14.07.2011

Lecture 4.

$\mathbb{Z}_p = \{ (a_n) \in \prod \mathbb{Z}/p^n : a_{n+1} \equiv a_n \ (p^n) \}$

$= \varprojlim_n \mathbb{Z}/p^n$ (projective limit)

$R_1 = \{0, 1, \dots p-1\}$ complete set of representatives of the residus classes mod p

- each integer m is congruent mod p to a unique elt. of R_1

$R_n = \{ \sum_{i=0}^{n-1} r_i p^i : r_i \in R_1 \}$ complete set of rep's of residue classes mod p^n

$a \in \mathbb{Z}_p \quad a = (a_n) \quad a_n \in R_n$

- if $a_{n+1} = \sum_{i=0}^{n} r_i p^i \qquad r_i \in R_1$

  then $a_n = \sum_{i=0}^{n-1} r_i p^i$

$a \to \sum_{i=0}^{\infty} r_i p^i \qquad r_i \in R_1$

$\mathbb{Z}_p \longleftrightarrow \{ \sum_{i=0}^{\infty} r_i p^n : r_i \in R_1 \}$

(a_n) when $a_n = \sum_{i=0}^{n-1} r_i p^i$

obvious multiplication / addition
or RHS is the same as that in $\mathbb{Z}_p$
„base p"

Ex: $p = 2 \quad -1 \in \mathbb{Z}_2$

$R_1 = \{0, 1\}$

$-1 \longleftrightarrow 1 \cdot 2^0 + 1 \cdot 2 + 1 \cdot 2^2 + \dots + 1 \cdot 2^n + \dots \overset{?}{=} \frac{1}{1-2} = -1$

p-adic valuation:

$\mathrm{ord}_p(\cdot) : \mathbb{Q}_p \to \mathbb{Z} \cup \{+\infty\}$

- $0 \neq x \in \mathbb{Q}_p, \ x = p^k u, \ u \in \mathbb{Z}_p^\times, \ k \in \mathbb{Z}$ - unique

  $\mathrm{ord}_p(x) := k$

- $\mathrm{ord}_p(0) = +\infty$

  $\mathrm{ord}_p(xy) = \mathrm{ord}_p(x) + \mathrm{ord}_p(y)$

  $x = p^k u, \ y = p^\ell v \qquad xy = p^{k+\ell} uv$

- $\mathrm{ord}_p(x) = 0 \iff x \in \mathbb{Z}_p^\times$

- $\mathrm{ord}_p\left(\frac{1}{x}\right) = -\mathrm{ord}_p(x)$

$\mathrm{ord}_p =$ homomorphism: $\mathbb{Q}_p^\times \to \mathbb{Z}$

- $\mathrm{ord}_p(x) \geq 0 \iff x \in \mathbb{Z}_p$
- $\mathrm{ord}_p(x) \geq n \iff x \in p^n\mathbb{Z}_p$
- $\mathrm{ord}_p(x+y) \geq \min\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}$; „=" if $\mathrm{ord}_p(x) \neq \mathrm{ord}$

$x = p^k u$, $y = p^e v$, $e \leq k$

$x + y = p^e \underbrace{(v + p^{k-e} u)}_{\in \mathbb{Z}_p}$

Ex. $\mathrm{ord}_2\left(\frac{3}{5}\right) = 0$

$\mathrm{ord}_3\left(\frac{3}{5}\right) = 1$

$\mathrm{ord}_5\left(\frac{3}{5}\right) = -1$

$\mathrm{ord}_2\left(\frac{3}{5}+1\right) = \mathrm{ord}_2\left(\frac{8}{5}\right) = 3$

$\mathrm{ord}_3\left(\frac{3}{5}+1\right) = \mathrm{ord}_3\left(\frac{8}{5}\right) = 0$

$\mathrm{ord}_5\left(\frac{3}{5}+1\right) = \mathrm{ord}_5\left(\frac{8}{5}\right) = -1$

p-adic absolute value:

$|\cdot|_p : \mathbb{Q}_p \to \mathbb{R}_{\geq 0}$

$|x|_p = p^{-\mathrm{ord}_p(x)}$ $\quad (|0|_p = 0)$

$x = p^k u$ $\quad |x|_p = p^{-k}$

- $|x|_p = 0 \iff x = 0$
- $|xy|_p = |x|_p \cdot |y|_p$
- $|x+y|_p \leq \underbrace{p^{-\min\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}}}_{\max\{|x|_p, |y|_p\}}$; „=" if $|x|_p \neq |y|_p$

Recall: $|x+y| \leq |x| + |y|$ triangle inequality

Ostrowski's Thm. If

$f : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ s.t.

