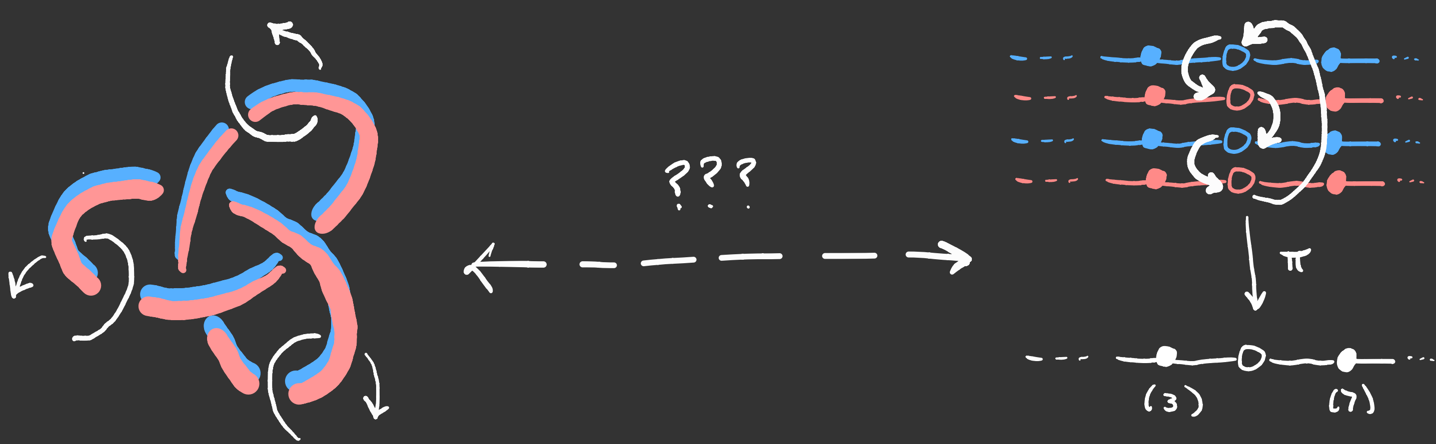
On the analogy between knots and primes

Gary Dunkerley

The University of Georgia

GSS October 26, 2021



slides available at:
garydunkerley.github.io

Quadratic Reciprocity

Let $p, q \in \mathbb{Z}$ be prime.

The <u>Legendre symbol</u> is defined as follows:

$$\left(\frac{p}{q}\right) := \begin{cases} 1 & \exists x : p \equiv x^2 \pmod{q} \\ -1 & \text{otherwise} \end{cases}$$

<u>Theorem</u> (Gauss)

If p, q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

<u>Folklore</u>

This has an interpretation in low-dimensional topology.

Knots

A knot is a family of embeddings

$$K : S^{n-2} \hookrightarrow S^n$$

considered up to "ambient isotopy."

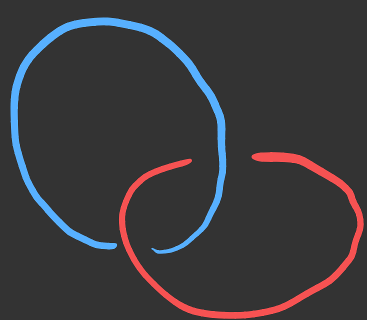
Fixing $n = 3$, we can represent (tame) knots via plane diagrams:

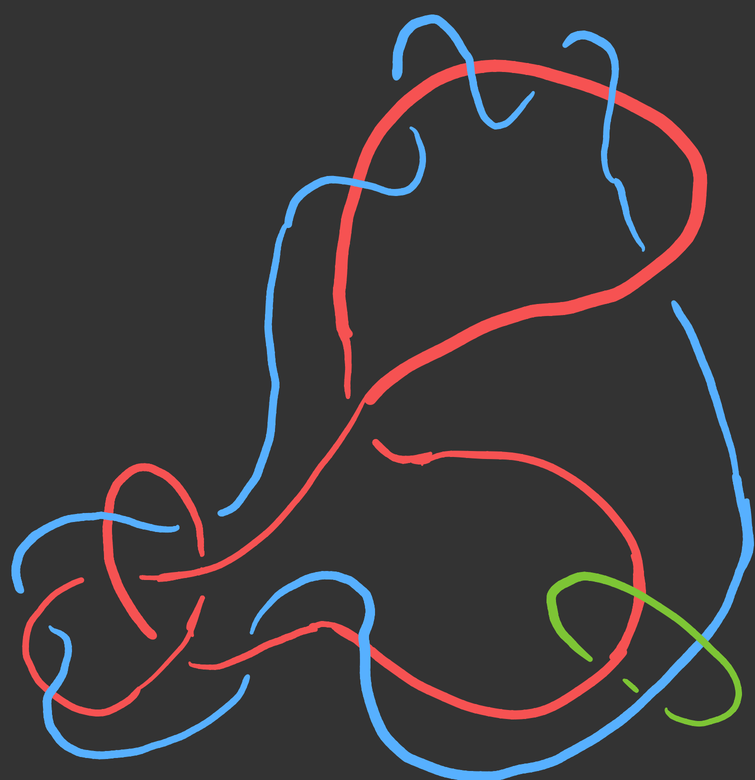
"Solomon's Seal Knot"
(5_1)

"Figure Eight Knot"
(4_1)

Links

A link is a disjoint family of knots



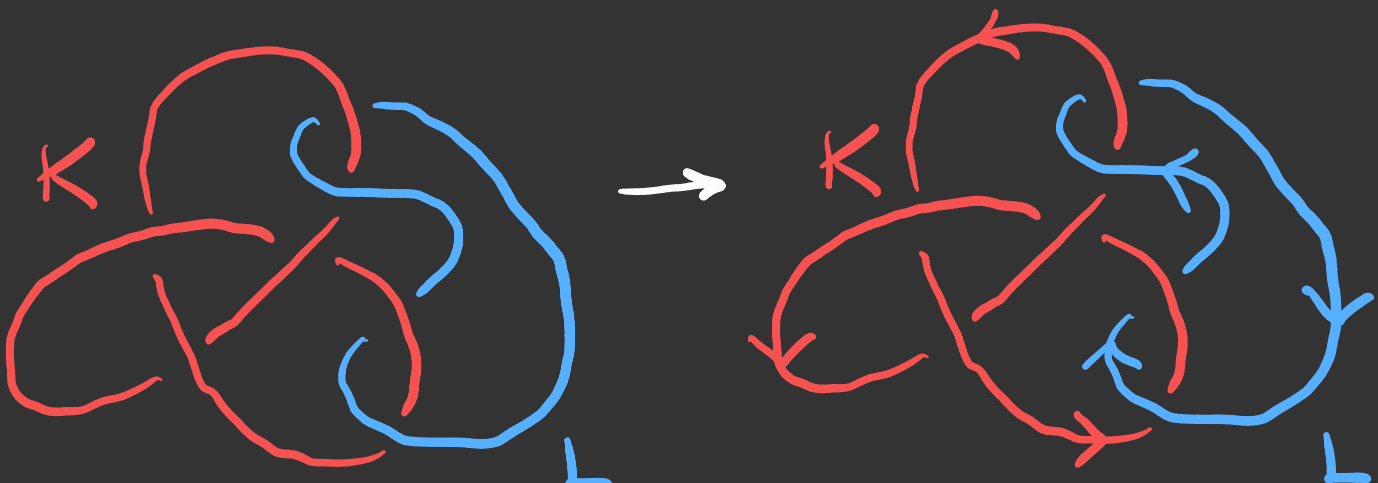


Linking Number

Given two components K and L in a link, how "entangled" are they?

