J. Math. Soc. Japan
Vol. 68, No. 3 (2016) pp. 1189–1218
doi: 10.2969/jmsj/06831189

Non-constant Teichmüller level structures and an application to the Inverse Galois Problem

By Kenji Sakugawa

(Received Aug. 17, 2012)
(Revised Nov. 20, 2014)

Abstract. In this paper, we generalize the Hurwitz space which is defined by Fried and Völklein by replacing constant Teichmüller level structures with non-constant Teichmüller level structures defined by finite étale group schemes. As an application, we give some examples of projective general symplectic groups over finite fields which occur as quotients of the absolute Galois group of the field of rational numbers $\mathbb{Q}$.

1. Introduction.

A famous open problem in Number theory called the Inverse Galois Problem is as follows.

Question 1.1 (IGP). Does every finite group occur as the Galois group of a finite Galois extension over the field of rational numbers $\mathbb{Q}$?

For a field k, we say that *IGP holds for* k when any finite group appears as a quotient of the absolute Galois group $G_k := \mathrm{Gal}(\bar{k}/k)$ of k. In this paper, we give some examples of finite groups which appear as quotients of $G_{\mathbb{Q}}$.

The following proposition is an immediate consequence of Hilbert's irreducibility theorem (cf. [**Vö**, Corollary 1.11, Theorem 1.23]).

Proposition 1.2 ([**Vö**, Theorem 1.13]). *Let F be a finite extension of $\mathbb{Q}$ or the maximal abelian extension of $\mathbb{Q}$. Then, IGP holds for F if IGP holds for $F(t)$.*

We remark that the category of finite Galois extensions of $F(t)$ is equivalent to the category of finite étale Galois coverings of the projective line $\mathbb{P}^1_F$ minus finitely many closed points. The advantage of considering IGP for $F(t)$ instead of IGP for F is that IGP for $F(t)$ admits a geometric approach for us. Let G be a finite group and r a positive integer. In the paper [**Fr-Vö**], Fried and Völklein considered the following set of equivalence classes:

$$\mathcal{H}_r^{\mathrm{in}}(G)(\mathbb{C}) := \{G\text{-coverings over } \mathbb{P}^1_{\mathbb{C}} \text{ ramified at exactly } r\text{-points on } \mathbb{P}^1_{\mathbb{C}}\}/\sim .$$

Here, we say that two coverings $f : X \to \mathbb{P}^1_{\mathbb{C}}$ and $g : Y \to \mathbb{P}^1_{\mathbb{C}}$ are equivalent if there exists

2010 *Mathematics Subject Classification.* Primary 12F12; Secondary 14D23.
Key Words and Phrases. Inverse Galois Problem, Hurwitz space, Hurwitz stack, Teichmüller level structure.

an isomorphism from X to Y over $\mathbb{P}^1_{\mathbb{C}}$. Fried and Völklein showed the following theorem.

PROPOSITION 1.3 (*cf.* [**Fr-Vö**, Theorem 1]). *Let G and r be as above. Then, there exists an algebraic variety $\mathcal{H}^{\mathrm{in}}_r(G)$ over $\mathbb{Q}$ whose $\mathbb{C}$-valued points are canonically identified with $\mathcal{H}^{\mathrm{in}}_r(G)(\mathbb{C})$. If the set of $\mathbb{Q}$-rational points of $\mathcal{H}^{\mathrm{in}}_r(G)$ is non-empty, there exists a geometrically connected $G/Z(G)$-covering over $\mathbb{P}^1_{\mathbb{Q}}$, where $Z(G)$ is the center of G. In particular, $G/Z(G)$ appears as a quotient of the absolute Galois group $G_{\mathbb{Q}}$ of $\mathbb{Q}$.*

The algebraic variety $\mathcal{H}^{\mathrm{in}}_r(G)$, which is not necessarily geometrically connected, is called the *Hurwitz space*. The important fact is that we have a group theoretic criterion for the existence of a $\mathbb{Q}$-rational point of $\mathcal{H}^{\mathrm{in}}_r(G)$. Let $\mathcal{C} = (C_1, \ldots, C_r)$ be an r-tuple of conjugacy classes of G. Put

$$\mathcal{E}^{\mathrm{in}}(\mathcal{C}) := \{(g_1, \ldots, g_r) \in G^r \mid g_i \in C_i,\ g_1 \cdots g_r = 1,\ \langle g_1, \ldots, g_r \rangle = G\}/\mathrm{Inn}(G).$$

The set $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ has an action of the pure braid group B_r and an action of $\mathrm{Aut}(G)$ (cf. Subsection 3.1). In [**M-M**], Malle and Matzat defined the j-th *braiding orbit genus* $g_j([g]) \in \mathbb{Z}_{\geq 0}$ for any $[g] \in \mathcal{E}^{\mathrm{in}}(\mathcal{C})$ and for any $1 \leq j \leq r-1$. We say that $\mathcal{C}$ is *braiding rigid* if B_r acts on $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ transitively.

PROPOSITION 1.4 (*cf.* [**M-M**, Chapter III, Theorem 5.7, Corollary 5.8]). *Assume that the following conditions are satisfied*:

(a) *The tuple $\mathcal{C}$ is braiding rigid. Moreover, for any $[g] \in \mathcal{E}^{\mathrm{in}}(\mathcal{C})$ and for any $1 \leq j \leq r-1$, we have $g_j([g]) = 0$ and the oddness condition (O_j) in the sense of* [**M-M**, p. 213] *holds for $[g]$ (see Definition* 3.20 *for the definition of the oddness condition).*
(b) *The tuple $\mathcal{C}$ is rational in the sense of* [**M-M**, p. 28] (*see Definition* 3.15 *the definition of rational tuples of conjugacy classes*).

Then, the Hurwitz space $\mathcal{H}^{\mathrm{in}}_r(G)$ contains a rational variety over $\mathbb{Q}$. In particular, $\mathcal{H}^{\mathrm{in}}_r(G)(\mathbb{Q})$ is non-empty, and $G/Z(G)$ appears as a quotient of $G_{\mathbb{Q}}$.

The Hurwitz space is generalized to the Hurwitz stack by Bertin, Wewers, Romagny and many other people (e.g. [**B-R**], [**M**], [**R**], [**We**]). In the paper [**R**], Romagny studied a relation between the Hurwitz stack and the moduli stack of stable curves with Teichmüller level structures. Recall that a Teichmüller level structure of a proper smooth curve X over a connected scheme S is an exterior surjection from the étale fundamental group $\pi_1^{\text{ét}}(X/S)$ to a finite group G (cf. [**D-M**, p. 106]). The new viewpoint of this paper is to replace a finite group G with a finite étale group scheme $\mathcal{G}$ over a scheme S. We define the Hurwitz stack as the classifying stack of $\mathcal{G}$-torsors over the projective line minus r-points. Note that our definition of the Hurwitz stack is slightly different from the definition of [**B-R**], [**R**] (cf. Remark 2.10) and we only treat the case of genus 0. Thanks to the new definition of the Hurwitz stack, we obtain the following group theoretic criterion for IGP:

MAIN THEOREM (Theorem 3.23). *Let G be a finite group such that the center of $\overline{G} := G/Z(G)$ is trivial. Assume that there exist a positive integer r, an r-tuple of conjugacy classes $\mathcal{C}$ of G, and a subgroup H of* $\mathrm{Aut}(G)$ *satisfying the following conditions*:

(a) *The tuple* $\mathcal{C}$ *is braiding rigid. Moreover, for any* $[g] \in \mathcal{E}^{\mathrm{in}}(\mathcal{C})$ *and for any* $1 \leq j \leq r-1$, *we have* $g_j([g]) = 0$ *and the oddness condition* (O_j) *holds for* $[g]$.
(b) *There exists a subgroup* V *of the symmetric group* S_r *such that the group* $H \times B_{r,V}$ *acts on* $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*) := \bigcup_{n \in (\mathbb{Z}/\sharp G\mathbb{Z})^\times} \mathcal{E}^{\mathrm{in}}(\mathcal{C}^n)$ *transitively* (*see Subsection* 3.1 *for the definition of* $B_{r,V}$).
(c) *The group* H *is isomorphic to* $(\mathbb{Z}/f\mathbb{Z}) \rtimes (\mathbb{Z}/f\mathbb{Z})^\times$ *for some odd positive integer* f *and the action of* H *on* $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)$ *factors through* $H \twoheadrightarrow (\mathbb{Z}/f\mathbb{Z})^\times \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$.
(d) *The* r*-tuple of conjugacy classes* $\mathcal{C}$ *is* not V*-symmetric* (*see Definition* 3.15 *for the definition of* V*-symmetric* r*-tuples*).

Let $\overline{G}'$ *be the subgroup of* $\mathrm{Aut}(\overline{G})$ *generated by* $\overline{G} = \mathrm{Inn}(\overline{G})$ *and the image of* H *in* $\mathrm{Aut}(\overline{G})$. *Then,* $\overline{G}'$ *appears as a quotient of the absolute Galois group* $G_{\mathbb{Q}}$ *of* $\mathbb{Q}$.

Finally, we explain an application of Main theorem to IGP. Let p be an odd prime and n a positive integer. Let $\mathbb{F}_p$ be a finite field of order p. We put $r := 2n+2$. Let $\mathcal{F}_r$ be the free group of rank r, and $\mathrm{Rep}_{\mathbb{F}_p}(\mathcal{F}_r)$ the category of linear representations of $\mathcal{F}_r$ on finite dimensional $\mathbb{F}_p$-vector spaces. Let $\{\sigma_1^{(r)}, \ldots, \sigma_r^{(r)}\}$ be a set of generators of $\mathcal{F}_r$. We will construct an object (W, ρ') of $\mathrm{Rep}_{\mathbb{F}_p}(\mathcal{F}_r)$ and a subgroup H of $\mathrm{Aut}(\mathrm{Im}(\rho'))$ satisfying the following conditions:

- W is an $\mathbb{F}_p$-vector space of dimension $2n$.
- The image of ρ' is isomorphic to $Sp_{2n}(\mathbb{F}_p)$.
- We put $g_i := \rho'(\sigma_i^{(r)})$. We denote by C_i the conjugacy class of $\mathrm{Im}(\rho') \cong Sp_{2n}(\mathbb{F}_p)$ containing g_i. Then, the triple $(G := \mathrm{Im}(\rho), H, \mathcal{C} := (C_1, \ldots, C_r))$ satisfies whole conditions of Main theorem.

For the triple $(G, H, \mathcal{C})$ as above, the group $\overline{G}'$ in Main theorem is isomorphic to the projective general symplectic group $PGSp_{2n}(\mathbb{F}_p)$. By applying Main theorem, we obtain the following corollary:

Corollary 1.5 (Proposition 4.20). *Let* p *be an odd prime and* n *a positive integer greater than* 1. *Then, the projective general symplectic group* $PGSp_{2n}(\mathbb{F}_p)$ *appears as a quotient of the absolute Galois group* $G_{\mathbb{Q}}$ *of* $\mathbb{Q}$.

Keys of an application to the Inverse Galois Problem are Proposition 4.18 and Lemma 4.19. When a power q of p is not a prime, the assertion of Proposition 4.18 does not hold in general and we do not know how to generalize Lemma 4.19 to $\mathbb{F}_q$. Therefore, we do not generalize Corollary 1.5 to general finite field $\mathbb{F}_q$ of characteristic p.

We give some remarks on previously known results on the Inverse Galois Problem. According to [**M-M**, Chapter II, Theorem 7.2], if $p \not\equiv \pm 1 \pmod{24}$ and $p \nmid n$, then $PSp_{2n}(\mathbb{F}_p)$ appears as a quotient of $G_{\mathbb{Q}}$. On the other hand, Hall proved the following theorem in [**H**]: For any positive integer n, there exists a constant l_0 such that $GSp_{2n}(\mathbb{F}_p)$ appears as a quotient of $G_{\mathbb{Q}}$ if $p > l_0$. For small n, the constant l_0 was calculated explicitly (e.g. $n = 2$ in [**A-V**], $n = 3$ in [**AAKMTV**]). It seems that the results of this paper do not belong to the results of these types.

The main tool of the construction of (W, ρ') is the theory of middle convolution functors $\{\mathrm{MC}_\lambda^{(r)}\}_{\lambda \in \mathbb{F}_p^\times}$ developed by Dettweiler and Reiter ([**D-R**]). The middle convolution

$\mathrm{MC}_{\lambda}^{(r)}$ is a functor from the category $\mathrm{Rep}_{\mathbb{F}_p}(\mathcal{F}_r)$ to itself. We start from certain one dimensional representation (V, ρ) such that the image of ρ is contained in an orthogonal group. Then, for $(W, \rho') := \mathrm{MC}_{-1}^{(r)}(V, \rho)$, the image of ρ' is contained in a symplectic group (cf. Lemma 4.8). Finally, we check the conditions of Main theorem by using properties of middle convolution functors.

The plan of the paper is as follows:

PLAN. In Subsection 2.1, we define Teichmüller level structures of proper smooth curves and define the moduli stack of Teichmüller level structures on the projective line minus simple divisors. In Subsection 2.2, we introduce the Hurwitz stack. Then, in Subsection 2.3, we discuss the relation between the above two stacks and the Inverse Galois Problem.

Subsection 3.1 is a summary on braid groups. In Subsection 3.2, we give a description of the coarse moduli scheme of the Hurwitz stack. Then, in Subsection 3.2, we prove Main theorem.

We recall middle convolution functors in Subsection 4.1. We recall the notion of the linearly rigidity in Subsection 4.2. In Subsection 4.3, we give some group theoretic lemmata. Then, in the final subsection, we give a proof of Corollary 1.5.

NOTATION. For a set S, we denote the order of S by $\sharp S$. Let $s_1, \ldots, s_r$ be elements of a set S. Then, we denote by $(s_1, \ldots, s_r)$ (resp. $\{s_1, \ldots, s_r\}$) the ordered set (resp. the unordered set) consisting of $s_1, \ldots, s_r$. For a group G and an element g of G, we denote the conjugacy class of G containing g by $O_G(g)$. For a positive integer n, we denote the identity matrix of size n by E_n. For a perfect field k, we fix an algebraic closure $\overline{k}$ of k and denote the absolute Galois group $\mathrm{Gal}(\overline{k}/k)$ of k by G_k. In this paper, we always regard $\overline{\mathbb{Q}}$ as a subfield of $\mathbb{C}$.

ACKNOWLEDGMENTS. The author would like to thank Professor Tadashi Ochiai for reading this paper carefully and valuable discussions. Also, the author would like to thank Professor Tetsushi Ito for some useful suggestions and comments on the whole of this paper.

2. Teichmüller level structures and Hurwitz stacks.

In this section, we introduce Teichmüller level structures and the classifying stack of Teichmüller level structures on the projective line minus simple divisors. Next, we define the Hurwitz stack. Then, we study a relation between these two stacks.

2.1. Teichmüller level structures.

Let S be a connected scheme and $\mathbb{P}$ a set of primes containing all residue characteristics of S. Let $(\mathrm{l.c.gr}^{\mathbb{P}}/S)$ be the category of finite étale group schemes over S whose orders of geometric fibers are prime to all elements of $\mathbb{P}$. Note that the objects of $(\mathrm{l.c.gr}^{\mathbb{P}}/S)$ are not necessarily commutative group schemes over S. First, we recall the definition of exterior homomorphisms.

DEFINITION 2.1 ([**D-M**, p. 106]). Let $\mathcal{G}$ and $\mathcal{H}$ be objects of $(\mathrm{l.c.gr}^{\mathbb{P}}/S)$. The

set $\mathrm{Hom}^{\mathrm{ext}}_{\mathrm{l.c.gr}^{\mathbb{P}}}(\mathcal{H},\mathcal{G})$ is the quotient of the set of homomorphisms $\mathrm{Hom}_{\mathrm{l.c.gr}^{\mathbb{P}}}(\mathcal{H},\mathcal{G})$ by the action of $\mathcal{H}$ induced by its action on itself by inner automorphisms. An *exterior homomorphism* from $\mathcal{H}$ to $\mathcal{G}$ is an element of $\mathrm{Hom}^{\mathrm{ext}}_{\mathrm{l.c.gr}^{\mathbb{P}}}(\mathcal{H},\mathcal{G})$. An *exterior surjection* from $\mathcal{H}$ to $\mathcal{G}$ is an exterior homomorphism whose representatives are surjections. We denote the set of exterior surjections from $\mathcal{H}$ to $\mathcal{G}$ by $\mathrm{Surj}^{\mathrm{ext}}(\mathcal{H},\mathcal{G})$.

