Europ. J. Combinatorics (1987) **8**, 145–149

A Note on Pseudo-reflections

OFER GABBER

In this note, we show that if V is a finite dimensional vector space equipped with a non-degenerate bilinear form, and one has a set of pseudo-reflections on V, preserving the form and having no non-zero common fixed vector, then the group G generated by this set is 'sufficiently large' in the sense that for every linear transformation $T: V \to V$, there exists an element $g \in G$ such that $g - T$ is invertible.

Recall (cf. [1], Déf. 1 page 66) that if D is a (skew-)field and V is a D vector space, then a linear transformation $T: V \to V$ is called a pseudo-reflection iff rank $(T - \mathrm{id}_V) = 1$, i.e. iff T is of the form $x \mapsto x + f(x)\nu$ for some $\nu \in V - \{0\}$ and $f \in V^\vee - \{0\}$. [Here $V^\vee$ denotes the right D-module $\mathrm{Hom}_D(V, D)$ (on which the right D action is defined by $fd = (\nu \mapsto f(\nu)d)$ $\forall f \in V^\vee$, $\forall d \in D$).] Clearly f (resp. ν) is uniquely determined by T up to right (resp. left) multiplication by an element of D^*.

In this note, we consider the following situation B: V is of dimension n over D, and $T_i: V \to V$ $(1 \leq i \leq n)$ are invertible pseudo-reflections s.t. if we write $T_i = (x \mapsto x + f_i(x)\nu_i)$ then $(\nu_i)_{1 \leq i \leq n}$ is a basis of V and $(f_i)_{1 \leq i \leq n}$ is a basis of $V^\vee$.

We shall use the following notations: $\underline{n}$ is the set $\{1, 2, \ldots, n\} = \{k \in \mathbb{Z} \mid 0 < k \leq n\}$, and R is the set of pairs $(A, <)$, where A is a subset of $\underline{n}$ and $<$ is a strict total order on A. Equivalently (up to a canonical bijection) R can be described as the set of pairs $(k, (i_1, \ldots, i_k))$ where $0 \leq k \leq n$ and the i_js $(1 \leq j \leq k)$ are distinct elements of $\underline{n}$.

For any element $(A, <)$ of R, we consider the linear transformation $T_{(A,<)} =^{\mathrm{def}} \prod_{a \in A} T_a$, where the product of the T_as is taken according to the total ordering $<$ of A, in other words if we use the second description of R then $T_{(A,<)} = T_{i_1} \cdot T_{i_2} \cdot \cdots \cdot T_{i_k}$.

Our main result is the following:

THEOREM 1. (*Under situation* B.) *If* $S: V \to V$ *is any linear transformation, then*

(i) *there exists an element* $(A, <)$ *of* R *s.t. the transformation* $S - T_{(A,<)} \in \mathrm{End}(V)$ *is invertible**.

(ii) *There exists an element* $(A, <)$ *of* R *s.t.* $ST_{(A,<)} - 1$ *and* $T_{(A,<)}S - 1$ *are invertible.*

(iii) *If* D *is commutative and* $D \hookrightarrow \bar{D}$ *is an algebraic closure of* D, *and* $\lambda \in \bar{D}^*$, *then there exists an element* $(A, <) \in R$ *s.t.* λ *is not an eigenvalue of* $ST_{(A,<)}$.

PROOF. (ii)$\Rightarrow$(iii): Apply part (ii) with S replaced by $\lambda^{-1}S$. (i)$\Rightarrow$(ii): We notice that $T_i^{-1} = (x \mapsto f_i(x)\alpha_i\nu_i)$ where $\alpha_i = (1 + f_i(\nu_i))^{-1} \in D^*$, so that $(V, T_1^{-1}, \ldots, T_n^{-1})$ still satisfies the hypotheses of B. Applying (i) to $(V, T_1^{-1}, \ldots, T_n^{-1})$, we get that there exists $(A, <) \in R$ s.t. $S - T_{i_1}^{-1} \cdots T_{i_k}^{-1} = S - (T_{i_k} \cdot \cdots \cdot T_{i_1})^{-1}$ is invertible, i.e. s.t. $S \cdot T_{i_k} \cdot \cdots \cdot T_{i_1} - 1_V$ is invertible, equivalently $(T_{i_k} \cdot \cdots \cdot T_{i_1}) \cdot S - 1_V$ is invertible.

