TSUKUBA J. MATH.
Vol. 27 No. 2 (2003), 307–317

ON A DECOMPOSITION OF BRUHAT TYPE FOR A CERTAIN FINITE GROUP

By

Koji TSUSHIMA

1. Introduction

B. Runge studied a connection between the invariant ring of a certain finite group and the ring of Siegel modular forms in [3]. The generators of this finite group are defined to be based on the action of Siegel modular group on the theta constant. This finite group is the subgroup of the general linear group $Gl(2^g, \mathbf{C})$. This group has been studied on several papers, for example, see [2].

Also, he studied a generalization of the above observation for Siegel-Jacobi forms in [5]. A certain finite group related to [5] is able to be defined in the same way of the case of [3] (see also [1]). This finite group is sometimes called metaplectic group.

On the other hand, in [4], he discribed that the finite group in [3] relates to the theory of Fourier transformations. Particularly, he proved that the finite group has a decomposition of Bruhat type (p. 183, theorem 2.2). This decomposition theorem was efficiently used for the computation of dimension formula (or Poincaré series) of ring of modular forms in [4].

Furthermore, in [6], he studied a invariant ring of weight polynomials for a binary linear code. Each of weight polynomials is homogeneous polynomial which is invariant of action of above finite group. And, he discribed that his theory in [6] can be generalized for the other codes.

When we consider a generalization of Runge's theory, as one step, we may take up the above metaplectic group. In addition, the study of the structure of this metaplectic group interests in the viewpoint of not only the generalization of Runge's theory but also group theory.

The purpose of this paper is to show a decomposition theorem of Bruhat type for a certain metaplectic group.

Received November 28, 2001.
Revised September 11, 2002.

2. Notations and Some Properties of the Finite Group

Throughout in this paper, $\mathbf{Z}/m\mathbf{Z}$ denotes the ring of integers modulo m.

In accordance with [5], we denote by $\mathbf{H}_g$ the Siegel upper half space of genus g defined by

$$\mathbf{H}_g := \{Z \in M(g, \mathbf{C}) \mid Z\text{: symmetric}, \operatorname{Im}(Z) > 0\}.$$

Moreover we introduce for any positive integer m and $a \in (\mathbf{Z}/2m\mathbf{Z})^g$ the following theta functions

$$f_a^{(m)}(\tau, z) = \sum_{x \in \mathbf{Z}^g} e\left(m\tau\left[x + \frac{a}{2m}\right] + \left\langle x + \frac{a}{2m}, 2mz\right\rangle\right)$$

for $(\tau, z) \in \mathbf{H}_g \times \mathbf{C}^g$, where $e(\cdot) = exp\, 2\pi i(Trace(\cdot))$ for matrices and numbers, $\tau[x] = {}^t x\tau x$ and $\langle\ ,\ \rangle$ denotes the standard scalar product. The functions

$$f_a^{(m)} := f_a^{(m)}(\tau, 0) = \sum_{x \in \mathbf{Z}^g} e\left(m\tau\left[x + \frac{a}{2m}\right]\right)$$

are the corresponding theta constants.

It is well known that the symplectic group (Siegel modular group) $Sp(2g, \mathbf{Z})$ is generated by

$$J = \begin{pmatrix} 0 & 1_g \\ -1_g & 0 \end{pmatrix}, \begin{pmatrix} 1_g & S \\ 0 & 1_g \end{pmatrix}; \quad {}^t S = S \in M(g, \mathbf{Z}).$$

These generators of $Sp(2g, \mathbf{Z})$ acts theta constants $f_a^{(m)}$ as follows:

For $J = \begin{pmatrix} 0 & 1_g \\ -1_g & 0 \end{pmatrix}$, we define

$$T_g := e\left(\frac{1}{8}\right)^g \left(\frac{1}{\sqrt{2m}}\right)^g e\left(\left(\frac{\langle a, b\rangle}{2m}\right)\right)_{a, b \in (\mathbf{Z}/2m\mathbf{Z})^g},$$

then

$$J(f_a^{(m)}) = \sqrt{\det(-\tau)} \sum_{b \in (\mathbf{Z}/2m\mathbf{Z})^g} (T_g)_{a,b} f_b^{(m)}$$

for all $a \in (\mathbf{Z}/2m\mathbf{Z})^g$.

