stichting
mathematisch
centrum

AFDELING ZUIVERE WISKUNDE ZN 93/79 NOVEMBER
(DEPARTMENT OF PURE MATHEMATICS)

A.M. COHEN

ON SUBLATTICES OF THE LEECH LATTICE AND PRIMITIVE REFLECTION GROUPS

2e boerhaavestraat 49 amsterdam

On sublattices of the Leech lattice and primitive reflection groups

by

Arjeh M. Cohen

ABSTRACT

The object of this paper is to prove that among the integral lattices invariant under a finite real primitive reflection group in dimension ≥ 3 there occurs a sublattice of the unimodular integral lattice of type E_8. An analogue for the complex primitive reflection groups is proved (where E_8 is replaced by the Leech lattice) as well as a partial result of this kind for the quaternionic case.

KEY WORDS & PHRASES: *Finite reflection groups, Leech lattice, lattice* E_8*, quaternions.*

0. INTRODUCTION

It is well known that to a finite unitary group a lattice Λ can be associated that is integral with respect to the unitary inner product h (cf. [4]). In the particular case of a (real, complex or quaternionic) reflection group such a lattice can be constructed from a so-called root system. Moreover, h determines a quadratic form which, if paired with the lattice, yields a known quadratic $\mathbb{Z}$-module (occurring in [8]) whose automorphism group contains the given reflection group. The choice of this quadratic form originates from [13]. It turns out that the lattices corresponding to root systems of the "exceptional" real and complex reflection groups occur within the Leech lattice Λ_{24}. This leads to the following result.

THEOREM.

(i) *Any real primitive reflection group* $\neq W(A_n)$ *in dimension* $n \geq 3$ *is a subgroup of the group* $W(E_8)$ *of automorphisms of the lattice of type* E_8.

(ii) *The commutator subgroup of any complex (non-real) primitive reflection group in dimension* $n \geq 3$ *can be embedded in either* $W(E_8)$ *or* $\mathrm{Aut}(\Lambda_{24})$, *the group of automorphisms of the Leech lattice.*

The proof of this theorem is given below. It depends on the classification of the reflection groups. As for the real reflection groups, BOURBAKI [1] is a good reference. The complex reflection groups are classified by SHEPHARD & TODD [9], who used results from H.H. Mitchell and H.F. Blichfeldt, and later by the author [2]. The quaternionic reflection groups are classified in [3]. The notations concerning these groups will follow those of [1], [2] and [3].

1. PRELIMINARIES

Let F be a subfield (possibly skew) of the skew field $\mathbb{H}$ of the real quaternions which is of finite degree over $\mathbb{Q}$ and is invariant under quaternionic conjugation $x \to \bar{x}$ $(x \in \mathbb{H})$. Put $V = F^n$ and $\langle x|y\rangle = \Sigma_{i=1}^{n} \bar{x}_i y_i$ $(x = (x_i),$ $y = (y_i) \in F^n)$. Thus $(V, \langle\cdot|\cdot\rangle)$ is a unitary right vector space over F. Furthermore, U(V) and $U_n(F)$ denote the group of unitary transformations on V.

DEFINITION. A transformation $s \in U_n(F)$ is called a *reflection* whenever there are $a \in V\setminus\{0\}$ and $\lambda \in U_1(\mathbb{H})$ such that

$$s(x) = x - a(1-\lambda)\langle a|x\rangle\langle a|a\rangle^{-1} \qquad (x \in V).$$

The vector a is then called a *root* of s. Moreover the reflection s determined by a, λ in this way, will be denoted by $S_{a,\lambda}$.

A *reflection group* G in $(V,\langle\cdot|\cdot\rangle)$ is a group generated by reflections within U(V).

A *pre-root system* Σ in $(V,\langle\cdot|\cdot\rangle)$ is a nonempty finite subset Σ of $V \times U_1(F)$ such that (with π_1 the projection on V and π_2 the projection on $U_1(F)$):

(i) $\pi_2(\pi_1^{-1}(a)) \leq U_1(F)$ for any $a \in \pi_1(\Sigma)$

(ii) $(a,\lambda),(b,\mu) \in \Sigma \Rightarrow (S_{a,\lambda}(b),\mu) \in \Sigma$.

