HURWITZ QUATERNIONIC INTEGERS AND SEIFERT FORMS

L'Enseignement Mathématique, t. 39 (1993), p. 107-119

HURWITZ QUATERNIONIC INTEGERS AND SEIFERT FORMS

by Parvati SHASTRI

Dedicated to the memory of late Prof. K.G. Ramanathan

§1. INTRODUCTION

The aim of this paper is to answer a question which arose from the work of Kervaire [K] on Seifert forms.

A *Seifert form* B on a finitely generated free $\mathbf{Z}$-module L, is a bilinear form

$$B : L \times L \to \mathbf{Z}$$

such that $B + B'$ is unimodular, i.e. $\det(B + B') = \pm 1$, where B' denotes the transpose of B. Such forms occur in knot theory. The Seifert form associated with the fibres of an odd dimensional fibred knot is unimodular. Motivated by this, M. Kervaire considers in [K] the following question:

1.1. QUESTION. Let S be a unimodular symmetric bilinear form on a finitely generated free $\mathbf{Z}$-module L. Does there exist a unimodular form

$$B : L \times L \to \mathbf{Z} \,,$$

such that $S = B + B'$?

If S admits such a decomposition, then obviously B is not symmetric and S is even. If S is indefinite, the answer to the above question is easily shown to be in the affirmative if and only if the rank of L exceeds 2 ([K], p. 176). To answer the question in the positive definite case, Kervaire introduces the notion of a perfect isometry.

1.2. *Definition.* Let R be a commutative ring and M a finitely generated R-module. An R-linear isomorphism τ of M is called *perfect* if $1 - \tau$ is invertible.

He proves:

1.3. PROPOSITION. *A unimodular symmetric bilinear form S admits a decomposition $S = B + B'$ with B unimodular if and only if S has a perfect isometry.*

Thus, Question 1.1 reduces to the following.

1.4. QUESTION. Given a unimodular symmetric bilinear form S, does there exist a perfect isometry of S?

Note that if S is positive definite and even, then the rank of S is a multiple of 8. M. Kervaire gives a complete answer to Question 1.4, for positive definite forms of rank less than or equal to 24. For forms of arbitrary rank, he proves the following partial result, using the theory of the associated root systems.

Let $\mathrm{R} = \{x \in L \mid S(x, x) = 2\}$. Suppose that R is a root system in $\mathbf{R}^n$ of rank n ($=$ rank L). Then the irreducible components of R are of type A, D, or E; and we have:

1.5. THEOREM ([K], Cor. 3, Prop. 4).

(a) *If* R *has an irreducible component of type* A_{2k-1}, E_7 *or* D_{k+4}, *with* $k \geqslant 1$, *then there does not exist any perfect isometry of* (L, S).

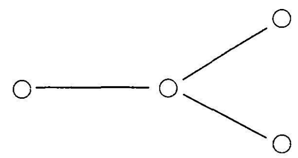
(b) *If* $\mathrm{R} = \perp_{1 \leqslant i \leqslant p} \mathrm{A}_{2k_i} \perp q\mathrm{E}_6 \perp r\mathrm{E}_8$, *then there exists a perfect isometry of* L, *inducing a perfect isomorphism of the abelian group* $\mathbf{Z}\mathrm{R}^{\#}/\mathbf{Z}\mathrm{R}$, *which corresponds to multiplication by* -1, *where* $\mathbf{Z}\mathrm{R}^{\#}$ *denotes the dual of the lattice* $\mathbf{Z}\mathrm{R}$.

Note that the case of R having an irreducible component of type D_4 is not covered by this theorem. In this paper we give an analogue of (b) for this case. In fact, we first consider the case in which R is of type $n\mathrm{D}_4$. In this case, we show (Th. 5.2) that (L, S) admits a perfect isometry if and only if the isometry class of (L, S) contains a symmetric bilinear space (L', S') of some hermitian space over the Hurwitz quaternionic integers. The analogue of Proposition 1.5 follows from this immediately (Theorem 5.3). In the final section we also give some examples.

§2. THE ROOT SYSTEM D_4 AND THE HURWITZ QUATERNIONIC INTEGERS

The fact that the root lattice $\mathbf{Z}\mathrm{D}_4$ can be identified with the lattice of Hurwitz quaternionic integers was long recognized: see for instance ([C-S]). However we give here a direct proof of this fact and recall some arithmetical facts about these quaternionic integers, which are needed in the sequel.

We first fix the following terminology. By a $\mathbf{Z}$-*lattice* we mean a pair (L, b), where L is a finitely generated free $\mathbf{Z}$-module and $b: L \times L \to \mathbf{Z}$ a positive definite, even, symmetric bilinear form. If the set $\{x \in L \mid b(x, x) = 2\}$ forms a root system of type nD_4 where the rank of L equals $4n$, then we call it a $\mathbf{Z}$-*lattice of type* nD_4. If L is contained in $\mathbf{R}^m$ and b is induced by the Euclidean inner product on $\mathbf{R}^m$, we call it a *Euclidean* $\mathbf{Z}$-*lattice*. The symbol D_4 will always mean the root system in $\mathbf{R}^4$ with the Euclidean inner product, corresponding to the Dynkin diagram



