Canad. Math. Bull. Vol. **35** (3), 1992 pp. 400–409

FACTORIZATION INTO SYMMETRIES AND TRANSVECTIONS OF GIVEN CONJUGACY CLASSES

FRIEDER KNÜPPEL

ABSTRACT. The u-invariant $u(K)$ of a field K is the smallest number $k \in \mathbb{N} \cup \{\infty\}$ such that every k-dimensional regular quadratic form over K is universal. Let $O(V,f)$ be the orthogonal group of a finite-dimensional regular metric vector space over a field K of characteristic distinct from 2. Let $\pi \in O(V)$, $B(\pi) := V(\pi - 1)$, $\dim[B(\pi) \cap \text{kernel}(\pi - 1)] \geq u(K)$. Given $\lambda_1, \ldots, \lambda_m \in K^*$ where $m := \dim B(\pi) - u(K) + 1$. Then $\pi = \sigma_1 \cdot \cdots \cdot \sigma_k$ where $k := \dim B(\pi)$ and σ_i is a symmetry with negative space Ka_i and $f(a_i, a_i) = \lambda_i$ for $i \in \{1, \ldots, m\}$. We prove similar theorems also for symplectic groups where transvections are taken as generators.

The present paper emerged from an attempt to provide short self-contained proofs of the results [1] and [2] within a more general frame. Let G be the orthogonal or symplectic group of an n-dimensional vector space V over a field. Call $\sigma \in G$ *simple* if $\dim\big(\text{kernel}(\sigma - 1)\big) = n - 1$. We want to write a given $\pi \in G$ as a product of simple elements of G such that the number of factors is small and certain factors belong to prescribed conjugacy classes of G. Background material for reading this paper may be found in [3].

1. **Prerequisites, notations and basic facts.** Let K be a field with $\text{char}\, K \neq 2$. Let $u := u(K)$ denote the u-invariant of K. By definition u is the smallest number $k \in \mathbb{N}$ (∞ if such a number k does not exist) with the following property: If Q is a regular quadratic form on a K-vector space W and $\dim W \geq u$ then $Q(W) = K$, *i.e.* Q is universal. Observe that $u(K) = 2$ when K is finite.

Let V be an n-dimensional vector space ($n \in \mathbb{N}$) and $f\colon V \times V \longrightarrow K$ a regular symmetric or skew-symmetric bilinear form. Let $G := \{\pi \in \text{GL}(V) \mid f(a\pi, b\pi) = f(a,b) \text{ for all } a, b \in V\}$. When f is symmetric then G is called an *orthogonal group* $O(V)$, when f is skew-symmetric then G is a symplectic group $\text{Sp}(V)$.

For $\pi \in \text{End}(V)$ let $B(\pi) := V(\pi - 1)$ be the path, $F(\pi) := \text{kernel}(\pi - 1)$ the fix and $N(\pi) := F(-\pi)$ the negative space of π. Clearly, $\dim B(\pi) + \dim F(\pi) = n$ and $N(\pi) \subset B(\pi)$. Call π *simple* if $\dim B(\pi) = 1$. If $\pi \in G$ then $F(\pi)^{\perp} = B(\pi)$. We use frequently the path rule:

(1) Let $\varphi, \pi \in \text{End}(V)$. Then $B(\varphi\pi) \subset B(\varphi) + B(\pi)$.

In particular this rule yields

(2) Let $\pi = \sigma_1 \cdot \cdots \cdot \sigma_s$ for simple elements $\sigma_1, \ldots, \sigma_s \in \text{End}(V)$. Then $\dim B(\pi) \leq s$. If $\dim B(\pi) = s$ then $B(\pi) = B(\sigma_1) \oplus \cdots \oplus B(\sigma_s)$.

Received by the editors April 5, 1991; revised December 19, 1991.
AMS subject classification: 51N30, 11E57, 15A23, 14L35.

https://doi.org/10.4153/CMB-1992-053-5 Published online by Cambridge University Press

The simple elements in $O(V)$ are the symmetries σ_a where $a \in V$ is anisotropic. The symmetry σ_a is defined by the property $B(\sigma_a) = Ka$. The simple elements of $\mathrm{Sp}(V)$ are the (symplectic) transvections $\tau_{\mu,w}\colon v \longmapsto v + \mu f(v,w)w$ where $w \in V\backslash O$ and $\mu \in K^*$. Observe that $B(\tau_{\mu,w}) = Kw$ and $\tau_{\mu,w}^{-1} = \tau_{-\mu,w}$. For $\lambda \in K^*$ call σ_a a λ-symmetry if $\lambda K^{*2} = d\big(B(\sigma_a)\big) = f(a,a)K^{*2}$; call $\tau_{\mu,w}$ a λ-transvection if $\lambda K^{*2} = \mu K^{*2}$. Let $\Theta\colon O(V) \longrightarrow K^*/K^{*2}$ denote the spinorial norm. Then $\Theta(\sigma_a) = f(a,a)K^{*2}$ for each symmetry σ_a.

We will frequently use the following elementary lemma.

LEMMA 1.1. *Let G be an orthogonal or symplectic group. Let $\varphi \in G$ and τ a simple element of G. The following statements are equivalent.*

(i) $\dim F(\varphi\tau) = \dim F(\varphi) + 1$.
(ii) $B(\tau) \not\subset B(\varphi\tau)$;
(iii) $B(\varphi) = B(\tau) \oplus B(\varphi\tau)$;
(iv) $B(\varphi\tau)$ *is properly contained in* $B(\varphi)$;
(v) $F(\varphi)$ *is properly contained in* $F(\varphi\tau)$.

The following facts are well-known and easy to prove.

(3) Let $\lambda \in K^*$. The set $S(\lambda)$ of λ-symmetries in $O(V)$ is a conjugacy class in $O(V)$. The set $T(\lambda)$ of λ-transvections is a conjugacy class in $\mathrm{Sp}(V)$.

(4) Let $\pi \in O(V)$ and $B(\pi) \not\subset F(\pi)$ (*i.e.* $B(\pi)$ is not totally isotropic). Then π is a product of $\dim B(\pi)$ symmetries.

