TOKYO J. MATH.
VOL. 6, NO. 1, 1983

On the Number of Regular Elliptic Conjugacy Classes in the Siegel Modular Group of Degree 2n

Hisaichi MIDORIKAWA

Tsuda College

Introduction

Let G be the real symplectic group $Sp(2n, \boldsymbol{R})$ of degree $2n$ and Γ be the Siegel modular group $Sp(2n, \boldsymbol{Z})$. For a given cyclotomic polynomial f with degree $2n$ over $\boldsymbol{Q}$, we denote by $\Gamma(f)$ the set of all elements in Γ with the characteristic polynomial f. By $\Gamma(f)/\Gamma$ and $\Gamma(f)/G$, we shall mean the Γ-conjugacy classes of $\Gamma(f)$ and G-conjugacy classes of $\Gamma(f)$, respectively (for the detailed statements, see §4). The purpose of this paper is to prove the following two theorems.

THEOREM I. *Let Γ and $\Gamma(f)$ be the same as above. Then $\Gamma(f)$ is not empty.*

Let f be a fixed cyclotomic polynomial over $\boldsymbol{Q}$ with degree $2n$. We use the following notations:

k; the splitting field of f over $\boldsymbol{Q}$,

k_0; the real subfield of k with $|k:k_0|=2$,

A; the absolute ideal class group of k,

$\boldsymbol{H}$; the subgroup of A defined by $\boldsymbol{H}=\{C(\mathfrak{a})\in A; N\mathfrak{a}$ is principal in $k_0\}$, where $\mathfrak{a}$ is a fractional ideal in k, $N\mathfrak{a}$ is the relative norm of $\mathfrak{a}$ to k_0 and $C(\mathfrak{a})$ is the class in A containing $\mathfrak{a}$,

$\boldsymbol{H}^+$; the subgroup of $\boldsymbol{H}$ defined by $\boldsymbol{H}^+=\{C(\mathfrak{a})\in\boldsymbol{H}; N\mathfrak{a}=(\omega)$ and ω is totally positive over $\boldsymbol{Q}\}$,

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

$\boldsymbol{E}_0^+$; the group of all totally positive units in k_0,

$N\boldsymbol{E}=\{N\varepsilon;\ \varepsilon$ is a unit $k\}$,

$|S|$; the number of elements in a finite set S,

$(A\colon B)$; the index of a subgroup B in a group A.

Under these notations we have

Received March 11, 1982
Revised October 3, 1982

THEOREM II. *Let Γ be the Siegel modular group with degree $2n$ and f the m-th cyclotomic polynomial over $\boldsymbol{Q}$ with $\phi(m)=2n$ where ϕ is Euler function. Then we have* (1) $|\Gamma(f)/G|=(\boldsymbol{E}_0:\boldsymbol{E}_0^+)(\boldsymbol{H}:\boldsymbol{H}^+)$, *and* (2) $|\Gamma^G(f)/\Gamma|=(\boldsymbol{E}_0^+:N\boldsymbol{E})|\boldsymbol{H}^+|$ *for each class* $\Gamma^G(f)$ *in* $\Gamma(f)/G$.

We remark that the class number of conjugacy classes in $GL(n, \boldsymbol{Z})$ with a given irreducible characteristic polynomial is described by the ideal class number of a certain algebraic number field (cf. C. G. Latimer and C. C. MacDuffee [5], O. Taussky [8]). Our proof of the above two theorems are based on the correspondence, which is due to Taussky [8], between conjugacy classes in $GL(2n, \boldsymbol{Z})$ and ideal classes.

Concerning to the conjugacy classes $GL(n, F)$ and $Sp(2n, F)$ over a finite field F, there are many results (cf. J. A. Green [3], T. A. Springer [7], G. E. Wall [11] and A. Borel et al. [1]).

The contents of this paper are as follows. After the preparations, we define in §2 the dual ideal of a given fractional ideal in a cyclotomic field, and calculate it following Dedekind [2]. In §3 we introduce the notation of the admissible systems and study its relation to the regular elliptic elements in $Sp(2n, \boldsymbol{Z})$ and give a proof of Theorem I. Lemma 3.2 in this section is the fundamental lemma, and plays an essential role to prove Theorem I and Theorem II. In the last section we shall have Theorem II by using the correspondence between $\Gamma(f)/\Gamma$ and a certain subgroup of $A\times k_0^\times/Nk^\times$ where $k^\times=k-\{0\}$, $k_0^\times=k_0\cap k^\times$.

REMARK. After completing this work, the author was informed that there are several papers concerning the elliptic conjugacy classes in $Sp(4, \boldsymbol{Z})$; especially I. Münchhausen has given a complete list of conjugacy classes in $Sp(4, \boldsymbol{Z})$.

§1. Preliminaries.

For a subring $\boldsymbol{R}$ of the field $\boldsymbol{C}$ of complex numbers, we denote by $M(n, \boldsymbol{R})$ and $GL(n, \boldsymbol{R})$ the ring of all $n\times n$ matrices with entries in $\boldsymbol{R}$ and the multiplicative group of all $n\times n$ invertible matrices with entries in $\boldsymbol{R}$, respectively. The symplectic group $G_c=Sp(2n, \boldsymbol{C})$ is defined by

$$G_c=\{g\in GL(2n, \boldsymbol{C});\ {}^tgJg=J\} \tag{1.1}$$

where $J=\begin{pmatrix} 0 & 1_n \\ -1_n & 0 \end{pmatrix}$ and 1_n is the identity matrix with degree n. Let $\langle\ ,\ \rangle$ be the skew-symmetric bilinear form on $\boldsymbol{C}^{2n}\times\boldsymbol{C}^{2n}$ defined by

$$\langle x, y\rangle={}^txJy\ .$$

Then we have that

(1.2) an element g in $GL(2n, \boldsymbol{C})$ belongs to $Sp(2n, \boldsymbol{C})$ if and only if $\langle gx, gy\rangle = \langle x, y\rangle$ for all x, y in $\boldsymbol{C}^{2n}$.

Let θ be an involutive automorphism of G_c defined by

$$\theta(x) = JxJ^{-1} . \tag{1.3}$$

We shall denote the group of all real points in G_c by G, the group of all integral matrices in G by Γ, and put $K = \{x \in G; \theta(x) = x\}$. Γ is the Siegel modular group, and K is a maximal compact subgroup of the simple Lie group G. Let $\mathfrak{S}$ be the set of all positive definite matrices in G. Then $\mathfrak{S}$ can be identified with the Siegel upper plane. We define an action of G on $\mathfrak{S}$ by the rule;

$$G \times \mathfrak{S} \ni (g, p) \longrightarrow {}^t gpg \in \mathfrak{S} .$$

DEFINITION 1. An element g in G is called elliptic if g stabilizes a point in $\mathfrak{S}$.