For $\begin{pmatrix} 1_g & S \\ 0 & 1_g \end{pmatrix}$ we have

$$\begin{pmatrix} 1_g & S \\ 0 & 1_g \end{pmatrix}(f_a^{(m)})(\tau) = f_a^{(m)}(\tau + S) = e\left(\frac{S[a]}{4m}\right) f_a^{(m)}(\tau),$$

where $S[a] = {}^t aSa$.

So, in accordance with [1] and [5], we shall take following $(2m)^g \times (2m)^g$-matrices T_g and D_S:

$$T_g := \left(\frac{1+i}{\sqrt{2}}\right)^g \left(\frac{1}{\sqrt{2m}}\right)^g (\xi^{\langle a,b\rangle})_{a,b \in (\mathbf{Z}/2m\mathbf{Z})^g}$$

where ξ denotes the $2m$-th root of unity, $\langle\, ,\rangle$ denotes the standard scalar product and i denotes $\sqrt{-1}$,

$$D_S := diag(\eta^{S[a]} \text{ for } a \in (\mathbf{Z}/2m\mathbf{Z})^g)$$

for S runs over all integral symmetric $g \times g$-matrices, η denotes the $4m$-th root of unity, and $S[a] = {}^t aSa$. Let

$$\mathscr{G}_{g,m} := \langle T_g, D_S\rangle$$

be the subgroup of the unitary group $U((2m)^g, \mathbf{C}) \subset Gl((2m)^g, \mathbf{C})$ generated by T_g and D_S. This finite group is sometimes called metaplectic group of index m, genus g. As show in [1], this group $\mathscr{G}_{g,m}$ is a finite group.

Based on the argument of [5], we define a mapping φ from the above finite group to symplectic group

$$\varphi : \mathscr{G}_{g,m} \to Sp(2g, \mathbf{Z}/2m\mathbf{Z}).$$

This mapping φ is a surjective group homomorphism, which corresponds to $T_g \mapsto \begin{pmatrix} 0 & 1_g \\ -1_g & 0 \end{pmatrix}$ and $D_S \mapsto \begin{pmatrix} 1_g & S \\ 0 & 1_g \end{pmatrix}$. Further, there is a following diagram among the group and symplectic group:

$$Sp(2g, \mathbf{Z}) \xrightarrow{\psi} \mathscr{G}_{g,m}/\{\pm 1\} \xrightarrow{\varphi} Sp(2g, \mathbf{Z}/2m\mathbf{Z}).$$

The mapping ψ is a natural homomorphism. A mapping $Sp(2g, \mathbf{Z}) \to \mathscr{G}_{g,m}$ is not homomorphism in general, so we consider $\mathscr{G}_{g,m}/\{\pm 1\}$ instead of $\mathscr{G}_{g,m}$.

In this paper, we shall restrict the m is a prime p and $g = 1$ on the above definition. That is,

$$\mathscr{G} := \mathscr{G}_{1,p} = \langle T, D\rangle$$

where

$$T := T_1 = \frac{1+i}{2\sqrt{p}}(\xi^{ab})_{a,b \in \mathbf{Z}/2p\mathbf{Z}}$$

and

$$D := D_{(1)} = diag(\eta^{a^2} \text{ for } a \in \mathbf{Z}/2p\mathbf{Z}).$$

The center $Z(\mathscr{G})$ of the above group $\mathscr{G}$ is generated by $i^p = (\sqrt{-1})^p$ and T^2, i.e.

$$Z(\mathscr{G}) = \langle i^p, T^2 \rangle.$$

In addition, we shall define the element Q_σ as following product of T and D_σ:

$$Q_\sigma := T^4 D_{\sigma^{-1}} T D_\sigma T D_{\sigma^{-1}} T$$

where

$$D_\sigma := diag(\eta^{\sigma a^2} \text{ for } a \in \mathbf{Z}/2p\mathbf{Z})$$

for $\sigma \in (\mathbf{Z}/4p\mathbf{Z})^\times$. These elements T, D and Q_σ have the following relations:

$$T^8 = D^{4p} = Q_1 = 1, \quad T^4 = DTDTDT = -1,$$

$$TQ_\sigma = Q_{\sigma^{-1}} T \text{ up to scalar multiple } \pm i.$$

If $\sigma = \sigma^{-1}$ then Q_σ and T are always commutative.