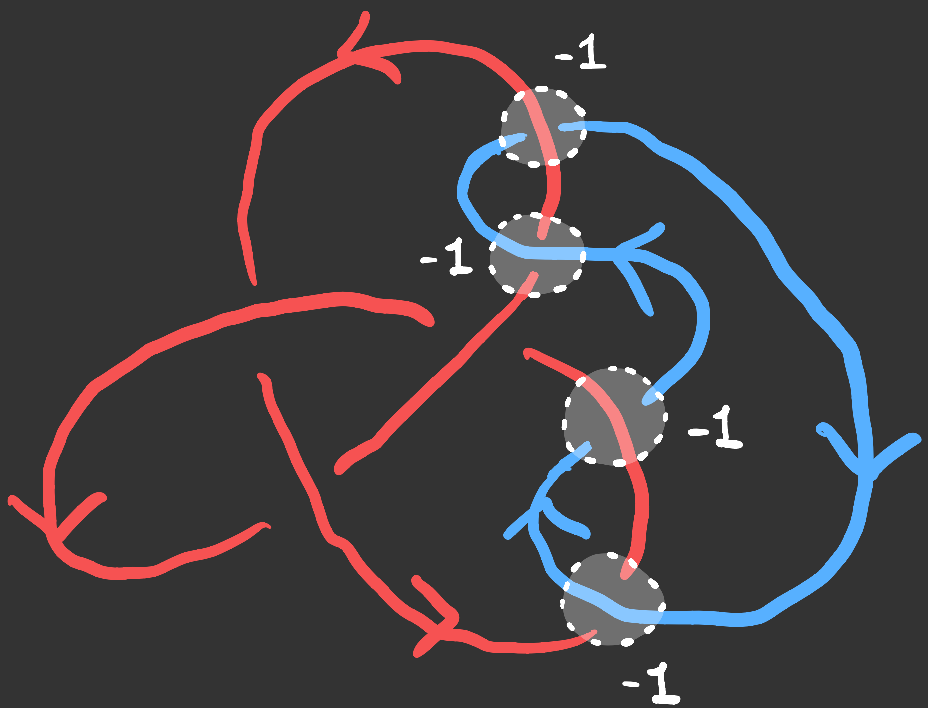
We measure this with the linking number, computed as follows:

1. Orient your link diagram



2. Assign weights to crossings:

3. Sum the crossing weights for each intracomponent crossing and divide this by 2.



$$\ell(K, L) = \frac{-1 + -1 + -1 + -1}{2} = -2$$

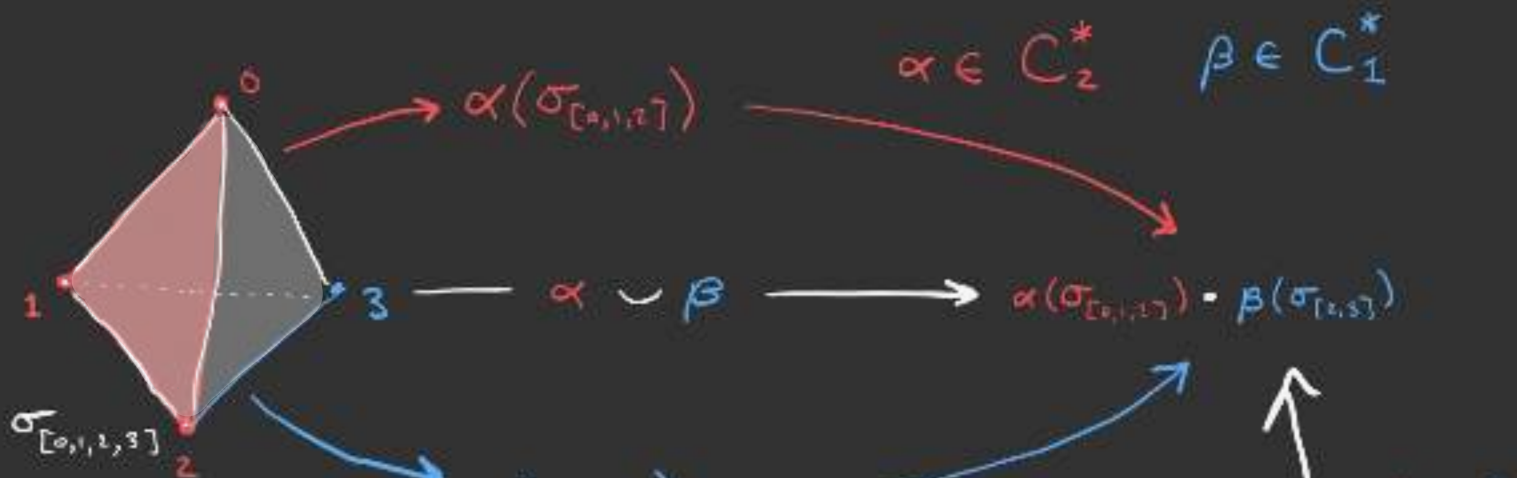
<u>Exercise</u> Linking number is well-defined up to sign and $\ell(K, L) = \ell(L, K)$.

This may be easier to see from a cohomological perspective.

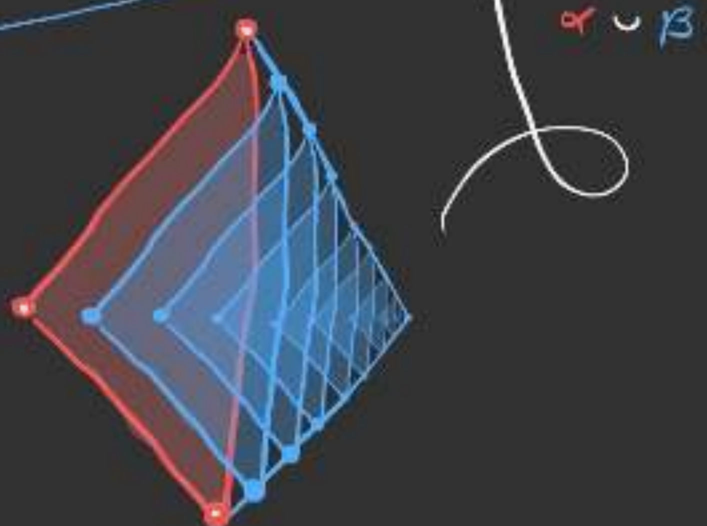
Cup Product

$$(\alpha^p \smile \beta^q)(\sigma_{[0,1,\dots,p+q]}) = \alpha^p(\sigma_{[0,1,\dots,p]}) \cdot \beta^q(\sigma_{[p,p+1,\dots,p+q]})$$

The cup product turns a product of cells into a product of maps.

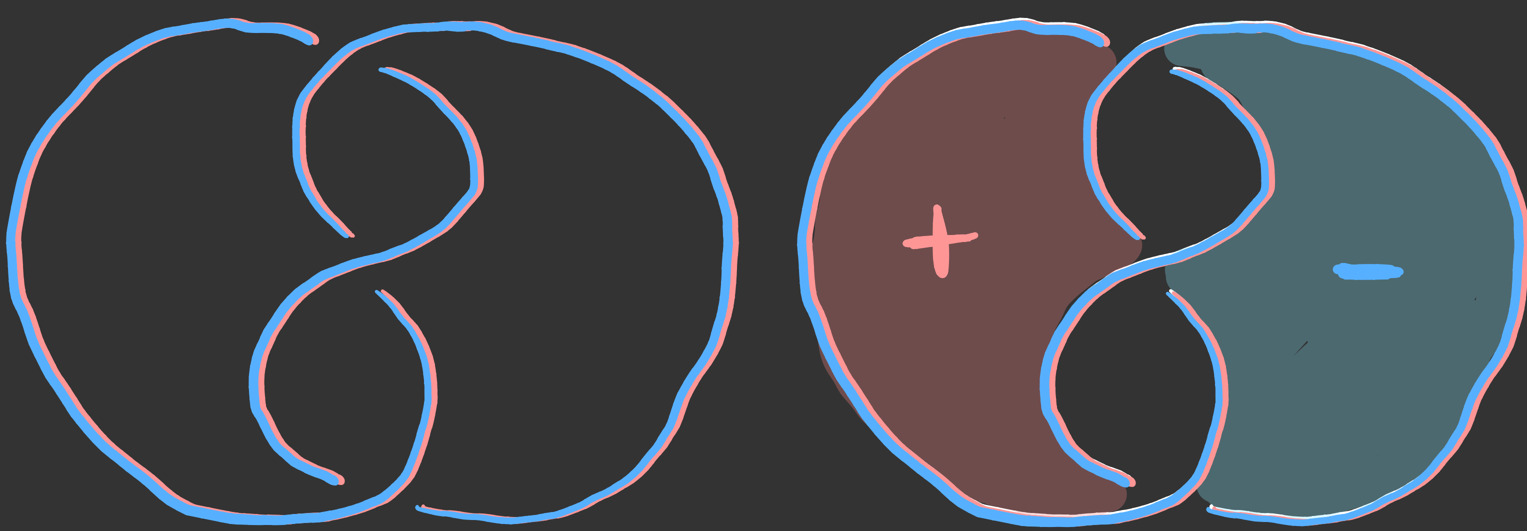


"A '$\sigma_{[2,3]}$'s worth' of $\sigma_{[0,1,2]}$ is sent to a '$\beta(\sigma_{[2,3]})$'s worth' of $\alpha(\sigma_{[0,1,2]})$."