Let $\overline{X} \to S$ be a proper smooth curve whose geometric fibers are connected and $D \hookrightarrow \overline{X}$ a relative normal crossing divisor over S. Let $s : S \to \overline{X} \setminus D =: X$ be a section of the structure morphism of X. As in [**D-M**, Section 5.5], we construct the pro-object $\pi_1((\overline{X},D)/S,s)^{\mathbb{P}}$ of $(\mathrm{l.c.gr}^{\mathbb{P}}/S)$ satisfying the following conditions (cf. [**SGA1**, Exposé 13]):

(1) The set of exterior surjections $\mathrm{Hom}^{\mathrm{ext}}_{\mathrm{l.c.gr}^{\mathbb{P}}}(\pi_1((\overline{X},D)/S,s)^{\mathbb{P}},\ \mathcal{G})$ is equal to the set of global sections of the étale sheaf $R^1f_*(\mathrm{Ker}(f^*\mathcal{G} \to s_*\mathcal{G}))$ for any object $\mathcal{G}$ of $(\mathrm{l.c.gr}^{\mathbb{P}}/S)$ (cf. [**D-M**, Section 5.5, (i)]). Here, $f : X \to S$ is the structure morphism of X.
(2) The formation of $\pi_1((\overline{X},D)/S,s)^{\mathbb{P}}$ is compatible with any base change.

Note that the set $\mathrm{Hom}^{\mathrm{ext}}_{\mathrm{l.c.gr}^{\mathbb{P}}}(\pi_1((\overline{X},D)/S,s)^{\mathbb{P}},\mathcal{G})$ is independent of the choice of the section s. Since a section $s : S \to X$ of f exists étale locally on S, we can define the étale sheaves $\underline{\mathrm{Hom}}^{\mathrm{ext}}(\pi_1((\overline{X},D)/S)^{\mathbb{P}},\mathcal{G})$ and $\underline{\mathrm{Surj}}^{\mathrm{ext}}(\pi_1((\overline{X},D)/S)^{\mathbb{P}},\mathcal{G})$ on S. We give the definition of Teichmüller level structures on smooth curves which is a generalization of the definition in [**D-M**, Definition 5.6].

Definition 2.2. Let $\mathcal{G}$ be an object of $(\mathrm{l.c.gr}^{\mathbb{P}}/S)$. A *Teichmüller structure of level* $\mathcal{G}$ on $(D \hookrightarrow X/S)$ is a global section of the étale sheaf $\underline{\mathrm{Surj}}^{\mathrm{ext}}(\pi_1((\overline{X},D)/S)^{\mathbb{P}},\mathcal{G})$.

If the group scheme $\mathcal{G}$ is a constant group scheme G, then the definition of Teichmüller level structures as above coincides with the definition of Teichmüller level structures in the sense of Deligne-Mumford (cf. [**D-M**, Definition 5.6]).

Example 2.3. We give examples of Teichmüller level structures.

(1) Let n be a positive integer which is prime to all elements of $\mathbb{P}$ and g a positive integer. We assume that the divisor D is empty and $\overline{X}$ is a proper smooth curve of genus g over S. Then, a Teichmüller structure of level $(\mathbb{Z}/n\mathbb{Z})^{2g}$ on X/S is nothing but an isomorphism of étale sheaves

$$\alpha : R^1f_*(\mathbb{Z}/n\mathbb{Z}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^{2g}.$$

Here, $f : X \to S$ is the structure morphism. We say that α is a *Jacobi structure* of level n on X if α preserves the homogeneous symplectic structures on the both hand sides (cf. [**D-M**, Definition 5.4]).
(2) Let S be a $\mathbb{Z}[1/6]$-scheme. We put $S' := \mathbb{G}_{m,\mathbb{Z}[1/6]} \times_{\mathrm{Spec}\mathbb{Z}[1/6]} S$ and consider the following group homomorphisms:

$$\rho : \pi_1^{\text{ét}}(S',\bar{s}') \to \pi_1^{\text{ét}}(\mathbb{G}_{m,\mathbb{Z}[1/6]},\bar{s}'') \to \mathbb{Z}/2\mathbb{Z} \cong (\mathbb{Z}/3\mathbb{Z})^{\times} \hookrightarrow GSp_{2g}(\mathbb{Z}/3\mathbb{Z}).$$

Here, $\bar{s}'$ is a geometric point of S', $\bar{s}''$ is a projection of $\bar{s}'$, the second map is induced by the étale double cover $\mathbb{G}_{m,\mathbb{Z}[1/6]} \to \mathbb{G}_{m,\mathbb{Z}[1/6]}$, $x \mapsto x^2$ and the last inclusion is given by $a \mapsto \mathrm{diag}(a, 1, a, 1, \ldots, a, 1)$. Let $\mathcal{G}_\rho$ be the finite étale group scheme over S' defined by ρ. Let $f' : X \times_S S' \to S'$ be the base change of f by $S' \to S$. We say that a Teichmüller structure

$$\alpha : R^1 f'_*(\mathbb{Z}/3\mathbb{Z}) \xrightarrow{\sim} \mathcal{G}_\rho$$

of level $\mathcal{G}_\rho$ on $X \times_S S'$ is a *twisted Jacobi structure* of level 3 by ρ on X if α preserves the homogeneous symplectic structures on the both hand sides.

In Example 2.6 below, we compare the classifying stacks of these level structures.

REMARK 2.4. (1) The definition of Teichmüller structures on $(D \hookrightarrow \overline{X}/S)$ of level $\mathcal{G}$ does not depend on the set $\mathbb{P}$. Moreover, there exists a bijection between the set of Teichmüller structures of level $\mathcal{G}$ on $(D \hookrightarrow \overline{X}/S)$ and the set of isomorphism classes of $f^*\mathcal{G}$-torsors over $X = \overline{X} \setminus D$.

(2) In other words, a Teichmüller structure on $(D \hookrightarrow \overline{X}/S)$ of level $\mathcal{G}$ is a global section of the étale sheaf $R^1 f_* f^* \mathcal{G}$ which corresponds to an exterior surjection (cf. [**D-M**, p. 106]).

LEMMA 2.5. *The functor*

$$\Psi_{S,\mathcal{G}} : (\mathrm{Sch}/S) \longrightarrow (\mathrm{Sets})$$

$$[T \to S] \longmapsto \{\textit{Teichmüller structures on } (D_T \hookrightarrow \overline{X}_T/T) \textit{ of level } \mathcal{G}_T\}/\cong$$

is represented by a finite étale scheme over S. Here, $\mathcal{G}_T$ is the pull-back of $\mathcal{G}$ by the structure morphism $T \to S$.

PROOF. Let $f : X \to S$ be the structure morphism of X. By the definition of the Teichmüller structure of level $\mathcal{G}$, $\Psi_{S,\mathcal{G}}$ coincides with a subfunctor of $R^1 f_* f^* \mathcal{G}$ consisting of sections corresponding to exterior surjections on the étale site $S_{\text{ét}}$. Note that, since the characteristic of S is prime to $\mathbb{P}$, any Teichmüller structures of level $\mathcal{G} \in \mathrm{Ob}(\mathrm{l.c.gr}^{\mathbb{P}}/S)$ is tamely ramified along D. Therefore, according to [**SGA1**, Exposé 13, Corollary 2.9], $R^1 f_* f^* \mathcal{G}$ is represented by a finite étale scheme over S (cf. [**D-M**, Lemma 5.7]). Since the set of exterior surjections are stable under the action of the étale fundamental group of S, we deduce that $\Psi_{S,\mathcal{G}}$ is also represented by a finite étale scheme over S. □

The following example is one of the motivations of our definition of non-constant Teichmüller level structures. We can control the number of connected components of certain classifying spaces of level structures by twisting them.

EXAMPLE 2.6. We use the same notation as in Example 2.3 (2). We put $S = \mathrm{Spec}(\mathbb{Z}[1/6])$ and $S' := \mathbb{G}_{m,\mathbb{Z}[1/6]}$. Let $\mathcal{M}_g^0[1/6]$ be the moduli stack of proper smooth curves of genus g over $\mathbb{Z}[1/6]$-schemes. We denote by ${}_3\mathcal{M}_g^0[1/6]$ (resp. by ${}_{3,\rho}\mathcal{M}_g^0[1/6]$) the stack over $\mathrm{Spec}\mathbb{Z}[1/6]$ (resp. $\mathbb{G}_{m,\mathbb{Z}[1/6]}$) classifying proper smooth curves of genus

g with Jacobi structures of level 3 (resp. twisted Jacobi structures of level 3 by ρ). By Lemma 2.5, the canonical 1-morphism ${}_3\mathcal{M}_g^0[1/6] \to \mathcal{M}_g^0[1/6]$ (resp. ${}_{3,\rho}\mathcal{M}_g^0[1/6] \to \mathbb{G}_{m,\mathbb{Z}[1/6]} \times_{\mathrm{Spec}\mathbb{Z}[1/6]} \mathcal{M}_g^0[1/6]$) is relatively representable and finite étale. Note that, according to [**D-M**, (5.14)], ${}_3\mathcal{M}_g^0[1/6]$ is a $\mathbb{Z}[\mu_3, 1/6]$-scheme whose geometric fibers are connected. Then, we have the following isomorphism:

$$ {}_3\mathcal{M}_g^0[1/6] \otimes_{\mathbb{Z}[1/6]} \mathbb{Z}[\mu_3, 1/6] \cong \coprod_{i \in (\mathbb{Z}/3\mathbb{Z})^\times} {}_3\mathcal{M}_g^0[1/6]. $$

We remark that ${}_3\mathcal{M}_g^0[1/6]$ has a canonical action of $GSp_{2g}(\mathbb{Z}/3\mathbb{Z})$ induced by the action of it on level structures. Moreover, if the determinant of an element σ of $GSp_{2g}(\mathbb{Z}/3\mathbb{Z})$ is not equal to 1, σ permutes the connected components of ${}_3\mathcal{M}_g^0[1/6] \otimes_{\mathbb{Z}[1/6]} \mathbb{Z}[\mu_3, 1/6]$.

On the other hand, by definition, the pull-back of ${}_{3,\rho}\mathcal{M}_g^0[1/6]$ by the étale double cover $h : \mathbb{G}_{m,\mathbb{Z}[1/6]} \to \mathbb{G}_{m,\mathbb{Z}[1/6]},\ x \mapsto x^2$ is canonically isomorphic to $\mathbb{G}_{m,\mathbb{Z}[1/6]} \times_{\mathrm{Spec}\mathbb{Z}[1/6]} {}_3\mathcal{M}_g^0[1/6]$. Indeed, the pull-back of $\mathcal{G}_\rho$ by h is canonically isomorphic to the constant group scheme $(\mathbb{Z}/3\mathbb{Z})^{2g}$. Hence, we have:

$$ h^*({}_{3,\rho}\mathcal{M}_g^0[1/6]) \otimes_{\mathbb{Z}[1/6]} \mathbb{Z}[\mu_3, 1/6] \cong \coprod_{i \in (\mathbb{Z}/3\mathbb{Z})^\times} \mathbb{G}_{m,\mathbb{Z}[\mu_3,1/6]} \times_{\mathrm{Spec}\mathbb{Z}[\mu_3,1/6]} {}_3\mathcal{M}_g^0[1/6]. $$

If $g \equiv 1 \pmod 2$, the non-trivial Deck transformation of h permutes the connected components of $h^*({}_{3,\rho}\mathcal{M}_g^0[1/6]) \otimes_{\mathbb{Z}[1/6]} \mathbb{Z}[\mu_3, 1/6]$. In this case, we deduce that ${}_{3,\rho}\mathcal{M}_g^0[1/6]$ is a $\mathbb{Z}[1/6]$-scheme whose geometric fibers are connected.

Let r be a positive integer and SDiv_r (resp. OS_r) the moduli stack of simple divisors of degree r of the projective line $\mathbb{P}^1$ (resp. ordered different r-sections of the projective line $\mathbb{P}^1$). According to [**Fu**, Proposition 5.4], the stack SDiv_r (resp. OS_r) is represented by a smooth $\mathbb{Z}$-scheme. We denote it by $\widetilde{\mathcal{U}}_r$ (resp. $\mathcal{U}_r$). The canonical morphism $\mathcal{U}_r \to \widetilde{\mathcal{U}}_r$ defined by forgetting the order is a finite étale S_r-covering.

Definition 2.7. Let S be a scheme, $\mathbb{P}$ a set of primes containing all residue characteristics of S and $\mathcal{G}$ an object of $(\mathrm{l.c.gr}^{\mathbb{P}}/S)$. Then, we define ${}_{\mathcal{G}}\mathrm{SDiv}_{r,S}$ to be the moduli stack of Teichmüller structures of level $\mathcal{G}$ on the projective line minus simple divisors of degree r. That is, objects and morphisms of ${}_{\mathcal{G}}\mathrm{SDiv}_{r,S}$ are defined as follows:

- Objects: An object of the category ${}_{\mathcal{G}}\mathrm{SDiv}_{r,S}$ is a pair $(D \hookrightarrow \mathbb{P}^1_T, \xi)$ where T is an S-scheme, $(D \hookrightarrow \mathbb{P}^1_T)$ an object of SDiv_r and ξ a Teichmüller structure on $(D \hookrightarrow \mathbb{P}^1_T/T)$ of level $\mathcal{G} \times_S T$.
- Morphisms: A morphism

  $$ f : (D \hookrightarrow \mathbb{P}^1_T, \xi) \longrightarrow (D' \hookrightarrow \mathbb{P}^1_{T'}, \xi') $$

  is a morphism from $(D \hookrightarrow \mathbb{P}^1_T)$ to $(D' \hookrightarrow \mathbb{P}^1_{T'})$ in the category $\mathrm{SDiv}_{r,S}$ such that the pull-back of ξ' is ξ.

COROLLARY 2.8. *The canonical* 1*-morphism*

$$ {}_{\mathcal{G}}\mathrm{SDiv}_{r,S} \to \mathrm{SDiv}_{r,S} := \mathrm{SDiv}_r \times_{\mathrm{Spec}\mathbb{Z}} S $$

is representable and finite étale surjective. In particular, ${}_{\mathcal{G}}\mathrm{SDiv}_{r,S}$ *is represented by a smooth* S*-scheme.*

PROOF. This is an elementary consequence of Lemma 2.5 and the fact that SDiv_r is represented by a smooth $\mathbb{Z}$-scheme. □

2.2. Hurwitz stacks.

In this subsection, we define the Hurwitz stack and relate it to the moduli stack of Teichmüller level structures on the projective line minus simple divisors defined in Subsection 2.1.

DEFINITION 2.9. Let S be a scheme and $\mathbb{P}$ a set of primes containing all residue characteristics of S. Let $\mathcal{G}$ be an object of $(\mathrm{l.c.gr}^{\mathbb{P}}/S)$ and r a positive integer. We define the *Hurwitz stack* $\mathcal{H}^r(\mathcal{G}/S)$ as follows:

- Objects: An object of the category $\mathcal{H}^r(\mathcal{G}/S)$ is a quadruple

$$ (C/T, D \hookrightarrow \mathbb{P}^1_T, f : C \to \mathbb{P}^1_T \setminus D, \mu : C \times_T \mathcal{G}_T \to C), $$

  where
  (a) T is an S-scheme and C/T is a smooth curve whose geometric fibers are connected.
  (b) $(D \hookrightarrow \mathbb{P}^1_T)$ is an object of SDiv_r.
  (c) $f : C \to \mathbb{P}^1_T \setminus D$ is a finite étale morphism of T-schemes.
  (d) $\mu : C \times_T \mathcal{G}_T \to C$ is an action of $\mathcal{G}_T := \mathcal{G} \times_S T$ over $\mathbb{P}^1_T \setminus D$ such that the morphism $\mathrm{pr}_1 \times \mu : C \times_T \mathcal{G}_T \to C \times_{\mathbb{P}^1_T \setminus D} C$ is an isomorphism.
- Morphisms: A morphism

$$ (C/T, D \hookrightarrow \mathbb{P}^1_T, f, \mu) \to (C'/T', D' \hookrightarrow \mathbb{P}^1_{T'}, f', \mu') $$

  is a commutative diagram

$$ \begin{array}{ccc} C & \xrightarrow{f} & \mathbb{P}^1_T \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ C' & \xrightarrow[f']{} & \mathbb{P}^1_{T'} \end{array} $$

  such that β induces a morphism $(D \hookrightarrow \mathbb{P}^1_T) \longrightarrow (D' \hookrightarrow \mathbb{P}^1_{T'})$ in the category SDiv_r and α is compatible with the action of $\mathcal{G}_T$ and $\mathcal{G}_{T'}$.

