2023/03/03 Talk Plan

Key
- · To write
- To say
- · Supplementary Notes

Intro: · In the 60s Barry Mazur pointed out knots in 3-fold are analogous to primes in Number Field.
- · Goal of today is to show snippets of this analogy.
- · For now this analogy is simply motivational, can't prove NT results from working w/ primes.

Agenda
1. Correspondence between Knots & Primes
2. Decomposition of Knots & Primes
3. Linking numbers and the Power Residue Symbol
4. Higher linking numbers of Knots & Primes.

There is an algebraic analogue of the fundamental group called the étale fundamental group: étale maps morally corresponds to a covering map of topological spaces, so the étale fundamental group is defined as a limit of the automorphism groups of all finite étale maps.

§1: Knots and primes

M: Compact 3-manifold, say $M = S^3$ ⟷ $\mathcal{O}_K$ number ring of a number field K, e.g $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$

$\pi_1(S^3) = 1$ — $\pi_1(\operatorname{Spec}\mathbb{Z}) = \operatorname{Gal}(\mathbb{Q}^{ur}/\mathbb{Q}) = 1$

Knot $K: S^1 \hookrightarrow M$ ⟷ Prime ideal $p \trianglelefteq \mathcal{O}_K$, $\operatorname{Spec}\mathbb{F}_p \hookrightarrow \operatorname{Spec}\mathcal{O}_K$

$\pi_1(K) \cong \pi_1(S^1) = \mathbb{Z}$ — $\pi_1(\operatorname{Spec}\mathbb{F}_p) = \operatorname{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \hat{\mathbb{Z}}$

Knot Group $\pi_1(M\setminus K)$ ⟷ Galois group unramified outside p $\pi_1((\operatorname{Spec}\mathcal{O}_K)\setminus p)$

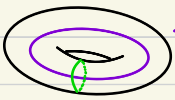
$M\setminus K$ not compact, instead we can remove a tubular neighbourhood of M.

V_K: tubular ngbd of K ⟷ $\mathcal{O}_{K_p}$: Local Ring at p

$\pi_1(V_K) \cong \pi_1(S^1) = \mathbb{Z}$ — $\pi_1(\operatorname{Spec}\mathcal{O}_{K_p}) = \operatorname{Gal}(K_p^{ur}/K_p) \cong \operatorname{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \hat{\mathbb{Z}}$

∂V_K boundary of V_K ⟷ K_p: Local field at p.

$\pi_1(V_K) \cong \pi_1(S^1 \times S^1) = \mathbb{Z}^2 = \langle \alpha, \beta \mid [\alpha,\beta] \rangle$



$\pi_1(\operatorname{Spec} K_p)$ hard to calculate, instead have tame quotient
$\pi_1^t(\operatorname{Spec} K_p) = \langle \sigma, \tau \mid \tau^{p-1}[\tau,\sigma] = 1 \rangle$
σ frobenius, τ monodromy. Will elaborate a little more later.

§2 Decomposition of Knots and Primes

§2.1 Knots

Defn (Ramified Covering Space)

Let $L = L_1 \amalg L_2 \amalg \cdots \amalg L_s \hookrightarrow M$ be a link, a cts map $f: N \to M$ is a ramified covering over L if:
- · $f|_{N\setminus f^{-1}(L)}: N\setminus f^{-1}(L) \longrightarrow M\setminus L$ is a covering map
- · For each $y \in f^{-1}(L)$, $\exists$ ngbds $D^2\times I \cong U \ni y$, $D^2 \times I \cong V \ni f(y)$, s.t $f_*: U \to V$ is $(z \mapsto z^e)\times \mathrm{id}$

  (identifying $D^2 \cong \{|z| \le 1\} \subseteq \mathbb{C}$

This is like ramification of Riemann Surfaces, have ramification over a co-dimension 2 submanifold so intuitively the map is "wrapping" around the submanifold

e is fixed for each component link L_i, we call this the __ramification degree__ of L_i

