The Hecke algebras for the orthogonal group $SO(2,3)$ and the paramodular group of degree 2

by

Jonas Gallenkämper, Aloys Krieg

Abstract

In this paper we consider the integral orthogonal group with respect to the quadratic form of signature $(2,3)$ given by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \perp \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \perp (-2N)$ for squarefree $N \in \mathbb{N}$. The associated Hecke algebra is commutative and the tensor product of its primary components, which turn out to be polynomial rings over $\mathbb{Z}$ in 2 algebraically independent elements.

The integral orthogonal group is isomorphic to the paramodular group of degree 2 and level $N$, more precisely to its maximal discrete normal extension. The results can be reformulated in the paramodular setting by virtue of an explicit isomorphism. The Hecke algebra of the non-maximal paramodular group inside $Sp(2; \mathbb{Q})$ fails to be commutative if $N > 1$.
1 Introduction

The Hecke theory plays an important role in the arithmetic theory of modular forms. Dealing with Siegel modular forms, a structure theorem was derived by Shimura [14] (cf. [1], [2]). Considering paramodular groups, such a result does not seem to be known. Dealing with orthogonal groups, authors (cf. [7], [15]) usually define their Hecke algebra as the tensor product of local components. On the other hand, several authors have investigated the connection between the paramodular group and the orthogonal group $SO(2, 3)$ (cf. [4], [5], [6], [13]).

In this paper we derive a structure result for the Hecke algebra associated with $SO(2, 3)$. By means of an explicit isomorphism we obtain analogous results for the paramodular group of degree 2 and squarefree level $N$. Moreover, we show that the Hecke algebra for the non-maximal paramodular subgroup inside $Sp_2(Q)$ also coincides with the tensor product of its primary components, but fails to be commutative similar to the case of the Fricke groups in [10]. Most of these results are contained in [3], where also results on the Hecke theory for $O(2, n + 2)$ are given.

Let us fix some notation. Let $(U, G)$ be a Hecke pair, i.e. $U$ is a subgroup of $G$ and each double coset $UgU$, $g \in G$, decomposes into finitely many right cosets $Uh$, $h \in G$. Denote by $\mathcal{H}(U, G)$ the Hecke algebra over $\mathbb{Z}$ of $(U, G)$ just as in [1], [2], [9], [14].

2 The orthogonal group $SO(2, 3)$

We fix further notation throughout the whole paper. Given a squarefree $N \in \mathbb{N}$ let

$$
S_N = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -2N & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad \tilde{S}_N = \begin{pmatrix} 0 & 0 & 1 \\ 0 & S_N & 0 \\ 1 & 0 & 0 \end{pmatrix}
$$

be even symmetric matrices of signature $(1, 2)$ resp. $(2, 3)$. Consider the attached special orthogonal groups

$$
SO(S_N; \mathbb{R}) := \{K \in SL_3(\mathbb{R}); S_N[K] = S_N\},
$$

$$
SO(\tilde{S}_N; \mathbb{R}) := \{M \in SL_5(\mathbb{R}); \tilde{S}_N[M] = \tilde{S}_N\},
$$

where the prime stands for the transpose and $A[B] := B^tAB$ for matrices $A, B$ of suitable size. Let $SO_0(S_N; \mathbb{R})$ resp. $SO_0(\tilde{S}_N; \mathbb{R})$ stand for the connected component of the identity matrix $E$ (of suitable size), which was
characterized in [11], sect. 2. For the integers instead of the reals we use the analogous notations for the subgroups, in particular
\[ \Gamma_N := SO_0(S_N; \mathbb{Z}), \quad \tilde{\Gamma}_N := SO_0(\hat{S}_N; \mathbb{Z}). \]

Just as in [11] we consider the matrices
\[ M_\lambda := \begin{pmatrix} 1 & -\lambda S_N & -\frac{1}{2}S_N[\lambda] \\ 0 & E & \lambda \\ 0 & 0 & 1 \end{pmatrix}, \]
\[ \tilde{M}_\lambda := \begin{pmatrix} 1 & 0 & 0 \\ \lambda & E & 0 \\ -\frac{1}{2}S_N[\lambda] & -\lambda S_N & 1 \end{pmatrix}, \quad \lambda \in \mathbb{R}^3, \]
\[ J^* := \begin{pmatrix} 0 & 0 & -1 \\ 0 & V & 0 \\ -1 & 0 & 0 \end{pmatrix}, \quad V := \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}, \]
\[ M_F := \begin{pmatrix} F_0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & F^* \end{pmatrix}, \quad F = \begin{pmatrix} \alpha \beta \\ \gamma \delta \end{pmatrix} \in SL_2(\mathbb{R}), \quad F^* = \begin{pmatrix} \alpha & -\beta \\ -\gamma & \delta \end{pmatrix}, \]
\[ \tilde{M}_F := \begin{pmatrix} \alpha E & 0 & \beta I \\ 0 & 1 & 0 \\ \gamma I & 0 & \delta E \end{pmatrix}, \quad F = \begin{pmatrix} \alpha \beta \\ \gamma \delta \end{pmatrix} \in SL_2(\mathbb{R}), \quad I = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \]
\[ \tilde{K} := \begin{pmatrix} 1 & 0 & 0 \\ 0 & K & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad K \in SO_0(S_N; \mathbb{R}) \]
in \( SO_0(\hat{S}_N; \mathbb{R}) \) as well as
\[ K_\mu := \begin{pmatrix} 1 & 2N\mu & N\mu^2 \\ 0 & 1 & \mu \\ 0 & 0 & 1 \end{pmatrix}, \quad \tilde{K}_\mu := \begin{pmatrix} 1 & 0 & 0 \\ \mu & 1 & 0 \\ N\mu^2 & 2N\mu & 1 \end{pmatrix}, \quad \mu \in \mathbb{R}, \]
in \( SO_0(S_N; \mathbb{R}) \).
Lemma 1. Let $N \in \mathbb{N}$ be squarefree.

