33. On Regular Elliptic Conjugacy Classes of the Siegel Modular Group

By Hisaichi MIDORIKAWA
Tsuda College

(Communicated by Shokichi IYANAGA, M. J. A., March 12, 1982)

1. Introduction. In this paper we announce two theorems on regular elliptic conjugacy classes of the Siegel modular group of degree $2n$. The detailed discussion with proof will appear elsewhere. For the general modular group $GL(n, \boldsymbol{Z})$, it was shown by C. G. Latimer and C. C. MacDuffee [3] and O. Taussky [4] that the number of conjugacy classes, which have an irreducible characteristic polynomial, is equal to the number of ideal classes of a subring in a certain algebraic number field. Especially, if the characteristic polynomial of a conjugacy class is a cyclotomic polynomial f, then that ring consists of all algebraic integers in the splitting field of f over $\boldsymbol{Q}$.

Let $\Gamma = Sp(2n, \boldsymbol{Z})$ be the Siegel modular group of degree $2n$. Concerning the conjugacy classes of Γ, we get some results analogous to the above mentioned result for $GL(n, \boldsymbol{Z})$. Our results in this paper are an existence proof of the "regular elliptic elements" in Γ and a formula in class number for the "regular elliptic elements" of Γ. We shall state our results more precisely after the preparations in § 2.

2. Preliminaries. Let $G = Sp(2n, \boldsymbol{R})$ be the real symplectic group of degree $2n$. The group G is defined by

$$G = \{g \in GL(2n, \boldsymbol{R}) ; {}^t gJg = J\} \tag{2.1}$$

where $J = \begin{pmatrix} 0 & 1_n \\ -1_n & 0 \end{pmatrix}$ and 1_n is the identity matrix of degree n. Let $\mathfrak{S}$ be the set of all positive definite symmetric matrices in G. Then $\mathfrak{S}$ is identified with the Siegel upper half space. The group G acts on $\mathfrak{S}$ by the rule $G \times \mathfrak{S} \ni (g, p) \to {}^t gpg \in \mathfrak{S}$.

Definition 1. An element g in G is called *elliptic* if g fixes an element in $\mathfrak{S}$.

Let $O(2n)$ be the orthogonal group of degree $2n$ and put $K = O(2n) \cap G$. Then K is a maximal compact subgroup of G. It is easily seen that an element h in G is elliptic if and only if h is conjugate to an element in K.

Let us define a regular element in G. We denote the Lie algebra of G by $\mathfrak{g}$. The adjoint action of G on $\mathfrak{g}$ is defined by

$$Ad(g)X = gXg^{-1}, \quad g \in G, \quad X \in \mathfrak{g}.$$

The rank $r(G)$ of G is defined by the following formula:

$$r(G)=\operatorname*{Min}_{g\in G}\dim \operatorname{Ker}(Ad(g)-1).$$

The rank of $Sp(2n, \boldsymbol{R})$ is equal to n.

Definition 2. An element g in G is called *regular* if

$$\dim \operatorname{Ker}(Ad(g)-1)=r(G).$$

Let Γ be the Siegel modular group $Sp(2n, \boldsymbol{Z})$ of degree $2n$. Γ is the set of all integral matrices in G.

Lemma. *An element γ in Γ is regular* (and) *elliptic if and only if the characteristic polynomial f of γ is decomposed into mutually distinct cyclotomic polynomials over $\boldsymbol{Q}$ and the degree of any irreducible factor of f over $\boldsymbol{Q}$ is $\geqq 2$.*

3. Main theorems. Our first result is the following.

Theorem I. *Let f be the mth cyclotomic polynomial with degree $2n=\phi(m)$ where ϕ is the Euler function. Then the Siegel modular group $Sp(2n, \boldsymbol{Z})$ has a regular elliptic element with the characteristic polynomial f.*

For a fixed cyclotomic polynomial f with degree $2n$, we put

$$\Gamma(f)=\{\gamma\in\Gamma\,;\ \text{the characteristic polynomial of } \gamma \text{ is } f\}.$$

Definition 3. Two elements γ and γ' in $\Gamma(f)$ are called Γ-(respectively G-)*conjugate* if there exists an element g in Γ (respectively in G) such that $g\gamma g^{-1}=\gamma'$.