REMARK 2.10. The category $\mathcal{H}^r(\mathcal{G}/S)$ is an algebraic stack over S. To prove this fact, we may assume that the group scheme $\mathcal{G}$ is a constant group scheme $G = G_S$.

Indeed, there exists a finite étale surjective morphism $S' \to S$ such that $\mathcal{G} \times_S S' \cong G_{S'}$. Then, $\mathcal{H}^r(\mathcal{G}/S) \times_S S'$ is canonically isomorphic to $\mathcal{H}^r(\mathcal{G} \times_S S'/S') \cong \mathcal{H}^r(G/\mathrm{Spec}\mathbb{Z}) \times_{\mathrm{Spec}\mathbb{Z}} S'$. On the other hand, $\mathcal{H}^r(\mathcal{G}/S) \times_S S' \to \mathcal{H}^r(\mathcal{G}/S)$ is also a finite étale surjective 1-morphism. Thus, if $\mathcal{H}^r(G/\mathrm{Spec}\mathbb{Z}) \times_{\mathrm{Spec}\mathbb{Z}} S'$ is algebraic, $\mathcal{H}^r(\mathcal{G}/S)$ is also algebraic. According to [**B-W**, Proposition 1.2.1], $\mathcal{H}^r(G/\mathrm{Spec}\mathbb{Z})$ is an algebraic stack over $\mathbb{Z}$ (cf. Chapter 1.2.2 of loc. cit.). Thus, the stack $\mathcal{H}^r(\mathcal{G}/S)$ is also algebraic.

We recall the notion of rigidifications of algebraic stacks ([**R**]). Let $\mathcal{M}$ be an algebraic stack over a scheme S. Let H be a group scheme over S which is flat, separated and of finite presentation. Assume that the following conditions are satisfied:

(Act) For any S-scheme T and for any object x of $\mathcal{M}(T)$, there exists an injection

$$i_x : H_T \to \underline{\mathrm{Aut}}_T(x)$$

which is compatible with arbitrary base change.

(N) For any S-scheme T and for any objects x, y of $\mathcal{M}(T)$, the group scheme H_T is normal in the sheaf $\underline{\mathrm{Hom}}_T(x, y)$. That is, for any section u (resp. h) of $\underline{\mathrm{Hom}}_T(x, y)$ (resp. H_T), the section $u^{-1} \circ i_y(h) \circ u$ of $\underline{\mathrm{Aut}}_T(x)$ is an element in the image of $H_T(T)$ by i_x.

Then, there exists an algebraic stack $\mathcal{M} /\!\!/ H$ over S and a canonical 1-morphism

$$p : \mathcal{M} \to \mathcal{M} /\!\!/ H$$

which has the following universal property: For any algebraic stack $\mathcal{N}$ over S, any 1-morphism $f : \mathcal{M} \to \mathcal{N}$ over S, any S-scheme T and any object x of $\mathcal{M}(T)$ such that f sends the image of sections of H_T under i_x to the identity automorphism of $f(x)$, there exists a unique 1-morphism $g : \mathcal{M} /\!\!/ H \to \mathcal{N}$ over S such that $f = g \circ p$. The pair $(\mathcal{M} /\!\!/ H, p)$ is unique up to a unique isomorphism.

Definition 2.11 ([**R**, Section 5]). The pair $(\mathcal{M} /\!\!/ H, p)$ is called the *rigidification* of $\mathcal{M}$ along H. It is usually denoted by $\mathcal{M} /\!\!/ H$ for short.

The following proposition relates the Hurwitz stack with the moduli stack classifying Teichmüller level structures on the projective line minus simple divisors.

Proposition 2.12 ([**R**, Proposition 7.2.1]). *There exists a canonical equivalence of categories*:

$$\mathcal{H}^r(\mathcal{G}/S) /\!\!/ Z(\mathcal{G}) \xrightarrow{\sim} {}_{\mathcal{G}}\mathrm{SDiv}_{r,S},$$

where $Z(\mathcal{G})$ is the center of the group scheme $\mathcal{G}$ and $\mathcal{H}^r(\mathcal{G}/S) /\!\!/ Z(\mathcal{G})$ is the rigidification of the Hurwitz stack $\mathcal{H}^r(\mathcal{G}/S)$ along $Z(\mathcal{G})$.

Proof. There exists a canonical 1-morphism

$$f : \mathcal{H}^r(\mathcal{G}/S) \to {}_{\mathcal{G}}\mathrm{SDiv}_{r,S}$$

which is defined by forgetting automorphisms of $\mathcal{G}$-torsors. Note that $Z(\mathcal{G})$ acts on each object of $\mathcal{H}^r(\mathcal{G}/S)$ as automorphisms of $\mathcal{G}$-torsors. It is clear that the action of $Z(\mathcal{G})$ on each object of $\mathcal{H}^r(\mathcal{G}/S)$ satisfies the conditions (Act) and (N). By the definition of the rigidification, the 1-morphism f factors through the canonical 1-morphism

$$p : \mathcal{H}^r(\mathcal{G}/S) \to \mathcal{H}^r(\mathcal{G}/S) \ /\!\!/ Z(\mathcal{G}).$$

That is, there exists a unique 1-morphism

$$g : \mathcal{H}^r(\mathcal{G}/S) \ /\!\!/ Z(\mathcal{G}) \to {}_{\mathcal{G}}\mathrm{SDiv}_{r,S}$$

such that $f = g \circ p$.

In order to prove that g induces an equivalence of categories, we recall the following fact: Let $\mathcal{M}$ and $\mathcal{N}$ be algebraic stacks over S and $u : \mathcal{M} \to \mathcal{N}$ a 1-morphism. Let $v : S' \to S$ be a finite étale surjective morphism. Then, u is an equivalence of categories if and only if $v^*(u) : \mathcal{M}_{S'} \to \mathcal{N}_{S'}$ is an equivalence of categories. Here, $\mathcal{M}_{S'}$ (resp. $\mathcal{N}_{S'}$) is the base change of $\mathcal{M}$ (resp. $\mathcal{N}$) by $v : S' \to S$. Thus, we may assume that $\mathcal{G}$ is a constant group scheme G over S. The fully-faithfulness of g follows from the following fact: Let $X \to \mathbb{P}^1_k$ be a connected finite étale Galois covering of $\mathbb{P}^1_k$ minus finitely many closed points with Galois group G where k is an algebraically closed field. Then, the set of automorphisms of X over $\mathbb{P}^1_k$ which commutes with the action of G is equal to the center of G. It is easy to check that the 1-morphism g is essentially surjective. □

COROLLARY 2.13. *The Hurwitz stack $\mathcal{H}^r(\mathcal{G}/S)$ has a coarse moduli scheme which is smooth over S.*

PROOF. By the general theory of rigidifications of algebraic stacks, $\mathcal{H}^r(\mathcal{G}/S)$ has a coarse moduli algebraic space if and only if its rigidification $\mathcal{H}^r(\mathcal{G}/S) \ /\!\!/ Z(\mathcal{G})$ has a coarse moduli algebraic space (cf. [**R**, Theorem 5.1 (iv)]). Moreover, if they exist, two algebraic spaces are the same. Thus, according to Proposition 2.12, it is sufficient to show that ${}_{\mathcal{G}}\mathrm{SDiv}_{r,S}$ is represented by a smooth S-scheme. This claim is already proved in Corollary 2.8. □

DEFINITION 2.14. We denote the coarse moduli scheme of the Hurwitz stack $\mathcal{H}^r(\mathcal{G}/S)$ by $H^r(\mathcal{G}/S)$.

By the proof of Corollary 2.13, the scheme $H^r(\mathcal{G}/S)$ is a finite étale covering of the scheme $\widetilde{\mathcal{U}}_r \times_{\mathrm{Spec}\mathbb{Z}} S$.

COROLLARY 2.15. *Assume that the center $Z(\mathcal{G})$ of $\mathcal{G}$ is trivial. Then, the Hurwitz stack $\mathcal{H}^r(\mathcal{G}/S)$ is represented by the scheme $H^r(\mathcal{G}/S)$.*

REMARK 2.16. When $S = \mathrm{Spec}(\mathbb{Q})$ and $\mathcal{G}$ is the constant finite group scheme G, the scheme $H^r(G/\mathrm{Spec}(\mathbb{Q}))$ is equal to the disjoint union of the classical Hurwitz spaces $\{\mathcal{H}^{\mathrm{in}}_t(G)\}_{t \le r}$ defined by Fried and Völklein ([**Fr-Vö**]).

2.3. Relation with the Inverse Galois Problem.

In this subsection, we show some relations between the Hurwitz stack and the Inverse Galois Problem. We use the following notation in this subsection.

NOTATION 2.17. Let F be a field of characteristic 0 and $\overline{F}$ an algebraic closure of F. Let r be a positive integer. Let S be a locally Noetherian connected F-scheme and $\bar{s}$ a geometric point of S. Let G be a finite group and

$$\rho : \pi_1^{\text{ét}}(S, \bar{s}) \to \mathrm{Aut}(G)$$

a continuous group homomorphism.

(1) We denote by $\mathcal{G}_\rho$ the finite étale group scheme over S defined by ρ. That is to say, the representation $\mathcal{G}_{\rho,\bar{s}}$ of $\pi_1^{\text{ét}}(S, \bar{s})$ is equal to ρ (cf. Remark 3.4).
(2) Let $f : T \to S$ be a morphism of locally Noetherian connected schemes and $\bar{t} \to T$ a geometric point over $\bar{s}$. We denote by $f_* : \pi_1^{\text{ét}}(T, \bar{t}) \to \pi_1^{\text{ét}}(S, \bar{s})$ the homomorphism between étale fundamental groups induced by f.

PROPOSITION 2.18. *Assume that the set of F-rational points $H^r(\mathcal{G}_\rho/S)(F)$ is non-empty. For an F-rational point $x \in H^r(\mathcal{G}_\rho/S)(F)$, the composite of* $\mathrm{Spec}(F) \xrightarrow{x} H^r(\mathcal{G}_\rho/S) \to S$ *induces a map $G_F = \pi_1^{\text{ét}}(\mathrm{Spec}F, \mathrm{Spec}\overline{F}) \to \pi_1^{\text{ét}}(S, \bar{s})$. We denote it by x_*. Then, there exists a geometrically connected $\mathcal{G}_{\rho\circ x_*}/Z(\mathcal{G}_{\rho\circ x_*})$-torsor over a projective line minus r-points over F.*

PROOF. Since $H^r(\mathcal{G}_\rho/S)$ is the coarse moduli scheme of the Hurwitz stack $\mathcal{H}^r(\mathcal{G}_\rho/S)$, there exists a section $\xi : \mathrm{Spec}(\overline{F}) \to \mathcal{H}^r(\mathcal{G}_\rho/S)$ which is a lift, up to isomorphisms, of the image of x in $H^r(\mathcal{G}_\rho/S)(\overline{F})$. Let $\mathcal{T}$ be the $\mathcal{G}_\rho$-torsor over a projective line minus r-points over $\overline{F}$ corresponding to ξ. For each element $\sigma \in G_F = \mathrm{Gal}(\overline{F}/F)$, there exists an isomorphism $t_\sigma : \sigma^*\mathcal{T} \xrightarrow{\sim} \mathcal{T}$. Since the rigidification of $\mathcal{H}^r(\mathcal{G}_\rho/S)$ along $Z(\mathcal{G}_\rho)$ is isomorphic to $H^r(\mathcal{G}_\rho/S)$, we have $t_\sigma \circ \sigma^*(t_\tau) \equiv t_{\tau\sigma} \mod Z(\mathcal{G}_\rho)$ for any $\sigma, \tau \in G_F$. Thus, by Weil descent, the image of ξ under the 1-morphism $\mathcal{H}^r(\mathcal{G}_\rho/S) \to \mathcal{H}^r((\mathcal{G}_\rho/Z(\mathcal{G}_\rho))/S)$ defines an object of $\mathcal{H}^r((\mathcal{G}_\rho/Z(\mathcal{G}_\rho))/S)(F)$. Here, the 1-morphism of stacks $\mathcal{H}^r(\mathcal{G}_\rho/S) \to \mathcal{H}^r((\mathcal{G}_\rho/Z(\mathcal{G}_\rho))/S)$ is induced by the canonical homomorphism $\mathcal{G}_\rho \to \mathcal{G}_\rho/Z(\mathcal{G}_\rho)$. Since $\mathcal{G}_\rho/Z(\mathcal{G}_\rho)$ is the finite étale group scheme over S defined by the group homomorphism

$$\bar{\rho} := \rho \pmod{Z(G)} : \pi_1^{\text{ét}}(S, \bar{s}) \to \mathrm{Aut}(G/Z(G)),$$

we deduce the conclusion of the proposition. □

We remark that there exists a canonical one-to-one correspondence between the isomorphism classes of $\mathcal{G}$-torsors over S and $\mathrm{H}^1_{\text{ét}}(S, \mathcal{G}) = \mathrm{H}^1_{\text{cont}}(\pi_1^{\text{ét}}(S, \bar{s}), G)$. Here, $\mathrm{H}^1_{\text{cont}}(\pi_1^{\text{ét}}(S, \bar{s}), G)$ is the continuous group cohomology with coefficients in G and $\pi_1^{\text{ét}}(S, \bar{s})$ acts on G via ρ.

LEMMA 2.19. *Let Q be a group, H a finite group with an action of Q and $c : Q \to H$ a 1-cocycle. Assume that the following conditions are satisfied*:

(a) *The group Q acts on H via the group homomorphism $\nu : Q \to \mathrm{Aut}(H)$.*
(b) *There exists a subgroup K of Q such that $\nu(K) = \{\mathrm{id}\}$ and $c(K) = H$.*

Then, there exists a surjective group homomorphism $c' : Q \to \mathrm{Im}(\nu)\mathrm{Inn}(H)$. Here, $\mathrm{Im}(\nu)\mathrm{Inn}(H)$ is the subgroup of $\mathrm{Aut}(H)$ generated by $\mathrm{Im}(\nu)$ and $\mathrm{Inn}(H)$.

PROOF. Let q and q' be elements of Q. By the definition of 1-cocycles, we have $c(qq') = c(q)\nu(q)(c(q'))$. We denote by $\bar{c}$ the composite of c with the canonical group homomorphism $H \to \mathrm{Inn}(H) \subset \mathrm{Aut}(H)$. Set $c'(q) := \bar{c}(q)\nu(q)$. Since

$$\begin{aligned} c'(qq') &= \bar{c}(qq')\nu(qq') = (\bar{c}(q)\nu(q)\bar{c}(q')\nu(q)^{-1})(\nu(q)\nu(q')) = \bar{c}(q)\nu(q)\bar{c}(q')\nu(q') \\ &= c'(q)c'(q'), \end{aligned}$$

the map c' is a group homomorphism. Finally, we shall show the surjectivity of c'. Since $c(K) = H$ and $K \subset \ker(\nu)$, $\mathrm{Inn}(H)$ is contained in $\mathrm{Im}(c')$. Thus, it is sufficient to prove $\mathrm{Im}(\nu) \subset \mathrm{Im}(c')$. Let q be an element of Q. Then, by the condition (b), there exists $k \in K$ with $c(k) = c(q)$. Hence, we have

$$c'(k^{-1}q) = \bar{c}(k^{-1}q)\nu(k^{-1}q) = \bar{c}(k)^{-1}\bar{c}(q)\nu(q) = \nu(q).$$

This completes the proof of the lemma. □

We put $\overline{G} := G/Z(G)$. For a continuous group homomorphism $\tilde{\rho} : G_F = \mathrm{Gal}(\overline{F}/F) \to \mathrm{Aut}(\overline{G})$, we denote by $\overline{G}_{\tilde{\rho}}$ the subgroup of $\mathrm{Aut}(\overline{G})$ generated by $\mathrm{Im}(\tilde{\rho})$ and $\mathrm{Inn}(\overline{G})$.

