# Bollettino Unione Matematica Italiana



Eric Schellhammer


## On the Tits building of paramodular groups


*Bollettino dell'Unione Matematica Italiana, Serie 8*, Vol. **9-B** (2006), n.3, p. 619–643.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_2006_8_9B_3_619_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 2006.

Bollettino U. M. I.
(8) **9**-B (2006), 619-643

# On the Tits Building of Paramodular Groups.

ERIC SCHELLHAMMER

**Sunto.** – *Investighiamo i buildings di Tits dei gruppi paramodulari con o senza struttura di livello canonica, rispettivamente. Questi danno importanti informazioni combinatoriche sul bordo della compattificazione toroidale dello spazio dei moduli delle varietà abeliane non principalmente polarizzate.*
*Diamo una classificazione completa delle rette isotropiche per tutti questi gruppi. Inoltre, per le polarizzazioni square-free, coprime e senza struttura di livello, mostriamo che c'è solo un sottospazio isotropico di dimensione massima.*
*In un lavoro successivo a questo, useremo queste informazioni per dare un risultato di tipo generale per lo spazio dei moduli delle varietà abeliane non principalmente polarizzate con struttura di livello completa.*

**Summary.** – *We investigate the Tits buildings of the paramodular groups with or without canonical level structure, respectively. These give important combinatorical information about the boundary of the toroidal compactification of the moduli spaces of non-principally polarised Abelian varieties.*
*We give a full classification of the isotropic lines for all of these groups. Furthermore, for square-free, coprime polarisations without level structure we show that there is only one top-dimensional isotropic subspace.*
*In a sequel to this paper we will use this information to establish a general type result for the moduli space of non-principally polarised Abelian varieties with full level structure.*

## 1. – Introduction.

We fix $(e_1, \ldots, e_g)$ with $e_i | e_{i+1}$ for all $i = 1, \ldots, g-1$. Let $\Delta := \mathrm{diag}(e_1, \ldots, e_g)$, $\Lambda := \left(\begin{smallmatrix} 0 & \Delta \\ -\Delta & 0 \end{smallmatrix}\right)$. Let $\mathfrak{L} := \mathbb{Z}^{2g} \subset \mathbb{C}^g$ and let $\mathfrak{L}^\vee$ be the lattice dual to $\mathfrak{L}$ with respect to the bilinear form $\langle x, y \rangle := x\Lambda\,{}^t y$, namely

$$\mathfrak{L}^\vee := \{y \in \mathfrak{L} \otimes \mathbb{Q} \big| \forall x \in \mathfrak{L} \ : \ \langle x, y \rangle \in \mathbb{Z}\}.$$

Recall that the paramodular group, respectively the paramodular group with a canonical level structure can be defined as follows:

$$\tilde{\Gamma}_{\mathrm{pol}} := \{M \in \mathrm{SL}(2g, \mathbb{Z}) \big| M\Lambda\,{}^t M = \Lambda\} \quad \text{and}$$
$$\tilde{\Gamma}_{\mathrm{pol}}^{\mathrm{lev}} := \{M \in \tilde{\Gamma}_{\mathrm{pol}} \big| M|_{\mathfrak{L}^\vee/\mathfrak{L}} = \mathrm{id}|_{\mathfrak{L}^\vee/\mathfrak{L}}\}.$$

Their action on the Siegel upper half space $\mathfrak{S}_g$ is given by

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} : \tau \mapsto (A\tau + B\Delta)(C\tau + D\Delta)^{-1}\Delta.$$

The quotient spaces $\mathcal{A}_{\mathrm{pol}} := \mathfrak{S}_g/\tilde{\Gamma}_{\mathrm{pol}}$ and $\mathcal{A}_{\mathrm{pol}}^{\mathrm{lev}} := \mathfrak{S}_g/\tilde{\Gamma}_{\mathrm{pol}}^{\mathrm{lev}}$ are the moduli spaces of Abelian varieties with fixed polarisation of the given type without or with canonical level structure, respectively. It is well known (1) that these groups are conjugate to subgroups of $\mathrm{Sp}(2g, \mathbb{Q})$, namely $\Gamma_{\mathrm{pol}} := R^{-1}\tilde{\Gamma}_{\mathrm{pol}}R$ and $\Gamma_{\mathrm{pol}}^{\mathrm{lev}} := R^{-1}\tilde{\Gamma}_{\mathrm{pol}}^{\mathrm{lev}}R$ where $R := \left(\begin{smallmatrix} 1 & \\ & \Delta \end{smallmatrix}\right)$. The action of these groups on $\mathfrak{S}_g$ is the one induced from $\mathrm{Sp}(2g, \mathbb{Q})$, namely

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} : \tau \mapsto (A\tau + B)(C\tau + D)^{-1},$$

and the respective quotient spaces are isomorphic to $\mathcal{A}_{\mathrm{pol}}$ and $\mathcal{A}_{\mathrm{pol}}^{\mathrm{lev}}$, respectively. All of these groups also act on $\mathbb{Q}^{2g}$ by matrix multiplication from the right.

A subspace $V \subset \mathbb{Q}^{2g}$ is called isotropic if for all $u, v \in V$ we have $\langle u, v\rangle = 0$. The Tits building describes the configurations of the conjugacy classes of these isotropic spaces with respect to the action of the different groups defined above. It provides useful information about the combinatorical structure of the boundary components of toroidal compactifications (2). Instead of considering the whole building we focus on the one- and $g$-dimensional spaces only.

The main results of this paper are the classification of isotropic lines in Corollary 4.2 and Corollary 4.6, and Theorem 5.3, which says that under some conditions there is only one top-dimensional isotropic space.

## 2. – Divisors of vectors.

Let us begin the analysis of the Tits building by the one-dimensional isotropic subspaces of $\mathbb{Q}^{2g}$. Given a polarisation type $(e_1, \ldots, e_g)$, we may chose $e_1 = 1$ without changing the group $\tilde{\Gamma}_{\mathrm{pol}}$.

NOTATION 2.1.

Let $d_i := e_{i+1}/e_i$ for $i = 1, \ldots, g-1$ and define

$$d_{i:j} := \begin{cases} \dfrac{e_{j+1}}{e_i} = \displaystyle\prod_{n=i}^{j} d_n & \text{for } i \leq j \\ 1 & \text{for } i > j \end{cases}.$$

(1) see eg. [HKW, p. 11].
(2) see [AMRT].

Then all $d_i$ are positive integers and the polarisation type is given by $(1, d_1, d_{1:2}, \dots, d_{1:g-1})$. Let $T(s)$ be a function depending on some integer variable $s$. Then we define

$$\gcd\big(T(s)\big)_{s=i}^{j} := \gcd\big(T(i), \dots, T(j)\big) \quad \text{and} \quad T(s_1|s_2) := \gcd\big(T(s_1), T(s_2)\big).$$

DEFINITION 2.2. – *Special polarisation types.*

We call a polarisation type $(1, d_1, \dots, d_{1:g-1})$ *square-free* if all $d_i$ are square-free. If a polarisation type satisfies $\gcd(d_i, d_j) = 1$ for all $i \neq j$ we call it a *coprime polarisation type*.

First of all, we define the divisors $D_i(v)$ of a vector $v \in \mathbb{Z}^{2g}$ for $i = 1, \dots, g-1$. To keep the notation easier, we shall drop the vector $v$ where possible and write $D_i := D_i(v)$.

DEFINITION 2.3. – *Divisors.*

Define the *divisors* $D_i := D_i(v)$ *of a primitive vector* $v \in \mathbb{Z}^{2g}$ recursively:

$$D_i := \gcd\left(d_i, \gcd\Big(\frac{v_{j|g+j}}{D_{j:i-1}}\Big)_{j=1}^{i}\right) \in \mathbb{N}_{>0}.$$

Here, $D_{i:j}$ is defined as a product, analogously to $d_{i:j}$.

DEFINITION 2.4. – *Ideal of lattice and vector.*

For a vector $v \in \mathbb{Z}^{2g}$ let $(v, \mathfrak{L}) := \{\langle v, l\rangle \,|\, l \in \mathfrak{L}\}$ which is an ideal in $\mathbb{Z}$, namely

$$(v, \mathfrak{L}) = (v_1, d_1 v_2, d_{1:2} v_3, \dots, d_{1:g-1} v_g, v_{g+1}, d_1 v_{g+2}, \dots, d_{1:g-1} v_{2g}) \subset \mathbb{Z}.$$

LEMMA 2.5. – *For* $1 \leq k \leq i < g$ *and* $m$ *such that* $\frac{m}{D_{k:i-1}} \in \mathbb{Z}$*, the following equivalence holds:*

$$\frac{m}{D_{k:i-1}} \in \Big(d_i, \frac{(v, \mathfrak{L})}{D_{1:i-1}}\Big) \iff \frac{d_{1:k-1}}{D_{1:k-1}} \frac{m}{D_{k:i-1}} \in \Big(d_i, \frac{(v, \mathfrak{L})}{D_{1:i-1}}\Big). \tag{1}$$

PROOF. – The implication "⇒" is trivial; the other direction can be proved by induction, substituting $m' = d_{k-1} m$. ■

LEMMA 2.6. – *The ideal* $(D_i)$ *can also be given by*

$$(D_i) = \Big(d_i, \frac{(v, \mathfrak{L})}{D_{1:i-1}}\Big).$$

PROOF. – Let $A_i := \big(d_i, \frac{(v,\mathfrak{L})}{D_{1:i-1}}\big)$. We know from the definitions that

$$\begin{aligned} A_i &= \left(d_i, \gcd\Big(\frac{d_{1:j-1}v_{j|g+j}}{D_{1:i-1}}\Big)_{j=1}^{g}\right) \\ &= \left(d_i, \gcd\Big(\frac{d_{1:j-1}v_{j|g+j}}{D_{1:i-1}}\Big)_{j=1}^{i}, d_i\gcd\Big(\frac{d_{1:i-1}d_{i+1:j-1}v_{j|g+j}}{D_{1:i-1}}\Big)_{j=i+1}^{g}\right) \\ &= \left(d_i, \gcd\Big(\frac{d_{1:j-1}}{D_{1:j-1}}\frac{v_{j|g+j}}{D_{j:i-1}}\Big)_{j=1}^{i}\right) \qquad (2) \end{aligned}$$

Since now all terms in (2) are multiples of terms in the definition of $D_i$, we obviously have $A_i \subset (D_i)$. For the other inclusion we apply Lemma 2.5 to every element in (2) to obtain that all terms in the definition of $D_i$ are contained in $A_i$. ∎

COROLLARY 2.7. – *Invariance.*
*The divisors $D_i$ of a vector $v$ are invariant under the action of $\tilde{\Gamma}_{\mathrm{pol}}$ on $\mathbb{Z}^{2g}$.*

PROOF. – Consider the invariance of $(v, \mathfrak{L})$ under the action of $M \in \tilde{\Gamma}_{\mathrm{pol}}$:

$$(vM, \mathfrak{L}) = \{vM\Lambda\,{}^t l \mid l \in \mathbb{Z}^{2g}\} = \{v\Lambda({}^tM)^{-1}\,{}^t l \mid l \in \mathbb{Z}^{2g}\} = \{v\Lambda\,{}^t l \mid l \in \mathbb{Z}^{2g}\} = (v, \mathfrak{L}).$$

This holds because $({}^tM)^{-1}$ is an integer matrix due to $\det(M) = 1$, and $M\Lambda = \Lambda({}^tM)^{-1}$ by the definition of $\tilde{\Gamma}_{\mathrm{pol}}$. The invariance of $D_i$ follows from Lemma 2.6. ∎

REMARK 2.8. – Let us point out that the divisors $D_i$ are not independent and therefore not every possible combination of divisors of the $d_i$ given by the polarisation type can actually occur. E. g. take $g = 3$ and $d_1 = 4, d_2 = 6$ so that we have a polarisation type $(1, 4, 24)$. Now, there is no vector with the divisors $D_1 = D_2 = 2$ because that would mean that

$$D_1 = \gcd(4, v_1, v_4) = 2 \quad \text{and} \qquad (3)$$

$$D_2 = \gcd\Big(6, \frac{v_1}{2}, \frac{v_4}{2}, v_2, v_5\Big) = 2, \qquad (4)$$

where equation (4) clearly shows that 4 divides both $v_1$ and $v_4$, which is a contradiction to (3). The additional restriction on the divisors $D_i$ is the following:

THEOREM 2.9. – *Restrictions on $D_i$.*
*For $1 \le i < j \le g-1$ we have*

$$\gcd\Big(\frac{d_i}{D_i}, D_j\Big) = 1. \qquad (5)$$

*Moreover, any ordered set of positive integers* $\{D_i\} := \{D_1, \ldots, D_{g-1}\}$ *satisfying* $D_i | d_i$ *and condition (5) does occur as set of divisors of a vector* $v \in \mathbb{Z}^{2g}$.