(i) $f(x) = 0 \iff x = 0$

(ii) $f(xy) = f(x) f(y)$

(iii) $f(x+y) \leq f(x) + f(y)$

Then either:

(a) $f(x) = 1 \quad \forall x \neq 0$

(b) $f(x) = |x|^{\alpha}, \ 0 < \alpha \leq 1$

(c) $f(x) = |x|_p^{\beta}, \ \beta \geq 1.$

$1 + 2^{-1} + 2^{-2} + \dots + 2^{-n} + \dots = 2$

$S_n = 1 + 2^{-1} + \dots + 2^{-n} = 2 - 2^{-n}$

$2 - 2^{-n}$ is gently „close" to 2 in the sence measoured by usual absolute value

gives $\varepsilon > 0$, $|2 - (2 - 2^{-n})| < \varepsilon$ if $n >> 0$.

We'll replace the usual absolute value $| \ |$ with the p-adic abs. value $|\cdot|_p$

$x, y \in \mathbb{Z}_p$

„$x+y$ close": $|x-y|_p$ small

this should be a small real number

$|x-y|_p \leq p^{-m} \iff ord_p(x-y) \geq m \iff x-y \in p^m \mathbb{Z}_p$

(i.e. $p^m \mid x-y$)

$-1 \qquad 1 + 2 + 2^2 + \dots = -1$ (2-adic convergence)

2-adic expansion $\sigma_n = 1 + 2 + 2^2 + \dots + 2^n = \dfrac{2^{n+1} - 1}{2 - 1} = 2^{n+1} - 1$

$|-1 - \sigma_n|_2 = |-1 - (-1 + 2^{n+1})|_2 = |2^{n+1}|_2 = \underbrace{2^{-1-n}}_{\text{small if } n \text{ large}}$

sequences series (p-agically)

$\{a_n\}$, $a_n \in \mathbb{Q}_p$ sequence $n \geq 0$

Converges to a: means

for $\varepsilon > 0$ s.t. $|a - a_n|_p < \varepsilon$ if $n > N_\varepsilon$

$\exists N_\varepsilon > 0$

natural candidates fo convergent seq's:

cauchy sequences:

$\{a_n\}$ s.t. for $\varepsilon > 0 \ \exists N_\varepsilon > 0$ s.t. $|a_n - a_m|_p < \varepsilon$, $\forall n, m > N_\varepsilon$

In $\mathbb{Q}_p$ every Caushy sequence converges.

$a_n = p^{k_n} u_n$, $k_n \in \mathbb{Z}$, $u_n \in \mathbb{Z}_p^{\times}$

κ_n imbounded: $\{a_n\} \to 0$ p-adically

κ_n bounded: for $\varepsilon << 1$

$|p^{\kappa_n} u_n - p^{\kappa_m} u_m|_p < p^{-j} \qquad j >> 0$

$= |p|_p^{\kappa_n} \, |u_n - p^{\kappa_m - \kappa_n} u_m|_p$

$|p^{\kappa} u_n - p^{\kappa} u_m|_p < p^{-j} \qquad j >> 0$

$|u_n - u_m|_p < p^{\kappa - j}$

$u_n \equiv u_m \mod p^{\kappa - j} \quad \forall\, n, m >> 0$

Every elt of $\mathbb{Q}_p$ is the limit of a Cauchy sequence of rational numbers

$x \in \mathbb{Q}_p$, $\exists \{r_n\}$, $r_n \in \mathbb{Q}$ c.s. s.t. $\{r_n\} \to x$

$x = p^{\kappa} u$, $u = \{u_n\}$, $u_n \in \mathbb{Z}/p^n$, $u_{n+1} \equiv u_n \mod p^n$

[Can assume] $u_n \equiv r_n \mod p^n$, $r_n \in R_n$

Then $\{r_n\}$ is a sequence of ~~of~~ rational numbers

$r_n = \sum_{i=0}^{n-1} c_i p^i$, $c_i \in R_1 = \{0, 1, \ldots, p-1\}$

$|r_n - r_m|_p = |\sum_{i=n}^{m-1} c_i p^i|_p = |p^n|_p \cdot |c_n + c_{n+1} p + \ldots + c_{m-1} p^{m-n-1}|_p \leq p^{-n}$

$n \leq m$

$u = \{u_n\} = \{r_n \mod p^n\}$

$u - r_m = \{\underbrace{r_n - r_m}_{0 \text{ if } m \geq n} \mod p^n\}$

$p^m \mid u - r_m$

This mean $|u - r_m|_p \leq p^{-m}$ so $\{r_m\} \to u$

$\sum_{i=0}^{\infty} c_i p^i = u$ in $\mathbb{Q}_p$.

C_p = set of (p-adic) Cauchy sequences $\{r_n\}$, $r_n \in \mathbb{Q}$ w.r.t. $|\;|_p$

- ring under mult + addition of sequences

$C_p \twoheadrightarrow \mathbb{Q}_p \qquad (*)$ Kernel of $(*)$ = set of Cauchy sequences that converse to 0

$\{r_n\} \longmapsto$ its limit (p-adic) $\quad \{\{r_n\} \text{ c.s.} : |r_n|_p \to 0\} = N_p$

Then $C_p / N_p \xrightarrow{\sim} \mathbb{Q}_p$