Zonal functions for the unitary groups and applications to hermitian lattices

Christine Bachoc

Laboratoire A2X
Université Bordeaux I
351, cours de la Libération,
33405 Talence, France
bachoc@math.u-bordeaux.fr

Gabriele Nebe

Abteilung Reine Mathematik,
Universität Ulm,
89069 Ulm, Germany
nebe@mathematik.uni-ulm.de

Abstract

We study the decomposition of the space $L^2(S^{n-1})$ under the actions of the complex and quaternionic unitary groups. We give an explicit basis for the space of zonal functions, which in the second case takes account of the action of the group of quaternions of norm 1. We derive applications to hermitian lattices.

keywords: lattice, theta series, unitary groups, zonal function.

1 Introduction

It is a classical fact that the functional space $L^2(S^{n-1})$ on the unit sphere S^{n-1} of the Euclidean space $\mathbb{R}^n$ decomposes under the action of the orthogonal group $O(\mathbb{R}^n)$ into the sum of the harmonic spaces Harm_k of degree k. As shown by B. Venkov, the zonal spherical functions associated to this decomposition are a powerful tool to study Euclidean lattices. A key property is that, if $P(x) \in \mathrm{Harm}_k$, then the theta series $\theta_{L,P}$ associated to P and to the lattice L is a modular form. This property, together with the expression of the zonal spherical functions by means of Gegenbauer polynomials, was used in [23] (see also [5, Chap.18]) to recover Niemeier's classification of the even unimodular lattices in dimension 24 and in [3] to prove the non existence of lattices with certain properties.

In this paper, we follow the same line with respect to hermitian lattices. The unitary groups over the complex numbers and the quaternion numbers replace the orthogonal group. We discuss the decomposition of the space $L^2(S^{n-1})$ under their respective action and describe a basis of the zonal spherical functions. In the quaternionic case, the irreducible components have multiplicities greater than one, hence there is no canonical choice of a basis for the zonal spherical functions; we construct a specific basis which takes account of the action of the quaternions of norm one.

Then we derive explicit results on the hermitian unimodular lattices over the Eisenstein ring $\mathbb{Z}[(1+\sqrt{-3})/2]$ and over the Hurwitz order. Some of them explain certain results previously obtained by the full classification of the corresponding genus. We show how the concise and elegant treatment of the Niemeier lattices of minimum 2 given by B. Venkov in [23] (see also [5, Chap.18]) can be extended to these cases. We also prove the non existence of extremal Eisenstein lattices of (real) dimension 48.

2 The group $O(\mathbb{R}^n)$.

In this section we recall some well-known facts on harmonic analysis for the orthogonal group $O(\mathbb{R}^n)$. The space $\mathbb{R}^n$ is considered with its usual Euclidean structure given by $x \cdot y = \sum_{i=1}^n x_i y_i$. The unit sphere S^{n-1} is a homogeneous space for the action of the orthogonal group; if we fix a base point y, the stabilizer O_y of y in $O(\mathbb{R}^n)$ is isomorphic to $O(\mathbb{R}^{n-1})$. The group $O(\mathbb{R}^n)$ acts on the functional space $L^2(S^{n-1})$ by $(u.f)(x) = f(xu)$

and the decomposition into irreducible subspaces is given by

$$L^2(S^{n-1}) = \oplus_{k\geq 0}\mathrm{Harm}_k \tag{1}$$

where Harm_k is the kernel of the Laplace operator $\Delta = \sum \frac{\partial^2}{\partial x_i^2}$ in the space of homogeneous polynomials of degree k in the coordinates $x_1, \dots, x_n$. (In (1) we again denote Harm_k the space of polynomial functions on the unit sphere). Moreover, the spaces Harm_k are pairwise non isomorphic $O(\mathbb{R}^n)$-modules, hence the O_y-invariant elements (so-called zonal spherical functions) are spanned by a single element $Z_{k,y}$ which is known to be expressed in terms of the Gegenbauer polynomials $G_k^{n/2-1}(X)$ ([24, Section 9.3.2]):

$$Z_{k,y}(x) = G_k^{n/2-1}(x \cdot y). \tag{2}$$

3 The group $U(\mathbb{C}^n)$.

3.1 Notations.

We take the following notations: the group

$$U(\mathbb{C}^n) := \{P : P \in M_n(\mathbb{C}) \mid P\bar{P}^t = \mathrm{Id}\} \tag{3}$$

acts by right multiplication on the vector space $\mathbb{C}^n$ which is endowed with the usual hermitian form

$$h(z, z') := \sum_{i=1}^{n} z_i \bar{z}'_i. \tag{4}$$

The mapping

$$\begin{aligned} \mathbb{C} &\to \mathbb{R}^2 \\ z = x + yi &\to (x, y) \end{aligned} \tag{5}$$

extends to an embedding $\phi : \mathbb{C}^n \to \mathbb{R}^{2n}$, which respects the Euclidean structures, i.e. $\phi(z) \cdot \phi(z) = h(z, z)$, where "$\cdot$" denotes the usual scalar product on $\mathbb{R}^{2n}$ given by $x \cdot y = \sum_{i=1}^{2n} x_i y_i$. Hence this mapping induces an inclusion of the groups $U(\mathbb{C}^n) < O(\mathbb{R}^{2n})$. We set

$$U_1 := \{\lambda : \lambda \in \mathbb{C} \mid \lambda\bar{\lambda} = 1\}. \tag{6}$$

The multiplicative group U_1 acts by left multiplication on $\mathbb{C}^n$ as a subgroup of $O(\mathbb{R}^{2n})$. It is worth noticing that $U(\mathbb{C}^n)$ is the centralizer of U_1 in $O(\mathbb{R}^{2n})$.

It follows from the next section that even for every irreducible $O(\mathbb{R}^{2n})$-module Harm_k, the matrices that commute with the action of $U(\mathbb{C}^n)$ on Harm_k are precisely the linear combinations of elements in U_1. If one would know this in advance, this gives the decomposition of Harm_k into irreducible $U(\mathbb{C}^n)$-modules by the double commutant theorem [10, Th. 3.3.7]. The same holds for the pair $U(\mathbb{H}^n)$ and Q_1 in $O(\mathbb{R}^{4n})$ treated in Section 4.

3.2 Decomposition of Harm_k under $U(\mathbb{C}^n)$.

We need to decompose further the space Harm_k (relative to the $2n$ real variables) under the action of the subgroup $U(\mathbb{C}^n)$. This decomposition is described in [24, Section 11.2], we recall it here. We assume for the rest of the paper that k is even. In view of applications to lattices, it is the only case of interest. We first consider the action (by left multiplication on $\mathbb{C}^n$) of the group U_1. We set

$$V_w^{(k)} := \{f : f \in \mathrm{Harm}_k \mid f(\lambda x) = \lambda^w f(x) \text{ for all } \lambda \in U_1\}. \tag{7}$$

Because U_1 is abelian, the following decomposition holds:

$$\mathrm{Harm}_k := \oplus_{w\in\mathbb{Z}} V_w^{(k)}. \tag{8}$$

Moreover, because the respective actions of U_1 and of $U(\mathbb{C}^n)$ commute, this decomposition is preserved by $U(\mathbb{C}^n)$. It turns out that it is the irreducible decomposition for $U(\mathbb{C}^n)$. In order to prove this, we compute the zonal functions in $V_w^{(k)}$. We fix $z' \in S^{2n-1}$ and set $U_{z'} := \mathrm{Stabilizer}(z', U(\mathbb{C}^n))$. The group $U_{z'}$ is isomorphic to $U(\mathbb{C}^{n-1})$. We denote by Hom_k the space of homogeneous polynomials of degree k with complex coefficients in the $2n$ variables $x_1, y_1, x_2, y_2, \ldots, x_n, y_n$. The zonal functions are elements of the space

$$\mathrm{Hom}_k^{U_{z'}} := \{f : f \in \mathrm{Hom}_k \mid f(xu) = f(x) \text{ for all } u \in U_{z'}\}. \tag{9}$$

With an obvious meaning, we denote $z = (z_1, \ldots, z_n) = (x_1+iy_1, \ldots, x_n+iy_n)$, and see $h(z, z') = (x_1 + iy_1)\bar{z_1}' + \cdots + (x_n + iy_n)\bar{z_n}'$ as an element of Hom_1.

