PRODUCTS OF SIMILAR MATRICES

DAVE WITTE

(Communicated by Ronald M. Solomon)

ABSTRACT. Let A and B be $n \times n$ matrices of determinant 1 over a field K, with $n > 2$ or $|K| > 3$. We show that if A is not a scalar matrix, then B is a product of matrices similar to A. Analogously, we conjecture that if a and b are elements of a semisimple algebraic group G over a field of characteristic zero, and if there is no normal subgroup of G containing a but not b, then b is a product of conjugates of a. The conjecture is verified for orthogonal groups and symplectic groups, and for all semisimple groups over local fields. Thus, in a connected, semisimple Lie group with finite center, the only conjugation-invariant subsemigroups are the normal subgroups.

1. INTRODUCTION

It is well known that the group $\mathrm{SL}_n(K)$ of $n \times n$ matrices of determinant 1 over a field K is simple, modulo the scalar matrices, if $n > 2$ or $|K| > 3$. More precisely, if $A \in \mathrm{SL}_n(K)$, and A is not a scalar matrix, then every element of $\mathrm{SL}_n(K)$ can be written as a product of matrices that are conjugate to either A or A^{-1}. We show that the inverse is superfluous:

3.3′. Theorem. *Let $A \in \mathrm{SL}_n(K)$, where K is a field, and assume that either $n > 2$ or $|K| > 3$. If A is not a scalar matrix, then every element of $\mathrm{SL}_n(K)$ is a product of matrices conjugate to A.*

This result is equivalent to the assertion that every conjugation-invariant subsemigroup of $\mathrm{SL}_n(K)$ is either central or all of $\mathrm{SL}_n(K)$, when $n > 2$ or $|K| > 3$ (see 2.2). In a group that is not simple, the normal subgroups provide obvious examples of conjugation-invariant subsemigroups. There is considerable literature on invariant subsemigroups of Lie groups (see [Nee] and [Hof] for background and references), but an analogue of the preceding result shows that these obvious examples are the only ones in the semisimple case.

4.5′. Corollary. *A connected, semisimple Lie group G has finite center iff every* (*not necessarily closed*) *conjugation-invariant subsemigroup of G is a normal subgroup.*

We conjecture that the same is true for semisimple algebraic groups over any field of characteristic 0. (The author does not have the expertise to speculate on algebraic groups over fields of characteristic p.)

1.1. Conjecture. If G is a semisimple algebraic group over a field K of characteristic zero, then every conjugation-invariant subsemigroup of G_K is a normal subgroup.

As evidence for this, we prove the conjecture if

1. K is an algebraically closed field (cf. 4.3); or
2. K is a local field (cf. 4.4); or
3. G is a special linear group over any field, not necessarily of characteristic zero (cf. 3.3); or
4. G is a (split) symplectic group over any field, not necessarily of characteristic zero (cf. 5.2); or
5. G is a special orthogonal group over any field, not necessarily of characteristic zero (cf. 6.4).

The assertion of the conjecture can be rephrased as the statement that G_K is not partially orderable (see 2.2). It is also relevant to the calculation of bounded cohomology (see 2.4).

Which arithmetic groups are partially orderable? Corollaries 2.5 and 2.6 show that an answer to this question might be used to enlarge the class of arithmetic groups that are known not to act on the circle (see [Wit]).

1.2. *Remark.* If G is a special linear group or symplectic group or special orthogonal group, our proofs show there is some $n = n(G)$ such that, for every $x \in G_K$, the identity element is a product of no more than n conjugates of x. This suggests that it may be possible to prove a quantitative version of the conjecture. Namely, for each $x \in G_K$, perhaps there is some $n \in \mathbb{Z}^+$ and some normal subgroup N containing x, such that every element of N is a product of no more than n conjugates of x. Can n be chosen independent of x?

1.3. *Example* ([GMR]). The conclusion of Conjecture 1.1 does not hold for general simple groups G, even if G is assumed to have torsion. Let $(X, <)$ be the countable universal poset and $G = \mathrm{Aut}(X, <)$. If g is any nonidentity element of G, then every element of G can be written as a product of at most 16 conjugates of alternately g and its inverse [GMR, Thm. 1'], so G is simple in a very strong sense. The group G also has torsion [GMR, Lem. 3.9]. However, G contains strongly embracing elements (that is, elements h that satisfy $x < xh$ for all $x \in X$) [GMR, Cor. 3.3], and products or conjugates of strongly embracing elements are again strongly embracing, so the conjugation-invariant subsemigroup generated by a strongly embracing element is **not** all of G.

2. PRELIMINARY REMARKS

Most of 2.1–2.3 can be found in [Fuc, Chap. II], which also contains much additional information. Proposition 2.2 shows that our main results can be reformulated in a variety of ways. The introduction focuses on versions (2) and (4), but version (5) is more convenient for the proofs in later sections.

