PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 132, Number 1, Pages 37–46
S 0002-9939(03)07033-3
Article electronically published on May 9, 2003

FREE PRODUCTS IN LINEAR GROUPS

D. S. PASSMAN

(Communicated by Lance W. Small)

Abstract. Let R be a commutative integral domain of characteristic 0, and let G be a finite subgroup of $\mathrm{PGL}_n(R)$, the projective general linear group of degree n over R. In this note, we show that if $n \geq 2$, then $\mathrm{PGL}_n(R)$ also contains the free product $G * T$, where T is the infinite cyclic group generated by the image of a suitable transvection.

1. Introduction

Let R be a commutative integral domain of characteristic 0, and let $\mathrm{GL}_n(R)$ denote the general linear group of degree n over R, namely the group of invertible $n \times n$ R-matrices. If $R^\bullet$ is the set of scalar matrices in $\mathrm{GL}_n(R)$, then $R^\bullet$ is isomorphic to the group of units of R, and $\mathrm{GL}_n(R)/R^\bullet = \mathrm{PGL}_n(R)$ is the projective general linear group. Our goal here is to show that if G is a finite subgroup of $\mathrm{PGL}_n(R)$ and if $n \geq 2$, then $\mathrm{PGL}_n(R)$ also contains the free product $G * T$, where T is the infinite cyclic group generated by the image of a suitable transvection, namely a transformation of the form $1 + \tau$, where τ has rank 1 and square 0.

The above proposition actually arose as part of an argument to show that if H is a finite group having a noncentral subgroup G of prime order p, then the unit group of the integral group ring $Z[H]$ contains the free product $G * T$ for some infinite cyclic group T. Obviously, the proof of such a result must use the irreducible representations of the rational group algebra $Q[H]$ and then, under suitable conditions, properties of linear groups over characteristic 0 integral domains. Since the linear group results turned out to be of independent interest, they are being published separately. Indeed, a second paper [GM], written at the same time as this work, contains an alternate approach to the existence of free products in linear groups.

For the most part, we work in $\mathrm{GL}_n(C)$, where C is the field of complex numbers, and the key result here is

Theorem 1.1. *Let V be a finite-dimensional complex vector space, and let G be a subgroup of the general linear group $\mathrm{GL}(V)$ with $|G : (G \cap C^\bullet)| < \infty$. Furthermore, let $\tau \colon V \to V$ be a nonzero linear transformation of square 0, and write $K = \ker \tau$ and $I = \operatorname{im} \tau = \tau(V)$. If $gI \cap K = 0$ for all $g \in G \setminus (G \cap C^\bullet)$, then for all sufficiently large complex numbers $c \in C$, we have*

$$\langle G, 1 + c\tau \rangle / (G \cap C^\bullet) \cong \big(G/(G \cap C^\bullet)\big) * T,$$

Received by the editors August 26, 2002.
2000 *Mathematics Subject Classification.* Primary 20E06, 20H20.

where T is the infinite cyclic group generated by the image of the unit $1+c\tau$ in this factor group.

Observe that $(1+c\tau)(1-c\tau) = 1-c^2\tau^2 = 1$, so $1+c\tau \in \mathrm{GL}(V)$ and, of course, $\langle G, 1+c\tau\rangle$ indicates the subgroup of $\mathrm{GL}(V)$ generated by G and the element $1+c\tau$. As will be apparent, the proof of Theorem 1.1 contains enough information to compute the lower bound on the size of c when τ has rank 1. Indeed, we have

Corollary 1.2. *Let V be a finite-dimensional complex inner product vector space, let G be a subgroup of the general linear group $\mathrm{GL}(V)$ with $|G:(G\cap C^\bullet)|<\infty$, and assume that $(C^\bullet G)\cap \mathrm{SL}(V)$ acts in a unitary manner on V. Furthermore, let $\tau\colon V\to V$ be a linear transformation of square 0 and rank 1, write $I=\operatorname{im}\tau = Cv$, $K=\ker\tau$, and suppose that $gv\notin K$ for all $g\in G\setminus(G\cap C^\bullet)$. If m is the minimum value of $|\tau(gv)|/|gv|$ over all $g\in G\setminus(G\cap C^\bullet)$, and if c is a complex number with $|c|\geq 27\,\|\tau\|/m^2$, then we have*

$$\langle G, 1+c\tau\rangle/(G\cap C^\bullet)\cong \big(G/(G\cap C^\bullet)\big)*T,$$

where T is the infinite cyclic group generated by the image of the unit $1+c\tau$ in this factor group.