We denote

$$[a, b, r] := h(z, z')^a \overline{h(z, z')}^b h(z, z)^r$$

with the convention that $[a, b, r] = 0$ if a, b or r is negative. It is worth noticing that the degree of $[a, b, r]$ is $a + b + 2r$ and that $\lambda.[a, b, r] = \lambda^{a-b}[a, b, r]$.

Proposition 3.1 *The zonal functions in Hom_k are the linear combinations of the elements $[a,b,r]$ with $a+b+2r=k$. Moreover,*

$$\Delta[a,b,r] = 4ab[a-1,b-1,r] + 4r(a+b+r-1+n)[a,b,r-1]. \qquad (10)$$

Proof. The space Hom_k is generated by elements of the form $(z\cdot y)^{k-2r}(z\cdot z)^r$ when $r \in [0\dots k/2]$ and y varies in S^{2n-1}. The identity $z\cdot y = (h(z,y) + \overline{h(z,y)})/2$ shows that the $h(z,y)^a\overline{h(z,y)}^b h(z,z)^r$ with $a+b+2r=k$ generate Hom_k. We can complete z' to an orthonormal basis $(z', e_2, \dots, e_n)$, write y on this basis, develop again and apply suitable elements of $U_{z'} = U(\mathbb{C}e_2 + \dots + \mathbb{C}e_n)$ (diagonal matrices are enough) to see that an element of $\mathrm{Hom}_k^{U_{z'}}$ is a linear combination of $[a,b,r]$.

The computation of Δ on $[a,b,r]$ is straightforward and can also be found in [24, Section 11.2.2(13)]. $\square$

Notation: We denote $[a, b \mod c]$ the set of integers u, such that $a \leq u \leq b$ and $u \equiv a \mod c$.

Theorem 3.2 *The spaces V_w^k are non zero if and only if $w \in [-k, k \mod 2]$, and in these cases they are $U(\mathbb{C}^n)$-irreducible and pairwise non isomorphic.*

Proof. The formula (10) shows that there is up to a multiplicative factor a unique zonal function in $V_w^{(k)}$, which is a linear combination of the $[a,b,r]$ with $a+b+2r=k$ and $a-b=w$. Since $w = k-2b-2r$, we have $w \in [-k, k \mod 2]$. It proves that $\dim(\mathrm{Harm}_k^{H_{z'}}) = k+1$. Since the decomposition (8) shows that at least $k+1$ components appear in the irreducible decomposition of Harm_k, Frobenius theorem proves the result. $\square$

Definition 3.3 *We denote by $Z_w^{(k)}$ the unique zonal function in $V_w^{(k)}$ of the form*

$$Z_w^{(k)}(z,z') = \sum_{r=0}^{(k+w)/2} \alpha_r[\frac{k+w}{2} - r, \frac{k-w}{2} - r, r] \qquad (11)$$

with $\alpha_0 = 1$ and the coefficients α_r are computed recursively using (10).

Remarks and examples

- It is worth noticing that, clearly $Z_{-w}^{(k)} = \overline{Z_w^{(k)}}$.

- For all k, $Z_k^{(k)}(z,z') = h(z,z')^k$.
- If $k=2$, $Z_0^{(2)}(z,z') = h(z,z')\overline{h(z,z')} - \frac{1}{n}h(z,z)$.
- The zonal functions for the symmetric space $\mathbb{P}(\mathbb{C}^n)$ are computed in [11]. They are equal to $Z_0^{(k)}$ (up to a normalization) because $Z_0^{(k)}(\lambda z,z') = Z_0^{(k)}(z,z')$ for all λ.

4 The group $U(\mathbb{H}^n)$.

4.1 Notations.

The field of quaternion numbers is $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$, where $i^2 = j^2 = -1$, $ij = -ji = k$. The conjugate of $q = x_1 + x_2 i + x_3 j + x_4 k$ is $\overline{q} = x_1 - x_2 i - x_3 j - x_4 k$. The isomorphism $\mathbb{C} \simeq \mathbb{R} + \mathbb{R}i$ gives $\mathbb{H}$ the structure of a left $\mathbb{C}$-vector space. We identify $\mathbb{R} + \mathbb{R}i$ with $\mathbb{C}$ and denote also $q = z_1 + z_2 j$ with $z_i \in \mathbb{C}$. Then $jz_2 = \overline{z_2}j$ and $\overline{q} = \overline{z_1} - z_2 j$.

The group

$$U(\mathbb{H}^n) := \{P : P \in M_n(\mathbb{H}) \mid P\bar{P}^t = \mathrm{Id}\} \tag{12}$$

acts by right multiplication on the space $\mathbb{H}^n$ which is endowed with the usual hermitian form

$$H(q,q') := \sum_{i=1}^{n} q_i \bar{q}'_i. \tag{13}$$

The mapping (with the previous notations)

$$\begin{array}{ccc} \mathbb{H} & \rightarrow \mathbb{C}^2 & \rightarrow \mathbb{R}^4 \\ q & \rightarrow (z_1,z_2) & \rightarrow (x_1,x_2,x_3,x_4) \end{array} \tag{14}$$

extends to embeddings $\mathbb{H}^n \rightarrow \mathbb{C}^{2n} \rightarrow \mathbb{R}^{4n}$, which respect the hermitian and Euclidean structures and therefore induce the inclusions of the groups $U(\mathbb{H}^n) < U(\mathbb{C}^{2n}) < O(\mathbb{R}^{4n})$. We set

$$Q_1 := \{\mu : \mu \in \mathbb{H} \mid \mu\bar{\mu} = 1\}. \tag{15}$$

The multiplicative group Q_1 acts by left multiplication on $\mathbb{H}^n$ as a subgroup of $O(\mathbb{R}^{4n})$ because, if $\mu \in Q_1$, $\mathrm{Trace}(H(\mu q, \mu q')) = \mathrm{Trace}(\mu H(q,q')\overline{\mu}) = \mathrm{Trace}(H(q,q'))$. The elements of $U(\mathbb{H}^n)$ are exactly the elements in $O(\mathbb{R}^{4n})$ which commute with the action of Q_1.

4.2 Decomposition of Harm_k under $U(\mathbb{H}^n)$.

We now describe the decomposition of Harm_k (in the $4n$ variables) under $U(\mathbb{H}^n)$ and the zonal functions associated to this decomposition. We start with the decomposition under the action of Q_1.

The multiplicative group Q_1 is isomorphic to $SU_2(\mathbb{C})$ by

$$\mu = z_1 + z_2 j \to \begin{pmatrix} z_1 & z_2 \\ -\overline{z_2} & \overline{z_1} \end{pmatrix}. \tag{16}$$

Its irreducible representations are given by the spaces $W_p = \mathbb{C}X^p + \mathbb{C}X^{p-1}Y + \cdots + \mathbb{C}Y^p$ of homogeneous polynomials in the two variables X, Y of degree p. If we denote $I(W_p)^{(k)}$ the isotypic component of W_p in Harm_k, we have

$$\mathrm{Harm}_k = \oplus_p I(W_p)^{(k)}. \tag{17}$$

Since the weights of W_p are $[-p, p \mod 2]$, clearly the values of p for which $I(W_p)^{(k)}$ is non zero belong to $[0, k \mod 2]$.

