Available at
www.ElsevierMathematics.com
POWERED BY SCIENCE DIRECT
Journal of Algebra 268 (2003) 286–289
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

Residual properties of free products of finite groups

Martin W. Liebeck [a,*] and Aner Shalev [b,1]

[a] Department of Mathematics, Imperial College, London SW7 2BZ, England, UK
[b] Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel

Received 14 February 2002

Communicated by Efim Zelmanov

Abstract

Using a probabilistic approach we establish a new residual property of free products of finite groups.

1. Introduction

A group G is said to be residually (in) a set S of groups if the kernels of all epimorphisms from G to members of S intersect trivially. In this note we consider the following question: given finite groups A and B, for which infinite collections S of finite simple groups is the free product $A*B$ residually S? When S consists of alternating groups a definitive answer is given in [4]. In [1, Theorem 1.2] we proved that if A, B are nontrivial and not both 2-groups, and S is a collection of finite simple classical groups of unbounded ranks, then $A*B$ is residually S. In this paper we improve this result as follows:

Theorem. *Let A, B be nontrivial finite groups, not both 2-groups. Then there exists an integer $r=r(A,B)$ depending only on A, B, such that if S is an infinite collection of finite simple classical groups, all of rank at least r, then the free product $A*B$ is residually S.*

Note that some assumption on the groups in S is needed in order to make A and B embeddable in such groups.

* Corresponding author.
E-mail address: m.liebeck@ic.ac.uk (M.W. Liebeck).
1 The author acknowledges the support of an EPSRC Visiting Fellowship at Imperial College London, and a grant from the Israel Science Foundation.

0021-8693/$ – see front matter
doi:10.1016/S0021-8693(03)00338-7

An immediate consequence of the Theorem is that for any nontrivial finite group A, there exists $r = r(A)$ such that if S is an infinite collection of classical groups of rank at least $r(A)$, then $A * \mathbb{Z}$ is residually S. This improves [1, Theorem 1.3(iii)].

The proof uses probabilistic methods as in [1], combined with added ingredients supplied by [2,3,5], where results on the linearity of some free products are established.

2. Proof of the Theorem

We begin with a definition taken from [1]. If A is a finite group, k is a field, and V is a kA-module, we say that V is a *virtually free* kA-module if $V \downarrow A = F \oplus U$, where $F \neq 0$ is free and $\dim U < 2|A| + 4$; the corresponding representation $A \to GL(V)$ is also said to be virtually free. And if W is a vector space over k and $A \leqslant GL(W)$, we say A is embedded *virtually freely* in $GL(W)$ if W is virtually free as a kA-module. In such a situation, if $Z = Z(GL(W))$, then the image of A in $PGL(W)$ is $AZ/Z \cong A$, and we say also that A is embedded virtually freely in $PGL(W)$. If $\alpha : A \to GL(W)$ is the corresponding representation, we shall abuse notation slightly by using α to denote both maps $A \to GL(W)$ and $A \to PGL(W)$. Note that if $g \in GL(W)$, then the map $\alpha^g : a \to \alpha(a)^g$ $(a \in A)$ is also a virtually free embedding.

As observed in [1], any finite group A can be embedded virtually freely in any classical simple group X with natural module V of dimension $n \geqslant 2|A| + 4$ over $\mathbb{F}_q$. Here is an explicit such embedding. If $X = PSL(V)$, write $\dim V = m|A| + k$ with $1 \leqslant k \leqslant |A|$, and embed A freely in the subgroup $GL_{m|A|}(q)$ of X. And when $X \neq PSL(V)$, write $\dim V = 2m|A| + k$ with $4 \leqslant k < 2|A| + 4$; then A embeds freely in $GL_{m|A|}(q)$, which is a subgroup of X, and this yields a virtually free embedding of A in X.

Let A, B be nontrivial finite groups, not both 2-groups. By [1, Theorem 2.3], there is an integer $r(A, B) \geqslant \max(2|A| + 4, 2|B| + 4)$ such that if X is a finite classical simple group of rank at least $r(A, B)$, and A, B are embedded virtually freely in X, then for randomly chosen $t \in X$, the probability that $\langle tAt^{-1}, B\rangle = X$ tends to 1 as $|X| \to \infty$.

Let S be an infinite collection of finite simple classical groups, all of rank at least $r(A, B)$. Since the result is proved in [1, Theorem 1.2] in the case where S contains groups of unbounded ranks, we may assume that the ranks of the classical groups in S are bounded, and indeed that S consists of groups of the form $X(q)$, simple groups of fixed Lie type X over fields $\mathbb{F}_q$, where $q \to \infty$. Such groups $X(q)$ are of the form $(G_{\sigma_q})'$, where $G = G(K)$ is an adjoint simple algebraic group of fixed type over K, the algebraic closure of $\mathbb{F}_p(T)$ (T an indeterminate), σ_q is a Frobenius q-power morphism and q is a power of p. Note that as $q \to \infty$ the prime p may vary.