Seifert Surfaces

Given a knot $K \subset S^3$, it bounds an oriented, bicollared surface in S^3 called a Seifert surface.



K $\qquad\qquad$ Σ_K

One can always be found using Seifert's algorithm on a knot diagram.

Linking Number

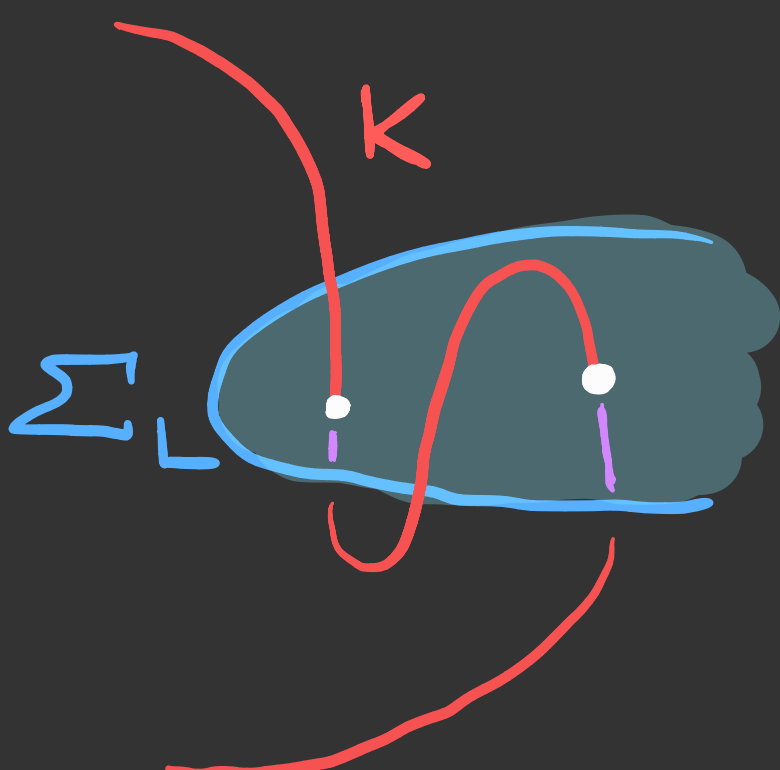
Given $K, L \hookrightarrow S^3$, algebraic topology gives us

$$[K] \in H_1(S^3 \setminus L)$$

$$[\Sigma_L] \in H_2(S^3 \setminus L)$$

and their Poincaré duals satisfy:

$$PD[K] \smile PD[\Sigma_L] = PD[K \cap \Sigma_L]$$



Algebraic intersection number <u>is</u> the linking number

Who cares?

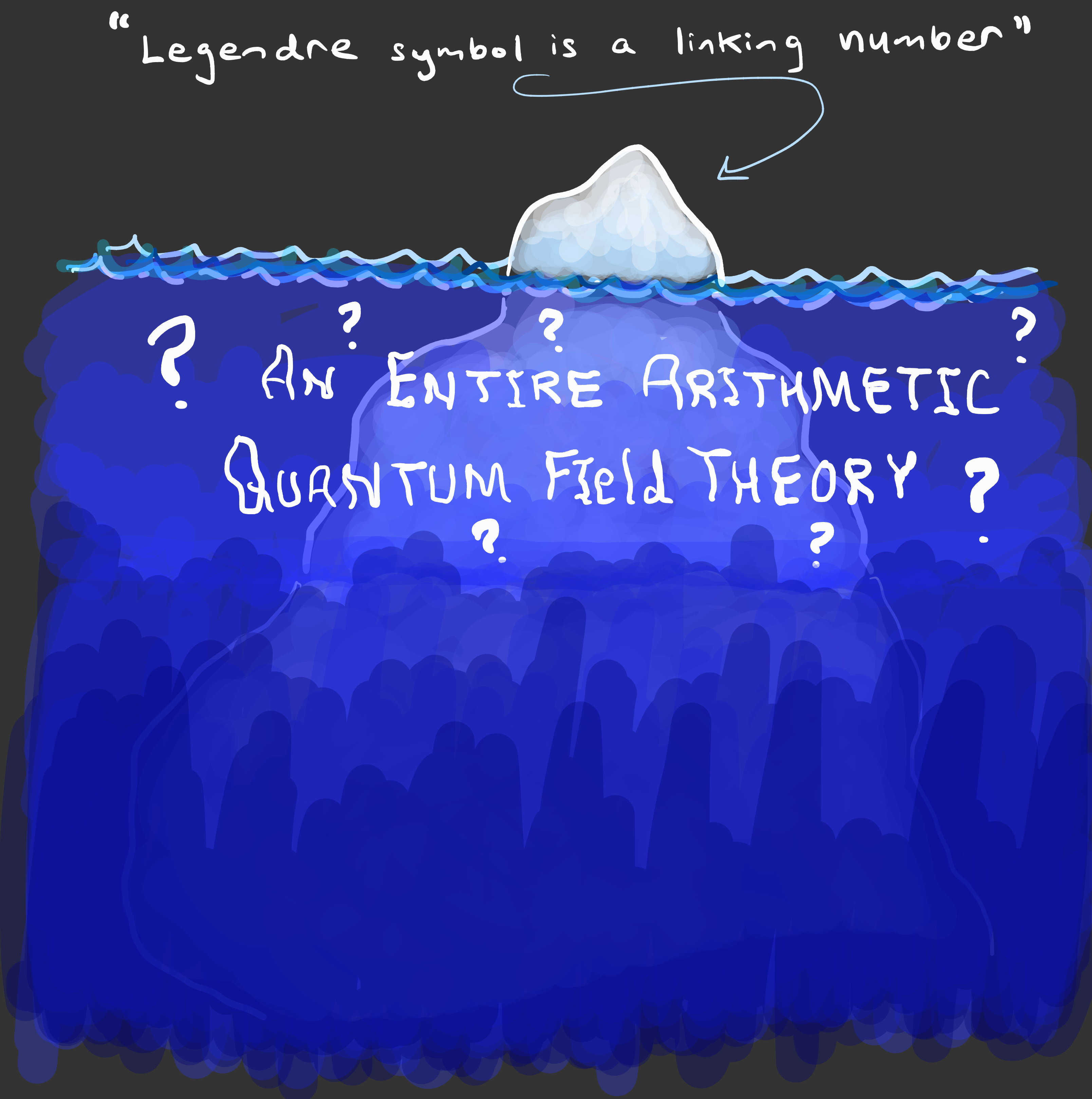
Folklore (Morishita, Mazur, etc.)

The Legendre symbol "is" a linking number of "arithmetic knots."

Quadratic reciprocity "is" the symmetry of the linking number.

Dream Gauss' original definition of the linking number was physically motivated and makes an appearance in Chern-Simmons theory.

Low-dimensional topology has benefitted greatly from its relationship with mathematical physics (Reshetikhin-Turaev, HOMFLY, Seiberg-Witten, etc.)


"Legendre symbol is a linking number"
An Entire Arithmetic
Quantum Field Theory
? ? ? ? ? ? ?

What are arithmetic knots?

- $\mathrm{Spec}(\mathbb{Z}) :=$ all prime ideals in $\mathbb{Z}$

- We can turn $\mathrm{Spec}(\mathbb{Z})$ into an affine scheme by giving it a sheaf of rings:

$$\mathcal{O}_{\mathrm{Spec}(\mathbb{Z})}(U_a) := \left\{ \frac{r}{a^n} \;\middle|\; a \in \mathbb{Z} \setminus \{0\},\ n \in \mathbb{Z}^{\geq 0} \right\}$$

- Problem: Zariski topology doesn't yield a satisfactory $\pi_1(\mathrm{Spec}(\mathbb{Z}))$, it's not immediately clear what "circles" should be.