The proof of Theorem 1(i) will be based on the consideration of a 'largest invertible principal minor'. We wish to find an element $(A, <) \in R$ s.t. $S' - (T_{(A,<)} - \mathrm{id}_V)$ is invertible, where $S' =^{\mathrm{def}} S - \mathrm{id}_V$, i.e. s.t. $\forall \nu \in V - \{0\}$ we have that $S'\nu \neq T_{(A,<)}\nu - \nu$. Since $f_1, \ldots, f_n$ form a basis of $V^\vee$, we can speak about the dual basis $\nu'_1, \ldots, \nu'_n$ of V defined by the condition that $f_i(\nu'_j) = \delta_{ij}$. We represent $S': V \to V$ by a matrix M [as in [3] Chapter XIII, Section 3] by taking $\nu'_1, \ldots, \nu'_n$ to be a basis for the source space, and $\nu_1, \ldots, \nu_n$ to be a

* The hypothesis that the T_is are invertible will not be needed in the proof of part (i).

0195-6698/87/020145+05 $02.00/0

basis for the target space. We have $S'\nu'_j = \sum_i M_{ij}\nu_i$, i.e.

$$S'\nu = \sum_{i,j} M_{ij} f_j(\nu)\nu_i \quad \forall \nu \in V.$$

For every subset $I \subset \underline{n}$ we can consider the square $I \times I$ submatrix m_I of M obtained by restricting the value of the indices (i,j) to be in $I \times I$. Let $P(\underline{n})_{\mathrm{inv}} = \{I \subset \underline{n} \mid M_I$ is invertible$\}$; we partially order $P(\underline{n})_{\mathrm{inv}}$ by inclusion. The ring $\mathrm{Mat}_{\varnothing}(D)$ of $\varnothing$ by $\varnothing$ matrices with entries in D, whose underlying set is [by definition, compare [3, XIII § 1] and [2, Section 10, No. 1-7]] the set of functions from $\varnothing \times \varnothing$ to D, has exactly one element (namely the function [with graph] $\varnothing$) which is thus both the identity element and the zero element, and hence every element in that ring is invertible. Hence $M_{\varnothing}$ is invertible, i.e. $\varnothing \in P(\underline{n})_{\mathrm{inv}}$, so $P(\underline{n})_{\mathrm{inv}}$ is non-empty and hence admits a maximal element $\bar{I}$.

Let $\mathscr{L}(M): D^{\underline{n}} \to D^{\underline{n}}$ be the linear transformation represented by M. [Thus the choice of the basis (ν'_i) (resp. (ν_j)) for V_{source} (resp. V_{target}) allows us to 'identify' S' with $\mathscr{L}(M)$.] Thus the composition $D^{\underline{n}} \to_{\mathscr{L}(M)} D^{\underline{n}} \to_{\mathrm{pr}_{\bar{I}}} D^{\bar{I}}$ maps $D^{\bar{I}}$ (regarded as a subspace of $D^{\underline{n}}$) isomorphically onto $D^{\bar{I}}$, and thus the linear subspace $W =^{\mathrm{def}} \mathrm{Ker}(\mathrm{pr}_{\bar{I}} \circ \mathscr{L}(M)) \subset D^{\underline{n}}$ is such that $D^{\underline{n}} = D^{\bar{I}} \oplus W$. In other words, if C denotes $\underline{n} - \bar{I}$, pr_C induces an isomorphism $W \to^{\zeta} D^C$. Composing the inverse of this isomorphism with $\mathscr{L}(M)$ we get a map $D^C \to_{\zeta^{-1}} W \to_{\mathscr{L}(M)} D^C (\subset D^{\underline{n}})$. Let N be the $C \times C$ matrix representing the last linear transform.

