

Numbers and geometry

Peter Schöbe

Aim: Study integers

$$\mathbb{Z} = \{ \dots, -2, -1, 0, 1, 2, 3, \dots \}$$

- Are there solutions in integers?

Fermat's Last Theorem (Wiles 1994):

$$x^n + y^n = z^n, \quad n > 2 \quad \Rightarrow \quad xyz = 0.$$

- How many?
 $y^2 = x^3 + ax + b,$ a, b given.

Finite or infinite number of solutions?

~ Birch-Swinnerton-Dyer conjecture.

Examples: (No solutions)

i) $x^2 = -1$: No solutions in \mathbb{R} \Rightarrow no solutions in \mathbb{Z} .

ii) $x^2 = 2$, or $x^2 = 2y^2$: look at powers of 2 in prime factorization.
 \Rightarrow no solutions in \mathbb{Z} .

iii) $x^2 + y^2 = 3z^2$:

Claim. If 3 divides $x^2 + y^2$, then 3 divides xy .

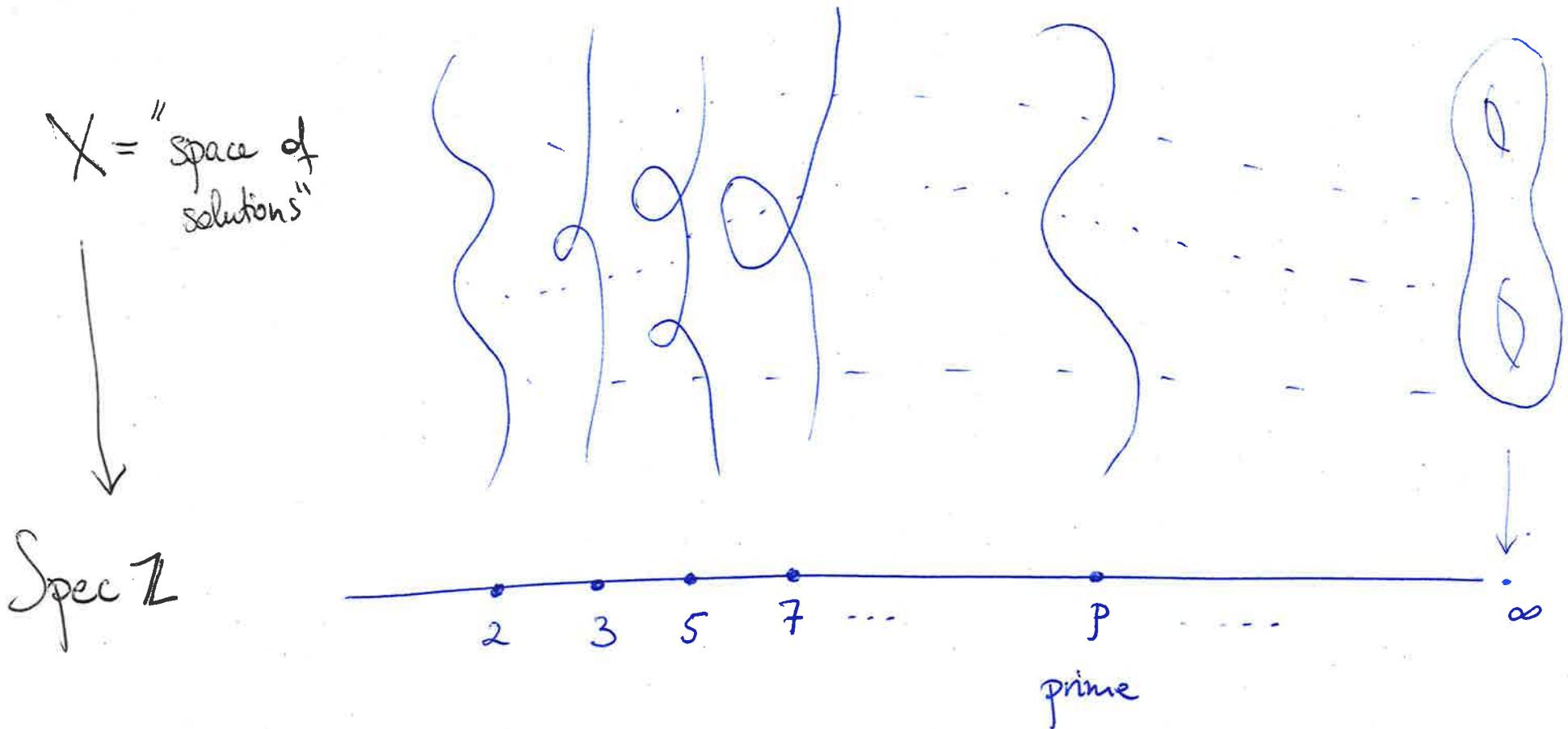
Proof. Table of residues of division by 3:

