Bijection: $\sum_{i=0}^{\infty} a_i p^i \mid a_i \in \mathbb{Z}_{\leq p-1}$

Why does $\sum_{i=0}^{\infty} a_i p^i$ converge?

$|a_i p^i|_p \leq p^{-i} \to 0$ so $\sum_{i=0}^{\infty} a_i p^i$ converges.

Or: $v_p (\sum_{i=0}^{\infty} a_i p^i - \sum_{i=0}^{\infty} b_i p^i) = \text{first index } i$ s.t. $a_i \neq b_i$.

If $x, y \in \mathbb{Z}_p$, $x \neq y$ then $\exists k \forall k \neq x \neq y (p^k)$

Map $\mathbb{Z}_p \to \prod \mathbb{Z}/p^k \mathbb{Z}$ is injective.

HW: $\mathbb{Z}_p = \{ x \in \prod \mathbb{Z}/p^k \mathbb{Z} \mid x_{k+1} = x_k (p^k) \}$. (If know image of $x$ in $\mathbb{Z}/p^k \mathbb{Z}$, it determines the image mod $p^l$ for $l \leq k$)

($\mathbb{Z}_p$ is the prof-p completion of $\mathbb{Z}$)
realizes \( \Omega \) as \( \lim_{p \to p^k} \Omega_{p^k} \) which is \( \mathcal{C} \) as a closed subset of \( \bigcap_{1}^{\infty} \Omega_{p^k} \).

From this pov, \( \Sigma_{p^k} \) converges because residue mod \( p^k \) is eventually constant.

---

Last time: "functional analysis":

Thm: \( F \) complete with nontrivial absolute value.
Then unique topology on \( F \). \( F \)-usf making it a TVS, any \( F \)-subspace of an \( F \)-TVS is closed.

Cor: \( \mathbb{Q} \) algebraic have at most one extension of \( L \) to \( L \).
Assume \( F \) is non-archimedian

Thm: (Hensel's lemma) for \( \frac{\mathbb{Q}}{\mathbb{Z}} \)

1. If have \( x \in F \) st. \( | \frac{f(x)}{f'(x)} | < 1 \), then have \( y \in F \) st. \( f(y) = 0 \), \( |y-x| < C \).

2. Suppose \( f = \text{image of } f \) in \( \mathbb{Q}/\mathbb{Z} \) has \( f \neq 0 \) and that \( f = gh \) in \( K[x] \), \( (g, h) = 1 \). Then \( \exists g, h \in \mathbb{Q}[x] \) lifting \( g, h \), st. \( f = gh \), \( \deg g = \deg h \).
(1) Last time (Newton's method)

(2) \( d = \deg f, \ k = \deg \overline{g} \). Choose preimages \( g_0, h_0 \)

\( \rightarrow \overline{g}, \overline{h} \) with \( \deg g_0 = \deg \overline{g} = k, \ \deg h_0 = \deg \overline{h} \).

let \( \pi \in \mathcal{P} \), to be chosen later. Suppose that

for some \( n \), have \( p_i, q_i \in \mathcal{O}[x], 1 \leq i \leq n \) s.t.

\[
\deg p_i < k \quad \deg q_i \leq d \cdot k
\]

s.t. for \( g_n = g_0 + \sum_{i=1}^{n} \pi^i p_i \)

\( h_n = h_0 + \sum_{i=1}^{n} \pi^i q_i \)

have \( f = g_n h_n \ (\Pi^{n+1}) \)

Then for any \( p_{n+1}, q_{n+1} \), have:

\[
f - g_{n+1} h_{n+1} = (f - g_n h_n) - \prod_{n}^{n+1} g_n q_{n+1} - \prod_{n+1}^{n+2} p_{n+1} h_n
\]

\[= (f - g_n h_n) - \prod_{n}^{n+1} (g_n q_{n+1} + p_{n+1} h_n) \ (\Pi^{n+2})\]
So \( \prod^{(h+1)} (f - g_{h+1} h_{\nu h}) = \frac{f - g_n h_n}{\prod^h (h_{\nu h})} - (g_n g_{h+1} + p_{h+1} h_n) \) \( (\pi) \)

Goal: Choose \( p_{h+1}, q_{h+1} \) s.t. RHS is 0 mod \( \pi \).

Then \( f - g_{h+1} h_{\nu h} = 0 \) \( (\prod^{h+2}) \)

Want \( p_{h+1}, q_{h+1} \) s.t. \( g_n g_{h+1} + p_{h+1} h_n = \frac{f - g_n h_n}{\prod^h} \) \( (\mu) \)

But \( g_n = g_0 \) \( (\mu) \), \( h_n = h_0 \) \( (\mu) \), so want

\[ g_0 g_{h+1} + p_{h+1} h_0 = \frac{f - g_n h_n}{\prod^h} \] \( (\mu) \).

Applying Bezout in \( k[SxT] \), have \( a, b \in U[S\times T] \)

s.t. \( a g + b h = 1 \) i.e. \( a g_0 + b h_0 = 1 \) \( (\pi') \).

May assume \( 1 > |\nu| > |a g_0 + b h_0 - 1| \).

Max |coeff|

Let \( r_n = \frac{f - g_n h_n}{\prod^h} \). Then since \( a g_0 + b h_0 = 1 \) \( (\pi) \)

\[ g_0 (a r_n) + h_0 (b r_n) = r_n \] \( (\mu) \)
looks like $g_0 q_{n+1} + h_0 p_{n+1} \equiv r_n \pmod{p}$ except 
$\deg(b r_n) \text{ could be } \leq k$.