- ...but given a theory of coverings we could define

$$\pi_1(X) \cong \mathrm{Aut}_X(\tilde{X})$$

with $\tilde{X}$ being some universal covering object.

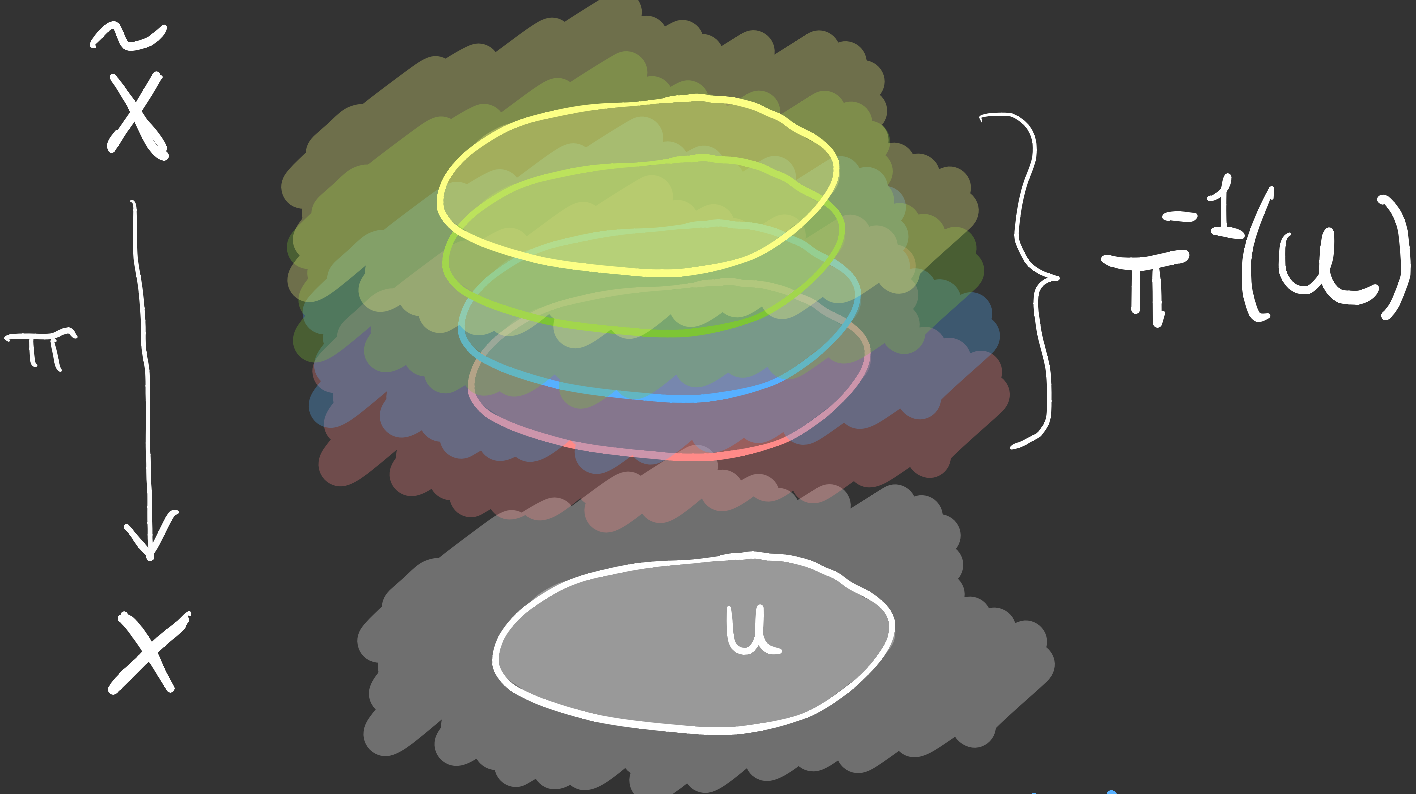
Covering Spaces

Given a space X, a covering space is a space $\tilde{X}$ with a map $\pi : \tilde{X} \longrightarrow X$ that satisfies

- $|\pi^{-1}(x)| = |\pi^{-1}(y)| \quad \forall x, y \in X$
- $\forall x \in X : \exists\, \mathcal{U}_x$ s.t. $\pi^{-1}(\mathcal{U}_x) \cong \bigsqcup_i \mathcal{U}_x$

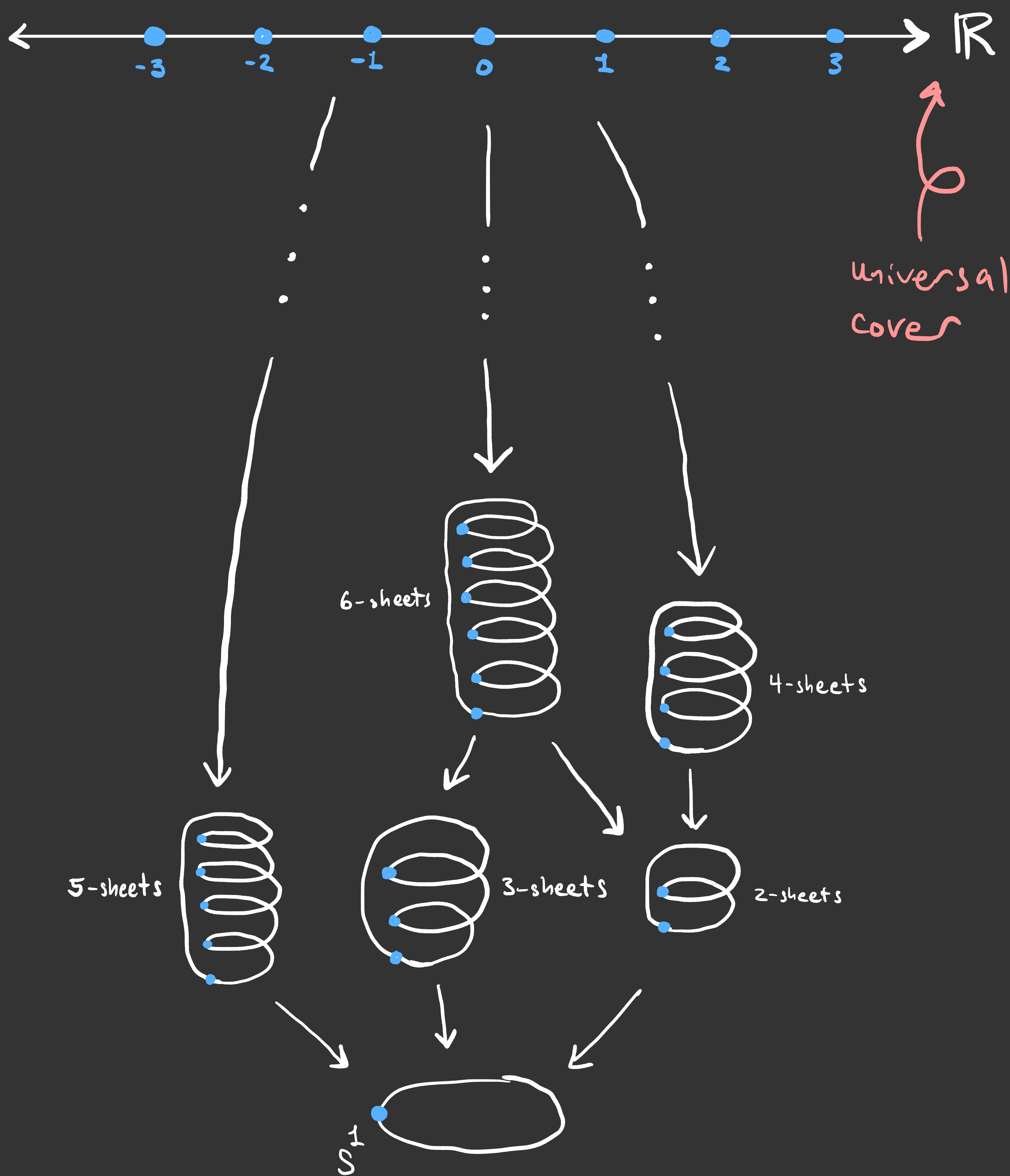
"sheets" of the cover

If your space X is *especially nice* then it has a simply-connected covering space called the universal cover of X.

