Arizona Winter School

p-adic lecture 2: A Deeper Analysis

Last time:

- $\mathbb{Q}_p$ as sums $\sum_{i=n_0} b_i p^i$

  *examples: $p=5$

  $4\cdot\frac{1}{5} + 3\cdot 1 + 2\cdot 5 + 0\cdot 5^2 + \cdots$

- $\mathbb{Z}_p$ as sums $\sum_{i=n_0} b_i p^i$ with $n_0 \geq 0$

  *examples $p=5$

  $1/3 = 2 + 3\cdot 5 + 1\cdot 5^1 + 3\cdot 5^2 + \cdots$

2.1 Absolute Values

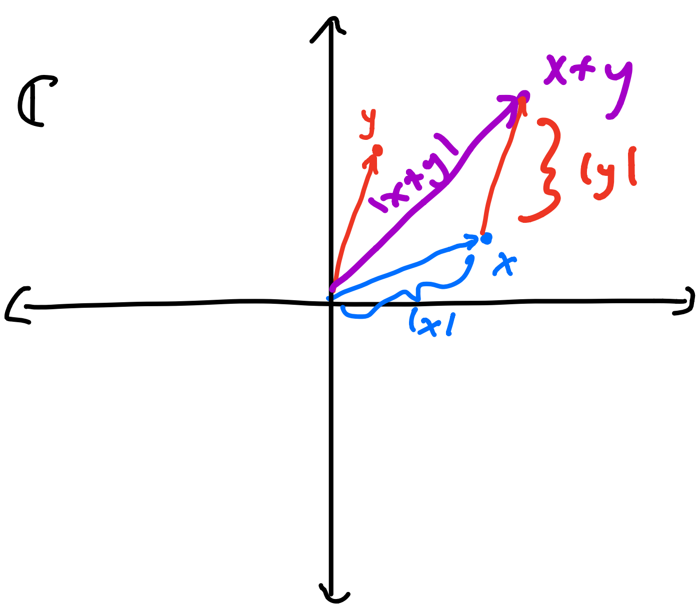
- Formalizing "size"

Definition:
For a field k, an <u>absolute value</u> on k is a function
$$|\cdot| : k \longrightarrow \mathbb{R}_{\geq 0} \text{ such that}$$

i) $|x| = 0$ iff $x = 0$
ii) $|xy| = |x||y|$ for all $x, y \in k$
iii) $|x+y| \leq |x| + |y|$, "triangle inequality"
We say an absolute value $|\cdot|$ is <u>nonarchimedean</u> if also
iv) $|x+y| \leq \max\{|x|, |y|\}$ Note: iv $\Rightarrow$ iii

- Example 0: $k = \mathbb{C}$. For $z = a+bi$, $a, b \in \mathbb{R}$,
$$|z| := \sqrt{z\bar{z}} = \sqrt{a^2+b^2}$$

Picture of triangle inequality:



- Example 1: $k = \mathbb{Q}$. The "usual" absolute value

$$|x|_\infty = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

- Example p

  - $k = \mathbb{Q}$. Want: highly divisible by p = "small"
  - We measure divisibility by p with a "valuation"

$$v_p : \mathbb{Z} - \{0\} \longrightarrow \mathbb{R}$$

as follows. For each $n \in \mathbb{Z} - \{0\}$, let $v_p(n)$ be the unique integer s.t

$$n = p^{v_p(n)} n' \quad \text{with } p \nmid n'$$

★ Examples:

$n = 200$.

②	①
$200 = 5^2 \cdot 8$	$v_5(200) = 2$
$200 = 3^0 \cdot 200$	$v_3(200) = 0$
$200 = 2^3 \cdot 25$	$v_2(200) = 3$

- We extend v_p to $\mathbb{Q}^\times$ via

$$v_p\left(\frac{a}{b}\right) := v_p(a) - v_p(b)$$

and set $v_p(0) := +\infty$.

★ Examples:

$x = 3/200$

$5^{-2} \cdot 3/8$	$v_5(x) = -2$
$3^{1} \cdot 1/200$	$v_3(x) = 1$
$2^{-3} \cdot 3/25$	$v_2(x) = -3$

$$\boxed{\begin{array}{l}\text{Prop 1: Let } x,y \in \mathbb{Q}. \\ 1.\ v_p(xy) = v_p(x) + v_p(y) \\ 2.\ v_p(x+y) \geq \min\{v_p(x), v_p(y)\}\end{array}}$$

like log

Proof sketch: suppose $x, y \in \mathbb{N}$.