Let $\mathscr{A} = \mathbf{Q} \oplus \mathbf{Q}i \oplus \mathbf{Q}j \oplus \mathbf{Q}k$ denote the quaternion division algebra over $\mathbf{Q}$, defined by

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k .$$

Let $h: \mathscr{A}^n \times \mathscr{A}^n \to \mathscr{A}$ be the hermitian form defined by

$$h((x_1 \dots x_n), (y_1, \dots, y_n)) = \sum_1^n x_i \bar{y}_i ,$$

where bar denotes the conjugation in $\mathscr{A}$. If $Tr: \mathscr{A} \to \mathbf{Q}$ denotes the trace map $Tr(x) = x + \bar{x}$, then $Tr \circ h$ is a positive definite symmetric bilinear form over $\mathbf{Q}$. Let $\mathscr{H}$ denote the Hurwitz quaternionic integers in $\mathscr{A}$ i.e. $\mathscr{H} = \{(a + bi + cj + dk)/2 \mid a, b, c, d \in \mathbf{Z}$, with the same parity$\}$. Then, $\mathscr{H}$ is a maximal order in $\mathscr{A}$ and $(\mathscr{H}, Tr \circ h)$ is a $\mathbf{Z}$-lattice. It is trivial to verify that $\xi_1 = (1 + i + j + k)/2$, $\xi_2 = (1 + i + j - k)/2$, $\xi_3 = (1 + i - j + k)/2$, and $\xi_4 = (1 - i + j + k)/2$ form a $\mathbf{Z}$-basis of $\mathscr{H}$. Let $\mathscr{H}^*$ denote the dual of $\mathscr{H}$ in $\mathscr{A}$. Then we have

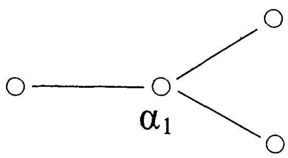
2.1. PROPOSITION.

(a) *The* $\mathbf{Z}$-*lattice* $(\mathscr{H}, Tr \circ h)$ *is isometric to the Euclidean lattice* $\mathbf{Z}D_4$.

(b) *The group of units of* $\mathscr{H}$ *forms a root system isomorphic to* D_4.

(c) *Every* $\mathbf{Z}$-*lattice of type* nD_4 *is isometric to a* $\mathbf{Z}$-*lattice* L *such that* $\mathscr{H}^n \subset L \subset \mathscr{H}^{*n}$, *where the bilinear form on* L *is induced by* $Tr \circ h$.

Proof. Let $\{\varepsilon_i\}$ denote the standard orthonormal basis in $\mathbf{R}^4$, and let $\alpha_1 = \varepsilon_2 - \varepsilon_3$, $\alpha_2 = \varepsilon_1 - \varepsilon_2$, $\alpha_3 = \varepsilon_3 - \varepsilon_4$, $\alpha_4 = \varepsilon_3 + \varepsilon_4$. Then $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ is a basis for the root system D_4. The associated Dynkin diagram is given by



If b denotes the Euclidean inner product on $\mathbf{R}^4$, then, $\tau: \mathscr{H} \to \mathbf{Z}D_4$ defined by $\tau(\xi_1) = \alpha_1$, $\tau(\xi_i) = -\alpha_i$, $2 \leqslant i \leqslant 4$, is an isometry of $(\mathscr{H}, Tr \circ h)$ onto $(\mathbf{Z}D_4, b)$. This proves (a). We note that an element x in $\mathscr{H}$ is a unit if and only if $Tr \circ h(x) = 2$. Hence (b) follows from the above isometry. Since $Tr \circ h$ is nondegenerate, the dual of $\mathscr{H}$ in $\mathscr{A}$ is the same as the dual of $\mathscr{H}$ in $\mathscr{A} \otimes_Q \mathbf{R} \simeq \mathbf{R}^4$. From (a) it follows that $\mathscr{H}^*$ is isometric to $(\mathbf{Z}D_4)^{\#}$. Thus (c) follows from the fact that every $\mathbf{Z}$-lattice of type nD_4 is isometric to a Euclidean $\mathbf{Z}$-lattice L such that $(\mathbf{Z}D_4)^n \subset L \subset (\mathbf{Z}D_4^{\#})^n$.

Let us now recall a few arithmetical facts about the Hurwitz quaternionic integers, details of which can be found in [R]. The dual $\mathscr{H}^*$ is a two-sided full $\mathscr{H}$-module in $\mathscr{A}$ i.e. an $\mathscr{H}$-submodule of $\mathscr{A}$ which contains a $\mathbf{Q}$-basis of $\mathscr{A}$. The set of all two-sided full $\mathscr{H}$-submodules of $\mathscr{A}$ is a free abelian group with the set of all maximal ideals of $\mathscr{H}$ as basis. Further the inverse of $\mathscr{H}^*$ is a maximal ideal in $\mathscr{H}$. In fact, $(\mathscr{H}^*)^{-1} = \mathscr{P}$, $\mathscr{P} = (1 + i)$, $\mathscr{P}^2 = (2)$, $\mathscr{P} = \bar{\mathscr{P}}$, and $\mathscr{H}/\mathscr{P} \simeq \mathbf{F}_4$. We have,

2.2. PROPOSITION.

(a) *The quotient* $\mathscr{H}^*/\mathscr{H}$ *has the natural structure of a vector space of dimension one over* $\mathbf{F}_4$.

