Last time:

R ring, $I \subseteq R$

$\rightsquigarrow \hat{R} = \varprojlim_n R/I^n$ complete top. ring for inv. limit top.

I f.g. $\Rightarrow$ inv. top. on $\hat{R}$ is the $I \cdot \hat{R}$-adic topology

($\Rightarrow$ $\hat{R}$ is I-adic completion of R)

E.g: $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n$

La 1: R ring, $I = (r)$,

$r \in R$ non-zero div.

($\leadsto$ r is non-zero div. on $\hat{R}$)

1) If R/I int. domain

$\Rightarrow$ $\hat{R}$ int. domain

2) If $R = \hat{R}$ ("R is I-adically complete"),

$S \subseteq R$, s.t. $S \xleftrightarrow{1:1} R/I$,

then

$$S^{\mathbb{N}} \overset{1:1}{\hookrightarrow} R$$

$$(s_i)_{i \geq 0} \longmapsto \sum_{i=0}^{\infty} s_i r^i$$

(even homeo. {}, when S is discrete & $S^{\mathbb{N}} = \prod_{\mathbb{N}} S$ carries product topology)

Prf: 1) Let $a = (a_m)_m$, $b = (b_m)_m \in \hat{R}$

$\quad \Vert$

$\varprojlim R/I^m$

assume $a, b \neq 0$,

$a \cdot b = 0$

Let m_0, n_0 be minimal, s.t.

$a_{m_0+1} \neq 0$, $b_{n_0+1} \neq 0$

$\Rightarrow \quad a = r^{m_0} \cdot x$, $b = r^{n_0} \cdot y$

Last time

$\ker(\hat{R} \to R/I^a) = r^a \cdot \hat{R} \quad \forall a \geq 0$

$\Rightarrow 0 = a \cdot b = r^{m_0+n_0} \cdot x \cdot y$

$\Rightarrow \quad 0 = x \cdot y$ ⚡ (r non-zero div. on $\hat{R}$)

as $\bar{x}, \bar{y} \in R/I$ are non-zero

2)

Well-definedness

La2: A J-adically complete ring (A ring, $J \subseteq A$ ideal) $a_i \in A$, $i \geq 0$. Then

$\sum_{i=0}^{\infty} a_i$ conv.

$\Leftrightarrow$ $a_i \to 0$, $i \to \infty$

Moreover,

$$\left(\sum_{i=0}^{\infty} x_i\right)\left(\sum_{j=0}^{\infty} y_j\right) = \sum_{i=0}^{\infty} \sum_{j=0}^{i} x_{i-j} \cdot y_j$$

etc.

Proof of La2:

"⇒" $a_n = \sum_{i=0}^{n} a_i - \sum_{i=0}^{n-1} a_i$

$$\qquad\qquad \downarrow{\scriptstyle n\to\infty} \qquad\quad \downarrow{\scriptstyle n\to\infty}$$

$$\sum_{i=0}^{\infty} a_i - \sum_{i=0}^{\infty} a_i$$

"⇐" A J-adically complete

STP ⇒ $\left(\sum_{i=0}^{n} a_i\right)_n$ Cauchy

Let $U \subseteq A$ be any nbhd of 0

⇒ $\exists\, m > 0,\ J^m \subseteq U$.

There ex. $i_0 \gg 0$

s.t. $a_i \in J^m \ \forall i \geq i_0$

$\Rightarrow \forall n \geq n' \geq i_0$

$\sum_{i=n'}^{n} a_i \in J^m$ ($\because J^m \subseteq A$ is a subgroup)

$\Rightarrow \left(\sum_{i=0}^{n} a_i\right)_n$ is Cauchy. $\square_{\text{Pf. La2}}$

Upshot: $\varphi : S^{\mathbb{N}} \xrightarrow{1:1} R$

$(s_i)_{i\geq 0} \mapsto \sum_{i=0}^{\infty} \underbrace{s_i r^i}_{I^i}$

well-def'd.