The group $U(\mathbb{H}^n)$, as a subgroup of $U(\mathbb{C}^{2n})$, preserves the decomposition (8), and, since it commutes with Q_1, it also preserves the decomposition (17). So we have the decomposition of $U(\mathbb{H}^n)$ modules:

$$\mathrm{Harm}_k = \bigoplus_{\substack{w\in[-k,k \mod 2] \\ p\in[0,k \mod 2] \\ p\geq w}} I(W_p)^{(k)} \cap V_w^{(k)}. \tag{18}$$

Theorem 4.1 *Let $R_p^{(k)} := I(W_p)^{(k)} \cap V_p^{(k)}$. For all $p \in [0, k \mod 2]$, the spaces $R_p^{(k)}$ are irreducible and pairwise non isomorphic $U(\mathbb{H}^n)$-modules. For all $w \in [-p, p \mod 2]$, $I(W_p)^{(k)} \cap V_w^{(k)} \simeq R_p^{(k)}$, and we have the following decomposition:*

$$\mathit{Harm}_k \simeq \oplus_{p\in[0,k \mod 2]} (p+1) R_p^{(k)}. \tag{19}$$

This decomposition is also described in [12, Section 1.2], where the Young diagram associated to $R_p^{(k)}$ is given. Since we need a concrete description of the zonal functions and since such a description leads to the decomposition in Theorem 4.1, we give another proof.

Proof. (of Theorem 4.1)

We fix q', $H(q', q') = 1$ and define $U_{q'} := \mathrm{Stabilizer}(q', U(\mathbb{H}^n))$. The group $U_{q'}$ is isomorphic to $U(\mathbb{H}^{n-1})$; the zonal functions are the elements of

$\mathrm{Hom}_k^{U_{q'}}$. The orbits of $U_{q'}$ acting on the unit sphere are clearly characterized by $H(q,q')$, so the zonal functions are functions of $H(q,q')$. However, we cannot express them as polynomials in $H(q,q')$, $\overline{H(q,q')}$ like in the complex case because these last expressions are polynomials in the $4n$ coordinates with coefficients in $\mathbb{H}$ and hence do not commute. We shall more conveniently express them in terms of the complex hermitian form $h(q,q')$ on $\mathbb{C}^{2n}$. We take the following notation:

$$[a,b,c,d,r] := h(q,q')^a h(q,jq')^b \overline{h(q,q')}^c \overline{h(q,jq')}^d h(q,q)^r. \tag{20}$$

Proposition 4.2 *The zonal functions for $U(\mathbb{H}^n)$ in Hom_k are the linear combinations of the elements $[a,b,c,d,r]$ with $a+b+c+d+2r=k$. Moreover,*

$$\begin{aligned}\Delta[a,b,c,d,r] =& 4ac[a-1,b,c-1,d,r] + 4bd[a,b-1,c,d-1,r] \\ &+ 4r(k-r-1+2n)[a,b,c,d,r-1].\end{aligned} \tag{21}$$

Proof. Same proof as for Proposition 3.1. □

If $\lambda \in U_1$, then $\lambda.[a,b,c,d,r] = \lambda^{a+b-c-d}[a,b,c,d,r]$. It is worth noticing that U_1 is a maximal torus of Q_1. A maximal torus of $U(\mathbb{H}^n)$ is

$$\mathbb{T} := \{T := \begin{pmatrix} \lambda_1 & & & & \\ & \overline{\lambda_1} & & & \\ & & \ddots & & \\ & & & \lambda_n & \\ & & & & \overline{\lambda_n} \end{pmatrix} \in U(\mathbb{C}^{2n}) \mid \lambda_i \in U_1\}. \tag{22}$$

Up to a change of basis, we can assume that $q' = (1,0,\dots,0) \in \mathbb{H}^n$. Then, if $q = (q_1,\dots,q_n)$ with $q_1 = z_1 + z_2 j$, one easily computes $[a,b,c,d,r] = z_1^a z_2^b \overline{z_1}^c \overline{z_2}^d (\sum_{i=1}^n q_i \overline{q_i})^r$, and hence $T.[a,b,c,d,r] = \lambda_1^{a-b-c+d}[a,b,c,d,r]$. So the elements $[a,b,c,d,r]$ are weight vectors for respectively Q_1 and $U(\mathbb{H}^n)$. Note that the Laplace operator preserves both values $a+b-c-d$ and $a-b-c+d$ (from (21), or because it commutes with the actions of the groups Q_1, $U(\mathbb{H}^n)$). We denote by $E^{(k)}_{w,w'}$ the $\mathbb{C}$-vector space

$$\begin{aligned} E^{(k)}_{w,w'} := \mathrm{span}\{[a,b,c,d,r] \mid\ & a+b+c+d = k-2r, \\ & a+b-c-d = w, \\ & a-b-c+d = w'\}. \end{aligned} \tag{23}$$

The Laplace operator Δ maps $E^{(k)}_{w,w'}$ onto $E^{(k-2)}_{w,w'}$ (one can see that Δ is surjective because Proposition 4.2 shows that if the $[a,b,c,d,r]$ are ordered in such a way that r decreases and then lexicographically, the matrix of Δ is upper triangular with non zero coefficients on the diagonal). This space is not reduced to $\{0\}$ if and only if w and w' are even and belong to $[-k \dots k]$ (k is always assumed to be even). Clearly $\dim(E^{(k)}_{w,w'}) = \frac{1}{2}(\frac{k-\max(|w|,|w'|)}{2} + 1)(\frac{k-\max(|w|,|w'|)}{2} + 2)$. We obtain that $\dim(\ker \Delta \cap E^{(k)}_{w,w'}) = \frac{k-\max(|w|,|w'|)}{2} + 1$. One can check that

$$\dim(\mathrm{Harm}_k^{U_{q'}}) = \sum_{w,w' \in [-k,k \mod 2]} \frac{k - \max(|w|,|w'|)}{2} = \sum_{p \in [0,k \mod 2]} (p+1)^2.$$

Now we finish the proof of Theorem 4.1. Let R be an irreducible $U(\mathbb{H}^n)$-subspace of $R^{(k)}_p$. Then, for all $q \in Q_1$, qR is isomorphic to R and is contained in one of the $V^{(k)}_w$. The space $\mathbb{C}[Q_1]R$ is a Q_1-subspace of $I(W_p)^{(k)}$, therefore it is isomorphic to the sum of copies of W_p, and hence it intersects non trivially all the $V^{(k)}_w$ for $w \in [-p, p \mod 2]$. Finally, there is at least one subspace isomorphic to R in each $V^{(k)}_w$ with $w \in [-p, p \mod 2]$, which proves that the multiplicity m_R of R is at least equal to $p+1$. By Frobenius theorem, $\dim(\mathrm{Harm}_k^{U_{q'}}) = \sum_R m_R^2$, and we have computed that $\dim(\mathrm{Harm}_k^{U_{q'}}) = \sum_{p \in [0,k \mod 2]} (p+1)^2$, so we can conclude that the subspaces $R^{(k)}_p$ are irreducible and isomorphic to $I(W_p)^{(k)} \cap V^{(k)}_w$ for all $w \in [-p, p \mod 2]$. □

4.3 A special basis of $\mathrm{Harm}_k^{U_{q'}}$.

We have proved in Theorem 4.1 that $I(W_p)^{(k)} \simeq (p+1)R^{(k)}_p$, so the space of zonal functions in $I(W_p)^{(k)}$ is of dimension $(p+1)^2$. We describe in this section an algorithmic method that computes a basis of $\mathrm{Harm}_k^{U_{q'}}$, on which the action of Q_1 is explicit.

We need to introduce a certain hermitian product on Hom_k. It is defined on the monomials in the $4n$-indeterminates x_i of the same degree k by:

$$< x^\alpha, x^\beta >:= \delta_{\alpha,\beta} \binom{k}{\alpha}^{-1} \tag{24}$$

where $\binom{k}{\alpha} = \frac{k!}{\alpha_1! \dots \alpha_{4n}!}$ is the multinomial coefficient. It has the nice property to be $U(\mathbb{C}^{4n})$-invariant (see [22]). Therefore the irreducible $O(\mathbb{R}^{4n})$-subspace Harm_k is orthogonal to $(\sum_{i=1}^{4n} x_i^2)\mathrm{Hom}_{k-2}$ because the latter has no constituent isomorphic to the dual $(\mathrm{Harm}_k)^* \cong \mathrm{Harm}_k$ of Harm_k.

