Last time:

Metric and topology on $\mathbb{Q}_p$

- open balls $\{x \in \mathbb{Q}_p \mid |x-a| < r\}$

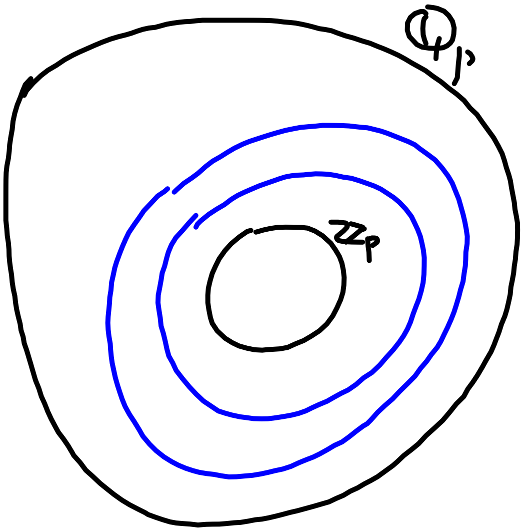
$$= \{x \in \mathbb{Q}_p \mid v(x-a) \geq n\}$$

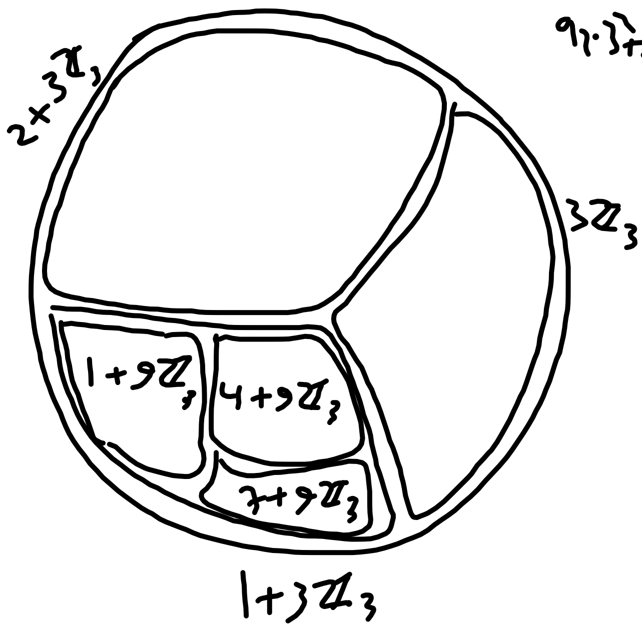
$$= \{x \in \mathbb{Q}_p \mid x \equiv a \mod p^n\}$$

p-adic numbers that agree with a in the digits up to p^n.

$$\mathbb{Q}_p = \bigcup_{n\geq 1} p^{-n}\mathbb{Z}_p$$

$$\mathbb{Z}_3 = \{a_0 + a_1 3 + a_2 \cdot 3^2 + \dots\}$$





Convergence & power series

In any non-Archimedean field $K, |\cdot|$

(i) $|x+y| \leq \max(|x|,|y|)$ — defn of non-Arch.

(ii) $|x_1+\dots+x_n| \leq \max_i(|x_i|)$ — (i) + induction

(iii) $|x+y| = |x|$ if $|y|<|x|$ — (i) for $x+y$ and for $(x+y)+(-y)$

(iv) $|x_1+\dots+x_n| = |x_1|$ if $|x_i|<|x_1|$ for $i \geq 2$ (induction)

(v) $(x_n)_{n\geq 1}$ Cauchy $\Leftrightarrow$ $|x_{n+1}-x_n| \to 0$ as $n\to\infty$.

If K is complete

$$\sum_{n=1}^{\infty} x_n \text{ converges} \iff x_n \to 0.$$

Freshman's dream

In $\mathbb{Q}_p$:

1) <u>Geometric series</u>

$$\frac{1}{1-x} = 1+x+x^2+x^3+\dots \quad \text{converges} \iff |x|<1$$

$$\iff x \in p\mathbb{Z}_p.$$

2) p-adic logarithm

$$\log_p(1+x) := x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \dots$$

This series converges precisely on $p\mathbb{Z}_p = \{x \mid |x|<1\}$

Proof If $x \notin p\mathbb{Z}_p$ then $v(x) \leq 0$ and

$$v\left(\frac{x^n}{n}\right) = nv(x) - v(n) \leq -v(n) \leq 0 \not\to \infty$$

so the series diverges.

