Braid groups, Galois groups and some algebraic curves

Dimitrios Noulas

National and Kapodistrian University of Athens

Elliptic Curves and their Applications — CIMPA
July 2025
Armenia, Yerevan

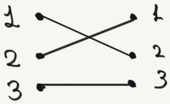
H.F.R.I. Hellenic Foundation for Research & Innovation

Greece 2.0 NATIONAL RECOVERY AND RESILIENCE PLAN

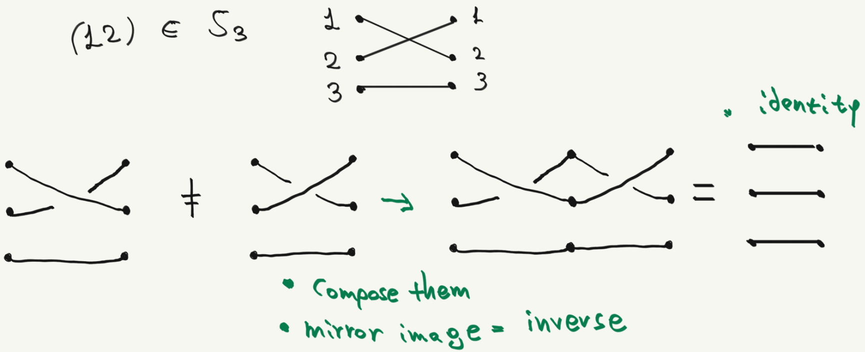
Funded by the European Union NextGenerationEU

What is a Braid group?

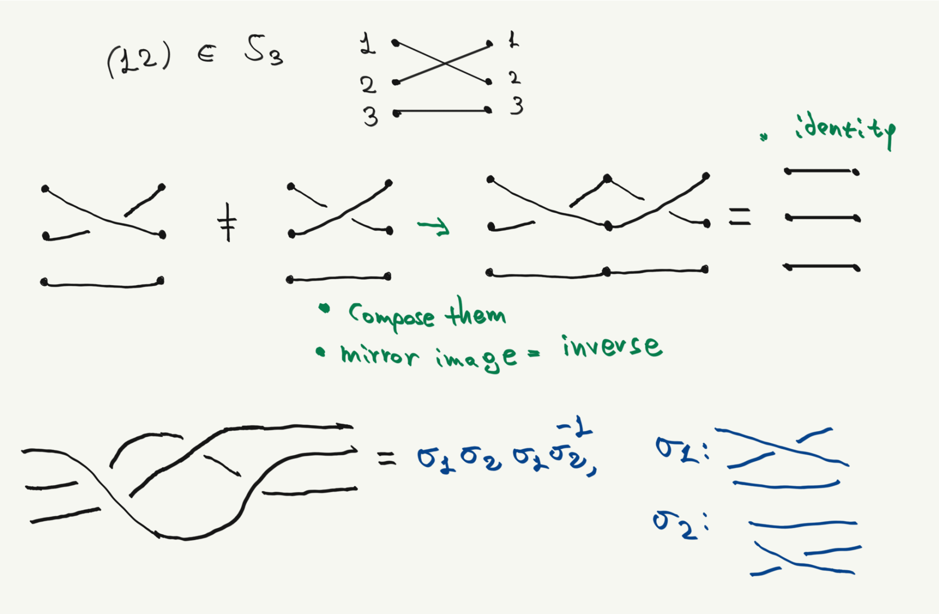
$(12) \in S_3$



What is a Braid group?



What is a Braid group?



Artin representation of B_3

Let $F = \langle x_1, x_2, x_3 \mid x_1 x_2 x_3 = 1 \rangle$ be the free group on two generators x_1, x_2. Then,

$$B_3 \leq \mathrm{Aut}(F)$$

generated by σ_1, σ_2 such that

$$\sigma_i(x_{i+1}) = x_i,\ \sigma_i(x_i) = x_i x_{i+1} x_i^{-1},\ \sigma_i(x_k) = x_k$$

Artin representation of B_3

Let $F = \langle x_1, x_2, x_3 \mid x_1 x_2 x_3 = 1 \rangle$ be the free group on two generators x_1, x_2. Then,

$$B_3 \leq \mathrm{Aut}(F)$$

generated by σ_1, σ_2 such that

$$\sigma_i(x_{i+1}) = x_i, \ \sigma_i(x_i) = x_i x_{i+1} x_i^{-1}, \ \sigma_i(x_k) = x_k$$

Pure braids

In particular, there is a subgroup:

$$PB_3 = \{\sigma \in \mathrm{Aut}(F) : \sigma(x_i) \sim x_i\},$$

where $\sim$ denotes conjugation by an element (differs for every input).

