On conjugacy classes of the Pro-$\ell$ braid group of degree $2$

Kaneko, Masanobu
Department of Mathematics, Faculty of Science, University of Tokyo

https://hdl.handle.net/2324/20418
On Conjugacy Classes of the Pro-\(l\) braid Group of Degree 2

By Masanobu Kaneko

Department of Mathematics, Faculty of Science, University of Tokyo

(Communicated by Shokichi Iyanaga, M. J. A., Sept. 12, 1986)

0. Introduction. In [2], Y. Ihara studied the “pro-\(l\) braid group” of degree 2 which is a certain big subgroup \(\Phi \subset \text{Out} \, \mathbb{F}\) of the outer automorphism group of the free pro-\(l\) group \(\mathbb{F}\) of rank 2. There is a canonical representation \(\varphi_q : G_q \to \Phi\) of the absolute Galois group \(G_q = \text{Gal} (\overline{\mathbb{Q}}/\mathbb{Q})\) which is unramified outside \(l\), and for each prime \(p \neq l\), the Frobenius of \(p\) determines a conjugacy class \(C_p\) of \(\Phi\) which is contained in the subset \(\Phi_p \subset \Phi\) formed of all elements of “norm” \(p\) (loc. cit. Ch. I). In this note, we shall prove that \(\Phi_p\) contains infinitely many \(\Phi\)-conjugacy classes, at least if \(p\) generates \(\mathbb{Z}\) topologically. It is an open question whether one can distinguish the Frobenius conjugacy class from other norm-\(p\)-conjugacy classes.

1. The result. Let \(l\) be a rational prime. We denote by \(\mathbb{Z}_l\), \(\mathbb{Z}_l^\times\) and \(\mathbb{Q}_l\), respectively, the ring of \(l\)-adic integers, the group of \(l\)-adic units and the field of \(l\)-adic numbers. As in [2], let \(\mathbb{F} = \mathbb{F}(\alpha)\) be the free pro-\(l\) group of rank 2 generated by \(x, y, z\), \(xyz = 1\), \(\Phi = \text{Brd}(\mathbb{F})\), and \(\Phi_p = \text{Brd}(\mathbb{F}/\mathbb{Q}_p)\) be the pro-\(l\) braid group of degree 2, \(\text{Nr}(\sigma) \in \mathbb{Z}_l^\times\) be the norm of \(\sigma \in \Phi\), and for \(\alpha \in \mathbb{Z}_l^\times\), \(\Phi_\alpha\) be the “norm-\(\alpha\)-part”, i.e., \(\Phi_\alpha = \{ \sigma \in \Phi \mid \text{Nr}(\sigma) = \alpha \}\).

Theorem. If \(\alpha \in \mathbb{Z}_l^\times\) generates \(\mathbb{Z}_l^\times\), then the set \(\Phi_\alpha\) contains infinitely many \(\Phi\)-conjugacy classes.

Remarks. 1) In [2], it is proved under the same assumption, that \(\Phi_\alpha\) contains at least two \(\Phi\)-conjugacy classes. (Corollary of Proposition 8, Ch. I.)

2) In [1], M. Asada and the author studied the “pro-\(l\) mapping class group” and obtained a result similar to 1).

2. Proof. Our method of proof is to consider the projection of \(\Phi\) to the group \(\overline{\Phi} = \text{Brd}(\mathbb{F}/\mathbb{F}^\prime)\), where \(\mathbb{F}^\prime = \mathbb{F} / (\mathbb{F}^\prime, \mathbb{F}^\prime)\), and we use the same symbols \(x, y, z\) for their classes mod \(\mathbb{F}^\prime\). By Theorem 3 in [2] Ch. II, the group \(\overline{\Phi}\) is explicitly realized as follows. Define the group \(\Theta\) by

\[
\Theta = \{ (\alpha, F) \mid \alpha \in \mathbb{Z}_l^\times, F \in \mathbb{A}_l^\times, F + uvw\mathbb{A} = \theta_a \}
\]

with the composition law \((\alpha, F)(\beta, G) = (\alpha \beta, F \cdot G^i)\), where \(\mathbb{A}_l = \mathbb{Z}_l[[u, v, w]]/(1 + u)(1 + v)(1 + w) - 1 \simeq \mathbb{Z}_l[[u, v]]\).