We see that an element g in G is elliptic if and only if there exists h in G such that hgh^{-1} belongs to K (i.e. g is conjugate to an element in K).

Let $\mathfrak{g}$ be the Lie algebra of G. $\mathrm{Ad}\,(g)$ $(g \in G)$ denotes the linear transformation on G defined by $\mathrm{Ad}\,(g)X = gXg^{-1}$, $X \in \mathfrak{g}$. We now put $r(G) = \mathrm{Min}_{g \in G} \dim \mathrm{Ker}\,(\mathrm{Ad}\,(g) - 1)$, which is called the rank of G, and we have $r(G) = n$ for the group $G = Sp(2n, \boldsymbol{R})$.

DEFINITION 2. Let g be an element in G. Then g is called regular if $\dim \mathrm{Ker}\,(\mathrm{Ad}\,(g) - 1) = r(G)$.

It is known that an element g in G is regular if and only if the centralizer of g in G forms a Cartan subgroup.

LEMMA 1.1. *Let $\Gamma = Sp(2n, \boldsymbol{Z})$ be the Siegel modular group and γ an element in Γ with the characteristic polynomial f. Then γ is elliptic if and only if γ is semisimple (i.e. γ is diagonalizable over $\boldsymbol{C}$) and all irreducible factors of f over $\boldsymbol{Q}$ are cyclotomic.*

PROOF. Suppose γ is elliptic. Since γ lies in a compact discrete subgroup of G, the order of γ is finite and γ is semisimple. Hence all irreducible factors of f are cyclotomic. Conversely assume that γ is semisimple and all irreducible factors of f are cyclotomic. Then the subgroup H of G generated by γ is of finite order. Hence a conjugate subgroup of H is contained in K.

LEMMA 1.2. *Let γ be an elliptic element in Γ. Then γ is regular if and only if the characteristic polynomial f of γ is decomposed into the mutually distinct cyclotomic polynomials and the degrees of these factors are larger than or equal to two.*

PROOF. Let γ be an elliptic element in Γ. By Lemma 1.1 all irreducible factors of f are cyclotomic and γ is semisimple. Consequently the absolute value of each root of f is equal to one, and $\mathrm{Ad}(\gamma)$ is semisimple. Hence there exists g in $GL(n, \boldsymbol{C})$ and $\zeta_1, \zeta_2, \cdots, \zeta_n$ in $\boldsymbol{C}$ such that

$$g\gamma g^{-1}=\begin{pmatrix} \zeta_1 & & & & & 0 \\ & \ddots & & & & \\ & & \zeta_n & & & \\ & & & \bar{\zeta}_1 & & \\ & & & & \ddots & \\ 0 & & & & & \bar{\zeta}_n \end{pmatrix}, \quad |\zeta_i|=1 \ (1\leqq i\leqq n) . \tag{1.4}$$

Let us now prove the lemma. Suppose that f is the minimal polynomial of γ and the degree of any irreducible factor of f is larger than or equal to two. Then we have $\zeta_i\bar{\zeta}_j\neq 1$ for $i\neq j$ and $\zeta_i\zeta_j\neq 1$ for $1\leqq i, j\leqq n$. From this fact it follows that $\dim \mathrm{Ker}(\mathrm{Ad}(\gamma)-1)=r(G)$. Hence γ is regular. Finally we assume that γ is regular. In view of the above arguments we have immediately $\zeta_i\bar{\zeta}_j\neq 1$ $(1\leqq i<j\leqq n)$, $\zeta_i\zeta_j\neq 1$ $(1\leqq i, j\leqq n)$, where ζ_i's are the same as in (1.4). Therefore each two irreducible factors of f are distinct and the degree of any irreducible factor is larger than or equal to two. This completes our proof.

§2. Dual ideal of a fractional ideal.

Let f be a fixed cyclotomic polynomial with degree n over $\boldsymbol{Q}$. Let ζ be a root of f and put $k=\boldsymbol{Q}(\zeta)$, and let $G(k/\boldsymbol{Q})$ be the Galois group of k over $\boldsymbol{Q}$, $(x, y)={}^t y\bar{x}$ is the canonical positive definite hermitian form on $\boldsymbol{C}^n\times\boldsymbol{C}^n$. Let $\mathfrak{a}$ be a fractional ideal in k with $\boldsymbol{Z}$-basis $\{\omega_1, \omega_2, \cdots, \omega_n\}$. We put $x={}^t(\omega_1, \omega_2, \cdots, \omega_n)$ and $\Delta(\mathfrak{a})=\det(x, x', \cdots, x^{(n-1)})$, where $x, x', \cdots, x^{(n-1)}$ are all algebraic conjugate vectors of x over $\boldsymbol{Q}$. Let $\mathfrak{o}$ be the ring of all algebraic integers in k. Since k is a cyclotomic field over $\boldsymbol{Q}$, $\mathfrak{o}$ is generated by $1, \zeta, \zeta^2, \cdots, \zeta^{n-1}$ over $\boldsymbol{Z}$ (cf., for instance, H. Hasse [4] or T. Takagi [8]). Therefore we have $|\Delta(\mathfrak{o})|^2=\pm N_k f'(\zeta)$, where N_k is the norm of k over $\boldsymbol{Q}$ and f' is the derivative of f.

Let $\mathfrak{a}$ be a fractional ideal of k and $x={}^t(\omega_1, \omega_2, \cdots, \omega_n)$ be the same as above. Since $\Delta(\mathfrak{a})\neq 0$ there exists a unique x^* in k^n such that

$$(2.1)\qquad (\sigma(x), x^*) = \begin{cases} 1 & \text{if } \sigma=1 \\ 0 & \text{otherwise} \end{cases} \quad \text{for all } \sigma \text{ in } G(k/\boldsymbol{Q}) .$$

We put $x^* = {}^t(\omega_1^*, \omega_2^*, \cdots, \omega_n^*)$. Then (2.1) is equivalent to

$$(2.2)\qquad \text{Trace}\,(\omega_i\bar{\omega}_j^*) = \delta_{ij} \quad \text{where } \delta_{ij} \text{ is the Kronecker's delta} .$$

Let us now define the dual ideal $\mathfrak{a}^*$ of $\mathfrak{a}$ by

$$(2.3)\qquad \mathfrak{a}^* = \{\mu \in k;\ \text{Trace}\,(\alpha\bar{\mu}) \in \boldsymbol{Z} \quad \text{for all } \alpha \text{ in } \mathfrak{a}\} .$$

By (2.2) and (2.3) we have immediately that $\mathfrak{a}^*$ is a fractional ideal in k. The following lemma is well known (see R. Dedekind [2] or H. Hasse [4]).

