Congruence Subgroups and Orthogonal Groups

by

Adrian Hauffe-Waschbüsch and Aloys Krieg

November 2020

We derive explicit isomorphisms between certain congruence subgroups of the Siegel modular group and the Hermitian modular group and the modular group over the Hurwitz quaternions of degree 2 and the discriminant kernels of special orthogonal groups \( SO(2, n), n = 3, 4, 6 \). The proof is based on an application of linear algebra adapted to the number theoretical needs.

**Keywords:** Siegel modular group, Hermitian modular group, modular group over Hurwitz quaternions, congruence subgroup, orthogonal group, discriminant kernel

**Classification:** 11F46, 11F55

---

\(^1\) Adrian Hauffe-Waschbüsch, Lehrstuhl A für Mathematik, RWTH Aachen University, D-52056 Aachen, adrian.hauffe@matha.rwth-aachen.de

\(^2\) Aloys Krieg, Lehrstuhl A für Mathematik, RWTH Aachen University, D-52056 Aachen, krieg@rwth-aachen.de
1 Introduction

In the classical theory modular forms such as theta series are described in the setting of $Sp_n(\mathbb{R})$ (cf. [1]). About 20 years ago Borcherds ([1]) established a product expansion for modular forms on $SO(2, n)$.

It is well-known that there exists an isomorphism between the symplectic group $Sp_{2n}(\mathbb{R})$ resp. the special split unitary group $SU(2, 2; \mathbb{C})$ resp. the quaternionic symplectic group $Sp(2, 2; \mathbb{H})$ and the special orthogonal group $SO(2, n; \mathbb{R})$, $n = 3, 4, 6$. An explicit form based on linear algebra can in the first two cases be found in [6] and [12]. If one is interested in modular forms, it is necessary to adapt this isomorphism to number theoretical needs in order to identify modular forms with respect to discriminant kernels (cf. [14], [13], [15]) with Siegel and Hermitian modular forms with respect to congruence subgroups. This approach can be extended to the quaternions, where the missing determinant leads to particular difficulties.

Given a non-degenerate symmetric even matrix $T \in \mathbb{Z}^{m \times m}$ let

$$SO(T; \mathbb{R}) := \{U \in SL_m(\mathbb{R}); U^\text{tr}TU = T\}$$

denote the attached special orthogonal group. Let $SO_0(T; \mathbb{R})$ stand for the connected component of the identity matrix $I$ and $SO_0(T; \mathbb{Z})$ for the subgroup of integral matrices. The discriminant kernel

$$\mathcal{D}(T; \mathbb{Z}) := \{U \in SO_0(T; \mathbb{Z}); M \in I + \mathbb{Z}^{m \times m}T\}$$

is clearly a normal subgroup of $SO_0(T; \mathbb{Z})$. Given $N \in \mathbb{N}$ we moreover define

$$U(N) \oplus T := \begin{pmatrix} 0 & 0 & N \\ 0 & T & 0 \\ N & 0 & 0 \end{pmatrix}$$

for the orthogonal sum with the rescaled hyperbolic plane.

2 Siegel modular group

Denote by

$$\Gamma_2(\mathbb{Z}) := \{M \in \mathbb{Z}^{4 \times 4}; M^\text{tr}JM = J\}, \quad J = J^{(4)} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad I = I^{(2)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

the Siegel modular group of degree 2. Throughout the paper we will always choose a block decomposition of $M$

\begin{equation}
M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \quad A = (a_{ij}), B = (b_{ij}), C = (c_{ij}), D = (d_{ij}) 2 \times 2 \text{ blocks.}
\end{equation}
Now let
\[ S_0 = U(1) \oplus (-2) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -2 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad S_1 = U(1) \oplus S_0 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & S_0 & 0 \\ 1 & 0 & 0 \end{pmatrix}. \]

We fix a notation for \( \tilde{M} \)
\[ \tilde{M} = \begin{pmatrix} \alpha & a^r S_0 & \beta \\ b & K & c \\ \gamma & d^r S_0 & \delta \end{pmatrix}, \quad \alpha, \beta, \gamma, \delta \in \mathbb{R}. \]

For \( 2 \times 2 \) matrices the adjoint is defined by
\[ \left( \begin{array}{cc} \alpha & \beta \\ \gamma & \delta \end{array} \right)^\# = \left( \begin{array}{cc} \delta & -\beta \\ -\gamma & \alpha \end{array} \right). \]

Denote the symmetric \( 2 \times 2 \) matrices by \( \text{Sym}_2(\mathbb{R}) \) and define
\[ \varphi : \text{Sym}_2(\mathbb{R}) \to \mathbb{R}^3, \quad \left( \begin{array}{cc} \alpha & \beta \\ \beta & \gamma \end{array} \right) \mapsto \left( \begin{array}{c} \alpha \\ \beta \\ \gamma \end{array} \right). \]

