SUT Journal of Mathematics
Vol. 53, No. 1 (2017), 73–85

On two-dimensional Galois representations with squarefree conductor

Masanari Kida and Yusuke Sudo

(Received April 1, 2017; Revised June 14, 2017)

Abstract. The isomorphism classes of the images of irreducible two-dimensional Galois representations with squarefree conductor are determined.

AMS 2010 *Mathematics Subject Classification.* 11F80.

Key words and phrases. Galois representation, Artin conductor, isoclinism.

§1. Introduction

Let $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group of the field of rational numbers and ρ a continuous representation on a two-dimensional complex vector space V:

$$\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(V).$$

The kernel of the representation ρ is of finite index in $G_{\mathbb{Q}}$; hence the image is a finite subgroup of $\mathrm{GL}(V) \cong \mathrm{GL}(2, \mathbb{C})$. Thus ρ induces a faithful representation of a finite group $\mathrm{Gal}(K/\mathbb{Q})$ on V, where K is the subfield of $\bar{\mathbb{Q}}$ fixed by $\ker \rho$. The representation ρ is called *odd* if $\det(\rho(c))$ of a complex conjugation $c \in G_{\mathbb{Q}}$ is -1, and called *even* otherwise.

For a prime number p, let $G^{(i)}$ be the i-th higher ramification group of a prime ideal $\mathfrak{p}$ lying above p in $G_{\mathbb{Q}}$. We define the local conductor at p by

$$f(\rho, p) = \sum_{i=0}^{\infty} \frac{|G^{(i)}|}{|G^{(0)}|} \left(\chi(1) - \chi(G^{(i)})\right)$$

where χ is the character afforded by the representation ρ. It is shown that the local conductor is independent of the choice of the prime ideal $\mathfrak{p}$ lying above p and is a non-negative integer. In particular, the local conductor is 0 if the

inertia group of $\mathfrak{p}$ acts trivially on V, and hence it is 0 for all but finitely many primes p. Moreover $f(\rho, p) \leq 2$ holds if p is tamely ramified in $K/\mathbb{Q}$.

The Artin conductor of ρ is defined by

$$N = N(\rho) = \prod_p p^{f(\rho,p)},$$

where p runs over all prime numbers. It measures how wild the ramification in $K/\mathbb{Q}$ is.

By the theorems by Deligne-Serre [10] and Khare-Wintenberger [7], there exists a one-to-one correspondence between odd two-dimensional irreducible Galois representations ρ with conductor N and normalized newforms of weight one and level N with character $\det \rho$. Therefore it is natural to ask how far this correspondence reaches. In this paper, we answer this question in terms of the image of the Galois representation under certain condition on the Artin conductor. To be more precise, we determine the possible isomorphism classes of the image $\rho(G_{\mathbb{Q}})$ under the assumption that $N(\rho)$ is squarefree.

In Section 8 of [10], Serre gave a certain classification of two-dimensional odd Galois representations of prime conductor. In [9], Nakazato extended Serre's result to determine possible orders of $\rho(G_{\mathbb{Q}})$ if ρ is of icosahedral type. Thus our result can be considered as an extension and a refinement of their results.

To state our main theorem, let us recall the fact about the associated projective representation $\tilde{\rho}$:

$$\begin{array}{ccc} G_{\mathbb{Q}} & \xrightarrow{\rho} & \mathrm{GL}(V) \\ & \searrow^{\tilde{\rho}} & \downarrow \\ & & \mathrm{PGL}(V), \end{array}$$

where the vertical map is a natural projection. The image of $\tilde{\rho}$ is a finite subgroup of $\mathrm{PGL}(2, \mathbb{C})$ and the finite subgroups of $\mathrm{PGL}(2, \mathbb{C})$ are completely classified. If $\tilde{\rho}$ is reduced, then $\tilde{\rho}(G_{\mathbb{Q}})$ is isomorphic to a cyclic group C_n of order n. If it is irreducible, then the projective image is isomorphic to one of the following groups:

$$D_n \text{ (dihedral group of order } 2n), \ A_4, \ S_4, \text{ or } A_5. \tag{1.1}$$

We say that the representation ρ is of type H if $\tilde{\rho}(G_{\mathbb{Q}})$ is isomorphic to the group H in (1.1).