Claim. *For every non empty subset $J \subset C$, the matrix N_J is not invertible.*

Proof. If N_J were invertible, we claim that it would follow that $M_{\bar{I} \cup J}$ is invertible, contradicting the maximality of $\bar{I}$ in $P(n)_{\mathrm{inv}}$. To show this implication, we observe that the decomposition $D^{\underline{n}} = D^{\bar{I}} \oplus W$ restricts to give an isomorphism $D^{\bar{I} \cup J} = D^{\bar{I}} \oplus \zeta^{-1}(D^J)$. The transformation $\mathrm{pr}_{\bar{I} \cup J} \circ \mathscr{L}(M)$ on this space carries $D^{\bar{I}}$ isomorphically onto a complement of the subspace D^J of $D^{\bar{I} \cup J}$, and it carries $\zeta^{-1}(D^J)$ into D^J. Therefore we see that $\mathscr{L}(M_{\bar{I} \cup J}) = \mathrm{pr}_{\bar{I} \cup J} \circ \mathscr{L}(M)|_D^{\bar{I} \cup J} \simeq \mathrm{id}_{D^I} \oplus N_J$, and thus it is invertible iff N_J is.

Claim. *The set C can be totally ordered s.t. with respect to the resulting bijection $C \simeq \{1, 2, \ldots, s\}$ $(s = |C|)$ one has that the matrix N is strictly upper triangular, i.e. $N_{\alpha\beta} = 0$ for $\beta \leq \alpha$, $\alpha, \beta \in C$.*

Proof. We use only the conclusion of the previous claim. The proof will be by induction on the size of C. If $|C| = 0$ on 1, then $N = 0$ by the hypotheses. If $c_1 \in C$ is an element such that $N_{d,c_1} = 0$ $\forall d \in C$, then we take c_1 to be the first element of C, and using the induction hypothesis we totally order $C - \{c_1\}$ so as to make $N_{C-\{c_1\}}$ strictly upper triangular. So it remains to show that such a c_1 exists. If not, then $\forall c \in C$, $\exists d \in C$ s.t. $N_{dc} \neq 0$. Since by our hypotheses the diagonal entries of N are zero, we see that $d \neq c$. Starting from an arbitrary $c_0 \in C$ (recall that we may assume $|C| > 1$), we get a sequence $c_0, c_1, c_2, \ldots$ s.t. $(\forall i) N_{c_{i+1}, c_i} \neq 0$, $c_{i+1} \neq c_i$. If we continue the sequence until $c_{|C|}$, we see that two members of the sequence must be equal. Hence there exists a sequence of elements of C of the form $a_0, a_1, \ldots, a_k = a_0$, s.t. $k \geq 2$, $N_{a_{i+1}, a_i} \neq 0$ $\forall 0 \leq i < k$. We call a $(k+1)$-tuple of elements of C having the above properties an allowed cycle of length k. (In the definition of 'allowed cycle', one may replace the condition $k \geq 2$ by $k \geq 1$; note that as the diagonal entries of N are zero, there is no allowed cycle of length 1.) Consider an allowed cycle $(a_0, a_1, \ldots, a_k)$ of minimal length k. Then $a_0, \ldots, a_{k-1}$ are distinct (because if $a_r = a_s$, $0 \leq r < s \leq k-1$, we get a shorter allowed cycle $(a_r, a_{r+1}, \ldots, a_s)$). Furthermore, we have that $N_{a_j, a_i} = 0$ if $j \not\equiv i+1 \pmod k$. (Indeed, if $j \not\equiv i+1 \pmod k$ and $N_{a_j, a_i} \neq 0$, we get a shorter allowed cycle $(a_i, a_j, a_{j+1}, \ldots, a_{j+t})$ of length $t+1$, where

$0 \le t < k-1$ is s.t. $j+t \equiv i \pmod k$. (Here we define $\forall n \in \mathbb{Z}$, $a_n = a_r$ where $r = n - [n/k]k$, i.e. $m \mapsto a_m$ is regarded as a function on $\mathbb{Z}/k\mathbb{Z}$.).) Hence the matrix N_J for $J = \{a_1, \dots, a_k\}$ is invertible (since the linear transformation it defines on D^J sends De_{a_i} isomorphically onto $De_{a_{i+1}}$, $\forall i \in \mathbb{Z}/k\mathbb{Z}$).

