PRODUCTS OF STRICTLY HYPERBOLIC CONJUGACY CLASSES IN SYMPLECTIC GROUPS

KLAUS NIELSEN

Abstract. We call a conjugacy class of the symplectic group $\mathrm{Sp}(2n, K)$ over a field K strictly hyperbolic if its minimal polynomial is of the form $q(x)q^*(x)$, where the polynomial $q(x)$ is prime to its reciprocal $q^*(x) := x^n q(x^{-1})$. It is shown that the product of 2 cyclic, strictly hyperbolic conjugacy classes of $\mathrm{Sp}(2n, K)$ contains all nonscalar elements of $\mathrm{Sp}(2n, K)$. It follows that the projective symplectic group has a conjugacy class of covering number 2, i.e. $\mathrm{PSp}(2n, K) = \Omega^2$ for some conjugacy class Ω of $\mathrm{PSp}(2n, K)$. This verifies a conjecture of J. G. Thompson in the special case of a (finite) projective symplectic group.

1. Introduction

There is a conjecture, usally attributed to J. G. Thompson, that a finite simple nonabelian group G has a conjugacy class Ω of covering number 2; i.e $G = \Omega^2$. Thompson's conjecture has been verified for several groups, e.g. for the alternating and the sporadic groups. For references.see [13] or [6]. Furthermore, it is known that the following simple groups have a conjugacy class of covering number 2:

(1) $\mathrm{PSL}(n, K)$ (Lev [12, Theorem 5] for $|K| \geq 4$, and [13, Theorem 3]) for all fields K
(2) $\mathrm{PSp}(2n, K)$ if $-1 \in K^2$,
(3) $\mathrm{PSU}(V, K, h)$ if $|K| > 9$ and h is hyperbolic (Bünger [1, Satz 4.1.19]).

A short proof for Lev's results in the case $K \neq \mathrm{GF}(2)$ or n odd was given in [2]. That $\mathrm{PSp}(2n, K)$ has a conjugacy class of covering number 2 if $-1 \in K^2$, is a trivial consequence of a theorem of Wonenburger. She showed that a symplectic transformation is the product of 2 skew-symplectic involutions [17, Theorem 2]. Hence if$-1 \in K^2$, then a symplectic transformation the product of 2 symplectic skew-involutions.

A great breakthrough was made in 1998 by Ellers and Gordeev [6], who proved the Thompson conjecture for all simple groups of Lie type over a field with more than 8 elements.

Almost 30 years ago, I proved that the projective symplectic group $\mathrm{PSp}(2n, K)$ has a conjugacy class of covering number 2 provided that $2n \geq 4$. But I lost interest in the subject, after Ellers and Gordeev had published their result.

Recently, Larsen and Tiep [10] showed that Thompson's conjecture holds for almost all finite simple groups. So there seems to be still some interest in Thompson's conjecture.

Date: November 15, 2024.

2020 *Mathematics Subject Classification.* 15A15, 15F10.

Key words and phrases. symplectic group, conjugacy classes.

Theorem 1.1. *Let $2n \geq 4$. Let Ω_1, Ω_2 be cyclic, strictly hyperbolic conjugacy classes of* $\mathrm{Sp}(2n, K)$.

(1) *If $K = \mathrm{GF}(3)$ or $2n \geq 6$ or Ω_1 and Ω_2 are triangularizable, then $\Omega_1\Omega_2$ contains all nonscalar elements of* $\mathrm{Sp}(2n, K)$.
(2) *If $2n = 4$, then $\Omega_1\Omega_2$ contains all elements M of $\mathrm{Sp}(2n, K)$ with $M^2 \neq \mathrm{I}_4$.*

Corollary 1.2. *Let $2n \geq 4$, and let $2n \geq 6$ if $K = \mathrm{GF}(2)$. Then $\mathrm{Sp}(2n, K) = \Omega^2 \cup -\mathrm{I}_{2n}$ for some cyclic, strictly hyperbolic conjugacy class of* $\mathrm{Sp}(2n, K)$.

Proof. By 1.1, it suffices to show that there exists a monic polynomial $q \in K[x]$ of degree n such that q is prime to its reciprocal. If $|K| \geq 4$, let $q(x) = (x - \lambda)^n$, where $\lambda \neq 0, \pm 1$. If $K = \mathrm{GF}(3)$ and $n = 2m$ is even let $q(x) = (x^2 - x - 1)^m$. If $K = \mathrm{GF}(3)$ and $n = 2m + 3$ is odd let $q(x) = (x^2 - x - 1)^m(x^3 - x - 1)$. If $K = \mathrm{GF}(2)$ let $q(x) = x^n + x^{m+1} + 1$, where $m = \lfloor \frac{n}{2} \rfloor$. $\square$

For the proof of 1.1, we prove 2 auxilary results. Let $\mathrm{Sp}(2n, K)$ denote the standard symplectic group, the set of all automorphs of the matrix

$$G = \begin{pmatrix} 0 & \mathrm{I}_n \\ -\mathrm{I}_n & 0 \end{pmatrix};$$

i.e. $P \in \mathrm{Sp}(2n, K)$ if $PGP' = G$, where P' denotes the transpose of P.

Let Ω be conjugacy of $\mathrm{Sp}(2n, K)$. By $\mathrm{PC}(\Omega)$ we denote the set of all matrices $A \in \mathrm{M}(n, K)$ occuring as the upper principle corner of some

$$P = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Omega.$$

It is an interesting open problem to determine $\mathrm{PC}(\Omega)$. In the general linear group the analogue problem is completely solved by the interlacing theorem of R.C. Thompson [16, Theorem 6] and E. M. de Sá [3, Theorem 5.4]:

Proposition 1.3. *Let $A \in \mathrm{M}(p, K), P \in \mathrm{M}(p + q, K)$ with invariant factors $i_k(A)$ and $i_k(P)$. Then there exist matrices X, Y, Z such that*

$$P \sim \begin{pmatrix} A & X \\ Y & Z \end{pmatrix}.$$

if and only if $i_k(P) | i_k(A) | i_{k+2q}(P)$.

In the case of a conjugacy class of a hyperbolic unitary vector space, Bünger has shown that $\mathrm{PC}(\Omega)$ contains nonscalar matrix with determinant α provided that $\det \Omega = \alpha\overline{\alpha}^{-1}$.

For our purposes, it is sufficient to show

Lemma 1.4. *Let $2n \geq 4$, and let Ω be a nonscalar conjugacy of* $\mathrm{Sp}(2n, K)$.