(4′) Let $\pi \in \mathrm{Sp}(V)$ and $B(\pi) \not\subset N(\pi)$ (*i.e.* $\pi^2 \neq 1$). Then π is a product of $\dim B(\pi)$ transvections.

2. **Results.**

PROPOSITION 1. *Let $K \neq \mathrm{GF}\,3$, $\pi \in O(V)$, $s := \dim\big(B(\pi) \cap F(\pi)\big) + 1$ and $\lambda_1, \ldots, \lambda_s \in L(\pi) := \{Q(v) \mid v \in B(\pi)\} \setminus \{0\}$. Then $\pi = \sigma_1 \cdot \cdots \cdot \sigma_{\dim B(\pi)}$ for symmetries σ_i such that $\sigma_1 \in S(\lambda_1), \ldots, \sigma_s \in S(\lambda_s)$.*

THEOREM 1. *Let $K \neq \mathrm{GF}\,3$ and $\pi \in O(V)$ such that $\dim B(\pi)/\big(B(\pi) \cap F(\pi)\big) \geq u$. Let $m := \dim B(\pi) - u + 1$. Given $\lambda_1, \ldots, \lambda_m \in K^*$. Then $\pi = \sigma_1 \cdot \cdots \cdot \sigma_{\dim B(\pi)}$ for symmetries σ_i such that $\sigma_1 \in S(\lambda_1), \ldots, \sigma_m \in S(\lambda_m)$.*

THEOREM 2. *Let $K \neq \mathrm{GF}\,3$ and $\pi \in O(V)$. Let*

$$m := \max\{\dim B(\pi) - u + 1, \dim \operatorname{rad} B(\pi) + 1\}.$$

Given $\lambda_1, \ldots, \lambda_m \in L(\pi) := \{Q(v) \mid v \in B(\pi)\} \setminus \{0\}$. Then $\pi = \sigma_1 \cdot \cdots \cdot \sigma_{\dim B(\pi)}$ for symmetries σ_i such that $\sigma_1 \in S(\lambda_1), \ldots, \sigma_m \in S(\lambda_m)$.

COROLLARY 1. *Let $K \neq \mathrm{GF}\,3$ and $\pi \in O(V)$ such that $\dim B(\pi)/\big(B(\pi) \cap F(\pi)\big) \geq u$. Let $m := \dim B(\pi) - u + 1$. Then $\pi = \sigma_1 \cdot \cdots \cdot \sigma_{\dim B(\pi)}$ for symmetries σ_i with $\sigma_1, \ldots, \sigma_m \in$* kernel Θ.

The following two corollaries apply in particular to finite fields.

https://doi.org/10.4153/CMB-1992-053-5 Published online by Cambridge University Press

COROLLARY 2. *Let* $u \leq 2$ *and* $K \neq \mathrm{GF}\,3$. *Let* $\pi \in O(V)$, $\dim B(\pi)/\big(B(\pi) \cap F(\pi)\big) \geq u$ *and* $\lambda_1, \ldots, \lambda_{\dim B(\pi)} \in K$ *such that* $\lambda_1 \cdot \cdots \cdot \lambda_{\dim B(\pi)} K^{*2} = \Theta(\pi)$. *Then* $\pi = \sigma_1 \cdot \cdots \cdot \sigma_{\dim B(\pi)}$ *for* λ_i*-symmetries* σ_i, $i \in \{1, \ldots, \dim B(\pi)\}$.

COROLLARY 3. *Let* $u \leq 2$ *and* $K \neq \mathrm{GF}\,3$ *and* $\pi \in \mathrm{kernel}(\Theta)$.

a) If $\dim B(\pi)/\big(B(\pi) \cap F(\pi)\big) \geq u$ *then* $\pi = \sigma_1 \cdot \cdots \cdot \sigma_{\dim B(\pi)}$ *for 1-symmetries (i.e. symmetries in* $\mathrm{kernel}\,\Theta$*).*

b) If $\dim B(\pi)/\big(B(\pi) \cap F(\pi)\big) < u$ *and* $\pi \neq 1$ *then* π *is a product of* $\dim B(\pi) + 2$ 1*-symmetries, but not a product of less than* $\dim B(\pi)+2$ 1*-symmetries, with the following exception: If* $\dim B(\pi)/\big(B(\pi) \cap F(\pi)\big) = 1$ *and* $Q(a) = 1$ *for some* $a \in B(\pi)$ *then* π *is a product of* $\dim B(\pi)$ 1*-symmetries.*

c) $\mathrm{kernel}\,\Theta$ *is generated by the set of* 1*-symmetries.*

PROPOSITION 2. *Let* $K \neq \mathrm{GF}\,3$, $\pi \in \mathrm{Sp}(V)$, $s := \dim N(\pi) + 1$ *and* $\lambda_1, \ldots, \lambda_s \in L(\pi) := \{-f(v, v\pi) \mid v \in V\} \setminus \{0\}$. *Then* $\pi = \tau_1 \cdot \cdots \cdot \tau_{\dim B(\pi)}$ *for transvections* τ_i *such that* $\tau_1 \in T(\lambda_1), \ldots, \tau_s \in T(\lambda_s)$.

THEOREM 3. *Let* $K \neq \mathrm{GF}\,3$ *and* $\pi \in \mathrm{Sp}(V)$ *such that* $\dim B(\pi)/N(\pi) \geq u$. *Let* $m := \dim B(\pi) - u + 1$. *Given* $\lambda_1, \ldots, \lambda_m \in K^*$. *Then* $\pi = \tau_1 \cdot \cdots \cdot \tau_{\dim B(\pi)}$ *for some transvections* τ_i *such that* $\tau_1 \in T(\lambda_1), \ldots, \tau_m \in T(\lambda_m)$.

THEOREM 4. *Let* $K \neq \mathrm{GF}\,3$ *and* $\pi \in \mathrm{Sp}(V)$. *Let*

$$m := \max\{\dim B(\pi) - u + 1, \dim N(\pi) + 1\}.$$

Given $\lambda_1, \ldots, \lambda_m \in L(\pi) := \{-f(v, v\pi) \mid v \in V\} \setminus \{0\}$. *Then* $\pi = \tau_1 \cdot \cdots \cdot \tau_{\dim B(\pi)}$ *for some transvections* τ_i *such that* $\tau_1 \in T(\lambda_1), \ldots, \tau_m \in T(\lambda_m)$.