Given \( M \in \text{Sp}_2(\mathbb{R}) \) of the form (1) we define \( \tilde{M} \in \mathbb{R}^{5 \times 5} \) in (3) by
\[ \tilde{M} = \begin{pmatrix} a^r & b & c \\ b^r & -\beta & \gamma \\ \gamma & c^r & -\alpha \end{pmatrix}, \]

\[ \alpha = \text{det} A, \quad \beta = -\text{det} B, \quad \gamma = -\text{det} C, \quad \delta = \text{det} D, \]
\[ a = -\varphi(A^t B), \quad b = -\varphi(AC^t), \quad c = \varphi(BD^t), \quad d = \varphi(C^t D). \]

\( K \) is the representative matrix of the endomorphism
\[ f_M : \text{Sym}_2(\mathbb{R}) \to \text{Sym}_2(\mathbb{R}), \quad Z \mapsto AZD^t + BZ^t C^t, \]

with respect to the basis \( \left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right), \left( \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right), \left( \begin{array}{cc} 0 & 0 \\ 0 & 1 \end{array} \right) \).

Our first result is

**Theorem 1.** a) \( \Gamma_2(\mathbb{Z})/\{\pm I\} \) is isomorphic to \( D(S_1; \mathbb{Z}) \) via (3), (7), (8).

b) Given \( N \in \mathbb{N} \) the discriminant kernel \( D(NS_1; \mathbb{Z}) \) is isomorphic to the principal congruence subgroup of level \( N \)
\[ \{ M \in \Gamma_2(\mathbb{Z}); \quad M \equiv \varepsilon I \text{ mod } N, \quad \varepsilon \in \mathbb{Z}, \quad \varepsilon^2 \equiv 1 \text{ mod } N \}/\{\pm I\} \]
via (3), (7), (8).

c) Given \( n, N \in \mathbb{N}, \quad n \mid N \) the mapping (3), (7), (8) is an isomorphism between the
congruence subgroup
\[
\begin{align*}
M &\in \Gamma_2(\mathbb{Z}), \\
\det A &\equiv \det D \equiv 1 \mod N, \ a_{21} \equiv b_{22} \equiv d_{12} \equiv 0 \mod n, \\
c_{11} &\equiv 0 \mod Nn, \ c_{12} \equiv c_{21} \equiv c_{22} \equiv 0 \mod N
\end{align*}
\]

and
\[
FD(U(N) \oplus U(n) \oplus (-2); \mathbb{Z})F^{-1} \subseteq D(S_1; \mathbb{Z}), \quad F = \text{diag (1, 1, 1, n, N)}.
\]

Proof. a) This is the case \(N = 1\) of Lemma 5 in [6].
b) At first (6), (7), (8) show that the image of the principal congruence subgroup is contained in the discriminant kernel. Given \(\tilde{M} \in D(\mathbb{Z})\) of the form (3) part a) yields \(B \equiv C \equiv 0 \mod N\), because \(\det A\) and \(\det D\) are coprime to \(N\) in (7). Now observe (cf. [9], p. 44) that
\[
\pm M_0 = \pm (I \times J) \mapsto \tilde{M}_0 = \begin{pmatrix} -J & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & J \end{pmatrix}, \quad J = J^{(2)}.
\]

If we conjugate by \(M_0\) resp. \(\tilde{M}_0\), the same argument shows that \(M\) is congruent to a diagonal matrix \(\mod N\). The determinantal conditions on the blocks of \(M\) and \(M_0M_0^{-1}\) as well as \(AD^r \equiv I \mod N\) imply
\[
M \equiv \varepsilon I \mod N, \quad \varepsilon \in \mathbb{Z}, \quad \varepsilon^2 \equiv 1 \mod N.
\]
c) The image of the congruence subgroup (9) is contained in (10) by (6), (7), (8). Given \(M \in FD(U(N) \oplus U(n) \oplus (-2); \mathbb{Z})F^{-1}\) we have
\[
\alpha \equiv \delta \equiv 1 \mod N, \quad b, d \equiv 0 \mod N.
\]
We obtain \(C \equiv 0 \mod N\). Now we apply the same procedure to \(\tilde{M}_0M\tilde{M}^{-1}\). This leads to
\[
a_{21} \equiv b_{22} \equiv d_{12} \equiv 0 \mod n.
\]
The determinantal conditions on the \(A\)- and \(D\)-blocks as well as \(AD^r \equiv I \mod n\) imply that all the diagonal entries of \(M\) are congruent to \(\varepsilon \mod n\) for some \(\varepsilon \in \mathbb{Z}\) satisfying \(\varepsilon^2 \equiv 1 \mod n\). From these congruences and the fact that the last entry of \(b = -\varphi(AC^2)\) is divisible by \(Nn\), we get \(c_{11} \equiv 0 \mod Nn\).