Why should we care?

Why should we care?

A wild Modular group appeared!

$$B_3/Z(B_3) \cong \mathrm{SL}_2(\mathbb{Z})/\{\pm I\},$$

where $Z(B_3)$ is the center generated by $(\sigma_1\sigma_2)^3$. Remember $(ST)^3 = 1$?

Why should we care?

A wild Modular group appeared!

$$B_3/Z(B_3) \cong \mathrm{SL}_2(\mathbb{Z})/\{\pm I\},$$

where $Z(B_3)$ is the center generated by $(\sigma_1\sigma_2)^3$. Remember $(ST)^3 = 1$?

A scary generalization

$\mathrm{Mod}(S) =$ "∞-differentiable orientation preserving homeomorphisms of S up to homotopy equivalence".

Why should we care?

A wild Modular group appeared!

$$B_3/Z(B_3) \cong \mathrm{SL}_2(\mathbb{Z})/\{\pm I\},$$

where $Z(B_3)$ is the center generated by $(\sigma_1\sigma_2)^3$. Remember $(ST)^3 = 1$?

A scary generalization

$\mathrm{Mod}(S) =$ "∞-differentiable orientation preserving homeomorphisms of S up to homotopy equivalence".

Examples

$\mathrm{Mod}(D_3) = B_3$, where D_3 is the closed disk with three marked points.
$\mathrm{Mod}(S_{0,4}) = \mathrm{PSL}_2(\mathbb{Z})$, $\quad S_{0,4}$ is the sphere with 4 punctures.
$\mathrm{Mod}(S)$ is a subgroup of $\mathrm{Out}(\pi_1(S))$ in general.

Galois Theory reminder

Galois group

$$\mathrm{Gal}(K/L) = \{\sigma : K \to K, \text{ field automorphisms }, \ \sigma(x) = x \text{ for all } x \in L\}$$

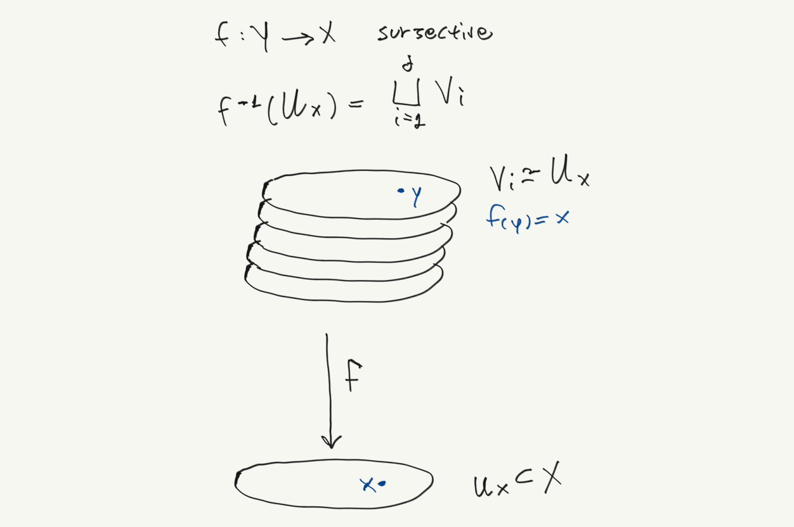
$$\begin{array}{ccc}
K = \mathbb{Q}(\sqrt{3}+\sqrt{2}+\sqrt{5}) & & 1 \\
| & & | \\
L_1 = \mathbb{Q}(\sqrt{3}, \sqrt{2}) & & \mathrm{Gal}(K/L_1) \\
| & & | \\
L_2 = \mathbb{Q}(\sqrt{3}) & & \mathrm{Gal}(K/L_2) \\
| & & | \\
\mathbb{Q} & & \mathrm{Gal}(K/\mathbb{Q})
\end{array}$$

What is the Fundamental group $\pi_1(X)$?