(1) *Let $\mathrm{char}\, K = 2$. Then $\mathrm{PC}(\Omega)$ contains*
  (a) *the identity matrix I_n*
  (b) *a transvection or a diagonal matrix $\mathrm{I}_{n-2} \oplus [\epsilon, \epsilon^{-1}]$, where $\epsilon \neq 1$,*
  (c) *a diagonal matrix $\delta\mathrm{I}_1 \oplus \mathrm{I}_{n-1}$ or a matrix $Q \oplus \mathrm{I}_{n-2}$, where Q has minimal polynomial $x^2 + \delta$.*
(2) *Let $\mathrm{char}\, K \neq 2$, and assume that $i_2(\Omega) = x - 1$. Then $\mathrm{PC}(\Omega)$ contains*
(3) *a transvection and all diagonal matrices $\mathrm{I}_{n-1} \oplus \delta\mathrm{I}_1$.*
(4) *Let $\mathrm{char}\, K \neq 2$ and $i_2(\Omega) = 1$. Then $\mathrm{PC}(\Omega)$ contains a nonprimary matrix with prescribed determinant δ if*

(a) $2n \geq 6$ *or*
(b) Ω *is not involutory and* $K \neq \mathrm{GF}(3)$ *or*
(c) Ω *is not involutory and* $\delta \neq 1$.

We also need

Lemma 1.5. *Let* $n \geq 2$. *Let* Φ, Δ *be cyclic conjugacy classes of* $\mathrm{GL}(n, K)$. *Then* $\Phi\Delta$ *contains*

(1) *all nonprimary matrices* $M \in \mathrm{GL}(n, K)$ *with determinant* $\det \Phi\Delta$,
(2) *a transvection if* $\det \Phi\Delta = 1$ *and* $\Delta \neq \Phi^{-1}$.

This is a result of Bünger and the author [2, Theorem 4.2] and generalizes an earlier result of Lev [11, Lemma 5]. For the convenience of the reader, we provide a short proof.

Using 1.4 and 1.5, we can prove 1.1:

Proof of 1.1. Let Ω be a nonscalar conjugacy class of $\mathrm{Sp}(2n, K)$. Let $\mu(\Omega_1) = q_1 q_1^*, \mu(\Omega_2) = q_2 q_2^*$, where q_1 and q_2 are prime to their reciprocals. Then $\mathrm{PC}(\Omega)$ contains a matrix $A = A_1 A_2$, where A_1 and A_2 cyclic, and $\mu(A_1) = q_1, \mu(A_2) = q_2$. If $K = \mathrm{GF}(3)$, $2n = 4$, and Ω is involutory, then $\mathrm{PC}(\Omega)$ contains a skew-involution . Now

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

Now let

$$W = \begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

Then the Schur complement $D - CA^{-1}B$ of A in W is $A^+ = (A')^{-1} = A_1^+ A_2^+$. Hence

$$W = \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A_1 & 0 \\ CA_2^{-1} & A_1^+ \end{pmatrix} \begin{pmatrix} A_2 & A_1^{-1}B \\ 0 & A_1^+ \end{pmatrix} \in \Omega_1 \Omega_2.$$

□

In a similar way, one can deal with unitary and orthogonal groups. Bünger uses a theorem of Lev [12, Theorem 2] to prove his result [1, 1 Satz 4.1.19] in the unitary group $\mathrm{PSU}(V, K, h)$ of a hyperbolic hermitian form h. Therefore he has to assume that $|K| > 9$. To cover the remaining cases $K = \mathrm{GF}(4)$ and $K = \mathrm{GF}(9)$, one needs a new factorization for the genral linear group. We will prove such a theorem in a following paper.

2. Preliminaries

2.1. **Notations.**

For a linear mapping φ of V let $\mathrm{B}^j(\varphi)$ denote the image and $\mathrm{Fix}^j(\varphi)$ the kernel of $(\varphi - 1)^j$. The space $\mathrm{B}(\varphi) := \mathrm{B}^1(\varphi)$ is the path or residual space of φ. And $\mathrm{Fix}(\varphi) := \mathrm{Fix}^1(\varphi)$ is the fix space of φ. Further, let $\mathrm{Neg}^j(\varphi) = \mathrm{Fix}^j(-\varphi)$. The space $\mathrm{Neg}(\varphi) = \mathrm{Neg}^1(\varphi)$ is the negative space of φ.

By $\mu(\varphi)$ we denote the minimal polynomial of φ. Clearly, the spaces $\mathrm{B}^j(\varphi)$ and $\mathrm{Fix}^j(\varphi)$ are φ-invariant.

Remark 2.1. *Let* $\varphi \in \mathrm{Sp}(V)$.

(1) φ *is involutory if and only if* $\mathrm{B}(\varphi) = \mathrm{Neg}(\varphi)$;

(2) $\mathrm{B}^j(\varphi)^\perp = \mathrm{Fix}^j(\varphi)$;

Definition 2.1. *Let φ be a linear transfromation of V. A subspace T of V is called anti-invariant (w.r.t. φ) if $T \cap T\varphi = 0$. The minimal rank $\mathrm{mr}(\varphi)$ of a linear transformation φ is defined as $\mathrm{mr}(\varphi) := \min\{\mathrm{rank}(\varphi - \lambda); \lambda \in \overline{K}\}$, where $\overline{K}$ is an algebraic closure of K.*

We have $\mathrm{mr}(\varphi) = m$ if and only if $i_m(\varphi) = 1 \neq i_{m+1}(\varphi)$. It is known that φ has an anti-invariant subspace of dimension m if and only if $2m \leq \dim V$ and $\mathrm{mr}(\varphi) \geq m$. This follows e.g. immediately from 1.3.

Lemma 2.2. *Let $\varphi \in \mathrm{Sp}(V)$. If $\dim \mathrm{Fix}(\varphi) = n =: \frac{\dim V}{2}$, then φ has a totally degenerate anti-invariant subspace of dimension n.*

Proof. It is easy to see that an arbitrary subspace of dimension $\geq n$ has a totally degenerate complement. So if T is a totally degenerate complement of $\mathrm{Fix}(\varphi)$, then $T \cap \mathrm{B}(\varphi) = 0$. Hence $V = T \oplus T(1-\varphi) = T \oplus T\varphi$. □

2.2. **Products of symmetric matrices.**

Lemma 2.3. *Let $P \in \mathrm{M}(n, K)$ be cyclic. Then there exists a symmetric matrix S (with maximal Witt index) such that $P^S = P'$ is the transposed of P.*

Proof. See e.g. [15, §6] or [9, Theorem 66]. □

2.3. **The symplectic matrix group.**

Usually, we work basis-free, but sometimes it is more convenient to compute with matrices. A matrix P is an automorph of a matrix G if $PGP' = G$. By $\mathrm{Sp}(2n, K)$ we denote the standard symplectic group, the set of all automorphs of the skew-sum

$$G = [-\mathrm{I}_n \setminus \mathrm{I}_n] = \begin{pmatrix} 0 & \mathrm{I}_n \\ -\mathrm{I}_n & 0 \end{pmatrix},$$

of $-\mathrm{I}_n$ and I_n. Note that some authors and computer algebra systems like gap use the skew-sum of $-\mathrm{R}_n$ and R_n instead, where R_n denotes the reverse identiy matrix of $\mathrm{GL}(n, K)$.