Remarks. a) Our definition of a principal congruence subgroup slightly differs from the usual one, given merely by \(\varepsilon = 1\) or \(\varepsilon = \pm 1\) in b) (cf. [8]).
b) It follows from c) that \(D(U(N) \oplus U(1) \oplus (-2); \mathbb{Z})\) is isomorphic to the more familiar congruence subgroup
\[
\{M \in \Gamma_2(\mathbb{Z}); \quad C \equiv 0 \mod N, \ \det A \equiv \det D \equiv 1 \mod N\}.
\]
c) In the language of lattices c) of Theorem 1 refers to the orthogonal group with respect to \( U(N) \oplus U(n) \oplus A_1(-1) \). The case of an arbitrary orthogonal sum with two hyperbolic planes over \( \mathbb{Z} \) can be reduced to Theorem 1 c) by the elementary divisor theorem.

3 Hermitian modular group

Let \( K = \mathbb{Q}(\sqrt{-m}), \ m \in \mathbb{N} \) squarefree, be an imaginary quadratic number field with discriminant \( d_K \) and ring of integers \( \mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega_K \), given by

\[
\begin{align*}
d_K &= \begin{cases} 
-m, & \text{if } m \equiv 3 \mod 4, \\
-4m, & \text{else}.
\end{cases} \\
\omega_K &= \begin{cases} 
(m + \sqrt{-m})/2, & \text{if } m \equiv 3 \mod 4, \\
\sqrt{-m}, & \text{else}.
\end{cases}
\end{align*}
\]

(11)

The Hermitian modular group of degree 2 with respect to \( K \) (cf. [2]) is defined by

\[
\Gamma_2(\mathcal{O}_K) := \{ M \in SL_4(\mathcal{O}_K) ; \ M^{tr}JM = J \}.
\]

In this case we define

\[
S_K = \begin{pmatrix} 2 & 2 \text{Re}(\omega_K) & 2 \text{Re}(\omega_K)^2 \end{pmatrix}, \quad S_0 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -S & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad S_1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & S_0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \in \mathbb{Z}^{6 \times 6}.
\]

(12)

Note that

\[
(Z \times Z)S_K = \begin{cases} Z \times mZ, & \text{if } d_K \text{ is odd,} \\
2Z \times 2mZ, & \text{if } d_K \text{ is even.}
\end{cases}
\]

(13)

In this setting we consider the Hermitian \( 2 \times 2 \) matrices \( \text{Her}_2(\mathbb{C}) \) instead of \( \text{Sym}_2(\mathbb{R}) \) in section 2 and replace (5) by

\[
\varphi : \text{Her}_2(\mathbb{C}) \to \mathbb{R}^4, \quad \begin{pmatrix} \alpha \\ \beta + \gamma \omega_K \\ \delta \end{pmatrix} \mapsto (\alpha, \beta, \gamma, \delta)^{tr}.
\]

(5')

Given \( M \in \Gamma_2(\mathcal{O}_K) \) we define \( \tilde{M} \in \mathcal{D}(S_1;\mathbb{Z}) \) by (3), (6), (7), (8') with the notion of \( \varphi \) from (5') as well as

\[
K \text{ is the representative matrix of the endomorphism}
\]

\[
f_M : \text{Her}_2(\mathbb{C}) \to \text{Her}_2(\mathbb{C}), \quad Z \mapsto AZD^2 + BZ^t C^t,
\]

with respect to the basis \( \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & \omega_K \\ \omega_K & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \).

(8')

If we consider congruences mod \( N \), i.e. \( \mod N \mathcal{O}_K, N \in \mathbb{N} \), the result is

**Theorem 2.** a) \( \Gamma_2(\mathcal{O}_K)/\{\pm I\} \) is isomorphic to \( \mathcal{D}(S_1;\mathbb{Z}) \) via (5'), (6'), (7'), (8').

b) Given \( N \in \mathbb{N} \) the discriminant kernel \( \mathcal{D}(NS_1;\mathbb{Z}) \) is isomorphic to the principal con-
gruence subgroup of level $NO_K$,

$$\{ M \in \Gamma_2(O_K); M \equiv I \mod N, \varepsilon \in \mathbb{Z}, \varepsilon^2 \equiv 1 \mod N \}/\{ \pm I \}$$

via (5'), (6), (7), (8').

c) Given $n, N \in \mathbb{N}, n \mid N$ the mapping due to (5') - (8') is an isomorphism between the congruence subgroup

$$M \in \Gamma_2(O_K); a_{11} \equiv d_{11} \equiv \overline{a}_{22} \equiv \overline{d}_{22} \equiv \varepsilon \mod n, \varepsilon \in O_K, \varepsilon \overline{\varepsilon} \equiv 1 \mod n,$$

$$\det A \equiv \det D \equiv 1 \mod N, a_{21} \equiv b_{22} \equiv d_{12} \equiv 0 \mod n,$$

$$c_{11} \equiv 0 \mod Nn, c_{12} \equiv c_{21} \equiv c_{22} \equiv 0 \mod N$$

(14)

and

$$FD(U(N) \oplus U(n) \oplus (-S_K); \mathbb{Z}) F^{-1} \subseteq D(S_1; \mathbb{Z}), \ F = \text{diag} (1, 1, 1, 1, n, N).$$

Proof. a) This is Theorem 3 in [12].

