Math. J. Okayama Univ. **53** (2011), 155–165

# AN EXPLICIT $PSp_4(3)$-POLYNOMIAL WITH 3 PARAMETERS OF DEGREE 40

Hidetaka Kitayama

Abstract. We will give an explicit polynomial over $\mathbb{Q}$ with 3 parameters of degree 40 as a result of the inverse Galois problem. Its Galois group over $\mathbb{Q}$ (resp. $\mathbb{Q}(\sqrt{-3})$) is isomorphic to $PGSp_4(3)$ (resp. $PSp_4(3)$) and it is a regular $PSp_4(3)$-polynomial over $\mathbb{Q}(\sqrt{-3})$. To construct the polynomial and prove its properties above we use some results of Siegel modular forms and permutation group theory.

## 1. Introduction

In this paper, we will construct an explicit polynomial with 3 parameters of degree 40 which has properties in Theorem 1.1 below. In this section, we will explain its background.

**Definition 1.1.** *Let $G$ be a finite group and $K$ be a field. An extension $L/K$ is called $G$-extension over $K$ if $L/K$ is a Galois extension and the Galois group $Gal(L/K)$ is isomorphic to $G$. A polynomial $f(X) \in K[X]$ is called a $G$-polynomial over $K$ if the Galois group $Gal(f(X)/K)$ is isomorphic to $G$.*

The inverse Galois problem asks whether there exists a $G$-extension over $K$ for a given field $K$ and a finite group $G$. This problem has been studied by many mathematicians as one of the most important problems in number theory, especially for the case of the rational number field $\mathbb{Q}$. It is still unknown whether this problem is affirmative for every finite group, but it has been proven affirmatively for a lot of kinds of finite groups. (See [10]. ) In this paper, we will consider the constructive aspects of this problem. Our problem is formulated as follows:

**Problem 1.1.** *Construct an explicit polynomial having $G$ as the Galois group for a given transitive permutation group $G$.*

Note that Problem 1.1 for groups which are not conjugate as subgroups of the symmetric group are distinct from each other even if they are isomorphic as abstract groups. Complete results of Problem 1.1 for all transitive permutation groups of degree up to 15 were given in [8]. The purpose of this paper is to give results for transitive permutation groups of degree 40. Our main theorem is as follows. We will prove this theorem in section 5.

*Mathematics Subject Classification.* Primary 12Y05, 11C08.

*Key words and phrases.* inverse Galois problem, explicit polynomials, Siegel modular forms.

**Theorem 1.1.** *A polynomial $F(x,y,z;X) \in \mathbb{Q}(x,y,z)[X]$ with 3 parameters $x,y,z$ of degree 40, constructed in section 4, has the following properties*:
(1) *the Galois group of $F(x,y,z;X)$ over $\mathbb{Q}(x,y,z)$ is conjugate to the primitive group $(40,4)$ in the GAP code. It is isomorphic to $PGSp_4(3)$,*
(2) *the Galois group of $F(x,y,z;X)$ over $\mathbb{Q}(\sqrt{-3})(x,y,z)$ is conjugate to the primitive group $(40,3)$ in the GAP code. It is isomorphic to $PSp_4(3)$,*
*(3) $F(x,y,z;X)$ is a regular $PSp_4(3)$-polynomial over $\mathbb{Q}(\sqrt{-3})$.*

Here a regular $G$-polynomial is defined as follows:

**Definition 1.2.** *A polynomial $f(\mathbf{t};X) \in K(\mathbf{t})[X]$ with some parameters $\mathbf{t} = (t_1, \cdots, t_n)$ is called regular if it satisfies $\mathrm{Spl}(f(\mathbf{t};X)/K(\mathbf{t})) \cap \overline{K} = K$, where $\mathrm{Spl}(f(\mathbf{t};X)/K(\mathbf{t}))$ is the splitting field of $f(\mathbf{t};X)$ over $K(\mathbf{t})$ and $\overline{K}$ is an algebraic closure of $K$.*

We give some remarks concerning Theorem 1.1.