1. $x = p^{v_p(x)} n_x, \ y = p^{v_p(y)} n_y$

2. WLOG $v_p(x) \geq v_p(y)$.

$$x+y = p^{v_p(x)} n_x + p^{v_p(y)} n_y$$
$$= \underbrace{p^{v_p(y)} \left(p^{v_p(x) - v_p(y)} n_x + n_y \right)}_{v_p \geq v_p(y)}$$

False for 10-adics!

- We now define an absolute value in which highly divisible by $p \Leftrightarrow$ small. We set

$$\boxed{\begin{array}{ll} |x|_p = p^{-v_p(x)} & \text{if } x \neq 0 \\ |0|_p = 0 & \end{array}}$$

* Examples:

$$|3/200|_5 = 5^2 = 25$$

$$|3/1200|_3 = 3^{-1} = 1/3$$

p-atalanta step $\rightarrow$ $|4 \cdot 5^4|_5 = 5^{-4} = 1/625$

Atalanta step $\rightarrow$ $|1/2^{10}|_2 = 2^{10} = 1024$

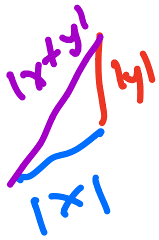
So... if $p=2$... then $1/2^{10}$ is....

Prop 2
$|\cdot|_p$ is an absolute value, and it is nonarchimedean.

Proof: $p^{\text{proposition 1}}$.

2.2 Nonarchimedean Journey

- These metrics have cool features!



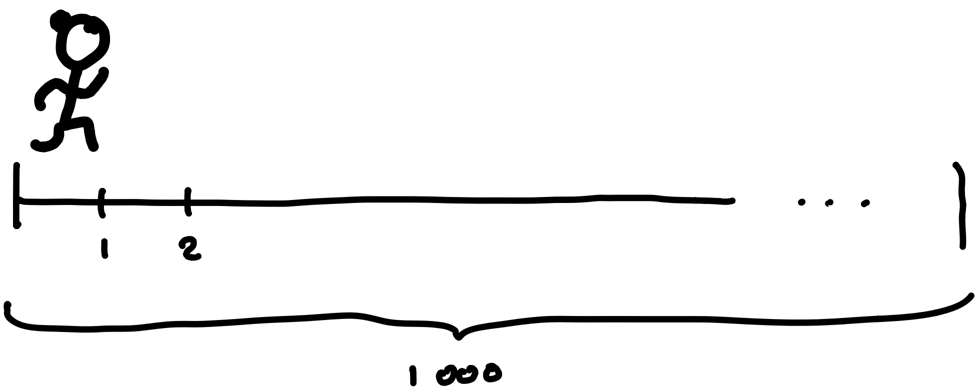
Prop 3 "All Δs are isosceles"
If $|\cdot|$ is a nonarchimedean absolute value, then if $|x| \neq |y|$, then $|x+y| = \max\{|x|, |y|\}$

Proof: WLOG, suppose $|x| > |y|$. Then

$$|x+y| \leq |x| = |x+y-y| \leq \max\{|x+y|, |y|\}$$

$$\Rightarrow |x| = |x+y| \qquad \blacksquare$$

- Very different from arch. abs. value
  - Arch Ex: Atalanta running 1 m at a time:



$$|1+1|_\infty = 2 \not\leq \max\{1, 1\}.$$

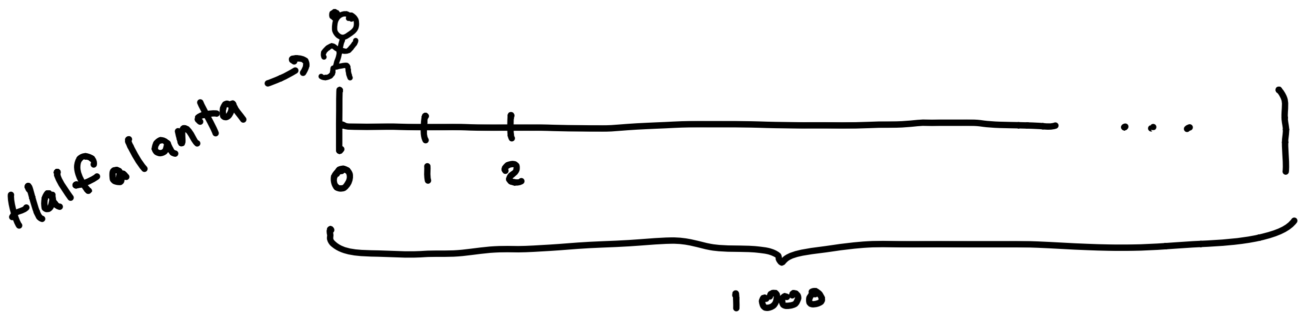
- Nonarch: easy to calculate, sometimes!
  - $\left|\underbrace{1}_{1} + \underbrace{1\cdot 5}_{1/5}\right|_5 = \max\{|1|, |5\cdot 1|\} = 1$
  - $|4\cdot 5 + 4\cdot 5^2|_5 = \max\{|4\cdot 5|, |4\cdot 5^2|\} = \frac{1}{5}$

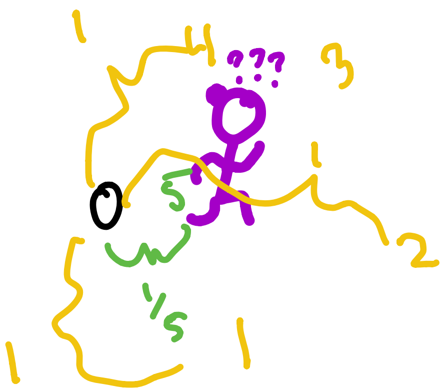
$$\overset{1/5}{} \qquad \overset{1/5^2}{}$$

$$* \; |1 + 4|_5 = |5| = \tfrac{1}{5} \not> \max\{|1|, |4|\}$$

$$1 \qquad 1$$

- A journey of a thousand meters...





> **Prop 4:**
> Let k be a field and let ϕ be the unique nonzero ring homomorphism $\phi : \mathbb{Z} \to k$, which sends $n \mapsto \underbrace{1 + 1 + \dots + 1}_{n \text{ times}}$. Then an abs. val. $|\cdot|$ is nonarchimedean iff $|\phi(n)| \leq \; \forall n \in \mathbb{Z}$.

p-adic integers are $x \in \mathbb{Q}_p$ with $|x|_p \leq 1$

Proof: $\Rightarrow$ induction on n, $|n+1| \le \max\{|n|, 1\} \le 1$ (iv).

$\Leftarrow$ by previous reasoning, ETS $|x+1| \le \max\{|x|, 1\}$.

$$|x+1|^n = \left|\sum_{i=0}^{n} \binom{n}{i} x^i\right| \le \sum_{i=0}^{n} \left|\binom{n}{i}\right| |x^i| \le \sum_{i=0}^{n} |x|^i \le (n+1)\max\{1, |x|^n\}$$

so $|x+1| \le (n+1)^{1/n} \max\{1, |x|\}$. Take $\lim_{n\to\infty}$.

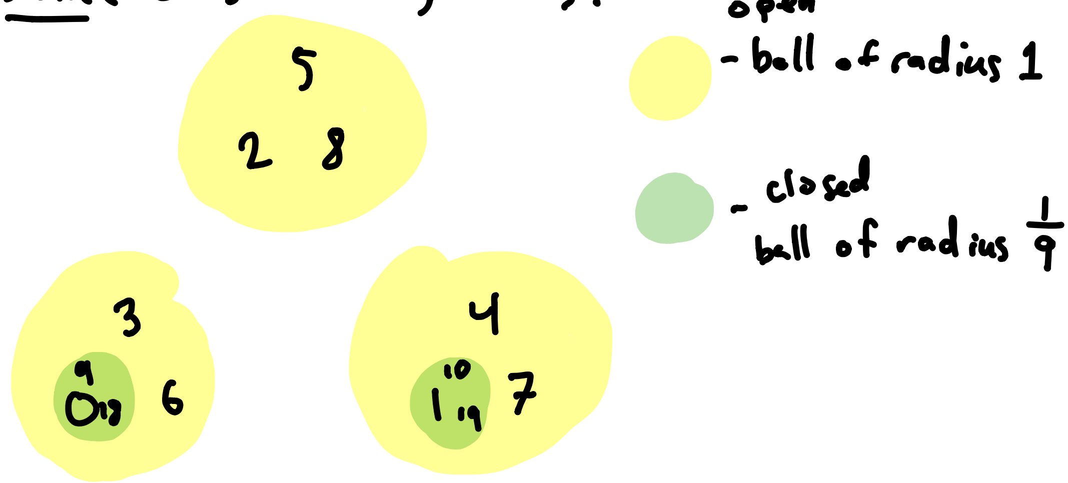
- In archimedean norms, integers can be arbitrarily large.