Let $X := M\setminus L$, $Y := N\setminus f^{-1}(L)$, Let $G := \operatorname{Gal}(M/S^3) = \operatorname{Gal}(Y/X)$ i.e this is the Quotient of $\pi_1(S^3\setminus L)$ that corresponds to the covering space $N\setminus f^{-1}(L)$

Let K be a knot in M that is either a component of L or disjoint to L. V_K tubular ngbd

$f^{-1}(K)$ will be a link in N, say $f^{-1}(K) = K_1 \cup \cdots \cup K_r$, V_{K_i} the component of $f^{-1}(V_K)$ containing K_i

Pick a basepoint $x \in \partial V_K$, then G acts on $f^{-1}(x) = \{y_1, \cdots, y_n\}$, where $n = \#G$. $x \notin L$

G acts transitively on $f^{-1}(x) \Rightarrow G$ acts transitively on $\partial K_1, \cdots, \partial K_r$ and thus $K_1, \cdots, K_r$

We define the stabiliser of K_i to be the decomposition group

Decomposition Group: $D_{K_i} := \{g \in G \mid g(K_i) = K_i\}$

The decomposition groups are all conjugate to each other:

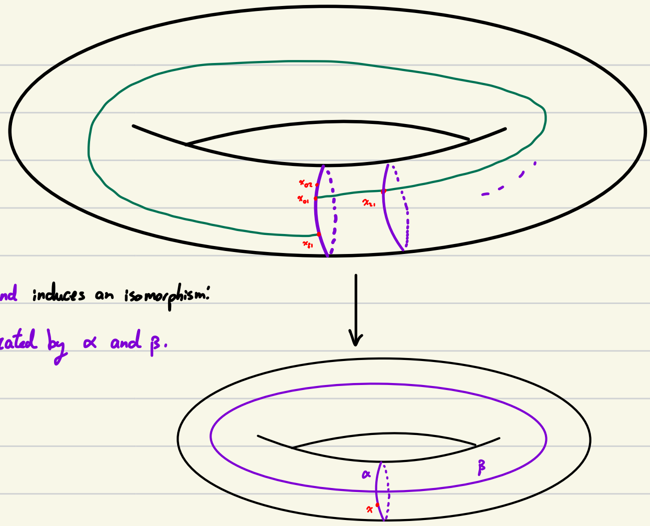
If $g(K_i)=K_j$, then $D_{K_j} = g D_{K_i} g^{-1}$.

Moreover, g induces a homeomorphism of tubular boundaries

$$g|_{\partial V_{K_i}} : \partial V_{K_i} \xrightarrow{\sim} \partial V_{K_j}.$$

In particular for $g \in D_{K_i}$, $g \mapsto g|_{\partial V_{K_i}}$ gives a covering space automorphism of ∂V_{K_i} and induces an isomorphism:

$D_{K_i} \cong Gal(\partial K_i / \partial K)$. This is a cover of a torus, is generated by α and β.



The map $g \mapsto g|_{K_i}$ induces a homomorphism:

$$D_{K_i} \longrightarrow Gal(K_i/K)$$

Define the inertia group I_{K_i} to be the kernel of this homomorphism.

Meridians get sent to the identity, so I_{K_i} is generated by α.

Again I_{K_i} & I_{K_j} are conjugate.

Upshot: We can understand D_{K_i} and I_{K_i} by looking at how they act on $f^{-1}(x)$.

Fix x^i_{01} a point in $f^{-1}(x) \cap \partial V_{K_i}$. Let the orbit of x^i_{01} under α be $\{x_{01}, x_{02}, \dots, x_{0e}\}$.

Then $\# I_{K_i} = e$, the ramification degree.

Define $x_{mn} = \beta^m \cdot x_{0n}$, and define f to be the minimal m s.t. $x_{f1} \in \{x_{01}, \dots, x_{0e}\}$.

f is the <u>covering degree</u> of K_i over K.

$$ef = |f^{-1}(x) \cap \partial K_i|$$

Then we have: $efr = n = \# G$.

Some special cases:

$D_{K_i} = 1 \iff e=f=1,\ r=n$ K decomposes completely.

