2021

Arizona Winter School

p-adic Lecture 5: Relearning how to Function ☹

Background image: Fernando Villegas Negrete

NB: throughout this lecture, $|\cdot|$ will denote $|\cdot|_p$

5.1 Functions and Continuity

- We have built up $\mathbb{Q}_p$ as an analogue of $\mathbb{R}$. We want to develop a theory of functions on $\mathbb{Q}_p$

- We define continuity, derivatives like for $\mathbb{R}$:

Definition
Let $U \subseteq \mathbb{Q}_p$ be an open set. A function $f: U \longrightarrow \mathbb{Q}_p$ is <u>continuous</u> at $x_0 \in U$ if $\forall \varepsilon > 0 \ \exists \delta > 0$ s.t.
$$|x - x_0| < \delta \implies |f(x) - f(x_0)| < \varepsilon.$$

- Ex: polynomials in X cts everywhere, same proof as in $\mathbb{R}$
- Nonex: $f(x) = 1/x$ for $x \neq 0$ and $f(0) = 0$, since $\lim_{n\to\infty} p^n = 0$ but $\left|\frac{1}{p^n}\right| \to \infty$

Definition
Let $U \subseteq \mathbb{Q}_p$ be an open set. A function $f: U \longrightarrow \mathbb{Q}_p$ is <u>differentiable</u> at $x_0 \in U$ if the limit
$$f'(x_0) = \lim_{h\to 0} \frac{f(x_0+h) - f(x_0)}{h} \quad \text{exists.}$$
If $f'(x_0)$ exists $\forall x_0 \in U$ we say f is differentiable in U.

- Ex: polys in X differentiable everywhere, same proof as in $\mathbb{R}$, and for $f(X) = X^n$, $f'(X) = nX^{n-1}$

- We can also state the mean value theorem, but it's false!

- Also, there are functions which are not loc. constant, but whose deriv. is the zero function!

Ex: $f: \mathbb{Z}_p \to \mathbb{Q}$, $f\left(\sum_{i=0}^{\infty} a_i p^i\right) = \sum_{i=0}^{\infty} a_i p^{2i}$

$12121\cdots \mapsto 10201\cdots$

- We can't do calculus etc the same way as in $\mathbb{R}$.

5.2 A Series of Fortunate Events

- We focus now on functions defined by power series (in $\mathbb{R}$ this is how e^x and $\sin x$ arise)

- Given a power series, we want to determine where it defines a function (i.e. where it converges, the region of convergence)

> **Theorem 5.3**
> Let $f(X) = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{Q}_p[[X]]$ and define
> $$\rho = \frac{1}{\limsup \sqrt[n]{|a_n|}}.$$
> 1. If $\rho = 0$, then $f(x)$ converges iff $x = 0$.
> 2. If $\rho = \infty$, then $f(x)$ converges $\forall x \in \mathbb{Q}_p$
> 3. If $0 < \rho < \infty$, and $\lim_{n\to\infty} |a_n| = 0$, then $f(x)$ converges iff $|x| \le \rho$.
> 4. If $0 < \rho < \infty$, and $\lim_{n\to\infty} |a_n| \neq 0$, then $f(x)$

more straightforward than in $\mathbb{R}$

converges iff $|x|<\rho$.

5. Let $D_f = \{x \in \mathbb{Q}_p : f(x) \text{ converges}\}$. The function
$$f : D_f \to \mathbb{Q}_p, \quad x \mapsto f(x)$$
is continuous.

Proof:

Caution! *If the series $\sum_{n=1}^{\infty} x_n$ converges, then $(x_n)_{n\in\mathbb{N}}$ is a null sequence, but the converse is false!*

courtesy of Joanne Beckford

$\mathbb{Q}_p$:

Follows from the fact that $\sum a_n x^n$ converges iff $\lim |a_n x^n| = 0$.

The proof for 5 is identical to the proof over $\mathbb{R}$. $\boxtimes$

- Example: $f(X) = \sum p^n X^n$.

$$\rho = \limsup \frac{1}{\sqrt[n]{|p|^n}} = \limsup \frac{1}{|p|} = p, \text{ and } |a_n| \to 0$$
so $D = B_{cl}(0, p)$.

