Tohoku Math. J.
55 (2003), 271–282

RIGID BRAID ORBITS RELATED TO $\mathrm{PSL}_2(P^2)$ AND SOME SIMPLE GROUPS

TAKEHITO SHIINA

(Received May 23, 2001)

Abstract. We apply the braid orbit theorem to projective semilinear groups over the finite fields with p^2 elements and some almost simple groups of Lie type. The projective special linear groups $\mathrm{PSL}_2(p^2)$ with $p \equiv \pm 3 \pmod 8$, the Tits simple group, and some small simple groups occur regularly as Galois groups over the rationals.

Introduction. Let G be a finite group with trivial center and $\mathbf{C} = (C_1, \ldots, C_s)$ a rational class vector of G. We denote by $\Sigma(\mathbf{C})$ the set of generating s-systems in $\mathbf{C}$:

$$\Sigma(\mathbf{C}) := \{\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_s) \mid \sigma_i \in C_i,\ \sigma_1 \cdots \sigma_s = 1,\ \langle \sigma_1, \ldots, \sigma_s \rangle = G\}.$$

The inner automorphism group $\mathrm{Inn}(G) \cong G$ naturally acts on $\Sigma(\mathbf{C})$ and the *pure Hurwitz braid group* H_s acts on the orbit space $\Sigma(\mathbf{C})/\mathrm{Inn}(G)$. An H_s-orbit in $\Sigma(\mathbf{C})/\mathrm{Inn}(G)$ is called a *braid orbit*. In his *rigid braid orbit theorem* [7] Matzat determined certain conditions on a braid orbit for the existence of a regular extension N over the rational function field $\boldsymbol{Q}(T)$ with Galois group G and with ramification structure $\mathbf{C}$.

Przywara [9] applied this theorem to the almost simple group $\mathrm{P\Sigma L}_2(25)$ with class vector $\mathbf{C} = (2A, 2C, 2D, 12A)$ and proved that the projective linear group $\mathrm{PSL}_2(25)$ occurs regularly as Galois group over $\boldsymbol{Q}$.

In this paper we take another class vector $\mathbf{C} = (2C, 2D, pA, pB)$ of $\mathrm{P\Sigma L}_2(p^2)$ for any prime number $p \equiv \pm 3 \pmod 8$ and obtain the following theorem.

THEOREM 0.1. *The projective linear group* $\mathrm{PSL}_2(p^2)$ *occurs regularly as Galois group over* $\boldsymbol{Q}$ *for any prime number* $p \equiv \pm 3 \pmod 8$.

Concerning Galois realizations of such simple groups, Feit [4] and Mestre [8] showed in different ways that $\mathrm{PSL}_2(p^2)$ occurs regularly as Galois group over $\boldsymbol{Q}$ for $p \equiv \pm 2 \pmod 5$. Furthermore, there are several works in the theory of modular forms. First, Ribet [11] proved that $\mathrm{PSL}_2(p^2)$ occurs as Galois group over $\boldsymbol{Q}$ for any prime p if 144169 is a nonsquare modulo p. Reverter and Vila [10] extended this result for primes p such that one of the integers 18209, 51349, 144169, 2356201, 18295489, 63737521 is a nonsquare modulo p. Moreover, Dieulefait and Vila [2] obtained similar result in the case which a prime less than 20 is a nonsquare modulo p. Hilbert's irreducibility theorem assures that if a group G occurs regularly as Galois group over $\boldsymbol{Q}$, then there exist infinitely many linearly disjoint Galois

---

2000 *Mathematics Subject Classification.* Primary 12F12; Secondary 20D06, 20F36.
Key words and phrases. Inverse Galois problem, finite simple groups, braid actions.

extensions over $\boldsymbol{Q}$ with Galois group G. So our theorem is a generalization of the case which 2 is a nonsquare modulo p in their result.

In another direction we explicitly compute some braid orbits of small almost simple groups of Lie type. Using the computer algebra system GAP [13], we find suitable braid orbits for the Tits simple group ${}^2F_4(2)'$, the smallest Steinberg triality group ${}^3D_4(2)$, and some small almost simple groups.

THEOREM 0.2. *The following simple groups of Lie type occur regularly as Galois groups over* $\boldsymbol{Q}$:

$$S_4(4),\ U_4(3),\ L_5(2),\ U_5(2),\ {}^2F_4(2)',\ L_3(9),\ {}^3D_4(2),\ G_2(4),\ S_6(3),\ U_6(2)\,.$$

1. Rigid braid orbit theorem. The *full Hurwitz braid group* $\tilde{H}_s$ is generated by elements $\beta_1, \ldots, \beta_{s-1}$ with the following relations:

$$\beta_i\beta_j = \beta_j\beta_i \quad \text{for } |i-j|>1\,,$$
$$\beta_i\beta_{i+1}\beta_i = \beta_{i+1}\beta_i\beta_{i+1} \quad \text{for } 1\le i\le s-2\,,$$
$$\beta_1\cdots\beta_{s-2}\beta_{s-1}^2\beta_{s-2}\cdots\beta_1 = 1\,.$$

There exists a surjective homomorphism $q_s\colon \tilde{H}_s \ni \beta_i \longmapsto (i, i+1) \in S_s$, where S_s is the symmetric group on s letters and $(i, i+1)$ is a transposition. We denote the kernel of q_s by H_s, which is a normal subgroup of $\tilde{H}_s$ and has generators

$$\beta_{ij} := (\beta_i^2)^{\beta_{i+1}^{-1}\cdots\beta_{j-1}^{-1}} = (\beta_{j-1}^2)^{\beta_{j-2}\cdots\beta_i} \quad \text{for } 1\le i<j\le s\,. \tag{1.1}$$

The group H_s is called the *pure Hurwitz braid group*.