If $x \in p\mathbb{Z}_p$ then $v(x) \geq 1$

$$v\left(\frac{x^n}{n}\right) = n\,v(x) - v(n) \geq n - v(n) \geq \frac{n}{2} \to \infty$$

as $n \to \infty \Rightarrow$ converges

Why $\frac{n}{2} \geq v(n)$? If not,

$n < 2v(n) \Rightarrow p^n \mid n^2$ impossible unless $p = n = 2$.

Ex $\log_2(\overset{1+2}{3}) = 2^2+2^4+2^5+2^6+2^7+2^{11}+O(2^{12})$

$\log_2(\underset{1+2}{-1}) = 0.$

Q Do usual rules apply, e.g.

$$\log_p\left((1+x)(1+y)\right) = \log_p(1+x)+\log_p(1+y)$$

for all $x, y \in p\mathbb{Z}_p$?

A Yes

<u>Proof</u> True / $\mathbb{C}$, $\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \ldots$

is an analytic fnc (in some nbd of 0) and

because $\log((1+x)(1+y)) = \log(1+x) + \log(1+y)$

. by uniqueness of Taylor expansions, this equality

must hold for power series (i.e. their terms agree).

Therefore their values agree in any field $(\supseteq \mathbb{Q})$

where they converge, in particular for $x, y \in p\mathbb{Z}_p$.

So for example $\log_2 9 = 2\log_2 3$.

3) p-adic exponential function

$$\exp_p(x) := 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$

$v(n^{th}\text{ term}) = n v(x) - v(n!)$

What is valuation of the n^{th} term

Lemma $v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$

Pf clear.

$1 \; 2 \; \dots \; n$

contribute $\lfloor \frac{n}{p} \rfloor$ p's to $n!$

+ higher order terms

$$x = p^{nv(x) - v(n!)}$$
$$n - \frac{n}{p-1}$$

Cor $v_p(n!) \leq \dfrac{n}{p-1}$

Pf $\displaystyle\sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor \leq \sum_{i=1}^{\infty} \frac{n}{p^i} = \frac{n}{p} \frac{1}{1-\frac{1}{p}}$

$$= \frac{n}{p-1}$$

Cor $\exp_p$ converges

- $(p>2)$ for $x \in p\mathbb{Z}_p$ (i.e. $|x|<1$)
- $(p=2)$ for $x \in 4\mathbb{Z}_2$ (i.e. $|x| < \frac{1}{2}$)

Pf For these x $v\left(\frac{x^n}{n!}\right) \to \infty$ as $n \to \infty$.

As above,

- $\exp_p(x+y) = \exp_p(x)\exp_p(y)$ $\quad x,y \equiv 0 \bmod p$ (resp $\equiv 0 \bmod 4$)
- $\exp_p(\log_p(1+x)) = 1+x$ $\quad x \equiv 0 \bmod p$ (resp $x \equiv 0 \bmod 4$)
- $\log_p(\exp_p(x)) = x$ $\quad$ — " — .

$$\frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!}$$

<u>Power function</u>

$$(1+x)^\alpha = \sum_{n=0}^{\infty} \binom{\alpha}{n} x^n \quad , \ldots$$

[+ sin, cos, ...]

<u>Exc</u> Prove that $\sqrt{6} \in \mathbb{Z}_5$.

$$= (1+5)^{1/2}$$

§ Additive structure of $\mathbb{Q}_p$, $\mathbb{Z}_p$

- $\mathbb{Q}_p$ (uncountably dim.) $\mathbb{Q}$-vector space.
  $\cup$
  $\mathbb{Z}_p$ (— " —) torsion-free ab. group.
- There is a ring hom. "reduction mod p^n" for any $n \geq 1$

$$\mathbb{Z}_p \longrightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$$
$$x \longmapsto x \bmod p^n$$

$\leftarrow$ [obvious map ($\mathbb{Z}_p \leftarrow \mathbb{Z}$), well-defined, injective, surjective because $\mathbb{Z} \subset \mathbb{Z}_p$ is dense]