Quick answer: A Galois group (of some sort...)

What is the Fundamental group $\pi_1(X)$?

Quick answer: A Galois group (of some sort...)
$\pi_1(X)$ classifies:



Examples

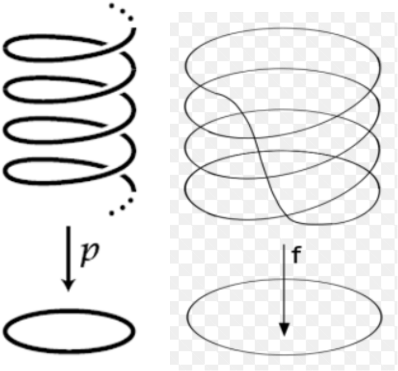
$$p : \mathbb{R} \longrightarrow S^1$$
$$\theta \longmapsto e^{i\theta},$$

and $\pi_1(S^1) = \mathbb{Z}$.

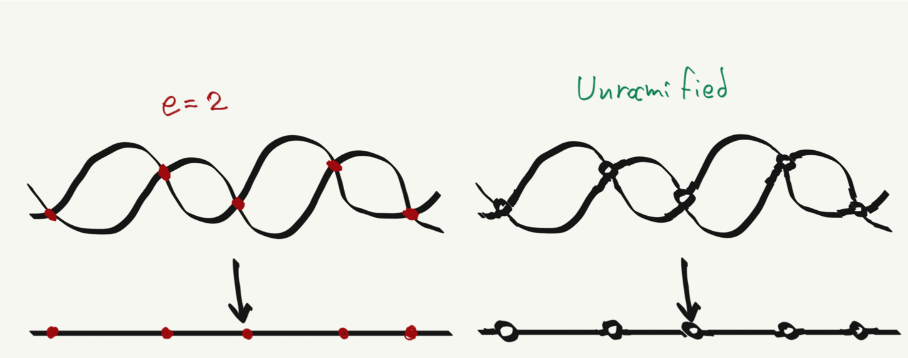
Examples

$$p : \mathbb{R} \longrightarrow S^1$$
$$\theta \longmapsto e^{i\theta},$$

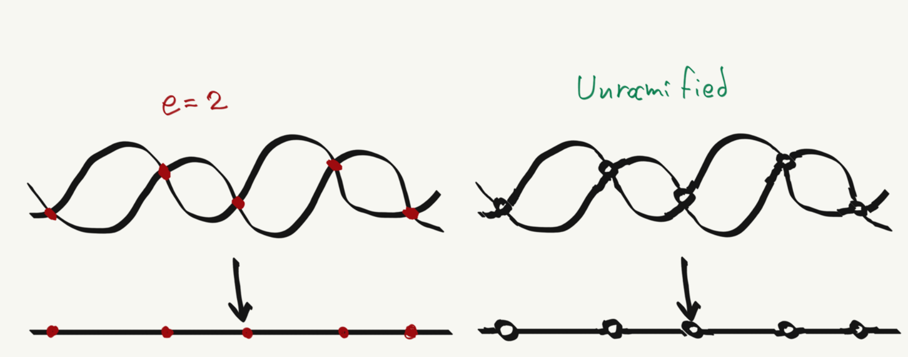
and $\pi_1(S^1) = \mathbb{Z}$. There is a subcovering f corresponding to $4\mathbb{Z}$:



Branched covers to topological covers



Branched covers to topological covers



From elliptic curves

Let $E : y^2 = x(x-1)(x-\lambda)$ then the rational map to $\mathbb{P}^1$ being the first projection is ramified over $0, 1, \lambda, \infty$ with ramification indices 2.

P-adic numbers reminder

Profinite (or pro-p) completion

Given a group G, one can form the inverse limit

$$\varprojlim G/N$$

that runs over all finite index normal subgroups N with some sort of "compatible" maps between the quotients.

