BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 78, Number 4, July 1972

HECKE RINGS OF CONGRUENCE SUBGROUPS

BY NELO D. ALLAN

Communicated by M. Gerstenhaber, December 27, 1971

Let k be a $\mathfrak{p}$-adic field and let $\hat{G}$ be a reductive group defined over k. Let G be a semigroup in $\hat{G}$, i.e. a multiplicative subset with the same unity as $\hat{G}$ We shall assume that there exists an open compact subgroup Δ of $\hat{G}$ which is contained in G. Let $\mathcal{R}(G, \Delta)$ be the free Z-module generated by the double cosets of G modulo Δ, with a product defined as in [3, Lemma 6]. We have an associative ring with unity which we shall call the Hecke Ring of G with respect to Δ. Let Δ_0 be a normal subgroup of Δ satisfying our conditions H-1 and H-2 of §1. Our purpose is to find generators and relations for $\mathcal{R}(G, \Delta_0) = \mathcal{R}$. There exists a finitely generated polynomial ring $Z[G]$ which together with the group ring $Z[\Delta/\Delta_0]$ generates $\mathcal{R}$; moreover $\mathcal{R}$ is a $Z[\Delta/\Delta_0]$-bimodule having $Z[D]$ as basis. Our hypothesis H-1 and H-2 are verified for the principal congruence subgroups of most of the classical groups considered in [2].

We thank Mr. J. Shalika for the helpful discussions during the preparation of this work and also for pointing out some hopes that this might bring in solving Harish-Chandra conjecture on the finite dimensionality of the irreducible continuous representations of these rings.

1. **General results.** Let T be a connected k-closed subgroup of G consisting only of semisimple elements, and N^+ and N^- be maximal k-closed unipotent subgroups normalized by T. We set $N^+ = N^+ \cap \Delta$, and $U^- = N^- \cap \Delta$. We shall now state our first condition:

Condition H-1. There exists a finitely generated semigroup D in T such that $G = \Delta D \Delta$ (disjoint union), and for all $d \in D$ we have $dU^+d^{-1} \subset U^+$ and $d^{-1}U^-d \subset U^-$.

We turn now to our second condition. We let Δ_0 be a normal subgroup of Δ and we set $U_0^+ = U^+ \cap \Delta_0$ and $U_0^- = U^- \cap \Delta_0$. We shall assume that $T \cdot N^+ \cap \Delta_0 = (T \cap \Delta_0) \cdot U_0^+$.

Condition H-2. There exists a semigroup D in T such that $\Delta_0 = U_0^+ V U_0^-$ for a certain subgroup V of Δ_0 normalized by D, and for all d in D we have $dU_0^+d^{-1} \subset U_0^+$ and $d^{-1}U_0^-d \subset U_0^-$.

Let us denote by $\bar{1}$ the unity of $\mathcal{R}$ and by $\bar{g}$ the double coset $\Delta_0 g \Delta_0$. We shall denote the product in $\mathcal{R}$ by $*$.

THEOREM 1. *Condition* H-2 *implies that* $D = \Delta_0 D \Delta_0$ *is a semigroup in* $\hat{G}$ *and* $\mathcal{R}(\hat{D}, \Delta_0) \simeq Z[D]$.

AMS 1969 *subject classifications.* Primary 2220; Secondary 2265, 4256, 2070.
Key words and phrases. Hecke rings, algebraic groups, locally compact groups, convolution algebras.

PROOF. Our condition implies that for all $d_1, d_2 \in \boldsymbol{D}$, we have $\Delta_0 d_1 \Delta_0 d_2 \Delta_0 = \Delta_0 d_1 d_2 \Delta_0$, or $\bar{d}_1 * \bar{d}_2 = m \cdot \overline{d_1 d_2}$, with $m \in \boldsymbol{Z}$, and it remains to prove that $m = 1$. From H-2 we can write

$$\Delta_0 d \Delta_0 = \bigcup \{\Delta_0 d u_j | j = 1, \ldots, \omega(d),\ u_j \in \boldsymbol{U}_0^-\}.$$