The following two corollaries apply in particular to finite fields.

For $\pi \in \mathrm{Sp}(V)$ let $d(\pi)$ denote the discriminant of the bilinear form $f_\pi \colon B(\pi) \times B(\pi) \longrightarrow K, f_\pi\big(v(\pi - 1), b\big) := -f(v, b)$. For more details on f_π see 4.1.

COROLLARY 4. *Let* $u \leq 2$ *and* $K \neq \mathrm{GF}\,3$. *Let* $\pi \in \mathrm{Sp}(V)$, $\dim B(\pi)/N(\pi) \geq u$ *and* $\lambda_1, \ldots, \lambda_{\dim B(\pi)} \in K$ *such that*

$$\lambda_1 \cdot \cdots \cdot \lambda_{\dim B(\pi)} (-1)^{\dim B(\pi)} K^{*2} = d(\pi).$$

Then $\pi = \tau_1 \cdot \cdots \cdot \tau_{\dim B(\pi)}$ *for* λ_i*-transvections* τ_i, $i \in \{1, \ldots, \dim B(\pi)\}$.

COROLLARY 5. *Let* $u \leq 2$ *and* $K \neq \mathrm{GF}\,3$. *Given* $\lambda \in K^*$ *and* $\pi \in \mathrm{Sp}(V)$.

a) If $\dim B(\pi)/N(\pi) \geq u$ *and* $d(\pi) = (-\lambda)^{\dim B(\pi)} K^{*2}$ *then* $\pi = \tau_1 \cdot \cdots \cdot \tau_{\dim B(\pi)}$ *for* λ*-transvections* τ_i.

b) If $\dim B(\pi)/N(\pi) \geq u$ *and* $d(\pi) \neq (-\lambda)^{\dim B(\pi)+1} K^{*2}$ *then* $\pi = \tau_1 \cdot \cdots \cdot \tau_{\dim B(\pi)+1}$ *for some* λ*-transvections* τ_i *and* π *is not a product of less than* $\dim B(\pi) + 1$ λ*-transvections.*

c) If $\dim B(\pi)/N(\pi) < u$ *then* $\pi = \tau_1 \cdot \cdots \cdot \tau_{\dim B(\pi)+1}$ *for* λ*-transvections* τ_i *and* π *is not a product of less than* $\dim B(\pi) + 1$ λ*-transvections, with the following exception: If*

https://doi.org/10.4153/CMB-1992-053-5 Published online by Cambridge University Press

$\dim B(\pi)/N(\pi) = 1$ *and* $f(w, w\pi) = \lambda$ *for some* $w \in V$ *then* $\pi = \tau_1 \cdot \cdots \cdot \tau_{\dim B(\pi)}$ *for some* λ*-transvections* τ_i.

REMARKS. 1. Corollary 3 includes the main result of [1] and Corollary 5 improves the main result of [2]. We need not consider normal forms. The procedure when proving Theorems 3 and 4 on symplectic groups and the corresponding Theorems 1 and 2 on orthogonal groups is essentially the same. This is achieved with the help of E. T. Wall's bilinear form.

2. We have proved similar Theorems within the more general approach when K is a local ring. However, in the present exposition we want to avoid difficulties due to such a generalization.

3. In our Theorems we must exclude $K = \mathrm{GF}\,3$. Let $K = \mathrm{GF}\,3$. It is fairly easy to find out when kernel Θ is generated by its symmetries; this is *e.g.* always true when $n \geq 5$; *cf.* 3.7. But we guess it is difficult to determine the *minimal* number of factors in a representation of a given $\pi \in$ kernel Θ as a product of 1-symmetries (as it is achieved in Corollary 3 when $K \neq \mathrm{GF}\,3$). Our arguments to this point are lengthy and involved. The analogue gap appears in Corollary 5 for symplectic groups.

3. **The orthogonal case.**

We assume that f is symmetric and write $Q(v) := f(v, v)$.

3.1 . Let $K \neq \mathrm{GF}\,3$ and $w \in V$ with $Q(w) \neq 0$. There is a basis $C = \{c_1, \ldots, c_n\}$ for V such that $Q(c) = Q(w)$ for every $c \in C$. Furthermore, we can achieve that $c_i \perp c_j$ for $i,j \in \{1, \ldots, n - u + 1\}$ and $i \neq j$.

PROOF BY INDUCTION. Let $n \geq 2$. Choose an $n-1$-dimensional regular subspace T of V with $w \in T$. By our hypothesis we obtain a basis C for T such that $Q(c) = Q(w)$ for each $c \in C$. Since $K \neq \mathrm{GF}\,3$ we find some anisotropic $z \in V \setminus (T \cup T^{\perp})$. Then $T\sigma_z \neq T$, hence $c'\sigma_z \notin T$ for some $c' \in C$. Clearly, $C \cup \{c'\sigma_z\}$ is a basis for V with the desired property. The "furthermore" statement follows now immediately from the definition of u.

3.2 . Theorem 1 holds under the additional assumption that $B(\pi)$ is regular and $m := \dim B(\pi) - u + 1 \leq 2$.

PROOF. Using 1.(4) we can assume that $m \geq 1$, hence $m \in \{1, 2\}$. Observe that $\pi - 1 \in \mathrm{GL}(V)$.