LEMMA 2.1. *Let f be a cyclotomic polynomial over $\boldsymbol{Q}$ with degree n and k be the splitting field of f over $\boldsymbol{Q}$. Then for a given ideal $\mathfrak{a}$ in $\mathfrak{o}$, the dual ideal $\mathfrak{a}^*$ of $\mathfrak{a}$ is of the form; $\mathfrak{a}^* = 1/(\bar{f}'(\zeta)\bar{\mathfrak{a}})$ where $\bar{\mathfrak{a}}$ is the complex conjugate of $\mathfrak{a}$.*

PROOF. Let $\{\omega_1, \omega_2, \cdots, \omega_n\}$ be a $\boldsymbol{Z}$-basis of $\mathfrak{a}$, and $x = {}^t(\omega_1, \omega_2, \cdots, \omega_n)$, $x^* = {}^t(\omega_1^*, \omega_2^*, \cdots, \omega_n^*)$. Since Trace $(\omega_1\bar{\omega}_1^*) = 1 \in \mathfrak{a}^*$, $\mathfrak{d} = 1/\mathfrak{a}^*$ is an ideal in $\mathfrak{o}$. We put, for each fixed μ in $\mathfrak{a}^*$ and for a number i $(1 \leqq i \leqq n)$

$$g_i(t) = \text{Trace}\,(\bar{\mu}\omega_i f(t)/(t-\zeta)) .$$

Then we have

$$g_i(t) = \text{Trace}\,(\bar{\mu}\omega_i a_0)t^{n-1} + \text{Trace}\,(\bar{\mu}w_i a_1)t^{n-2} + \cdots + \text{Trace}\,(\bar{\mu}\omega_i a_{n-1}) ,$$

where $a_0, a_1, \cdots, a_{n-1}$ are the algebraic integers in k determined by

$$f(t)/(t-\zeta) = a_0 t^{n-1} + a_1 t^{n-2} + \cdots + a_{n-1} .$$

Therefore all coefficients of $g_i(t)$ are rational integers. Furthermore, since

$$g_i(t) = \bar{\mu}\omega_i f(t)/(t-\zeta) + \bar{\mu}'\omega_i' f(t)/(t-\zeta') + \cdots + \bar{\mu}^{(n-1)}\omega_i^{(n-1)} f(t)/(t-\zeta^{(n-1)}) ,$$

we obtain $g_i(\zeta) = \bar{\mu}\omega_i f'(\zeta)$ for μ in $\mathfrak{a}^*$ and $i = 1, 2, \cdots, n$. It follows from these facts that $\mathfrak{z} = f'(\zeta)\bar{\mathfrak{a}}^*\mathfrak{a}$ is an ideal in $\mathfrak{o}$. Bearing in mind

$$(2.4)\qquad \bar{\mathfrak{d}}\mathfrak{z} = f'(\zeta)\mathfrak{a} ,$$

it is enough to verify that $\mathfrak{z} = \mathfrak{o}$. Put $A = (x, x', \cdots, x^{(n-1)}) \in M(n, k)$. Then we have $\det A^{-1} = \pm N_k\mathfrak{a}^* \varDelta(\mathfrak{o})$ because $A^{-1} = ({}^t\bar{x}^*, {}^t(\bar{x}^*)', \cdots, {}^t(\bar{x}^*)^{(n-1)})$ (see (2.2)). Hence $N_k\mathfrak{d} = \pm\varDelta(\mathfrak{o}) \det A = N_k\mathfrak{a}\,|\varDelta(\mathfrak{o})|^2 = \pm N_k(f'(\zeta)\mathfrak{a})$. On the other hand by (2.4) we have $N_k(f'(\zeta)\mathfrak{a}) = N_k\mathfrak{d}N_k\mathfrak{z}$. Consequently $N_k\mathfrak{z} = 1$ and $\mathfrak{z} = \mathfrak{o}$ as required.

LEMMA 2.2. *Let f be the m-th cyclotomic polynomial with degree $n=\phi(m)$ and k be the splitting field of f over $\boldsymbol{Q}$. Then there exists a unit ε^* in k such that*

(2.5) $\bar{f}'(\zeta)(\lambda\varepsilon^*)^{-1}$ *are real for all purely imaginary numbers λ in k,*

where ζ is a fixed root of f.

PROOF. We first assume that m is of the form; $m=l^h$, where l is a prime number. Since $t^{l^h}-1=f(t)(t^{l^{h-1}}-1)$, we have $f'(\zeta)=l^h(\zeta^{l^{h-1}}-1)^{-1}(\zeta^{l^h-1})$.

For the case $l=2$, we have $\zeta^{l^{h-1}}=-1$, and hence

$$f'(\zeta)=-2^{h-1}\zeta^{-1}\,. \tag{2.6}$$

In this case $\varepsilon^*=1$ for $m\leqq 2$ and $\varepsilon^*=\bar{\zeta}^{-1}\sqrt{-1}$ for $m>2$.

If $l\neq 2$, then there exists a primitive l-th root of unity ξ such that $\zeta^{l^{h-1}}=\xi^2$. Consequently for the case $m=l^h$, $l\neq 2$ we have

$$f'(\zeta)=l^h\zeta^{l^h-1}\xi^{-1}(\xi-\xi^{-1})^{-1}\,. \tag{2.7}$$

In this case $\bar{\varepsilon}^*=\zeta^{l^h-1}\xi^{-1}$. In view of (2.6) and (2.7) we can choose a unit ε^* in k satisfying (2.5) in Lemma 2.2 for the case $m=l^h$ with l prime.

Finally suppose that m is, at least, divided by two distinct prime numbers. Then $\zeta-\sigma(\zeta)(\sigma\in G(k/\boldsymbol{Q}), \sigma\neq 1)$ is a unit in k. We put $\bar{\varepsilon}^*=f'(\zeta)(\zeta-\bar{\zeta})^{-1}$. Then ε^* satisfies (2.5). This completes the proof of the lemma.