c) Proceed in the same way as in the proof of Theorem 1 c) and observe that $A \overline{Dr} \equiv I \mod n$, where in this situation

$$\pm M_0 = \pm (I \times J) \mapsto \widetilde{M}_0 = \begin{pmatrix} -J & 0 & 0 \\ 0 & I & 0 \\ 0 & 0 & J \end{pmatrix}, \ I = I^{(2)}, \ J = J^{(2)}.$$

b) Proceed as before. Note that any $M$ in the preimage satisfies

$$M \equiv \text{diag} (\varepsilon, \overline{\varepsilon}, \varepsilon, \overline{\varepsilon}) \mod N, \varepsilon \in O_K, \varepsilon \overline{\varepsilon} \equiv 1 \mod n.$$ 

As $\widetilde{M}$ belongs to the discriminant kernel, we conclude

$$f_M \left( \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right) \equiv \begin{pmatrix} * & \varepsilon^2 \\ \varepsilon^2 & * \end{pmatrix} \mod N \text{ resp. } \mod 2N$$

from (13), hence

$$\varepsilon^2 \equiv 1, \varepsilon \equiv \overline{\varepsilon} \begin{cases} \mod N, & \text{if } d_{K} \text{ is odd} \\ \mod 2N, & \text{if } d_{K} \text{ is even} \end{cases}$$

Thus $\varepsilon$ may be chosen in $\mathbb{Z}$.

In order to obtain congruence subgroups, which contain $Sp_2(\mathbb{Z})$ properly, we need an ideal $\mathcal{I}$ in $O_K$ satisfying $\mathcal{I} = \mathcal{I}$. Thus we consider a squarefree divisor $N \mid d_K$ and the integral ideal $\mathcal{I}_N$ of reduced norm $N$. As $N \mid \omega_K^2$ in (11), we get

$$\mathcal{I}_N = \mathbb{Z}N + \mathbb{Z} \omega_K, \ \mathcal{I}_N^2 = NO_K.$$ (15)
In this case we define

\[ T = \begin{pmatrix} 2N & 2 \text{Re}(\omega_K) \\ 2 \text{Re}(\omega_K) & 2|\omega_K|^2/N \end{pmatrix}. \]  

We observe that

\[ (\mathbb{Z} \times \mathbb{Z})T \begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix} = (N\mathbb{Z} \times \mathbb{Z})S_K. \]  

**Theorem 3.** Given a squarefree divisor \( N \) of \( d_K \) the mapping due to (5') - (8') yields an isomorphism between the principal congruence subgroup \( \mathcal{S} \) \( \mathcal{S} \frac{\mathcal{I}}{\mathcal{I}N} \{ M \in \Gamma_2(\mathcal{O}_K); M \equiv \varepsilon I \mod \mathcal{I}_N, \varepsilon \in \mathbb{Z}, \varepsilon^2 \equiv 1 \mod N \}/\{ \pm I \}

\[ G_N^{-1}D(U(N) \oplus U(N) \oplus (-T); \mathbb{Z})G_N, \ G_N = \text{diag}(1, 1, 1, N, 1, 1). \]  

**Proof.** Note that \( H \in \mathcal{I}_N^{2 \times 2}, H = \overline{H}^r \) satisfies

\[ \varphi(H) \equiv (0, 0, *, 0)^r \mod N \]

because of (15). Using (5') - (8') a verification shows that the images of the matrices in (18) are contained in (19). Any representative of \( \mathcal{O}_K/\mathcal{I}_N \) may be chosen in \( \mathbb{Z} \). Hence we conclude in the same way as in the proof of Theorem 2 that any \( M \) in the preimage of

\[ G_N^{-1}D(U(N) \oplus U(N) \oplus (-T); \mathbb{Z})G_N \cap D(S_1; \mathbb{Z}) \]

satisfies

\[ M \equiv \varepsilon I \mod \mathcal{I}_N, \varepsilon \in \mathbb{Z}, \varepsilon^2 \equiv 1 \mod N. \]

Now start with an arbitrary \( \tilde{M} = (\tilde{m}_{ij}) \in G_N^{-1}D(U(N) \oplus U(N) \oplus (-T); \mathbb{Z})G_N \). It follows from Theorem 3 in [12] that the preimage of \( \tilde{M} \) has the form

\[ W_{\ell}L = L^*W_{\ell}, \ell | d_K \text{ squarefree}, \ L, L^* \in \Gamma_2(\mathcal{O}_K), \]

where \( W_{\ell} \) is an arbitrary matrix in \( (1/\sqrt{\ell})\mathcal{I}_\ell^{4 \times 4} \) satisfying \( W_{\ell}^r JW_{\ell} = J \) and \( \det W_{\ell} = 1 \).