**Remark 1.1.** *Explicit polynomials over $\mathbb{Q}$ with 1 parameter for $PSp_4(3)$ and $PGSp_4(3)$ as transitive permutation groups of degree 27 are given in p.412 of [10] and they are regular $PSp_4(3)$- and $PGSp_4(3)$-polynomials over $\mathbb{Q}$. As mentioned in Theorem 1.1 our polynomial $F(x,y,z;X)$ is just a regular $PSp_4(3)$-polynomial over $\mathbb{Q}(\sqrt{-3})$. But our result is new because explicit polynomials with 3 parameters for these two groups as transitive permutation groups of degree 40 have not been known before.*

**Remark 1.2.** *We will construct our polynomial by using some results of Siegel modular forms in section 4. Note that we only have its Galois group over $\mathbb{C}(x,y,z)$ at this stage and it is a difficult problem to descend fields of definition to $\mathbb{Q}$. In the case of $SL_2(\mathbb{Z})$, Shih studied this problem in [12] by using the theory of canonical systems of models and achieved regular Galois extensions over $\mathbb{Q}$. In our case, so far, we can not improve our polynomial to have regularity over $\mathbb{Q}$.*

**Notation.** The groups $PSp_4(3)$ and $PGSp_4(3)$ are defined as follows. We define the symplectic group by

$$Sp_4(\mathbb{Z}) := \{g \in M_4(\mathbb{Z}) | {}^t g \cdot J \cdot g = J\}$$

where J:=$\begin{pmatrix} 0_2 & 1_2 \\ -1_2 & 0_2 \end{pmatrix}$ and $1_2$ is the unit matrix. The following two subgroups of $Sp_4(\mathbb{Z})$ will be important.

$$\begin{aligned} \Gamma_0(3) &:= \{g \in Sp_4(\mathbb{Z}) | g \equiv \begin{pmatrix} A & B \\ 0_2 & D \end{pmatrix} \bmod 3\}, \\ \Gamma(3) &:= \{g \in Sp_4(\mathbb{Z}) | g \equiv 1_4 \bmod 3\}. \end{aligned}$$

By definition, we have $\Gamma(3) < \Gamma_0(3) < Sp_4(\mathbb{Z})$. It is known that the index $(Sp_4(\mathbb{Z}) : \Gamma_0(3)) = 40$ and $(Sp_4(\mathbb{Z}) : \Gamma(3)) = 51840$. $\Gamma(3)$ is a normal subgroup of $Sp_4(\mathbb{Z})$, so we put $Sp_4(3) := Sp_4(\mathbb{Z})/\Gamma(3)$ and define

$$PSp_4(3) := Sp_4(3)/\{\pm 1_4\}.$$

This is a non-abelian simple group of order 25920. We also define

$$PGSp_4(3) := \{g \in GL(4, \mathbb{F}_3) \mid {}^t g \cdot J \cdot g = v \cdot J \ , \ v \in \mathbb{F}_3^{\times}\}/\{\pm 1_4\}.$$

This is a non-abelian group of order 51840 which is isomorphic to $PSp_4(3) \rtimes C_2$.

## 2. Preliminaries from Siegel modular forms

We will consider a $PSp_4(3)$-extension by using some results of Siegel modular forms. So we review Siegel modular forms to fix notation. We denote by $H_2$ the Siegel upper half plane of degree 2, that is,

$$H_2 := \{Z \in M_2(\mathbb{C}) | {}^t Z = Z, Im(Z) > 0\}.$$

The group $Sp_4(\mathbb{Z})$ acts on $H_2$ by

$$gZ = (AZ + B)(CZ + D)^{-1}$$

for any $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp_4(\mathbb{Z})$ and any $Z \in H_2$. For any natural number $k$ and a holomorphic function $F$ on $H_2$, we put

$$F|[g]_k(Z) = \det(CZ + D)^{-k} F(gZ).$$

For a finite index subgroup $\Gamma$ of $Sp_4(\mathbb{Z})$, we denote by $A_k(\Gamma)$ the space of all Siegel modular forms of weight $k$ of $\Gamma$, that is,

$$A_k(\Gamma) = \{F : \text{a holomorphic function on } H_2 \mid F|[g]_k = F \text{ for all } g \in \Gamma\}.$$

We put $A(\Gamma) = \oplus_{k=0}^{\infty} A_k(\Gamma)$. The space $A(\Gamma)$ is a graded ring. The explicit structure of $A(Sp_4(\mathbb{Z}))$ and $A(\Gamma_0(3))$ is known as in the following theorems.