If Σ is a pre-root system in V, then the $S_{a,\lambda}$ with $(a,\lambda) \in \Sigma$ generate a finite group, denoted by $W(\Sigma)$. Now Σ is called a *root system* if the additional property

(iii) $(\forall a \in \pi_1(\Sigma))(a\lambda \in \pi_1(\Sigma) \Longleftrightarrow a\lambda \in W(\Sigma)a)$

holds.

We mention the following proposition (cf. [2] and [3]).

PROPOSITION. *If G is a reflection group in a unitary vector space* $(V,\langle\cdot|\cdot\rangle)$, *then there exists a root system* Σ *in* V *such that* $G = W(\Sigma)$.

NOTATION. If G is a reflection group and a the root of a reflection in G, we shall denote by H_a the finite subgroup $\{\lambda \in U_1(F) \mid S_{a,\lambda} \in G\}$ of $U_1(F)$. In the special cases to be considered in the sequel, H_a does not depend on the choice of a, and so we shall often omit the subscript and simply write H.

In addition to F, V, $\langle\cdot|\cdot\rangle$ as above, we need the ring D of algebraic integers of $F \cap \mathbb{R}$ and the quadratic form $q_0: V \to F \cap \mathbb{R}$ given by $q_0(x) = \langle x|x\rangle$ $(x \in V)$. For ease of presentation the latter form will also be used to indicate the restriction to a given submodule of V.

The notions "order" and "lattice over an order" are as in [6].

LEMMA. *Let* R *be an order in* F *and let* Σ *be a root sysetm in* V. *If* $\Delta \subset \pi_1(\Sigma)$ *is a set of roots satisfying both*

$$W(\Sigma) = \langle S_{a,\lambda} \mid a \in \Delta,\ \lambda \in H_a \rangle$$

and

$$\langle a|a\rangle, (1-\lambda)\langle a|b\rangle/\langle a|a\rangle \in R \qquad (a,b \in \Delta,\ \lambda \in H_a),$$

then $\Lambda = \Sigma_{x\in\Delta} xR$ *is an* R*-lattice and* (Λ, q_0) *is a quadratic* D*-module. In particular,* $W(\Sigma)$ *is a subgroup of* $\mathrm{Aut}(\Lambda, q_0)$.

PROOF. Straightforward. □

Instead of constructing the lattice from the root system as the lemma suggests, we shall most frequently retrieve the root system Σ from a given lattice Λ and use the lemma to infer that (Λ, q_0) is invariant under $W(\Sigma)$.

We next introduce representatives of the three conjugacy classes of finite subgroups whose complexifications yield primitive subgroups in $Sl_2(\mathbb{C})$. Put $\zeta = \frac{1}{2}(-1-i-j-k)$; $\eta = (i+j)/\sqrt{2}$; $\tau = (1+\sqrt{5})/\sqrt{2}$, and $\omega = \frac{1}{2}(-1+(1-\tau)i-\tau j)$. Then $Te = \langle i, \zeta\rangle$; $Oc = \langle Te, \eta\rangle$ and $Ic = \langle Te, \omega\rangle$ are the binary tetrahedral, binary octhahedral and binary icosahedral groups of orders 24, 48 and 120 respectively. We shall also make use of the subgroup $Qu_3 = \langle \omega, k\rangle$ of order 12 of Ic. The rings $\mathbb{Z}[Te]$, $\mathbb{Z}[Oc]$ and $\mathbb{Z}[Ic]$ are maximal orders in the skew fields $\mathbb{H}_1$, $\mathbb{H}_2$ and $\mathbb{H}_5$ of quaternions over $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$ respectively. Moreover, $\mathbb{Z}[Qu_3]$ defines an order contained in $\mathbb{Z}[Ic]$. The projections $t : \mathbb{Q}(\sqrt{\ell}) \to \mathbb{Q}$ for $\ell = 1,2,5$ are defined by

$$\left.\begin{aligned} t_1(x) &= x \\ t_2(x+y(1-\sqrt{2})) &= x \\ t_5(x+y\tau) &= x \end{aligned}\right\} \quad (x,y \in \mathbb{Q}).$$

Finally for $\ell = 1,2,5$ and $F \subset \mathbb{H}_\ell$ the quadratic form $q_\ell : F^n \to \mathbb{Q}$ is given by $q_\ell = t_\ell \circ q_0$. Observe that q_ℓ is positive definite.