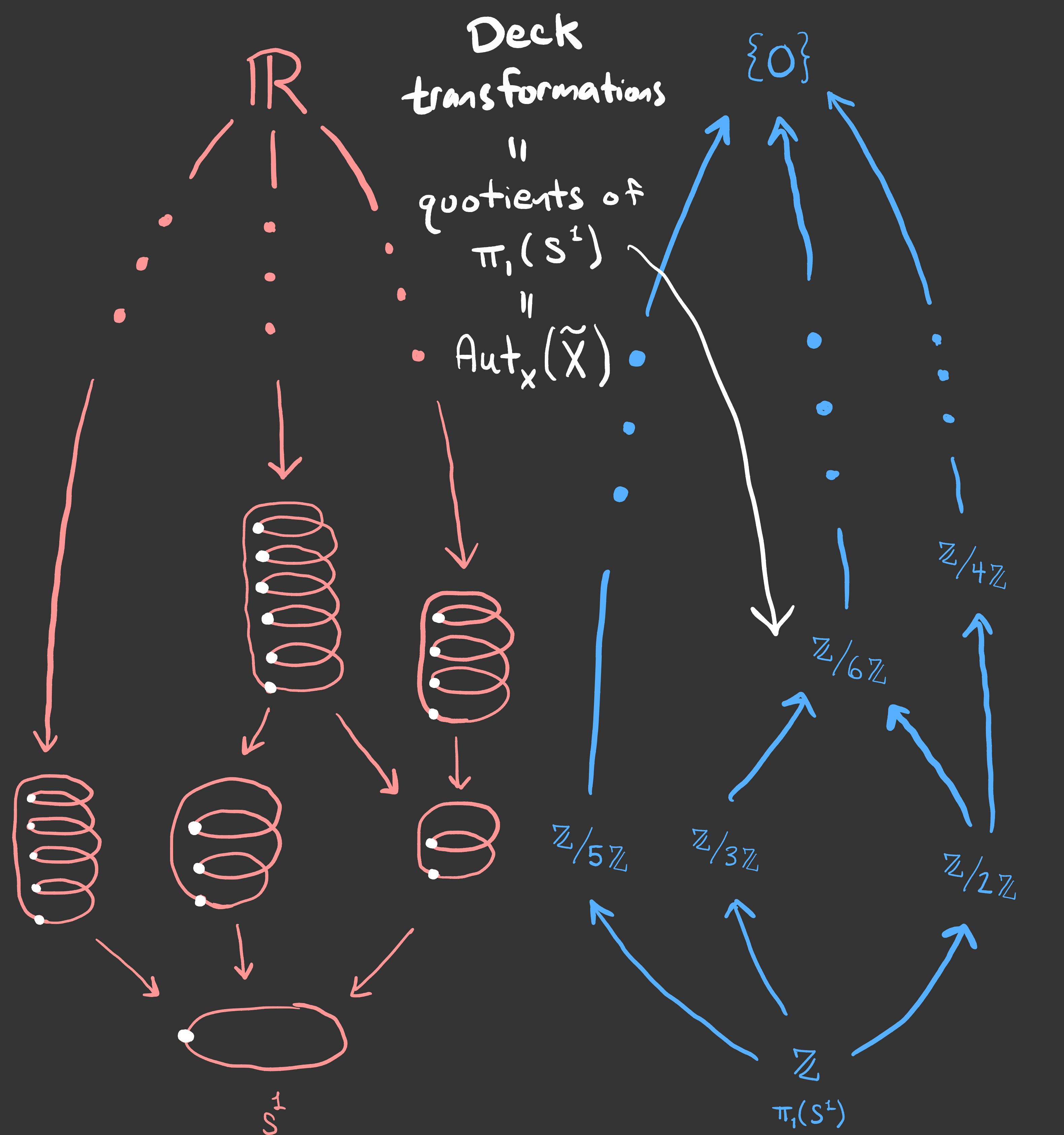


* connected
locally path-connected
semilocally simply connected

EXAMPLE: S^1-Covers



Galois Correspondance



Étale Coverings

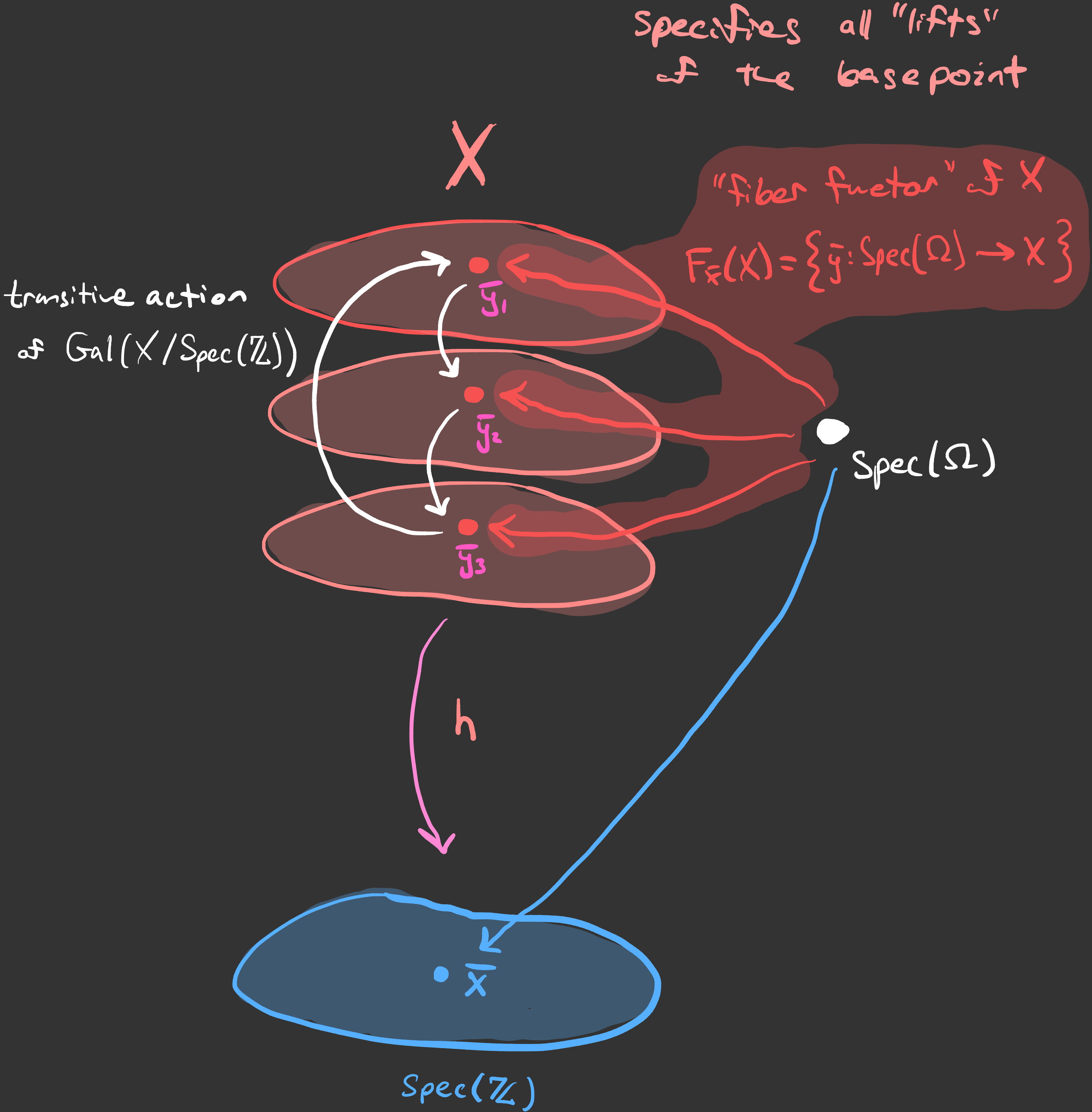
The correct objects to look at are finite Galois coverings $\mathrm{Spec}(\mathbb{Z})$; schemes that are spectra of finite connected Galois algebras over $\mathbb{Z}$.