Now we can state our main theorem.

Theorem 1.1. *Let ρ be a two-dimensional irreducible Galois representation. If the Artin conductor N of ρ is squarefree, then the image of ρ is isomorphic to one of the following groups:*

(i) if ρ is of type A_4, then

$$(24,3),(48,33),(72,3),(72,25),(144,36),(144,157);$$

(ii) if ρ is of type S_4, then

$$(48,29),(96,67),(96,192),(144,121),(144,122),(192,187),$$
$$(192,963),(288,400),(288,903),(576,1988),(576,5472);$$

(iii) if ρ is of type A_5, then

$$(240,93),(360,51),(600,54),(720,420),(1200,483),$$
$$(1800,328),G_1.$$

Here (m,n) denotes the n-th group of order m in the GAP finite group database and the group G_1 of order 3600 *is given by*

$$S_{32} \supset G_1 = \langle (1,2,3),(4,5,6,7,8)$$
$$(9,28,25,13,20)(10,11,17,27,18)(12,22,30,19,14)(15,16,23,21,24),$$
$$(10,26)(13,19)(14,29)(15,32)(17,25)(18,24)(20,31)(21,28)(22,27)(23,30)\rangle \tag{1.2}$$

Some partial results concerning D_n-type will also be given in Proposition 2.1.

This paper is organized as follows: In Section 2, we give upper bounds on the order of the image of ρ. In Section 3, we prove Theorem 1.1 after giving some group-theoretic preliminaries. In Section 4, we discuss an example to get representations with squarefree conductor.

§2. Upper bounds on the order of the image

In this section, we give upper bounds on the order of the image $\rho(G_{\mathbb{Q}})$ of two-dimensional irreducible Galois representations by using methods in Serre [10] and Nakazato [9]. However, we do *not* assume that ρ is odd (see Proposition 3.6 and the remark following the proposition). The main result in this section is the following proposition.

Proposition 2.1. *Let $\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(2,\mathbb{C})$ be a two-dimensional irreducible Galois representation with squarefree Artin conductor. Then the following statements hold:*

(i) if ρ is of type D_n with odd n, then

$$|\rho(G_{\mathbb{Q}})| = 2dd', 4dd', \text{ or } 8dn$$

with some divisors d, d' of n;

(ii) if ρ is of type D_n with even n, then

$$|\rho(G_{\mathbb{Q}})| = dd', 2dd', \text{ or } 4dn$$

with some divisors d, d' of n. Further if $|\rho(G_{\mathbb{Q}})| = dd'$, then at least one of d or d' is even;

(iii) if ρ is of type A_4, then

$$|\rho(G_{\mathbb{Q}})| = 24, 48, 72, \text{ or } 144;$$

(iv) if ρ is of type S_4, then

$$|\rho(G_{\mathbb{Q}})| = 48, 72, 96, 144, 192, 288, \text{ or } 576;$$

(v) (cf. [9, Theorem 1]) if ρ is of type A_5, then

$$|\rho(G_{\mathbb{Q}})| = 240, 360, 600, 720, 1200, 1800, \text{ or } 3600.$$

The proof of the proposition relies on the following lemma by Nakazato.

Lemma 2.2 ([9, Lemma 1])**.** *Let ρ be a two-dimensional irreducible Galois representation and $\tilde{\rho}$ the projective Galois representation attached to ρ. For each prime p dividing N, let I_p be the inertia group of p. If the Artin conductor N of ρ is squarefree, then, for each $p|N$, there is a one-dimensional representation ψ of I_p which is not the trivial representation 1_{I_p} satisfying*

$$\rho|_{I_p} \cong \psi \oplus 1_{I_p}. \tag{2.1}$$

Moreover, we have the following isomorphisms:

$$\tilde{\rho}(I_p) \cong \rho(I_p) \cong \det(\rho(I_p)) \cong \psi(I_p). \tag{2.2}$$

Let Q be one of the groups in (1.1) and assume ρ is of type Q.

The determination of the order of $\rho(G_{\mathbb{Q}})$ is proceeded as follows. Consider the determinant map $\det : \rho(G_{\mathbb{Q}}) \longrightarrow \mathbb{C}^{\times}$. We obviously have

$$|\rho(G_{\mathbb{Q}})| = |\mathrm{Ker}\det| \cdot |\mathrm{Im}\det|. \tag{2.3}$$

We shall determine the orders of the kernel and the image in (2.3) using the method in [9].