Fix q with $X(q) = (G_{\sigma_q})' \in S$, and fix virtually free embeddings $\alpha : A \to X(q)$ and $\beta : B \to X(q)$ as explicitly described above. For $t \in G$, define $\psi_t : A * B \to G$ to be the homomorphism sending $a \to t\alpha(a)t^{-1}$ for $a \in A$ and $b \to \beta(b)$ for $b \in B$.

Claim. *There exists $t \in G$ for which ψ_t is injective.*

Proof. We first handle the case where $G = PSL_n(K)$. We aim to apply the argument of [3, Proposition 1.3]. To do this, we need first to argue that we can choose the virtually free embeddings α, β to have the property that the matrix entries $\alpha(a)_{n1} \neq 0$ and $\beta(b)_{1n} \neq 0$ for all $1 \neq a \in A$, $1 \neq b \in B$. This will be achieved by replacing α, β by suitable conjugates α^g, β^g with $g \in G$.

Let $1 \neq a \in A$ and $\alpha(a) = (a_{ij})$. If there exist i, j with $i \neq j$ and $a_{ij} \neq 0$, choose an even permutation sending $i \to n$, $j \to 1$; setting P to be the corresponding permutation matrix, we have $\alpha^P(a)_{n1} \neq 0$. If no such i, j exist then (a_{ij}) is diagonal, and is non-scalar as α is virtually free; applying a permutation again, we may take $a_{11} \neq a_{nn}$, and now setting $Q = I + E_{n1}$ we have $\alpha^Q(a)_{n1} \neq 0$.

This shows that for each $1 \neq a \in A$,

$$V_a = \left\{g \in G\colon\ \alpha^g(a)_{n1} = 0\right\}$$

is a proper subvariety of G. Likewise, so is $U_b = \{g \in G\colon\ \beta^g(b)_{1n} = 0\}$ for $1 \neq b \in B$. Since G is not a finite union of proper subvarieties, we can choose $g \in G$ not lying in any V_a or U_b, and then we have our desired α^g, β^g, with which we replace α, β.

At this point, the argument of the proof of [3, 1.3] shows that if $t \in G$ is the image of the matrix $\mathrm{diag}(1, T, T^2, \ldots, T^{n-1})$, then ψ_t is injective. This proves the claim for $G = PSL_n(K)$.

Now suppose $G \neq PSL_n(K)$. From the description of α and β, we may take it that there is a subgroup $GL_m(q)$ of $X(q)$ containing the images of α and β, and this $GL_m(q)$ lies in a subgroup $GL_m(K)$ of G. By the $PSL_n(K)$ case, there exists $t \in GL_m(K)$ such that ψ_t is injective. This completes the proof of Claim. □

Let $1 \neq w \in A * B$, and define

$$V_w = \left\{t \in G\colon\ \psi_t(w) = 1\right\},$$

a subvariety of G. By Claim, V_w is proper in G. Also V_w is σ_q-invariant. By [1, 5.6], there is a constant $c = c(w)$ such that $|(V_w)_{\sigma_q}| < cq^{\dim V_w}$. We have $\dim V_w < \dim G$, and from the order formulae for simple groups, $|X(q)| < c' q^{\dim G}$ for some absolute constant c'. It follows that

$$\frac{|\{t \in X(q)\colon\ \psi_t(w) \neq 1\}|}{|X(q)|} \geqslant 1 - c_1 q^{\dim V_w - \dim G} \geqslant 1 - c_2 q^{-1} \to 1 \quad \text{as } q \to \infty. \tag{1}$$

As discussed above, [1, Theorem 2.3] implies that

$$\frac{|\{t \in X(q)\colon\ \langle t\alpha(A)t^{-1}, \beta(B)\rangle = X(q)\}|}{|X(q)|} \to 1 \quad \text{as } q \to \infty. \tag{2}$$

From (1) and (2), it follows that if q is large enough, there exists $t \in X(q)$ such that $\langle t\alpha(A)t^{-1}, \beta(B)\rangle = X(q)$ and $\psi_t(w) \neq 1$. This shows that $A * B$ is residually S, and the proof of the Theorem is complete.

References

[1] M.W. Liebeck, A. Shalev, Residual properties of the modular group and other free products, J. Algebra 268 (2003) 264–285.

[2] V.I. Nisnevic, Über Gruppen die durch Matrizen über einem kommutativen Feld isomorph darstellbar sind, Mat. Sb. 8 (1940) 395–403.

[3] P.B. Shalen, Linear representations of certain amalgamated products, J. Pure Appl. Algebra 15 (1979) 187–197.

[4] M.C. Tamburini, J.S. Wilson, A residual property of free products, Math. Z. 186 (1984) 525–530.

[5] B.A.F. Wehrfritz, Generalized free products of linear groups, Proc. London Math. Soc. 27 (1973) 402–424.