Let $(p) \in \mathrm{Spec}(\mathbb{Z})$. Fixing an algebraically closed field Ω of characteristic p (e.g. an algebraically closed extension of $\mathbb{F}_p$) we fix a map called the geometric base point $\bar{x} : \mathrm{Spec}(\Omega) \longrightarrow \mathrm{Spec}(\mathbb{Z})$

$h : Y \longrightarrow \mathrm{Spec}(\mathbb{Z})$ a finite Galois covering implies action of

$$\mathrm{Gal}(X/\mathrm{Spec}(\mathbb{Z})) := \mathrm{Aut}_{\mathrm{Spec}(\mathbb{Z})}(X)$$

on "fiber functor" is transitive.


specifies all "lifts" of the basepoint
X
"fiber functor" of X
$F_{\bar{x}}(X) = \{\bar{y} : \mathrm{Spec}(\Omega) \to X\}$
transitive action of $\mathrm{Gal}(X/\mathrm{Spec}(\mathbb{Z}))$
$\bar{y}_1$
$\bar{y}_2$
$\bar{y}_3$
$\mathrm{Spec}(\Omega)$
h
$\bar{x}$
$\mathrm{Spec}(\mathbb{Z})$

A Universal Cover!

Theorem (Morishita THM 2.23)

There is a projective system of pointed, finite Galois covers

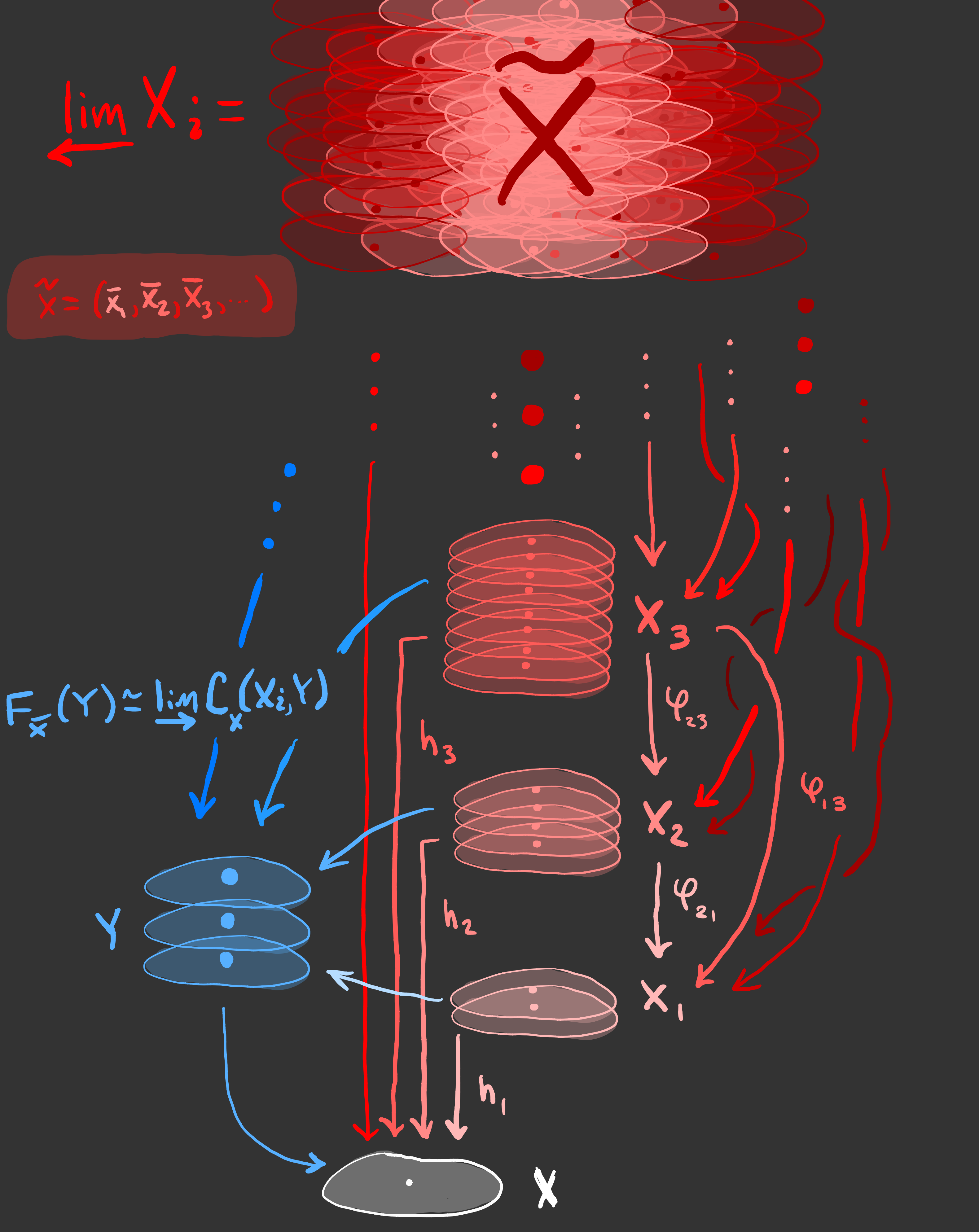
$$((h_i : X_i \to X, \bar{x}_i, \varphi_{ij})$$

such that for any finite étale cover $h: Y \to X$ we get

$$F_{\bar{x}}(Y) \overset{\text{bijection}}{\simeq} \varinjlim C_x(X_i, Y) = \frac{\bigsqcup C_x(X_i, Y)}{\substack{\phi_1 \sim \phi_2 \Leftrightarrow \exists\, \varphi_{ik}, \varphi_{ij} \\ \text{s.t. } \varphi_{ik}(\phi_1) = \varphi_{ij}(\phi_2)}}$$

The system from the theorem yields at long last, the étale fundamental group:

$$\pi_1^{\text{ét}}(X, \bar{x}) = \mathrm{Gal}(\tilde{X}/X) := \varprojlim \mathrm{Gal}(X_i/X)$$



$\varprojlim X_i = \tilde{X}$
$\tilde{x} = (\bar{x}_1, \bar{x}_2, \bar{x}_3, \dots)$
$F_{\tilde{x}}(Y) \simeq \varinjlim C_X(X_i, Y)$
X_3
φ_{23}
X_2
φ_{13}
φ_{21}
X_1
h_3
h_2
h_1
Y
X

Finally, fixing $q = p^n$ for some prime p, we leverage finite field properties to conclude:

$$\overline{\mathbb{F}}_q = \varinjlim_n \mathbb{F}_{q^n}$$

Then if $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q / \mathbb{F}_q)$ is the Frobenius automorphism:

$$\sigma : x \longmapsto x^q$$

the correspondance $\sigma|_{\mathbb{F}_{q^n}} \longmapsto 1 \pmod n$ tells us $\mathrm{Gal}(\mathbb{F}_{q^n} / \mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$ so

$$\pi_1^{\text{ét}}(\mathrm{Spec}(\mathbb{F}_q), \bar{x}) = \varprojlim_n \mathrm{Gal}(\mathbb{F}_{q^n} / \mathbb{F}_q)$$

$$\cong \varprojlim_n \mathbb{Z}/n\mathbb{Z} := \hat{\mathbb{Z}}$$

the profinite integers

$\mathrm{Spec}(\mathbb{F}_p)$ are arithmetic knots!!

- Higher étale homotopy groups also exist and $\pi_i^{\text{ét}}(\mathrm{Spec}(\mathbb{F}_q)) \cong 0$ for all $i \geq 2$, so our $\mathrm{Spec}(\mathbb{F}_q)$ are "profinite circles," e.g. $K(\hat{\mathbb{Z}}, 1)$!

Eilenberg-MacLane Space

- $\pi_1^{\text{ét}}(\mathrm{Spec}(\mathbb{Z})) \cong 0$

- Moreover, a technical result known as Artin-Verdier duality tells us that the étale cohomological dimension of $\mathrm{Spec}(\mathbb{Z})$ is three*.