PROOF. – **Necessity:** : Restrictions on $D_i$ For $1 \le i < j \le g-1$ we have

$$\gcd\big(d_i D_i, D_j\big) = 1. \tag{6}$$

Moreover, any ordered set of positive integers $\{D_i\} := \{D_1, , D_{g-1}\}$ satisfying $D_i | d_i$ and condition (6) does occur as set of divisors of a vector $v \in \mathbb{Z}^{2g}$.

**Necessity:** Take $i < j$ and assume $n := \gcd\Big(\frac{d_i}{D_i}, D_j\Big) \neq 1$. Let $p$ be a prime dividing $n$ and denote by $\exp(p; n)$ the maximal integer such that $p^{\exp(p;n)} | n$. Obviously, $\exp(p; n) \geq 1$. Since $D_i | d_i$ we have $\exp(p; D_i) \le \exp(p; d_i)$.

If $\exp(p; D_i) = \exp(p; d_i)$ then $\exp(p; d_i D_i) = 0$ in contradiction to $p|n$. So we have the strict inequality $\exp(p; D_i) < \exp(p; d_i)$.

Since by definition

$$D_i = \gcd\left(d_i, \gcd\Big(\frac{v_{k|g+k}}{D_{k:i-1}}\Big)_{k=1}^{i}\right) \quad \text{the strict inquality implies}$$

$$\exp(p; D_i) = exp\left(p; \gcd\Big(\frac{v_{k|g+k}}{D_{k:i-1}}\Big)_{k=1}^{i}\right) \quad \text{and hence}$$

$$exp\left(p; \gcd\Big(\frac{v_{k|g+k}}{D_{k:i}}\Big)_{k=1}^{i}\right) = 0.$$

Since $j > i$ we have

$$D_j = \gcd\left(d_j, \gcd\Big(\frac{v_{k|g+k}}{D_{k:j-1}}\Big)_{k=1}^{j}\right) \quad | \quad \gcd\Big(\frac{v_{k|g+k}}{D_{k:i}}\Big)_{k=1}^{i}.$$

This leads to

$$0 \le \exp(p; D_j) \le \exp\left(p; \gcd\Big(\frac{v_{k|g+k}}{D_{k:i}}\Big)_{k=1}^{i}\right) = 0$$

which is a contradiction to $p|n$. So, $n = 1$.

**Sufficiency:** Choose integers $D_i$ satisfying the conditions stated in the lemma. Consider the vector

$$v = (D_{1:g-1}, D_{2:g-1}, , D_{g-1}, 1, 0, , 0) \in \mathbb{Z}^{2g}.$$

It is easy to calculate that the divisors $D_i(v)$ are exactly the chosen $D_i$.

This lemma has an interesting consequence:

COROLLARY 2.10. – *Characterising property of* $D_{1:g-1}$ .
*For a given polarisation type* $(1, d_1, \ldots, d_{1:g-1})$*, the value* $D_{1:g-1}(v)$ *determines all the values* $D_i(v)$ *uniquely.*

PROOF. – Let $d_1, \ldots, d_{g-1}$ and $D_{1:g-1}$ be given. Then Theorem 2.9 leads to the following:

$$\gcd\left(\frac{d_1}{D_1}, D_2\right) = \ldots = \gcd\left(\frac{d_1}{D_1}, D_{g-1}\right) = 1 \Longrightarrow \gcd\left(\frac{d_1}{D_1}, D_{2:g-1}\right) = 1$$
$$\Longrightarrow \gcd(d_1, D_{1:g-1}) = D_1$$

so that we can determine $D_1$ from $d_1$ and $D_{1:g-1}$. Divide $D_{1:g-1}$ by $D_1$ to obtain $D_{2:g-1}$ and apply the same lemma. By iterating this method all values $D_i$ are obtained. ■

## 3. – Properties of symplectic matrices.

We now want to investigate divisibility properties of the matrix entries of $M \in \Gamma$ for the different groups $\Gamma$ we defined.

DEFINITION 3.1. – *Triangular polarisation matrices.*
Define the sets of matrices

$$\mathbb{D}(\Delta) := \left\{(s_{ij}) \in \mathbb{Z}^{g\times g} \middle| j < i \Longrightarrow d_{j:i-1} | s_{ij}\right\} \quad \text{and}$$
$$\mathbb{SD}(\Delta) := \mathbb{D}(\Delta) \cap \mathrm{SL}(g, \mathbb{Z}) = \left\{S \in \mathbb{D}(\Delta) \middle| \det(S) = 1\right\}.$$

LEMMA 3.2. – *The set* $\mathbb{D}(\Delta)$ *with the normal matrix operations is a ring with unity. Its subset* $\mathbb{SD}(\Delta)$ *is a multiplicative group.*

PROOF. – It is a straightforward computation to check that $\mathbb{D}(\Delta)$ is indeed a ring with unity.

Since $\mathbb{SD}(\Delta) \subset \mathrm{SL}(g, \mathbb{Z})$ per definition, it is obvious that for any $S \in \mathbb{SD}(\Delta)$ the inverse $T := S^{-1}$ exists, is an integer matrix and has determinant 1. It remains to show that $T = (t_{ij}) \in \mathbb{D}(\Delta)$. By Cramer's rule we know $t_{ij} = \frac{1}{|S|}|S^{(j,i)}| = |S^{(j,i)}|$ where $S^{(j,i)}$ is the minor of $S$ constructed by removing the $j$th row and $i$th column.

For $j \geq i$ there is no additional condition. Now let $j < i$ and fix $n \in \{j, \ldots, i-1\}$. We have to show that $d_n$ divides $\det(S^{(j,i)})$. This is the statement of Lemma 6.1 where we let $d = d_n$ and $k = n$. Using this for all $j \leq n \leq i-1$ we obtain $d_{j:i-1} | t_{ij}$ which completes the proof that $T \in \mathbb{SD}(\Delta)$. ■

LEMMA 3.3. – *We have the following congruence conditions:*

$$\tilde{\Gamma}_{\mathrm{pol}} \subset \mathbb{D}(\Delta)^{2\times 2}$$

*where* $\mathbb{D}(\Delta)^{2\times 2} := \left\{ \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \middle| A, B, C, D \in \mathbb{D}(\Delta) \right\}$.

PROOF. – Let $M = (m_{i,j}) \in \tilde{\Gamma}_{\mathrm{pol}}$ and chose $k \in \{1, \ldots, g-1\}$. Denote the index set

$$I_k := \{k+1, \ldots, g, g+k+1, \ldots, 2g\}.$$

Now chose any $i \in I_k$ and let $v := e_i \in \mathbb{Z}^{2g}$ be the $i$th unit vector. The invariance under the action of $\tilde{\Gamma}_{\mathrm{pol}}$ and some easy computation shows that

$$d_k = D_k(v) = D_k(vM) = \gcd\left(d_k, \frac{m_{i,j}}{D_{j:k-1}}, \frac{m_{i,g+j}}{D_{j:k-1}}\right).$$

This reasoning for all valid combinations of values leads exactly to the divisibility condition for $M \in \mathbb{D}(\Delta)^{2\times 2}$. ■

LEMMA 3.4. – *For the conjugate group we have*

$$\Gamma_{\mathrm{pol}} = \mathrm{Sp}\,(2g, \mathbb{Q}) \cap \begin{pmatrix} \mathbb{D}(\Delta) & \mathbb{D}(\Delta)\Delta \\ \Delta^{-1}\mathbb{D}(\Delta) & \Delta^{-1}\mathbb{D}(\Delta)\Delta \end{pmatrix}.$$

PROOF. – This follows from Lemma 3.3 by conjugating with $R$. ■

For the groups with canonical level structure we obtain additional conditions:

LEMMA 3.5.

$$\tilde{\Gamma}^{\mathrm{lev}}_{\mathrm{pol}} = \left\{ M \in \tilde{\Gamma}_{\mathrm{pol}} \middle| M \in \left( \begin{pmatrix} {}^t\mathfrak{d} \\ {}^t\mathfrak{d} \end{pmatrix} 1_{2g} \right) \otimes \mathbb{Z} + \mathbb{1} \right\}$$

*where* $\mathfrak{d} := (1, d_1, \ldots, d_{1:g-1})$ *and* $1_{2g} := (1, \ldots, 1) \in \mathbb{Z}^{2g}$. *The tensor denotes that each matrix entry of the rank 1 matrix in brackets may be multiplied by an integer* $z_{ij}$.

PROOF. – Denote the obvious basis of $\mathfrak{L} \subset \mathbb{C}^g$ by $\{e_1, \ldots, e_{2g}\}$. Then a basis of the dual lattice $\mathfrak{L}^\vee$ can be given by $\{\frac{1}{d_{1:i-1}} e_{i|g+i}\}_{i=1,\ldots,g}$. By definition, a matrix $M \in \tilde{\Gamma}_{\mathrm{pol}}$ is in $\tilde{\Gamma}^{\mathrm{lev}}_{\mathrm{pol}}$ if and only if it satisfies $M_{\mathfrak{L}^\vee/\mathfrak{L}} = \mathrm{id}_{\mathfrak{L}^\vee/\mathfrak{L}}$. This is satisfied if and only if for all $i = 1, \ldots, g$ we have

$$\frac{1}{d_{1:i-1}} e_{i|g+i} M \equiv_{\mathfrak{L}} \frac{1}{d_{1:i-1}} e_{i|g+i} \iff \frac{1}{d_{1:i-1}} e_{i|g+i}(M - \mathbb{1}) \in \mathbb{Z}^{2g}$$

This means that $d_{1:i-1}$ divides every entry in the $i$th and $g+i$th row of the matrix $M - \mathbb{1}$ which is exactly the condition we wanted to prove. ■

LEMMA 3.6.

$$\Gamma_{\rm pol}^{\rm lev} = \{M \in \Gamma_{\rm pol} | M \in \left(\begin{pmatrix} {}^t\mathfrak{d} \\ {}^t 1_g \end{pmatrix} (1_g, \mathfrak{d})\right) \otimes \mathbb{Z} + \mathbb{1}\}$$

*where again* $\mathfrak{d} := (1, d_1, \dots, d_{1:g-1})$ *and* $1_g := (1, \dots, 1) \in \mathbb{Z}^g$.