Lemma 2.4. *Let Ω be a conjugacy class of $\mathrm{Sp}(2n, K)$. Let*

$$P = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Omega.$$

Then

(1) $A^X \in \mathrm{PC}(\Omega)$ *for all* $X \in \mathrm{GL}(n, K)$.
(2) $A + BS \in \mathrm{PC}(\Omega)$ *for all symmetric matrices* $S \in \mathrm{M}(n, K)$.
(3) $D \in \mathrm{PC}(\Omega)$.

Proof. Let

$$Y = \begin{pmatrix} X & 0 \\ 0 & X^+ \end{pmatrix}, G = \begin{pmatrix} 0 & \mathrm{I}_n \\ -\mathrm{I}_n & 0 \end{pmatrix}, T = \begin{pmatrix} \mathrm{I}_n & 0 \\ S & \mathrm{I}_n \end{pmatrix}.$$

Then

$$P^X = \begin{pmatrix} A^X & X^{-1}BX^+ \\ X'CX & D^{X^+} \end{pmatrix}, P^G = \begin{pmatrix} D & -C \\ -B & A \end{pmatrix},$$

$$P^T = \begin{pmatrix} A + BS & B \\ C + DS - SA - SBS & D - SB \end{pmatrix} \in \Omega.$$

□

Lemma 2.5. *Let*

$$P = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}(2p, K), Q = \begin{pmatrix} R & S \\ T & U \end{pmatrix} \in \mathrm{Sp}(2q, K).$$

Then the diagonal sum of P and Q

$$P \boxplus Q := \begin{pmatrix} A \oplus R & B \oplus S \\ C \oplus T & D \oplus U \end{pmatrix} \in \mathrm{Sp}(2p + 2q, K).$$

2.4. **Orthogonally indecomposable transformations.** The proof of lemma 1.4 demands a closer look at orthogonally indecomposable symplectic transformations.

According to Huppert [7, 1.7 Satz], an orthogonally indecomposable transformation of $\mathrm{Sp}(V)$ is either[1]

(1) bicyclic with elementary divisors $e_1 = e_2 = (x \pm 1)^m$ (type 1) or
(2) indecomposable as an element of $\mathrm{GL}(V)$ (type 2) or
(3) cyclic with minimal polynomial $(qq^*)^t$, where q is irreducible and prime to its reciprocal q^*, where $q^*(x) = q(0)^{-1}x^{\partial q}q(x^{-1})$ (type 3).

Definition 2.2. *Let $\varphi \in \mathrm{Sp}(V)$. We say that φ is hyperbolic if V is the direct sum of 2 totally degenerate φ-invariant subspaces.*

Definition 2.3. *Let $\varphi \in \mathrm{Sp}(V)$ orthogonally indecomposable of type 1. We say that φ is orthogonally indecomposable of type*

(1) *1o if* $\dim V \equiv 2 \mod 4$,
(2) *1e if* $\dim V \equiv 0 \mod 4$.

In [7, 2.3 Satz] and [7, 2.4 Satz], Huppert proved the following:

Proposition 2.6. *Let* $\operatorname{char} K \neq 2$. *Let $\varphi \in \mathrm{Sp}(V)$ be orthogonally indecomposable of type 1. Then* $\dim V \equiv 2 \mod 4$, *and φ is hyperbolic.*

Corollary 2.7. *Let* $\operatorname{char} K \neq 2$ *Let $\varphi \in \mathrm{Sp}(V)$ be orthogonally indecomposable of type 1 with minimal polynomial $(x+1)^{2m+1}$. Then φ has a symplectic square root with minimal polynomial $(x^2+1)^{2m+1}$.*

Lemma 2.8. *Let* $\operatorname{char} K = 2$. *Let $\varphi \in \mathrm{Sp}(V, f)$ be orthogonally indecomposable of type 1e. Then φ is hyperbolic.*

Proof. See Bünger [1, Satz 1.5.5]. We give a short proof:

Clearly, φ is hyperbolic if $\dim V = 4$. So let $\dim V \geq 8$. Obviously, φ is orthogonally indecomposable on $\mathrm{B}(\varphi)/\mathrm{Fix}(\varphi)$. By induction, $\mathrm{B}(\varphi)/\mathrm{Fix}(\varphi) = [\langle u\rangle_\varphi + \mathrm{Fix}(\varphi)]/\mathrm{Fix}(\varphi) \oplus [\langle w\rangle_\varphi + \mathrm{Fix}(\varphi)]/\mathrm{Fix}(\varphi)$, where $\langle u\rangle_\varphi$ and $\langle w\rangle_\varphi$ are totally degenerate.

Let $a \in \mathrm{Fix}^3(\varphi)$. Then $\langle a\rangle_\varphi$ is totally degenerate:

If $\dim V \geq 12$, then $\mathrm{Fix}^3(\varphi)$ is totally degenerate, if $\dim V = 8$, then $\langle a\rangle_\varphi$ is totally degenerate as φ is orthogonally indecomposable.

Let $u = x + x\varphi$. We compute $f_{i,j} := f((a+x)(1+\varphi)^i, (a+x)(1+\varphi)^j) = f(x(1+\varphi)^i, x(1+\varphi)^j) + f(x(1+\varphi)^i, a(1+\varphi)^j) + f(a(1+\varphi)^i, x(1+\varphi)^j)$, as $\langle a\rangle_\varphi$ is totally degenerate. Clearly, $f_{i,j} = 0$ if $i + j \geq 3$. Further $f_{0,2} = f_{1,1} = 0$. Finally, $f_{0,1} = f(x, x\varphi) + f(x, a\varphi) + f(a, x\varphi) = f(x, x\varphi) + f(x(1+\varphi)^2, a\varphi)$. Hence $\langle x + a\rangle_\varphi$ is totally degenerate for a suitable a, as $\mathrm{Fix}^3(\varphi) \not\subseteq [x(1+\varphi)^2]^\perp$. Similarly, there exist $z \in V - \mathrm{B}(\varphi), c \in \mathrm{Fix}^3(\varphi)$ such that $w = z + z\varphi$ and $\langle z + c\rangle_\varphi$ is totally degenerate. Obviously, $V = \langle x + a\rangle_\varphi \oplus \langle z + c\rangle_\varphi$. □

[1]Our type enumeration follows Huppert [7]. In [8] Huppert uses a different enumeration.

2.4.1. *Type 2, 3.*

Lemma 2.9. *Let $\varphi \in \mathrm{Sp}(V, f)$ be orthogonally indecomposable of type 2 or 3. Then in a suitable basis of V,*

$$\varphi = \begin{pmatrix} 0 & \epsilon \mathrm{I}_m \\ -\epsilon \mathrm{I}_m & D \end{pmatrix}, f = \begin{pmatrix} 0 & F \\ -F & 0 \end{pmatrix},$$

where $\epsilon = \pm 1$, D is indecomposable, and F and DF are symmetric.