$D_{K_i} = G \iff ef = n,\ r=1$

$I_{K_i} = 1 \iff e=1,\ fr=n$

$I_{K_i} = G \iff e=n,\ f=r=1$ K totally ramified

<u>§2.2 Primes</u>

<u>Defn (Ramification of a prime)</u>

Let L/K be a finite extension of number fields. p a prime ideal of $\mathcal{O}_K$.

$p\mathcal{O}_L$ is an ideal in $\mathcal{O}_L$, but not necessarily prime.

$\mathcal{O}_L$ Dedekind domain so has unique prime factorisation

$$p\mathcal{O}_L = P_1^{e_1} \cdots P_r^{e_r} \qquad P_i \cap \mathcal{O}_K = p$$

p is <u>unramified</u> in L if $e_i = 1$ $\forall i$. e_i is the <u>ramification degree</u> of P_i

Quotienting induces an extension of residue fields: Let $f_i = [\mathcal{O}_L/P_i : \mathcal{O}_K/p]$, then if $\mathcal{O}_K/p = \mathbb{F}_p$, $\mathcal{O}_L/P_i = \mathbb{F}_{p^{f_i}}$.

f_i is called the <u>residue degree</u> of P_i

<u>Theorem:</u> $\sum e_i f_i = [L:K] = n$ Proof omitted, quite involved.

Suppose now that L/K is Galois, then $Gal(L/K)$ acts transitively on $\{P_1, \dots, P_r\}$ Pf omitted

Then for $\sigma \in Gal(L/K)$:

$$p\mathcal{O}_L = \sigma(p)\mathcal{O}_L = \sigma(P_1)^{e_1}\sigma(P_2)^{e_2}\cdots\sigma(P_r)^{e_r} \quad \Rightarrow \quad e_1 = e_2 = \cdots = e_r = e$$

$$\Rightarrow \mathcal{O}_L/P_i \cong \mathcal{O}_L/\sigma(P_i)$$

$$\Rightarrow f_1 = f_2 = \cdots = f_r = f$$

$$\Rightarrow efr = n$$

Decomposition group: Stabiliser of P_i

$$D_{P_i} = \{\sigma \in Gal(L/K) \mid \sigma(P_i) = P_i\}$$ Note again that the decomposition groups are conjugate.

By orbit-stabliser: D_{P_i} has order ef.

Fixing a P_i, $D_{P_i} \cong Gal(L_{P_i}/K_p)$.

Moreover: $\sigma \mapsto (\bar{\sigma} : \alpha \bmod P_i \mapsto \sigma(\alpha) \bmod P_i)$ defines a surjective map: Surjectivity not obvious, but proof omitted.

$$D_{P_i} \cong Gal(L_{P_i}/K_p) \longrightarrow Gal(\mathbb{F}_{p^f}/\mathbb{F}_p)$$ cyclic of order f, generated by frobenius.

We define I_{P_i} to be the kernel of this map. Then $|I_{P_i}| = e$ Inertia groups are conjugate.

Special Cases:

$D_{P_i} = 1 \iff e = f = 1,\ r = n$ $\quad$ p decomposes completely.

$D_{P_i} = G \iff ef = n,\ r = 1$

$I_{P_i} = 1 \iff e = 1,\ fr = n$

$I_{P_i} = G \iff e = n,\ f = r = 1$ $\quad$ p totally ramified

Extra complexity in prime case: D_{K_i} is quotient of $\mathbb{Z}^2$ so always abelian, but D_{P_i} is generally non-abelian

I_{K_i} is cyclic and generated by α, I_{P_i} not necessarily cyclic (only cyclic if L_P/K_p is tame)

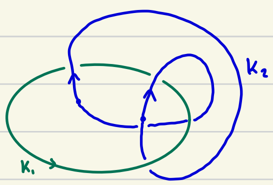
§3. Linking numbers and Power Residue Symbols

§3.1 Linking numbers

Let K_1, K_2 be knots in S^3. Wikipedia says linking number might be fractional or undefined in other 3-folds, but I can't find any source/example of this?