P-adic numbers reminder

Profinite (or pro-p) completion

Given a group G, one can form the inverse limit

$$\varprojlim G/N$$

that runs over all finite index normal subgroups N with some sort of "compatible" maps between the quotients.

P-adics

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

Two ways to view these:

$$x = \sum_{k=0}^{\infty} a_k p^k$$

P-adic numbers reminder

Profinite (or pro-p) completion

Given a group G, one can form the inverse limit

$$\varprojlim G/N$$

that runs over all finite index normal subgroups N with some sort of "compatible" maps between the quotients.

P-adics

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

Two ways to view these:

$$x = \sum_{k=0}^{\infty} a_k p^k$$

$$(\beta_n \bmod p^n) : \quad \beta_1 = a_0, \beta_2 = a_0 + a_1 p, \beta_3 = a_0 + a_1 p + a_2 p^2, \ldots$$

Two useful examples

Tate module of Elliptic Curve

$$\varprojlim E[p^n]$$

with compatible maps

$$E[p^{m+1}] \longrightarrow E[p^m]$$

can also be applied to the Weil pairing.

Two useful examples

Tate module of Elliptic Curve

$$\varprojlim E[p^n]$$

with compatible maps

$$E[p^{m+1}] \longrightarrow E[p^m]$$

can also be applied to the Weil pairing.

Free pro-p group

The pro-p completion of F will be denoted by $\mathcal{F}$. Elements can be words of the form:

$$1, w, w^2, w^3, \ldots, w^x, \ldots$$

with $x = \sum_{k=0}^{\infty} a_k p^k \in \mathbb{Z}_p$ by some sort of "continuity".

Our favourite topological space...

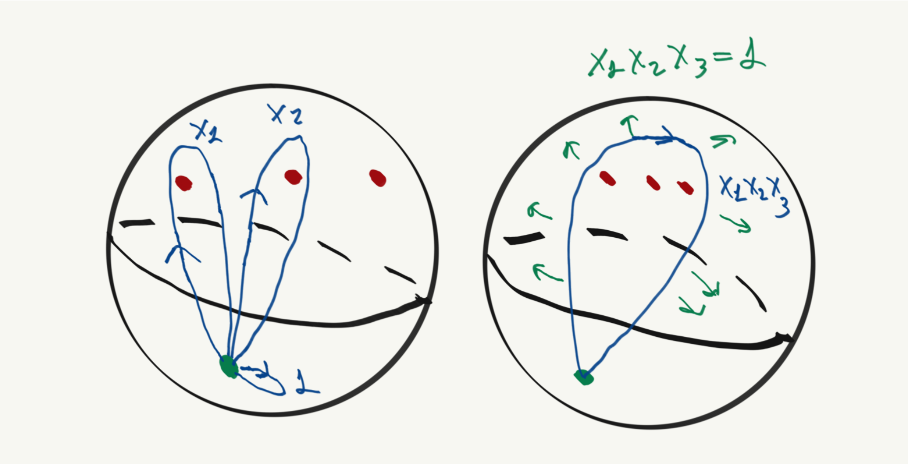
... is the punctured projective line

Let X be $\mathbb{P}^1_{\mathbb{C}} - \{0, 1, \infty\}$. Then $\pi_1(X) = F$

Our favourite topological space...