We choose

\[ W_{\ell} = \begin{pmatrix} V_{\ell}^r & 0 \\ 0 & V_{\ell}^{-1} \end{pmatrix}, \ V_{\ell} = \begin{pmatrix} \mu u/\sqrt{\ell} & \nu N\sqrt{\ell} \\ N\sqrt{\ell} & \mu/\sqrt{\ell} \end{pmatrix}, \]

\[ u = \ell + m + \sqrt{-m}, \mu, \nu \in \mathbb{Z}, \mu\mu/\ell - \nu N^2\ell = 1. \]
Now let \( m \equiv 1 \mod 4 \) and \( N' = \gcd(N, m) \). As
\[
\tilde{W}_\ell = \begin{pmatrix} 1 & 0 & 0 \\ 0 & K_\ell & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad K_\ell \equiv \begin{pmatrix} \mu & * & 0 \\ 0 & * & 0 \\ 0 & * & u\pi/\ell \end{pmatrix} \mod N,
\]
the standard procedure shows that \( L' \) is congruent to a diagonal matrix mod \( \mathcal{I}_N \). The special choice of \( W_\ell \) shows that this is also true for \( L \), i.e.
\[
L \equiv \text{diag}(\varepsilon, \delta, \delta, \varepsilon) \mod \mathcal{I}_N, \quad \varepsilon, \delta \in \mathbb{Z}, \quad \varepsilon\delta \equiv 1 \mod N.
\]
This leads to
\[
\tilde{L} \in \text{diag}(1, \varepsilon^2, 1, 1, \delta^2, 1) + \Lambda,
\]
\[
\Lambda = G_N^{-1} \mathbb{Z}^{6 \times 6} \text{ diag}(N, N, 2N', 2mN/N', N, N).
\]
Thus we obtain for \( \tilde{W}_\ell = (\tilde{w}_{ij}) \)
\[
\tilde{w}_{43} = -2\mu - 2\mu m/\ell \equiv 0 \mod 2N'/N,
\]
\[
\tilde{w}_{34} \equiv 2\mu m(m + 1)(m + \ell)/\ell \equiv 0 \mod 2mN/N',
\]
which implies \( \ell \mid m \) by considering odd and even \( N \) separately. Then
\[
\tilde{w}_{44} = 1 - 2\mu m(m + 1)/\ell \equiv 1 \mod 2m/N'
\]
leads to \( \ell \mid N' \). Finally
\[
\tilde{w}_{33} \equiv 1 + 2\mu m(m - 1)/\ell \equiv 1 \mod 2N'
\]
gives \( N'\ell \mid m \) and \( \ell = 1 \), as \( m \) is squarefree. Thus we get \( L \in \Gamma_2(\mathcal{O}_K) \) and the claim follows from the considerations above.

The (simpler) cases \( m \equiv 2, 3 \mod 4 \) are dealt with in the same way. \(\square\)

**Remarks.**

a) If \( d_K \) is even and \( N \mid m \), the choice of another basis shows that
\[
\mathcal{D} \left( U(N) \oplus U(N) \oplus \begin{pmatrix} -2N & 0 \\ 0 & -2m/N \end{pmatrix} ; \mathbb{Z} \right)
\]
is isomorphic to the principal congruence subgroup mod \( \mathcal{I}_N \).

b) If we conjugate by \( \text{diag}(\sqrt{-m}, 1, -1/\sqrt{-m}, 1) \) we see that the principal congruence subgroup mod \( \mathcal{I}_m \) is isomorphic to the discriminant kernel \( \mathcal{D}(U(m) \oplus U(m) \oplus (-S_K) ; \mathbb{Z}) \) via Theorem 2.
4 Quaternionic modular group

In this section we consider the Hamiltonian quaternions
\[ \mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k, \quad k = ij = -ji, \quad i^2 = j^2 = -1. \]

If \( b_1, b_2, b_3, b_4 \) is a basis of \( \mathbb{H} \) over \( \mathbb{R} \), we define
\[ S = (b_\mu \overline{b}_\nu + b_\nu \overline{b}_\mu)_{\nu,\mu}, \quad S_0 = U(1) \oplus (-S), \quad S_1 = U(1) \oplus S_0 \in \mathbb{R}^{8 \times 8}. \]

We replace \( \phi \) in (5) by \( \phi : \text{Her}_2(H) \rightarrow \mathbb{R}^6 \),
\[ (5^*) \]
which describes the coordinates with respect to the basis
\[
\begin{pmatrix}
1 & 0 \\
0 & 0
\end{pmatrix}, \quad \begin{pmatrix}
0 & b_1 \\
\overline{b}_1 & 0
\end{pmatrix}, \quad \begin{pmatrix}
0 & b_2 \\
\overline{b}_2 & 0
\end{pmatrix}, \quad \begin{pmatrix}
0 & b_3 \\
\overline{b}_3 & 0
\end{pmatrix}, \quad \begin{pmatrix}
0 & b_4 \\
\overline{b}_4 & 0
\end{pmatrix}, \quad \begin{pmatrix}
0 & 0 \\
0 & 1
\end{pmatrix}.
\]