$$x^2 + y^2$$

$y \backslash x$	0	1	2
0	0	1	1
1	1	2	2
2	1	2	2

Compute in
 $\{0, 1, 2\} = \mathbb{Z}/3\mathbb{Z}$

Picture: given any system of polynomial equations,



Algebraic Geometry

Goal: Study **geometry** in terms of **algebra**.

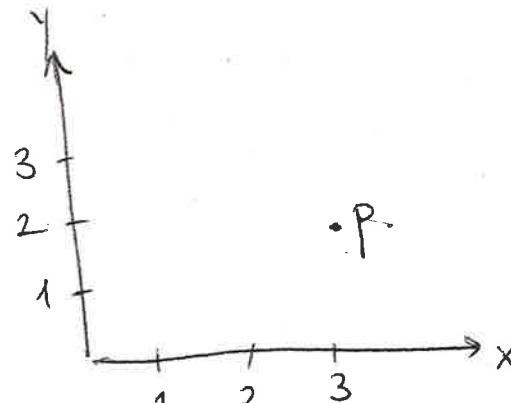
Dually, turn **algebra** into **geometry**,

Descartes

Coordinates.

space $X = \text{plane}$.

Choose coordinates xy



~ define continuous maps $f: X \rightarrow \mathbb{R}$
eg. $P \mapsto$ x-coordinate of P .

→ Any (usual) space X can be studied through

$$C(X, \mathbb{R}) = \{ \text{continuous maps } f: X \rightarrow \mathbb{R} \}$$

Point $p \in X$

map $C(X, \mathbb{R}) \longrightarrow \mathbb{R} (= C(\{p\}, \mathbb{R}))$

$$f \longmapsto f(p)$$

$$C(X, \mathbb{R}) : \text{ring } (+, -, \cdot)$$

$$\mathbb{R} : \text{field } (+, -, \cdot, \div)$$

space $\xrightarrow{\quad}$ ring

point $\xrightarrow{\quad}$ field.

Algebra

A ring

K field

maps $A \rightarrow K$

Geometry

$\text{Spec } A$ space

$\text{Spec } K$ point

points of $\text{Spec } A$

Rings:

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

$\frac{-7}{13}$

e^π

i

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \dots, n-1\}$$

$$1 + (n-1) = 0.$$

Fields:

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$

p prime.

$$\frac{1}{2} = 2 \in \mathbb{Z}/3\mathbb{Z}.$$

$\text{Spec } \mathbb{Z} = \{\mathbb{Z} \rightarrow K \mid K \text{ field}\}$

$= \{K \text{ field}\} \ni \{\mathbb{F}_2, \mathbb{F}_3, \dots, \mathbb{F}_p, \dots, \mathbb{Q}, \mathbb{R}\}$

