\Phi f(a+h,a) = \dfrac{f(a+h)-f(a)}{h}$ has a limit $f'(a) = \lim_{h\to 0} \Phi f(a+h,a)$

Definition: We say that *f* is strictly differentiable at a point $a \in X$ and denote this property by $f \in S^1(a)$ if the difference quotients

$\Phi f(x,y) = \dfrac{f(x)-f(y)}{x-y}$ have a limit $f'(a) = \lim_{(x,y)\to(a,a)} \Phi f(x,y)$

Zero Derivative Surprise: In p-adic analysis, a function can have a (strict) derivative of zero everywhere, but not be a constant function. This is because the p-adic numbers are totally disconnected, allowing functions to "jump" without being continuous in the real sense.

Hensel's Lemma: An important analytical tool, essentially a p -adic version of Newton's method, that allows for finding roots of polynomials by refining approximate roots.

Integration in Q_p

Haar Measure: Because p-adic numbers are locally compact groups, they have a natural translation-invariant measure (the Haar measure), which is used to define integration.

p-adic Gamma Function: A specific function of interest defined using these principles.

Coleman's Theory: A powerful theory of p-adic line integrals (or "p-adic abelian integrals") that enables a "Fundamental Theorem of Calculus" analogue, which can demonstrate that the integral of a 1/x function over a closed loop is zero, despite the different topological structure.

3 Real analysis

[3]

Real analysis studies real numbers R, focusing on continuity, limits, and integration on a line, while complex analysis explores functions over complex numbers c= a + b i, which form a 2D plane.

Real analysis is the branch of mathematical analysis that is concerned with properties of real numbers and real-valued functions. Classical real analysis provides the rigorous foundations of calculus, specifically convergent series, limits, continuity, differentiability, smoothness, and integrability. Central to the subject is the completeness of the real numbers, which distinguishes the real numbers from the rational numbers and underlies many basic results about limits and continuous functions.

Basics

Limit

Definition. Let f be a real-valued function defined on E⊂R. We say that f(x) tends to L as x approaches x0, or that the limit of f(x) as x approaches x0 is L if, for any ε>0, there exists δ>0 such that for all x∈E, 0<|x−x0|<δ implies that |f(x)−L|<ε. We write this symbolically as $f(x) \to L$ as $x \to x_0$

Definition. Let (an) be a real-valued sequence. We say that (an) is a Cauchy sequence if, for any ε>0, there exists a natural number N such that $m,n \geq N$ implies that $|a_m - a_n| < \varepsilon$.

It can be shown that a real-valued sequence is Cauchy if and only if it is convergent.

Uniform and pointwise convergence

Roughly speaking, pointwise convergence of functions f_n to a limiting function f:E→R, denoted $f_n \to f$, simply means that given any x∈E, $f_n(x) \to f(x)$ as $n \to \infty$. In contrast, uniform convergence is a stronger type of convergence, in the sense that a uniformly convergent sequence of functions also converges pointwise, but not conversely.

Uniform convergence requires members of the family of functions, f_n, to fall within some error ε>0 of f for every value of x∈E, whenever n≥N, for some integer N.

Compactness

Definition. A set E⊂R is compact if it is closed and bounded.

Definition. A set E in a metric space is compact if every sequence in E has a convergent subsequence.

Continuity

Definition. If I⊂R is a non-degenerate interval, we say that f:I→R is continuous at p∈I if

$$\lim_{x \to p} f(x) = f(p)$$

We say that f is a continuous map if f is continuous at every $p \in I$.

Definition. If X is a subset of the real numbers, we say a function $f:X \to R$ is uniformly continuous on X if,

for any ε>0, there exists a δ>0 such that for all x,y∈X, |x−y|<δ implies that |f(x)−f(y)|<ε.

Definition. Let I⊂R be an interval on the real line. A function f:I→R is said to be absolutely continuous on I if for every positive number ε, there is a positive number δ such that whenever a finite sequence of pairwise disjoint sub-intervals $(x_1,y_1),(x_2,y_2),\ldots,(x_n,y_n)$ of I satisfies

$$\sum_{k=1}^{n} (y_k - x_k) < \delta$$

then

$$\sum_{k=1}^{n} |f(y_k) - f(x_k)| < \varepsilon$$

Differentiability

A function f: R→R is differentiable at a if the limit

$$f'(a) = \lim_{x \to a} \frac{f(x) - f(a)}{x - a} \text{ exists}$$

Series convergence

$$\sum_{k=1}^{n} \frac{1}{2^k} = 1$$

$$\sum_{k=1}^{n} \frac{1}{k} = \infty$$

$$\sum_{k=1}^{n} \frac{(-1)^k}{k} = \log 2$$

Taylor series

The Taylor series of a real or complex-valued function $f(x)$ that is infinitely differentiable at a real or complex number a is the power series

$$f(x) = \sum_{i=0}^{k} \frac{f^i(a)}{i!}(x-a)^i$$

Fourier series

The Fourier series of a complex-valued P-periodic function $f(x)$, integrable over the interval [0,P] on the real line, is defined as a trigonometric series of the form

$$f(x) = \sum_{k=-\infty}^{\infty} c_k \exp(i\ 2\pi k\, x / P)$$

$$c_k = \frac{1}{P}\int_0^P f(x)\exp(-i\ 2\pi k\, x / P)\,dx$$

real form

$$f_N(x) = a_0 + \sum_{k=1}^{N}\left(a_k \cos(\ 2\pi k\, x / P) + b_k \sin(\ 2\pi k\, x / P)\right)$$

$$a_0 = \frac{1}{P}\int_0^P f(x)\,dx\ ,\ a_k = \frac{2}{P}\int_0^P f(x)\cos(\ 2\pi k\, x / P)\,dx\ ,\ b_k = \frac{2}{P}\int_0^P f(x)\sin(\ 2\pi k\, x / P)\,dx$$

Integration

We say that the Riemann integral of f on [a,b] is S if for any ε>0 there exists δ>0 such that,
for partition $\Delta_i = (x_{i+1} - x_i)$ $x_i \in [a,b]$ with mesh ‖Δi‖<δ , we have

$$\left| S - \sum_{k=1}^{n} f(x_i)\Delta_i \right| < \varepsilon$$

i.e. $\int_a^b f(x)\,dx = \lim_{n\to\infty} \sum_{i=1}^{n-1} f(x_i)(x_{i+1} - x_i)$ for $x_i \in [a,b]$

Important results

Bolzano-Weierstraß

The theorem states that each infinite bounded sequence in R_n has a convergent subsequence, i.e. R_n is locally compact.

Heine–Borel theorem

For a subset S of Euclidean space R_n , the following two statements are equivalent:

- S is compact, that is, every open cover of S has a finite subcover
- S is closed and bounded.

L'Hôpital's rule

$$\lim_{x \to c} \frac{f(x)}{g(x)} = \lim_{x \to c} \frac{f'(x)}{g'(x)}$$

where f′ and g′ are the derivatives of f and g .

Mean value theorem

Let f:[a,b]→R be a continuous function on the closed interval [a,b] , and differentiable on the open interval (a,b) , where a<b .

Then there exists $c \in [a,b]$ such that $f'(c) = \frac{f(b) - f(a)}{b - a}$

Taylor's theorem

Let k≥1 be an integer and let the function f:R→R be k times differentiable at the point a∈R .

Then there exists a function h_k:R→R such that

$$f(x) = \sum_{i=0}^{k} \frac{f^i(a)}{i!}(x-a)^i + h_k(x)$$

and remainder $h_k(x) = \frac{f^{k+1}(\xi)}{(k+1)!}(x-a)^{k+1}$, $\xi \in [a,x]$

$$\lim_{x \to a} h_k(x) = 0$$

Weierstrass approximation theorem

Let $f : [a,b] \to R$ be a continuous function.

If ε > 0 is given, then there exists a polynomial function p_n such that $|f(x) - p_n(x)| < \varepsilon$ for all $x \in [a,b]$

$$p_n(x) = \sum_{i=0}^{n} f\left(a + \frac{i}{n}(b-a)\right) B_{i,n}^{a,b}(x)$$

Here, the approximating polynomials are the Bernstein polynomials

$$B_{i,n}^{a,b}(x) = \frac{1}{(b-a)^n} \binom{n}{i} (x-a)^i (x-b)^{n-i}$$

with the error

$$\|f - p_n\| \le \frac{\pi}{2} \frac{1}{(n+1)^k} \|f^{(k)}\|$$

Fundamental theorem of calculus

Let f be a continuous real-valued function defined on a closed interval [a, b].

Let $F = I_a f$ be the function defined, for all x in [a, b], by

$$(I_a f)(x) = \int_a^x f(t)\,dt$$

Then F is uniformly continuous on [a, b] and differentiable on the open interval (a, b), and

$$(I_a f)'(x) = f(x)$$

for all x in (a, b) so F is an antiderivative of f.

Newton–Leibniz theorem

Let f be a real-valued function on a closed interval $[a,b]$ and F a continuous function on $[a,b]$ which is an antiderivative (inverse-derivative) of f in (a,b): $F'(x) = f(x)$

If f is Riemann integrable on $[a,b]$ then $F(b) - F(a) = \int_a^b f(t)\,dt$

Dini theorem

If X is a compact topological space, and $(f_n)n \in N$ is a monotonically increasing sequence (meaning $f_n(x) \le f_{n+1}(x)$ for all $n \in N$ and $x \in X$) of continuous real-valued functions on X which converges pointwise to a continuous function f:X→R , then the convergence is uniform.

Banach fixed-point theorem

Let (X,d) be a non-empty complete metric space with a contraction mapping $f: X \to X$

$d(f(x), f(y)) \le q\,d(x, y)$, q<1 , $x, y \in X$

Then f admits a unique fixed point $x_* \in X$, meaning $f(x_*) = x_*$

Furthermore, x_* can be found as follows:

start with $x_0 \in X$ and iterate

$x_{n+1} = f(x_n)$, then $x_n \to x_*$

Hahn-Banach theorem: functional with given values

Let $(x_i)i \in I$ be vectors in a real or complex normed space X and let $(c_i)i \in I$ be scalars also indexed by $I \neq \emptyset$.

There exists a continuous linear functional f on X such that $f(x_i) = c_i$ for all $i \in I$

if and only if there exists a K>0 such that for any choice of scalars $(s_i)i \in I$ where all but finitely many s_i are 0, the following holds:

$$\left|\sum_{i \in I} s_i c_i\right| < K \left|\sum_{i \in I} s_i x_i\right|$$ (linear form is low-bounded)

Stokes theorem

Let Σ be a smooth oriented surface in R_3 , parametrized by $\Sigma(u,v)$,

with boundary $\partial\Sigma \equiv \Gamma$, parametrized by $\Gamma(t)$.