... is the punctured projective line

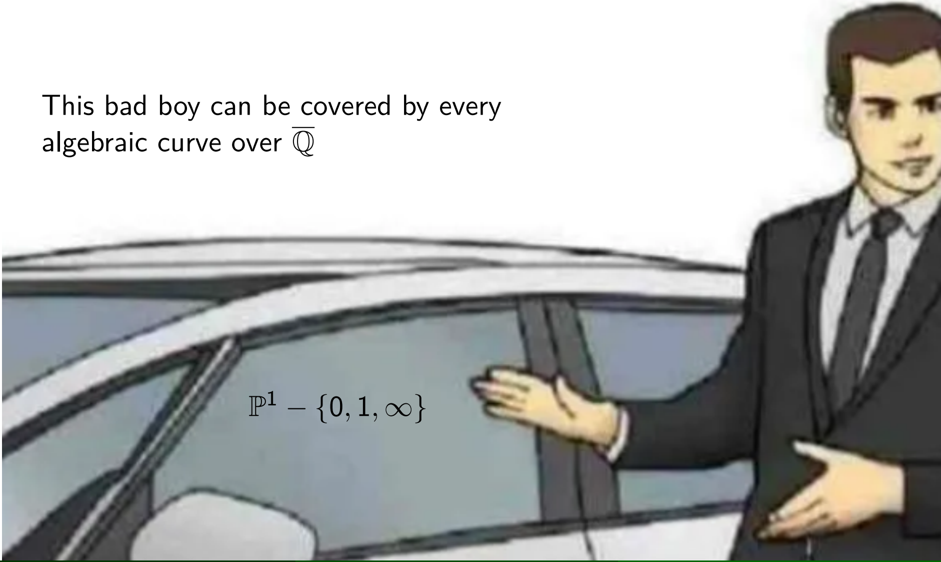
Let X be $\mathbb{P}^1_{\mathbb{C}} - \{0, 1, \infty\}$. Then $\pi_1(X) = F$



But why?

But why?

This bad boy can be covered by every algebraic curve over $\overline{\mathbb{Q}}$



A celebrated theorem

Theorem (Belyi)

The algebraic curve C over $\mathbb{C}$ can be defined over $\overline{\mathbb{Q}}$ if and only if there exists a ramified cover $C \to \mathbb{P}^1$ branched above three points.

A celebrated theorem

Theorem (Belyi)

The algebraic curve C over $\mathbb{C}$ can be defined over $\overline{\mathbb{Q}}$ if and only if there exists a ramified cover $C \to \mathbb{P}^1$ branched above three points.

One of the many consequences

The curve C can be realized as a quotient $\Gamma \setminus \mathbb{H}$ after compactification, where Γ is a finite index subgroup of the modular group.

A celebrated theorem

Theorem (Belyi)

The algebraic curve C over $\mathbb{C}$ can be defined over $\overline{\mathbb{Q}}$ if and only if there exists a ramified cover $C \to \mathbb{P}^1$ branched above three points.

One of the many consequences

The curve C can be realized as a quotient $\Gamma \setminus \mathbb{H}$ after compactification, where Γ is a finite index subgroup of the modular group.

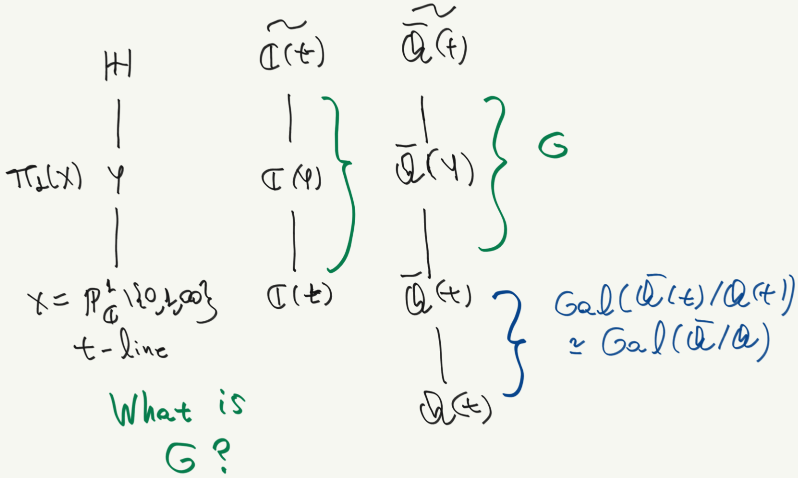
EC example revisited

For the elliptic curve $y^2 = x(x-1)(x-\lambda), \lambda \in \overline{\mathbb{Q}}$ the projection $(x, y) \mapsto x$ is ramified over $\{0, 1, \infty, \lambda\}$. Compose this with

$$\frac{x-\lambda}{x(1-\lambda)},$$

to reduce them to $\{0, 1, \infty\}$.

