L'Enseignement Mathématique (2) 56 (2010), 173–185

FREE SUBGROUPS IN GROUPS WITH FEW RELATORS

by John S. WILSON

1. INTRODUCTION

In [11], we proved the following result:

THEOREM 1. *Let G be an abstract (resp. pro-p) group which has a presentation with n generators $x_1, \dots, x_n$ and m relators, where $m < n$, and let Y be any generating set for G. Then there are $n - m$ elements of Y that freely generate a free abstract (resp. pro-p) group.*

The Freiheitssatz proved by Magnus in [3] in 1930 is essentially the special case of Theorem 1 for abstract groups with $Y = \{x_1, \dots, x_n\}$ and $m = 1$. In [5] and [6] Romanovskiĭ proved the case of Theorem 1 in which $Y = \{x_1, \dots, x_n\}$. The proof of the general case in [11] was indirect, relying on Romanovskiĭ's result in [6]. In [9] Romanovskiĭ and the author gave a direct proof of a more general result concerning quotients of a free product of n groups, for the case of abstract groups. Our first object here is to give a much simpler proof of Theorem 1 in the abstract case and to indicate the modifications required for the case of pro-p groups. We shall also prove a result for pro-p groups that is similar in spirit to the main result of [9]; this result has the following consequence.

THEOREM 2. *Let G be a finitely generated pro-p group generated by a family $\mathcal{A}$ of n finitely generated pro-p subgroups each having $\mathbf{Z}_p$ as an image, and suppose that the kernel R of the natural map from the free pro-p product F of the groups in $\mathcal{A}$ to G is generated (as a closed normal subgroup) by m elements, where $m < n$. Let $\mathcal{B}$ be a family of subgroups of G that generate G. Then $\bigcup\{B \mid B \in \mathcal{B}\}$ contains $n - m$ elements that freely generate a free pro-p group.*

In particular, either $|\mathcal{B}| \geqslant n - m$ or some subgroup in $\mathcal{B}$ contains a non-abelian free pro-p subgroup.

ACKNOWLEDGEMENTS. The author would like to thank the Forschungsinstitut für Mathematik at ETH, Zürich for its generous hospitality and support during the writing of this paper. He is also grateful to Pierre de la Harpe for helpful comments on an earlier version.

2. PROOF OF THEOREM 1

Theorem 1 is reminiscent of the Steinitz exchange lemma from linear algebra; indeed, it is a precise analogue of the statement that if V is an n-dimensional vector space over a field Q and R is a subspace of dimension at most m, then any set Y such that $R \cup Y$ spans V contains $n - m$ elements that are linearly independent modulo R. Most earlier proofs of results like Theorem 1 have relied on

(a) the above statement from linear algebra, but with V a right vector space over a skew-field Q,

(b) the Magnus embedding, and

(c) a rather complicated induction argument.

In the proof below, (c) is eliminated. We begin therefore with the ingredient (b).

Our notation for conjugates and commutators in a group G is as follows: we write $a^b = b^{-1}ab$ and $[a,b] = a^{-1}b^{-1}ab$. We shall write N' for the *derived group* of a group N; in the case of pro-p groups, N' refers of course to the *closure* of the abstract group generated by all commutators.

2.1 THE MAGNUS EMBEDDING

Let H be a group and M a right $\mathbf{Z}H$-module. It is convenient to write elements of the split extension $G = H \ltimes M$ as matrices

$$\begin{pmatrix} h & 0 \\ m & 1 \end{pmatrix} \qquad (h \in H,\ m \in M).$$

Thus matrix multiplication

$$\begin{pmatrix} h_1 & 0 \\ m_1 & 1 \end{pmatrix} \begin{pmatrix} h_2 & 0 \\ m_2 & 1 \end{pmatrix} = \begin{pmatrix} h_1h_2 & 0 \\ m_1h_2 + m_2 & 1 \end{pmatrix}$$

reflects the fact that $(h_1m_1)(h_2m_2) = (h_1h_2)(m_1^{h_2}m_2)$. We may regard M as a $\mathbf{Z}G$-module, and then the map δ taking $g \in G$ to its $(2,1)$-entry is a *derivation*, i.e. $\delta(g_1g_2) = (\delta g_1)g_2 + \delta g_2$ for all $g_1,\, g_2 \in G$. The *Magnus embedding* for abstract groups is the map j from F/R' in (b), (c) below.

