77. 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 $\Phi \subset \mathrm{Out}\,\mathfrak{F}$ of the outer automorphism group of the free pro-l group $\mathfrak{F}$ of rank 2. There is a canonical representation $\varphi_Q : G_Q \to \Phi$ of the absolute Galois group $G_Q = \mathrm{Gal}(\bar{Q}/Q)$ which is unramified outside l, and for each prime $p \neq l$, the Frobenius of p determines a conjugacy class C_p of Φ 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 Φ_p contains *infinitely* many Φ-conjugacy classes, at least if p generates $Z_l^\times$ 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 Z_l, $Z_l^\times$ and 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 $\mathfrak{F} = \mathfrak{F}^{(2)}$ be the free pro-l group of rank 2 generated by x, y, z, $xyz = 1$, $\Phi = \mathrm{Brd}^{(2)}(\mathfrak{F}; x, y, z)$ be the pro-l braid group of degree 2, $\mathrm{Nr}(\sigma) \in Z_l^\times$ be the norm of $\sigma \in \Phi$, and for $\alpha \in Z_l^\times$, Φ_α be the "norm-α-part", i.e., $\Phi_\alpha = \{\sigma \in \Phi \mid \mathrm{Nr}(\sigma) = \alpha\}$.

Theorem. *If $\alpha \in Z_l^\times$ generates $Z_l^\times$, then the set Φ_α contains infinitely many Φ-conjugacy classes.*

Remarks. 1) In [2], it is proved under the same assumption, that Φ_α contains at least two Φ-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 Φ to the group $\Psi = \mathrm{Brd}^{(2)}(\mathfrak{F}/\mathfrak{F}''; x, y, z)$, where $\mathfrak{F}'' = [\mathfrak{F}', \mathfrak{F}']$, $\mathfrak{F}' = [\mathfrak{F}, \mathfrak{F}]$ and we use the same symbols x, y, z for their classes mod $\mathfrak{F}''$. By Theorem 3 in [2] Ch. II, the group Ψ is explicitly realized as follows. Define the group Θ by

$$\Theta = \{(\alpha, F) \mid \alpha \in Z_l^\times,\ F \in \mathcal{A}^\times,\ F + uvw\mathcal{A} = \theta_\alpha\}$$

with the composition law $(\alpha, F)(\beta, G) = (\alpha\beta, F \cdot G^{j_\alpha})$, where

$$\mathcal{A} = Z_l[[u, v, w]]/((1+u)(1+v)(1+w)-1) \simeq Z_l[[u, v]],$$

†) 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.

θ_α is certain class mod uvw determined by α, and j_α is a unique automorphism of the Z_l-algebra $\mathcal{A}$ determined by

$$(1+u)\longrightarrow(1+u)^\alpha,\quad (1+v)\longrightarrow(1+v)^\alpha,\quad (1+w)\longrightarrow(1+w)^\alpha.$$

Then, $\Psi\simeq\Theta$ and $\Psi_1\simeq 1+uvw\mathcal{A}$. Here, for $\alpha\in Z_l^\times$, Ψ_α is the norm-α-part. Henceforth, we identify Ψ(resp. Ψ_1) with Θ(resp. $1+uvw\mathcal{A}$) by this isomorphism.

Now, we shall prove that if α generates $Z_l^\times$, Ψ_α contains infinitely many Ψ-conjugacy classes.

We fix an element $(\alpha, F_\alpha)\in\Psi_\alpha$. For any $(\alpha, H)\in\Psi_\alpha$, write

$$H=F_\alpha(1+uvwH_0),\qquad H_0\in\mathcal{A}.$$

Since α generates $Z_l^\times$, the centralizer of (α, H) in Ψ contains an element with arbitrary norm. Thus, in Ψ_α, Ψ-conjugacy is equivalent to Ψ_1-conjugacy. Let

$$G=1+uvwG_0\in\Psi_1,\qquad G_0\in\mathcal{A}.$$

Then

(1) $$G^{-1}(\alpha, H)G=(\alpha, HG^{j_\alpha}G^{-1})\in\Psi_\alpha$$

and

(2) $$HG^{j_\alpha}G^{-1}=F_\alpha(1+uvwH_0)(1+uvwG_0)^{j_\alpha}(1+uvwG_0)^{-1}.$$

If we write

(3) $$HG^{j_\alpha}G^{-1}=F_\alpha(1+uvwJ),\qquad J\in\mathcal{A},$$

we get

(4) $$J\equiv H_0+(uvw)^{j_\alpha-1}G_0^{j_\alpha}-G_0 \qquad \mathrm{mod}\, uvw.$$