How do we define linking number? Intuitively it is the number of times a knot "wraps around" the other knot, but

Additionally also need to orient K_1, K_2



$lk(K_1, K_2) = 2$

The meridian also wraps around K_1, so we can relate the two:

$$X := S^3 \setminus int(\partial V_{K_1})$$

Consider $G_{K_1} = \pi_1(S^3 \setminus K_1)$ and α be a meridian of K_1.

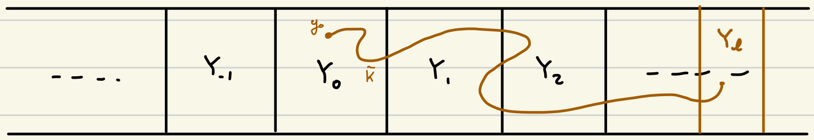
There is a surjective map $\psi_\infty : G_{K_1} \twoheadrightarrow \mathbb{Z}$ that sends α to $1 \in \mathbb{Z}$.

Why does ψ_∞ exist? $H_1(G) \cong G/[G,G] \cong \langle \alpha \rangle$, so send $\alpha \mapsto 1$.

Let X_∞ be the covering space of X corresponding to $\operatorname{Ker}\psi_\infty$.

i.e $Gal(X_\infty/X) \cong \mathbb{Z}$.

X_∞ looks like:



Each Y_i is X cut along a surface, this surface is called the Seifert surface. Seifert Surface: Oriented surface S such that $\partial S = K$.

Can think about $\mathbb{R}$ as a covering of S^1, we "cut" S^1 at a point and glue ∞ copies together.

Existence first proven by Frankl and Pontryagin

Algorithm for construction given by Seifert.

Proposition:

Have map $\rho_\infty : G_{K_1} = \pi_1(S^3 \setminus K_1) \longrightarrow Gal(X_\infty / X) \cong \mathbb{Z}$

Suppose τ generates $Gal(X_\infty/X)$, the map sending Y_i to Y_{i+1}. and pick basept of π_1 so that basept on K_2.

Then: $\rho_\infty([K_2]) = \tau^{lk(K_1,K_2)}$

Pf: Consider a lift $\tilde{K}$ of the path K_2 to X_∞, so that lift starts at Y_0.

Then the path moving from Y_i to $Y_{i\pm1}$ indicates the linking number changing by ±1

So if $\tilde{K}$ ends at Y_ℓ, then $\ell = lk(K_1, K_2)$,

$\rho_\infty([K_2])(y_0) \in Y_\ell$, $\therefore \rho_\infty([K_2])$ must also must coincide w/ the map in $Gal(X_\infty/X)$ sending Y_0 to Y_ℓ.

$\Rightarrow \rho_\infty([K_2]) = \tau^\ell$

For Primes the analogous result is considerably weaker, so first I state weaker version of Knot result.

If we compose ψ_∞ with quotient map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ and call this map ψ_n, define X_n and $\rho_n : G_{K_1} \longrightarrow Gal(X_n/X) \cong \mathbb{Z}/n\mathbb{Z}$ analogously.

Then: $\rho_n : [K_2] \mapsto lk(K_1, K_2) \bmod n$

Relation to decomposition:

The linking of K_1 and K_2 relates to the decomposition of K_2 over a cyclic covering of $M \setminus K_1$, or cyclic covering of M ramified over K_1.

Let $h_2 : X_2 \to X$ be the covering map, then:

$$h_2^{-1}(K_2) = \begin{cases} 2 \text{ disjoint Knots} & \text{if } lk(K_1,K_2) \equiv 0 \bmod 2 \\ 1 \text{ big Knot} & \text{if } lk(K_1,K_2) \equiv 1 \bmod 2 \end{cases}$$

In fact: the number of components that K_2 splits into in X_n is determined by $\gcd(lk(K_1,K_2), n)$

K_2 unramified $\Rightarrow fr = n$

$f =$ order of element in $Gal(X_n/X)$ corresponding to longitude of K_2.