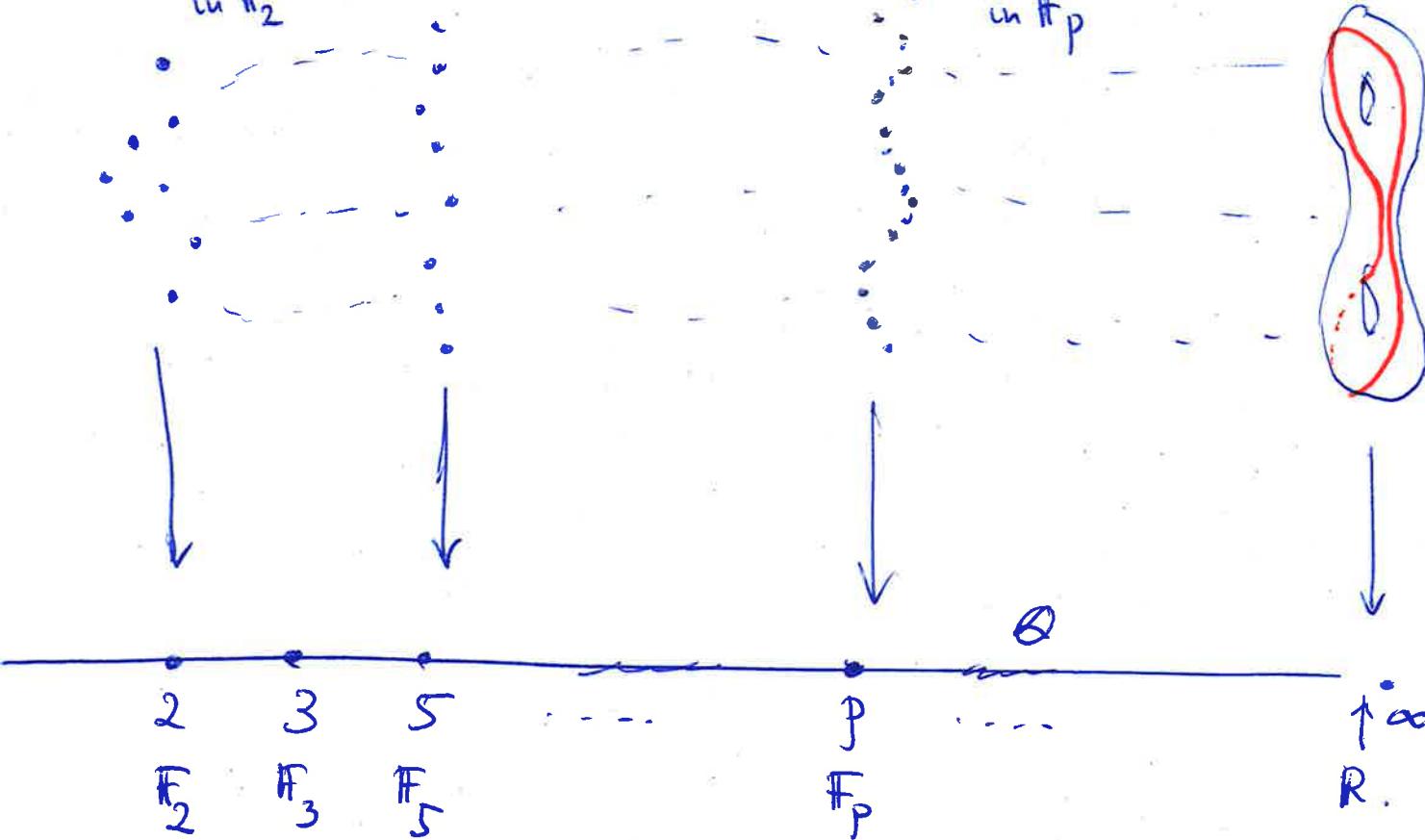
X = "space of
solutions"

$X(\mathbb{F}_2) = \text{solutions}$
in \mathbb{F}_2

$X(\mathbb{F}_5)$

$X(\mathbb{F}_p) = \text{solutions}$
in \mathbb{F}_p

$X(\mathbb{R}) \subseteq X(\mathbb{C})$



Better: Allow only algebraically closed fields K .

Examples: $\mathbb{C} \supseteq \bar{\mathbb{Q}} = \{x \in \mathbb{C} \mid \exists a_0, \dots, a_{n-1} \in \mathbb{Q}: x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0\}$

$\overline{\mathbb{F}_p}$ = algebraic closure of \mathbb{F}_p .

= $\bigcup_{r \geq 1} \mathbb{F}_{p^r}$, \mathbb{F}_{p^r} unique (up to isom.) field with p^r elements.