Key: leading coeff of $g_0$ is in $0^x \circ 0^p$ 
(eq. has $l \cdot 1 = 1$) since $\deg g = \deg \bar{g}$.

$\Rightarrow$ can divide with remainder:

$$b r_n = s_{n+1} g_0 + p_{n+1} \ , \ \deg p_{n+1} < \deg g_0 = k$$

$$\downarrow$$

$$g_0(a r_n + s_{n+1} h_0) + h_0 p_{n+1} \equiv r_n \pmod{p}$$

define $q_{n+1}$ by omitting from $a r_n + s_{n+1} h_0$
any coeff divisible by $\bar{a}$.
Then have:

$$g_0 q_{n+1} + h_0 p_{n+1} \equiv r_n \pmod{p}$$

$\deg p_{n+1} < k$.

Suppose $\deg q_{n+1} = l > d-k$. The highest-degree term of $g_0 q_{n+1}$ would have degree $l+k > d$.

But $r_n$ has $\deg \leq d$, so leading coeff of $g_0 q_{n+1}$
would be divisible in \( \pi \), so leading coeff of \( q_{n+1} \), contradiction.

For this to work we need: \(|\pi| > |a_0 + b_0|\) and need \( f = q_0 h_0 \). Then \(|\pi| > |f - q_0 h_0|\)

we can do this since \( f - q_0 h_0 = 0 \).

Cor of (2): Suppose \( f \in O[x] \), \( a \in O \) s.t.
\[ f(\alpha) = 0, \quad f'(\alpha) \neq 0 \]

Then \( f \in O[\alpha] \) s.t. \( \beta = \alpha(p) \) and \( f(\beta) = 0 \)

So \( \alpha \) is a simple root, can write \( f = (x - \alpha) \cdot h(x) \) with \( h(\alpha) \neq 0 \), i.e. \( (x - \alpha, h) = 1 \)

By (2) have \( f = (x - \beta) h \) with \( \beta \in O \), \( h \in O[x] \)

Cor: Let \( f \in O[x] \) be irred, of degree \( d \), so \( q_{n+1} \neq 0 \)

\[ f = \sum_{i=0}^{d} a_i x^i \]. Then \( |f| = \max |a_d|, |a_{d-1}| \).
Proof: divide \( f \) by \( |f| \) to assume WLOG that \( |f| = 1 \). If \( |a|, |a_d| < 1 \) then \( f \) has degree \( d \) & vanishes at \( 0 \) so can write \( f = x^r h \) with \( h \) prime to \( x^r \), \( 1 \leq r < d \)

\[ \Rightarrow \text{can write } f = g h \text{ with } g = x^r, 1 \leq \deg g < d \text{, contradicts irreducibility of } f. \]

Cor: let \( f \in \mathbb{F} \) be irreducible, monic.

If \( a_d \neq 0 \) then \( f \in \mathbb{F} \)

if not (divide by \( |f| \) to get poly in \( \mathbb{F} \), irreducible, with largest coefficient not \( a_0, a_d \)).

Problems: \( L/\mathbb{F} \) finite, want to extend \( 1/\mathbb{F} \) to \( L \).

Knew: if have an extension, it's unique.

Suppose that \( 1/\mathbb{L} \) is such an extension, \( L/\mathbb{F} \) is Galois then for any \( \sigma \in \text{Gal}(L/\mathbb{F}) \), \( 1 \sigma x \mathbb{L} \) is also an extension so \( 1 \sigma x \mathbb{L} = 1 x \mathbb{L} \), so \( 1 N_{\mathbb{F}/\mathbb{F}} x \mathbb{L} = 1 \prod \sigma x \mathbb{L} = 1 \prod \sigma x \mathbb{L} = x \mathbb{L} \) so \( 1 x \mathbb{L} = 1 N_{\mathbb{F}/\mathbb{F}} x \mathbb{L} \).
Thm: Let $L$ be complete with $1$, $l$ which is non-trivial & non-arch. Let $L/F$ be algebraic of degree $n$. Then $1|_{L}^{1} = |N_{L}^{1}1|_{F}^{1}$ is an absolute value on $L$ extending $|1|_{F}$.

Proof: Certainly $1|_{P}^{1} = |1|_{P}^{P}1 < (N_{F}^{1}P) = N_{F}1$.

Let $\alpha \in L$ s.t. $N_{F}^{1}\alpha \in O_{F}$. Let $f \in F[x]$ be the min poly of $\alpha$. Then $f$ is monic, const coeff is $N_{F}^{1}\alpha \in O_{F}$, $f$ is irreducible $\implies f \in O_{F}[x]$.

$(N_{F}^{1}\alpha < (f(0))^{1} \iff \alpha \in O_{F})$

So $\alpha$ is integral over $O_{F}$.

Converse immediate.

$\implies$ there is a quadratic of $L$.

$\implies$ if $|\alpha|_{L} \leq 1$, then $|1 + \alpha|_{L} \leq 1$

$\implies$ if $\alpha, \beta$ have $|\alpha|_{L} \leq |\beta|_{L}$ and $\beta > 0$ then

$|\alpha + \beta|_{L} = |\beta|_{L} |\alpha|_{\beta} + 1|_{L} \leq |\beta|_{L}$. 
\[ |\frac{|a|}{b}| \leq 1 \Rightarrow \frac{a}{b} \text{ is in ring} \]

Cor.: Can extend to any algebraic extension.