Annales Mathematicae Silesianae 12 (1998), 93–103

Prace Naukowe Uniwersytetu Śląskiego nr 1751, Katowice

CLIFFORD–LITTLEWOOD–ECKMANN GROUPS AS ORTHOGONAL GROUPS OF FORMS OF HIGHER DEGREE

ANDRZEJ SŁADEK AND ADAM WESOŁOWSKI

Abstract. Forms of degree higher than 2 behave in a quite different way than quadratic forms. Jordan [J] proved finiteness of orthogonal groups of nonsingular forms of degree $\geqslant 3$, whereas it is known that quadratic forms, even if nonsingular, provide us mainly with infinite orthogonal groups. In this paper we describe the orthogonal groups of separable forms of degree at least 3 and for any Clifford–Littlewood–Eckmann group G we construct a form over the rational number field $\mathbb{Q}$ with the orthogonal group isomorphic to G.

Introduction

Throughout the paper let d be a natural number at least 3 and K be a field of characteristic 0 or greater than d. A pair (V, θ) is called a d–linear space of dimension n over K if V is a vector K–space of dimension n and θ is a symmetric d–linear form on V. In the category of d–linear spaces one can consider two natural operations: an orthogonal sum $\perp$ and tensor product $\otimes$. It turns out that any non-degenerate d–linear space can be uniquely decomposed into an orthogonal sum of indecomposable spaces (see [H, Prop. 2.3], [P, Th. 6.3, Cor. 6.4]).

A K–linear isomorphism $\varphi : V \to V'$ is called an isomorphism of d–linear spaces (V, θ) and (V', θ') if for any $v_1, \ldots, v_d \in V$ we have

$$\theta(v_1, \ldots, v_d) = \theta'(\varphi(v_1), \ldots, \varphi(v_d)).$$

Received on September 10, 1998.

1991 *Mathematics Subject Classification.* 11E76, 11E12.

Key words and phrases: Clifford–Littlewood–Eckmann group, multilinear space, orthogonal group of a form of higher degree.

Supported by Grant DST/IM/3/98.

If $(V,\theta) = (V',\theta')$ then an isomorphism is called an *isometry* of (V,θ). Isometries of (V,θ) form a group which we denote by $\mathbf{Aut}_K(V,\theta)$. Unique decomposition of non-degenerate d–linear spaces into indecomposable ones allows us to describe the structure of $\mathbf{Aut}_K(V,\theta)$ with the help of the orthogonal groups of the indecomposable summands of (V,θ). To explain it in more detail let us assume that (V,θ) has the following decomposition

$$((V_{1,1},\theta_{1,1}) \perp \ldots \perp (V_{1,n_1},\theta_{1,n_1})) \perp \ldots \perp ((V_{k,1},\theta_{k,1}) \perp \ldots \perp (V_{k,n_k},\theta_{k,n_k})),$$

where the spaces $(V_{i,j},\theta_{i,j})$ and $(V_{r,s},\theta_{r,s})$ are isomorphic if $i = r$ and not isomorphic otherwise.

THEOREM ([P, TH. 6.7], [W1, TW.2.2.1 AND TW. 2.2.2]). *If (V,θ) has the decomposition into indecomposable summands as above, then*

$$\mathbf{Aut}_K(V,\theta) \cong \prod_{i=1}^{k}((\mathbf{Aut}_K(V_{i,1},\theta_{i,1})^{n_i} \rtimes \mathbf{S}(n_i)),$$

where $\rtimes$ stands for the semidirect product with the following action of the symmetric group $\mathbf{S}(n_i)$ on the group $\mathbf{Aut}_K(V_{i,1},\theta_{i,1}))^{n_i}$:

$$((\varphi_1,\ldots,\varphi_{n_i}),\sigma) \longmapsto (\varphi_{\sigma^{-1}(1)},\ldots,\varphi_{\sigma^{-1}(n_i)})$$

According to the above Theorem the description of $\mathbf{Aut}_K(V,\theta)$ is complete if the orthogonal groups of the indecomposable summands of (V,θ) are known. One of the significant difference between quadratic and higher degree forms is the following result of Jordan [J].