Let G be a finite group with trivial center and $\Sigma_s(G)$ the set of all generating s-systems of G:

$$\Sigma_s(G) := \{\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_s) \mid \sigma_1\cdots\sigma_s = 1,\ \langle\sigma_1, \ldots, \sigma_s\rangle = G\}\,.$$

The group $\tilde{H}_s$ acts on the orbit space $\Sigma_s(G)/\mathrm{Inn}(G)$ in the following way.

$$[\sigma_1, \ldots, \sigma_s]^{\beta_i} = [\sigma_1, \ldots, \sigma_{i-1}, \sigma_i\sigma_{i+1}\sigma_i^{-1}, \sigma_i, \sigma_{i+2}, \ldots, \sigma_s]\,. \tag{1.2}$$

Then the subgroup H_s acts on $\Sigma(\mathbf{C})/\mathrm{Inn}(G)$, where $\mathbf{C} = (C_1, \ldots, C_s)$ is a given class vector of G. The number $l(\mathbf{C}) := |\Sigma(\mathbf{C})/\mathrm{Inn}(G)|$ is called the *class number* of $\mathbf{C}$. We denote by $B = B(\boldsymbol{\sigma})$ the H_s-orbit of $[\boldsymbol{\sigma}]$ under this action and call B a *braid orbit*.

Let $H_{\boldsymbol{\sigma}}$ be the stabilizer of $[\boldsymbol{\sigma}] \in \Sigma(\mathbf{C})/\mathrm{Inn}(G)$ in H_s. A braid orbit $B = B(\boldsymbol{\sigma})$ is said to be *rigid* when for each $[\boldsymbol{\tau}] \ne [\boldsymbol{\sigma}]$ there exists no automorphism α of H_s with $H_{\boldsymbol{\tau}} = H_{\boldsymbol{\sigma}}^{\alpha}$. Let π_B be the permutation representation of H_s on a braid orbit B and c_i the number of cycles in $\pi_B(\beta_{is})$. Then we can define the *braid orbit genus* $g_s(B)$ of B by

$$g_s(B) := 1 - |B| + \frac{1}{2}\sum_{i=1}^{s-1}(|B| - c_i)\,.$$

Additionally, we consider the following *oddness condition*.

(O_s) In the permutation representation on B, one of the cycle lengths occurs an odd number of times in some β_{is}.

Let $\boldsymbol{Q}_{\mathbf{C}}$ be the number field generated by the values of irreducible characters of G at $C_1, \ldots, C_s$ over the rationals. The class vector $\mathbf{C} = (C_1, \ldots, C_s)$ is said to be *rational* if $\boldsymbol{Q}_{\mathbf{C}} = \boldsymbol{Q}$, or equivalently if $(C_1^m, \ldots, C_s^m) = \mathbf{C}$ for any integer m prime to $|G|$. Then we can describe the *rigid braid orbit theorem* as follows.

THEOREM 1.1 (Matzat [7]). *Let G be a finite group with trivial center and* $\mathbf{C} = (C_1, C_2, C_3, C_4)$ *a class vector of G. Further assume that $\Sigma(\mathbf{C})/\mathrm{Inn}(G)$ has a rigid H_4-orbit B which has genus $g_4(B) = 0$ and satisfies the oddness condition* (O_4). *Then there exists a regular extension over $\boldsymbol{Q}_{\mathbf{C}}(T)$ with Galois group G and with ramification structure* $\mathbf{C}$.

Although this theorem was stated for arbitrary s in [7], here we restrict it to $s = 4$ for simplicity. See Matzat [7] or Malle and Matzat [6] for the proof of the theorem.

From (1.1) and (1.2) the action of β_{i4} on $\Sigma(\mathbf{C})/\mathrm{Inn}(G)$ can be described explicitly as follows.

$$[\sigma_1, \sigma_2, \sigma_3, \sigma_4]^{\beta_{14}} = [\sigma_1^{\sigma_2\sigma_3}, \sigma_2, \sigma_3, \sigma_4^{\sigma_2\sigma_3}]\,,$$
$$[\sigma_1, \sigma_2, \sigma_3, \sigma_4]^{\beta_{24}} = [\sigma_1, \sigma_2^{\sigma_3\sigma_1}, \sigma_3, \sigma_4^{\sigma_1\sigma_3}]\,,$$
$$[\sigma_1, \sigma_2, \sigma_3, \sigma_4]^{\beta_{34}} = [\sigma_1, \sigma_2, \sigma_3^{\sigma_1\sigma_2}, \sigma_4^{\sigma_1\sigma_2}]\,.$$

If there exists an automorphism $\alpha \in \mathrm{Aut}(H_s)$ with $H_{\boldsymbol{\tau}} = H_{\boldsymbol{\sigma}}^{\alpha}$, we have

$$|B(\boldsymbol{\tau})| = |H_s : H_{\boldsymbol{\tau}}| = |H_s : H_{\boldsymbol{\sigma}}| = |B(\boldsymbol{\sigma})|\,.$$

Consequently, in the case which $\Sigma(\mathbf{C})/\mathrm{Inn}(G)$ has a unique H_s-orbit B of length l, the orbit B is rigid. In particular, if $l = 2$ (resp. $l = 1$), the rigid orbit B has genus $g_4(B) = 0$ and satisfies the oddness condition (O_4). Hence we obtain the following corollary.

COROLLARY 1.2. *Under the condition of the theorem, if $\Sigma(\mathbf{C})/\mathrm{Inn}(G)$ has a unique H_4-orbit B of length* 2 (resp. 1), *there exists a regular extension over $\boldsymbol{Q}_{\mathbf{C}}(T)$ with Galois group G and with ramification structure* $\mathbf{C}$.

2. The groups $\mathrm{P\Sigma L}_2(p^2)$**.** The p-Frobenius map $\boldsymbol{F}_{p^2} \ni s \longmapsto \bar{s} := s^p \in \boldsymbol{F}_{p^2}$ induces the following automorphism of the projective linear group $H := \mathrm{PSL}_2(p^2)$.

$$\varphi\colon H \ni \rho = \begin{pmatrix} s & t \\ u & v \end{pmatrix} \longmapsto \begin{pmatrix} \bar{s} & \bar{t} \\ \bar{u} & \bar{v} \end{pmatrix} =: \bar{\rho} \in H\,.$$

We define the projective semilinear group $G := \mathrm{P\Sigma L}_2(p^2)$ by the semi-direct product of H with this automorphism φ. Hereafter p denotes a fixed prime number with $p \equiv \pm 3 \pmod 8$. In this case, 2 is a nonsquare of $\boldsymbol{F}_p$, so we have $\boldsymbol{F}_{p^2} = \boldsymbol{F}_p(\sqrt{2})$, where $\sqrt{2}$ is a root of $x^2 - 2 \in \boldsymbol{F}_p[x]$. We can easily check that $\bar{\sqrt{2}} = -\sqrt{2}$ and $r := -2 + \sqrt{2}$ is a nonsquare of $\boldsymbol{F}_{p^2}$. The conjugacy classes $2C$, $2D$, pA, pB in G are defined as the classes of the following elements, respectively.

$$\varphi\,,\quad \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\varphi\,,\quad \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\,,\quad \begin{pmatrix}1 & 0\\ r & 1\end{pmatrix}\,.$$

We take the rational class vector $\mathbf{C} = (2C, 2D, pA, pB)$.