The notation concerning root systems is taken from [2], [3].

2. RESULTS

PROPOSITION 1. *Let G be a unitary reflection group in* F^n *such that the triple* n, F, G *occurs in a row of table* 1. *Then there is an order* R *in* F, *a* G-*invariant* R-*lattice* Λ *in* F^n *and a* G-*invariant quadratic form* $q\colon \mathbb{F}^n \to \mathbb{Z}$ *such that* (Λ, q) *is the lattice of type* E_8.

PROOF. Given n, F and G, the choice of $\ell \in \{1,2,5\}$ such that $q = q_\ell$ yields the desired quadratic form as well as the choice of R can be read from the table.

Table 1

Presentations of the lattice of type E_8

n	F	G	H	R	ℓ
1	$\mathbb{H}_5$	Ic	Ic	$\mathbb{Z}[Ic]$	5
1	$\mathbb{H}_2$	Oc	Oc	$\mathbb{Z}[Oc]$	2
2	$\mathbb{H}_5$	$W(O_2)$	$\langle\omega\rangle$	$\mathbb{Z}[Qu_3]$	1
2	$\mathbb{H}_1$	$W(P_2)$	$\langle i,j\rangle$	$\mathbb{Z}[Te]$	1
4	$\mathbb{H}_1$	$W(L_4)$	$\langle\zeta\rangle$	$\mathbb{Z}[\zeta]$	1
4	$\mathbb{Q}(i)$	$EW(N_4)$	$\{\pm 1\}$	$\mathbb{Z}[i]$	1
4	$\mathbb{Q}(\sqrt{2})$	$W(F_4)$	$\{\pm 1\}$	$\mathbb{Z}[\sqrt{2}]$	2
4	$\mathbb{Q}(\sqrt{5})$	$W(H_4)$	$\{\pm 1\}$	$\mathbb{Z}[\tau]$	5
8	$\mathbb{Q}$	$W(E_8)$	$\{\pm 1\}$	$\mathbb{Z}$	1

Now put $\theta = i + j$. Notice that both $(\theta\mathbb{Z}[Ic], q_5)$ and $(\theta\mathbb{Z}[Oc], q_2)$ are integral even unimodular $\mathbb{Z}$-lattices and therefore isomorphic to the lattice of type E_8. On the other hand, restriction of scalars in these two modules of rank 1 to orders R (described in the table for the respective cases) induces R-lattices for which the set Δ of points closest to the origin with respect to q_0 forms a set of roots for the corresponding reflection group. In fact $\Sigma = \Delta \times H$ (with H as in the table) is a root system satisfying the conditions of the lemma with $\Delta = \pi_1(\Sigma)$. As Λ is generated as R-module by Δ, the group G consists of automorphisms of (Λ, q_0) and thus of (Λ, q). □

COROLLARY 1. *Part (i) of the theorem holds.*

PROOF. According to the well known classification of real reflection groups, the groups to be considered are $W(H_3)$, $W(F_4)$, $W(H_4)$, $W(E_6)$, $W(E_7)$, $W(E_8)$. Thanks to the obvious inclusions $W(H_3) \subset W(H_4)$ and $W(E_6) \subset W(E_7) \subset W(E_8)$, we only need to verify that $W(H_4)$, $W(F_4)$ are in $W(E_8)$. But this is stated in the proposition. □

COROLLARY 2. *The complex reflection groups* $W(L_3)$, $W(M_3)$, $W(N_4)$, $EW(N_4)$, $W(L_4)$ *are subgroups of* $W(E_8)$.