PROOF. – This follows directly from Lemma 3.5 by conjugating with $R$. ■

One important result from this lemma is the following observation: Although $\Gamma_{\rm pol}$ may have rational non-integer entries, this is no longer possible for its subgroup $\Gamma_{\rm pol}^{\rm lev}$:

COROLLARY 3.7.

$$\Gamma_{\rm pol}^{\rm lev} \subset \mathrm{Sp}(2g, \mathbb{Z}).$$

PROOF. – With Lemma 3.4 we know $\Gamma_{\rm pol}^{\rm lev} \subset \Gamma_{\rm pol} \subset \mathrm{Sp}\,(2g, \mathbb{Q})$, and since the condition given in Lemma 3.6 implies that all matrix entries must be integers the claim follows immediately. ■

## 4. – Orbits of isotropic lines.

In this section we construct two sets of vectors that are in one-to-one correspondence to the orbits of the group actions of $\tilde{\Gamma}_{\rm pol}$ and $\tilde{\Gamma}_{\rm pol}^{\rm lev}$, respectively.

### 4.1. – *Orbits of isotropic lines under* $\tilde{\Gamma}_{\rm pol}^{\rm lev}$

LEMMA 4.1. – *Orbits of isotropic lines under* $\tilde{\Gamma}_{\rm pol}^{\rm lev}$

(i) *Under the action of* $\tilde{\Gamma}_{\rm pol}^{\rm lev}$, *every vector* $v \in \mathbb{Z}^{2g}$ *can be transformed into*

$$\tilde{v} = (D_{1:g-1}(v), *, \dots, *, 0, *, \dots, *)$$

*where the given 0 is at the* $g + 1$*st place.*

(ii) *Two vectors* $v, w \in \mathbb{Z}^{2g}$ *are conjugate under* $\tilde{\Gamma}_{\rm pol}^{\rm lev}$ *if and only if*

$$D_{1:g-1}(v) = D_{1:g-1}(w) \quad \text{and} \quad \forall i = 1, \dots, 2g : v_i \equiv w_i \bmod D_{1:g-1}.$$

PROOF. – **Part (i):**
Since $v$ is primitive, not all entries $v_i$ are zero. Hence we can assume (if

necessary after a suitable transformation with a matrix in $\tilde{\Gamma}^{\mathrm{lev}}_{\mathrm{pol}}$) that $v_1 \neq 0$. By definition of $D_i$ we know that $\frac{v_{j|g+j}}{D_{j:k}} \in \mathbb{Z}$ for $j \leq k < g$ and so it makes sense to say

$$\gcd\Big(\gcd\Big(\frac{v_{j|g+j}}{D_{j:g-1}}\Big)_{j=1}^{i}, \frac{d_i}{D_i}\Big) \text{ divides } \gcd\Big(\gcd\Big(\frac{v_{j|g+j}}{D_{j:i}}\Big)_{j=1}^{i}, \frac{d_i}{D_i}\Big)$$

where the second gcd is equal to 1, again by definition of $D_i$. Hence, we also have

$$\gcd\Big(\gcd\Big(\frac{v_{j|g+j}}{D_{j:g-1}}\Big)_{j=1}^{i}, \frac{d_i}{D_i}\Big) = 1. \tag{7}$$

Now define

$$I := \Big(\frac{v_{1|g+1}}{D_{1:g-1}}, \frac{d_1}{D_1}\frac{v_{2|g+2}}{D_{2:g-1}}, \dots, \frac{d_1}{D_1}\frac{d_{2:g-1}v_{g|2g}}{D_{2:g-1}}\Big). \tag{8}$$

Using (7) for $i = 1, \dots, g-1$, we may drop the factors $\frac{d_i}{D_i}$ successively to obtain

$$I = \Big(\frac{v_{1|g+1}}{D_{1:g-1}}, \frac{v_{2|g+2}}{D_{2:g-1}}, \dots, \frac{v_{g-1|2g-1}}{D_{g-1}}, v_{g|2g}\Big),$$

and since $\gcd(v_1, \dots, v_{2g}) = 1$ we have $I = (1)$. With 6.2 we can now find $\lambda_i$ such that

$$\Big(\frac{v_1}{D_{1:g-1}}, \frac{v_{g+1}}{D_{1:g-1}} + \sum_{i=2}^{g} \lambda_i \frac{d_{1:i-1}v_i}{D_{1:g-1}} + \sum_{i=2}^{g} \lambda_{g+i}\frac{d_{1:i-1}v_{g+i}}{D_{1:g-1}}\Big) = (1) \quad \text{or equivalently}$$

$$\Big(v_1, v_{g+1} + \sum_{i=2,\dots,g} (\lambda_i d_{1:i-1} v_i + \lambda_{g+i} d_{1:i-1} v_{g+i})\Big) = (D_{1:g-1}).$$

The matrix

$$M := \left(\begin{array}{cccc|cccc} 1 & -\lambda_{g+2} & \dots & -\lambda_{2g} & 0 & \lambda_2 & \dots & \lambda_g \\ & 1 & & & d_1\lambda_2 & & & \\ & & \ddots & & \vdots & & & \\ & & & 1 & d_{1:g-1}\lambda_g & & & \\ \hline & & & & 1 & & & \\ & & & & d_1\lambda_{g+2} & 1 & & \\ & & & & \vdots & & \ddots & \\ & & & & d_{1:g-1}\lambda_{2g} & & & 1 \end{array}\right)$$

is in $\tilde{\Gamma}^{\mathrm{lev}}_{\mathrm{pol}}$ according to Lemma 3.5. The entries of the vector $v' := vM$ satisfy the relation $\gcd(v'_1, v'_{g+1}) = D_{1:g-1}$ by definition of $\lambda_i$. Therefore, there exist $t_1, t_2 \in \mathbb{Z}$ with $t_1 v'_1 + t_2 v'_{g+1} = D_{1:g-1}$, and the matrix $N$ that differs from the unit matrix only in the entries

$$\begin{pmatrix} n_{1,1} & n_{1,g+1} \\ n_{g+1,1} & n_{g+1,g+1} \end{pmatrix} = \begin{pmatrix} t_1 & \frac{-v'_{g+1}}{D_{1:g-1}} \\ t_2 & \frac{v'_1}{D_{1:g-1}} \end{pmatrix} \tag{9}$$

transforms $v'$ into a vector of the form $\tilde{v} = v'N = (D_{1:g-1}, *, \dots, *, 0, *, \dots, *)$.

**Part (ii) – Necessity:** Since the divisors are invariant under the action of $\tilde{\Gamma}_{\text{pol}}^{\text{lev}}$, we must have $D_i(v) = D_i(w)$ for conjugate vectors $v$ and $w$ which obviously implies $D_{1:g-1}(v) = D_{1:g-1}(w)$.

Now, let $M \in \tilde{\Gamma}_{\text{pol}}^{\text{lev}}$ such that $w = vM$ and let $k \in \{1, \dots, 2g\}$. To keep the notation easier we only consider the case $k \leq g$, the other case $g < k \leq 2g$ can be treated similarly. By definition we know that $D_{i:g-1}$ divides $v_i$ and $v_{g+i}$. From Lemma 3.5 we obtain

$$\begin{aligned} w_k &= \sum_{\substack{i=1,\\ i\neq k}}^{g} m_{ik} v_i + \sum_{i=1}^{g} m_{g+i,k} v_{g+i} + m_{kk} v_k \\ &= \sum_{\substack{i=1,\\ i\neq k}}^{g} (D_{1:i-1} m'_{ik} D_{i:g-1} v'_i) + \sum_{i=1}^{g} (D_{1:i-1} m'_{g+i,k} D_{i:g-1} v'_{g+i}) + (d_{1:k-1} n + 1) v_k \\ &\equiv 0 + 0 + d_{1:k-1} n D_{k:g-1} \frac{v_k}{D_{k:g-1}} + v_k \bmod D_{1:g-1} \quad \text{and since } \frac{v_k}{D_{k:g-1}} \in \mathbb{Z} \\ &\equiv v_k \bmod D_{1:g-1}. \end{aligned}$$

**Sufficiency:** Due to part (i) we can assume $v$ and $w$ to be given in the form

$$\begin{aligned} v &= (D_{1:g-1}(v), v_2, \dots, v_g, 0, v_{g+2}, \dots, v_{2g}) \quad \text{and} \\ w &= (D_{1:g-1}(w), w_2, \dots, w_g, 0, w_{g+2}, \dots, w_{2g}), \end{aligned}$$

where $v_1 = w_1$. Let $D_i := D_i(v) = D_i(w)$. Since $v_i \equiv w_i \bmod D_{1:g-1}$, let $n_i$ be defined by

$$w_i = n_i D_{1:g-1} + v_i \quad \text{for} \quad i = 2, \dots, g, g+2, \dots, 2g.$$

The matrix $M$ defined as

$$M := \left(\begin{array}{cccc|cccc} 1 & n_2 & \cdots & n_g & 0 & n_{g+2} & \cdots & n_{2g} \\ & 1 & & & d_{1:1} n_{g+2} & & & \\ & & \ddots & & \vdots & & & \\ & & & 1 & d_{1:g-1} n_{2g} & & & \\ \hline & & & & 1 & & & \\ & & & & -d_{1:1} n_2 & 1 & & \\ & & & & \vdots & & \ddots & \\ & & & & -d_{1:g-1} n_g & & & 1 \end{array}\right) \in \tilde{\Gamma}_{\text{pol}}^{\text{lev}}$$

transforms $v$ into $vM = (D_{1:g-1}, w_2, \ldots, w_g, \overline{v}_{g+1}, w_{g+2}, \ldots, w_{2g})$ where

$$\overline{v}_{g+1} = d_{1:1}n_{g+2}v_2 + \ldots + d_{1:g-1}n_{2g}v_g + 0 - d_{1:1}n_2v_{g+2} - \ldots - d_{1:g-1}n_gv_{2g}.$$

Since $D_{i:g-1}$ divides $v_i$ and $v_{g+i}$ by definition, we know that $D_{1:g-1}$ divides every term of $\overline{v}_{g+1}$ and thus $\gcd(D_{1:g-1}, \overline{v}_{g+1}) = D_{1:g-1}$. This implies that we can find a matrix $N$ as in (9) which transforms $vM$ into $w$ and thus $v$ and $w$ are conjugate under $\tilde{\Gamma}^{\text{lev}}_{\text{pol}}$. ■

COROLLARY 4.2. – *Set of representatives*
*A set of representatives for the orbits of* $\tilde{\Gamma}^{\text{lev}}_{\text{pol}}$ *is given by the vectors*

$$\tilde{v} = (D_{1:g-1}, D_{2:g-1}a_2, D_{3:g-1}a_3, \ldots, a_g, 0, D_{2:g-1}a_{g+2}, D_{3:g-1}a_{g+3}, \ldots, a_{2g})$$

