20. On Certain Elliptic Conjugacy Classes of the Siegel Modular Group

By Ki-ichiro HASHIMOTO
Department of Mathematics, Waseda University

(Communicated by Shokichi IYANAGA, M. J. A., March 12, 1985)

0. In this note we describe some results on the parametrization of the elliptic conjugacy classes in $\Gamma_n=\mathrm{Sp}(n, \boldsymbol{Z})$, the Siegel modular group of degree n, of the elements whose minimal polynomials are irreducible over $\boldsymbol{Q}$, hence are cyclotomic polynomials $\Phi_m(X)$. Our first result (Theorem 1) shows the bijective correspondence of the conjugacy classes in Γ_n with $\Phi_m(X)$ and the isometric classes of (skew-)hermitian forms over the ring of integers of the splitting field K of $\Phi_m(X)$, which generalizes our previous result [4]. Then we study in more details the case of $\varphi(m)=2n$, where the elements are regular. Especially, we show that the number of such conjugacy classes in Γ_n is equal to $h^-(K)$, the relative class number of K, multiplied by a power of 2 which is the number of "*integral*" classes in $\mathrm{Sp}(n, \boldsymbol{Q})$ or $\mathrm{Sp}(n, \boldsymbol{R})$. This refines a result of Midorikawa [6]. In Theorem 3, we characterize the integral conjugacy classes in $\mathrm{Sp}(n, \boldsymbol{R})$ in terms of their eigenvalues as an element of $\mathrm{U}(n)$, the maximal compact subgroup. There are two proofs for our results, one of which is an application of our previous result [3]. Details will appear elsewhere.

1. **Notations.**

$\sharp(S):=$ the cardinality of a finite set S.

$\Phi_m(X):=\prod_{d\mid m}(X^d-1)^{\mu(m/d)}$, m-th cyclotomic polynomial.

$K:=\boldsymbol{Q}(\zeta_m)$, $\zeta_m=e^{2\pi i/m}$; $K_o:=\boldsymbol{Q}(\zeta_m+\zeta_m^{-1})$.

$O_K, O_{K_o}:=$ the ring of integers of K, K_o.

$\mathfrak{d}=\mathfrak{d}(K/\boldsymbol{Q})$, the Differente of $K/\boldsymbol{Q}$.

$t:=\sharp\{\mathfrak{p}$; prime ideals in K_o, ramified in $K/K_o\}$.

$=1$, or 0 according as m is a prime power or not ($m\not\equiv 2$, mod 4).

For a commutative ring A with 1,

$$\mathrm{Sp}(n, A):=\left\{g\in \mathrm{SL}_{2n}(A)\,;\, gJ_n{}^tg=J_n,\ J_n=\begin{pmatrix}0 & -1_n\\ 1_n & 0\end{pmatrix}\right\}.$$

$\Gamma_n:=\mathrm{Sp}(n, \boldsymbol{Z})$, the Siegel modular group of degree n.

$G_{\boldsymbol{Q}}:=\mathrm{Sp}(n, \boldsymbol{Q})$, $\quad G_{\boldsymbol{R}}:=\mathrm{Sp}(n, \boldsymbol{R})$.

For a subgroup H of $G_{\boldsymbol{R}}$,

$H(\Phi_m):=\{g\in H$; g is semi-simple with minimal polynomial $\Phi_m(X)\}$.

$C_H(g):=\{x^{-1}gx\,;\, x\in H\}$, the H-conjugacy class of g.

$H(\Phi_m)/\!/H:=$ the set of H-conjugacy classes in $H(\Phi_m)$.

2. **Results.** We assume, throughout this note, that m ($\not\equiv 2$, mod 4) is a positive integer satisfying $2n\equiv 0 \bmod \varphi(m)$, where $\varphi(m)=\sharp(\boldsymbol{Z}/m\boldsymbol{Z})^*$.

Let (V, f) be the vector space of dimension $2n$ over $\boldsymbol{Q}$, which is equipped with the standard alternating form

(1) $\qquad f(x, y)=xJ_n{}^t y=\sum_{i=1}^{n}(x_{i+n}y_i-x_i y_{i+n}), \qquad x, y \in V=\boldsymbol{Q}^{2n}.$

If $g \in G_{\boldsymbol{Q}}(\Phi_m)$ is an element of $G_{\boldsymbol{Q}}=\mathrm{Aut}(V, f)$, one can give V a structure of K-module by the action of g on V, through the isomorphism $\boldsymbol{Q}(g)\cong\boldsymbol{Q}(\zeta_m)=K$. Then the map $f_{x,y}: K\to\boldsymbol{Q}$ defined by $f_{x,y}(\alpha):=f(x\alpha, y)$ being $\boldsymbol{Q}$-linear, one sees that there is a unique element $H_g(x, y)$ of V such that

(2) $\qquad f(x\alpha, y)=\mathrm{Tr}_{K/\boldsymbol{Q}}(\alpha H_g(x, y)), \qquad$ for any $\alpha \in K$.