Proof. It is well known that a linear transformation is the product of 2 involutions if and only if it is similar to its inverse. This is a result usually attributed to Wonenburger [17, Theorem 1] and Doković [4, Theorem 1]. The same authors have also shown that a symplectic transformation is the product of 2 skew-symplectic involutions, Wonenburger [17, Theorem 2] for $\operatorname{char} K \neq 2$ and Doković [5, Theorem 1] for $\operatorname{char} K = 2$. In fact, an involution $\rho \in \mathrm{GL}(V)$ inverting φ must be already be skew-symplectic: Let $V = \langle u \rangle_\varphi$, and put $w = u\rho$. Then $f(u\varphi^i\rho, w\varphi^j\rho) = f(w\varphi^{-i}, u\varphi^{-j}) = f(w\varphi^j, u\varphi^i) = -f(u\varphi^i, w\varphi^j)$.

So let $\varphi = \sigma\tau$ be the the product of 2 skew-symplectic involutions. If $\operatorname{char} K \neq 2$ or φ is not unipotent, then $\mathrm{Fix}(\sigma)$ and $\mathrm{Neg}(\sigma)$ are totally degenerate, and $\dim \mathrm{Fix}(\sigma) = \dim \mathrm{Neg}(\sigma) = n$.

Assume first that $\mathrm{Neg}(\varphi) = 0$ or $\operatorname{char} K \neq 2$. Replacing φ by $-\varphi$, we may assume that $\mathrm{Neg}(\varphi) = 0$. Then $V = \mathrm{Fix}(\tau) \oplus \mathrm{Fix}(\sigma)\tau$ or $V = \mathrm{Neg}(\sigma) \oplus \mathrm{Neg}(\sigma)\sigma$.

So let $\operatorname{char} K = 2$, and let φ be unipotent. Then $\varphi = \sigma\tau$ is the product of 2 involutions with $\dim \mathrm{Fix}(\sigma) = n + 1 = \dim \mathrm{Fix}(\tau) + 1$: φ is similar to

$$\tau = \begin{pmatrix} 0 & \mathrm{I}_m \\ \mathrm{I}_n & N \end{pmatrix} \varphi = \begin{pmatrix} \mathrm{I}_n & 0 \\ N & \mathrm{I}_n \end{pmatrix} \varphi = \begin{pmatrix} 0 & \mathrm{I}_m \\ \mathrm{I}_m & 0 \end{pmatrix},$$

where N is nilpotent and cyclic. Let S be a complement of $\mathrm{Fix}(\varphi)$ in $\mathrm{Fix}(\sigma)$ containing $\mathrm{B}(\sigma)$. Then S is totally degenerate, and $V = S \oplus S\tau$.

Hence in a suitable basis,

$$\sigma = \begin{pmatrix} \mathrm{I}_m & 0 \\ D & -\mathrm{I}_m \end{pmatrix}, \tau = \begin{pmatrix} 0 & \mathrm{I}_m \\ \mathrm{I}_m & 0 \end{pmatrix}, \varphi = \begin{pmatrix} 0 & \mathrm{I}_m \\ -\mathrm{I}_m & D \end{pmatrix},$$

$$f = \begin{pmatrix} 0 & F \\ -F' & 0 \end{pmatrix} = \begin{pmatrix} 0 & \mathrm{I}_m \\ -\mathrm{I}_m & D \end{pmatrix} \begin{pmatrix} 0 & F \\ -F' & 0 \end{pmatrix} \begin{pmatrix} 0 & -\mathrm{I}_m \\ \mathrm{I}_m & D' \end{pmatrix}$$
$$= \begin{pmatrix} 0 & F' \\ -F & DF' - FD' \end{pmatrix}.$$

□

2.4.2. *Type 1e.*

Following Kaplansky [9, p.80], we say that a symplectic transformation φ is alternate if $f(v\varphi, v) = 0$ for all $v \in V$. If $\operatorname{char} K \neq 2$, then all symplectic involutions are alternate.

Lemma 2.10. *Let $\varphi \in \mathrm{Sp}(V, f)$. Let $\varphi = \sigma\tau$ be the product of 2 alternate involutions σ, τ. If U is a φ-cyclic subspace of V, then $U\sigma, U\tau \leq U^\perp$.*

Proof. Let $U = \langle u \rangle_\varphi$. It suffices to show that $u\sigma \in U^\perp$. We have $f(u\sigma, u\varphi^{2j}) = f(u\sigma\varphi^{-j}, u\varphi^j) = f(u\varphi^j\sigma, u\varphi^j) = 0$ and $f(u\sigma, u\varphi^{2j+1}) = f(u\sigma\varphi^{-j}, u\varphi^{j+1}) = f(u\varphi^j\sigma, u\varphi^{j+1}) = f(u\varphi^j\sigma, u\varphi^j\sigma\tau) = 0$. □

Lemma 2.11. *Let* $\operatorname{char} K = 2$. *Let*

$$H = \begin{pmatrix} 0 & \mathrm{I}_t \\ \mathrm{I}_t & 0 \end{pmatrix}, M = \begin{pmatrix} N_t & 0 \\ 0 & N_t' \end{pmatrix}, P = \begin{pmatrix} 0 & H \\ H & M \end{pmatrix},$$

where N_t *is a cyclic nilpotent matrix. Then* $P \in \mathrm{Sp}(2n, K)$ *is orthogonally indecomposable of type 1e.*

Proof.

$$P = \begin{pmatrix} 0 & H \\ H & M \end{pmatrix} = \begin{pmatrix} 0 & H \\ H & 0 \end{pmatrix} \begin{pmatrix} \mathrm{I}_n & HM \\ 0 & \mathrm{I}_n \end{pmatrix}$$

is the product of 2 alternate involutions. Further, P is bicyclic with minimal polynomial $(x+1)^n$. Hence P must be orthogonally indecomposable of type 1: otherwise $\dim \operatorname{Fix}(T) = n$ by 2.10.

□

Corollary 2.12. *Let* $P \in \mathrm{Sp}(2n, K)$. *Then* P *is conjugate to a matrix*

$$P_1 := \begin{pmatrix} 0 & B \\ -B^{-1} & D \end{pmatrix},$$

where B *is symmetric, if and only if* P *has no elementary divisor* $(x \pm 1)^{2t+1}$ *of odd degree.*

Proof. It follows from 2.9 and 2.11 that P is conjugate to P_1 if P has no elementary divisor $(x \pm 1)^{2t+1}$ of odd degree. Conversely, P_1 is similar to a matrix

$$M_D := \begin{pmatrix} 0 & \mathrm{I}_n \\ -\mathrm{I}_n & D \end{pmatrix}.$$

If $D = X \oplus Y$, then M_D is similar to $M_X \oplus M_Y$. So we may assume that K is algebraicly closed and that D is cyclic with minimum polynomial $(x - \lambda)^n$. But then M_D is cyclic with minimum polynomial $(x^2 - \lambda x + 1)^n$. □

Remark 2.13. *The Dickson transform of a polynomial* $p(x) \in K[x]$ *of degree* m *is the polynomial* $p(x + x^{-1})x^n$. *It can be shown that the invariant divisors of* P_1 *are the Dickson transforms of the invariant divisors of* D. *We have just used this fact in the proofs of 2.12 and 2.9.*

2.4.3. *Type 1o.*

Lemma 2.14. *Let* $\operatorname{char} K \neq 2$. *Let* $\varphi \in \mathrm{Sp}(V)$ *be orthogonally indecomposable of type 1 with minimal polynomial* $(x + 1)^{2m+1}$. *Then* φ *is conjugate to a matrix*

$$\begin{pmatrix} -\mathrm{I}_n & B \\ C & -\mathrm{I}_n + CB \end{pmatrix} \in \mathrm{Sp}(2n, K),$$

where $\operatorname{rank} B = \operatorname{rank} C = n - 1$.