Let $m = 1$ and $\lambda_1 \in K^*$. Then $\dim B(\pi) = u$. Choose $c \in B(\pi)$ with $Q(c) = \lambda_1$. Let $\sigma_1 := \sigma_c$ and $\varphi := \pi\sigma_1$. Then $\dim B(\pi) = \dim B(\varphi) \oplus B(\sigma_c)$. If $\dim B(\varphi) = 1$ then φ is a symmetry. Else $\dim B(\varphi) > \frac{1}{2} \dim B(\pi)$, hence $B(\varphi)$ is not totally isotropic. In both cases φ is a product of $\dim B(\varphi)$ symmetries and the assertion follows. Now let $m = 2$ and $\lambda_1, \lambda_2 \in K^*$. We claim that

$$(*) \qquad Q\big(b(\pi - 1)^{-1}\big) \neq 0 \text{ and } Q(b) = \lambda_1 \text{ for some } b \in B(\pi).$$

Indeed $(*)$ yields the assertion: Let $a := b(\pi - 1)^{-1}$ and $\sigma_1 := \sigma_b$. Then $\varphi := \pi\sigma_1$ satisfies $F(\varphi) = Ka$, hence $B(\varphi) = a^{\perp}$ is regular. The previous case $m = 1$ supplies symmetries $\sigma_2, \ldots, \sigma_{\dim B(\pi)}$ such that $\varphi = \sigma_2 \cdot \cdots \cdot \sigma_{\dim B(\pi)}$ and $Q(v_2) = \lambda_2$. The assertion follows.

PROOF OF $(*)$. Using $l := \dim B(\pi) \geq u$ and 3.1 we obtain a basis $\{b_1, \ldots, b_l\}$ for $B(\pi)$ such that $Q(b_i) = \lambda_1$ for $i \in \{1, \ldots, l\}$.

First let us assume

(+) For each i, j with $1 \leq i < j \leq l$ there is some $b_{ij} \in Kb_i + Kb_j$ such that $Q(b_{ij}) = \lambda_1$ and Kb_i, Kb_j, Kb_{ij} are distinct.

At least one of the vectors $w_i := b_i(\pi - 1)^{-1}$ and $w_{ij} := b_{ij}(\pi - 1)^{-1}$ is anisotropic: Else each subspace $Kw_i + Kw_j$ $(1 \leq i < j \leq l)$ would be totally isotropic as it contains three distinct singular 1-dimensional subspaces; hence $B(\pi)$ would be totally isotropic. Therefore $(*)$ holds true.

Now let us assume that (+) is not valid. Then $\frac{1}{2}|K^*| \leq 2$, in particular $|K| = 5$ and $l = u + 1 = 3$. We may assume that the subspace $Kb_1 + Kb_2$ is anisotropic, hence $Q(b_{12}) = \lambda_1$ and Kb_1, Kb_2, Kb_{12} are distinct for some $b_{12} \in Kb_1 + Kb_2$. At least one of the vectors $b_1(\pi - 1)^{-1}$, $b_2(\pi - 1)^{-1}$ and $b_{12}(\pi - 1)^{-1}$ is isotropic; else $B(\pi)$ would contain a 2-dimensional totally isotropic subspace. Thus we proved $(*)$ also in this case.

3.3. Let $K \neq \mathrm{GF}\,3$ and $\pi \in O(V)$ such that $B(\pi)$ is singular. Let $\lambda \in L(\pi)$ where

$$L(\pi) := \{Q(v) \mid v \in B(\pi)\} \setminus \{0\}$$

(Observe that $L(\pi) = K^*$ whenever $\dim B(\pi)/\operatorname{rad} B(\pi) \geq u$). There is a λ-symmetry σ such that $B(\pi) = B(\pi\sigma) \oplus B(\sigma)$ and $\dim \operatorname{rad} B(\pi\sigma) = \dim \operatorname{rad} B(\pi) - 1$; hence $\operatorname{rad} B(\pi\sigma) = B(\pi\sigma) \cap \operatorname{rad} B(\pi)$ and $L(\pi\sigma) = L(\pi)$.

PROOF. As $B^2(\pi) := V(\pi - 1)^2$ is properly contained in $B(\pi)$ we can find a subspace U such that $B(\pi) = U \oplus \operatorname{rad} B(\pi)$ and $U \not\subset B^2(\pi)$. Then $Q(w) = \lambda$ for some $w \in U$. Statement 4.1 supplies a basis for U whose vectors c fulfill $Q(c) = \lambda$. At least one element of the basis, say a, is not contained in $B^2(\pi)$. Simple arguments show that $\sigma := \sigma_a$ meets the requirements.

3.4 *Proof of Proposition 1.* Using 3.3 $s - 1$ times we obtain λ_i-symmetries σ_i $(i \in \{1, \ldots, s-1\})$ such that $B(\pi\sigma_1 \cdot \cdots \cdot \sigma_{s-1})$ is regular and

$$B(\pi) = B(\pi\sigma_1 \cdot \cdots \cdot \sigma_{s-1}) \oplus B(\sigma_1) \oplus \cdots \oplus B(\sigma_{s-1}) \text{ and } L(\pi\sigma_1 \cdot \cdots \cdot \sigma_{s-1}) = L(\pi).$$

We can choose a λ_s-symmetry σ_s such that $B(\sigma_s) \subset B(\pi\sigma_1 \cdot \cdots \cdot \sigma_{s-1})$. Then $\dim B(\pi\sigma_1 \cdot \cdots \cdot \sigma_s) = \dim B(\pi) - s$ and $\dim\big(\operatorname{rad} B(\pi\sigma_1 \cdot \cdots \cdot \sigma_s)\big) \leq 1$. 1.(4) completes the proof.

3.5 *Proof of Theorems 1 and 2.* Since Theorem 2 is just a combination of Proposition 1 and Theorem 1 we need only consider Theorem 1. Suppose that the assumptions in Theorem 1 are valid.

If $m \leq 0$ the assertion follows from 1.(4). So we can assume that $m \geq 1$. We proceed by induction. If $\dim B(\pi) = 1$ then $u = 1$ and $m = 1$; hence $K^{*2} = K^*$ and π is a λ_1-symmetry.

Let $\dim B(\pi) \geq 2$.

https://doi.org/10.4153/CMB-1992-053-5 Published online by Cambridge University Press

CASE I. $B(\pi)$ is regular. If $m \leq 2$ then 3.2 yields the assertion. Now let $m \geq 3$. Choose $a \in B(\pi)$ with $Q(a) = \lambda_1$; this is possible since $\dim B(\pi)/\operatorname{rad} B(\pi) \geq u$. Then $\sigma_1 := \sigma_a$ fulfills $B(\pi) = B(\pi\sigma_1) \oplus B(\sigma_1)$ and $\dim \operatorname{rad} B(\pi\sigma_1) \leq 1$. Thus

$$\dim B(\pi\sigma_1)/\operatorname{rad} B(\pi\sigma_1) \geq \dim B(\pi) - 2 \geq u.$$

Hence $\pi\sigma_1$ fulfills the requirements of the theorem and the induction hypothesis applies.