Lemma 4.3 *Let $a,b,c,d,a',b',c',d',r' \in \mathbb{Z}_{\geq 0}$ with $a+b+c+d = a'+b'+c'+d'+2r' = k$. Then*

$$< [a,b,c,d,0],[a',b',c',d',r'] >= \begin{cases} \frac{2^k h(q',q')^{k-r'}\binom{r'}{a-a'}}{\binom{k}{a,b,c,d}} & \text{if } \begin{cases} a-a' = c-c' \geq 0 \\ b-b' = d-d' \geq 0 \end{cases} \\ 0 & \text{otherwise} . \end{cases}$$

Proof. We first assume that $h(q',q') = 1$. Then, we can replace q' by $q'u$ with $u \in U(\mathbb{C}^{2n})$, and assume that $q' = (1,0,\dots,0) \in \mathbb{C}^{2n}$. If $(z_1,\dots,z_{2n})$ are the complex coordinates of q, then $[a,b,c,d,r] = z_1^a z_2^b \overline{z_1}^c \overline{z_2}^d (\sum_{s=1}^{2n} z_s \overline{z_s})^r$. If $z_s = x_{2s-1} + x_{2s} i$, $[a,b,c,d,r] = (x_1 + x_2 i)^a (x_3 + x_4 i)^b (x_1 - x_2 i)^c (x_3 - x_4 i)^d (\sum_{s=1}^{4n} x_s^2)^r$. Let

$$U := \begin{pmatrix} \begin{smallmatrix} 1 & 1 \\ i & -i \end{smallmatrix} & & & & \\ & \begin{smallmatrix} 1 & 1 \\ i & -i \end{smallmatrix} & & & \\ & & \sqrt{2} & & \\ & & & \ddots & \\ & & & & \sqrt{2} \end{pmatrix} \in M_{4n}(\mathbb{C})$$

then $U\overline{U}^t = 2\mathrm{Id}_{4n}$ and hence $\frac{1}{\sqrt{2}} U \in U_{4n}(\mathbb{C})$. If we let $(y_1,\dots,y_{4n}) = (x_1,\dots,x_{4n})U$, one has $[a,b,c,d,r] = y_1^a y_3^b y_2^c y_4^d (y_1 y_2 + y_3 y_4 + \sum_{s\geq 5} y_s^2/2)^r$. The computation of $< [a,b,c,d,0],[a',b',c',d',r'] >$ follows from the fact that this hermitian product is $U(\mathbb{C}^{4n})$-invariant and from the expression (24).

In the general case, $q' = \lambda(1,0,\dots,0)$ with $\lambda \in \mathbb{C}$ and the function $[a,b,c,d,r]$ is multiplied by $\overline{\lambda}^{a+d}\lambda^{b+c}$. An easy computation shows that the previous hermitian product is multiplied by $(\lambda\overline{\lambda})^{k-r'} = h(q',q')^{k-r'}$. $\square$

Remark 4.4 *With the Lemma 4.3, we are able to compute the hermitian product of any two elements of $Harm_k^{U_{q'}}$: such functions are linear combinations of some $[a,b,c,d,r]$ from Proposition 4.2, and are orthogonal to the elements of $h(q,q)Hom_{k-2}$ so, in one of them we can ignore the terms $[a,b,c,d,r]$ with $r \neq 0$.*

Recall that W_p is the $\mathbb{C}$-vector space of homogeneous polynomials of degree p in two variables. It is equipped with the same hermitian product, given by $< X^{p-a}Y^a, X^{p-b}Y^b >= \delta_{a,b}\binom{p}{a}^{-1}$, which is invariant under the action of $SU_2(\mathbb{C})$.

Proposition 4.5 *There exists an essentially unique basis* $\{Z^{(k)}_{p,w,w'}\}_{w,w'\in[-p,p \mod 2]}$ *of the zonal functions of* $I(W_p)^{(k)}$ *such that :*

- $Z^{(k)}_{p,w,w'} \in E^{(k)}_{w,w'}$
- $\{Z^{(k)}_{p,w,w'}\}_{w'\in[-p,p \mod 2]}$ *is a basis of* $I(W_p)^{(k)} \cap V^{(k)}_w$
- *For all* w' *the set* $\{Z^{(k)}_{p,w,w'}\}_{w\in[-p,p \mod 2]}$ *is a basis of a* Q_1*-space isomorphic to* W_p*, such that the mapping* $Z^{(k)}_{p,w,w'} \to X^{\frac{p+w}{2}} Y^{\frac{p-w}{2}}$ *is an isomorphism of* Q_1*-modules, and an isometry for the hermitian products* $<,>$*.*

The uniqueness of this basis holds up to the change $Z^{(k)}_{p,w,w'} \to a_{w'} Z^{(k)}_{p,w,w'}$ *with* $a_{w'} \in U_1$*.*

Proof. We assume by induction that we have proved the proposition for $I(W_k)^{(k)}, \dots, I(W_{p+2})^{(k)}$. We have previously seen that $\dim(\ker \Delta \cap E^{(k)}_{p,w'}) = (k-p)/2 + 1$ for $w' \in [-p, p \mod 2]$. We have already constructed in this space $(k-p)/2$ elements $Z^{(k)}_{t,p,w'}$ for $t \in [k, p+2 \mod 2]$. It should be noticed that $Z^{(k)}_{p,p,w'}$ must be orthogonal to them because it belongs to a different isotypic component. So the conditions: $Z^{(k)}_{p,p,w'} \in \ker \Delta \cap E^{(k)}_{p,w'}$, $< Z^{(k)}_{p,p,w'}, Z^{(k)}_{t,p,w'} >= 0$ for all $t \in [k, p+2 \mod 2]$, and $< Z^{(k)}_{p,p,w'}, Z^{(k)}_{p,p,w'} >= 1$ determine the elements $Z^{(k)}_{p,p,w'}$ up to the multiplication by a complex number of norm 1. For each w' fixed, $Z^{(k)}_{p,p,w'}$ is a highest weight vector of the Q_1-module spanned by $Z^{(k)}_{p,p,w'}$, which therefore is isomorphic to W_p. Up to an element of U_1, $Z^{(k)}_{p,p,w'}$ is sent to X^p, and we define $Z^{(k)}_{p,w,w'}$ to be the preimage of $X^{\frac{p+w}{2}} Y^{\frac{p-w}{2}}$ by this isomorphism. The element $Z^{(k)}_{p,w,w'}$ must be of the form $\mu.Z^{(k)}_{p,p,w'}$ with $\mu \in Q_1$, hence it remains a zonal function, hence a linear combination of some $[a,b,c,d,r]$. We must have $a+b-c-d = w$ because it reflects the fact that $X^{\frac{p+w}{2}} Y^{\frac{p-w}{2}}$ is a weight vector for the weight w, and $a-b-c+d = w'$ because the actions of Q_1 and $U(\mathbb{H}^n)$ commute. $\square$

We end this subsection with some remarks on the algorithmic computation of the basis described in Proposition 4.5. The next lemma makes more precise the action of Q_1 on the $[a,b,c,d,r]$.