What are the finite covers over $\mathbb{Q}$?



Throw everything to the mix

Let $\Pi_{\mathbb{Q}}$ (resp. $\Pi_{\overline{\mathbb{Q}}}$) classify the finite covers of degree power of p over $\mathbb{Q}$ (resp. $\overline{\mathbb{Q}}$).

Throw everything to the mix

Let $\Pi_{\mathbb{Q}}$ (resp. $\Pi_{\overline{\mathbb{Q}}}$) classify the finite covers of degree power of p over $\mathbb{Q}$ (resp. $\overline{\mathbb{Q}}$). Grothendieck:

$$\Pi_{\overline{\mathbb{Q}}} = \mathcal{F}$$

the pro-p completion!

Throw everything to the mix

Let $\Pi_{\mathbb{Q}}$ (resp. $\Pi_{\overline{\mathbb{Q}}}$) classify the finite covers of degree power of p over $\mathbb{Q}$ (resp. $\overline{\mathbb{Q}}$). Grothendieck:

$$\Pi_{\overline{\mathbb{Q}}} = \mathcal{F}$$

the pro-p completion!

The outer representation

$$1 \longrightarrow \mathcal{F} \longrightarrow \Pi_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow 1$$

yields

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Out}(\mathcal{F})$$

with image

$$\{\sigma \in \mathrm{Out}(\mathcal{F}) : \quad \sigma(x_i) \sim x_i^{a_\sigma}\}$$

for some p-adic number a_σ. In particular there is a subgroup for all σ such that $a_\sigma = 1$, familiar?

A climb up the Fermat tower

Through Galois correspondence, the commutator subgroup $\mathcal{F}' = [\mathcal{F}, \mathcal{F}]$ contains all fields:

$$\overline{\mathbb{Q}}(t^{1/p^n}, (1-t)^{1/p^n}),$$

A climb up the Fermat tower

Through Galois correspondence, the commutator subgroup $\mathcal{F}' = [\mathcal{F}, \mathcal{F}]$ contains all fields:

$$\overline{\mathbb{Q}}(t^{1/p^n}, (1-t)^{1/p^n}),$$

in other words all curves of the form:

$$X^{p^n} + Y^{p^n} = Z^{p^n}$$

A climb up the Fermat tower

Through Galois correspondence, the commutator subgroup $\mathcal{F}' = [\mathcal{F}, \mathcal{F}]$ contains all fields:

$$\overline{\mathbb{Q}}(t^{1/p^n}, (1-t)^{1/p^n}),$$

in other words all curves of the form:

$$X^{p^n} + Y^{p^n} = Z^{p^n}$$

Theorem (Y. Ihara)

Only $[x_1, x_2]$ is needed to fully describe the braid-like Galois action on $\mathcal{F}'/\mathcal{F}''$

A climb up the Fermat tower

Through Galois correspondence, the commutator subgroup $\mathcal{F}' = [\mathcal{F}, \mathcal{F}]$ contains all fields:

$$\overline{\mathbb{Q}}(t^{1/p^n}, (1-t)^{1/p^n}),$$

in other words all curves of the form:

$$X^{p^n} + Y^{p^n} = Z^{p^n}$$

Theorem (Y. Ihara)

Only $[x_1, x_2]$ is needed to fully describe the braid-like Galois action on $\mathcal{F}'/\mathcal{F}''$

$$\sigma \cdot [x_1, x_2] = F_\sigma \; [x_1, x_2]$$

and F_σ is a (formal) power series over $\mathbb{Z}_p$

A climb up the Fermat tower

Through Galois correspondence, the commutator subgroup $\mathcal{F}' = [\mathcal{F}, \mathcal{F}]$ contains all fields:

$$\overline{\mathbb{Q}}(t^{1/p^n}, (1-t)^{1/p^n}),$$

in other words all curves of the form:

$$X^{p^n} + Y^{p^n} = Z^{p^n}$$

Theorem (Y. Ihara)

Only $[x_1, x_2]$ is needed to fully describe the braid-like Galois action on $\mathcal{F}'/\mathcal{F}''$

$$\sigma \cdot [x_1, x_2] = F_\sigma \ [x_1, x_2]$$

and F_σ is a (formal) power series over $\mathbb{Z}_p$

Conjecture

Is $F_\sigma(\zeta_{p^n}^a - 1, \zeta_{p^n}^b - 1, \zeta_{p^n}^c - 1)$, well-defined?