Set $v_j = d u_j d^{-1} \in \boldsymbol{N}^-$. If $\Delta_0 d u_j = \Delta_0 d_1$ for some d_1 in $\boldsymbol{D}$, then we have $\bar{v}_j = \bar{1}$ and we may replace d_1 by d. This is equivalent to the existence of $v \in \Delta_0$ such that $vd = du_j$. Now we set $\Delta_0 d_i \Delta_0 = \bigcup \Delta_0 d u_j^{(i)}$, $i = 1, 2$, and we recall that m is the number of pairs (i, j) such that

$$\Delta_0 d_1 d_2 = \Delta_0 d_1 u_i^{(1)} d_2 u_j^{(2)}.$$

We have $v d_1 d_2 = d_1 d_2 \tilde{u}_i^{(1)} u_j^{(2)} = d_1 u_i^{(1)} v_j^{(2)} d_2$, for some $\tilde{u}_i^{(1)}$ in Δ_0, and this implies $\bar{v}_j^{(2)} = 1$ and consequently we have $\bar{v}_i^{(1)} = \bar{1}$. Therefore $m = 1$. Q.E.D.

THEOREM 2. *The conditions* H-1 *and* H-2 *with the same* $\boldsymbol{D}$ *imply the finite generation as a ring of* $\mathscr{R}$. *Moreover* $\mathscr{R}$ *is a* $\boldsymbol{Z}[\Delta/\Delta_0]$*-bimodule having* $\boldsymbol{Z}[\boldsymbol{D}]$ *as a basis.*

PROOF. We let $\{d_1, \ldots, d_r\}$ be a set of generators for $\boldsymbol{D}$. Let $\{\alpha_1, \ldots, \alpha_h\}$ be a complete set of representatives for Δ modulo Δ_0. Normality of Δ_0 implies that $\overline{\alpha_i d \alpha_j} = \bar{\alpha}_i * \bar{d} * \bar{\alpha}_j$. Also we have $\overline{\alpha_i \alpha_j} = \bar{\alpha}_i * \bar{\alpha}_j$ and for any $d, d' \in \boldsymbol{D}$, $\overline{dd'} = \bar{d} * \bar{d}'$. Now H-1 implies that for any $g \in \boldsymbol{G}$ there exist $\alpha_i, \alpha_j \in \Delta$ and $d \in \boldsymbol{D}$ such that $\bar{g} = \overline{\alpha_i d \alpha_j}$ and also that for any h in Δ and any $1 \leqq i, j \leqq r$, $\bar{d}_i * \overline{h d_j} = \bar{d}_i * \bar{h} * \bar{d}_j = \overline{d_i h} * \bar{d}_j$ is a linear combination with coefficients in $\boldsymbol{Z}$ of the elements $\overline{\alpha_i d \alpha_j}$. Therefore the number of generators of $\mathscr{R}$ is $r \cdot h_0$, where h_0 is the minimal number of generators of Δ/Δ_0. Q.E.D.

2. **Relations.** We observe that Theorem 2 gives us some relations among the generators of $\mathscr{R}$. Let us introduce some notation; for fixed $d \in \boldsymbol{D}$, we shall let $\boldsymbol{L}(d)$ (resp. $\boldsymbol{R}(d)$) be the set of $\{\bar{\alpha} | \alpha \in \Delta, \overline{\alpha d} = \overline{d\alpha'}$, for some $\alpha' \in \Delta$ (resp. $\overline{d\alpha} = \overline{\alpha' d}$)$\}$. $\boldsymbol{L}(d)$ and $\boldsymbol{R}(d)$ are subgroups of $\bar{\Delta}$. We denote by $\boldsymbol{R}'(d)$ and $\boldsymbol{L}'(d)$ the respective subgroups of $\boldsymbol{R}(d)$ and $\boldsymbol{L}(d)$ consisting of those elements $\bar{\alpha}$ such that $\bar{\alpha}'$ can be chosen as $\bar{1}$. It is easy to verify that $\boldsymbol{R}'(d) = \{\bar{\alpha} | \alpha \in d^{-1} \boldsymbol{U}_0^+ d \cap \Delta\} = \overline{d^{-1} \Delta_0 d \cap \Delta}$ and $\boldsymbol{L}'(d) = \{\bar{\alpha} | \alpha$ lies in $d \boldsymbol{U}_0^- d^{-1} \cap \Delta\} = \overline{d \Delta_0 d^{-1} \cap \Delta}$. We have the following straightforward lemmas:

LEMMA 1. $\bar{\alpha}_i * \bar{d} * \bar{\alpha}_r = \bar{\alpha}_j * \bar{d}' * \bar{\alpha}_s$ *if and only if* $\bar{d} = \bar{d}'$, $\bar{\alpha}_j \in \bar{\alpha}_i * \boldsymbol{L}(d)$ *and* $\bar{\alpha}_s \in \boldsymbol{R}'(d) * \bar{\psi} * \bar{\alpha}_r$, $\overline{\alpha_i^{-1} \alpha_j} * \bar{d} = \bar{d} * \bar{\psi}$ *for some* $\psi \in \Delta$.

LEMMA 2. *Suppose that for all the generators* d *of* $\boldsymbol{D}$ *we have* $d \boldsymbol{U}_0^- d^{-1} \subset \boldsymbol{U}^-$. *If* d *and* d' *are generators of* $\boldsymbol{D}$ *and if* $g \in \Delta$, *then*

$$\bar{d} * \overline{g d'} = \theta(d, g) * \bar{\alpha} * \bar{d}_1 * \bar{\alpha}',$$

where $\alpha, \alpha' \in \Delta$ *and* $d_1 \in D$ *are such that* $\overline{dgd'} = \overline{\alpha d_1 \alpha'}$, *and* $\theta(d, g) = m \cdot$ (*sum of all elements of* $L'(d)$ W, *where* W *is the subgroup of* $L'(d)$ *consisting of all* $\bar{\alpha}$ *such that* $\bar{\alpha} * \overline{dgd'} = \overline{dgd'}$). *m is not greater than the order of the group*

$$\bar{g} * L'(d') * \bar{g}^{-1} \cap R'(d).$$

Finally, we would like to observe that $\mathscr{R}$ has an involution induced by $g \to g^{-1}$ in the case where G is a group. If, moreover, there exists $\theta \in \Delta$ such that for all $d \in D$, $d^{-1} = \theta^{-1} d\theta$, then the mapping $\bar{\alpha} \to \overline{\theta\alpha\theta^{-1}}$ induces the isomorphisms $R'(d) \simeq L'(d)$ and $R(d) \simeq L(d)$.

EXAMPLES. Let K be a division algebra central over k, $\mathfrak{O}$ be the ring of integers of K, $\mathfrak{p}$ its prime and π a fixed generator of $\mathfrak{p}$. Given $a \in K$ we shall denote by ord(a) the power of π in a. We let q be the number of elements in $\mathfrak{O}/\mathfrak{p}$. For any positive integer m, $\mathfrak{O}/\mathfrak{p}^m$ has q^m elements. Let S be a subring of K and let $M_n(S)$ denote the ring of all n by n matrices with entries in S; if $g \in M_n(S)$ and $1 \leqq i, j \leqq n$, then $(g)_{ij}$ will denote the (i, j)-entry of g and if we set $(g)_{ij} = g_{ij}$, we write $g = (g_{ij})$; by e_{ij} we denote the matrix having 1 as (i, j)-entry and zero otherwise, and E_n or simply E will denote the identity of $M_n(S)$. $Gl_n(K)$ is the group of units of $M_n(K)$.