- Example: $g(X) = \sum X^n$, $\rho = 1$, $|a_n| \not\to 0$
  Region of convergence for g: $B(0,1) = p\mathbb{Z}_p$

- We can define sum & product power series, and they are sum & product <u>as functions</u>

  For $f(X) = \sum a_n X^n$, $g(X) = b_n X^n$,

  $$(f+g)(X) := \sum (a_n + b_n) X^n$$

  $$(fg)(X) := \sum_{n=0}^{\infty} \sum_{k=0}^{n} a_k b_{n-k} X^n$$

- Can the composition $f \circ g$ be written as a power series? If so, how?
  - Solve recursively for what the coeffs of $h(X) = (f \circ g)(X)$ would have to be, call that the <u>formal composition</u>

> **Proposition 5.4**
> Let $f, g, h \in \mathbb{Q}_p[\![X]\!]$ be as above. Let $x \in \mathbb{Q}_p$ and suppose
> 1. $g(x)$ converges
> 2. f converges at $g(x)$
> 3. $\forall n$ $|b_n x^n| \leq |g(x)|$
>
> Then $h(x)$ converges and $f(g(x)) = h(x)$

- Note: false without 1, 2, 3 !

- What else might we want to do? Recenter a power series. Where would the new series converge?

Theorem 5.5

Let $f(X) = \sum a_n X^n$, and let $\alpha \in D_f$ (f converges at α).
For each $m \geq 0$, define

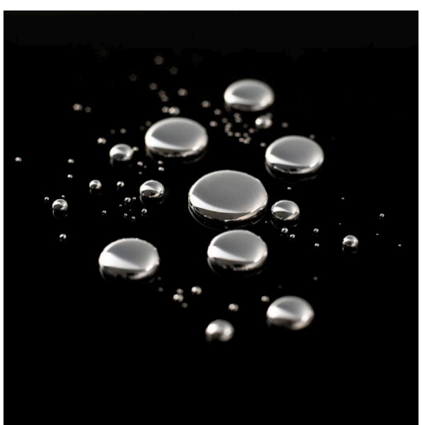
$$b_m := \sum_{n \geq m} \binom{n}{m} a_n \alpha^{n-m}$$

$$g(X) := \sum_{m=0}^{\infty} b_m (X-\alpha)^m.$$

1. The series defining b_m converges $\forall m$
2. $D_f = D_g$ (same region of convergence!)
3. For any $x \in D_f$, $f(x) = g(x)$.

Proof: omitted (see Gouvea 5.4.2)

But we note: ETS f, g have same <u>radius</u> of convergence since $\alpha \in D_f \cap D_g$ and p-adic disks "are either concentric or disjoint, like drops of mercury" – Yves Andrès



- This is a cool fact, but it means we can't do analytic continuation like we do in $\mathbb{C}$.

- On to derivatives and differences:

Theorem 5.6
Let $f, g \in \mathbb{Q}_p[[X]]$, and suppose there is a non-stationary (i.e. not eventually constant) sequence $x_m \in \mathbb{Q}_p$: $\lim x_m = 0$ s.t. $f(x_m) = g(x_m)$ $\forall m$. Then $f(X) = g(X)$ (same coefficients!)

Proof sketch: Same as for $\mathbb{R}$. WTS difference is 0 power series. If $h \in \mathbb{Q}_p[[X]]$, $h(x_n) \to$ const. term of h. ∎

Theorem 5.7
Let $f(X) = \sum a_n X^n \in \mathbb{Q}_p[[X]]$ and let f' be the formal derivative of $f(X)$. Let $x \in \mathbb{Q}_p$. If $x \in D_f$ then $x \in D_{f'}$ and

$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h}$$

Proof: if $x \neq 0$, we see

$$|n a_n x^{n-1}| \leq |a_n x^{n-1}| = \frac{1}{|x|} |a_n x^n| \to 0$$

so $f'(x)$ converges.

Next, let $r \in \mathbb{Q}: D_f = B_{cl}(0, r)$. Suppose $|h| < |x| \leq r$ then

$$\frac{f(x+h) - f(x)}{h} = \sum_{n=1}^{\infty} \sum_{m=1}^{n} a_n \binom{n}{m} x^{n-m} h^{m-1}.$$

then $\left| a_n \binom{n}{m} x^{n-m} h^{m-1} \right| \leq \underbrace{|a_n| r^{n-1}}_{\to 0}$, does not depend on h

So we can set $h = 0$ and

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

$\square$

- Our coveted result follows immediately!