Here, we shall consider the following Borel subgroup $\mathscr{B}$ of $\mathscr{G}$:

$$\mathscr{B} := \langle i^p, T^2, T^{-1}D^{2p}T, D, Q_\sigma \rangle = \langle i^p, D \rangle \langle T^2, T^{-1}D^{2p}T \rangle \langle Q_\sigma \rangle.$$

All elements of the Borel subgroup $\mathscr{B}$ are monomial matrix. The Borel subgroup $\mathscr{B}$ is a generalization of monomial group $H_{g,4}$ in [3] or [4].

3. The main results

In this section, let p be odd prime.

We shall recall that the Borel subgroup $\mathscr{B} = \langle i^p, T^2, T^{-1}D^{2p}T, D, Q_\sigma \rangle$ and the center $Z(\mathscr{G}) = \langle i^p, T^2 \rangle$. We shall prove following theorem.

THEOREM 1. *There is a decomposition*

$$\mathscr{G} = \langle \mathscr{B}, T \rangle = \mathscr{B} \cup \mathscr{B} T \mathscr{B}.$$

PROOF. Since $T^2 \in \mathscr{B}$, we may prove that $T\mathscr{B}T \subset \mathscr{B} \cup \mathscr{B}T\mathscr{B}$. We take an element b of $\mathscr{B}$, and its express by

$$b = x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}$$

where $x_k \in \mathscr{B}$ and $\varepsilon_k = \pm 1$ $(k = 1, \dots, r)$.

We shall consider the following two statements (S1) and (S2):

(S1) $\quad TbT \in \mathscr{B} \cup \mathscr{B}T\mathscr{B}$ for any $b \in \mathscr{B}$.

(S2) $TbT = z$ or $TbT = zTx^{\varepsilon}$ for some $z \in \mathscr{B}$ and $x \in \mathscr{B}$, $\varepsilon = \pm 1$.

At first, we shall show that the statement (S2) hold on $r = 0, 1$ and 2 for each generators of $\mathscr{B}$.

(In the case of $r = 0$)
We see that $TT = T^2 \in \mathscr{B}$.

(In the case of $r = 1$)
About the generator i^p, we see that $T(i^p)^{\varepsilon_1}T = T^2(i^p)^{\varepsilon_1} \in \mathscr{B}$.
About the generator T^2, we shall remark that $T^4 = -1$. Then we have $T(T^2)^{\varepsilon_1}T = T^2(T^2)^{\varepsilon_1} = \pm 1 \in \mathscr{B}$.
About the generator $T^{-1}D^{2p}T$, we see that $T(T^{-1}D^{2p}T)^{\varepsilon_1}T = (D^{2p})^{\varepsilon_1}T^2 \in \mathscr{B}$.
About the generator D, we shall remark that $DTDTDT = -1$.
For the case of $\varepsilon_1 = 1$, it follows that $TDT = -D^{-1}T^{-1}D^{-1} = -D^{-1}T^{-2}TD^{-1}$. Since $-D^{-1}T^{-2} \in \mathscr{B}$ and $D^{-1} \in \mathscr{B}$, we obtain (S2).
For the case of $\varepsilon_1 = -1$, we have $TD^{-1}T = T^2(T^{-1}D^{-1}T^{-1})T^2 = -T^4DTD = DTD$.
About the generator Q_σ, we shall remark that $TQ_\sigma = Q_{\sigma^{-1}}T$ up to scalar multiple $\pm i$, and $\pm i \in \mathscr{B}$. Then we have $T(Q_\sigma)^{\varepsilon_1}T = Q_{\sigma^{-1}}^{\varepsilon_1}T^2 \in \mathscr{B}$.