LEMMA 1. *Let R be a normal subgroup of the free group F with basis $\{x_1, \dots, x_n\}$, and let $H = F/R$. Let M be a $\mathbf{Z}H$-module and $t_1, \dots, t_n \in M$.*

(a) *The assignment*

$$x_i \mapsto \begin{pmatrix} x_iR & 0 \\ t_i & 1 \end{pmatrix}$$

determines a homomorphism

$$\mu\colon F \to \begin{pmatrix} H & 0 \\ M & 1 \end{pmatrix}.$$

(b) $R' \leqslant \ker \mu \leqslant R$; *let j be the map from F/R' induced by μ.*

(c) *If M is the free $\mathbf{Z}H$-module with basis $\{t_1, \dots, t_n\}$ then j is injective.*

Proof. Assertion (a) is clear, and so is (b) since the image of R under μ is abelian. The following proof of (c), included for the reader's convenience, is due to Romanovskiĭ.

There is certainly an embedding θ of F/R' in a group of the form

$$\begin{pmatrix} H & 0 \\ N & 1 \end{pmatrix}$$

for a $\mathbf{Z}H$-module N. Indeed, we can take for N the abelian group B of all functions $b\colon H \to R/R'$, which is a right $\mathbf{Z}H$-module with action defined by $(bh)(x) = b(xh^{-1})$ for $b \in B$, $h \in H$, $x \in H$; since the split extension of B by H is the unrestricted standard *wreath product* $R/R' \,\overline{\mathrm{wr}}\, F/R$, the existence of a suitable map θ follows from the Kaloujnine–Krasner theorem ([1]; see also e.g. [10, Theorem 4.4.1]). Explicitly, θ can be defined as follows. Choose a set-theoretic section $\sigma\colon F/R \to F/R'$ to the canonical projection $q\colon F/R' \to F/R$ (that is, a function such that its composite with q is the identity map on F/R), and for each $fR' \in F/R'$ define $\delta(fR') \in B$ by

$$(\delta(fR'))(uR) = \sigma(uf^{-1}R) \cdot fR' \cdot (\sigma(uR))^{-1} \qquad \text{for all } uR \in F/R\,.$$

Simple calculations show that (with B written multiplicatively) we have $\delta(\bar{f}_1\bar{f}_2) = (\delta\bar{f}_1)^{\bar{f}_2}(\delta\bar{f}_2)$ for all $\bar{f}_1, \bar{f}_2 \in F/R'$ and also that if $\bar{f} \in R/R'$ and $\delta\bar{f}$ is the identity element of B then $\bar{f}$ is the identity element of R/R'. It follows immediately that the map θ defined by

$$\theta(fR') = \begin{pmatrix} fR & 0 \\ \delta(fR') & 1 \end{pmatrix} \in \begin{pmatrix} H & 0 \\ N & 1 \end{pmatrix}$$

is an injective homomorphism.

To prove (c) it suffices now to show that the diagram

$$\begin{array}{ccccc} F & \longrightarrow & F/R' & \xrightarrow{\ \theta\ } & \begin{pmatrix} H & 0 \\ N & 1 \end{pmatrix} \\ & & {\scriptstyle j}\searrow & & \nearrow{\scriptstyle \bar{\theta}} \\ & & & \begin{pmatrix} H & 0 \\ M & 1 \end{pmatrix} & \end{array}$$

can be completed with a map $\bar{\theta}$. Define $v_i \in N$ by

$$\theta(x_iR') = \begin{pmatrix} x_iR & 0 \\ v_i & 1 \end{pmatrix},$$

and let $\kappa\colon M \to N$ be the $\mathbf{Z}H$-module homomorphism defined by $t_i \mapsto v_i$. Then the map

$$\begin{pmatrix} h & 0 \\ m & 1 \end{pmatrix} \longmapsto \begin{pmatrix} h & 0 \\ \kappa m & 1 \end{pmatrix}$$

has the required property.