(note: fix $i \geq 0$

$\Rightarrow s_j \cdot r^j \in I^i \ \forall j \geq i$

as I^i is an ideal

Injectivity:

Assume $\sum_{i=0}^{\infty} s_i \cdot r^i = \sum_{i=0}^{\infty} s_i' r^i$

$\Rightarrow \forall n \geq 0 \quad \sum_{i=0}^{\infty} s_i \cdot r^i \equiv \sum_{i=0}^{\infty} s_i' \cdot r^i \mod I^n$

$$\underbrace{\sum_{i=0}^{n-1} s_i \cdot r^i}_{=} \qquad \underbrace{\sum_{i=0}^{n-1} s_i' \cdot r^i}_{=}$$

($\hat{R} \to R/I^n$ cont.)

$\Rightarrow$ In part, $s_0 \equiv s_0' \mod I^n$

$\Rightarrow s_0 = s_0'$

by def. of S

$$\boxed{\begin{gathered} s_n \cdot r^n \equiv s_n' \cdot r^n \\ \mod I^{n+1} \\ \Rightarrow s_n \equiv s_n' \mod I \end{gathered}}$$

$\Rightarrow$ inductively, $s_n = s_n' \; \forall n$

(use $0 \to R/I \xrightarrow{r^n} R/I^{n+1} \to R/I^n \to 0$)

Surjectivity: Let $a \in R$

$\Rightarrow \exists\, s_0 \in S_1$ s.t. $s_0 \equiv a \mod I$

$\Rightarrow \exists\, s_1 \in S_1$ s.t.

$$\frac{s_0 - a}{r} \equiv s_1 \mod I = (r)$$

makes sense
(r non-zero div. on $R = \hat{R}$)

$\Rightarrow a \equiv s_0 + s_1 \cdot r \mod I^2$

$\Rightarrow$ we can find sequence $(s_i)_{i \geq 0}$ with $s_i \in S_1$ s.t.

$$a \equiv \sum_{i=0}^{n} s_i \cdot r^i \mod I^{n+1}$$

in $R = \hat{R}$

$$\Rightarrow a = \sum_{i=0}^{\infty} s_i r^i \quad \left(\text{as } \bigcap_n I^n = \{0\}\right)$$

Ex: p prime

$\Rightarrow \mathbb{Z}_p = \{ \sum_{i=0}^{\infty} a_i p^i \mid a_i \in \{0, \dots, p-1\} \}$

We know $\frac{1}{2} \in \mathbb{Z}_5^\times$

$$\frac{1}{2} = \frac{-2}{1-5} = \frac{-4+2}{1-5}$$

$$= 1 + \frac{2}{1-5}$$

$$= 1 + \sum_{i=0}^{\infty} 2 \cdot 5^i$$

geom. series

⚠ Addition / multiplication in $\mathbb{Z}_p$ are difficult to write down expicitly in terms of inf. sums. (10)

(Very different from power series
$\mathbb{F}_p[[z]] \overset{1:1}{\longleftrightarrow} \mathbb{Z}_p$)
homeo

La 3: 1) $\mathbb{Z}_p^\times = \varprojlim_{n} (\mathbb{Z}/p^n)^\times$

$$= \left\{ \sum_{i=0}^{\infty} a_i p^i \;\middle|\; a_i \in \{0, \dots, p-1\},\ a_0 \neq 0 \right\}$$

2) $\mathbb{Q}_p := \mathrm{Frac}(\mathbb{Z}_p) = \mathbb{Z}_p[\frac{1}{p}]$

$$= \left\{ \sum_{i \gg -\infty}^{\infty} a_i \cdot p^i \;\middle|\; a_i \in \{0, \dots, p-1\} \right\}$$

Prf: 1) Last time

R I-adic. complete

$\Rightarrow R^\times = \{ r \in R \mid \bar{r} \in (R/I)^\times \}$

(Exercise: $I \subseteq \operatorname{rad} R = \bigcap_{\substack{m \in R \\ \text{max.}}} m$)

$\hat{R} = \varprojlim_n R/I^n \subseteq \prod_n R/I^n$

2) Clear each element $a \in \mathbb{Z}_p \setminus \{0\}$ can be written uniquely as

