H. NAKAZATO
KODAI MATH. J.
3 (1980), 380—384

ON ODD TWO-DIMENSIONAL ICOSAHEDRAL GALOIS REPRESENTATIONS WITH SQUARE FREE CONDUCTOR

BY HAJIME NAKAZATO

Introduction

Let $\boldsymbol{Q}$ be an algebraic closure of the rational number field $\boldsymbol{Q}$, and let G be the Galois group $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$. In [2], Deligne and Serre proved that the Mellin transform of a normalized new form of weight 1 with character is the Artin L-function of a continuous two-dimensional representation of G. The purpose of this paper is to investigate such representations of G.

Let

$$\rho : G \longrightarrow \mathrm{GL}(2,\boldsymbol{C})$$

be a two-dimensional continuous complex linear representation of G, and let

$$\varepsilon=\det(\rho) : G \longrightarrow \mathrm{GL}(1,\boldsymbol{C})=\boldsymbol{C}^{\times} .$$

Let $c\in G$ be a "complex conjugate", or Frobenius at infinity. We say that ρ is odd if $\varepsilon(c)=-1$. Let N be the (Artin) conductor of ρ. The conductor of ε divides N (cf. [4]). Let χ be a character of a group H; $\chi : H\rightarrow \boldsymbol{C}^{\times}$. Then we say that χ has order n if the image of χ has order n, and we denote it by; $\mathrm{ord}(\chi)=n$.

Let $\tilde{\rho}$ be the projective representation of G attached to the linear representation ρ of G;

$$\begin{array}{ccc} G & \xrightarrow{\ \rho\ } & \mathrm{GL}(2,\boldsymbol{C}) \\ & \searrow^{\tilde{\rho}} & \downarrow \\ & & \mathrm{PGL}(2,\boldsymbol{C}) . \end{array}$$

The image of $\tilde{\rho}$ is a finite subgroup of $\mathrm{PGL}(2,\boldsymbol{C})$. Hence it is one of the followings;

1) cyclic groups,
2) dihedral groups,
3) the alternating groups A_4, A_5, and the symmetric group S_4.

We say that ρ is of type A_4 (resp. S_4, A_5) if $\tilde{\rho}(G)\cong A_4$ (resp. S_4, A_5) (cf. [6]), and that ρ is icosahedral if it is of type A_5.

Received July 17, 1979

Our main result is the following theorem.

THEOREM I. *Let ρ be an odd continuous two-dimensional linear representation of G with conductor N. Suppose that ρ is of type A_5, and that N is square free. Then the order of the image of ρ is* 240, 720, 1200 *or* 3600.

Remark. In § 8 of [6], Serre has remarked that if N is a prime then the order of the image of ρ is 240. See Remark 1 in § 2 and Proposition in § 3. Moreover we see that if N is a product of two distinct primes then the order of the image of ρ is 240, 720 or 1200. See Remark 2 in § 2.

§ 1. Local theory

Let $N=\prod_p p^{m(p)}$, and let $I_p \subset G$ be an inertia subgroup of a prime p.

LEMMA 1. *Suppose that $m(p)=1$. Then ρ is tamely ramified at p. Moreover there exists a one-dimensional representation $\phi \neq id$ of I_p such that $\rho|_{I_p}$ is isomorphic to the representation $\phi \oplus id$ of I_p. We have:*

$$\begin{array}{ccccc} & & \varepsilon(I_p) & & \\ & \overset{\sim}{\nearrow} & & \overset{\sim}{\searrow} & \\ \rho(I_p) & & & & \phi(I_p)\,. \\ & \underset{\sim}{\searrow} & & \underset{\sim}{\nearrow} & \\ & & \tilde{\rho}(I_p) & & \end{array}$$