LEMMA 2.3. *Let f and k be the same as in the above lemma. We denote the maximal real subfield of k by k_0, the unit group of k (resp. k_0) by $\boldsymbol{E}$ (resp. $\boldsymbol{E}_0$) and the relative norm of k to k_0 by N. Then we have $N\boldsymbol{E}=Nk\cap\boldsymbol{E}_0$.*

PROOF. It is enough to show that $Nk\cap\boldsymbol{E}_0\subset N\boldsymbol{E}$. Let ξ be an element in k satisfying $N\xi=\varepsilon\in\boldsymbol{E}_0$. Since every conjugate of $\xi\bar{\xi}^{-1}$ has absolute value 1, there is a root of the unity η in k such that $\xi=\pm\bar{\xi}\eta$. Consequently $\xi^2=\pm\eta N\xi=\pm\varepsilon\eta$. Therefore ξ is a root of t^2-a where a is an algebraic integer in k. This implies that ξ is an algebraic integer in k. Since $N\xi=\varepsilon$ and since ε is a unit in k_0, we conclude that ξ belongs to $\boldsymbol{E}$. Hence the lemma follows.

§3. Admissible systems associated with regular elliptic elements in the Siegel modular group.

Let G and Γ be respectively the real symplectic group with degree $2n$ and the Siegel modular group in G. Let f be a fixed cyclotomic polynomial with degree $2n$. We denote by $\Gamma(f)$ the set of all elements in Γ with f as the characteristic polynomial. Since f is irreducible over $\boldsymbol{Q}$, all elements in $\Gamma(f)$ are regular elliptic (see Lemma 1.2). Throughout this section we shall fix f and a root ζ of f. Let $k=\boldsymbol{Q}(\zeta)$ (resp. $k_0=\boldsymbol{Q}(\zeta+\zeta^{-1})$) be the field generated by ζ (resp. $\zeta+\zeta^{-1}$). For a fractional ideal $\mathfrak{a}$ in k, a vector x in k^{2n} is said to generate $\mathfrak{a}$ if $\mathfrak{a}$ is generated by all entries in x over $\boldsymbol{Z}$. If x in k^{2n} generates a fractional ideal $\mathfrak{a}$, we say that x belongs to $\mathfrak{a}$ and write $\mathfrak{a}=\mathfrak{a}(x)$.

DEFINITION 3.1. A triple (x, y, λ) in $k^{2n}\times k^{2n}\times k$ is called an admissible system if it satisfies the following conditions (1), (2) and (3):

(1) There exists a nontrivial fractional ideal $\mathfrak{a}$ in k such that $\mathfrak{a}=\mathfrak{a}(x)$,

(2) $y=x^*$ where x^* is the same as in (2.1),

(3) $Jx=\lambda x^*$.

Let $\mathfrak{a}$ be a fractional ideal in k. An admissible system (x, x^*, λ) is said to belong to $\mathfrak{a}$ (or $\mathfrak{a}$ has an admissible system (x, x^*, λ)) if $\mathfrak{a}=\mathfrak{a}(x)$.

REMARK 3.1. If (x, x^*, λ) is admissible, then λ is purely imaginary. Actually since $(x, Jx)=\bar{\lambda}$ and ${}^tJ=-J$, we have $\bar{\lambda}=({}^tJx, x)=-\overline{(x, Jx)}=-\lambda$.

LEMMA 3.1. *Let γ be an element in $\Gamma(f)$ and x an eigenvector of γ corresponding to the eigenvalue ζ. We define x^* by* (2.1). *Then there exists λ in k such that (x, x^*, λ) is admissible.*

PROOF. By the definition of x^*, we have immediately ${}^t\gamma^{-1}x^*=\zeta x^*$. On the other hand, since ${}^t\gamma^{-1}=J\gamma J^{-1}$, we obtain ${}^t\gamma^{-1}Jx=\zeta Jx$. Hence it follows from the irreducibility of f that $Jx=\lambda x^*$ for a suitable element λ in k. It remains to prove that x generates an ideal in k. Let $\mathfrak{a}$ be the $\boldsymbol{Z}$-module generated by all entries in $x={}^t(\omega_1, \omega_2, \cdots, \omega_{2n})$. For any integer i, we have $\gamma^i x=\zeta^i x$· Therefore $\zeta^i\omega_j$ belongs to $\mathfrak{a}$ for $i, j=1, 2, \cdots, 2n$. Bearing in mind $\{1, \zeta, \zeta^2, \cdots, \zeta^{2n-1}\}$ forms a $\boldsymbol{Z}$-base of $\mathfrak{o}$, $\mathfrak{a}$ is a fractional ideal in k as required.

REMARK 3.2. Let γ be an element in $GL(2n, \boldsymbol{Z})$ with the characteristic polynomial f. We choose an eigenvector x of γ corresponding to the eigenvalue ζ, and let $\mathfrak{a}=\mathfrak{a}_\gamma$ be the ideal generated by x. We see that the ideal class $C(\mathfrak{a}_\gamma)$ in the ideal class group $\boldsymbol{A}$ of k is uniquely determined by γ. Consequently we can define a mapping ψ of $GL(f)$ to $\boldsymbol{A}$ by $\gamma\rightarrow C(\mathfrak{a}_\gamma)$ where $GL(f)=\{\gamma\in GL(2n, \boldsymbol{Z})$; the characteristic polynomial of $\gamma=f\}$. This mapping is due to O. Taussky, and furthermore ψ induces a bijection of $GL(f)/GL(2n, Z)$ to $\boldsymbol{A}$ (cf. O. Taussky [8] or M. Newman p. 52, [6]). Let us now state our fundamental lemma of this paper.

LEMMA 3.2. *Let f, k, k_0 be the same as in the above lemma. Then a nontrivial fractional ideal $\mathfrak{a}$ in k has an admissible system if and only if there exists a purely imaginary number λ in k such that $\lambda\mathfrak{a}^*=\mathfrak{a}$, where $\mathfrak{a}^*$ is the dual ideal of $\mathfrak{a}$ defined by* (2.3).

PROOF. Suppose $\mathfrak{a}$ has an admissible system (x, x^*, λ). Then $\mathfrak{a}$ is generated by x and $\mathfrak{a}^*$ is generated by x^*. Since $Jx=\lambda x^*$ and $J\in GL(2n, \boldsymbol{Z})$, we have $\mathfrak{a}=\lambda\mathfrak{a}^*$, and λ is purely imaginary (see Remark 3.1.). Conversely assume that $\mathfrak{a}=\lambda\mathfrak{a}^*$ for a purely imaginary number λ in k. We choose a $\boldsymbol{Z}$-basis $\omega_1, \omega_2, \cdots, \omega_{2n}$ of $\mathfrak{a}$, and put $x={}^t(\omega_1, \omega_2, \cdots, \omega_{2n})$. By the assumption of $\mathfrak{a}$, there is a matrix U in $GL(2n, \boldsymbol{Z})$ such that $Ux=\lambda x^*$. Since ${}^tU^{-1}x^*=(\bar{\lambda})^{-1}x$ and λ is purely imaginary, we have ${}^tU^{-1}Ux=\lambda(\bar{\lambda})^{-1}x=-x$. Therefore U is a skew-symmetric element of $GL(2n, \boldsymbol{Z})$. Consequently there exists h in $GL(2n, Z)$ such that $U={}^thJh$ (see, for instance, M. Newman [5], p. 57). We put $y=hx$. Then $\mathfrak{a}$ is generated by y and $Jy=\lambda{}^th^{-1}x^*=\lambda y^*$. Hence (y, y^*, λ) is an admissible system of $\mathfrak{a}$. This completes our proof.