THEOREM. *If (V,θ) is a non-singular d–linear space, then the orthogonal group $\mathbf{Aut}_K(V,\theta)$ is finite.*

In fact Jordan's Theorem is usually stated for K being algebraically closed, but using the standard scalar extension procedure it can be easily derived for any field of characteristic 0 or greater than d. Jordan's Theorem suggests the following question (stated explicitly by Suzuki [Su]): *Which finite groups can be represented as $\mathbf{Aut}_K(V,\theta)$ for suitable (V,θ)?*

Let us slightly reformulate the above question.

QUESTION. *Let $\mathcal{R}$ be a family of d–linear spaces over the field K. Which finite groups can be represented as $\mathbf{Aut}_K(V,\theta)$ for suitable $(V,\theta) \in \mathcal{R}$?*

In the paper we answer our Question for Clifford–Littlewood–Eckmann groups (described below) and the family of separable d–linear spaces (described in the next section) over the rationals.

For any pair of non-negative integers s and t, let $\mathbf{G}_{s,t}$ denote the group defined with the help of generators $\varepsilon, a_1, \ldots, a_s, b_1, \ldots, b_t$ and relations:

$$(\spadesuit)\qquad \begin{cases} (1) & \varepsilon^2 = 1, & \\ (2) & a_i^2 = \varepsilon & i = 1, \ldots, s, \\ (3) & b_j^2 = 1 & j = 1, \ldots, t, \\ (4) & a_i b_j = \varepsilon b_j a_i & i = 1, \ldots, s,\ j = 1, \ldots, t, \\ (5) & a_i a_l = \varepsilon a_l a_i & i, l = 1, \ldots, s,\ i \neq l, \\ (6) & b_m b_j = \varepsilon b_j b_m & j, m = 1, \ldots, t,\ j \neq m, \\ (7) & \varepsilon b_j = b_j \varepsilon & j = 1, \ldots, t. \end{cases}$$

Groups $\mathbf{G}_{s,t}$ form an important family of 2–groups. Lam and Smith [LS] offer the reader a very interesting historical survey (in which they propose to call these groups *Clifford–Littlewood–Eckmann groups*, abbreviated as *CLE-groups*) as well as a complete description of the algebraic structure of $\mathbf{G}_{s,t}$. The most basic groups among the $\mathbf{G}_{s,t}$'s are:

$\mathbf{Z}_2 = \mathbf{G}_{0,0}$ (the cyclic group of two element)

$\mathbf{C} := \mathbf{G}_{1,0}$ (the cyclic group of order 4)

$\mathbf{K} := \mathbf{G}_{0,1}$ (the Klein 4–group)

$\mathbf{Q} := \mathbf{G}_{2,0}$ (the quaternion group of order 8)

$\mathbf{D} := \mathbf{G}_{0,2}$ (the dihedral group of order 8)

In the family of CLE-groups one can define a product $\dot{\times}$ in the following way:

$$G \ \dot{\times}\ H := (G \times H)/(\varepsilon_G, \varepsilon_H).$$

In the sequel we shall write GH for $G \dot{\times} H$ and G^k for $G \ldots G$ with k factors. Lam and Smith proved that all the CLE-groups can be built from the groups $\mathbf{C}$, $\mathbf{K}$, $\mathbf{Q}$ and $\mathbf{D}$.

Decomposition Theorem ([LS, Th. 2.10]). *If G is a CLE-group different from $\mathbf{G}_{0,0}$, then G is isomorphic to exactly one of the following products:*

$$\mathbf{D}^i,\ \mathbf{D}^i\mathbf{Q},\ \mathbf{D}^i\mathbf{K},\ \mathbf{D}^i\mathbf{Q}\mathbf{K} \text{ or } \mathbf{D}^i\mathbf{C} \text{ for some } i \geqslant 0.$$

An additional aim we want to get in the paper is to emphasise the beauty and usefulness of the Decomposition Theorem for CLE-groups.

1. Separable d–linear space and its orthogonal group

Let d be a natural number at least 3 and let K be a field of characteristic 0 or greater than d.