*where* $\{D_i\}$ *runs through the set of all possible divisors as given in Theorem* 2.9 *and*

$$0 \le a_i < D_{1:i-1}, \quad 0 \le a_{g+i} < D_{1:i-1} \quad \text{for } i = 2, \ldots, g.$$

PROOF. – This follows easily from the above Lemma 4.1 considering that by definition $D_{i:g-1}|v_{i|g+i}$, and using Theorem 2.9 for the restrictions on $\{D_i\}$. ■

### 4.2. – *Orbits of isotropic lines under* $\tilde{\Gamma}_{\text{pol}}$.

DEFINITION 4.3. – *Representative vectors for* $\tilde{\Gamma}_{\text{pol}}$.
For $v = (v_1, \ldots, v_{2g}) \in \mathbb{Z}^{2g}$ and $i = 1, \ldots, g$, let

$$\hat{v}_i := \gcd(v_{1|g+1}, \ldots, v_{i|g+i}, d_i v_{i+1|g+i+1}, \ldots, d_{i:g-1}v_{g|2g}) \quad \text{and}$$

$$\hat{v} := (\hat{v}_1, \ldots, \hat{v}_g, 0, \ldots, 0) \in \mathbb{Z}^{2g}.$$

In this form, adjacent entries are related in the following ways:

LEMMA 4.4. – *Properties of* $\hat{v}_i$.
*For all primitive* $v \in \mathbb{Z}^{2g}$, *the* $\hat{v}_i$ *satisfy the following relations:*

(i) $\hat{v}_1 = D_{1:g-1}(v)$ *and* $\hat{v}_g = 1$
(ii) $\forall i = 1, \ldots, g-1 \ : \ \hat{v}_i | d_i\hat{v}_{i+1}$
(iii) $\forall i = 2, \ldots, g \ : \ \hat{v}_i | \hat{v}_{i-1}$
(iv) $\forall i = 2, \ldots, g-1 \ : \ \hat{v}_i = \gcd(\hat{v}_{i-1}, v_{i|g+i}, d_i\hat{v}_{i+1})$.

PROOF. – **Part (i):**
By definition we already know that $D_{1:g-1}|\hat{v}_1$. The definition of $\hat{v}_1$ immediately

gives $(\frac{\hat{v}_1}{D_{1:g-1}}) = I$ with $I$ defined as in equation (8) on page 9. We have already proved that $I = (1)$ and hence we have $\hat{v}_1 = D_{1:g-1}$ as claimed.

Since $v$ is primitive, we have $\hat{v}_g = \gcd(v_1, \ldots, v_{2g}) = 1$.

**Part (ii) and (iii):**

These follow immediately from comparing the elements of the greatest common divisors in the definitions of $\hat{v}_i$ and $\hat{v}_{i+1}$ or $\hat{v}_{i-1}$, respectively.

**Part (iv):**

Define $v_i' := \gcd(\hat{v}_{i-1}, v_{i|g+i}, d_i\hat{v}_{i+1})$. From the definition of $\hat{v}_i$ and parts (iii) and (ii) we see that $\hat{v}_i$ divides $\gcd(\hat{v}_{i-1}, v_{i|g+i}, d_i\hat{v}_{i+1}) = v_i'$. On the other hand, from the definition of $v_i'$ we see that $v_i'$ divides $\gcd(v_{1|g+1}, \ldots, v_{i-1|g+i-1}, v_{i|g+i}, d_i v_{i+1|g+i+1}, \ldots, d_{i:g-1}v_{g|2g}) = \hat{v}_i$. Since both are positive integers, this proves equality. ■

We now show that there is a unique $\hat{v}$ in each orbit.

LEMMA 4.5. – *Orbits of isotropic lines under $\tilde{\Gamma}_{\mathrm{pol}}$.*
*Let $\sim$ denote congruence with respect to the action of $\tilde{\Gamma}_{\mathrm{pol}}$. Then*

(i) $v \sim \hat{v}$.

(i) $v \sim w \iff \hat{v} = \hat{w}$ *(here we have equality, not only congruence)*

PROOF. – **Part (i)**

We prove congruence by giving matrices that transform $v$ into $\hat{v}$ iteratively. In the $i$th step the $i$th component of the vector will become $\hat{v}_i$ whereas the $(g+i)$th component will become zero. The existence of such matrices is shown by induction.

For the first step we refer to Lemma 4.1 where it has already been done using a matrix $M \in \tilde{\Gamma}_{\mathrm{pol}}^{\mathrm{lev}} \subset \tilde{\Gamma}_{\mathrm{pol}}$. For the other steps we shall now construct matrices in a similar way. Assume that we have completed the first $i-1$ steps and hence have a vector of the form

$$v = (\hat{v}_1, \ldots, \hat{v}_{i-1}, v_i, \ldots, v_g, 0, \ldots, 0, v_{g+i}, \ldots, v_{2g}).$$

Lemma 6.2 tells us that we can find $\lambda_j$ such that

$$\gcd\Bigg(v_{g+i}, v_i + \sum_{\substack{j=1,\ldots,g\\ j\neq i}} \lambda_j d_{i:j-1} v_j + \sum_{\substack{j=1,\ldots,g\\ j\neq i}} \lambda_{g+j} d_{i:j-1} v_{g+j}\Bigg)$$
$$= \gcd\big(v_{1|g+1}, \ldots, v_{i|g+i}, d_i v_{i+1|g+i+1}, \ldots, d_{i:g-1} v_{g|2g}\big) = \hat{v}_i.$$

Since $v_{g+1} = \ldots = v_{g+i-1} = 0$ we may obviously choose $\lambda_{g+1} = \ldots = \lambda_{g+i-1} = 0$.

Now we can define the matrix

$$M := \left(\begin{array}{ccccccc|ccccccc}
1 & & & \lambda_1 & & & & * & & & & & & \\
& \ddots & & \vdots & & & & & \ddots & & & & & \\
& & 1 & \lambda_{i-1} & & & & & & * & & & & \\
& & & 1 & & & & & & & 0 & & & \\
& & & d_i\lambda_{i+1} & 1 & & & & & & & 0 & & \\
& & & \vdots & & \ddots & & & & & & & \ddots & \\
& & & d_{1:g-1}\lambda_g & & & 1 & & & & & & & 0 \\
\hline
& & & 0 & & & & 1 & & & & & & \\
& & & \vdots & & & & & \ddots & & & & & \\
& & & 0 & & & & & & 1 & & & & \\
0 & \dots & 0 & 0 & \lambda_{g+i+1} & \dots & \lambda_{2g} & * & \dots & * & 1 & * & \dots & * \\
& & & d_i\lambda_{g+i+1} & & & & & & & & 1 & & \\
& & & \vdots & & & & & & & & & \ddots & \\
& & & d_{i:g-1}\lambda_{2g} & & & & & & & & & & 1
\end{array}\right)$$

Where the $*$ in the upper right quadrant are $\lambda_1 \frac{d_{1:i-1}v_{g+i}}{\hat{v}_1}, \dots, \lambda_{i-1} \frac{d_{i-1}v_{g+1}}{\hat{v}_{i-1}}$ and those in the lower right quadrant are $-d_{1:i-1}\lambda_1, \dots, -d_{i-1}\lambda_{i-1}, 1, -\lambda_{i+1}, \dots, -\lambda_g$ so that $M \in \tilde{\Gamma}_{\mathrm{pol}}$. Define $w := vM$. Then

$$w_j = \begin{cases} \hat{v}_j & \text{for } 1 \leq j < i \\ v_j \pm \lambda_k v_{g+i} & \text{for } i < j \leq g \\ 0 & \text{for } g < j < g+i \\ v_{g+i} & \text{for } j = g+i \\ v_j \pm \lambda_k v_{g+i} & \text{for } g+i < j \leq 2g \end{cases}$$

for the appropriate indices $k$. Furthermore, the definition of $\lambda_j$ guarantees that we have $\gcd(w_i, w_{g+i}) = \hat{v}_i$. This shows that $\hat{w} = \hat{v}$.

We complete the induction step using a matrix $N$ as in (9).

**Part (ii):**

$\Leftarrow$: Using (i), we immediately obtain $v \sim \hat{v} = \hat{w} \sim w$.

$\Rightarrow$: Since we know from part (i) that $v$ is conjugate to $\hat{v}$, we may assume $v$ and $w$ to be of the form $\hat{v}$ and $\hat{w}$, respectively. Since $v \sim w$ there exists a matrix $M \in \tilde{\Gamma}_{\mathrm{pol}}$ such that $w = vM$. We will show that $\hat{v}_j$ divides $\hat{w}_j$ for all $j = 1, \dots, g$.

Fix $j \in \{1, \dots, g\}$. We have

$$\begin{aligned}
\hat{v}_j &= \gcd(v_1, \dots, v_j, d_j v_{j+1}, \dots, d_{j:g-1} v_g) \quad \text{and} \\
\hat{w}_j &= \gcd(w_1, \dots, w_j, d_j w_{j+1}, \dots, d_{j:g-1} w_g) \\
&= \gcd\Big( \sum_{i=1}^{g} m_{i,1} v_i, \dots, \sum_{i=1}^{g} m_{i,j} v_i, d_j \sum_{i=1}^{g} m_{i,j+1} v_i, \dots, d_{j:g-1} \sum_{i=1}^{g} m_{i,g} v_i \Big).
\end{aligned}$$

Consider a single entry in this gcd and denote it by

$$W_k = \begin{cases} \sum_{i=1}^{g} m_{ik} v_i & \text{for } 1 \leq \ k \leq \ j \\ d_{j:k-1} \sum_{i=1}^{g} m_{ik} v_i & \text{for } j < \ k \leq \ g \end{cases}.$$

Lemma 3.3 tells us that $m_{ik} = d_{k:i-1} m'_{ik}$ if $k < i$ and hence we can rewrite this as follows: For $1 \leq k \leq j$ we have

$$W_k = \sum_{i=1}^{k} m_{ik} v_i + \sum_{i=k+1}^{j} (d_{k:i-1} m'_{ik}) v_i + \sum_{i=j+1}^{g} (d_{k:j-1} d_{j:i-1} m'_{ik}) v_i.$$

The summands in the first two sums each contain the factor $v_i$ with $i \leq j$; the summands of the last sum the factors $d_{j:i-1} v_i$ with $i > j$. A similar reasoning holds for $j < k \leq g$. We therefore obtain that each $W_k$ is a multiple of $\gcd(v_1, \ldots, v_j, d_{j:j} v_{j+1}, \ldots, d_{j:g-1} v_g) = \hat{v}_j$ and therefore $\hat{v}_j | \hat{w}_j$.

On the other hand, since $M^{-1} \in \tilde{\Gamma}_{\text{pol}}$ and $v = wM^{-1}$ we now also know that $\hat{w}_j$ divides $\hat{v}_j$ for all $j = 1, \ldots, g$, thus $\hat{v} = \hat{w}$.