Proof. By 2.7, φ has a symplectic square root with minimal polynomial $(x^2 + 1)^{2m+1}$. Using 2.12, we see that φ is conjugate to a matrix

$$P = \begin{pmatrix} 0 & B \\ -B^{-1} & D \end{pmatrix} \begin{pmatrix} 0 & B \\ -B^{-1} & D \end{pmatrix} = \begin{pmatrix} -\mathrm{I}_n & BD \\ -DB^{-1} & D^2 - \mathrm{I}_n \end{pmatrix}.$$

As above, we observe that D must be cyclic and nilpotent. □

Lemma 2.15. *Let* $\operatorname{char} K = 2$. *Let* $\varphi \in \mathrm{GL}(W)$ *be cyclic with characteristic polynomial* $(x + 1)^{2m+1}$, *where* $m \geq 1$. *Let* $\varphi = \sigma\tau$ *be a product of two involutions. Then*

(1) $\dim \mathrm{Fix}(\sigma) = m+1 = \dim \mathrm{Fix}(\tau), \dim \mathrm{B}(\sigma) = m = \dim \mathrm{B}(\tau)$.
(2) $\mathrm{B}(\varphi) = \mathrm{B}(\sigma) \oplus \mathrm{B}(\tau)$, $\mathrm{Fix}(\varphi) = \mathrm{Fix}(\sigma) \cap \mathrm{Fix}(\tau)$.
(3) *If* $\mathrm{B}(\sigma) \cap \mathrm{Fix}(\varphi) = 0$, *then*
$V = \mathrm{Fix}(\tau) \oplus \mathrm{B}(\sigma)$, $\mathrm{B}(\sigma) \not\subseteq \mathrm{B}^2(\varphi)$, $\mathrm{Fix}(\varphi) \subseteq \mathrm{B}(\tau) \subseteq \mathrm{B}^2(\varphi)$.
(4) *Either* $\mathrm{B}(\varphi) = \mathrm{B}(\tau) \oplus \mathrm{B}(\tau)\varphi$ *or* $\mathrm{B}(\varphi) = \mathrm{B}(\sigma) \oplus \mathrm{B}(\sigma)\varphi$.
(5) *Either* $V = \mathrm{Fix}(\tau) \oplus \mathrm{B}(\sigma)$ *or* $V = \mathrm{Fix}(\sigma) \oplus \mathrm{B}(\tau)$.

Proof. 1 and 2 are clear. We prove 3: Suppose that $\mathrm{B}(\sigma) \cap \mathrm{Fix}(\varphi) = 0$. Then $\mathrm{Fix}(\sigma) = \mathrm{B}(\sigma) \oplus \mathrm{Fix}(\varphi) \subseteq \mathrm{B}(\varphi)$ and $\mathrm{B}^2(\varphi) \supseteq \mathrm{Fix}(\sigma)(1+\varphi) = \mathrm{B}(\tau)$. It follows that $\mathrm{B}(\sigma) \not\subseteq \mathrm{B}^2(\varphi)$. From $\varphi = \sigma\tau = \tau\sigma^\tau$ we deduce that $\mathrm{Fix}(\varphi) \subseteq \mathrm{B}(\tau)$. □

Lemma 2.16. *Let* $\mathrm{char}\, K = 2$. *Let* $\varphi \in \mathrm{Sp}(V)$ *be orthogonally indecomposable of type 1, and let* $\dim V = 2n \equiv 2 \mod 4$. *Let* $\varphi = \sigma\tau$ *be a product of two involutions* $\sigma, \tau \in \mathrm{Sp}(V)$. *Let* $V = U_1 \oplus U_2$, *where* U_1, U_2 *are* $\langle \sigma, \tau \rangle$*-invariant. Then*
(1) $\mathrm{B}(\varphi) = \mathrm{B}(\sigma) \oplus \mathrm{B}(\tau)$.
(2) $\mathrm{Fix}(\varphi) = [\mathrm{B}(\sigma) \cap \mathrm{Fix}(\tau)] \oplus [\mathrm{B}(\tau) \cap \mathrm{Fix}(\sigma)]$.
(3) (a) $U_1 = \mathrm{Fix}(\sigma_1) \oplus \mathrm{B}(\tau_1)$ *and* $U_2 = \mathrm{B}(\sigma_2) \oplus \mathrm{Fix}(\tau_2)$ *or*
(b) $U_1 = \mathrm{B}(\sigma_1) \oplus \mathrm{Fix}(\tau_1)$ *and* $U_2 = \mathrm{Fix}(\sigma_2) \oplus \mathrm{B}(\tau_2)$.
(4) *If* σ *and* τ *are alternate, then* U_1 *and* U_2 *are totally degenerate.*

Proof. 1: follows from 2.16(2).
2: We have $\mathrm{Fix}(\varphi) \not\subseteq \mathrm{B}(\sigma)$: Otherwise $\mathrm{Fix}(\sigma) \subseteq \mathrm{B}(\varphi)$, and by 1), $\mathrm{Fix}(\sigma) = \mathrm{Fix}(\sigma) \cap \mathrm{B}(\varphi) = \mathrm{B}(\sigma) \oplus [\mathrm{B}(\tau) \cap \mathrm{Fix}(\sigma)] = \mathrm{B}(\sigma)$, a contradiction. Similarily, $\mathrm{Fix}(\varphi) \not\subseteq \mathrm{B}(\tau)$.
3: follows from 2.
4: If σ and τ are alternate, then U_1 and U_2 are totally degenerate by 2.10.
□

Corollary 2.17. *Let* $\mathrm{char}\, K = 2$. $\varphi \in \mathrm{Sp}(V)$ *be orthogonally indecomposable of type 1, and let* $\dim V = 2n \equiv 2 \mod 4$. *Then* φ *is conjugate to a matrix*

$$\begin{pmatrix} \mathrm{I}_n & B \\ C & \mathrm{I}_n + CB \end{pmatrix} \in \mathrm{Sp}(2n, K),$$

where $\mathrm{rank}\, B = \mathrm{rank}\, C = n-1$.