(b) *The hermitian form* h *induces a hermitian form* $\eta(h)$ *on* $\mathscr{H}^*/\mathscr{H}$, *with values in* $\mathscr{H}^{*2}/\mathscr{H}^*$, *which is isometric to the standard hermitian form on* $\mathbf{F}_4$.

Proof. (a) This follows from the fact that, $\mathscr{H}^*$ is an $\mathscr{H}$-module of rank one and $\mathscr{P}\mathscr{H}^* = \mathscr{H}^*\mathscr{P} = \mathscr{H}$.

(b) This follows from the commutativity of the diagram:

$$\begin{array}{ccc} \mathscr{H}^*/\mathscr{H} \times \mathscr{H}^*/\mathscr{H} & \to & \mathscr{H}^{*2}/\mathscr{H}^* \\ \downarrow & & \downarrow \\ \mathscr{H}/\mathscr{P} \times \mathscr{H}/\mathscr{P} & \to & \mathscr{H}/\mathscr{P} \end{array}$$

where the vertical arrows are the isomorphisms induced by multiplication by $1 + i$ and 2 respectively and the horizontal arrows are the respective hermitian forms.

From now on, we shall identify $\mathscr{H}^*/\mathscr{H}$ with $\mathbf{F}_4$, as a one dimensional vector space for the choice of the basis $1/1 + i$.

2.3. PROPOSITION.

(a) *Let* $\mathcal{H}^n \subseteq L \subseteq \mathcal{H}^{*n}$ *be a* **Z**-*module. Then* $(L, Tr \circ h)$ *is integral if and only if* $\eta(L)$ *is a totally isotropic subspace of the symmetric bilinear space* $(\mathbf{F}_4^n, Tr \circ \eta(h))$, *where* $\eta(h)$ *is the standard hermitian form on* $\mathbf{F}_4^n$.

(b) *The* **Z**-*lattice* $(L, Tr \circ h)$ *is unimodular if and only if* $\eta(L)$ *is a maximal totally isotropic subspace of* $(\mathbf{F}_4^n, Tr \circ \eta(h))$.

Proof. (a) This follows easily from 2.2.

(b) This follows from (a), since L is unimodular if and only if L is maximal integral.

§3. PERFECT ISOMETRIES OF $\mathcal{H}$-LATTICES

In this section we show that certain special class of **Z**-lattices admit perfect isometries. We begin with the following definition.

3.1. *Definition.* A **Z**-lattice (L, b) is called an $\mathcal{H}$*-lattice* if L is an $\mathcal{H}$-module and $b = Tr \circ h$ for some hermitian form h.

3.2. PROPOSITION. *Every* $\mathcal{H}$*-lattice has a perfect isometry.*

Proof. Let $(L, Tr \circ h)$ be an $\mathcal{H}$-lattice. Let $\sigma : L \to L$ denote left (or right) multiplication by ξ where ξ is one of the units $(1 \pm i \pm j \pm k)/2$. Then,

$$Tr \circ h(\sigma(x), \sigma(y)) = Tr \circ h(\xi x, \xi y) = Tr(\xi h(x, y)\bar{\xi})$$
$$= \xi h(x, y)\bar{\xi} + \xi \overline{h(x, y)}\bar{\xi} = \xi(h(x, y) + \overline{h(x, y)})\,\bar{\xi} = \xi\bar{\xi}(h(x, y) + \overline{h(x, y)})$$
$$= h(x, y) + \overline{h(x, y)} = Tr \circ h(x, y) .$$

Therefore σ is an isometry. Since the minimal polynomial of σ is $x^2 - x + 1$, $\det(1 - \sigma) = 1$ and hence σ is perfect.

As a special case of this we have:

3.3. COROLLARY. *The* $\mathcal{H}$*-lattice* $(\mathcal{H}, Tr \circ h)$ *has a perfect isometry.*

3.4. PROPOSITION. *Every perfect isometry of* $(\mathcal{H}, Tr \circ h)$ *induces a perfect* $\mathbf{F}_2$*-isomorphism of* $\mathcal{H}^*/\mathcal{H} = \mathbf{F}_4$, *which corresponds to multiplication by* ω, *where* $\mathbf{F}_2(\omega) = \mathbf{F}_4$.

Proof. Note that every perfect isometry σ of $\mathcal{H}$ extends naturally to a perfect isometry of $\mathcal{H}^*$, inducing a perfect $\mathbf{F}_2$-isomorphism $\eta(\sigma)$ of $\mathcal{H}^*/\mathcal{H}$, η denoting the induced map on the quotient. The proof of the proposition is complete in view of the following simple lemma.

3.5. LEMMA. *An $\mathbf{F}_2$-linear isomorphism of $\mathbf{F}_4$ is perfect if and only if it corresponds to multiplication by ω, where ω denotes a primitive element of $\mathbf{F}_4$ over $\mathbf{F}_2$.*

Proof. An $\mathbf{F}_2$-linear isomorphism of $\mathbf{F}_4$ is perfect if and only if it has no fixed point other than the trivial element. Since, $GL_2(\mathbf{F}_2) \simeq S_3$, it is easy to see that every perfect isomorphism of $\mathbf{F}_4$, corresponds to multiplication by ω, ω being as above.