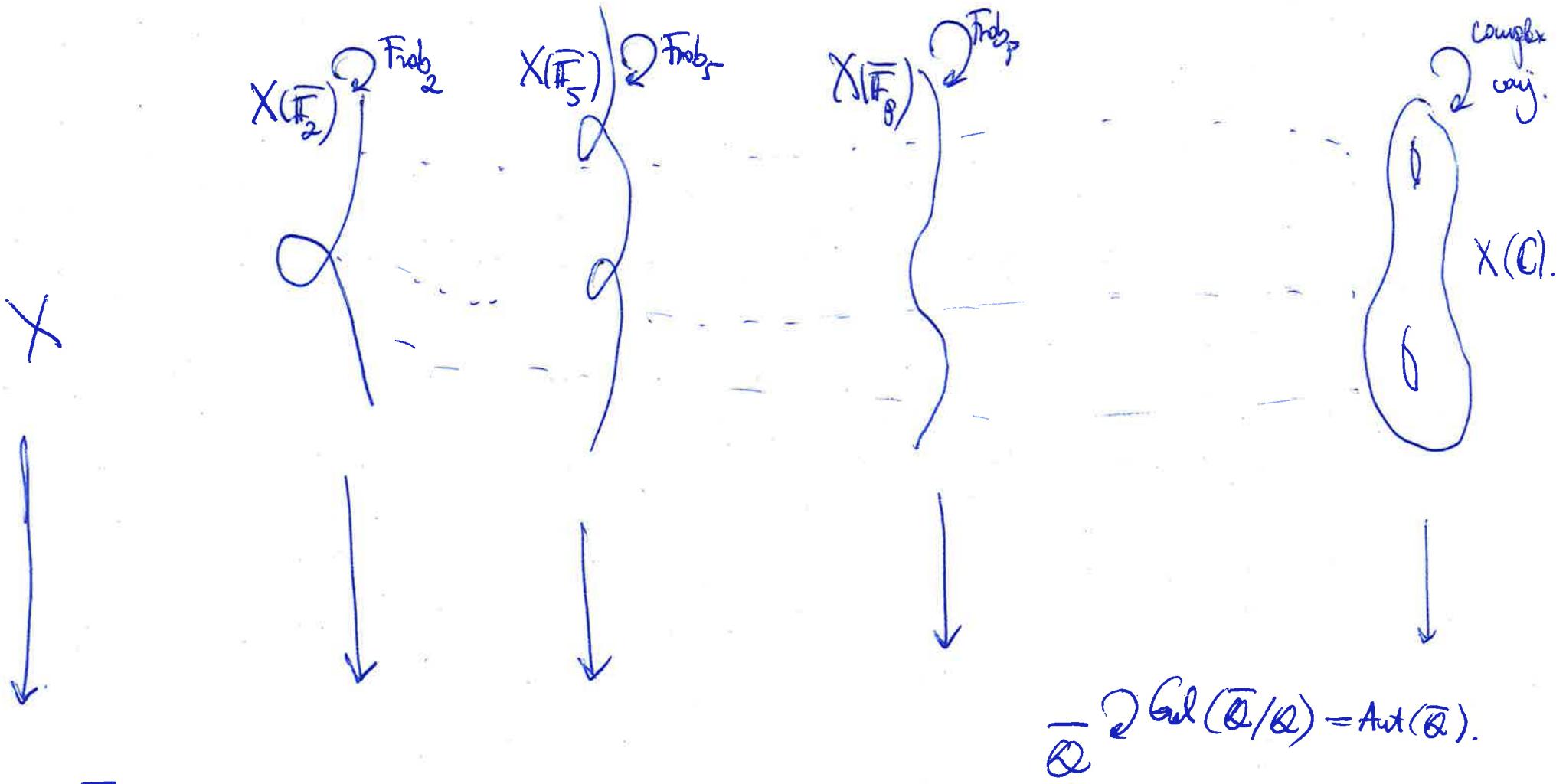
Proposition. If K field of characteristic p , i.e.

$$\underbrace{1+1+\dots+1}_p = 0 \in K,$$

"Frobenius"

then $x \mapsto x^p$ commutes with $+, -, \cdot, \div$.

Example ($p=2$) $(x+y)^2 = x^2 + 2xy + y^2 = x^2 + y^2$ if $2=0$.