PROOF. Note that $W(L_3) \subset W(M_3) \subset W(L_4)$ and that $W(N_4) \subset EW(N_4)$. □

COROLLARY 3. *The quaternionic reflection group* $W(O_1)$ $(\cong s\ell_2(5))$, $W(O_2)$ $(\cong s\ell_2(9))$ *and* $W(P_2)$ *are subgroups of* $W(E_8)$.

REMARKS.

(i) The root system of type F_4 appearing in the proposition differs from Bourbaki's in as much as for any root x the squared length $q_0(x) = \langle x|x\rangle$ is 2.

(ii) The groups $W(O_1)$ and $W(O_2)$ are the groups $s\ell_2(5)$ and $s\ell_2(9)$ studied by I. NARUKI in [6] as subgroups of $W(E_8)$.

(iii) By the methods used above one could also establish the inclusion $W(B_n) \subset W(D_{2n})$.

(iv) The groups $EW(N_4)$ and $W(L_4)$ were found as subgroups of $W(E_8)$ centralizing a so-called regular element of order 4, 3 respectively, by T.A. SPRINGER in [12].

Let K_{12} denote the 12-dimensional lattice described by N.J.A. SLOANE in [18]. For G a linear group, the subgroup of G of elements having determinant = 1 is written as G^+.

PROPOSITION 2. *For* $W(K_6)$, $W(Q_3)$ *(and* $W(R_3)$ *respectively) there exists a root system* Σ *of* G *spanning a lattice* Λ *and a* G*-invariant quadratic form* q *on* Λ *with integral values such that* (Λ,q) *is isomorphic to* K_{12} *(and to the Leech lattice* Λ_{24} *respectively). Moreover,* (Λ,q) *is a sublattice of* Λ_{24} *such that* $(\mathrm{Aut}(\Lambda,q))^+ \subset \mathrm{Aut}(\Lambda_{24})$.

PROOF. The vectors in the $\mathbb{Z}[Ic]$-lattice

$$M = \begin{pmatrix}2\\0\\0\end{pmatrix}\mathbb{Z}[Ic] + \begin{pmatrix}\theta\\\theta\\0\end{pmatrix}\mathbb{Z}[Ic] + \begin{pmatrix}1\\\zeta^2+\tau\\1\end{pmatrix}\mathbb{Z}[Ic] \qquad (\text{where } \theta = i+j)$$

closest to the origin with respect to q_0 span a root system for the reflection group $W(R_3)$ (take $H = \{\pm 1\}$). The θ-conjugate of this root system is explicitly given in [2]. Now (M,q_5) is the Leech lattice as portrayed in [11].

Consider the root system with $H = \{\pm 1\}$ spanned by the roots in M that up to a permutation of coordinates look like

$$\begin{pmatrix}2\\0\\0\end{pmatrix}\zeta^2 j\lambda, \quad \begin{pmatrix}1\\p\\0\end{pmatrix}(-\zeta^2+\tau k)\zeta^2 j\lambda, \quad \begin{pmatrix}p\\s\\r(-\zeta^2+\tau k)\end{pmatrix}\zeta^2 j\lambda$$

for $p,s,r \in \langle i,j\rangle$ such that $psr \in \{\pm 1\}$ and $\lambda \in Qu_3$. It is of type Q_3 and gives rise to a $\mathbb{Z}[Qu_3]$-lattice Λ as indicated in the lemma. This lattice is contained in M and the corresponding group $W(Q_3)$ is a subgroup of $W(R_3)$ as it is generated by reflections in $W(R_3)$. Finally, restricting scalars of Λ to $\mathbb{Z}[\omega]$ yields a $\mathbb{Z}[\omega]$-lattice Λ^0 whose points closest to the origin with respect to q_0 span a root system of type K_6.