Presumably the factor 27 above can be appreciably decreased with more care, but we will not pursue this further. Note that, if A and B are groups, then the free product $A*B$ contains the free product of the conjugate subgroups $A^b=b^{-1}Ab$ for all $b\in B$. In particular, the preceding results have a number of obvious corollaries. Less obvious is

Theorem 1.3. *Let R be a characteristic 0 integral domain and let G be a finite subgroup of $\mathrm{PGL}_n(R)$. If $n\geq 2$, then $\mathrm{PGL}_n(R)$ contains the free product $G*T$, where T is the infinite cyclic group generated by the image of a suitable transvection $1+\tau\in \mathrm{SL}_n(Z)\subseteq \mathrm{SL}_n(R)$.*

As an immediate consequence, we obtain

Corollary 1.4. *Let R be a characteristic 0 integral domain and let G be a finite subgroup of $\mathrm{GL}_n(R)$ with $G\cap R^\bullet = 1$. If $n\geq 2$, then $\mathrm{GL}_n(R)$ contains the free product $G*T$, where T is the infinite cyclic group generated by a suitable transvection $1+\tau\in \mathrm{SL}_n(Z)\subseteq \mathrm{SL}_n(R)$.*

As is to be expected, the proof of Theorem 1.1 ultimately depends upon the "ping-pong" lemma of F. Klein (see [H, Lemma II.24]). For convenience, we state and quickly prove this result in precisely the form we require.

Lemma 1.5. *Let Γ be a group generated by subgroups G and T, and let G contain a normal subgroup Δ of Γ. Suppose Γ acts on a set X and let P and Q be disjoint nonempty subsets of X. If $\Delta Q\subseteq Q$, $(G\setminus\Delta)P\subseteq Q$, $(T\setminus 1)Q\subseteq P$, and $|T|>2$, then $\Gamma/\Delta\cong (G/\Delta)*T$.*

Proof. It suffices to show that no element $\gamma\in\Delta$ can be written as a nonempty alternating product of elements coming from $G\setminus\Delta$ and $T\setminus 1$. Suppose by way of contradiction that such a product $\gamma=\gamma_1\gamma_2\cdots\gamma_n$ exists with $n\geq 1$. If the product starts and ends in $G\setminus\Delta$, that is, if $\gamma_1,\gamma_n\in G\setminus\Delta$, then by conjugating this expression by a nonidentity element of T, we obtain a similar expression, but this time starting and ending in $T\setminus 1$. Next, if $\gamma_1\in G\setminus\Delta$ and $\gamma_n\in T\setminus 1$, then since $|T|>2$, we can conjugate γ by an element of $T\setminus\{1,\gamma_n^{-1}\}$ to obtain a similar product but starting and ending in $T \setminus 1$. Since the same argument handles the $\gamma_1 \in T \setminus 1$, $\gamma_n \in G \setminus \Delta$ situation, we can therefore replace any such expression by one with $\gamma_1, \gamma_n \in T \setminus 1$. But then, the alternating nature of the action of $G \setminus \Delta$ and $T \setminus 1$ on P and Q yields $\gamma Q \subseteq Q$ and $\gamma_1\gamma_2 \cdots \gamma_n Q \subseteq P$, and this is a contradiction since $\gamma = \gamma_1\gamma_2 \cdots \gamma_n$, and since P and Q are disjoint nonempty subsets of X. □

2. Proof of Theorem 1.1

The goal of this section is to prove Theorem 1.1 and its corollary. To start with, we suppose that V is a finite-dimensional complex vector space and that G is a subgroup of $\mathrm{GL}(V)$ with $|G : (G \cap C^\bullet)| < \infty$. If $H = C^\bullet G \cap \mathrm{SL}(V)$, then it is clear that $G \subseteq C^\bullet H$ and that $|H : (H \cap C^\bullet)| < \infty$. Furthermore, since $H \cap C^\bullet$ consists of scalar operators of determinant 1, it follows that $|H \cap C^\bullet| \le \dim_C V < \infty$. Thus H is a finite group and, as is well known, there exists a Hermitian inner product $(\ , \ )$ defined on V with H acting as unitary transformations. Indeed, if $[\ , \ ]$ is any Hermitian inner product, then we merely define $(a, b) = \sum_{h \in H} [ha, hb]$ for all $a, b \in V$. Now fix any such inner product $(\ , \ )$, let $S = \{v \in V \mid (v, v) = 1\}$ be the unit sphere in V, and define the real-valued distance function $d\colon V^\bullet \times V^\bullet \to R$ by

$$d(a, b) = \left| \frac{a}{|a|} - \frac{b}{|b|} \right| \ge 0$$

for all nonzero vectors $a, b \in V$. Since $d(a, b) \le \big|a/|a|\big| + \big|b/|b|\big| = 2$, we see that V has d-diameter at most 2. Indeed, the diameter is precisely 2 since $d(a, -a) = 2$.