Proof. Let $D_p \supset I_p$ be the decomposition group of the place v of $\bar{\boldsymbol{Q}}$ such that I_p is the inertia group of v. We identify D_p with the Galois group $\mathrm{Gal}(\bar{\boldsymbol{Q}}_p/\boldsymbol{Q}_p)$ of an algebraic closure $\bar{\boldsymbol{Q}}_p$ of the p-adic number field $\boldsymbol{Q}_p$. Let $K \subset \bar{\boldsymbol{Q}}_p$ be the fixed field of $\mathrm{Ker}(\rho|_{D_p})$. Then we have $\mathrm{Gal}(K/\boldsymbol{Q}_p) \cong \rho(D_p)$. Let $H=\mathrm{Gal}(K/\boldsymbol{Q}_p)$, and let $\rho' : H \to \mathrm{GL}(2,\boldsymbol{C})$ be the representation of H induced by $\rho|_{D_p}$. Let V be a representation space of ρ', and let G_i ($i \geqq 0$) be the corresponding ramification groups (G_0 being the inertia group) in H. By the formula of Artin conductor, we have

$$m(p)=\sum_{i=0}^{\infty} \frac{|G_i|}{|G_0|}\mathrm{codim}(V^{G_i})$$

(cf. [4], [5]). If ρ is not tamely ramified at p. Then we have: $G_1 \neq \{id\}$. Since ρ' is a faithfull representation, we have: $(\mathrm{codim}(V^{G_0}) \geqq)$ $\mathrm{codim}(V^{G_1}) \geqq 1$. Hence

$$\begin{aligned} m(p) &= \sum_{i=0}^{\infty} \frac{|G_i|}{|G_0|}\mathrm{codim}(V^{G_i}) \\ &\geqq \frac{|G_0|}{|G_0|}\mathrm{codim}(V^{G_0}) + \frac{|G_1|}{|G_0|}\mathrm{codim}(V^{G_1}) \\ &\geqq 1 + \frac{|G_1|}{|G_0|}\,. \end{aligned}$$

So we have: $m(p)\geqq 2$. This contradicts the assumption that $m(p)=1$. The first assertion is proved.

Since ρ is tamely ramified at p, $\rho(I_p)$ is a cyclic group. Hence there exist one-dimensional representations ψ_1 and ψ_2 of I_p such that $\rho|_{I_p}$ is isomorphic to $\psi_1\oplus\psi_2$. Considering the conductors of $\rho|_{I_p}$ and $\psi_1\oplus\psi_2$, we have:

$$\psi_1=id \quad \text{and} \quad \psi_2\neq id, \quad \text{or} \quad \psi_1\neq id \quad \text{and} \quad \psi_2=id\,.$$

Therefore $\rho|_{I_p}$ is isomorphic to $\psi\oplus id$ with $\psi\neq id$. The proof is completed.

Remark. Let N be square free. Then by Lemma 1 the conductor of $\tilde{\rho}$ (see §6 of [6]) is N and the conductor of ε is N.

§2. The order of ε

THEOREM II. *Let ρ be an odd continuous two-dimensional representation of G with conductor N, and put $\varepsilon=\det(\rho)$. Suppose that N is square free. Then we have the followings.*

i) *The order of ε is 6, if ρ is of type A_4.*
ii) *The order of ε is 2, 4, 6 or 12, if ρ is of type S_4.*
iii) *The order of ε is 2, 6, 10 or 30, if ρ is of type A_5.*

Remark 1. If N is a prime. Then the followings were obtained in Theorem 7 of [6].

i) There exists no representation of type A_4.
ii) The order of ε is 2 or 4, if ρ is of type S_4.
iii) The order of ε is 2, if ρ is of type A_5.

Remark 2. Suppose that N is a product of two distinct primes. Then we have the followings.

i) The order of ε is 6, if ρ is of type A_4.
ii) The order of ε is 2, 4, 6 or 12, if ρ is of type S_4.
iii) The order of ε is 2, 6 or 10, if ρ is of type A_5.

To obtain Theorem II, we use the following lemma.

LEMMA 2. *The Galois group G is generated, in the sense of topological groups by all conjugates of inertia subgroups of all primes.*

Proof. Let G' be the subgroup of G generated by all conjugates of inertia subgroups of all primes. Then the fixed field of G' is unramified over $\boldsymbol{Q}$. Hence we have: $G=G'$, by Minkowski's Theorem (cf. [1], Chap. 2, Sec. 6, Problem 4, p. 129).