If a vector field $F(x, y, z)$ has continuous first-order partial derivatives in Σ,

then

$$\iint_{\Sigma} (\nabla \times F) \cdot d\Sigma = \oint_{\partial\Sigma} F \cdot d\Gamma$$

Newton-Raphson approximation method

The Newton-Raphson method is a solution procedure for a zero α of a differentiable function f

$x_{n+1} = x_n - f(x_n) / f'(x_n)$

the error at n steps $\varepsilon_n = |\alpha - x_n|$, $\xi_n \in [x_n, \alpha]$

is $|\varepsilon_{n+1}| = \varepsilon_n{}^2 \frac{|f''(\xi_n)|}{2|f'(\xi_n)|}$, so the convergence is quadratic.

4 Complex analysis

[4]

Complex analysis, traditionally known as the **theory of functions of a complex variable**, is the branch of mathematical analysis that investigates functions of complex numbers.

Complex analysis features superior rigidity in comparison with real analysis—differentiability implies infinite differentiability (analyticity)—unlike real analysis where derivatives may not be continuous.

Complex functions that are differentiable at every point of an open subset Ω of the complex plane are said to be holomorphic on Ω. In the context of complex analysis, the derivative of f at z_0 is defined to be

$$f'(z_0) = \lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0}$$

Important results

Great Picard's Theorem

If an analytic function f has an essential singularity at a point w, then on any punctured neighborhood of w, $f(z)$ takes on all possible complex values, with at most a single exception, infinitely often.

Laurent series

The Laurent series for a complex function $f(z)$ about a point c is given by

$$f(z) = \sum_{k=-\infty}^{\infty} a_k (z-c)^k$$

where a_n and c are constants, with a_n defined by a line integral that generalizes Cauchy's integral formula:

$$a_k = \frac{1}{2\pi i} \oint_{\gamma} \frac{f(z)}{(z-c)^{k+1}} dz$$

The path of integration γ is counterclockwise around a curve enclosing c and lying in an annulus A in which f (z) is holomorphic (=analytic).

Liouville's theorem

A bounded function that is holomorphic in the entire complex plane must be constant.

Riemann mapping theorem

If U is a non-empty simply connected open subset of the complex number plane **C** which is not all of **C**, then there exists a biholomorphic mapping f from U onto the open unit disk

$$D = \{ z \in C \mid |z| < 1 \}$$

The map f is essentially unique: if z_0 is an element of U and φ is an arbitrary angle, then there exists precisely one f as above such that $f(z_0) = 0$ and such that the argument of the derivative of f at the point z_0 is equal to φ.

Runge's approximation theorem : approximation by rational functions

Denoting by C the set of complex numbers, let K be a closed subset of $C \cup \{\infty\}$ and let f be a function which is holomorphic on an open set containing K. If A is a set containing at least one complex number from every connected component of $C \cup \{\infty\} \setminus K$, then there exists a sequence (r_n) of rational functions which converges uniformly to f on K and such that all the poles of the functions (r_n) are in A.

5 P-adic numbers mathematical foundations

[1]

Ring of p-adic integers Z_p

A p-adic integer is a formal series with prime p

$a=\sum_{i\geq 0} a_i p^i$, as a list $a=\{a_0,a_1,a_2,...\}=S_p\left(\sum_{i\geq 0} a_i p^i\right)$

with integral coefficients a_i satisfying

$0\leq a_i \leq p-1$

Addition

with addition mod(p) with carry

$a+b \bmod(p)=\{a_0,a_1,a_2,...\}+_{p,c}\{b_0,b_1,b_2,...\}$

where $a+b \bmod(p)=S_p(a+b)$

with involution mapping $\sigma(a)=\sum_{i\geq 0}(p-1-a_i)\,p^i$

we have the additive inverse $-a=1+\sigma(a)$

specifically $-1=p-1$

negative p-adic numbers except -1 have the form $\{a_0,...,a_n,p-1,p-1,...\}$

Multiplication

Multiplication is multiplication mod(p) with carry

$a*b \bmod(p)=\{a_0,a_1,a_2,...\}*_{p,c}\{b_0,b_1,b_2,...\}$

where $a*b \bmod(p)=S_p(a*b)$

From this follows

$$\sum_{i\geq 0} p^i=\frac{1}{1-p}$$

Order

Order of $a=\{0,...,0,a_n,...\}=S_p\left(\sum_{i\geq n} a_i p^i\right)$ is $v(a)=n$ the index of lowest $a_i\neq 0$, $v(0)=0$

Properties:

$v(ab)=v(a)+v(b)$

$v(a+b)\geq \min(v(a),v(b))$

Ring of p-adic integers Z_p has no zero divisors

The group $Z_p^{\times}$ of invertible elements in the ring Z_p consists ofthe p-adic integers of order zero,

$$Z_p^{\times} = \left\{ a = \sum_{i \geq 0} a_i p^i \mid a_0 \neq 0 \right\}$$

with inverse a^{-1} with the properties

$b_0 = a_0^{-1} \bmod p$, $a_0 b_0 = 1 + k\,p$, $a \cdot b_0 = 1 + k\,p + \alpha b_0\,p = 1 + \kappa p$, $a^{-1} = b_0 (1 + \kappa p)^{-1}$, $(1 + \kappa p)^{-1} = 1 - \kappa p + (\kappa p)^2 \ldots$

The *p*-adic numbers are useful in solving Diophantine equations.

For example, the equation $x^2 = 2$ can easily be shown to have no solutions in the field of 2-adic numbers (we simply take the valuation of both sides). Because the 2-adic numbers contain the rationals as a subset, we can immediately see that the equation has no solutions in the rationals.

So we have an immediate proof of the irrationality of $\sqrt{2}$.

There is a common argument that is used in solving Diophantine equations:

in order to show that an equation has no solutions in Q, we show that it has no solutions in an extension field.

For another example, consider $x^2 + 1 = 0$. This equation has no solutions in Q because it has no solutions in the reals R , and Q is a subset of R.

Now consider the converse. Suppose we have an equation that does have solutions in R and in all the Q_p for every prime p.

Can we conclude that the equation has a solution in Q?

Unfortunately, in general, the answer is no, but there are classes of equations for which the answer is yes.

Such equations are said to satisfy the Hasse principle.

p-adic numbers Q_p form a non-Archimedean field

p-adic numbers Qp form a non-Archimedean field, meaning they violate the Archimedean property: large numbers do not inevitably accumulate to exceed a fixed value. They are based on a p-adic absolute value where magnitude depends on divisibility by a prime *p*, making small values those divisible by high powers of p .

Key Aspects of p-adic Non-Archimedean Structure:

The Ultrametric Inequality:

p-adic numbers satisfy a "strong" triangle inequality

$|x - y| \leq \max(|x|, |y|)$, rather than standard $|x - y| \leq |x| + |y|$.

Distance and Topology:

In p-adic metric spaces, all triangles are isosceles (two equal sides), and any point inside a ball is considered its center.

Non-Archimedean Valuation:

The p-adic valuation $|n|_p$ of any integer is $|n|_p \leq 1$ (ultrametric space)

Comparison with reals

Unlike real numbers, where 1+1+1+... exceeds any integer, adding numbers with small p-adic norm does not increase the total norm.

For instance, in p-adic numbers, 1+2+4+8+... does not diverge to infinity, it converges to -1.

p-adic numbers are totally disconnected

The p-adic numbers Q_p form a totally disconnected topological space, not a connected one. In contrast to the real number line, which is a single connected piece, the p-adic numbers have a structure similar to a Cantor set—they are broken into infinitely many separate, disjoint pieces.

Open and Closed Balls: Every p-adic ball is both open and closed (clopen).
Disjoint Sets: Given any two points $x, y \in Q_p$, you can find a clopen set containing x and not y, which breaks the space into disconnected sets

Comparison with Real Numbers
Real Numbers R :You cannot split R into two disjoint open sets without leaving gaps.
The intermediate values theorem (IVT) is valid
If $f:[a,b] \to R$ is continuous and y is between f(a) and f(b) : $y \in \left[f(a), f(b) \right]$, then there is some $c \in [a,b]$ with $y = f(c)$
p-adic numbers Q_p: Q_p can be partitioned into disjoint sets like $pZ_p, 1+pZ_p, \ldots$ without gaps, **IVT is not valid**
Fractal topology: p-adic integers Zp can be visualized as a infinitely branching tree rather than a line

p-adic integers Z_p

One way to think about *p*-adic integers is using "base *p*". For example, every integer can be written in base *p*, e.g.

$$50 = 1212_3 = 1 \cdot 3^3 + 2 \cdot 3^2 + 1 \cdot 3^1 + 2 \cdot 3^0$$

Informally, ***p*-adic integers** can be thought of as integers in base-*p*, but the digits extend *infinitely to the left*.

Complex p-adic numbers C_p
For *p* a prime number, the field of complex p-adic numbers C_p is to the p-adic numbers Q_p as the complex numbers C are to the real numbers.
Complex numbers C may be characterized as follows:
the standard absolute value (norm) on the rational numbers Q uniquely extends to an algebraic closure $\bar{Q}$, and the completion is the complex numbers.
In direct analogy with this: **algebraic closure $\bar{Q}_p$ is the field C_p**
The completion of the algebraic closure of a normed field is still algebraically closed.

Topological space Zp
Metric
Metric is based on p-adic valuation

$$a = \{a_0, a_1, \ldots\} = S_p\left(\sum_{i \geq n_1} a_i p^i \right), \; b = \{b_0, b_1, \ldots\} = S_p\left(\sum_{i \geq n_2} b_i p^i \right)$$

order $v(a) = n_1$ the index of lowest $a_i \neq 0$, $v(b) = n_2$, absolute value $|a| = p^{-v(a)}$
p-adic metric $d(a,b) = |a-b| = p^{-v(a-b)}$
Mapping Zp to Rn

The mapping $\psi_b(a)$ $a,b \in Z_p$ $b>=p$

$$\Psi_{b,p}\left(\sum_{i\geq 0} a_i p^i\right) = \vartheta \sum_{i\geq 0} \frac{a_i}{b^{i+1}} \quad \vartheta = \frac{b-1}{p-1}$$

is a continuous homomorphism $Z_p \to [0,1]$, injective for $b>p$.