DEFINITION. A d–linear space (V, θ) over K is called *separable* if V is a separable finitely dimensional commutative $K-$ algebra and θ is a scaled trace form of degree d, i.e. there exists an invertible $\alpha \in V$ such that for any $v_1, \ldots, v_d \in V$ we have

$$\theta(v_1, \ldots, v_d) = \mathbf{Tr}_{V/K}(\alpha v_1 \ldots v_d),$$

where $\mathbf{Tr}_{V/K}$ stands for the usual trace map $V \to K$. In the sequel we denote such a space by $(V, < \alpha >_d)$. It is not difficult to check that $(V, < \alpha_d >)$ is non-singular.

REMARK. In fact the original definition of a separable d–linear space is different from that one given above. For the aim we want to get there is no need to recall it. Of course both definitions are equivalent and the interested reader can find it in [HP, Section 3].

Because of the first theorem in the Introduction our main interest is mainly concentrated on indecomposable separable spaces.

THEOREM 1.1 ([HP, LEMMATA 3.10 AND 3.11]). *The separable space $(V, < \alpha >_d)$ (over K) is indecomposable if and only if V is a separable field extension of K.*

The proof of the above Theorem bases on the fact that a separable finitely dimensional commutative K–algebra is a product of separable field extensions of K and that the product corresponds to the orthogonal product of $d-$ linear spaces.
Since we think about the description of the group $\mathbf{Aut}_K(L, < \alpha >_d)$ for a separable field extension L of the field K, it is natural to ask about a single isometry of $(L, < \alpha >_d)$. The answer one can find in the literature.

THEOREM 1.2 ([HP, TH. 3.12; W2, TW. 3.1.5]). *Assume that the space $(L, < \alpha >_d)$ is indecomposable. If f is an isometry of $(L, < \alpha >_d)$, then there exists an element φ of the Galois group $\mathbf{G}(L/K)$ and $a \in L^*$, $a \neq 0$ such that $f = f(1)\varphi$ and $\varphi(\alpha) = \alpha a^d$.*

For an indecomposable space $(L, <\alpha>_d)$ consider the following map

$$e : \mathbf{Aut}_K(L, <\alpha>_d) \longrightarrow \mathbf{G}(L/K), \quad e(f) := f(1)^{-1} f.$$

By Theorem 1.2 the map e is well defined and

$$\operatorname{im} e \subseteq \mathbf{G}_{\alpha,d}(L/K) := \{\varphi \in \mathbf{G}(L/K) : \bigvee_{a \in L^*} \varphi(\alpha) = \alpha a^d\}.$$

In fact we have $\operatorname{im} e = \mathbf{G}_{\alpha,d}(L/K)$, because it is a routine matter to check that if the isomorphism φ satisfies $\varphi(\alpha) = \alpha a^d$, then the scaled map $f := a\varphi$ is an isometry such that $e(f) = \varphi$.

Now suppose $f \in \ker e$. Then f must be a scalar map: $f(x) = f(1)x$, for any $x \in L$. Since

$$\mathbf{Tr}_{L/K}(\alpha \underbrace{1 \cdot \ldots \cdot 1}_{d}) = \mathbf{Tr}_{L/K}(\alpha \underbrace{f(1) \cdot \ldots \cdot f(1)}_{d})$$

and the trace map $\mathbf{Tr}_{L/K}$ is non-degenerate, we have

$$f(1) \in \mu_d(L) := \{x \in L : x^d = 1\}.$$

Thus we can define another map

$$i : \mu_d(L) \longrightarrow \mathbf{Aut}_K(L, <\alpha>_d), \quad i(\epsilon) := m_\epsilon,$$

where $m_\epsilon(x) = \epsilon x$, for $x \in L$.

In the consequence we have got the following.

THEOREM 1.3. *The sequence*

$$(\clubsuit) \qquad 1 \longrightarrow \mu_d(L) \xrightarrow{i} \mathbf{Aut}_K(L, <\alpha>_d) \xrightarrow{e} \mathbf{G}_{\alpha,d}(L/K) \longrightarrow 1$$

is exact.