(In the case of $r = 2$)
First, as element b in (S2), we take the product of the generator i^p and all generators of $\mathscr{B}$.

$T(i^p)^{\varepsilon_1}(i^p)^{\varepsilon_2}T = T^2(i^p)^{\varepsilon_1+\varepsilon_2} \in \mathscr{B}$.
$T(i^p)^{\varepsilon_1}(T^2)^{\varepsilon_2}T = (i^p)^{\varepsilon_1}T^2(T^2)^{\varepsilon_2} = \pm(i^p)^{\varepsilon_1} \in \mathscr{B}$.
$T(i^p)^{\varepsilon_1}(T^{-1}D^{2p}T)^{\varepsilon_2}T = (i^p)^{\varepsilon_1}T(T^{-1}D^{2p}T)^{\varepsilon_2}T = (i^p)^{\varepsilon_1}(D^{2p})^{\varepsilon_2}T^2 \in \mathscr{B}$.
$T(i^p)^{\varepsilon_1}D^{\varepsilon_2}T = (i^p)^{\varepsilon_1}TD^{\varepsilon_2}T \in \mathscr{B}$.
$T(i^p)^{\varepsilon_1}Q_\sigma^{\varepsilon_2}T = (i^p)^{\varepsilon_1}TQ_\sigma^{\varepsilon_2}T \in \mathscr{B}$.

Next, as element b in (S2), we take the product of the generator T^2 and all generators of $\mathscr{B}$.

$T(T^2)^{\varepsilon_1}(i^p)^{\varepsilon_2}T = \pm(i^p)^{\varepsilon_2} \in \mathscr{B}$.
$T(T^2)^{\varepsilon_1}(T^2)^{\varepsilon_2}T = \pm T^2 \in \mathscr{B}$.
$T(T^2)^{\varepsilon_1}(T^{-1}D^{2p}T)^{\varepsilon_2}T = (T^2)^{\varepsilon_1}T(T^{-1}D^{2p}T)^{\varepsilon_2}T \in \mathscr{B}$.
$T(T^2)^{\varepsilon_1}D^{\varepsilon_2}T = (T^2)^{\varepsilon_1}TD^{\varepsilon_2}T \in \mathscr{B}$.
$T(T^2)^{\varepsilon_1}Q_\sigma^{\varepsilon_2}T = (T^2)^{\varepsilon_1}TQ_\sigma^{\varepsilon_2}T \in \mathscr{B}$.

Next, as element b in (S2), we take the product of the generator $T^{-1}D^{2p}T$ and all generators of $\mathscr{B}$.

$T(T^{-1}D^{2p}T)^{\varepsilon_1}(i^p)^{\varepsilon_2}T = (i^p)^{\varepsilon_2}(D^{2p})^{\varepsilon_1}T \in \mathscr{B}$.
$T(T^{-1}D^{2p}T)^{\varepsilon_1}(T^2)^{\varepsilon_2}T = (T^2)^{\varepsilon_2}(D^{2p})^{\varepsilon_1}T \in \mathscr{B}$.
$T(T^{-1}D^{2p}T)^{\varepsilon_1}(T^{-1}D^{2p}T)^{\varepsilon_2}T = (D^{2p})^{\varepsilon_1}TT^{-1}TT^{-1}(D^{2p})^{\varepsilon_2} = (D^{2p})^{\varepsilon_1+\varepsilon_2}$.
Since $D^{4p} = 1$, we obtain (S2).
$T(T^{-1}D^{2p}T)^{\varepsilon_1}D^{\varepsilon_2}T = (D^{2p})^{\varepsilon_1}TD^{\varepsilon_2}T \in \mathscr{B}$.
$T(T^{-1}D^{2p}T)^{\varepsilon_1}Q_\sigma^{\varepsilon_2}T = (D^{2p})^{\varepsilon_1}TQ_\sigma^{\varepsilon_2}T \in \mathscr{B}$.