The set $\Gamma(f)$ is divided into a certain number of the conjugate classes. We denote the sets of G-conjugacy classes and Γ-conjugacy classes in $\Gamma(f)$ by $\Gamma(f)/G$ and $\Gamma(f)/\Gamma$ respectively. Each class $\Gamma^G(f)$ in $\Gamma(f)/G$ is divided into Γ-conjugate classes. We denote the set of these classes by $\Gamma^G(f)/\Gamma$. $\Gamma^G(f)/\Gamma$ is a subset of $\Gamma(f)/\Gamma$.

Let A be the ideal class group of the splitting field k of the cyclotomic polynomial f over $\boldsymbol{Q}$.

Notations. k_0: the real subfield of k with $[k: k_0]=2$.

$C(\mathfrak{a})$: the class in A containing a given fractional ideal $\mathfrak{a}$ in k.

$\boldsymbol{H}$: the subgroup of A defined by $\boldsymbol{H}=\{C(\mathfrak{a})\,;\ N\mathfrak{a}$ is principal in $k_0\}$, when N means the norm from k to k_0.

$\boldsymbol{H}^+$: the subgroup of $\boldsymbol{H}$ defined by $\boldsymbol{H}^+=\{C(\mathfrak{a})\,;\ N\mathfrak{a}=(\omega),\ \omega$ is totally positive in $k_0\}$.

$\boldsymbol{E}$ (resp. $\boldsymbol{E}_0$): the unit group of k (resp. k_0).

$\boldsymbol{E}_0^+$: the group of all totally positve units in k_0.

$|S|$: the number of elements in a given finite set S.

$(L: M)$: the index of a subgroup M in L.

Under these notations we have the following theorem.

Theorem II. *Let Γ be the Siegel modular group of degree $2n$ and f be the mth cyclotomic polynomial with the degree $2n=\phi(m)$. Then we have*

(1) $$|\Gamma(f)/G|=(\boldsymbol{E}_0: \boldsymbol{E}_0^+)(\boldsymbol{H}: \boldsymbol{H}^+),$$

(2) $$|\Gamma^G(f)/\Gamma|=(\boldsymbol{E}_0^+ : N\boldsymbol{E})\,|\boldsymbol{H}^+|$$

for each class $\Gamma^G(f)$ *in* $\Gamma(f)/G$ *where* $N\boldsymbol{E}=\{N\varepsilon\,;\,\varepsilon\in\boldsymbol{E}\}$.

Example. Let $f(t)=t^4+t^3+t^2+t+1$. Then f is the 5th cyclotomic polynomial over $\boldsymbol{Q}$. For the groups $\Gamma=Sp(4,\boldsymbol{Z})$ and $G=Sp(4,\boldsymbol{R})$, the number of conjugacy classes is as follows.

(1) $|\Gamma(f)/G|=2^2$, (2) $|\Gamma^G(f)/\Gamma|=1$.

4. Outline of the proofs of the theorems. Let f be a fixed cyclotomic polynomial with degree $2n$ and ζ is a root of $f=0$. By $k=\boldsymbol{Q}(\zeta)$ (resp. $k_0=\boldsymbol{Q}(\zeta+\zeta^{-1})$), we denote the field generated by ζ (resp. $\zeta+\zeta^{-1}$) over $\boldsymbol{Q}$. It is known that the ring of algebraic integers $\mathfrak{O}$ in k is generated by $1, \zeta, \zeta^2, \cdots, \zeta^{2n-1}$ over $\boldsymbol{Z}$ (cf. H. Hasse [2]).

Let γ be an element in Γ with the characteristic polynomial f and $\boldsymbol{x}\in k^{2n}$ be an eigenvector of γ corresponding to the eigenvalue ζ. Since the ring $\mathfrak{O}$ is generated by $1, \zeta, \zeta^2, \cdots$ over $\boldsymbol{Z}$ and f is irreducible, we have the following

(3.1) The entries of $\boldsymbol{x}$ generate a fractional ideal $\mathfrak{a}$ in k.