**Theorem 2.1** (Igusa[6])**.**

$$\bigoplus_{k=0}^{\infty} A_k(Sp_4(\mathbb{Z})) = \mathbb{C}[\phi_4, \phi_6, \chi_{10}, \chi_{12}] \oplus \chi_{35}\mathbb{C}[\phi_4, \phi_6, \chi_{10}, \chi_{12}].$$

*$\phi_4, \phi_6, \chi_{10}, \chi_{12}$ are algebraically independent over $\mathbb{C}$.*

**Theorem 2.2** (Ibukiyama[5], Aoki and Ibukiyama[1])**.** *We put*

$$B := \mathbb{C}[\alpha_1, \beta_3, \gamma_4, \delta_3] \ , \ C := \mathbb{C}[\alpha_1^2, \beta_3^2, \gamma_4, \delta_3^2]$$

*then*

$$\bigoplus_{k=0}^{\infty} A_k(\Gamma_0(3)) = B^{(even)} \oplus C\alpha_1\chi_{14} \oplus C\beta_3\chi_{14} \oplus C\delta_3\chi_{14} \oplus C\alpha_1\beta_3\delta_3\chi_{14}.$$

$\alpha_1, \beta_3, \gamma_4, \delta_3$ *are algebraically independent over* $\mathbb{C}$.

## 3. Preliminaries from permutation group theory

In this section, we review permutation group theory. A subgroup $G$ of $S_n$, the symmetric group of degree $n$, is called transitive if arbitrary two elements in $\{1, \cdots, n\}$ can be permuted each other by $G$-action. It is well known that the Galois group of an irreducible separable polynomial of degree $n$ is a transitive subgroup of $S_n$. GAP[2] has data bases of classification of transitive subgroups of $S_n$ for $n$ up to 30. These are based on Hulpke[4]. By using the data, we see the following fact.

**Lemma 3.1.** *The least degree of which* $PSp_4(3)$ *can be realized as a transitive subgroup of the symmetric group is 27.*

Next we consider primitive groups, which are of special type in transitive groups.

**Definition 3.1.** *Let* $G$ *be a transitive subgroup of* $S_n$. $G$ *is called primitive if there are no partitions of* $\{1, \cdots, n\}$ *which satisfy the following two conditions.*

(1) $\{1, \cdots, n\} = \cup_{i=1}^{r} B_i,\ r \geq 2,$
$\sharp B_i \geq 2\ (i = 1, \ldots, r)$ *and* $B_i \cap B_j = \emptyset\ (i \neq j)$.
(2) $G$ *induces a transitive action on* $\{B_1, \ldots, B_r\}$.

GAP[2] has data bases of classification of primitive subgroups of $S_n$ for $n$ up to 2499. These are based on Colva M. Roney-Dougal [11]. Among these, we will use the following.

**Lemma 3.2.** *Primitive groups of degree 40 are one of the following 8 groups up to conjugacy.*

$$PSp_4(3)a, PSp_4(3)b, PGSp_4(3)a, PGSp_4(3)b,$$
$$PSL_4(3), PGL_4(3), A_{40}, S_{40}.$$

*(The symbols "a" and "b" mean that one group is isomorphic but is not conjugate to the other.)*

## 4. Construction of a $PSp_4(3)$-polynomial

In this section, we will consider $PSp_4(3)$-extension by using Theorem 2.1 and 2.2 and construct a polynomial which has $PSp_4(3)$ as its Galois group over the rational function field over $\mathbb{C}$ of dimension 3.

For a finite index subgroup $\Gamma$ of $Sp_4(\mathbb{Z})$, we denote by $K(\Gamma)$ the modular function field of $\Gamma$, that is, the field which consists of meromorphic functions on $H_2$ which are invariant with respect to the action of $\Gamma$. It is known that $K(\Gamma)$ is generated by fractions of modular forms for $\Gamma$ of the same weight.