3.6. PROPOSITION. *Let L be a $\mathbf{Z}$-lattice such that $\mathcal{H}^n \subseteq L \subseteq \mathcal{H}^{*n}$. If L is an $\mathcal{H}$-lattice, then L has a perfect isometry, which corresponds to multiplication by ω, on the quotient $\mathcal{H}^{*n}/\mathcal{H}^n$.*

Proof. Multiplication by ξ is a perfect isometry of $\mathcal{H}^n$ which extends naturally to a perfect isometry of $\mathcal{H}^{*n}$. Clearly the induced map on the quotient $\mathcal{H}^{*n}/\mathcal{H}^n$ is multiplication by ω. Since L is an $\mathcal{H}$-module, it preserves L as well.

In particular,

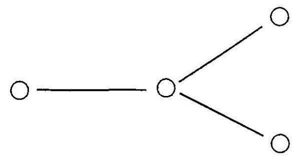
3.7. COROLLARY. *Every $\mathcal{H}$-lattice $(L, Tr \circ h)$ of type $n\mathrm{D}_4$ has a perfect isometry.*

It is but natural to ask whether every $\mathbf{Z}$-lattice of type $n\mathrm{D}_4$ which has a perfect isometry necessarily admits the structure of an $\mathcal{H}$-lattice. We shall show that this is indeed true. For doing this we need to recall some basic facts on the automorphisms of the root system $n\mathrm{D}_4$.

§4. AUTOMORPHISMS OF THE ROOT SYSTEM $n\mathrm{D}_4$ AND PERFECT ISOMETRIES

For any root system R, let $\mathcal{W}(\mathrm{R})$ denote the Weyl group of R (i.e. the group generated by the reflections defined by the roots). Then $\mathcal{W}(\mathrm{R})$ is a normal subgroup of $Aut\,\mathrm{R}$, which preserves every $\mathbf{Z}$-lattice L such that $\mathbf{Z}\mathrm{R} \subseteq L \subseteq \mathbf{Z}\mathrm{R}^{\#}$. We thus get a natural map $\eta: Aut\,\mathrm{R}/\mathcal{W}(\mathrm{R}) \to Aut_{\mathbf{Z}}(\mathbf{Z}\mathrm{R}^{\#}/\mathbf{Z}\mathrm{R})$. In view of ([H], p. 72; [C-S], p. 432) this is an injection.

An element σ in $Aut(\mathrm{R})/\mathscr{W}(\mathrm{R})$ preserves L if and only if $\eta(\sigma)$ preserves the corresponding subgroup $\eta(L)$ of $\mathbf{Z}\mathrm{R}^{\#}/\mathbf{Z}\mathrm{R}$. If $\mathrm{R} = \mathrm{D}_4$, $Aut\,\mathrm{R} = \mathscr{W}(\mathrm{R}) \underset{s}{\ltimes} S_3$, where, $\underset{s}{\ltimes}$ denotes the semi direct product and S_3 is the automorphism group of the associated Dynkin diagram:



Consequently, for $\mathrm{R} = n\mathrm{D}_4$, $Aut\,\mathrm{R}/\mathscr{W}(\mathrm{R}) \simeq S_3^n \underset{s}{\ltimes} S_n \simeq (GL_2(\mathbf{F}_2))^n \underset{s}{\ltimes} S_n$. Thus the elements of $Aut\mathrm{R}/\mathscr{W}(\mathrm{R})$ are "monomial matrices" where each row and each column consists of exactly one element of $GL_2(\mathbf{F}_2)$. It acts naturally on $(\mathbf{Z}\mathrm{D}_4^{\#})^n/\mathbf{Z}\mathrm{D}_4^n$. In view of the identification of $\mathbf{Z}\mathrm{D}_4^{\#}/\mathbf{Z}\mathrm{D}_4 \simeq \mathscr{H}^*/\mathscr{H}$, we have the following proposition.

4.1. PROPOSITION.

(a) $Aut(\mathscr{H}^n)/\mathscr{W}(\mathscr{H}^n) \simeq S_3^n \underset{s}{\ltimes} S_n \simeq (GL_2(\mathbf{F}_2))^n \underset{s}{\ltimes} S_n$.

(b) *If U denotes the group of units of $\mathscr{H}$, then U is a subgroup of $Aut\,\mathscr{H}$ and $U/(\mathscr{W}(\mathscr{H}) \cap U) \simeq \{1, \omega, \omega^2\}$, where $\mathbf{F}_2(\omega) = \mathbf{F}_4$.*

(c) *The conjugation in $\mathscr{H}$ belongs to the Weyl group $\mathscr{W}(\mathscr{H})$.*

Proof. (a) This statement is an immediate consequence of the identification $\mathbf{Z}\mathrm{D}_4 \simeq \mathscr{H}$.

(b) By (a), $Aut\,\mathscr{H}/\mathscr{W}(\mathscr{H}) \simeq S_3 \simeq GL_2(\mathbf{F}_2)$. Since $\eta(U) = \{1, \omega, \omega^2\}$, (b) follows.

(c) The conjugation in $\mathscr{H}$ is a product of reflections defined by i, j and k.