CLAIM. *The set C with its ordering $i_1, \dots, i_k$ considered in the previous claim is such that $S - T_{i_1} \cdot \dots \cdot T_{i_k}$ is invertible*

PROOF. We have to show that if $\nu \in V - \{0\}$ then

$$S'\nu \neq (T_{i_1} \cdot \dots \cdot T_{i_k})\nu - \nu = \sum_{m=1}^{k} (T_{i_m} - 1)((T_{i_{m+1}} \cdot \dots \cdot T_{i_k})\nu).$$

Indeed, suppose that

$$S'\nu = \sum_{m=1}^{k} (T_{i_m} - 1)((T_{i_{m+1}} \cdot \dots \cdot T_{i_k})\nu) \tag{$*$}$$

holds. Since $\mathrm{Im}(T_{i_m} - 1) = De_{i_m}$, we have that the right-hand side of the equality $(*)$ lies in $\sum_{m=1}^{k} De_{i_m}$, the subspace of V_{target} corresponding to $D^C \subset D^n$. Hence if we write $(\forall l \le i \le n)$ $\omega_i = f_i(\nu)$, so that $\vec{\omega} =^{\text{def}} (\omega_1, \dots, \omega_n) \in D^n$ and $\sum_{i=1}^{n} (\mathscr{L}(M)\vec{\omega})_i e_i = S'\nu$, then $(\mathrm{pr}_{D^I} \circ \mathscr{L}(M))(\vec{\omega}) = 0$, i.e. $\vec{\omega}$ lies in the subspace W of D^n defined above. Under the isomorphism $W \to_{\mathrm{pr}_C/W} D^C$, which was denoted above by ζ, the point $\vec{\omega}$ corresponds to the point $(\omega_j)_{j \in C}$. Hence, by the definition of N, we have that

$$\mathscr{L}(N) \colon (\omega_j)_{j \in C} \mapsto (\xi_j)_{j \in C},$$

where

$$\sum_{j \in C} \xi_j e_j = S'\nu \overset{(*)}{=} \sum_{m=1}^{k} f_{i_m}(T_{i_{m+1}} \cdot \dots \cdot T_{i_k}\nu) e_{i_k},$$

i.e. we have

$$\xi_{i_m} = f_{i_m}((T_{i_{m+1}} \cdot \dots \cdot T_{i_k})\nu), \quad \forall 1 \le m \le k. \tag{$**$}$$

Case (i): $T_{i_\alpha}(\nu) = \nu$ $\forall 1 \le \alpha \le k$. In this case we have by the formula $T_{i_\alpha}(x) = x + f_{i_\alpha}(x)\nu_{i_\alpha}$ that $f_{i_\alpha}(\nu) = 0$ $(\forall 1 \le \alpha \le k)$. Thus the C-coordinates of $\vec{\omega}$ are zero, and since $\vec{\omega} \in W$ and ζ is an isomorphism we get that $\vec{\omega} = 0$, i.e. $\nu = 0$, which gives a contradiction.

Case (ii): $\exists 1 \le \alpha \le k$ s.t. $T_{i_\alpha}(\nu) \neq \nu$. Put

$$m \overset{\text{def}}{=} \max\{1 \le \alpha \le k \mid T_{i_\alpha}(\nu) \neq \nu\}.$$

Thus $f_{i_m}(\nu) \neq 0$ and $f_{i_\lambda}(\nu) = 0$ $\forall m < \lambda \le k$.

(a) As $(T_{i_{m+1}} \cdot \dots \cdot T_{i_k})\nu = \nu$, $(**)$ gives that $\xi_{i_m} = f_{i_m}(\nu) \neq 0$, i.e. the i_mth coordinate of $\mathscr{L}(N)((\omega_j)_{j \in C})$ is non-zero.