A climb up the Fermat tower

Through Galois correspondence, the commutator subgroup $\mathcal{F}' = [\mathcal{F}, \mathcal{F}]$ contains all fields:

$$\overline{\mathbb{Q}}(t^{1/p^n}, (1-t)^{1/p^n}),$$

in other words all curves of the form:

$$X^{p^n} + Y^{p^n} = Z^{p^n}$$

Theorem (Y. Ihara)

Only $[x_1, x_2]$ is needed to fully describe the braid-like Galois action on $\mathcal{F}'/\mathcal{F}''$

$$\sigma \cdot [x_1, x_2] = F_\sigma \; [x_1, x_2]$$

and F_σ is a (formal) power series over $\mathbb{Z}_p$

Conjecture

Is $F_\sigma(\zeta_{p^n}^a - 1, \zeta_{p^n}^b - 1, \zeta_{p^n}^c - 1)$, well-defined? Answer: Yes! (Ihara-Kaneko-Yukinari, Anderson, Coleman)

Some references

Inspiration

Y. Ihara, *Profinite braids, Galois representations and complex multiplications*, Annals of Mathematics (1986).
Y. Ihara, *Braid groups, Galois groups and arithmetic functions.*

Some references

Inspiration

Y. Ihara, *Profinite braids, Galois representations and complex multiplications*, Annals of Mathematics (1986).
Y. Ihara, *Braid groups, Galois groups and arithmetic functions.*

Rachel Davis, Rachel Pries, Vesna Stojanoska, Kirsten Wickelgren:

Galois action on the homology of Fermat curves (2016)
The Galois action and cohomology of a relative homology group of Fermat Curves (2019)
The Galois action on the lower central series of the fundamental group of the Fermat curve (2023)

Some references

Inspiration

Y. Ihara, *Profinite braids, Galois representations and complex multiplications*, Annals of Mathematics (1986).
Y. Ihara, *Braid groups, Galois groups and arithmetic functions.*

Rachel Davis, Rachel Pries, Vesna Stojanoska, Kirsten Wickelgren:

Galois action on the homology of Fermat curves (2016)
The Galois action and cohomology of a relative homology group of Fermat Curves (2019)
The Galois action on the lower central series of the fundamental group of the Fermat curve (2023)

Ihara viewpoint

A. Kontogeorgis, P. Paramantzoglou, Galois action on homology of generalized Fermat curves. (2019)

Where to now?

- Notion of heavenly elliptic curves and abelian varieties - Cam McLeman, Christopher Rasmussen (2025).

Where to now?

- Notion of heavenly elliptic curves and abelian varieties - Cam McLeman, Christopher Rasmussen (2025).
- "Replace" $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ by $\mathrm{Mod}(S)$ (Soon, joint with A. Kontogeorgis, M. Karakikes, S. Karanikolopoulos)

Where to now?

- Notion of heavenly elliptic curves and abelian varieties - Cam McLeman, Christopher Rasmussen (2025).
- "Replace" $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ by $\mathrm{Mod}(S)$ (Soon, joint with A. Kontogeorgis, M. Karakikes, S. Karanikolopoulos)
- The story goes on: Cyclic covers, to elementary abelian covers, to non-abelian covers

$$\begin{aligned} y^n = f(x), &\quad \mathbb{Z}/n\mathbb{Z}, \\ x^n + y^n = z^n, &\quad \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \\ \text{Heisenberg curves}, &\quad (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) \rtimes \mathbb{Z}/n\mathbb{Z} \end{aligned}$$

"A climb up the Heisenberg tower", (in preparation, not soon... or maybe...)

Thank you!

Ευχαριστώ πολύ!

$$\downarrow$$

$$x^n + y^n = 1$$

$$\downarrow$$

$$\mathbb{P}^1 \setminus \{0, 1, \infty\}$$