Next, as element b in (S2), we take the product of the generator D and all generators of $\mathscr{B}$.
$TD^{\varepsilon_1}(i^p)^{\varepsilon_2}T = (i^p)^{\varepsilon_2}TD^{\varepsilon_1}T \in \mathscr{B}$.
$TD^{\varepsilon_1}(T^2)^{\varepsilon_2}T = (T^2)^{\varepsilon_2}TD^{\varepsilon_1}T \in \mathscr{B}$.
$TD^{\varepsilon_1}(T^{-1}D^{2p}T)^{\varepsilon_2}T = TD^{\varepsilon_1}TT^{-1}(T^{-1}D^{2p}T)^{\varepsilon_2}T \in \mathscr{B}$.
$TD^{\varepsilon_1}D^{\varepsilon_2}T = TD^{\varepsilon_1}TT^{-1}D^{\varepsilon_2}T \in \mathscr{B}$.
$TD^{\varepsilon_1}Q_\sigma^{\varepsilon_2}T = TD^{\varepsilon_1}TT^{-1}Q_\sigma^{\varepsilon_2}T \in \mathscr{B}$.

Next, as element b in (S2), we take the product of the generator Q_σ and all generators of $\mathscr{B}$.
$TQ_\sigma^{\varepsilon_1}(i^p)^{\varepsilon_2}T = (i^p)^{\varepsilon_2}TQ_\sigma^{\varepsilon_1}T \in \mathscr{B}$.
$TQ_\sigma^{\varepsilon_1}(T^2)^{\varepsilon_2}T = (T^2)^{\varepsilon_2}TQ_\sigma^{\varepsilon_1}T \in \mathscr{B}$.
About the $TQ_\sigma^{\varepsilon_1}(T^{-1}D^{2p}T)^{\varepsilon_2}T$.
If $\varepsilon_1 = \varepsilon_2 = 1$, then $TQ_\sigma T^{-1}D^{2p}T^2 = Q_{\sigma^{-1}}D^{2p}T^2 \in \mathscr{B}$.
If $\varepsilon_1 = 1$ and $\varepsilon_2 = -1$, then $TQ_\sigma^{\varepsilon_1}T^{-1}(D^{2p})^{-1}T^2 = TQ_\sigma T(D^{2p})^{-1} \in \mathscr{B}$.
In the case of $\varepsilon_1 = -1$, we take $TQ_\sigma^{-1} = T^2T^{-1}Q_\sigma^{-1}$.
$TQ_\sigma^{\varepsilon_1}D^{\varepsilon_2}T = TQ_\sigma^{\varepsilon_1}TT^{-1}D^{\varepsilon_2}T \in \mathscr{B}$.
$TQ_\sigma^{\varepsilon_1}Q_\sigma^{\varepsilon_2}T = TQ_\sigma^{\varepsilon_1}TT^{-1}Q_\sigma^{\varepsilon_2}T \in \mathscr{B}$.

Further, we shall show that the statement (S1). We use induction on r ($r \geq 2$). Since $T^2 \in Z(\mathscr{G})$,

$$\begin{aligned} TbT &= T(x_1^{\varepsilon_1}\cdots x_r^{\varepsilon_r})T \\ &= T^{-2}T(x_1^{\varepsilon_1}x_2^{\varepsilon_2})TT(x_3^{\varepsilon_3}\cdots x_r^{\varepsilon_r})T. \end{aligned}$$

If $T(x_1^{\varepsilon_1}x_2^{\varepsilon_2})T = z$, then

$$TbT = T^{-2}zT(x_3^{\varepsilon_3}\cdots x_r^{\varepsilon_r})T \in \mathscr{B} \cup \mathscr{B}T\mathscr{B}.$$

If $T(x_1^{\varepsilon_1}x_2^{\varepsilon_2})T = zTx^{\varepsilon}$, then we shall put $Tx^{\varepsilon}T = z'Tx'^{\varepsilon'}$ for some $z' \in \mathscr{B}$ and $x' \in \mathscr{B}$, $\varepsilon' = \pm 1$. So,

$$TbT = T^{-2}zz'Tx'^{\varepsilon'}(x_3^{\varepsilon_3}\cdots x_r^{\varepsilon_r})T \in \mathscr{B} \cup \mathscr{B}T\mathscr{B}.$$

This completes the proof of theorem 1. □

Moreover, the group $\mathscr{G}$ is decomposed as the following Theorem 2. This is the main theorem of this paper.

