~ Distinguishing Braid Groups trough profinite Methods ~

F. Gavazzi

Ph.D. students seminar, Dijon, 26/03/25.

Intro: In this talk we will try to distinguish some groups by looking at their finite quotients. The groups under consideration will be the Braid groups.

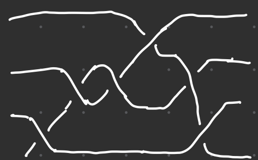
1§. Braid Groups

• **Def** The BRAID GROUP on n strands, denoted by $\mathcal{B}_n$, is the group defined by the following presentation:

$$\mathcal{B}_n = \left\langle \sigma_1, \dots, \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\sigma_j = \sigma_j\sigma_i & |i-j|\geq 2 \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} & \forall i = 1, \dots, n-2 \end{array} \right\rangle$$

A braid $\beta \in \mathcal{B}_n$ looks like a diagram as below:

β :



$\beta \in \mathcal{B}_4$

The generators are:

σ_i

While the relations are

$\sigma_i\sigma_j = \sigma_j\sigma_i \quad |i-j|\geq 2 \qquad \Big| \qquad \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$

• **Comments**:

* $\mathcal{B}_n$ is infinite for every n. For example $\langle \sigma_i \rangle \cong \mathbb{Z}$

* The abelianized $\mathcal{B}_n^{ab} = \mathbb{Z}$ for all n.

$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \rightsquigarrow \quad \sigma_i\sigma_{i+1} =: g \qquad g\sigma_i g^{-1} = \underline{\sigma_i\sigma_{i+1}\sigma_i}\,\sigma_{i+1}^{-1}\sigma_i^{-1} = \sigma_{i+1}\cancel{\sigma_i}\cancel{\sigma_{i+1}}\cancel{\sigma_{i+1}^{-1}}\cancel{\sigma_i^{-1}} = \sigma_{i+1}$

the (adjacent) generators are conjugate $\rightsquigarrow$ In the abelianized all the generators have the same image

$y = x^{-1}xy = xx^{-1}y = x\underbrace{g^{-1}y^{-1}gy}_{\text{commutator}} \Rightarrow [y]_{ab} = [x]_{ab}$

* For all $n \in \mathbb{N}_{\geq 2}$, we can define a group hom
$$\omega : \mathcal{B}_n \longrightarrow \mathfrak{S}_n, \quad \sigma_i \longmapsto t_i = (i, i+1)$$
that is surjective!

for example, if

$\beta =$ 

$\longmapsto$ $\begin{array}{l} 1 \mapsto 3 \\ 2 \mapsto 2 \\ 3 \mapsto 4 \\ 4 \mapsto 1 \end{array} \in \mathfrak{S}_4$

$= (1\,3\,4)$

$\rightsquigarrow$ $\mathfrak{S}_n$ is always a finite quotient of B_n.

* Braid groups are examples of ARTIN GROUPS, fascinating structures poorly understood in general.

(Naive) QUESTION: If $B_n \cong B_m$, does it imply that $n = m$?

Answer 1: YES. Thm by Paris, 2004, proven in the more general setting of spherical type Artin groups.

Answer 2: YES. Thm by Van der Lek, 1983. 〃 〃 〃 Artin groups.

if $n < m$, the map $\begin{array}{rcl} B_n & \longrightarrow & B_m \\ \sigma_i & \longmapsto & \sigma_i \end{array} \quad \forall\, i = 1, \dots, n-1$ is injective (and non surjective).

So we can distinguish all braid groups up to isomorphism.

(Less naive) QUESTION: Is there a finer way to distinguish them?

Answer: Profinite completion.

• 2 § Profinite completion of groups

2.1: Inverse systems and limits:

• **Def** Let $(I, \leq)$ be a directed poset. A family of groups $(G_i)_{i \in I}$ with (surjective) homomorphisms $f_{ij} : G_j \longrightarrow G_i$ whenever $i \leq j$ is an INVERSE SYSTEM if $\forall\ i \leq j \leq k$, $f_{ik} = f_{ij} \circ f_{jk}$.

$$\begin{tikzcd} G_k \arrow[r, "f_{jk}"] \arrow[dr, "f_{ik}"'] & G_j \arrow[d, "f_{ij}"] \\ & G_i \end{tikzcd}$$