We will continue to study of the admissible systems.

LEMMA 3.3. *If two admissible systems (x, x^*, λ) and (y, y^*, μ) belong to the same fractional ideal in k, then $\lambda\mu^{-1}$ is a unit in k_0. Conversely for each unit ε in k_0 and an admissible system (x, x^*, λ), there exists an admissible system (y, y^*, μ) such that $\mu=\lambda\varepsilon^{-1}$ and $\mathfrak{a}(x)=\mathfrak{a}(y)$.*

PROOF. If two admissible systems (x, x^*, λ) and (y, y^*, μ) belong to the same ideal $\mathfrak{a}(x)=\mathfrak{a}(y)$, then we have $\lambda\mathfrak{a}^*(x)=\mu\mathfrak{a}^*(y)$. Hence $\lambda\mu^{-1}$ is a unit in k. Furthermore, since λ and μ are purely imaginary, $\lambda\mu^{-1}$ is a unit in k_0.

Let us prove the second assertion of this lemma. Let (x, x^*, λ) and ε be, respectively, an admissible system and a unit in k_0. Define a linear transformation U on k^{2n} by $U\sigma(x)=\sigma(\varepsilon^{-1})J\sigma(x)$, $\sigma\in G(k/\boldsymbol{Q})$. Then we have $U\in GL(2n, \boldsymbol{Z})$, because $J\in GL(2n, \boldsymbol{Z})$ and ε is a unit in k_0. Moreover a direct calculation shows that $(\sigma(x), Ux)=(\sigma(x), -{}^tUx)$ for all σ in $G(k/\boldsymbol{Q})$. This implies that there is an element h in $GL(2n, \boldsymbol{Z})$ such that $U={}^thJh$. Put $y=hx$ and $\mu=\lambda\varepsilon^{-1}$, then (y, y^*, μ) is an admissible system belonging to $\mathfrak{a}(x)$.

DEFINITION 3.2. Let (x, x^*, λ) and (y, y^*, μ) be two admissible systems. These systems are called G-(resp. Γ-)equivalent if there are g in G (resp. Γ) and ξ_σ in $\boldsymbol{C}$ (resp. ξ in k) such that $g\sigma(x)=\xi_\sigma\sigma(y)$ (resp. $g\sigma(x)=\sigma(\xi y)$) for all σ in $G(k/\boldsymbol{Q})$.

LEMMA 3.4. *Let N be the relative norm of k to k_0. Then two admissible systems (x, x^*, λ) and (y, y^*, μ) are Γ-equivalent if and only if $\lambda\mu^{-1} \in Nk^\times (k^\times = k - \{0\})$ and $\mathfrak{a}(x)\mathfrak{a}(y)^{-1}$ is a principal ideal in k.*

PROOF. First we assume that (x, x^*, λ) and (y, y^*, μ) are Γ-equivalent. Then $gx = \xi y$ for some g in Γ and ξ in k. Consequently, since $(\xi y, J\xi y) = \bar{\mu} N\xi$ and $(gx, Jgx) = \langle gx, g\bar{x}\rangle = \langle x, \bar{x}\rangle = \bar{\lambda}$, we see that $\lambda\mu^{-1}$ belongs to $Nk^\times$.

Conversely, assume that $\lambda\mu^{-1}$ belongs to $Nk^\times$ and that $\mathfrak{a}(x)^{-1}\mathfrak{a}(y) = (\xi)$ for ξ in k. Then we can choose U in $GL(2n, \boldsymbol{Z})$ satisfying $y = U\xi x$. Hence we have $(\sigma(y), Jy) = \lambda^{-1}\mu(\sigma(x), Jx)$ and $(\sigma(y), Jy) = (\sigma(x), {}^tUJUx)N\xi$ for all σ in $G(k/\boldsymbol{Q})$. Combining these equations we have

$$Jx = \lambda\mu^{-1} N\xi\, {}^tUJUx\ . \tag{3.1}$$

On the other hand, by the assumption of $\lambda\mu^{-1}$, there exists η in k such that $N\eta = \lambda\mu^{-1}N\xi$. In view of (3.1), $N\eta$ is an eigenvalue of a unimodular integral matrix $J^{-1}\,{}^tUJU$. Therefore $N\eta$ is a unit in k_0 We now apply Lemma 2.3 to η. Then η is a unit in k. Let V be a unique element in $GL(2n, \boldsymbol{Z})$ satisfying $Vx = \eta x$. By using (3.1), we have ${}^tV^{-1}Jx = \lambda\,{}^tV^{-1}x^* = \lambda(Vx)^* = \lambda\bar{\eta}^{-1}x^* = \bar{\eta}^{-1}Jx = {}^tUJUVx$. Put $g = UV$. Then we have that g belongs to Γ, $y = U\xi x = \xi\eta^{-1}gx$ and $\xi\eta^{-1} \in k$. Hence (x, x^*, λ) and (y, y^*, μ) are Γ-equivalent.

LEMMA 3.5. *Two admissible systems (x, x^*, λ) and (y, y^*, μ) are G-equivalent if and only if $\lambda\mu^{-1}$ is totally positive in k_0.*

PROOF. Since the "only if part" of the lemma is obvious, it is enough to show the "if part". By the assumption of $\lambda\mu^{-1}$, we have that $\sigma(\lambda\mu^{-1})$ is positive for any σ in $G(k/\boldsymbol{Q})$. We put $F(t) = \prod_{\sigma \in G(k/\boldsymbol{Q})} (t^2 - \sigma(\xi))$, $\xi = \lambda\mu^{-1}$. Let $\tilde{k}$ be the splitting field of $Ff = 0$ over $\boldsymbol{Q}$. Then for each σ in $G(k/\boldsymbol{Q})$ there is $\tilde{\sigma}$ in $G(\tilde{k}/\boldsymbol{Q})$ such that σ is the restriction of $\tilde{\sigma}$ to k satisfying $\rho\tilde{\sigma} = \tilde{\sigma}\rho$ where ρ is the conjugation of $\boldsymbol{C}$. We fix these $\tilde{\sigma}$ and define a linear transformation g on $\boldsymbol{C}^{2n}$ by putting $g\tilde{\sigma}(x) = \tilde{\sigma}(\sqrt{\xi})\tilde{\sigma}(y)$. Since $\tilde{\sigma}(\sqrt{\xi})$ is a root of $t^2 - \sigma(\xi)$ and $\sigma(\xi) > 0$, we have that $\sigma(\sqrt{\xi})$ is real. Hence $g\tilde{\sigma}(x) = \bar{g}\tilde{\sigma}(x)$ for all σ. Furthermore we have $(g\sigma(x), Jgx) = (\sigma(x), Jx)$ for all σ in $G(k/\boldsymbol{Q})$. Thus we get $g \in G$, $g\sigma(x) = \xi_\sigma\sigma(y)$ and $\xi_\sigma \in \boldsymbol{C}$ for all σ in $G(k/\boldsymbol{Q})$. This completes our proof.