2.1. Definition. A partial order (which is assumed to be antireflexive, antisymmetric, and transitive) on a group G is *invariant* if

$$\forall a, b, c \in G, \qquad a < b \Rightarrow (ac < bc \ \& \ ca < cb).$$

The empty relation (in which $\forall a, b \in G, \ a \not< b$) is the trivial example of an invariant partial order. We say that a group G is *partially orderable* if there exists a nontrivial invariant partial order on G.

2.2. Proposition. *Let G be a group. Then the following are equivalent:*

1. *The group G is not partially orderable.*
2. *Every conjugation-invariant subsemigroup of G is a (normal) subgroup.*
3. *Every conjugation-invariant subsemigroup of G contains the identity element e.*
4. *For every $x, y \in G$, either y is a product of conjugates of x, or there is a normal subgroup of G containing x but not y.*
5. *For every $x \in G$, there exists a sequence of elements $a_1, a_2, \ldots, a_n$ of G such that $x^{a_1} x^{a_2} \cdots x^{a_n} = e$.*

Proof. $(1 \Rightarrow 2)$ We prove the contrapositive. Let N be a conjugation-invariant subsemigroup of G that is not a subgroup. Then $N \neq N^{-1}$, where $N^{-1} = \{n^{-1} \mid n \in N\}$. Because N^{-1} is also a conjugation-invariant subsemigroup, we may assume $N \not\subset N^{-1}$. It is not difficult to verify that $N \setminus N^{-1}$ is a semigroup, so, by replacing N with $N \setminus N^{-1}$, we may assume $N \cap N^{-1} = \emptyset$. Define a partial order on G by $a < b$ if $a^{-1}b \in N$. Since N is conjugation invariant, it is easy to verify that this partial order is invariant.

$(2 \Rightarrow 4)$ The subsemigroup of G generated by the conjugates of x is conjugation-invariant, so, by assumption, it is a normal subgroup N of G. If $y \in N$, then, by definition of N, we know that y is a product of conjugates of x.

$(4 \Rightarrow 3)$ Let N be a conjugation-invariant subsemigroup, and let $x \in N$. Every normal subgroup of G contains e, so e is a product of conjugates of x. Because N is conjugation invariant, we know that N contains each of these conjugates. Thus, $e \in N$.

$(3 \Rightarrow 5)$ The subsemigroup of G generated by the conjugates of x is conjugation-invariant so, by assumption, it must be the case that e is a product of conjugates of x.

$(5 \Rightarrow 1)$ We prove the contrapositive. Suppose G is partially ordered, so there exist $b, c \in G$ with $b > c$. Let $x = bc^{-1}$. Then, because the partial order is invariant, we must have $x > e$. Indeed, we must have $x^a > e$, for all $a \in G$. Then, by invariance and transitivity, we have $x^{a_1} x^{a_2} \cdots x^{a_n} > e$. Hence $x^{a_1} x^{a_2} \cdots x^{a_n} \neq e$. $\square$

2.3. *Remark.* Let G be a group.

1. If G is a finite group (or, more generally, a torsion group), then G is not partially orderable.
2. Let N be a normal subgroup of G. If G is partially orderable, then either N or G/N is partially orderable.
3. Let N be a normal subgroup of G. If G/N is partially orderable, then G is partially orderable.
4. Let N be a finite, normal subgroup of G. Then G is partially orderable iff G/N is partially orderable.

5. Every finite-index subgroup of a partially-orderable group is partially order-able.

6. A group with a partially orderable subgroup of finite index need not be partially orderable. For example, the infinite cyclic group $\mathbb{Z}$ is an index-2 subgroup of the infinite dihedral group D_∞. There is a natural order on $\mathbb{Z}$, but every element of D_∞ is conjugate to its inverse.

The following proposition, its two corollaries, and the bounded cohomology group $H_b^2(G, \mathbb{R})$ are not needed elsewhere in this paper.

2.4. Proposition. *If G is a group that is not partially orderable, then the natural homomorphism from $H_b^2(G, \mathbb{R})$ to $H^2(G, \mathbb{R})$ is injective.*

Proof. If the homomorphism has a nontrivial kernel, then there is an unbounded function $f\colon G \to \mathbb{R}$ such that the coboundary $\alpha(x, y) = f(x) + f(y) - f(xy)$ is bounded. It is an important fact that the function f can be chosen to be constant on conjugacy classes [Bav, Prop. 3.3.1]. Then

$$\{g \in G \mid f(g) > \|\alpha\|_\infty\}$$

is a conjugation-invariant subsemigroup of G that does not contain e, so Proposition 2.2 implies that G is partially orderable. $\square$

2.5. Corollary. *Let Γ be a lattice in a connected, semisimple Lie group G with finite center. If*

- *$\Gamma/[\Gamma, \Gamma]$ is finite;*
- *$H^2(\Gamma; \mathbb{R}) = 0$; and*
- *Γ is not partially orderable;*

then every continuous action of Γ on the circle S^1 has a finite orbit.