Lemma 4.6 *Let* $\mu \in Q_1$*. For all* $[a,b,c,d,r]$*,* $\mu.[a,b,c,d,r]$ *is a* $\mathbb{C}$*-linear combination of elements* $[a',b',c',d',r']$*, with* $r' = r$*.*

Proof. We can write $\mu = z_1 + z_2 j$. Then $\overline{h(\mu q, \mu q)} = h(q,q)$, $h(\mu q, q') = z_1 h(q,q') + z_2 h(jq,q')$ and $h(jq,q') = -\overline{h(q,jq')}$. We replace in the expression (20) of $[a,b,c,d,r]$ and obtain a linear combination of elements $[a',b',c',d',r']$, with $r'=r$. $\square$

We assume that we have constructed the $\{Z^{(k)}_{t,w,w'}\}_{w,w'\in[-t,t \mod 2]}$ for all $t\in[k,p+2 \mod 2]$. We now wish to compute the $\{Z^{(k)}_{p,w,w'}\}_{w,w'\in[-p,p \mod 2]}$. We first determine the $Z^{(k)}_{p,p,w'}$ (up to a multiplicative factor in U_1) as described in the proof of Proposition 4.5. Since $Z^{(k)}_{p,w,w'}$ is of the form $\mu.Z^{(k)}_{p,p,w'}$, from Lemma 4.6 it is a linear combination of $[a,b,c,d,r]$ with $r\le(k-p)/2$. One can then check that the space of functions in $\ker\Delta\cap E^{(k)}_{w,w'}$, which are orthogonal to all the $Z^{(k)}_{t,w,w'}$ for $t\in[k,p+2 \mod 2]$ and which have the additional property that $r\le(k-p)/2$, is one-dimensional. Let Z be a generator of this space, we know that $Z^{(k)}_{p,w,w'}=\alpha Z$ for some complex number α. In order to compute α, we use the action of $\mu=(1-j)/\sqrt{2}$. One easily computes that $<\mu.X^p, X^{\frac{p+w}{2}}Y^{\frac{p-w}{2}}>=2^{-p/2}$. It remains to calculate $<\mu.Z^{(k)}_{p,p,w'},Z>$, which is easy with Lemma 4.3 and the rules described in the proof of Lemma 4.6.

Remarks and examples

- Easy rules link $Z^{(k)}_{p,w,w'}$ with $Z^{(k)}_{p,-w,w'}$ and $Z^{(k)}_{p,w,-w'}$. The expression of $Z^{(k)}_{p,-w,w'}$ is obtained from $Z^{(k)}_{p,w,w'}$ by replacing each term $[a,b,c,d,r]$ by $(-1)^{a+c}[d,c,b,a,r]$, and the expression of $Z^{(k)}_{p,w,-w'}$ by $(-1)^{a+c}[b,a,d,c,r]$.
- If $k=2$, $Z^{(2)}_{0,0,0}(q,q')=H(q,q')\overline{H(q,q')}-\frac{1}{n}H(q,q)$, and:

$$\begin{cases} Z^{(2)}_{2,2,2}(q,q')=\frac{1}{2}h(q,q')^2\\ Z^{(2)}_{2,2,0}(q,q')=h(q,q')\overline{h(q,q')}\\ Z^{(2)}_{2,0,2}(q,q')=\frac{1}{2}h(q,q')\overline{h(q,jq')}\\ Z^{(2)}_{2,0,0}(q,q')=-\frac{1}{2}h(q,q')\overline{h(q,q')}+\frac{1}{2}h(q,jq')\overline{h(q,jq')}. \end{cases}$$

- The zonal functions for the symmetric space $\mathbb{P}(\mathbb{H}^n)$ are computed in [11]. They are equal to $Z^{(k)}_{0,0,0}$ (up to a normalization) because $Z^{(k)}_{0,0,0}(\mu q,q')=Z^{(k)}_{0,0,0}(q,q')$ for all μ (note that these functions correspond to the only irreducible component with multiplicity equal to one).

- In view of applications to lattices, we are lead to consider sums of the type $\sum_{x\in S} Z(x)$ where S is closed for the left multiplication by some finite group $U < Q_1$ (see Section 5; we may consider lattices with an hermitian structure over a maximal order of a quaternion field defined over $\mathbb{Q}$, S is the set of lattice vectors of given norm, and U is the group of units of the maximal order). In that case, we need only consider the zonal functions which are U-invariant. Proposition 4.2 shows that we only need to know a basis for the polynomials of degree p which are invariant for the action of $U < SU_2(\mathbb{C})$, and transfer this basis through the Q_1-isomorphism explicitly given. For example, the first non trivial invariant for the group $\mathcal{M}^*$ (29) is the degree 6 polynomial $X^5Y - XY^5$. So we take account of one zonal function in degree 2 and 4 (namely $Z^{(2)}_{0,0,0}$ and $Z^{(4)}_{0,0,0}$), and of 4+1 zonal functions in degree 6 (namely $Z^{(6)}_{0,0,0}$, and the $Z^{(6)}_{6,4,w'} - Z^{(6)}_{6,-4,w'}$ for $w' \in [0, 6 \mod 2]$).

5 Applications to lattices

We consider lattices with an hermitian structure over a field K, which is either a totally imaginary quadratic field, or a quaternion field over $\mathbb{Q}$, ramified at ∞.

We take the following notations: in the quadratic case, $K = \mathbb{Q}(\sqrt{-d})$ where $d > 0$ and $-d$ is the discriminant of K. The ring of integers of K is denoted O_K and its unit group O_K^*. The complex conjugation on K is denoted $x \to \overline{x}$. In the quaternionic case, we again denote O_K a fixed maximal order of K, O_K^* its group of units and $x \to \overline{x}$ the conjugation. The discriminant of O_K is denoted d.

The left K-vector space K^n is endowed with the hermitian form $h_K(z, z') := \sum_{i=1}^n z_i \overline{z'_i}$. An hermitian lattice L over K is an O_K-submodule of K^n of full rank. Its hermitian dual is defined by

$$L^{*h_K} := \{x : x \in K^n \mid h_K(x, L) \subset O_K\}. \tag{25}$$

The lattice L is also a Euclidean lattice when considered as a $\mathbb{Z}$-module, for the scalar product $x \cdot y := \mathrm{Trace}_{K/\mathbb{Q}}(h_K(x, y))$ and of rank $2n$ in the quadratic case and $4n$ in the quaternionic case (in this last case, $\mathrm{Trace}_{K/\mathbb{Q}}$ is the reduced trace). We set $L_{\mathbb{Z}} := (L, x \cdot y)$. The dual of $L_{\mathbb{Z}}$ and the hermitian dual of L are related by:

$$L_{\mathbb{Z}}^* = D_K^{-1} L^{*h_K} \tag{26}$$

where D_K^{-1} is the inverse different of O_K, i.e. the dual with respect to the reduced trace. In particular, if L is hermitian unimodular, i.e. $L^{*h_K} = L$ and D_K is a principal ideal, then $L_{\mathbb{Z}}$ is d-modular as an Euclidean lattice, in the sense of [16].

Such lattices have been widely studied ([1], [2], [5], [9], [21]). We shall be concerned with numerical applications in the cases: $K = \mathbb{Q}(\sqrt{-3})$, and $K = \mathbb{Q}_{2,\infty} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$, where $i^2 = j^2 = -1$, $ij = -ji = k$ (in these two cases the order of the unit groups are the largest possible, which allows easier computations as we shall see later).

In the case $K = \mathbb{Q}(\sqrt{-3})$, $d = 3$. We denote $w := (-1 + \sqrt{-3})/2$. The hermitian unimodular lattices have been classified up to the real dimension 24 by W. Feit [9]. They are special cases of 3-modular lattices, for which the theta series θ_L is a modular form for the Fricke group $\Gamma^*(3)$. As shown in [16], this property leads to an upper bound for the minimum of such a lattice:

$$\min(L) \leq 2[n/6] + 2 \tag{27}$$

(here n is the rank over $K = \mathbb{Q}(w)$). A lattice is said to be extremal if its minimum attains this bound; the Coxeter-Todd lattice K_{12} is an example of an hermitian unimodular lattice which is extremal. Of course the dimensions which are multiples of 6 are the most interesting ones. Feit's classification has shown that there is no extremal hermitian unimodular lattice for $n = 12$. However a 3-modular 24-dimensional extremal $\mathbb{Z}$-lattice was discovered in [14]. This lattice has the structure of a $\mathbb{Z}[w]$-module but is not hermitian unimodular.