(cf. corollary (i) of p.131 of [7]). We consider a sequence of the modular function fields of $Sp_4(\mathbb{Z})$, $\Gamma_0(3)$ and $\Gamma(3)$:

$$K(Sp_4(\mathbb{Z})) \subset K(\Gamma_0(3)) \subset K(\Gamma(3)).$$

It is known that these three fields are purely transcendental over $\mathbb{C}$ of dimension 3. (cf. [6],[5],[3]). Note that $K(\Gamma(3))/K(Sp_4(\mathbb{Z}))$ is a $PSp_4(3)$-extension and $K(\Gamma_0(3))/K(Sp_4(\mathbb{Z}))$ is a non-Galois extension of degree 40. We will compute a polynomial which defines the extension $K(\Gamma_0(3))/K(Sp_4(\mathbb{Z}))$. Then the splitting field of the polynomial over $K(Sp_4(\mathbb{Z}))$ is $K(\Gamma(3))$ because the Galois group $\mathrm{Gal}(K(\Gamma(3))/K(Sp_4(\mathbb{Z}))) \simeq PSp_4(3)$ is simple. Thus the polynomial is a $PSp_4(3)$-polynomial over $\mathbb{C}$ with 3 parameters of degree 40. (We will consider the Galois group over $\mathbb{Q}$ in section 5.) To carry out this computation, we need the following three steps.

1. We will compute transcendental basis over $\mathbb{C}$ of $K(Sp_4(\mathbb{Z}))$ and $K(\Gamma_0(3))$.
2. We will find a primitive element of the extension $K(\Gamma_0(3))/K(Sp_4(\mathbb{Z}))$.
3. We will compute the irreducible polynomial of the element of Step2 over $K(Sp_4(\mathbb{Z}))$. This is a polynomial we want.

**Step 1.** We will compute transcendental basis over $\mathbb{C}$ of $K(Sp_4(\mathbb{Z}))$ and $K(\Gamma_0(3))$ by using Theorem 2.1 and 2.2. By the structure of $\oplus_{k=0}^{\infty} A_k(Sp_4(\mathbb{Z}))$, we see that the former (resp. latter) part of it consists of even (resp. odd) weight functions. We also see that every odd weight function is a product of $\chi_{35}$ and a even weight function. So we see that $K(Sp_4(\mathbb{Z}))$ consists of fractions of functions of the same weight belonging to $\mathbb{C}[\phi_4, \phi_6, \chi_{10}, \chi_{12}]$. Hence $K(Sp_4(\mathbb{Z}))$ is generated by all functions of the form

$$\phi_4{}^a \phi_6{}^b \chi_{10}{}^c \chi_{12}{}^d, \ (a, b, c, d \in \mathbb{Z}, 2a + 3b + 5c + 6d = 0).$$

We can determine transcendental basis of $K(Sp_4(\mathbb{Z}))$ over $\mathbb{C}$ by computing $\mathbb{Z}$-basis of the free $\mathbb{Z}$ module of rank 3,

$$V := \{\mathbf{x} \in \mathbb{Z}^4 | (2\ 3\ 5\ 6)\mathbf{x} = 0\}$$

because $\phi_4, \phi_6, \chi_{10}, \chi_{12}$ are algebraically independent over $\mathbb{C}$.

We put

$$A := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 3 & 6 & -1 \\ -2 & -3 & -5 & 1 \end{pmatrix}.$$

Then we have

$$\begin{aligned} V &= \{\mathbf{x} \in \mathbb{Z}^4 | (0\ 0\ 0\ 1)A^{-1}\mathbf{x} = 0\} \\ &= \mathbb{Z}A \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \oplus \mathbb{Z}A \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \oplus \mathbb{Z}A \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \\ &= \mathbb{Z} \begin{pmatrix} 1 \\ 0 \\ 2 \\ -2 \end{pmatrix} \oplus \mathbb{Z} \begin{pmatrix} 0 \\ 1 \\ 3 \\ -3 \end{pmatrix} \oplus \mathbb{Z} \begin{pmatrix} 0 \\ 0 \\ 6 \\ -5 \end{pmatrix}. \end{aligned}$$

It follows that

$$K(Sp_4(\mathbb{Z})) = \mathbb{C}\left(\frac{\phi_4{\chi_{10}}^2}{{\chi_{12}}^2}, \frac{\phi_6{\chi_{10}}^3}{{\chi_{12}}^3}, \frac{{\chi_{10}}^6}{{\chi_{12}}^5}\right).$$