We first consider the image. By our assumption, every ramifying prime p in the fixed field of $\mathrm{Ker}\rho$ is tamely ramified. This implies that $\rho(I_p)$ is a cyclic group. By (2.2), it is isomorphic to a cyclic subgroup of Q. Since there is no unramified extension over $\mathbb{Q}$, $\rho(I_p)$'s must generate the whole group $\rho(G_{\mathbb{Q}})$

([9, Lemma 2]). Again by (2.2) these $\det(\rho(I_p))$'s must generate $\det(\rho(G_{\mathbb{Q}}))$, which is a group of roots of unity. We know the possible orders l of cyclic subgroups of Q:

$$\begin{aligned}
&\text{if } Q \cong D_n, \text{ then } l = 2, d \ (d|n);\\
&\text{if } Q \cong A_4, \text{ then } l = 2, 3, 6;\\
&\text{if } Q \cong S_4, \text{ then } l = 2, 3, 4, 6, 12;\\
&\text{if } Q \cong A_5, \text{ then } l = 2, 3, 5, 6, 10, 15, 30.
\end{aligned}$$

Note that $\langle \det(I_p)\rangle_{p|N} \cong \langle \tilde{\rho}(I_p)\rangle_{p|N} \subset \tilde{\rho}(G_{\mathbb{Q}})$. Since there is no element of order 4 in A_4 or A_5, the order of $\langle \det(I_p)\rangle_{p|N}$ cannot be 4 in these case. We consequently obtain the following lemma.

Lemma 2.3 (cf. [9, Theorem II])**.** *Let ρ be a two-dimensional irreducible Galois representation with squarefree Artin conductor with the determinant map* $\det : \rho(G_{\mathbb{Q}}) \longrightarrow \mathbb{C}^{\times}$. *Then the possible orders of the image of* det *are given as follows:*

$$\begin{aligned}
&\textit{if } \rho \textit{ is of type } D_n \textit{ with } n \textit{ odd, then } |\mathrm{Im}\det| = 2, d, 2d \ (d|n);\\
&\textit{if } \rho \textit{ is of type } D_n \textit{ with } n \textit{ even, then } |\mathrm{Im}\det| = 2, d \ (d|n);\\
&\textit{if } \rho \textit{ is of type } A_4, \textit{ then } |\mathrm{Im}\det| = 3, 6, 9;\\
&\textit{if } \rho \textit{ is of type } S_4, \textit{ then } |\mathrm{Im}\det| = 2, 3, 4, 6, 12, 24;\\
&\textit{if } \rho \textit{ is of type } A_5, \textit{ then } |\mathrm{Im}\det| = 2, 3, 5, 6, 10, 15, 30.
\end{aligned}$$

Proof. Everything is almost clear from the discussion above except possibly the following details. Because of (2.2), we see $|\mathrm{Im}\det| \neq 1$. By the argument in the proof of [10, Theorem 7], if ρ is of type A_4, then $|\mathrm{Im}\det| \neq 2$. □

Next we determine the order of the kernel of the determinant map in (2.3). We denote the kernel by K in this discussion. If K is trivial, then $\rho(G_{\mathbb{Q}})$ is cyclic as a subgroup of $\mathbb{C}^{\times}$; hence so is $\tilde{\rho}(G_{\mathbb{Q}})$. This means that ρ is reducible. This contradicts our assumption. Thus K is a non-trivial normal subgroup of $\rho(G_{\mathbb{Q}})$.

