Last time: <u>inverse limits</u>

$(I, \leq)$ p.o. set

$(A_i)_{i \in I}$ groups, ring, top. spaces, ...

$\pi_{ij} : A_j \longrightarrow A_i$ maps for $i \leq j$.

<u>Def</u> $A = \varprojlim_{A_i} = \{ (a_i) \in \prod_{i \in I} A_i \mid \pi_{ij}(a_j) = a_i \ \forall i \leq j \}$

Ex $I = (\mathbb{N}, \leq)$

$$A_i = k[t]/t^i$$ ← polynomials $a_0 + a_1 t + \dots + a_{i-1} t^{i-1}$

$$\pi_{ij} : A_j \xrightarrow[\text{mod } t^i]{} A_i \qquad i \leq j.$$

$$\varprojlim_{i \in \mathbb{N}} \frac{k[t]}{t^i} = k[[t]]$$ power series

compatible sequences of polys

$a_0 + a_1 t + a_2 t^2 + \dots$

Ex Similarly, $A_i = \mathbb{Z}/p^i\mathbb{Z}$, $A_j \xrightarrow[\text{mod } p^i]{} A_i$ $i \leq j$

$$\varprojlim_{i \in \mathbb{N}} \mathbb{Z}/p^i\mathbb{Z} \cong \mathbb{Z}_p = \{a_0 + a_1 p + a_2 p^2 + \dots \quad a_i \in \{0, \dots, p-1\}\}.$$

as topological rings (Exc.: with discrete topology on $\mathbb{Z}/p^i\mathbb{Z}$ the inverse limit top. on $\varprojlim$ is the p-adic top. on $\mathbb{Z}_p$).

Same basic open sets $a + p^r\mathbb{Z}_p$.

<u>Ex</u> $I = (\mathbb{N}, |)$

$A_i = \mathbb{Z}/i\mathbb{Z}$, same π_{ij} as above (mod i)

$$\varprojlim_{i \in I} \mathbb{Z}/i\mathbb{Z} = \hat{\mathbb{Z}} \leftarrow \text{topological ring}$$

<u>Exc</u> $\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$.

Rmk Inverse limits can be defined in any category

Given (I, A_i, π_{ij}) want $A = \varprojlim_{I} A_i$ s.t.

1) Have maps $f_i : A \longrightarrow A_i$ s.t. $\pi_{ij} \circ f_j = f_i$

2) A is universal w.r.to this property.

§ Completion $\Leftrightarrow$ inverse limits

$K, |\cdot|$ non-Archimedean, $\mathcal{O}, \mathfrak{m}$.

v assoc. valuation, normalise s.t. $v(\pi) = 1$ for some $\pi \in \mathfrak{m} \setminus \{0\}$.

Prop K complete w.r.to $|\cdot|$ $\Leftrightarrow$ the map

$$\mathcal{O} \longrightarrow \varprojlim_{i \in \mathbb{N}} \mathcal{O}/\pi^i \mathcal{O}$$
$$x \longmapsto (x \bmod \pi^i)_i$$

is an isomorphism.

called the completion of a ring $\mathcal{O}$ w.r.to an ideal (π)

Pf Write $K = \bigcup_x (x + \mathcal{O})$ ← open and closed sets $x \in K/\mathcal{O}$ cosets.

K complete $\iff$ each $x + \mathcal{O}$ is complete

$\iff$ $\mathcal{O}$ is complete w.r.t. $|\cdot|$ $\iff$

(A) $\forall (x_n) \subseteq \mathcal{O}$ with $|x_n - x_{n+1}| \to 0$ $\exists!\, x \in \mathcal{O}$ s.t. $|x_n - x| \to 0$

Now $\mathcal{O} \to \varprojlim \mathcal{O}/\pi^n\mathcal{O}$ is $\cong$ $\iff$

(B) $\forall (x_n) \subseteq \mathcal{O}$ with $v(x_n - x_{n+1}) \geq n$ $\exists!\, x \in \mathcal{O}$ s.t. $v(x - x_n) \geq n$

But every sequence as in (A) has a subsequence as in (B), so (A) $\iff$ (B) $\blacksquare$.

§ Profinite groups

G_i finite groups, $i \in I$ p.o.set,
with discrete topology

$\pi_{ij} : G_j \to G_i$ gp. homs as before.

Def $G = \varprojlim_{i \in I} G_i$ is called a profinite group

and the inverse limit topology the profinite topology

(the coarsest topology that makes the natural projections $G \to G_i$ continuous.)

Rmk G_i are compact $\Rightarrow$ so is $G \leq \prod G_i$.

Ex $(\mathbb{Z}_p, +)$, $(\mathbb{Z}_p^\times, \times)$, $(\mathbb{F}_p[[t]], +)$,
$(\hat{\mathbb{Z}}, +)$, $(\hat{\mathbb{Z}}^\times, \times)$.