LEMMA 3.6. *A nontrivial fractional ideal $\mathfrak{a}$ has an admissible system if and only if $N\mathfrak{a}$ is a principal ideal in k_0, where $N\mathfrak{a}$ is the relative norm of $\mathfrak{a}$ to k_0.*

PROOF. In view of Lemma 3.2 we see that a fractional ideal $\mathfrak{a}$ has an admissible system if and only if $\mathfrak{a}=\lambda\mathfrak{a}^*$ for a purely imaginary number λ in k. Consequently, be using Lemma 2.1 an Lemma 2.2 we conclude the lemma.

THEOREM 1. *Let $\Gamma=Sp(2n, \boldsymbol{Z})$ be the Siegel modular group of degree $2n$ and f an arbitrary cyclotomic polynomial with degree $2n$. Then Γ has a regular elliptic element with the characteristic polynomial f.*

PROOF. Let $\mathfrak{a}$ be a nontrivial principal ideal in k. Then $N\mathfrak{a}$ is principal in k_0. Applying Lemma 3.6 to $\mathfrak{a}$, there exists an admissible system (x, x^*, λ) such that x generates $\mathfrak{a}$. We define γ in $GL(2n, \boldsymbol{Z})$ by putting $\gamma\sigma(x)=\sigma(\zeta)\sigma(x)$ for all σ in $G(k/\boldsymbol{Q})$. Since $Jx=\lambda x^*$, we have immediately ${}^t\gamma J\gamma=J$. Hence γ is a regular elliptic element in Γ with the characteristic polynomial f. This completes our proof.

§4. Class number of a regular elliptic conjagacy class in the Siegel modular group.

Let $\Gamma=Sp(2n, \boldsymbol{Z})$ be the Siegel modular group with degree $2n$. We fix a cyclotomic polynomial with degree $2n$ and a root ζ of f. Let k (resp. k_0) be the field generated by $\boldsymbol{Q}$ and ζ (resp. $\zeta+\zeta^{-1}$). We shall denote by $k^\times$ (resp. $k_0^\times$) the multiplicative group of k (resp. k_0), and let

A; the group of all nontrivial fractional ideals in k,

$\boldsymbol{A}$; the absolute ideal class group of k,

$C(\mathfrak{a})$; the ideal class in $\boldsymbol{A}$ containing a given ideal $\mathfrak{a}$ in A,

$N\mathfrak{a}$; the relative norm of $\mathfrak{a}$ to k_0,

H; the group of all $\mathfrak{a}$ in A satisfying $N\mathfrak{a}=(\omega)$ for a certain element ω in k_0,

$\boldsymbol{H}$; the group of all $C(\mathfrak{a})$, $\mathfrak{a}\in H$,

$\boldsymbol{H}^+$; the subgroup of $\boldsymbol{H}$ defined by $\boldsymbol{H}^+=\{C(\mathfrak{a}); N\mathfrak{a}=(\omega)$ for a totally positive number ω 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 positive units in k_0,

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

Let $\Gamma(f)$ be the set of all elements in Γ with the characteristic polynomial f. We define an action of Γ on $\Gamma(f)$ by the rule

$$\Gamma\times\Gamma(f)\ni(\gamma, x)\longrightarrow\gamma x\gamma^{-1}\in\Gamma(f)\ . \tag{4.1}$$

$\Gamma(f)$ is decomposed into the orbits of Γ. We denote the set of these orbits by $\Gamma(f)/\Gamma$, and we call an orbit in it a "Γ-conjugacy class". We also consider G-conjugacy classes ($G=Sp(2n, \boldsymbol{R})$) of $\Gamma(f)$ defined below.

DEFINITION 4.1. Two elements γ and γ' in $\Gamma(f)$ are called G-conjugate if there exists g in G such that $g\gamma g^{-1}=\gamma'$.

The set of all G-conjugacy classes in $\Gamma(f)$ is denoted by $\Gamma(f)/G$. From the definitions of $\Gamma(f)/\Gamma$ and $\Gamma(f)/G$, we see that $\Gamma(f)/\Gamma$ is decomposed into a number of classes in $\Gamma(f)/G$ (i.e. for any class $\Gamma^{a}(f)$ in $\Gamma(f)/G$, $\Gamma^{a}(f)/\Gamma\subset\Gamma(f)/\Gamma$).

The main purpose of this section is to give the formulae for $|\Gamma(f)/G|$ and $|\Gamma^{a}(f)/\Gamma|$. Let $\tilde{H}$ be the subgroup of $H\times k_0^\times$ defined by

$$(4.2)\qquad \tilde{H}=\{(\mathfrak{a},\omega);\ N\mathfrak{a}=(\omega),\ (\mathfrak{a},\omega)\in H\times k_0^\times\}\ .$$

We define a mapping π of $\tilde{H}$ to $A\times k_0^\times/Nk^\times$ by

$$(4.3)\qquad \pi(\mathfrak{a},\omega)=(C(\mathfrak{a}),\ \omega Nk^\times)\quad\text{for } (\mathfrak{a},\omega) \text{ in } \tilde{H}\ .$$

Then $\pi(\tilde{H})$ is a subgroup of $A\times k_0^\times/Nk^\times$. First of all we shall consider a mapping of $\pi(\tilde{H})$ to $\Gamma(f)/\Gamma$. Let $(\mathfrak{a},\omega)$ be an element in $\tilde{H}$. By using Lemma 3.6, there exists an admissible system (x, x^*, λ) such that $\mathfrak{a}=\mathfrak{a}(x)$ (i.e. $\mathfrak{a}$ is generated by x), $Jx=\lambda x^*$ and $\mathfrak{a}=\lambda\mathfrak{a}^*$. On the other hand, by using Lemma 2.1 and Lemma 2.2, we have $N\mathfrak{a}=(\bar{f}'(\bar{\zeta})^{-1}\lambda\varepsilon^*)$, $\bar{f}'(\bar{\zeta})^{-1}\lambda\varepsilon^*\in k_0$, where ε^* is the same as in Lemma 2.2. Consequently there exists a unit ε in k_0 such that $\bar{f}'(\bar{\zeta})^{-1}\lambda\varepsilon^*=\varepsilon\omega$. We put

$$(4.4)\qquad \lambda_\omega=\varepsilon^{-1}\lambda\ .$$

Then Lemma 3.3 implies directly the following Lemma 4.1.