Let Z be the subgroup of $\rho(G_{\mathbb{Q}})$ consisting of scalar matrices. Then we have an exact sequence:

$$1 \longrightarrow Z \longrightarrow \rho(G_{\mathbb{Q}}) \longrightarrow \tilde{\rho}(G_{\mathbb{Q}}) \longrightarrow 1. \tag{2.4}$$

Since there is no faithful representation of degree 2 of A_4, S_4 and A_5, the case $Z = 1$ is possible only when ρ is of type D_n. The composition homomorphism $K \longrightarrow \rho(G_{\mathbb{Q}}) \longrightarrow \rho(G_{\mathbb{Q}})/Z \cong Q$ induces an injective homomorphism $K/K \cap Z \longrightarrow Q$. Since K is a normal subgroup of $\rho(G_{\mathbb{Q}})$, the group $K/K \cap Z$

is also isomorphic to a normal subgroup of Q. We claim that $K/K \cap Z$ is not trivial. Suppose to the contrary that $K/K \cap Z$ is trivial. Since, by definition, we have $K \cap Z = \{I\}$ or $\{\pm I\}$ with the identity matrix I, this implies that $K = \{I\}$ or $K = \{\pm I\}$. In either case, we have a surjective homomorphism $\mathrm{Im}\det \cong \rho(G_{\mathbb{Q}})/K \longrightarrow \rho(G_{\mathbb{Q}})/Z(\rho(G_{\mathbb{Q}}))$. Since $\mathrm{Im}\det$ is cyclic, it follows that $\rho(G_{\mathbb{Q}})$ is abelian. This is a contradiction. We thus conclude that $K/K \cap Z$ is isomorphic to a non-trivial normal subgroup of Q. The possible normal subgroups of Q are:

$$\begin{aligned}
&\text{if } Q \cong D_n, \text{ then } C_d \ (d|n), D_n;\\
&\text{if } Q \cong A_4, \text{ then } C_2 \times C_2, A_4;\\
&\text{if } Q \cong S_4, \text{ then } C_2 \times C_2, A_4, S_4;\\
&\text{if } Q \cong A_5, \text{ then } A_5.
\end{aligned}$$

If $K \cap Z = \{I\}$, then K cannot be one of A_4, S_4 and A_5 because these groups cannot be embedded into $\mathrm{GL}(2,\mathbb{C})$. Therefore, we obtain possible orders of $K = \mathrm{Ker}\det$.

Lemma 2.4. *Let ρ be a two-dimensional irreducible Galois representation with squarefree Artin conductor with the determinant map* $\det : \rho(G_{\mathbb{Q}}) \longrightarrow \mathbb{C}^{\times}$. *Then the possible orders of the kernel of* det *are given as follows:*

$$\begin{aligned}
&\textit{if } \rho \textit{ is of type } D_n, \textit{ then } |\mathrm{Ker}\det| = d, 2d, 4n \ (d|n);\\
&\textit{if } \rho \textit{ is of type } A_4, \textit{ then } |\mathrm{Ker}\det| = 4, 8, 24;\\
&\textit{if } \rho \textit{ is of type } S_4, \textit{ then } |\mathrm{Ker}\det| = 4, 8, 24, 48;\\
&\textit{if } \rho \textit{ is of type } A_5, \textit{ then } |\mathrm{Ker}\det| = 120.
\end{aligned}$$

Since $|\rho(G_{\mathbb{Q}})|$ must be divisible by $|Q|$, some combinations of the orders of the image and the kernel are impossible. Combining (2.3) and Lemmas 2.3 and 2.4, we have completed the proof of Proposition 2.1.

§3. The isomorphism classes of the image

In the previous section, we have determined the possible orders of $\rho(G_{\mathbb{Q}})$ when the conductor $N(\rho)$ is squarefree. In this section, we study group structure of $\rho(G_{\mathbb{Q}})$ and determine its isomorphism class.

We write $G = \rho(G_{\mathbb{Q}})$ for simplicity throughout this section. As we noted before, G is a finite group. The Galois representation ρ induces a faithful representation $G \longrightarrow \mathrm{GL}(2,\mathbb{C})$, which we also denote by ρ. By (2.4), G is a central extension of Q in (1.1) by Z:

$$1 \longrightarrow Z \longrightarrow G \longrightarrow Q \longrightarrow 1 \text{ (exact)}, \tag{3.1}$$

where Z is contained in the center $Z(G)$ of G. In this situation, Q acts on Z trivially, and there is a bijective correspondence between the (normalized) cohomology classes in $\mathrm{H}^2(Q, Z)$ and the equivalence classes of central extensions of Q by Z (see [4, Sec.17.4 Theorem 36]). Since G has a faithful representation, Z is a cyclic group by [6, (2.32)]. Since ρ is always a lifting of a projective representation of Q, namely, G has the projective lifting property (see [6, (11.11)]).

