D2: p-adic numbers

Montag, 23. Juni 2025 16:37

$K=\mathbb{Q}$. Given an LRS $(a_n)_{n\geq 0}$ we can interpolate

$$a_n = P_1(n)\lambda_1^n + \dots + P_s(n)\lambda_s^n \quad (\lambda_i \in \mathbb{C},\ \forall n \gg 1),$$ analytic in n

Problem: $\mathbb{N}_0$ not contained in a compact subset of $\mathbb{R}$

Let $p \in \mathbb{P}$. $\quad \dots \twoheadrightarrow \mathbb{Z}/p^3\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p^2\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p\mathbb{Z} \twoheadrightarrow 0$

$$\mathbb{Z}_p := \varprojlim_{i\geq 0} \mathbb{Z}/p^i\mathbb{Z} = \{ (\underbrace{a_i + p^i\mathbb{Z}}_{=\bar{a}_i})_{i\geq 0} \in \prod_{i\geq 0} \mathbb{Z}/p^i\mathbb{Z} : a_i + p^j\mathbb{Z} = a_j + p^j\mathbb{Z} \text{ if } j\leq i\}$$

inverse limit, limit (category theory)

$\mathbb{Z}_p$ is the ring of p-adic integers.

$\mathbb{Z}_p$ is a domain with $\mathbb{Z}_p^\times = \{ (a_i + p^i\mathbb{Z})_{i\geq 0} : p \nmid a_1\}$ [Exc.]

$\exists$ epimorphisms $\pi_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$, $(\bar{a}_i)_{i\geq 0} \to \bar{a}_n$.

$\varepsilon: \mathbb{Z} \hookrightarrow \mathbb{Z}_p$, $a \mapsto (\bar{a})_{i\geq 0}$ is a ring monomorphism, wlog $\mathbb{Z} \subseteq \mathbb{Z}_p$

[Injectivity: $\varepsilon(a) = 0 \Rightarrow \forall i: a \in p^i\mathbb{Z} \Rightarrow a = 0.$]

$\mathbb{Z}_p$ is also a metric space:

$$d\big((\bar{a}_i)_i, (\bar{b}_i)_i\big) := p^{-v} \text{ where } v = \max\{i \geq 0 : \bar{a}_i = \bar{b}_i\} \in \mathbb{N}_0 \cup \{\infty\}$$

$(p^{-\infty} := 0)$

d is an ultrametric: For $\alpha, \beta, \gamma \in \mathbb{Z}_p$

$$d(\alpha,\beta) = 0 \Leftrightarrow \alpha = \beta$$

$$d(\alpha,\beta) = d(\beta,\alpha)$$

ultrametric inequality

$$d(\alpha,\gamma) \leq \max\{d(\alpha,\beta), d(\beta,\gamma)\} \leq d(\alpha,\beta) + d(\beta,\gamma)$$

Notation: $|\alpha|_p := d(\alpha, 0)$ p-adic absolute value $(d(\alpha,\beta) = |\alpha-\beta|_p)$,

$v_p(\alpha) := v$ s.t. $|\alpha|_p = p^{-v_p(\alpha)}$ p-adic valuation

Then $v_p(a) = \max\{e \geq 0 : p^e \mid a\}$

Prop 2.1 $\mathbb{Z}_p$ is (sequentially) complete.

Prop 2.1 $\mathbb{Z}_p$ is (sequentially) complete.

Proof: Let $(\alpha_n)_{n\geq 0}$ be a Cauchy sequence in $\mathbb{Z}_p$.

$\Rightarrow \forall \underset{=p^{-i}}{\varepsilon}>0\ \exists N_0\geq 0\ \forall m,n\geq N_0:\ d(\alpha_m,\alpha_n)<\underset{=p^{-i}}{\varepsilon}\quad \left[\Leftrightarrow \pi_j(\alpha_m)=\pi_j(\alpha_n) \text{ for } j\leq i.\right]$

Let $i\geq 0 \rightarrow (\pi_i(\alpha_m))_{m\geq 0}$ in $\mathbb{Z}/p^i\mathbb{Z}$ is eventually constant, say equal to $b_i+p^i\mathbb{Z}$. Let $\beta:=(b_i+p^i\mathbb{Z})_{i\geq 0}$.

$\Rightarrow \forall p^{-i}>0\ \exists N_0\geq 0\ \forall n\geq N_0:\ \pi_j(\alpha_n)=\pi_j(\beta)$ for $j\leq i$ $\left[\Leftrightarrow d(\alpha_n,\beta)<p^{-i}\right]$

$\Rightarrow \lim\limits_{n\to\infty}\alpha_n=\beta.$ $\square$

Cor 2.2 If $(\alpha_m)_{m\geq 0}$ is a sequence in $\mathbb{Z}_p$, then

$$\sum_{m=0}^{\infty}\alpha_m := \lim_{n\to\infty}\sum_{m=0}^{n}\alpha_m \text{ converges} \Leftrightarrow \lim_{m\to\infty}\alpha_m=0.$$

Proof: „$\Rightarrow$" like Analysis I.