(b) But $\mathscr{L}(N)((\omega_j)_{j \in C}) = (\sum_{j \in C} N_{ij}\omega_j)_{i \in C}$ and N is strictly upper triangular for the above ordering of C, so $\xi_{i_m} = \sum_{j \in C} N_{i_m, j}\omega_j = \sum_{m' > m} N_{i_m, i_{m'}}\omega_{i_{m'}} = 0$ (as the $\omega_{i_{m'}} = f_{i_{m'}}(\nu)$ are zero). This is a contradiction.

REMARK 1. If we take in Theorem 1 (ii) $S = \mathrm{id}_V$, i.e. $S' = 0_V$, then in the preceeding proof $M = 0_n$, $P(\underline{n})_{\mathrm{inv}} = \varnothing$, $\bar{I} = \varnothing$, $N = 0_n$, so the proof specializes to the fact that for every $(A, <) \in R$ s.t. $A = \underline{n}$, we have that $T_{(A,<)} - 1$ is invertible. This implies that if $V' \subsetneqq V''$ are subspaces of V stable under the operators $(T_i)_{1 \le i \le n}$, and $W =^{\text{def}} V''/V'$, then the transformations $T_i \colon W \to W$ induced by the T_is cannot all be 1_W. (Indeed, if they were all 1, then $R =^{\text{def}} T_{(A,<)} - 1$ would induce the map $1_W - 1_W = 0_W$ on V''/V', i.e. $R(V'') \subset V'$, but as R is invertible $V'' \to_{\widetilde{R}} R(V'')$, so the inclusion $V' \supset R(V'')$ gives an inequality $\dim V' \geqslant \dim V''$ contradicting the fact that $\dim V'' = \dim V' + \dim W > \dim V'$ by hypothesis.)

THEOREM 2. *Suppose that V is a vector space of dimension n over a commutative field D, $G \subset \mathrm{Aut}_D(V)$ a group generated by pseudo-reflections, and assume that there exists a non-degenerate G-invariant bilinear form $B: V \times V \to D$. Then the condition*

(0) $$V^G = 0$$

implies

(*i*) $$\forall S \in \mathrm{End}_D(V), \qquad \exists g \in G \ \text{ s.t. } g - S \textit{ is invertible},$$

and

(*ii*) $$\forall S \in \mathrm{End}_D(V), \qquad \exists g \in G \text{ s.t.} \qquad 1 - gS \text{ and } 1 - Sg \textit{ are invertible}.$$

PROOF. Clearly, as in the proof of Theorem 1 (ii), replacing g by g^{-1} we have that (i)$\Leftrightarrow$(ii). To prove (i) assuming (0), we use Theorem 1; it thus suffices to know that there exist n elements $g_i = (x \mapsto x + f_i(x)\nu_i)$ $(1 \leqslant i \leqslant n)$ in G s.t. (ν_i) are linearly independent in V and (f_i) are linearly independent in V^V. Fix a generating set $\Sigma \subset G$ consisting of pseudo-reflections. Write $\Sigma = \{\gamma_j = (x \mapsto x + f_j(x)\nu_j) \mid j \in J\}$. The fact that $V^G = 0$ means that $(V^\Sigma =) \bigcap_{j \in J} \mathrm{Ker}(f_j) = 0$. Hence (by the 'duality' $U \mapsto U^\perp$ between subspaces of V and $V^\perp$, cf. [2, Section 7 No. 5]) the f_js generate V^v, and hence it is possible to choose a basis for V^v of the form $(f_{j_1}, \dots, f_{j_n})$, $j_i \in J$. We take $g_i = \gamma_{j_i}(1 \leqslant i \leqslant n)$, and check the following

CLAIM. *$g_1, \dots, g_n$ satisfy condition* B.