LEMMA 2. *Let $\delta\colon H \to W$ be a derivation from a group H to a right H-module W. If $H = \langle Z \rangle$ then the subset δH lies in the $\mathbf{Z}H$-submodule W_1 generated by δZ.*

Proof. If δh_1, $\delta h_2 \in W_1$ then $\delta(h_1h_2^{-1}) = (\delta h_1)h_2^{-1} - (\delta h_2)h_2^{-1} \in W_1$.

2.2 Embedding of group rings in skew-fields

We recall that a group G is called *orderable* if it has a total order $\leqslant$ such that if a, $b \in G$ and $a \leqslant b$ then $xay \leqslant xby$ for all $x, y \in G$; the pair $(G, \leqslant)$ is then an *ordered group*. It is well known and easily checked that if $G = H \ltimes A$ is a split extension of ordered groups $(H, \leqslant_H)$, $(A, \leqslant_A)$, and if $1 \leqslant_A a \in A$ and $h \in H$ imply $1 \leqslant_A a^h$, then G becomes an ordered group with respect to the order defined as follows: $h_1a_1 \leqslant h_2a_2$ if and only if either $h_1 <_H h_2$, or $h_1 = h_2$ and $a_1 \leqslant_A a_2$. The following lemma is also no doubt well known.

Lemma 3. *Each group G has a unique normal subgroup K minimal such that G/K is orderable.*

Proof. Let $(K_\lambda)_{\lambda \in \Lambda}$ be the set of kernels of maps from G to orderable groups and set $K = \bigcap K_\lambda$. We fix an order on each group G/K_λ, and we may take the set Λ to be well ordered. Now we can define an order on G/K by writing $aK < bK$ if for some $\mu \in \Lambda$ we have $aK_\mu < bK_\mu$ and $aK_\lambda = bK_\lambda$ for all $\lambda < \mu$.

An *ordered skew-field* is a skew-field Q together with an order $\leqslant$ such that both Q under addition and the set $\{h \in Q \mid h > 0\}$ under multiplication are ordered groups with respect to $\leqslant$; denote the latter group by $U_+(Q)$.

We need the following result proved by B.H. Neumann [4].

Proposition 1. *Let H be an ordered group. Then $\mathbf{Z}H$ can be embedded in an ordered skew-field Q in such a way that the order on Q induces an embedding of H (as an ordered group) in $U_+(Q)$.*

A standard candidate for Q is the skew-field of formal expressions $q = \sum_{h \in H} \lambda_h h$ with $\lambda_h \in \mathbf{Q}$ for all $h \in H$ and with support $\{h \in H \mid \lambda_h \neq 0\}$ inversely well-ordered; then $U_+(Q)$ is the set of elements q such that $\lambda_m > 0$, where $m \in H$ is the greatest element of the support of q. For the details we refer to Neumann [4], or [2, §14 and Corollary 18.6]. (In fact Neumann works with the ring of formal expressions with well-ordered support, and his embedding of H in $U_+(Q)$ is order-reversing; an order-preserving embedding is obtained by composing the inversion map on H with this embedding.)

LEMMA 4. *Let H, Q be as above and let V be a finite-dimensional right vector space over Q; thus V is naturally a $\mathbf{Z}H$-module. Then the split extension $H \ltimes V$ is orderable.*

Proof. We may regard V as the space $Q^{(n)}$ of n-tuples of elements of Q. We define an order on V by writing $(x_1, \ldots, x_n) < (y_1, \ldots, y_n)$ if $y_i - x_i > 0$ for the first non-zero $y_i - x_i$. Thus if $0 < v \in V$ and $h \in H$ then $vh > 0$, and so the split extension is orderable from above.

2.3 PROOF OF THE THEOREM: ABSTRACT CASE

Let G be as in the statement of Theorem 1, and let F be free with basis $\{x_1, \ldots, x_n\}$. Thus the kernel R of the obvious map from F to G can be generated as a normal subgroup by elements $r_1, \ldots, r_m$, where $m < n$. Lemma 3 guarantees the existence of a smallest normal subgroup S of F with $R \leqslant S$ and F/S orderable. Write $\overline{G} = F/S$.