LEMMA 4.1. *For each* $(\mathfrak{a},\omega)$ *in* $\tilde{H}$, *there exists an admissible system* (x, x^*, λ_ω) *such that* $\bar{f}'(\bar{\zeta})^{-1}\lambda_\omega\varepsilon^*=\omega$, *where* ε^* *is the same as Lemma* 2.2.

Let $(\mathfrak{a},\omega)$ be an element in $\tilde{H}$. We choose admissible system (x, x^*, λ_ω) as in the above lemma. Let γ be an element in Γ satisfying $\gamma x=\zeta x$. We define a mapping Ψ of $\pi(\tilde{H})$ to $\Gamma(f)/\Gamma$ by

(4.5) $\Psi(\pi(\mathfrak{a},\omega))=C(\gamma)$, where $C(\gamma)$ is the class in $\Gamma(f)/\Gamma$ containing γ.

LEMMA 4.2. *Let* Ψ *be the mapping defined by* (4.5). *Then* Ψ *is well-defined and is a bijective mapping of* $\pi(\tilde{H})$ *to* $\Gamma(f)/\Gamma$.

PROOF. We first verify the well-definedness of Ψ. Let $\pi(\mathfrak{a},\omega)=\pi(\mathfrak{a}',\omega')$, and γ, γ' be two elements in Γ defined by two admissible systems (x, x^*, λ_ω) and $(y, y^*, \lambda_{\omega'})$. Since $\lambda_{\omega'}\lambda_\omega^{-1}=\omega\omega'^{-1}\in Nk$ and $\mathfrak{a}\mathfrak{a}'^{-1}=\mathfrak{a}(x)\mathfrak{a}(y)^{-1}$ is principal, we see that (x, x^*, λ_ω) and $(y, y^*, \lambda_{\omega'})$ are Γ-equivalent (see Lemma 3.4). Consequently we have $gx=\xi y$ for some g in Γ and ξ in $k^\times$. Hence, by the definitions of γ and γ', we get $g\gamma x=\gamma' gx$.

This implies that $\Psi(\pi(\mathfrak{a}, \omega))=\Psi(\pi(\mathfrak{a}', \omega'))$.

Secondly we shall show that Ψ is injective. Suppose that $\Psi(\pi(\mathfrak{a}, \omega))=\Psi(\pi(\mathfrak{a}', \omega'))$ holds for two elements $(\mathfrak{a}, \omega)$ and $(\mathfrak{a}', \omega')$ in $\tilde{H}$. We choose two admissible systems (x, x^*, λ_ω) and $(y, y^*, \lambda_{\omega'})$ which define γ and γ', where $C(\gamma)=\Psi(\pi(\mathfrak{a}, \omega))$, $C(\gamma')=\Psi(\pi(\mathfrak{a}', \omega'))$. Then we have $g\gamma g^{-1}=\gamma'$ for a certain element g in Γ. Bearing in mind that the characteristic polynomial f of γ' is irreducible over $\boldsymbol{Q}$, there exists ξ in $k^\times$ such that $gx=\xi y$. Again, by using Lemma 3.4, we have that $\mathfrak{a}(x)\mathfrak{a}(y)^{-1}=\mathfrak{a}\mathfrak{a}'^{-1}$ is principal and $\omega\omega'^{-1}=\lambda_\omega\lambda_{\omega'}^{-1}$ belongs to $Nk^\times$. Thus we get $\pi(\mathfrak{a}, \omega)=\pi(\mathfrak{a}', \omega')$. It remains to prove that Ψ is surjective. Let γ be an element in $\Gamma(f)$. According to Lemma 3.1, there is an admissible system (x, x^*, λ) such that $\gamma x=\zeta x$. We put $\mathfrak{a}(x)=\mathfrak{a}$ and $\omega=f'(\zeta)^{-1}\lambda\varepsilon^*$. Then $\Psi(\pi(\mathfrak{a}, \omega))=C(\gamma)$. This completes our proof.

Let $\tilde{\boldsymbol{H}}$ and $\tilde{\boldsymbol{H}}^+$ be

$$(4.6)\qquad \tilde{\boldsymbol{H}}=\pi(\tilde{H}),\ \tilde{\boldsymbol{H}}^+=\{\pi(\mathfrak{a}, \omega)\in\tilde{\boldsymbol{H}};\ \omega \text{ is totally positive}\}\,.$$

LEMMA 4.3. *Let $\tilde{\boldsymbol{H}}$ and $\tilde{\boldsymbol{H}}^+$ be the same as above. Then two classes $\Psi(\pi(\mathfrak{a}, \omega))$ and $\Psi(\pi(\mathfrak{a}', \omega'))$ $(\pi(\mathfrak{a}, \omega), \pi(\mathfrak{a}', \omega')\in\tilde{\boldsymbol{H}})$ in $\Gamma(f)/\Gamma$ are G-equivalent if and only if $\pi(\mathfrak{a}, \omega)\pi(\mathfrak{a}', \omega')^{-1}$ belongs to $\tilde{\boldsymbol{H}}^+$. In particular, $\Psi(\tilde{\boldsymbol{H}}^+)$ forms a class in $\Gamma(f)/G$.*

PROOF. Let $\pi(\mathfrak{a}, \omega)$ and $\pi(\mathfrak{a}', \omega')$ be two elements in $\tilde{\boldsymbol{H}}$. We first assume that $\pi(\mathfrak{a}, \omega)\pi(\mathfrak{a}', \omega')^{-1}$ belongs to $\boldsymbol{H}^+$, and choose (x, x^*, λ_ω) and $(y, y^*, \lambda_{\omega'})$ as in Lemma 4.1. Therefore $\Psi(\pi(\mathfrak{a}, \omega))$ and $\Psi(\pi(\mathfrak{a}', \omega'))$ are defined by these two systems. From our assumption we see that $\omega\omega'^{-1}=\lambda_\omega\lambda_{\omega'}^{-1}$ is totally positive. Hence it follows from Lemma 3.5 that (x, x^*, λ_ω) and $(y, y^*, \lambda_{\omega'})$ are G-equivalent. Therefore $\Psi(\pi(\mathfrak{a}, \omega))$ and $\Psi(\pi(\mathfrak{a}', \omega'))$ are G-equivalent. Conversely suppose that $\Psi(\pi(\mathfrak{a}, \omega))$ and $\Psi(\pi(\mathfrak{a}', \omega'))$ are G-equivalent. Then two systems which define $\Psi(\pi(\mathfrak{a}, \omega))$ and $\Psi(\pi(\mathfrak{a}', \omega'))$ are G-equivalent. Consequently Lemma 3.5 implies the conclusion of this lemma.