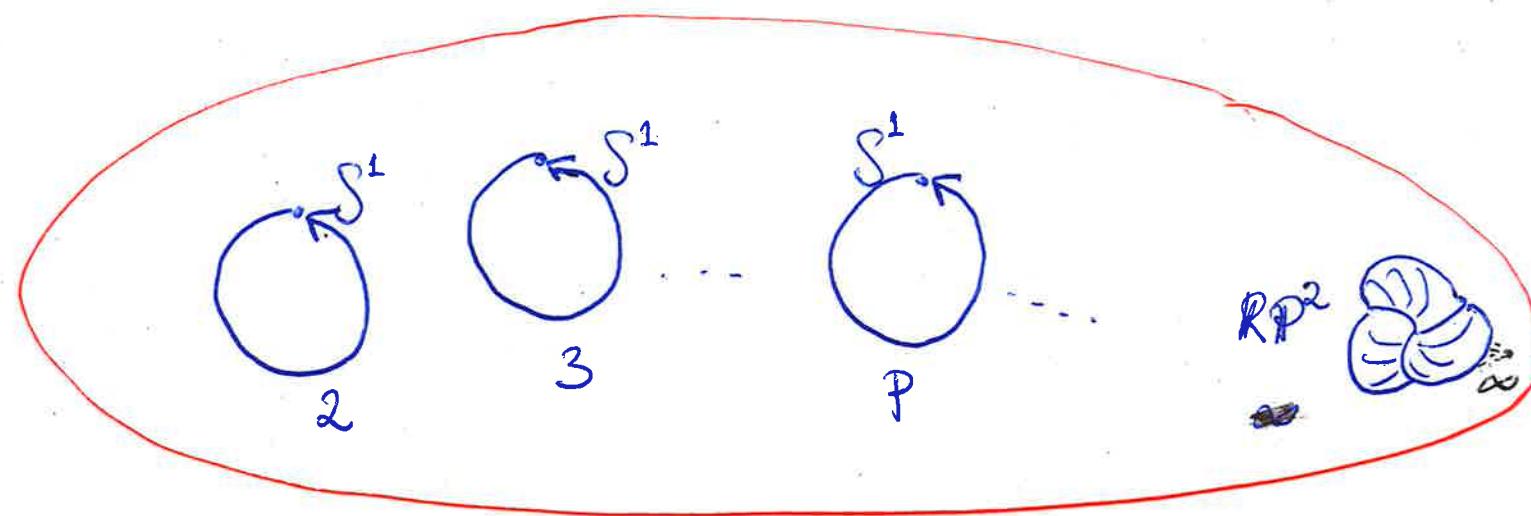


Spec \mathbb{Z}

2	3	5	\dots	p	\dots	\mathbb{Q}
\bar{F}_2	\bar{F}_3	\bar{F}_5	\dots	\bar{F}_p	\dots	\mathbb{C}
G	G	G	\dots	G	\dots	\mathbb{C}
Frob_2	Frob_3	Frob_5	\dots	Frob_p	\dots	complex conjugation.

Picture:

$$\text{Spec } \mathbb{Z} \ni \bar{\mathbb{F}_p} \supset \text{Frob}_p$$



$\text{Spec } \mathbb{Z}$.

Properties of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \Rightarrow \text{Spec } \mathbb{Z}$ behaves like 3-manifold.

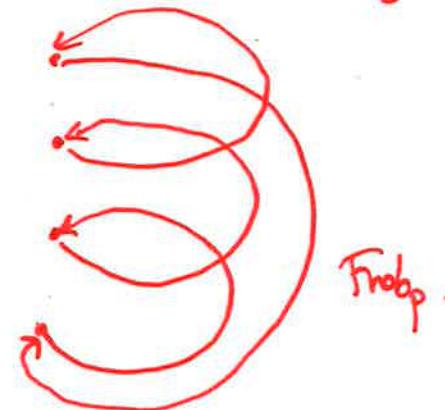
(duality in etale cohomology like Poincaré duality of 3-manifold).

Analogy $\text{Spec } \mathbb{F}_p \simeq \text{circle}$

Then:

$$\{\text{finite extensions of } \mathbb{F}_p\} \simeq \{\text{fin. coverings of } S^1\}^\oplus$$

\mathbb{F}_{p^n}



Frob.

$\text{Hom}(\mathbb{F}_{p^n}, \bar{\mathbb{F}}_p)$.

Finite set



Field / Galois
theory.

topology / fundamental groups.