$=$ order of $\quad \sigma = \rho([K_2]) = \tau^{lk(L,K)}$

§3.2 Legendre Symbol

We work backwards

Let $p, q \equiv 1 \bmod 4$. There is a unique quadratic extension of $\mathbb{Q}$ that is ramified only at q, which is $K = \mathbb{Q}(\sqrt{q})$, $\mathcal{O}_K = \mathbb{Z}[(1+\sqrt{q})/2]$

p is unramified in $\mathbb{Q}(\sqrt{q})$, so the frobenius map at p lifts uniquely to a map $\sigma_p \in Gal(K/\mathbb{Q})$

The decomposition gp D_p is generated by σ_p. $\therefore f =$ order of σ_p

We define the linking number mod 2 to be:

$$lk_2(p,q) = \begin{cases} 0 & p \text{ splits in } K \iff \sigma_p \text{ is the identity} \\ 1 & p \text{ is inert in } K \iff \sigma_p \text{ not identity.} \end{cases}$$

$$
\begin{aligned}
lk_2(q,p)=0 &\iff \sigma_p = id_K \\
&\iff \sigma_p(\sqrt{q}) = \sqrt{q} \\
&\iff \sqrt{q} \in \mathbb{F}_p^\times \\
&\iff q \in (\mathbb{F}_p^\times)^2 \\
&\iff q \text{ is a Quadratic Residue mod} p \\
&\iff \left(\tfrac{q}{p}\right) = 1
\end{aligned}
$$

reduce mod p

$$\therefore \quad (-1)^{lk_2(q,p)} = \left(\frac{q}{p}\right)$$

So the Legendre symbol gives the mod 2 linking number

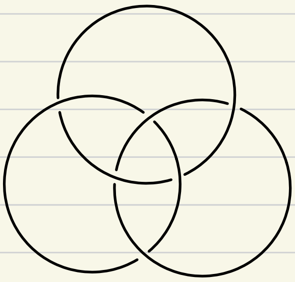
This can be generalised to mod n linking numbers, but the base field needs to contain the nth roots of unity.

In this case the mod n linking number co-incides with the power residue symbol.

§4. Higher linking numbers

Very brief overview, almost all details omitted.

Motivation: Borromean Rings



Any 2 knots are unlinked, but all 3 of them are linked.

Milnor invariants made to detect this

Idea: · Given $K_1, \cdots, K_n$, construct a covering that is ramified over $K_1, \cdots, K_{n-1}$

- Galois group generated by meridians
- Linking of $K_1, \cdots, K_n$ depends on the decomposition of K_n, given by order of longitude

meridians and monodromies sent to $\begin{pmatrix} 1 & & \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$, generates uppertriangular unipotent matrix group

longitude/frobenius of form $\begin{pmatrix} 1 & 0 & \cdots & 0 & a \\ & \ddots & & & \vdots \\ & & & & 0 \\ 0 & & & & 1 \end{pmatrix}$

Similarly for primes: · given $p_1, \cdots, p_n$, want to construct extension ramified over $p_1, \cdots, p_{n-1}$

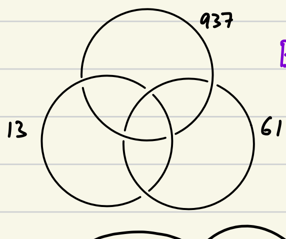
- Galois group generated by monodromies
- Linking number depends on order of frobenius σ_{p_n} or decomposition of p_n

Open Question: How to construct these extensions explicitly?

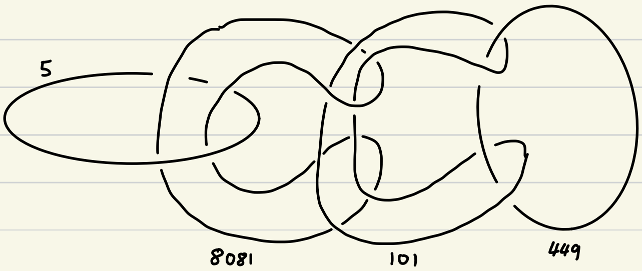
mod 2, 3 primes: Rédei (1939)

mod 2, 4 primes: Amano (2014)

mod 3, 3 primes: Amano, Mizusawa, Morishita (2018)



Borromean Primes.



"Milnor link of 4 components"