Lemma 2.1. *Let $0 \ne a, b \in V$.*

(i) *If $\lambda \in C^\bullet$, then $d(\lambda a, \lambda b) = d(a, b)$.*
(ii) *If $g \in G$, then $d(ga, gb) = d(a, b)$.*
(iii) *$d(a, b) \le 2|a - b|/|a|$.*

Proof. Part (i) is clear and then (ii) follows since $G \subseteq C^\bullet H$ and since H consists of unitary transformations. For (iii), note that

$$v = \frac{a}{|a|} - \frac{b}{|b|} = \frac{a - b}{|a|} - \frac{b}{|b|} \cdot \frac{|a| - |b|}{|a|} = v' - v''.$$

Since $|v'| = |a - b|/|a|$ and $|v''| = \big||a| - |b|\big|/|a| \le |a - b|/|a|$, it follows that

$$d(a, b) = |v| \le |v'| + |v''| \le \frac{2|a - b|}{|a|},$$

as required. □

Now let A and B be subsets of V with $A^\bullet, B^\bullet \ne \emptyset$, where $A^\bullet = A \setminus 0$. Then we define

$$d(A, B) = d(A^\bullet, B^\bullet) = \inf \{d(a, b) \mid a \in A^\bullet, \ b \in B^\bullet\}.$$

We are particularly interested in subsets of V closed under multiplication by $C^\bullet$. Since these correspond (except for a possible 0 element) to subsets of the projective space of V, we call these projective subsets of V. Observe that if A is projective, then $\{a/|a| \mid a \in A^\bullet\} = A \cap S$ and $A^\bullet = C^\bullet(A \cap S)$, where the latter is the set of all products, not sums of products. Hence, for every subset $B \subseteq V$, we have $d(A, B) = d(A \cap S, B)$. In particular, if B is also projective, then $d(A, B) = d(A \cap S, B \cap S)$.

Lemma 2.2. *Let $A, B \subseteq V$ with $A^\bullet, B^\bullet \neq \emptyset$.*

(i) *If $\lambda \in C^\bullet$, then $d(\lambda A, \lambda B) = d(A, B)$. In particular, if B is projective, then $d(\lambda A, B) = d(A, B)$, so $d(C^\bullet A, B) = d(A, B)$.*
(ii) *If $g \in G$, then $d(gA, gB) = d(A, B)$.*
(iii) *If A and B are subspaces of V, then $d(A, B) = |a_0 - b_0|$ for some $a_0 \in A \cap S$, $b_0 \in B \cap S$. In particular, if $A \cap B = 0$, then $d(A, B) > 0$.*

Proof. Parts (i) and (ii) are immediate from the corresponding parts of Lemma 2.1. For (iii), we note that A and B are projective sets, so

$$d(A, B) = d(A \cap S, B \cap S) = \inf \{|a - b| \mid a \in A \cap S,\ b \in B \cap S\}.$$

Thus the result follows since $A \cap S$ and $B \cap S$ are compact and since $|\ |\colon V \to R$ is a continuous function. □

We now turn to the

Proof of Theorem 1.1. Recall that $I = \operatorname{im} \tau$, $K = \ker \tau$, and $gI \cap K = 0$ for all $g \in G \setminus (G \cap C^\bullet)$. We use the inner product and distance function as given above, and we proceed in a series of steps.

Step 1. *Notation and the definitions of ε, P and Q.*

Proof. If $g \in G \setminus (G \cap C^\bullet)$, then $gI \cap K = 0$, so $d(gI, K) > 0$ by Lemma 2.2(iii). Thus since $C^\bullet I = I$ and $|G : (G \cap C^\bullet)| < \infty$, we can choose a real number $\varepsilon > 0$ so that $d(gI, K) \geq 3\varepsilon$ for all elements $g \in G$ not contained in $G \cap C^\bullet$. Note that $\varepsilon \leq 2/3$ since V has diameter 2. Let

$$P = \{v \in V^\bullet \mid d(v, I) < \varepsilon\}.$$

Then $P \supseteq I^\bullet$, so $P \neq \emptyset$. Furthermore, since I is a projective set, it follows from Lemma 2.2(i) that P is also a projective set.

If $g \in G$, then Lemma 2.2(ii) implies that

$$gP = \{gv \in V^\bullet \mid d(v, I) < \varepsilon\} = \{w \in V^\bullet \mid d(w, gI) < \varepsilon\},$$

and we define

$$Q = \bigcup_{g \in G \setminus (G \cap C^\bullet)} gP.$$

Then $Q \neq \emptyset$ and, by definition, we have $\big(G \setminus (G \cap C^\bullet)\big)P \subseteq Q$. Note also that P and Q are projective sets, so $(G \cap C^\bullet)P \subseteq P$ and $(G \cap C^\bullet)Q \subseteq Q$. □

Step 2. *$d(K, Q) \geq 2\varepsilon$ and hence $P \cap Q = \emptyset$.*

Proof. We use the fact that K, Q and I are all projective sets. Let $a \in K \cap S$ and $b \in Q \cap S$. Then $b \in gP \cap S$ for some $g \in G \setminus (G \cap C^\bullet)$, so the definition of gP implies that there exists $c \in gI \cap S$ with $|b - c| = d(b, c) < \varepsilon$. Now $|a - c| = d(a, c) \geq d(K, gI) \geq 3\varepsilon$, so

$$|a - b| + \varepsilon > |a - b| + |b - c| \geq |a - c| \geq 3\varepsilon,$$

and therefore $|a - b| > 2\varepsilon$. Since $d(K, Q)$ is the infimum of these values $|a - b|$, we conclude that $d(K, Q) \geq 2\varepsilon$.