Proof. We have a decomposition $V = S \oplus T$, with $\mathrm{B}(\sigma) \subseteq S \subseteq \mathrm{Fix}(\sigma)$ and $\mathrm{B}(\tau) \subseteq T \subseteq \mathrm{Fix}(\tau)$: Take $S = \mathrm{Fix}(\sigma_1) \oplus \mathrm{B}(\sigma_2), T = \mathrm{B}(\tau_1) \oplus \mathrm{Fix}(\tau_2)$ or $S = \mathrm{B}(\sigma_1) \oplus \mathrm{Fix}(\sigma_2), T = \mathrm{Fix}(\tau_1) \oplus \mathrm{B}(\tau_2)$. Then in a suitable basis

$$\sigma = \begin{pmatrix} \mathrm{I}_n & 0 \\ C & \mathrm{I}_n \end{pmatrix}, \tau = \begin{pmatrix} \mathrm{I}_n & B \\ 0 & \mathrm{I}_n \end{pmatrix}, \varphi = \begin{pmatrix} \mathrm{I}_n & B \\ C & \mathrm{I}_n + CB \end{pmatrix}.$$

□

Remark 2.18. *It can be shown that* φ *has a cyclic square root even if* $\mathrm{char}\, K = 2$; *see* [14, Corollary 3.7]. *So 2.17 follows also from 2.12.*

Corollary 2.19. *Let* $P \in \mathrm{Sp}(2n, K)$. *Then* P *is conjugate to a matrix*

$$\begin{pmatrix} \mathrm{I}_n & B \\ C & \mathrm{I}_n + CB \end{pmatrix}.$$

Proof. If P has no elementary divisor $(x \pm 1)^{2t+1}$ of odd degree, then using 2.12, we see that P is conjugate to

$$\begin{pmatrix} \mathrm{I}_n & 0 \\ -B^{-1} & \mathrm{I}_n \end{pmatrix} \begin{pmatrix} 0 & B \\ -B^{-1} & D \end{pmatrix} \begin{pmatrix} \mathrm{I}_n & 0 \\ B^{-1} & \mathrm{I}_n \end{pmatrix} = \begin{pmatrix} \mathrm{I}_n & B \\ (D - 2\mathrm{I}_n)B^{-1} & D - \mathrm{I}_n \end{pmatrix}.$$

□

3. Principal corners of a symplectic conjugacy class: Proof of 1.4

3.1. The case $\operatorname{char} K = 2$.

Lemma 3.1. *Let $\operatorname{char} K = 2$. Let $\delta \in K^*$. Let $\Omega \subseteq \mathrm{Sp}(4, K)$ be a nonscalar conjugacy class. Then $\mathrm{PC}(\Omega)$ contains*

1. *a transvection or a nonprimary with determinant one,*
2. *a matrix with characteristic polynomial $(x+1)(x+\delta)$ or $(x^2+\delta)$.*

Proof. It follows from 2.19 that Ω contains a matrix

$$\begin{pmatrix} \mathrm{I}_2 & B \\ C & \mathrm{I}_2 + CB \end{pmatrix}.$$

By 2.4, $\mathrm{PC}(\Omega)$ contains all matrices $\mathrm{I}_2 + BS$, where S is symmetric. If $\operatorname{rank} B = 1$ or B has discriminant 1, then $\mathrm{PC}(\Omega)$ contains a transvection:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

If B is alternating, then $\mathrm{PC}(\Omega)$ contains all traceless matrices:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \lambda & \mu \\ \mu & \nu \end{pmatrix} = \begin{pmatrix} 1+\mu & \nu \\ \lambda & 1+\mu \end{pmatrix}.$$

Clearly, $\mathrm{PC}(\Omega)$ contains all diagonal matrices if B is diagonal. □

Corollary 3.2. *Let $\operatorname{char} K = 2$. Let $\Omega \subseteq \mathrm{Sp}(2n, K)$ be a nonscalar conjugacy class. Let $\delta \in K^*$. Then $\mathrm{PC}(\Omega)$ contains*

1. *the identity matrix I_n,*
2. *a transvection or all diagonal matrices $\mathrm{I}_{n-2} \oplus D_2$,*
3. *a diagonal matrix $\delta\mathrm{I}_1 \oplus \mathrm{I}_{n-1}$ or a matrix $Q \oplus \mathrm{I}_{n-2}$, where Q has minimal polynomial $x^2+\delta$.*

3.2. The case $\operatorname{char} K \neq 2$.

Lemma 3.3. *Let $\operatorname{char} K \neq 2$. Let $\Omega \subseteq \mathrm{Sp}(4, K)$ be a nonscalar conjugacy class. Then $\mathrm{PC}(\Omega)$ contains*

1. *a transvection if $\imath_2(\Omega) = x - 1$,*
2. *all traceless matrices of $\mathrm{GL}(2, K)$ if Ω is involutory,*
3. *all diagonal matrices of $\mathrm{GL}(2, K)$ if Ω has no elementary divisor $x \pm 1$,*
4. *all nonscalar triangular matrices of $\mathrm{GL}(2, K)$ if Ω is not involutory and $\mu(\Omega) = (x-1)p(x)$, where $p(1) \neq 0$.*

Proof. We use 2.4 without further reference. If Ω consists of transvections, then Ω contains a matrix

$$\begin{pmatrix} \mathrm{I}_2 & B \\ 0 & \mathrm{I}_2 \end{pmatrix},$$

where rank $B = 1$. Then $\mathrm{PC}(\Omega)$ contains

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}.$$

Now let $\mathrm{mr}(\Omega) \geq 2$. By 2.2 and 2.12, Ω contains a matrix

$$\begin{pmatrix} 0 & B \\ -B^{+} & D \end{pmatrix}.$$

2: If Ω is involutory, then B is alternating, and $\mathrm{PC}(\Omega)$ contains all matrices BS, where $S \in \mathrm{GL}(2, K)$ is symmetric.
3: If Ω has no elementary divisor $x \pm 1$, then we can assume that B is symmetric. In this case, $\mathrm{PC}(\Omega)$ contains all diagonal matrices.
4: By 2.12, B be not symmetric. Furthermore, $B \neq -B'$: Otherwise,

$$\begin{pmatrix} 0 & B \\ -B^{+} & D \end{pmatrix} = \begin{pmatrix} B & 0 \\ 0 & B^{-1} \end{pmatrix} \begin{pmatrix} 0 & \mathrm{I}_2 \\ \mathrm{I}_2 & BD \end{pmatrix}$$

is the product of an alternating and a symmetric matrix. But then $\Omega = -\Omega$, a contradiction. Hence we can assume that B is (upper) triangular. In this case, $\mathrm{PC}(\Omega)$ contains all nonsingular (upper) triangular matrices. □

Lemma 3.4. *Let* $\mathrm{char}\, K \neq 2$, *and* $2n \geq 6$. *Let* $\Omega \subseteq \mathrm{Sp}(2n, K)$ *be a nonscalar conjugacy class of* $\mathrm{Sp}(2n, K)$. *Let* $\delta \in K^*$. *Then* $\mathrm{PC}(\Omega)$ *contains*

(1) I_n, *a transvection, and all dilatations if* Ω *consist of transvections,*
(2) *a nonprimary matrix with prescribed determinant if* $\mathrm{mr}(\Omega) \geq 2$.