Now recall the definition of the standard map (or transgression) η of G (see [6, (11.12)]). Let $M(Q) = \mathrm{H}^2(Q, \mathbb{C}^\times)$ be the Schur multiplier, where the action of Q on $\mathbb{C}^\times$ is trivial. Let $\hat{Z} = \mathrm{Hom}(Z, \mathbb{C}^\times)$ be the character group of Z. We assume that the class of 2-cocycle f in $\mathrm{H}^2(Q, Z)$ corresponds to the extension (3.1). Then we define $\eta(\varphi)$ for $\varphi \in \hat{Z}$ by the cohomology class of $\varphi \circ f$ in $M(Q)$. The standard map η is a homomorphism. Also it is surjective if and only if G has the projective lifting property ([6, (11.13)]). Since the image of η coincides with the dual of $[G, G] \cap Z$ (see [11, Theorem 9.6]), the projective lifting property is easily verified for a given G.

If the standard map of G is bijective, then G is called a *Schur cover* (or representation group). It is not uniquely determined up to isomorphism but is determined up to isoclinism (see below for the definition). Since the Schur covers are important in the following discussion, we include a table of them. For the computation, we refer to [11, Chap.2 §9 and Chap.3 §2].

Q	$\lvert M(Q)\rvert$	Schur covers
D_n (n is odd)	1	D_n
D_n (n is even)	2	D_{2n}, Q_n
A_4	2	$(24, 3) = \mathrm{SL}(2, 3)$
S_4	2	$(48, 28) = C_2.S_4, (48, 29) = \mathrm{GL}(2, 3)$
A_5	2	$(120, 5) = \mathrm{SL}(2, 5)$

In the table, the Schur covers are specified by GAP numbers and/or Atlas names. In particular, Q_n is the generalized quaternion group of order $4n$.

We now need the following notion of isoclinism first introduced by P. Hall ([5]) and later generalized in the following form in [2, III.1.1]. To proceed the definition, we note that, for any central extension (3.1), the commutator map $k_G : G/Z \times G/Z \longrightarrow G' = [G, G]$ given by $k_G(aZ, bZ) = [a, b]$ is well-defined.

Definition 3.1. Let

$$C_1 : 1 \longrightarrow Z_1 \longrightarrow G_1 \longrightarrow Q_1 \longrightarrow 1 \quad \text{(exact)}, \tag{3.2}$$

$$C_2 : 1 \longrightarrow Z_2 \longrightarrow G_2 \longrightarrow Q_2 \longrightarrow 1 \quad \text{(exact)} \tag{3.3}$$

be central extensions. They are *isoclinic* if there exist isomorphisms $\varphi : G_1/Z_1 \xrightarrow{\sim} G_2/Z_2$ and $\psi : {G_1}' \xrightarrow{\sim} {G_2}'$ such that the following diagram is

commutative:

$$\begin{array}{ccc} G_1/Z_1 \times G_1/Z_1 & \xrightarrow{k_{G_1}} & {G_1}' \\ \downarrow{\scriptstyle \varphi\times\varphi} & & \downarrow{\scriptstyle \psi} \\ G_2/Z_2 \times G_2/Z_2 & \xrightarrow{k_{G_2}} & {G_2}'. \end{array}$$

If the two central extensions above are isoclinic, we call (φ, ψ) an *isoclinism*.

In addition, $Z_1 = Z(G_1)$ and $Z_2 = Z(G_2)$ hold, then we say that G_1 and G_2 are isoclinic groups.

Isoclinism is an equivalence relation on central extensions of finite groups and each isoclinism class contains a stem extension which is, by definition, an extension (3.1) satisfying $Z \subset G'$ (see [2, III.2.7 Proposition]). The last condition is equivalent to the injectivity of the standard map η of G ([11, Theorem 9.6]). Thus, in our case, the stem extensions are Schur covers. Since all these Schur covers satisfy $Z = Z(G)$ in (3.1), it follows from [2, III.1.4] that all groups in the isoclinism classes satisfy $Z = Z(G)$. In other words, all central extensions of Q in (1.1) are isoclinic to Schur covers of Q.

The following theorem is due to Tappe [12].

