We've been classifying quad sp. over fields k ($\mathbb{C}, \mathbb{R}, \mathbb{F}_p$)
This is an arithmetic problem → understanding squares!

Big Pic

Def A field k is **algebraically closed** if every non-const poly w/ coeff in k has roots in k.

e.g. $\mathbb{C}$ is alg closed

Thm Every field k has an "alg closure" $\overline{k}$ s.t.
- $\overline{k}$ is alg closed
- $\overline{k}/k$ is an alg extension. every elt of $\overline{k}$ is a root of poly with coeff in k

(think of recall Sp: quotient)

$\mathbb{C}/\mathbb{R}$

$\overline{k}$ unique up to iso.

Def The **absolute Galois gp** of k, called G_k, is the gp of all field auto of $\overline{k}$ that restrict to the identity on k

G_k measures how much arithmetic is over k.

Ex $k = \mathbb{R}$, $\overline{k} = \mathbb{C}$

$\sigma \in G_k$ $\sigma : \mathbb{C} \to \mathbb{C}$ field aut $\sigma|_{\mathbb{R}} = id$

$a \in \mathbb{R}$, $b \in \mathbb{C}$ $\sigma(ab) = \sigma(a)\sigma(b) = a \cdot \sigma(b)$

$\Rightarrow \sigma$ is $\mathbb{R}$ linear. $\sigma(1) = 1$ (field homom)

$i^2 = -1 \Rightarrow -1 = \sigma(-1) = \sigma(i)^2$

$\Rightarrow \sigma(i) = \pm i$

$G_k = \{1, \gamma\} \cong \mathbb{Z}/2\mathbb{Z}$ ← conjugation

field	$\mathbb{C}$	$\mathbb{R}$	$\mathbb{F}_p$	$\mathbb{Q}_p$	$\mathbb{Q}$
G_k	trivial	$\mathbb{Z}/2\mathbb{Z}$	$\widehat{\mathbb{Z}}$ (cish)	Shockingly complicated but known it is solvable	very hard

actually $\widehat{\mathbb{Z}}$ profinite comp of $\mathbb{Z}$

$= \varprojlim \mathbb{Z}/n\mathbb{Z}$

easy → hard

Constr of $\mathbb{Q}_p$ ⟶ fix prime p.

Recall $|\cdot|$ is the abs val on $\mathbb{Q}$. Can define Cauchy sequence of $\mathbb{R}$ by eqv class of Cauchy seq in $\mathbb{Q}$.
↳ completion of $\mathbb{Q}$.

Defn let $x \in \mathbb{Q}$. Can write $x = p^r \frac{a}{b}$ where $r \in \mathbb{Z}$, a, b coprime to p.
define $|x|_p = p^{-r}$, $|0|_p = 0$.

e.g. $|p^3|_p = \frac{1}{p^3}$ small
$|p^{-3}|_p = p^3$ big

$|n|_p \leq 1 \ \forall n \in \mathbb{Z}$.

Things are close if high p divisibility.

Prop
- $|0|_p = 0$
- $|1|_p = 1$
- $|xy|_p = |x|_p \cdot |y|_p$
- Ultrametric inequality.
  $|x+y|_p \leq \max(|x|_p, |y|_p)$

↳ Ex.
$|x|_p = |y|_p = 1$
x has no ps in num or denom
xy has no p's in denom
$\Rightarrow |xy|_p \leq 1$

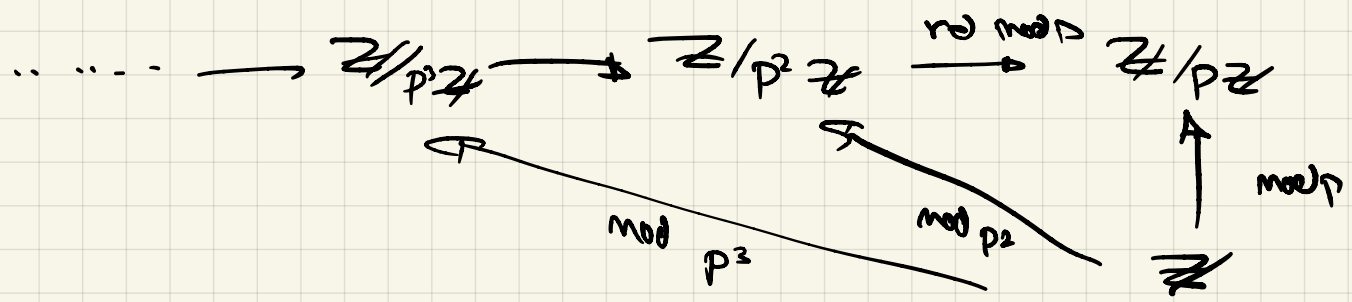
Def $\mathbb{Q}_p$ is the compl of $\mathbb{Q}$ wrt $|\cdot|_p$

Basics
- $\mathbb{Q}_p$ is a field.
- $\mathbb{Q} \subset \mathbb{Q}_p$ contained & dense.
- $|\cdot|_p$ is still well def in $\mathbb{Q}_p$ $|\cdot|: \mathbb{Q}_p \to \mathbb{R}_{\geq 0}$

Def $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$. ↳ this is a subring of $\mathbb{Q}_p$ (not a field)
$\mathbb{Z} \leq \mathbb{Z}_p$.
↳ closure by prop.

Fact $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$?

⟶



An elt of $\mathbb{Z}$ gives a comp seq of elt of $\mathbb{Z}/p^n\mathbb{Z}$ $\forall n$

Def) $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is the seq of all comp seq i.e.

$(x_1, x_2, \dots)$ s.t. $x_i \in \mathbb{Z}/p^i\mathbb{Z}$ $x_{i+1} \equiv x_i \pmod{p^i}$

Fact) -1 is a square in $\mathbb{Z}_5$.

$\mathbb{Z}/5\mathbb{Z}$ → $2, 3$ ($\equiv \pm 2$) are square roots of -1

$\mathbb{Z}/25\mathbb{Z}$ → ± 7 are

$\mathbb{Z}/125\mathbb{Z}$ → how to reduce 7 mod 25

$x = 25y + 7$

$x^2 = 49 + 2 \cdot 7 \cdot 25y \pmod{5^3}$

(to make -1)

$0 = x^2 + 1 = 50 + 2 \cdot 7 \cdot 25y$

$= 25(2 + 2 \cdot 7y) = 0 \pmod 5$

(is a soln)

$\mathbb{Z}/5^4\mathbb{Z}$ ....

There are 2 compatible seq (pos, neg) of sq rt of -1.

(so define two roots of -1 in $\varprojlim \mathbb{Z}/5^n\mathbb{Z}$.

The integers give seq $(2, 7, \dots)$ give a Cauchy seq if you wanna think as $\mathbb{Z}_p$ in that way.

Rem) if $(n, p) = 1$ & $n = \square$ in $\mathbb{F}_p$ (square)

$\Rightarrow n = \square$ in $\mathbb{Z}_p$