Proof. From the proposition, we see that $H_b^2(\Gamma; \mathbb{R}) = 0$. Since $\Gamma/[\Gamma, \Gamma]$ is finite, we know that $H^1(\Gamma; \mathbb{R}/\mathbb{Z})$ is finite. Therefore, from the exact sequence

$$H^1(\Gamma; \mathbb{R}/\mathbb{Z}) \to H_b^2(\Gamma; \mathbb{Z}) \to H_b^2(\Gamma; \mathbb{R}),$$

we conclude that $H_b^2(\Gamma; \mathbb{Z})$ is finite. Therefore, for every $\omega \in H_b^2(\Gamma; \mathbb{Z})$, there is a finite-index subgroup Γ' of Γ such that the restriction of ω to Γ' is the zero element of $H_b^2(\Gamma'; \mathbb{Z})$. Thus, from fundamental work of E. Ghys [Ghy, Thm. A(1) (and Prop. 2–3)], we conclude that every action of Γ on S^1 has a finite orbit. $\square$

2.6. Corollary. *Let Γ be a lattice in a connected, semisimple Lie group G with finite center. If*

- *$\Gamma'/[\Gamma', \Gamma']$ is finite, for every finite-index subgroup Γ' of Γ;*
- *$H^2(\Gamma; \mathbb{R}) = 0$; and*
- *Γ is not partially orderable;*

then every C^1 action of Γ on the circle S^1 factors through an action of a finite quotient of Γ.

Proof. From the preceding corollary, we know that some finite-index subgroup Γ' of Γ has a fixed point p. We may assume the action of Γ' is orientation preserving, by replacing Γ' with an index-2 subgroup if necessary. Since $\Gamma'/[\Gamma', \Gamma']$ is finite, and S^1 is one-dimensional, we see that the action of Γ' on the tangent space $T_p S^1$ must be trivial. (Also note that Γ' is finitely generated [Rag, Rem. 13.21, p. 210].) Hence, from the Thurston Stability Theorem [Thu, Thm. 3], we conclude that Γ' acts trivially on S^1, so the kernel of the Γ-action is a finite-index subgroup of Γ. $\square$

The following lemma is well known (cf. [B–T, pf. of Lem. 8.3, p. 123]), but the author is unable to locate a proof in the literature. A similar result in the setting of Lie groups appears in [Var, Thm. 2.7.5, p. 71], with essentially the same proof. The only significant difference is that we assume H is semisimple, because (unlike the situation for Lie groups) it is not true that every Lie subalgebra is the Lie algebra of an algebraic subgroup, though it is true for semisimple Lie subalgebras.

2.7. Lemma. *Let G and H be algebraic groups over a field K of characteristic 0, with Lie algebras $\mathcal{G}$ and $\mathcal{H}$. If H is semisimple and simply connected, then every homomorphism from $\mathcal{H}_K$ to $\mathcal{G}_K$ is the differential of a K-homomorphism from H to G.*

Proof. Let $\psi\colon \mathcal{H}_K \to \mathcal{G}_K$ be a homomorphism, and let $\mathcal{A}_K \subset \mathcal{H}_K \oplus \mathcal{G}_K$ be the graph of ψ. Then $\mathcal{A}_K$ is a semisimple Lie subalgebra of $\mathcal{H}_K \oplus \mathcal{G}_K$, so there is a connected K-subgroup A of $H \times G$ whose Lie algebra is $\mathcal{A}_K$ [Hoc, Thm. VIII.3.2, p. 112]. Let $\pi_H\colon A \to H$ and $\pi_G\colon A \to G$ be the natural projections. Since the projection of $\mathcal{A}_K$ to $\mathcal{H}_K$ is surjective, we see that π_H is surjective and, since $\mathcal{A}_K \cap \mathcal{G}_K = 0$, we see that $\ker \pi_H$ is finite. Therefore, π_H is a central isogeny. Since H is simply connected, this implies that π_H is an isomorphism. Thus, $\pi_H^{-1}\colon H \to A$ is regular, so the composite

$$\varphi\colon H \xrightarrow{\ \pi_H^{-1}\ } A \xrightarrow{\ \pi_G\ } G$$

is regular. Because A is the graph of φ, it is easy to see that $\mathcal{A}$ is the graph of $d\varphi$, so $d\varphi|_{\mathcal{H}_K} = \psi$. □

The following version of the Jacobson-Morosov Lemma seems to be well known (cf. [K–L, §2.4, p. 166]), but, as is the case for the preceding lemma, the author is unable to locate a proof in the literature.