• **Def** Given an inverse (or projective system) of groups $(G_i, f_{ij})_{i \in I}$, the INVERSE LIMIT of this system denoted by $\varprojlim_{i \in I} G_i$ is a subgroup of the product $\prod_{i \in I} G_i$ such that

$$\varprojlim_{i \in I} G_i = \left\{ \vec{g} = (g_1, \dots, g_i, \dots) \in \prod_{i \in I} G_i \;\middle|\; g_i = f_{ij}(g_j) \right\}$$

equivalently, the following diagram commutes:

$$\begin{tikzcd} G_j \arrow[rr, "f_{ij}"] & & G_i \\ & \varprojlim_{i\in I} G_i \arrow[ul, "\pi_j"] \arrow[ur, "\pi_i"'] \arrow[u, phantom, "\circlearrowright"] & \end{tikzcd}$$

$$\varprojlim_{i\in I} G_i \subseteq \prod_{i\in I} G_i$$

$$\pi_i : \prod_{i\in I} G_i \twoheadrightarrow G_i$$

• 2.2. Main example: p-adic integers:

Let p be a prime, $I = \mathbb{N}^*$. Consider the family of groups $\left(\mathbb{Z}/p^i\mathbb{Z}\right)_{i\in I}$. For $i \leq j$, we have a surj.

$$f_{ij} : \mathbb{Z}/p^j\mathbb{Z} \longrightarrow \mathbb{Z}/p^i\mathbb{Z}.$$

The pair $(\mathbb{Z}/p^i\mathbb{Z}, f_{ij})$ is an INVERSE SYSTEM!

We can compute its inverse limit

$$\varprojlim_{i\in I} \left(\mathbb{Z}/p^i\mathbb{Z}\right) = \left\{ \vec{n} = (n_1, .., n_i, ..) \in \prod_{i\in I} \mathbb{Z}/p^i\mathbb{Z} \;\middle|\; f_{ij}(n_j) = [n_j]_{\text{mod } p^i} = n_i \right\}$$

• Def This inverse limit is the GROUP of p-ADIC INTEGERS $\mathbb{Z}_p$

What are its elements?

$$\vec{n} \in \mathbb{Z}_p \quad \text{s.t.} \quad \vec{n} = (n_1, n_2, \dots), \quad \overset{\text{eq. class}}{n_i} \in \mathbb{Z}/p^i\mathbb{Z}$$

For example, fix $n_1 \overset{\text{abuse of notation}}{=} [n_1]_p = \{ n \in \mathbb{Z} \mid n = n_1 + \alpha p, \alpha \in \mathbb{Z} \}$

The second component n_2 must be such that $[n_2]_p = n_1 \Rightarrow n_2 = n_1 + \alpha_1 p$, where $\alpha_1 \in \{0, \dots, p-1\}$.

Analogously, $\forall j$, n_j must be such that $[n_j]_{p^i} = n_i$ for all $i < j$. Namely:

$$\boxed{n_j = \alpha_{j-1} p^{j-1} + \alpha_{j-2} p^{j-2} + \dots + \alpha_1 p + \alpha_0 \qquad \alpha_i \in \{0, .., p-1\}}$$

An element in $\mathbb{Z}_p$ can be univoquely determined by the tuple of the α_i's, thus

$$n \in \mathbb{Z}_p, \qquad n = \sum_{i=0}^{\infty} \alpha_i p^i$$

Rmk: The n_i's could be zero until a certain $k \in \mathbb{N}_{\geq 0}$. In this case $n = \sum_{i=k}^{\infty} \alpha_i p^i$

2.3: More generally: finite quotients of groups

Our groups G will be taken under certains hypotheses

• **Def** Let G be a group. $\mathcal{N}(G) = \{ N \trianglelefteq G \mid [G:N] < \infty \}$ is the set of finite index normal subgroups of G.

$\mathcal{F}_q(G) = \{ G/N \mid N \in \mathcal{N}(G) \}$ is the set of finite quotients of G.

I can give to $\mathcal{F}_q(G)$ the structure of inverse system given by $(G/N, f_{NM})_{N \in \mathcal{N}(G)}$

if $N \triangleleft M$, then $G/N \xrightarrow{f_{MN}} G/M = \dfrac{G/N}{M/N}$. We can show that the triangles $N \triangleleft M \triangleleft L$ commute.

• **Def** The PROFINITE COMPLETION $\hat{G}$ of a group G is the inverse limit of the inverse system $(G/N, f_{NM})_{N \in \mathcal{N}(G)}$

Namely:

$$\hat{G} = \varprojlim_{N \in \mathcal{N}(G)} = \left\{ \vec{g} = (gN_1, gN_2, \ldots,) \in \prod_{\substack{i \in \mathbb{N} \\ N_i \in \mathcal{N}(G)}} G/N_i \;\middle|\; \text{if } N_j \triangleleft N_i,\ gN_i = f_{N_i N_j}(gN_j) \right\}$$

example: $\mathbb{Z}$

Take $\mathbb{Z} = G$. Its finite index subgroups are $\mathcal{N}(\mathbb{Z}) = \{ n\mathbb{Z},\ n \in \mathbb{N} \}$.

Its finite quotients are $\mathcal{F}_q(\mathbb{Z}) = \{ \mathbb{Z}/n\mathbb{Z},\ n \in \mathbb{N} \}$.