THEOREM 2. *Let $\Gamma=Sp(2n, \boldsymbol{Z})$ be the Siegel modular group with degree $2n$ and f be the m-th cyclotomic polynomial over $\boldsymbol{Q}$ with $2n=\phi(m)$. Let $\Gamma(f)$, $\Gamma(f)/\Gamma$, $\Gamma(f)/G$, $\boldsymbol{H}$, $\boldsymbol{H}^+$, $\boldsymbol{E}$, $\boldsymbol{E}_0$ and $\boldsymbol{E}_0^+$ be the same as above. Then we have*

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

(2) $|\Gamma^G(f)/\Gamma|=(\boldsymbol{E}_0^+\colon N\boldsymbol{E})|\boldsymbol{H}^+|$ *for each class $\Gamma^G(f)$ in $\Gamma(f)/G$.*

PROOF. In view of Lemma 4.2 and Lemma 4.3, it is enough to show that the following (4.7) is valid;

$$(4.7) \qquad |\tilde{\boldsymbol{H}}^+|=(\boldsymbol{E}_0^+: N\boldsymbol{E})|\boldsymbol{H}^+| \text{ and } |\tilde{\boldsymbol{H}}|=(\boldsymbol{E}_0: N\boldsymbol{E})|\boldsymbol{H}| ,$$

where $\tilde{\boldsymbol{H}}$ and $\tilde{\boldsymbol{H}}^+$ are the same as (4.6). Therefore

$$\tilde{\boldsymbol{H}}=\{(C(\mathfrak{a}), \omega Nk^\times); \mathfrak{a}\in A, N\mathfrak{a}=(\omega)\} \text{ and}$$
$$\tilde{\boldsymbol{H}}^+=\{(C(\mathfrak{a}), \omega Nk^\times); \mathfrak{a}\in A, N\mathfrak{a}=(\omega), \omega \text{ is totally positive}\} .$$

For a fixed $C(\mathfrak{a})$ in $\boldsymbol{H}$, we put $\tilde{\boldsymbol{H}}_{C(\mathfrak{a})}=\{(C(\mathfrak{a}), \omega Nk^\times); N\mathfrak{a}=(\omega), \omega\in k_0\}$. Then we have (see Lemma 3.3)

$$\tilde{\boldsymbol{H}}_{C(\mathfrak{a})}=\{(C(\mathfrak{a}), \omega_0\varepsilon Nk), \varepsilon\in \boldsymbol{E}_0\}$$

for a fixed element ω_0 in $k_0^\times$ satisfying $N\mathfrak{a}=(\omega_0)$. Consequently we have $|\tilde{\boldsymbol{H}}_{C(\mathfrak{a})}|=(\boldsymbol{E}_0: N\boldsymbol{E})$. Furthermore, since $|\tilde{\boldsymbol{H}}|=\sum_{C(\mathfrak{a})\in \boldsymbol{H}}|\tilde{\boldsymbol{H}}_{C(\mathfrak{a})}|$, we have the second identity of (4.7). The first identity of (4.7) can be shown by using the same arguments as above. Thus our conclusion follows.

Finally we give an example.

EXAMPLE. Consider 5-th cyclotomic polynomial $f(t)=t^4+t^3+t^2+t+1$. Let ζ be a root of $f=0$, and put $\xi=\zeta+\zeta^{-1}-(\zeta^2+\zeta^{-2})$. Then we have $\xi^2=5$. Consequently we have $k_0=\boldsymbol{Q}(\sqrt{5})$, $\boldsymbol{E}_0=\{\pm(2+\sqrt{5})^m, m=0, \pm1, \pm2, \cdots\}$, $\boldsymbol{E}_0^+=\{(2+\sqrt{5})^{2m}, m=0, \pm1, \cdots\}$ where k_0 is the maximal real subfield of $\boldsymbol{Q}(\zeta)$, and $\boldsymbol{E}_0$ and $\boldsymbol{E}_0^+$ are, respectively, the unit group of k_0 and the group of all totally positive elements in $\boldsymbol{E}_0$. It is known that all fractional ideals of $\boldsymbol{Q}(\zeta)$ are principal. Hence we have

(1) $|\Gamma(f)/G|=4$,

(2) $|\Gamma^G(f)/\Gamma|=1$ for any class $\Gamma^G(f)$ in $\Gamma(f)/G$.

References

[1] A. BOREL et AL., Seminar on Algebraic Groups and Related Finite Groups, Lecture Notes in Math., **131**, Springer, 1970.

[2] R. DEDEKIND, Über die Diskriminanten Endlicher Körper, Gesammelte mathematische Werke, Bd. 1, Braunschweig, 1936.

[3] J. A. GREEN, The character of the finite general linear group, Trans. Amer. Math. Soc., **80** (1955), 402-447.

[4] H. HASSE, Zahlen Theorie, Acadèmie-Verlag, Berlin, 1949.

[5] C. G. LATIMER and C. C. MACDUFFEE, A correspondence between classes of ideals and classes of matrices, Ann. of Math., **34** (1933), 313-316.

[6] M. NEWMAN, Integral Matrices, Academic Press, 1972.

[7] T. A. SPRINGER, Over symplectische Transformationes, Thesis, Univ. Leiden, 1951.

[8] T. TAKAGI, Algebraic Number Theory, Iwanami Shoten (in Japanese), 1971.

[9] O. TAUSSKY, On a theorem of Latimer and MacDuffee, Canad. J. Math., **1** (1949), 300-302.

[10] O. TAUSSKY, On matrix classes corresponding to an ideal and its inverse, Illinois J.

Math., **1** (1957), 108-113.

[11] G. E. WALL, On the conjugacy classes in the unitary, symplectic and orthogonal groups, J. Austral. Math. Soc., **3** (1963), 1-62.

Present Address:
DEPARTMENT OF MATHEMATICS
TSUDA COLLEGE
KODAIRA-SHI, TOKYO 187