a) Given $g \in \mathbb{Z}^3$ with $S_N[g] = 0$, there exists a matrix $K \in \Gamma_N$ such that
   
   $$Kg = (\gamma, 0, 0)', \quad \gamma = \pm \gcd(g).$$

b) Given $g \in \mathbb{Z}^5$ with $\hat{S}_N[g] = 0$, there exists a matrix $M \in \hat{\Gamma}_N$ such that
   
   $$Mg = (\gamma, 0, 0, 0)', \quad \gamma = \gcd(g).$$

Proof. a) Apply Corollary 4 and (15) in [11].

b) Multiply by a suitable matrix $M_{F, F} \in SL_2(\mathbb{Z})$, in (4) in order to assume $g = (\ast, \ast, \ast, 0)'$ without restriction. Then use a) and (5) in order to obtain $g = (\ast, \ast, 0, 0)'$. Finally, we get the result by a matrix $M_{G, G} \in SL_2(\mathbb{Z})$, from (4).

We use the results in order to obtain suitable representatives for right cosets in

$$G_N := SO_0(S_N; \mathbb{Q}), \quad \hat{G}_N := SO_0(\hat{S}_N; \mathbb{Q}).$$

Lemma 2. Let $N \in \mathbb{N}$ be squarefree.

a) Let $\frac{1}{m}K \in G_N$ with $m \in \mathbb{N}$ and integral $K$. Then the right coset $\Gamma_N K$ contains a unique representative of the form

   $$L = \left( \begin{array}{ccc} \alpha^* & 2Nm\mu/\delta^* & N\mu^2/\delta^* \\ 0 & m & \mu \\ 0 & 0 & \delta^* \end{array} \right), \quad \alpha^*, \delta^* \in \mathbb{N}, \quad \alpha^*\delta^* = m^2, \quad \mu \in \{0, 1, \ldots, \delta^* - 1\}. \quad (7)$$

b) Let $\frac{1}{m}M \in \hat{G}_N$ with $m \in \mathbb{N}$ and integral $M$. Then the right coset $\hat{\Gamma}_N M$ contains a unique representative of the form

   $$\left( \begin{array}{ccc} \alpha & a' & \beta \\ 0 & L & c \\ 0 & 0 & \delta \end{array} \right), \quad \alpha, \delta \in \mathbb{N}, \quad \alpha\delta = m^2, \quad c \in \{0, 1, \ldots, \delta - 1\}, \quad \beta = \frac{-1}{2s}S_N[c], \quad a = -\frac{1}{s}L'S_Nc, \quad \beta \in \mathbb{Z}. \quad (8)$$

where $L$ has the form (7). In this case $\alpha$ is the gcd of the first column of $M$.

Proof. a) For the existence apply Lemma 1 and (6) with an appropriate $\mu \in \mathbb{Z}$. As block triangular matrices form a group, we obtain the last row in the form $(0, 0, *)$ from the explicit form of the inverse in [11]. As this matrix belongs to the connected component of $E$, we get $\alpha^*, \delta^* \in \mathbb{N}$. Given
two matrices in the right coset of such a form multiply by the inverse of one from the right. Then one successively sees that they need to be equal. 
b) This part follows along the same lines using Lemma 1, a), (5) and (2) with an appropriate \( \lambda \in \mathbb{Z}^3 \). The shape of the first row is a consequence of \( \hat{S}_N[M] = m^2 \hat{S}_N \) (cf. [11]).

A necessary condition that the matrices in (7) and (8) occur is that they are integral.

A direct consequence is

**Corollary 1.** Let \( N \in \mathbb{N} \) be squarefree. Then \( (\Gamma_N, \mathcal{G}_N) \) and \( (\hat{\Gamma}_N, \hat{\mathcal{G}}_N) \) are Hecke pairs.

Next we consider double cosets.

**Lemma 3.** Let \( N \in \mathbb{N} \) be squarefree and \( \frac{1}{m} K \in \mathcal{G}_N \) with \( m \in \mathbb{N} \) and integral \( K \). Then the double coset \( \Gamma_N K \Gamma_N \) contains a unique representative of the form

\[
\text{diag}(\alpha^*, m, \delta^*), \quad \alpha^*, \delta^* \in \mathbb{N}, \quad \alpha^* \delta^* = m^2, \quad \alpha^* | m | \delta^*.
\]

The double coset is uniquely determined by the Smith invariants of \( K \).

**Proof.** The result follows from Theorem 4 in [10] in combination with Corollary 4 in [11].

Finally, we consider \( (\hat{\Gamma}_N, \hat{\mathcal{G}}_N) \).

**Theorem 1.** Let \( N \in \mathbb{N} \) be squarefree. Each double coset \( \hat{\Gamma}_N(\frac{1}{m} M) \hat{\Gamma}_N \), \( \frac{1}{m} M \in \mathcal{G}_N \) with \( m \in \mathbb{N} \) and integral \( M \), contains a unique representative of the form

\[
\frac{1}{m} \text{diag}(\alpha, \alpha^*, m, \delta^*, \delta),
\]

where

\[
\alpha, \alpha^*, \delta, \delta^* \in \mathbb{N}, \quad \alpha \delta = \alpha^* \delta^* = m^2, \quad \alpha \ | \ \alpha^* \ | \ m \ | \ \delta^* \ | \ \delta.
\]

The double coset is uniquely determined by the Smith invariants of \( M \).

