# Lecture : p-adic numbers II

Last time:

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^k\mathbb{Z} = \left\{ (a_1, a_2, a_3, \dots) \;\middle|\; \begin{array}{l} a_k \in \mathbb{Z}/p^k\mathbb{Z} \\ a_{k+1} \equiv a_k \bmod p^k \end{array} \right\}$$

$$\begin{array}{ccccccccc} \mathbb{Z}/p & \leftarrow & \mathbb{Z}/p^2\mathbb{Z} & \leftarrow & \mathbb{Z}/p^3\mathbb{Z} & \leftarrow & \mathbb{Z}/p^4\mathbb{Z} & \leftarrow & \cdots \\ a_1 & & a_2 & & a_3 & & a_4 & & \end{array}$$

Have $a_{k+1} = a_k + b_k p^k$ with $b_k \in \{0, 1, \dots, p-1\}$ and write $(a_k) \text{"="} \sum_{k=0}^{\infty} b_k p^k$ $\left(\Longrightarrow a_n = \sum_{k=0}^{n-1} b_k p^k\right)$

**Prop:** $\mathbb{Z}_p^\times = \{ a_1 = b_0 \neq 0 \} = \{ (a_k) \notin p\mathbb{Z}_p \}$ ← unique ideal of $\mathbb{Z}_p$.

**Pf:** Suppose $(a_k) \in \mathbb{Z}_p^\times$, with $(a_k)^{-1} = (c_k)$. Then $a_k c_k = 1$ in $\mathbb{Z}/p^k\mathbb{Z}$. In particular $a_1 \neq 0$.

Conversely, suppose $a_1 \neq 0$. Since $a_k \equiv a_1 \bmod p$, $a_k$ is coprime to $p$ and hence $p^k$. So if $c_k$ is the inverse of $a_k \bmod p^k$ we have $(a_k)^{-1} = (c_k)$. ▨

[Foreshadowing of Hensel's Lemma]

Define

$$\mathbb{Q}_p = \text{field of fractions of } \mathbb{Z}_p \overset{\text{By prop}}{=} \mathbb{Z}_p\left[\tfrac{1}{p}\right] = \{ p^{-m} a \mid a \in \mathbb{Z}_p \}$$

$$= \left\{ b_{-m} p^{-m} + b_{-m+1} p^{-(m+1)} + \cdots \;\middle|\; \begin{matrix} b_{-m} \neq 0 \\ b_k \in \{0,1,\dots,p-1\} \end{matrix} \right\}$$

[Mention Hensel's motivation: "Function Theory" = Complex analysis]

<u>Valuation of $\mathbb{Q}_p$</u>: $|x|_p = p^{-\nu(x)}$ where $x = p^{\nu(x)} y$ and $y \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$.

"additive valuation."

<u>Analog:</u> Meromorphic functions and order of zero at 0. $f(z) = a_n z^n + a_{n+1} z^{n+1} + \cdots$, $a_n \neq 0$, $n \in \mathbb{Z}$.

$\boxed{\underline{\underline{\text{Note}}}: \mathbb{Z}_p^\times = \{a \in \mathbb{Z}_p \mid |a| = \underline{1}\}}$

Have $\mathbb{Q} \subseteq \mathbb{Q}_p$ by $r = p^k \frac{x}{y} \longmapsto p^k \underbrace{x y^{-1}}_{\in \mathbb{Z}_p}$ (coprime to $p$)

in particular:

ⓐ The char of $\mathbb{Q}_p$ is 0.

ⓑ $\mathbb{Z}_{(p)} = \left\{ \frac{x}{y} \mid x, y \in \mathbb{Z},\ y \notin (p) \right\} \subseteq \mathbb{Z}_p$

<u>Ex</u>: $-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots = (-1, -1, -1, \dots)$

$a_k = (p-1)\cdot(1 + \cdots + p^{k-1}) = p^k - 1 \equiv -1 \bmod p^k.$

$$\frac{1}{1-p} = 1 + p + p^2 + p^3 + p^4 + \cdots$$

$a_k = \dfrac{p^k - 1}{p-1}$ so $a_k \cdot (1-p) \equiv 1 \bmod p^k.$

Have to integrate correctly. E.g. could have defined

$|r|_p = 2^{-k}$ Precisely, any valuation of $\mathbb{Q}$

is of the form $|\cdot|^a$ where $|\,|$ is one of the above and $a > 0$.