2.8. Lemma (Jacobson-Morosov)**.** *Let G be a reductive algebraic group over a field K of characteristic zero. If u is any unipotent element of G_K, then there is a K-homomorphism $\phi\colon \mathrm{SL}_2 \to G$, such that $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)^{\phi} = u$.*

Proof (cf. [B–T, pf. of Lem. 8.3, p. 123]). We may assume $u \neq e$. Since tori do not have nontrivial unipotent elements, we may assume G is semisimple. From the theory of the exponential and logarithmic functions for unipotent algebraic groups, we see that the Zariski closure U of $\langle u \rangle$ is a connected, one-dimensional, unipotent subgroup of G [Hum, Lem. 15.1C, p. 96], so the Lie algebra $\mathcal{U}$ of U is a one-dimensional, ad-nilpotent subalgebra of $\mathcal{G}$. Thus, by the Jacobson-Morosov Lemma [Jac, Thm. 17(1), p. 100], there is a Lie subalgebra $\mathcal{H}_K$ of $\mathcal{G}_K$ that is isomorphic to $\mathrm{sl}_2(K)$ and contains $\mathcal{U}_K$. Because semisimple subalgebras are algebraic [Hoc, Thm. VIII.3.2, p. 112], there is an algebraic subgroup H of G whose Lie algebra is $\mathcal{H}$. Since U is connected and $\mathcal{U} \subset \mathcal{H}$, then $U \subset H$.

Since SL_2 is simply connected, then there is a K-homomorphism $\phi\colon \mathrm{SL}_2 \to H$ whose differential is an isomorphism from $\mathrm{sl}_2(K)$ onto $\mathcal{H}_K$ (see 2.7). The naturality of the exponential and logarithmic functions implies that $\mathrm{SL}_2(K)^{\phi}$ contains every unipotent element of H_K. In particular, there is some unipotent $v \in \mathrm{SL}_2(K)$ with $v^{\phi} = u$. Because any unipotent element of $\mathrm{SL}_2(K)$ is conjugate to $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ under the automorphism group $\mathrm{PGL}_2(K)$, we may assume $v = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. □

1010 DAVE WITTE

3. Special linear groups

3.1. Lemma. *Let K be a field. For every $T \in \mathrm{SL}_n(K)$, either $T^n = \mathrm{Id}$, or there is some $A \in \mathrm{SL}_n(K)$, such that $(TATA^{-1})^2$ has a nonzero fixed vector.*

Proof. If T is a scalar matrix then, because $\det(T) = 1$, we have $T^n = \mathrm{Id}$. Thus, we may assume T is not a scalar matrix, so there is some nonzero vector v in K^n that is not an eigenvector for T. Then v and vT are linearly independent, so there is some $A \in \mathrm{SL}_n(K)$ with $(vT)A = v$ and $vA = -vT$. We have $vTATA^{-1} = -v$, so $(TATA^{-1})^2$ fixes v, as desired. □

3.2. Lemma. *Let G be a reductive algebraic group over a field K. For every unipotent element u of G_K, there exist $a_1, a_2, \ldots, a_k \in G_K$ with $u^{a_1} u^{a_2} \cdots u^{a_k} = e$.*

Proof. If K is of characteristic p, then there is some $k \in \mathbb{Z}^+$ such that $u^{p^k} = e$; hence, we may assume K is of characteristic 0. Then, by the Jacobson-Morosov Lemma (2.8), we may assume $G = \mathrm{SL}_2$ and $u = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix} \right)$. Letting $a = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix} \right)$, a simple calculation shows $(uu^a u)^4 = a^4 = e$, as desired. The reader may recognize this calculation as one of the Steinberg relations [H–O, Eqn. (E4), p. 28]. □

3.3. Theorem. *For every $T \in \mathrm{SL}_n(K)$, there exists a sequence of elements A_1, $A_2, \ldots, A_m$ of $\mathrm{SL}_n(K)$ such that $T^{A_1} T^{A_2} \cdots T^{A_m} = \mathrm{Id}$.*

Proof. Let N be the subsemigroup of $\mathrm{SL}_n(K)$ generated by the conjugates of T; we wish to show $\mathrm{Id} \in N$. Lemma 3.1 implies that some element T_1 of N has a nonzero fixed vector. (Now, the conclusion is trivial if $n = 1$, so assume $n > 1$.) Then, since $\mathrm{SL}_n(K)$ is transitive on the nonzero vectors in K^n, we may assume, by replacing T_1 with a conjugate, that T_1 fixes $e_n = (0, 0, \ldots, 0, 1)$.