**Proof.** Let \( \alpha \) be the smallest positive \((1,1)\)-entry of the matrices in \( \hat{\Gamma}_N M \hat{\Gamma}_N \). By Lemma 2 including its notations we may assume that \( M \) is upper triangular. Using Lemma 3 and the embedding (5), we may assume

\[
L = \text{diag}(\alpha^*, m, \delta^*), \quad \alpha^*, \delta^* \in \mathbb{N}, \quad \alpha^* \delta^* = m^2, \quad \alpha^* \ | \ m \ | \ \delta^*.
\]
If we multiply by $\widetilde{M}_\lambda$, $\lambda = (1,0,0)'$, in (2) from the right, we obtain a matrix with $\alpha$ and $\alpha^*$ in the first column. The choice of $\alpha$ and Lemma 2 lead to

$$\alpha \mid \alpha^*.$$ 

If we multiply by matrices $M_F$, $\widetilde{M}_G$, $F, G \in SL_2(\mathbb{Z})$, in (4) and (4') from the right, we may replace $\alpha$ by $\gcd(\alpha, a_1, a_3)$ if $a = (a_1, a_2, a_3)'$. Hence, $\alpha \mid a_1$ and $\alpha \mid a_3$. Multiplication by $M_\lambda$, $\lambda = \frac{1}{\alpha}(a_3, 0, a_1)' \in \mathbb{Z}^3$, in (2) from the right leads to

$$a_1 = a_3 = c_1 = c_3 = 0.$$ 

If we cancel the second and fourth row and column in $\frac{1}{m}M$, we obtain a matrix in $\mathcal{G}_N$. Using this embedding of $\Gamma_N$ into $\hat{\Gamma}_N$ instead of (5), Lemma 3 gives us the desired form. As the Smith invariants are unique even for all double cosets with respect to $GL_5(\mathbb{Z})$, the result follows.

3 The Hecke algebra for the orthogonal groups $\Gamma_N$ and $\hat{\Gamma}_N$

First, we obtain a kind of multiplicativity in the Hecke algebras.

Lemma 4. Let $N \in \mathbb{N}$ be squarefree and let $l, m \in \mathbb{N}$ be coprime.

a) Given $\frac{1}{l}L, \frac{1}{m}M \in \mathcal{G}_N$ with integral $L, M$, one has

$$\Gamma_N \left( \frac{1}{l}L \right) \Gamma_N \cdot \Gamma_N \left( \frac{1}{m}M \right) \Gamma_N = \Gamma_N \left( \frac{1}{lm}LM \right) \Gamma_N.$$ 

b) Given $\frac{1}{l}L, \frac{1}{m}M \in \mathcal{G}_N$ with integral $L, M$, one has

$$\hat{\Gamma}_N \left( \frac{1}{l}L \right) \hat{\Gamma}_N \cdot \hat{\Gamma}_N \left( \frac{1}{m}M \right) \hat{\Gamma}_N = \hat{\Gamma}_N \left( \frac{1}{lm}LM \right) \hat{\Gamma}_N.$$ 

Proof. The double cosets are uniquely determined by the Smith invariants, which are multiplicative due to [12], Theorem II.5. Hence, only the double coset of $\frac{1}{lm}LM$ can occur in the product. The multiplicity is 1 due to a standard argument (cf. [10], Lemma V(6.1)).

Given a prime $p$, i.e. $p \in \mathbb{P}$, we consider the subgroups

$$\mathcal{G}_{N,p} := \left\{ \frac{1}{p^r}K \in \mathcal{G}_N; \ K \text{ integral, } r \in \mathbb{N}_0 \right\},$$ 

$$\widehat{\mathcal{G}}_{N,p} := \left\{ \frac{1}{p^r}M \in \widehat{\mathcal{G}}_N; \ M \text{ integral, } r \in \mathbb{N}_0 \right\}.$$
**Theorem 2.** If $N \in \mathbb{N}$ is squarefree, the Hecke algebras $\mathcal{H}(\Gamma_N, G_N)$ and $\mathcal{H}(\hat{\Gamma}_N, \hat{G}_N)$ are commutative and coincide with the tensor product of their primary components

$$\bigotimes_p \mathcal{H}(\Gamma_N, G_{N,p}) \text{ resp. } \bigotimes_p \mathcal{H}(\hat{\Gamma}_N, \hat{G}_{N,p}).$$

**Proof.** For $\Gamma_N$ the result is due to [10] in combination with [11]. According to Theorem 1, the mapping $M \mapsto M^{-1}$ is an involution which induces the identity on each double coset. Hence, the Hecke algebra is commutative by virtue of the standard argument (cf. [9], Corollary I(7.2)). The tensor product decomposition is a consequence of Theorem 1 and Lemma 4. □

It follows from [10] and [11] that

$$\mathcal{H}(\Gamma_N, G_{N,p}) = \mathbb{Z} \left[ \Gamma_N \frac{1}{p} \text{diag} (1, p, p^2) \Gamma_N \right].$$

