

**Tutorial on p -adic numbers,
 \mathbb{Q}_p and \mathbb{C}_p ,
and p -adic analysis**

Robert L. Benedetto
Amherst College

Fields Institute
Mini-Workshop on p -adic Dynamics

Monday, October 27, 2008

Absolute Values

Definition. An *absolute value* $|\cdot|_v$ on a field K is a function

$$|\cdot|_v : K \rightarrow [0, \infty)$$

such that for all $x, y \in K$,

- (1) $|x|_v = 0 \iff x = 0$,
- (2) $|xy|_v = |x|_v \cdot |y|_v$,
- (3) $|x + y|_v \leq |x|_v + |y|_v$.

If $|\cdot|_v$ in fact satisfies the stronger *ultrametric* triangle inequality

$$(3') \quad |x + y|_v \leq \max\{|x|_v, |y|_v\},$$

then we say $|\cdot|_v$ is *non-archimedean*.

Otherwise, we say $|\cdot|_v$ is *archimedean*.

The “usual” absolute value (on \mathbb{Q} , or \mathbb{R} , or \mathbb{C}), denoted $|\cdot|_\infty$, is archimedean.

The p -adic absolute value on \mathbb{Q}

Fix $p \in \mathbb{Z}$ prime. The p -adic absolute value $|\cdot|_p$ on \mathbb{Q} is the unique absolute value on \mathbb{Q} such that

$$|p|_p = \frac{1}{p}.$$

More precisely,

$$\left| \frac{r}{s} p^n \right|_p = p^{-n} \quad \text{for } r, s \in \mathbb{Z} \text{ not divisible by } p,$$

and

$$|0|_p = 0. \quad [\text{Idea: } |0|_p = |0 \cdot p^\infty|_p = p^{-\infty} = 0.]$$

Example. $-\frac{2401}{2400} = -\frac{7^4}{2^5 \cdot 3 \cdot 5^2}$, so

$$\left| -\frac{2401}{2400} \right|_v = \begin{cases} 2401/2400 & \text{if } v = \infty, \\ 32 & \text{if } v = 2, \\ 3 & \text{if } v = 3, \\ 25 & \text{if } v = 5, \\ 1/2401 & \text{if } v = 7, \\ 1 & \text{if } v = p > 7 \text{ prime.} \end{cases}$$

Basic properties of $|\cdot|_p$ for prime p .

- Having p 's in your numerator makes you “small”; having p 's in your denominator makes you “big”.
- $|\cdot|_p$ is non-archimedean, i.e,

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

So the sum of arbitrarily many “small” numbers is still “small”.

- If $|x|_p \neq |y|_p$, then

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

“All triangles are isocetes.”

(True for any non-archimedean metric space.)

- The closed unit disk contains all integers.

Side notes:

1. (**Ostrowski's Theorem.**) For any absolute value $|\cdot|_v$ on \mathbb{Q} , either:

(a.) $|\cdot|_v$ is trivial, i.e, $|x|_v = \begin{cases} 1 & \text{if } x \neq 0, \\ 0 & \text{if } x = 0, \end{cases}$

(b.) $|\cdot|_v = |\cdot|_\infty^\alpha$ for some $0 < \alpha \leq 1$,

(c.) $|\cdot|_v = |\cdot|_p^\alpha$ for some prime p and some $0 < \alpha < \infty$,

$M_{\mathbb{Q}} := \{\infty, 2, 3, 5, 7, \dots\}$ is the set of **places** of \mathbb{Q} .
(Equivalence classes of nontrivial absolute values on \mathbb{Q}).

2. The choice of normalization $|p|_p = 1/p$ makes the **product formula** true:

$$\prod_{v \in M_{\mathbb{Q}}} |x|_v = 1 \quad \text{for all } x \in \mathbb{Q}^\times.$$

\mathbb{Q}_p and \mathbb{Z}_p

Definition. \mathbb{Z}_p , the ring of p -adic integers, is the completion of \mathbb{Z} with respect to $|\cdot|_p$.

\mathbb{Q}_p , the field of p -adic rationals, is the completion of \mathbb{Q} with respect to $|\cdot|_p$.

Note: Any nonnegative integer may be uniquely represented as

$$\sum_{n=0}^N a_n p^n, \quad a_n \in \{0, 1, \dots, p-1\}.$$

So: Any p -adic integer $x \in \mathbb{Z}_p$ may be uniquely represented as

$$x = \sum_{n=0}^{\infty} a_n p^n, \quad a_n \in \{0, 1, \dots, p-1\}.$$

That includes negative integers. E.g.:

$$-1 = \sum_{n=0}^{\infty} (p-1)p^n \in \mathbb{Z}_p.$$

$$\mathbb{Z}_p = \left\{ \sum_{n=0}^{\infty} a_n p^n : a_n \in \{0, 1, \dots, p-1\} \right\}.$$

\mathbb{Z}_p is a ring: add and multiply **with carrying**.