Finally, $\tau^2 = 0$, so $I \subseteq K$ and hence $d(I, Q) \geq d(K, Q) \geq 2\varepsilon$. In particular, if $v \in Q$, then $d(v, I) \geq d(Q, I) \geq 2\varepsilon > \varepsilon$. Thus $v \notin P$, and hence $P \cap Q = \emptyset$. □

Step 3. *There exists a real number $r > 0$ with the property that if $\lambda \in C$ with $|\lambda| \geq r$, then $(1+\lambda\tau)Q \subseteq P$.*

Proof. Write $V = K \dotplus Y$, a direct sum of subspaces. Since $K = \ker\tau$ and $I = \operatorname{im}\tau$, the restriction of τ to Y yields an invertible linear transformation $\sigma\colon Y \to I$. Thus $\sigma^{-1}\colon I \to Y$ and we let $s^{-1} = \|\sigma^{-1}\|$ be the norm of this map. In other words, $|\sigma^{-1}z| \leq s^{-1}|z|$ for all $z \in I$. In particular, if $y \in Y$, then $y = \sigma^{-1}(\tau y)$, so $|y| \leq s^{-1}|\tau y|$ and $|\tau y| \geq s|y|$. Set $r = 3/(s\varepsilon^2)$ and note that $rs\varepsilon - 1 = (3-\varepsilon)/\varepsilon > 2/\varepsilon$ since $1 > \varepsilon > 0$.

Now let $v \in Q^\bullet$, so $d(v,K) \geq d(Q,K) \geq 2\varepsilon$ by Step 2, and write $v = x + y \in K \dotplus Y = V$ with $x \in K$ and $y \in Y$. If $x = 0$, then $v = y$, so $|y| = |v| \geq \varepsilon|v|$ since $1 > \varepsilon > 0$. On the other hand, if $x \neq 0$, then, by Lemma 2.1(iii) with $a = v$ and $b = x$, we have $2|y|/|v| \geq d(v,x) \geq d(Q,K) \geq 2\varepsilon$, so again we obtain $|y| \geq \varepsilon|v|$. In other words, $|y| \geq \varepsilon|v|$ in all cases and hence $y \neq 0$. Now let $\lambda \in C$ with $|\lambda| \geq r$, and note that $1+\lambda\tau$ is an invertible linear transformation on V with inverse $1-\lambda\tau$. Thus $w = (1+\lambda\tau)v \neq 0$.

Since $x \in K = \ker\tau$, we have

$$w = (1+\lambda\tau)v = v + \lambda\tau v = v + \lambda\tau(x+y) = v + \lambda\tau y$$

and $\lambda\tau y \in I$. Furthermore, $y \neq 0$, so $\tau y = \sigma y \neq 0$ and hence $\lambda\tau y \neq 0$. Thus, by Lemma 2.1(iii) again with $a = w$ and $b = \lambda\tau y$, we have

$$d(w,I) \leq d(w,\lambda\tau y) \leq 2|v|/|w|.$$

Now $|\lambda\tau y| = |\lambda|\,|\tau y| \geq |\lambda|\,s\,|y| \geq |\lambda|\,s\varepsilon\,|v|$, so

$$|w| = |v + \lambda\tau y| \geq |\lambda\tau y| - |v| \geq (|\lambda|\,s\varepsilon - 1)|v|.$$

Indeed, since $|\lambda| \geq r$, we have $|\lambda|\,s\varepsilon - 1 \geq rs\varepsilon - 1 > 2/\varepsilon$, and hence $|w| > 2\,|v|/\varepsilon$. Consequently, $d(w,I) \leq 2\,|v|/|w| < \varepsilon$ and $w \in P$, as required. □

Step 4. *Completion of the proof.*

Proof. Let $c \in C$ with $|c| \geq r$, let $t = 1 + c\tau$ and write $T = \langle t\rangle$. Since $t^n = 1 + nc\tau$, we see that $t^n = 1$ if and only if $n = 0$, and hence T is infinite cyclic. Furthermore, if $n \neq 0$, then $|nc| \geq |c| \geq r$, so Step 3 implies that $t^nQ \subseteq P$. In other words, $(T \setminus 1)Q \subseteq P$. We also observed in Steps 1 and 2 that $\big(G \setminus (G \cap C^\bullet)\big)P \subseteq Q$ and that $P \cap Q = \emptyset$. In particular, since $|T| > 2$, we conclude from Lemma 1.5 that $\langle G,T\rangle/(G \cap C^\bullet) \cong \big(G/(G \cap C^\bullet)\big) * T$, and the theorem is proved. □

Next we show that the proof of Theorem 1.1 contains enough information to compute specific bounds when τ has rank 1. For this, we first indicate how to compute the distance between a nonzero vector and a subspace of the vector space. Again, we assume that V is a finite-dimensional complex vector space having a Hermitian inner product $(\ ,\ )$.

Lemma 2.3. *Let $0 \neq v \in V$ and let A be a nonzero subspace of V.*

(i) *If $(v,A) = 0$, then $d(v,A)^2 = 2$.*

(ii) *If $(v,A) \neq 0$, write $B = A \cap v^\perp$, so that B is a subspace of A of codimension 1, and let $A = Ca \dotplus B$, where $Ca = A \cap B^\perp$. Then*

$$d(v,A)^2 = 2\left(1 - \frac{|(v,a)|}{|v|\,|a|}\right).$$

Proof. We can assume that $|v| = 1$.