Let Q be an ordered skew-field containing $\mathbf{Z}\overline{G}$ as in Proposition 1. Let V be the right vector space over Q with basis $\{t_1, \ldots, t_n\}$, and let M be the $\mathbf{Z}\overline{G}$-submodule generated by $t_1, \ldots, t_n$; thus M is a free $\mathbf{Z}\overline{G}$-module with basis $\{t_1, \ldots, t_n\}$. Define

$$\theta\colon F \to \begin{pmatrix} \overline{G} & 0 \\ M & 1 \end{pmatrix} \quad \text{by} \quad x_i \mapsto \begin{pmatrix} x_i S & 0 \\ t_i & 1 \end{pmatrix}$$

and

$$\delta\colon F \to M \quad \text{by} \quad \theta f = \begin{pmatrix} fS & 0 \\ \delta f & 1 \end{pmatrix}.$$

Let U be the subspace of V spanned by $\{\delta r_1, \ldots, \delta r_m\}$, and write $W = V/U$, $r = \dim W$; so $r \geqslant n - m$. Let $\bar{\delta}$ be the map $f \mapsto U + \delta f$. Thus the set $\{\bar{\delta} x_1, \ldots, \bar{\delta} x_n\}$ spans W.

Consider the map

$$\varphi\colon \begin{pmatrix} \overline{G} & 0 \\ M & 1 \end{pmatrix} \to \begin{pmatrix} \overline{G} & 0 \\ (M+U)/U & 1 \end{pmatrix},$$

and let $\psi = \varphi\theta$. By Lemma 4, the codomain of ψ is orderable, and so $F/\ker\psi$ is orderable. But $\ker\psi \leqslant S$ and $r_1, \ldots, r_m \in \ker\psi$, and hence $\ker\psi = S$. Therefore ψ induces an injective map

$$j\colon \overline{G} \rightarrowtail \begin{pmatrix} \overline{G} & 0 \\ W & 1 \end{pmatrix}.$$

Now let $Y \subseteq F$ generate F modulo R. Since $R \leqslant \ker\psi$ we have $\bar{\delta} R = 0$, and therefore, since $\bar{\delta}$, like δ, is a derivation, $\bar{\delta} Y$ spans W by Lemma 2;

let $\{\bar{\delta}y_1, \ldots, \bar{\delta}y_r\} \subseteq \bar{\delta}Y$ be a basis. In particular, $\bar{\delta}y_1, \ldots, \bar{\delta}y_r$ generate a free $\mathbf{Z}\overline{G}$-submodule of W.

Let E be the free group with basis $\{y_1, \ldots, y_r\}$, and define $\alpha\colon E \to \overline{G}$ by $y_i \mapsto y_i S$. Let $N = \ker\alpha$. By Lemma 1, the map

$$\beta\colon y_i \mapsto \begin{pmatrix} y_i S & 0 \\ \bar{\delta}y_i & 1 \end{pmatrix}$$

has kernel N'. But $\beta = j\alpha$ and j is injective, and hence $N = N'$. Since N is also a subgroup of a free group, and hence free, we must have $N = 1$. Therefore the subgroup $\langle y_1, \ldots, y_r\rangle$ of F is free modulo S, and so free modulo R.

The reader will notice that the proof above gives a stronger result than Theorem 1: with the hypotheses of the theorem there is a homomorphism from G to an orderable group P such that $n - m$ elements of Y map to a basis of a free subgroup of P. The reader will also notice that there is no need to introduce M in the above proof. The reason for doing so will appear in the next section.

2.4 Modifications for the pro-p case

The arguments of Section 2.3 apply without essential change in the pro-p case; all subgroups are now understood to be closed, all maps continuous, and modules are modules for the *completed group ring* $\mathbf{Z}_p[[G]]$ of G over $\mathbf{Z}_p$. For information about pro-p groups and their completed group rings we refer the reader to [10]. Instead of appealing to the Kaloujnine–Krasner theorem to embed an extension in a split extenson, we may use the following well-known result.

LEMMA 5. *Let A be a (closed) abelian normal subgroup of a pro-p group G and let $H = G/A$. Then G can be embedded in a pro-p group $H \ltimes B$ with B abelian, in such a way that the composite of the embedding and the map $H \ltimes B \to H$ is the quotient map $G \to H$.*

Proof. Let $(N_\lambda)_{\lambda\in\Lambda}$ be a family of open normal subgroups with $\bigcap N_\lambda = 1$. The Kaloujnine–Krasner theorem for finite groups gives embeddings

$$j_\lambda\colon G/N_\lambda \to G/AN_\lambda \ltimes B_\lambda$$

with each B_λ an abelian p-group, and we consider the subgroup of the Cartesian product $\mathrm{Cr}\,(G/AN_\lambda \ltimes B_\lambda)$ generated by the abelian normal subgroup $\mathrm{Cr}\,B_\lambda$ and the image of G under the map $g \mapsto (j_\lambda(gN_\lambda))$.