\(^{1)}\) This is a part of the master’s thesis of the author at the University of Tokyo (1985). He wishes to express his sincere gratitude to Professor Y. Ihara for his advice and encouragement.
\( \theta_* \) is certain class mod \( uvw \) determined by \( \alpha \), and \( i_* \) is a unique automorphism of the \( \mathbb{Z} \)-algebra \( A \) determined by
\[
(1 + u) \longrightarrow (1 + u)^*, \quad (1 + v) \longrightarrow (1 + v)^*, \quad (1 + w) \longrightarrow (1 + w)^*.
\]
Then, \( \varphi \cong \theta \) and \( \mathcal{F}_i \cong 1 + uvwA \). Here, for \( \alpha \in \mathbb{Z}_i^\times \), \( \varphi_* \) is the norm-\( \alpha \)-part. Henceforth, we identify \( \varphi \) (resp. \( \varphi_* \)) with \( \theta \) (resp. \( 1 + uvwA \)) by this isomorphism.

Now, we shall prove that if \( \alpha \) generates \( \mathbb{Z}_i^\times \), \( \varphi_* \) contains infinitely many \( \varphi \)-conjugacy classes.

We fix an element \((\alpha, F_\alpha) \in \varphi_*\). For any \((\alpha, H) \in \varphi_*\), write
\[
H = F_\alpha(1 + uvwH_0), \quad H_0 \in A.
\]
Since \( \alpha \) generates \( \mathbb{Z}_i^\times \), the centralizer of \((\alpha, H)\) in \( \varphi \) contains an element with arbitrary norm. Thus, in \( \varphi_* \), \( \varphi \)-conjugacy is equivalent to \( \varphi \)-conjugacy. Let
\[
G = 1 + uvwG_0 \in \varphi, \quad G_0 \in A.
\]
Then
\[
G^{-1}(\alpha, H)G = (\alpha, HG^{i_\alpha}G^{-i}) \in \varphi_*
\]
and
\[
HG^{i_\alpha}G^{-1} = F_\alpha(1 + uvwH_0)(1 + uvwG_0)^{i_\alpha}(1 + uvwG_0)^{-1}.
\]
If we write
\[
HG^{i_\alpha}G^{-1} = F_\alpha(1 + uvwJ), \quad J \in A,
\]
we get
\[
J \equiv H_0 + (uvw)^{i_\alpha}G_0^{i_\alpha} - G_0 \mod uvw.
\]
Now, identify \( \mathcal{A} \) with \( \mathbb{Z}_i[[u, v]] \) and write
\[
G_0 \mod u = b_0 + b_1v + b_2v^2 + \cdots, \quad b_i \in \mathbb{Z}_i (i \geq 0).
\]
We view \( b_i (i \geq 0) \) as variables over \( \mathbb{Z}_i \). Direct calculation shows that we can write
\[
(uvw)^{i_\alpha}G_0^{i_\alpha} - G_0 \mod u = \sum_{i=0}^\infty (\alpha^{i+1} - 1)b_i + Q_i(b_0, b_1, \cdots, b_{i-1})v^i
\]
where \( Q_i \) is a linear form determined alone by \( \alpha \) with coefficients in \( \mathbb{Z}_i \) in \( i \) variables. (Put \( Q_0 = 0 \).) For \((\alpha, H), (\alpha, H') \in \varphi_*\), write
\[
H = F_\alpha(1 + uvwH_0), \quad H' = F_\alpha(1 + uvwH_0'), \quad H_0, H_0' \in A,
\]
\[
H_0 \mod u = h_0 + h_1v + h_2v^2 + \cdots, \quad H_0' \mod u = h_0' + h_1'v + h_2'v^2 + \cdots, \quad h_i, h_i' \in \mathbb{Z}_i,
\]
\[
h(H) = (h_0, h_1, h_2, \cdots), \quad h(H') = (h_0', h_1', h_2', \cdots).
\]
Then by (1)--(5), if \((\alpha, H) \) and \((\alpha, H') \) are \( \varphi \)-conjugate to each other, there exist \( b_i \in \mathbb{Z}_i, i = 0, 1, 2, \cdots \), such that
\[
h_i = h_i' + (\alpha^{i+1} - 1)b_i + Q_i(b_0, b_1, \cdots, b_{i-1}) \quad \text{for all } i.
\]
In view of this, we shall define an equivalence relation in \( \mathbb{Z}_i^\sim = \{h = (h_0, h_1, h_2, \cdots) \mid \forall h_i \in \mathbb{Z}_i \} \). For \( h = (h_0, h_1, h_2, \cdots) \in \mathbb{Z}_i^\sim \) and \( i \geq 3 \), define an element \( R_i(h) \in Q_i \) inductively by
\[
R_i(h) = \frac{1}{\alpha^i - 1} (h_{i-3} - Q_{i-3}(R_3(h), R_4(h), \cdots, R_{i-1}(h))).
\]
It follows from (6) that, for \( h = (h_0, h_1, \cdots) \), \( h' = (h_0', h_1', \cdots) \in \mathbb{Z}_i^\sim \) corresponding to \( H_0, H_0' \),
\[
b_i = R_{i+3}(h) - R_{i+3}(h') \quad (i \geq 0).
\]
(Note that \( Q_i \) is a linear form.) Since \( \alpha \) generates \( \mathbb{Z}_i^\times \), \( \alpha^i - 1 \in \mathbb{Z}_i^\times \) unless
So, for any integer $k \geq 1$, define
\[ h \sim^{(k)} h' \text{ if and only if } R_{t+1}(h) - R_{t+1}(h') \in \mathbb{Z}_l \text{ for any } i \]
satisfying $1 \leq i \leq k$. 
This is an equivalence relation in $\mathbb{Z}_l^\infty$. We call its equivalence class $(k)$-equivalence class. Therefore $(\alpha, H) \sim (\alpha, H')$ ($\Psi_l$-conjugate to each other) implies $h(H) \sim^{(k)} h(H')$ for all $k \geq 1$.