(i) If $(v, A) = 0$ and $x \in A \cap S$, then $d(v,x)^2 = |v-x|^2 = |v|^2 + |x|^2 = 2$ since v and x are perpendicular.

(ii) We can clearly assume that $|a| = 1$. If $x \in A$ with $|x| = 1$, then $x = \lambda a + b$ with $\lambda \in C$, $b \in B$ and with $1 = |x|^2 = |\lambda|^2 + |b|^2$. Next, we have

$$\begin{aligned} d(v,x)^2 &= |v-x|^2 = |v|^2 + |x|^2 - (v,x) - (x,v) \\ &= 2 - (v, \lambda a) - (\lambda a, v) = 2 - 2\,\Re\mathrm{e}\big(\bar{\lambda}(v,a)\big). \end{aligned}$$

This is clearly minimized when $|\lambda| = 1$ and when $\bar{\lambda}(v,a)$ is real and positive. Thus $\lambda = (v,a)/|(v,a)|$ and $d(v,A)^2 = 2 - 2|(v,a)|$. □

With this, we can prove

Lemma 2.4. *Let $v, \alpha \in V \setminus 0$ and let $\tau\colon V \to V$ be the linear transformation given by $\tau(x) = (x, \alpha)v$ for all $x \in V$.*

(i) *If $K = \ker \tau$ and $0 \neq w \in V$, then $d(w, K) \geq |(w,\alpha)|/(|w|\,|\alpha|)$.*

(ii) $\|\tau\| = |\alpha|\,|v|$.

Proof. Since $\tau(x) = (x, \alpha/|\alpha|)\,|\alpha| v$, it suffices to assume that $|\alpha| = 1$. Furthermore, for part (i), we may assume that $|w| = 1$.

(i) If $(w, K) = 0$, then $d(w,K) = \sqrt{2} > |w||\alpha| \geq |(w,\alpha)|$ by the first part of the previous lemma. Thus we can suppose that $(w,K) \neq 0$, and we use the notation of the second part above. Since $K = \alpha^{\perp}$, we see that $B = \alpha^{\perp} \cap w^{\perp}$, and note that $a = w - (w,\alpha)\alpha \in K$. Moreover, $(a, K) = (w, K) \neq 0$, so $a \neq 0$, and it is clear that $a \perp B$. Thus Lemma 2.3(ii) implies that $d(w,K)^2 = 2 - 2|(w,a)|/|a|$. Now

$$(w,a) = (w,w) - |(w,\alpha)|^2 = 1 - |(w,\alpha)|^2,$$

and

$$|a|^2 = |w|^2 + |(w,\alpha)|^2 - 2|(w,\alpha)|^2 = 1 - |(w,\alpha)|^2.$$

It therefore follows that

$$d(w,K)^2 = 2 - 2\sqrt{1 - |(w,\alpha)|^2} \geq |(w,\alpha)|^2,$$

so $d(w,K) \geq |(w,\alpha)|$, as required.

(ii) Observe that $V = C\alpha \dotplus K$ is an orthogonal direct sum of subspaces. In particular, if $x \in V \setminus K$, then $x = \lambda\alpha + k$ for some $0 \neq \lambda \in C$ and $k \in K$, and hence $|x|^2 = |\lambda|^2|\alpha|^2 + |k|^2 = |\lambda|^2 + |k|^2$. Furthermore, $\tau(x) = \tau(\lambda\alpha) = \lambda(\alpha,\alpha)v = \lambda v$. Thus

$$\frac{|\tau(x)|}{|x|} = \frac{|\lambda|\,|v|}{\sqrt{|\lambda|^2 + |k|^2}} = \frac{|v|}{\sqrt{1 + |k|^2/|\lambda|^2}} \leq |v|,$$

and it is clear that $\|\tau\| = |v|$. □

We close this section with the

Proof of Corollary 1.2. We follow the proof of Theorem 1.1 and use its notation. Furthermore, since $\tau\colon V \to V$ has rank 1 with $0 \neq v \in I = \operatorname{im}\tau$, we can assume that $\tau(x) = (x,\alpha)v$ for some fixed vector $0 \neq \alpha \in V$. Of course, $K = \ker\tau = \alpha^{\perp}$.

Note that, by Lemma 2.2(i), we have $d(gI, K) = d(Cgv, K) = d(gv, K)$ for any $g \in G$. Furthermore, by Lemma 2.4(i), we have

$$d(gv, K) \geq |(gv,\alpha)|/(|gv|\,|\alpha|) = |\tau(gv)|/(|gv|\,|v|\,|\alpha|).$$

Thus, by definition, we can take ε to be

$$\varepsilon = \frac{1}{3}\min\left\{ \frac{|\tau(gv)|}{|gv|\,|v|\,|\alpha|} \;\middle|\; g \in G \setminus (G \cap C^\bullet) \right\} = \frac{m}{3\,|v|\,|\alpha|},$$

where m is the minimum value of $|\tau(gv)|/|gv|$ over all $g \in G \setminus (G \cap C^\bullet)$.