If we extend \( \phi \) by \( \mathbb{C} \)-linearity, we obtain a bijection between the quaternionic half-space \( H(2;\mathbb{H}) \) (cf. [9], p. 46) and the orthogonal half-space \( H_S \) (cf. [7], [11]). We compare the action of \( Sp_2(H) := \{ M \in \mathbb{H}^{4 \times 4}; \overline{M}trJM = J \} \) on \( H(2;\mathbb{H}) \) via \( Z \mapsto M\langle Z \rangle = (AZ + B)(CZ + D)^{-1} \) with the action of \( SO_0(S_1;\mathbb{R}) \) on \( H_S \) (cf. [11])
\[ z \mapsto M\{ z \} := \left( -\frac{1}{2} z^r S_0 z \cdot b + Kz + c \right) \cdot (M\{ z \})^{-1}, \]
\[ M\{ z \} := -\frac{1}{2} z^r S_0 z \cdot \gamma + d^r S_0 z + \delta, \]
in the notation of (3).

**Lemma 1.** \( \phi \) induces an isomorphism of the groups
\[ Sp_2(H)/\{ \pm I \} \rightarrow SO_0(S_1;\mathbb{R})/\{ \pm I \}, \quad M \mapsto \pm \tilde{M}, \]
via
\[ \phi(M\langle Z \rangle) = \tilde{M}(\phi(Z)) \quad \text{for all} \quad Z \in H(2;\mathbb{H}). \]

**Proof.** The assertion is verified for standard generators on both sides (cf. [9] Lemma II.1.4, [11]). \( \square \)

Let \( "^\lor" \) stand for the standard embedding \( \mathbb{H} \hookrightarrow \mathbb{C}^{2 \times 2} \) and its extension to matrices (cf. [9] chap. I, §2). Then a verification for the standard generators yields
\[ \left( \tilde{M}(\phi(Z)) \right)^2 = \det(CZ + D)^\lor. \]

Note that the notation of \( X^t \) in (4) over the quaternions only makes sense for \( X = X^{tr} \).
In this case we define
\[ \det X = x_{11}x_{22} - x_{12}x_{21} \] with \( (\det X)^2 = \det X^\vee \).

Now a verification leads to
\[ (6^*) \quad \alpha = \pm \sqrt{\det A^\vee}, \quad \beta = \pm \sqrt{\det B^\vee}, \quad \gamma = \pm \sqrt{\det C^\vee}, \quad \delta = \pm \sqrt{\det D^\vee}, \]
\[ (7^*) \quad a = \pm \varphi(\alpha A^{-1} B), \quad b = \pm \varphi(\gamma AC^{-1}), \quad c = \pm \varphi(\delta BD^{-1}), \quad d = \pm \varphi(\gamma C^{-1} D), \]
if the matrices involved have got rank 2. Note that for instance also
\[ b = \pm \varphi((\alpha CA^{-1})^2), \quad d = \pm \varphi((\delta D^{-1} C)^2) \]
hold. In the sequel \( A \) and \( D \) will always have rank 2 in order to avoid technical difficulties. \( K \) is again the representative matrix of an endomorphism \( f_M \) with respect to the basis above. If \( \det D^\vee \neq 0 \) we have
\[ (8^*) \quad f_M(Z) = \delta AZD^{-1} + BZ^2(D^{-1} C)^2 \delta D^{-1}. \]

Note that \( \delta \neq 0 \) determines all the signs in \((6^*), (7^*)\) and \((8^*)\) uniquely in view of \((21)\).

Now we consider the Hurwitz quaternions
\[ \mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\omega, \quad \omega = \frac{1}{2}(1 + i + j + k), \quad S = \begin{pmatrix} 2 & 0 & 0 & 1 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix}. \]

If \( 0 \neq X \in \mathcal{O}^{2 \times 2} \) let
\[ \rho(X) := \max\{ \ell \in \mathbb{N}; \frac{1}{\ell} X \in \mathcal{O}^{2 \times 2} \}. \]

Moreover we consider the prime ideal \( \wp \) of even quaternions
\[ \wp = \{ a \in \mathcal{O}; \frac{1}{2} a \bar{a} \in 2\mathbb{Z} \} = 2\mathbb{Z} + \mathbb{Z}(1 + i) + \mathbb{Z}(1 + j) + \mathbb{Z}(1 + k). \]

Note that
\[ \mathcal{O}/\wp = \{ \wp, 1 + \wp, \omega + \wp, \overline{\omega} + \wp \} \cong \mathbb{F}_4. \]

**Lemma 2.** If \( X \) is any block among \( A, B, C, D \) of \( M \in \text{Sp}_2(\mathcal{O}) \) with \( \det X^\vee \neq 0 \), then there exist \( U, V \in \text{GL}_2(\mathcal{O}) \) as well as \( m, n \in \mathbb{N} \) such that
\[ UXV = \begin{pmatrix} m & 0 \\ 0 & mn \end{pmatrix} \text{ or } \begin{pmatrix} m(1 + i) & 0 \\ 0 & mn(1 + i) \end{pmatrix}, \]
where \( n \) is odd in the latter case. Moreover one has
\[ a) \ \sqrt{\det X^\vee} \in \mathbb{N}. \]
b) $\sqrt{\det X^\vee X^{-1}} \in \mathcal{O}^{2\times 2}$.

c) $m = \rho(X) = \rho(\sqrt{\det X^\vee X^{-1}})$.