THEOREM 2. *The group $\mathscr{G}$ has the following decomposition*:

$$\mathscr{G} = \mathscr{B} \bigsqcup_{\alpha=0}^{2p-1} D^{\alpha}T\mathscr{B} \bigsqcup_{\beta=0}^{p-1} D^{\beta}TD^{2}\mathscr{B} \bigsqcup_{\gamma=0,1} D^{\gamma}TD^{p}T\mathscr{B} \ (\textit{disjoint union})$$

where $\mathscr{B} = \langle i^p, D\rangle\langle T^2, T^{-1}D^{2p}T\rangle\langle Q_\sigma\rangle$.

PROOF. From the mention of §2, there exists the surjective group homomorphism

$$\varphi : \mathscr{G} \to Sp(2, \mathbf{Z}/2p\mathbf{Z})$$

which corresponds to $T \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $D \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. We shall remark that the symplectic group $Sp(2, \mathbf{Z}/2p\mathbf{Z})$ equals to the special linear group $Sl(2, \mathbf{Z}/2p\mathbf{Z})$, and $Sl(2, \mathbf{Z}/2p\mathbf{Z}) = Sl(2, \mathbf{Z}/2\mathbf{Z}) \times Sl(2, \mathbf{Z}/p\mathbf{Z})$.

Now, we put $\varphi(\mathscr{B}) := N$. Since

$$N \subset Sl(2, \mathbf{Z}/2p\mathbf{Z}) = Sl(2, \mathbf{Z}/2\mathbf{Z}) \times Sl(2, \mathbf{Z}/p\mathbf{Z}),$$

there are $N' \subset Sl(2, \mathbf{Z}/2\mathbf{Z})$ and $N'' \subset Sl(2, \mathbf{Z}/p\mathbf{Z})$ such that $N = N' \times N''$. From the result of Theorem 1, we have

$$\mathscr{G} = \mathscr{B} \cup \mathscr{B}T\mathscr{B}.$$

So, if we map T to $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $\mathscr{B}$ to N we get

$$Sl(2, \mathbf{Z}/2p\mathbf{Z}) \supset N \cup N\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}N.$$

Here, we take $h \in \ker\varphi$. If $h \in \mathscr{B}T\mathscr{B}$, then $\varphi(h) \in N\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}N$ and $\varphi(h) \notin N$. However, since $\varphi(h) = 1$, thus $\ker\varphi \subset \mathscr{B}$.

On the other hand, the cardinal of representative elements of RHS of this theorem is clearly $3(p+1)$. Therefore, the index

$$[\mathscr{G} : \mathscr{B}] \leq 3(p+1).$$

And since $\varphi(\mathscr{B}) \subset \mathscr{B}$, thus

$$[Sl(2, \mathbf{Z}/2p\mathbf{Z}) : \varphi(\mathscr{B})] \leq 3(p+1).$$

Moreover, we have

$$Sl(2,\mathbf{Z}/2p\mathbf{Z})/N \simeq Sl(2,\mathbf{Z}/2\mathbf{Z})/N' \times Sl(2,\mathbf{Z}/p\mathbf{Z})/N''.$$

The $Sl(2,\mathbf{Z}/2\mathbf{Z})/N'$ is isomorphic to the projective space $\mathbf{P}^1(\mathbf{Z}/2\mathbf{Z}) = \{\infty, 0, 1\}$ and the $Sl(2,\mathbf{Z}/p\mathbf{Z})/N''$ is isomorphic to the projective space $\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z}) = \{\infty, 0, 1, \dots, p-1\}$. Thus the index

$$[Sl(2,\mathbf{Z}/2p\mathbf{Z}) : N] = \#(\mathbf{P}^1(\mathbf{Z}/2\mathbf{Z})) \times \#(\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})) = 3(p+1).$$