Theorem 3.2 (Tappe [12, (1.7) Theorem])**.** *Let C_1, C_2 be central extensions given by* (3.2) *and* (3.3) *respectively. Assume that $Q = Q_1 = Q_2$. Then C_1 and C_2 are isoclinic if and only if the images of the standard maps of G_1 and G_2 are same in $M(Q)$.*

Summing up the discussion above, we obtain the following proposition.

Proposition 3.3. *Let ρ be a two-dimensional irreducible Galois representation. The image $G = \rho(G_{\mathbb{Q}})$ satisfies the following properties:*

- *G is a central extension* (3.1) *of Q in* (1.1)*;*
- *the kernel Z of the extension is cyclic and coincides with $Z(G)$;*
- *the standard map of G is surjective, equivalently $|M(Q)| = |G' \cap Z|$;*
- *G is isoclinic to a Schur cover of Q.*

Note that the fourth condition follows from the third condition if we know the Schur multiplier $M(Q)$.

By these criteria, we extract possible finite groups of orders given in Proposition 2.1 from the database of small groups built in Magma [3].

Proposition 3.4. *The following tables contain the finite groups $G = \rho(G_{\mathbb{Q}})$ satisfying the conditions of Propositions 2.1 and 3.3 and admitting faithful irreducible representations with determinant conditions given in Lemmas 2.3 and 2.4.*

(i) If ρ is of type A_4, then G is isomorphic to one of the following groups:

Group ID	$\lvert Z(G)\rvert$	$\lvert\mathrm{Ker}\det\rvert$	$\lvert\mathrm{Im}\det\rvert$	*FR*	*odd*
$(24,3)$	2	8	3	2	
$(48,33)$	4	8	6	4	*Yes*
$(72,3)$	6	8	9	6	
$(72,25)$	6	24	3	6	
$(144,36)$	12	8	18	12	*Yes*
$(144,157)$	12	24	6	12	*Yes*

.

(ii) If ρ is of type S_4, then G is isomorphic to one of the following groups:

Group ID	$\lvert Z(G)\rvert$	$\lvert\mathrm{Ker}\det\rvert$	$\lvert\mathrm{Im}\det\rvert$	*FR*	*odd*
$(48,29)$	2	24	2	2	*Yes*
$(96,67)$	4	24	4	4	*Yes*
$(96,192)$	4	48	2	4	*Yes*
$(144,121)$	6	48	3	4	
$(144,122)$	6	24	6	4	*Yes*
$(192,187)$	8	24	8	8	*Yes*
$(192,963)$	8	48	4	8	*Yes*
$(288,400)$	12	24	12	8	*Yes*
$(288,903)$	12	48	6	8	*Yes*
$(576,1988)$	24	24	24	16	*Yes*
$(576,5472)$	24	48	12	16	*Yes*

(iii) If ρ is of type A_5, then G is isomorphic to one of the following groups:

Group ID	$\lvert Z(G)\rvert$	$\lvert\mathrm{Ker}\det\rvert$	$\lvert\mathrm{Im}\det\rvert$	*FR*	*odd*
$(240,93)$	4	120	2	4	*Yes*
$(360,51)$	6	120	3	4	
$(600,54)$	10	120	5	8	
$(720,420)$	12	120	6	4	*Yes*
$(1200,483)$	20	120	10	14	*Yes*
$(1800,328)$	30	120	15	16	
G_1	60	120	30	32	*Yes*

In each table, the "FR" column contains the numbers of the faithful representations with given determinant condition and the "odd" column contains "Yes" if G contains an element of order 2 which is mapped to -1 by $\det\circ\rho$ for some ρ. The group G_1 in the last row is the group defined by (1.2)

Some comments are in order.

There is no database contained in Magma for the groups of order 3600. Thus we had to compute the cohomology group to obtain $\mathrm{H}^2(A_5, C_{60}) \cong \mathbb{Z}/2\mathbb{Z}$. There are two distinct extensions: one is a split extension $A_5 \times C_{60}$ and the other is a non-split extension. Computing $G' \cap Z(G)$ reveals that the latter is the correct one. The coset action by a certain core-free subgroup gives the expression in (1.2). See [11, 2 Theorem 9.18] for some information on central extensions for perfect groups (A_5 is a perfect group).