- $\mathbb{Z} \supseteq p\mathbb{Z} \supseteq p^2\mathbb{Z} \supseteq \cdots$ $\leftarrow$ ab. gps

  filtration, $\bigcap = 0$, successive quotients $\mathbb{Z}/p\mathbb{Z}$

  $\mathbb{Z}_p \supseteq p\mathbb{Z}_p \supseteq p^2\mathbb{Z}_p \supseteq \cdots$ $\leftarrow$ ab. gps.

  filtration, $\bigcap = 0$, successive quotients $\mathbb{Z}/p\mathbb{Z}$

$$\frac{p^n\mathbb{Z}_p}{p^{n+1}\mathbb{Z}_p} \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

$$x \longmapsto n^{\text{th}} \text{ p-adic digit.}$$

- Look at units in $\mathbb{Z}_p$

  recall: $a \in \mathbb{Z}_p$ is a unit $\Leftrightarrow$ $v_p(a) = 0$ $\Leftrightarrow$ $a \bmod p \neq 0$.

§ Multiplicative structure of $\mathbb{Z}_p^\times$, $\mathbb{Q}_p^\times$

$$U_n := 1 + p^n \mathbb{Z}_p = \ker\left(\mathrm{red} : \mathbb{Z}_p^\times \xrightarrow{\bmod p^n} \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times\right)$$

subgroup of $\mathbb{Z}_p^\times$.

So $\mathbb{Z}_p^\times$ has a filtration by (open and closed) subgps

$$\mathbb{Z}_p^\times \supseteq \underset{\overset{\parallel}{U_1}}{1 + p\mathbb{Z}_p} \supseteq \underset{\overset{\parallel}{U_2}}{1 + p^2\mathbb{Z}_p} \supseteq \cdots$$

with $\mathbb{Z}_p^\times / U_1 \cong (\mathbb{Z}/p\mathbb{Z})^\times$, $\quad U_n / U_{n+1} \cong \mathbb{Z}/p\mathbb{Z}$

$x \longmapsto 0^{th}$ p-adic digit $\qquad x \longmapsto n^{th}$ p-adic digit.

Thm As (topological) groups

(a) $\mathbb{Q}_p^\times \cong \mathbb{Z}_p^\times \times \mathbb{Z}$

(b) $U_n = (1 + p^n\mathbb{Z}_p, \times) \cong (\mathbb{Z}_p, +)$

for all $n \geq 1$ if p odd
for all $n \geq 2$ if $p = 2$.

(c) $\mathbb{Z}_p^\times \cong \mathbb{Z}_p \times (\mathbb{Z}/p\mathbb{Z})^\times$ if $p > 2$

$\cong \mathbb{Z}_2 \times \{\pm 1\}$ if $p = 2$.

Aside on split exact sequences

[all maps are homs]

A sequence of ab. groups

$$0 \longrightarrow A \xrightarrow{\alpha} B \underset{\gamma}{\overset{\beta}{\rightleftarrows}} C \longrightarrow 0$$

is **exact** if α injective, β surjective, and β induces $B/A \xrightarrow[\sim]{\beta} C$.

It **splits** if $\exists\, \gamma : C \to B$ s.t. $\beta \circ \gamma = id_C$.

Equivalently $A \times C \cong B$

$$a, c \longrightarrow \alpha(a) + \gamma(c)$$

Not every exact seq. splits:

<u>Ex</u> $0 \longrightarrow \mathbb{Z} \xrightarrow{i_1} \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \xrightarrow{p_2} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$

splits

$0 \longrightarrow \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \xrightarrow{\text{mod } 2} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$

does not.

(no non-trivial gp. homs $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$).

Often used to prove that $B \cong A \times C$ non-canonically

(γ not unique).

Ex B any fin. gen. ab. group (units $\mathcal{O}_K^\times$ in a number field K,

or $E(\mathbb{Q})$ gp. of rational pts on an elliptic curve)

$\Rightarrow B \cong T \times \mathbb{Z}^r$ T finite (torsion)

$r \geq 0$ rank.

but this is usually non-canonical.

The group T is canonical,

$$T = \{ x \in B \mid x \text{ has finite order} \}$$

and

$$0 \longrightarrow T \longrightarrow B \longrightarrow \mathbb{Z}^r \longrightarrow 0$$

splits (exc: any $0 \to A \to B \to \mathbb{Z}^r \to 0$ always splits)

but splitting is not unique $\Rightarrow$ no canonical copy of $\mathbb{Z}^r$ inside B.

