*Publ. Math. Debrecen*
**41 / 3–4** (1992), 189–198

# A square of set of elements of order two in orthogonal groups

By JAN AMBROSIEWICZ (Białystok)

Let $G$ be group, $K_m = \{g \in G : \ o(g) = m\}$, $O_n(K,f)$ a group of automorphisms of the vector space $V_n(K)$ which leave invariant a quadratic form $f$ of determinant different from zero.

It is known that the group $O_n(K,f)$, $\mathrm{char}K \neq 2$, is generated by reflections, (see [4], pp 68–69).

In this paper we will prove a stronger theorem:

If $K$ is the real field $\mathbb{R}$ or $K = GF(p^s)$, $p > 2$, then $O_n(K,f) = K_2K_2$.

If $K$ is the complex field $\mathbb{C}$ or $K = GF(2^s)$, then $O_n(K,f) \neq K_2K_2$.

It also has been proved that $PGL(2,K) = K_2K_2$ while $PGL(n,K) \neq K_2K_2$ with $n \geq 3$, where $PGL(n,K) = GL(n,K)/Z$, (cf [7]).

Notations are standard. In addition we will use the following notations:

$$F_s = \begin{bmatrix} 0 & & 1 \\ & \ddots & \\ 1 & & 0 \end{bmatrix}, \quad E_s = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}, \quad F_s, E_s \in M_{s\times s}(K)\,.$$

${}^tA$ – transpose of the matrix $A$ with regard to the second diagonal of $A, O_n^+(K,f)$ – a subgroup of matrices of $O_n(K,f)$, called rotations, $\Omega_n\ (K,f)$ – a commutant of $O_n^+(K,f)$. Throughout the paper the symbol $f$ denotes a quadratic form of determinant from zero.

We will often use the following lemmas.

**Lemma 1.** *Let $G$ be a group. An element $g \in K_2^m$, $(m \geq 2)$ if and only if there is an element $x \in K_2^{m-1}$, $x \neq g$ such that $xgx = g^{-1}$, (see [2]).*

**Lemma 2.** i) *If $K = GF(p^s)$, $p > 2$, then in the vector space $V_n(K)$ there exists an orthogonal basis in which each quadratic form of determi-*

*nant different from zero takes the form*

$$f(x) = \sum_{i=1}^{n-1} x_i^2 + \eta x_n^2 \,, \tag{1}$$

*where $\eta = 1$ for $n$ odd but $\eta = 1$ or a particular not square $\nu$ for $n$ even.*
ii) *If $K = GF(2^s)$, then in the vector space $V_n(K)$ there exists an orthogonal basis in which each quadratic form of determinant different from zero takes the form*

$$\begin{aligned} f(x) &= x_1x_2 + x_3x_4 + \cdots + x_{n-2}x_{n-1} + x_n^2 \\ &\qquad \textit{for } n \textit{ odd and} \\ f(x) &= x_1x_2 + x_3x_4 + \cdots + x_{n-3}x_{n-2} + x_{n-1}x_n + \lambda \left(x_{n-1}^2 + x_n^2\right) \\ &\qquad \textit{for } n \textit{ even}, \end{aligned} \tag{2}$$

*where $\lambda = 0$ or is a particular one of the values $\alpha$ for which $x_{n-1}x_n + \alpha(x_{n-1}^2 + x_n^2)$ is irreducible in the $GF(2^s)$, (see [5], pp 158, 197).*

**Lemma 3.** *Let $A_i \in GL(n_i, K)$, $B = \operatorname{diag}(A_1 \dots A_k) \in Gl(n, K)$, $n = n_1 + n_2 \dots n_k$, $K = GF(p^s)$, $p > 2$. If $A_i$ fulfils at least one of the following conditions*

$$i) \quad \begin{cases} A_i^t &= A_i \\ A_i^t A_i &= E \end{cases} \qquad ii) \quad \begin{cases} {}^tA_i &= A_i \\ A_i^t A_i &= E \end{cases}$$

*then there exists $T \in K_2$ such that $TBT = B^{-1}$ and $B \in K_2K_2$.*

Proof. If i) holds, then $A_i = A_i^{-1}$ and $T_iA_iT_i = A_i^{-1}$, where $T_i = -E$ for $A_i \neq -E$ and $T_i = F$ for $A_i = -E$. If ii) holds, then a calculation shows that $T_iA_iT_i = A_i^t = A_i^{-1}$, where $T_i = F$ for $A_i \neq F$ and $T_i = -E$ for $A_i = F$.