REMARK 1.4. For any $\varphi \in \mathbf{G}_{\alpha,d}(L/K)$ let $a_\varphi \in L^*$ be such that $\varphi(\alpha) = \alpha a_\varphi^d$. Of course, an element a_φ is uniquely defined modulo $\mu_d(L)$. By Theorem 1.3 any element f of the orthogonal group $\mathbf{Aut}_K(L, <\alpha>_d)$ has the following form

$$f = m_\epsilon \circ m_{a_\varphi} \circ \varphi, \text{ for } \epsilon \in \mu_d(L), \ \varphi \in \mathbf{G}_{\alpha,d}(L/K),$$

whereas the action in $\mathbf{Aut}_K(L, <\alpha>_d)$ is as follows

$$(m_\epsilon \circ m_{a_\varphi} \circ \varphi) \circ (m_\xi \circ m_{a_\psi} \circ \psi) = m_{\epsilon\psi(\xi)} \circ m_{a_\varphi \varphi(a_\psi)} \circ \varphi \circ \psi.$$

2. CLE-groups as orthogonal groups

On the one hand it follows from the relations (♠) defining CLE-group that the element ε is central and the group $\mathbf{G}_{s,t}$ is a central extension of $\{1, \varepsilon\}$ by $\mathbb{Z}_2^{s+t}$, whereas on the other hand the sequence (♣) shows that the orthogonal group $\mathbf{Aut}_K(L, <\alpha>_d)$ is a group extension of $\mu_d(L)$ by $\mathbf{G}_{\alpha,d}(L/K)$. Looking for the realization of a CLE-group as an orthogonal group $\mathbf{Aut}_K(L, <\alpha>_d)$ we choose the field L as a multiquadratic extension of K with $\mu_d(L) = \{1, -1\}$. The last equality enforces d to be even. Then the isometry m_{-1} is a central involution in $\mathbf{Aut}_K(L, <\alpha>_d)$. The Galois group $\mathbf{G}(L/K)$ is an elementary 2-group. For $\varphi \in \mathbf{G}(L/K)$ denote by $\mathbf{N}_\varphi$ the standard norm map $L \longrightarrow L^\varphi$, $\mathbf{N}_\varphi(x) := x\varphi(x)$. If $\varphi \in \mathbf{G}_{\alpha,d}(L/K)$, then $(\mathbf{N}_\varphi(a_\varphi))^d = 1$, that is, $\mathbf{N}_\varphi(a_\varphi) \in \{1, -1\}$.

In the sequel we assume $K = \mathbb{Q}$ and $d > 2$ is an even number. Let $b_1, \ldots, b_n, c_1, \ldots, c_m$ be natural numbers linearly independent modulo $\mathbb{Q}^{*2}$ and let

$$L_1 = \mathbb{Q}(\sqrt{b_1}, \ldots, \sqrt{b_n}), \quad L_2 = \mathbb{Q}(\sqrt{c_1}, \ldots, \sqrt{c_m}).$$

Then

$$L_1 \cap L_2 = \mathbb{Q}, \quad \mu_d(L_1) = \mu_d(L_2) = \mu_d(L_1L_2) = \{1, -1\}$$

and

$$\mathbf{G}(L_1/\mathbb{Q}) \cong \mathbb{Z}_2^n, \quad \mathbf{G}(L_2/K) \cong \mathbb{Z}_2^m, \quad \mathbf{G}(L_1L_2/\mathbb{Q}) \cong \mathbb{Z}_2^{m+n}.$$

THEOREM 2.1. *Assume d, L_1, L_2 are as above and $\alpha_i \in L_i^*$, are such that $\mathbf{G}_{\alpha_i,d}(L_i/\mathbb{Q}) = \mathbf{G}(L_i/\mathbb{Q})$, $i = 1, 2$. Then*

(1) $\mathbf{G}_{\alpha_1\alpha_2,d}(L_1L_2/\mathbb{Q}) = \mathbf{G}(L_1L_2/\mathbb{Q})$,

(2) $\mathbf{Aut}_{\mathbb{Q}}(L_1L_2, <\alpha_1\alpha_2>_d) \cong \mathbf{Aut}_{\mathbb{Q}}(L_1, <\alpha_1>_d) \dot{\times} \mathbf{Aut}_{\mathbb{Q}}(L_2, <\alpha_2>_d)$.