Hence,

$$\begin{aligned} 3(p+1) &\geq [Sl(2,\mathbf{Z}/2p\mathbf{Z}) : \varphi(\mathscr{B})] \\ &\geq [Sl(2,\mathbf{Z}/2p\mathbf{Z}) : \mathscr{B}] = 3(p+1). \end{aligned}$$

Next, we shall show that the RHS of this theorem is left invariant by the action of T and D. We put $t := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $d^u := \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ for $u \in (\mathbf{Z}/2p\mathbf{Z})^\times$. We use the well known relations:

$$\begin{aligned} td^ut^{-1} &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ -u & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -u^{-1} \\ 0 & 1 \end{pmatrix}\begin{pmatrix} u^{-1} & 0 \\ 0 & u \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -u^{-1} \\ 0 & 1 \end{pmatrix} \end{aligned}$$

and

$$\begin{aligned} td^utN &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}N \\ &= \begin{pmatrix} 1 & -u^{-1} \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}N. \end{aligned}$$

From the above relation, for the action of T (we use the symbol $\cdot$; this is the product of matrix), we get

$$T \cdot (D^l T\mathscr{B}) = D^{-l^{-1}} T\mathscr{B}$$

for $l = 1, 3, \dots, p-1, p+1, \dots, 2p-1$, $l^{-1} \in (\mathbf{Z}/2p\mathbf{Z})^\times$,

$$T \cdot (D^n T\mathscr{B}) = D^m T D^2 T\mathscr{B}$$

for $n = 2, \dots, 2p-2$, $m = 2^{-1} - n^{-1} \pmod p$, and

$$T \cdot (DTD^pT\mathscr{B}) = D^{(p+1)/2}TD^2T\mathscr{B}.$$

Since $T^2 \in Z(\mathscr{G})$, so $T \cdot (T\mathscr{B}) = \mathscr{B}$, $T \cdot (TD^pT\mathscr{B}) = D^pT\mathscr{B}$ is obvious.

On the other hand, for the action of D (as above, we use the symbol $\cdot$), we get

$$D \cdot (\mathscr{B}) = \mathscr{B},$$
$$D \cdot (D^vT\mathscr{B}) = D^{v+1}T\mathscr{B} \quad \text{for } v = 0, \dots, 2p-2,$$
$$D \cdot (D^{2p-1}T\mathscr{B}) = T\mathscr{B}.$$

And

$$D \cdot (D^wTD^2T\mathscr{B}) = D^{w+1}TD^2T\mathscr{B} \quad \text{for } w = 0, \dots, p-2,$$
$$D \cdot (D^{p-1}TD^2T\mathscr{B}) = TD^2T\mathscr{B},$$
$$D \cdot (DTD^pT\mathscr{B}) = TD^pT\mathscr{B}.$$

This completes the proof of theorem 2. □

4. Some Remarks

For $p = 2$ case (i.e., $a \in \mathbf{Z}/4\mathbf{Z}$), the group $\mathscr{G}$ is as follows:

$$\mathscr{G} = \left\langle T = \frac{1+i}{2\sqrt{2}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}, D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \eta & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & \eta \end{pmatrix} \right\rangle$$

where $i = \sqrt{-1}$ and $\eta^8 = 1$. In this case, we have

$$Z(\mathscr{G}) = \langle -1, T^2 \rangle = \left\{ \pm 1, \pm \begin{pmatrix} i & 0 & 0 & 0 \\ 0 & 0 & 0 & i \\ 0 & 0 & i & 0 \\ 0 & i & 0 & 0 \end{pmatrix} \right\} = \{Q_1, Q_3, Q_5, Q_7\},$$

$$\mathscr{B} = \left\langle -1, T^2, T^{-1}D^4T = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, D \right\rangle.$$

The order of $\mathscr{G}$ is 384, the order of Borel subgroup $\mathscr{B}$ of $\mathscr{G}$ is 64, and the index $[\mathscr{G} : \mathscr{B}] = 6$.