REMARK 2.1. Here we follow from the notation of $\mathrm{PSL}_2(25)$ in ATLAS [1]. In the character table of $\mathrm{PSL}_2(9) \cong A_6$, however, the notation in ATLAS is somewhat different. Indeed, our classes $2C$ and $2D$ correspond to $2B$ and $2C$ in the table of $\mathrm{PSL}_2(9)$.

LEMMA 2.1.

(i) $2C = \left\{ \begin{pmatrix}c_1 & c_2\\ c_3 & \bar{c}_1\end{pmatrix}\varphi \,\middle|\, c_2, c_3 \in \boldsymbol{F}_p\sqrt{2},\ c_1\bar{c}_1 - c_2c_3 = 1 \right\}$,

where $\boldsymbol{F}_p\sqrt{2} := \{n\sqrt{2} \mid n \in \boldsymbol{F}_p\} = \{s \in \boldsymbol{F}_{p^2} \mid s + \bar{s} = 0\}$.

(ii) $2D = \left\{ \begin{pmatrix}d_1 & d_2\\ d_3 & -\bar{d}_1\end{pmatrix}\varphi \,\middle|\, d_2, d_3 \in \boldsymbol{F}_p,\ d_1\bar{d}_1 + d_2d_3 = -1 \right\}$.

(iii) $pA = \left\{ \begin{pmatrix}1 + a_1a_2 & a_1^2\\ -a_2^2 & 1 - a_1a_2\end{pmatrix} \,\middle|\, (a_1, a_2) \neq (0, 0) \right\}$.

(iv) $pB = \left\{ \begin{pmatrix}1 + b_1b_2r & b_1^2r\\ -b_2^2r & 1 - b_1b_2r\end{pmatrix} \,\middle|\, (b_1, b_2) \neq (0, 0) \right\}$.

PROOF. (i) Conjugating φ by $\rho = \begin{pmatrix}s & t\\ u & v\end{pmatrix} \in H$ and $\rho\varphi$, we get

$$\rho^{-1}\varphi\rho = \rho^{-1}\bar{\rho}\varphi = \begin{pmatrix}\bar{s}v - t\bar{u} & \bar{t}v - t\bar{v}\\ \bar{s}u - s\bar{u} & s\bar{v} - \bar{t}u\end{pmatrix}\varphi\,,$$

$$(\rho\varphi)^{-1}\varphi(\rho\varphi) = \varphi^{-1}\rho^{-1}\varphi\rho\varphi = \bar{\rho}^{-1}\rho\varphi\,.$$

Hence $2C \subseteq \left\{ \begin{pmatrix}c_1 & c_2\\ c_3 & \bar{c}_1\end{pmatrix}\varphi \,\middle|\, c_2, c_3 \in \boldsymbol{F}_p\sqrt{2},\ c_1\bar{c}_1 - c_2c_3 = 1 \right\}$. Since the centralizer of φ is

$$C_G(\varphi) = \left\{ \begin{pmatrix}s & t\\ u & v\end{pmatrix} \,\middle|\, s, t, u, v \in \boldsymbol{F}_p \text{ or } s, t, u, v \in \boldsymbol{F}_p\sqrt{2} \right\} \cdot \langle\varphi\rangle \cong \mathrm{PGL}_2(p) \cdot \langle\varphi\rangle\,,$$

the cardinal of $2C$ is

$$|2C| = \frac{|\mathrm{P\Sigma L}_2(p^2)|}{2|\mathrm{PGL}_2(p)|} = \frac{p^2(p^2-1)(p^2+1)}{2p(p-1)(p+1)} = \frac{p(p^2+1)}{2}\,.$$

Using $|\{c_1 \in \boldsymbol{F}_{p^2} \mid c_1\bar{c}_1 = 1\}| = p + 1$, we can count the elements of the right-hand side of (i), namely,

$$\left| \left\{ \begin{pmatrix}c_1 & c_2\\ c_3 & \bar{c}_1\end{pmatrix}\varphi \,\middle|\, c_2, c_3 \in \boldsymbol{F}_p\sqrt{2},\ c_1\bar{c}_1 - c_2c_3 = 1 \right\} \right| = \frac{p(p^2+1)}{2} = |2C|\,.$$

Hence the equality (i) holds. Other cases (ii), (iii), (iv) are similar. □

Let U be the union of $\{0\}$ and a representative system of $\boldsymbol{F}_p^\times/\{\pm 1\}$ with $1 \in U$ and V the following subset of U.

$$V := \{u \in U \mid -2 + u\sqrt{2} \notin \boldsymbol{F}_{p^2}^{\times 2}\} = \{u \in U \mid 2 - u^2 \in \boldsymbol{F}_p^{\times 2}\}\,.$$

LEMMA 2.2. *Each* $[\boldsymbol{\sigma}] \in \Sigma(\mathbf{C})/\mathrm{Inn}(G)$ *is represented by* $\boldsymbol{\sigma} = (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ *with*

$$\begin{aligned}
\sigma_1 &= \begin{pmatrix} s + u\sqrt{2} & -u\sqrt{2} \\ (2u - sv)\sqrt{2} & s - u\sqrt{2} \end{pmatrix} \varphi\,, \quad & \sigma_2 &= \begin{pmatrix} t + u\sqrt{2} & -t \\ t - s & -t + u\sqrt{2} \end{pmatrix} \varphi\,, \\
\sigma_3 &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\,, & \sigma_4 &= \begin{pmatrix} 1 & 0 \\ -2 + v\sqrt{2} & 1 \end{pmatrix}\,.
\end{aligned} \tag{2.1}$$