(This fact is due to O. Taussky [4].) Let $(\boldsymbol{x},\boldsymbol{y})$ be the canonical positive definite Hermitian form on $\boldsymbol{C}^{2n}\times\boldsymbol{C}^{2n}$ and $G(k/\boldsymbol{Q})$ be the Galois group of k over $\boldsymbol{Q}$. Then for each eigenvector $\boldsymbol{x}$ of γ corresponding to the eigenvalue ζ, there exists $\boldsymbol{x}^*$ in k^{2n} satisfying the following (3.2) for any σ in $G(k/\boldsymbol{Q})$.

$$(\sigma(\boldsymbol{x}),\boldsymbol{x}^*)=\begin{cases}1 & \text{if } \sigma=1\\ 0 & \text{if } \sigma\neq 1.\end{cases} \tag{3.2}$$

Since $\boldsymbol{x}^*$ is an eigenvector of ${}^t\gamma^{-1}$ and ${}^t\gamma J\gamma=J$, we have the following

(3.3) $J\boldsymbol{x}=\lambda\boldsymbol{x}^*$ for an element λ in k.

From these observations arises a question; what is an ideal $\mathfrak{a}$ which has the system $(\boldsymbol{x},\boldsymbol{x}^*,\lambda)$ satisfying (3.1)–(3.3)? The answer to the question given below constitutes the fundamental lemma in this paper. Let $\mathfrak{a}$ be a fractional ideal in k.

Lemma. *A fractional ideal* $\mathfrak{a}$ *in* k *has the system* $(\boldsymbol{x},\boldsymbol{x}^*,\lambda)$ *satisfying* (3.1)–(3.3) *if and only if* $N\mathfrak{a}$ *is a principal ideal in* k_0.

Using the lemma, Theorem I can be proved as follows. Let $\mathfrak{a}$ be a principal ideal in k. Then $N\mathfrak{a}$ is principal in k_0. Applying the above lemma to $\mathfrak{a}$, there exists a system $(\boldsymbol{x},\boldsymbol{x}^*,\lambda)$ satisfying (3.1)–(3.3). Following O. Taussky [4], we define a linear transformation γ on k^{2n} by $\gamma\sigma(\boldsymbol{x})=\sigma(\zeta\boldsymbol{x})$ for σ in $G(k/\boldsymbol{Q})$. Since the entries in $\boldsymbol{x}$ generate the ideal $\mathfrak{a}$, γ belongs to $GL(2n,\boldsymbol{Z})$. Furthermore since $J\boldsymbol{x}=\lambda\boldsymbol{x}^*$, we have ${}^t\gamma J\gamma=J$. Thus γ belongs to $Sp(2n,\boldsymbol{Z})$ and f is the characteristic polynomial of γ. Hence γ is regular elliptic.

Remark. Let $\boldsymbol{x}$ and $\boldsymbol{x}^*$ be the same as above and put $\mathfrak{a}=$the ideal generated by $\boldsymbol{x}$, $\mathfrak{a}^*=$the ideal generated by $\boldsymbol{x}^*$. Then the complex conjugate of $\mathfrak{a}^*$ is the socalled "complementary ideal of $\mathfrak{a}$" (cf. R. Dedekind [1] or O. Taussky [5]).

The proof of Theorem II is also based on our fundamental lemma.

References

[1] R. Dedekind: Über die Diskriminanten endlicher Körper. Gesammelte math. Werke, Bd. I, Braunschweig (1930).
[2] H. Hasse: Zahlentheorie. Akademie Verlag (1949).
[3] C. G. Latimer and C. C. MacDuffee: A correspondence between classes of ideals and classes of matrices. Ann. of Math., **34**, 313–316 (1933).
[4] O. Taussky: On a theorem of Latimer and MacDuffee. Can. J. Math., **1**, 300–302 (1949).
[5] ——: On matrix classes corresponding to an ideal and its inverse. Illinois J. Math., **1**, 108–113 (1957).