Case I. $\hat{G} = Gl_n(K)$. We let $G = Gl_n(K)$, $T = T_n$ = diagonal matrices in G, N^+(resp. N^-) the group of all unipotent upper (resp. lower) triangular matrices in G, $\Delta = G_{\mathfrak{O}} = Gl_n(\mathfrak{O})$. Let $D_n = \{d \in T \mid d = \operatorname{diag}[\pi^{r_1}, \ldots, \pi^{r_n}], r_1 \geqq r_2 \geqq \cdots \geqq r_n\}$. It is clear that D_n satisfies H-1. For any $r \geqq 1$ we set $\Delta_0 = \Delta_r = \{g \in \Delta \mid g = 1 \bmod \mathfrak{p}^r\}$ = the rth congruence subgroup of Δ. We have $T \cdot N^+ \cap \Delta_r = (T \cap \Delta_r) \cdot U_0^+$. We let $V = T \cap \Delta_r$ and $V' = T \cap \Delta$. Condition H-2 will follow from the following lemma:

LEMMA 3. $\Delta_r = U_0^+ V U_0^- = U_0^- V U_0^+$.

PROOF. Let $g \in \Delta_r$. As V normalizes both U_0^+ and U_0^- we may assume that all diagonal entries of g are 1. If we consider $g' = (E - g_{in} e_{in})g$, $i \neq n$, then $E - g_{in} e_{in} \in U_0^+$ and $(g')_{in} = 0$. These operations will reduce to zero the nondiagonal entries of the last column of g. Now it suffices to transpose the resulting matrix, repeat the operation and apply induction. Q.E.D.

REMARK. Let $d \in D$ be such that $r_n \geqq 0$. For any $\bar{v} \in L'(d)$ we can choose a representative such that $d^{-1} v d = u = (u_{ij}) \in U^-$ where $u_{ij} = 0$, for $i < j$, $u_{ii} = 1$ for all i, and $u_{ij} = a_{ij} \pi^r$ with $\operatorname{ord}(a_{ij}) < r_j - r_i$. Hence $\omega(d) = q^m, m = \sum_{i<j} (r_j - r_i)$. Also $d^{-1} = \theta d \theta$, $\theta = e_{1n} + \cdots + e_{n1}$ and for the generators of D, $d^{-1} \Delta_r d$ and $d \Delta_r d^{-1}$ are contained in Δ_{r-1}, because $r_1 = 1$.

Finally we would like to remark that in the case $n = 2$ and $K = k$ we have $m(Z(u)w, d) = 1$ if u is a unit, and equal to q, otherwise, where

$$d = \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}, \quad w = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z(u) = \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}.$$

Also if u is a unit, $d * \overline{Z(u)wd} = \overline{dZ(u)wd}$. This well determines the multiplication in $\mathcal{R}$.

The case where $G = Sl_n(k)$, and D, Δ, Δ_r, V being the respective intersection of the corresponding groups with $Sl_n(k)$, is covered by our Theorem 2.

Case II. *Unitary groups.* Let K denote either k, or a quadratic extension of k, or else a quaternion division algebra over k. Let ρ denote respectively, the identity, the nontrivial automorphism of K over k, and an involution of K. Clearly ρ can always be extended to an involution of $M_n(K)$. Let $h \geqq 0$ and let $n = 2p + b$; we subdivide every matrix $g \in M_n(K)$ into 9 blocks $g = (g_{ij})$, $i, j = 1, 2, 3$, in such way that $g_{11}, g_{33} \in M_p(K)$ and $g_{22} \in M_b(K)$. Let $\mathfrak{O}$ be the ring of integers of K, and fix an $H \in M_n(\mathfrak{O})$, such that $H^\rho = \gamma H$, $\gamma = \pm 1$, $H = (h_{ij})$, $h_{13} = \gamma h_{31} = \theta = e_{1\rho} + \cdots + e_{\rho 1}$, $h_{22} = V$ and $h_{ij} = 0$ otherwise, where V corresponds to an anisotropic form, if $b \neq 0$. We let G be the connected component of the group $\{g \in Gl_n(K) | g^\rho H g = \mu(g)H$, where μ is the multiplier$\}$, and we let G_0 be the correspondent group of V. We let

$$T = \{h \in G | h = \mathrm{diag}[z, h_0, \mu(h_0)\theta(z^\rho)^{-1}\theta],\ h_0 \in G_0 \text{ and } z \in T_p\},$$

and we denote by N^+, N^-, Δ and Δ_r the intersection of the corresponding group in $Gl_n(K)$ with G. We let $V = T \cap \Delta_r$ which clearly normalizes U_0^+ and U_0^-.