CASE II. $B(\pi)$ is singular. Then 3.3 supplies a λ_1-symmetry σ_1 such that $B(\pi) = B(\pi\sigma_1) \oplus B(\sigma_1)$ and $\dim \operatorname{rad} B(\pi\sigma_1) = \dim \operatorname{rad} B(\pi) - 1$. Then $\dim B(\pi\sigma_1)/\operatorname{rad} B(\pi\sigma_1) = \dim B(\pi)/\operatorname{rad} B(\pi) \geq u$. The assertion follows by induction.

3.6 *Proof of Corollaries 1, 2, and 3.* All assertions are obvious from Theorem 1, apart from Corollary 3b). First assume that $\dim B(\pi)/\operatorname{rad} B(\pi) = 1$. Let $\varkappa$ denote the discriminant of $B(\pi)/\operatorname{rad} B(\pi)$ with respect to f. Then $\Theta(\sigma_a) = Q(a)K^{*2} = \varkappa$ for each anistropic vector $a \in B(\pi)$. Now 1.(4) and (2) imply:

(i) π is a product of $\dim B(\pi)$ 1-symmetries if and only if $\varkappa = K^{*2}$.

Now let $\varkappa \neq K^{*2}$. As $1 \leq \dim B(\pi) < n$ we can choose some $a \in V$ such that $Q(a) = 1$. Then $B(\pi\sigma_a) = B(\pi) \oplus Ka$ and $\dim\big(B(\pi\sigma_a)/\operatorname{rad} B(\pi\sigma_a)\big) \geq 1$; *cf.* 1.1. Using the previous case or Corollary 3a) we conclude that $\pi\sigma_a$ is a product of $\dim B(\pi\sigma_a)$ 1-symmetries. Hence we obtain

(ii) If $\varkappa \neq K^{*2}$ then π is a product of $\dim B(\pi) + 2$ 1-symmetries and not a product of less than $\dim B(\pi) + 2$ 1-symmetries.

The last statement follows from (i) and since every symmetry σ has $\det \sigma = -1$.

Now let $B(\pi)$ be totally isotropic. Then $2 \leq \dim B(\pi) < n$. Choose some $a \in V$ such that $Q(a) = 1$. Then $B(\pi\sigma_a) = B(\pi) \oplus Ka$, $\dim\big(B(\pi\sigma_a)/\operatorname{rad} B(\pi\sigma_a)\big) = 1$ and $d\big(B(\pi\sigma_a)/\operatorname{rad} B(\pi\sigma_a)\big) = Q(a)K^{*2} = K^{*2}$. Using (i) we obtain the assertion.

3.7 . Having in mind $K = \mathrm{GF}\,3$ where our previous arguments do not apply we include the following proposition.

PROPOSITION. *Let $u \leq 2$ and let $\mathfrak{S} \subset O(V)$ be the set of 1-symmetries.*

a) Let $n \geq 5$ and σ_a, σ_b distinct symmetries such that $\sigma_a\sigma_b \in$ kernel Θ. *Then $\sigma_a \cdot \sigma_b$ is a product of four elements of $\mathfrak{S}$.*

b) Let $u \leq 2$ and $K \neq$ GF 3 *or $n \geq 5$. Then* kernel Θ *is generated by $\mathfrak{S}$.*

PROOF. a) Let $T := Ka + Kb$. If T is regular choose $c \in T$ such that $Q(c) = 1$. Then $\dim B(\sigma_a\sigma_b\sigma_c) = 1$ and $\Theta(\sigma_a\sigma_b\sigma_c) = K^{*2}$, hence $\sigma_a\sigma_b\sigma_c \in \mathfrak{S}$ and $\sigma_a\sigma_b \in \mathfrak{S}\cdot\mathfrak{S}$. If T is singular then $\dim T^{\perp} = n - 2$ and $\dim(\operatorname{rad} T^{\perp}) = \dim(\operatorname{rad} T) = 1$. Hence $T^{\perp}$ contains a 2-dimensional regular subspace D, and we can choose some anisotropic $d \in D$ such that $Q(d) = Q(a)$. Then $Ka + Kd$ and $Kd + Kb$ are regular. Hence $\sigma_a\sigma_d, \sigma_d\sigma_b \in \mathfrak{S}\cdot\mathfrak{S}$ by the previous case and finally $\sigma_a \cdot \sigma_b = \sigma_a\sigma_d\sigma_d\sigma_b \in \mathfrak{S}\cdot\mathfrak{S}\cdot\mathfrak{S}\cdot\mathfrak{S}$.

b) By Corollary 3 we can assume that $K = \mathrm{GF}\,3$ and $n \geq 5$. Every $\pi \in$ kernel Θ is a product of 1-symmetries and -1-symmetries where the number of -1-symmetries is even; *cf.* 1.(4). Hence a) yields the assertion.

4. **The symplectic case.**

4.1 *A brief look at E. T. Wall's bilinear form.* As in 1. let G be an orthogonal group $O(V)$ or a symplectic group $\mathrm{Sp}(V)$ given by the regular form f. Every $\pi \in G$ supplies a bilinear form

$$f_\pi: B(\pi) \times B(\pi) \longrightarrow K, \quad f_\pi\big(v(\pi - 1), b\big) := -f(v, b)$$

where $v \in V$ and $b \in B(\pi)$; *cf.* [4]. Wall's form f_π is regular (but usually not symmetric). We write $M \perp_\pi N$ when $M, N \subset B(\pi)$ and $f_\pi(m, n) = 0$ for every $m \in M$ and $n \in N$. Let $d(\pi)$ denote the discriminant of f_π. The mapping $Q_\pi: B(\pi) \longrightarrow K$, $b \longmapsto f_\pi(b, b)$ is a quadratic form and the associated symmetric bilinear form is $g_\pi: B(\pi) \times B(\pi) \longrightarrow K$, $g_\pi(a, b) := \frac{1}{2}[Q_\pi(a+b) - Q_\pi(a) - Q_\pi(b)]$. It is easy to verify that elements π, φ of G are conjugate if and only if their forms f_π and f_φ are equivalent, *i.e.* there is a linear bijection $\omega: B(\pi) \longrightarrow B(\varphi)$ such that $f_\pi(a, b) = f_\varphi(a\omega, b\omega)$ holds for all $a, b \in B(\pi)$. This yields