Next we will determine transcendental basis of $K(\Gamma_0(3))$. By the structure of $A(\Gamma_0(3))$, we see that the first part of it consists of even weight functions and the other parts odd weight. We also see that every odd weight function is a product of $\chi_{14}$ and $\alpha_1, \beta_3, \gamma_4, \delta_3$. Thus we can see $K(\Gamma_0(3))$ is generated by all functions of the form

$${\alpha_1}^a{\beta_3}^b{\gamma_4}^c{\delta_3}^d,\ (a, b, c, d \in \mathbb{Z}, a + 3b + 4c + 3d = 0).$$

We can determine transcendental basis by the same way as above and get

$$K(\Gamma_0(3)) = \mathbb{C}\left(\frac{\beta_3}{\alpha_1^3}\ ,\ \frac{\gamma_4}{\alpha_1^4}\ ,\ \frac{\delta_3}{\alpha_1^3}\right).$$

For simplicity, we put

$$a := \frac{\beta_3}{{\alpha_1}^3}\ ,\ b := \frac{\gamma_4}{{\alpha_1}^4}\ ,\ c := \frac{\delta_3}{{\alpha_1}^3}\ ,$$

$$x := \frac{\phi_4{\chi_{10}}^2}{{\chi_{12}}^2}\ ,\ y := \frac{\phi_6{\chi_{10}}^3}{{\chi_{12}}^3}\ ,\ z := \frac{{\chi_{10}}^6}{{\chi_{12}}^5}\ ,$$

then we have

$$K(Sp_4(\mathbb{Z})) = \mathbb{C}(x, y, z)\ ,\ K(\Gamma_0(3)) = \mathbb{C}(a, b, c).$$

**Step 2.**

We will find a primitive element of the extension $K(\Gamma_0(3))/K(Sp_4(\mathbb{Z}))$. We have the following relations ([1],p.259).

$$\begin{aligned}
\phi_4 &= 8\alpha_1\beta_3 + 41\alpha_1^4 - 162\gamma_4 + 5\alpha_1\delta_3 \\
\phi_6 &= 277\alpha_1^6 - 2187\alpha_1^2\gamma_4 + 80\alpha_1^3\beta_3 + \frac{11}{8}\delta_3^2 + \beta_3^2 + \frac{7}{2}\beta_3\delta_3 + \frac{91}{2}\alpha_1^3\delta_3 \\
\chi_{10} &= \gamma_4(8\alpha_1^3 + 2\beta_3 - \delta_3)^2/6144 \\
\chi_{12} &= (-124416\alpha_1^8\gamma_4 - 192\alpha_1^3\beta_3^2\delta_3 - 768\alpha_1^6\beta_3\delta_3 + 16\alpha_1^3\delta_3^3 + 256\alpha_1^3\beta_3^3 \\
&\quad +4096\alpha_1^9\beta_3 + 153\alpha_1^6\beta_3^2 - 1024\alpha_1^9\delta_3 + 16\beta_3^4 - \delta_3^4 - 16\beta_3^3\delta_3 + 4\beta_3\delta_3^3 \\
&\quad +4096\alpha_1^{12} + 7776\alpha_1^2\beta_3\delta_3\gamma_4 + 10077696\alpha_1^4\gamma_4^2 - 62208\alpha_1^5\beta_3\gamma_4 \\
&\quad +31104\alpha_1^5\delta_3\gamma_4 + 2519424\alpha_1\beta_3\gamma_4^2 - 1944\alpha_1^2\delta_3\gamma_4 - 7776\alpha_1^2\beta_3^2\gamma_4 \\
&\quad -68024448\gamma_4^3 - 1259712\alpha_1\delta_3\gamma_4^2)/3981312
\end{aligned}$$