We can no longer use ordered groups as in Section 2.3, because, for example, we need to ensure that $U \cap M$ is closed in the $\mathbf{Z}_p[[G]]$-module M. Instead we need to use a deep result of Romanovskiĭ [6].

A filtration

$$A = A_{(1)} \geqslant \cdots \geqslant A_{(i)} \geqslant \cdots$$

of normal subgroups of a profinite with $\bigcap A_{(i)} = 1$ is called *convergent* if each neighbourhood of 1 contains some subgroup $A_{(i)}$. Write $\mathcal{N}$ for the class of all finitely generated pro-p groups having a convergent filtration with torsion-free central factors. If G is any finitely generated pro-p group then G has a unique minimal normal subgroup K such that $G/K \in \mathcal{N}$, namely the intersection of the kernels of all maps from G to torsion-free nilpotent pro-p groups.

PROPOSITION 2 (cf. [6, Proposition 7]). *Let H be a pro-p group in $\mathcal{N}$ and let L be the completed group ring $\mathbf{Z}_p[[H]]$ of H. Then there exist a filtration $(H_i)_{i \geqslant 1}$ with torsion-free central factors and a skew-field $Q \geqslant L$ such that the following holds: if $n \geqslant 1$ and U is a subspace of the vector space $Q^{(n)}$, then*

(i) *$U \cap L^{(n)}$ is closed in $L^{(n)}$, and*

(ii) *the $\mathbf{Z}_p$-module $M = L^{(n)}/(U \cap L^{(n)})$ has a filtration $(M_j)_{j \geqslant 1}$ of closed submodules such that $[M_j, H_i] \leqslant M_{i+j}$ and M_j/M_{j+1} is a torsion-free group for all i, j; moreover*

(iii) *$(H_i M_i)_{i \geqslant 1}$ is a filtration of $H \ltimes M$ with torsion-free central factors, and so $H \ltimes M \in \mathcal{N}$.*

In the proof of Theorem 1 for pro-p groups, we take S/R to be the intersection of the kernels of all maps from F/R to torsion-free nilpotent pro-p groups; thus $F/S \in \mathcal{N}$ and S is the smallest normal subgroup containing R with this property. Define ψ as in the proof in Section 2.3. It follows from Proposition 2 that the codomain of ψ is a pro-p group and is in $\mathcal{N}$. The rest of the proof from Section 2.3 now applies without any change.

3. IMAGES OF FREE PRODUCTS OF PRO-p GROUPS

3.1 THE MAGNUS EMBEDDING FOR FREE PRO-p PRODUCTS

The Magnus embedding used in Section 2 has been modified by Shmel′kin and Romanovskiĭ to the case of free products of groups. Everything that we require can be deduced from the following special case of Romanovskiĭ [7, Theorem 3].

LEMMA 6. *Let F be the free pro-p product of the pro-p groups $A_1, \dots, A_n$ and let $H = F/R$, where R is a (closed) normal subgroup such that $A_i \cap R = 1$ for $i = 1, \dots, n$. Let T be the free right $\mathbf{Z}_p[[H]]$-module with basis $\{t_1, \dots, t_n\}$. Let*

$$\mu\colon F \longrightarrow \begin{pmatrix} H & 0 \\ T & 1 \end{pmatrix}$$

be the homomorphism defined on the free factors A_i of F by

$$a \mapsto \begin{pmatrix} aR & 0 \\ t_i(a-1) & 1 \end{pmatrix} \quad \textit{for } a \in A_i\,.$$

Then $\ker \mu = R'$.

As observed in [8, Lemma 5], Lemma 6 may be modified as follows.