For the action of T, we get

$$T \cdot (T\mathscr{B}) = \mathscr{B},$$

$$T \cdot (DT\mathscr{B}) = -D^{-1}T^{-1}D^{-1}\mathscr{B} = D^{-1}T\mathscr{B} = D^3D^4T\mathscr{B} = D^3TT^{-1}D^4T\mathscr{B} = D^3T\mathscr{B},$$

$$T \cdot (TD^2T\mathscr{B}) = D^2T\mathscr{B}.$$

For the action of D, we calculate the commutator

$$[D^4, T] = (D^4)^{-1}T^{-1}D^4T = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \in \mathscr{B}.$$

Then,

$$D \cdot (D^3T\mathscr{B}) = D^4T\mathscr{B} = TD^4[D^4, T]\mathscr{B} = T\mathscr{B}.$$

Further, $D \cdot (\mathscr{B}) = \mathscr{B}$,

$$D \cdot (TD^2T\mathscr{B}) = DTDDT\mathscr{B} = T^{-1}D^{-1}T^{-1}T^{-1}D^{-1}T^{-1}\mathscr{B}$$

$$= TD^6T\mathscr{B} = TD^2TT^{-1}D^4T\mathscr{B} = TD^2T\mathscr{B}.$$

Hence, we get

$$\mathscr{G} = \mathscr{B} \bigsqcup_{\alpha=0}^{3} D^\alpha T\mathscr{B} \bigsqcup TD^2T\mathscr{B} \quad (p = 2 \text{ case}).$$

In [5], B. Runge determined the kernel of theta representation. By using this result, it is possible to determine the group structure more in detail, which has been also indicated in [1]. So, we guess that the result of this paper can be generalized for the group defined with respect to $\mathbf{Z}/2m\mathbf{Z}$, more generally $(\mathbf{Z}/2m\mathbf{Z})^g$. However, there is no direct generalization for the group defined for $\mathbf{Z}/m\mathbf{Z}$, because the action of Siegel modular group $Sp(2g, \mathbf{Z})$ on the theta constant (see § 2) is not well defind in the case that m is odd.

The result of the generalization for $\mathbf{Z}/2m\mathbf{Z}$ may be more complicate than the result of this paper. For example, the group $\mathscr{G}'$ for $\mathbf{Z}/16\mathbf{Z}$ ($m = 8$ case) is given. In this case, the order of $\mathscr{G}'$ is 24576, the order of Borel subgroup $\mathscr{B}'$ of $\mathscr{G}'$ is 1024, and the index $[\mathscr{G}' : \mathscr{B}'] = 24$. In this case, we can take up 1, $D^\alpha T$ ($\alpha = 0, \dots, 15$), $D^\beta TD^2T$ ($\beta = 0, \dots, 3$), $TD^4T, TD^8T, TD^{12}T$, as representative elements of the coset $\mathscr{G}'/\mathscr{B}'$. Here, the representative element $TD^{12}T$ is not applied for the theorem of this paper. This fact is easily checked by using a computer.

Acknowledgement

The author would like to heartily thank to Professor Tatsuo Kimura, Professor Jun Morita and Professor Bernhard Runge. Prof. T. Kimura is my advisor, who always gives me much encouragement and mathematical knowledges. Prof. J. Morita discusses with me about explicit way to solve this problem. Last but not least, Prof. B. Runge suggests me to try this problem and gives me many useful advises.

References

[1] E. Bannai, S. T. Dougherty, M. Harada and M. Oura, Type II Codes, Even Unimodular Lattices, and Invariant Rings, IEEE Trans. Inform. Theory, **45** (1999), pp. 1194–1205.
[2] P. Kleidman and M. Liebeck, The subgroup structure of the finite classical groups, LMS Lecture Note 129, Cambridge University Press, 1990.
[3] B. Runge, On Siegel modular forms, Part I, J. reine. angew. Math., **436** (1993), pp. 57–85.
[4] B. Runge, On Siegel modular forms, Part II, Nagoya Math. J., **138** (1995), pp. 179–197.
[5] B. Runge, Theta functions and Siegel-Jacobi forms, Acta Math., **175** (1995), pp. 165–196.
[6] B. Runge, Codes and Siegel modular forms, Discrete Math., **148** (1996), pp. 175–204.

Institute of Mathematics
University of Tsukuba
Ibaraki, 305, Japan