Proof. Let $X = A$ without restriction. Now choose $U, V \in GL_2(\mathcal{O})$ such that $UAV$ is in elementary divisor form (cf. [10]) and consider

$$M^* = \begin{pmatrix} A^* & B^* \\ * & * \end{pmatrix} = \begin{pmatrix} U & 0 \\ 0 & U^{tr-1} \end{pmatrix} M \begin{pmatrix} V & 0 \\ 0 & V^{tr-1} \end{pmatrix}.$$  

Then $A^*B^*tr$ is Hermitian and $(A^*, B^*)$ is the upper $2 \times 4$ block of a matrix in $GL_4(\mathcal{O})$. Hence the determinants $\det Y^\vee$, whenever $Y$ runs through all $2 \times 2$ blocks of $(A^*, B^*)$, are coprime. This leads to the result in view of

$$\sqrt{\det A^\vee V^{-1}A^{-1}U^{-1}} = \begin{pmatrix} mn & 0 \\ 0 & m \end{pmatrix} \text{ or } \begin{pmatrix} mn(1-i) & 0 \\ 0 & m(1-i) \end{pmatrix}. \quad \square$$

Next we want to describe the discriminant kernel. Therefore let

$$\Gamma_2(\mathcal{O}) := \{ M \in Sp_2(\mathcal{O}); \det(M \text{ mod } \wp) \equiv 1 \text{ mod } \wp \}$$

stand for the special modular group, which satisfies

$$Sp_2(\mathcal{O}) = \Gamma_2(\mathcal{O}) \cup (\omega I) \cdot \Gamma_2(\mathcal{O}) \cup (\overline{\omega} I) \cdot \Gamma_2(\mathcal{O}),$$

as well as (cf. [5])

$$\Gamma_2^*(\mathcal{O}) = Sp_2(\mathcal{O}) \cup \left( \frac{1+i}{\sqrt{2}} \right) Sp_2(\mathcal{O}).$$

**Theorem 4.**

a) In (20) the special modular group $\Gamma_2(\mathcal{O})/\{ \pm I \}$ is isomorphic to the discriminant kernel $D(S_1; \mathbb{Z})/\{ \pm I \}$.

b) In (20) the extended modular group $\Gamma_2^*(\mathcal{O})/\{ \pm I \}$ is isomorphic to $SO_0(S_1; \mathbb{Z})/\{ \pm I \}$.

Proof. Verify the inclusions for generators of the groups above (cf. [9] Theorem II.2.3, [5, 11]). Note that $SO(S; \mathbb{Z})$ is a group of order 576, which is described in [5], and use

(22) \((Z \times Z \times Z \times Z)S = (2Z \times 2Z \times 2Z \times Z) \cup (1, 1, 1, 0) + (2Z \times 2Z \times 2Z \times Z). \quad \square\)

Now we are going to describe congruence subgroups of $Sp_2(\mathcal{O})$. Note that the congruence $X \equiv I \text{ mod } N$ in Lemma 2 does not imply $\sqrt{\det X^\vee} \equiv 1 \text{ mod } N$ in general. As an example consider

$$N = 15, \quad X = \text{diag}(1 + 15(20i + 76j + 280k), 1 + 15\omega),$$

$$\sqrt{\det X^\vee} = 67, 721 \equiv 11 \text{ mod } 15.$$  

Therefore we use a variant of the definition of the discriminant kernel.
Corollary 1. Given $N \in \mathbb{N}$, then (20) yields an isomorphism between
\[
\{M \in \Gamma_2(O); M \equiv \varepsilon I \mod N, \varepsilon \in \mathbb{Z}, \varepsilon^2 \equiv 1 \mod N\}/\{\pm I\},
\]
if $N$ is odd, resp.
\[
\{M \in \Gamma_2(O); M \equiv \varepsilon I \mod N, \varepsilon \in \mathbb{Z}, \varepsilon^2 \equiv 1 \mod N, \varepsilon(a_{11}+a_{22}) \equiv \varepsilon^2+1 \mod N\}/\{\pm I\},
\]
if $N$ is even, and
\[
\{\tilde{M} \in SO_0(O_1; \mathbb{Z}); \tilde{M} \equiv \rho I + \mathbb{Z}^{8\times8} N S_1, \rho \in \mathbb{Z} \text{ odd}, \rho^2 \equiv 1 \mod N\}/\{\pm I\}.
\]
(23)

Proof. Note that (23) is contained in $D(S_1; \mathbb{Z})/\{\pm I\}$. Proceed in the same way as in the proof of Theorem 2. Use (6*), (7*), (8*) as well as $\alpha \delta \equiv 1 \mod N$ whenever $\tilde{M}$ is congruent to a diagonal matrix mod $N$. If $M$ is congruent to a diagonal matrix mod $N$, one observes the conditions
\[
a_{11} u \overline{a}_{22} \equiv u \mod N \text{ for all } u \in O
\]
and for $N$ even $a_{11} \overline{a}_{22} - 1 \equiv a_{11} \overline{a}_{22} - i \equiv a_{11} \rho \overline{a}_{22} - j \mod 2N,$

due to (22), which leads to the claim. ☐

The additional condition for even $N$ above, in particular ensures that $\sqrt{\det A^T} \equiv \pm 1 \mod 2^k$, if $N = 2^k N'$ with odd $N'$.