$a = u \cdot p^n, n \geq 0, u \in \mathbb{Z}_p^\times$

$\Rightarrow \mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$ $\square$

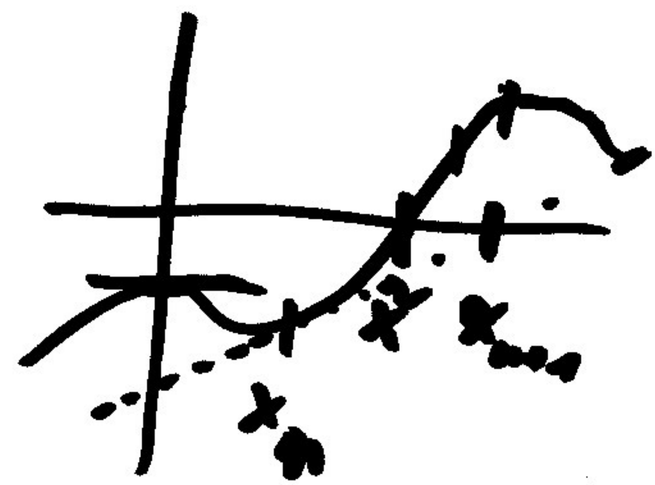
Compare to: p prime

$\mathbb{R} = \{ \sum_{i >> -\infty}^{\infty} a_i \cdot p^{-i} \mid a_i \in \{0, \dots, p-1\} \}/_{\sim}$

Recall: can solve in $\mathbb{R}$ equations via approximation

Newton method

$f : \mathbb{R} \to \mathbb{R}$



Let x_0 close to $\tilde{x}$

Set $x_{n+1} = x_n - \dfrac{f(x_n)}{f'(x_n)}$ must assume this $\neq 0$

$\Leftrightarrow 0 = f'(x_n) \cdot (x_{n+1} - x_n) + f(x_n)$

Then $\{x_n\}_n$ conv. to a zero of f (sometimes)

Prop. 4: R I-adically complete
(Hensel's lemma) (~~if~~ I nilpotent was an exercise)

⚠ $f \in R[X]$, $r_0 \in R$, s.t.

i) $f(r_0) = 0 \mod I$

("r_0 is close to a zero")

ii) $f'(r_0) \in R^\times$ ($\Leftrightarrow \overline{f'(r_0)} \in (R/I)^\times$)

Set $r_{n+1} = r_n - \dfrac{f(r_n)}{f'(r_n)} \in R$

Then 1) $r_n \equiv r_0 \mod I$

$$\Rightarrow \underset{\overset{\parallel}{f'(r_0)}}{f'(r_n)} \in (R/I)^\times$$

2) $\{r_n\}_n$ is Cauchy

3) Let $r \in R$ be its limit

$f(r) = 0$

Prf: 1) By induction

$(f(r_n) \in I, f'(r_n) \in R^\times)$

2)+3): $f(r_{n+1}) \in I^{2^{n+1}} \ \forall n \geq -1$

Write (Taylor exp.)

$$f(r_{n+1}) = \underbrace{f(r_n) + f'(r_n)(r_{n+1} - r_n)}_{=0} + \underset{\in R}{s} \cdot (\underbrace{r_{n+1} - r_n}_{\frac{f(r_n)}{f'(r_n)} \in I^{2^n}})^2$$

$\Rightarrow f(r_{n+1}) \in I^{2^{n+1}} \ \forall n \geq -1$

$\Rightarrow \quad r_{n+1} - r_n \in I^{2^n} \quad \forall\, n \geq 0$

$\Rightarrow \quad r_m - r_n \in I^{2^n} \quad \forall\, m \geq n$

$$\Big(r_m - r_n = \underbrace{r_m - r_{m-1}}_{\in\, I^{2^{m-1}}} + \dots + \underbrace{r_{n+1} - r_n}_{\in\, I^{2^n}} \Big)$$

$$I^{2^{m-1}} \subseteq \dots \subseteq I^{2^n}$$

$\Rightarrow \quad \{r_n\}_n$ Cauchy,

$r = \lim\limits_{n \to \infty} r_n$

$\Rightarrow \lim\limits_{n\to\infty} f(r_n) = f(r)$

$\quad \overset{\parallel}{0} \leftarrow f(r_n) \in I^{2^n}$

$\square$

Powerful tool to solve equations 16

Assume $p=3$ (e.g. $\mu_{p-1} \subseteq \mathbb{Q}_p$)

$f(X) = X^3 + X + 1 \in \mathbb{Z}_3[X]$

$\Rightarrow f(1) = 1 + 1 + 1 \equiv 0 \mod 3$

$f'(1) = 3 \cdot 1^2 + 1 \not\equiv 0 \mod 3$

$\Rightarrow X^3 + X + 1$ has solution in $\mathbb{Z}_3$

Digression:

How does the top. space of $\mathbb{Z}_p$ look like?