LEMMA 4. $\Delta_r = U_0^+ V U_0^-$.

PROOF. Let $g = (g_{ij}) \in \Delta_r$. We can apply Lemma 3 to g_{33} and we can write $g_{33} = n_1 h_1 u_1$. If we denote by $n = \mathrm{diag}[\theta(n_1^\rho)^{-1}\theta, E, n_1]$, $h = \mathrm{diag}[\theta(h_1^\rho)^{-1}\theta, E, h_1]$ and $u = \mathrm{diag}[\theta(u_1^\rho)^{-1}\theta, E, u_1]$, then $n \in U_0^+$, $h \in V$, and $u \in U_0^-$ and replacing g by $h^{-1}n^{-1}gu^{-1}$ we may assume that $g_{33} = E$. We take now $g' = (g'_{ij}) \in U_0^+$ with $g'_{12} = \gamma\theta g_{23}^\rho V$, $g'_{13} = \gamma\theta g_{13}^\rho\theta$ and $g'_{23} = -g_{23}$ and $g'' = \mathrm{diag}[E, h_0, E]$ in V, for a convenient $h_0 \in G_0$; hence $g''g'g \in U_0^-$. Q.E.D.

Now we consider Λ as in [2, §9], $l = 0$, $D = \{\pi^r | r \in \Lambda\}$ and $D' = \{d \in \Delta | \mu(d) = 1\}$. We take $\hat{G} = G$ and $G' = \{g \in G | \mu(g) = 1\}$ and consider their respective subgroups Δ, Δ', V, V', etc. It can be easily checked that in all the cases discussed in [2, §9], our Theorems 1 and 2 remain valid for (G', Δ') and for (G, Δ) with the exception of the case $(O) n = 2p$. For G' we also have the extra assumptions of Lemma 2 and we also have a $\theta = (\theta_{ij})$; $\theta_{13} = \gamma\theta_{31} = \theta$, $\theta_{22} = E$, $\theta_{ij} = 0$ otherwise, such that $d^{-1} = \theta d \theta$, $\pi^\rho = \gamma\pi$.

Closing this note we shall make two remarks:

REMARK. For the adjoint representation of a Chevalley type group we have condition H-1 by [**1**].

REMARK. Let $\mathscr{H}$ be a Hilbert space and let $\mathscr{B}(\mathscr{H})$ be the algebra of all bounded operators on $\mathscr{H}$. Suppose that there exists a finite group G of unitary operators and a finite set of commuting operators $D_1, \ldots, D_r$ all in $\mathscr{B}(\mathscr{H})$ such that all D_i's are not necessarily normal. Let $\mathscr{B}$ be the weak closure of the algebra generated by 1 and all the D_i. If we assume that every $A \in \mathscr{B}(\mathscr{H})$ can be written as a finite sum of $g_i B_{ij} g_j$, $g_i, g_j \in G$ and $B_{ij} \in \mathscr{B}$, does this necessarily imply that the dimension of $\mathscr{H}$ is finite? The positive answer of this question together with our Theorem 2 will imply Harish-Chandra's conjecture in these cases.

REFERENCES

1. N. Iwahori and H. Matsumoto, *On some Bruhat decomposition and the structure of the Hecke rings of p-adic Chevalley groups*, Inst. Hautes Études Sci. Publ. Math. No. 25 (1965), 5–48. MR **32** #2486.

2. I. Satake, *Theory of spherical functions on reductive algebraic groups over p-adic fields*, Inst. Hautes Études Sci. Publ. Math. No. 18 (1963), 5–69. MR **33** #4059.

3. T. Tamagawa, *On the ζ-function of a division algebra*, Ann. of Math. (2) **77** (1963), 387–405. MR **26** #2468.

UNIVERSIDAD NACIONAL DE COLOMBIA, BOGOTA, COLOMBIA, SOUTH AMERICA

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN AT PARKSIDE, RACINE, WISCONSIN 53403