数理解析研究所講究録
第 884 巻 1994 年 105-111

Coverings of $\mathbb{P}^1 - \{0,1,\infty\}$ with restricted "vertical" ramifications.[1]

Yasutaka Ihara
RIMS, Kyoto University

Let S be any set of prime numbers, and put

$$\mathbb{Z}_S = \mathbb{Z}[\tfrac{1}{p};\ p \in S],$$

$\mathbb{Q}_S$: the maximal Galois extension over $\mathbb{Q}$ unramified outside $S \cup (\infty)$

So, $\pi_1(\mathrm{Spec}\,\mathbb{Z}_S) = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$. We propose to study the action of this group on

$$\pi_1^{\langle S\rangle} := \mathrm{Ker}\left(\pi_1(\mathbb{P}^1 - \{0,1,\infty\}/\mathbb{Z}_S) \to \pi_1(\mathrm{Spec}\,\mathbb{Z}_S)\right),$$

where

$$\mathbb{P}^1 - \{0,1,\infty\}/\mathbb{Z}_S = \mathrm{Spec}\,\mathbb{Z}_S[t,\ 1/t,\ 1/(1-t)] \qquad (t\text{: a variable}).$$

In terms of Galois theory of function fields, $\pi_1^{\langle S\rangle} = \mathrm{Gal}(M_S/\mathbb{Q}_S(t))$, where:

$$\begin{tikzcd}
 & & M & \cdots\ \text{max } \mathrm{Gal}/\bar{\mathbb{Q}}(t) \text{ unram. outside } t=0,1,\infty \\
 & M_S \arrow[r, dash] \arrow[d, dash, "\pi_1^{\langle S\rangle}"'] & \bar{\mathbb{Q}}\cdot M_S \arrow[u, dash] \arrow[d, dash] & \cdots\ \text{max } \mathrm{Gal}/\mathbb{Q}(t) \text{ in } M \text{ in which } v_\ell\ (\ell \notin S) \text{ are all unramified.} \\
\mathbb{Q}(t) \arrow[r, dash] & \mathbb{Q}_S(t) \arrow[r, dash] & \bar{\mathbb{Q}}(t) &
\end{tikzcd}$$

Here, v_ℓ is the unique extension of the ℓ-adic valuation of $\mathbb{Q}$ to $\mathbb{Q}(t)$ such that ℓ is a prime element and the residue class of t is transcendental over $\mathbb{F}_\ell$.

---

1) Although the titles are not the same, this is a resumé of my talk at the conference on March 28, 94.

We have the following two short exact sequences

$$(*) \qquad 1 \to \mathrm{Gal}(M/\bar{\mathbb{Q}} M_S) \to \underset{\substack{\| \\ \hat{F}_2 \ \left(\substack{\text{free profinite} \\ \text{rank } 2}\right)}}{\mathrm{Gal}(M/\bar{\mathbb{Q}}(t))} \to \underset{\substack{\| \\ \pi_1^{\langle S\rangle}}}{\mathrm{Gal}(M_S/\bar{\mathbb{Q}}_S(t))} \to 1,$$

$$(**) \qquad 1 \to \pi_1^{\langle S\rangle} \to \mathrm{Gal}(M_S/\mathbb{Q}(t)) \to \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}) \to 1.$$

The most basic question is, perhaps, whether $(**)$ is useful in the (future) study of $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$. I cannot say anything about this now. Here, I state some results of my "first thought" related to $(*)$, $(**)$.

<u>Terminology</u>: "S-number": integers whose prime factors all belong to S;
"S-group": finite group whose order is an S-number;
"pro-S group": proj. limit of S-groups ($|S|=1 \Rightarrow$ pronilpotent, $|S|=2 \Rightarrow$ prosolvable).
$F_2^{\text{pro-}S}$: the pro-S completion of the free group of rank 2, i.e., the projective limit of all finite S-groups appearing as quotients of F_2.

Statement of results :

(i) Ramification indices of $t=0,1,\infty$ in any finite subextensions of $M_S/\mathbb{Q}_S(t)$ are S-numbers.[2)]

(ii) For any open subgroup $H \subset \pi_1^{\langle S\rangle}$, its abelianization H^{ab} is a direct product of a pro-S group and a finite group.

These two are saying that $\pi_1^{\langle S\rangle}$, as a quotient of $\hat{F}_2$, is not so big. The next (iii) says something to the opposite direction.

(iii) $\mathrm{Gal}(M/\bar{\mathbb{Q}} M_S)$, the kernel in $(*)$, contains no non-trivial S-group as its quotient. In particular, $\hat{F}_2 \to F_2^{\text{pro-}S}$ factors through $\pi_1^{\langle S\rangle}$, as $\hat{F}_2 \to \pi_1^{\langle S\rangle} \to F_2^{\text{pro-}S}$ (both $\to$ are surjective).