Analogy Galois groups / fundamental groups

Thm (Galois) k perfect field, \bar{k} algebraic closure.

$$\{ \text{finite extensions of } k \} \cong \{ \text{sets with } \text{Gal}(\bar{k}/k)-\text{action} \}^{\text{op}}$$
$$k' \longleftrightarrow \text{Hom}_{\bar{k}}(k', \bar{k}) \hookrightarrow \text{Gal}(\bar{k}/k)$$

Thm X (nice) topological space, $x \in X$.

$$\{ \text{coverings of } X \} \cong \{ \text{sets with } \pi_1(X, x)-\text{action} \}.$$
$$p: \tilde{X} \rightarrow X \longleftrightarrow p^{-1}(x) \hookrightarrow \pi_1(X, x)$$

Question: k perfect field. Is there a nice topological space

$$X(k)$$

such that

$$\{ \text{finite extensions of } k \} \simeq \{ \text{finite coverings of } X(k) \}^{\text{op}}$$

$$k \rightarrow k' \quad \mapsto \quad X(k') \rightarrow X(k)$$

2

Examples:

$$k = \mathbb{F}_p \quad \leadsto \quad X(k) = S^1$$

$$k = \mathbb{R} \quad \leadsto \quad X(k) = \mathbb{RP}^2 = S^2 / (\mathbb{Z}/2\mathbb{Z})$$

Then (Kucharczyk-S., 2016). Let α/\mathbb{Q} such that

$$S_n = e^{2\pi i/n} \in k, \text{ all } n \geq 1.$$

Then there is functional compact Hausdorff space $X(k)$
s.t.

$$\{ \text{finite extensions of } k \} = \{ \text{finite coverings of } X(k) \}^{\text{op}}$$
$$k' \mapsto X(k').$$

Moreover,

$$H^i(\text{Gal}(\bar{k}/k), \mathbb{Z}/n\mathbb{Z}) \cong H^i(X(k), \mathbb{Z})/n$$

Galois cohomology

Čech cohomology
(singular)

Facts

i) formally implies $\text{Gal}(\bar{k}/k)$ torsion free.

ii) $k = \mathbb{Q}^{\text{cycl}} = \mathbb{Q}(S_{n, n \geq 1})$

iii) $\pi_1(X(k)) \subsetneq \text{Gal}(\bar{k}/k)$ dense subgroup,

acts naturally on set

$$\log \bar{\mathbb{Q}} \subseteq \mathbb{G}$$

of logarithms of algebraic numbers.

Construction

Consider pairs (V, f) : V finite-dim'l k -vector space,
 $f: V \rightarrow V$ endomorphism.

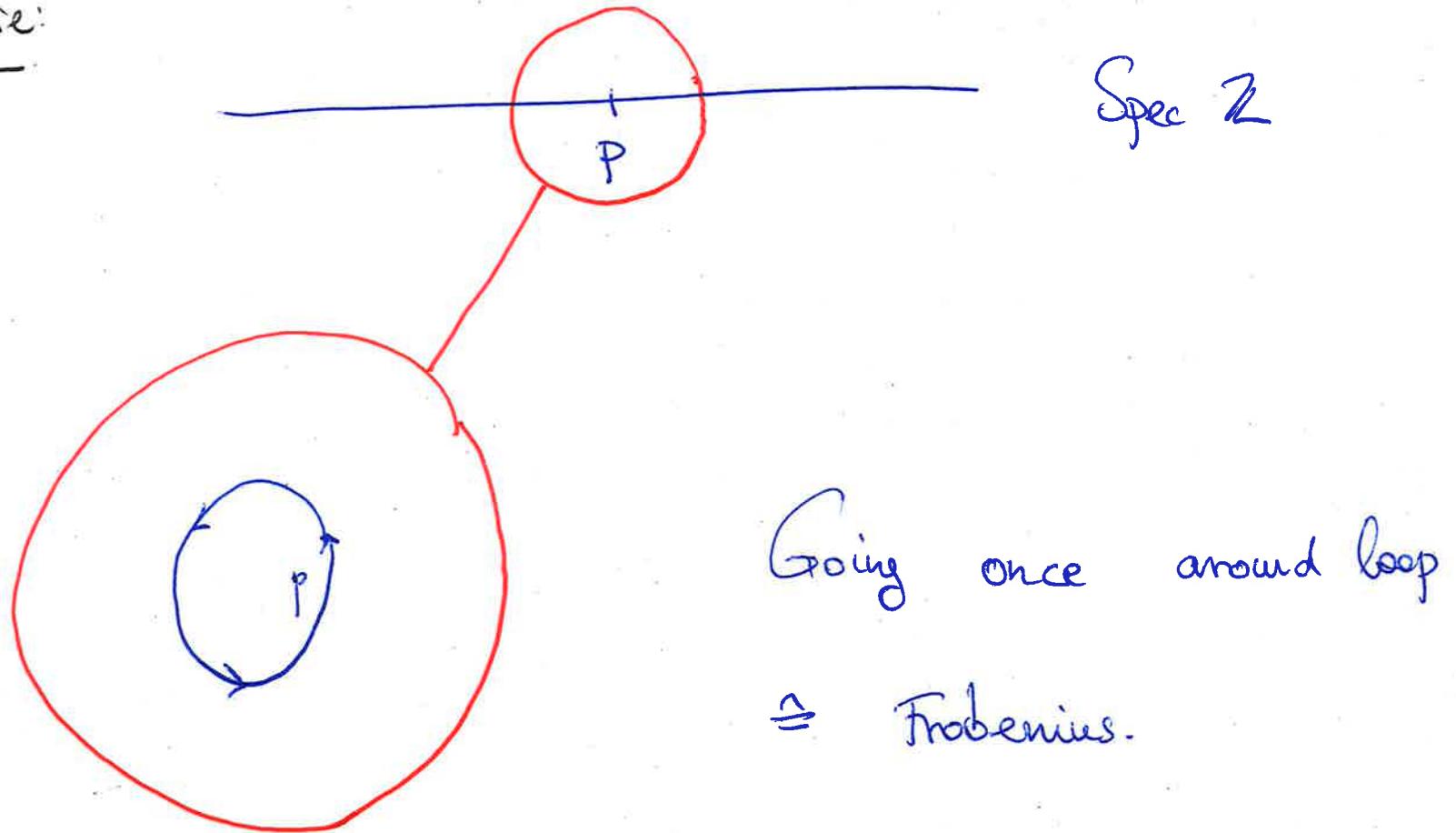
Can add $(V, f) + (W, g) := (V \oplus W, f \oplus g)$,