Next, observe that $V = K \dotplus C\alpha$ and that τ restricted to $C\alpha$ determines an isomorphism $\sigma\colon C\alpha \to I$ given by $\lambda\alpha \mapsto \lambda|\alpha|^2 v$. Thus $\sigma^{-1}\colon \mu v \mapsto \mu\alpha/|\alpha|^2$ for all $\mu \in C$ and hence $s^{-1} = \|\sigma^{-1}\| = 1/(|v|\,|\alpha|)$. Finally, we set

$$r = \frac{3}{s\varepsilon^2} = \frac{27\,|v|\,|\alpha|}{m^2} = \frac{27\,\|\tau\|}{m^2},$$

by Lemma 2.4(ii). But r is the lower bound for the size of the complex numbers c given by the proof of Theorem 1.1, so the result follows. □

3. Proof of Theorem 1.3

In this section, we quickly prove Theorem 1.3 and its corollary. Then we discuss two examples of interest. We start with

Proposition 3.1. *Let R be a subring of the complex numbers C and let G be a subgroup of $\mathrm{GL}_n(R)$ with $|G : (G \cap R^\bullet)| < \infty$. If $n \geq 2$, then there exists a transvection $1 + \tau \in \mathrm{SL}_n(Z) \subseteq \mathrm{SL}_n(R)$ such that*

$$\langle G, 1 + t\tau\rangle/(G \cap R^\bullet) \cong \big(G/(G \cap R^\bullet)\big) * \langle 1 + t\tau\rangle$$

for all sufficiently large $t \in R$ (measured in C).

Proof. Of course, $\mathrm{GL}_n(R) \subseteq \mathrm{GL}_n(C)$, and we let $\mathrm{GL}_n(C)$ act on the C-vector space $V \cong C^n$. Furthermore, let $V' \cong Q^n$ embed naturally in V, where Q is the field of rational numbers. For each $g \in G \setminus (G \cap R^\bullet)$, the eigenspaces for g in V, with eigenvalues in C, are finitely many proper subspaces of V. Moreover, it is clear that all group elements in the coset $g(G \cap R^\bullet)$ have the same eigenspaces, but with possibly different eigenvalues. Thus since $|G : (G \cap R^\bullet)| < \infty$, the eigenspaces for all elements $g \in G \setminus (G \cap R^\bullet)$ constitute just finitely many proper subspaces of V, say these are $V_1, V_2, \ldots, V_k$. In particular, since $CV' = V$, the intersections $V_i' = V_i \cap V'$ are finitely many proper Q-subspaces of V'. Thus, since Q is an infinite field, we have $\bigcup_{i=1}^k V_i' \neq V'$, and hence we can choose $v \in V'$ not in any of these proper subspaces. It follows that $gv \notin Cv$ for all $g \in G \setminus (G \cap R^\bullet)$. Indeed, since $g(G \cap R^\bullet)Cv = Cgv$, we obtain just finitely many 1-dimensional subspaces of V in this manner, and they are all distinct from Cv.

Note that the images of these lines in V/Cv determine finitely many subspaces $L_1/Cv, L_2/Cv, \ldots, L_\ell/Cv$, with $\dim_C L_i = 2$. Now consider the vector space dual W of V, and let $W' = \{\lambda \in W \mid \lambda(V') \subseteq Q\}$ be the rational subspace naturally embedded in W. If $\widetilde{W} = \{\lambda \in W \mid \lambda(Cv) = 0\}$, then each $\widetilde{W}_i = \{\lambda \in W \mid \lambda(L_i) = 0\}$ is a proper subspace of $\widetilde{W}$, so it follows easily as above that there exists a linear functional $f \in W'$ with $f(Cv) = 0$, but with $f(Cgv) \neq 0$ for all $g \in G \setminus (G \cap R^\bullet)$. Now define $\tau\colon V \to V$ by $\tau(x) = f(x)v$ for all $x \in V$. Obviously, τ has rank 1 with image $I = Cv$ and with $\ker\tau = \ker f = K$ of codimension 1 in V. Furthermore, by the definitions of V' and W', τ corresponds to a matrix with entries in Q. In particular, we can multiply τ by a nonzero element of Z to clear denominators. This new τ corresponds to a Z-matrix, but with the same image I and kernel K and, since $f(v) = 0$, we have $I \subseteq K$ and hence $\tau^2 = 0$. On the other hand, since

$f(gv) \neq 0$ and since I is 1-dimensional, we have $gI \cap K = Cgv \cap K = 0$ for all $g \in G \setminus (G \cap R^\bullet)$, and therefore Theorem 1.1 yields the result. □

Note that, in the above argument, if $V_i' = V_i \cap V' \neq 0$ and if V_i is an eigenspace for $g \in G \subseteq \mathrm{GL}_n(R)$, then the corresponding eigenvalue is certainly contained in F, the field of fractions of R. With Proposition 3.1 in hand, Theorem 1.3 is now essentially obvious. There is just one small observation that needs to be made.