About the exact sequence $(**)$,

(iv) The standard Puiseux embedding $M \hookrightarrow \bar{\mathbb{Q}}\{\{t\}\} = \bigcup_{N\geq 1} \bar{\mathbb{Q}}((t^{1/N}))$ induces $M_S \hookrightarrow \mathbb{Q}_S\{\{t\}\}$, and M_S is stable under the coefficientwise $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$-action on $\mathbb{Q}_S\{\{t\}\}$. This $\mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$-action on $M_S/\mathbb{Q}(t)$ gives a "nice" splitting of $(**)$

Remarks If $S=\phi$, then $\mathbb{Q}_S=\mathbb{Q}$, $M_S=\mathbb{Q}(t)$ and $\pi_1^{\langle S\rangle}=\{1\}$.
When $S=\{p\}$, I do not know whether $\pi_1^{\langle p\rangle} \xrightarrow{\sim} F_2^{\text{pro-}p}$ or not.
When $S=\{2,p\}$ $(p\neq 2)$, $\pi_1^{\langle S\rangle}$ is not a pro-S group.
When $S=\{\text{all primes}\}$, then $\mathbb{Q}_S=\bar{\mathbb{Q}}$, $M_S=M$ and $\pi_1^{\langle S\rangle}=\hat{F}_2$.

---

2) This property depends on the choice of three points on $\mathbb{P}^1$; $t=0,1,\infty$. If they were, e.g., $t=0,12^3,\infty$, then this property would not hold (unless $S\ni 2,3$)

Main ingredients for proofs.

(i) As T. Saito noted, (i) is obtained directly from the generalized Abhyankar lemma ([SGA 1] Exp XIII).

(ii) This proof relies on a result of Coleman [Co]. More precisely, it is reduced to the following statement which is (essentially) in [Co]:

Let A be an abelian variety over a number field k, and S be any set of primes of k. Assume A has good reduction outside S. For each positive integer n with $(n, S) = 1$, let $A[n]$ denote the group of all n-torsion points of $A(\bar{k})$, and $K[n]$ be its subgroup generated by the kernel of reduction mod v in $A[n]$, where v runs over all prime divisors of the field $k(A[n])$ dividing n. Then the order of $A[n]/K[n]$ is bounded by a positive number which depends only on A and k (in fact, only on $A \otimes \bar{\mathbb{Q}}$).

(iii) The proof relies on standard arguments of Grothendieck's ([SGA 1]) on descent of etale coverings; the only additional points to be checked are:

(a) For any finite subextension $L/\mathbb{Q}_S(t)$ in M_S, the integral closure of $\mathbb{P}^1/\mathbb{Z}_S$ in L is regular outside S (including points above $t = 0, 1, \infty$ as long as they are not above S).

(b) The pro-S completion of the fundamental group of a compact Riemann surface of genus > 1 has trivial center.

The assertion (a) can be checked easily, while (b) is proved in [Na].

(iv) The point is to prove the $\mathbb{Q}_S$-rationality of places of M_S above $t \to 0, 1, \infty$. This follows by using the purity of branch loci on suitable Fermat curves whose exponents are S-numbers.

<u>Some open problems:</u>

(Problem I) Characterize $\pi_1^{\langle S \rangle}$ as quotient of $\hat{F}_2$.

Related questions:

(Q1) Is $\pi_1^{\langle S \rangle}$ the biggest quotient of $\hat{F}_2$ on which $Gal(\bar{\mathbb{Q}}/\mathbb{Q}_S)$ acts trivially?

(Q2) Is the center of $\pi_1^{\langle S \rangle}$ trivial?

(Q3) In connection with the result (ii), let H_0^{ab} denote the coprime-to-S part of the torsion subgroup of H^{ab}. Then what can one say about the group $\varprojlim_H H_0^{ab}$?

(Problem II) Is the homomorphism

$$\varphi_S : \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}) \to \mathrm{Aut}\ \pi_1^{\langle S\rangle}$$

(defined by the splitting (iv) of the exact sequence (**)) <u>injective</u> ?

When $S = \{\text{all primes}\}$, φ_S is injective by the wellknown injectivity of Bolyi for the Galois representation $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Out}\ \hat{\pi}_1(\mathbb{P}^1 - \{0,1,\infty\}/\bar{\mathbb{Q}})$. I do not know at present whether φ_S is injective in any other cases, e.g. even when $S = \{\text{all primes}\} - \{p\}$.

In general, let $\mathbb{Q}_S^*$ $(\mathbb{Q} \subset \mathbb{Q}_S^* \subset \mathbb{Q}_S)$ denote the field corresponding to the kernel of φ_S. What we know about $\mathbb{Q}_S^*$:

(*) $\mathbb{Q}_S^*$ contains all higher circular S-units (the obvious generalization of higher circular l-units in [A-I]).

(**) Let $n \geq 1$, and $S = S_n = \{p;\ p \text{ divides } n(n-1)\}$. Assume $\pi_1^{\langle S\rangle}$ is center-free. Then $\mathbb{Q}_S^*$ contains the splitting field of the equation $x^{n-2} + 2x^{n-3} + 3x^{n-4} + \cdots + (n-1) = 0$.

References :

[A-I] G. Anderson – Y. Ihara ; Pro-ℓ branched coverings of $\mathbb{P}^1$ and higher circular ℓ-units ; Ann of Math 128 (1988), 271-293.

[Co] R. Coleman ; A remark on kernels of reduction ; Proc AMS 104 (1988) 699–701.

[Na] H. Nakamura ; Galois rigidity of pure sphere braid groups and profinite calculus ; J. Math. Sci ; the Univ of Tokyo 1 (1994), in press.

[SGA 1] A. Grothendieck ; Revêtements étales et groupe fondamental, SLN 224.