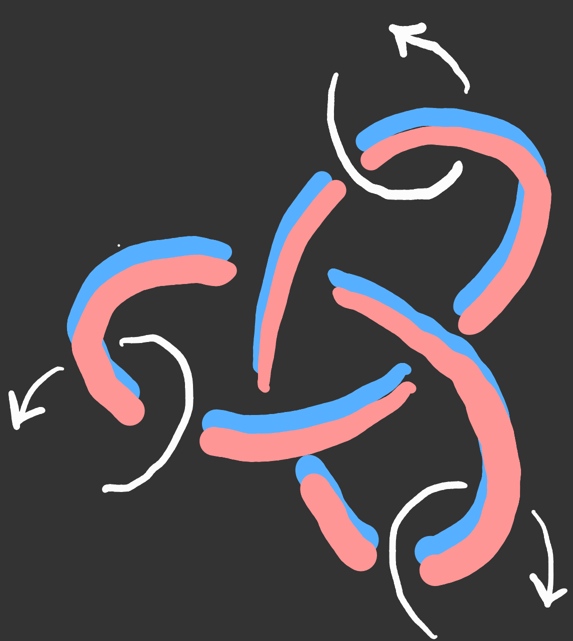
- So $\mathrm{Spec}(\mathbb{Z})$ is "like" a simply connected orientable, 3-manifold (true for any $\mathcal{O}_K$)!

* modulo 2-torsion

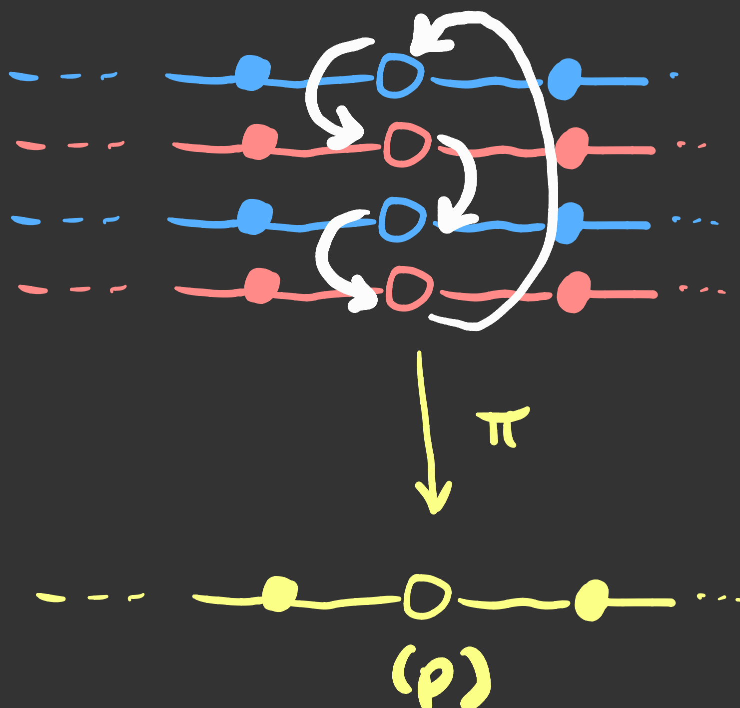
Knot Groups

- we associate to a knot K its knot group, $\pi_1(S^3 \setminus K)$.
- meanwhile, the prime group for a prime p is

$$G_p := \pi_1^{\text{ét}}(\operatorname{Spec}(\mathbb{Z}) \setminus (p))$$



$\pi_1(S^3 \setminus K)$



$\pi_1^{\text{ét}}(\operatorname{Spec}(\mathbb{Z}) \setminus (p))$

ARITHMETIC LINKING

Let p, q odd primes and

$p, q \equiv 1 \pmod 4$

- Let α a primitive root mod q (e.g. everything coprime w/ α is a power of α)
- Define a group homomorphism

$$\Phi : \underbrace{\mathbb{F}_q^\times \times (1 + q\mathbb{Z}_q)}_{G_q} \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

$$\Phi(\alpha) = 1, \quad \Phi(1 + q\mathbb{Z}_q) = 0$$

- We get a quadratic extension

$$K \cong \mathbb{Q}(\sqrt{q^*}), \quad q^* := (-1)^{\frac{q-1}{2}} q$$

- Get an étale double cover of $\mathrm{Spec}(\mathbb{Z}) \setminus (q)$:

$$X_2 := \mathrm{Spec}\left(\mathbb{Z}\left[\frac{1+\sqrt{q^*}}{2}, \frac{1}{q}\right]\right)$$

and a homomorphism

$$\rho : G_q \longrightarrow \mathrm{Gal}(X_2, \mathrm{Spec}(\mathbb{Z}) \setminus (q))$$

- Define the mod 2 linking number $lk_2(q, p)$ to be the image of the Frobenius automorphism $\sigma_p : x \longmapsto x^p$ under ρ.

Geometric Quadratic Reciprocity

Theorem

For p, q odd primes and $p, q \equiv 1 \pmod 4$ we have

$$(-1)^{\operatorname{lk}_2(q,p)} = \left(\frac{q^*}{p}\right)$$

Proof If $\operatorname{lk}_2(q,p) = 0$, then

$\rho(\sigma_p) = \mathrm{id}_{X_2}$, so $\sigma_p(\sqrt{q^*}) = \sqrt{q^*}$

$\Rightarrow \sqrt{q^*} \in \mathbb{F}_p^\times \Rightarrow q^* \in (\mathbb{F}_p^\times)^2$

$\Rightarrow q^*$ a quadratic residue mod p

$\Rightarrow \left(\frac{q^*}{p}\right) = 1$ $\square$

A bit more algebra tells us that in the cover

$$h: X_2 \longrightarrow \mathrm{Spec}(\mathbb{Z}) \setminus (q)$$

we have

$$h_2^{-1}((p)) = \begin{cases} \{\#_1, \#_2\} & lk_2(p,q) = 0 \\ \# & lk_2(p,q) = 1 \end{cases}$$

e.g. q^* a quadratic residue mod p

e.g. q^* a quadratic non-residue mod p

Further Down the Rabbit Hole

link $\longleftrightarrow$ $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n\}$

link group $\longleftrightarrow$ $\pi_1^{\text{ét}}(\mathrm{Spec}(\mathcal{O}_K) \setminus S)$

Borromean rings $\longleftrightarrow$ Borromean primes

Hurewicz isomorphism $\longleftrightarrow$ unramified class field theory

factorization properties of random integers $\longleftrightarrow$ properties of random braids

Reidemeister torsion $\longleftrightarrow$ Riemann zeta function

REFERENCES

- Morishita, *Knots and Primes*
- Mazur, "Knots, Primes, and Po"
- Rolfsen, *Knots and Links*
- Hatcher, *Algebraic Topology*
- Shmakov, "Galois Representations in Étale Fundamental Groups and the Profinite Grothendieck-Teichmüller Group"

Special thanks to:

- Arvind & Zack
- Raemeon & Sasha
- my collaborator

Étale Coverings

- A ring homomorphism $\phi : R \to S$ is **finite étale** if

  (i) S a finitely generated, flat R-module

  (ii) For any $\mathfrak{p} \in \mathrm{Spec}(R)$,

$$S \otimes_R \underbrace{R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}}_{\text{residue field of the localization of } R \text{ at } \mathfrak{p}.} \simeq \underbrace{K_1 \times \cdots \times K_r}_{\text{finite, separable extensions of } R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}} \times \underbrace{\psi}_{\text{some isomorphism of } R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}\text{-algebras}}$$

- specifying R an "integrally closed domain" (e.g. contains all roots of monics in $R[x]$) then an R-algebra S is a **connected finite étale algebra** over R if

  (i) there is finite separable extension K of $\mathrm{Frac}(R)$ s.t. S is the integral closure of R in K.

  (ii) $R \hookrightarrow S$ is finite étale

- a finite étale algebra over R is a pro connected finite étale algebras.