Now we construct the matrix

$$\begin{aligned} &T = \operatorname{diag}(T_1, \dots, T_k), \text{where} \\ &T_i = -E \text{ if } (-E)A_i(-E) = A_i^{-1} \text{ or } \quad T_i = F \text{ if } FA_iF = A_i^{-1} \,. \end{aligned} \tag{3}$$

Thus

$$TBT = \operatorname{diag}(A_1^{-1}, \dots, A_k^{-1}) = B^{-1} \,. \tag{4}$$

From the construction of $T$ we see that $T \neq E$, $T^2 = E$. Therefore $B \in K_2K_2$ by (4) and Lemma 1.

**Lemma 4.** *Let $A \in GL(2,K)$, $\operatorname{char} K = 2$, $|K| \neq 2$. If $A$ fulfils at least one of the following conditions*

$$i)\ \begin{cases} A^t &= A \\ A^t A &= E \end{cases} \qquad ii)\ \begin{cases} {}^tA &= A \\ A^t A &= E \end{cases}$$

*then there exists $T \neq A$ such that $T \in K_2$, $TAT = A^{-1}$ and $A \in K_2K_2$.*

Proof. If $A \neq F$ fulfils i) or ii) then we can take $T = F$. If $A = F$, then there exists $T = \left[\begin{smallmatrix} u & v \\ v & u \end{smallmatrix}\right] \neq A$, $u^2 + v^2 = 1$, by $|K| \neq 2$. In both cases $TAT = A^{-1}$. Hence $A \in K_2K_2$ by Lemma 1.

**Theorem 1.** *If $K = R$, then $O_n(K,f) = K_2K_2$.*

Proof. Each matrix of $O_n(K,f)$ is orthogonally similar to the matrix

$$(5) \quad A = \operatorname{diag}\left( \begin{bmatrix} \cos\varphi_i, & \sin\varphi_i \\ -\sin\varphi_i, & \cos\varphi_i \end{bmatrix}, \dots \begin{bmatrix} \cos\varphi_r, & \sin\varphi_r \\ -\sin\varphi_r, & \cos\varphi_r \end{bmatrix}, E_k, E_s \right).$$

The matrices in brackets fulfil conditions i) or ii) of Lemma 3. The matrix (3) is an orthogonal matrix so $A \in K_2K_2 \subseteq O_n(R,f)$ by Lemma 3. Since $K_2K_2$ is a normal set, $O_n(R,f) \subseteq K_2K_2 \subseteq O_n(R,f)$.

**Theorem 2.** *Let $A \in O_n(K,f)$. If $K = R$ or $K = GF(p^s)$, $p > 2$, $f$ – quadratic form* (1) *with $\mu = 1$, then $A \in K_2$ iff $A^t = A$, $A \neq E$.*

Proof. It is known that $f$ is an inner product in the case $K = R$; $f$ is also an inner product in the case $K = GF(p^s)$, $p > 2$, by Lemma 2. Hence if $A \in O_n(K,f)$, then $A^tA = AA^t = E$. If $A \in K_2$, then $A^t = A^tE = A^tA^2 = A^tAA = A$.

Conversely, if $A^t = A$, $A \neq E$, then $AA^t = AA = A^2 = E$. Hence $A \in K_2$.