Now we define

$$T_{N,1}(p) : = \hat{\Gamma}_N \frac{1}{p} \text{diag} (1, p, p, p^3) \hat{\Gamma}_N,$$

$$T_{N,2}(p) : = \hat{\Gamma}_N \frac{1}{p} \text{diag} (1, 1, p^2, p^2) \hat{\Gamma}_N.$$

Representatives of the right cosets in these double cosets can be computed from Lemma 2. For instance, the number of right cosets in $T_{N,1}(p)$ is

$$1 + p + p^2 + p^3, \quad \text{if } p \nmid N,$$

$$p + 2p^2 + p^3, \quad \text{if } p | N.$$

**Theorem 3.** Let $N \in \mathbb{N}$ be squarefree and $p$ a prime. The primary component $\mathcal{H}(\hat{\Gamma}_N, \hat{G}_{N,p})$ consists of all polynomials in $T_{N,1}(p), T_{N,2}(p)$, which are algebraically independent. $\mathcal{H}(\hat{\Gamma}_N, \hat{G}_N)$ does not contain any zero-divisors.

**Proof.** Let $\mathcal{H}^{(r)}_{N,p}$, $r \in \mathbb{N}_0$, denote the $\mathbb{Z}$-module spanned by all the double cosets

$$\hat{\Gamma}_N \left( \frac{1}{p^r} M \right) \hat{\Gamma}_N, \quad \frac{1}{p^r} M \in \hat{G}_{N,p}, \quad M \text{ integral}.$$

Hence, we have

$$\mathcal{H}^{(0)}_{N,p} = \mathbb{Z} \hat{\Gamma}_N, \quad \mathcal{H}^{(1)}_{N,p} = \mathbb{Z} \hat{\Gamma}_N + \mathbb{Z} T_{N,1}(p) + \mathbb{Z} T_{N,2}(p)$$

7
due to Theorem 1. Now let
\[ \hat{\Gamma}_N \left( \frac{1}{p^r} M \right) \hat{\Gamma}_N \in H_{N,p}^{(r)} \setminus H_{N,p}^{(r-1)}, \quad r \geq 2. \]

By Theorem 1, we may assume that
\[ M = \text{diag} (1, p^s, p^r, p^{2r-s}, p^{2r}), \quad 0 \leq s \leq r. \]

If \( s \geq 1 \), the \( p \)-rank of this matrix is 1,
\[ L := \text{diag} (1, p^{s-1}, p^{r-1}, p^{2r-2-s}, p^{2r-2}), \]
\[ \hat{\Gamma}_N \left( \frac{1}{p^{r-1}} L \right) \hat{\Gamma}_N \in H_{N,p}^{(r-1)}. \]

The same arguments as in [9], Proposition V(8.1), show that
\[ T_{N,1}(p) \cdot \hat{\Gamma}_N \left( \frac{1}{p^{r-1}} L \right) \hat{\Gamma}_N = \hat{\Gamma}_N \left( \frac{1}{p^r} M \right) \hat{\Gamma}_N + R, \]
where \( R \in H_{N,p}^{(r-1)} \). If \( s = 0 \), let
\[ L := \text{diag} (1, 1, p^{r-1}, p^{2r-2}, p^{2r-2}), \]
\[ \hat{\Gamma}_N \left( \frac{1}{p^{r-1}} L \right) \hat{\Gamma}_N \in H_{N,p}^{(r-1)}. \]

Just as above we conclude that
\[ T_{N,2}(p) \cdot \hat{\Gamma}_N \left( \frac{1}{p^{r-1}} L \right) \hat{\Gamma}_N = \hat{\Gamma}_N \left( \frac{1}{p^r} M \right) \hat{\Gamma}_N + R_1 + R_2, \]
where \( R_1 \in H_{N,p}^{(r-1)} \) and
\[ R_2 \in \sum_{s=1}^{r} \mathbb{Z} \hat{\Gamma}_N \left( \frac{1}{p^s} \text{diag} (1, p^s, p^r, p^{2r-s}, p^{2r}) \right) \hat{\Gamma}_N. \]

Hence, an induction shows that \( T_{N,1}(p), T_{N,2}(p) \) generate \( H(\hat{\Gamma}_N, \hat{G}_{N,p}) \). The number of double cosets in \( H_{N,p}^{(r)} \) is \( \binom{r+2}{2} \) due to Theorem 1. A polynomial \( T_{N,1}(p)^u \cdot T_{N,2}(p)^v \), \( u, v \in \mathbb{N}_0 \), belongs to \( H_{N,p}^{(r)} \) if and only if \( u + v \leq r \). As the number of these polynomials also equals \( \binom{r+2}{2} \), the double cosets \( T_{N,1}(p) \) and \( T_{N,2}(p) \) are algebraically independent. \( \square \)
4 The Hecke algebra for the extended paramodular group $\Sigma^*_N$

The symplectic group of degree 2

$$\text{Sp}_2(\mathbb{R}) := \{M \in \mathbb{R}^{4 \times 4}; \ J[M] = J\}, \ J = \begin{pmatrix} 0 & -E \\ E & 0 \end{pmatrix},$$

acts on the Siegel half-space of degree 2

$$H_2(\mathbb{R}) := \{Z = X + iY \in \mathbb{C}^{2 \times 2}; \ Z = Z', \ Y > 0\}$$

via

$$Z \mapsto M\langle Z \rangle = (AZ + B)(CZ + D)^{-1}, \ M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