PROOF. Let $\Phi : \mathbf{G}(L_1/\mathbb{Q}) \times \mathbf{G}(L_2/\mathbb{Q}) \longrightarrow \mathbf{G}(L_1L_2/\mathbb{Q})$ be a group isomorphism such that $\Phi(\varphi_1, \varphi_2)_{|L_i} = \varphi_i$, $i = 1, 2$. If $\varphi = \Phi(\varphi_1, \varphi_2) \in \mathbf{G}(L_1L_2/\mathbb{Q})$, then $\varphi(\alpha_1\alpha_2) = \alpha_1\alpha_2(a_{\varphi_1}a_{\varphi_2})^d$. It proves (1).

Now consider the map

$$\Psi : \mathbf{Aut}_{\mathbb{Q}}(L_1, <\alpha_1>_d) \times \mathbf{Aut}_{\mathbb{Q}}(L_2, <\alpha_2>_d) \longrightarrow \mathbf{Aut}_{\mathbb{Q}}(L_1L_2, <\alpha_1\alpha_2>_d),$$

$$\Psi(m_{\epsilon_1} \circ m_{a_{\varphi_1}} \circ \varphi_1, m_{\epsilon_2} \circ m_{a_{\varphi_2}} \circ \varphi_2) := m_{\epsilon_1\epsilon_2} \circ m_{a_{\varphi_1}a_{\varphi_2}} \circ \Phi(\varphi_1, \varphi_2).$$

One can check that Ψ is a group epimorphism with $\ker \Psi = < (m_{-1}, m_{-1}) >$ as required. □

Decomposition Theorem and Theorem 2.1 show that the realization of the CLE–groups **C**, **K**, **Q** and **D** as orthogonal groups is the main step towards the realization of any CLE-group as an orthogonal group.

Realization of C and K. Let $L = \mathbb{Q}(\sqrt{b})$, where $b > 1$ is a square-free natural number. Let σ be a non-trivial element of the Galois group $\mathbf{G}(L/\mathbb{Q})$. Suppose $\alpha, a_\sigma \in L^*$ are such that $\sigma(\alpha) = \alpha a_\sigma^d$ (a little bit further we shall examine the existence of such elements). As we have observed $\epsilon_\sigma := \mathbf{N}_\sigma(a_\sigma) \in \{1, -1\}$. By Remark 1.4

$$\mathbf{Aut}_{\mathbb{Q}}(L, < \alpha >_d) = \{m_1, m_{-1}, m_{a_\sigma} \circ \sigma, m_{-a_\sigma} \circ \sigma\}$$

and $(m_{\pm a_\sigma} \circ \sigma)^2 = m_{\epsilon_\sigma}$. Thus $\mathbf{Aut}_{\mathbb{Q}}(L, < \alpha >_d)$ is cyclic when $\epsilon_\sigma = -1$ and the Klein 4-group when $\epsilon_\sigma = 1$.

THEOREM 2.2. *Under the notation fixed above we have the following:*

(1) *For any square-free natural number $b > 1$ there exists $\alpha \in L^*$ such that $\mathbf{G}_{\alpha,d}(L/\mathbb{Q}) = \mathbf{G}(L/\mathbb{Q})$ and $\mathbf{Aut}_{\mathbb{Q}}(L, < \alpha >_d)$ is the Klein 4-group.*

(2) *There exists $\alpha \in L^*$ such that $\mathbf{G}_{\alpha,d}(L/\mathbb{Q}) = \mathbf{G}(L/\mathbb{Q})$ and the group $\mathbf{Aut}_{\mathbb{Q}}(L, < \alpha >_d)$ is cyclic if and only if b is a sum of two squares of rational numbers.*

PROOF. Since $\mathbf{N}_\sigma(X + Y\sqrt{b}) = X^2 - bY^2$, first of all we should solve over $\mathbb{Q}$ the equation

$$(\diamondsuit) \qquad X^2 - bY^2 = \epsilon_\sigma$$

to get $a_\sigma = X + Y\sqrt{b}$ with $\mathbf{N}_\sigma(a_\sigma) = \epsilon_\sigma \in \{1, -1\}$. If $\epsilon_\sigma = 1$, then the equation $(\diamondsuit)$ is solvable for any b. If $\epsilon_\sigma = -1$, then $(\diamondsuit)$ is solvable if and only if b is a sum of two squares. To finish the proof it suffices to notice that for

$$\alpha = \frac{1}{1 + a_\sigma^d}.$$

we have $\sigma(\alpha) = \alpha a_\sigma^d$, that is, $\mathbf{G}_{\alpha,d}(L/\mathbb{Q}) = \mathbf{G}(L/\mathbb{Q})$. □