Finally we consider the congruence mod $\varphi$.

Corollary 2. The principal congruence subgroup
\[
\{M \in Sp_2(O); M \equiv \varepsilon I \mod \varphi, \varepsilon = 1, \omega, \overline{\omega}\}/\{\pm I\}
\]
is isomorphic to
\[
D(U(2) \oplus U(2) \oplus (-S); \mathbb{Z})/\{\pm I\}.
\]

Proof. Proceed in the same way as in the proof of Theorem 2. Matrices $M$ in the preimage of $FD(U(2) \oplus U(2) \oplus (-S); \mathbb{Z}) F^{-1}$ satisfy
\[
a_{21} \equiv b_{22} \equiv d_{12} \equiv c_{12} \equiv c_{22} \equiv 0 \mod 2, \ c_{11} \equiv 0 \mod 4
\]
as well as $\det(M \mod \varphi) \equiv 1 \mod \varphi$. Hence the diagonal entries of $M$ are odd quaternions. Thus the diagonal is congruent to
\[
\text{diag}(\varepsilon, \overline{\varepsilon}, \varepsilon, \overline{\varepsilon}) \mod \varphi, \varepsilon = 1, \omega, \overline{\omega}.
\]

Now conjugate by diag $(1+i, 1, \frac{1}{2}(1+i), 1)$. In view of
\[
(1+i)\omega(1+i)^{-1} \in \overline{\varphi} + \varphi
\]
the claim follows. ☐
Remarks. a) All the elementary divisor forms in Lemma 2 actually occur:
\[
\begin{pmatrix}
X & -I \\
I & 0
\end{pmatrix}, \quad X = \text{diag} (m, mn) \text{ or } X = m \begin{pmatrix}
2 & 1 + i \\
1 - i & n + 1
\end{pmatrix}.
\]
b) Clearly one can also consider the other types of discriminant kernels of the form \( D(U(N) \oplus U(n) \oplus (-S); \mathbb{Z}) \) just as in Theorem 2.
c) The case \( SO_0(2, 10) \) was dealt with in the same way as in Theorem 4 in [3].

References

[1] Borcherds, R. Automorphic forms with singularities on Grassmannians. *Invent. Math.*, 132:491–562, 1998.

[2] Braun, H. Hermitian modular functions III. *Ann. Math.*, 53:143–160, 1950.

[3] Dieckmann, C., Krieg, A. and M. Woitalla. The graded ring of modular forms on the Cayley half-space of degree two. *Ramanujan J.*, 48:385–398, 2019.

[4] Freitag, E. *Siegesche Modulfunktionen*, volume 254 of *Grundl. Math. Wiss.* Springer-Verlag, Berlin, 1983.

[5] Freitag, E. and C.F. Hermann. Some modular varieties of low dimension. *Adv. Math.*, 152:203–287, 2000.

[6] Gallenkämper, J. and A. Krieg. The Hecke algebras for the orthogonal group \( SO(2, 3) \) and the paramodular group of degree 2. *Int. J. Number Theory*, 14:2409–2423, 2018.

[7] Gritsenko, V.A. Fourier-Jacobi functions of \( n \) (variables). *J. Sov. Math.*, 53:243–252, 1991.

[8] Klingen, H. Bemerkung über Kongruenzgruppen der Modulgruppe \( n \)-ten Grades. *Arch. Math.*, 10:113–122, 1959.

[9] Krieg, A. *Modular forms on half-spaces of quaternions*, volume 1143 of *Lect. Notes Math.*, Springer-Verlag, Berlin, 1985.

[10] Krieg, A. The elementary divisor theory over the Hurwitz order of integral quaternions. *Linear Multilinear Algebra*, 21:325–344, 1987.

[11] Krieg, A. Integral orthogonal groups. In T. Hagen et al., editors, *Dynamical systems, number theory and applications*, pages 177–195. World Scientific, Hackensack, N.J. edition, 2016.
[12] Krieg, A., Raum, M. and A. Wernz. The maximal discrete extension of the Hermitian modular group. 2019. ArXiv:1910.12466.

[13] Wang, H. and B. Williams. On some free algebras of orthogonal modular forms. 2020. ArXiv:2007.00055.

[14] Wang, H. and B. Williams. Projective spaces as orthogonal modular varieties. 2020. ArXiv:2008.08392.

[15] Williams, B. Two graded rings of Hermitian modular forms. 2020. ArXiv:2001.04154.