- a finite Galois algebra S over R is a connected finite étale algebra if for any $\mathfrak{p} \in \mathrm{Spec}(R)$ and any algebraically closed field $\bar{K}$ containing $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$

$$\mathrm{Aut}(S/R) \circlearrowright_{\text{simply transitive}} \mathrm{Hom}_{R\text{-alg}}(S, \bar{K})$$

Exercise

S a finite Galois algebra over R iff $K/\mathrm{Frac}(R)$ is a finite Galois extension

We can then define

$$\mathrm{Gal}(S/R) := \mathrm{Gal}(K/\mathrm{Frac}(R))$$

A morphism of schemes

$$f: Y \longrightarrow \mathrm{Spec}(\mathbb{Z})$$

is a finite étale covering (FEC) if there is a finite étale algebra

$$B \cong B_1 \times \cdots \times B_n \quad \text{over } \mathbb{Z}$$

such that

$$\mathrm{Spec}(B) = \coprod_{i=1}^{n} \mathrm{Spec}(B_i)$$

and the associated ring homomorphism is the inclusion

$$\mathbb{Z} \hookrightarrow B$$

h' a subcovering of a FEC h if $\exists\, \varphi$ such that the diagram commutes.

$$\begin{tikzcd} & X \arrow[dl, "\varphi"'] \arrow[dd, "h"] \\ X' \arrow[dr, "h'"'] & \\ & Y \end{tikzcd}$$

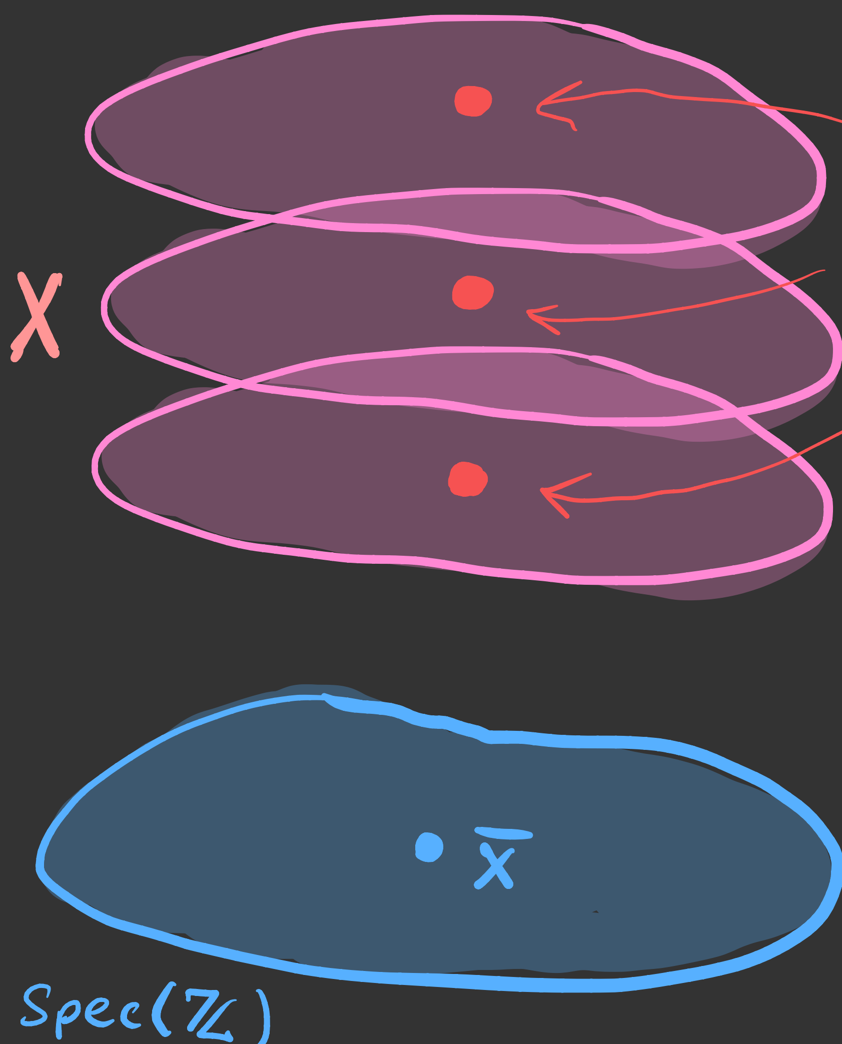
$\varphi \in C_Y(X, X')$

e.g. a morphism of finite étale coverings

The set of all such φ that are isomorphism yield the group of covering transformations $\mathrm{Aut}_Y(X)$.

Let $\mathfrak{p} \in \operatorname{Spec}(\mathbb{Z})$ and $\bar{K}$ an algebraically closed field extension of $\mathbb{Z}_{\mathfrak{p}}/\mathfrak{p}\mathbb{Z}_{\mathfrak{p}}$, then we get a morphism $\bar{x} : \operatorname{Spec}(\bar{K}) \longrightarrow \operatorname{Spec}(\mathbb{Z})$ called the geometric basepoint.

fix a algebreically closed field of char p.



"fiber functor of $\bar{x}$"

$$F_{\bar{x}}(X) := \operatorname{Hom}_{\operatorname{Spec}(\mathbb{Z})}(\operatorname{Spec}(\bar{K}), X)$$

This is finite Galois if $X = \operatorname{Spec}(B)$ for B a finite Galois algebra over $\mathbb{Z}$.

e.g.

$\operatorname{Aut}_{\operatorname{Spec}(\mathbb{Z})}(X)$ acts transitively on $F_{\bar{x}}(X)$

(CO)HOMOLOGY

Given a chain complex:

$$\mathcal{C} := \cdots \longrightarrow C_{i+1} \xrightarrow{\partial_{i+1}} C_i \xrightarrow{\partial_i} C_{i-1} \longrightarrow \cdots$$

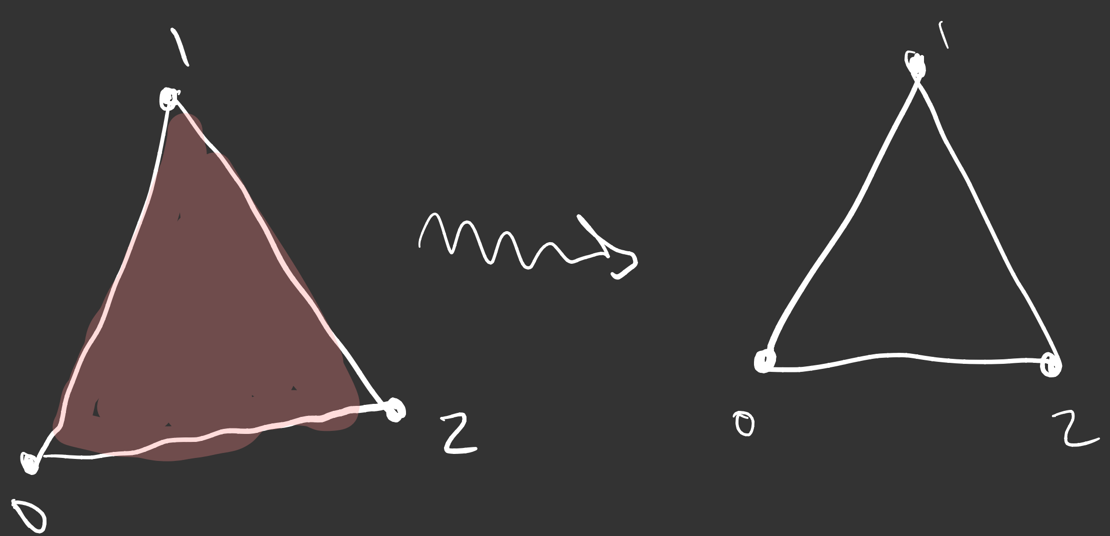
and a commutative ring R, we can construct a **cochain complex**:

$$\mathcal{C}^* := \cdots \longleftarrow C^*_{i+1} \xleftarrow{d_i} C^*_i \xleftarrow{d_{i-1}} C^*_{i-1} \longleftarrow \cdots$$

where

$C^*_k = \mathrm{Hom}(C_k, A)$

$C^*_k = \mathrm{Hom}(C_k, R)$ and $d_k(\varphi) = \varphi \circ \partial_{k+1}$



Given a chain complex $\mathcal{C}$ associated to a CW-complex X, its k^{th}-homology group is:

$$H_k(X) = \frac{\ker(\partial_k)}{\operatorname{Im}(\partial_{k+1})}$$

We call the homology groups of the cochain complex $\mathcal{C}^*$ the cohomology with coefficients in R, notationally:

$$H^k(X;R) := \frac{\ker(d_k)}{\operatorname{Im}(d_{k-1})}$$

Intuition

- Homology introduces a comparison between simple geometric objects that attach together to form more complicated spaces
- Cohomology tells us how these simple geometric objects pass through our space on their way to a group or ring.