PROPOSITION 2.20. *Let $\mathcal{G}'$ be a finite étale group scheme over F defined by a continuous group homomorphism $\tilde{\rho} : G_F \to \mathrm{Aut}(\overline{G})$. We put $X := \mathbb{P}^1_F \setminus \{x_1, \ldots, x_r\}$ with $\{x_1, \ldots, x_r\} \in \widetilde{\mathcal{U}}_r(F)$. Let $h : X \to \mathrm{Spec}(F)$ be the structure morphism. Assume that there exists a geometrically connected $h^*\mathcal{G}'$-torsor $\mathcal{T}$ over X. Then, there exists a finite étale Galois covering Y of X with Galois group $\overline{G}_{\tilde{\rho}}$. Moreover, Y is geometrically connected if and only if $\overline{G}_{\tilde{\rho}} = \mathrm{Inn}(\overline{G})$. In this case, we have $Y \otimes_F \overline{F} = \mathcal{T} \otimes_F \overline{F}$.*

PROOF. Let $\bar{x}$ be a geometric point of X and

$$c : \pi_1^{\text{ét}}(X, \bar{x}) = \pi_1^{\text{ét}}(X \otimes_F \overline{F}, \bar{x}) \rtimes G_F \to \overline{G}$$

a 1-cocycle corresponding to the $h^*\mathcal{G}'$-torsor $\mathcal{T}$. By definition, $\pi_1^{\text{ét}}(X, \bar{x})$ acts on $\overline{G}$ via $\pi_1^{\text{ét}}(X, \bar{x}) \to G_F \xrightarrow{\tilde{\rho}} \mathrm{Aut}(\overline{G})$. The composite of these maps is also denoted by $\tilde{\rho}$. Moreover, since $\mathcal{T}$ is geometrically connected, the restriction of c to $\pi_1^{\text{ét}}(X \otimes_F \overline{F}, \bar{x})$ is surjective. Therefore, by applying Lemma 2.19 for $Q = \pi_1^{\text{ét}}(X, \bar{x})$, $\nu = \tilde{\rho}$ and $K = \pi_1^{\text{ét}}(X \otimes_F \overline{F}, \bar{x})$, we have a surjective group homomorphism $c' : \pi_1^{\text{ét}}(X, \bar{x}) \to \overline{G}_{\tilde{\rho}}$. It is easy to see from the definition that c' is continuous and corresponds to a finite étale Galois covering $Y \to X$ with Galois group $\overline{G}_{\tilde{\rho}}$. This implies the first assertion of the proposition.

We shall show the second assertion. The étale $\overline{G}_{\tilde{\rho}}$-covering $Y \to X$ is geometrically connected if and only if $c'(\pi_1^{\text{ét}}(X \otimes_F \overline{F}, \bar{x})) = \overline{G}_{\tilde{\rho}}$. On the other hand, the restriction of

c' to $\pi_1^{\text{ét}}(X \otimes_F \overline{F}, \bar{x})$ coincides with the composite of c with $\overline{G} \to \mathrm{Inn}(\overline{G})$ (see the proof of Lemma 2.19). Thus, we have $Y \otimes_F \overline{F} = \mathcal{T} \otimes_F \overline{F}$ and $c'(\pi_1^{\text{ét}}(X \otimes_F \overline{F}, \bar{x})) = \mathrm{Inn}(\overline{G})$. This completes the proof of the proposition. □

For an F-rational point $x \in H^r(\mathcal{G}_\rho/S)(F)$, we put

$$\bar{\rho}_x := \bar{\rho} \circ x_* : G_F \to \pi_1^{\text{ét}}(S, \bar{s}) \to \mathrm{Aut}(\overline{G})$$

and put $\overline{G}_x := \overline{G}_{\bar{\rho}_x}$. The following corollary is an elementary consequence of Proposition 2.18 and Proposition 2.20.

Corollary 2.21. *There exists a finite étale Galois covering Y of the projective line $\mathbb{P}^1_F$ minus finitely many closed points with Galois group $\overline{G}_x$. Moreover, Y is geometrically connected if and only if $\overline{G}_x = \mathrm{Inn}(\overline{G})$.*

We will give an example where $\overline{G}_x$ does not coincide with $\mathrm{Inn}(\overline{G})$ in Subsection 3.3 (cf. Corollary 3.19).

3. Main theorem.

In this section, we prove Main theorem in Introduction and give a group theoretic criterion for a finite group G to appear as quotients of the absolute Galois group $G_{\mathbb{Q}}$ of $\mathbb{Q}$ (cf. Theorem 3.23, Corollary 3.24).

3.1. Hurwitz braid groups.

In this subsection, we summarize definitions and basic facts on braid groups which we will use later.

Definition 3.1. Let r be a positive integer greater than 1. The (*Hurwitz*) *braid group* $\widetilde{B}_r$ is an abstract group generated by $\{Q_1, \ldots, Q_{r-1}\}$ with the following relations:

$$Q_i Q_{i+1} Q_i = Q_{i+1} Q_i Q_{i+1} \text{ for } 1 \leq i \leq r-2, \tag{1}$$

$$Q_i Q_j Q_i^{-1} Q_j^{-1} = 1 \text{ for } 1 \leq i, j \leq r-1,\ |i-j| \geq 2, \tag{2}$$

$$Q_1 \cdots Q_{r-2} Q_{r-1}^2 Q_{r-2} \cdots Q_1 = 1. \tag{3}$$

Remark 3.2. In [**M-M**, Chapter III], Malle and Matzat use the notation $\widetilde{H}_r$ for the Hurwitz braid group. We use another notation in this paper because we already use the notation H^r for the Hurwitz space.

It is well-known that the braid group $\widetilde{B}_r$ is isomorphic to the topological fundamental group $\pi_1^{\text{top}}(\widetilde{\mathcal{U}}_r(\mathbb{C}), x)$ of the configuration space $\widetilde{\mathcal{U}}_r(\mathbb{C})$ (cf. [**M-M**, Chapter III, Theorem 1.4]). Later, we will identify these two groups.

Recall that there exists a surjective group homomorphism from the braid group to the symmetric group

$$q_r : \widetilde{B}_r \twoheadrightarrow S_r,\ Q_i \mapsto (i, i+1)$$

corresponding to the topological S_r-covering $\mathcal{U}_r(\mathbb{C}) \to \widetilde{\mathcal{U}}_r(\mathbb{C})$.

DEFINITION 3.3. We define the *pure* (*Hurwitz*) *braid group* B_r to be the kernel of q_r. For a subgroup V of S_r, we denote by $B_{r,V}$ the inverse image of V under q_r.

According to [**M-M**, Chapter III, Theorem 1.1], the pure braid group B_r is generated by

$$Q_{i,j} := Q_{j-1} \cdots Q_{i+1} Q_i^2 Q_{i+1}^{-1} \cdots Q_{j-1}^{-1} \text{ for } 1 \leq i < j \leq r.$$

By definition, B_r is isomorphic to the topological fundamental group of $\mathcal{U}_r(\mathbb{C})$. For a subgroup V of S_r, we denote by $\mathcal{U}_{r,V}$ the finite étale covering of the scheme $\widetilde{\mathcal{U}}_r$ corresponding to V.

3.2. A description of $H^r(\mathcal{G}_\rho/S)$.

We use the following notation in this subsection. Let G be a finite group such that the center of $\overline{G} := G/Z(G)$ is trivial and F a finite extension of $\mathbb{Q}$ contained in $\mathbb{C}$. Let S be an algebraic variety over F and $\bar{s}$ a $\mathbb{C}$-valued point of S lying over an F-valued point $s \in S(F)$. Let

$$\rho : \pi_1^{\text{ét}}(S, \bar{s}) \to \mathrm{Aut}(G)$$

be a continuous group homomorphism and $\mathcal{G}$ a finite étale group scheme over S defined by ρ.

Let $\bar{x} = ((x_1, \ldots, x_r), \bar{s}) = (\bar{x}', \bar{s})$ be a $\mathbb{C}$-valued point of $\mathcal{U}_r \times_{\mathrm{Spec}\mathbb{Z}} S$. We assume that $\bar{x}'$ is over a $\mathbb{Q}$-rational point $x' \in \mathcal{U}_r(\mathbb{Q})$. We also regard $\bar{x}$ as a geometric point of $\widetilde{\mathcal{U}}_r \times_{\mathrm{Spec}\mathbb{Z}} S$.

First, we describe a finite étale covering

$$H^r(\mathcal{G}_\rho/S) \to \widetilde{\mathcal{U}}_r \times_{\mathrm{Spec}\mathbb{Z}} S$$

as a representation of $\pi_1^{\text{ét}}(\widetilde{\mathcal{U}}_r \times_{\mathrm{Spec}\mathbb{Z}} S, \bar{x})$ on a finite set. We fix the isomorphism

$$\pi_1^{\text{ét}}(\widetilde{\mathcal{U}}_r \times_{\mathrm{Spec}\mathbb{Z}} S, \bar{x}) \xrightarrow{\sim} (\pi_1^{\text{ét}}(\widetilde{\mathcal{U}}_r \otimes_{\mathbb{Z}} \mathbb{C}, \bar{x}') \times \pi_1^{\text{ét}}(S \otimes_{\mathbb{Z}} \mathbb{C}, \bar{s})) \rtimes G_F$$

induced by $(x' \times s)_*$ (cf. [**SGA1**, Exposé XIII, Proposition 4.6]).

REMARK 3.4. Let T be a locally Noetherian connected scheme and $\bar{t}$ a geometric point of T. Note that there exists the following equivalence of categories:

$$\begin{array}{ccc} (\text{Finite étale coverings of } T) & \xrightarrow{\sim} & (\text{Representations of } \pi_1^{\text{ét}}(T, \bar{t}) \text{ on finite sets}) \\ f : W \to T & \longmapsto & f^{-1}(\bar{t}). \end{array}$$

We regard the finite étale covering $H^r(\mathcal{G}_\rho/S) \to \widetilde{\mathcal{U}}_r \times_{\mathrm{Spec}\mathbb{Z}} S$ as a representation of the étale fundamental group $\pi_1^{\text{ét}}(\widetilde{\mathcal{U}}_r \times_{\mathrm{Spec}\mathbb{Z}} S, \bar{x})$ by using the above equivalence of categories.

The geometric fiber of the morphism $H^r(\mathcal{G}_\rho/S) \to \widetilde{\mathcal{U}}_r \times_{\mathrm{Spec}\mathbb{Z}} S$ at $\bar{x}$ is canonically identified with the set of exterior surjections $\mathrm{Surj}^{\mathrm{ext}}(\pi_1^{\text{ét}}(\mathbb{P}^1_{\mathbb{C}} \setminus \{x_1, \ldots, x_r\}),\ \mathcal{G}_{\rho,\bar{s}})$ (cf. Definition 2.1). Let us describe the action of the étale fundamental group of $\widetilde{\mathcal{U}}_r$ on this geometric fiber. Recall that we regard $\overline{\mathbb{Q}}$ as a subfield of $\mathbb{C}$ in this paper. It is known that the étale fundamental group of $\widetilde{\mathcal{U}}_r \otimes_{\mathbb{Z}} \overline{\mathbb{Q}}$ is canonically isomorphic to the profinite completion of the Hurwitz braid group $\widetilde{B}_r$ (cf. Subsection 3.1) and we identify these two groups.

Proposition 3.5 (*cf.* [**Fr-Vö**, Section 1.3]). *Let $\bar{\eta}$ be a geometric point of $\mathbb{P}^1_{\mathbb{C}} \setminus \{x_1, \ldots, x_r\}$ and σ_i the element of $\pi_1^{\text{ét}}(\mathbb{P}^1_{\mathbb{C}} \setminus \{x_1, \ldots, x_r\}, \bar{\eta})$ corresponding to the homotopy class of a loop which rounds x_i counterclockwise. Then, the action of $\pi_1^{\text{ét}}(\widetilde{\mathcal{U}}_r \otimes_{\mathbb{Z}} \mathbb{C}, \{x_1, \ldots, x_r\})$ on the set of exterior surjections $\mathrm{Surj}^{\mathrm{ext}}(\pi_1^{\text{ét}}(\mathbb{P}^1_{\mathbb{C}} \setminus \{x_1, \ldots, x_r\}),\ \mathcal{G}_{\rho,\bar{s}})$ coincides with the action induced by the action of $\pi_1^{\text{ét}}(\widetilde{\mathcal{U}}_r \otimes_{\mathbb{Z}} \mathbb{C}, \{x_1, \ldots, x_r\})$ on $\pi_1^{\text{ét}}(\mathbb{P}^1_{\mathbb{C}} \setminus \{x_1, \ldots, x_r\}, \bar{\eta})$ defined as follows*:

$$Q_i(\sigma_j) := \begin{cases} \sigma_j & (j > i+1 \text{ or } j < i) \\ \sigma_i \sigma_{i+1} {\sigma_i}^{-1} & (j = i) \\ \sigma_i & (j = i+1). \end{cases}$$

Remark 3.6. The above action does not depend on the choice of $\bar{\eta}$.

Next, we describe the actions of $\pi_1^{\text{ét}}(S \otimes_F \mathbb{C}, \bar{s})$ and G_F on the set of exterior surjections $\mathrm{Surj}^{\mathrm{ext}}(\pi_1^{\text{ét}}(\mathbb{P}^1_{\mathbb{C}} \setminus \{x_1, \ldots, x_r\}),\ \mathcal{G}_{\rho,\bar{s}})$.

Proposition 3.7. *The action of $\pi_1^{\text{ét}}(S \otimes_F \mathbb{C}, \bar{s})$ on the set of exterior surjections $\mathrm{Surj}^{\mathrm{ext}}(\pi_1^{\text{ét}}(\mathbb{P}^1_{\mathbb{C}} \setminus \{x_1, \ldots, x_r\}),\ \mathcal{G}_{\rho,\bar{s}})$ is described as follows*:

$$u[f] = [\rho(u) \circ f],\ \forall u \in \pi_1^{\text{ét}}(S \otimes_F \mathbb{C}, \bar{s}),\ \forall f \in \mathrm{Surj}(\pi_1^{\text{ét}}(\mathbb{P}^1_{\mathbb{C}} \setminus \{x_1, \ldots, x_r\}),\ \mathcal{G}_{\rho,\bar{s}}).$$

Proposition 3.8. *The action of $G_F = \mathrm{Gal}(\overline{F}/F)$ on the set of exterior surjections $\mathrm{Surj}^{\mathrm{ext}}(\pi_1^{\text{ét}}(\mathbb{P}^1_{\mathbb{C}} \setminus \{x_1, \ldots, x_r\}),\ \mathcal{G}_{\rho,\bar{s}})$ coincides with the composite of the action induced by the outer action of G_F on the étale fundamental group*

$$\pi_1^{\text{ét}}(\mathbb{P}^1_{\mathbb{C}} \setminus \{x_1, \ldots, x_r\}, \bar{\eta}) \cong \pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{F}} \setminus \{x_1, \ldots, x_r\}, \bar{\eta})$$

(*cf.* [**SGA1**, Exposé 10]) *and the action of G_F on $\mathcal{G}_{\rho,\bar{s}}$. Here, we regard G_F as a subgroup of $\pi_1^{\text{ét}}(S, \bar{s})$ via s_*.*

Proposition 3.7 and Proposition 3.8 are elementary consequences of the following lemma.

Lemma 3.9. *Let k be a field of characteristic 0. Let G be a finite group and $\phi : G_k \to \mathrm{Aut}(G)$ a continuous group homomorphism. Let $\{x_1, \ldots, x_r\}$ be a k-rational point of $\widetilde{\mathcal{U}}_r$ and*

$$f : \mathbb{P}^1_k \setminus \{x_1, \ldots, x_r\} \to \mathrm{Spec}(k)$$

the structure morphism. Let $\bar{\eta}$ be a geometric point of $\mathbb{P}^1_k \setminus \{x_1, \ldots, x_r\}$. Then, the action of G_k on the set of exterior surjections $\mathrm{Surj}^{\mathrm{ext}}(\pi_1^{\text{ét}}(\mathbb{P}^1_{\bar{k}} \setminus \{x_1, \ldots, x_r\}, \bar{\eta}), G)$ *is described as follows:*

$$\beta[f] = \phi(\beta) \circ [f \circ \mathrm{Int}(\beta)],\ \forall \beta \in G_k,\ \forall [f] \in \mathrm{Surj}^{\mathrm{ext}}(\pi_1^{\text{ét}}(\mathbb{P}^1_{\bar{k}} \setminus \{x_1, \ldots, x_r\}, \bar{\eta}), G).$$

Here, we regard G_k as a subgroup of $\pi_1^{\text{ét}}(\mathbb{P}^1_k \setminus \{x_1, \ldots, x_r\}, \bar{\eta})$ by taking a section of the fundamental exact sequence (*cf.* [**SGA1**, Exposé 10])

$$1 \to \pi_1^{\text{ét}}(\mathbb{P}^1_{\bar{k}} \setminus \{x_1, \ldots, x_r\}, \bar{\eta}) \to \pi_1^{\text{ét}}(\mathbb{P}^1_k \setminus \{x_1, \ldots, x_r\}, \bar{\eta}) \to G_k \to 1,$$

and $\mathrm{Int}(\beta)$ *is the inner automorphism by β.*

REMARK 3.10. The above action of G_k does not depend on the choice of the section of the fundamental exact sequence.