The numbers of faithful representations of the groups can be computed by Magma. But there is a systematic way to count them. In fact, we can prove the following.

Proposition 3.5. *Let G be a stem group. Assume that $|M(G)| = 2$ and that there are m two-dimensional irreducible representations of G and n representations among them are faithful. Let H be a group isoclinic to G with cyclic kernel. Then there are $\dfrac{|H|}{|G|}m$ two-dimensional irreducible representations of H among which $\varphi(|H|)n$ representations are faithful. Here we denote by φ the Euler's totient function.*

The first half of this proposition follows from [12, (3.2) Theorem].

To obtain the number of faithful representations with given determinantal order, we compute matrix representations for solvable groups and determine the determinant character of the the representations. The method for non-solvable groups is a bit ad-hoc. We compute $Z(\rho) = \{g \in G \mid |\rho(g)| = 2\}$ for an irreducible representation ρ of degree 2. By [6, (2.27)], the image $\rho(g)$ of $g \in Z(\rho)$ is a scalar matrix, hence the determinant is easy to calculate. These determinant values usually (in our case always) determine a unique character which must agree with the determinant of ρ.

To determine whether ρ is odd is subtler. If ρ is an odd representation, then the image of the determinant contains -1, thus the order of the image of the determinant map is obviously even. Moreover, we can prove the following proposition.

Proposition 3.6. *Let G be a stem group given by* (3.1) *and H a group isoclinic to G. Assume that there exists an injection from $Z(G)$ to $Z(H)$ and that $M(Q) = 2$. Assume also that there exists an irreducible two-dimensional representation ρ of G satisfying $\mathrm{Tr}(\rho(g)) = 0$ for every element g of order 4. Then H has an irreducible two-dimensional representation whose determinant takes -1 at a conjugacy class of an element of order 2 if and only if there is an element of order 2 in H which is not contained in the center of H.*

The assumptions for the existence of such ρ are satisfied if Q is one of D_n (n is even), A_4, S_4 or A_5.

If $H = \mathrm{Gal}(K/\mathbb{Q})$ and the complex conjugation lies in $Z(H)$, then the field K is called a CM-field. Hence the condition in Proposition 3.6 is that $K/\mathbb{Q}$ is *not* a CM-field.

In [1], Artin proved that every element in $G_{\mathbb{Q}}$ of order 2 is conjugate to the complex conjugation but we do not know whether every element of order 2 in a finite group can be realized as a complex conjugation.

We omit the proofs of Propositions 3.5 and 3.6 because they require some extra work on the representations of isoclinic groups. The proofs will appear in a forthcoming paper.

From Proposition 3.4, Theorem 1.1 readily follows.

Remark 3.7. If the conductor $N = N(\rho)$ is a prime p, then $\det(I_p)$ must be equal to the whole $\det(G_{\mathbb{Q}})$. Since $\det(I_p)$ is isomorphic to a cyclic subgroup of $\tilde{\rho}(G_{\mathbb{Q}})$, we have:

- if ρ is of type A_4, then $\rho(G_{\mathbb{Q}})$ is isomorphic to one of $(24,3), (48,33), (72,3), (72,25)$;
- if ρ is of type S_4, then $\rho(G_{\mathbb{Q}})$ is isomorphic to one of $(48,29), (96,67), (96,192), (192,963)$;
- if ρ is of type A_5, then $\rho(G_{\mathbb{Q}})$ is isomorphic to one of $(240,93), (360,51), (600,54)$.

This prime conductor case is studied by Serre [10, §8] for odd representations and by Vignéras [13] for even representations.

§4. An example

Our results do not guarantee the existence of finite Galois extension $K/\mathbb{Q}$ with Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ isomorphic to one of the groups in Theorem 1.1 whose Artin representation has a squarefree conductor. Also all faithful representations counted in Proposition 3.4 does not necessarily give rise to representations with squarefree conductor. We explain this by an example.