The orthogonal group $SO_0(\hat{S}_N; \mathbb{R})$ acts on the orthogonal half-space

$$\mathcal{H}_N := \{z = x + iy = (\tau_1, w, \tau_2)' \in \mathbb{C}^3; \ \text{Im} \tau_1 > 0, \ S_N[y] > 0\}$$

via

$$z \mapsto \tilde{M}\langle z \rangle := \frac{1}{M(z)}(-\frac{1}{2}S_N[z]b + Kz + c),$$

where

$$\tilde{M} = \begin{pmatrix} \alpha & d'S_N & \beta \\ b & K & c \\ \gamma & d'S_N & \delta \end{pmatrix}, \ \tilde{M}\{z\} = -\frac{\gamma}{2}S_N[z] + d'S_Nz + \delta.$$

We consider the bijection between the complex symmetric $2 \times 2$ matrices and $\mathbb{C}^3$

$$\phi_N : \begin{pmatrix} \alpha & \beta \\ \beta & \gamma \end{pmatrix} \mapsto (\alpha, \beta, N\gamma)',$$

which satisfies

$$\phi_N(H_2(\mathbb{R})) = \mathcal{H}_N.$$

There is an isomorphism between $\text{Sp}_2(\mathbb{R})/\{\pm E\}$ and $SO_0(\hat{S}_N; \mathbb{R})$, where $\pm M \mapsto \tilde{M}$, given by

$$\phi_N(M\langle Z \rangle) = \tilde{M}\langle \phi_N(Z) \rangle \text{ for all } Z \in H_2(\mathbb{R})$$

(cf. [4], [11]). Note that (2) and (3) lead to

$$\begin{pmatrix} E & S \\ 0 & E \end{pmatrix} = M_\lambda, \ \lambda = \phi_N(S), \ \bar{J}_N = J^*, \ J_N = \begin{pmatrix} 0 & -I^{-1} \\ I & 0 \end{pmatrix}, \ I = \begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix}.$$
We obtain an explicit form of this isomorphism if we use the abbreviation
\[
\begin{pmatrix}
\alpha & \beta \\
\gamma & \delta
\end{pmatrix}^\sharp
= \begin{pmatrix}
\delta & -\beta \\
-\gamma & \alpha
\end{pmatrix}
\]
for the adjoint matrix, via \(\phi_N(Z) = z\),
\[
\det(CZ + D) = \tilde{M}(z), \ (AZ + B)(CZ + D)^\sharp = \frac{1}{2} S_N[z]b + Kz + c,
\]
where
\[
\gamma = -(\det C)/N, \ d = \phi_N(C^\sharp D)/N, \ \delta = \det D,
\alpha = \det A, \ a = -N\phi_N(A^\sharp B), \ \beta = -N \det B,
\]
\[
b = -\frac{1}{N} \phi_N(AC^\sharp), \ c = \phi_N(BD^\sharp), \ K = (r, s, t),
\phi_N(AZD^\sharp + BZC^\sharp) = \tau_1 r + ws + N\tau_2 t = Kz.
\]
Note that the formulas for the first row of \(\tilde{M}\) may be obtained from the last row of \((\tilde{J}_N \tilde{M}) = \tilde{J}^\ast \tilde{M}\).

Let \(\Sigma_N\) denote the (rational) paramodular group given by all the matrices in \(\text{Sp}_2(\mathbb{Q})\) of the form
\[
\begin{pmatrix}
a_1 & a_2 N & b_1 & b_2 \\
a_3 & a_4 & b_3 & b_4/N \\
c_1 & c_2 N & d_1 & d_2 \\
c_3 N & c_4 N & d_3 N & d_4
\end{pmatrix}, \text{ where } a_i, b_i, c_i, d_i \in \mathbb{Z}.
\]
Note that for \(M \in \Sigma_N\) the matrices
\[
\begin{pmatrix}
a_1 & b_1 \\
c_1 & d_1
\end{pmatrix} \mod N, \ \begin{pmatrix}
a_4 & b_4 \\
c_4 & d_4
\end{pmatrix} \mod N \text{ belong to } \text{SL}_2(\mathbb{Z}/N\mathbb{Z}).
\]
The extended paramodular group \(\Sigma_N^\ast\) is generated by \(\Sigma_N\) and \(W_d, \ d \mid N, \)
where
\[
W_d = \begin{pmatrix}
V_d^{-1} & 0 \\
0 & V_d^\ast r
\end{pmatrix}, \ V_d = \frac{1}{\sqrt{d}} \begin{pmatrix}
\alpha d & \beta N \\
\gamma & \delta d
\end{pmatrix}, \ \alpha, \beta, \gamma, \delta \in \mathbb{Z}, \ \det V_d = 1.
\]
It is a maximal discrete normal extension of \(\Sigma_N\) (cf. [8]). Thus, we obtain

**Lemma 5.** Let \(N \in \mathbb{N}\) be squarefree. Then an isomorphism
\[
\text{Sp}_2(\mathbb{R})/\{\pm E\} \rightarrow \text{SO}_0(\tilde{S}_N; \mathbb{R}), \ \pm M \mapsto \tilde{M},
\]
satisfying $\mathfrak{g}$ is given by (10). This isomorphism maps
\[
G := \left\{ \frac{1}{\sqrt{m}} M \in \text{Sp}_2(\mathbb{R}); \ M \text{ integral}, m \in \mathbb{N} \right\} \text{ onto } \text{SO}_0(\hat{S}_N; \mathbb{Q}),
\]
\[
\Sigma^*_N \text{ onto } \hat{\Gamma}_N,
\]
\[
\Sigma_N \text{ onto } \{ M = (m_{ij}) \in \hat{\Gamma}_N; \ m_{33} \equiv 1 \text{ mod } 2N \},
\]
which is the discriminant kernel in $\hat{\Gamma}_N$.