LEMMA 7. *The conclusion of Lemma 6 remains true if the hypothesis on T is replaced by the requirement that $\{t_2, \dots, t_n\}$ is a basis of T and $t_1 = 0$.*

Proof. This follows from the formula

$$\begin{pmatrix} 1 & 0 \\ t_1 & 1 \end{pmatrix}^{-1} \begin{pmatrix} aR & 0 \\ t_i(a-1) & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ t_1 & 1 \end{pmatrix} = \begin{pmatrix} aR & 0 \\ (t_i - t_1)(a-1) & 1 \end{pmatrix}.$$

3.2 DERIVATIONS TO RIGHT VECTOR SPACES

We prove the following result concerning derivations from pro-p groups G to right vector spaces V over skew-fields containing $\mathbf{Z}_p[[G]]$. The derivations under consideration are understood to be continuous regarded as maps into finitely generated $\mathbf{Z}_p[[G]]$-submodules of V; a derivation $\delta\colon G \to V$ is *inner* if there exists some $v \in V$ such that $\delta g = v(g-1)$ for all $g \in G$.

PROPOSITION 3. *Suppose that G is a finitely generated pro-p group such that $\mathbf{Z}_p[[G]]$ can be embedded in a skew-field Q, and suppose that G is generated by subgroups A and B. Let δ be a derivation from G to a right vector space V over Q. If the restrictions $\delta|_A$, $\delta|_B$ are both inner derivations, then either G is the free pro-p product of A, B or δ is inner.*

Proof. By hypothesis, there are m_A, $m_B \in V$ such that $\delta|_A$, $\delta|_B$ are the maps $a \mapsto m_A(a-1)$, $b \mapsto m_B(b-1)$. Let M be the $\mathbf{Z}_p[[G]]$-module generated by $m_B - m_A$, let F be the free pro-p product of A, B, and N the kernel of the map $q\colon F \to G$ extending the identity maps on A, B.

Suppose that δ is not inner; then $m_A \neq m_B$ and the map $\gamma\colon g \mapsto \delta g - m_A(g-1)$ is a non-zero derivation. By Lemma 7 the (continuous) homomorphism

$$\mu\colon F \to \begin{pmatrix} F/N & 0 \\ M & 1 \end{pmatrix}$$

defined on $A \cup B$ by

$$a \mapsto \begin{pmatrix} aN & 0 \\ 0 & 1 \end{pmatrix}, \quad b \mapsto \begin{pmatrix} bN & 0 \\ (m_B - m_A)(b-1) & 1 \end{pmatrix}$$

has kernel N'. Define $\widetilde{\gamma}\colon F \to V$ by

$$\mu f = \begin{pmatrix} fN & 0 \\ \widetilde{\gamma} f & 1 \end{pmatrix}.$$

Then $\widetilde{\gamma}$ and γq are (continuous) derivations from F that agree on $A \cup B$, and so they are equal. However for $n \in N$ we have $\widetilde{\gamma} n = \gamma q n = 0$, and so $\mu n = 1$. Thus $N = N'$, and since N is a pro-p group we have $N = 1$, as required.

3.3 DI-GROUPS

In order to state and prove the next result concisely, we make a definition, concerning circumstances under which certain *derivations* are guaranteed to be *inner*. We say that a finitely generated pro-p group G is a DI-*group* if its completed group ring $\mathbf{Z}_p[[G]]$ can be embedded in a skew-field and if whenever Q is a skew-field containing $\mathbf{Z}_p[[G]]$ and $\delta\colon G \to V$ is a derivation to a finite-dimensional space over Q then δ is inner. Again, our derivations are continuous maps into finitely generated $\mathbf{Z}_p[[G]]$-submodules.

Clearly $\mathbf{Z}_p$ is a DI-group, and, by Proposition 3, any pro-p group that is generated by two DI-subgroups either is the free pro-p product of the two subgroups or is again a DI-group.