Let S_{n-1} be the image of $\mathrm{SL}_{n-1}(K)$ in $\mathrm{SL}_n(K)$, under the natural embedding (in the upper left corner, so S_{n-1} fixes e_n). By induction on n, there exists a sequence of elements $A_1, A_2, \ldots, A_m$ of S_{n-1}, such that the element

$$T_2 = T_1^{A_1} T_1^{A_2} \cdots T_1^{A_m}$$

acts trivially on the quotient $K^n / \langle e_n \rangle$. Thus, $T_2 = \begin{pmatrix} \mathrm{Id} & * \\ 0 & 1 \end{pmatrix}$ is unipotent, so the desired conclusion follows from Lemma 3.2. □

4. Semisimple algebraic groups over local fields

4.1. Proposition. *Let G be a reductive algebraic group over a perfect field K. For every element x of G_K, there exist $a_1, a_2, \ldots, a_m \in G_K$ such that $x^{a_1} x^{a_2} \cdots x^{a_m}$ is semisimple.*

Proof. Let $x = su$ with s semisimple, u unipotent, and $su = us$ (the Jordan decomposition of x [Bor, Thm. 4.4(1), p. 83]). By replacing x with a power x^n, we may assume the Zariski closure of $\langle s \rangle$ is connected (and, hence, is a torus). Then $C_G(s)$ is reductive [Hum, Cor. 26.2A, p. 159] and contains u so, by Lemma 3.2, there is a sequence of elements $a_1, a_2, \ldots, a_m$ of $C_{G_K}(s)$, such that $u^{a_1} u^{a_2} \cdots u^{a_m} = e$. Since each a_i centralizes s, it follows that

$$x^{a_1} x^{a_2} \cdots x^{a_m} = s^m (u^{a_1} u^{a_2} \cdots u^{a_m}) = s^m$$

is semisimple. □

4.2. Proposition. *Let G be a semisimple algebraic group over a field K. For every K-split semisimple element x of G_K, there exist $a_1, a_2, \ldots, a_m \in G_K$ such that*

$$x^{a_1} x^{a_2} \cdots x^{a_m} = e.$$

Proof. We may assume G is connected. By assumption, x is contained in some maximal K-split torus A of G. Let W_K be the relative Weyl group of G_K, with respect to A_K. Then

$$\prod_{w \in W_K} x^w \in C_{A_K}(W_K) \subset Z(G_K).$$

Since $Z(G_K)$ is finite, some power of this element is e. □

4.3. Corollary. *If G is a semisimple algebraic group over an algebraically closed field K, then, for every element x of G_K, there exist $a_1, a_2, \ldots, a_m \in G_K$ such that $x^{a_1} x^{a_2} \cdots x^{a_m} = e$.*

Proof. By Proposition 4.1, we may assume x is semisimple. Because K is algebraically closed, every semisimple element is K-split, so Proposition 4.2 completes the proof. □

4.4. Theorem. *Let G be a semisimple algebraic group over a local field K of characteristic zero. Then, for every element x of G_K, there exist $a_1, a_2, \ldots, a_m \in G_K$ such that $x^{a_1} x^{a_2} \cdots x^{a_m} = e$.*

Proof. From Lemma 4.1, we may assume x is semisimple, so the conjugacy class C of x in G is Zariski closed (cf. [B–H, Prop. 10.1]). We may assume G is connected, so C is an irreducible variety. We may also assume that no proper, normal subgroup of G contains x.

Let $\overline{K}$ be the algebraic closure of K. From Corollary 4.3 (and 2.2), we know that every element of $G_{\overline{K}}$ is a product of elements of $C_{\overline{K}}$, so there is some $m \in \mathbb{Z}^+$ such that the Zariski closure of the m-fold product $(C_{\overline{K}})^m$ has the same dimension as G. Since G is an irreducible variety, this implies that $(C_{\overline{K}})^m$ is Zariski dense in G. Thus, the map

$$G \times G \times \cdots \times G \to G \colon (g_1, g_2, \ldots, g_m) \mapsto x^{g_1} x^{g_2} \cdots x^{g_m}$$

is dominant, so we conclude from the Inverse Function Theorem that $(C_K)^m$ contains a Hausdorff-open subset of G_K [P–R, Cor. 1 of Prop. 3.3, p. 113]. (To avoid confusion with the Zariski topology, we use the adjective "Hausdorff" to indicate the topology on G_K that arises from the locally compact topology on K.) Thus, $(C_K)^m$ contains a Hausdorff neighborhood of some element g of G_K. From Lemma 4.1 (or the fact that semisimple elements are Hausdorff-dense), we know that some product of conjugates of g is a semisimple element, so some $(C_K)^n$ contains a Hausdorff neighborhood of some semisimple element s of G_K.

Write $s = ak$, where a belongs to a K-split torus and k belongs to a K-anisotropic torus (and $ak = ka$). Let $\mathcal{O}$ be a Hausdorff neighborhood of e in G_K such that $ak\mathcal{O} \subset (C_K)^n$. Since anisotropic tori are compact [B–T, Cor. 9.4, p. 127], we know that $\langle k \rangle$ has an accumulation point, and then it is not difficult to see that e is an accumulation point. Thus, there is some $p \in \mathbb{Z}^+$ with $k^{-p} \in \mathcal{O}$. So

$$a^p \in a^p k^p \mathcal{O} \subset (ak\mathcal{O})^p \subset \big((C_K)^n\big)^p.$$

Proposition 4.2 (with a^p in the place of x) completes the proof. □

4.5. Corollary. *Let G be a connected, semisimple real Lie group. Then G has finite center iff for every element x of G, there are $a_1, a_2, \ldots, a_m \in G$ such that $x^{a_1} x^{a_2} \cdots x^{a_m} = e$.* $\square$