COROLLARY 4.6. – *Set of representatives .*
*A set of representatives for the orbits of $\tilde{\Gamma}_{\text{pol}}$ is given by the vectors*

$$\hat{v} = (D_{1:g-1}, D_{2:g-1} a_2, D_{3:g-1} a_3, \ldots, D_{g-1} a_{g-1}, 1, 0, \ldots, 0) \in \mathbb{Z}^{2g}$$

*where $\{D_i\}$ runs through the set of possible divisors as given in Theorem 2.9 and $a_i \geq 0$ with*

$$a_i | \gcd(D_{i-1} a_{i-1}, \frac{d_i}{D_i} a_{i+1}) \quad \text{for } i = 2, \ldots \ , g-1 \tag{10}$$

where we let $a_1 = a_g = 1$.

PROOF. – The vectors $\hat{v}$ defined in Definition 4.3 can indeed be given in the form stated above: The factors $D_{i:g-1}$ must be present because of the divisibility conditions implied by the definition. Define $a_i := \frac{\hat{v}_i}{D_{1:g-1}}$. The values for $a_1$ and $a_g$ follow from Lemma 4.4 part (i). Then Lemma 4.4 part (iv) shows that for $i = 2, \ldots, g-1$ the condition on $a_i$ is required.

The fact that this is indeed a set of representatives follows from the just established Lemma 4.5. ■

COROLLARY 4.7. – *Coprime polarisation types.*
*If the polarisation type is coprime then $a_i = 1$ for all $i = 1, \ldots, g$. In parti-*

*cular, the orbits can be represented by the vectors*

$$\hat{v} = (D_{1:g-1}, 0, \ldots, 0, 1, 0, \ldots, 0)$$

*where all $D_i$ dividing $d_i$ occur without further restriction.*

PROOF. – By induction over $i$ one can use (10) and the coprimality of the polarisation type to prove that for $i = 2, \ldots, g-1$ we have $a_i | \gcd(D_{1:i-1}, a_{i+1})$. Now we can use the fact that $a_g = 1$ which implies recursively that indeed $a_i = 1$ for all $i = g-1, \ldots, 2$. The claim follows from the fact that, according to Corollary 2.10, the value $D_{1:g-1}(v)$ determines all $D_i(v)$ uniquely.

It is obvious that Theorem 2.9 does not imply any restrictions on the $D_i$ in the coprime case. ∎

## 5. – Orbits of isotropic $g$-spaces under $\tilde{\Gamma}_{\mathrm{pol}}$

In this section we only consider types of polarisations that are square-free and coprime. For these polarisation types we prove that $\tilde{\Gamma}_{\mathrm{pol}}$ acts transitively on the $g$-dimensional isotropic subspaces of $\mathbb{Q}^{2g}$.

In order to do this we consider primitive integer vectors $v^1, \ldots, v^g$ that generate an isotropic subspace $h = v^1 \wedge \ldots \wedge v^g \subset \mathbb{Q}^{2g}$. We may restrict the discussion to those sets of vectors that form a $\mathbb{Z}$-basis of $h_{\mathbb{Z}} := h \cap \mathbb{Z}^{2g}$, in other words $h_{\mathbb{Z}} = \bigoplus \mathbb{Z} v^i$. In this case primitivity with respect to $h_{\mathbb{Z}}$ implies primitivity with respect to $\mathbb{Z}^{2g}$.

The main point of the proof is that any $h_{\mathbb{Z}}$ of rank $g$ has a basis satisfying the following property:

$$D_{1:g-1}(v^i) = d_{1:i-1} \quad \text{for all } i = 1, \ldots, g. \tag{11}$$

To construct such a basis we use two basic transformations:

- The operation of $\gamma \in \tilde{\Gamma}_{\mathrm{pol}}$ on all of the $v^i$. Let $\tilde{v}^i := \gamma(v^i)$ for all $i = 1, \ldots, g$. Since the $D_i$ are invariant under the operation of $\tilde{\Gamma}_{\mathrm{pol}}$, we can find a basis of $h$ satisfying property 11 if and only if we can find such a basis of $\tilde{h}$.
- A linear combination of basis vectors of $h$ given as multiplication by a unimodular matrix $A$. Since $A^{-1}$ exists and is an integer matrix, the vectors $v_i$ are linear combinations of the $\tilde{v}_i := v_i A$ and hence the lattice $h_{\mathbb{Z}}$ remains unchanged by this transformation. Additionally, Lemma 6.3 gives the following property: assume that the basis transformation only involves the vectors $i_1, \ldots, i_n$. Then

$$\gcd\big(D_k(\tilde{v}^{i_1}), \ldots, D_k(\tilde{v}^{i_n})\big) = \gcd\big(D_k(v^{i_1}), \ldots, D_k(v^{i_n})\big)$$

  for any $1 \leq k \leq g-1$.

During the proofs, we shall denote the vectors after any transformation by $\tilde{v}_i$ but then, by abuse of notation, relabel them as $v_i$.

In the case $g = 2$, this problem was treated by Friedland and Sankaran in [FS]. The following lemmata are generalizations of the corresponding steps to arbitrary genus.

LEMMA 5.1. – *Fix a square-free, coprime polarisation. Let $h \subset \mathbb{Q}^{2g}$ be an isotropic subspace and $v^1, \dots, v^g$ a $\mathbb{Z}$-basis of $h_{\mathbb{Z}}$. Let $2 \leq n \leq g$ and $1 \leq i_1, \dots, i_n \leq g$ a set of $n$ distinct indices. Then*

$$\gcd\big(D_k(v^{i_1}), \dots, D_k(v^{i_n})\big) = 1 \quad \textit{for all } k \geq\ g - n + 1.$$

PROOF. – Since the order of the vectors is irrelevant for the gcd, we may assume $i_j = j$ for all $j = 1, \dots, n$. The claim of the lemma is obviously implied by the statement

$$m_k := \gcd\big(D_k(v^1), \dots, D_k(v^n)\big) = 1 \quad \text{for } k = g - n + 1 \tag{12}$$

since higher values for $k$ mean smaller values for $n$ and hence we have that a set of fewer $D_k$ is already coprime.

Now, the basic idea of the proof is to show that we can construct a basis vector $w$ with the property that $m_k$ divides every entry. Since basis vectors are primitive, this implies that $m_k = 1$ as claimed.

We shall write the basis vectors as row vectors of a matrix, where $*$ is to stand for any value in $\mathbb{Z}$, $\bullet_k \in m_k\mathbb{Z}$ and $\times \in \mathbb{Z}\backslash m_k\mathbb{Z}$.

**Part I:**

We first bring the basis into a standard form which is given by the following description.

**Claim 1:** Let $g \in \mathbb{N}$ and $n = 2, \dots, g$. Let $q := \lfloor \frac{n+1}{2} \rfloor$ and $j = 1, \dots, q$. Then we can transform the basis $v^1, \dots, v^n$ into the following form:

$$\text{for } 1 \leq\ i \leq\ j-1 : v^i = (\underbrace{*, \dots, *}_{g-j}, \underbrace{0, \dots, 0}_{j-i}, 1, \underbrace{0, \dots, 0}_{i-1}; \underbrace{*, \dots, *}_{g-j}, \underbrace{\bullet_k, \dots, \bullet_k}_{j-i}, \underbrace{0, \dots, 0}_{i})$$

$$\text{for } i = j : v^j = (*, \underbrace{0, \dots, 0}_{g-j-1}, 1, \underbrace{0, \dots, 0}_{j-1}; \underbrace{0, \dots, 0}_{g})$$

$$\text{for } j+1 \leq\ i \leq\ n-j : v^i = (\underbrace{*, \dots, *}_{g-j}, \underbrace{0, \dots, 0}_{j}; 0, \underbrace{*, \dots, *}_{g-j-1}, \underbrace{0, \dots, 0}_{j})$$

$$\text{for } n-j+1 \leq\ i \leq\ n-1 : v^i = (\underbrace{*, \dots, *}_{g-j}, \underbrace{0, \dots, 0}_{j}; 0, \underbrace{*, \dots, *}_{g-j-1}, \underbrace{0, \dots, 0}_{n-i}, \underbrace{\bullet_k, \dots, \bullet_k}_{j-n+i})$$

$$\text{for } i = n : v^n = (\underbrace{*, \dots, *}_{g-j}, \underbrace{0, \dots, 0}_{j}; \underbrace{*, \dots, *}_{g-j}, \underbrace{\bullet_k, \dots, \bullet_k}_{j}).$$

We fix $g$ and prove claim 1 by considering the values $n = 2, \dots, g$ separately, using induction over $j$. For $j = 1$, the first and fourth condition are empty and the second one is implied by Corollary 4.7. We transform the basis such that $v^1$ has the given form. To fulfil conditions three (if $n \geq 3$) and five we proceed as follows:

For $i = 2, \dots, n$ replace $v^i$ by $\tilde{v}^i := v^i - v^i_g v^1$ such that $\tilde{v}^i_g = 0$. Since $v^1 \wedge \dots \wedge v^n$ is an isotropic space, we know that for $i = 2, \dots, n$

$$(13) \qquad 0 = \langle v^1, v^i \rangle = D_{1:g-1}(v^1) v^i_{g+1} + d_{1:g-1} v^i_{2g} \implies v^i_{g+1} = -\frac{d_{1:g-1}}{D_{1:g-1}(v^1)} v^i_{2g}.$$

If all $v^i_{2g} = 0$ we already have a basis satisfying conditions three and five. Otherwise we may assume that $v^n_{2g} \neq 0$. For all $i = 2, \dots, n-1$ where $v^i_{2g} \neq 0$ we fulfil condition three iteratively the following way: there exist integers $\lambda, \mu$ such that $\lambda v^i_{2g} + \mu v^n_{2g} = \gcd(v^i_{2g}, v^n_{2g})$. By replacing

$$\tilde{v}^i := \frac{v^n_{2g}}{\gcd(v^i_{2g}, v^n_{2g})} v^i - \frac{v^i_{2g}}{\gcd(v^i_{2g}, v^n_{2g})} v^n \quad \text{and} \quad \tilde{v}^n := \lambda v^i + \mu v^n$$

we obtain a new basis where $\tilde{v}^i_{2g} = 0$ and due to (13) also $\tilde{v}^i_{g+1} = 0$. Hence, we have achieved that $\tilde{v}^i$ satisfies condition three. Note that $\tilde{v}^n_{2g} = \gcd(v^i_{2g}, v^n_{2g}) \neq 0$ and so we may proceed with the next $i$. For condition five we use the isotropy

$$(14) \qquad 0 = \langle v^1, v^n \rangle = D_{1:g-1}(v^1) v^n_{g+1} + d_{1:g-1} v^n_{2g} \equiv d_{1:g-1} v^n_{2g} \bmod (m_k)^2.$$

From the facts that $\gcd(d_r, m_k) = 1$ for $r \neq k$ and $\gcd(\frac{d_k}{m_k}, m_k) = 1$ since the polarisation type is coprime and square-free, we obtain $m_k | v^n_{2g}$. This completes the proof of condition five for $j = 1$.

Now we continue the induction over $j$ by assuming that claim 1 is true for some $j = 1, \dots, q-1$ and establish it for $j+1$. This is done by essentially the same methods we have used for $j = 1$. Here, we use Corollary 4.7 for genus $g - j$ to find a matrix that transforms $v^{j+1}$ as desired but leaves the entries $g - j + 1, \dots, g, 2g - j + 1, \dots, 2g$ of all vectors unchanged.