Realization of D and Q. Let $L = \mathbb{Q}(\sqrt{b_1}, \sqrt{b_2})$, where b_1 and b_2 are square-free natural numbers > 1 independent modulo $\mathbb{Q}^{*2}$. Let φ_1, φ_2 be generaters of $\mathbf{G}(L/\mathbb{Q})$ such that for $i, j = 1, 2$ we have

$$\varphi_i(\sqrt{b_j}) = (-1)^{\delta_{ij}}\sqrt{b_j}.$$

Suppose $\alpha, a_1, a_2 \in L^*$ are such that $\varphi_i(\alpha) = \alpha a_i^d$ (the existence of such elements will be discussed a little bit further). Then for $\varphi_3 := \varphi_1 \circ \varphi_2$ we have

$$\varphi_3(\alpha) = \alpha(a_2\varphi_2(a_1))^d = \alpha(a_1\varphi_1(a_2))^d.$$

It follows that $a_2\varphi_2(a_1) = \epsilon_{12}a_1\varphi_1(a_2)$, for some $\epsilon_{12} \in \{1, -1\}$. If we abbreviate $\mathbf{N}_i$ for $\mathbf{N}_{\varphi_i}$, then $\epsilon_1 := \mathbf{N}_1(a_1), \epsilon_2 := \mathbf{N}_2(a_2) \in \{1, -1\}$. Put $a_3 := a_2\varphi_2(a_1)$. By easy computation we get $\mathbf{N}_3(a_3) = \epsilon_1\epsilon_2\epsilon_{12}$. By Remark 1.4

$$\mathbf{Aut}_{\mathbb{Q}}(L, <\alpha>_d) = \{m_1, m_{-1}\} \cup \{m_{a_i} \circ \varphi_i, m_{-a_i} \circ \varphi_i : i = 1, 2, 3\}$$

and $(m_{\pm a_\epsilon} \circ \sigma)^2 = m_{\epsilon_\epsilon}$. Thus

$$\mathbf{Aut}_{\mathbb{Q}}(L, <\alpha>_d) \cong \mathbf{Q} \iff \epsilon_1 = \epsilon_2 = \epsilon_{12} = -1,$$

$$\mathbf{Aut}_{\mathbb{Q}}(L, <\alpha>_d) \cong \mathbf{D} \iff \epsilon_{12} = -1 \wedge (\epsilon_1 = 1 \vee \epsilon_2 = 1).$$

Before we start discussing the relation among b_1, b_2 and the structure of $\mathbf{Aut}_{\mathbb{Q}}(L, <\alpha>_d)$ notice that for $a_1, a_2 \in L^*$ and $\epsilon_1, \epsilon_2, \epsilon_{12} \in \{1, -1\}$ satisfying

$$(\heartsuit) \qquad \begin{cases} \mathbf{N}_1(a_1) = \epsilon_1 \\ \mathbf{N}_2(a_2) = \epsilon_2 \\ a_2\varphi_2(a_1) = \epsilon_{12}a_1\varphi_1(a_2) \end{cases}$$

it suffices to define

$$\alpha := \frac{1}{a_1^d + a_2^d + (a_1\varphi_1(a_2))^d}$$

to get

$$\mathbf{G}_{\alpha,d}(L/\mathbb{Q}) = \mathbf{G}(L/\mathbb{Q}).$$

Thus the only thing left is finding sufficient conditions for b_1, b_2 that guarantee existence of a solution

$$a_1 = X_1 + X_2\sqrt{b_1} + X_3\sqrt{b_2} + X_4\sqrt{b_1b_2},$$
$$a_2 = Y_1 + Y_2\sqrt{b_1} + Y_3\sqrt{b_2} + Y_4\sqrt{b_1b_2}$$

of ($\heartsuit$). Taking into account the definition of $\mathbf{N}_1, \mathbf{N}_2, \varphi_1, \varphi_2$ and putting $\epsilon_{12} = -1$ we can rewrite ($\heartsuit$) equivalently in the following way:

$$(\blacklozenge) \qquad \begin{cases} (1) & X_1^2 - b_1X_2^2 + b_2X_3^2 - b_1b_2X_4^2 = \epsilon_1 \\ (2) & X_1X_3 - b_1X_2X_4 = 0 \\ (3) & Y_1^2 + b_1Y_2^2 - b_2Y_3^2 - b_1b_2Y_4^2 = \epsilon_2 \\ (4) & Y_1Y_2 - b_2Y_3Y_4 = 0 \\ (5) & X_1Y_1 - b_1b_2X_4Y_4 = 0 \\ (6) & X_2Y_1 - b_2X_3Y_4 = 0 \\ (7) & X_1Y_3 - b_1X_4Y_2 = 0 \\ (8) & X_2Y_3 - X_3Y_2 = 0 \end{cases}$$

THEOREM 2.3. *Keep the notation fixed above and suppose that b_2 is a sum of two squares. Then*

(1) *If the quadratic form $< 1, b_2 >$ represents b_1, then there exists $\alpha \in L^*$ such that $\mathbf{G}_{\alpha,d}(L/\mathbb{Q}) = \mathbf{G}(L/\mathbb{Q})$ and $\mathbf{Aut}_{\mathbb{Q}}(L, <\alpha>_d) \cong \mathbf{Q}$.*

(2) *If the quadratic form $< 1, -b_2 >$ represents $-b_1$, then there exists $\alpha \in L^*$ such that $\mathbf{G}_{\alpha,d}(L/\mathbb{Q}) = \mathbf{G}(L/\mathbb{Q})$ and $\mathbf{Aut}_{\mathbb{Q}}(L, <\alpha>_d) \cong \mathbf{D}$.*

PROOF. As we have noticed the structure of the orthogonal group depends on the solvability of the system of quadratic equation ($\blacklozenge$). Suppose that b_2 is a sum of two squares. We are looking for a solution of ($\blacklozenge$) of the following form: $X_1 = X_4 = 0$, $X_2 = kX_3$, $Y_2 = kY_3$, $Y_1 = k^{-1}b_2Y_4$, where $k \in \mathbb{Q}^*$ will be properly chosen below. To find the indeterminates X_3, Y_3 and Y_4 one should solve the following system of equations:

$$\begin{cases} (b_2 - k^2b_1)X_3^2 = \epsilon_1 \\ b_2(b_2 - k^2b_1)(k^{-1}Y_4)^2 + (k^2b_1 - b_2)Y_3^2 = \epsilon_2 \end{cases}$$

Solvability of the last system of equations is equivalent to the fact that (a) $k^2b_1 - b_2 \in -\epsilon_1\mathbb{Q}^{*2}$ and (b) the quadratic form $< 1, -b_2 >$ represents $-\epsilon_1\epsilon_2$. Notice that for $\epsilon_1 = \epsilon_2 = -1$ (the case of $\mathbf{Q}$) as well as for $\epsilon_1 = \epsilon_2 = 1$ (the case of $\mathbf{D}$) the condition (b) holds, because b_2 is a sum of two squares. Suppose the quadratic form $< 1, b_2 >$ represents b_1, that is, $b_1 = A^2 + B^2b_2^2$. Then for $k = B^{-1}$ we have $k^2b_1 - b_2 = (AB^{-1})^2 \in \mathbb{Q}^{*2}$. Thus (a) for $\epsilon_1 = -1$ holds. The proof of the statement (1) is finished. In the same way one can finish the proof of (2). □

REMARK 2.4. Notice that the condition which appeared in Theorem 2.3 (1) holds for example for $b_2 = 17$ and $b_1 = 33$. Since every binary quadratic

form over $\mathbb{Q}$ represents infinitely many elements modulo $\mathbb{Q}^{*2}$, for any natural numbers $c_1, \ldots, c_n$ independent modulo $\mathbb{Q}^{*2}$ one can find square-free natural numbers b_1 and b_2 such that b_2 is a sum of two squares, the quadratic form $< 1, -b_2 >$ represents $-b_1$ and $c_1, \ldots, c_n, b_1, b_2$ are independent modulo $\mathbb{Q}^{*2}$.