(2) If $\pi^\gamma = \varphi$ then $d(\pi) = d(\varphi)$ for all $\pi, \varphi, \gamma \in G$, and

(2′) Suppose that $\pi, \varphi \in G$ are simple. Then $\pi^\gamma = \varphi$ for some $\gamma \in G$ if and only if $d(\pi) = d(\varphi)$.

If G is orthogonal and σ_a denotes the symmetry with $B(\sigma_a) = Ka$ then $d(\sigma_a) = Q_\sigma(a, a) = 2Q(a)K^{*2}$ where $Q(a) := f(a, a)$. If G is symplectic and $\tau_{\mu,w}$ is a transvection then $d(\tau_{\mu,w}) = Q_\tau(w, w)K^{*2} = -\mu K^{*2}$ and $d(\tau_{\mu,w}^{-1}) = \mu K^{*2}$.

In the sequel we shall consider a symplectic group $\mathrm{Sp}(V) = \mathrm{Sp}(V, f)$.

Let $\pi \in \mathrm{Sp}(V)$ and $a, b = v(\pi - 1) \in B(\pi)$. Then $2g_\pi(a, b) = -f\big(a(\pi + 1), v\pi\big)$. Hence we obtain

$$\text{(3)} \qquad \mathrm{rad}\big(B(\pi), Q_\pi\big) := \mathrm{rad}\big(B(\pi), g_\pi\big) = N(\pi).$$

We shall repeatedly use the following lemma.

LEMMA 4.1.1. *Let $\varphi \in \mathrm{Sp}(V)$ and τ a transvection. The following statements are equivalent.*

(i) $\dim F(\varphi\tau) = \dim F(\varphi) + 1$.

(ii) $B(\tau) \not\subset B(\varphi\tau)$;

(iii) $B(\varphi) = B(\tau) \oplus B(\varphi\tau)$;

(iv) There is some $z \in B(\varphi)$ such that $\tau = \tau_{\mu,z}$ where $\mu := Q_\varphi(z)^{-1}$.

If these conditions hold then the following properties are true.

(j) $B(\tau) \perp_\varphi B(\varphi\tau)$;

(jj) $f_\varphi|_{B(\tau)} = -f_\tau$ *and* $f_\varphi|_{B(\varphi\tau)} = f_{\varphi\tau}$;

(jjj) $d(\varphi) = -d(\tau) \cdot d(\varphi\tau)$.

PROOF. The equivalence of (i), (ii) and (iii) is part of 1.1. If (i) is valid then $v(\varphi - 1) = z$ and $v \in F(\varphi\tau) \backslash F(\varphi)$ for some v, hence (i) $\Rightarrow$ (iv). Conversely, a short computation shows (iv) $\Rightarrow$ (i). Statements (j) and (jj) follow almost immediately from the definitions; (j) and (jj) entail (jjj).

COROLLARY 4.1.2. *Let $\pi \in \mathrm{Sp}(V)$ and τ a transvection such that $B(\pi\tau) = B(\tau) \oplus B(\pi)$. Then $d(\pi\tau) = d(\tau) \cdot d(\pi)$.*

PROOF. 4.1.1(jjj) implies that $d(\pi\tau) = -d(\tau^{-1}) \cdot d(\pi\tau\tau^{-1}) = d(\tau) \cdot d(\pi)$.

https://doi.org/10.4153/CMB-1992-053-5 Published online by Cambridge University Press

COROLLARY 4.1.3. *If* $\tau_1, \ldots, \tau_k$ *are* $\lambda_1, \ldots, \lambda_k$*-transvections such that* $\pi := \tau_1 \cdot \cdots \cdot \tau_k$ *and* $k \leq \dim B(\pi)$ *[hence* $k = \dim B(\pi)$ *and* $B(\pi) = B(\tau_1) \oplus \cdots \oplus B(\tau_k)$ *by 1.(2)] then*

$$d(\pi) = (-1)^k \lambda_1 \cdot \cdots \cdot \lambda_k \cdot K^{*2}.$$

In [2] a mapping called ρ is used. We want to mention that ρ is closely related to the discriminant mapping of Wall's bilinear form:

DEFINITION/COROLLARY 4.1.4. *Given some* $\lambda \in K^*$. *For* $\pi \in \mathrm{Sp}(V)$ *we define* $\rho(\pi) := (-\lambda)^{\dim B(\pi)} \cdot d(\pi)$. *Then* $\rho(\tau_{\mu,w}) = \lambda\mu K^{*2}$; *hence* $\tau_{\mu,w}$ *is a* λ*-transvection if and only if* $\rho(\tau_{\mu,w}) = K^{*2}$. *If* $\pi \in \mathrm{Sp}(V)$ *is a product of* $\dim B(\pi)$ λ*-transvections then* $\rho(\pi) = K^{*2}$.

4.2 . Let $\pi \in \mathrm{Sp}(V)$ and $z \in B(\pi) \backslash B(-\pi)$ such that $Q_\pi(z) \neq 0$. Let $\lambda := Q_\pi(z)^{-1}$ and $\tau := \tau_{\lambda,z}$. Then $B(\pi) = B(\tau) \oplus B(\pi\tau)$ and $\dim F(\pi\tau) = \dim F(\pi) + 1$ and $\dim N(\pi\tau) = \dim N(\pi) - 1$; hence $N(\pi\tau) = B(\pi\tau) \cap N(\pi)$ and $L(\pi\tau) = L(\pi)$.

PROOF. This is immediate from 4.1.1 since $N(\pi\tau) = F(-\pi\tau)$.