Define $\mathbb{Q}_p' = \{$completion of $\mathbb{Q}$ wrt $|\,|_p\}$

$\mathbb{Z}_p' = \{$ " $\mathbb{Z}$ " $\} = \overline{\mathbb{Z}}$ in $\mathbb{Q}_p'$.

<u>Thm</u>: $\mathbb{Q}_p' \cong \mathbb{Q}_p$ and $\mathbb{Z}_p' \cong \mathbb{Z}_p$

<u>Isomorphisms</u>: $\mathbb{Q}_p \longrightarrow \mathbb{Q}_p'$

$$\sum_{k=m}^{\infty} b_k p^k \longmapsto \sum_{k=m}^{\infty} b_k p^k \Big\}\text{ actual convergent series}$$

<u>Point</u>: $\left\{S_n = \sum_{k=m}^{n} b_k p^k\right\}$ is a Cauchy sequence in $\mathbb{Q}$.

$$|S_{n'} - S_n|_p = \left|\sum_{k=n+1}^{n'} b_k p^k\right|_p \le \max_{n<k\le n'} \underbrace{|b_k p^k|_p}_{=p^{-k}} = p^{-(n+1)}$$

hence converges in $\mathbb{Q}_p'$.

<u>Inverse isomorphism</u>: Enough to describe $\mathbb{Z}_p' \to \mathbb{Z}_p$

Show $\mathbb{Z}_p' / p^k \mathbb{Z}_p' \cong \mathbb{Z}/p^k\mathbb{Z}$ which then

gives the map $a \in \mathbb{Z}_p' \longmapsto (a_k) \in \mathbb{Z}_p$. [See Neukirch for details]

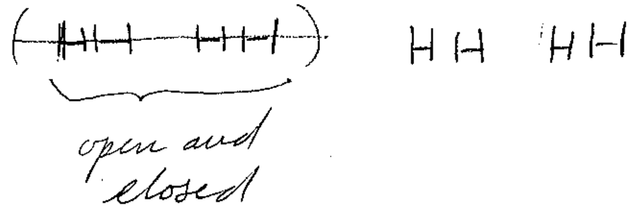
## Topology on $\mathbb{Z}_p$: profinite topology

Basis: $\mathcal{U}_{a,k} = \{ \text{preimage of } a \text{ under } \mathbb{Z}_p \longrightarrow \mathbb{Z}/p^k\mathbb{Z} \}$

(i.e. just enough open sets to make ↑ cont if $\mathbb{Z}/p^k\mathbb{Z}$ has the discrete topology.)

Rmk: $\mathcal{U}_{a,k}$ is both open and closed. Not hard to show

$\mathbb{Z}_p \cong$ Cantor set




---

## Alternate view:

Def: A (multiplicative) valuation on a field $K$ is a function $|\cdot| : K \longrightarrow \mathbb{R}$ s.t.

ⓐ $|x| = 0 \iff x = 0$

ⓑ $|xy| = |x||y|$

ⓒ $|x+y| \le |x| + |y|$

trivial val $= |k| = \begin{cases} 0 & k = 0 \\ 1 & k \neq 0 \end{cases}$

Ostrowski's Thm: The nontrivial valuations on $\mathbb{Q}$ are

ⓘ $|\cdot|_\infty$ - the usual absoute value on $\mathbb{Q}$.

ⓘⓘ $|\cdot|_p$ - the p-adic absolute value

$$|r|_p = p^{-k} \quad \text{where } r = p^k \frac{x}{y} \text{ with } x, y \text{ coprime to } p.$$