Proof of Theorem 1.3. Since G is finite, there exists a finitely generated subgroup H of $\mathrm{GL}_n(R)$ such that $H/(H \cap R^\bullet) = G$. We can now assume that R is generated by the finitely many entries in the matrices representing these finitely many generators of H and in the matrices of their inverses. In other words, R is a countable characteristic 0 domain, and hence it can be embedded in the complex numbers C. By Proposition 3.1, there exists a transvection $1 + \tau \in \mathrm{SL}_n(Z) \subseteq \mathrm{SL}_n(R)$ such that

$$\langle H, 1 + t\tau\rangle/(H \cap R^\bullet) \cong \big(H/(H \cap R^\bullet)\big) * \langle 1 + t\tau\rangle = G * \langle 1 + t\tau\rangle$$

for all sufficiently large $t \in R$. Furthermore, note that $\langle H, 1 + t\tau\rangle \cap R^\bullet = H \cap R^\bullet$. Indeed, this is obvious if $G = 1$, and it is immediate when $G \neq 1$ since $G * \langle 1 + t\tau\rangle$ has trivial center. This completes the proof. □

In a real sense, the final argument above using the center of the free product is unnecessary. A close look at the proof of Theorem 1.1 shows that the ping-pong lemma is applied to the action of the group $\langle G, 1 + c\tau\rangle$ on certain projective subsets of V. Furthermore, the proof of that lemma not only shows that $\langle G, 1+c\tau\rangle/(G \cap C^\bullet)$ is a free product, but also that it acts faithfully when permuting the sets P and Q. As a consequence, $\langle G, 1 + c\tau\rangle/(G \cap C^\bullet)$ acts faithfully on the projective space of V.

Next, we have

Proof of Corollary 1.4. Let $^-\colon \mathrm{GL}_n(R) \to \mathrm{PGL}_n(R)$ be the natural map. Since $\overline{G}$ is finite, Theorem 1.3 implies that there exists a transvection $1+\tau \in \mathrm{SL}_n(Z) \subseteq \mathrm{SL}_n(R)$ such that $\langle \overline{G}, \overline{T}\rangle \cong \overline{G} * \overline{T}$, where $T = \langle 1 + \tau\rangle$. But $\overline{G} \cong G$ and $\overline{T} \cong T$, so we have $\langle G, T\rangle \cong G * T$, as required. □

We close this paper by considering two examples of interest. The first one comes from [GM].

Example 3.2. Let V be a complex vector space with basis $\{v_0, v_1, \ldots, v_n\}$, and let $G \subseteq \mathrm{GL}(V)$ be a subgroup of order $n+1$ that regularly permutes the basis vectors. Suppose $\tau\colon V \to V$ is defined by $\tau(v_i) = a_i v_0$ with $a_0 = 0$, but with $0 \neq a_i \in C$ for all $i = 1, 2, \ldots, n$. Then $\langle G, 1 + c\tau\rangle = G * \langle 1 + c\tau\rangle$ for all complex numbers c that satisfy

$$|c| \geq \frac{27\left(|a_1|^2 + |a_2|^2 + \cdots + |a_n|^2\right)^{1/2}}{\min\{|a_1|^2, |a_2|^2, \ldots, |a_n|^2\}}.$$

Proof. Let the Hermitian inner product $(\ ,\ )$ be defined on V so that $\{v_0, v_1, \ldots, v_n\}$ is an orthonormal basis. Then certainly G acts as unitary operators on V. Furthermore, if we set $\alpha = \bar{a}_1 v_1 + \bar{a}_2 v_2 + \cdots + \bar{a}_n v_n$, then $\tau(x) = (x, \alpha) v_0$ for all $x \in V$. Since $G \cap C^\bullet = 1$, Corollary 1.2 implies that $\langle G, 1 + c\tau\rangle = G * \langle 1 + c\tau\rangle$ if c is a complex number with $|c| \geq 27\|\tau\|/m^2$, where $m = \min\{|\tau(gv_0)|/|gv_0| \mid g \in G \setminus 1\}$. By Lemma 2.4(ii), $\|\tau\| = |\alpha|\,|v_0| = (|a_1|^2 + |a_2|^2 + \cdots + |a_n|^2)^{1/2}$. Furthermore, if $g \in G \setminus 1$, then $gv_0 = v_i$ for some $i \neq 0$, and all such v_i occur. Thus, since

$\tau(gv_0) = \tau(v_i) = a_i v_0$, it follows that $m = \min\{|a_i| \mid i \neq 0\}$ and, in particular, we have $m^2 = \min\{|a_i|^2 \mid i \neq 0\}$. □

In a recent unpublished note, Dan Goldstein showed that if p is an odd prime and ζ is a primitive complex pth root of unity, then $\mathrm{SL}_2(Q[\zeta + \zeta^{-1}])$ contains the free product $G_1 * G_2$ of two cyclic groups of order p. Our final example is motivated by this result.