> **Theorem 5.8**
> Suppose $f, g \in \mathbb{Q}_p[\![X]\!]$ and that f, g converge for $|x| < \rho$. If $f'(x) = g'(x)\ \forall |x| < \rho$, then $\exists$ a constant $C \in \mathbb{Q}_p$: $f(x) = g(X) + C$.

Proof: f', g' have the same coefficients, hence so do f, g aside from potentially the constant term. $\square$

5.3 Rooting Around (because pigs root around)

- We now explore the zeros of functions defined by power series

- But first, an important and useful topological fact:

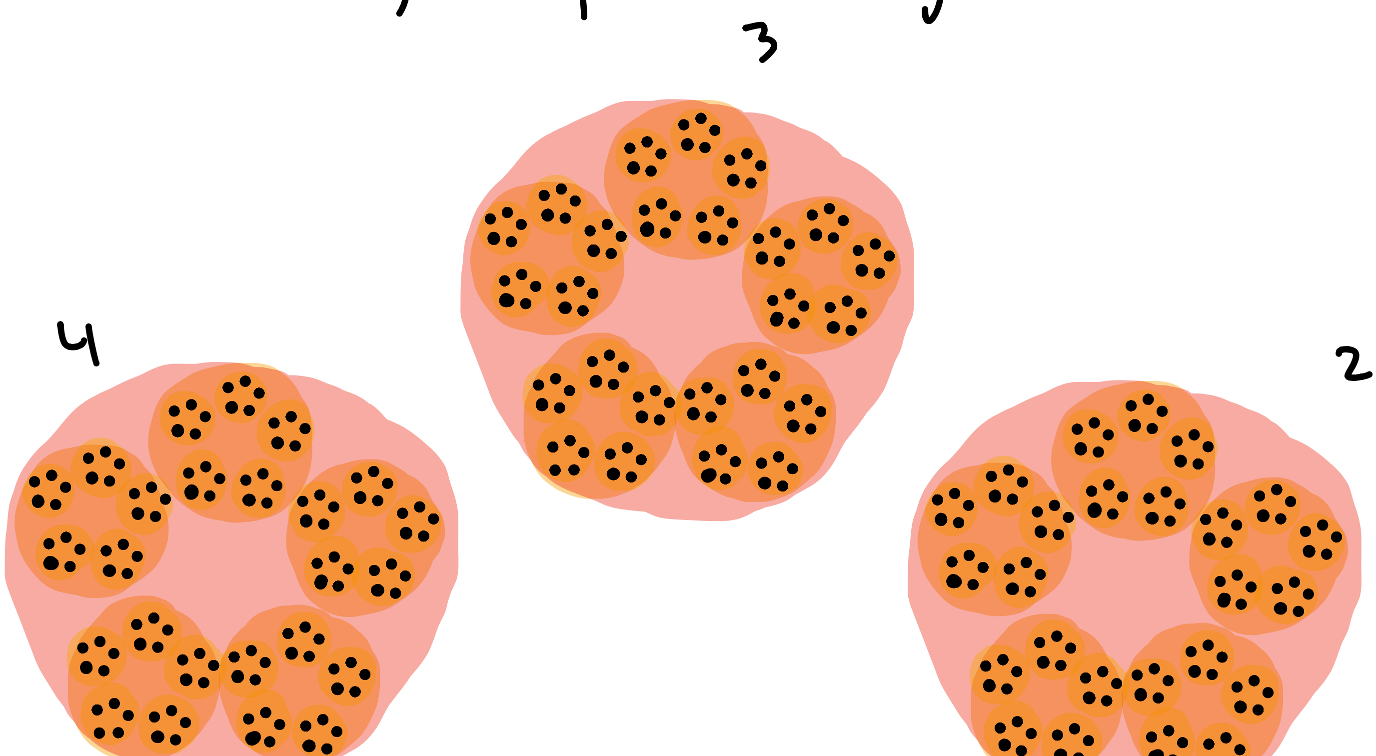
Theorem 5.9

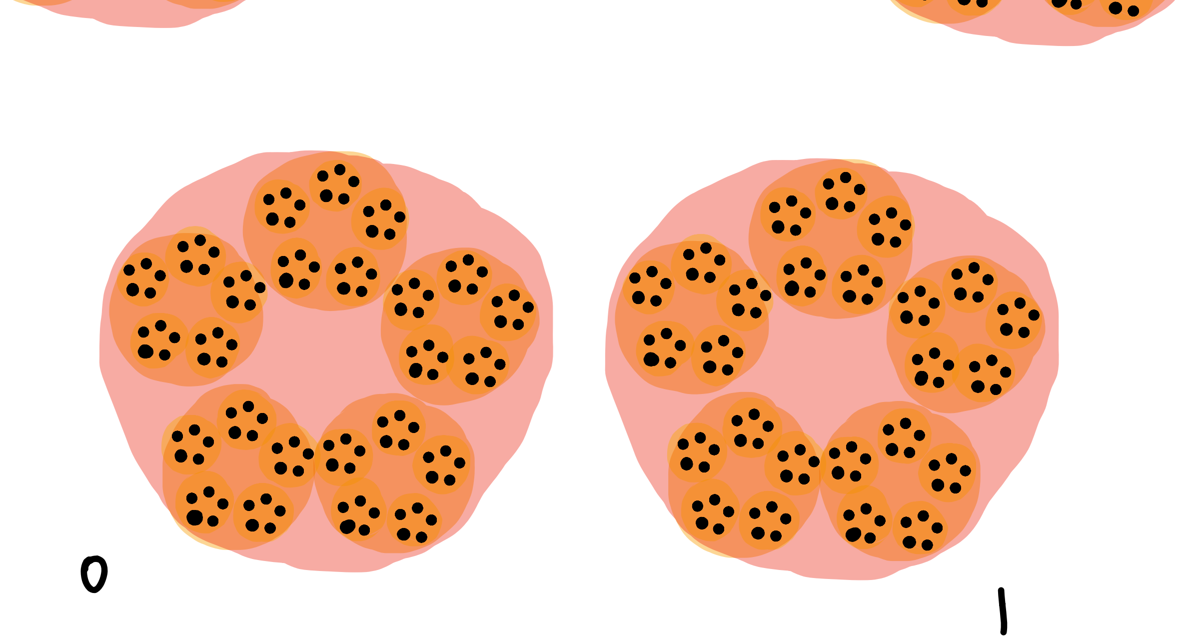
$\mathbb{Z}_p$ is compact

Proof: $\mathbb{Z}_p$ is a closed subset of $\mathbb{Q}_p$, which is complete, so $\mathbb{Z}_p$ is complete.
And for $\varepsilon > 0$, $\exists\, N \in \mathbb{N} : p^{-N} < \varepsilon$. And

$$\mathbb{Z}_p = \bigcup_{i=0}^{p^N - 1} i + p^N \mathbb{Z}_p$$