Here $s, t \in \boldsymbol{F}_p$, $u \in U$, $v \in V$ *are unique for each* $[\boldsymbol{\sigma}]$ *and satisfy following relations.*

$$s + t = 2uv\,, \quad st = 2u^2 - 1\,.$$

PROOF. By conjugation we put

$$\sigma_1 = \begin{pmatrix} c_1 & c_2 \\ c_3 & \bar{c}_1 \end{pmatrix} \varphi\,, \quad \sigma_2 = \begin{pmatrix} d_1 & d_2 \\ d_3 & -\bar{d}_1 \end{pmatrix} \varphi\,, \quad \sigma_3 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\,,$$
$$\sigma_4 = \begin{pmatrix} 1 + b_1 b_2 r & b_1^2 r \\ -b_2^2 r & 1 - b_1 b_2 r \end{pmatrix}$$

as in Lemma 2.1. Here we may assume that $b_2 \neq 0$. Indeed, if $b_2 = 0$, we have

$$\begin{pmatrix} d_1 & d_2 \\ d_3 & -\bar{d}_1 \end{pmatrix} \varphi = \begin{pmatrix} c_1 + c_3(1 + b_1^2 r) & c_2 + \bar{c}_1(1 + b_1^2 r) \\ c_3 & \bar{c}_1 \end{pmatrix} \varphi$$

from the equation $\sigma_2 = \sigma_3 \sigma_4 \sigma_1$. This means that $c_3 \in \boldsymbol{F}_p \cap \boldsymbol{F}_p\sqrt{2} = \{0\}$, so the equation cannot hold. Hence we can take $\tau = \begin{pmatrix} 1 & -b_1 b_2^{-1} \\ 0 & 1 \end{pmatrix}$. Then

$$\sigma_3^\tau = \sigma_3, \quad \sigma_4^\tau = \begin{pmatrix} 1 & 0 \\ b_1 b_2 r & 1 \end{pmatrix}\,.$$

Now we can rewrite

$$\sigma_1 = \begin{pmatrix} c_1 & c_2 \\ c_3 & \bar{c}_1 \end{pmatrix} \varphi\,, \quad \sigma_2 = \begin{pmatrix} d_1 & d_2 \\ d_3 & -\bar{d}_1 \end{pmatrix} \varphi\,, \quad \sigma_3 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\,, \quad \sigma_4 = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}\,.$$

Since $\sigma_2 = \sigma_3 \sigma_4 \sigma_1$, we get

$$\begin{pmatrix} d_1 & d_2 \\ d_3 & -\bar{d}_1 \end{pmatrix} \varphi = \begin{pmatrix} (1 + b)c_1 + c_3 & (1 + b)c_2 + \bar{c}_1 \\ bc_1 + c_3 & bc_2 + \bar{c}_1 \end{pmatrix} \varphi\,.$$

Here we put $d_1 = t + u\sqrt{2}$, $d_3 = t - s$ for $s, t, u \in \boldsymbol{F}_p$ and solve this equation:

$$\begin{aligned}
&c_1 = s + u\sqrt{2}\,, \quad c_2 = -u\sqrt{2}\,, \\
&d_1 = t + u\sqrt{2}\,, \quad d_2 = -t\,, \quad d_3 = t - s\,.
\end{aligned}$$

Then $b = -2 + v\sqrt{2}$ with $v \in V$ and $c_3 = (2u - sv)\sqrt{2}$, where s, t, u, v satisfy the above relations. To exclude multiplicity of ± 1 we may assume that $u \in U$. Then s, t, u, v are unique for each $[\boldsymbol{\sigma}]$. Indeed, when

$$(\sigma_1, \sigma_2, \sigma_3, \sigma_4)^\tau = (\sigma_1', \sigma_2', \sigma_3', \sigma_4') \quad \text{for}$$
$$\sigma_3 = \sigma_3' = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 0 \\ -2 + v\sqrt{2} & 1 \end{pmatrix}, \quad \sigma_4' = \begin{pmatrix} 1 & 0 \\ -2 + v'\sqrt{2} & 1 \end{pmatrix},$$

we can see that $\tau = 1$ by the definition of V, and hence $(\sigma_1, \sigma_2, \sigma_3, \sigma_4) = (\sigma_1', \sigma_2', \sigma_3', \sigma_4')$. □

Conversely, the elements in (2.1) actually generate the projective semilinear group G for such $s, t \in \boldsymbol{F}_p$, $u \in U$, $v \in V$. This fact follows from Dickson's classical theorem:

THEOREM 2.1 (Dickson [3]). *For any prime number p, if $(p, n) \neq (3, 2)$, then*

$$\mathrm{PSL}_2(p^n) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix} \right\rangle. \tag{2.2}$$

Here r is any generator of $\boldsymbol{F}_{p^n}/\boldsymbol{F}_p$.

Dickson's theorem makes an exception of $(p, n) = (3, 2)$, but even in such a case, if r is a nonsquare of $\boldsymbol{F}_{p^n}$, then (2.2) holds. A proof of the theorem is found, for example, in [5, Th. 8.4]. By elementary number theory there exist $(p - \varepsilon)/4$ choices for $v \in V$ and $(p - \varepsilon)/2$ choices for $s, t \in \boldsymbol{F}_p$, $u \in U$, where $\varepsilon = (-1)^{(p-1)/2}$. So the class number of $\mathbf{C}$ is

$$l(\mathbf{C}) = \frac{(p - \varepsilon)^2}{8}.$$

3. The orbits of length 2. Let Q^+ (resp. Q^-) denote the subgroup of G which is generated by φ and all upper (resp. lower) triangle matrices. Further, let $P^\pm$ be the subgroup of $Q^\pm$ which is generated by φ and all triangles whose diagonal elements are 1. Notice that P^+ is the centralizer of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ in G.