PROOF. Let $\mathcal{G}_\phi$ be a finite étale group scheme over $\mathrm{Spec}(k)$ defined by ϕ. By definition, the étale sheaf $R^1 f_* f^* \mathcal{G}_\phi$ is the sheafification of the presheaf:

$$L/k \mapsto \mathrm{H}^1(\mathbb{P}_L \setminus \{x_1, \ldots, x_r\}, f^* \mathcal{G}_\phi).$$

Here L is an étale k-algebra. The action of $\beta \in G_k$ is decomposed as follows:

$$\begin{array}{ccc} \mathrm{H}^1(\mathbb{P}^1_{\bar{k}} \setminus \{x_1, \ldots, x_r\}, G) & \longrightarrow & \mathrm{H}^1(\mathbb{P}^1_{\bar{k}} \setminus \{x_1, \ldots, x_r\}, G) \\ & \searrow^{\beta^*} \quad \circlearrowleft\ \phi(\beta) & \uparrow \\ & & \mathrm{H}^1(\mathbb{P}^1_{\bar{k}} \setminus \{x_1, \ldots, x_r\}, G), \end{array}$$

where β^* is induced by the pull-back of torsors by β and $\phi(\beta)$ is the morphism induced by $\phi(\beta) \in \mathrm{Aut}(G)$. □

DEFINITION 3.11. For a $\pi_1^{\text{ét}}(\widetilde{\mathcal{U}}_r \times_{\mathrm{Spec}\mathbb{Z}} S, \bar{x})$-stable subset X of $\mathrm{Surj}^{\mathrm{ext}}(\pi_1^{\text{ét}}(\mathbb{P}^1_{\mathbb{C}} \setminus \{x_1, \ldots, x_r\}),\ \mathcal{G}_{\rho,\bar{s}})$, we denote by $H^r(\mathcal{G}_\rho/S)(X)$ the finite étale covering of $\widetilde{\mathcal{U}}_r \times_{\mathrm{Spec}\mathbb{Z}} S$ corresponding to the $\pi_1^{\text{ét}}(\widetilde{\mathcal{U}}_r \times_{\mathrm{Spec}\mathbb{Z}} S, \bar{x})$-set X (cf. Remark 3.4).

3.3. A group theoretic criterion of Galois realizations over $\mathbb{Q}$.

In this subsection, we give a generalization of the braid orbit theorem (cf. [**M-M**, Chapter III, Theorem 5.6]). We fix a finite group G and a positive integer r. First, we define special subsets of $G^r/\mathrm{Inn}(G)$. Here the group $\mathrm{Inn}(G)$ acts on G^r diagonally.

DEFINITION 3.12 ([**Vö**, Section 1]). (1) We define the finite subset $\mathcal{E}_r^{\mathrm{in}}(G)$ of $G^r/\mathrm{Inn}(G)$ as follows:

$$\mathcal{E}_r^{\mathrm{in}}(G) := \{(g_1, \ldots, g_r) \in G^r \mid g_1 \cdots g_r = 1,\ \langle g_1, \ldots, g_r\rangle = G\}/\mathrm{Inn}G.$$

We denote the class of $g = (g_1, \ldots, g_r) \in G^r$ in $\mathcal{E}_r^{\mathrm{in}}(G)$ by $[g]$ or $[g_1, \ldots, g_r]$.

(2) Let $\mathcal{C} = (C_1, \ldots, C_r)$ be an r-tuple of conjugacy classes of G and V a subgroup of the symmetric group S_r. We define the subset $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ of $\mathcal{E}_r^{\mathrm{in}}(G)$ by

$$\mathcal{E}^{\mathrm{in}}(\mathcal{C}) := \{[g_1, \ldots, g_r] \in \mathcal{E}_r^{\mathrm{in}}(G) \mid g_i \in C_i,\ 1 \le \forall i \le r\}$$

and we define the subset $\mathcal{E}_V^{\mathrm{in}}(\mathcal{C})$ of $\mathcal{E}_r^{\mathrm{in}}(G)$ by

$$\mathcal{E}_V^{\mathrm{in}}(\mathcal{C}) := \{[g_1, \ldots, g_r] \in \mathcal{E}_r^{\mathrm{in}}(G) \mid \exists \tau \in V,\ g_i \in C_{\tau(i)},\ 1 \le \forall i \le r\}.$$

We define $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*) := \bigcup_n \mathcal{E}^{\mathrm{in}}(\mathcal{C}^n)$ and $\mathcal{E}_V^{\mathrm{in}}(\mathcal{C}^*) := \bigcup_n \mathcal{E}_V^{\mathrm{in}}(\mathcal{C}^n)$, where n runs through positive integers prime to $\sharp G$.

(3) For a $\overline{\mathbb{Q}}$-rational point $(x_1, \ldots, x_r)$ of $\mathcal{U}_r$, we define the isomorphism

$$i((x_1, \ldots, x_r)) : \mathrm{Surj}^{\mathrm{ext}}(\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{x_1, \ldots, x_r\}), G) \xrightarrow{\sim} \mathcal{E}_r^{\mathrm{in}}(G)$$

by $[f] \mapsto [f(\sigma_1), \ldots, f(\sigma_r)]$. Here, σ_i is the element of $\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{x_1, \ldots, x_r\})$ corresponding to the homotopy class of a loop rounding x_i counterclockwise.

Let $\{x_1, \ldots, x_r\}$ be a $\mathbb{Q}$-rational point of $\widetilde{\mathcal{U}}_r$. We regard the finite set $\mathrm{Surj}^{\mathrm{ext}}(\pi_1^{\text{ét}}(\mathbb{P}^1_{\mathbb{C}} \setminus \{x_1, \ldots, x_r\}), G)$ as a finite set with an action of $\pi_1^{\text{ét}}(\widetilde{\mathcal{U}}_r, p)$, where p is a geometric point of $\widetilde{\mathcal{U}}_r$ over $\{x_1, \ldots, x_r\}$. According to Proposition 3.8 and [**M-M**, Chapter I, Proposition 4.3], the scheme $H^r(\mathcal{G}_\rho/S)(\mathcal{E}_V^{\mathrm{in}}(\mathcal{C}^*))$ is defined over $\mathbb{Q}$ for any $V \subset S_r$. Next, we define the action of the braid group $\widetilde{B}_r$ and the automorphism group $\mathrm{Aut}(G)$ of G on the set $\mathcal{E}_r^{\mathrm{in}}(G)$.

Definition 3.13. We define the actions of $\widetilde{B}_r$ and $\mathrm{Aut}(G)$ as follows:

$$\begin{aligned} Q_i[g_1, \ldots, g_r] &:= [g_1, \ldots, g_{i-1}, g_{i+1}, g_{i+1}^{-1} g_i g_{i+1}, g_{i+2}, \ldots, g_r]\ (1 \le i \le r-1) \\ f[g_1, \ldots, g_r] &:= [f(g_1), \ldots, f(g_r)],\ \forall f \in \mathrm{Aut}(G) \\ \forall [g_1, \ldots, g_r] &\ \in\ \mathcal{E}_r^{\mathrm{in}}(G). \end{aligned}$$

Let $\mathcal{C}$ be an r-tuple of conjugacy classes of G. By definition, the pure braid group B_r acts on the set $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$. We say that $\mathcal{C}$ is *braiding rigid* if the action of B_r on $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ is transitive.

Remark 3.14. The action of $\widetilde{B}_r \cong \pi_1^{\mathrm{top}}(\widetilde{\mathcal{U}}_r(\mathbb{C}), \{x_1, \ldots, x_r\})$ on $\mathcal{E}_r^{\mathrm{in}}(G)$ is compatible with the isomorphism $i((x_1, \ldots, x_r))$ (cf. Proposition 3.5). Thus, there exists a canonical one-to-one correspondence between $\widetilde{B}_r$-orbits (resp. $B_{r,V}$-orbits) in $\mathcal{E}_r^{\mathrm{in}}(G)$ and connected components of the scheme $H^r(G/\overline{\mathbb{Q}})$ (resp. $H^r(G/\overline{\mathbb{Q}}) \times_{\widetilde{\mathcal{U}}_r} \mathcal{U}_{r,V}$) (cf. Remark 3.4).

DEFINITION 3.15 (*cf.* [**M-M**, Chapter I, Section 4.4]). Let $\mathcal{C} = (C_1, \ldots, C_r)$ be an r-tuple of conjugacy classes of G and V a subgroup of the symmetric group S_r. We say that $\mathcal{C}$ is *V-symmetric* if, for a positive integer m prime to $\sharp G$, there exists an element τ of V such that

$$\mathcal{C}^m := (C_1^m, \ldots, C_r^m) = (C_{\tau(1)}, \ldots, C_{\tau(r)}).$$

We say that $\mathcal{C}$ is *rational* if $\mathcal{C}$ is S_r-symmetric. For a conjugacy class C of G, we say that C is *rational* if the 1-tuple (C) is rational.

REMARK 3.16. Let g be an element of G and C a conjugacy class of G containing g. Then, C is rational if and only if $C^m = C$ for any positive integer m prime to the order of g.

LEMMA 3.17. *Let $\mathcal{C} = (C_1, \ldots, C_r)$ be an r-tuple of conjugacy classes of G and V a subgroup of S_r. Let $x = (x_1, \ldots, x_r)$ be a $\overline{\mathbb{Q}}$-rational point of $\mathcal{U}_r$ such that the image of x under the canonical map $\mathcal{U}_r(\overline{\mathbb{Q}}) \to \mathcal{U}_{r,V}(\overline{\mathbb{Q}})$ is a $\mathbb{Q}$-rational point of $\mathcal{U}_{r,V}$. Let $[g]$ be an element of $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ and $Y \to \mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{x_1, \ldots, x_r\}$ a finite étale G-covering corresponding to $[g]$ via the isomorphism*

$$i((x_1 \ldots, x_r)) : \mathrm{Surj}^{\mathrm{ext}}(\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{x_1, \ldots, x_r\}), G) \cong \mathcal{E}_r^{\mathrm{in}}(G).$$

If Y is defined over $\mathbb{Q}$, $\mathcal{C}$ is V-symmetric.

PROOF. Assume that Y is defined over $\mathbb{Q}$. First, we remark that Y is defined over $\mathbb{Q}$ if and only if $[g]$ is stabilized by $G_{\mathbb{Q}}$. Let σ be an element of $G_{\mathbb{Q}}$. Then, by the remark above, we have $\sigma[g] =: [g'_1, \ldots, g'_r] = [g]$. In particular, g'_i is contained in C_i. According to [**M-M**, Chapter I, Proposition 4.3], g'_i is contained in $C_{j_i}^{\chi_{\mathrm{cyc}}(\sigma)}$, where j_i is defined by $\sigma(x_i) = x_{j_i}$ and $\chi_{\mathrm{cyc}} : G_{\mathbb{Q}} \to \widehat{\mathbb{Z}}^{\times}$ is the cyclotomic character. Thus, C_i coincides with $C_{j_i}^{\chi_{\mathrm{cyc}}(\sigma)}$. On the other hand, since the image of x in $\mathcal{U}_{r,V}$ is a $\mathbb{Q}$-rational point, there exists $\tau \in V$ with $x_{j_i} = x_{\tau(i)}$ for any i. Therefore, we have $C_i = C_{\tau(i)}^{\chi_{\mathrm{cyc}}(\sigma)}$ for any i. Since χ_{cyc} is surjective, we deduce that $\mathcal{C}$ is V-symmetric. □

PROPOSITION 3.18. *We put $\overline{G} := G/Z(G)$. Let $\mathcal{G}'$ be the finite étale group scheme over $\mathbb{Q}$ defined by a continuous group homomorphism $\tilde{\rho} : G_{\mathbb{Q}} \to \mathrm{Aut}(\overline{G})$. We put $X := \mathbb{P}^1_{\mathbb{Q}} \setminus \{x_1, \ldots, x_r\}$ for a $\mathbb{Q}$-rational point $\{x_1, \ldots, x_r\} \in \widetilde{\mathcal{U}}_r(\mathbb{Q})$. Let $h : X \to \mathrm{Spec}(\mathbb{Q})$ be the structure morphism. Let $\mathcal{T}$ be a geometrically connected $h^*\mathcal{G}'$-torsor over X, C_i the conjugacy class of $\overline{G}$ corresponding to the inertia group of $\mathrm{Gal}(\mathcal{T} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}/X \otimes_{\mathbb{Q}} \overline{\mathbb{Q}})$ at x_i and V a subgroup of S_r. Take a $\overline{\mathbb{Q}}$-rational point $(x_1, \ldots, x_r) \in \mathcal{U}_r(\overline{\mathbb{Q}})$ in the inverse image of $\{x_1, \ldots, x_r\}$. Assume that the image of $(x_1, \ldots, x_r)$ under the canonical map $\mathcal{U}_r(\overline{\mathbb{Q}}) \to \mathcal{U}_{r,V}(\overline{\mathbb{Q}})$ is a $\mathbb{Q}$-rational point of $\mathcal{U}_{r,V}$. Then, if $(C_1, \ldots, C_r)$ is not V-symmetric, $\overline{G}_{\tilde{\rho}} := \mathrm{Inn}(\overline{G})\mathrm{Im}(\rho)$ does not coincide with $\mathrm{Inn}(\overline{G})$.*

PROOF. Assume that $\overline{G}_{\tilde{\rho}} = \mathrm{Inn}(\overline{G})$. Then $\mathcal{T} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \to X \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ is a connected $\mathrm{Inn}(\overline{G})$-covering defined over $\mathbb{Q}$ (cf. Proposition 2.20). According to Lemma 3.17, this

implies that $\mathcal{C} := (C_1, \ldots, C_r)$ is V-symmetric. But it contradicts the assumption that $\mathcal{C}$ is not V-symmetric. □

By applying Proposition 3.18 to the case where $\tilde{\rho} = \bar{\rho}_x$ for $x \in H^r(\mathcal{G}_\rho/S)(\mathbb{Q})$, we obtain the following corollary (see Corollary 2.21 for the definition of $\bar{\rho}_x$).

Corollary 3.19. *Let us take the same notation as in Corollary* 2.21. *Let V be a subgroup of S_r and $\mathcal{C}$ an r-tuple of conjugacy classes of G which is not V-symmetric. Assume that $F = \mathbb{Q}$ and $x \in H^r(\mathcal{G}_\rho/S)(\mathbb{Q})$ can be lifted to a $\mathbb{Q}$-rational point of $H^r(\mathcal{G}_\rho/S) \times_{\widetilde{\mathcal{U}}_r} \mathcal{U}_{r,V}$. Furthermore, assume that x is contained in the geometric connected component corresponding to $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$. Then, $\overline{G}_x := \overline{G}_{\bar{\rho}_x}$ in the sense of Corollary* 2.21 *does not coincide with* $\mathrm{Inn}(\overline{G})$.

Finally, we recall the definition of braid orbit genera and the oddness condition in the sense of [**M-M**]. Let Γ_s^r be the subgroup of the pure braid group B_r generated by $\{Q_{i,j} \mid 1 \leq i < j \leq r,\ s < j\}$ and $\Gamma_s := \Gamma_{s-1}^r/\Gamma_s^r$. We put $\Gamma_r^r := \{1\}$.

Definition 3.20 (*cf.* [**M-M**, Chapter III, Section 5.2]). Let $\mathcal{E}$ be a finite set with an action of B_r and s an element of $\mathcal{E}$. We denote by s_j the image of s in the set of Γ_j^r-orbits $\mathcal{E}/\Gamma_j^r$. Let $\mathcal{B}_j(s) := s_j\Gamma_j$ be the orbit of s_j in $\mathcal{E}/\Gamma_j^r$ under the action of $\Gamma_j = \Gamma_{j-1}^r/\Gamma_j^r$ for $1 \leq j \leq r-1$. Denote the set of the orbits under the action of $Q_{i,j}\Gamma_j^r$ in $\mathcal{B}_j(s) \subset \mathcal{E}/\Gamma_j^r$ by $\{\mathcal{O}_{i,j,k}\}_{k=1}^{c_{i,j}}$, where $c_{i,j}$ is the number of the orbits.

(1) The *j-th braid orbit genus* $g_j(s)$ of s as follows:

$$g_j(s) := 1 - \sharp\mathcal{B}_j(s) + \frac{1}{2}\sum_{i=1}^{j-1}(\sharp\mathcal{B}_j(s) - c_{i,j}).$$

(2) (cf. [**M-M**, Chapter III, Section 5.2]) The *oddness condition* for $s \in \mathcal{E}$ is as follows:
(O_j): There exist $i < j$ and $1 \leq k \leq c_{i,j}$ such that the order of the finite set

$$\{k' \in \mathbb{Z}_{\geq 1} \mid 1 \leq k' \leq c_{i,j},\ \sharp O_{i,j,k'} = \sharp O_{i,j,k}\}$$

is odd.