We now consider the perfect isomorphisms of $(\mathscr{H}^{*n})/\mathscr{H}^n$ arising out of $Aut(\mathscr{H}^n)/\mathscr{W}(\mathscr{H}^n)$. We begin by fixing the following notation:

Let $V = \mathbf{F}_4^n = X_1 \perp X_2 \perp \ldots X_n$ with respect to the standard hermitian form on V, where $X_i \simeq \mathbf{F}_4 = \mathbf{F}_2 \oplus \mathbf{F}_2 = \{0, 1, \omega, \omega^2\}$. Let G denote the group of all $n \times n$ monomial matrices with entries in $M_2(\mathbf{F}_2)$, where each row and each column consists of exactly one element of $GL_2(\mathbf{F}_2)$. Note that every element of G can be uniquely expressed as $\alpha . \tau$, where α is the diagonal matrix $\operatorname{diag}(\alpha_1, \ldots, \alpha_i, \ldots, \alpha_n)$, with α_i in $GL_2(\mathbf{F}_2)$ and τ is an $n \times n$ permutation matrix. We have, 4.2. LEMMA. *Let* σ *belonging to* G *be perfect and let* $X = X_i$ *for some* i. *Let* m *be the smallest positive integer for which* σ^m *maps* X *onto itself. Then* σ^m/X *is perfect.*

Proof. The idea of the proof is similar to ([K], Prop. 2). We show that $(1-\sigma^m)/X$ is surjective. Let $M = \sum_{0 \leqslant i \leqslant m-1} \sigma^i(X)$. Then σ leaves M invariant. Therefore σ is a perfect isomorphism of M. Hence $(1-\sigma)/M$: $M \to M$ is surjective. Let x be an element of X. Since, $(x, 0, \ldots, 0)$ belongs to M, there exists an element y in M such that $(1-\sigma)(y) = (x, 0, \ldots, 0)$. Let $y = (y_0, y_1, \ldots, y_{m-1})$, where y_i belongs to $\sigma^i(X)$. Then,

$$(1-\sigma)(y) = (y_0 - \sigma(y_{m-1}), \quad y_1 - \sigma(y_0), \ldots, y_{m-1} - \sigma(y_{m-2})) .$$

Hence, $y_0 - \sigma(y_{m-1}) = x, y_1 = \sigma(y_0), \ldots, y_{m-1} = \sigma(y_{m-2})$. Further, $\sigma(y_{m-1}) = \sigma^2(y_{m-2}) = \ldots = \sigma^m(y_0)$. Thus $(1-\sigma^m)(y_0) = x$. This implies that $(1-\sigma^m)/X$ is surjective.

4.3. COROLLARY. *Let* σ *be an element of* G *which is perfect. Suppose that* $\sigma = \alpha . \tau$, *where* $\alpha = \operatorname{diag}(\alpha_1, \ldots, \alpha_i, \ldots, \alpha_n)$, $\alpha_i \in GL_2(\mathbf{F}_2)$, $\tau = \tau_1 . \tau_2 \ldots \tau_r$, *and* τ_i *are disjoint cyclic permutations of length* n_i. *Let* T_i *denote the set of indices belonging to the permutation* τ_i. *Then* $(\sigma)^{n_i}/X_j$ *is perfect for every* j *belonging to* T_i.

Proof. Note that for every j belonging to T_i, n_i is the smallest positive integer such that $(\sigma)^{n_i}$ maps X_j onto itself.

4.4. COROLLARY. If σ *is as above, then* $(\sigma)^{n_i}/X_j$ *corresponds to multiplication by* ω *or* ω^2, *for every* j *belonging to* T_i.

Proof. Follows from Corollary 4.3, and Lemma 3.5.

4.5. COROLLARY. *If* σ *is as above, and* $X^{(i)} = \sum_{j \in T_i} X_j$, *then* $(\sigma)^{n_i}/X^{(i)}$ *is the matrix* $\operatorname{diag}(\alpha_1, \ldots, \alpha_j, \ldots \alpha_{n_i})$, *where* α_j *belongs to* $\{\omega, \omega^2\}$.

Proof. Clear from Corollary 4.4.

4.6. PROPOSITION. *Let* σ *be an element of* G *which is perfect and let* $\sigma = \alpha . \tau$, *where* α *and* τ *are as in Corollary 4.4. Then there exists an integer* $l \geqslant 1$, *such that* σ^l *is perfect and* $\sigma^l = \beta . \tau'$, *where* β *is the matrix* $\operatorname{diag}(\beta_1, \ldots, \beta_j, \ldots, \beta_n)$, *with* β_j *in* $GL_2(\mathbf{F}_2)$ *and* τ' *is a product of disjoint cyclic permutations* τ_i *of length* 3^{k_i}.

Proof. Let $\tau = \tau_1 . \tau_2 \dots \tau_r$, where τ_i are disjoint cyclic permutations of length $n_i = 3^{k_i} . l_i$, with $(3, l_i) = 1$. Let l denote the least common multiple of the l_i. We show that σ^l is perfect. By Corollary 4.5, σ^{n_i}/X_j is multiplication by ω or ω^2 for every j belonging to T_i. This implies that $(\sigma)^{n_i l/l_i}/X_j$ corresponds to multiplication by ω or ω^2 for every such j, since $(l/l_i, 3) = 1$ and ω is an element of order 3. Hence, $(\sigma^l)^{3^{k_i}}/X^{(i)}$ is the matrix $\operatorname{diag}(\alpha_1, \dots, \alpha_j, \dots \alpha_{n_i})$ where α_j belongs to $\{\omega, \omega^2\}$. Clearly this implies that $\sigma^l/X^{(i)}$ has no nontrivial fixed point. Since T_i are disjoint, it follows that σ^l has no nontrivial fixed point and hence σ^l is perfect. Obviously σ^l has the required property and the proposition follows.