**Part II:**

We are now in a position to try and transform the basis such that we obtain a basis vector $w$ having the property that $m_k$ divides every entry of $w$. Recall that this proves the lemma since basis vectors are primitive and hence $m_k$ must be equal to 1.

Because of the entry 1 in the vectors $v^1, \dots, v^q$ where all other vectors have zeroes, it does not make sense to use them in the construction of $w$. The other vectors are such that $m_k$ divides all but the critical entries $v^i_r$ where $k < r < g - q + 1$ or $g + k < r < 2g - q + 1$ either by definition of $m_k$ or by construction of $v^i$. These are exactly $2\delta_n$ entries in each of the $\delta_n + 1$ vectors $v^{q+1}, \dots, v^n$, where $\delta_n := \lfloor \frac{n}{2} \rfloor - 1$.

For $g \leq 3$ we have $n \leq 3$ which gives $\delta_n = 0$. Hence, for this case the proof is complete. To treat higher $g$ we give an explicit construction for $w$. The methods used are basically the ones described before in Part I, but in order to make the proof more accessible we have developed the following short hand notation: First of all, notice that neither the number of critical entries nor that of useful vectors depends on $g$ but only on $\delta_n$; we can therefore work independently of $g$. We use the following methods to transform the basis or to gain information:

$\overset{|i;x|}{\rightsquigarrow}$ We use a matrix $N \in \tilde{\Gamma}_{\text{pol}}$ as in (9) changing the entries in the $x$th column of both halves of each vector. This is done in such a way that $\tilde{v}_i^x = 0$ and $\tilde{v}_i^{g+x} = \gcd(v_i^x, v_i^{g+x})$.

$\overset{(i,j;x)}{\rightsquigarrow}$ We replace the vectors $i$ and $j$ by a linear combination – this is done by multiplication with a unimodular matrix. After the transformation we have $\tilde{v}_i^x = 0$ and $\tilde{v}_j^x = \gcd(v_i^x, v_j^x)$. It is important to note that if $v_i^x$ or $v_j^x$ is $\times$, then so is $\tilde{v}_j^x$.

$\overset{(i)=1}{\rightsquigarrow}$ We use the fact that the $i$th basis vector is primitive to gain $\times$ at some entry.

$\overset{\langle i,j \rangle}{\rightsquigarrow}$ We use the isotropy $\langle v_i, v_j \rangle = 0$ as in 14 to gain $\bullet_k$ at some entry.

$\overset{\vec{i}}{\rightsquigarrow}$ We use Lemma 6.4 on $v_i$. This transformation involves all columns $x$ where $v_i^x$ is not divisible by $m_k$. Since the vector remains primitive, the gcd thus constructed can be written as $\times$. (All its multiples can only be given as $\star$.)

For some steps to be possible we need certain entries of the basis vectors to be non-zero. We assume this to be the case where needed. If these entries would vanish, we could either alter the order of the basis vectors, skip the step in question of even arrive directly at a contradiction proving our claim.

The transformations in the following construction are given in full generality. To illustrate the procedure, we complement it with the matrices for the case $\delta_n = 5$.

$$\left(\begin{array}{ccccc|ccccc} * & * & * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * & * & * \end{array}\right) \overset{|1;1|}{\rightsquigarrow} \cdots \overset{|1;g-1|}{\rightsquigarrow} \left(\begin{array}{ccccc|ccccc} 0 & 0 & 0 & 0 & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * & * & * \end{array}\right)$$

$$\overset{(2,g+1;1)}{\rightsquigarrow} \overset{(3,g+1;1)}{\rightsquigarrow} \cdots \overset{(2,3;g-1)}{\rightsquigarrow} \left(\begin{array}{ccccc|ccccc} 0 & 0 & 0 & 0 & * & * & * & * & * & * \\ 0 & 0 & 0 & 0 & * & * & * & * & * & * \\ 0 & 0 & 0 & * & * & * & * & * & * & * \\ 0 & 0 & * & * & * & * & * & * & * & * \\ 0 & * & * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * & * & * \end{array}\right)$$

$$\overset{(1,2;g+1)}{\rightsquigarrow} \left(\begin{array}{ccccc|ccccc} 0 & 0 & 0 & 0 & * & 0 & * & * & * & * \\ 0 & 0 & 0 & 0 & * & * & * & * & * & * \\ 0 & 0 & 0 & * & * & * & * & * & * & * \\ 0 & 0 & * & * & * & * & * & * & * & * \\ 0 & * & * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * & * & * \end{array}\right) \overset{|1;g|}{\rightsquigarrow} \left(\begin{array}{ccccc|ccccc} 0 & 0 & 0 & 0 & 0 & 0 & * & * & * & * \\ 0 & 0 & 0 & 0 & * & * & * & * & * & * \\ 0 & 0 & 0 & * & * & * & * & * & * & * \\ 0 & 0 & * & * & * & * & * & * & * & * \\ 0 & * & * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * & * & * \end{array}\right)$$

$$\overset{\vec{1}}{\rightsquigarrow}\left(\begin{array}{ccccc|ccccc} 0&0&0&0&0&0&*&*&*&\times\\ 0&*&*&*&*&*&*&*&*&*\\ 0&*&*&*&*&*&*&*&*&*\\ 0&*&*&*&*&*&*&*&*&*\\ 0&*&*&*&*&*&*&*&*&*\\ 0&*&*&*&*&*&*&*&*&* \end{array}\right) \overset{(2,g+1;2)}{\rightsquigarrow}\overset{(3,g+1;2)}{\rightsquigarrow}\cdots\overset{(2,4;g-1)}{\rightsquigarrow}\overset{(3,4;g-1)}{\rightsquigarrow} \left(\begin{array}{ccccc|ccccc} 0&0&0&0&0&0&*&*&*&\times\\ *&0&0&0&*&*&*&*&*&*\\ *&0&0&0&*&*&*&*&*&*\\ *&0&0&*&*&*&*&*&*&*\\ *&0&*&*&*&*&*&*&*&*\\ *&*&*&*&*&*&*&*&*&* \end{array}\right)$$

$$\overset{\langle 1,2\rangle}{\rightsquigarrow}\overset{\langle 1,3\rangle}{\rightsquigarrow}\left(\begin{array}{ccccc|ccccc} 0&0&0&0&0&0&*&*&*&\times\\ *&0&0&0&\bullet_k&*&*&*&*&*\\ *&0&0&0&\bullet_k&*&*&*&*&*\\ *&0&0&*&*&*&*&*&*&*\\ *&0&*&*&*&*&*&*&*&*\\ *&*&*&*&*&*&*&*&*&* \end{array}\right) \overset{(2,3;2g)}{\rightsquigarrow} \left(\begin{array}{ccccc|ccccc} 0&0&0&0&0&0&*&*&*&\times\\ *&0&0&0&\bullet_k&*&*&*&*&0\\ *&0&0&0&\bullet_k&*&*&*&*&*\\ *&0&0&*&*&*&*&*&*&*\\ *&0&*&*&*&*&*&*&*&*\\ *&*&*&*&*&*&*&*&*&* \end{array}\right)$$

$$\overset{|2;1|}{\rightsquigarrow}\left(\begin{array}{ccccc|ccccc} 0&0&0&0&0&0&*&*&*&\times\\ 0&0&0&0&\bullet_k&*&*&*&*&0\\ *&0&0&0&\bullet_k&*&*&*&*&*\\ *&0&0&*&*&*&*&*&*&*\\ *&0&*&*&*&*&*&*&*&*\\ *&*&*&*&*&*&*&*&*&* \end{array}\right)$$

Now repeat the following steps for $i=2,\dots,g-1$:

$$\overset{\vec{i}}{\rightsquigarrow}\left(\begin{array}{ccccc|ccccc} 0&0&0&0&0&0&*&*&*&\times\\ 0&0&0&0&\bullet_k&*&*&*&\times&0\\ *&*&*&*&\bullet_k&*&*&*&*&*\\ *&*&*&*&*&*&*&*&*&*\\ *&*&*&*&*&*&*&*&*&*\\ *&*&*&*&*&*&*&*&*&* \end{array}\right) \overset{(i+1,g+1;1)}{\rightsquigarrow}\cdots\overset{(i+1,i+2;g-i)}{\rightsquigarrow} \left(\begin{array}{ccccc|ccccc} 0&0&0&0&0&*&*&*&*&\times\\ 0&0&0&0&\bullet_k&*&*&*&\times&0\\ 0&0&0&*&*&*&*&*&*&*\\ 0&0&*&*&*&*&*&*&*&*\\ 0&*&*&*&*&*&*&*&*&*\\ *&*&*&*&*&*&*&*&*&* \end{array}\right)$$

$$\overset{\langle i,i+1\rangle}{\rightsquigarrow}\cdots\overset{\langle 1,i+1\rangle}{\rightsquigarrow}\left(\begin{array}{ccccc|ccccc} 0&0&0&0&0&*&*&*&*&\times\\ 0&0&0&0&\bullet_k&*&*&*&\times&0\\ 0&0&0&\bullet_k&\bullet_k&*&*&*&*&*\\ 0&0&*&*&*&*&*&*&*&*\\ 0&*&*&*&*&*&*&*&*&*\\ *&*&*&*&*&*&*&*&*&* \end{array}\right)$$

$$\overset{(i+1,1;2g)}{\rightsquigarrow}\cdots\overset{(i+1,i;2g-(i-1))}{\rightsquigarrow}\left(\begin{array}{ccccc|ccccc} 0&0&0&\bullet_k&\bullet_k&*&*&*&*&\times\\ 0&0&0&\bullet_k&\bullet_k&*&*&*&\times&0\\ 0&0&0&\bullet_k&\bullet_k&*&*&*&0&0\\ 0&0&*&*&*&*&*&*&*&*\\ 0&*&*&*&*&*&*&*&*&*\\ *&*&*&*&*&*&*&*&*&* \end{array}\right)$$