$\Psi_{b,p}(a)$ gives a linear model of Zp in the interval [0, 1]; the image is a *fractal subset* A of this interval.

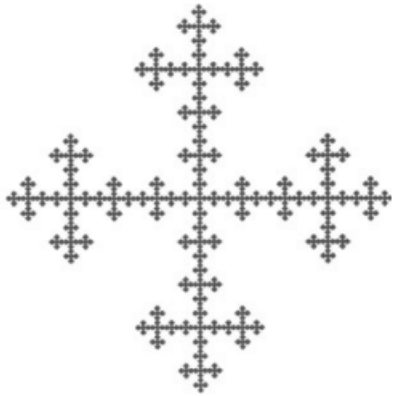
With the mapping $v : S = \{0,1,2,...p-1\} \to R^n$, $v(S) = \Sigma \subset R^n$

we obtain a vector map

$$\Psi_{v,b} : Z_p \to R^n \ , \ \sum_{i\geq 0} a_i p^i \to \vartheta \sum_{i\geq 0} \frac{v(a_i)}{b^{i+1}}, \ \vartheta = b-1$$

The image $F_{v,b} = \Psi_{v,b}(Z_p)$, and $F = \bigcup_{v\in\Sigma}\left(\vartheta \frac{v}{b} + \frac{F}{b}\right)$, defines a sequence if images converging to a complete fractal image of Zp .

Example: p = 5, n=2, V = R^2, and the map v defined by
v(0) = (0,0), v(1) = (1,0), v(2) = (0,1), v(3) = (-1,0), v(4) = (0, -1)
The image of Ψ, is a union of the similar subsets
$\Psi(k + pZ_p)$ 0<=k<=4



Fractal image of Z_5 in R^2 [1]

Topology and continuity

Z_p is a topological ring, i.e. addition, multiplication and inverse-map are continuous in the p-adic metrics.
The mapping

$$x = \sum a_i p^i \to \lim_{n\to\infty}(x \bmod p^n) = \lim_{n\to\infty}\left(\sum_{i<n} a_i p^i\right) \ , \ Z_p \to \lim_{n\to\infty} Z / p^n Z$$

is a continous ring isomorphism.

Balls of Zp

The ball $B_r(a) = \left\{ d_p(x,a) = |x-a|_p < r \right\}$ is uniquely determined by

$a = a_0 + a_1 p + ... + a_n p^n + ...$ and $r = p^{-n}$

$B_r(a)$ is the same as $B_{r'}(a)$ for r'>r .

The Field Qp of p-adic Numbers

In Q_p, every element x may be written in a unique way as

$$x = \sum_{i=k}^{\infty} a_i p^i$$

where k is some integer such that $a_k \neq 0$ and each a_i is in $\{0, \ldots, p-1\}$.

with integral and fractional part decomposition $Q_p = Z_p + Z[1/p]$

with the denominations

integral part $[x] = \sum_{i \geq 0} a_i p^i \in Z_p$

fractional part $\langle x \rangle = \sum_{i<0} a_i p^i \in Z[1/p]$

i.e. Q_p admits a partition into clopen balls

$\{x + Z_p\} = \{\langle x \rangle + y \mid y = [x] \in Z_p\}$

Proposition The map $\tau : Q_p \to C^x \quad x \mapsto \exp(2\pi i \langle x \rangle)$ is a homomorphism.

It defines an isomorphism $Q_p / Z_p \cong \mu_{p^\infty}$ of the additive group Q_p/Z_p with the group of p-th power roots of unity in the complex field C.

Hensel's principles

First principle: zeros of polynomials

Let P(X, Y) ∈ Z[X, Y] be a polynomial with integral coefficients

Proposition The following properties are equivalent

- P=0 has a solution in Z_p
- for all n>= 0, P=0 has a solution in Z_p/p^nZ
- for all n>= 0, there are integers a_n b_n such that $P(a_n, b_n) = 0 \bmod (p^n)$

Second principle: Newton method for zeros

P(X) ∈ Z[X] , integer x, with $P(x)=0 \bmod p$, i.e. $P(a_0)= p\,t$
then for some integer b

$$P(a_0 + a_1 p) = P(a_0) + P'(a_0)\,a_1 p + (a_1 p)^2\, b$$

we have the Newton approximation method

$$\hat{x} = a_0 + a_1 p = a_0 - \frac{p\,t}{P'(a_0)} = x - P(a_0)/P'(a_0)$$

$$a_1 = -t/P'(a_0) \bmod (p)$$

and $P(\hat{x}) = P(a_0 + a_1 p) = 0 \bmod (p^2)$

Newton iteration $\hat{x}(x)$

Proposition Let P∈ Z_p[X] and x∈ Z_p be such that $P(x) = 0 \bmod (p^n)$

If $k = v(P'(x)) < n/2$ then $\hat{x}(x) = N_p(x) = x - P(x)/P'(x)$ satisfies

- $P(\hat{x}) = 0 \bmod (p^{n+1})$ improvement
- $\hat{x} = x \bmod (p^{n-k})$ controlled loss
- $v(P'(\hat{x})) = v(P'(x)) = k$ invitation to iteration

Example: Newton algorithm for roots of polynomial p(x)=x^2-2, i.e. $\sqrt{2}$ [2]
error in p-adic half-norm

start value $x_0 = 7/5$, x_{p0}= {-1, {2, 1, 0, 0, 0, 0, 0, 0, 0, 0}}

iter=1, in Q $x_1 = 99/70$ error $|p(x_1)|$=1/4900 , in Q_p x_{p1}= {-1, {1, 9, 0, 4, 2, 3, 11, 15, 4, 10}} error $|p(x_{p1})|_{hp}$=0.001397

iter=2, in Q $x_1 = 19601/13660$ error $|p(x_1)|$=5.2 10^{-9} , in Q_p x_{p1}= {-1, {9, 4, 1, 10, 13, 12, 14, 0, 11, 16}} error $|p(x_{p1})|_{hp}$ = 0.000778

Reduction of zeros mod(p^n) to mod(p^{n-k})
Theorem Hensel's Lemma
Let P∈ Z_p[X] and x∈ Z_p satisfy $P(x) = 0 \bmod (p^n)$

If $k = v(P'(x)) < n/2$, the there exist a unique root of P, ξ∈ Z_p such that

$\xi = x \bmod (p^{n-k})$ and $v(P'(\xi)) = v(P'(x)) = k$

ξ is the unique root satisfying the apriori weaker congruence
$\xi = x \bmod (p^{k+1})$

Recovering rationals from p-adic

Recovering a rational number (a/b) from its (p)-adic expansion $\frac{a}{b}=\sum a_i p^i$ is achieved by finding a rational approximation (N/D) that matches the first *n* digits of the expansion. This is typically done using the Euclidean algorithm to solve $a_i=\frac{N}{D}\bmod\left(p^n\right)$ or by recognizing a repeating p-adic digit sequence.

Euclidean Algorithm (Rational Reconstruction)

Given a (p)-adic truncated number $x=t+O\left(p^n\right)$, search for a rational (u/v) such that $\frac{u}{v}=t\bmod\left(p^n\right)$.

The Extended Euclidean Algorithm on (p^n, t) yields a sequence of remainders (r_n).

When a remainder becomes smaller than $r_n<\sqrt{p^n/2}$, it can be identified as a potential numerator or denominator.

Calculation with period=repeating sequence

p-adic representation of a rational x=p^v a/b, we obtain the result

$x_p=\left\{v,\left\{a_1,...,a_{n-1},\overline{a}_n,...,\overline{a}_{n+L-1}\right\}\right\}$

with period $\overline{a}_n,...,\overline{a}_{n+L-1}$ start position *n*, and period length *L* .

We obtain the rational *x* from x_p in the form $x=f_{rat}(x_p,n,L)$

$$x=p^v\left(\sum_{i=1}^{n-1}a_i p^{i-1}-\frac{\sum_{i=n}^{n+L-1}a_i p^{i-1}}{p^L-1}\right)$$

For precision *N* digits , and for rationals $|x|<p$ and long periods *L>N* , we can approximate

n=1 , L=N-1

6 Finite extensions of Qp

[1]

The field Qp is not algebraically closed: It admits algebraic extensions of arbitrarily large degrees. These extensions are the p-adic fields to be studied here. Each one is a finite-dimensional, hence locally compact, normed space over Q_p .

Structure of p-adic fieds

Square roots p>2

For $a\in Q_p$ *1<a<p* , *a* not being a square

then $Q_p\left(\sqrt{a}\right)$, $Q_p\left(\sqrt{p}\right)$, $Q_p\left(\sqrt{ap}\right)$, are the only quadratic extensions of Q_p

Square roots p=2

all seven quadratic extensions of Q_p are

$$Q_2\left(\sqrt{-1}\right),\ Q_2\left(\sqrt{\pm 5}\right),\ Q_2\left(\sqrt{\pm 2}\right),\ Q_2\left(\sqrt{\pm 10}\right)$$

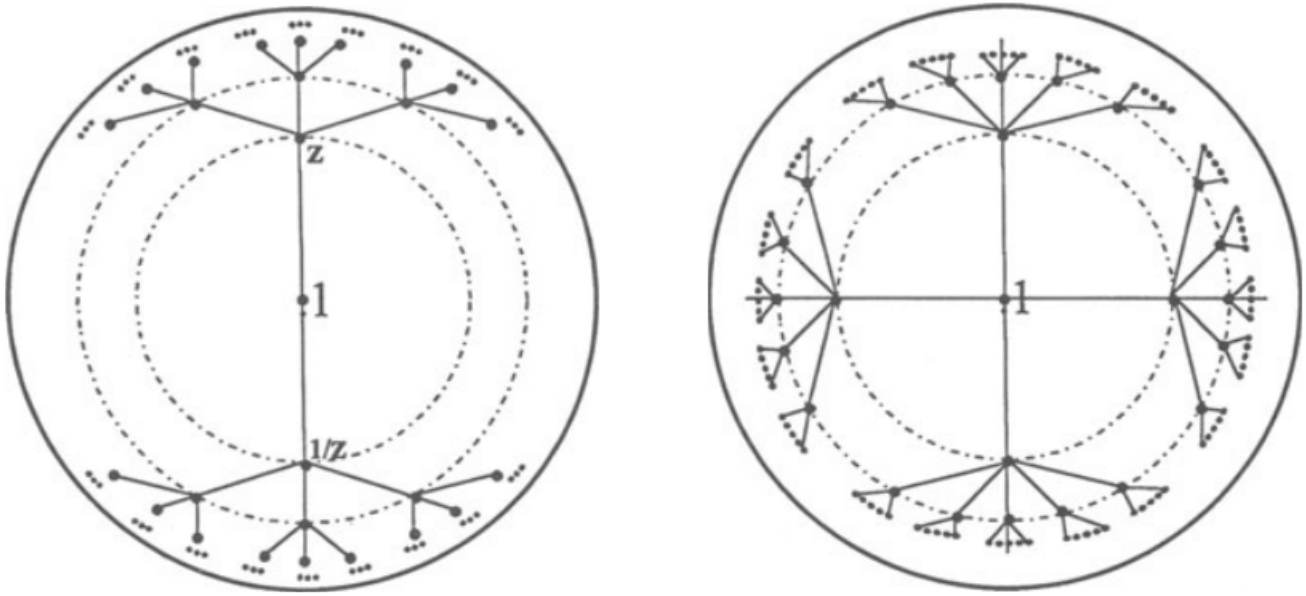
Roots of unity ξ with $\xi^n = 1$

Roots of unity

If p>2, group of roots of unity in Q_p are the p-1 roots of $x^{p-1} = 1$

and $\sqrt{-1} \in Q_p \Leftrightarrow 4 \mid p-1 \Leftrightarrow p = 1 \bmod 4$

If p=2, group of roots of unity in Q_p are ± 1



Location of the p^nth roots ofunity on the unit sphere (p = 3 and 5) [1]

Automorphisms

Theorem The only automorphism of Q_p is the identity.