PROOF. As $f_{j_1}, \dots, f_{j_n}$ form a basis of V^v, it remains to show that $\nu_{j_1}, \dots, \nu_{j_n}$ form a basis of V. Note that the bilinear form B defines two D-isomorphisms $V \to V^v$, $\phi_1: \nu \mapsto (x \mapsto B(x, \nu))$ and $\phi_2: \nu \mapsto (x \mapsto B(\nu, x))$. The ϕ_μ are G-equivariant, where G acts on V^v by the contragredient action $(g \mapsto (g^t)^{-1})$. One checks that $(\gamma_j^t)^{-1}$ is given by $f \mapsto f + f_i \alpha_i f(\nu_i)$, where $\alpha_i = (1 + f_i(\nu_i))^{-1} \in D^*$. Hence $\mathrm{Im}((\gamma_j^t)^{-1} - 1) = \langle f_j \rangle$, while $\mathrm{Im}(\gamma_j - 1) = \langle \nu_j \rangle$. $\forall \mu \in \{1, 2\}$, the map $\phi_\mu: V \to V^v$ must induce an isomorphism $\mathrm{Im}(\gamma_j - 1) \to \mathrm{Im}((\gamma_j^t)^{-1} - 1)$, so $\phi_\mu(\nu_j)$ is proportional to f_j. Thus the statement that the one-dimensional spaces $\langle \nu_{j_i} \rangle$ are linearly independent (resp. span V) is equivalent to the statement that the one-dimensional spaces $\langle f_{j_i} \rangle$ are linearly independent (resp. span V^v). So $(\nu_{j_1}, \dots, \nu_{j_n})$ is a basis of V, as desired.

REMARK 2. Under the hypotheses of Theorem 2, the following conditions are equivalent:

(0) $$V^G = 0,$$

(0)′ $$V_G = 0 \quad \left(\text{recall that } V_G = V \Big/ \Big(\sum_{g \in G} (g-1)V \Big)\right),$$

condition (i) above,
condition (ii) above,
(iii) $\exists \gamma \in G$ s.t. $\gamma - 1$ is invertible,
(iv) When we regard V as a DG-module as in [2, page 453], V has no non zero DG-module subquotient which has a trivial G action.

PROOF. The fact that (0)$\Leftrightarrow$(0)′ follows by considering the G-isomorphism ϕ_μ ($\mu = 1$ or 2), which induces an isomorphism

$$V^G \tilde{\to} (V^v)^G = \{f: V \to D, D\text{-linear} | \forall g \in G, f(g^{-1}\nu) = f(\nu) \forall \nu \in V\} \simeq (V_G)^v.$$

The statement ((0)[or (0)′]$\Rightarrow$(i) $\wedge$ (ii)) holds by Theorem 2. For the implication (i)$\Rightarrow$(iii)$\Rightarrow$(iv) see Remark 1. Finally (0) (resp. (0)′) is a special case of (iv), when the subquotient considered is a submodule of V (resp. a quotient module of V).

REMARK 3. Theorem 2 and Remark 2 can be extended to the case where D is not necessarily commutative, $\sigma: D \to D$ an anti-homomorphism, and $B: V \times V \to D$ is a non degenerate G-invariant form which is σ-sesquilinear (in the sense of [Bourbaki, Algèbre, Chapter IX, Section 1]), i.e. B is $\mathbb{Z}$-bilinear and $B(\alpha\nu, \beta\omega) = \alpha B(\nu, \omega)\sigma(\beta) \forall \alpha, \beta \in D$, $\forall \nu, \omega \in V$. In the proof of Remark 3, one uses the G-isomorphism $\phi_1: \sigma_! V \to V^v$ or $\phi_2: V \to (\sigma_! V)^v$, where $\sigma_! V$ is the right D-module associated to the left D^{op}-module $(D^{op}) \otimes_D V$, where the $\otimes$ product is taken with respect to the ring homomorphism $D \to_\sigma D^{op}$.

REFERENCES

1. N. Bourbaki, *Groupes et Algèbres de Lie,* (Chap. 4, 5, 6), Hermann, Paris, 1968.
2. N. Bourbaki, *Algèbre,* Chap. II, 3[e] édition, Hermann, Paris, 1962.
3. S. Lang, *Algebra,* Addison Wesley, 1965.

Received 13 August 1984 and in revised form 19 January 1985

OFER GABBER
Department of Mathematics, Institut des Hautes Etudes Scientifiques,
35 route de Chartres, 91440 Bures-sur-Yvette, France