is a covering of $\mathbb{Z}_p$ by finitely many balls of radius $< \varepsilon$, so $\mathbb{Z}_p$ is also totally bounded. $\blacksquare$





- Back to the zeros:

Strassman's Theorem
Let $f(X)=\sum_{n=0}^{\infty} a_n X^n$ be a nonzero elt of $\mathbb{Q}_p[\![X]\!]$.
Suppose $\lim_{n\to\infty} a_n = 0$ (so $f(x)$ converges $\forall x\in\mathbb{Z}_p$).
Let N be the integer s.t.

$$|a_N| = \max_{n\in\mathbb{N}} |a_n| \quad \text{and} \quad |a_n|<|a_N| \text{ for } n>N.$$

Then the function $f:\mathbb{Z}_p\to\mathbb{Q}_p$, $x\mapsto f(x)$ has at most N zeros.
Also, if $\{\alpha_1,\dots,\alpha_m\}$ are the zeros of f, then $\exists g\in\mathbb{Q}_p[\![X]\!]$:

$$f(X)=(X-\alpha_1)\cdots(X-\alpha_m)g(X)$$

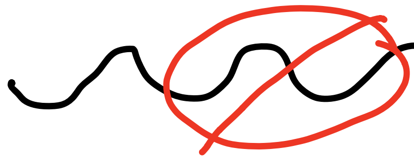
s.t. g converges on $\mathbb{Z}_p$ and has no zeros in $\mathbb{Z}_p$.

Proof sketch: induct on N, rearrange series to factor out $X-\alpha$ for α a root (Gouvea 5.4.6).