We prove in Theorem 5.6 that there are no extremal hermitian unimodular lattices for the relative dimension $n = 24$ (and we also recover Feit's result for dimension 12).

In the case $K = \mathbb{Q}_{2,\infty}$, the maximal orders are conjugate to the Hurwitz order $\mathcal{M}$:

$$\mathcal{M} = \mathbb{Z}[1, i, j, w := \frac{-1 + i + j + k}{2}]. \tag{28}$$

Its group of units is

$$\mathcal{M}^* = \{\pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2}\} \tag{29}$$

and has 24 elements. As an abstract group, it is isomorphic to $SL_2(3) \cong 2.Alt_4$. The hermitian unimodular lattices over the Hurwitz order are special cases of 2-modular lattices, and therefore satisfy the estimate

$$\min(L) \leq 2[n/4] + 2 \tag{30}$$

(here n is the rank over $\mathbb{Q}_{2,\infty}$). They have been classified up to the relative dimension 8 (see [1] and [2]). This classification has shown that none of the lattices of dimension 8 reach the bound (30).

5.1 Root lattices.

Let L be a lattice which is integral over O_K, meaning that $L \subset L^{*h_K}$. We set

$$R(L) := \{x : x \in L \mid h_K(x, x) = 2\}. \tag{31}$$

The elements of $R(L)$ are called the roots of L, and are the norm 4 elements in $L_{\mathbb{Z}}$ (note that $h_K(x, x)$ is always in $\mathbb{Z}$). To $x \in R(L)$ we can associate the reflection

$$\rho_x(y) := y - h_K(x, y)x \tag{32}$$

which preserves the lattice L. If $U(L)$ denotes the group of unitary transformations preserving L, the reflections ρ_x generate a subgroup $W(L)$ of $U(L)$ which is a finite, complex or quaternionic, reflection group. Just like in the case of the Euclidean root lattices, one easily proves that a lattice L spanned by its roots is the orthogonal sum of indecomposable sublattices spanned by their roots, and that, if the sublattice spanned by the roots is indecomposable, then the group $W(L)$ is irreducible.

The complex irreducible finite reflection groups have been classified by Shephard and Todd [20] and their invariant lattices are studied in [15]. To such a group, one can associate an essentially unique reduced root system (see [15, Definition 19]). If L is indecomposable and is spanned by $R(L)$, then $R(L)$ is a reduced K-root system for $W(L)$ in the sense of [15], with the additional property that all the roots have the same length.

The quaternionic irreducible finite reflection groups are classified by A. M. Cohen [4], together with their root systems. In the quaternionic case, it happens that the root system is not uniquely determined by the group (see [4]), but not in the cases we are dealing with (the groups are defined over $\mathbb{Q}_{2,\infty}$).

Proposition 5.1 *Let $R \subset \{x : x \in \mathbb{C}^n$ or $\mathbb{H}^n \mid h(x,x) = 2\}$ be a finite set such that the reflections ρ_x, $x \in R$ generate a finite irreducible subgroup of $U(\mathbb{C}^n)$ (or of $U(\mathbb{H}^n)$) and act transitively on R. Then*

$$\sum_{r \in R} h(x,r)\overline{h(y,r)} = \frac{2|R|}{n} h(x,y). \tag{33}$$

Proof. Let G denote the group generated by the reflections associated to R. Let $\phi(x,y) = \sum_{r \in R} h(x,r)\overline{h(y,r)}$. Clearly ϕ is a non-degenerate hermitian form which is G-invariant; since G is irreducible, it must be a multiple of $h(x,y)$. The multiplicative factor is computed by application of the Laplace operator Δ. $\square$

Definition 5.2 *By analogy with the Euclidean case (see [22, Proposition 5.5]), we define the* Coxeter number *of a K-root system R to be*

$$h(R) := \frac{2|R|}{|O_K^*|n}.$$

Remark 5.3 *Equation (33) can be read also as: $\sum_{r \in R} Z_0^{(2)}(x,r) = 0$ (respectively $\sum_{r \in R} Z_{0,0,0}^{(2)}(x,r) = 0$ in the quaternionic case).*

In the complex case, if moreover R is closed for the multiplication by the sixth roots of unity, which is the case if $R = R(L)$ and L is a hermitian lattice over $K = \mathbb{Q}(\sqrt{-3})$, then $\sum_{r \in R} Z_2^{(2)}(x,r) = 0$ holds trivially; hence R is a spherical 2-design in the sense of [22].

In the quaternionic case, the same result holds if R is closed under multiplication by a group of units U, which has no harmonic polynomial invariants of degree 2. This is the case for the group $\mathcal{M}^*$ (the first non trivial invariant of $\mathcal{M}^*$ occurs at degree 6).

In view of the previous remark, we list from [15], [9] and [4] the possible irreducible root systems over $\mathbb{Q}(\sqrt{-3})$ and over $\mathbb{Q}_{2,\infty}$ which can occur as the roots of an integral lattice. We shall denote by L_R the lattice spanned by R and by $\det(L_R)$ its determinant as an O_K-lattice.

If $R \subset \mathbb{R}^n$ is an irreducible Euclidean root system with roots of equal length, namely if R is one of $\{A_n, D_n, E_6, E_7, E_8\}$, then $O_K^* R := \{ur, u \in O_K^*, r \in R\}$ is one of them and $|O_K^* R| = |O_K^*||R|/2$.

The other irreducible root systems over $\mathbb{Q}(\sqrt{-3})$ which can occur as the roots of an integral lattice are:

Table 1:

R	$\lvert R\rvert$	$h(R)$	$W(R)$	$\det(L_R)$
$\mathbb{Z}[w]^*A_n$	$3n(n+1)$	$n+1$	$G_1(n) \simeq S_{n+1}$	$n+1$
$\mathbb{Z}[w]^*D_n$	$6n(n-1)$	$2(n-1)$	$G_2(2,2,n)$	4
$D_n(1-w)$	$9n(n-1)$	$3(n-1)$	$G_2(3,3,n)$	$(1-w)^2$
R_5	270	18	G_{33}	2
R_6	756	42	G_{34}	1
$\mathbb{Z}[w]^*E_6$	216	12	G_{35}	3
$\mathbb{Z}[w]^*E_7$	378	18	G_{36}	2
$\mathbb{Z}[w]^*E_8$	720	30	G_{37}	1

- $D_n(1-w) := \{(u,v,0,\ldots,0)_\sigma \in \mathbb{C}^n \mid u,v \in \mathbb{Z}[w]^*, u+v \equiv 0 \mod 1-w\}$.
- $R_5 := \mathbb{Z}[w]^*A_5 \cup \{\frac{\pm 1}{1-w}(1,w,w^2,1,w,w^2)_\sigma\}$.
- $R_6 := D_6(1-w) \cup \{\frac{\pm 1}{1-w}(u_1,u_2,u_3,u_4,u_5,u_6), u_i \in \mathbb{Z}[w]^* \mid u_i \equiv 1 \mod (1-w)$ and $\sum_{i=1}^{6} u_i \equiv 0 \mod 3\}$.

where $(x_1,\ldots,x_n)_\sigma$ denotes any permutation of $(x_1,\ldots,x_n)$.

The lattice spanned by R_6 is the Coxeter-Todd lattice K_{12}. Table 1 summarizes the properties of these root systems.