5. Symplectic groups

5.1. Lemma. *Let $\langle | \rangle$ be a (nondegenerate) symplectic form on a nonzero vector space V over a field. For every $T \in \mathrm{Sp}(V, \langle | \rangle)$, there is some $A \in \mathrm{Sp}(V, \langle | \rangle)$, such that $(TATA^{-1})^2$ fixes a nonzero vector in V.*

Proof. If every vector is an eigenvector for T, then T is a scalar matrix. Because T is symplectic, this implies $T = \pm \mathrm{Id}$, so $T^2 = \mathrm{Id}$. Thus, we may assume some $v \in V$ is *not* an eigenvector for T.

Case 1. *We have $\langle v \mid vT \rangle = 0$.* We may choose a basis $x_1, \ldots, x_n, y_1, \ldots, y_n$ for V, with $\langle x_i \mid x_j \rangle = \langle y_i \mid y_j \rangle = 0$ and $\langle x_i \mid y_j \rangle = \delta_{ij}$ for all i and j, such that $x_1 = v$ and $x_2 = vT$. Define $A \in \mathrm{Sp}(V, \langle | \rangle)$ by

$$x_1 A = x_2, \qquad x_2 A = x_1, \qquad y_1 A = y_2, \qquad y_2 A = y_1$$

$$x_i A = x_i, \ y_i A = y_i, \ \forall i > 2.$$

Then $vTATA^{-1} = v$.

Case 2. *We have $\langle v \mid vT \rangle \neq 0$.* The restriction of $\langle | \rangle$ to $\langle v, vT \rangle$ is non-degenerate, so $\langle v, vT \rangle^\perp$ is a complementary subspace. Define $A \in \mathrm{Sp}(V, \langle | \rangle)$ by

$$vA = vT, \qquad (vT)A = -v$$

$$wA = w, \ \forall w \in \langle v, vT \rangle^\perp.$$

Then $v(TATA^{-1}) = -v$, so $(TATA^{-1})^2$ fixes v. $\square$

5.2. Theorem. *Let $\langle | \rangle$ be a nondegenerate, symplectic form on a vector space V over a field. Then, for every $T \in \mathrm{Sp}(V, \langle | \rangle)$, there exists a sequence of elements A_1, $A_2, \ldots, A_m$ of $\mathrm{Sp}(V, \langle | \rangle)$, such that $T^{A_1} T^{A_2} \cdots T^{A_m} = \mathrm{Id}$.*

Proof. From the preceding lemma, we may assume T fixes a vector v. Note that $v^\perp$ is T-invariant, and T acts as the identity on the quotient $V/v^\perp$. By induction, we may also assume that T acts as the identity on the symplectic vector space $v^\perp / \langle v \rangle$. So T acts as the identity on each quotient of the flag

$$0 \subset \langle v \rangle \subset v^\perp \subset V.$$

Therefore, T is unipotent, so Lemma 3.2 completes the proof. $\square$

6. Special orthogonal groups

6.1. Lemma. *Let $\langle | \rangle$ be a nondegenerate, symmetric bilinear form on a vector space V over an infinite field K, with $\dim V \geq 3$ and $\mathrm{char} \, K \neq 2$. For every $T \in \mathrm{SO}(V, \langle | \rangle)$, either T^2 is unipotent, or there is some $A \in \mathrm{SO}(V, \langle | \rangle)$, such that $TATA^{-1}$ fixes an anisotropic vector in V.*

Proof. First, we show that we may assume no anisotropic vector of V is an eigenvector for T. Suppose, to the contrary, that $vT = \lambda v$, for some $\lambda \in K$, and v is anisotropic. Because T is an orthogonal matrix, we must have $\lambda = \pm 1$. Therefore, T^2 fixes the anisotropic vector v.

We now know that, for every anisotropic $v \in V$, the vectors v and vT are linearly independent. Assume, for the moment, that the restriction of $\langle | \rangle$ to $\langle v, vT \rangle$ is nondegenerate. Because $\langle v \mid v \rangle = \langle vT \mid vT \rangle$ and $\langle vT \mid v \rangle = \langle v \mid vT \rangle$, and there is a third coordinate that can be taken to its negative to get the determinant to be 1, there is $A \in \mathrm{SO}(V, \langle | \rangle)$ with $(vT)A = v$ and $vA = vT$. Therefore, $vTATA^{-1} = v$.

We may now assume, for every anisotropic vector $v \in V$, that the vectors v and vT are linearly independent, but the restriction of $\langle | \rangle$ to $\langle v, vT \rangle$ is degenerate. Since $\langle vT \mid vT \rangle = \langle v \mid v \rangle$, this implies that $\langle vT \mid v \rangle = \pm \langle v \mid v \rangle$. Thus,

for every anisotropic $v \in V$, either $(vT - v) \perp \langle v, vT \rangle$ or $(vT + v) \perp \langle v, vT \rangle$.