We shall show that the number of $(k)$-equivalence classes in $\mathbb{Z}_l^\infty$ tends to infinity as $k \to \infty$. Let $k \geq 2$ and $l^r \| k$, i.e., $l^r$ is the exact power of $l$ dividing $k$. Then $(\alpha^{k(l-1)} - 1)\mathbb{Z}_l = l^{r+1}\mathbb{Z}_l$. We claim that a $(k-1)$-equivalence class consists of $l^{r+1}$ distinct $(k)$-equivalence classes. To see this, we fix a manner of $l^r$-adic expansion” of an element in $\mathbb{Q}_l$, i.e., for $a \in \mathbb{Q}_l$, we write $a = \sum_{i=-m}^{\infty} a_i l^i \in \mathbb{Q}_l$, $a_i \in \mathbb{Z}$, $0 \leq a_i \leq l-1$, $m \in \mathbb{Z}$. We define the “fractional part” $\{a\}$ of $a$ as $\sum_{i=-m}^{\infty} a_i l^i$. Then $h \sim^{(k)} h'$ is equivalent to
\[ \{R_{t+1}(h)\} = \{R_{t+1}(h')\} \] for all $i$, $1 \leq i \leq k$.

Put
\[ \tilde{R}_t(h) = \{R_{t+1}(h)\} \].

If $h$ runs through a $(k-1)$-equivalence class, $Q_{r(l-1)-1}(0, \ldots, 0, \tilde{R}_t(h), 0, \ldots, 0, \tilde{R}_{t+1}(h), 0, \ldots, 0, \tilde{R}_{t+2}(h), 0, \ldots, 0)$ is independent of $h$ and the sum of this element and $(\alpha^{k(l-1)} - 1)R_{t+1}(h)$ belongs to $\mathbb{Z}_l$. By the definition of $R_{k(l-1)}(h)$, we see easily that this sum takes every value mod $l^{r+1}(l^r \| k)$ as $h$ varying in a $(k-1)$-equivalence class. Therefore, a $(k-1)$-equivalence class consists of $l^{r+1}$ distinct $(k)$-equivalence classes and hence the number of $(k)$-equivalence class in $\mathbb{Z}_l^\infty$ tends to infinity as $k \to \infty$. By definition, the map $\Psi_a \ni (\alpha, H) \mapsto h(H) \in \mathbb{Z}_l^\infty$ is surjective. Therefore, we have shown that, if $\alpha \in \mathbb{Z}_l^\infty$ generates $\mathbb{Z}_l^\infty$, the set $\Psi_a$ contains infinitely many $\Psi_l$-conjugacy classes.