From Theorems 1 and 2 we have

**Corollary 2.1.** *If $K = R$, then each matrix of $O_n(K,f)$ is a product of two symmetric matrices.*

**Corollary 2.2.** *If $K = GF(p^s)$, $p > 2$, $f$ – quadratic form* (1) *with $\eta = 1$, then $O_2(K,f) = K_2K_2$ and each matrix is a product of symmetric matrices.*

Proof. A simple calculation shows that

$$O_2(K,f) = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix}, \begin{bmatrix} a & b \\ b & -a \end{bmatrix},\ a^2 + b^2 = 1 \right\}.$$

These matrices fulfil the conditions i) and ii) of Lemma 3. Thus they belong to $K_2K_2$, by Lemma 3. The second part of the Theorem follows from Theorem 2.

**Theorem 3.** *If $K = GF(p^s)$, $p > 2$, $f-$ quadratic form* (1) *with $\eta \neq 1$, then $O_2(K, f) = K_2K_2$.*

Proof. A calculation shows, that matrices of the group $O_2(K, f)$ have the form

$$A = \begin{bmatrix} a & b \\ -b\eta^{-1} & a \end{bmatrix}, \quad B = \begin{bmatrix} a & b \\ b\eta^{-1} & -a \end{bmatrix}, \; a^2 + \eta d^2 = \eta \,.$$

We have

$$TAT = A^{-1},\; T \in K_2, \quad \text{where } T = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \neq A$$

$$SBS = B^{-1}, \quad \text{where } S = -E \neq B \,.$$

Hence $A, B \in K_2K_2$, by Lemma 1.

**Lemma 5.** *In the group $PGL(2, K)$, $K_2K_2 = PGL(2, K)$.*

Proof. A calculation shows that

$$K_2 = \left\{ \begin{bmatrix} u & 0 \\ 0 & v \end{bmatrix}, \begin{bmatrix} x & y \\ t & -x \end{bmatrix}, \; u \neq v,\; u^2 + v^2 = s,\; x^2 + yt = k, \right.$$
$$\left. s, k \in K^x \right\}.$$

We have

(6) $$TA_1T = A_1^{-1}Z, \text{ where}$$
$$T = \begin{bmatrix} 1 & ab^{-1} \\ 0 & -1 \end{bmatrix} Z = \begin{bmatrix} b & a \\ 0 & -b \end{bmatrix} Z,\; A_1 = \begin{bmatrix} 0 & 1 \\ b & a \end{bmatrix} Z$$
and $A_1Z \neq TZ \in K_2$.

(7) $$TA_2 = A_2^{-1}Z,\; A_2Z \neq TZ \in K_2, \text{ where}$$
$$T = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} Z, \quad A_2 = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} Z \,.$$

From (6), (7) and Lemma 1 follows that $A_1Z$, $A_2Z \in K_2K_2$. The set $K_2K_2$ is a normal set, so matrices similar to $A_1Z$, $A_2Z$ also belong to the set $K_2K_2$. It is known that each matrix of $GL(2, K)$ is similar to the matrix $A_1$ or $A_2$. Thus in the group $PGL(2, K)$ each matrix is similar to the matrix $A_1Z$ or $A_2Z$. Therefore $PGL(2, K) \subseteq K_2K_2 \subseteq PGL(2, K)$.

The Lemma 5 does not hold for $n \geq 3$.

**Theorem 4.** *If $n \geq 3$, then $K_2K_2 \neq PGL(n, K)$.*

Proof. Let us consider all the possible cases: i) $|K| > 3$, $|K| \neq GF(4)$, ii) $|K| = 2$, iii) $|K| = 3$, iv) $|K| = 4$.

In the case i) let $A = \mathrm{diag}(u^{-1}, u, 1),\ B = \mathrm{diag}(1, u, u^{-1}) \in GL(3, K)$. In this case there is an element $u$ such that $u^3 \neq 1$. A calculation shows that if $\bar{A} = AZ,\ \bar{B} = BZ$, then $\bar{A}, \bar{B} \in K_2K_2$ but $\bar{A}\bar{B} \notin K_2K_2$ by Lemma 1. Therefore the matrices $\mathrm{diag}(A, E_s)Z$,
$\mathrm{diag}(B, E_s)Z \in M_{n\times n}\ (K),\ n = 3 + s$, belong to the set $K_2K_2$ but their product does not belong to the set $K_2K_2$. In the remaining cases we act similarly, namely in the case ii) we take