Let V be a subgroup of S_r. Let $\mathcal{E}$ be a finite set with an action of $B_{r,V}$. Now, we fix an algebraically closed field $\bar{k}$ of characteristic 0 and an isomorphism $\widehat{B}_{r,V} \cong \pi_1^{\text{ét}}(\mathcal{U}_{r,V} \otimes_{\mathbb{Q}} \bar{k}, \bar{p})$, where $\widehat{B}_{r,V}$ denotes the profinite completion of $B_{r,V}$. Then, the $B_{r,V}$-set $\mathcal{E}$ corresponds to a finite étale covering $\mathcal{U}_{r,V}(\mathcal{E}) \to \mathcal{U}_{r,V} \otimes_{\mathbb{Q}} \bar{k}$. For an element s of $\mathcal{E}$, let $\mathcal{U}_{r,V}(s)$ be the connected component of $\mathcal{U}_{r,V}(\mathcal{E})$ corresponding to the $B_{r,V}$-orbit of s. The function field of $\mathcal{U}_{r,V}(s)$ coincides with $\overline{\mathbb{Q}}K_s$ in [**M-M**, Chapter III, Theorem 3.7].

The following proposition is proved in [**M-M**, Chapter III, Theorem 5.6, Theorem 5.7].

Proposition 3.21 ([**M-M**, Chapter III, Theorem 5.6, Theorem 5.7]). *Let V be a subgroup of S_r, $\mathcal{E}$ a finite set with an action of $B_{r,V}$ and s an element of $\mathcal{E}$. If $g_j(s) = 0$*

for any $1 \leq j \leq r-1$, $\mathcal{U}_{r,V}(s)$ is a rational variety over $\bar{k}$. Moreover, if $\mathcal{U}_{r,V}(s)$ is defined over a subfield k of $\bar{k}$ and s satisfies the oddness condition (O_j) for any $1 \leq j \leq r-1$, $\mathcal{U}_{r,V}(s)$ is a rational variety over k.

PROPOSITION 3.22. *Let $\mathcal{C}$ be an r-tuple of conjugacy classes of G and H a subgroup of $\mathrm{Aut}(G)$. Assume that the following three conditions are satisfied*:

(a) *The tuple $\mathcal{C}$ is braiding rigid. Moreover, for any $[g] \in \mathcal{E}^{\mathrm{in}}(\mathcal{C})$ and for any $1 \leq j \leq r-1$, we have $g_j([g]) = 0$ and the oddness condition (O_j) holds for $[g]$.*
(b) *There exists a subgroup V of S_r such that $H \times B_{r,V}$ acts on $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)$ transitively.*
(c) *H is isomorphic to $(\mathbb{Z}/f\mathbb{Z}) \rtimes (\mathbb{Z}/f\mathbb{Z})^\times$ for some odd positive integer f greater than 1 and the action of H on $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)$ factors through $H \twoheadrightarrow (\mathbb{Z}/f\mathbb{Z})^\times \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$.*

Let $\bar{x}$ be a geometric point of $\mathbb{G}_{m,\mathbb{Q}} \times_{\mathrm{Spec}\mathbb{Q}} \mathcal{U}_{r,V}$ over an F-rational point of $\mathbb{G}_{m,\mathbb{Q}} \times_{\mathrm{Spec}\mathbb{Q}} \mathcal{U}_{r,V}$. We denote by $\bar{s}$ (resp. $\bar{x}'$) the projection of $\bar{x}$ to $\mathbb{G}_{m,\mathbb{Q}}$ (resp. $\mathcal{U}_{r,V}$). Let $\rho : \pi_1^{\text{ét}}(\mathbb{G}_{m,\mathbb{Q}}, \bar{s}) \to \mathrm{Aut}(G)$ be the continuous group homomorphism defined by

$$\pi_1^{\text{ét}}(\mathbb{G}_{m,\mathbb{Q}}, \bar{s}) \cong \widehat{\mathbb{Z}} \rtimes G_{\mathbb{Q}} \twoheadrightarrow (\mathbb{Z}/f\mathbb{Z}) \rtimes (\mathbb{Z}/f\mathbb{Z})^\times \cong H \subset \mathrm{Aut}(G).$$

Here, the homomorphism $G_{\mathbb{Q}} \twoheadrightarrow (\mathbb{Z}/f\mathbb{Z})^\times$ is given by the composite of the cyclotomic character $\chi_{\mathrm{cyc}} : G_{\mathbb{Q}} \to \widehat{\mathbb{Z}}^\times$ and the canonical homomorphism $\widehat{\mathbb{Z}}^\times \to (\mathbb{Z}/f\mathbb{Z})^\times$. Then, the set of $\mathbb{Q}$-rational points $(H^r(\mathcal{G}_\rho/\mathbb{G}_{m,\mathbb{Q}}) \times_{\widetilde{\mathcal{U}}_r} \mathcal{U}_{r,V})(\mathbb{Q})$ is non-empty.

PROOF. We put $S := \mathbb{G}_{m,\mathbb{Q}}$ and let $H(\mathcal{C}^*)_V$ be the open and closed subscheme of $H^r(\mathcal{G}_\rho/S) \times_{\widetilde{\mathcal{U}}_r} \mathcal{U}_{r,V}$ corresponding to the $\pi_1^{\text{ét}}(S \times_{\mathrm{Spec}\mathbb{Q}} \mathcal{U}_{r,V}, \bar{x})$-set $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)$. By the condition (b), $H(\mathcal{C}^*)_V \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ is a connected scheme. We show that the set of $\mathbb{Q}$-rational points of $H(\mathcal{C}^*)_V$ is non-empty.

First, we show the proposition when $B_{r,V}$ acts on $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)$ transitively. Let $h : S \to S, x \to x^2$ be the étale double cover. To prove the existence of $\mathbb{Q}$-rational points of $H(\mathcal{C}^*)_V$, it is enough to show that the pull-back $(h \times \mathrm{pr}_2)^* H(\mathcal{C}^*)_V$ of $H(\mathcal{C}^*)_V$ by $h \times \mathrm{pr}_2 : S \times_{\mathrm{Spec}\mathbb{Q}} \mathcal{U}_{r,V} \to S \times_{\mathrm{Spec}\mathbb{Q}} \mathcal{U}_{r,V}$ is a rational variety over $\mathbb{Q}$. Let k be the function field of S and $\bar{k}$ an algebraic closure of k. Then, the finite étale covering

$$\mathrm{Spec}(\bar{k}) \times_S (h \times \mathrm{pr}_2)^* H(\mathcal{C}^*)_V \to \mathrm{Spec}(\bar{k}) \times_{\mathrm{Spec}\mathbb{Q}} \mathcal{U}_{r,V}$$

corresponds to the finite $B_{r,V}$-set $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)$ (cf. the condition (c)). Therefore, by the condition (a), (b) and Proposition 3.21, $\mathrm{Spec}(k) \times_S (h \times \mathrm{pr}_2)^* H(\mathcal{C}^*)_V$ is a rational variety over k. Since $k \cong \mathbb{Q}(t)$, $(h \times \mathrm{pr}_2)^* H(\mathcal{C}^*)_V$ is a rational variety over $\mathbb{Q}$.

Next, we show the proposition when the action of $B_{r,V}$ on $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)$ is not transitive. Let $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*) = \bigsqcup_{i=1}^m \mathcal{E}_i$ be the decomposition into the $B_{r,V}$-orbits. By the condition (b), H acts on the set $\{\mathcal{E}_1, \ldots, \mathcal{E}_m\}$ transitively. Because the action of H on $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)$ factors through the group $\mathbb{Z}/2\mathbb{Z}$, we have $m = 2$ and H permutes two connected $B_{r,V}$-sets $\mathcal{E}_1$ and $\mathcal{E}_2$ non-trivially. Therefore, $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)/H$ is isomorphic to $\mathcal{E}_1$ as a $B_{r,V}$-set. Consider the following canonical map between $\pi_1^{\text{ét}}(S \times_{\mathrm{Spec}\mathbb{Q}} \mathcal{U}_{r,V}, \bar{x})$-sets

$$\alpha : \mathcal{E}^{\mathrm{in}}(\mathcal{C}^*) \to (\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)/B_{r,V}) \times (\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)/H).$$

Since the action of $H \times B_{r,V}$ on $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)$ is transitive by the condition (b), the above map α is surjective. Further, by the above argument, the order of $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)/H$ (resp. $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)/B_{r,V}$) is equal to the order of $\mathcal{E}_1$ (resp. 2). Thus, α is an isomorphism of $\pi_1^{\text{ét}}(S \times_{\mathrm{Spec}\mathbb{Q}} \mathcal{U}_{r,V}, \bar{x})$-sets. Since the action of $\pi_1^{\text{ét}}(S \times_{\mathrm{Spec}\mathbb{Q}} \mathcal{U}_{r,V}, \bar{x})$ on $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)/H$ (resp. $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)/B_{r,V}$) factors through the canonical homomorphism

$$\pi_1^{\text{ét}}(S \times_{\mathrm{Spec}\mathbb{Q}} \mathcal{U}_{r,V}, \bar{x}) \to \pi_1^{\text{ét}}(\mathcal{U}_{r,V}, \bar{x}') \text{ (resp. } \pi_1^{\text{ét}}(S \times_{\mathrm{Spec}\mathbb{Q}} \mathcal{U}_{r,V}, \bar{x}) \to \pi_1^{\text{ét}}(S, \bar{s})),$$

$H(\mathcal{C}^*)_V$ is of the form $S' \times_{\mathrm{Spec}\mathbb{Q}} W$ where S' (resp. W) is a finite étale covering of S (resp. $\mathcal{U}_{r,V}$). Since the étale fundamental group of S acts on a geometric fiber of $H(\mathcal{C}^*)_V \to S \times_{\mathrm{Spec}\mathbb{Q}} \mathcal{U}_{r,V}$ via ρ, S' is an étale double cover of S (cf. the condition (c)). Thus, S' is isomorphic to $\mathbb{G}_{m,\mathbb{Q}}$ and the covering morphism $S' \to S$ is defined by $\mathbb{G}_{m,\mathbb{Q}} \to \mathbb{G}_{m,\mathbb{Q}}, x \to ax^2$ for some $a \in \mathbb{Q}^\times$.

To prove the existence of a $\mathbb{Q}$-rational point of $H(\mathcal{C}^*)_V$, it is enough to prove W is a rational variety over $\mathbb{Q}$ because $S' \cong \mathbb{G}_{m,\mathbb{Q}}$. The finite étale covering $W \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \to \mathcal{U}_{r,V} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ corresponds to the $B_{r,V}$-set $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)/H$. Recall that $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)/H$ is isomorphic to $\mathcal{E}_1$ as $B_{r,V}$-sets. Hence, by the condition (a), there exists an element $s \in \mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)/H$ such that $g_j(s) = 0$ for any $1 \leq j \leq r-1$ and the oddness condition (O_j) holds for s. Therefore, we deduce from Proposition 3.21 that W is a rational variety over $\mathbb{Q}$. □

The following theorem is one of the main results of this paper:

THEOREM 3.23. *Let G be a finite group such that the center of $\overline{G} := G/Z(G)$ is trivial. Let r be a positive integer, $\mathcal{C}$ an r-tuple of conjugacy classes of G and H a subgroup of* $\mathrm{Aut}(G)$. *Assume that the triple $(G, H, \mathcal{C})$ satisfies the conditions* (a), (b) *and* (c) *of Proposition* 3.22. *Furthermore, assume that the following condition* (d) *is satisfied*:

(d) *The r-tuple of conjugacy classes $\mathcal{C}$ is not V-symmetric.*

Let $\overline{G}'$ be the subgroup of $\mathrm{Aut}(\overline{G})$ *generated by $\overline{G} = \mathrm{Inn}(\overline{G})$ and the image of H in* $\mathrm{Aut}(\overline{G})$. *Then, the set of $\mathbb{Q}$-rational points $H^r(\mathcal{G}_\rho/\mathbb{G}_{m,\mathbb{Q}})(\mathbb{Q})$ is non-empty. For any $\mathbb{Q}$-rational point $x \in H^r(\mathcal{G}_\rho/\mathbb{G}_{m,\mathbb{Q}})(\mathbb{Q})$, we have $\overline{G}_x = \overline{G}'$ (see above Corollary* 2.21 *for the definition of $\overline{G}_x$). In particular, $\overline{G}'$ appears as a quotient of the absolute Galois group $G_\mathbb{Q}$ of $\mathbb{Q}$.*

PROOF. Let us take the same notation as in Proposition 3.22 and we put $\bar{\rho} := \rho \pmod{Z(G)}$. According to Proposition 3.22, there exists a $\mathbb{Q}$-rational point $y \in (H^r(\mathcal{G}_\rho/\mathbb{G}_{m,\mathbb{Q}}) \times_{\widetilde{\mathcal{U}}_r} \mathcal{U}_{r,V})(\mathbb{Q})$. We denote by x the image of y under the canonical projection $H^r(\mathcal{G}_\rho/\mathbb{G}_{m,\mathbb{Q}}) \times_{\widetilde{\mathcal{U}}_r} \mathcal{U}_{r,V} \to H^r(\mathcal{G}_\rho/\mathbb{G}_{m,\mathbb{Q}})$. Since $\mathrm{Im}(\bar{\rho}_x) \subset \mathrm{Im}(\bar{\rho})$, the group $\overline{G}_x$ is contained in $\overline{G}' = \mathrm{Inn}(\overline{G})\mathrm{Im}(\bar{\rho})$ and it contains $\mathrm{Inn}(\overline{G})$. Since $\mathcal{C}$ is not V-symmetric, $\overline{G}_x$ does not coincide with $\mathrm{Inn}(\overline{G})$ (cf. Corollary 3.19). Since $\mathrm{Inn}(\overline{G}) \subset \overline{G}_x \subset \overline{G}'$ and $[\overline{G}' : \mathrm{Inn}(\overline{G})] = 2$ (cf. the condition (c)), we have $\overline{G}' = \overline{G}_x$. The last assertion follows from Proposition 2.20 and Proposition 1.2. □

COROLLARY 3.24. *Let G be a finite group such that the center of $\overline{G} := G/Z(G)$ is trivial. Let $\mathcal{C} = (C_1, \ldots, C_r)$ be an r-tuple of conjugacy classes of G and H a subgroup*

of $\mathrm{Aut}(G)$. *Assume that the following three conditions are satisfied*:

(b′) *The group* H *acts on* $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)$ *transitively.*
(c′) *The group* H *is isomorphic to* $(\mathbb{Z}/f\mathbb{Z}) \rtimes (\mathbb{Z}/f\mathbb{Z})^\times$ *for some odd positive integer* f *and the action of* H *on* $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)$ *factors through* $H \twoheadrightarrow (\mathbb{Z}/f\mathbb{Z})^\times \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$.
(d′) *For some* $1 \leq j \leq r$, *the conjugacy class* C_j *is not rational.*

Then, $\overline{G}'$ *appears as a quotient of* $G_{\mathbb{Q}}$.

PROOF. It is sufficient to show that $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ is singleton. Indeed, if $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ is singleton, then the condition (a) of Proposition 3.22 is automatically satisfied. Because H acts on $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)$ transitively, the condition (b) of Proposition 3.22 is satisfied. The condition (c) of Proposition 3.22 and the condition (c′) of this corollary are the same. By the conditions (b′) and (c′) of this corollary, the order of $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)$ is less than or equal to 2. On the other hand, $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)$ does not coincide with $\mathcal{E}^{\mathrm{in}}(\mathcal{C})$ because C_j is not rational. Therefore, we have $\sharp\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*) = 2$ and $\sharp\mathcal{E}^{\mathrm{in}}(\mathcal{C}) = 1$. This completes the proof of the corollary. □

REMARK 3.25. A finite étale $\overline{G}'$-covering whose existence is guaranteed in the proof of Theorem 3.23 is *not* geometrically connected because $\overline{G}' \neq \mathrm{Inn}(\overline{G}) = \overline{G}$ (cf. Corollary 2.21). Therefore, Theorem 3.23 is not useful to solve the Regular Inverse Galois Problem (for the Regular Inverse Galois Problem, see [**Fr-Vö**, Introduction]).

4. An Application to the Inverse Galois Problem.

In this section, we give an application of our Main theorem to the Inverse Galois Problem.