THEOREM 3. *Let F be the free pro-p product of a family $\mathcal{A}$ of n finitely generated pro-p groups each having $\mathbf{Z}_p$ as an image, and let R be a normal subgroup of F generated (as a normal subgroup) by m elements of F, where $m < n$. Let S be the intersection of all normal subgroups N of F with $R \leqslant N$ and F/N torsion-free nilpotent.*

Write $\overline{G} = F/S$, and for $A \in \mathcal{A}$ write $\overline{A}$ for the image of A in $\overline{G}$. Let $\mathcal{B}$ be a family of DI-*subgroups of $\overline{G}$, set $J = \langle B \mid B \in \mathcal{B} \rangle$, and suppose that for each A in $\mathcal{A}$ with $\overline{A} \neq 1$, the subgroups $\overline{A}$ and J do not generate their free product in $\overline{G}$. Then $|\mathcal{B}| \geqslant n - m$, and there are $n - m$ members of $\mathcal{B}$ that generate in $\overline{G}$ their free product.*

Theorem 3 implies the result stated as Theorem 2 in the Introduction. Assume the hypotheses of Theorem 2 and define S, $\overline{G}$ as in Theorem 3. Let $\mathcal{B}_1$ be the family of all procyclic subgroups of groups in $\mathcal{B}$ and let $\overline{\mathcal{B}}_1$ be the family of non-trivial images of members of $\mathcal{B}_1$ in $\overline{G}$; since $\overline{G}$ is torsion-free, $\overline{\mathcal{B}}_1$ consists of DI-subgroups. By Theorem 3 there are $n - m$ members of $\overline{\mathcal{B}}_1$ that freely generate a free pro-p subgroup of $\overline{G}$, and thus their pre-images in $\mathcal{B}_1$ freely generate a free pro-p subgroup of G. Theorem 2 follows.

3.4 Proof of Theorem 3

Assume the hypotheses of the theorem. Write $\mathcal{A} = \mathcal{A}_1 \cup \mathcal{A}_2$, where $\mathcal{A}_1$ contains all subgroups A with non-trivial images in $\overline{G}$ and $\mathcal{A}_2 = \mathcal{A} \setminus \mathcal{A}_1$. We can replace all groups A from $\mathcal{A}_1$ by their images in $\overline{G}$ and also identify them with their images in $\overline{G}$. Let Q be a skew-field containing $\mathbf{Z}_p[[\overline{G}]]$ with the properties given by Proposition 2. By hypothesis, for each $A \in \mathcal{A}_2$ there is a non-zero continuous homomorphism ν_A from A to the additive group of Q. Let V be the right vector space over Q with basis $\{t_A \mid A \in \mathcal{A}\}$ and let M be the $\mathbf{Z}_p[[G]]$-submodule with basis $\{t_A \mid A \in \mathcal{A}\}$. Define a group homomorphism

$$\theta \colon F \to \begin{pmatrix} \overline{G} & 0 \\ M & 1 \end{pmatrix}$$

by specifying its restriction $\theta|_A$ to the free factors as follows:

$$a \mapsto \begin{pmatrix} a & 0 \\ t_A(a-1) & 1 \end{pmatrix}, \qquad \text{for } a \in A \in \mathcal{A}_1,$$

$$a \mapsto \begin{pmatrix} 1 & 0 \\ \nu_A(a)\, t_A & 1 \end{pmatrix}, \qquad \text{for } a \in A \in \mathcal{A}_2.$$

Since the subspace of V spanned by the bottom left-hand entries of the images of the elements of F contains all elements t_A, it is equal to V.

Let R be generated as a normal subgroup of F by $r_1, \ldots, r_m$. The images θr_i have the form

$$\begin{pmatrix} 1 & 0 \\ u_i & 1 \end{pmatrix}$$

and so they all lie in the subgroup

$$\begin{pmatrix} 1 & 0 \\ U \cap M & 1 \end{pmatrix},$$

where U is the subspace of V spanned by $\{u_1, \dots, u_m\}$. Write $W = V/U$. Then the kernel K of the map

$$\psi\colon F \to \begin{pmatrix} \overline{G} & 0 \\ W & 1 \end{pmatrix}$$

induced by θ contains R. Moreover K consists of the elements of S whose images under θ have bottom left entry in $U \cap M$. It follows from Proposition 2 that $U \cap M$ is closed in M and that $\overline{G} \ltimes (M/(U \cap M)) \in \mathcal{N}$; therefore $F/K \in \mathcal{N}$, and by the definition of S we conclude that $K = S$ and that θ induces an injective map

$$j\colon \overline{G} \to \begin{pmatrix} \overline{G} & 0 \\ W & 1 \end{pmatrix}.$$

By construction we have

$$jg = \begin{pmatrix} g & 0 \\ \delta g & 1 \end{pmatrix},$$

where $\delta\colon \overline{G} \to W$ is a derivation.