However, the set of anisotropic vectors is Zariski dense in V, and, for each $\varepsilon \in \{1, -1\}$, the set of vectors v such that $(vT + \varepsilon v) \perp v$ and $(vT + \varepsilon v) \perp vT$ is Zariski closed. So, because V is an irreducible variety, we conclude that either

$$\forall v \in V, \ (vT - v) \perp \langle v, vT \rangle \quad \text{or} \quad \forall v \in V, \ (vT + v) \perp \langle v, vT \rangle.$$

There is no harm in replacing T with $-T$, so we may assume

$$(6.2) \qquad\qquad\qquad \forall v \in V, \ (vT - v) \perp \langle v, vT \rangle.$$

Let $w \perp \mathrm{range}(T - \mathrm{Id})$. For all $v \in V$, we have

$$
\begin{aligned}
0 &= \langle (v + w)(T - \mathrm{Id}) \mid v + w \rangle && ((6.2)) \\
&= \langle v(T - \mathrm{Id}) \mid w \rangle + \langle w(T - \mathrm{Id}) \mid v \rangle && \text{(bilinearity and (6.2))} \\
&= \langle w(T - \mathrm{Id}) \mid v \rangle && \text{(definition of } w).
\end{aligned}
$$

Since the bilinear form is nondegenerate, we conclude that $w(T - \mathrm{Id}) = 0$. Thus, the restriction of T to $\mathrm{range}(T - \mathrm{Id})^{\perp}$ is Id.

Thus, letting $A = \mathrm{Id}$, the restriction of $TATA^{-1}$ to $\mathrm{range}(T - \mathrm{Id})^{\perp}$ is Id, so we have the desired conclusion unless $\mathrm{range}(T - \mathrm{Id})^{\perp}$ is totally isotropic. On the other hand, $\mathrm{range}(T - \mathrm{Id})$ is totally isotropic by (6.2), so this can only happen if $\dim(\mathrm{range}(T - \mathrm{Id})) = (\frac{1}{2}) \dim V$ and $\mathrm{range}(T - \mathrm{Id}) = \mathrm{range}(T - \mathrm{Id})^{\perp}$. Then, from the conclusion of the preceding paragraph, we conclude that the restriction of T to $\mathrm{range}(T - \mathrm{Id})$ is Id. Hence, T is unipotent. $\square$

6.3. Lemma. *Let $\langle | \rangle$ be a nondegenerate, symmetric bilinear form on a vector space V over an infinite field K of characteristic 2. For every $T \in \mathrm{SO}(V, \langle | \rangle)$, there exists a sequence $A_1, A_2, \ldots, A_m$ of elements of $\mathrm{SO}(V, \langle | \rangle)$, such that $T^{A_1} T^{A_2} \cdots T^{A_m} = \mathrm{Id}$.*

Proof. From Theorem 5.2, we may assume $\langle | \rangle$ is not symplectic. (That is, some vector in V is anisotropic.) If T fixes some anisotropic vector $v \in V$, then, by induction on $\dim V$, we may assume the restriction of T to $v^{\perp}$ is Id, so $T = \mathrm{Id}$. Thus, from the proof of Lemma 6.1 (except the final paragraph), we see that we may assume every vector in $R = \mathrm{range}(T - \mathrm{Id})$ is isotropic (see 6.2), and that the restriction of T to $R^{\perp}$ is Id (so $T - \mathrm{Id}$ annihilates $R^{\perp}$). Now $\langle | \rangle$ naturally induces a symplectic form on $R/(R \cap R^{\perp})$, so it follows from Theorem 5.2 that we may assume $T - \mathrm{Id}$ annihilates $R/(R \cap R^{\perp})$. Then $T - \mathrm{Id}$ annihilates V/R, $R/(R \cap R^{\perp})$, and $R \cap R^{\perp}$. Therefore, T is unipotent, so Lemma 3.2 completes the proof. $\square$

6.4. Theorem. *Let $\langle | \rangle$ be a nondegenerate, symmetric bilinear form on a vector space V over a field K, with $\dim V \geq 3$. For every $T \in \mathrm{SO}(V, \langle | \rangle)$, there exists a sequence of elements A_1, A_2, $\ldots$, A_m of $\mathrm{SO}(V, \langle | \rangle)$, such that $T^{A_1} T^{A_2} \cdots T^{A_m} = \mathrm{Id}$.*

Proof. The desired conclusion is obvious if $\mathrm{SO}(V, \langle | \rangle)$ is finite, so we may assume K is infinite. Furthermore, from Lemma 6.3, we may assume that char $K \neq 2$. Then, from Lemma 6.1 (and 3.2), we may assume T fixes an anisotropic vector e_3 of V. Thus, $e_3^{\perp}$ is T-invariant, and the restriction of the bilinear form to this complementary subspace is nondegenerate. By induction, we may assume $\dim(e_3^{\perp}) = 2$, which means $\dim V = 3$. Choose an orthogonal basis $\{e_1, e_2\}$ of $e_3^{\perp}$ (with respect to $\langle | \rangle$), and define $A \in \mathrm{SO}(V, \langle | \rangle)$ by $e_i A = (-1)^i e_i$, $i = 1, 2, 3$.