4.1. Middle convolution functors.

In this subsection, we recall definitions and basic properties of middle convolution functors given in [**D-R**]. We fix a positive integer r and a field K. We denote the free group of rank r by $\mathcal{F}_r$. We fix a set of generators $\{\sigma_1^{(r)}, \ldots, \sigma_r^{(r)}\}$ of $\mathcal{F}_r$.

DEFINITION 4.1. We denote the category of finite dimensional linear representations of $\mathcal{F}_r$ over K by $\mathrm{Rep}_K(\mathcal{F}_r)$. In other words, $\mathrm{Rep}_K(\mathcal{F}_r)$ is the category of pairs (V, ρ_V), where V is a finite dimensional K-vector space and $\rho_V : \mathcal{F}_r \to GL(V)$ is a group homomorphism. We often denote an object (V, ρ_V) of $\mathrm{Rep}_K(\mathcal{F}_r)$ by V.

We often identify an object (V, ρ_V) of $\mathrm{Rep}_K(\mathcal{F}_r)$ with an r-tuple of elements $(\rho_V(\sigma_1^{(r)}), \ldots, \rho_V(\sigma_r^{(r)}))$ of $GL(V)$.

DEFINITION 4.2 ([**D-R**, Definition 2.2]). Let (V, ρ_V) be an object of $\mathrm{Rep}_K(\mathcal{F}_r)$. For each $\lambda \in K^\times$, we define a functor

$$\mathrm{C}_\lambda^{(r)} : \mathrm{Rep}_K(\mathcal{F}_r) \to \mathrm{Rep}_K(\mathcal{F}_r)$$

as follows: For $1 \leq i \leq r$, we set $X_i := \rho_V(\sigma_i^{(r)})$. We define $\mathrm{C}_\lambda^{(r)}((V, \rho_V)) := (V^r, \mathrm{C}_\lambda^{(r)}(\rho_V))$, where $\mathrm{C}_\lambda^{(r)}(\rho_V)$ is a representation of $\mathcal{F}_r$ on V^r of dimension $r \cdot \dim V$

such that $\mathrm{C}_\lambda^{(r)}(\rho_V)(\sigma_i^{(r)})$ is defined to be the following matrix:

$$\begin{array}{c} \\ i \\ \\ \\ \\ r-i \\ \\ \end{array}\!\!\begin{array}{c} \overbrace{\qquad\qquad}^{i} \quad \overbrace{\qquad\qquad\qquad\qquad\qquad\qquad}^{r-i} \\ \left(\begin{array}{ccccccc} \mathrm{Id}_V & & & & & & \\ & \mathrm{Id}_V & & & & & \\ & & \ddots & & & & \\ X_1-\mathrm{Id}_V & X_2-\mathrm{Id}_V & \cdots & \lambda X_i & \lambda(X_{i+1}-\mathrm{Id}_V) & \cdots & \lambda(X_r-\mathrm{Id}_V) \\ & & & & \mathrm{Id}_V & & \\ & & & & & \ddots & \\ & & & & & & \mathrm{Id}_V \end{array}\right) \end{array}$$

LEMMA 4.3 ([**D-R**, Lemma 2.4]). *Let (V,ρ_V) be an object of $\mathrm{Rep}_K(\mathcal{F}_r)$ and λ an element of $K^\times$. Then, the subspaces*

$$\mathcal{K}_\lambda^{(r)}((V,\rho_V)) := {}^t(\mathrm{Ker}(\rho_V(\sigma_1^{(r)})-\mathrm{Id}_V),\dots,\mathrm{Ker}(\rho_V(\sigma_r^{(r)})-\mathrm{Id}_V))$$

and

$$\mathcal{L}_\lambda^{(r)}((V,\rho_V)) := \bigcap_{i=1}^{r}\mathrm{Ker}\big(\mathrm{C}_\lambda^{(r)}(\rho_V)(\sigma_i^{(r)})-\mathrm{Id}_V\big)$$

of the underlying K-vector space of $\mathrm{C}_\lambda^{(r)}(V)$ are stable under the action of $\mathcal{F}_r$.

We recall the definition of the middle convolution functor $\mathrm{MC}_\lambda^{(r)}$.

DEFINITION 4.4 ([**D-R**, Definition 2.5]). For each element λ of $K^\times$, we define the *middle convolution functor* $\mathrm{MC}_\lambda^{(r)}$, which is a functor from $\mathrm{Rep}_K(\mathcal{F}_r)$ to itself, as follows:

$$\mathrm{MC}_\lambda^{(r)}((V,\rho_V)) := \mathrm{C}_\lambda^{(r)}((V,\rho_V))/\big(\mathcal{K}_\lambda^{(r)}((V,\rho_V))+\mathcal{L}_\lambda^{(r)}((V,\rho_V))\big).$$

In the paper [**D-R**], Dettweiler and Reiter showed basic properties of middle convolution functors. We recall some of their results.

LEMMA 4.5 ([**D-R**, Lemma 2.7 (b)]). *For an element $\lambda\in K^\times\setminus\{1\}$, we have the following equality*:

$$\dim(\mathrm{MC}_\lambda^{(r)}((V,\rho_V))) = \sum_{i=1}^{r}\mathrm{rk}(\rho_V(\sigma_i^{(r)})-\mathrm{Id}_V) - \dim\mathrm{Ker}\big(\lambda\rho_V(\sigma_1^{(r)})\cdots\rho_V(\sigma_r^{(r)})-\mathrm{Id}_V\big).$$

LEMMA 4.6 ([**D-R**, Corollary 4.2]). *Let (V,ρ_V) be an object of $\mathrm{Rep}_K(\mathcal{F}_r)$ satisfying*

one of the following conditions (a) *or* (b):

(a) $\dim V \geq 2$ *and the representation* (V, ρ_V) *of* $\mathcal{F}_r$ *is irreducible.*
(b) $\dim V = 1$ *and at least two of* $\rho_V(\sigma_i^{(r)})$ *are non-trivial.*

We put $(W, \rho_W) := \mathrm{MC}_\lambda^{(r)}((V, \rho_V))$. *Then, we have the following equalities*:

$$\mathrm{rk}\big(\rho_V(\sigma_i^{(r)}) - \mathrm{Id}_V\big) = \mathrm{rk}\big(\rho_W(\sigma_i^{(r)}) - \mathrm{Id}_W\big) \text{ for } 1 \leq i \leq r$$

and

$$\mathrm{rk}\big(\lambda\rho_V(\sigma_1^{(r)}) \cdots \rho_V(\sigma_r^{(r)}) - \mathrm{Id}_V\big) = \mathrm{rk}\big(\rho_W(\sigma_1^{(r)}) \cdots \rho_W(\sigma_r^{(r)}) - \lambda\mathrm{Id}_W\big).$$

LEMMA 4.7 ([**D-R**, Proposition 3.5, Theorem 3.6]). *Let* $\mathcal{R}$ *be a full subcategory of* $\mathrm{Rep}_K(\mathcal{F}_r)$ *whose objects are direct sums of objects satisfying one of the conditions* (a) *or* (b) *in Lemma* 4.6. *Then the middle convolution functor* $\mathrm{MC}_\lambda^{(r)}$ *induces an equivalence of categories* $\mathrm{MC}_\lambda^{(r)} : \mathcal{R} \xrightarrow{\sim} \mathcal{R}$. *Moreover, the functor* $\mathrm{MC}_{\lambda^{-1}}^{(r)}$ *is a quasi-inverse of* $\mathrm{MC}_\lambda^{(r)}$. *In particular, for* $(V, \rho_V) \in \mathcal{R}$ *and* $\lambda \in K^\times$, (V, ρ_V) *is irreducible if and only if* $\mathrm{MC}_\lambda^{(r)}((V, \rho_V))$ *is irreducible.*

The following property is important for our applications:

LEMMA 4.8 ([**D-R**, Corollary 5.10]). *Let* (V, ρ_V) *be an object of* $\mathrm{Rep}_K(\mathcal{F}_r)$ *of dimension* n. *If* $\mathrm{Im}(\rho_V)$ *is a subgroup of a symplectic group of size* n (*resp. an orthogonal group of size* n), *then* $\mathrm{Im}(\mathrm{MC}_{-1}^{(r)}(\rho_V))$ *is a subgroup of an orthogonal group of size* m (*resp. a symplectic group of size* m), *where* $m = \dim \mathrm{MC}_{-1}^{(r)}((V, \rho_V))$.

4.2. The linearly rigidity.

Here, we recall the notion of the linearly rigidity and recall some properties of linearly rigid tuples. We fix a positive integer r and a field K.

DEFINITION 4.9. (1) Let V be a finite dimensional K-vector space and $(g_1, \ldots, g_r)$ an r-tuple of elements of $GL(V)$. We put $g_{r+1} := (g_1 g_2 \cdots g_r)^{-1}$. We say that $(g_1, \ldots, g_r)$ is *linearly rigid* if, for any $g_i' \in O_{GL(V)}(g_i)$ $(1 \leq i \leq r+1)$, there exists $g \in GL(V)$ such that $g_i' = g g_i g^{-1}$ for any $1 \leq i \leq r+1$.
(2) Let (V, ρ_V) be an object of $\mathrm{Rep}_K(\mathcal{F}_r)$. We say that (V, ρ_V) is *linearly rigid* if $(\rho_V(\sigma_1^{(r)}), \ldots, \rho_V(\sigma_r^{(r)}))$ is linearly rigid.

REMARK 4.10. By definition, 1-dimensional linear representations of $\mathcal{F}_r$ over K are automatically linearly rigid.

The following proposition is easily checked by the definition of the linearly rigidity.

PROPOSITION 4.11. *Let* V *be a finite dimensional* K*-vector space and* $(g_1, \ldots, g_r)$ *a linearly rigid* r*-tuple of elements of* $GL(V)$ *satisfying* $g_1 \cdots g_r = 1$. *Let* $G := \langle g_1, \ldots, g_r \rangle$ *be the subgroup of* $GL(V)$ *generated by* $\{g_1, \ldots, g_r\}$, $N := N_{GL(V)}(G)$ *the normalizer of* G *in* $GL(V)$ *and* $\mathcal{C} := (O_G(g_1), \ldots, O_G(g_r))$. *Assume that the index* $[N : G]$ *divides* $\sharp G$

and that the conjugacy class $O_N(g_i)$ of N containing g_i is rational for any $1 \leq i \leq r$. Then, N acts on $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)$ transitively.

PROOF. Take $[g'_1, \ldots, g'_r] \in \mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)$. Then, by definition, there exists a positive integer n prime to $\sharp G$ such that $g'_i \in O_G(g_i)^n$. Since $[N : G]$ divides $\sharp G$, n is also prime to $\sharp N$. Therefore, by the assumption that $O_N(g_i)$ is rational, we have $O_N(g_i)^n = O_N(g_i)$. Note that $O_N(g_i)$ is contained in $O_{GL(V)}(g_i)$. Thus, by the definition of the linearly rigidity, there exists $h \in GL(V)$ satisfying $hg'_ih^{-1} = g_i$ for any $1 \leq i \leq r$. It is clear that $h \in N$. This completes the proof of the proposition. □

LEMMA 4.12 ([**D-R**, Corollary 4.4]). *Let (V, ρ_V) be an object of $\mathrm{Rep}_K(\mathcal{F}_r)$. If V is linearly rigid and satisfies one of the conditions* (a) *or* (b) *of Lemma* 4.6*, then $\mathrm{MC}^{(r)}_\lambda((V, \rho_V))$ is also linearly rigid for any $\lambda \in K^\times$.*

4.3. Group theoretic preliminaries.

In this subsection, we recall some group theoretic lemmata on symplectic groups over finite fields which we will use later. In this subsection, we fix an odd prime p. Let q be a power of p.

DEFINITION 4.13. Let K be a field and n a positive integer. We say that an element $g \in GL_n(K)$ is a *transvection* if g is unipotent and $\mathrm{rk}(g - E_n) = 1$.

LEMMA 4.14 ([**Wa**, Theorem 1.1]). *Let n be a positive integer greater than 2 and H an irreducible subgroup of $GL_n(\mathbb{F}_q)$ generated by transvections. Then, one of the following holds*:

(a) *H is conjugate to the special linear group $SL_n(\mathbb{F}_{q_0})$ for some $\mathbb{F}_{q_0} \subset \mathbb{F}_q$.*
(b) *n is even, and H is conjugate to the symplectic group $Sp_n(\mathbb{F}_{q_0})$ for some $\mathbb{F}_{q_0} \subset \mathbb{F}_q$.*
(c) *H is conjugate to the special unitary group $SU_n(\mathbb{F}_{q_0})$ for some $\mathbb{F}_{q_0^2} \subset \mathbb{F}_q$.*

We recall the definition of $Sp_{2n}(\mathbb{F}_q)$ and $GSp_{2n}(\mathbb{F}_q)$. Let $\Omega_{2n} \in GL_{2n}(\mathbb{F}_q)$ be the block diagonal symplectic matrix defined by

$$\Omega_{2n} := \begin{pmatrix} 0 & 1 & & & \\ -1 & 0 & & & \\ & & \ddots & & \\ & & & 0 & 1 \\ & & & -1 & 0 \end{pmatrix}.$$

Then, we define $Sp_{2n}(\mathbb{F}_q)$ (resp. $GSp_{2n}(\mathbb{F}_q)$) to be $\{g \in GL_{2n}(\mathbb{F}_q) \mid g\Omega_{2n}g^t = \Omega_{2n}\}$ (resp. $\{g \in GL_{2n}(\mathbb{F}_q) \mid g\Omega_{2n}g^t = a\Omega_{2n}$ for some $a \in \mathbb{F}_q^\times\}$), where g^t is the transpose of g. Further, we define $PSp_{2n}(\mathbb{F}_q)$ (resp. $PGSp_{2n}(\mathbb{F}_q)$) to be the quotient of $Sp_{2n}(\mathbb{F}_q)$ (resp. $GSp_{2n}(\mathbb{F}_q)$) by its center.

LEMMA 4.15. *There exists a group homomorphism $\nu : \mathbb{F}_q \rtimes \mathbb{F}_q^\times \hookrightarrow GSp_{2n}(\mathbb{F}_q)$ such that the composite of ν with the canonical group homomorphism*

$$GSp_{2n}(\mathbb{F}_q) \to PGSp_{2n}(\mathbb{F}_q)/PSp_{2n}(\mathbb{F}_q) \cong \mathbb{Z}/2\mathbb{Z}$$

is surjective. Moreover, the image of ν *in* $\mathrm{Aut}(PSp_{2n}(\mathbb{F}_q))$ *is not contained in* $\mathrm{Inn}(PSp_{2n}(\mathbb{F}_q))$.

PROOF. Let $V := \mathbb{F}_q^{2n}$ and $(\ ,\ )$ the standard symplectic form on V defined by Ω_{2n}. Then, there exists a basis $e_1, \ldots, e_n, f_1, \ldots, f_n$ satisfying $(e_i, e_j) = 0$, $(f_i, f_j) = 0$, $(e_i, f_j) = \delta_{i,j}$ for all i, j (cf. [**K-L**, Chapter 2, Proposition 2.4.1]). Set $V_1 := \mathbb{F}_q e_1 + \mathbb{F}_q f_1$ and $(\ ,\ )_1$ the restriction of $(\ ,\ )$ to V_1. We define $\nu : \mathbb{F}_q \rtimes \mathbb{F}_q^\times \hookrightarrow GSp(V, (\ ,\ ))$ as follows:

$$\nu(y, x)(e_i) := xe_i + yf_i,\ \nu(y, x)(f_i) := f_i \text{ for } y \in \mathbb{F}_q,\ x \in \mathbb{F}_q^\times.$$

By definition, ν is a group homomorphism. Moreover, the similitude character of $\nu(y, x)$ is equal to x. Therefore, the composite of ν with $GSp(V, (\ ,\ )) \to PGSp(V, (\ ,\ ))/PSp(V, (\ ,\ )) \cong \mathbb{Z}/2\mathbb{Z}$ is surjective.

By construction, $\nu(0, x)$ acts on $PSp_{2n}(\mathbb{F}_q)$ non-trivially and is not contained in $PSp_{2n}(\mathbb{F}_q)$ if $x \in \mathbb{F}_q^\times \setminus (\mathbb{F}_q^\times)^2$. This implies the last assertion. □

REMARK 4.16. We call a basis $\{e_1, \ldots, e_n, f_1, \ldots, f_n\}$ of V satisfying $(e_i, e_j) = 0$, $(f_i, f_j) = 0$, $(e_i, f_j) = \delta_{i,j}$ a standard basis of $(\mathbb{F}_q^{2n}, (\ ,\ ))$. According to the proof of [**K-L**, Chapter 2, Proposition 2.6], for any two non-zero vectors $v_1, v_2 \in \mathbb{F}_q^{2n}$ with $(v_1, v_2) \neq 0$, there exists $a \in \mathbb{F}_q^\times$ such that $\{av_1, v_2\}$ is a part of a standard basis of $(\mathbb{F}_q^{2n}, (\ ,\ ))$.