The only algebraic automorphism ofthe real field *R* is the identity

Gaussian integers

$Z(i) = Z \oplus iZ \subset C$

with base element $b = i(i+1)$, $S = \{0,1\}$

Proposition

The elements of Z_2[i] admitting a finite expansion $\sum_{j=0}^{n} a_j b^j$, $a_j \in S$,

in base *b* are precisely the Gaussian integers, with

$$Z(i) = \left\{ \sum_{i=0}^{n} a_i b^j \right\}$$

Gaussian rationals

The field of Gaussian rationals provides an example of an algebraic number field that is both a quadratic field $Q\left(\sqrt{d}\right)$ and a cyclotomic field $Q(\zeta_n)$, $\zeta_n = e^{2\pi i/n}$.

Like all quadratic fields it is a Galois extension of **Q** with Galois group cyclic of order two, in this case generated $Q(\zeta_n)$ by complex conjugation.

As with cyclotomic fields more generally, the field of Gaussian rationals is neither ordered nor complete (as a metric space).
The Gaussian integers Z(i) form the ring of integers of Q(i). The set of all Gaussian rationals is countably infinite.
The field of Gaussian rationals is also a two-dimensional vector space over Q with natural basis {1,i}.

Hexagonal field of 3-adic numbers

$K = Q_3\left(\sqrt{-3}\right)$

contains $\zeta = \left(1+\sqrt{-3}\right)/2$ is root of unity order 6

Proposition

Let $b = \sqrt{-3}$, $\zeta = \left(1+\sqrt{-3}\right)/2$, $S = \{0,1,\zeta\}$

Then the finite sums $\sum_{J} a_j b^j$, $a_j \in S$, fill up the hexagonal lattice $Z(\zeta)$ in C

7 Complete p-adic fields

[1]

In order to be able to define K-valued functions by means of series (mainly power series), we have to assurne that K is complete.
It turns out that the algebraic closure Q_a^p is not complete, so we shall consider its completion C_p :This field turns out to be algebraically closed and is a natural domain for the study of "analytic functions ".
However, this field is not spherically complete, Hahn-Banach theorem is not valid.
In functional analysis, the **Hahn–Banach theorem** is a central result that allows the extension of bounded linear functionals defined on a vector subspace to the whole space.
Given a collection $(f_i)_{i\in I}$ of bounded linear functionals on a normed space X and a collection of scalars $(c_i)_{i\in I}$, determine if there is an x∈X such that $f_i(x) = c_i$ for all i∈I.

This is a reason for enlarging Q_a^p in a more radical way than just completion, and we shall construct a spherically complete, algebraically closed field Ω_p (containing Q_a^p and C_p) having still another convenient property, namely $|\Omega_p| = R_{\geq 0}$.

This ensures that all spheres of positive radius in Ω_p are non-empty

$B_{<r}(a) \neq B_{\leq r}(a)$ for r>0

The Algebraic Closure Q_a^p of Q_p

- Closure Q_a^p has infinite extension over Q_p

because: polynomial $x^e - p$ is irreducible, defines an extension of degree e .

- Closure Q_a^p is a separable metric space (dense subspace Q_p)

A separable metric space is a metric space (X,d) with a dense countable subspace S.

- The absolute values of algebraic numbers over Q_p are fractional powers of p
- The space is Q_a^p neither complete nor locally compact

(locally compact =every point of X has a compact (= closed and bounded) neighbourhood.)

Continuity of polynomial roots

Theorem Continuity of roots of equations

Let be K a finite extension of Q_p, given $a \in Q_p^a$ root of a monic (highest coefficient 1) polynomial $f \in K[X]$ of degree n .

Then there is ε>0, so that for any monic polynomial $g \in K[X]$ of degree n with $\|g - f\| < \varepsilon$,

g has a root b generating this field:

$K(b) = K(a)$

where polynomial norm $\|f\| = \max_{i \leq n} |a_i|$ for $f(X) = \sum_{i \leq n} a_i X^i$

Corollary

For a monic polynomial $f \in K[X]$ of degree n with root a, and (g_i) sequence of monic polynomials which converges coefficientwise $\|g_i - f\| \to 0$,

then there is a sequence of roots $x_i = root(g_i)$ with $x_i \in K(a)$ convergent to a : $|x_i - a|_p \to 0$

Theorem Finitely many extensions of Q_p

Let be K a finite extension of Q_p, then there are finitely many extensions of Q_p of degree n in Q_a^p .

Ramified extensions (disconnected in n components)

If we add a primitive p-th root of unity $\zeta_p = \sqrt[p]{1}$ to Q_p , we obtain a disconnected extension of degree *p-1* .

K/ Q_p is disconnected in *p-1* components, and is generated by $\sqrt[p-1]{-p}$

The universal p-adic field Ω_p

R (real numbers) is the normed ring of bounded sequences $\alpha = (\alpha_i)$, $\alpha_i \in Q_a^p$, with norm $\|\alpha\| = \sup_i |\alpha_i|$

For U=filter of low-bounded ∞-sets in N, $U=\{[n,\infty)\,|\,n\in N\}$

Each bounded sequence of real numbers $\alpha=(\alpha_i)$ has a limit along U, and $a=\varphi(\alpha)=\lim_U|\alpha_i|<\infty$ is finite.

Proposition1 Closure Ω_p of Q_a^p

$J=\varphi^{-1}(0)$ is a maximal ideal of R, and the field $\Omega_p=R/J$ is an extension of the field Q_a^p.

Ω_p = set of bounded finite sequences α in Q_a^p with absolute value $|a|=\varphi(\alpha)=\lim_U\alpha_i>0$

Proposition2: For the non-zero $|\Omega_p^\times|=R_{>0}$, i.e. absolute values cover all reals.

Proposition3: Ω_p is algebraically closed

Proposition4: Ω_p is spherically complete

Definition: An ultrametric space X is called spherically complete when all decreasing sequences of closed balls have a nonempty intersection

Completion C_p of field Q_a^p

Definition $C_p=\bar{Q}_p^a$ is the metric completion (limit of series in Q_a^p)

Properties

C_p is separable metric space

C_p is not locally compact

The field C_p is algebraically closed

The field C_p is not spherically complete

The field C_p has the cardinality of the continuum

The fields C and C_p are isomorphic.

$A_p=\{x\in C_p\,|\,|x|\le 1\}$ unit ball is maximal subring of C_p

$M_p=\{x\in C_p\,|\,|x|<1\}$ unit ball is maximal ideal of A_p

$U(1)=\{x\in C_p\,|\,|x|=1\}\subset C_p^\times$ unit sphere

$U(1)=A_p-M_p\subset C_p^\times$

$\mu=\mu(C_p)$ group of roots of unity in the complex field C_p

F_{p^∞} is the algebraic closure of Galois field F_p

$\mu=\mu_{(p)}\cdot\mu_{p^\infty}$, $U(1)\cong\mu_{(p)}\times(1+M_p)$

where $\mu_{(p)}$ subgroup roots of unity of order prime to p, μ_{p^∞} subgroup of the p-th power roots ofunity (in C_p).

Projection $U(1)\to\mu_{(p)}$ is the Teichmüller character

Field $\supset B_{\leq 1} \supset B_{<1}$	Residue field	Nonzero $\lvert . \rvert$	Properties
$\mathbf{Q}_p \supset \mathbf{Z}_p \supset p\mathbf{Z}_p$	$\mathbf{F}_p$	$p^{\mathbf{Z}}$	locally compact
$K \supset R \supset P = \pi R$	$\mathbf{F}_q$ $(q = p^f)$	$\lvert\pi\rvert^{\mathbf{Z}} = p^{\frac{1}{e}\mathbf{Z}}$	$\begin{cases} ef = \dim_{\mathbf{Q}_p} K < \infty \\ \text{locally compact} \end{cases}$
$\mathbf{Q}_p^a \supset A^a \supset M^a$	$k^a = \mathbf{F}_p^a = \mathbf{F}_{p^\infty}$	$p^{\mathbf{Q}}$	$\begin{cases} \text{algebraically closed} \\ \text{not locally compact} \end{cases}$
$\mathbf{C}_p \supset \mathbf{A}_p \supset \mathbf{M}_p$	$\mathbf{F}_p^a = \mathbf{F}_{p^\infty}$	$p^{\mathbf{Q}}$	$\begin{cases} \text{algebraically closed} \\ \text{complete} \end{cases}$
$\Omega_p \supset A_\Omega \supset M_\Omega$	k_Ω uncountable	$\mathbf{R}_{>0}$	$\begin{cases} \text{algebraically closed} \\ \text{spherically complete} \end{cases}$

$\varphi(n) = p^n \in C_p^\times$, $Q \to C_p^\times$ is an injective homomorphism

Theorem Roots of unity

$\zeta \in \mu_{p^\infty} \subset C_p$ roots of unity of order p^t t>=1, then

$|\zeta - 1| = |p|^{1/\varphi(p^t)} < 1$, where $\varphi(p^t) = p^{t-1}(p-1)$

First Inequality

Denote by I = (p , T) the ideal of the ring Z[T] generated by the prime p and the variable T .

