13. A Formula for the Number of Semi-simple Conjugacy Classes in the Arithmetic Subgroups

By Ki-ichiro HASHIMOTO
Department of Mathematics, Waseda University

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

0. The purpose of this note is to present a general formula for the number of conjugacy classes in the arithmetic subgroups of a reductive algebraic group G defined over an algebraic number field k, of those elements which are contained in a single semi-simple conjugacy class of G_k.

It is known that the semi-simple conjugacy classes in the classical groups are parametrized by isomorphism classes of various kinds of hermitian forms. Moreover, the centralizer of the elements in a class is the unitary group of the corresponding hermitian forms (c.f. [1], [5], [8], [9], [10]). From this fact, one can deduce the *Hasse-Principle* for the conjugacy classes in the classical groups defined over algebraic number fields ([1], [5]). Now it seems natural to expect that, also for the groups over the ring of integers, the sets of conjugacy classes are parametrized by isometric classes of hermitian forms, so that their numbers are counted by the class numbers of such forms. In fact our previous paper [6] proves that this is exactly the case for a class of involutive elements in the Siegel modular group $\mathrm{Sp}(n, Z)$. The formula we shall give here shows that this is also true in the most general sense: it expresses the number of our conjugacy classes as a sum of the class numbers of the centralizer, up to the local factors which turn out to be one in most cases.

Notation. We write $g_1 \underset{H}{\sim} g_2$ if g_1, g_2 are H-conjugate for a subgroup H of G, and denote by $G/\!/H$ the set of H-conjugacy classes in G.

1. Let G be a reductive algebraic group defined over an algebraic number field k, and suppose that $G_k \subseteq GL_n(k)$. By an idèlic arithmetic subgroup U, we mean an open subgroup of G_A, the idèle group of G, which is of the form

$$U=\prod_{\mathfrak{p}} U_{\mathfrak{p}} \times G_\infty, \qquad U_{\mathfrak{p}}=G_{k_{\mathfrak{p}}} \cap GL_n(O_{\mathfrak{p}}),$$

where $G_{k_{\mathfrak{p}}}$ is the $\mathfrak{p}$-adic completion of G_k, $O_{\mathfrak{p}}$ is the ring of integers of $k_{\mathfrak{p}}$, and G_∞ is the archimedian part of G_A. By the reduction theory, it is known that G_A is decomposed as a disjoint union of finite double cosets Ug_iG_k $(1 \leq i \leq H)$, where $H=H(U)$ is the class number of U in G_A. Then the groups $\Gamma_i := G_k \cap g_i^{-1}Ug_i$ are called (global) *arithmetic subgroups* corresponding to U.

2. Let $g \in G_k$ be a semi-simple element, and put

$$C_k(g) := \{x^{-1}gx \,;\, x \in G_k\} \qquad (G_k\text{-conjugacy class of } g)$$

$$(1) \qquad Z_G(g) := \{x \in G_k \,;\, xg=gx\} \qquad (\text{centralizer of } g \text{ in } G_k)$$

$$M_k(g, \Gamma_i) := \{x \in G_k\,;\ x^{-1}gx \in \Gamma_i\}.$$

These are k-closed subsets of G_k, and $Z_G(g)$ is a k-subgroup of G which is again reductive. Let V be an idèlic arithmetic subgroup of $Z_G(g)_A$, and write, as above, $Z_G(g)_A = \coprod_{j=1}^{h} Z_G(g)_k z_j V$ with $h = H(V) =:$ the class number of V in $Z_G(g)_A$. Also put $\Lambda_j = Z_G(g)_k \cap z_j V z_j^{-1}$ $(1 \leq j \leq h)$. We denote by gen(V) the $Z_G(g)_A$-conjugacy class of the idèlic arithmetic subgroups in $Z_G(g)_A$ represented by V, and call it the *genus* of V. Then the set $C_k(g) \cap \Gamma_i$ is divided into a disjoint union

(2) $$C_k(g) \cap \Gamma_i = \coprod_{\mathrm{gen}\,(V)} C(g, V, i) \cap \Gamma_i,$$

where $C(g, V, i) := \{x^{-1}gx\,;\ x \in G_k,\ (Z_G(g)_A \cap xU_i x^{-1}) \in \mathrm{gen}\,(V)\}$, $U_i = g_i^{-1}Ug_i$. It is easy to show that the map $x^{-1}gx \to$(coset of x) induces the bijection

(3) $$C(g, V, i) \cap \Gamma_i /\!/ \Gamma_i \xrightarrow{\sim} Z_G(g)_k \backslash M(g, \Gamma_i, V)/\Gamma_i,$$

where $M(g, \Gamma_i, V) := \{x \in G_k\,;\ x^{-1}gx \in \Gamma_i,\ (Z_G(g)_A \cap xU_i x^{-1}) \in \mathrm{gen}\,(V)\}$. Put $M_A(g, U, V) := \{x \in G_A\,;\ x^{-1}gx \in U,\ (Z_G(g)_A \cap xUx^{-1}) \in \mathrm{gen}\,(V)\}$. Then it is easy to prove the following

Lemma 1. *We have* $G_A = \coprod_{i=1}^{H} G_k g_i^{-1} U$. *For each* i $(1 \leq i \leq H)$, *the map* $ag_i^{-1}u$ $(a \in G_k, u \in U) \to$*(coset of* a*) induces a bijection*

(4) $$Z_G(g)_k \backslash M_A(g, U, V) \cap G_k g_i^{-1} U/U \xrightarrow{\sim} Z_G(g)_k \backslash M(g, \Gamma_i, V)/\Gamma_i.$$

Corollary 2. $\sum_{i=1}^{H} \#(Z_G(g)_k \backslash M(g, \Gamma_i, V)/\Gamma_i) = \#(Z_G(g)_k \backslash M_A(g, U, V)/U)$.