It is immediate to show that $H_g(x, y)$ defines a skew hermitian form on the K-module V, with respect to the conjugation of K/K_0 which corresponds to that of $\boldsymbol{Q}(g)$ induced by $g\to J_n{}^t g J_n^{-1}\ (=g^{-1})$. The principle of Milnor [7] and Springer-Steinberg [9] in our situation is the following:

Lemma 1. *The correspondence $g\to H_g$ defines a canonical bijection between $G_{\boldsymbol{Q}}(\Phi_m)/\!/G_{\boldsymbol{Q}}$ and the set of isomorphic classes of skew-hermitian forms on $V\cong K^{2n/\varphi(m)}$ over K.*

Now we consider the integral version of this correspondence. Let $L=\boldsymbol{Z}^{2n}$ be the standard lattice in V on which we restrict f so that $\Gamma_n=\mathrm{Aut}(L, f)$. Then an element g of $\Gamma_n(\Phi_m)$ defines as above a structure of O_K-module on L, hence it gives us an O_K-lattice in our skew-hermitian space (V, H_g). Our first result is:

Theorem 1. *With the above notations, the O_K-lattice L in the skew-hermitian space (V, H_g) is $\mathfrak{d}^{-1}$-modular. Conversely, any $\mathfrak{d}^{-1}$-modular lattice over O_K in a skew-hermitian space of rank $2n/\varphi(m)$ defines by* (2) *an element g of $\Gamma_n(\Phi_m)$. The correspondence $g\to(L, H_g)$ induces a canonical bijection between $\Gamma_n(\Phi_m)/\!/\Gamma_n$ and the set $H_n(\Phi_m)$ of isometric classes of $\mathfrak{d}^{-1}$-modular skew-hermitian lattices of rank $2n/\varphi(m)$ over O_K.*

Here we recall that an O_K-lattice in (V, H_g) is called $\mathfrak{a}$-modular for an ideal $\mathfrak{a}$ of K, if it satisfies $L=\mathfrak{a}L^*$, where $L^*:=\{x \in V; H_g(x, L)\subseteq O_K\}$ is the dual lattice of L (cf. [5], [8]).

Remark 1. By scaling H_g with a pure element of K, one can restate the above results in terms of hermitian forms over K. Thus, it generalizes the main result of [4].

Definition 1. We call a $G_{\boldsymbol{Q}}$ or $G_{\boldsymbol{R}}$-conjugacy class $C(g)$ in $G_{\boldsymbol{R}}(\Phi_m)$ "*integral*", if it is represented by an element of Γ_n i.e., $C(g)\cap\Gamma_n\neq\phi$.

In what follows, we assume that $\varphi(m)=2n$, so that the elements of $G_{\boldsymbol{R}}(\Phi_m)$ are regular. Then the rank of our skew-hermitian space V being one, we can identify O_K-lattices L in V with ideals in the cyclotomic field K.

Lemma 2. *In a given skew-hermitian space (V, H) of rank one, the set of $\mathfrak{d}^{-1}$-modular lattices* (*or ideals*) *form a single genus with respect to the unitary group $U(V, H)$.*

From this lemma and the standard knowledge of the classification of hermitian forms (cf. [5], [8]), one can derive the following:

Theorem 2. *Suppose $\varphi(m)=2n$.*

(i) *For each integral $G_{\boldsymbol{Q}}$-conjugacy class $C_{G_{\boldsymbol{Q}}}(g)$, we have*

$$\sharp\,[C_{G_Q}(g)\cap\Gamma_n /\!/ \Gamma_n]=h^-(K)$$

($=h(K)/h(K_o)$: *the relative class number of* K).

(ii) *The number of integral* G_Q*-conjugacy classes in* $G_Q(\Phi_m)/\!/G_Q$ *is equal to* 2^{n+t-1}.

(iii) *The number of integral* G_R*-conjugacy classes in* $G_R(\Phi_m)/\!/G_R$ *is also equal to* 2^{n+t-1}.

(iv) $$\sharp\,[\Gamma_n(\Phi_m)/\!/\Gamma_n]=2^{n+t-1}h^-(K).$$

Remark 2. Our method for the above result (i) provides an alternative proof of the well known fact that $h(K_o)$ divides $h(K)$.