Now, let M be an $\mathbf{F}_2$-linear subspace of V, which is invariant under a perfect isomorphism σ belonging to G. By the previous proposition, we can assume, by replacing σ by σ^m, that M is invariant under $\sigma = \alpha . \tau$, where α is as in Corollary 4.4 and $\tau = \tau_1 . \tau_2 \dots \tau_r$, τ_i being cyclic permutations of length 3^{k_i}.

4.7. PROPOSITION. *If M is an $\mathbf{F}_2$-linear subspace of V which has a perfect isomorphism σ belonging to G, then M is invariant under the action of a diagonal matrix,* $\operatorname{diag}(\alpha_1, \dots, \alpha_i, \dots, \alpha_n)$ *where each α_i belongs to $\{\omega, \omega^2\}$.*

Proof. By replacing σ by a suitable power we may assume that

$$\sigma = \operatorname{diag}(\beta_1, \dots, \beta_i, \dots, \beta_n)\, \tau_1 \tau_2 \dots \tau_r$$

where β_i belongs to $GL_2(\mathbf{F}_2)$ for every i and τ_i are disjoint cyclic permutations of length 3^{k_i}. Further, since disjoint cycles commute we may assume that the length of τ_i is 3^k for $1 \leqslant i \leqslant s$ and the length of τ_i is less than 3^k for $s < i \leqslant r$. Let $T = \{i \in \{1, 2, \dots, n\} \mid i \text{ occurs in the permutation } \tau_1 \tau_2 \dots \tau_s\}$. Let $M_1 = M \cap \sum_{i \in T} X_i$ and $N_1 = M \cap \sum_{i \notin T} X_i$. We claim that $M = M_1 \oplus N_1$ and that M_1 is invariant under $\operatorname{diag}(\alpha_1, \dots, \alpha_i, \dots, \alpha_n)$, where each α_i belongs to $\{\omega, \omega^2\}$. Let $(x, y) \in M$, where $x \in \perp_{i \in T} X_i$, $y \in \perp_{i \notin T} X_i$. Since

$$\sigma^{3^k} = \operatorname{diag}(\alpha_1, \dots, \alpha_i, \dots, \alpha_n)\ ,$$

where α_i belongs to $\{\omega, \omega^2\}$ for $i \in T$ and $\alpha_i = 1$ for $i \notin T$, it follows that, $(x, y) + \sigma^{3^k}(x, y) + (\sigma^{3^k})^2(x, y) = (0, y)$ belongs to M. Hence $(x, 0)$ belongs to M as well. Thus $M = M_1 \oplus N_1$. Clearly M_1 is invariant under $\operatorname{diag}(\alpha_1, \dots, \alpha_i, \dots, \alpha_n)$, α_i being in $\{\omega, \omega^2\}$. Since σ/N_1 is perfect, by repeating the above argument we obtain a similar decomposition of $N_1 : N_1 = M_2 \oplus N_2$. This process terminates in a finite number of steps and we obtain a decomposition $M = M_1 \oplus M_2 \oplus \dots \oplus M_k$, where each M_j is invariant under $\operatorname{diag}(\alpha_1, \dots, \alpha_i, \dots \alpha_n)$, α_i being in $\{\omega, \omega^2\}$.

§5. Main Theorem and examples

In this final section we prove our main results 5.2, 5.3 and give some examples. We begin with,

5.1. Proposition. *Let L be a unimodular $\mathbf{Z}$-lattice of type $n\mathrm{D}_4$ such that $\mathscr{H}^n \subset L \subset \mathscr{H}^{*n}$. If L admits a perfect isometry, then there exists an isometry $\delta = \operatorname{diag}(\delta_1, \dots, \delta_i, \dots, \delta_n)$ on $\mathscr{H}^{*n}$, where δ_i is the isometry on $\mathscr{H}^*$ given by left multiplication by ξ or right multiplication by $\bar{\xi}$ such that L is invariant under δ.*

Proof. Let σ be a perfect isometry of $(L, Tr \circ h)$. Then σ induces an automorphism of $\mathscr{H}^n$ and extends naturally to a perfect isometry of $\mathscr{H}^{*n}$. In view of ([K], p. 179), $\eta(\sigma)$ is a perfect isomorphism of $\mathbf{F}_4^n$, leaving $\eta(L)$ invariant. Therefore by Proposition 4.7 there exists $\alpha = \operatorname{diag}(\alpha_1, \dots, \alpha_i, \dots, \alpha_n)$ with α_i in $\{\omega, \omega^2\}$ such that $\eta(L)$ is invariant under α. Let δ_i denote left multiplication on $\mathscr{H}^*$ by $\xi = (1 + i + j + k)/2$ if $\alpha_i = \omega$ and right multiplication by $\bar{\xi} = (1 - i - j - k)/2$, if $\alpha_i = \omega^2$. Let $\delta = \operatorname{diag}(\delta_1, \dots, \delta_i, \dots, \delta_n)$. Since δ induces an isometry of $\mathscr{H}^{*n}$ which fixes $\mathscr{H}^n$ and $\eta(\delta) = \alpha$ leaves $\eta(L)$ invariant it follows that δ leaves L invariant.