4.3 . Let $K \neq \mathrm{GF}\,3$, $\pi \in \mathrm{Sp}(V)$ such that $N(\pi) \neq 0$ and $\lambda \in L(\pi) := \{Q_\pi(z) \mid z \in B(\pi)\} \setminus \{0\}$ (clearly $\dim B(\pi)/N(\pi) \geq u$ implies that $L(\pi) = K^*$; *cf.* 4.1(3)). There is a λ-transvection τ such that $\dim F(\pi\tau) = \dim F(\pi) + 1$ and $\dim N(\pi\tau) = \dim N(\pi) - 1$ and $L(\pi\tau) = L(\pi)$.

PROOF. $B(\pi^2) = B(\pi) \cap B(-\pi)$ is a proper subspace of $B(\pi)$. Hence $B(\pi) = A \oplus N(\pi)$ and $A \not\subset B(\pi^2)$ for some subspace A. Then A is regular with respect to the quadratic form Q_π; *cf.* 4.1(3). We have $N(\pi) = \mathrm{rad}\big(B(\pi), g_\pi\big)$; *cf.* 4.1(3). Hence $Q_\pi(z) = \lambda$ for some $z \in A$. By 3.1 A has a basis whose vectors c fulfill $Q_\pi(c)^{-1} = \lambda$. Clearly, $a \in B(\pi) \backslash B(\pi^2)$ holds for at least one of them. Finally, 4.2 shows that $\tau := \tau_{\lambda,a}$ meets the requirements.

4.4 . Let $\pi \in \mathrm{Sp}(V)$ and $\tau = \tau_{\mu,z}$ such that $N(\pi) = 0$ and $\dim F(\pi\tau) = \dim F(\pi) + 1$. Then $N(\pi\tau) = 0$ if and only if $Q_\pi\big(z(\pi + 1)^{-1}\big) \neq 0$.

PROOF. We have $\mu^{-1} = Q_\pi(z) = -f(w, w\pi)$ where $z = w(\pi - 1)$; *cf.* 4.1.1. Let $d := w(\pi + 1)^{-1}$. If $N(\pi\tau) \neq O$ is true then $\mu \cdot f\big(d(\pi - 1), d(\pi - 1)\pi\big) = 1$. This entails $f\big(d(\pi - 1), d(\pi - 1)\pi\big) = -f\big(d(\pi + 1), d(\pi + 1)\pi\big)$. We conclude that $0 = f(d, d\pi) = -Q_\pi\big(z(\pi + 1)^{-1}\big)$. If conversely $Q_\pi\big(z(\pi + 1)^{-1}\big) = 0$ holds then $d(\pi - 1) = z(\pi + 1)^{-1} \in N(\pi\tau)$.

4.5 . Theorem 2 holds under the additional assumption that $N(\pi) = 0$ and $m := \dim B(\pi) - u + 1 \leq 2$.

PROOF. We can assume that $m \geq 1$, hence $m \in \{1, 2\}$; *cf.* 1.4′.

Let $m = 1$ and $\lambda_1 \in K^*$. Then $\dim B(\pi) = u$. Choose $c \in B(\pi)$ with $Q_\pi(c) = -\lambda_1^{-1}$. Let $\tau_1 := \tau_{-\lambda_1,c}$ and $\varphi := \pi\tau_1$. Then $\dim B(\pi) = \dim B(\varphi) \oplus B(\tau_1)$ and τ_1^{-1} is a λ_1-transvection; *cf.* 4.1.1. If $\dim B(\varphi) = 1$ then φ is a transvection. Else $\dim B(\varphi) >$

https://doi.org/10.4153/CMB-1992-053-5 Published online by Cambridge University Press

$\frac{1}{2}\dim B(\pi)$, hence $B(\varphi)$ is not totally isotropic with respect to Q_π. This means that $\varphi^2 \neq 1$. In both cases φ is a product of $\dim B(\varphi)$ transvections; *cf.* 1.(4′).

Now let $m = 2$ and $\lambda_1, \lambda_2 \in K^*$. We claim that

$$(*) \qquad Q_\pi\big(b(\pi+1)^{-1}\big) \neq 0 \text{ and } Q_\pi(b) = -\lambda_1^{-1} \text{ for some } b \in B(\pi).$$

Replacing λ_1 by $-\lambda_1^{-1}$, Q by Q_π and $\pi - 1$ by $\pi + 1$ in the proof of $(*)$ in 3.2 we obtain a proof of the present statement $(*)$. Indeed $(*)$ yields the assertion: Let $\tau_1 := \tau_{-\lambda_1,b}$. Then $\varphi := \pi\tau_1$ satisfies $B(\pi) = B(\tau_1) \oplus B(\varphi)$ and $N(\varphi) = 0$; *cf.* 4.1.1 and 4.4. Furthermore, τ_1^{-1} is a λ_1-transvection. The previous case $m = 1$ supplies transvections $\tau_2, \ldots, \tau_{\dim B(\pi)}$ such that $\varphi = \tau_2, \ldots, \tau_{\dim B(\pi)}$ and τ_2 is a λ_2-transvection. The assertion follows.

4.6 *Proof of Proposition 2.* The proof is a consequence 4.3. To carry out the details replace in the proof of Proposition 1 Q by Q_π and $\operatorname{rad} B(\pi)$ by $N(\pi)$ and symmetries by transvections.

4.7 *Proof of Theorems 3 and 4.* As in 3.5 it suffices to prove Theorem 3. If $m \leq 0$ then 1.(4′) yields the assertion. So we assume that $m \geq 1$. We proceed by induction on $\dim B(\pi)$. If $\dim B(\pi) = 1$ then $u = 1$ and $m = 1$; hence $K^{*2} = K^*$ and π is a transvection. Clearly the assertion holds in this case.

Let $\dim B(\pi) \geq 2$.