multiply $(V, f) \cdot (W, g) := (V \otimes W, f \otimes g)$.

Up to deformation retract,

$$X(k) = \left\{ \begin{array}{l} \text{maps } \{(V, f)\} \rightarrow C \text{ compatible with } +, \cdot, \\ \text{s.t. } (k, f_n) \mapsto f_n, \text{ all } n \geq 1 \end{array} \right\}.$$

Picture:



Neighborhood of P ?

~ fields K such that $p \neq 0$, but
 "p close to zero"

Example. $K = \mathbb{Q}_p = \left\{ \sum_{i=-\infty}^{\infty} a_i p^i \mid a_i \in \{0, 1, \dots, p-1\} \right\}$.

p -adic numbers

$$= \left\{ \dots a_3 a_2 a_1 a_0, a_{-1} a_{-2} \right\}.$$

"p-adic expansion infinite to the left"

p-adic absolute value:

$$|p^n|_p = \frac{1}{p^n} \xrightarrow{n \rightarrow \infty} 0$$

$$\left| \frac{1}{4} \right|_2 = 4$$

$$|2000|_2 = \frac{1}{16}$$

Examples.

i) $x^2 = -1$ No solutions in $\mathbb{R} \Rightarrow$ no solutions in \mathbb{Z}, \mathbb{Q}

ii) $x^2 = 2y^2$ No solutions in $\mathbb{Q}_2 \Rightarrow$ no solutions in \mathbb{Z}, \mathbb{Q} .

iii) $x^2 + y^2 = 3z^2$ No solutions in $\mathbb{Q}_3 \Rightarrow$ no solutions in \mathbb{Z}, \mathbb{Q} .

Then (Hasse-Minkowski).

$$\sum_{i=1}^n a_i x_i^2 = b \text{ has solution in } \mathbb{Q} \Leftrightarrow \text{solutions in all } \mathbb{Q}_p, \mathbb{R}.$$

Local-global-principle

Back to $\overline{\mathbb{Q}_p}$

$\overline{\mathbb{Q}_p}$ infinite extension of \mathbb{Q}_p

$\text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ large.

Thm (local Tate duality). $\text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ behaves like fundamental group of

compact Riemann surface = algebraic curve / \mathbb{C} .
smooth projective

Thm (Fargues-Fontaine) There is a "smooth projective" curve $X(\mathbb{Q}_p)$

with $\pi_1(X) \cong \text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$.