(But note: carrying from the p^n to p^{n+1} column is the *smaller* direction.)

For example:

$$\begin{aligned} 1 + (-1) &= 1 + ((p-1) + (p-1)p + (p-1)p^2 + \dots) \\ &= p + (p-1)p + (p-1)p^2 + \dots \\ &= p^2 + (p-1)p^2 + \dots = \dots = 0. \end{aligned}$$

\mathbb{Z}_p also contains all rational numbers with no p 's in the denominator: e.g.

$$\begin{aligned} \sum_{n=0}^{\infty} 2 \cdot 5^n &= 2 + 2 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + \dots \\ &= \frac{2}{1-5} = -\frac{1}{2}. \end{aligned}$$

(Geometric series, $|5|_5 < 1$.)

So $-\frac{1}{2} \in \mathbb{Z}_5$.

$$\mathbb{Q}_p = \left\{ \sum_{n=m}^{\infty} a_n p^n : a_n \in \{0, 1, \dots, p-1\} \right\}.$$

The absolute value $|\cdot|_p$ extends to \mathbb{Q}_p by

$$\left| \sum a_n p^n \right|_p = p^{-m},$$

where m is the smallest integer such that $a_m \neq 0$.

We also write $v_p(x) = m$. The function

$$v_p(\cdot) := -\log_p |\cdot|_p$$

is called the *p-adic valuation*.

Simple Observations and Terminology

- $|\mathbb{Q}_p|_p = \{0\} \cup p^{\mathbb{Z}} = \{0\} \cup \{p^m : m \in \mathbb{Z}\}$.
- $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$ (i.e., closed unit disk)
- $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\}$ (i.e., open unit disk) is the unique maximal ideal of \mathbb{Z}_p .
- $\mathbb{Z}_p/p\mathbb{Z}_p$ is called the **residue field** of \mathbb{Z}_p (or of \mathbb{Q}_p). It is isomorphic to \mathbb{F}_p , the field of p elements.
- \mathbb{Q}_p is the field of fractions of \mathbb{Z}_p .

Fact: Let $\{x_n\}_{n \geq 0}$ be a sequence in \mathbb{Q}_p . Then

$$\sum_{n=0}^{\infty} x_n \text{ converges in } \mathbb{Q}_p \iff \lim_{n \rightarrow \infty} x_n = 0.$$

(True for any **complete non-archimedean** ring, not just \mathbb{Q}_p .)

Hensel's Lemma. (Simplified version.)

Let $g(z) \in \mathbb{Z}_p[z]$ be a polynomial and $x \in \mathbb{Z}_p$ such that

$$|g(x)|_p < 1 \quad \text{and} \quad |g'(x)|_p = 1.$$

Then there is (a unique) $\alpha \in \mathbb{Z}_p$ with

$$|x - \alpha|_p < 1 \quad \text{and} \quad g(\alpha) = 0.$$

Example. $p = 5$.

There is an element $\sqrt{-1} \in \mathbb{Z}_5$ near 2,

because $g(z) = z^2 + 1$ has $g'(z) = 2z$, and so

$$|g(2)|_5 = |5|_5 < 1$$

and

$$|g'(2)|_5 = |4|_5 = 1.$$

In fact:

$$\sqrt{-1} = 2 + 1 \cdot 5 + 2 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + 4 \cdot 5^5 + 2 \cdot 5^6 + \dots$$

Algebraic Extensions

But \mathbb{Q}_p is not algebraically closed. E.g. $\sqrt{2}, \sqrt{5} \notin \mathbb{Q}_5$:

- If $\alpha^2 = 2$ for some $\alpha \in \mathbb{Q}_5$, then $|\alpha|_5 = 1$,
since $|\alpha|_5^2 = |2|_5 = 1$. But for any $w \in \mathbb{Z}_5$ and for
each choice of $a = 1, 2, 3, 4$,

$$(a + 5w)^2 - 2 \in (a^2 - 2) + 5\mathbb{Z}_5$$

and so cannot be 0.

- If $\beta^2 = 5$, then $|\beta|_5 = 1/\sqrt{5}$, which is not the absolute value of any element of \mathbb{Q}_5 .

The absolute value $|\cdot|_p$ extends in a unique way to the field $K = \mathbb{Q}_5(\sqrt{2})$ and to $L = \mathbb{Q}_5(\sqrt{5})$ and, more generally, to any algebraic extension of \mathbb{Q}_p .