After the repetition we obtain a matrix of the following form:

$$\left(\begin{array}{ccccc|ccccc} 0&\bullet_k&\bullet_k&\bullet_k&\bullet_k&*&*&*&*&\times\\ 0&\bullet_k&\bullet_k&\bullet_k&\bullet_k&*&*&*&\times&0\\ 0&\bullet_k&\bullet_k&\bullet_k&\bullet_k&*&*&\times&0&0\\ 0&\bullet_k&\bullet_k&\bullet_k&\bullet_k&*&\times&0&0&0\\ 0&\bullet_k&\bullet_k&\bullet_k&\bullet_k&*&0&0&0&0\\ *&*&*&*&*&*&*&*&*&* \end{array}\right) \overset{(g)=1}{\rightsquigarrow} \left(\begin{array}{ccccc|ccccc} 0&\bullet_k&\bullet_k&\bullet_k&\bullet_k&*&*&*&*&\times\\ 0&\bullet_k&\bullet_k&\bullet_k&\bullet_k&*&*&*&\times&0\\ 0&\bullet_k&\bullet_k&\bullet_k&\bullet_k&*&*&\times&0&0\\ 0&\bullet_k&\bullet_k&\bullet_k&\bullet_k&*&\times&0&0&0\\ 0&\bullet_k&\bullet_k&\bullet_k&\bullet_k&\times&0&0&0&0\\ *&*&*&*&*&*&*&*&*&* \end{array}\right)$$

$$\overset{\langle g,g+1\rangle}{\rightsquigarrow}\overset{\langle g-1,g+1\rangle}{\rightsquigarrow}\cdots\overset{\langle 1,g+1\rangle}{\rightsquigarrow}\left(\begin{array}{ccccc|ccccc} 0&\bullet_k&\bullet_k&\bullet_k&\bullet_k&*&*&*&*&\times\\ 0&\bullet_k&\bullet_k&\bullet_k&\bullet_k&*&*&*&\times&0\\ 0&\bullet_k&\bullet_k&\bullet_k&\bullet_k&*&*&\times&0&0\\ 0&\bullet_k&\bullet_k&\bullet_k&\bullet_k&*&\times&0&0&0\\ 0&\bullet_k&\bullet_k&\bullet_k&\bullet_k&\times&0&0&0&0\\ \bullet_k&\bullet_k&\bullet_k&\bullet_k&\bullet_k&*&*&*&*&* \end{array}\right)$$

$$\overset{(g+1,1;2g)}{\rightsquigarrow}\overset{(g+1,2;2g-1)}{\rightsquigarrow}\cdots\overset{(g+1,g;g+1)}{\rightsquigarrow}\left(\begin{array}{ccccc|ccccc} \bullet_k&\bullet_k&\bullet_k&\bullet_k&\bullet_k&*&*&*&*&\times\\ \bullet_k&\bullet_k&\bullet_k&\bullet_k&\bullet_k&*&*&*&\times&0\\ \bullet_k&\bullet_k&\bullet_k&\bullet_k&\bullet_k&*&*&\times&0&0\\ \bullet_k&\bullet_k&\bullet_k&\bullet_k&\bullet_k&*&\times&0&0&0\\ \bullet_k&\bullet_k&\bullet_k&\bullet_k&\bullet_k&\times&0&0&0&0\\ \bullet_k&\bullet_k&\bullet_k&\bullet_k&\bullet_k&0&0&0&0&0 \end{array}\right)$$

Now, all entries of the last row vector are divisible by $m_k$ while it is supposed to be a primitive vector, giving the contradiction. ■

LEMMA 5.2. – *Fix a square-free, coprime polarisation. In any rank-n-sublattice $\tilde{h}_{\mathbb{Z}} \subset h_{\mathbb{Z}}$ with $2 \leq n \leq g$ we find a vector $v$ satisfying $D_{g-n+1}(v) = 1$.*

PROOF. – Let $k := g - n + 1$ and denote a basis of $\tilde{h}_Z$ by $\tilde{u}^1, \ldots, \tilde{u}^n$. Let $m := \min\{D_k(u) \big| u \in \tilde{h}_{\mathbb{Z}}\}$. Now, let $\hat{u}^1 \in \tilde{h}_{\mathbb{Z}}$ be a primitive vector with $D_k(\hat{u}^1) = m$. We can obviously always find such a vector. Our aim is to show that $m = 1$. Since $\hat{u}^1$ is primitive, [OR, Kapitel 3, Satz 10] tells us that we can find $\hat{u}^2, \ldots, \hat{u}^n$ such that $\hat{u}^1, \ldots, \hat{u}^n$ is a basis of $\tilde{h}_{\mathbb{Z}}$. According to Corollary 4.7 we can find a transformation $\gamma$ such that in the basis $u^i := \gamma\hat{u}^i$ of $\gamma\tilde{h}_{\mathbb{Z}}$ the $k$th entry of $u^1$ is $u^1_k = D_{k:g-1}(u^1) = mD_{k+1:g-1}(u^1)$. Note that due to the invariance of the divisors we have the equality $m = \min\{D_k(u) \big| u \in \gamma\tilde{h}_{\mathbb{Z}}\}$.

We modify the basis as follows: Let $i = 2, \ldots, n$. If the $k$th entry of $u^i$ is equal to zero, we leave $u^i$ unchanged. Otherwise, we use the transformation previously denoted by $\overset{(1,i;k)}{\rightsquigarrow}$ to obtain $\tilde{u}^i_k = 0$ and $\tilde{u}^1_k = \gcd(u^1_k, u^i_k)$. After repeating this procedure for $i = 2, \ldots, n$ we modify the basis one more time by letting $v^1 := \tilde{u}^1$ and $v^i := \tilde{u}^i + \tilde{u}^1$ for $i \geq 2$, so that now the $k$th entries of all vectors $v^1, \ldots, v^n$ are equal to $\tilde{u}^1_k$.

Since for all $i = 1, \ldots, n$ we know that $D_k(v^i)$ divides $v^i_k = \gcd(u^1_k, \ldots, u^n_k)$ and $d_i$ by definition, we may conclude that $D_k(v^i)$ divides $\gcd(d_k, u^1_k) = \gcd(d_k, mD_{k+1:g-1}(u^1)) = m$ which implies $D_k(v^i) \leq m$.

On the other hand, from the definition of $m$ we know $D_k(v^i) \geq m$ since $v^i \in \gamma\tilde{h}_{\mathbb{Z}}$ and $m$ is minimal. Therefore, $D_k(v^i) = m$ for all $i = 1, \ldots, n$. This shows that, using Lemma 5.1, $m = \gcd\big(D_k(v^1), \ldots, D_k(v^n)\big) = 1$ which shows that $D_k(u^1) = m = 1$ as claimed. ■

THEOREM 5.3. – *Fix a square-free, coprime polarisation. Then $\tilde{\Gamma}_{\text{pol}}$ acts transitively on the g-dimensional isotropic subspaces of $\mathbb{Q}^{2g}$*

PROOF. – Let $e_k$ be the $k$th unit vector. We want to show that, given any $g$-dimensional isotropic subspace $h \subset \mathbb{Q}^{2g}$ we can find a basis $u^1, \ldots, u^g$ of $h_{\mathbb{Z}}$ such that there exists a transformation $\gamma \in \tilde{\Gamma}_{\text{pol}}$ satisfying $\gamma u^i = e^i$ for $i = 1, \ldots, g$. The proof is by induction.

More precisely, we want to show the following for any $k \in \{0, \ldots, g\}$:

**Claim 1:** We can transform the basis $u^1, \ldots, u^g$ of $h_{\mathbb{Z}}$ such that

$$
\begin{aligned}
&u^i = e^i \quad \text{for } i = 1, \ldots, k \text{ and} \\
&u^i = (\underbrace{0, \ldots, 0}_{k}, \underbrace{*, \ldots, *}_{g-k}, \underbrace{0, \ldots, 0}_{k}, \underbrace{*, \ldots, *}_{g-k}) \quad \text{for } i = k+1, \ldots, g.
\end{aligned}
\tag{15}
$$

For $k = 0$ this is trivially true and hence we may use this as start for the induction. Assume that claim 1 is true for some $k \in \{0, \dots, g-2\}$. Denote the isotropic subspace generated by $u^{k+1}, \dots, u^g$ by $\tilde{h}$. Note that we may apply Lemma 5.2 for this subspace without losing property (15): of the basic transformations mentioned at the beginning of this section only the operation of $\gamma \in \tilde{\Gamma}_{\text{pol}}$ could cause problems since it affects all basis vectors simultaneously. However, we may restrict ourselves to using transformations of the form

$$\gamma = \left(\begin{array}{cc|cc} \mathbb{1}_k & & & \\ & A & & B \\ \hline & & \mathbb{1}_k & \\ & C & & D \end{array}\right) \in \tilde{\Gamma}_{\text{pol}} \tag{16}$$

and these leave the property (15) valid. Hence, Lemma 5.2 tells us that we may assume (if necessary after suitable transformations) that the basis $u^{k+1}, \dots, u^g$ of $\tilde{h}_{\mathbb{Z}}$ is such that $D_i(u^i) = 1$ for $i = k+1, \dots, g-1$.

If $k = g-2$, the vector $v := u^{g-1}$ already has the property that $D_{k+1:g-1}(v) = 1$. Otherwise, we let

$$v := \sum_{n=k+1}^{g-1} d^{(n)}_{k+1:g-1} u^n,$$

where $d^{(c)}_{a:b} := d_{a:c-1} d_{c+1:b}$. Since $\gcd(d^{(k+1)}_{k+1:g-1}, \dots, d^{(g-1)}_{k+1:g-1}) = 1$ we see that $v$ is primitive and hence we can find a basis $v^{k+1}, \dots, v^g$ of $\tilde{h}_{\mathbb{Z}}$ where $v^{k+1} = v$. We want to show that $D_{k+1:g-1}(v) = 1$ for $0 \le k < g-1$. Again, we use induction to prove

**Claim 2:** For $j = k, \dots, g-1$ we have $D_{k+1:j}(v) = 1$.

Again, for $j = k$ the claim is trivially true and we have a start for the induction. Assume now that claim 2 is true for some $j \in \{k, \dots, g-2\}$. Then

$$\begin{aligned} D_{j+1}(v) &= \gcd\left(d_{j+1}, \gcd\left(\frac{v_{s|g+s}}{D_{s:j}(v)}\right)_{s=1}^{j+1}\right) \quad \text{and since } v_{1|\,g+1} = \dots = v_{k|\,g+k} = 0, \\ &= \gcd\left(d_{j+1}, \gcd\left(\frac{v_{s|g+s}}{D_{s:j}(v)}\right)_{s=k+1}^{j+1}\right) \end{aligned}$$

By assumption $D_{k+1:j}(v) = 1$, which implies $D_{s:j}(v) = 1$ since $s \ge k+1$. Hence

$$\begin{aligned} &= \gcd\left(d_{j+1}, \gcd\left(v_{s|g+s}\right)_{s=k+1}^{j+1}\right) \\ &= \gcd\left(d_{j+1}, \gcd\left(\sum_{n=k+1}^{g-1} d^{(n)}_{k+1:g-1} u^n_{s|g+s}\right)_{s=k+1}^{j+1}\right) \quad \text{leaving out multiples of } d_{j+1} \\ &= \gcd\left(d_{j+1}, \gcd\left(d^{(j+1)}_{k+1:g-1} u^{j+1}_{s|g+s}\right)_{s=k+1}^{j+1}\right) \quad \text{and coprimality of the } d_i \text{ gives} \\ &= \gcd\left(d_{j+1}, \gcd\left(u^{j+1}_{s|g+s}\right)_{s=k+1}^{j}\right) \end{aligned}$$

and since the polarisation is coprime we have $\gcd(d_{j+1}, D_{1:j}(u^{j+1})) = 1$ and therefore

$$= \gcd\left(d_{j+1}, \gcd\Big(\frac{u^{j+1}_{s|g+s}}{D_{s:j}(u^{j+1})}\Big)_{s=k+1}^{j+1}\right) \quad \text{and since } u^{j+1}_{1|\,g+1} = \ldots = u^{j+1}_{k|\,g+k} = 0,$$

$$= \gcd\left(d_{j+1}, \gcd\Big(\frac{u^{j+1}_{s|g+s}}{D_{s:j}(u^{j+1})}\Big)_{s=1}^{j+1}\right) = D_{j+1}(u^{j+1}) = 1.$$

This shows that claim 2 is true for $j+1$, completing the proof that $D_{k+1:g-1}(v) = 1$ for any $k \in \{0, \ldots, g-1\}$.