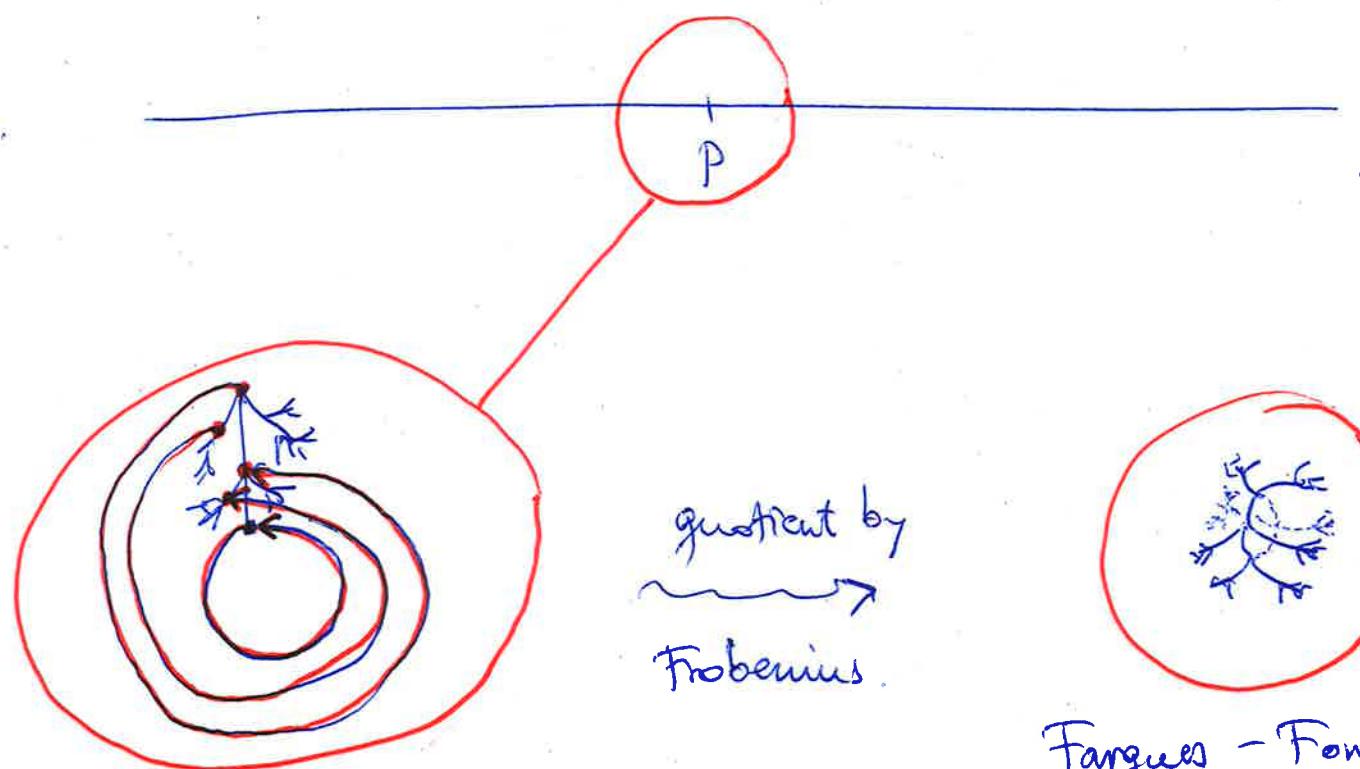
It parametrizes fields in which p is close to zero.

Theorem Space of fields K s.t. "p close to zero"

Can be given structure of a curve (in sense of nonarch.
geometry) + Frobenius acts on it.

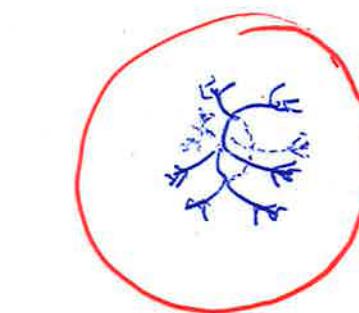
Fargues-Fontaine curve = quotient by Frobenius.

Spec Z.



quotient by
Frobenius.

nonarchimedean curves
look like infinitely
branching trees.



Fargues - Fontaine curve.

Thank You!