Then $(1+T)^{p^n} - 1 \in T \cdot I^n$, $n \geq 0$

Second Inequality Let $t \in C_p$, $|t| \leq 1$

Then $\left|(1+T)t^{p^n} - 1\right| \leq |t| \max\left(|t|, |p|\right)^n$, $n \geq 0$

Third Inequality

K finite extension of Q_p , $K \supset R \supset P$

Then $(1+P)^{p^n} \subset 1 + P^{n+1}$, $n \geq 0$

Proposition Torsion in $C_p^{\ x}$

For $x \in C_p$, $x \in 1 + M_p \Leftrightarrow \lim_{n\to\infty} x^{p^n} = 1$

8 Continuous functions on Qp and Zp

[1]

Since Q_p admits a partition into clopen balls

$B_{Z_p}(x) = x + Z_p = \{x \in Q_p / Z_p\}$

it is enough to study continuous functions on Zp .

Thus, we shall typically study continuous functions $Z_p \to C_p$

Since the natural numbers N form a dense subset of the ring Z_p , we shall start by the study of functions on N or Z and with values in any abelian group.

• In classical analysis, real- or complex-valued functions that are continuous on an interval can be uniformly approximated by polynomial functions (theorem of Weierstrass), but there is no canonical series representation for them.

It is a specific feature of p-adic analysis that continuous functions $C(Z_p; C_p)$: $Z_p \to C_p$ have a canonical Mahler series representation.

Definition of the Mahler Series

Any continuous function $f \in C(Z_p, Q_p)$ can be uniquely expanded in the form $f(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n}$, where

$\binom{x}{n} = \frac{x(x-1)...(x-n+1)}{n!}$ are the binomial coefficient polynomials

and the Mahler coefficients are defined by $a_n = \nabla^n f(0)$, with forward difference operator $\nabla f(x) = f(x+1) - f(x)$

the series is uniformly convergent with $\lim_{n \to \infty} a_n = 0$

• Due to the granular structure of Zp, the *locally constant functions* also constitute a dense subspace of $C(Z_p; C_p)$

These functions correspond to the *step functions* on an interval in the classical theory.

Functions of an Integer Variable

Polynomial $f(x) \in Q[x]$ can take integer values:

$\frac{1}{p}x^p - \frac{1}{p}x$ for prime p, more general binomial polynomial $\binom{x}{n}$ $n \geq 0$

forward-difference operator on the binomial functions $\nabla f(x) = f(x+1) - f(x)$

$\nabla \binom{x}{0} = 0$, $\nabla \binom{x}{i} = \binom{x}{i-1}$ $i \geq 1$

compare: the **differential operator** *D* on x-powers $x^i / i!$

$D(x^0) = 0$, $D\left(\frac{x^i}{i!}\right) = \frac{x^{i-1}}{(i-1)!}$ $i \geq 1$

Mahler series

Theorem

Let be $f : Z_p \to C_p$ arbitrary map.

Then there is a unique sequence $(a_i)_{i\geq 0} \in C_p$ such that

$$f(x) = \sum_{x\geq i\geq 0} a_i \binom{x}{i} \quad a_i = \nabla^i f(0)$$

$$\binom{x}{i} = \frac{x(x-1)\ldots(x-i+1)}{i!}$$ binomial polynomials

forward difference operator $\nabla f(x) = f(x+1) - f(x)$

Mahler series $f(x) = \sum_{x\geq i\geq 0} \nabla^i f(0) \binom{x}{i}$

analogous to classical analysis Taylor series $f(x) = \sum_{i=0}^{k} \frac{f^i(a)}{i!}(x-a)^i$

Integer-valued polynomials on Z

Theorem : Module of polynomial functions $L = L(Z) \subset Q[x]$ integer-valued on *N* is generated by the binomial polynomials $\sum m_i \binom{x}{i}$

Corollary If a polynomial $P \in Q[x]$ with degree d>=0 takes integral values on d+1 consecutive integers, then takes integral values on all integers.

Periodic functions on Z

For a finite (Galois) field F_p

Proposition

For $i < p^t$, the functions $\binom{\cdot}{i} : Z \to F_p$, $x \mapsto \binom{x}{i} \bmod(p)$ are periodic of period $T=p^t$.

They form a base of space of T-periodic maps.

Theorem

Le *M* be a vector space over F_p , and $f : Z \to M$ periodic function of period $T=p^t$.

Then f can be uniquely written in the form

$$f(x) = \sum_{T\geq i\geq 0} a_i \binom{x}{i}$$

Indefinite sum functions on Z

- ∇ is to be compared to the derivation operation D
- sum operator $Sf(x) = F(x)$, $F(n) = \sum_{0\leq i\leq n} f(i)$ is the inverse in comparison to the integration operator $\int f(x)dx$

Examples sum operator
f=1 , S1(n)=n

f=Id , $Sf(n)=\sum_{i<n} i=\binom{n}{2}=\frac{n(n-1)}{2}$

$f(n)=\binom{n}{k}$ binomial polynomial, $S\binom{n}{k-1}=\binom{n}{k}\quad k\geq 1$

$f(n)=n^2$, $Sf(n)=2\binom{n}{3}+\binom{n}{2}$

Proposition 1

$f(n)=\sum_{i\geq 0} c_i\binom{n}{i}$, $Sf(n)=\sum_{i\geq 0} c_i\binom{n}{i+1}$

Proposition 2 combination

$\nabla\circ S=id$, $S\circ\nabla=id-P_0$, $\nabla\circ S-S\circ\nabla=P_0$

where zero value operator $P_0 f=f(0)id$

Shifted convolution

Functions $f,g:Z\to Z_p$, shifted convolution product is

$f\underline{*}g(n)=\sum_{i+j=n-1} f(i)g(j)$

Theorem Mahler expansion with remainder
For every function f on Z and every integer n>=0, we have

Mahler series $f(x)=\sum_{x\geq i\geq 0}\nabla^i f(0)\binom{x}{i}$

$f(x)=f(0)\cdot 1+\nabla^1 f(0)\binom{x}{1}+\nabla^2 f(0)\binom{x}{2}+\ldots+\nabla^n f(0)\binom{x}{n}+R_{n+1}f$

with van-Hamme remainder $R_{n+1}f=\nabla^{n+1}f\,\underline{*}\binom{x}{n}$

Continuous Functions on Zp

Uniform convergence

Theorem. Let *X* be a topological space, *M* a complete metric space with metric d_M, and $(f_n)_{n\geq 0}$ sequence of continuous functions $X\to M$,
with metrics

$d(f_m, f_n) = \sup_{x \in X} d_M(f_m, f_n) \to 0$ for $m, n \to \infty$ (Cauchy criterion)

then $\lim_d f_n = f$ is a continuous function $X \to M$

Polynomial approximation for functions on Zp

For a continuous function f: Zp→R, consider continuous injection φ: Zp→R (e.g. canonical embedding), then f can be uniforrnly approximated by polynomial expressions in φ (Stone-Weierstrass)

Maximum of a continuous function is attained

continuous function f: $Z_p \to C_p$, then for $|f| : Z_p \to R$ the supremum is attained $\exists x \in Z_p, \sup_{Z_p} |f| = f(x)$

Examples of p-adic continuous functions on Zp

- polynomial $f \in C_p[X]$ is a continuous function f: Zp→Cp
- $x \in Z_p \to |x| \le 1$, so power series $f(x) = \sum_{i \ge 0} a_i x^i$ with $a_i \in C_p$, $|a_i| \to 0$ converges uniformly and f: Zp→Cp is a continous function.

The norm is defined by $\|f\| = \sup_{x \in Z_p} |f(x)| = \max_{x \in Z_p} |f(x)| < \infty$

- $f(x) = \sum_{i \ge 0} a_i p^{2i}$, $x = \sum_{i \ge 0} a_i p^i$, is continuous and differentiable everywhere, $f' \equiv 0$, with $|f(x) - f(y)| = |x - y|^2$

but f is not locally constant.

- $f(x) = \sum_{i \ge 0} a_i p^{mi}$, $x = \sum_{i \ge 0} a_i p^i$, is continuous and differentiable everywhere, $f' \equiv 0$, with $|f(x) - f(y)| = |x - y|^2$

but f is not locally constant.

Mahler series

binomial polynomials define continuous functions

$b_k(x) = \binom{x}{k}$, $\|b_k\| = 1$

Mahler series: $\sum_{i \ge 0} a_i b_i(x)$, $a_i \in C_p$, $|a_i| \to 0$

Example:

$\sum_{k \ge 0} t^k \binom{x}{k}$, $t \in C_p$, $|t| < 1$ converges uniformly to continuous $f : Z_p \to C_p$, $f(x) = \sum_{i \ge 0} t^i \binom{x}{i} = (1+t)^x$,

Mahler theorem

Theorem 1

Let $f : Z_p \to C_p$ continuous, $a_k = \nabla^k f(0)$, then

$|a_k|_p \to 0,\ \sum_{x \geq k \geq 0} a_k \binom{x}{k} \to f(x)$ uniformly convergent, and $\|f\| \leq \sup_{k \geq 0} |a_k|_p$

Theorem 2

Let $f : Z_p \to C_p$ continuous, $a_k = \nabla^k f(0)$, then the following properties are equivalent

- $|a_k|_p \to 0$
- $\sum_{x \geq k \geq 0} a_k \binom{x}{k} \to f(x)$ uniformly convergent
- f(x) uniformly continuous
- $\|\nabla^k f\| \to 0$

Theorem 3 extension on Q_p

Let $f : Q_p \to C_p$ continuous, $a_k = \nabla^k f(0)$, then

$|a_k|_p \to 0,\ \sum_{x \geq k \geq 0} a_k \binom{x}{k} \to f(x)$ uniformly convergent, and $\|f\| \leq \sup_{k \geq 0} |a_k|_p$

Corollary1: any continuous $f : Z_p \to C_p$ has limited Mahler expansion

$$\sum_{x \geq k \geq 0} a_k \binom{x}{k} \to f(x)$$

$$f(x) = f(0) \cdot 1 + \nabla^1 f(0) \binom{x}{1} + \nabla^2 f(0) \binom{x}{2} + \ldots + \nabla^n f(0) \binom{x}{n} + R_{n+1} f$$

with van-Hamme remainder $R_{n+1} f = \nabla^{n+1} f \stackrel{*}{-} \binom{x}{n}$, $\|R_{n+1} f\| = \|\nabla^{n+1} f\| \to 0$, $n \to \infty$

with the van Hamme form of the remainder

a_k satisfy

$$\sum_{k \geq 0} a_k \binom{x}{k} = \exp(-x) \sum_{k \geq 0} f(k) \frac{x^k}{k!}$$

shifted convolution

$$f \stackrel{*}{-} g(n) = \sum_{i+j=n-1} f(i) g(j),\ |f \stackrel{*}{-} g(n)| \leq \max_{i+j=n-1} |f(i)\, g(j)| \leq \|f\| \|g\| ,\ \|f \stackrel{*}{-} g\| \leq \|f\| \|g\|$$