Proof. a) First assume that Ω has no elementary divisor $(x \pm 1)^{2t+1}$ of odd degree Then $\mathrm{PC}(\Omega)$ contains all diagonal matrices.
b) Next assume that Ω is orthogonally indecomposable of type 1 with $\mu(\Omega) = (x - \epsilon)^n$. Then $\mathrm{PC}(\Omega)$ contains all diagonal matrices $D = \epsilon\mathrm{I}_1 \oplus D_2$
c) Let $\Omega = \epsilon\mathrm{I}_2 \perp \Psi$, where Ψ has no elementary divisor $(x \pm 1)^{2t+1}$ of odd degree. Again, $\mathrm{PC}(\Omega)$ contains all diagonal matrices $D = \epsilon\mathrm{I}_1 \oplus D_2$.

In any case, $\mathrm{PC}(\Omega)$ contains a nonprimary matrix with prescribed determinant. So we may assume that $2n = 6$ and $\Omega = \mathrm{I}_2 \perp \epsilon\mathrm{I}_2 \perp \Psi$.

i) If $\Psi = \mathrm{I}_2$, then $\epsilon = -1$ and $\mathrm{PC}(\Omega)$ contains all matrices with mimimal polynomial $(x - 1)(x^2 + \delta)$.
ii) If $\Psi = -\mathrm{I}_2$, then $\mathrm{PC}(\Omega)$ contains all matrices with mimimal polynomial $(x + \epsilon)(x^2 + \delta)$.
ii) Let $\Psi \neq \pm\mathrm{I}_2$.
   (a) If $\mu_\Psi(1) \neq 0$, then $\mathrm{PC}(\Omega)$ contains all matrices $\epsilon\mathrm{I}_1 \oplus U$, where U is upper triangular.
   (b) If $\epsilon = -1$ and $\mu_\Psi(-1) \neq 0$, then $\mathrm{PC}(\Omega)$ contains all matrices $\mathrm{I}_1 \oplus U$, where U is upper triangular.
   (c) If $\epsilon = 1$ and $\mu_\Psi(1) \neq 0$, then $\mathrm{PC}(\Omega)$ contains all matrices I_3, all dialatations and transvections.

□

4. Proof of theorem 1.1

Lemma 4.1. *Let $U \in \mathrm{GL}(m-1, K)$ is upper triangular. Then there exist polynomials $g_j(x)$ of degree $\leq m-j-1$ with nonvanishing constant term such that the matrix*

$$Y := \begin{pmatrix} 0 & U \\ y_0 & y \end{pmatrix},$$

where $y = (y_0, \ldots, y_{m-1})$, has characteristic polynomial

$$\chi(Y) = \det x\mathrm{I}_m - Y = t^m + \sum_{j=0}^{m-1} y_j g_j(x) x^j.$$

The polynomials $g_j(x)x^j$ are linearly independent.

Lemma 4.2. *Let $U_1 \in \mathrm{GL}(m, K), U_2 \in \mathrm{GL}(n-m, K)$ be upper triangular matrices. Let Φ be a cyclic similarity class of $\mathrm{GL}(n, K)$ with $\det \Phi = (-1)^{n+1} \det U_1 U_2$. Then there exists a matrix $Z \in \mathrm{M}(m, n-m, K)$ such that*

$$P_Z := \begin{pmatrix} 0 & \mathrm{I}_{n-1} \\ 1 & 0 \end{pmatrix} \begin{pmatrix} U_1 & Z \\ 0 & U_2 \end{pmatrix} \in \Phi.$$

Proof. Let $z = (z_{m-1}, \ldots, z_1)', \widetilde{z} = (z_{m+1}, \ldots . z_{n-1})$,

$$U_1 = \begin{pmatrix} u_1 & b \\ 0 & W_1 \end{pmatrix}, U_2 = \begin{pmatrix} u_2 & c \\ 0 & W_2 \end{pmatrix}, Z = \begin{pmatrix} z_m & y \\ z & 0 \end{pmatrix}.$$

Then

$$P_Z = \begin{pmatrix} 0 & \mathrm{I}_{n-1} \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u_1 & b & y_1 & y \\ 0 & W_1 & z & 0 \\ 0 & 0 & u_2 & c \\ 0 & 0 & 0 & W_2 \end{pmatrix} = \begin{pmatrix} 0 & W_1 & z & 0 \\ 0 & 0 & u_2 & c \\ 0 & 0 & 0 & W_2 \\ u_1 & b & z_m & \widetilde{z} \end{pmatrix}.$$

Clearly, P_Z is cyclic. Let

$$Y := \begin{pmatrix} 0 & W_2 \\ z_m & \widetilde{z} \end{pmatrix}.$$

We compute the characteristic polynomial $\chi(P_Z)$ of P_Z by Laplace expansion by the first m columns:

$$\chi(P_Z) = x^m \chi(Y) + \sum_{j=1}^{m-1} z_j f_j(x) x^j,$$

where the polynomials $f_j(x)$ are of degree $\leq m-j-1$ and independent of U_1 and U_2, and $f_j(0) \neq 0$. □

Lemma 4.3. *Let Φ, Δ be similarity classes of cyclic matrices in $\mathrm{GL}(n, K)$. Let $P_1 \in \mathrm{GL}(m, K), P_2 \in \mathrm{GL}(n-m, K)$ with $\det P_1 P_2 = \det \Phi\Delta$. Then there exists a matrix $C \in \mathrm{M}(m, n-m, K)$ such that*

$$\begin{pmatrix} P_1 & C \\ 0 & P_2 \end{pmatrix} \in \Delta\Phi.$$

Proof. We may assume that $P_1 = L_1 U_1$ and $P_2 = L_2 U_2$, where L_1, L_2 are lower and U_1, U_2 are upper triangular. By 4.2, there exists a matrix Z such that

$$\begin{pmatrix} 0 & \mathrm{I}_{n-1} \\ 1 & 0 \end{pmatrix} \begin{pmatrix} U_1 & Z \\ 0 & U_2 \end{pmatrix} \in \Delta.$$

Further, there exists a matrix X such that

$$\begin{pmatrix} L_1 & X \\ 0 & L_2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ \mathrm{I}_{n-1} & 0 \end{pmatrix} \in \Omega :$$

$$\begin{pmatrix} \mathrm{R}_m & 0 \\ 0 & \mathrm{R}_{n-m} \end{pmatrix} \begin{pmatrix} L_1 & X \\ 0 & L_2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ \mathrm{I}_{n-1} & 0 \end{pmatrix} \begin{pmatrix} \mathrm{R}_m & 0 \\ 0 & \mathrm{R}_{n-m} \end{pmatrix}$$

$$\begin{pmatrix} L_1^{\mathrm{R}_m} & \mathrm{R}_m X \mathrm{R}_{n-m} \\ 0 & L_2^{\mathrm{R}_{n-m}} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ \mathrm{I}_{n-1} & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 \\ \mathrm{I}_{n-1} & 0 \end{pmatrix} \begin{pmatrix} L_1^{\mathrm{R}_m} & \mathrm{R}_m X \mathrm{R}_{n-m} \\ 0 & L_2^{\mathrm{R}_{n-m}} \end{pmatrix}.$$