Proof. Apply [11], Corollary 3. Clearly, the image of $G$ is contained in $\text{SO}_0(\hat{S}_N; \mathbb{Q})$. As the latter group is generated by
\[
M_\lambda, \lambda \in \mathbb{Q}^3, \ J^*, \ \text{diag} (\alpha, 1, 1, 1/\alpha), \ \alpha \in \mathbb{Q}, \ \alpha > 0, \ \hat{K}, \ K \in \text{SO}_0(S_N; \mathbb{Q}),
\]
the surjectivity follows from [11], Theorem 4.

As the groups are isomorphic, this is true for the attached Hecke algebras as well (cf. [9]). Note that for $u, v \in \mathbb{N}$
\[
M = \pm \frac{1}{\sqrt{u^2v}} \text{diag} (1, u, u^2v, uv) \Rightarrow \tilde{M} = \frac{1}{uv} \text{diag} (1, v, u, uv, u^2v).
\]
Thus, we can reformulate Theorem 1 and Lemma 5 as

**Lemma 6.** Let $N \in \mathbb{N}$ be squarefree.

(a) Given $M \in G$, then the double coset $\Sigma_N^* M \Sigma_N^*$ contains a unique representative of the form
\[
\frac{1}{\sqrt{u^2v}} \text{diag} (1, u, u^2v, uv), \ u, v \in \mathbb{N}.
\]

(b) Given $L, M \in G$ such that the common denominators of $L$ and $M$ are coprime, then
\[
\Sigma_N^* L \Sigma_N^* \cdot \Sigma_N^* M \Sigma_N^* = \Sigma_N^* (LM) \Sigma_N^*.
\]

If we define the cases $uv = p, p \in \mathbb{P}$, in (14) as
\[
T_{N,1}^*(p) := \Sigma_N^* \frac{1}{\sqrt{p}} \text{diag} (1, 1, p, p) \Sigma_N^*,
\]
\[
T_{N,2}^*(p) := \Sigma_N^* \frac{1}{p} \text{diag} (1, p, p^2, p) \Sigma_N^*,
\]
the result of Theorem 3 can be reformulated as

**Theorem 4.** Let $N \in \mathbb{N}$ be squarefree. Then the Hecke algebra $\mathcal{H}(\Sigma_N^*, \mathcal{G})$ is commutative, does not contain any zero-divisors, and coincides with the tensor product of its primary components, which are the polynomials over $\mathbb{Z}$ in the algebraically independent elements $T_{N,1}^*(p)$ and $T_{N,2}^*(p)$, $p \in \mathbb{P}$.
5 The Hecke algebra for the paramodular group $\Sigma_N$

As an application, we consider the Hecke algebra with respect to $\Sigma_N$. Note that

$$\Sigma_N W_d \Sigma_N = \Sigma_N W_d = W_d \Sigma_N \text{ for all } d \mid N,$$

(16) $\Sigma_N W_d \Sigma_N \cdot \Sigma_N W_e \Sigma_N = \Sigma_N W_f \Sigma_N$,  \quad f = \frac{de}{\gcd(d, e)^2}, \quad d \mid N, \quad e \mid N.$

Hence, we have for all $M \in G$

(17) $\Sigma^*_N M \Sigma^*_N = \bigcup_{d \mid N, e \mid N} \Sigma_N W_d MW_e \Sigma_N,$

(18) $\Sigma_N W_d MW_e \Sigma_N = \Sigma_N W_d \Sigma_N \cdot \Sigma_N M \Sigma_N \cdot \Sigma_N W_e \Sigma_N.$

If we denote the double cosets with respect to $\Sigma_N$ instead of $\Sigma^*_N$ in (14) by $T_N$, the result is

Corollary 2. Let $N \in \mathbb{N}$ be squarefree. Then the Hecke algebra $H(\Sigma_N, G)$ is generated by the double cosets

$$\Sigma_N, \quad \Sigma_N W_p \Sigma_N (p \in \mathbb{P}, \ p \mid N), \quad T_{N,1}(q), \quad T_{N,2}(q) (q \in \mathbb{P}).$$

If $N > 1$, then $H(\Sigma_N, G)$ fails to be commutative and contains zero-divisors.

Proof. Assume that the Hecke algebra is commutative and that $N > 1$. We may choose

$$V_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 0 & N \\ -1 & 0 \end{pmatrix}.$$

In view of $(\Sigma_N W_N \Sigma_N)^2 = \Sigma_N$ in (16) this yields

$$\Sigma_N W_N MW_N \Sigma_N = \Sigma_N M \Sigma_N,$$

i.e.

(*) $W_N MW_N LM^{-1} \in \Sigma_N$

for some $L \in \Sigma_N$. If we set

$$M = \frac{1}{N} \text{diag}(1, N, N^2, N)$$

then (\ref{eq:18}) yields $L \in \mathbb{Z}^{4 \times 4}$ and the second column belongs to $N\mathbb{Z}^4$. This contradicts $\det L = 1$.