Proposition

Let f, g be two contnous functions $f, g : Z_p \to C_p$

Then shifted convolution $f \stackrel{*}{-} g : Z_p \to C_p$ is continuous

Corollary 2: For any continuous function $f:Z_p \to C_p \quad f(x)=\sum_{k\geq 0} a_k \binom{x}{k}$ the indefinite sum $Sf = f \stackrel{*}{-} 1$ is a continuous function

$Sf(x) = 1 \stackrel{*}{-} f = \sum_{k\geq 0} a_k \binom{x}{k+1}$, $\|Sf\| \leq \|f\|$

Corollary 3: The only linear form $\varphi : C(Z_p, K) \to K$ that is invariant under translation is the trivial one $\varphi = 0$

Example: $F(x) \to F(x+1)$

Corollary 4: $\sigma(x) = -1-x$, $\sigma : Z_p \to Z_p$, $S(f \circ \sigma)(x) = -Sf(-x)$

Example:

$a = 1+t \in C_p$

$f(x) = a^x = (1+t)^x = \sum_{k\geq 0} t^k \binom{x}{k}$

$Sf(x) = \sum_{k\geq 0} t^k \binom{x}{k+1} = \frac{(1+t)^x - 1}{t} = \frac{a^x - 1}{a-1}$

Locally constant functions on Zp

F_j =Locally constant functions on closed balls of radius $r_j = 1/p^j$

$F_j = F(Z / p^j Z) = F(Z_p / p^j Z_p) \subset F^c(Z_p)$

The length of an integer i>= 1 is the integer v = v(i)>=1 , which is the *highest non-zero coefficient* in p-adic expansion.

for integer n , $n_- = n - n_{v-1} p^{v-1}$ obtained by deleting its top digit in base p .

ψ_l characteristic function of ball $B_l = l + p^v Z_p$

Van-der-Putt expansion of functions on Zp

Proposition

If $f = \sum_i a_i \psi_i \in F_j$ locally constant function f: $Z_p \to \bar{Q}_p$,

then $a_0 = f(0)$, $a_n = f(n) - f(n_-)$ for $n>0$

and $\|f\| = \max_i |a_i| = \sup_i |a_i|$

Van-der-Putt theorem

Continuous function $f : Z_p \to \bar{Q}_p$,

$a_0 = f(0)$, $a_n = f(n) - f(n_-)$ for $n>0$

$n_- = n - n_{v-1} p^{v-1}$ obtained by deleting its top digit in base p

Then $|a_n| \to 0$, $\sum_n a_n$ converges uniformly to f, and $\|f\| = \max_i |a_i| = \sup_i |a_i|$

9 P-adic differentiation and integration

[1]

Differentiability

Definition For $f : X \to K$, X a ring, K a field , the sup-norm of is $\|f\|_s = \sup_{x \in X} |f(x)|$

Definition For $f : X \to K$, power series $f(x) = \sum_{k \geq 0} a_k x^k$, the Gauss norm of is $\|f\|_G = \sup_k |a_k|$

Definition We say that f is strictly differentiable at a point $a \in X$ and denote this property by $f \in S^1(a)$ if the difference quotients

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

have a limit $f'(a) = \lim_{(x,y) \to (a,a)} \Phi f(x, y)$

Then in a neighborhood V: $|f(x) - f(y)| = |f'(a)| |x - y|$ for $(x, y) \in V \times V$

Proposition

For $f : X \to K$, X a ring, K a field, the following properties are equivalent

- $f \in S^1(a)$ for all $a \in X$
- the function $\Phi f(x, y)$ defined on $X \times X - \Delta_X$ has a continuous extension on $X \times X$
- f is differentiable at every point $a \in X$, and there is a continuous function α on $X \times X$, vanishing on Δ_X

with $f(y) = f(x) + (y - x) f'(x) + (y - x) \alpha(x, y)$ for $x, y \in X$

Theorem

Let f be a continuous function on Z_p.

Then f is differentiable at y precisely when $(\nabla^k f)(y) / k \underset{k \to \infty}{\to} 0$

Then $f'(y) = \sum_{k \geq 1} (-1)^{k-1} (\nabla^k f)(y) / k$

Definition $f : X \to K$ is Lipschitz, when its differential quotient is uniformly bounded

$|f(x) - f(y)| = M |x - y|$ for $x, y \in X$

$|f(x) - f(y)| = M |x - y|$, $M \leq \|\Phi f\|_s$

binomial polynomials are Lipschitz : For $k \geq 1$ and $p^j \leq k \leq p^{j+1}$ we have

$$\left|\binom{x}{k}-\binom{y}{k}\right| = p^{j}\,|x-y|$$

Proposition

A continouous function $f(x)=\sum_{k\geq 0} c_k \binom{x}{k}$ $f\in C(Z_p)$ is Lipschitz precisely when $\{k|c_k|\}_{k\geq 0}$ is bounded

Corollary $f\in Lip(Z_p)$ and $f(x)=\sum_{k\geq 0} c_k \binom{x}{k}\in C(Z_p)$ Mahler series, then $\|\Phi f\|_s = \sup_{k\geq 1} \kappa_k |c_k|$

where $\kappa_k = \lfloor \log_p k \rfloor$

Theorem: Mahler series and strict differentiability

For a continuous function $f(x)=\sum_{k\geq 0} c_k \binom{x}{k}$ $f\in C(Z_p)$, we have

if $k|c_k|\to 0$ then $f\in S^1(Z_p)$

For a strictly differentiable function $f\in S^1(Z_p)$, then its indefinite sum is also strictly differentiable

$Sf(x)=\sum_{0\leq i\leq x} f(i)$, $Sf\in S^1(Z_p)$

Restricted power series and mean value

Definition power series $f(x)=\sum_{k\geq 0} a_k x^k$ with $a_k\to 0$ over field K is called restricted.

They form a normed algebra over K, with the Gauss norm $\|f\|_G = \sup_k |a_k| = \max_k |a_k|$

where $\|f\ g\|_G \leq \|f\|_G \|g\|_G$ for $|x|\leq 1$

Restricted ps are uniformly continuous

$|f(x+h)-f(x)|\leq |h|\|f\|_G$ if $|x|\leq 1$ and $|h|\leq 1$

and $|f(x+y)-f(x)-f(y)+f(0)|\leq \|f\|_G |x\ y|$ for $|x|\leq 1$ and $|y|\leq 1$

Theorem1 (analogy to calculus on R)

f(x) restricted ps, then f is a twice strictly differentiable function on the unit ball A of K : $f\in S^2(A)$.

The derivative of f is given by the restricted formal power series

$f'(x)=\sum_{k\geq 1} a_k k x^{k-1}$

Lemma n >=1 integer and $S_p(n) = S_p(n) = \sum_{k=1}^{n} k \bmod (p)$

Then the p-adic order of n! is $ord_p n! = \frac{n - S_p(n)}{p-1}$

Theorem2F1 (mean value)

f(x) restricted ps, $f(x) = \sum_{k\geq 0} a_k x^k$

and $|x| \leq 1$ and $|h| \leq r_p$, $r_p = \begin{cases} |p|^{1/(p-1)} & p > 2 \\ \sqrt{2} & p = 2 \end{cases}$

then $|f(x+h) - f(x)| \leq |h| \|f'\|_G$

Theorem2F2 (mean value)

$f \in C_p(X)$ ps that converges in the open unit ball $M_p = p Z_p$, and $\|f'(x)\|_{<1} < \infty$

with the restricted norm $\|f\|_{<1} = \sup_{|x|<1} |f(x)|$

then $|f(x+h) - f(x)| \leq |h| \|f'\|_{<1}$ for $|h| < r_p$, $r_p = \begin{cases} |p|^{1/(p-1)} & p > 2 \\ \sqrt{2} & p = 2 \end{cases}$

Theorem2F3 (mean value)

If $|x| \leq 1$ and $|h| \leq r_p$, $r_p = \begin{cases} |p|^{1/(p-1)} & p > 2 \\ \sqrt{2} & p = 2 \end{cases}$

then $|f(x+h) - f(x) - f'(x)h| \leq |h^2/2| \|f''\|_G$

Theorem3 fixed-point theorem

f(x) restricted ps in Q_p, with $\|f'\|_G < 1$, $B_{\leq 1}$ closed unit ball, and $\inf_{x \in B_{\leq 1}} |f(x) - x| \leq r_p$ $r_p = \begin{cases} |p|^{1/(p-1)} & p > 2 \\ \sqrt{2} & p = 2 \end{cases}$

then f has a fixed point in $B_{\leq 1}$: $\exists x_* \in B_{\leq 1} : f(x_*) = x_*$

Exponential and logarithm

Theorem power series

$\log(1+x) = \sum_{k\geq 1} \frac{(-1)^k x^k}{k}$ converges iff $|x|_p < 1$

$\exp(x) = \sum_{k\geq 0} \frac{x^k}{k!}$ converges iff $|x|_p < r_p$ $r_p = \begin{cases} |p|^{1/(p-1)} & p > 2 \\ \sqrt{2} & p = 2 \end{cases}$

Proposition1 $\left|\log(1+x)\right|_p = |x|_p \quad \left|\exp(x)\right|_p = 1$, $\left|1-\exp(x)\right|_p = |x|_p$

Proposition2

$\exp(x+y) = \exp(x)\cdot\exp(y)$, $\log\exp(x) = x$, $\exp\log(1+x) = 1+x$

Proposition3

$\exp(x)' = \exp(x)$, $\log(1+x)' = \dfrac{1}{1+x}$

Volkenborn integral and summation

Properties

$$f(x) = \sum_{x\geq k\geq 0} \nabla^k f(0)\binom{x}{k} \text{ , } \nabla f(x) = \sum_{x\geq k\geq 0} \nabla^{k+1} f(0)\binom{x}{k} = \sum_{x-1\geq k\geq 1} \nabla^k f(0)\binom{x}{k-1}$$

$$Sf(x) = \sum_{x\geq k\geq 0} \nabla^k f(0)\left(\sum_{x\geq l\geq 0}\binom{l}{k}\right), \; S\nabla f(x) = \sum_{x-1\geq k\geq 1} \nabla^k f(0)\left(\sum_{x-1\geq l\geq 0}\binom{l}{k-1}\right)$$