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \qquad B = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

and in the case iii)

$$A = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 0 & 2 \\ 0 & 1 & 0 \end{bmatrix}, \qquad B = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 2 & 2 \end{bmatrix}.$$

In the case iv) there exists an element $u$ such that $u^2 \neq 1$. A calculation shows that if $u^2 \neq 1$, then the matrix $\bar{A} = AZ$ with $A = \mathrm{diag}(u^2, u^2, u)$ cannot be similar to $A^{-1}Z$ in the group $PGL(3, K)$. Hence from Lemma 1 follows that $\bar{A} \notin K_2K_2$. Therefore the matrix
$\mathrm{diag}(A, E_s)Z \in M_{n\times n}\ (K),\ n = 3 + s$, does not belong to the set.

In the cases i), ii), iii) we proved more than stated in Theorem 4, namely

**Corollary 4.1.** *If $n \geq 3,\ K \neq GF(4)$, then $K_2K_2$ is not a subgroup of $PGL(n, K)$.*

By the way we remark that if $n \geq 3$, then $K_2K_2 \not\leq GL(n, K)$,
$K_2K_2 \not\leq SL(n, K)$ and $K_2K_2 \not\leq PSL(n, K)$, (see [2]).

**Theorem 5.** *If $K = GF(p^s),\ p > 2$, then*

*i)* $O_3^+ = (K, f) = K_2K_2$,

*ii)* $\Omega_3(k, f) = K_2K_2$, *where $-1$ is a square,*

*iii)* $K_2K_2 \not\leq \Omega_3(K, f)$, *where $-1$ is not a square.*

Proof. It is known (see [4] p.94) that $O_3^+(K, f) \simeq PGL(2, K)$ and $\Omega_3(K, f) \simeq PSL(2, K)$. Now i) follows from Lemma 5 while ii) and iii) follow from the theorem 5 of [2].

**Theorem 6.** *If $K = GF(p^s),\ p > 2$, then $O_3(K, f) = K_2K_2$.*

Proof. It is known (see [4] p.84) that $O_3(K, f)$ is a Cartesian product $E \times O_3^+(K, f)$. Let $(E, A) \in O_3(K, f)$. From Theorem 5 and Lemma 1 it follows that for each $A \in O_3^+(K, f)$ there exists $T_A \in K_2 \subset O_3^+(K, f)$ such that $T_A \neq A$ and $T_AAT_A = A^{-1}$. Hence the matrix $T = (E, T_A)$ fulfils conditions $T \neq (E, A)$, $T^2 = (E, E)$ and $T(E, A)T = (E, A)^{-1}$. Thus $(E, A) \in K_2K_2 \subseteq O_3(K, f)$ by Lemma 1. Therefore $O_3(K, f) \subseteq K_2K_2$.

**Theorem 7.** *If $K = GF(p^s)$, $p > 2$, then $O_n(K, f) = K_2K_2$.*

Proof. Induct on $n$. Theorem is true for $n = 2$, by Theorem 3 and Corollary 2.2, and for $n = 3$, by Theorem 6. Suppose that the Theorem holds for $n - 1$. Let $\dim V = n$, $A \in O_n(K, f)$. Since the determinant of $f$ is different from zero, there exists $v \in V$ such that $Av \neq O$. Let us consider all possible cases.

i). If $Av = v$, then $V = [\,v\,] \oplus [\,v\,]^{\perp}$ and $A([\,v\,]^{\perp}) = [\,v\,]^{\perp}$. In the basis $(v, e_2, \ldots, e_n)$, $e_i \in [\,v\,]^{\perp}$, the transformation has the matrix $A = \begin{bmatrix} 1 & 0 \\ 0 & A_1 \end{bmatrix}$. The matrix $A_1$ is an orthogonal $n-1$ by $n-1$ matrix. Hence $A_1 \in K_2K_2 \subseteq O_{n-1}(K, f')$ by the induction hypothesis. Therefore there exists $T_1 \neq A_1$, by Lemma 1, such that $T_1 \in K_2$ and $T_1A_1T_1 = A_1^{-1}$. The matrix $T = \begin{bmatrix} 1 & 0 \\ 0 & T_1 \end{bmatrix} \in O_n(K, f)$ fulfils all assumptions of Lemma 1 so $TAT = A^{-1}$. Hence $A \in K_2K_2 \subseteq O_n(K, f)$.