Moreover, note that (16) yields

$$(\Sigma_N W_N \Sigma_N - \Sigma_N) \cdot (\Sigma_N W_N \Sigma_N + \Sigma_N) = 0.$$

\hfill $\square$
It follows from Lemma 6 and (17) that each double coset $\Sigma_N M \Sigma_N$, $M \in G$, contains a representative in block diagonal form

$$\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}, \ AD' = E.$$  \hfill (19)

If we denote by $\nu(M)$ the minimal $m \in \mathbb{N}$ such that $\sqrt{m} M$ is of the form (11), then (16), (18), (19) and Corollary 3 in [10] applied to the $D$-block yield

**Lemma 7.** Let $N \in \mathbb{N}$ be squarefree and $d \in \mathbb{N}$, $d | N$. Then the double coset $\Sigma_N W_d \Sigma_N$ commutes with the double cosets

$$\Sigma_N W_e \Sigma_N, \ e | N, \ \Sigma_N \frac{1}{\sqrt{m}} \text{diag} (1, 1, m) \Sigma_N, \ m \in \mathbb{N}, \ \Sigma_N M \Sigma_N,$$

where $M \in G$ such that $d$ and $\nu(M)$ are coprime.

We write $u | N^\infty$ if the prime divisors of $u$ divide $N$. Given $d | N$ and $u, v \in \mathbb{N}$, let

$$u = u_1 u_2, \ u_1 | d^\infty, \ \gcd(du_1, u_2) = 1.$$  

As we may choose $\alpha, \delta \in du_1 \mathbb{Z}$ and $\beta, \gamma \in u_2 \mathbb{Z}$ in (13), we get

$$W_d \text{diag} (1, u, u^2v, uv) W_d \in \Sigma_N \text{diag} (u_1, u_2, u_1 u_2^2 v, u_1^2 u_2^2 v) \Sigma_N.$$  \hfill (20)

**Lemma 8.** Let $N \in \mathbb{N}$ be squarefree and $M \in G$. Then the double coset $\Sigma_N M \Sigma_N$ possesses a unique representative of the form

$$W_d \frac{1}{\sqrt{u_1^2 u_2^2 v}} \text{diag} (u_1, u_2, u_1 u_2^2 v, u_1^2 u_2^2 v), \ d | N, \ u_1, u_2, v \in \mathbb{N}, \ u_1 | N^\infty, \ \gcd(u_1, u_2) = 1, \ \nu(M) = du_1^2 u_2^2 v.$$

**Proof.** The existence is a consequence of Lemma 6, (17) and (20). For the uniqueness we observe that $u = u_1 u_2, v$ are unique due to Lemma 6 and $d$ in view of $\nu(M) = du_1^2 u_2^2 v$. By virtue of (12), the rank of $\text{diag} (u_1, u_1 u_2^2 v)$ over $\mathbb{Z}/p\mathbb{Z}$ is an invariant of the $\Sigma_N$-double coset for all $p \in \mathbb{P}, p | N$. This yields the uniqueness of $u_1$ and $u_2$. \hfill $\blacksquare$

Next, we derive a general form of multiplicativity.

**Lemma 9.** Let $N \in \mathbb{N}$ be squarefree and $L, M \in G$ such that $\nu(L)$ and $\nu(M)$ are coprime. Then

$$\Sigma_N L \Sigma_N \cdot \Sigma_N M \Sigma_N = \Sigma_N L M \Sigma_N = \Sigma_N M \Sigma_N \cdot \Sigma_N L \Sigma_N.$$
Proof. We choose representatives

\[
L = W_d \sqrt{u_1^2u_2^v} \text{diag} (u_1, u_2, u_1u_2^v, u_1^2u_2^v), \quad u = u_1u_2,
\]

\[
M = W_e \sqrt{r_1^2s} \text{diag} (r_1, r_2, r_1r_2^2s, r_1^2r_2s), \quad r = r_1r_2
\]

in the form of Lemma 8.

First, let \(d = e = 1\). It follows from Lemma 6 that the product consists of double cosets in \(\Sigma^*_NLM\Sigma^*_N\). As \(\sqrt{u_1^2u_2^v}vr_1^2sK\) for all the matrices \(K\) in \(\Sigma_NLM\Sigma_N\) are of the form (11), representatives of the double cosets, which might occur, are given by

\[
1 \sqrt{u_1^2u_2^v}vr_1^2s \text{diag} (t_1, t_2, t_1t_2^vs, t_1t_2vs), \quad t_1 | N^\infty, \gcd(t_1, t_2) = 1, \ t_1t_2 = ur
\]

due to (20). If follows from (12) that for \(U \in \mathbb{Z}^{2 \times 2}\) with \(\det U \equiv 1 \mod N\) the ranks of

\[
\begin{pmatrix}
  u_1 & 0 \\
  0 & u_1u_2^v
\end{pmatrix}U \begin{pmatrix} r_1 & 0 \\
  0 & r_1^2s
\end{pmatrix}
\]

and

\[
\begin{pmatrix}
  t_1 & 0 \\
  0 & t_1t_2vs
\end{pmatrix}
\]

over \(\mathbb{Z}/p\mathbb{Z}\) coincide for all \(p | N\). Thus, we have \(t_1 = u_1r_1\) and \(t_2 = u_2r_2\). The coefficient is 1 due to the standard argument (cf. [9, Lemma V(6.1)].

The case of general \(d\) and \(e\) can then be obtained from (18). Lemma 7 and (16) imply

\[
\Sigma_NLM \cdot \Sigma_NM\Sigma_N = \Sigma_NM\Sigma_N \cdot \Sigma_NLM = \Sigma_NW_{de}K\Sigma_N
\]

for some diagonal matrix \(K\), since \(du^2v\) and \(ev^2s\) are coprime. Thus, the product is a single double coset and we may choose \(ML\) or \(LM\) as a representative.