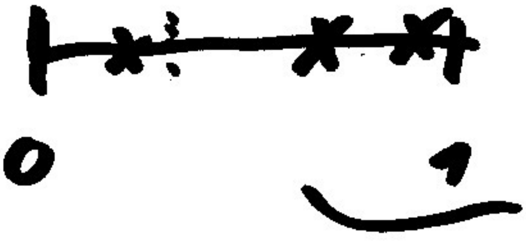
Have seen
$$\begin{array}{ccc} \mathbb{Z}_p & \xleftrightarrow{1:1} & \{0,\dots,p-1\}^{\mathbb{N}} \\ \parallel & \text{homeo} & \parallel \\ \varprojlim \mathbb{Z}/p^n & & \prod_{\mathbb{N}} \{0,\dots,p-1\} \end{array}$$

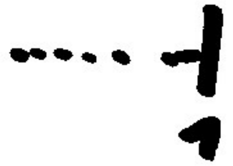
Ex: $p=2$

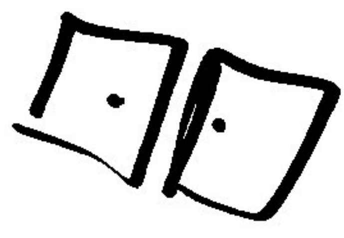
$\Rightarrow \mathbb{Z}_2 \overset{1:1}{\underset{\text{homeo}}{\longleftrightarrow}} \underbrace{\{0,2\}^{\mathbb{N}}}_{\text{Cantor set}} =: X$

Cantor set

$= \{x \in [0,1] \mid x$ has no 1 in its 3-adic expansion$\}$







In part.,

X compact, Hausdorff,
(Tychonoff)

totally disconnected ($\{x\}$ conn. comp.)

($\Updownarrow$

$\forall x \neq y \in X \ \exists\, U, V$ open + closed, s.t. $x \in U,\ y \in V,\ U \cap V = \emptyset$)

La5: Y top. space TFAE:

1) Y cpct, Hausdorff, tot. disc.

2) $Y \xrightarrow{\sim} \varprojlim_I Y_i$, Y_i finite, disc.

(I cofiltered cat.

$\Leftrightarrow$ i) $I \neq \emptyset$

ii) $\forall x, y \in I$ ex. $z \in I$ and morph. $z \to x, z \to y$

iii) $\forall x, y \in I$ $\forall a, b : x \to y$, ex. $z \xrightarrow{c} x$, s.t. $a \circ c = b \circ c$)

e.g. $I = (\ldots \to 2 \to 1 \to 0)$

$(\mathbb{N}, \leq)^{op}$

3) Y compact, Hausdorff, and each $y \in Y$ has a basis of compact + open nbhds.

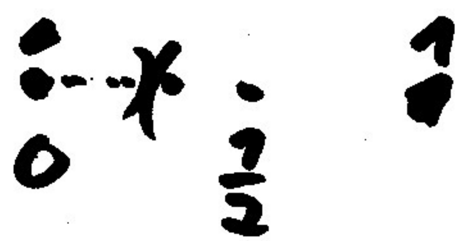
Such spaces are called profinite sets

Z top. space, $\mathcal{U} \subseteq \cancel{\{U \subseteq Z\}}$ $\subseteq \mathcal{P}(Z)$

nbhd basis of $z \in Z$, if. each $U \in \mathcal{U}$ is a nbhd of z and for each nbhd V of z ex. $U \in \mathcal{U}$, s.t. $U \subseteq V$

Ex: · $\mathbb{Z}_p$, Cantor set, $\prod_{\mathbb{N}}$ finite,

· $\{0\} \cup \{\frac{1}{n} \mid n \geq 1\}$



$\updownarrow$ bij.

· $\mathbb{N} \cup \{\infty\}$