Proof of Theorem II. Let $n_p=\text{ord}(\varepsilon|_{I_p})$ for each prime $p|N$, and let $n=\text{ord}(\varepsilon)$. Then n is even since ρ is odd. Let ζ be a primitive n-th root of unity. For a subset A of a group H, let $\langle A\rangle$ be the subgroup of H generated by A. By Lemma 2, we have

$$\varepsilon(G)=\langle\varepsilon(I_p)|\ \text{all primes } p|N\rangle .$$

So we have $\langle\zeta\rangle=\langle\zeta^{n/n_p}|$ all primes $p|N\rangle$. Hence there exist integers a_p, $p|N$, such that

$$1=\sum_{p|N} a_p\frac{n}{n_p} .$$

Since $\varepsilon(I_p)\cong\tilde{\rho}(I_p)$, $\varepsilon(I_p)$ is isomorphic to a cyclic subgroup of $\tilde{\rho}(G)$ for each $p|N$. For each $p|N$, n_p is 2 or 3 (resp. 2, 3 or 4; 2, 3 or 5) if ρ is of type A_4 (resp. S_4; A_5). Hence there exist non-negative integers a, b and c such that $n=2^a3^b5^c$. Moreover noting that n is even, we have the followings.

i) $a=1$, $0\leqq b\leqq 1$, $c=0$, if ρ is of type A_4.

ii) $1\leqq a\leqq 2$, $0\leqq b\leqq 1$, $c=0$, if ρ is of type S_4.

iii) $a=1$, $0\leqq b\leqq 1$, $0\leqq c\leqq 1$, if ρ is of type A_5.

Hence we have:

i) n is 2 or 6, if ρ is of type A_4.

ii) n is 2, 4, 6 or 12, if ρ is of type S_4.

iii) n is 2, 6, 10 or 30, if ρ is of type A_5.

By the same reason as in the proof of Theorem 7, pp. 276-277, in §8 of [6], if ρ is of type A_4 then n is 6. The proof is completed.

§3. The proof of Theorem I

The following proposition and Theorem II imply Theorem I.

PROPOSITION. *Let ρ be an odd continuous two-dimensional linear representation of G, and let n be the order of* $\det(\rho)$. *Suppose that ρ is of type A_5. Then the order of the image of ρ is* $120n$.

Proof. Let $H=\mathrm{Ker}(\rho(G)\xrightarrow{\det}\boldsymbol{C}^\times)$. Then $(\rho(G):H)=n$. Let Z be the subgroup of $\mathrm{GL}(2,\boldsymbol{C})$ consisting of all scalar matrices, and put $Z_0=\rho(G)\cap Z$. Then $\rho(G)/Z_0\cong A_5$. The subgroup H is a normal subgroup of $\rho(G)$. Hence from the following commutative diagram;

$$\begin{array}{ccc} H & \hookrightarrow & \rho(G) \\ \downarrow & & \downarrow \\ H/H\cap Z_0 & \hookrightarrow & \rho(G)/Z_0\cong A_5 , \end{array}$$

we see that $H/H\cap Z_0$ is a normal subgroup of A_5. Therefore we have $H/H\cap Z_0\cong A_5$, since A_5 is a simple group. By the definitions of H and Z_0, we have two cases;

a) $H\cap Z_0=\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right\}$,

b) $H\cap Z_0=\left\{\pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right\}$.

In the case a), we have $H\cong A_5$. Since H is a subgroup of GL(2,$\boldsymbol{C}$). This contradicts the classification of finite subgroups of GL(2,$\boldsymbol{C}$) (cf. § 26 of [3]). Therefore the case a) does not occur.

In the case b), the order of H is 120. Hence the order of $\rho(G)$ is $120n$. The proof is completed.

Remark. In this proposition, we make no assumption on the conductor of ρ.

References

[1] Z.I. Borevich & I.R. Shafarevich: Number Theory. Academic Press, New York and London, 1966.
[2] P. Deligne & J-P. Serre: Formes modulaires de poids 1. Ann. sci. E.N.S. 7, 507-530 (1974).
[3] L. Dornhoff: Group Representation Theory, Part A, Marcel Dekker, Inc., New York, 1971.
[4] I. Martinet: Character theory and Artin L-functions, Proceedings of a conference at Durham, 1977.
[5] J-P. Serre: Corps locaux. Hermann, Paris, 1968.
[6] J-P. Serre: Modular forms of weight one and Galois representation. Proceedings of a conference at Durham, 1977.

Department of Mathematics,
Tokyo Institute of Technology.