ii) If $Av = -v$, then in the basis $(v, e_2, \ldots, e_n)$ the transformation $A$ has the matrix $A = \begin{bmatrix} -1 & 0 \\ 0 & A_2 \end{bmatrix}$. The rest of the proof is similar to i).

iii) Now let $Av$ be without any conditions. Since $\operatorname{char} K \neq 2$ and $A$ is an orthogonal transformation, by simple calculation $f(v + Av) + f(-v + Av) = 4f(v) \neq 0$. Hence $f(v{+}Av) \neq 0$ or $f(-v{+}Av) \neq 0$. If $f(v{+}Av) \neq 0$, then $V = [v + Av] \oplus [v + Av]^{\perp}$ and the transformation

a) $$S_{v+Av}x = x - \frac{2B(x, v + Av)}{f(v + Av)}(v + Av) \text{ for all } \ x \in v$$

is an orthogonal reflection with regard to $[v + Av]^{\perp}$, (see [3] p.86).
For $x = Av$ we have

$$S_{v+Av}(Av) = Av - \frac{2B(Av, v + Av)}{f(v + Av)}(v + Av)$$

A simple calculation shows that $B(Av, v + Av) = \frac{1}{2}f(v + Av)$. Hence $S_{v+Av}Av = -v$ is an orthogonal transformation and as a result $A(v) = -S_{v+Av}(v)$ for all $v \in V$, by $S^2_{v+Av} = E$. Therefore $A(v + Av) = -S_{(v+Av)}(v + Av) = v + Av$, by a). Thus we obtain the case i). If $f(-v + Av) \neq 0$, then the same calculation gives $A(-v + Av) = -(-V + Av)$ i.e. the case ii). By mathematical induction, the theorem holds for every $n$.

**Theorem 8.** *In the unitary group $U_n(C,f)$, $K_2K_2 \neq U_n(C,f)$.*

Proof. If $n \geq 3$, then the matrix $A = \varepsilon E \in U_n(C,f)$, where $\varepsilon$ is a primary $n^{\text{th}}$ root of unity. There does not exist $T \in K_2$ such that $T^{-1}AT = A^{-1}$ because otherwise we receive $A^2 = E$, a contradiction.

If $n = 2$, the matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ must fulfil the following conditions: $a\bar{a} = c\bar{c} = 1$, $b\bar{b} + d\bar{d} = 0$, $a\bar{b} + c\bar{d} = 0$, $ad - bc = 1$.
Thus $A = \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}$, $a\bar{a}+b\bar{b} = 1$. A simple calculation shows that $A^2 = E$ iff $A = \pm E$.

The same formal calculation as in the proof of Theorem 8 in the case $n = 2$, shows that $K_2K_2 = \{E\}$ is the group $SU(2,p^{2k})$. The definition of $SU(2,p^{2k})$ is given in [6] p.194.

For the investigation of automorphism of a quadratic form over $K = GF(2^s)$ we need a few more lemmas.

**Lemma 6.** *Let $G$ be a group, $P$ a subset such that $P = P^{-1}$ and $G - P$ a subgroup of $G$. Then $G - P \leq PP$.*

Proof. We have

$$bP \cap P \neq \emptyset \text{ for each } b \in G - P\,. \tag{8}$$

If not, there exists $c \in G - P$ such that $cP \subset G - P$. Hence there exists $p \in P$ such that $cp = g \in G - P$ and $p = C^{-1}g \in G - P$, a contradiction. Now (8) implies that for each $b \in G-P$ there exist $p_1, p_2$ such that $bp_1 = p_2$ i.e. $b = p_2p_1^{-1} \in PP$, by $P^{-1} = P$. Hence $G - P \subset PP$.