LEMMA 4.17. *Let* $V = (\mathbb{F}_q^{2n}, (\ ,\ ))$ *be a symplectic space and* $g \in Sp(V)$ *a transvection. Then, there exist a standard basis* $\{e_1, \ldots, e_n, f_1, \ldots, f_n\}$ *and* $a \in \mathbb{F}_q^\times$ *satisfying the following conditions*:

$$g(e_1) = e_1 + af_1,\ g(e_i) = e_i,\ g(f_j) = f_j \text{ for all } 2 \leq i \leq n \text{ and } 1 \leq j \leq n.$$

PROOF. We remark that $(g-1)V$ is a 1-dimensional $\mathbb{F}_q$-vector space which is contained in $V^{g=1}$ because g is a transvection. Let v and w be non-zero elements of V satisfying $(g-1)v = w$. If $(v, w) \neq 0$, then there exist an element $a \in \mathbb{F}_q^\times$ and a standard basis $\{e_1, \ldots, e_n, f_1, \ldots, f_n\}$ of V satisfying $e_1 = av$ and $f_1 = w$ (cf. Remark 4.16). We shall show that $\{v, w\}^\perp$ is contained in $V^{g=1}$. Let z be an element of $\{v, w\}^\perp$. Then, we have $0 = (z, v) = (g(z), g(v)) = (g(z), v + w)$ and $0 = (z, w) = (g(z), g(w)) = (g(z), w)$. Therefore, the equality $(g(z), v) = 0$ holds. On the other hand, there exists $z' \in V^{g=1}$ and $\alpha \in \mathbb{F}_q$ such that $z = \alpha v + z'$ because the dimension of $V^{g=1}$ is $n-1$ and $v \notin V^{g=1}$. Since $(z, v) = 0$, z' is orthogonal to v. Therefore, we obtain the following equalities:

$$0 = (g(z), v) = (\alpha v + \alpha w + z', v) = \alpha(w, v) + (z', v) = \alpha(w, v).$$

This implies that $\alpha = 0$. Therefore, the basis $\{e_1, \ldots, e_n, f_1, \ldots, f_n\}$ satisfies the condition of the lemma. Next, we assume $(v, w) = 0$. In this case, there exists a non-zero element $w' \in V^{g=1}$ such that $(w, w') \neq 0$ because $\mathbb{F}_q v + V^{g=1} = V$. Set $v' := v + w'$. Then, we have $(g-1)v' = w$ and $(v', w) \neq 0$. By repeating the same argument as above,

we deduce the conclusion of the lemma. □

PROPOSITION 4.18. *Let $g \in Sp_{2n}(\mathbb{F}_p)$ be a transvection. Then, the conjugacy class of g in $Sp_{2n}(\mathbb{F}_p)$ (resp. $GSp_{2n}(\mathbb{F}_p)$) is not rational (resp. rational) (See Definition 3.15 for the definition of rational conjugacy classes).*

PROOF. Assume that there exist $r \in \mathbb{Z}_{\geq 1}$ and $h \in Sp_{2n}(\mathbb{F}_p)$ such that $hgh^{-1} = g^r$. Let a be an element of $\mathbb{F}_p^\times$ and $\{e_1, \ldots, e_n, f_1, \ldots, f_n\}$ a standard basis of $\mathbb{F}_p^{2n}$ satisfying the conditions of Lemma 4.17. Put $V_1 := \mathbb{F}_p e_1 + \mathbb{F}_p f_1$ and $V_2 := V_1^\perp$. Since $hgh^{-1} = g^r$, the automorphism h stabilize $V^{g=1}$. Therefore, we have $h(f_1) = bf_1 + w$ with some $b \in \mathbb{F}_p$ and $w \in V_2$. We also write $h(e_1) = ce_1 + df_1 + w'$ with $c, d \in \mathbb{F}_p$ and $w' \in V_2$. Moreover, we obtain the following equalities by direct computations:

$$hg(e_1) = h(e_1 + af_1) = ce_1 + df_1 + w' + baf_1 + aw = ce_1 + (ab + d)f_1 + aw + w',$$
$$g^r h(e_1) = g^r(ce_1 + df_1 + w') = c(e_1 + arf_1) + df_1 + w' = ce_1 + (acr + d)f_1 + w'.$$

Since $hg = g^r h$, we have $acr + d = ab + d$ by the equalities above. Since $aw + w' = w'$, we have $w = 0$. Hence, the equality $bc = 1$ holds because $(h(e_1), h(f_1)) = (e_1, f_1) = 1$. These imply that $r = b^2 \in (\mathbb{F}_p^\times)^2$. Since p is an odd prime, there exists a positive integer $r > 1$ which is prime to the order of g and whose image in $\mathbb{F}_p$ is not contained in $(\mathbb{F}_p^\times)^2$. Therefore, the conjugacy class of g in $Sp_{2n}(\mathbb{F}_p)$ is not rational.

On the other hand, for a positive integer r prime to the order of g, the elements g and g^r are conjugate in $GSp_{2n}(\mathbb{F}_p)$. Indeed, if we define $h' \in GSp_{2n}(\mathbb{F}_p)$ by the equalities

$$h'(e_1) = re_1,\ h'(e_i) = e_i,\ h'(f_j) = f_j \ \text{ for all } 2 \leq i \leq n,\ 1 \leq j \leq n,$$

we have $h'^{-1}gh' = g^r$. Therefore, the conjugacy class of g in $GSp_{2n}(\mathbb{F}_p)$ is rational (cf. Remark 3.16). This completes the proof of the proposition. □

4.4. An application to the Inverse Galois Problem.

In this subsection, we give an application of Theorem 3.23 to the Inverse Galois Problem.

LEMMA 4.19. *Let p be an odd prime and n a positive integer greater than 1. Then, there exists an linearly rigid $(2n+1)$-tuple $(g_1, \ldots, g_{2n+1})$ of $GL_{2n}(\mathbb{F}_p)$ satisfying the following conditions*:

(a) *The product $g_1 \cdots g_{2n+1}$ is equal to $-E_{2n}$. Here, E_{2n} is the identity matrix of size $2n$.*
(b) *For any $1 \leq i \leq 2n+1$, g_i is a transvection.*
(c) *The subgroup G of $GL_{2n}(\mathbb{F}_p)$ generated by $\{g_1, \ldots, g_{2n+1}\}$ is isomorphic to $Sp_{2n}(\mathbb{F}_p)$.*

PROOF. We define the object $V := (\mathbb{F}_p, \rho)$ of $\mathrm{Rep}_{\mathbb{F}_p}(\mathcal{F}_{2n+1})$ by $\rho(\sigma_i^{(2n+1)}) := -1 \in \mathbb{F}_p^\times$. Since V is linearly rigid and satisfies the condition (b) of Lemma 4.6, $(W, \rho') := \mathrm{MC}_{-1}^{(2n+1)}(V)$ is also a linearly rigid representation (cf. Lemma 4.12). We put $g_i := \rho'(\sigma_i^{(2n+1)})$ and $G := \langle g_1, \ldots, g_{2n+1} \rangle \subset GL(W)$. According to Lemma 4.7, the group G

is an irreducible subgroup of $GL(W)$. On the other hand, by Lemma 4.6, we deduce that ranks of $g_i - \mathrm{id}_W$ are 1 for all $1 \leq i \leq 2n+1$ and $g_1 \cdots g_{2n+1} = -\mathrm{id}_W$. Moreover, by the definition of the middle convolution functor, $g_1, \ldots, g_{2n+1}$ are unipotent elements. Hence, g_i are transvections for all $1 \leq i \leq 2n+1$. According to Lemma 4.5, the dimension of W over $\mathbb{F}_p$ is equal to $2n$. Then, by Lemma 4.14 and Lemma 4.8, G is isomorphic to $Sp_{2n}(\mathbb{F}_p)$. □

Note that the normalizer N of G is isomorphic to $GSp_{2n}(\mathbb{F}_p)$. Indeed, according to [**K-L**, Chapter 2, Theorem 2.1.4], the automorphism group of $PSp_{2n}(\mathbb{F}_p)$ is isomorphic to $PGSp_{2n}(\mathbb{F}_p)$.

PROPOSITION 4.20. *Let p be an odd prime and n a positive integer greater than 1. Then, the projective general symplectic group $PGSp_{2n}(\mathbb{F}_p)$ appears as a quotient of the absolute Galois group $G_{\mathbb{Q}}$ of $\mathbb{Q}$.*

REMARK 4.21. Proposition 4.18 and Lemma 4.19 are keys of an application to the Inverse Galois Problem. If we replace $\mathbb{F}_p$ by $\mathbb{F}_{p^r}$ with an even integer $r \geq 2$, the assertion of Proposition 4.18 does not hold in general. Assume that $r \geq 2$ is even. Then, any element in $\mathbb{F}_p^{\times}$ has a square root in $\mathbb{F}_{p^r}$. We can construct $h' \in Sp_{2n}(\mathbb{F}_{p^r})$ satisfying $h'^{-1}gh' = g^s$ by using this square root. We do not know how to generalize Lemma 4.19 to $\mathbb{F}_{p^r}$ with $r \geq 2$. Therefore, we do not generalize Proposition 4.20 to general finite fields of characteristic p.

PROOF. Let $(g_1, \ldots, g_{2n+1})$ be the linearly rigid tuple of $GL_{2n}(\mathbb{F}_p)$ satisfying all conditions of Lemma 4.19 and G the subgroup of $GL_{2n}(\mathbb{F}_p)$ generated by $\{g_1, \ldots, g_{2n+1}\}$. We put $r := 2n+2$, $g_{2n+2} := -E_{2n}$ and $C_i := O_G(g_i)$ for $1 \leq i \leq 2n+2$. Since G is isomorphic to $Sp_{2n}(\mathbb{F}_p)$ (cf. Lemma 4.19), the normalizer N of G in $GL(W)$ is isomorphic to $GSp_{2n}(\mathbb{F}_p)$. Let $\nu : \mathbb{F}_p \rtimes \mathbb{F}_p^{\times} \hookrightarrow N$ be a group homomorphism satisfying the condition of Lemma 4.15. Denote by H the image of $\mathrm{Im}(\nu)$ in $\mathrm{Aut}(G)$ under the canonical homomorphism $N \to \mathrm{Aut}(G)$.

CLAIM 1. *The triple $(G, H, \mathcal{C} := (C_1, \ldots, C_r))$ satisfies the three conditions of Corollary 3.24.*

We give a proof of the theorem under the assumption that Claim 1 holds. Let $\overline{G}$ be $G/Z(G)$. According to Lemma 4.15, the image of H in $\mathrm{Aut}(\overline{G}) \cong PGSp_{2n}(\mathbb{F}_p)$ is not contained in $\mathrm{Inn}(\overline{G}) = \overline{G} \cong PSp_{2n}(\mathbb{F}_p)$. Thus, the subgroup $\overline{G}'$ of $\mathrm{Aut}(\overline{G})$, which is generated by the image of H and $\mathrm{Inn}(\overline{G})$, coincides with $\mathrm{Aut}(\overline{G})$ because $[PGSp_{2n}(\mathbb{F}_p) : PSp_{2n}(\mathbb{F}_p)] = 2$. Thus, $\overline{G}'$ is isomorphic to $PGSp_{2n}(\mathbb{F}_p)$. According to Corollary 3.24, there exists a Galois extension of $\mathbb{Q}$ with Galois group $\overline{G}'$. This is the assertion that we want to show.

Let us show Claim 1. According to Proposition 4.18, any conjugacy class of $Sp_{2n}(\mathbb{F}_p)$ containing a transvection is not a rational conjugacy class of $Sp_{2n}(\mathbb{F}_p)$. Thus, the condition (d′) of Corollary 3.24 is satisfied. Furthermore, any conjugacy class of $GSp_{2n}(\mathbb{F}_p)$ containing a transvection is rational (cf. Proposition 4.18), we deduce that N acts on $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)$ transitively (cf. Proposition 4.11). On the other hand, the composite of the

canonical homomorphism $\mathbb{F}_p \rtimes \mathbb{F}_p^\times \hookrightarrow N \to \mathrm{Inn}(N)/\mathrm{Inn}(G) \cong \mathbb{Z}/2\mathbb{Z}$ is surjective (cf. Lemma 4.15). Thus, H acts on $\mathcal{E}^{\mathrm{in}}(\mathcal{C}^*)$ transitively. Therefore, the condition (b′) is satisfied. The condition (c′) is checked by the construction of an injection $\nu : \mathbb{F}_p \rtimes \mathbb{F}_p^\times \hookrightarrow N$. This completes the proof of Claim 1. □

References

[A-V] S. Arias-de-Reyna and N. Vila, Tame Galois realizations of $GSp_4(\mathbb{F}_\ell)$ over $\mathbb{Q}$, Int. Math. Res. Not. IMRN, **2011**, no. 9, 2028–2046.

[AAKMTV] S. Arias-de-Reyna, C. Armana, V. Karemaker, M. Rebolledo, L. Thomas and N. Vila, Galois representations and Galois realizations over $\mathbb{Q}$, preprint, arXiv:1407.5802v1 (2014).

[B-R] J. Bertin and M. Romagny, Champs de Hurwitz, Mém. Soc. Math. Fr. (N.S.) **125–126** (2011).

[B-W] I. Bouw and S. Wewers, Reduction of covers and Hurwitz spaces, J. Reine Angew. Math., **574** (2004), 1–49.

[D-M] P. Deligne and D. Mumford, The irreducibility of the space of curves of given genus, Inst. Hautes Études Sci. Publ. Math., **36** (1969), 75–109.

[D-R] M. Dettweiler and S. Reiter, An algorithm of Katz and its application to the Inverse Galois Problem, J. Symbolic Comput., **30** (2000), 761–798.

[Fr] M. Fried, Fields of definition of function fields and Hurwitz families, groups as Galois groups, Comm. Algebra, **5** (1977), no. 1, 17–82.

[Fu] W. Fulton, Hurwitz schemes and irreducibility of moduli of algebraic curves, Ann. of Math. (2), **90** (1969), 542–575.

[Fr-Vö] M. Fried and H. Völklein, The inverse Galois problem and rational points on moduli spaces, Math. Ann., **290** (1991), 771–800.

[H] C. Hall, An open-image theorem for a general class of abelian varieties with an appendix by Emmanuel Kowalski, Bull. Lond. Math. Soc., **43** (2011), no. 4, 703–711.

[K-L] P. Kleidman and M. Liebeck, The subgroup structure of the finite classical groups, London Mathematical Society Lecture Note Series, **129**, Cambridge University Press, Cambridge, 1990.

[M-M] G. Malle and B. H. Matzat, Inverse Galois theory, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1999.

[M] S. Mochizuki, The geometry of the compactification of the Hurwitz scheme, Publ. Res. Inst. Math. Sci., **31** (1995), no. 3, 355–441.

[R] M. Romagny, Group actions on stacks and applications, Michigan Math. J., **53** (2005), no. 1, 209–236.

[Th] J. G. Thompson, Some finite groups which appear as $\mathrm{Gal}(L/K)$ where $K \subset \mathbb{Q}(\mu_n)$, J. Algebra, **89** (1984), no. 2, 437–499.

[Vö] H. Völklein, Groups as Galois groups: An introduction, Cambridge Studies in Advanced Mathematics, **53**, Cambridge University Press, Cambridge, 1996.

[Wa] A. Wagner, Groups generated by elations, Abh. Math. Sem. Univ. Hamburg, **41** (1974), 190–205.

[We] S. Wewers, Construction of Hurwitz spaces, Thesis, preprint no. 21 of IEM, Essen (1998).

[SGA1] Rêvetements étales et groupe fondamental, Séminaire de Géométrie Algébrique du Bois Marie 1960–1961 (SGA1), dirigé par A. Grothendieck, augmenté de deux exposés de M. Raynaud, Springer Lecture Notes in Math., **224**, Springer-Verlag, Berlin-New York, 1971.

Kenji Sakugawa
Department of Mathematics
Graduate School of Science
Osaka University
Toyonaka
Osaka 560-0043, Japan
E-mail: k-sakugawa@cr.math.sci.osaka-u.ac.jp