We note that $t_A \in U$ for each $A \in \mathcal{A}_2$; this follows since $A \leqslant S = K$, which maps under θ to the group of matrices with bottom left entry in U.

Set $\dim W = r$; thus $r \geqslant n - m$. Since all groups in $\mathcal{B}$ are DI-groups, the restriction maps $\delta|_B$ have the form $b \mapsto s_B(b-1)$ for some elements $s_B \in W$. Let U_1/U be the subspace of W spanned by $\{s_B \mid B \in \mathcal{B}\}$. Fix $A \in \mathcal{A}_1$, set $L = \langle J, A \rangle$ and consider the composite $\bar{\delta}$ of the restriction $\delta|_L$ and the map $W = V/U \to W/U_1$. Since L is not the free product of J, A and since $\bar{\delta}|_J = 0$ and $\bar{\delta}|_A$ is an inner derivation, Proposition 3 implies that $\bar{\delta} = 0$. From the definition of δ it now follows that $t_A \in U_1$. Since this holds for all $A \in \mathcal{A}_1$, we conclude that U_1 contains $\{t_A \mid A \in \mathcal{A}\}$ and hence equals V. Therefore W is spanned by $\{s_B \mid B \in \mathcal{B}\}$. Choose $\mathcal{B}_0 \subseteq \mathcal{B}$ such that $\{s_B \mid B \in \mathcal{B}_0\}$ is a basis of V.

We claim that the subgroups in $\mathcal{B}_0$ generate their free pro-p product in $\overline{G}$. Write E for the free product of the groups $B \in \mathcal{B}_0$ and consider the homomorphism $\alpha\colon E \to \langle B \mid B \in \mathcal{B}_0 \rangle \leqslant \overline{G}$. Let $N = \ker \alpha$. We have $B \cap N = 1$ for each $B \in \mathcal{B}_0$ and

$$j\alpha b = \begin{pmatrix} b & 0 \\ s_B(b-1) & 1 \end{pmatrix} \qquad \text{for } b \in B \in \mathcal{B}_0 .$$

By Lemma 4 we have $\ker j\alpha = N'$, and hence $N = N'$ since j is injective. Since N is a pro-p group it follows that $N = 1$, so that α is injective. This concludes the proof of Theorem 3.

REFERENCES

[1] KALOUJNINE, L. et M. KRASNER. Produit complet des groupes de permutations et problème d'extension de groupes. III. *Acta Sci. Math. Szeged 14* (1951), 69–82.

[2] LAM, T. Y. *A First Course in Noncommutative Rings*. Second edition. Graduate Texts in Mathematics *131*. Springer-Verlag, New York, 2001.

[3] MAGNUS, W. Über diskontinuierliche Gruppen mit einer definierenden Relation. (Der Freiheitssatz). *J. Reine Angew. Math. 163* (1930), 141–165.

[4] NEUMANN, B.H. On ordered division rings. *Trans. Amer. Math. Soc. 66* (1949), 202–252.

[5] ROMANOVSKIĬ, N.S. Free subgroups of finitely-presented groups. *Algebra and Logic 16* (1978), 62–68.

[6] —— A generalized theorem on freedom for pro-p-groups. *Siberian Math. J. 27* (1986), 267–280.

[7] —— On Shmelʹkin embeddings for abstract and profinite groups. *Algebra and Logic 38* (1999), 326–334.

[8] ROMANOVSKIĬ, N.S. and J.S. WILSON. A Freiheitssatz for free products of pro-p groups. *J. Algebra 254* (2002), 226–240.

[9] ROMANOVSKIĬ, N.S. and J.S. WILSON. Free product decompositions in images of certain free products of groups. *J. Algebra 310* (2007), 57–69.

[10] WILSON, J.S. *Profinite Groups*. London Mathematical Society Monographs. New Series *19*. The Clarendon Press, Oxford University Press, New York, 1998.

[11] —— On growth of groups with few relators. *Bull. London Math. Soc. 36* (2004), 1–2.

(Reçu le 7 juillet 2009)

John S. Wilson

University College
Oxford OX1 4BH
United Kingdom
e-mail: wilsonjs@maths.ox.ac.uk