Remark 3. (i) and (iii) of Theorem 2 agree with the result of Midorikawa [6]; in fact one can easily show that the unpleasant factors H^+, E_o^+ in [6] which are difficult to calculate, cancel each other. We also remark that the relative class number $h^-(K)$ of K, being a product of the generalized Bernoulli numbers, can be calculated easily.

Remark 4. Theorem 2 is also a consequence of the general result of [3]; in fact we can show that $c_p(g, U_p, V_p)=1$ for all p, if $C_{G_Q}(g)$ is integral, and that the class number $h(V)$ of V ($=O_{K_A}^*$) in [3] is nothing but the class number of the genus of L.

To state the next result, we note that the standard maximal compact subgroup of G_R is identified with U(n), the unitary group of degree n, by the isomorphism $\begin{pmatrix} A & B \\ -B & A\end{pmatrix}\mapsto A+iB$. It is easy to see that $\sharp\,(G_R(\Phi_m)/\!/G_R)=2^n$, and the set $G_R(\Phi_m)/\!/G_R$ is represented by

(3) $g=g(\varepsilon_1\theta_1,\cdots,\varepsilon_n\theta_n)=\mathrm{diag}\,(e^{\varepsilon_1 i\theta_1},\cdots,e^{\varepsilon_n i\theta_n})\in \mathrm{U}(n),\qquad \varepsilon_j=\pm 1,$

where $(\theta_j)_{j=1}^n$ form a complete set of representatives of

$$\{(2\pi/m)k\,;\,k\in(\boldsymbol{Z}/m\boldsymbol{Z})^*,\text{ with }0<k<m/2\}.$$

Theorem 3. (i) *If* m *is a prime power, all* G_R*-conjugacy classes in* $G_R(\Phi_m)/\!/G_R$ *are integral.*

(ii) *Suppose* m *is not a prime power. Then the* G_R*-conjugacy class represented by* $g(\varepsilon_j\theta_j)$ *as in* (3) *is integral, if and only if*

(4) $$\prod_{j=1}^n \varepsilon_j=\prod_{\substack{p\mid m,\ p\neq 2\\ p^f\equiv -1\ (\mathrm{mod}\ m_p)}}(-1)^{\varphi(m_p)/2f}\quad (=(-1)^{n/2})^{*)}$$

where $m=p^e m_p$, $(p, m_p)=1$, *and* $f=f_p$ *if the degree of the prime factors* $\mathfrak{p}$ *of* p *in* $K_o/\boldsymbol{Q}$.

Example. (i) $n=2, m=2^2 3=12$. We have, for $p=3$, $3^1\equiv -1\ (\mathrm{mod}\ 4)$, $\varphi(m_3)/2f=2/2=1$, so that (4) implies $\varepsilon_1\varepsilon_2=-1$. Therefore $g(\pi/6, 5\pi/6)\in G_R(\Phi_{12})$ is *not* integral, as shown in Gottschling [1] (see also [2], Theorem 6-1).

(ii) Also one sees that for $n=4$, $m=15$, the classes of $g(2\pi\varepsilon_1/15, 4\pi\varepsilon_2/15, 8\pi\varepsilon_3/15, 14\pi\varepsilon_4/15)$ with $\varepsilon_1\varepsilon_2\varepsilon_3\varepsilon_4=-1$ ($\varepsilon_j=\pm 1$) are *not* integral.

---

*) *Added in Proof.* It can be shown that the right hand side of (4) is equal to $(-1)^{n/2}$.

References

[1] E. Gottschling: Über die Fixpunkte der Siegelschen Modulgruppe. Math. Ann., **143**, 111–149 (1961).

[2] K. Hashimoto: The dimension of the spaces of cusp forms on Siegel upper half plane of degree two (I). J. Fac. Sci. Univ. Tokyo, **30**-2, 403–488 (1983).

[3] ——: A formula for the number of semi-simple conjugacy classes in the arithmetic subgroups. Proc. Japan Acad., **61A**, 48–50 (1985).

[4] K. Hashimoto and R. J. Sibner: Involutive modular transformations on the Siegel upper half plane and an application to representations of quadratic forms (to appear in J. of Number Theory).

[5] R. Jacobowitz: Hermitian forms over local fields. Amer. J. Math., **84**, 441–465 (1962).

[6] H. Midorikawa: On the number of regular elliptic conjugacy classes in the Siegel modular group of degree $2n$. Tokyo J. Math., **6**, 25–38 (1983).

[7] J. Milnor: On isometries of inner product spaces. Invent. math., **8**, 83–97 (1969).

[8] G. Shimura: Arithmetic of unitary groups. Ann. of Math., **79**, 369–409 (1964).

[9] T. A. Springer and R. Steinberg: *Conjugacy classes*, seminar on algebraic groups and related finite groups. Lect. Notes in Math., vol. 131, Springer (1970).