In particular, $|\cdot|_p$ extends uniquely to $\overline{\mathbb{Q}_p}$, an algebraic closure of \mathbb{Q}_p .

[If $g(z) = z^d + a_{d-1}z^{d-1} + \cdots + a_0 \in \mathbb{Q}_p[z]$ is the minimal polynomial for α over \mathbb{Q}_p , then $|\alpha|_p := |a_0|_p^{1/d}$.]

Residue Fields and Ramification

Any algebraic extension K/\mathbb{Q}_p has ring of integers

$$\mathcal{O}_K = \{x \in K : |x|_p \leq 1\}$$

with unique maximal ideal

$$\mathcal{M}_K = \{x \in K : |x|_p < 1\}$$

and residue field

$$k = \mathcal{O}_K/\mathcal{M}_K.$$

Then k is an algebraic extension of \mathbb{F}_p .

Let $f = [k : \mathbb{F}_p]$, the **residue field extension degree**.

Let e be the index of the group $|\mathbb{Q}_p^\times|_p = \{p^m : m \in \mathbb{Z}\}$ in the larger group $|K^\times|_p$.

(If e is finite, then $|K^\times|_p = \{p^{m/e} : m \in \mathbb{Z}\}$.)

e is called the **ramification degree**.

Fact: $[K : \mathbb{Q}_p] = ef$.

Example. $K = \mathbb{Q}_5(\sqrt{2})$ has residue field

$$k = \mathbb{F}_5(\sqrt{2}) = \mathbb{F}_{25},$$

with $f = [\mathbb{F}_{25} : \mathbb{F}_5] = 2$.

Meanwhile, $|K^\times|_5 = |\mathbb{Q}_5^\times|_5$, so $e = 1$.

K/\mathbb{Q}_5 is an *unramified extension*.

Example. $L = \mathbb{Q}_5(\sqrt{5})$ has residue field $k = \mathbb{F}_5$,
so $f = 1$.

But $|L^\times|_5 = \{5^{m/2} : m \in \mathbb{Z}\}$, so $e = 2$.

L/\mathbb{Q}_5 is a *totally ramified extension*.

Example. $\overline{\mathbb{Q}}_p$ has residue field $\overline{\mathbb{F}}_p$,

so $f = [\overline{\mathbb{F}}_p : \mathbb{F}_p] = \infty$.

And $|\overline{\mathbb{Q}}_p^\times|_p = p^\mathbb{Q} = \{p^r : r \in \mathbb{Q}\}$, so $e = \infty$.

Fact. If K/\mathbb{Q}_p is a finite extension, then K is complete and locally compact.

Fact. If K/\mathbb{Q}_p is an *infinite algebraic* extension, then K is *neither* complete nor locally compact.

Definition.

\mathbb{C}_p is the completion of $\overline{\mathbb{Q}_p}$ with respect to $|\cdot|_p$.

Note:

$$\sum_{n=1}^{\infty} p^{1/n} p^n \in \mathbb{C}_p \setminus \overline{\mathbb{Q}_p}$$

and

$$\sum_{n=1}^{\infty} \alpha_n p^n \in \mathbb{C}_p \setminus \overline{\mathbb{Q}_p}$$

where α_n is a primitive $(p^n - 1)$ -st root of unity.

$|\cdot|_p$ extends canonically to \mathbb{C}_p .

$$|\mathbb{C}_p^\times|_p = p^{\mathbb{Q}}$$

Properties of \mathbb{C}_p

- (1) \mathbb{C}_p is complete **and** algebraically closed.
 - (2) As with **any** non-archimedean field:
 - (a) \mathbb{C}_p is **totally disconnected**.
 - (b) All disks are (topologically) open and closed.
 - (c) Any point of a disk is a center.
 - (d) Two disks intersect \Leftrightarrow one contains the other.
 - (3) \mathbb{C}_p is **not locally compact**.
 - (4) \mathbb{C}_p is **not spherically complete**.
-

Given $a \in \mathbb{C}_p$ and $r > 0$, denote by

$$D(a, r) = \{x \in \mathbb{C}_p : |x - a|_p < r\}$$

the open disk centered at a of radius r , and by

$$\overline{D}(a, r) = \{x \in \mathbb{C}_p : |x - a|_p \leq r\}$$

the closed disk.

Spherically Complete?

Definition. A metric space X is *spherically complete* if for every decreasing chain of nonempty open disks

$$D(a_1, r_1) \supseteq D(a_2, r_2) \supseteq D(a_3, r_3) \supseteq \cdots$$

we have $\bigcap_{n \geq 1} D(a_n, r_n) \neq \emptyset$.