We claim that $(AT)^2 = \mathrm{Id}$. (Because $A^{-1} = A$, this will complete the proof.) Clearly, $(AT)^2$ fixes e_3, so we need only show that the restriction of $(AT)^2$ to $W = e_3^{\perp}$ is the identity. To this end, let A' and T' be the restrictions of A and T to W. Because $\det(A'T') = -1$, we know $A'T' \notin \mathrm{SO}(W, \langle | \rangle)$; therefore, $A'T'$ is a reflection. (The Cartan-Dieudonné Theorem [Art, Thm. 3.20, p. 129] asserts that every element of $\mathrm{O}(n, \langle | \rangle)$ is a product of no more than n reflections. In the special case $n = 2$, this means that every element of $\mathrm{O}(2, \langle | \rangle)$ either is a reflection or is a product of two reflections—and, hence, belongs to $\mathrm{SO}(2, \langle | \rangle)$.) So $(A'T')^2 = \mathrm{Id}$, as desired. $\square$

References

[Art] E. Artin, *Geometric Algebra*, Interscience, New York, 1957. MR **18**:553e

[Bav] C. Bavard, Longueur stable des commutateurs, *Enseign. Math.* (2) **37** (1991) 109–150. MR **92g**:20051

[Bor] A. Borel, *Linear Algebraic Groups, 2nd ed.*, Springer-Verlag, Berlin/New York, 1991. MR **92d**:20001

[B–H] A. Borel and Harish-Chandra, Arithmetic subgroups of algebraic groups, *Ann. Math.* **75** (1962) 485–535. MR **26**:5081

[B–T] A. Borel and J. Tits, Groupes réductifs, *Publ. Math. Inst. Hautes Etud. Sci.* **27** (1965) 55–150. MR **34**:7527

[Fuc] L. Fuchs, *Partially Ordered Algebraic Systems*, Pergamon, London/New York, 1963. MR **30**:2090

[Ghy] E. Ghys, Groupes d'homéomorphismes du cercle et cohomologie bornée, *Contemporary Math.* **58**, Part III (1987) 81–106. MR **88m**:58024

[GMR] A. M. W. Glass, S. H. McCleary, and M. Rubin, Automorphisms groups of countable highly homogeneous partially ordered sets, *Math. Z.* 214 (1993) 55–66. MR **94i**:20005

[H–O] A. J. Hahn and O. T. O'Meara, *The Classical Groups and K-Theory*, Springer-Verlag, Berlin/New York, 1989. MR **90i**:20002

[Hoc] G. P. Hochschild, *Basic Theory of Algebraic Groups and Lie Algebras*, Springer-Verlag, Berlin/New York, 1981. MR **82i**:20002

[Hof] K. H. Hofmann, A short course on the Lie theory of semigroups I, *Seminar Sophus Lie* **1** (1991) 33–40. MR **92j**:22002

[Hum] J. E. Humphreys, *Linear Algebraic Groups*, Springer-Verlag, Berlin/New York, 1975. MR **53**:633

[Jac] N. Jacobson, *Lie Algebras*, Dover, New York, 1962. MR **26**:1345

[K–L] D. Kazhdan and G. Lusztig, Proof of the Deligne-Langlands Conjecture for Hecke algebras, *Invent. Math.* **87** (1987) 153–215. MR **88d**:11121

[Nee] K.-H. Neeb, Invariant Subsemigroups of Lie Groups, *Memoirs Amer. Math. Soc.* **104** (1993) no. 499. MR **94a**:22001

[P–R] V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory*, Academic Press, San Diego, 1994. MR **95b**:11039

[Rag]   M. S. Raghunathan, *Discrete Subgroups of Lie Groups*, Springer-Verlag, Berlin/New York, 1972. MR **58:**22394a

[Thu]   W. Thurston, A generation of the Reeb Stability Theorem, *Topology* **13** (1974) 347–352. MR **50:**8558

[Var]   V. S. Varadarajan, *Lie Groups, Lie Algebras, and Their Representations*, Springer-Verlag, Berlin/New York, 1984. MR **85e:**22001

[Wit]   D. Witte, Arithmetic groups of higher $\mathbb{Q}$-rank cannot act on 1-manifolds, *Proc. Amer. Math. Soc.* **122** (1994) 333–340. MR **95a:**22014

Department of Mathematics, Williams College, Williamstown, Massachusetts 01267
Current address: Department of Mathematics, Oklahoma State University, Stillwater, Oklahoma 74078
E-mail address: `dwitte@math.okstate.edu`