2.3 Having a Ball

Definitions: For $x, y \in k$, and $|\cdot|$ an abs. val on k

- the <u>distance</u> between x, y is $d(x,y) := |x-y|$
- the <u>open ball centered at x with radius r</u> is
$$B(x,r) := \{z \in k : |z-x| < r\}$$
- the <u>closed ball centered at x with radius r</u> is
$$B_{cl}(x,r) := \{z \in k : |z-x| < r\}$$

• Examples: some elts of $\mathbb{Q}$, $|\cdot|_3$.

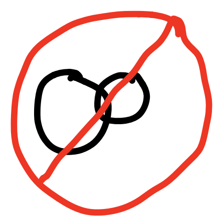


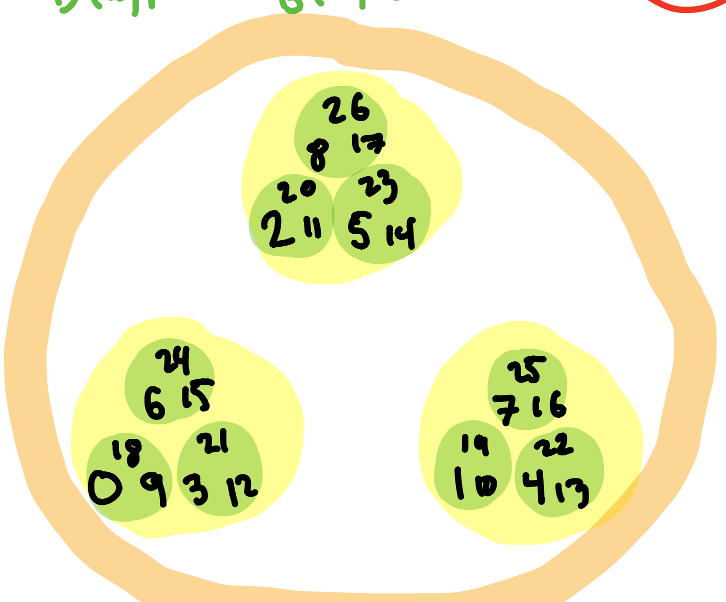
Prop 4: Amazing ball facts! Let $x \in k$, let $|\cdot|$ nonarch. abs. val, and let $r \in \mathbb{R}_{>0}$.

1. If $z \in B(x,r)$, then $B(x,r) = B(z,r)$
2. $B(x,r)$ is closed
3. $B_{cl}(x,r)$ is open
4. If $z \in k$ and $s \in \mathbb{R}_{>0}$ with $s \le r$, then if $B(x,r) \cap B(z,s) \neq 0$, then $B(z,s) \subseteq B(x,r)$

Proof: 1-3: exercise.

4: let $w \in \underbrace{B(x,r)}_{= B(w,r)} \cap \underbrace{B(z,s)}_{= B(w,s)}$. $\rightsquigarrow$





2.4 Common Values

- Is this just some anomalous outlier?

Definition: We say two abs. vals $|\cdot|$ and $|\cdot|'$ on k are <u>equivalent</u> if $\exists\, \alpha \in \mathbb{R}_{>0}$ s.t. $\forall x \in k$, $|x|' = |x|^\alpha$

- More characterisations: exercise

Ostrowski's Theorem
Every nontrivial absolute value $|\cdot|$ on $\mathbb{Q}$ is equivalent to $|\cdot|_p$ for some prime p (if $|\cdot|$ is nonarchimedean) or $|\cdot|_\infty$ (if $|\cdot|$ is nonarchimedean)

Proof sketch:

- Suppose $|\cdot|$ is archimedean.