„$\Leftarrow$" Let $N_0\geq 0$. $\forall n'\geq n\geq N_0$.

$$d\Big(\sum_{m=0}^{n}\alpha_m,\sum_{m=0}^{n'}\alpha_m\Big) = \Big|\sum_{m=n+1}^{n'}\alpha_m\Big|_p \leq \max\{|\alpha_{n+1}|_p,\dots,|\alpha_{n'}|_p\}\to 0 \text{ as}$$

$N_0\to\infty$. $\square$

Exm: $\displaystyle\sum_{i=0}^{\infty}p^i=\frac{1}{1-p}$

Thm 2.3: Every $\alpha\in\mathbb{Z}_p$ has a unique representation

$$\alpha=\sum_{i=0}^{\infty}a_i p^i \quad \text{with} \quad a_i\in\{0,1,\dots,p-1\}$$

Proof: *Existence:* Let $\alpha=(b_i+p^i\mathbb{Z})_{i\geq 0}$, $b_i\equiv b_j \bmod p^j$ if $j\leq i$.

Wlog. $0\leq b_i\leq p^i-1$. Then $b_i=c_{i-1}p^{i-1}+\dots+c_1p+c_0$ with unique $0\leq c_j\leq p-1$. (base p representation, $b_i\equiv b_j$ p^j for $j\leq i$ implies compatibility of digits!). Now $\alpha=\sum_{i=0}^{\infty}c_ip^i$.

... compatibility of digits). Now $\alpha = \sum_{i=0} c_i p^i$.

<u>Uniqueness</u>: Similar, but reverse. $\square$

<u>Exm</u>: $\sum_{i=0}^{\infty} (p-1)p^i = (p-1)\frac{1}{1-p} = -1$.

<u>Remark</u>: Can also construct $\mathbb{Z}_p$ as $\{\text{p-adic Cauchy sequences } / \mathbb{Z}\} / \{\text{null sequences}\}$

$\mathbb{Z}_p$ is the p-adic completion of $\mathbb{Z}$.

<u>Def</u>: $\mathbb{Q}_p$ is the field of fractions of $\mathbb{Z}_p$ $(\mathbb{Q} \subseteq \mathbb{Q}_p)$.

$$\mathbb{Q}_p = \left\{\frac{\alpha}{\beta} : \alpha, \beta \in \mathbb{Z}_p, \beta \neq 0\right\} \underset{\substack{\uparrow \\ \text{Since } \beta = p^n \beta' \text{ with } \beta' \in \mathbb{Z}_p^\times}}{=} \{p^{-n}\alpha' : \alpha' \in \mathbb{Z}_p, n \geq 0\} = \left\{\sum_{i=-n}^{\infty} a_i p^i : 0 \leq a_i \leq p-1, n \in \mathbb{Z}\right\}.$$

<u>(Convergent) power series</u>:

$\sum_{n=0}^{\infty} \alpha_n x^n \in \mathbb{Q}_p[[x]]$ has convergence radius $\rho = \left(\limsup_{n \to \infty} \sqrt[n]{|\alpha_n|_p}\right)^{-1}$

$f : D \ni 0 \to \mathbb{Q}_p$ is analytic at 0 if it is defined by a convergent power series.

<u>Facts</u>:

- f analytic at $0 \Rightarrow f^{(i)} = \sum_{n=0}^{\infty} \alpha_{n+i}(n+i)(n+i-1)\cdots(n+1)x^n$ analytic at 0
- Identity Theorem: If $f = \sum_{n=0}^{\infty} \alpha_n x^n$, $g = \sum_{n=0}^{\infty} \beta_n x^n$ converge in $D = \{x \in \mathbb{Z}_p : |x|_p < \rho\}$ and $(\gamma_i)_{i \geq 0}$ is a convergent seq. in D, s.t. $f(\gamma_i) = g(\gamma_i)$ $\forall i$, then $\alpha_n = \beta_n$ $\forall n$.

<u>Thm 2.4</u>: $\mathbb{Z}_p$ is sequentially compact

<u>Proof</u>: Let $(\alpha_m)_{m \geq 0}$ be a sequence in $\mathbb{Z}_p = \varprojlim_{i \geq 0} \mathbb{Z}/p^i\mathbb{Z}$.

For each i, $|\mathbb{Z}/p^i\mathbb{Z}| < \infty \xrightarrow[\text{principle}]{\text{pigeonhole}} (\underbrace{\pi_i(\alpha_m)}_{\in \mathbb{Z}/p^i\mathbb{Z}})_{m \geq 0}$ takes some value $b_i + p^i\mathbb{Z}$ infinitely often. WLOG $b_j \equiv b_i \mod p^i$ for $i \leq j$

principle $\underbrace{\qquad}_{\in \mathbb{Z}/p^i\mathbb{Z}}$, $m \geq 0$

$b_i + p^i\mathbb{Z}$ infinitely often. Wlog. $b_i \equiv b_j \mod p^j$ for $j \leq i$

Define $N(i) := \{ m \geq 0 : \pi_i(\alpha_m) = b_i + p^i\mathbb{Z} \}$, and $n_i := \min N(i)$

$\Rightarrow \lim\limits_{i \to \infty} \alpha_{n_i} = (b_i + p^i\mathbb{Z})_{i \geq 0}$. $\square$

<u>Cor 2.5:</u> $\alpha + p^i\mathbb{Z}_p = \{ \beta \in \mathbb{Z}_p : d(\alpha, \beta) \leq p^i \}$ is sequentially compact

<u>Proof:</u> $\mathbb{Z}_p \longrightarrow \alpha + p^i\mathbb{Z}_p$, $x \mapsto \alpha + p^i x$ is a homeomorphism.