By definition of $a$, $b$ and $c$, it is easy to see that

$$\begin{aligned}
\phi_4/\alpha_1^4 &= 8a - 162b + 5c + 41 \\
\phi_6/\alpha_1^6 &= 80a + \frac{91}{2}c - 2187b + a^2 + \frac{7}{2}ac + \frac{11}{8}c^2 + 277 \\
\chi_{10}/\alpha_1^{10} &= b(8 + 2a - c)^2/6144 \\
\chi_{12}/\alpha_1^{12} &= (16a^4 + (-16c + 256)a^3 + (-7776b - 192c + 1536)a^2 \\
&\quad +(2519424b^2 + (7776c - 62208)b + (4c^3 - 768c + 4096))a \\
&\quad +(-68024448b^3 + (-1259712c + 10077696)b^2 \\
&\quad +(-1944c^2 + 31104c - 124416)b + (-c^4 + 16c^3 - 1024c)) \\
&\quad /3981312.
\end{aligned}$$

We put

$$\theta := \frac{\chi_{10}{\alpha_1}^2}{\chi_{12}}.$$

We will prove that $\theta$ is a primitive element of the extension $K(\Gamma_0(3))/K(Sp_4(\mathbb{Z}))$. We have

$$\begin{aligned}
K(Sp_4(\mathbb{Z}))(\theta) &= \mathbb{C}(x, y, z, \theta) \\
&= \mathbb{C}(x/\theta^2, y/\theta^3, z/\theta^5, z/\theta^6) \\
&= \mathbb{C}(\phi_4/\alpha_1^4, \phi_6/\alpha_1^6, \chi_{10}/\alpha_1^{10}, \chi_{12}/\alpha_1^{12}) \\
&= \mathbb{C}(s, t, u, v),
\end{aligned}$$

where

$$s := \phi_4/\alpha_1^4 - 41, t := \phi_6/\alpha_1^6 - 277$$

$$u := 6144\chi_{10}/\alpha_1^{10}, v := 3981312\chi_{12}/\alpha_1^{12}.$$

Note that

$$\begin{aligned}
s &= 8a - 162b + 5c \\
t &= 80a + \frac{91}{2}c - 2187b + a^2 + \frac{7}{2}ac + \frac{11}{8}c^2 \\
u &= b(8 + 2a - c)^2 \\
v &= 16a^4 + (-16c + 256)a^3 + (-7776b - 192c + 1536)a^2 \\
&\quad +(2519424b^2 + (7776c - 62208)b + (4c^3 - 768c + 4096))a \\
&\quad +(-68024448b^3 + (-1259712c + 10077696)b^2 \\
&\quad +(-1944c^2 + 31104c - 124416)b + (-c^4 + 16c^3 - 1024c)).
\end{aligned}$$

We have to show that $a$, $b$ and $c$ belong to $\mathbb{C}(s,t,u,v)$ in order to show $\mathbb{C}(s,t,u,v) = \mathbb{C}(a,b,c)$. We define

$$\begin{aligned}
f &:= 8a - 162b + 5c - s \\
g &:= 80a + \frac{91}{2}c - 2187b + a^2 + \frac{7}{2}ac + \frac{11}{8}c^2 - t \\
h &:= b(8 + 2a - c)^2 - u \\
j &:= 16a^4 + (-16c + 256)a^3 + (-7776b - 192c + 1536)a^2 \\
&\quad +(2519424b^2 + (7776c - 62208)b + (4c^3 - 768c + 4096))a \\
&\quad +(-68024448b^3 + (-1259712c + 10077696)b^2 \\
&\quad +(-1944c^2 + 31104c - 124416)b + (-c^4 + 16c^3 - 1024c)) - v.
\end{aligned}$$

Here we assume $a$, $b$, $c$, $s$, $t$, $u$ and $v$ are seven independent variables. We compute a Gröbner basis of the ideal $< f, g, h, j >$ relative to the lexicographic order with $a > c > v > b > u > t > s$. Then we get a Gröbner basis which consists of 14 polynomials. Among them, one finds two polynomials $G_1$, $G_2$ without $a$, $c$ from which a linear equation of $b$ over $\mathbb{Z}[s,t,u,v]$ can be obtained. This implies $b \in \mathbb{C}(s,t,u,v)$. Also one finds another polynomial which is linear in $c$ over $\mathbb{Z}[u,v,s,t,b]$. Thus we see that $c \in \mathbb{C}(u,v,s,t,b)$. Finally, by definition of $s$: $s = 8a - 162b + 5c$, we have $a \in \mathbb{C}(s,t,u,v)$. It follows that

$$K(Sp_4(\mathbb{Z}))(\theta) = K(\Gamma_0(3)).$$

Thus Step2 has been completed.