  Let n_0 be the least elt of $\mathbb{N}$ s.t. $|n_0| > 1$, and let $\alpha \in \mathbb{R}$ s.t.
  $$|n_0| = n_0^\alpha$$
  We'll show that for this α,
  $$|n| = n^\alpha \quad \forall\, n \in \mathbb{N}.$$
  The result will follow by multiplicativity. So let $n \in \mathbb{N}$.
  We write $n = b_0 + b_1 n_0 + b_2 n_0^2 + \cdots + b_k n_0^k$ with $0 \le b_i < n_0$
  So $|n| \le |b_0| + |b_1| n_0^\alpha + |b_2| n_0^{2\alpha} + \cdots + |b_k| n_0^{k\alpha}$
  $$\le 1 + n_0^\alpha + n_0^{2\alpha} + \cdots + n_0^{k\alpha}$$
  $$\le n_0^{k\alpha} \boxed{\frac{n_0^\alpha}{n_0^\alpha - 1}} \quad \text{(geom. series)}$$

!! $C > 0$

$\leq C n^{\alpha}$

doesn't depend on n

So $\forall N \in \mathbb{N}$, $\quad |n^N| \leq C n^{N\alpha}$

$\rightarrow |n| \leq n^{\alpha}$.

Other direction: similar. Bound terms, take limit.

- Suppose $|\cdot|$ is nonarchimedean.
  Let n_0 be the smallest elt of $\mathbb{N}_{>0}$ s.t. $|n_0| < 1$.
  By mult. & nonarch, n_0 must be prime, let's call it p.
  If $p \nmid n$, then $\exists k \in \mathbb{Z}$ s.t. $n = kp + r$, with $0 < r < p$.

$$\rightsquigarrow |n| = |kp + r| \leq \max\{\underset{\substack{\vee \\ 1}}{|kp|}, \underset{\substack{\shortparallel \\ 1}}{|r|}\} = 1.$$

Lastly, any $n \in \mathbb{N}_{>0}$ can be written as

$n = p^n n'$ with $p \nmid n'$, and so

$|n| = |p|^n$. ∎

- Not only do we know all absolute values, but they fit together beautifully!

$$\boxed{\text{Product Formula: for any } x \in \mathbb{Q}, \text{ we had} \quad |x|_\infty \prod_{p \text{ prime}} |x|_p = 1}$$

2.5. Completing our Discussion

Definition: let k be a field, $|\cdot|$ an abs. val on k. A sequence of elts $(x_n)_{n\in\mathbb{N}}$ of k is <u>Cauchy</u> if $\forall \varepsilon>0$ $\exists M$: $|x_n - x_m| < \varepsilon$ if $n, m > M$.

- Ex: for $|\cdot|_\infty$ on $\mathbb{Q}$,

$$
\begin{array}{lll}
 & .3 & 3 \\
.03 & .33 & 3.1 \\
.003 & .333 & 3.14 \\
 & \vdots & \vdots
\end{array}
$$

- Ex: for $|\cdot|_5$ on $\mathbb{Q}$,

$$
\begin{array}{lll}
 & 4 & 2 \\
 & 4+4\cdot 5 & 2+3\cdot 5 \\
|4\cdot 5^2| = \frac{1}{5^2} & 4+4\cdot 5+4\cdot 5^2 & 2+3\cdot 5+1\cdot 5^2 \\
|4\cdot 5^3| = \frac{1}{5^3} & 4+4\cdot 5+4\cdot 5^2+4\cdot 5^3 & 2\cdot 3\cdot 5+1\cdot 5^2+3\cdot 5^3 \\
 & \vdots & \vdots
\end{array}
$$

Definition: a field k is <u>complete</u> with respect to an abs. val $|\cdot|$ if every Cauchy sequence has a limit in k

- $\mathbb{Q}$ is not complete w.r.t. $|\cdot|_\infty$. You can find a sequence

$(x_n)_{n\in\mathbb{N}}$ s.t. $\lim_{n\to\infty} x_n^2 = 2$, but $x^2=2$ has no soln. in $\mathbb{Q}$.