It is an inverse system with the maps:

$$n\mathbb{Z} \triangleleft m\mathbb{Z} \iff m \mid n. \qquad \mathbb{Z}/m\mathbb{Z} \xrightarrow{f_{nm}} \mathbb{Z}/n\mathbb{Z}$$

$$\hat{\mathbb{Z}} = \varprojlim_{n \in \mathbb{N}} (\mathbb{Z}/n\mathbb{Z}, f_{nm}) = \left\{ \vec{z} = (z_1, z_2, \ldots) \in \prod_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z} \;\middle|\; \text{if } m \mid n,\ z_n = f_{nm}(z_m) \text{, that is } z_m \equiv z_n \pmod{n} \right\}$$

$$\rightsquigarrow \boxed{\hat{\mathbb{Z}} = \prod_{p \text{ prime}} \mathbb{Z}_p}$$

• **Remark 1** There is a natural map

$$i : G \longrightarrow \hat{G}$$
$$g \longmapsto ([g]_{G/N})_{N \in \mathcal{N}(G)}$$

This homomorphism is injective if and only if

$\ker(i) = \{ g \in G \mid \forall N \in \mathcal{N}(G),\ [g] \text{ in } G/N \text{ is } \{1\} \} = \{1\}$

It is interesting to study the profinite completion of a group $\hat{G}$ when $\ker(i) = \{1\}$. Namely, when

$\forall g \in G,\ \exists N \in \mathcal{N}(G)$ s.t. $\pi_N : G \longrightarrow G/N$ sends g to $\pi_N(g) \neq 1$ non trivial element.

If G satisfies this condition, then we say that it is RESIDUALLY FINITE.

• Remark 2

Profinite completions are usually defined for topological spaces / topological groups. I can endow each group with a topology to get a topological group. In general, different topologies give different profinite completions of G. A deep theorem [Nikolov-Segal, 2007] says that if G is finitely generated, then all the topologies on G give the same $\widehat{G}$. Morally: if G is finitely generated, we can forget about the topology.

• Rmk 3 Braid groups are ⊛ = residually finite and fin. generated (thanks to [Digne])

QUESTION If G, H groups are ⊛ = residually finite and fin. generated, given $\widehat{G} \cong \widehat{H}$, does it mean that $G \cong H$?

Comment: This is not clear, for free groups it is a big conjecture.

Two non isomorphic groups can have the same profinite completion!

examples:
- $\widehat{\mathbb{Z}} \cong \widehat{\widehat{\mathbb{Z}}} = \widehat{\mathbb{Z}}$ but $\mathbb{Z} \not\cong \widehat{\mathbb{Z}}$!
- $\mathbb{Q}$ has not finite quotients (as $(\mathbb{Q},+)$). Thus $\widehat{\mathbb{Q}} = \{1\}$. Then $\widehat{\mathbb{Q}} \cong \widehat{\{1\}} = \{1\}$ but $\{1\} \not\cong \mathbb{Q}$!

QUESTION If $m \neq n$, $\widehat{B_m} \overset{?}{\cong} \widehat{B_n}$?

Here are the tools that we can use to study the prof. completion of ⊛ groups:

Results: let G, H be ⊛

1. $\widehat{G} \cong \widehat{H} \iff \mathcal{F}(G) = \mathcal{F}(H)$
2. $\widehat{G} \cong \widehat{H} \Rightarrow G^{ab} = H^{ab}$.
3. $\widehat{G} \cong \widehat{H} \Rightarrow \forall Q$ finite group, $|\mathrm{Hom}(G,Q)| = |\mathrm{Hom}(H,Q)|$.

Let's try with 2: $B_n^{ab} = \mathbb{Z} = B_m^{ab}$:(

• Thm [Kolay '23]
- Let $n \geq 5$. Then the smallest non abelian finite quotient of B_n is $\mathfrak{S}_n$.
- $\mathfrak{S}_3$ is the smallest non abelian finite quotient of B_3, B_4.

↝ Corollary If $\widehat{B_n} \cong \widehat{B_m}$, then $m = n$.

Proof: For $n \geq 5$ by [Kolay] B_n and B_m have different finite quotients, then different profinite completion.

We must distinguish B_3 from B_4. We use a variant of 3, we construct a surj. homomorphism

$B_3 = \langle \sigma_1', \sigma_2' \rangle$

$B_4 = \langle \sigma_1, \sigma_2, \sigma_3 \rangle$

$$\begin{aligned} \varphi : B_4 &\longrightarrow B_3 \\ \sigma_1 &\longmapsto \sigma_1' \\ \sigma_3 &\longmapsto \sigma_1' \\ \sigma_2 &\longmapsto \sigma_2' \end{aligned}$$

∎