Realization of any CLE-group

THEOREM 2.5. *If G is any CLE-group different from $\mathbf{G}_{0,0}$, then there exists a multiquadratic extension $L \subseteq \mathbb{R}$ of $\mathbb{Q}$ and $\alpha \in L^*$ such that*

$$\mathbf{Aut}_{\mathbb{Q}}(L, < \alpha >_d) \cong G.$$

PROOF. Let $K = \mathbb{Q}(\sqrt{2})$, $L = \mathbb{Q}(\sqrt{5})$ and $M = \mathbb{Q}(\sqrt{17}, \sqrt{33})$. Then by Theorem 2.2 and Theorem 2.3 there exist $\alpha \in K$, $\beta \in L$ and $\gamma \in M$ such that

$$\mathbf{Aut}_{\mathbb{Q}}(K, < \alpha >_d) \cong \mathbf{K}, \ \mathbf{Aut}_{\mathbb{Q}}(L, < \beta >_d) \cong \mathbf{C}, \ \mathbf{Aut}_{\mathbb{Q}}(M, < \gamma >_d) \cong \mathbf{Q}.$$

By Theorem 2.3 and Remark 2.4 we can choose square-free natural numbers
$b_{11}, b_{21}, \ldots, b_{1i}, b_{2i}$ and $\alpha_k \in L_k := \mathbb{Q}(\sqrt{b_{1k}}, \sqrt{b_{1k}})$, $k = 1, \ldots, i$, such that

$$\mathbf{Aut}_{\mathbb{Q}}(L_k, < \alpha_k >_d) \cong \mathbf{D}$$

and $2, 5, 17, 33, b_{11}, b_{21}, \ldots, b_{1i}, b_{2i}$ are independent modulo $\mathbb{Q}^{*2}$. Then by Theorem 2.1

$$\mathbf{Aut}_{\mathbb{Q}}(L_1 \ldots L_i, < \alpha_1 \ldots \alpha_i >_d) \cong \mathbf{D}^i$$
$$\mathbf{Aut}_{\mathbb{Q}}(ML_1 \ldots L_i, < \gamma\alpha_1 \ldots \alpha_i >_d) \cong \mathbf{D}^i\mathbf{Q}$$
$$\mathbf{Aut}_{\mathbb{Q}}(KML_1 \ldots L_i, < \alpha\gamma\alpha_1 \ldots \alpha_i >_d) \cong \mathbf{D}^i\mathbf{QK}$$
$$\mathbf{Aut}_{\mathbb{Q}}(LL_1 \ldots L_i, < \beta\alpha_1 \ldots \alpha_i >_d) \cong \mathbf{D}^i\mathbf{C}.$$

Decomposition Theorem for CLE-groups finishes the proof. □

Acknowledgment. We wish to thank Przemysław Koprowski for showing us the solution of the system of equation (♦) that we use in the proof of Theorem 2.3.

References

[H] D. K. Harrison, *A Grothendieck ring of higher degree forms*, J. Algebra, **35** (1975), 123–138.

[HP] D. K. Harrison and B. Pareigis, *Witt rings of higher degree forms*, Commun. Algebra., **16 (6)** (1988), 1275–1313.

[J] C. Jordan, *Memoire sur l'equivalence des formes*, J.Éc. Pol., **XVLIII** (1890), 112–150.

[LS] T. Y. Lam and T. Smith, *On the Clifford–Littlewood–Eckmann groups: a new look at periodicity mod 8*, Rocky Mountain J. Math., **19(3)** (1989), 749–786.

[P] A. Prószyński, *On the orthogonal decomposition of homogeneous polynomials*, Fund. Math., **XCVIII** (1978), 201–217.

[S] J. Schneider, *Orthogonal groups of non–singular forms of higher degree*, J. Algebra, **27** (1973), 1126.

[Su] H. Suzuki, *Automorphism groups of multilinear maps*, Osaka J. Math., **20** (1983), 659–673.

[W1] A. Wesołowski, *Automorfizmy form wyższych stopni*, Ph.D. Thesis, Uniw. Śląski, Katowice (1998).

[W2] bysame, *Automorphism and similarity groups of forms determined by the characteristic polynomials*, Commun. Algebra (to appear).

Instytut Matematyki
Uniwersytet Śląski
Bankowa 14
40–007 Katowice
Poland

e-mail:
sladek@ux2.math.us.edu.pl
wacek@ux2.math.us.edu.pl