Fact. A metric space X is *complete* if and only if for every decreasing chain of nonempty open disks

$$D(a_1, r_1) \supseteq D(a_2, r_2) \supseteq D(a_3, r_3) \supseteq \cdots$$

such that $\lim_{n \rightarrow \infty} r_n = 0$, we have $\bigcap_{n \geq 1} D(a_n, r_n) \neq \emptyset$.

Example. Let $a_n = \sum_{j=1}^n p^{1-1/j}$ and $r_n = |p|_p^{1-1/n}$.

Then, working in \mathbb{C}_p ,

$$D(a_1, r_1) \supseteq D(a_2, r_2) \supseteq D(a_3, r_3) \supseteq \cdots$$

but $\bigcap_{n \geq 1} D(a_n, r_n) = \emptyset$.

(Note: $r_n \searrow p^{-1} > 0$.)

Rational and Irrational Disks

Recall: all disks are both open and closed topologically.

If $r \notin p^{\mathbb{Q}}$, then $\overline{D}(a, r) = D(a, r)$; we call such a disk **irrational**.

If $r \in p^{\mathbb{Q}}$, then $\overline{D}(a, r)$ is a disjoint union of infinitely many (one for each element of $\overline{\mathbb{F}}_p$) translates of $D(a, r)$.

We call

$\overline{D}(a, r)$ a **rational closed disk**, and
 $D(a, r)$ a **rational open disk**.

Convergence of Power Series

Let $g(z) = \sum_{n \geq 0} c_n (z - a)^n \in \mathbb{C}_p[[z - a]]$.

For any $x \in \mathbb{C}_p$,

$$g(x) \text{ converges} \iff \lim_{n \rightarrow \infty} |c_n|_p \cdot |x - a|_p^n = 0.$$

In particular, for any $r > 0$,

$$\lim_{n \rightarrow \infty} |c_n|_p r^n = 0 \implies g(z) \text{ converges on } \overline{D}(a, r).$$

[If $r \in p^{\mathbb{Q}}$, the converse is also true.]

Root Test: The radius of convergence of g is

$$R = \left[\limsup_{n \rightarrow \infty} |c_n|_p^{1/n} \right]^{-1}.$$

Polynomials and Power Series

Let $g(z) = \sum_{n \geq 0} c_n(z - a)^n \in \mathbb{C}_p[[z - a]]$ be a nontrivial polynomial or power series with radius of convergence $0 < R \leq \infty$.

If $g(x) = 0$ for some $x \in \mathbb{C}_p \setminus \{a\}$, then there must be (at least) two integers $0 \leq i < j$ such that

$$|c_i(x - a)^i|_p = |c_j(x - a)^j|_p = \max_{n \geq 0} \{|c_n(x - a)^n|_p\}.$$

Fact. The converse is true: if $0 < r < R$ and

$$|c_i|_p r^i = |c_j|_p r^j = \max_{n \geq 0} \{|c_n|_p r^n\}$$

for some $0 \leq i < j$, then there is some $x \in \mathbb{C}_p$ with $|x|_p = r$ with $g(x) = 0$.

- Also true at $r = R$ if the disk of convergence is rational closed.
- Related to the theory of Newton Polygons.
- This whole slide is true for $\overline{\mathbb{Q}}_p$, not just \mathbb{C}_p .

[Still considering nontrivial $g(z) \in \mathbb{C}_p[[z - a]]$ with radius of convergence $0 < R \leq \infty$.]

Let $\tilde{a} \in \mathbb{C}_p$ lie in the disk of convergence; by composing with $z \mapsto z + (a - \tilde{a})$, we can write the same function as

$$g(z) = \sum_{n \geq 0} \tilde{c}_n (z - \tilde{a})^n \in \mathbb{C}_p[[z - \tilde{a}]]$$

For $0 < r < R$, let

$$s := \max_{n \geq 1} \{ |\tilde{c}_n|_p r^n \}$$

$$d_- := \text{minimum } n \geq 1 \text{ for which } |\tilde{c}_n|_p r^n = s$$

$$d_+ := \text{maximum } n \geq 1 \text{ for which } |\tilde{c}_n|_p r^n = s.$$

Then g maps

$$D(\tilde{a}, r) \quad d_- \text{-to-1 onto} \quad D(\tilde{c}_0, s)$$

and

$$\overline{D}(\tilde{a}, r) \quad d_+ \text{-to-1 onto} \quad \overline{D}(\tilde{c}_0, s).$$

In particular: g maps

- rational open disks to rational open disks
- rational closed disks to rational closed disks
- irrational disks to irrational disks

[for disks of radius less than R .]