5.2. Theorem. *Let (L, S) be an unimodular $\mathbf{Z}$-lattice of type $n\mathrm{D}_4$. Then, L has a perfect isometry if and only if there exists an $\mathscr{H}$-lattice (L', S') such that $L \simeq L'$.*

Proof. Clearly every $\mathscr{H}$-lattice admits a perfect isometry (3.2). Conversely let (L, S) be a $\mathbf{Z}$-lattice of type $n\mathrm{D}_4$, which admits a perfect isometry. In view of Proposition 2.1, we can assume that $\mathscr{H}^n \subseteq L \subseteq \mathscr{H}^{*n}$ and $S = Tr \circ h$. By Proposition 4.7 there exists a subset T of $\{1, 2, \dots, n\}$ such that L is invariant under $\delta = (\delta_1, \dots, \delta_i, \dots, \delta_n)$, where δ_i is left multiplication by ξ for $i \in T$ and δ_i is right multiplication by $\bar{\xi}$ for $i \notin T$. Let $f : \mathscr{H}^n \to \mathscr{H}^n$ be defined by $f = \operatorname{diag}(f_1, \dots, f_i, \dots, f_n)$ where $f_i = \mathrm{id}$ for $i \in T$ and $f_i =$ the involution on $\mathscr{H}$ for $i \notin T$. Then it is easy to check that f is an isometry of $(L, Tr \circ h)$ onto (L', S') where, $L' = f(L)$, and,

$$S'(x, y) = \sum_{i \in T} (x_i \bar{y}_i + y_i \bar{x}_i) + \sum_{i \notin T} (\bar{x}_i y_i + \bar{y}_i x_i) .$$

Clearly L' is invariant under left multiplication by ξ. Further, since $\mathscr{P}L' \subseteq \mathscr{P}\mathscr{H}^{*n} \subseteq \mathscr{H}^n \subseteq L'$, it follows that L' is an $\mathscr{H}$-lattice.

Finally, we have the following analogue of Proposition 1.5 for the case of lattices having components of type D_4.

5.3. THEOREM. *Let (L, S), be a positive definite unimodular symmetric bilinear space over $\mathbf{Z}$, of rank n. Suppose that the set of vectors of norm 2 form a root system of type*

$$R = \underset{1 \leqslant i \leqslant p}{\perp} A_{2k_i} \perp qE_6 \perp rE_8 \perp sD_4$$

with, $\sum_{1 \leqslant i \leqslant p} 2k_i + 6q + 8r + 4s = n$. *Then the following hold:*

(i) *The $\mathbf{Z}$-lattice L decomposes as $L = L_1 \perp L_2 \perp L_3$, where each L_i is unimodular, with asociated root systems of type $R_1 = \underset{1 \leqslant i \leqslant p}{\perp} A_{2k_i} \perp qE_6$, $R_2 = rE_8$, $R_3 = sD_4$, respectively.*

(ii) *The $\mathbf{Z}$-lattice L admits a perfect isometry if and only if L_3 is isometric to the trace form of an $\mathscr{H}$-lattice.*

(iii) *If L admits a perfect isometry, then it admits a perfect isometry σ such that the induced map $\eta(\sigma)$ on $\mathbf{Z}R^{\#}/\mathbf{Z}R$, corresponds to multiplication by -1, on the components corresponding to A_{2k_i}, E_6, and E_8, and to multiplication by ω, on the components corresponding to D_4.*

Proof. (i) Since E_8 is unimodular, it is clear that $L = L_2 \perp K$, where $L_2 \simeq r\mathbf{Z}E_8$, and K is unimodular with associated root system of type $R_1 \perp R_3$. So to prove (i), it is enough to prove that K decomposes as $L_1 \perp L_3$. This would follow if we show that $\eta(K)$ decomposes as, $\eta(K) = \eta(K) \cap (\mathbf{Z}R_1^{\#}/\mathbf{Z}R_1) \perp \eta(K) \cap (\mathbf{Z}R_3^{\#}/\mathbf{Z}R_3)$.

Let $z = (x, y) \in \eta(K)$, with x in $\mathbf{Z}R_1^{\#}/\mathbf{Z}R_1$ and y in $\mathbf{Z}R_3^{\#}/\mathbf{Z}R_3$. Since $\mathbf{Z}R_1^{\#}/\mathbf{Z}R_1$ is a group of exponent $3 . \prod_{1 \leqslant i \leqslant p} (2k_i + 1)$, and $\mathbf{Z}R_3^{\#}/\mathbf{Z}R_3 \simeq \mathbf{F}_4^m$, it follows that, $(0, y) = 3(\prod_{1 \leqslant i \leqslant p} (2k_i + 1))z \in \eta(K)$. Hence (i) follows.

The results (ii) and (iii) follow from (i), (5.2) and ([K], Prop. 4).