Main example:
L/K algebraic field ext., not necessarily finite;
say $L = \bigcup_{i \in I} L_i$ L_i/K finite Galois.

Then

$$\mathrm{Gal}(L/K) := \varprojlim_{i \in I} \mathrm{Gal}(L_i/K)$$

is a profinite topological group.

[Main Thm. of Galois theory

- intermediate fields $K \leq U \leq L$ $\xleftrightarrow{1:1}$ closed subgroups of $\mathrm{Gal}(L/K)$
- —"— s.t. U/K finite $\xleftrightarrow{1:1}$ open subgroups of $\mathrm{Gal}(L/K)$].

In particular, $\mathrm{Gal}(\overline{K}/K)$ is profinite.

<u>Exc</u> (i) $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \cong \hat{\mathbb{Z}}$.

$\mathrm{Frob}_p : x \mapsto x^p \longleftrightarrow 1$

(ii) $\mathrm{Gal}\left(\mathbb{Q}\left(\begin{smallmatrix}\text{all roots of}\\ \text{unity}\end{smallmatrix}\right)/\mathbb{Q}\right) \cong \hat{\mathbb{Z}}^\times$.

<u>Rmk</u> $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is unknown.

§ Local fields

Def K field, $|\cdot|$ abs. value. K is a local field if it is locally compact as a top. space.

{ Top. space X is compact if every open cover $X = \bigcup_{i \in I} U_i$ has a finite subcover.

X is locally compact if every pt $x \in X$ has an open nbd U s.t. $\overline{U}$ is compact.

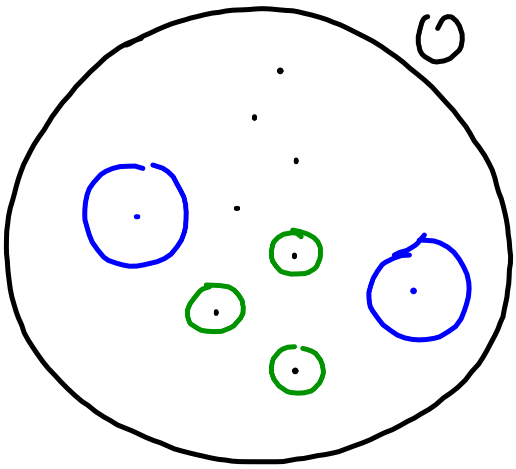
A metric space X is locally compact $\Leftrightarrow$ $\forall x \in X$ there is a compact disk $\{y \in X \mid d(x,y) \leq r\}$, some $r > 0$ }

<u>Lemma</u> K locally compact $\Leftrightarrow$ $\mathcal{O} = \{x \in K \mid |x| \leq 1\}$
closed unit ball
is compact.

<u>Pf</u> Exercise

<u>Lemma</u> K local (ly compact) $\Rightarrow$ K complete.

<u>Pf</u> If K not complete, take (x_i) Cauchy s.t. $|x_i| \leq 1$ (WLOG) and x_i has no limit in $\mathcal{O}$



$\forall x \in \mathcal{O}$ has an open nbd D_x s.t.

- $D_x \not\ni$ any x_i if $x \neq x_i$
- $D_{x_i} \not\ni x_j$ for $j \neq i$

Then $\mathcal{O} = \bigcup_x D_x$ has no finite subcover (need all D_{x_i} to cover (x_i))

$\Rightarrow \mathcal{O}$ not compact $\Rightarrow K$ not local.

<u>Thm</u> If K is a local field, then one of the following holds:

(1) $K \cong \mathbb{R}$ or $\mathbb{C}$ (Archimedean case)

(2) $K \cong \mathbb{F}_q((t))$ (Equal characteristic case)

(3) $K/\mathbb{Q}_p$ finite for some (unique) prime p (Mixed characteristic case)

Proof If K Archimedean, K local $\Rightarrow K$ complete

$\Rightarrow K \cong \mathbb{R}$ or $\mathbb{C}$ (and these two are indeed locally compact).

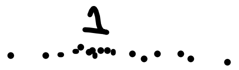
From now on,

$K, |\cdot|$ non-Archimedean, $\mathcal{O}, \mathfrak{m}$, $k = \mathcal{O}/\mathfrak{m}$.

Step 1 k is finite.

Pf $\underbrace{\mathcal{O}}_{\text{compact}} = \bigcup_{a \in \mathcal{O}/\mathfrak{m} = k} a + \mathfrak{m}$.

If k is infinite, this is an open cover of $\mathcal{O}$ with no finite subcover.



Step 2 $|\cdot|$ is discrete

Pf Otherwise $\exists\, x_i \in \mathfrak{m}$ s.t. $|x_i| \uparrow 1$

Then $\mathfrak{m} = \bigcup x_i \mathcal{O}$ ← open cover

and $\mathcal{O} = \bigcup_{a \in \mathcal{O}/\mathfrak{m}} \bigcup_{i} a + x_i \mathcal{O}$ ← again open cover, no finite subcover.