Now, identify $\mathcal{A}$ with $Z_l[[u, v]]$ and write

$$G_0 \,\mathrm{mod}\, u=b_0+b_1v+b_2v^2+\cdots,\qquad b_i\in Z_l\ (i\geq 0).$$

We view b_i $(i\geq 0)$ as variables over Z_l. Direct calculation shows that we can write

(5) $$(uvw)^{j_\alpha-1}G_0^{j_\alpha}-G_0 \,\mathrm{mod}\, u=\textstyle\sum_{i=0}^\infty\{(\alpha^{i+3}-1)b_i+Q_i(b_0, b_1, \cdots, b_{i-1})\}v^i$$

where Q_i is a linear form determined alone by α with coefficients in Z_l in i variables. (Put $Q_0=0$.) For (α, H), $(\alpha, H')\in\Psi_\alpha$, write

$$H=F_\alpha(1+uvwH_0),\quad H'=F_\alpha(1+uvwH_0'),\quad H_0, H_0'\in\mathcal{A},$$

$$H_0 \,\mathrm{mod}\, u=h_0+h_1v+h_2v^2+\cdots,\quad H_0' \,\mathrm{mod}\, u=h_0'+h_1'v+h_2'v^2+\cdots,\quad h_i, h_i'\in Z_l,$$

$$h(H)=(h_0, h_1, h_2, \cdots),\qquad h(H')=(h_0', h_1', h_2', \cdots).$$

Then by (1)–(5), if (α, H) and (α, H') are Ψ_1-conjugate to each other, there exist $b_i\in Z_l$, $i=0, 1, 2, \cdots$, such that

(6) $$h_i=h_i'+(\alpha^{i+3}-1)b_i+Q_i(b_0, b_1, \cdots, b_{i-1})\qquad \text{for all } i.$$

In view of this, we shall define an equivalence relation in $Z_l^\infty=\{h=(h_0, h_1, h_2, \cdots)\mid \forall h_i\in Z_l\}$. For $h=(h_0, h_1, h_2, \cdots)\in Z_l^\infty$ and $i\geq 3$, define an element $R_i(h)\in Q_l$ inductively by

(7) $$R_i(h)=\frac{1}{\alpha^i-1}\{h_{i-3}-Q_{i-3}(R_3(h), R_4(h), \cdots, R_{i-1}(h))\}.$$

It follows from (6) that, for $h=(h_0, h_1, \cdots)$, $h'=(h_0', h_1', \cdots)\in Z_l^\infty$ corresponding to H_0, H_0',

(8) $$b_i=R_{i+3}(h)-R_{i+3}(h')\qquad (i\geq 0).$$

(Note that Q_i is a linear form.) Since α generates $Z_l^\times$, $\alpha^i-1\in Z_l^\times$ unless

$l-1\,|\,i$. So, for any integer $k\geq 1$, define

$$h \overset{(k)}{\sim} h' \text{ if and only if } R_{i(l-1)}(h)-R_{i(l-1)}(h')\in \boldsymbol{Z}_l \text{ for any } i \text{ satisfying } \quad 1\leq i\leq k.$$

This is an equivalence relation in $\boldsymbol{Z}_l^\infty$. We call its equivalence class (k)-equivalence class. Therefore $(\alpha, H)\sim(\alpha, H')$ (Ψ_1-conjugate to each other) implies $h(H)\overset{(k)}{\sim}h(H')$ for all $k\geq 1$.

We shall show that the number of (k)-equivalence classes in $\boldsymbol{Z}_l^\infty$ tends to infinity as $k\to\infty$. Let $k\geq 2$ and $l^\nu\|k$, i.e., l^ν is the exact power of l dividing k. Then $(\alpha^{k(l-1)}-1)\boldsymbol{Z}_l=l^{\nu+1}\boldsymbol{Z}_l$. We claim that a $(k-1)$-equivalence class consists of $l^{\nu+1}$ distinct (k)-equivalence classes. To see this, we fix a manner of "l-adic expansion" of an element in $\boldsymbol{Q}_l$, i.e., for $a\in\boldsymbol{Q}_l$, we write $a=\sum_{i=-m}^{\infty}a_il^i\in\boldsymbol{Q}_l$, $a_i\in\boldsymbol{Z}$, $0\leq a_i\leq l-1$, $m\in\boldsymbol{Z}$. We define the "fractional part" $\{a\}$ of a as $\sum_{i=-m}^{-1}a_il^i$. Then $h\overset{(k)}{\sim}h'$ is equivalent to

$$\{R_{i(l-1)}(h)\}=\{R_{i(l-1)}(h')\} \quad \text{for all } i,\quad 1\leq i\leq k.$$