- Similarly, for $|\cdot|_7$, we found a sequence $(x_n)_n$ in $\mathbb{Q}$
$$x_n := \sum_{i=0}^{n} b_i 7^i$$
such that $7^{n+1} \mid (x_n^2 - 2)$, so $|x_n^2-2|_7 \le \frac{1}{7^{n+1}}$, so
$$\lim_{n\to\infty} x_n^2 = 2$$
but $x^2=2$ has no soln in $\mathbb{Q}$, so $\mathbb{Q}$ not complete wrt $|\cdot|_7$.

- $\mathbb{R}$ was constructed as a <u>completion</u> of $\mathbb{Q}$ wrt $|\cdot|_\infty$

$$\mathbb{R} := \{ (x_n)_{n\in\mathbb{N}} : x_n \in \mathbb{Q},\ (x_n) \text{ Cauchy wrt } |\cdot|_\infty \} / \sim$$
$$(x_n) \sim (x_n') \text{ if } \lim_{n\to\infty} |x_n - x_n'|_\infty = 0$$

- What if we complete wrt our new metrics? We <u>define</u>

$$\boxed{\begin{gathered}\mathbb{Q}_p := \{ (x_n)_{n\in\mathbb{N}} : x_n \in \mathbb{Q},\ (x_n) \text{ Cauchy wrt } |\cdot|_p \} / \sim \\ (x_n) \sim (x_n') \text{ if } \lim_{n\to\infty} |x_n - x_n'|_p = 0\end{gathered}}$$

2.6 Old $\mathbb{Q}_p$ vs New $\mathbb{Q}_p$?

Prop 5: Cauchy is easy!
Let $|\cdot|$ be a nonarch. abs. val. on a field k. Then $(x_n)_{n\in\mathbb{N}}$ is a Cauchy sequence if and only if
$$\lim_{n\to\infty} |x_{n+1} - x_n| = 0$$

Proof: If $m > n$, write $m = n + r$. Then
$$|x_m - x_n| = |x_{n+r} - x_{n+r-1} + x_{n+r-1} - \cdots + x_{n+1} - x_n|$$
$$\leq \max\{|x_{n+r} - x_{n+r-1}|, \ldots, |x_{n+1} - x_n|\}.$$

Corollary 6: series convergence is easy!
Let $|\cdot|$ be a nonarch. abs. val. on a field k. Let $(s_i)_{i\in\mathbb{N}}$ be a sequence of elts of k, and let
$$\sigma_n = \sum_{i=0}^{n} s_n$$
be a sequence of sums.

If $\lim_{n\to\infty} |s_n| = 0$, then σ_n is Cauchy.

Proof: $|\sigma_{n+1} - \sigma_n| = |s_n|$, prop 5.

- Recall: A sequence of integers $(a_n)_{n\in\mathbb{N}}$ s.t. $0 \leq a_n \leq p^n - 1$ is coherent if $\forall n \geq 1$,
$$a_n \equiv a_{n+1} \pmod{p^n}.$$

Prop 7: let p be a prime.
If $(a_n)_{n\in\mathbb{N}}$ is a coherent sequence of integers, then $(a_n)_{n\in\mathbb{N}}$ is Cauchy w.r.t. $|\cdot|_p$.

Proof: $p^n \mid (a_{n+1} - a_n) \Rightarrow |a_{n+1} - a_n|_p \leq \frac{1}{p^n}$.

$\Rightarrow \lim_{n\to\infty} |a_{n+1} - a_n|_p = 0$.

Prop 5 gives the result. ∎

Prop 8: let p be a prime.
Let $(b_i)_{i=n_0}^{\infty}$ be a sequence with $b_i \in \{0, 1, \ldots, p-1\}$, $n_0 \in \mathbb{Z}$. Let $a_n = \sum_{i=n_0}^{n} b_i p^i$.
then (a_n) is Cauchy wrt $|\cdot|_p$.

Proof: $|a_{n+1} - a_n|_p = |b_{n+1} p^{n+1}|_p = \frac{1}{p^{n+1}}$, prop 5 ∎