Example. $g(z) = pz^5 + pz^3 + z^2 + pz + p^3$.

Then $g(\overline{D}(0, r)) = \overline{D}(p^3, s)$, where

$$s = \begin{cases} |p|_p r = p^{-1}r & \text{if } 0 < r \leq p^{-1}, \\ r^2 & \text{if } p^{-1} \leq r \leq p^{1/3} \\ |p|_p r^5 = p^{-1}r^5 & \text{if } r \geq p^{1/3}. \end{cases}$$

because among the nonconstant terms pz^5 , pz^3 , z^2 , pz ,

- pz is uniquely dominant for $r < |p|_p$,
- $|pz|_p = |z^2|_p$ for $r = |p|_p$,
- z^2 is uniquely dominant for $|p|_p < r < |p|_p^{-1/3}$,
- $|z^2|_p = |pz^5|_p$ for $r = |p|_p^{-1/3}$,
- pz^5 is uniquely dominant for $r > |p|_p^{-1/3}$.

[Note: $\overline{D}(p^3, s) = \overline{D}(0, s)$ for $s \geq |p|_p^3 = p^{-3}$.]

Disks in $\mathbb{P}^1(\mathbb{C}_p)$

Recall: $\mathbb{P}^1(\mathbb{C}_p) = \mathbb{C}_p \cup \infty$.

Definition: A $\mathbb{P}^1(\mathbb{C}_p)$ -disk is either

- a disk $D \subseteq \mathbb{C}_p$, or
 - $\mathbb{P}^1(\mathbb{C}_p) \setminus D$, for some disk $D \subseteq \mathbb{C}_p$.
-

We can attach adjectives like rational, irrational, open, closed in the obvious way.

Fact:

If $g(z) \in \mathbb{C}_p(z)$ is a non-constant rational function, and if $D \subseteq \mathbb{P}^1(\mathbb{C}_p)$ is a $\mathbb{P}^1(\mathbb{C}_p)$ -disk,

then $g(D)$ is **either**

- all of $\mathbb{P}^1(\mathbb{C}_p)$, **or**
- a $\mathbb{P}^1(\mathbb{C}_p)$ -disk of the same type.

Very Basic Rigid Analysis

Definition.

A **connected affinoid** in $\mathbb{P}^1(\mathbb{C}_p)$ is a nonempty intersection of finitely many $\mathbb{P}^1(\mathbb{C}_p)$ -disks.

[i.e., a disk with finitely many proper subdisks removed.]

We can attach adjectives like rational, irrational, open, closed in the obvious way.

Fact. Let $A \subseteq \mathbb{P}^1(\mathbb{C}_p)$ be a connected affinoid, and let $g(z) \in \mathbb{C}_p(z)$ be a rational function of degree $d \geq 1$.

Then:

- (1) $g(A)$ is **either** all of $\mathbb{P}^1(\mathbb{C}_p)$ **or** a connected affinoid of the same type.
- (2) $g^{-1}(A)$ is a union of ℓ connected affinoids V_1, \dots, V_ℓ of the same type.

Moreover, for each i , g maps d_i -to-1 onto A ,

where $1 \leq d_i \leq d$, and $\sum_{i=1}^{\ell} d_i = d$.

Example. $g(z) = pz^3 - z^2 + z$. Then

- g maps the rational closed annulus $\overline{D}(0, 1) \setminus D(0, 1)$ onto the rational closed disk $\overline{D}(0, 1)$.

[**Note:** some points 1-to-1, others 2-to-1.]

- $g^{-1}(\overline{D}(0, 1)) = \overline{D}(0, 1) \cup \overline{D}(\frac{1}{p}, p^{-1})$,

With $\overline{D}(0, 1)$ mapping 2-to-1 onto itself,

and $\overline{D}(\frac{1}{p}, p^{-1})$ mapping 1-to-1 onto $\overline{D}(0, 1)$.

- $g^{-1}(\overline{D}(0, p^3)) = \overline{D}(0, p^{4/3})$,

with $\overline{D}(0, p^{4/3})$ mapping 3-to-1 onto $\overline{D}(0, p^3)$.

Example. $h(z) = z + \frac{1}{z} = \frac{z^2 + 1}{z}$.

Then $h^{-1}(\overline{D}(0, 1))$ is the annulus $\overline{D}(0, 1) \setminus D(0, 1)$.

And h maps $\overline{D}(0, 1) \setminus D(0, 1)$ 2-to-1 onto $\overline{D}(0, 1)$.