CASE I. $N(\pi) = 0$. If $m \leq 2$ then 4.5 applies. Now let $m \geq 3$, *i.e.* $\dim B(\pi) \geq u + 2$. Take an arbitrary vector $a \in B(\pi)$ with $Q_\pi(a) = -\lambda_1^{-1}$; this is possible since $\dim B(\pi) \geq u$ and $B(\pi)$ is regular with respect to Q_π. Then $\tau_1 := \tau_{-\lambda_1,a}$ fulfills $B(\pi) = B(\pi\tau_1) \oplus B(\tau_1)$ and $\dim N(\pi\tau_1) \leq 1$. Furthermore, τ_1^{-1} is a λ_1-transvection. Thus $\dim B(\pi\tau_1)/N(\pi\tau_1) \geq \dim B(\pi) - 2 \geq u$. Hence $\pi\tau_1$ meets the requirements of the Theorem and the induction hypothesis applies.

CASE II. $N(\pi) \neq 0$. 4.3 supplies a $-\lambda_1$-transvection τ_1 such that $B(\pi) = B(\pi\tau_1) \oplus B(\tau_1)$ and $\dim N(\pi\tau_1) = \dim N(\pi) - 1$. Then $\dim B(\pi\tau_1)/N(\pi\tau_1) = \dim B(\pi)/N(\pi) \geq u$ and τ_1^{-1} is a λ_1-transvection. The assertion follows by induction.

4.8 *Proof of Corollaries 4 and 5.*

LEMMA 4.8.1. *Let $l \geq u$, $\tau \in \mathrm{Sp}(V)$ a transvection and $\lambda_1, \ldots, \lambda_l \in K^*$. Then $\tau = \tau_1 \cdot \cdots \cdot \tau_l$ where τ_i is a λ_i-transvection and $B(\tau_i) = B(\tau)$, or $\tau_i = 1$, for each i.*

PROOF. Let $\tau = \tau_{\mu,z}$. By assumption, $\mu = \lambda_1\delta_1 + \cdots + \lambda_1\delta_1$ for suitable squares $\delta_i \in K^2$. Let $\tau_i := \tau_{\lambda_i\delta_i,z}$ if $\delta_i \neq 0$, else $\tau_i := 1$.

Corollary 4 follows immediately from Theorem 2, 1.(2) and 4.1.3. Statement a) in Corollary 5 is a special case of Corollary 4.

Corollary 5b) and c) will follow from the following statements (i), (ii) and (iii). Let $u \leq 2$, $K \neq \mathrm{GF}\,3$, $\pi \in \mathrm{Sp}(V)$ and $\lambda \in K^*$. Let $k := \dim B(\pi)$. If $d(\pi) \neq (-\lambda)^k K^{*2}$ then 4.1.3 entails that π is not a product of less than $k + 1$ λ-transvections.

First let us assume that $\dim B(\pi)/N(\pi) = 1$.

Due to 4.1(3) each $z \in B(\pi)\backslash N(\pi)$ yields the same value $\varkappa := Q_\pi(z)K^{*2}$.

By 1.(4′) π is a product of k transvections; each factor $\tau = \tau_{\mu,z}$ in such a product satisfies $-\mu K^{*2} = -d(\tau^{-1}) = -Q_{\tau^{-1}}(z)K^{*2} = Q_\pi(z) \cdot K^{*2} = \varkappa$; *cf.* 1.(2) and 4.1.1(jj). Furthermore, 4.1.3 yields that $d(\pi) = \varkappa^k$. We conclude:

(i) Let $\dim B(\pi)/N(\pi) = 1$. Then π is a product of k λ-transvections if and only if $\lambda K^{*2} = -\varkappa$.

Now let $\pi \in \mathrm{Sp}(V)$ and $\pi^2 \neq 1$. Using 1.(4′) we obtain a product φ of $k-1$ transvections and a transvection τ such that $\pi = \varphi \cdot \tau$. By 4.8.1 we have $\tau = \tau_1\tau_2$ where τ_1 is a λ-transvection with $B(\tau_1) = B(\tau)$ and τ_2 is a λ-transvection or $\tau_2 = 1$. Then $\varphi\tau_1$ is a product of k transvections. If $\dim B(\varphi\tau_1)/N(\varphi\tau_1) \geq 2$ then Corollary 5a) yields that $\varphi\tau_1$ is a product of k λ-transvections; hence π is a product of $k+1$ transvections. Else $\dim B(\varphi\tau_1)/N(\varphi\tau_1) = 1$ and $\varphi\tau_1$ is a product of k transvections such that one factor is a λ-transvection. Thus (i) yields that each factor is a λ-transvection. So π is a product of $k+1$ λ-transvections. Hence we proved

(ii) Let $\pi^2 \neq 1$. Then π is a product of at most $k+1$ λ-transvections.

(iii) Let $B(\pi) = N(\pi)$ and $\pi \neq 1$. Then π is a product of $k+1$ but not less than $k+1$ λ-transvections.

PROOF OF (iii). The not-less-statement follows from 1.(2) and 4.1.1(jj). If $\dim B(\pi) = 1$ then 4.8.1 yields the assertion. Let $\dim B(\pi) \geq 2$. An elementary argument shows: If τ is a transvection with $B(\tau) \subset B(\pi)$ then $B(\pi) = N(\pi) = B(\pi\tau) = N(\pi\tau) \oplus Kz$ for some $z \in V\backslash 0$. We can choose a $-\lambda$-transvection τ such that $B(\tau) \subset B(\pi)$. Then $Q_{\pi\tau}(z)K^{*2} = -\lambda K^{*2}$ by a simple calculation. In (i) we ascertained that $\pi\tau$ is a product of k λ-transvections. This completes the proof.

REFERENCES

1. E. W. Ellers and J. Malzan, *Products of Reflections in the Kernel of the Spinorial Norm*, Geom. Ded. **36**(1990), 279–285.

2. ———, *Products of λ-Transvections in* Sp(2n, q), Linear Algebra and Appl. **146**(1991), 121–132.

3. J. Hahn and O. T. O'Meara, *The Classical Groups and K-Theory*, Springer, 1989.

4. G. E. Wall, *On the Conjugacy Classes in the Unitary, Symplectic and Orthogonal Groups*, J. Austral. Math. Soc. **III**(1963), 1–62.

Mathematisches Seminar
Universität Kiel
Olshausenstraße 40
23 Kiel
Germany