(a) $0 \longrightarrow \mathbb{Z}_p^\times \longrightarrow \mathbb{Q}_p^\times \xrightarrow{v_p} \mathbb{Z} \to 0$

splits, by e.g. $\mathbb{Z} \longrightarrow \mathbb{Q}_p^\times$

$n \longmapsto p^n$

In other words, every $x \in \mathbb{Q}_p^\times$ can be written uniquely as $x = u \cdot p^n$, $u \in \mathbb{Z}_p^\times$, $n \in \mathbb{Z}$.

(b) $\exp_p : p^n\mathbb{Z}_p \xrightarrow{\ \sim\ } (1+p^n\mathbb{Z}_p, \times) = U_n$

$\log_p : 1+p^n\mathbb{Z}_p \xrightarrow{\ \sim\ } p^n\mathbb{Z}_p \cong \mathbb{Z}_p$

$$p^n x \leftarrow x$$

are isomorphisms, provided $n \geq 1$ $(p>2)$,
resp. $n \geq 2$ $(p=2)$.

(c) $\underline{p=2}$

$$\begin{tikzcd}
0 \arrow[r] & U_2 \arrow[r] \arrow[d, equal, "\log"] & \mathbb{Z}_2^\times \arrow[r] & (\mathbb{Z}/4\mathbb{Z})^\times \arrow[r] \arrow[d, equal] & 0 \\
& 1+4\mathbb{Z}_2 \cong 4\mathbb{Z}_2 \cong \mathbb{Z}_2 & x \mapsto x \bmod 4 & \{\pm 1\} &
\end{tikzcd}$$

$$\underset{\times}{1+4\mathbb{Z}_2} \qquad \underset{+}{4\mathbb{Z}_2}$$

and the sequence splits $(\mathbb{Z}/4\mathbb{Z})^\times \longrightarrow \mathbb{Z}_2^\times \quad \begin{matrix} 1 \longmapsto 1 \\ -1 \longmapsto -1 \end{matrix}$

In other words every number in $\mathbb{Z}_2^\times = 1 + 2\mathbb{Z}_2$

can be written uniquely as $\pm 1 \times \underbrace{\text{something}}_{\equiv 1 \bmod 4}$

$$(\text{and things} \equiv 1 \bmod 4, \times) \cong \mathbb{Z}_2$$

$$\exp(1+4x) \longleftarrow x$$

$\mathbb{Z}_2^\times$

$1+4\mathbb{Z}_2$

$3+4\mathbb{Z}_2$

$\overset{\exp}{\underset{\log}{\cong}}$ $(\mathbb{Z}_2, +)$

$$\mathbb{Z}_2^\times \cong \{\pm 1\} \times \mathbb{Z}_2$$

$\mathbb{R}^\times$

>0

<0

$\overset{\exp}{\underset{\log}{\cong}}$ $(\mathbb{R}, +)$

$$\mathbb{R}^\times \cong \{\pm 1\} \times \mathbb{R}$$

$\boxed{p>2}$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_1 & \longrightarrow & \mathbb{Z}_p^\times & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times & \longrightarrow & 0 \\ & & \parallel & & [a] & \longleftarrow & a & & \\ & & (1+p\mathbb{Z}_p, \times) & & & & & & \\ & & 2\wr\parallel & & & & & & \\ & & (\mathbb{Z}_p, +) & & & & & & \end{array}$$

and the sequence splits by Homework #3. ∎

Ex $p=5$ $(\mathbb{Z}/5\mathbb{Z})^\times$ cyclic group of order 4

$\{1, 2, 3, 4\}$

generator

$$\mathbb{Z}_5^\times \ni [1] = 1$$

$$[2] = 2 + 1\cdot 5 + 2\cdot 5^2 + 1\cdot 5^3 + 3\cdot 5^4 + \dots$$

$$[3] = 3 + 3\cdot 5 + 2\cdot 5^2 + 3\cdot 5^3 + 5^4 + \dots$$

$$[4] = -1$$

"i" and "$-i$" in $\mathbb{Q}_5$