Definition Volkenborn integral of $f \in S^1(Z_p)$

$$\int_{Z_p} f(x)\,dx = \lim_{n\to\infty}\frac{1}{p^n}\sum_{j=0}^{p^n} f(j) = (Sf)'(0)$$

Proposition1

$$\int_{Z_p} f(x)\,dx \leq p\|f\|_1$$

where $\|f\|_1 = \sup\left(\left|f(0)\right|, \left\|\dfrac{f(x)-f(y)}{x-y}\right\|\right)$

If $\|f_n - f\|_1 \to 0$ then $\int_{Z_p} f_n(x)\,dx \to \int_{Z_p} f(x)\,dx$

Proposition2

For $f \in S^1(Z_p)$

$$\int_{Z_p} \nabla f(x)\,dx = f'(0)$$

Proposition3 integration of Mahler series

For Mahler series $f(x) = \sum_{k\geq 0} c_k\binom{x}{k}$

$$\int_{Z_p} f(x)\,dx = \sum_{k\geq 0} (-1)^k\, c_k \,/\, (k+1)$$

Proposition4

For shift $\tau_x f(t) = f(x+t)$ we have the following properties

- $\tau_x f(t) = f(x+t)$
- $S\tau_x f = \tau_x S f - f(0)$
- $S\nabla f = \nabla S f - f(0)$
- $\int_{Z_p} \tau_x f(t)\,dt = (Sf)'(x)$
- $S(f)'(x) = \int_{Z_p} f(x+t)\,dt - \int_{Z_p} f(t)\,dt$
- $(\nabla S)(x) = f(floor(x+1))$

Proposition5

For $F(x) = \int_{Z_p} f(x+t)\,dt$, $F \in S^1(Z_p)$ and $F'(x) = \int_{Z_p} f'(x+t)\,dt$

Proposition6

For involution $\sigma(x) = -(x+1)$, then $\int_{Z_p} f(\sigma(x))\,dx = \int_{Z_p} f(x)\,dx$

Proposition7

For power series $f(x) = \sum_{k\geq 0} a_k x^k$, $\int_{Z_p} f(x)\,dx = \sum_{k\geq 0} a_k b_k$

with Bernoulli numbers b_k $\frac{t}{e^t - 1} = \sum_{k\geq 0} b_k \frac{t^k}{k!}$

Sums of powers

$$S(x^k) = b_k x + \sum_{2\leq j\leq k} \binom{k}{j-1} b_{k+1-j} \frac{x^{k+1}}{k+1}$$

$$S_k(n) := \sum_{i=1}^{n} i^k$$

$$S_1(n) = \frac{n(n-1)}{2}$$

$$S_2(n)=\frac{n(n-1)(2n-1)}{6}$$

$$S_3(n)=\frac{n^2(n-1)^2}{4}$$

$$S_k(p)=p\,b_k \bmod(p\,k\,Z_p)$$

$$S_k(2)=1 \bmod(k\,Z_2)$$

10 P-adic analytic functions and elements

[1]

Power series and their zeros

Definition $f(X)=\sum_{n\geq 0} a_n X^n$ nonzero power series $a_n \in Q_p$.

Its order is $\omega(f)=\min\{n\in N \mid a_n\neq 0\}$

radius of convergence $r_f=\sup\{r\geq 0 \mid |a_n| r^n \to 0\}$

$r_f>0$: f(X) is convergent ps (cps)

f, g convergent ps→ f*g is convergent ps

composition $f\circ g(X)=f(g(X))$

$(f\circ g)\circ h=f\circ(g\circ h)$

addition, multiplication f+g, f*g → integral domain= commutative zero-divisor free ring

Properties:

$r_f=\frac{1}{\limsup_{n\to\infty}|a_n|_p^{1/n}}$ radius of convergence

$\omega(f\,g)=\omega(f)+\omega(g)$ order is additive

$D\left(\sum_{n\geq 0} a_n X^n\right)=\sum_{n\geq 0} n a_n X^{n-1}$ derivative

chain rule $D(f\circ g)(x)=Df(g(x))\,Dg(x)$

$r_f = r_{Df}$

Proposition1 inverse substitute power series (ps)

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

there is inverse substitute *g(X)*, then $(f\circ g)(X)=X \leftrightarrow a_0=f(0)=0$ and $a_1=f'(0)\neq 0$

Definition growth modulus of f=convergent ps

$M_r(f) = \max_{n\geq 0} |a_n| r^n \quad 0 \leq r \leq r_f$ is ultrametric norm of f

with dominant monomial $a_n x^n$ and $M_r(f\,g) = M_r(f) M_r(g)$

Compare: classical property (on real numbers R)

$a_n >= 0$, $a_n r^n \to 0$, then $M(r) = \max_{n\geq 0} a_n r^n$ is a continuous convex function

Theorem infinite r_f

If $r_f = \infty$ and $|f(x)| \leq C|x|^N$ for $|x| \geq c$, then f=polynomial, *deg(f)<=N*

With ultrametric norm $M_r(f)$, $f(X) = \sum_{n\geq 0} a_n X^n$ ps, $\log = \log_p$

Newton polygon

We have the denominations and relations

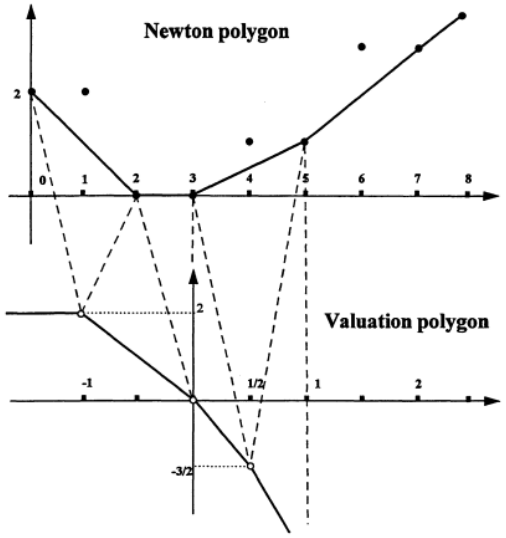
$\rho = \log r < \rho_f = \log r_f$

$\alpha_n = \log|a_n| = -ord_p a_n = -v_n$

$\mu_p = \log M_r(f) = \sup_{n\geq 0}(n\rho + \alpha_n)$

$h_\rho(\rho) := \inf_{n\geq 0}(v_n - n\rho), \ -\infty < \rho < \rho_f$ is valuation (lower) polygon of f

$s_\rho(n) := \sup_{-\infty<\rho<\rho_f}(v_n + n\rho)$ Newton (upper) polygon of f



Proposition2

$f(X)=\sum_{n\geq 0} a_n X^n$ restricted ps , i.e. $a_n \to 0$,

then $f(X)=f(a)+(X-a)g(X)$, $r_g > r_f$

Theorem (Strassman)

$f(X)=\sum_{n\geq 0} a_n X^n$ restricted ps ,

then f has finitely many zeros

for $\mu=\min\{n \mid |a_n| r^n = M_r(f)\} < v=\max\{n \mid |a_n| r^n = M_r(f)\}$

Corollary

f has at most v-μ zeros in the sphere $S_r(K)=\{x,|x|=r\}$

f has at most v zeros in the ball $B_{\leq r}$

f has at most μ zeros in the ball $B_{<r}$

Theorem (entire functions)

$f(X)=\sum_{n\geq 0} a_n X^n$ entire function in K, i.e. $r_f=\infty$

if f has no zeros in K^a, then f =const

if f has finitely many zeros in K^a, then f =polynomial

if $K=C_p$, then is equivalent

(i) f has infinitely many zeros ξ_k

(ii) f has a sequence ofcritical radii $r_i \to \infty$.

(iii) The growth of |x| is not bounded by a polynomial in |x|,

(iii) f is given bya convergent infinite product $f(X)=C\,x^m \prod_{root(f)=\xi_k \neq 0} (1-x/\xi_k)$

Theorem classical mean value (Rolle)

f : [a, b] $\sigma \to$ R continuous and differentiable on (a, b),

then there is a< c < b with

$$f'(c)=\frac{f(b)-f(a)}{b-a}$$

Theorem p-adic mean value

$f \in C_p(X)$ with $r_f > 1$

For $a \in A_p, b \in A_p$, $|a-b| < r_p = p^{1/(p-1)}$, then there is $\xi \in A_p$, $A_p=\{0,1,\ldots p-1\}$ with

$f(b)-f(a)=(b-a)f'(\xi)$

The same is true for point in $M_p = pZ_p$

Theorem p-adic maximum principle

$f \in C_p(X)$ with r<r_f

then $y = f(x)$, $|y| < M_r f$ takes all values in $0 \le y < |M_r f|$ with $|x| = r$,

and for $|y| = M_r f$, $|y - f(0)| = M_r f$, there is *x* with $y = f(x)$, $|x| = r$

Rational functions

Proposition $f \in C_p(X)$ non-zero rational function *f=g/h* with poles α_i

f has three types of Laurent series

$$\sum_{-m \le n < \infty} a_n x^n \ , \ 0 < |x| < \min\{|\alpha_i| \mid \alpha_i \neq 0\}$$

$$\sum_{-\infty \le n < \infty} a_n x^n \ , \ \max\{|\alpha_i| |\alpha_i| \le r_f\} < |x| < \min\{|\alpha_i| |\alpha_i| > r_f\}$$

$$\sum_{-m \le n < N} a_n x^n \ , \ |x| > \max\{|\alpha_i|\}$$

Properties ultrametric norm $M_r f$ on sphere $S_r = \{x \mid |x| = r\}$

if f has no pole on S_r , then $M_r f = \sup_{|x|=r} |f(x)|$

if f has no zero on S_r , then $M_r f = \inf_{|x|=r} |f(x)|$

if f has zeros and poles on S_r , then $|f(x)|$ assumes all values of $|C_p|$ on S_r

for *f=g/h* , $M_r f = M_r g / M_r h$

Theorem Mittag-Leffler classical on C: rational expansion of holomorphic function

For meromorphic function *g* on *U* with poles $a_i \ i = 1,...n$, *g=f+h*, where *h* is holomorphic function on *U*,

$$f(z) = \sum_k p_i(z, a_i) \ , \ p_i(z, a_i) = \sum_{k=1}^{n_k} \frac{c_{ik}}{(z - a_i)^k}$$

Theorem p-adic rational expansion

Let be $B_i = B_{<\sigma_i}(a_i)$, *1<i<l* , a finite set of disjoint open balls in the closed ball $B_{\le r}$ and consider rest set $D = B_{\le r} - \bigcup_i B_i$.