Lemma 3. *The following map induced by the inclusion map is* $H(V)$ *to one.*

(5) $$\phi : Z_G(g)_k \backslash M_A(g, U, V)/U \longrightarrow Z_G(g)_A \backslash M_A(g, U, V)/U.$$

Proof. For any $x \in M_A(g, U, V)$, we have

$$\begin{aligned}\phi^{-1}(Z_G(g)_A xU) &= Z_G(g)_k \backslash (Z_G(g)_A xU)/U \\ &\cong Z_G(g)_k \backslash (Z_G(g)_A \cdot xUx^{-1})/xUx^{-1} \\ &\cong Z_G(g)_k \backslash Z_G(g)_A/(Z_G(g)_A \cap xUx^{-1}) \\ &\cong Z_G(g)_k \backslash Z_G(g)_A/V.\end{aligned}$$

Q.E.D.

3. From (3), (4), (5), we have

(6) $$\sum_{i=1}^{H} \#(C(g, V, i) \cap \Gamma_i /\!/ \Gamma_i) = H(V) \cdot \prod_{\mathfrak{p}} \#(Z_G(g)_{\mathfrak{p}} \backslash M_{\mathfrak{p}}(g, U_{\mathfrak{p}}, V_{\mathfrak{p}})/U_{\mathfrak{p}}),$$

where $M_{\mathfrak{p}}(g, U_{\mathfrak{p}}, V_{\mathfrak{p}}) = \{x \in G_{\mathfrak{p}}\,;\ x^{-1}gx \in U_{\mathfrak{p}},\ Z_G(g)_{\mathfrak{p}} \cap xU_{\mathfrak{p}}x^{-1} \widetilde{z_G(g)}_{\mathfrak{p}} V_{\mathfrak{p}}\}$. Now we put

(7) $$c_{\mathfrak{p}}(g, U_{\mathfrak{p}}, V_{\mathfrak{p}}) = \#(Z_G(g)_{\mathfrak{p}} \backslash M_{\mathfrak{p}}(g, U_{\mathfrak{p}}, V_{\mathfrak{p}})/U_{\mathfrak{p}}),$$

and note that it gives the number of ways to embed the open subgroup $V_{\mathfrak{p}}$ of $Z_G(g)_{\mathfrak{p}}$ *optimally* into $U_{\mathfrak{p}}$, up to the $U_{\mathfrak{p}}$-conjugacy. From (2), (6), and (7), we have the following general formula for the number of total conjugacy classes in our arithmetic subgroups Γ_i $(1 \leq i \leq H)$, of the elements $C_k(g) \cap \Gamma_i$:

Theorem. *We have*

(8) $$\sum_{i=1}^{H} \#(C_k(g) \cap \Gamma_i /\!/ \Gamma_i) = \sum_{\mathrm{gen}\,(V)} H(V) \prod_{\mathfrak{p}} c_{\mathfrak{p}}(g, U_{\mathfrak{p}}, V_{\mathfrak{p}}),$$

where the sum is extended over the genera gen(V) *of idèlic arithmetic sub-*

groups V of $Z_G(g)_A$ such that $c_{\mathfrak{p}}(g, U_{\mathfrak{p}}, V_{\mathfrak{p}}) \neq 0$ for all $\mathfrak{p}$, and is actually a finite sum.

Remark. The above argument is a slight refinement of the method in [2].

With the knowledge of the parametrization of G_k-conjugacy classes developed in [1], [5], [8], and [9], this formula gives us an effective procedure to count explicitly the number of semi-simple conjugacy classes with given characteristic polynominals in a wide class of arithmetic subgroups of the classical groups. For example, one can give:

(a) a complete list of torsion elements in lower rank groups such as $\mathrm{Sp}(3, \boldsymbol{Z})$, $\mathrm{SU}(2, 1)$ over the ring of imaginary quadratic fields.

(b) a different proof of the main result in [6], and its analogue in the compact $\boldsymbol{Q}$-forms of $\mathrm{Sp}(n)$.

(c) a refinement of the results of Midorikawa [7] on the number of regular elliptic conjugacy classes in $\mathrm{Sp}(n, \boldsymbol{Z})$.

These will be treated in subsequent papers ([3], [4]).

References

[1] T. Asai: The conjugacy classes in the unitary, symplectic, and orthogonal groups over an algebraic number field. J. Math. Kyoto Univ., **16**, 325–350 (1976).

[2] K. Hashimoto: On Brandt matrices associated with the positive definite quaternion hermitian forms. J. Fac. Sci. Univ. Tokyo, **27**, 227–245 (1980).

[3] ——: On Certain Elliptic Conjugacy Classes of the Siegel Modular Group (to appear).

[4] ——: Involutive conjugacy classes in arithmetic subgroups of $\mathrm{Sp}(n)$ (in preparation).

[5] K. Hashimoto and T. Ibukiyama: On class numbers of positive definite binary quaternion hermitian forms. J. Fac. Sci. Univ. Tokyo, **27**, 549–601 (1980).

[6] 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).

[7] 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).

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

[9] G. E. Wall: On the conjugacy classes in the unitary, symplectic, and orthogonal groups. J. Austr. Math. Soc., **3**, 1–62 (1963).

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