Since Λ^0 is generated by its vectors closest to the origin with respect to q_0, we have that (Λ^0,q_0) is isomorphic to K_{12} almost by definition. Furthermore the $\mathbb{Z}[\omega]$-lattice Λ^0 occurs in LINDSEY's work [5] as the sublattice of his $\mathbb{Z}[\omega]$-lattice L. Up to a transformation Λ^0 consists of all vectors $x \in L$ for which the last 6 coordinates $x_1,\ldots,x_6$, vanish. J.H. Lindsey shows that an isomorph of $W(K_6)^+ = (\mathrm{Aut}(\Lambda^0,q_0))^+$ is a subgroup of $\mathrm{Aut}(\Lambda_{24})$ and acts faithfully on Λ. □

COROLLARY 4. *There exists embeddings of the groups* $W(J_3(4))$, $W(J_3(5))$, $W(Q_3)$, $W(R_3)$, $W(K_5)$ *and* $W(K_6)^+$ *in* $\mathrm{Aut}(\Lambda_{24})$.

PROOF. This results from the inclusions $W(J_3(4)), W(J_3(5)) \subset W(R_3)$ and $W(K_5) \subset W(K_6)^+$. □

This corollary and Corollary 2 of Proposition 1 together imply part (ii) of the theorem.

REMARKS.

(i) In the analogue of the 7 presentations for the lattice of E_8 obtained from $(\theta\mathbb{Z}[Ic], q_5)$ by restriction of scalars, one may expect interesting subgroups of $\mathrm{Aut}(\Lambda_{24})$ to come out if the same process is applied to (M, q_5). In fact, in [13] J. TITS exhibited the automorphism groups in the cases where the scalars are restricted to $\mathbb{Z}[Te]$ and to $\mathbb{Z}[\zeta]$.

(ii) If the scalars of the $\mathbb{Z}[Te]$-lattice connected with $W(P_2)$ are extended to a $\mathbb{Z}[Ic]$-lattice, we get (after equipping the lattice with the appropriate form) the $\mathbb{Z}$-lattice Λ_{16} referred to by N.J.A. SLOANE in [9]. It is the sublattice of the Leech lattice M presented within $(\mathbb{Z}[Ic])^3$ consisting of all vectors $x \in M$ of the form

$$x = \begin{pmatrix} x_1 \\ x_2 \\ 0 \end{pmatrix}.$$

3. REFERENCES

[1] BOURBAKI, N., *Groupes et algebres de Lie*, Chap. IV, V, VI, Hermann, Paris, 1968.

[2] COHEN, A.M., *Finite complex reflection groups*, Ann. Scient. Éc. Norm. Sup. 4 t 9 (1976), 379-436.

[3] COHEN, A.M., *Finite quaternionic reflection groups*, to appear in J. Algebra.

[4] FEIT, W., *On integral representations of finite groups*, Proc. London Math. Soc. (3) 29 (1974), 633-683.

[5] LINDSEY, J.H. II, *A correlation between* $PSU_4(3)$, *the Suzuki group and the Conway group*, Trans. Amer. Math. Soc. 157 (1971) 189-204.

[6] NARUKI, I., $S\ell_2(\mathbb{F}_9)$, $S\ell_2(\mathbb{F}_5)$ *als Untergruppen von* $W(E_8)$, preprint.

[7] ROGGENKAMP, K.W. & V. HUBER-DYSON, *Lattices over Orders I*, Springer Lect. Notes 115.

[8] SERRE, J.-P., *A course in Arithmetic*, Springer-Verlag (Graduate Texts in Math. #7) 1973.

[9] SHEPHARD, G.C. & J.A. TODD, *Finite unitary reflection groups,* Canad. J. Math. 6 (1954), 274-304.

[10] SLOANE, N.J.A., *Codes over* GF(4) *and complex lattices,* J. Algebra 52 (1978), 168-181.

[11] SLOANE, N.J.A., *Binary codes, lattices and sphere-packings,* in: *Combinatorial Surveys,* Proc. 6th British Combinatorial Conference, P.J. Cameron (ed.), Academic Press, London, 1977, 117-164.

[12] SPRINGER, T.A., *Regular elements of finite reflection groups,* Inv. Math. 25 (1974), 159-198.

[13] TITS, J., *Four presentations of the Leech lattice*, Informal note, 1978.