**Step 3.** We will compute the irreducible polynomial of the element $\theta$ of Step2 over $K(Sp_4(\mathbb{Z}))$. We can get a polynomial relation of $s$, $t$, $u$ and $v$ by eliminating $b$ from $G_1 = 0$ and $G_2 = 0$. Then we replace $s$, $t$, $u$ and $v$ in this relation by

$$s = x/\theta^2 - 41 \ , \ t = y/\theta^3 - 277$$
$$u = 6144z/\theta^5 \ , \ v = 3981312z/\theta^6 - 4096$$

and multiply it by $\theta^{40}$. Then we get a polynomial of $\theta$ over $\mathbb{Q}[x, y, z]$ which has degree 40. This is the irreducible polynomial of $\theta$ over $K(Sp_4(\mathbb{Z})) = \mathbb{C}(x, y, z)$ and its Galois group over $\mathbb{C}(x, y, z)$ is isomorphic to $PSp_4(3)$. We omit this polynomial here because it takes up too much space. We give an explicit form of $F(x, y, z; X)$ in [9].

## 5. Proof of Theorem 1.1

The polynomial $F(x, y, z; X)$ obtained in the previous section has $PSp_4(3)$ as Galois group over $\mathbb{C}(x, y, z)$. Actually, the coefficients of $F(x, y, z; X)$ are in $\mathbb{Q}[x, y, z]$. What can be said about its Galois group over an intermediate field of $\mathbb{C}/\mathbb{Q}$ ? By answering this question, we can prove Theorem 1.1. For simplicity, we denote $\mathbb{Q}(x, y, z)$ and $\mathbb{C}(x, y, z)$ by $K$ and $K'$ respectively. We also denote by $L$ and $L'$ the splitting field of $F(x, y, z; X)$ over $K$ and $K'$ respectively.

**Lemma 5.1.** *$PSp_4(3)$ is primitive as a transitive group of degree 40.*

*Proof.* Suppose $G \simeq PSp_4(3)$ is not primitive. Then $G$ has a partition of $\{1, \cdots, 40\}$ satisfying the condition of Definition 3.1. The group $H := \{g \in G \mid gB_i = B_i \ , \ \forall i = 1, \ldots, r\}$ is a normal subgroup of $G$. Because $PSp_4(3)$ is simple, $H$ is 1 or $G$. If $H = G$, then it contradicts transitivity of $G$. If $H = 1$, then $G \simeq PSp_4(3)$ as a permutation group of $\{B_1, \ldots, B_r\}$. This implies $r \mid 40$ and it contradicts Lemma 3.1. □

By definition of the symbols $L'$ and $K'$, $\mathrm{Gal}(L'/K')$ is a transitive group of degree 40. So $\mathrm{Gal}(L'/K')$ is primitive by Lemma 5.1. Because

$$\mathrm{Gal}(L/(L \cap K')) \simeq \mathrm{Gal}(L'/K')$$

and $\mathrm{Gal}(L/K)$ has this group as a subgroup, we see that $\mathrm{Gal}(L/K)$ is also a primitive group of degree 40. Thus $\mathrm{Gal}(L/K)$ is conjugate to one of the following 8 groups by Lemma 3.2.

$$PSp_4(3)a \ , \ PSp_4(3)b \ , \ PGSp_4(3)a \ , \ PGSp_4(3)b,$$

$$PSL_4(3) \ , \ PGL_4(3) \ , \ A_{40} \ , \ S_{40}.$$

We have to determine $\mathrm{Gal}(L/K)$ out of them. Because the intermediate field $L \cap K'$ is a Galois extension over $K$, $\mathrm{Gal}(L/(L \cap K'))$ is a normal subgroup of $\mathrm{Gal}(L/K)$. So we can exclude groups not containing $PSp_4(3)$ as their normal subgroups. Thus $\mathrm{Gal}(L/K)$ is conjugate to one of