LEMMA 3.1. *In the action of H_4, β_{24} and β_{34} have no fixed point on $\Sigma(\mathbf{C})/\mathrm{Inn}(G)$.*

PROOF. A G-orbit $[\boldsymbol{\sigma}] \in \Sigma(\mathbf{C})/\mathrm{Inn}(G)$ is represented by $\boldsymbol{\sigma} = (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ in the form as in Lemma 2.2. Suppose $[\boldsymbol{\sigma}]^{\beta_{24}} = [\boldsymbol{\sigma}]$. Then there exists $\tau_2 \in G$ such that $(\sigma_1, \sigma_2^{\sigma_3\sigma_1}, \sigma_3, \sigma_4^{\sigma_1\sigma_3}) = \boldsymbol{\sigma}^{\tau_2}$. Since τ_2 and σ_3 are commutative, τ_2 belongs to the centralizer P^+. If $\tau_2 \in H$, then the equality $\sigma_1^{\tau_2} = \sigma_1$ means $\tau_2 \in Q^+$. Further, if $\tau_2 \notin H$, the equality $\sigma_4^{\sigma_1\sigma_3\tau_2^{-1}} = \sigma_4$ leads $\sigma_1\sigma_3\tau_2^{-1} \in P^-$ and so

$$\begin{cases} \sigma_1 \in P^+ \\ \sigma_1\sigma_3\tau_2^{-1} = 1 \end{cases} \quad \text{or} \quad \begin{cases} \sigma_1 \in P^- \\ \tau_2 = \sigma_3\varphi \end{cases}$$

by a brief calculation. In the latter case we have $\sigma_1 = \varphi$. Therefore σ_1 belongs to the upper triangles Q^+ in either case. Thus

$$2u = sv, \quad s^2 - 2u^2 = 1\,,$$

which means $s^2(2 - v^2) = 2$. This contradicts that $2 - v^2$ is a square of $\boldsymbol{F}_p$.

Next we suppose that $[\boldsymbol{\sigma}]^{\beta_{34}} = [\boldsymbol{\sigma}]$. Then there exists $\tau_3 \in G$ such that $(\sigma_1^{\sigma_3\sigma_4}, \sigma_2^{\sigma_3\sigma_4}, \sigma_3, \sigma_4) = \boldsymbol{\sigma}^{\tau_3}$. Since τ_3 commutes with σ_3 and σ_4, Dickson's theorem shows that τ_3 commutes with any element of H, namely, $\tau_3 = 1$. Hence $\sigma_1^{\sigma_3\sigma_4} = \sigma_1$, and so σ_1 commutes with σ_2. Thus $\sigma_3\sigma_4 = \sigma_2^{-1}\sigma_1^{-1}$ has order 2, but we can calculate that

$$(\sigma_3\sigma_4)^2 = \begin{pmatrix} -1 + v\sqrt{2} & 1 \\ -2 + v\sqrt{2} & 1 \end{pmatrix}^2 = \begin{pmatrix} * & v\sqrt{2} \\ * & -1 + v\sqrt{2} \end{pmatrix},$$

which is a contradiction. □

PROPOSITION 3.1. *Let p be a prime number with $p \equiv \pm 3 \pmod 8$ and $G = \mathrm{P\Sigma L}_2(p^2)$ the projective semilinear group over $\boldsymbol{F}_{p^2}$. Then there exists a unique H_4-orbit of length* 2 *in $\Sigma(\mathbf{C})/\mathrm{Inn}(G)$ for the class vector $\mathbf{C} = (2C, 2D, pA, pB)$ of G.*

PROOF. From Lemma 3.1 and the identity $\beta_{14}\beta_{24}\beta_{34} = 1$, if $\Sigma(\mathbf{C})/\mathrm{Inn}(G)$ has an H_4-orbit B of length 2, then β_{14} fixes each element of B. So we suppose that $[\boldsymbol{\sigma}]^{\beta_{14}} = [\boldsymbol{\sigma}]$, where $\boldsymbol{\sigma}$ is of the form as in Lemma 2.2. Then there exists $\tau_1 \in G$ such that $(\sigma_1^{\sigma_2\sigma_3}, \sigma_2, \sigma_3, \sigma_4^{\sigma_2\sigma_3}) = \boldsymbol{\sigma}^{\tau_1}$. Since τ_1 and σ_3 are commutative, τ_1 belongs to the centralizer P^+.

If $\tau_1 \in H$ and so $\sigma_2^{\tau_1} = \sigma_2$, then we have $\sigma_2 \in Q^+$ and so $s = t = uv$. Thus

$$2u - sv = u^{-1}(2u^2 - suv) = u^{-1}(2u^2 - st) = u^{-1}\,.$$

We put

$$\boldsymbol{\tau}_v := \left(u \begin{pmatrix} v+\sqrt{2} & -\sqrt{2} \\ u^{-2}\sqrt{2} & v-\sqrt{2} \end{pmatrix} \varphi\,, \quad u \begin{pmatrix} v+\sqrt{2} & -v \\ 0 & -v+\sqrt{2} \end{pmatrix} \varphi\,, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ -2+v\sqrt{2} & 1 \end{pmatrix} \right),$$

which is a fixed point of β_{14}.

On the other hand, if $\tau_1 \notin H$ and so $\sigma_4^{\sigma_2\sigma_3\tau_1^{-1}} = \sigma_4$, then we get $\sigma_2\sigma_3\tau_1^{-1} \in P^-$. Since $\sigma_3\tau_1^{-1} \in P^+$, we can see that σ_2 is of the form $\begin{pmatrix} 1 & * \\ * & * \end{pmatrix}\varphi$, and hence $t = 1, u = 0$. We put

$$\boldsymbol{\sigma}_v := \left(\begin{pmatrix} 1 & 0 \\ -v\sqrt{2} & 1 \end{pmatrix} \varphi\,, \quad \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix} \varphi\,, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ -2+v\sqrt{2} & 1 \end{pmatrix} \right),$$

which is another fixed point of β_{14}.