- Consequences: f has fin. many zeros in $\mathbb{Z}_p$

- If f, g agree on infinitely many points in some disk $p^m\mathbb{Z}$, then $f = g$ as power series

- f cannot be "periodic" if f is nonconstant!
  If $\exists\, \pi \in p^n\mathbb{Z} : f(x+\pi) = f(x)\ \forall x \in p^m\mathbb{Z}$, f constant.



NO!

- Next: roots <u>beyond</u> $\mathbb{Q}_p$ ö

- We'll take the following theorem as a black box:

Theorem 5.11: Complex #s but make it p-adic

There exists a field $\mathbb{C}_p$ and a valuation $v_p(\cdot)$ on $\mathbb{C}_p$ (and hence nonarch abs. val $|\cdot| = p^{-v_p(\cdot)}$ on $\mathbb{C}_p$ s.t.

1. $\overline{\mathbb{Q}}_p \subset \mathbb{C}_p$ and $|\cdot|$ extends $|\cdot|_p$
2. $\mathbb{C}_p$ is complete & algebraically closed
3. $\overline{\mathbb{Q}}_p$ is dense in $\mathbb{C}_p$
4. $\{v_p(x) : x \in \mathbb{C}_p\} = \mathbb{Q}$

Tool for investigating roots:

Definition: Let $K = \mathbb{C}_p$ or a fin. ext. of $\mathbb{Q}_p$.
Let $f = a_0 + a_1 X + \cdots + a_n X^n \in K[X]$. Then the Newton polygon of f, denoted $NP_p(f)$, is the lower convex hull in $\mathbb{R}^2$ of the points

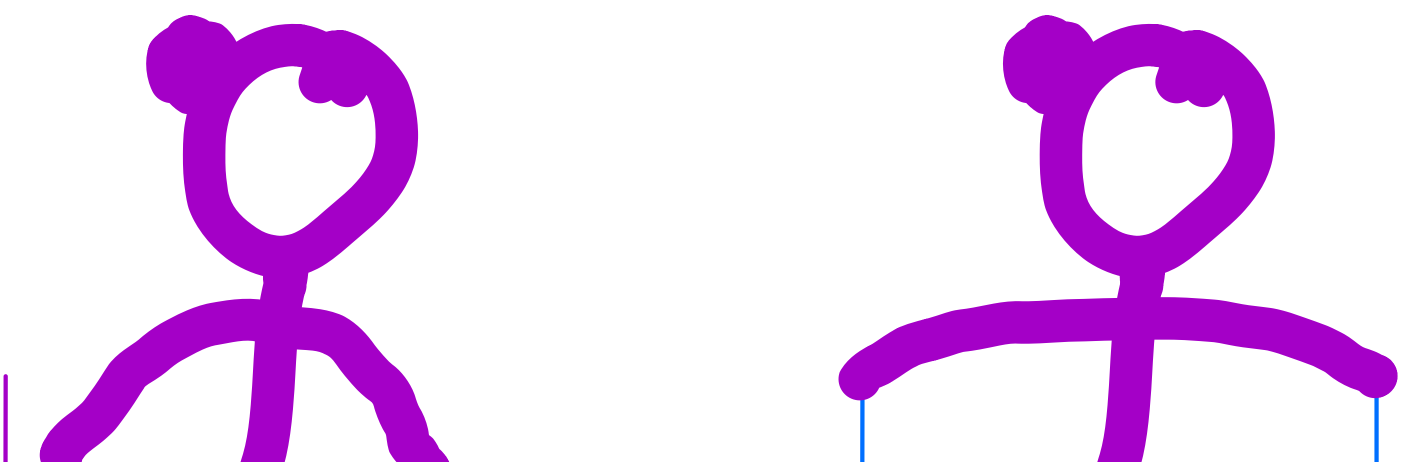
$$S = \{(i, v_p(a_i)) : i = 0, 1, \ldots, n \text{ and } a_i \neq 0\}$$

- Procedure: let rope hang below points of S, pull upward until it is taut

- Example: $NP_5(f)$

$$f(x) = 1 + 5x + \tfrac{1}{5}x^2 + 35x^3 + 25x^5 + 625x^6$$

$$S = \{ (0,0) \quad (1,1) \quad (2,-1) \quad (3,1) \quad (5,2) \quad (6,4) \}$$



blue polygon $= NP_5(f)$

- We define the "width" of a line segment as the length of its projection onto the x-axis.