Let $G = (48,33)$. This is of type A_4. The group G has a transitive group representation

$$\langle (1,14,5,11,16,8,2,13,6,12,15,7)(3,10,4,9),\\ (1,13)(2,14)(3,8)(4,7)(5,10)(6,9)(11,15)(12,16)\rangle \subset S_{16},$$

which is "16T60" in the transitive permutation group database. Let $K/\mathbb{Q}$ be a Galois extension with Galois group isomorphic to G. Let ρ be a Galois representation corresponding to $K/\mathbb{Q}$, that is $K = \bar{\mathbb{Q}}^{\mathrm{Ker}\rho}$. We use the same

symbol ρ for the faithful representation of G. If a prime p is ramified in $K/\mathbb{Q}$, then by the proof of Lemma 2.3 the ramification index e at p is 2 or 3. Let I_p be the inertia group of a prime ideal lying above p, which is a cyclic subgroup of G. By Lemma 2.2, we have $I_p/I_p \cap Z(G) \cong I_p$. By Lemma 2.2 we must have the inner product identity:

$$\langle \rho|_{I_p}, 1_{I_p} \rangle = 1.$$

For six irreducible representations $\rho = \rho_i$ $(i = 1, \dots, 6)$ of degree 2 of G, we have the values of the inner products:

	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
$\lvert \det \rho \rvert$	2	2	6	6	6	6
$e = 2$	1	1	1	1	1	1
$e = 3$	0	0	1	1	1	1

Hence if two primes p, q ramify in $K/\mathbb{Q}$ with ramification indices $2, 3$ respectively, then ρ_1 and ρ_2 do not have squarefree conductors.

To be more specific, let us consider the polynomial

$$f(x) = x^{16} - 5x^{14} + 18x^{12} - 40x^{10} + 63x^8 - 71x^6 + 43x^4 - 9x^2 + 4 \in \mathbb{Q}[x].$$

This polynomial is taken from the database of Klüners an Malle (see [8]) and the Galois group of the splitting field K of f is isomorphic to our G. The discriminant of the ring of integers of K is $7^{24}19^{32}$. Thus only 7 and 19 ramify tamely in $K/\mathbb{Q}$ and the ramification indices of them are 2 and 3 respectively. The Artin conductors of ρ_1 and ρ_2 are $7 \cdot 19^2$ whereas, for $i = 3, 4, 5, 6$, those of ρ_i are $7 \cdot 19$, which is squarefree.

References

[1] E. Artin, *Kennzeichnung des Körpers der reellen algebraischen Zahlen*, Abh. Math. Sem. Univ. Hamburg **3** (1924), no. 1, 319–323.

[2] F. R. Beyl and J. Tappe, *Group extensions, representations, and the Schur multiplicator*, Lecture Notes in Mathematics, vol. 958, Springer-Verlag, Berlin-New York, 1982.

[3] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.

[4] D. S. Dummit and R. M. Foote, *Abstract algebra*, third ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[5] P. Hall, *The classification of prime-power groups*, J. Reine Angew. Math. **182** (1940), 130–141.

[6] I. M. Isaacs, *Character theory of finite groups*, Academic Press, New York-London, 1976, Pure and Applied Mathematics, No. 69.

[7] C. Khare, *Serre's conjecture and its consequences*, Jpn. J. Math. **5** (2010), no. 1, 103–125.

[8] J. Klüners and G. Malle, *A database for field extensions of the rationals*, LMS J. Comput. Math. **4** (2001), 182–196 (electronic).

[9] H. Nakazato, *On odd two-dimensional icosahedral Galois representations with square free conductor*, Kodai Math. J. **3** (1980), no. 3, 380–384.

[10] J.-P. Serre, *Modular forms of weight one and Galois representations*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 193–268.

[11] M. Suzuki, *Group theory. I*, Grundlehren der Mathematischen Wissenschaften, vol. 247, Springer-Verlag, Berlin-New York, 1982.

[12] J. Tappe, *On isoclinic groups*, Math. Z. **148** (1976), no. 2, 147–153.

[13] M.-F. Vignéras, *Représentations galoisiennes paires*, Glasgow Math. J. **27** (1985), 223–237.

Masanari Kida
Department of Mathematics, Tokyo University of Science
Kagurazaka 1-3, Shinjuku, Tokyo 162-0827, Japan
E-mail: kida@rs.tus.ac.jp

Yusuke Sudo
Department of Mathematics, Tokyo University of Science
Kagurazaka 1-3, Shinjuku, Tokyo 162-0827, Japan
E-mail: 1115609@alumni.tus.ac.jp