<u>Step3</u> if $\operatorname{char} K = p > 0$, then $\operatorname{char} k = \operatorname{char} K$

so $k = \mathbb{F}_q$, $q = p^n$.

$$\begin{tikzcd} K & \\ \mathbb{F}_p \arrow[u, hook] \arrow[r, hook] & k = \mathbb{F}_{p^n} = \mathbb{F}_p\left(\begin{matrix}(p^n-1)\text{th} \\ \text{roots of unity}\end{matrix}\right) \end{tikzcd}$$

$$= \mathbb{F}_p(\text{roots of eqn } X^{p^n-1}-1)$$

Teichmuller lifts (or Hensel's lemma applied to $X^{p^n-1}-1$)

$\Rightarrow$ K contains (p^n-1)th roots of 1 $\Rightarrow$ $\mathbb{F}_q \hookrightarrow K$.

View $\mathbb{F}_q \subset \mathcal{O} \leq K$ as a set of representatives of the residue field in $\mathcal{O}$ $\quad \left[\mathcal{O} \xrightarrow{\text{mod } m} k \right]$

Take any uniformiser π of K.

Lemma long ago $\Rightarrow$

$$\mathcal{O} = \left\{ \sum_{n=0}^{\infty} a_n \pi^n \;\middle|\; a_n \in \mathbb{F}_q \right\} \overset{!}{=} k[[\pi]] \cong \mathbb{F}_q[[t]].$$

so $K \cong \mathbb{F}_q((t))$.

Step 4 If char $K = 0$, $\mathbb{Q} \hookrightarrow K$

Restriction of $|\cdot|$ to $\mathbb{Q}$ is

- non-trivial (otherwise .

if char $K=0$, $\mathbb{Q} \hookrightarrow K$

Res. of $|\cdot|$ to $\mathbb{Q}$ is

- non-trivial, otherwise $\mathbb{Z} \hookrightarrow \mathcal{O}$ is an infinite discrete set, and $\mathcal{O}$ is compact.
- non-Archimedean, — " —.

So $|\cdot|\big|_{\mathbb{Q}} \sim |\cdot|_p$ for some prime p. Take completions

$$\mathbb{Q} \hookrightarrow K \implies \mathbb{Q}_p \hookrightarrow K.$$

So enough to prove $[K:\mathbb{Q}_p] < \infty$.

i.e. K has a finite basis over $\mathbb{Q}_p$.

- $\mathbb{Z}_p \hookrightarrow \mathcal{O}$ and $\mathbb{F}_p \hookrightarrow k$. Say $[k:\mathbb{F}_p] = f$, and let $v_1 \dots v_f \in \mathcal{O}$ lift a basis $\overline{v_1}, \dots, \overline{v_f}$ of k over $\mathbb{F}_p$.
- $p \in \mathfrak{m} \Rightarrow v(p) = e \geq 1$, i.e. $p = \pi^e_{\times \text{unit}}$

  └ normalised ~~discrete~~ valuation $v: K^\times \twoheadrightarrow \mathbb{Z}$ for $|\cdot|$

- Exc: Check that $(v_i \pi^j)_{\substack{0 \le i < f \\ 0 \le j < e}}$ form a basis for $\mathcal{O}$ over $\mathbb{Z}_p$, and for K over $\mathbb{Q}_p$ $\blacksquare$

$\mathbb{F}_{p^n}((t))$

Rmk This might suggest that $K = \mathbb{F}_p((t))$ has only one extension of each degree $n \geq 1$, namely $\mathbb{F}_{p^n}((t))$. This is not so:

Ex $K = \mathbb{F}_p((t))$, p odd, look at quadratic exts

$$K^\times \cong \mathbb{F}_p^\times \times \underbrace{(1+m)}_{\text{all squares by Hensel}} \times \underbrace{\mathbb{Z}}_{\text{from } t^n}$$

$$K^\times / K^{\times 2} = \mathbb{F}_p^\times / \mathbb{F}_p^{\times 2} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \cong \underbrace{\frac{\mathbb{Z}}{2\mathbb{Z}}}_{1,\eta} \times \underbrace{\frac{\mathbb{Z}}{2\mathbb{Z}}}_{1,t}.$$

So K has 3 quad. exts,

$$K(\sqrt{\eta}) \cong \mathbb{F}_{p^2}((t))$$

$$K(\sqrt{t}) \underset{\sqrt{t} \longleftrightarrow t}{\cong} \mathbb{F}_p((t))$$

$$K(\sqrt{\eta t}) \underset{\sqrt{\eta t} \longmapsto t}{\cong} \mathbb{F}_p((t))$$