- This simple drawing gives us a <u>ton</u> of information about the roots of f.

Theorem 5.13
Let $f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in K[X]$. Let $m_1, \dots, m_r$ be the slopes of $NP_p(f)$, with corresponding widths $w_1, \dots, w_r$. Then for each $k: 1 \le k \le r$, $f(X)$ has exactly w_k roots (in $\mathbb{C}_p$, counting multiplicity) with abs. val p^{m_k} (so valuation $-m_k$).

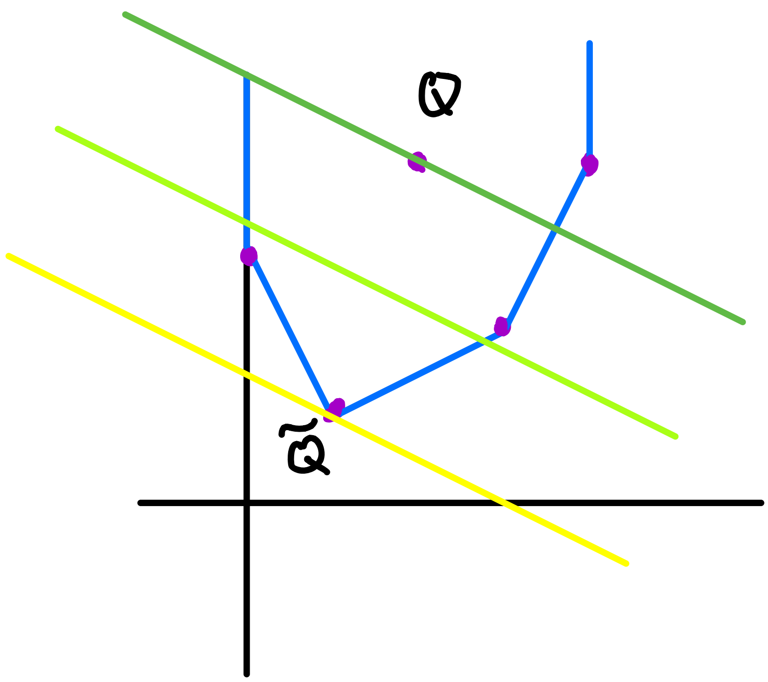
(partial) Proof: we will show that if $f(\alpha) = 0$, then $-v_p(\alpha)$ is a slope of $NP_p(f)$.

$$v_p(0) = v_p(f(\alpha)) = v_p\left(\sum_{i=0}^{n} a_i \alpha^i\right) \geq \min_i v_p(a_i \alpha^i)$$
$$= \min_i \{(v_p \alpha) \cdot i + v_p(a_i)\}$$
$$= \min\{(v_p \alpha) \cdot x + y : (x,y) \in S\}$$

- If the min is uniquely attained, $\geq$ becomes $=$, contradiction.

- We minimize $g(x,y)$, where $g(x,y) = (v_p \alpha) x + y$

- Claim: the min of g over points of S must occur at an extremal point of $NP_p(f)$.



- $(v_p \alpha) x + y = c$ is a line of slope $-v_p \alpha$.
  = points s.t. $g(x,y) = c$
- $(v_p \alpha) x + y = c' < c$
- $(v_p \alpha) x + y = c'' < c$

$\rightsquigarrow$ g smaller at $\tilde{Q}$.

Corollary 5.14: Eisenstein's Criterion

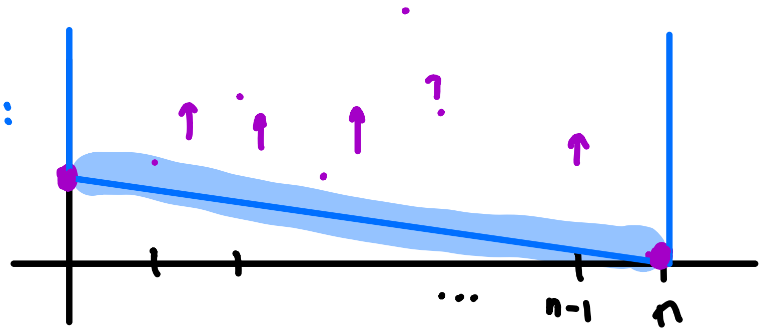
Let $p \in \mathbb{Z}$ be a prime and let

$$f(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + X^n \in \mathbb{Z}[X]$$

such that $p \mid a_i \ \forall i < n$ and $p^2 \nmid a_0$.
Then f is irreducible over $\mathbb{Q}$.