The irreducible root systems over $\mathbb{Q}_{2,\infty}$ which can occur as the roots of an integral lattice are, apart from the $\mathcal{M}^*R$ where R is a Euclidean root system:

- $D_n(1-w) := \{(u,v,0,\ldots,0)_\sigma \in \mathbb{H}^n \mid u,v \in \mathcal{M}^*, u+v \equiv 0 \mod 1-w\}$.
- $D_n(1+i) := \{(u,v,0,\ldots,0)_\sigma \in \mathbb{H}^n \mid u,v \in \mathcal{M}^*, u+v \equiv 0 \mod 1+i\}$.
- The root systems S_1, S_3 and U_5 given in Table II of [4].

The lattice spanned by S_3 is the Barnes-Wall lattice BW_{16}, the one spanned by S_1 is a sublattice of index $1+i$ of the previous one, and the one spanned by U_5 is a hermitian unimodular lattice of quaternionic rank 5. Table 2 summarizes the properties of these root systems.

Feit's classification of the $\mathbb{Z}[w]$-hermitian unimodular lattices of relative dimension 12 shows in particular that the roots of such a lattice span the

Table 2:

R	$\|R\|$	$h(R)$	$\det(L_R)$
$\mathcal{M}^*A_n$	$12n(n+1)$	$n+1$	$n+1$
$\mathcal{M}^*D_n$	$24n(n-1)$	$2(n-1)$	4
$D_n(1-w)$	$36n(n-1)$	$3(n-1)$	$(1-w)^2$
$D_n(1+i)$	$24n(4n-3)$	$2(4n-3)$	$(1+i)^2$
$\mathcal{M}^*R_5$	1080	18	2
$\mathcal{M}^*R_6$	3024	42	1
$\mathcal{M}^*E_6$	864	12	3
$\mathcal{M}^*E_7$	1512	18	2
$\mathcal{M}^*E_8$	2880	30	1
S_1	864	18	$(1+i)^2$
S_3	4320	90	1
U_5	3960	66	1

whole space, just like for the Niemeier lattices of minimum 2. B. Venkov has shown that one could prove *a priori* that an even unimodular lattice of dimension 24 has a root system either empty or of rank 24, and that in this last case it should belong to a limited set of possibilities because the Coxeter number of its irreducible components have to be equal. His argument relies on the use of theta series with harmonic coefficients. We prove here a completely analogous result for the $\mathbb{Z}[w]$-unimodular lattices of relative dimension 12 and for the $\mathcal{M}$-unimodular lattices of relative dimension 8.

Proposition 5.4 *Let L be a $\mathbb{Z}[w]$-hermitian unimodular lattice (respectively a $\mathcal{M}$-hermitian unimodular lattice) of dimension n. If $n \leq 12$ (respectively $n \leq 8$) and $R(L) \neq \emptyset$, then $R(L)$ has rank n, and the irreducible root systems occurring in $R(L)$ have the same Coxeter number.*

Proof. We briefly sketch the proof, since it is essentially the same as the one in [5, Chap 18, Prop. 2]. The study of the theta series with spherical coefficients for the modular lattices ([3], Theorem 3.1 and Proposition 3.2) shows that, in this range of dimension, we have

$$\sum_{r \in R(L)} P(r) = 0 \tag{34}$$

for all $P \in \mathrm{Harm}_2$. We then take $P(x) = Z_0^{(2)}(x,y)$ or $P(x) = Z_{0,0,0}^{(2)}(x,y)$ and obtain (here $h(x,y)$ stands for the complex or quaternionic hermitian form on $\mathbb{R} \otimes_{\mathbb{Q}} K^n$):

$$\sum_{r \in R(L)} h(y,r)\overline{h(y,r)} = \frac{2|R|}{n} h(y,y). \tag{35}$$

Taking $y \in R(L)^{\perp}$, we see that $y = 0$, and taking y in an irreducible component of the root system, we see from Proposition 5.1 that its Coxeter number is independent of the chosen component. □

Remark 5.5 *The previous proposition gives a strong constraint on the possible root systems for unimodular lattices. Of course it does not say anything on the eventuality that $R(L) = R_0^k$ for some R_0.*

In the case of $K = \mathbb{Q}(w)$ and $n = 12$, and if we assume that $R(L)$ contains at least two different types of irreducible root systems, from the inspection of Table 1, $R(L)$ is one of the following: $\mathbb{Z}[w]^*E_7 \perp R_5$ or $\mathbb{Z}[w]^*A_8 \perp D_4(1-w)$. It remains to study the effective existence of $\mathbb{Z}[w]$-hermitian unimodular lattices of dimension 12 with such roots. Feit's classification [9] proves that in both cases one and exactly one such lattice exists.

In the case of $K = \mathbb{Q}_{2,\infty}$ and $n = 8$, we are left with three possible root systems, $D_3(1+i) \perp \mathcal{M}^*U_5$, $\mathcal{M}^*A_5 \perp D_3(1-w)$ and $\mathcal{M}^*D_6 \perp D_2(1+i)$. It is proved in [2] that such lattices do exist and are unique.

5.2 Extremal hermitian unimodular lattices.

The property of a lattice L to be extremal forces its theta series to be uniquely determined. It also gives a constraint on the Jacobi theta series associated to the lattice, which, if the dimension is not too large, determines it uniquely. In [3], we make use in the Euclidean case of a method involving the properties of the theta series with spherical coefficients to compute such Jacobi theta series. It involves the zonal functions for the orthogonal group acting on the unit sphere, expressed in terms of the Gegenbauer polynomials.

In this section, we apply the same method but replace the polynomials used in [3] by the zonal functions for the unitary groups, the computation of which is explained in Sections 3 and 4. Since the general method is explained in details in [3], we shall not give here more information about it.

Let L be a hermitian lattice over K with the notations of the beginning of Section 5. Our goal is the computation of the following numbers:

$$N_{m,z}(y) := \mathrm{card}\{x, x \in L \mid h_K(x,x) = m \text{ and } h_K(x,y) = z\} \tag{36}$$

for certain choices of y (basically, y is a minimal vector of L).

We denote $L_{2m} := \{x, x \in L \mid h_K(x,x) = m\}$ (so that the index of L refers to the Euclidean norm $x \cdot x = 2h_K(x,x)$). The coefficient of q^m in the spherical theta series $\theta_{L,P} := \sum_{x\in L} P(x) q^{x\cdot x/2}$ equals the sum

$$\sum_{x\in L_{2m}} P(x). \tag{37}$$

Since the set L_{2m} is invariant under left multiplication by the elements of the finite group O_K^*, which act as a subgroup of the orthogonal group of the whole space, we can restrict our attention to the elements of $\mathrm{Harm}_k^{O_K^*}$. If the group O_K^* is reduced to $\{\pm 1\}$, it only means that we consider the polynomials of even degree. In the general case, the zonal functions which are invariant under the action of a given subgroup U of U_1 or of Q_1 are easy to compute. In the quadratic case, it means that we need to consider only the $Z_w^{(k)}$ with $w \equiv 0 \mod |U|$. In the quaternionic case, see the remark following Proposition 4.5.

5.2.1 $K = \mathbb{Q}(\sqrt{-3})$.

We consider an extremal lattice L of dimension $n = 6n'$ a multiple of 6. Let $S(L)$ denote the set of its minimal vectors, which have norm $2m = 2n' + 2$ (from (27)). The computation of the coefficients of the theta series of such lattices does not show any contradiction with their existence until $n' = 63$ ([19]). However, Feit's classification has shown that no extremal lattice exists for $n' = 2$ and none of them are constructed for higher n'.

It turns out that the numbers $N_{m,z}(y)$ (36) for $y \in S(L)$ are independent of the choice of y up to $n = 24$. It is worth noticing that only a finite number of z can satisfy $N_{m,z}(y) \neq 0$, and that $\sum_z N_{m,z}(y) = |S(L)|$ the first non-zero coefficient of the theta series of L. Table 3 gives the results of the computation of these numbers for the dimensions 12, 18, 24. We have omitted the value $N_{m,m}(y) = 6$ and we have taken z modulo $\mathbb{Z}[w]^*$ since clearly $N_{m,z}(y) = N_{m,uz}(y)$ for all $u \in \mathbb{Z}[w]^*$.