Next, we shall deduce the theorem from this. Let
\[ \Psi^- = \{ (\alpha, F) \in \Theta | F^\ell = \alpha(\ell uvw)^l \} \], \[ \Psi^- = \Psi^- \cap \Psi_a \] ($\alpha \in \mathbb{Z}_l^\infty$),
where $F^\ell = F^{l+1}$ for $F \in \mathbb{A}$. Let $\iota : \Phi \to \Psi$ be the natural map induced from $\text{Aut}(\mathbb{A}) \to \text{Aut}(\mathbb{A})$. Then, by Theorem 8 in [2] Ch. IV, the image of $\iota$ coincides with $\Psi^-$. So, it suffices to show that there are infinitely many elements in $\Psi_a$ which are not $\Psi_l$-conjugate to each other. We may choose our $(\alpha, F_a)$ from the minus part $\Psi_a^-$ of $\Psi_a$. Let $(\alpha, H) \in \Psi_a^-$ and write $H = F_a(1 + uvwH_0)$, $H_0 \in \mathbb{A}$. Then $1 + uvwH_0 \in \Psi^-$. It follows from this that $H_0 = \bar{H}_0 \mod u$. Conversely, for $H_0 \in \mathbb{A}$ satisfying $H_0 = \bar{H}_0 \mod u$, there exists $1 + uvwH_0 \in \Psi^-$ such that $H_0 = \bar{H}_0 \mod u$. This can be seen in the same way as in the proof of Proposition 1 (ii), Ch. III, [2]. Therefore, when $H$ runs through $\Psi_a^-$, i.e., $1 + uvwH_0$ runs through $\Psi^-$, $H_0 \mod u$ runs through every element satisfying $H_0 = \bar{H}_0 \mod u$. Now let
\[ H_0 \mod u = h_0 + h_1 v + h_2 v^2 + \cdots \]
The condition $H_0 = \bar{H}_0 \mod u$ is satisfied if and only if $h_{2i}, i = 0, 1, 2, \ldots$, are arbitrary and $h_{2i+1}, i = 0, 1, 2, \ldots$, are determined inductively by the relations
(9) \( h_1 = 0, \quad h_{2t+1} + tC_1 \cdot h_{2t} + tC_2 \cdot h_{2t-1} + \cdots + tC_{t-1} \cdot h_{t+2} + h_{t+1} = 0 \quad (i \geq 1). \)

This can be seen easily by expanding
\[
H_0 \mod u = h_0 - h_i v(1 - v + v^2 - \cdots) + h_2 v^2(1 - v + v^2 - \cdots)^2 - \cdots
\]
and comparing the coefficient of \( v^i \) for \( i = 0, 1, 2, \ldots \). So, to prove the theorem, it suffices to show that when \( h_0, h_1, h_2, \ldots \) vary freely in \( \mathbb{Z}_t \) and \( h_1, h_3, h_5, \ldots \), are determined by (9), the number of \((k)\)-equivalence classes to which \( h \) belongs tends to infinity as \( k \to \infty \). As before, this can be checked by a lengthy but straightforward calculation of the quantity
\[
(\alpha^{\ell(-1)} - 1)R_{\ell(-1)}(h)
+ Q_{\ell(-1)-3}(0, \ldots, 0, \bar{R}_4(h), 0, \ldots, 0, \bar{R}_2(h), 0, \ldots, 0, \bar{R}_{\ell-1}(h), 0, \ldots, 0) \mod \ell^{+1}.
\]

References