Proof:

$NP_p(f)$:



one line segment
slope $-\frac{1}{n}$
width n

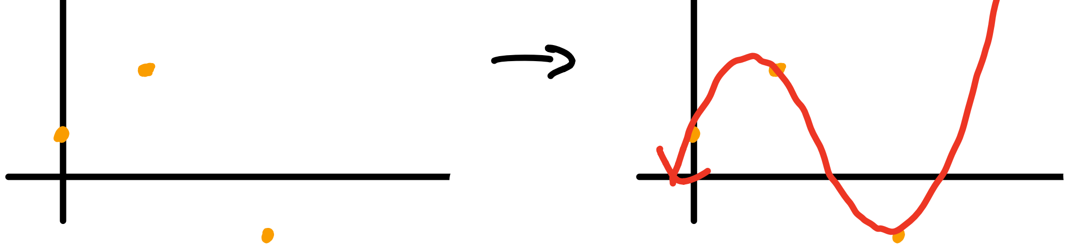
- By theorem, all roots of f have valuation $\frac{1}{n}$.
- But if α is a root of $g \in \mathbb{Q}[X]$ and g has degree d, then $v_p(\alpha) \in \frac{1}{d}\mathbb{Z}$.

(ex: if $\alpha^2 = p^3$, $2v_p(\alpha) = 3$ so $v_p(\alpha) = \frac{3}{2}$)

5.4 Connecting the Dots (another way)

- We will now step back and talk about how to construct p-adic functions via <u>interpolation</u>

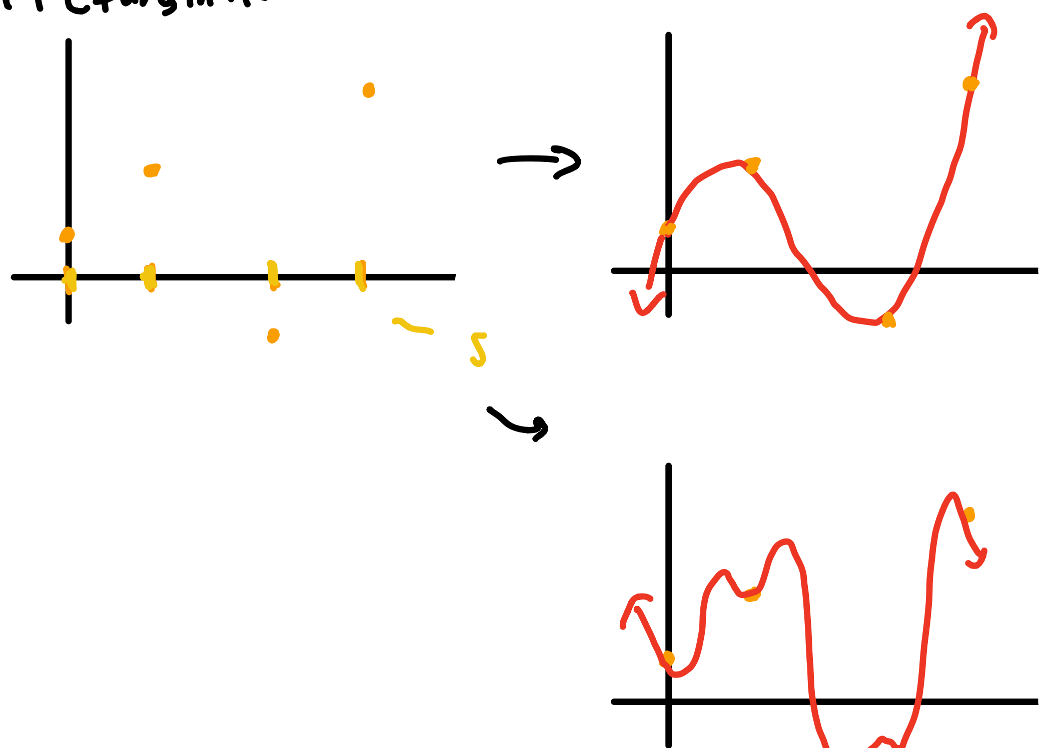
- Picture in $\mathbb{R}$:

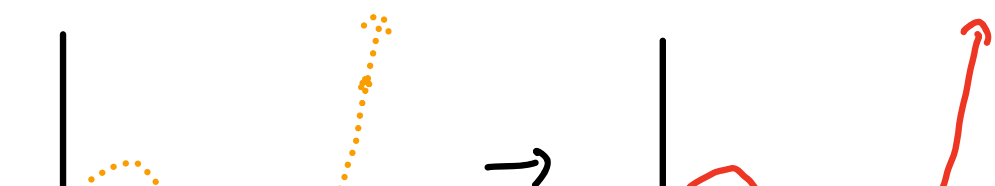


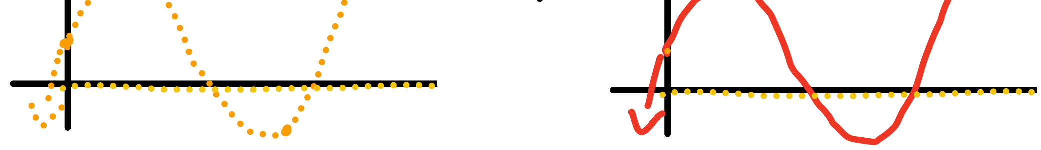
- Example in $\mathbb{Q}_p$: if $c \in \mathbb{Z}_p$ and $a \in \mathbb{Z}$, we can define
$$f(a) = c^a = c \cdot \underbrace{c \cdots}_{a \text{ times}} \cdot c$$
(or $f(c) = \frac{1}{c} \cdots \frac{1}{c}$ $-a$ times if $a < 0$).

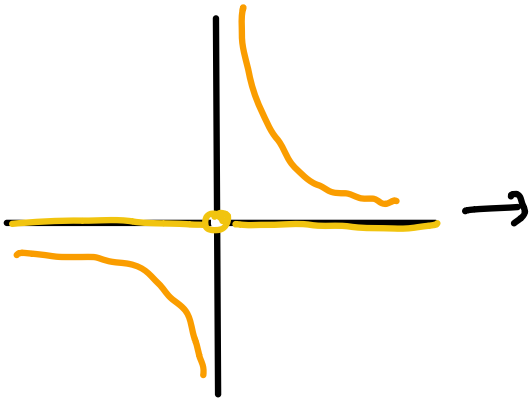
  - want to extend f to a function defined on more of $\mathbb{Q}_p$

- Pictures in $\mathbb{R}$:









???

Definition

For a valued field K and set $S \subseteq K$, a function $f : S \to K$ is <u>uniformly continuous</u> if $\forall \varepsilon > 0$ $\exists \delta > 0$ s.t. $\forall x, y \in S$,

$$|x-y| < \delta \Rightarrow |f(x) - f(y)| < \varepsilon.$$

same δ works $\forall x$!

Proposition 5.16

Let $S \subseteq \mathbb{Z}_p$ be a dense subset, and let $f : S \to \mathbb{Q}_p$ be a function. Then $\exists$ a continuous extension $\tilde{f} : \mathbb{Z}_p \to \mathbb{Q}_p$ of f to $\mathbb{Z}_p$ iff f is bounded and uniformly continuous. If $\tilde{f}$ exists, it is unique.

Proof: any extension $\tilde{f}$ is unique by density of S.

$\Longrightarrow$: If $\tilde{f}$ is cts, it is bdd & unif. cts by compactness of $\mathbb{Z}_p$.

$\Leftarrow$: If $x \in \mathbb{Z}_p$, then $x = \lim x_n$ for $x_n \in S$.

So $\lim |f(x_{n+1}) - f(x_n)| = 0$ since f bdd & unif. cts,

so we define:

$$\mathcal{F}(x) = \lim f(x_n)$$

$\blacksquare$ (?)

- What does this look like in $\mathbb{Q}_p$?

Proposition 5.17

For a set $S \subseteq \mathbb{Q}_p$, a function $f : S \to K$ is <u>uniformly continuous</u> if $\forall m \in \mathbb{Z}\ \exists N \in \mathbb{Z}$:

$$\alpha \equiv \beta \pmod{p^N} \Rightarrow f(\alpha) \equiv f(\beta) \pmod{p^m}$$

- Hence $\uparrow$ + boundedness on a dense set is enough to check for existence of interpolation of a function.