**Lemma 7.** *Let $G$ be a group, $H < G$. Then $(G - H)^2 \trianglelefteq G$, (see [1]).*

From Lemmas 6 and 7 results

**Theorem 9.** *Let $G$ be a group, $P$ a subset of $G$ such that $P = P^{-1}$ and $G - P$ a subgroup of $G$. Then $G - P < PP \trianglelefteq G$.*

By Lemma 2 a quadratic form over $GF(2^s)$ is

$$\text{a)} \quad f = x_1x_2, \qquad \text{b)} \quad f = x_1x_2 + \lambda(x_1^2 + x_2^2),\ \lambda \neq 0\,.$$

The following two theorems concern groups of automorphisms of forms a), b).

**Theorem 10.** *In the group $O_2(K,f)$, $K = GF(2^s)$ with $f = x_1x_2$, $K_2K_2 = O_2^+(K,f) \neq O_2(K,f)$.*

PROOF. If $|K| = 2$, then the theorem is evident because $K_2 = \{E\}$. If $|K| \neq 2$, then

$$O_2(K,f) = \left\{ \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}, \begin{bmatrix} 0 & b \\ b^{-1} & 0 \end{bmatrix},\ a,b \in K^x \right\},$$
$$K_2 = \left\{ \begin{bmatrix} 0 & b \\ b^{-1} & 0 \end{bmatrix};\ b \in K^x \right\}$$

and $O_2^+(K,f) = O_2(K,f) - K_2$ is a subgroup of $O_2(K,f)$. From Theorem 9 for $P = K_2$ we have $O_2^+(K,f) \leq K_2K_2 \lhd O_2(K,f)$. It is easy to see that $K_2K_2 \subseteq O_2^+(K,f)$. Hence $K_2K_2 = O_2^+(K,f)$.

**Theorem 11.** *If $K = GF(2^s)$, then in the group $O_2(K,f)$ with*

$$f = x_1x_2 + \lambda(x_1^2 + x_2^2), \quad \lambda \neq 0,$$
$$O_2^+(K,f) = O_2(K,f) - K_2 = K_2K_2 \neq O_2(K,f).$$

PROOF. The matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in O_2(K,f)$ must fulfil the conditions

$$ac\lambda^{-1} + a^2 + c^2 = 1, \quad bd\lambda^{-1} + b^2 + d^2 = 1, \quad ad + bc = 1. \tag{9}$$

Thus matrices of group $O_2(K,f)$ have the form $\begin{bmatrix} a & b \\ c & a \end{bmatrix}$ or $\begin{bmatrix} a & b \\ b & d \end{bmatrix}$ and

$$K_2 = \left\{ \begin{bmatrix} a & b \\ c & a \end{bmatrix},\ a \neq 1 \vee b \neq 0 \vee c \neq 0 \right\}.$$

The set

$$O_2^+(K,f) = \left\{ \begin{bmatrix} a & b \\ b & d \end{bmatrix},\ a \neq 1 \vee d \neq 0 \vee b \neq 1, \quad a + d = d\lambda^{-1} \right\}$$

is a subgroup of $O_2(K,f)$, (see [4], p.105). From Theorem 9 results that

$$O_2^+(K,f) \leq K_2K_2 \trianglelefteq O_2(K,f). \tag{10}$$

By Lemma 1 and a simple calculation we see that $F = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \notin K_2K_2$. Hence $K_2K_2 \neq O_2(K,f)$. Let us observe that $K_2K_2 \subseteq O_2^+(K,f)$. Indeed, we have

$$\begin{bmatrix} a & b \\ c & a \end{bmatrix} \cdot \begin{bmatrix} a_1 & b_1 \\ c_1 & a_1 \end{bmatrix} = \begin{bmatrix} aa_1 + bc_1, & ab_1 + ba_1 \\ ca_1 + ac_1 & cb_1 + aa_1 \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} = C.$$