Next we determine all pairs of these fixed points which are permuted by β_{34}. Since β_{34} maps $[\sigma_1, \sigma_2, \sigma_3, \sigma_4]$ to $[\sigma_1^{\sigma_3\sigma_4}, \sigma_2^{\sigma_3\sigma_4}, \sigma_3, \sigma_4]$, the uniqueness of representation (2.1) shows that

$$[\boldsymbol{\sigma}_v]^{\beta_{34}} \neq [\boldsymbol{\sigma}_{v'}]\,, \quad [\boldsymbol{\tau}_v]^{\beta_{34}} \neq [\boldsymbol{\tau}_{v'}]\,,$$
$$[\boldsymbol{\sigma}_v]^{\beta_{34}} = [\boldsymbol{\tau}_{v'}] \Longrightarrow v = v'\,,$$

for any $v, v' \in V$. For $(\sigma_1, \sigma_2, \sigma_3, \sigma_4) := \boldsymbol{\sigma}_v$ we calculate that

$$\sigma_2^{\sigma_3\sigma_4} = \begin{pmatrix} 1+v\sqrt{2} & -1 \\ 2-2v^2 & -1+v\sqrt{2} \end{pmatrix},$$

so if $[\boldsymbol{\sigma}_v]^{\beta_{34}} = [\boldsymbol{\tau}_v]$, then $v = 1$. Hence we obtain a unique H_4-orbit B of length 2, namely,

$$\begin{aligned} B &:= \{[\boldsymbol{\sigma}_1],\ [\boldsymbol{\tau}_1]\} \\ &= \left\{ \left[\begin{pmatrix} 1 & 0 \\ -\sqrt{2} & 1 \end{pmatrix}\varphi,\ \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix}\varphi,\ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ \begin{pmatrix} 1 & 0 \\ -2+\sqrt{2} & 1 \end{pmatrix} \right], \right. \\ &\qquad \left. \left[\begin{pmatrix} 1+\sqrt{2} & -\sqrt{2} \\ \sqrt{2} & 1-\sqrt{2} \end{pmatrix}\varphi,\ \begin{pmatrix} 1+\sqrt{2} & -1 \\ 0 & -1+\sqrt{2} \end{pmatrix}\varphi,\ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ \begin{pmatrix} 1 & 0 \\ -2+\sqrt{2} & 1 \end{pmatrix} \right] \right\}. \end{aligned}$$

□

PROOF OF THEOREM 0.1. By the rigid braid orbit theorem and its corollary, there exists a regular extension $N/\boldsymbol{Q}(T)$ with Galois group $\mathrm{P\Sigma L}_2(p^2)$ and with ramification structure $\mathbf{C} = (2C, 2D, pA, pB)$. The intermediate field L corresponding to the normal subgroup $\mathrm{PSL}_2(p^2)$ of $\mathrm{P\Sigma L}_2(p^2)$ is a quadratic extension over $\boldsymbol{Q}(T)$. Here two ramification points corresponding to pA and pB are unramified at $L/\boldsymbol{Q}(T)$, since these classes are included in $\mathrm{PSL}_2(p^2)$. Therefore the quadratic extension L is a rational function field over $\boldsymbol{Q}$, say $L = \boldsymbol{Q}(T')$. Thus we obtain a regular extension $N/\boldsymbol{Q}(T')$ with Galois group $\mathrm{PSL}_2(p^2)$. □

4. Some almost simple groups. Matzat improves the rigid braid orbit theorem for the class vectors which have some symmetries. This improvement is called the *twisted braid orbit theorem*. Using this theorem, we treat some finite simple groups listed in ATLAS.

Let $\mathbf{C} = (C_1, C_2, C_3, C_4)$ be a class vector of G with $C_1 = C_2$. Then one of the generators $\beta_1 \in \tilde{H}_4$ acts on $\Sigma(\mathbf{C})/\mathrm{Inn}(G)$. Now we put $\beta_1' := \beta_{14},\ \beta_2' := \beta_1,\ \beta_3' := \beta_{14}\beta_1$ and $H_4' := \langle H_4, \beta_1\rangle$. Let $B = B(\boldsymbol{\sigma})$ be an H_4'-orbit in $\Sigma(\mathbf{C})/\mathrm{Inn}(G)$ and c_i' be the number of cycles in the permutation representation of β_i' on B. Instead of the braid orbit genus $g_4(B)$, we use the *twisted braid orbit genus*:

$$g_4'(B) := 1 - |B| + \frac{1}{2}\sum_{i=1}^{3}(|B| - c_i').$$

Additionally, the oddness condition (O_s) is replaced by the next condition.

(O') In the permutation representation on B, one of the cycle lengths, summed over all β_i' of the same permutation type, occurs an odd number of times in some β_i'.

Then we can state the twisted braid orbit theorem.

THEOREM 4.1 (Matzat [7]). *Let G be a finite group with trivial center and $\mathbf{C} = (C_1, C_2, C_3, C_4)$ a class vector of G with $C_1 = C_2$. Further assume that $\Sigma(\mathbf{C})/\mathrm{Inn}(G)$ has a rigid H_4'-orbit B which has genus $g_4'(B) = 0$ and satisfies the oddness condition (O'). Then there exists a regular extension over $\mathbf{Q}_{\mathbf{C}}(T)$ with Galois group G and with ramification structure $\mathbf{C}$.*

We define the number $n(\mathbf{C}) := |\bar{\Sigma}(\mathbf{C})|/|\mathrm{Inn}(G)|$, where

$$\bar{\Sigma}(\mathbf{C}) := \{\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_s) \mid \sigma_i \in C_i,\ \sigma_1 \cdots \sigma_s = 1\}\,.$$

This number $n(\mathbf{C})$ can be calculated only by the character table of G (cf. [12, Ch. 7.3]). Further we define the number $n_H(\mathbf{C}) := |\bar{\Sigma}(\mathbf{C}) \cap H^s|/|\mathrm{Inn}(G)|$ for any subgroup H of G. To determine the class number of $\mathbf{C}$, we use such numbers $n_H(\mathbf{C})$ of the maximal subgroups H.

EXAMPLE 4.1. The Tits simple group ${}^2F_4(2)'$.

We take the rational class vector $\mathbf{C} = (2A, 2A, 2B, 8C)$ of the Tits group $G := {}^2F_4(2)'$ in ATLAS notation. The centralizers of these classes $2A$, $2B$, $8C$ have order 10240, 1536, 16, respectively. The character table of ${}^2F_4(2)'$ shows that

$$n(\mathbf{C}) = \frac{17971200^2}{10240^2 \cdot 1536 \cdot 16}\left(1 - \frac{150}{27^2} - \frac{275}{325^2} + \frac{14397}{351^2} - \frac{3675}{675^2}\right) = \frac{227}{2}\,.$$

TABLE 4.1. Irreducible characters of ${}^2F_4(2)'$.