For a rational function $f \in C_p(x)$ regular in D with poles in b_i , zero a_j with multiplicity μ_{a_j} , and $f_i = f_{B_i}$ the principal part functions of *f* on B_i ,

the canonical decomposition of *f* is $f = f_0 + \sum_{1\le i\le l} f_i$, $f_i = \prod_{a_j\in B_i}\left(\frac{x-a_j}{x-b_i}\right)^{\mu_{a_j}} =: 1+\omega_i$

with f_0 regular in, and $\|f\|_D = \max_{0\le i\le l}\|f_i\|_D$

Motzkin factorization

For *f=g/h* all zeros and po $B_{\le r}$ les in $B_{\le r}$, we have the factorization $f(x) = f_0(x)\prod_{1\le i\le l} f(x)_i$

with f_0 regular non-zero in $B_{\le r}$, $f_i(x) = (x-b_i)^{m_i} h_i(x)$, $\|h_i - 1\|_{B_i} < 1$, $\lim_{|x|\to\infty} h_i(x) = 1$

Analytic elements

Theorem Runge classical on C

A holomorphic function *f* defined in a domain $D \subset C$ can be uniforrnly approximated by means of rational functions

Definition $D \subset C_p$ closed , function $f : D \to C_p$ is analytic, if it is a uniform limit of rational functions.

Theorem Analytic functions on closed unit ball $B_{\le 1}$ form the algebra $C_p[x]$ of functions $f(x) = \sum_{n\ge 0} a_n x^n$ with norm

$\|f\| = \sup_{|x|\le 1}|f(x)| = \sup_{n\ge 0}|a_n|$

At x=1 it has the expansion $f(x) = c_0 + \sum_{m\ge 0}\lambda_m \frac{1}{(x-1)^{m+1}}$, $\lim_{m\to\infty}|\lambda_m| = 0$

Theorem p-adic Mittag-Leffler

$D \subset C_p$ closed, bounded, connected set, $B_i = B_{<\sigma_i}(a_i)$ family of holes,

then there is a direct sum decomposition for analytic functions $H(D) = H(B_D)\sum_i \oplus H_0(B_i)$,

where each $f \in H(D)$ $f = f_0 + \sum_i f_i$, with f_0 analytic in D, f_i analytic on B_i, $\lim_{x\to\infty} f_i(x) = 0$, $\lim_{i\to\infty}\|f_i\| = 0$

p-adic Gamma function Γp

Classical gamma function Γ

[2]

Gamma function has no zeros

$\Gamma(n) = (n-1)!$, $\operatorname{Re}s_{z=-k}(\Gamma(z)) = \frac{(-1)^k}{k!}$

$$\Gamma(z) = \int_0^\infty t^{z-1} \exp(-t)\, dt$$

$$\Gamma(z) = \left(z \exp(\gamma z) \prod_{r=1}^{\infty} \left(1 + \frac{z}{r}\right) \exp(-z/r) \right)^{-1}$$

$$\Gamma(z) = (z-1)\Gamma(z-1) \text{ functional equation}$$

$$\prod_{j=0}^{m-1} \Gamma\left(z + \frac{j}{m}\right) = (2\pi)^{(m-1)/2}\, m^{(1-2mz)/2}\, \Gamma(mz) \ , \ m \geq 2 \text{ Gaussian relation}$$

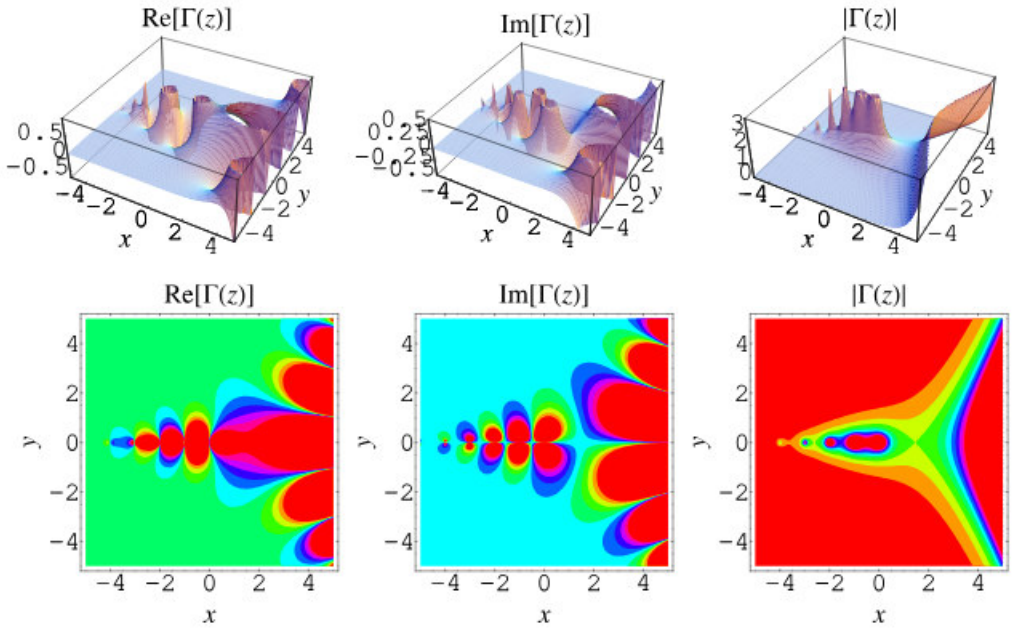
$$\zeta(z)\Gamma(z) = \int_0^\infty \frac{t^{z-1}}{\exp(t)-1} dt \text{ for Re[z]>1}$$

where $\zeta(z) = \sum_{k=1}^{\infty} \frac{1}{k^z}$ Riemann zeta function

$$\frac{1}{\Gamma(z)} = \left(z \exp\left(\gamma z - \sum_{k=2}^{\infty} \frac{(-1)^k\, \zeta(k)\, z^k}{k} \right) \right)$$

$$\gamma = \lim_{n\to\infty} \left(\sum_{k=1}^{n} \frac{1}{k} - \log n \right) = 0.5772...$$

where $\gamma = \lim_{n\to\infty} \left(\sum_{k=1}^{n} \frac{1}{k} - \log n \right) = 0.5772...$ Euler-Mascheroni constant



Morita p-adic gamma function Γp

Morita p-adic gamma function Γp $\Gamma_p : Z_p \to Q_p$

$$\Gamma_p(n) := (-1)^n \prod_{1 \le j < n,\, p \nmid j} j \quad n \ge 2$$

Wilson congruence $(p-1)! = -1 \bmod p$

$$\prod_{a \le j < a+p^\nu,\, p \nmid j} j = -1 \bmod p^\nu$$

f(n) satisfies $f(a) = f(a+p^\nu) \bmod p^\nu$, $f(a) = f(a+m\,p^\nu) \bmod p^\nu$

Properties Γ_p

$\Gamma_p(2) = 1$, $\Gamma_p(3) = -2$

$$\Gamma_p(n+1) = \begin{cases} n! & n = odd, n \le p-1 \\ -n! & n = even, n \le p-1 \end{cases}$$

$$\Gamma_p(n+1) = \frac{(-1)^{n+1}\, n!}{[n/p]!\, p^{[n/p]}}$$

$$\Gamma_p(x+1)=\begin{cases}-x\Gamma_p(x) & x\in Z_p^\times\\ -\Gamma_p(x) & x\in pZ_p\end{cases}$$ functional equation

Theorem $\Gamma_p : Z_p \to Q_p$ is continuous, with properties

$\Gamma_p(0)=1$, $\Gamma_p(1)=-1$, $\Gamma_p(2)=1$

$\Gamma_p(n+1)=(-1)^{n+1}n!$, $1\le n<p$

$\left|\Gamma_p(x)\right|_p=1$

$\left|\Gamma_p(x)-\Gamma_p(y)\right|_p\le\left|x-y\right|_p$, $\left|\Gamma_p(x)-1\right|_p\le\left|x\right|_p$

$\Gamma_p(x+1)=h_p(x)\Gamma_p(x)$, where $h_p(x)=\begin{cases}-x & x\in Z_p^\times\\ -1 & x\in pZ_p\end{cases}$

$\Gamma_p(x)\Gamma_p(1-x)=(-1)^{R(x)}$, $R(x)=x \bmod p$

Proposition If *m>=1* prime to *p*, then

$$\prod_{j=0}^{m-1}\Gamma\left(x+\frac{j}{m}\right)=\varepsilon_m m^{1-R(mx)}\Gamma(mz)\ ,\ \varepsilon_m=\prod_{j=0}^{m-1}\Gamma_p\left(\frac{j}{m}\right)\ ,\ s(x)=\frac{R(x)-x}{p}$$

Γp has the Mahler series

$$\Gamma_p(x+1)=\sum_{k\ge0}a_k\binom{x}{k}\text{ , where }\sum_{k\ge0}(-1)^{k+1}a_k\frac{x^k}{k!}=\frac{1-x^p}{1-x}\exp\left(x+\frac{x^p}{p}\right)$$

With $L_\Gamma(x)=\log\Gamma_p(px)$

$$\left|\log\frac{\Gamma_p(px+py)}{\Gamma_p(px)\Gamma_p(py)}\right|_p=\left|L_\Gamma(x+y)-L_\Gamma(x)-L_\Gamma(y)\right|_p$$

$$\left|L_\Gamma(x+y)-L_\Gamma(x)-L_\Gamma(y)\right|_p\le\left|p^3xy(x+y)\right|_p$$

Congruences mod p

$$\binom{pn}{pk}=\binom{n}{k}\bmod\left(pnZ_p\right)$$

Kazandzidis

For all primes p>= 5 we have

$$\binom{pn}{pk}=\binom{n}{k}\bmod\left(p^3nk(n-k)\binom{n}{k}Z_p\right)$$

$$\left| \frac{p^{2n-3}}{2n\left(2n+1\right)} \right|_p \leq 1 \quad n \geq 3$$

References

[1] A. M. Robert, A course in p-adic analysis, Springer Science, New York, 2000
[2] J. Helm, Mathematica-notebook PadicCalc.nb, www.researchgate.net, 2026
[3] R. G. Bartle & D. R. Sherbert, Introduction to real analysis, John Wiley & Sons, 2011
[4] C. Thiele, Complex Analysis, Bonn University, 2016