From conditions (9) for $b_1 \neq 0,\ b \neq 0$ we have $s = c_{11} + c_{22} = bc_1 + cb_1 = bb_1^{-1}(a_1^2 + 1) + b_1 b^{-1}(a^2 + 1) = ba_1 + b_1 a\lambda^{-1} = c_{12}\lambda^{-1}$. The proof is similar if $c \neq 0,\ c_1 \neq 0$. Similarly it can be shown that $c_{21} = c_{12}$. Thus $C \in O_2(K, f)$. Therefore $K_2K_2 \subseteq O_2^+(K, f)$ and $O_2^+(K, f) = K_2K_2$, by (10).

**Lemma 8.** *If $K = GF(2^s)$, then $K_2K_2 \neq O_3(K, f)$.*

Proof. A calculation shows that $K_2$ consists of matrices

$$A = \begin{bmatrix} a & , a(a^2+1)b^{-2} & ,0 \\ b^2a^{-1} & , a & ,0 \\ b & , ab^{-1}(a+1) & ,1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & c^2 & 0 \\ 0 & 1 & 0 \\ 0 & c & 1 \end{bmatrix},$$

$$C = \begin{bmatrix} 0 & d & 0 \\ d^{-1} & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \qquad D = \begin{bmatrix} 1 & 0 & 0 \\ e^2 & 1 & 0 \\ e & 0 & 1 \end{bmatrix}.$$

We will show that $B \notin K_2K_2$. Suppose that there exists $T \in K_2$ such that $T \neq B$ and $TBT = B^{-1}$. The condition $T \neq B$ is fulfilled by matrices $A, C, D$. A simple calculation shows that the equalities $ABA = B$, $CBC = B$, $DBD = B$ do not hold. Thus $B \in K_2K_2$ by Lemma 1.

**Theorem 12.** *If $K = GF(2^s)$, then $K_2K_2 \neq O_n(K, f)$.*

Proof. If $n$ is even, then from Theorem 10, 11 and Lemma 1 it results that there exists $A_1 \in O_2(K, f)$ for wich there is no $T_1 \in K_2 \subset O_2(K, f)$ such that $T_1 \neq A_1$ and $T^{-1}A_1T_1 = A_1^{-1}$. Hence for $A = \mathrm{diag}(E_m, A_1) \in O_{m+2}(K, f)$ ($m$–even, $f$–extension quadratic form $f$ to $n = m + 2$) there is no $T \in K_2 \subset O_{m+2}(K, f')$ such that $T \neq A$, $T^{-1}AT = A^{-1}$. Therefore $A \notin K_2K_2 \subset O_{m+2}(K, f')$, by Lemma 1.

If $n$ is odd, the proof is the same except that we use Lemma 8, instead of Theorems 10, 11.

## References


[1] E. Ambrosiewicz, On the property $W$ for modular groups, *Demonstratio Mathematica,* Vol **XI,** Nr 2 (1978).

[2] J. Ambrosiewicz, On the square of sets of linear groups, *Rend. Sem. Mat. Univ. Padova,* Vol **75** (1986).

[3] Н. Бурбаки , Группы и Алгебры Ли, Москва, 1972.

[4] Ж. Дьёдонне , Геометрия классических групп, Москва, 1974.

[5] L. E. Dickson, Linear groups, *Berlin, Tubner*, 1900.

[6] B. Huppert, Endliche Gruppen I, *Springer–Verlag*, *Berlin Heidelberg New York*, 1967.

[7] F. Bachmann, Eine Kennzeichnung der Gruppe der gebrochen linearen Transformationen, *Math. Annalen, Bd.* **126.8** (1953), 79–92.

JAN AMBROSIEWICZ
INSTITUTE OF MATHEMATICS, TECHNICAL UNIVERSITY
OF BIAŁYSTOK
15–351 BIAŁYSTOK
UL. WIEJSKA 45 A
POLAND

*(Received May 21, 1991)*