	17971200	10240	1536	16
	$1A$	$2A$	$2B$	$8C$
χ_1	1	1	1	1
χ_4	27	-5	3	-1
χ_5	27	-5	3	-1
χ_8	325	5	-11	-1
χ_9	351	31	15	1

	$1A$	$2A$	$2B$	$8C$
χ_{10}	351	-1	-9	1
χ_{11}	351	-1	-9	1
χ_{15}	675	35	3	-1
χ_{18}	1300	20	-12	2
χ_{19}	1300	20	-12	-2

The maximal subgroup of ${}^2F_4(2)'$ which intersects with these classes $2A$, $2B$, $8C$ is conjugate to one of the groups G_1, G_2, G_3, G_3' of order 10240, 6144, 1440, 1440. The computer algebra system GAP provides the character tables of the Tits group and its maximal subgroups. Actually, we compute the number $n_{G_i}(\mathbf{C})$ as follows.

$$n_{G_1}(\mathbf{C}) = \frac{35}{2},\ n_{G_2}(\mathbf{C}) = \frac{11}{2},\ n_{G_3}(\mathbf{C}) = n_{G_3'}(\mathbf{C}) = 0\,.$$

Here any 4-system in $\mathbf{C} \cap (G_2)^4$ generates a subgroup of order 32, 64, or 128, which is also conjugate to a subgroup of G_1. Hence the class number is

$$l(\mathbf{C}) = \frac{227}{2} - \frac{35}{2} = 96\,.$$

Further we compute the permutation representation of H_4' on $\Sigma(\mathbf{C})/\mathrm{Inn}(G)$. Then we can verify that $B = \Sigma(\mathbf{C})/\mathrm{Inn}(G)$ is an H_4'-orbit of length 96 and β_i' has the following permutation type.

	permutation type
β_1'	$1^2 \cdot 2^2 \cdot 4^{10} \cdot 5^{10}$
β_2'	$1^4 \cdot 2 \cdot 4^{15} \cdot 5^6$
β_3'	2^{48}

Thus the orbit B is rigid and has genus

$$g_4'(B) = 1 - 96 + \frac{1}{2}(72 + 70 + 48) = 0\,.$$

By the twisted braid orbit theorem the Tits group ${}^2F_4(2)'$ occurs regularly as Galois group over $\boldsymbol{Q}$. □

EXAMPLE 4.2. The projective semilinear group $\mathrm{P\Sigma L}_3(9)$.

We take the rational class vector $\mathbf{C} = (2A, 2C, 3A, 4E)$ of the group $G := \mathrm{P\Sigma L}_3(9)$ in ATLAS notation. The sizes of their centralizers are 11520, 11232, 11664, 96 and two of the classes $2A$ and $3A$ are included in $\mathrm{PSL}_3(9)$. Here we extract the character table of $\mathrm{PSL}_3(9)$ in ATLAS.

TABLE 4.2. Irreducible characters of $\mathrm{PSL}_3(9)$.

	84913920	11520	11664		11232	96
	$1A$	$2A$	$3A$		$2C$	$4E$
χ_1	1	1	1	:	1	1
χ_2	90	10	9	:	12	4
χ_3	91	11	10	:	13	−3
χ_{77}	819	19	9	:	39	−1
χ_{84}	910	30	19	:	26	2
χ_{89}	910	−10	19	:	26	−2
χ_{90}	910	−10	19	:	26	−2

This table, however, contains the information of irreducible characters of $\mathrm{P\Sigma L}_3(9)$. Each character in this table splits into two characters of $\mathrm{P\Sigma L}_3(9)$. For example, the character χ_1 splits into $\tilde{\chi}_1$ and $\tilde{\chi}_1'$, where $\tilde{\chi}_1$ is the trivial character of $\mathrm{P\Sigma L}_3(9)$ and $\tilde{\chi}_1'$ is defined by $\tilde{\chi}_1'(g) = 1$ for $g \in \mathrm{PSL}_3(9)$ and $\tilde{\chi}_1'(g) = -1$ otherwise. Hence

$$n(\mathbf{C}) = \frac{84913920^2}{11520 \cdot 11232 \cdot 11664 \cdot 96} \cdot 2 \cdot \left(1 + \frac{4320}{90^2} - \frac{4290}{91^2} - \frac{6669}{819^2} + \frac{49400}{910^2}\right) = 106\,.$$

If a maximal subgroup H of $\mathrm{P\Sigma L}_3(9)$ intersects with all classes of $\mathbf{C}$, then H is conjugate to one of the groups G_1, G_1', G_2, G_3 of order 933120, 933120, 12096, 11232. We again use GAP to compute the number $n_H(\mathbf{C})$ for these maximal subgroups H:

$$n_{G_1}(\mathbf{C}) = n_{G_1'}(\mathbf{C}) = 32\,, \quad n_{G_2}(\mathbf{C}) = 3\,, \quad n_{G_3}(\mathbf{C}) = 19\,.$$

Here each 4-system in $\mathbf{C} \cap (G_3)^4$ generates a subgroup of order 864, 96, or 72, which is also conjugate to a subgroup of G_1 or G_1'. There exists a 4-system $\boldsymbol{\sigma}$ of $\mathbf{C} \cap (G_1)^4$ such that $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ generate a subgroup which is conjugate to some subgroup of G_1'. The number of such 4-systems is exactly $3|\mathrm{Inn}(G)|$, where these 4-systems generate subgroups of order 96. Thus

$$l(\mathbf{C}) = 106 - (32 + 32 - 3) - 3 = 42\,.$$

The group H_4 acts on $\Sigma(\mathbf{C})/\mathrm{Inn}(G)$ intransitively. Indeed, $\Sigma(\mathbf{C})/\mathrm{Inn}(G)$ has two H_4-orbits of length 18 and length 24. We take the shorter orbit B of length 18. In the transitive action of H_4 on B, the permutation types of $\beta_1, \beta_2, \beta_3$ are given in the next table.