Theorem 5.6 *Extremal $\mathbb{Z}[w]$-hermitian unimodular lattices of dimension 24 cannot exist.*

Proof. The numbers found in Table 3 cannot correspond to a lattice, although they are integral and positive, because they do not satisfy a certain convexity condition (analogous to the one used in [3, Prop. 7.1]) that we explain now:

Table 3: Computation of $N_{m,z}(y)$ for extremal unimodular $\mathbb{Z}[w]$-lattices, for $y \in S(L)$ and for $2m = \min(L)$.

dim(L)	min(L)	$N_{m,0}$	$N_{m,1}$	$N_{m,1-w}$	$N_{m,2}$	$N_{m,1+3w}$	$N_{m,3+w}$
12	6	1496	2673	198			
18	8	31569	67456	6528	2176		
24	10	598644	1461075	217350	75900	2875	2875

We use the hermitian product on Hom_k defined in (24), which has the property that $< (x \cdot y)^k, h >= h(y)$ for all $h \in \mathrm{Harm}_k$ (see [22]). We consider the element $H_k := \sum_{y \in S(L)} (x \cdot y)^k$ and its orthogonal projection $H_{k,w}$ on $V_w^{(k)}$. The positivity conditions: $< H_{k,w}, H_{k,w} > \geq 0$ must hold; on the other hand, the next lemma shows that $< H_{k,w}, H_{k,w} >$ is a linear combination of the numbers from Table 3.

Lemma 5.7 *Let $S \subset S^{2n-1}$ be a finite subset of the unit sphere. Let $H_k := \sum_{y \in S} (x \cdot y)^k$ and let $H_{k,w}$ be its orthogonal projection on $V_w^{(k)}$. Then*

$$< H_{k,w}, H_{k,w} >= \lambda_{k,w} \sum_{y,y' \in S} Z_w^{(k)}(y, y') \tag{38}$$

where $\lambda_{k,w} \in \mathbb{R}$ and has the same sign as $\sum_{r=0}^{(k+w)/2} \alpha_r$ with the notations of Definition 3.3.

Proof. Clearly, for y' fixed, the projection p of $(x \cdot y')^k$ onto $V_w^{(k)}$ is a zonal function so it is equal to $\lambda Z_w^{(k)}(x, y')$ for some $\lambda \in \mathbb{C}$. Since $< p, Z_w^{(k)}(x, y') >=< (x \cdot y')^k, Z_w^{(k)}(x, y') >= Z_w^{(k)}(y', y')$, we can calculate $\lambda = Z_w^{(k)}(y', y') / < Z_w^{(k)}(x, y'), Z_w^{(k)}(x, y') >$, which is independent of $y' \in S^{2n-1}$ and has the sign of $Z_w^{(k)}(y', y') = \sum_r \alpha_r$. Hence $< H_{k,w}, H_{k,w} >=< H_k, H_{k,w} >= \sum_{y \in S} H_{k,w}(y) = \lambda \sum_{y,y' \in S} Z_w^{(k)}(y, y')$. □

We conclude the proof of the theorem: since $Z_w^{(k)}(y, y')$ is a function of $h(y, y')$, the sum expressing $< H_{k,w}, H_{k,w} >$ is a linear combination of the numbers $N_{m,z}(y)$. In the case under consideration, we take $Z_6^{(6)}(y, y') = h(y, y')^6$ which gives a negative result, and therefore contradicts the existence of such a lattice. □

Remark 5.8 *The same argument yields the non existence of an extremal lattice in dimension* 12*. It does not say anything for the dimension* 18*, and the question of the existence of an extremal* $\mathbb{Z}[w]$*-unimodular lattice remains open in this case (such a lattice would have a better density that any other known Euclidean lattice of dimension* 36*).*

For the $\mathcal{M}$*-lattices, the method does not lead to significant results; for* $n = 8$*, the numbers* $N_{m,z}(y)$ *are uniquely determined but not for* $n = 12, 16$*, and we cannot deduce anything for the existence of extremal lattices.*

References

[1] C. Bachoc, Voisinage au sens de Kneser pour les réseaux quaternioniens, Comment. Math. Helv. **70** (1995), 350-374.

[2] C. Bachoc and G. Nebe, Classification of two genera of 32-dimensional lattices over the Hurwitz order, Experiment. Math. **6(2)** (1997), 151-162.

[3] C. Bachoc and B. Venkov, Modular forms, lattices and spherical designs, in "Réseaux euclidiens, "designs" sphériques et groupes", J. Martinet, éd., Enseign. Math., Monographie n∘ 37", Genève (2001), to appear.

[4] A. M. Cohen, Finite quaternionic reflection groups, J. Algebra (64) 2 (1980), 293-324.

[5] J. Conway and N.J.A. Sloane, "Sphere packings, Lattices and Groups", Springer-Verlag, 1988.

[6] Ph. Delsarte, J.M. Goethals and J.J. Seidel, Spherical codes and designs, Geom. Dedicata (6) (1977), 363-388.

[7] W. Ebeling, "Lattices and Codes", Vieweg, 1994.

[8] M. Eichler and D. Zagier, "The theory of Jacobi forms" Progress in Mathematics (55), Birkhäuser, 1985.

[9] W. Feit, Some lattices over $\mathbb{Q}(\sqrt{-3})$, J. Algebra (52) (1978), 248-263.

[10] R. Goodman and N. R. Wallach, "Representations and invariants of the classical groups", Cambridge University Press, 1998.

[11] S. G. Hoggar, t-designs in projective spaces, European J. Combin. 3 (1982), 233-254.

[12] T. Ibukiyama and Y. Ihara, On automorphic forms on the unitary symplectic group $\mathrm{Sp}(n)$ and $\mathrm{SL}_2(\mathbb{R})$, Math. Ann. 278 (1987), 307-327.

[13] F.J. MacWilliams, A. M. Odlyzko, N.J.A. Sloane and H.N. Ward, Self-Dual Codes over GF(4), J. Combin. Theory Ser. A (1978),288–318.

[14] G. Nebe, Finite subgroups of $\mathrm{GL}_{24}(\mathbb{Q})$, Experiment. Math. 5 (1996), no. 3, 163-195.

[15] G. Nebe, The root lattices of the complex reflection groups, J. Group Theory 2 (1999), no. 1, 15-38.

[16] H.-G. Quebbemann, Modular Lattices in Euclidean Spaces, J. Number Theory (54) (1995), 190-202.

[17] H.-G. Quebbemann, Atkin-Lehner eigenforms and strongly modular lattices, Enseign. Math. (43) (1997), 55-65.

[18] R. Scharlau and B. Hemkemeier, Classification of integral lattices with large class number, Math. Comp. (67) 222 (1998), 737-749.

[19] R. Scharlau and R. Schulze-Pillot, Extremal Lattices, "Algorithmic Algebra and Number Theory" (Heidelberg 1997), 139-170, Springer, Berlin, 1999

[20] G. C. Shephard and J. A. Todd, Finite unitary reflection groups, Canad. J. Math 6 (1954), 274-304.

[21] A. Schiemann, Classification of hermitian forms with the neighbour method, J. Symbolic Comput. (26) 4 (1998), 487-508.

[22] B. Venkov, Réseaux et designs sphériques, Notes taken by J. Martinet of lectures by B. Venkov (1996-1997, Bordeaux), in "Réseaux euclidiens, "designs" sphériques et groupes", J. Martinet, éd., Enseign. Math., Monographie n∘ 37", Genève (2001), to appear.

[23] B. Venkov, Even unimodular extremal lattices, Proc. Steklov Inst. Math. (165) (1984), 47-52.

[24] N. J. Vilenkin, "Representation of Lie groups and special functions, Volume 2", Mathematics and its Applications (74) (1993), Kluwer Academic Publishers.