Hence $\Phi\Delta$ contains the matrix

$$\begin{pmatrix} P_1 & L_1 X + Z U_2 \\ 0 & P_2 \end{pmatrix} = \begin{pmatrix} L_1 & X \\ 0 & L_2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ \mathrm{I}_{n-1} & 0 \end{pmatrix} \begin{pmatrix} 0 & \mathrm{I}_{n-1} \\ 1 & 0 \end{pmatrix} \begin{pmatrix} U_1 & Z \\ 0 & U_2 \end{pmatrix}.$$

□

Example 4.4. *Let $n \geq 2$. If $K = \mathrm{GF}(2)$ let $n \geq 3$. Let Φ, Δ be cyclic similarity classes of* $\mathrm{GL}(n, K)$*.*

(1) *$\Phi\Delta$ contains all matrices $M = X \oplus \delta \mathrm{I}_1$ if $\det M = \det \Phi\Delta$ and δ is not an eigenvalue of X.*
(2) *If Φ is reducible, then $\Phi\Phi^{-1}$ contains a transvection.*

Proof. 1: Let $L \in \mathrm{GL}(n-1, K)$ be lower triangular, and let $U \in \mathrm{GL}(n-1, K)$ be upper triangular matrix. There exist matrices

$$A = \begin{pmatrix} a & \delta \\ L & 0 \end{pmatrix} \in \Phi, B = \begin{pmatrix} 0 & U \\ \epsilon & b \end{pmatrix} \in \Delta.$$

Then

$$\begin{pmatrix} \delta\epsilon & aU + \delta b \\ 0 & LU \end{pmatrix} \in \Phi\Delta.$$

2: There exist matrices $Q \in \mathrm{GL}(m, K), R \in \mathrm{GL}(n-m, K)$, and $N, M \in \mathrm{M}(m, n-m, K)$ such that $\operatorname{rank} N, \operatorname{rank} M, \operatorname{rank}(N - M) = 1$ and

$$X = \begin{pmatrix} Q & M \\ 0 & R \end{pmatrix}, Y = \begin{pmatrix} Q & N \\ 0 & R \end{pmatrix} \in \Phi.$$

Now

$$XY^{-1} = \begin{pmatrix} \mathrm{I}_m & (M-N)R^{-1} \\ 0 & \mathrm{I}_{n-m} \end{pmatrix}$$

is a transvection. □

Remark 4.5. *It can be shown that $\Phi\Phi^{-1}$ contains no transvection if Φ is irreducible.*

Lemma 4.6. *Let Φ, Δ be nonscalar similarity classes of* $\mathrm{M}(2, K)$*. Assume that Φ is not irreducible.*

(1) *$\operatorname{tr}(\Phi\Delta) = K - \{\alpha \operatorname{tr} \Delta\}$ if and only if $(\Phi - \alpha \mathrm{I}_2)^2 = 0$ and Δ is irreducible.*
(2) *$\operatorname{tr}(\Phi\Delta) = K$ if and only if Φ is not primary or Δ is not irreducible.*

Proof. Let $\mu(\Phi) = (x - \lambda)(x - \alpha)$, $\mu(\Delta) = x^2 - \gamma x - \delta$. Then

$$\begin{pmatrix} \alpha & 0 \\ \mu & \lambda \end{pmatrix} \begin{pmatrix} 0 & 1 \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} 0 & \alpha \\ \lambda\gamma & \lambda\delta + \mu \end{pmatrix} \in \Omega\Delta$$

if $\lambda \neq \alpha$ or $\mu \neq 0$. If $\lambda = \alpha$ and Ψ is irreducible, then $\operatorname{tr}(\Phi\Delta) = K - \{\alpha \operatorname{tr} \Delta\}$:

$$\begin{pmatrix} \alpha & \mu \\ 0 & \alpha \end{pmatrix} \begin{pmatrix} \delta - \epsilon & \rho \\ \nu & \epsilon \end{pmatrix} = \begin{pmatrix} \alpha(\delta - \epsilon) + \mu\nu & \alpha\rho + \mu\epsilon \\ \alpha\nu & \alpha\epsilon \end{pmatrix}.$$

□

Using the computer algebra system gap, we can show

Example 4.7. *Let Ω, Ψ be cyclic conjuagcy classes of $\mathrm{Sp}(4,5)$ with $\mu(\Omega) = (x^2 + 2)(x^2 - 2), \mu(\Psi) = (x-2)^2(x+2)^2$. Then $\Omega\Psi$ contains no involution.*

References

[1] F. Bünger. Involutionen als Erzeugende unitärer Gruppen. Dissertation Kiel 1997. 1, 3, 5

[2] F. Bünger, K. Nielsen. A matrix-decomposition theorem for $\mathrm{GL}_n(K)$. Lin. Alg. Appl. **298**: 39–50, 1999. 1, 3

[3] E. M. Sá. Imbedding conditions for λ-matrices. Lin. Alg. Appl. **24**: 33–50, 1979. 2

[4] D. Ž. Đoković. Product of two involutions. Arch. Math. **18**: 582–584, 1967. 6

[5] D. Ž. Doković, The product of two involutions in the unitary group of a hermitian form. Indiana Univ. Math. J. 21: 449–456, 1971. 6

[6] E. W. Ellers, N. Gordeev. On the conjectures of J. Thompson and O. Ore. TAMS **350**: 3657–3671, 1998. 1

[7] B. Huppert. Isometrien von Vektorräumen I. Arch. Math. **35**: 164–176, 1980. 5

[8] B. Huppert. Angewandte Lineare Algebra. deGruyter, Berlin, Heidelberg, New York 1990. 5

[9] I. Kaplansky, Linear Algebra and Geometry. Chelsea, 1974. 4, 6

[10] M. Larsen, P. Tiep. Character estimates for finite classical groups and the asymptotic Thompson Conjecture. https://doi.org/10.48550/arXiv.2403.09047, 2025 1

[11] A. Lev. Products of Cyclic Conjugacy Classes in the Groups PSL(n, F). Lin. Alg. Appl. **179**: 59–83, 1993. 3

[12] A. Lev. Products of Cyclic Similarity Classes in the Groups $\mathrm{GL}_n(F)$, Lin. Alg. Appl. **202**: 235–266, 1994. 1, 3

[13] A. Lev. Covering The Group $\mathrm{PSL}_n(F)$ by The Square of a Conjugacy Class. Comm. Algebra **27**: 1207–1253, 1999. 1

[14] Bireflectionality in special orthogonal groups. https://doi.org/10.48550/arXiv.2409.20088, 2024. 8

[15] K. Shoda. Über die mit einer Matrix vertauschbaren Matrizen. Math. Z. **29**: 696–712, 1929. 4

[16] R. C. Thompson. Interlacing inequalities for invariant factors. Lin. Alg. Appl. **24**: 1–31, 1979. 2

[17] M. J. Wonenburger. Transformations which are products of two involutions. J. Math. Mech. **16**: 327–338, 1966. 1, 6

Email address: `klaus@nielsen-kiel.de`