For a prime \(p\) we define the primary component

\[
\mathbb{G}_p := \{M \in \mathbb{G}; \nu(M) = p^r, \ r \in \mathbb{N}_0\}.
\]

The analog of Theorem 4 is

**Theorem 5.** Let \(N \in \mathbb{N}\) be squarefree. Then the Hecke algebra \(\mathcal{H}(\Sigma_N, \mathbb{G})\) is the tensor product of the primary components \(\mathcal{H}(\Sigma_N, \mathbb{G}_p), p \in \mathbb{P}\). One has

\[
\mathcal{H}(\Sigma_N, \mathbb{G}_p) = \begin{cases}
  \mathbb{Z}[\mathcal{T}_{N,1}(p), \mathcal{T}_{N,2}(p)], & \text{if } p \nmid N, \\
  \mathbb{Z}[\Sigma_NW_p\Sigma_N, \mathcal{T}_{N,1}(p), \mathcal{T}_{N,2}(p)] & \text{if } p | N.
\end{cases}
\]

The primary component \(\mathcal{H}(\Sigma_N, \mathbb{G}_p)\) is commutative if and only if \(p \nmid N\).
Proof. According to Lemma 9 and Corollary 2 the result on the commutativity remains to be proved. If \( p \nmid N \) we may choose the same representatives of the right cosets as in the case \( N = 1 \), where the result follows from the standard case (cf. [1], [2], [3]).

The same calculations as above show that
\[
\Sigma_N W_p \Sigma_N \cdot T_{N,2}(p) \cdot \Sigma_N W_p \Sigma_N = \Sigma_N \frac{1}{p} \text{diag}(1, p, p^2) \Sigma_N,
\]
which is different from \( T_{N,2}(p) \) for \( p \mid N \) due to Lemma 8. Hence we have
\[
\Sigma_N W_p \Sigma_N \cdot T_{N,2}(p) \neq T_{N,2}(p) \cdot \Sigma_N W_p \Sigma_N.
\]

We add a

Remark. a) We have for all \( p \mid N \)
\[
\Sigma_N W_p \Sigma_N \cdot T_{N,1}(p) = T_{N,1}(p) \cdot \Sigma_N W_p \Sigma_N
\]
according to (18). One can prove along the lines of Lemma 9 that
\[
T_{N,1}(p) \cdot T_{N,2}(p) = \alpha T_{N,1}(p) + \beta \Sigma_N \frac{1}{\sqrt{p}} \text{diag}(1, p, p^3, p^2) \Sigma_N
\]
for some \( \alpha, \beta \in \mathbb{N} \). All the double cosets are invariant under \( M \mapsto M^{-1} \).

Hence, the induced anti-homomorphism from [2], Theorem I(7.1), yields
\[
T_{N,1}(p) \cdot T_{N,2}(p) = T_{N,2}(p) \cdot T_{N,1}(p) \quad \text{for all } p \in \mathbb{P}.
\]

b) Considering \( N r^2, r \in \mathbb{N} \), the paramodular group \( \Sigma_{N r^2} \) is conjugate to a subgroup of \( \Sigma_N \) of finite index. The same is true for the orthogonal groups in section 2 and 3.

References

[1] A.N. Andrianov, *Quadratic forms and Hecke operators* (Springer, 1987).

[2] E. Freitag, *Siegelsche Modulfunktionen* (Springer, 1983).
[3] J. Gallenkämper, *Themen der Hecke-Theorie zur orthogonalen Gruppe O*(2, n + 2), PhD thesis (RWTH Aachen, 2017).

[4] V.A. Gritsenko, Arithmetical lifting and its applications, *London Math. Soc. Lect. Notes Ser.* **215** (1995) 103-126.

[5] V.A. Gritsenko and K. Hulek, Commutator coverings of modular threefolds, *Duke Math. J.* **94** (1998) 509-542.

[6] V.A. Gritsenko and K. Hulek, Minimal Siegel modular threefolds, *Math. Proc. Cambridge Phil. Soc.* **123** (1998) 461-485.

[7] T. Hina and T. Sugano, On the local Hecke series of some classical groups over \( \wp \)-adic fields, *J. Math. Soc. Japan* **35** (1983) 133-152.

[8] G. Köhler, Erweiterungsfähigkeit paramodularer Gruppen, *Nachr. Akad. Wiss. Göttingen, II. math.-phys. Kl.* 1967 (1968) 229-238.

[9] A. Krieg, Hecke algebras, *Mem. Am. Math. Soc.* **435** (1990).

[10] A. Krieg, The Hecke algebras for the Fricke groups, *Result. Math.* **34** (1998) 342-358.

[11] A. Krieg, Integral Orthogonal Groups, in *Dynamical Systems, Number Theory and Applications*, ed. T. Hagen, F. Rupp, J. Scheurle (World Scientific, 2016) 177-195.

[12] M. Newman, *Integral Matrices* (Academic Press, 1972).

[13] B. Roberts and R. Schmidt, On modular forms for the paramodular groups. *Automorphic forms and zeta functions*, ed. S. Böcherer et al. (World Scientific, 2006) 334-364.

[14] G. Shimura, *Introduction to the arithmetic theory of automorphic functions* (Iwanami Shoten and Princeton University Press, 1971).

[15] T. Sugano, Jacobi forms and the theta lifting, *Comm. Math. Univ. Sancti Pauli* **44** (1995) 1-58.