Put

$$\tilde{R}_i(h)=\{R_{i(l-1)}(h)\}.$$

If h runs through a $(k-1)$-equivalence class, $Q_{k(l-1)-3}(0,\cdots,0,\tilde{R}_1(h),0,\cdots,0,\tilde{R}_2(h),0,\cdots,0,\tilde{R}_{k-1}(h),0,\cdots,0)$ is independent of h and the sum of this element and $(\alpha^{k(l-1)}-1)R_{k(l-1)}(h)$ belongs to $\boldsymbol{Z}_l$. By the definition of $R_{k(l-1)}(h)$, we see easily that this sum takes every value mod $l^{\nu+1}$ ($l^\nu\|k$) as h varying in a $(k-1)$-equivalence class. Therefore, a $(k-1)$-equivalence class consists of $l^{\nu+1}$ distinct (k)-equivalence classes and hence the number of (k)-equivalence class in $\boldsymbol{Z}_l^\infty$ tends to infinity as $k\to\infty$. By definition, the map $\Psi_\alpha\ni(\alpha,H)\to h(H)\in\boldsymbol{Z}_l^\infty$ is surjective. Therefore, we have shown that, if $\alpha\in\boldsymbol{Z}_l^\times$ generates $\boldsymbol{Z}_l^\times$, the set Ψ_α contains infinitely many Ψ-conjugacy classes.

Next, we shall deduce the theorem from this. Let

$$\Psi^-=\{(\alpha,F)\in\Theta\,|\,F\bar{F}=\alpha(uvw)^{j_\alpha-1}\},\quad \Psi_\alpha^-=\Psi^-\cap\Psi_\alpha\quad(\alpha\in\boldsymbol{Z}_l^\times),$$

where $\bar{F}=F^{j_{-1}}$ for $F\in\mathcal{A}$. Let $\gamma:\Phi\to\Psi$ be the natural map induced from $\mathrm{Aut}\,\mathfrak{F}\to\mathrm{Aut}\,(\mathfrak{F}/\mathfrak{F}'')$. Then, by Theorem 8 in [2] Ch. IV, the image of γ coincides with Ψ^-. So, it suffices to show that there are infinitely many elements in Ψ_α^- which are not Ψ_1-conjugate to each other. We may choose our (α,F_α) from the minus part Ψ_α^- of Ψ_α. Let $(\alpha,H)\in\Psi_\alpha^-$ and write $H=F_\alpha(1+uvwH_0)$, $H_0\in\mathcal{A}$. Then $1+uvwH_0\in\Psi_1^-$. It follows from this that $H_0\equiv\bar{H}_0 \bmod u$. Conversely, for $H_0\in\mathcal{A}$ satisfying $H_0\equiv\bar{H}_0\bmod u$, there exists $1+uvwH_0'\in\Psi_1^-$ such that $H_0'\equiv H_0\bmod u$. This can be seen in the same way as in the proof of Proposition 1 (ii), Ch. III, [2]. Therefore, when H runs through Ψ_α^-, i.e., $1+uvwH_0$ runs through Ψ_1^-, $H_0 \bmod u$ runs through every element satisfying $H_0\equiv\bar{H}_0\bmod u$. Now let

$$H_0 \bmod u=h_0+h_1v+h_2v^2+\cdots.$$

The condition $H_0\equiv\bar{H}_0\bmod u$ is satisfied if and only if h_{2i}, $i=0,1,2,\cdots$, are arbitrary and h_{2i+1}, $i=0,1,2,\cdots$, are determined inductively by the relations

(9) $\quad h_1=0, \quad h_{2i+1}+{}_iC_1\cdot h_{2i}+{}_iC_2\cdot h_{2i-1}+\cdots+{}_iC_{i-1}\cdot h_{i+2}+h_{i+1}=0 \quad (i\geq 1).$

This can be seen easily by expanding

$$\overline{H}_0 \bmod u = h_0 - h_1 v(1-v+v^2-\cdots)+h_2 v^2(1-v+v^2-\cdots)^2-\cdots$$

and comparing the coefficient of v^i for $i=0,1,2,\cdots$. So, to prove the theorem, it suffices to show that when $h_0, h_2, h_4, \cdots$, vary freely in $\boldsymbol{Z}_l$ and $h_1, h_3, h_5, \cdots$, 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

$$(\alpha^{k(l-1)}-1)R_{k(l-1)}(h) + Q_{k(l-1)-3}(0,\cdots,0,\tilde{R}_1(h),0,\cdots,0,\tilde{R}_2(h),0,\cdots,0, \tilde{R}_{k-1}(h),0,\cdots,0) \bmod l^{\nu+1}.$$

References

[1] M. Asada and M. Kaneko: On the automorphism group of some pro-l fundamental group (to appear in Advanced Studies in Pure Math.).

[2] Y. Ihara: Profinite braid groups, Galois representations and complex multiplications. Ann. of Math., **123**, 43–106 (1986).