	permutation type
β_1	$1^6 \cdot 2^2 \cdot 4^2$
β_2	$4^2 \cdot 5^2$
β_3	$2 \cdot 3^4 \cdot 4$

The orbit B is rigid, since it is a unique H_4-orbit of length 18 in $\Sigma(\mathbf{C})/\mathrm{Inn}(G)$, and has genus

$$g_4(B) = 1 - 18 + \frac{1}{2}(8 + 14 + 12) = 0\,.$$

Here we choose the class vector $\mathbf{C}$ such that just two classes $2A$ and $3A$ are included in $\mathrm{PSL}_3(9)$, so we have a regular extension over $\boldsymbol{Q}(T)$ with Galois group $\mathrm{PSL}_3(9)$, similarly as the proof of Theorem 0.1. □

We continue similar computation for several simple groups G of Lie type and their extensions $G.2$ by outer automorphisms of order 2. Any group in the tables below has a rigid braid orbit B with braid orbit genus $g_4(B) = 0$ (Table 4.3) or twisted braid orbit genus $g_4'(B) = 0$ (Table 4.4). In the case which $\Sigma(\mathbf{C})/\mathrm{Inn}(G.2)$ decomposes into two or three orbits, we underline the length of the orbit which we choose (ex. 24+<u>18</u>). For the extension groups $G.2$ we take the rational class vectors $\mathbf{C}$ such that just two classes of $\mathbf{C}$ are included in G. Hence the subgroups G of $G.2$ also occur regularly as Galois groups over $\boldsymbol{Q}$. In conclusion we obtain the Theorem 0.2 stated in the first place.

TABLE 4.3. Rigid braid orbits of some (almost) simple groups I.

	class vector $\mathbf{C}$	$l(\mathbf{C})$	types of $\beta_{14}, \beta_{24}, \beta_{34}$
$S_4(4)$	$(2A, 2B, 3A, 5E)$	12	$1^2{\cdot}3^2{\cdot}4$, $2{\cdot}5^2$, 2^6
$L_3(9).2$	$(2A, 2C, 3A, 4E)$	24+<u>18</u>	$1^6{\cdot}2^2{\cdot}4^2$, $4^2{\cdot}5^2$, $2{\cdot}3^4{\cdot}4$
$S_6(3)$	$(2A, 2A, 4A, 12C)$	2	2, 2, 1^2
$U_6(2)$	$(2A, 2A, 4C, 12F)$	6	$1^2{\cdot}4$, $1^2{\cdot}4$, 3^2

TABLE 4.4. Rigid braid orbits of some (almost) simple groups II.

	class vector **C**	$l(\mathbf{C})$	permutation types of $\beta_1', \beta_2', \beta_3'$		
$U_4(3).2$	$(2B, 2B, 3B, 5A)$	$\underline{10}$+5+5	$2^2{\cdot}3^2$,	$3^2{\cdot}4$,	2^5
$L_5(2).2$	$(2A, 2A, 4D, 6C)$	56	$1{\cdot}2^2{\cdot}3^2{\cdot}4^2{\cdot}5^3{\cdot}6{\cdot}8^2$,	$2^3{\cdot}3^6{\cdot}4^8$,	2^{28}
$U_5(2).2$	$(2A, 2A, 4D, 10A)$	40	$3{\cdot}4{\cdot}5^3{\cdot}6^3$,	$2^2{\cdot}3^{12}$,	2^{20}
${}^2F_4(2)'$	$(2A, 2A, 2B, 8C)$	96	$1^2{\cdot}2^2{\cdot}4^{10}{\cdot}5^{10}$,	$1^4{\cdot}2{\cdot}4^{15}{\cdot}5^6$,	2^{48}
${}^3D_4(2)$	$(2A, 2A, 3B, 12A)$	60	$3^2{\cdot}6^9$,	$1^3{\cdot}3^{15}{\cdot}4^3$,	2^{30}
$G_2(4)$	$(2A, 2A, 3A, 7A)$	14	$1^2{\cdot}3^4$,	$4{\cdot}5^2$,	2^7

REFERENCES

[1] J. H. CONWAY et al., Atlas of Finite Groups, Clarendon Press, Oxford, 1985.

[2] L. DIEULEFAIT AND N. VILA, Projective linear groups as Galois groups over $\boldsymbol{Q}$ via Modular Representations, J. Symbolic Computation 30 (2000), 799–810.

[3] L. E. DICKSON, Linear Groups with an Exposition of the Galois Field Theory, Teubner, Leibzig, 1901.

[4] W. FEIT, Rigidity of Aut($\mathrm{PSL}_2(p^2)$), $p \equiv \pm 2 \pmod 5$, $p \neq 2$, In: Proceedings of the Rutgers group theory year, 1983–1984 (New Brunswick, N. J., 1983–1984), 351–356, Cambridge Univ. Press, Cambridge, 1984.

[5] D. GORENSTEIN, Finite Groups, Harper and Row, New York-Evanston-London, 1968.

[6] G. MALLE AND B. H. MATZAT, Inverse Galois Theory, Springer-Verlag, Berlin, 1999.

[7] B. H. MATZAT, Zöpfe und Galoissche Gruppen, J. Reine Angew. Math. 420 (1991), 99–159.

[8] J.-F. MESTRE, Courbes hyperelliptiques à multiplications réelles, C. R. Acad. Sci. Paris Sér. I Math. 307 (1988), 721–724.

[9] B. PRZYWARA, Die Operation der Hurwitzschen Zopfgruppe auf den Erzeugendensystemklassen endlicher Gruppen, Diplomarbeit, Karlsruhe, 1988.

[10] A. REVERTER AND N. VILA, Some projective linear groups over finite fields as Galois groups over $\boldsymbol{Q}$, Contemp. Math. 186 (1995), 51–63.

[11] K. A. RIBET, On l-adic representations attatched to modular forms, Invent. Math. 28 (1975), 245–275.

[12] J.-P. SERRE, Topics in Galois Theory, Jones and Bartlett, Boston, 1992.

[13] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.2, Aachen, St. Andrews, 1999.

MATHEMATICAL INSTITUTE
TOHOKU UNIVERSITY
SENDAI MIYAGI, 980–8578
JAPAN