Hence, we can find $\gamma \in \tilde{\Gamma}_{\text{pol}}$ of the form (16) such that $\gamma v = e_{k+1}$. Under this operation the basis $v^{k+1}, \ldots, v^g$ of $\tilde{h}_{\mathbb{Z}}$ is transformed into a basis of $\gamma\tilde{h}_{\mathbb{Z}}$ which we shall, by abuse of notation, again denote by $v^{k+1}, \ldots, v^g$. Note that now $v^{k+1} = e_{k+1}$. Since $\gamma\tilde{h}$ is again an isotropic subspace, we have for $j = k+2, \ldots, g$:

$$0 = \langle v^{k+1}, v^j\rangle = d_{1:k} \cdot 1 \cdot v^j_{g+k+1} \quad \Longrightarrow \quad v^j_{g+k+1} = 0. \tag{17}$$

Thus, we obtain a basis $\tilde{u}^{k+1} := v^{k+1}, \tilde{u}^i := v^i - v^i_{k+1}v^{k+1}$ satisfying claim 1 for $k+1$. This completes the induction.

Now that we have reached (15) for $k = g-1$ it is easy to see that we only need one more transformation of the form (16) (where the matrices $A$ to $D$ are just integers) to prove claim 1 for $k = g$.

Since we have now shown that for any $g$-dimensional isotropic subspace $h$ we can find a basis of $h_{\mathbb{Z}}$ that can be transformed into $e_1, \ldots, e_g$ by the action of an element in $\tilde{\Gamma}_{\text{pol}}$, we have proved the transitivity of the group action. Note that this basis indeed satisfies property (11). ■

## 6. – Appendix: Technical lemmata

LEMMA 6.1. – *Let $g, d \in \mathbb{N}$ and $A = (a_{ij}) \in \mathbb{Z}^{g\times g}$. If there exists $k \in \{1, \ldots, g\}$ such that for all $i, j$ satisfying $1 \le j \le k \le i \le g$ we have $d|a_{ij}$, then $d|\det(A)$.*

PROOF. – For $g = 1$ the claim is trivial. The induction follows easily by developing along the $k$th column, since either $d|a_{i,k}$ or the assumption gives $d|\det(A^{(i,k)})$. ■

LEMMA 6.2. – *Let $x_1, x_2$ and $y_1, \ldots, y_i$ be integers with $x_1 \neq 0$ and $\gcd(x_1, x_2, y_1, \ldots, y_i) = d \in \mathbb{N}$. Then there exist integers $a_1, \ldots, a_i \in \mathbb{Z}$ such that $\gcd(x_1, x_2 + a_1y_1 + \ldots + a_iy_i) = d$.*

PROOF. – This is a fairly straightforward generalisation of [HKW, Part I, Lemma 3.35]. ■

LEMMA 6.3. – *Assume we are given a coprime polarisation type, vectors* $v^1, \ldots, v^n \in \mathbb{Z}^{2g}$ *and a unimodular integer matrix* $A$. *Consider the basis transformation* $U := AV$ *where* $u_i$ *and* $v_i$ *are the row vectors of* $U$ *and* $V$, *respectively. Then*

$$\gcd\big(D_k(u^1), \ldots, D_k(u^n)\big) = \gcd\big(D_k(v^1), \ldots, D_k(v^n)\big)$$

*for any* $1 \leq k \leq g-1$.

PROOF. – Assume the notation $A = (a_{il})$. The $j$th entry of the $i$th vector is given by $u_j^i = \sum_{l=1}^n a_{il} v_j^l$ and hence $\gcd(v_j^l)_{l=1}^n$ divides $u_j^i$ for all $i$. Since the polarisation type is coprime we have $\gcd(d_k, D_r(u^i)) = 1$ for $r \neq k$ which implies $D_k(u^i) = \gcd\big(d_k, \gcd(u^i_{j|g+j})_{j=1}^k\big)$ and so

$$\begin{aligned} \gcd\big(D_k(v^s)\big)_{s=1}^n &= \gcd\Big(d_k, \gcd\Big(\gcd\big(v^i_{j|g+j}\big)_{j=1}^k\Big)_{i=1}^n\Big) \\ &= \gcd\Bigg(d_k, \gcd\Big(\gcd\big(v^i_{j|g+j}\big)_{i=1}^n\Big)_{j=1}^k\Bigg) \quad \text{which divides} \\ &\gcd\Big(d_k, \gcd\Big(\gcd\big(u^i_{j|g+j}\big)_{j=1}^k\Big)_{i=1}^n\Big) = \gcd\big(D_k(u^s)\big)_{s=1}^n. \end{aligned}$$

Since $A^{-1}$ is also a unimodular integer matrix we also obtain divisibility in the other direction, and since both numbers are positive integers this implies equality. ■

LEMMA 6.4. – *Assume* $g \geq 2$ *with any polarisation type and* $v = (v_1, \ldots, v_g, 0, \ldots, 0) \in \mathbb{Z}^{2g}$. *Then there exists a matrix* $M \in \tilde{\Gamma}_{\text{pol}}$ *such that for* $u = (u_1, \ldots, u_{2g}) := vM \in \mathbb{Z}^{2g}$ *we have* $u_g = \gcd(v_1, \ldots, v_g)$. *Furthermore,* $M$ *can be chosen such that it is an automorphism of the sublattices* $\mathbb{Z}^g \times \{0\}^g \subset \mathbb{Z}^{2g}$ *and* $\{0\}^g \times \mathbb{Z}^g \subset \mathbb{Z}^{2g}$.

*If we choose a set of indices* $1 \leq i_1 < \ldots < i_n \leq g$ *then there exists* $M \in \tilde{\Gamma}_{\text{pol}}$ *such that* $u_{i_n} = \gcd(v_{i_1}, \ldots, v_{i_n})$ *and* $M$ *is an automorphism of the sublattices* $\bigoplus_j e_{i_j}\mathbb{Z}$ *and* $\bigoplus_j e_{g+i_j}\mathbb{Z}$ *where* $e_{i_j}$ *is the* $i_j$*th unit vector.*

PROOF. – **Claim 1:**

Assume $a, b, d \in \mathbb{Z}$ given. Let $\Delta = \text{diag}(1, d)$. Then there exists a matrix $G \in \mathbb{SD}(\Delta)$ such that $(a, b)G = (u, v)$ with $v = \gcd(a, b)$.

We prove this as follows: denote $x := \gcd(a, b)$. Then there exist integers $\alpha, \beta \in \mathbb{Z}$ such that $\alpha a + \beta b = x$. Chose $t$ to be the product of all primes dividing $d$ but not dividing $\beta$. Then it can easily be seen that $\gcd\big(\beta - t\frac{a}{x}, d(\alpha + t\frac{b}{x})\big) = 1$.

Hence there exist integers $\lambda, \mu \in \mathbb{Z}$ with $\lambda(\beta - t\frac{a}{x}) - \mu d(a + t\frac{b}{x}) = 1$ and the matrix

$$G = \begin{pmatrix} \lambda & a + t\frac{b}{x} \\ d\mu & \beta - t\frac{a}{x} \end{pmatrix}$$

satisfies the properties claimed.

**Claim 2:**

Assume $g \geq 2$, let $(1, d_1, \ldots, d_{1:g-1})$ be any polarisation type and $\Delta$ the diagonal matrix corresponding to it. For any $v = (v_1, \ldots, v_g) \in \mathbb{Z}^g$ we can find a matrix $G \in \mathbb{SD}(\Delta)$ such that $u := vG$ satisfies $u_g = \gcd(v_1, \ldots, v_g)$.

The proof is by induction and shows that $G$ can be chosen to be of the form

$$G = \begin{pmatrix} \beta_1 & 0 & \ldots & 0 & a_1 \\ 0 & \beta_2 & & 0 & a_2 \\ \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & \beta_{g-1} & a_{g-1} \\ d_{1:g-1}\gamma_1 & d_{2:g-1}\gamma_2 & \ldots & d_{g-1}\gamma_{g-1} & a_g \end{pmatrix}. \tag{18}$$

For $g = 2$ this is exactly Claim 1. For the induction, fix any $g \geq 2$ and assume we can find $G_g$ of the form (18) satisfying $\det G_g = 1$ and $\sum_{i=1}^{g} a_i v_i = \gcd(v_1, \ldots, v_g)$. Now let the polarisation type for $g+1$ be given by $(1, d_0, d_{0:1}, \ldots, d_{0:g-1})$ and $v = (v_0, v_1, \ldots, v_g)$.

We use Claim 1 with $a = v_0, b = \gcd(v_1, \ldots, v_g)$ and $d = d_{0:g-1} \prod_{i=1}^{g-1} \beta_i$ to obtain a matrix $G' = \begin{pmatrix} \mu_0 & \lambda_0 \\ d\mu_1 & \lambda_1 \end{pmatrix}$ satisfying $\det G' = 1$ and $\lambda_0 v_0 + \lambda_1 \gcd(v_1, \ldots, v_g) = \gcd(v_0, \ldots, v_g)$. Define the matrix $G_{g+1}$ to be

$$G_{g+1} := \begin{pmatrix} \mu_0 & 0 & 0 & \ldots & 0 & \lambda_0 \\ 0 & \beta_1 & 0 & & 0 & \lambda_1 a_1 \\ 0 & 0 & \beta_2 & & 0 & \lambda_1 a_2 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & \ldots & 0 & \beta_{g-1} & \lambda_1 a_{g-1} \\ d_{0:g-1}\mu_1 & d_{1:g-1}\gamma_1 & \ldots & d_{g-2:g-1}\gamma_{g-2} & d_{g-1}\gamma_{g-1} & \lambda_1 a_g \end{pmatrix}.$$

Some simple calculation shows that $G_{g+1}$ is as claimed.

Now we can conclude the proof of the lemma. Use Claim 2 to obtain a matrix $G \in \mathbb{SD}(\Delta)$ satisfying $u'_g = \gcd(v_1, \ldots, v_g)$ for $u' := (v_1, \ldots, v_g)G$. Since $\mathbb{SD}(\Delta)$ is a multiplicative group, $G^{-1} \in \mathbb{SD}(\Delta)$. Now, $M = \begin{pmatrix} G & 0 \\ 0 & G^{-1} \end{pmatrix}$ satisfies the properties claimed.

This last step goes through the same if we restrict everything to the sublattice $\bigoplus_j (e_{i_j}\mathbb{Z} \oplus e_{g+i_j}\mathbb{Z})$. ■

## REFERENCES

[AMRT] A. ASH - D. MUMFORD - M. RAPOPORT - Y. TAI, *Smooth Compactification of Locally Symmetric Varieties*, Brookline: Math Sci Press 1975.

[FS] M. FRIEDLAND - G. K. SANKARAN, *Das Titsgebäude von Siegelschen Modulgruppen vom Geschlecht 2*, Abh. Math. Sem. Univ. Hamburg **71** (2001), 49-68.

[HKW] K. HULEK - C. KAHN - S. H. WEINTRAUB *Moduli Spaces of Abelian Surfaces: Compactification, Degenerations and Theta Functions*, De Gruyter Expositions in Mathematics 12, 1993.

[OR] E. OELJEKLAUS - R. REMMERT, *Lineare Algebra I*, Springer-Verlag, 1974.

Gretchenstraße 39ª, 30161 Hannover, Germany
e-mail: Eric.Schellhammer@gmx.de

*Pervenuta in Redazione*
*il 31 maggio 2004*