$$PSp_4(3)a \ , \ PSp_4(3)b \ , \ PGSp_4(3)a \ , \ PGSp_4(3)b.$$

By consulting the data base of GAP[2], we can see that $PGSp_4(3)b$ is the only group not contained in $A_{40}$ and the other three groups are contained in $A_{40}$. So the discriminant of $F(x, y, z; X)$ determines whether $\mathrm{Gal}(L/K)$

is conjugate to $PGSp_4(3)b$ or not. We denote by $\mathbf{d}(F(x,y,z;X))$ the discriminant of $F(x,y,z;X)$. We can write

$$\mathbf{d}(F(x,y,z;X)) = f(x,y,z)g(x,y,z)^2$$

with some $f(x,y,z)$ and $g(x,y,z) \in \mathbb{Q}[x,y,z]$. We can assume that $f(x,y,z)$ is square free. On the other hand,

$$\mathbf{d}(F(x,y,z;X)) \in \mathbb{C}[x,y,z]^2$$

because $\mathrm{Gal}(L'/K') \simeq PSp_4(3)$, which is contained in $A_{40}$. Thus $f(x,y,z)$ must be constant and

$$\mathbf{d}(F(x,y,z;X)) = r \cdot g(x,y,z)^2$$

for a square free integer $r$. Whether $\mathrm{Gal}(L/K)$ is contained in $A_{40}$ or not depends on $r$. By computation, it turns out that $r \cdot g(1,1,1)^2 = -3 \cdot n^2$ for some $n \in \mathbb{Z}$. The left hand is the specialization of $\mathbf{d}(F(x,y,z;X))$ and the other hand is the discriminant of the specialized polynomial $F(1,1,1;X)$. Thus we get $r = -3$ and $\mathbf{d}(F(x,y,z;X)) = -3 \cdot g(x,y,z)^2$. It follows that if $k$ contains (resp. does not contain) $\sqrt{-3}$ then the Galois group of $F(x,y,z;X)$ over $k(x,y,z)$ is isomorphic to $PSp_4(3)$ (resp.$PGSp_4(3)$) for an intermediate field $k$ of $\mathbb{C}/\mathbb{Q}$ . Thus we can see that $F(x,y,z;X)$ is a regular $PSp_4(3)$-polynomial over $\mathbb{Q}(\sqrt{-3})$.

## Acknowledgement

The author would like to thank to Professor Tomoyoshi Ibukiyama of Osaka University for giving him this problem and various advices.

## References

[1] H.Aoki and T.Ibukiyama, *Simple graded rings of Siegel modular forms, differential operators and Borcherds products*, Int. J. Math. 16 (2005), 249-279.
[2] GAP, http://www.gap-system.org/.
[3] G.van der Geer, *Note on abelian schemes of level three*, Math. Ann. 278 (1987), 401-408.
[4] A.Hulpke, *Constructing Transitive Permutation Groups*, J. Symbolic. Computation. 39 (2005), 1-30.
[5] T.Ibukiyama, *On Siegel modular varieties of level 3*, Int. J. Math. 2 (1991) 17-35.
[6] J.Igusa, *On Siegel modular forms of genus two*, Amer. J. Math. 84 (1962), 175-200; I I, ibid. 86 (1964), 392-412.
[7] H.Klingen, *Introductory lectures on Siegel modular forms*, Cambridge University Press, 1990.
[8] J.Klüners and G.Malle, *Explicit Galois realization of transitive groups of degree up to 15*, J.Symbolic.Comput. 30 (2000), 675-716.
[9] H.Kitayama, *Appendix* in arXiv:0910.1755v1[math.NT]
[10] G.Malle, B.H.Matzat, *Inverse Galois Theory*, Springer, 1999.

[11] Colva M. Roney-Dougal, *The primitive permutation groups of degree less than 2500*, J. Alg. 292 (2005), 154-183.
[12] K.Shih, *On the construction of Galois extensions of function fields and number fields*, Math.Ann. 207 (1974), 99-120.

Department of Mathematics, Graduate School of Science, Osaka University, Machikaneyama 1-1, Toyonaka, Osaka, 560-0043, Japan
*e-mail address*: h-kitayama@cr.math.sci.osaka-u.ac.jp

(*Received July 27, 2009*)
(*Revised October 12, 2009*)