Example 3.3. Let p be an odd prime and let ζ be a complex primitive pth root of unity. Let

$$g = \begin{pmatrix} 0 & 1 \\ -1 & \zeta + \zeta^{-1} \end{pmatrix} \qquad \text{and} \qquad h = \begin{pmatrix} -1 & 1 \\ -1 & 1 \end{pmatrix}$$

be 2×2 matrices over the ring $R = Z[\zeta + \zeta^{-1}]$. If $r \in R$ with $|r| \geq p^3/2$, then $\mathrm{SL}_2(R)$ contains the free product $G * T$, where $G = \langle g \rangle$ is cyclic of order p and $T = \langle 1 + rh \rangle$ is infinite cyclic.

Proof. We work in the larger ring $Z[\zeta]$. If

$$\ell = \begin{pmatrix} 1 & 1 \\ \zeta^{-1} & \zeta \end{pmatrix}, \text{ then } \ell^{-1} g \ell = \begin{pmatrix} \zeta^{-1} & 0 \\ 0 & \zeta \end{pmatrix} \text{ and } \ell^{-1} h \ell = \mu \begin{pmatrix} 1 & -\zeta \\ \zeta^{-1} & -1 \end{pmatrix},$$

where $\mu = (1-\zeta)/(1+\zeta)$. Thus, it suffices to assume that V has basis $\{v_1, v_2\}$ with $gv_1 = \zeta^{-1} v_1$ and $gv_2 = \zeta v_2$. Furthermore, if $v = \zeta^{1/2} v_1 + \zeta^{-1/2} v_2$, then $h = \mu\tau$ where $\tau(v_1) = v_1 + \zeta^{-1} v_2 = \zeta^{-1/2} v$ and $\tau(v_2) = -(\zeta v_1 + v_2) = -\zeta^{1/2} v$. Now assume that $(\ ,\ )$ is an inner product on V with v_1 and v_2 orthonormal vectors. Then g is a unitary operator on V and $\tau(x) = (x, \alpha)v$, where $\alpha = \zeta^{1/2} v_1 - \zeta^{-1/2} v_2$. By Lemma 2.4(ii), $\|\tau\| = |\alpha|\,|v| = 2$, and $\tau(g^i v) = (g^i v, \alpha)v = (\zeta^{-i} - \zeta^i)v$. Thus $|\tau(g^i v)|/|g^i v| = |\zeta^i - \zeta^{-i}| = |2\,\Im\mathrm{m}(\zeta^i)|$, and hence

$$m = \min\left\{ \frac{|\tau(g^i v)|}{|g^i v|} \,\middle|\, i = 1, 2, \ldots, p-1 \right\} = 2\sin(\pi/p).$$

By Corollary 1.2, if c is a complex number with $|c| \geq 27\,\|\tau\|/m^2 = 27/(2\sin^2(\pi/p))$, then $\langle G, 1 + c\tau \rangle \cong G * \langle 1 + c\tau \rangle$.

In particular, if $r \in R$ with $|r\mu| \geq 27/(2\sin^2(\pi/p))$, then $\langle G, 1{+}rh \rangle \cong G{*}\langle 1{+}rh \rangle$. Finally, observe that $\mu = (1-\zeta)/(1+\zeta) = (\zeta^{-1/2} - \zeta^{1/2})/(\zeta^{-1/2} + \zeta^{1/2})$, so $|\mu| = |\Im\mathrm{m}(\zeta^{1/2})|/|\Re\mathrm{e}(\zeta^{1/2})|$. In particular, the smallest value for $|\mu|$ over all embeddings of $Z[\zeta]$ in C is $\tan(\pi/p)$, and hence we need $|r| \geq (27\cos(\pi/p))/(2\sin^3(\pi/p))$. Since the latter trigonometric expression is easily seen to be smaller than $p^3/2$, the condition $|r| \geq p^3/2$ guarantees that $\langle G, 1 + rh \rangle$ is a free product. □

Note that no nonidentity element of the subgroup $G = \langle g \rangle \subseteq \mathrm{SL}_2(R)$ can have an eigenvalue in $F = Q[\zeta + \zeta^{-1}]$. Thus, in view of the proof of Proposition 3.1 and the remarks that follow it, we could take h in the above example to be any nonzero Z-matrix of square 0. For instance, we could take h to be either of the matrix units $e_{1,2}$ or $e_{2,1}$. Of course, the bound on r would necessarily change. Our choice of the particular h in Example 3.3 is therefore somewhat random, but it does seem to be more symmetrically placed with respect to the matrix g. Furthermore, the same h can be used for $p = 2$ if we take $g = \mathrm{diag}(1, -1) \in \mathrm{GL}_2(Z)$.

Acknowledgement

The author thanks Dan Goldstein for his helpful comments.

References

[GM] J. Z. Gonçalves and A. Mandel, *Free groups generated by transvections*, to appear.

[H] P. de la Harpe, *Topics in Geometric Group Theory*, Chicago Lectures in Mathematics, Univ. of Chicago Press, Chicago, 2000. MR **2001i:**20081

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
E-mail address: `passman@math.wisc.edu`