5.4. *Examples.* We conclude this section by giving some examples of $\mathscr{H}$-lattices of type nD_4 as well as $\mathbf{Z}$-lattices of type nD_4 which are not $\mathscr{H}$-lattices. Let $\{e_k\}_{1 \leqslant k \leqslant n}$ denote the standard $\mathscr{H}$-basis of $\mathscr{H}^n$. We consider two cases. For $n = 4m$, let $\varepsilon_{j+1} = \sum_{k=2j+1}^{2j+4} e_k, 0 \leqslant j \leqslant 2m - 2$, and

$\varepsilon_{2m} = \sum_{k=0}^{2m-1} e_{2k+1}$. For $n = 4m + 2$, let $\varepsilon_{j+1} = \sum_{k=2j+1}^{2j+4} e_k, 0 \leqslant j \leqslant 2m - 1$, and $\varepsilon_{2m+1} = \sum_{k=0}^{2m-1} e_{2k+1} + \xi e_{4m+1} + \bar{\xi} e_{4m}$. Let $\lambda = 1/1 + i$ and let L_n be the $\mathscr{H}$-lattice generated by $\mathscr{H}^n \cup \{\lambda\varepsilon_1, \lambda\varepsilon_2, \ldots, \lambda\varepsilon_{n/2}\}$. In view of [M-O-S], $\eta(L)$ is a maximal totally isotropic subspace of $\mathbf{F}_4^n$, and every vector $x \in \eta(L)$ has at least four nonzero coordinates. Since $Tr \circ h(x, x) \geqslant 1$, for every x belonging to $\mathscr{H}^*$, it follows easily that the set of vectors of norm 2 in L_n is $n\mathrm{D}_4$. Clearly L_n is unimodular.

For $n = 6$, this gives the unique unimodular $\mathbf{Z}$-lattice of type $6\mathrm{D}_4$ which is also an $\mathscr{H}$-lattice. In view of [M-O-S], table III, and Proposition 2.3, one can determine all indecomposable $\mathbf{Z}$-lattices of type $n\mathrm{D}_4$ for $n \leqslant 14$, which are $\mathscr{H}$-lattices. The following construction gives an example of a $\mathbf{Z}$-lattice of type $8\mathrm{D}_4$ which does not admit a perfect isometry. (In particular this shows that the smallest dimension for which there exists a $\mathbf{Z}$-lattice of type $n\mathrm{D}_4$ which is not an $\mathscr{H}$-lattice is 32). For $1 \leqslant k \leqslant 8$, let ρ_k be equal to ξ if k is even and let ρ_k be equal to 1 if k is odd. Let $\beta_{j+1} = \sum_{i=2j+1}^{2j+4} \rho_i e_i$, $\beta_{j+4} = \sum_{i=2j+1}^{2j+4} \rho_{i+1} e_i$ for $n \leqslant j \leqslant 2$, $\beta_7 = \xi \,.\, \sum_{i=1}^{4} e_{2i}$ and $\beta_8 = \bar{\xi} \,.\, \sum_{i=1}^{4} e_{2i-1}$. Let Λ be the $\mathbf{Z}$-linear subspace of $\mathscr{H}^{*8}$ spanned by $\mathscr{H}^8$ and $\{\lambda\beta_i\}_{1 \leqslant i \leqslant 8}$. Then $\eta(\Lambda)$ is a maximal totally isotropic subspace of $(\mathbf{F}_4^8, Tr \circ \eta(h))$. It can be easily checked that Λ is a $\mathbf{Z}$-lattice of type $8\mathrm{D}_4$. Further $\eta(\Lambda)$ is not invariant under $\mathrm{diag}(\alpha_1, \ldots, \alpha_i, \ldots, \alpha_8)$ for any choice of α_i in $\{\omega, \omega^2\}$. Thus in view of Proposition 4.7, the lattice Λ does not admit any perfect isometry. The above construction easily generalizes to give a family of $\mathbf{Z}$-lattices Λ_{4n} of dimension $16m$, $m \geqslant 2$, which are not $\mathscr{H}$-lattices.

ACKNOWLEDGEMENT. I thank Eva Bayer for critically going through an earlier version of the manuscript and for making useful comments, which led to a better exposition of this work. My thanks are also due to my teachers R. Parimala and R. Sridharan who showed deep interest in my work. I thank H.G. Quebbemann for carefully going through the manuscript and making valuable suggestion.

REFERENCES

[C-S] CONWAY, J.H. and N.J.A. SLOANE. *Sphere packings, Lattices and Groups.* Springer Verlag, New York, Tokyo, 1988.

[H] HUMPHREY, J.E. *Introduction to Lie Algebra and Representation Theory.* Springer Verlag, New York, Berlin, 1972.

[M-O-S] MACWILLIAMS, F.J., A.M. ODLYZKO and N.J.A. SLOANE. Self dual codes over $GF(4)$. *JCT, Series A 25* (1978), 288-318.

[K] KERVAIRE, M. Formes de Seifert et formes quadratiques entières. *L'Enseignement Math. 31* (1985), 173-186.

[Q] QUEBBEMANN, H.G. An application of Siegel's formula over Quaternion orders. *Mathematika 31* (1984), 12-16.

[R] REINER, I. *Maximal Orders.* Academic Press, London, New York, 1975.

[V] VENKOV, B.B. The classification of integral even unimodular 24-dimensional quadratic forms. *TMIS 148* (1978), 65-76.

(Reçu le 9 mars 1992)

Parvati Shastri

Centre of Advanced Study
Department of Mathematics
University of Bombay, Vidyanagari
Bombay, 400098, India

vide-leer-empty