JOURNAL OF ALGEBRA **196,** 101–113 (1997)
ARTICLE NO. JA977082

Subgroups of the Nottingham Group

Rachel Camina*

Lehrstuhl B für Mathematik, RWTH Aachen, Templergraben 64, 52062 Aachen, Germany

Communicated by Peter M. Neumann

Received April 14, 1996

INTRODUCTION

The Nottingham group, J, may be described as the group of normalized automorphisms of the ring $\mathbf{F}_p[[t]]$, namely, those automorphisms acting trivially on $(t)/(t)^2$. It is a finitely generated pro-p group. Originally defined by Jennings [2] (as a group of formal power series under substitution), it was really Johnson [3] and York [10] who brought J to the attention of group theorists. In this paper we prove the following result.

THEOREM. *Every countably based pro-p group can be embedded, as a closed subgroup, in the Nottingham group.*

A simple corollary of this result is a positive answer to the conjecture, posed by Shalev [5], as to whether a free abstract group of rank 2 can be embedded in J.

The first result in this direction is the theorem of Leedham-Green and Weiss, which says that every finite p-group can be embedded in J. The proof of this theorem depends on two papers of Witt dating from the 1930s [8, 9]. To set the stage, we first briefly summarise these papers and then prove the result of Leedham-Green and Weiss, which is still unpublished.

Next, we analyse where these finite subgroups of J lie. More precisely, we analyse where the elements of these subgroups lie in J with respect to a natural filtration of J, which is closely related to its lower central series. Once this has been established it is possible to ''link up'' these finite subgroups in a suitable way and hence prove that every finitely generated pro-p group can be embedded, as a closed subgroup, in J. We can then

* E-mail: rachel@willi.math.rwth-aachen.de.

0021-8693/97 $25.00

apply a theorem of Lubotzky and Wilson [4], and conclude that every countably based pro-p group can be embedded in J.

PRELIMINARIES

Let A denote the automorphism group of the field $\mathbf{F}_p((t))$. Then A is equal to the group of continuous automorphisms of $\mathbf{F}_p((t))$. This follows from the fact that the valuation of $\mathbf{F}_p((t))$, defined by $v(\sum_{i=k}^{\infty} a_i t^i) = k$, where $a_k \neq 0$, is the only normalized valuation of $\mathbf{F}_p((t))$ with respect to which $\mathbf{F}_p((t))$ is complete. An element g of A is therefore defined by its action on t and is of the following form:

$$tg = \sum_{i=1}^{\infty} \alpha_i t^i, \qquad \alpha_i \in \mathbf{F}_p, \qquad \alpha_1 \neq 0.$$

We can now define the Nottingham group.

DEFINITION 1. The Nottingham group, J, is defined as the subgroup of $A = \mathrm{Aut}(\mathbf{F}_p((t)))$ consisting of automorphisms of the form

$$t \mapsto t + \sum_{i=2}^{\infty} \alpha_i t^i, \qquad \alpha_i \in \mathbf{F}_p.$$

When we want to be precise about which field J is acting on, we shall write $J(t)$ for J. The following lemma is clear.

LEMMA 1. *J is a normal subgroup of index $p-1$ in A.*

Next we define a chain of subsets J_n $(n \geq 1)$ of J by

$$J_n := \{g \in J : tg \equiv t \bmod t^{n+1}\}.$$

It is clear that $J_n \trianglelefteq J$ and $|J/J_n| = p^{n-1}$. It can then be proved that $J \cong \lim_{\leftarrow} (J/J_n)$. So J is a pro-p group, in fact, a finitely generated pro-p group [3].

The next definition, although simple, will be very useful throughout this paper.

DEFINITION 2. If $1 \neq g \in J$ there exists an integer $n \geq 1$ such that $g \in J_n \setminus J_{n+1}$. Define this n to be the depth of g, $D(g)$. Further, define the depth of the identity to be ∞. When J is acting on the field $\mathbf{F}_p((t))$, and we want to indicate this in the depth function, we write $D_t(g)$.

THE WITT ALGORITHM

In this section we summarise some of Witt's results, on which the rest of this paper will be based. Witt [8] constructs abelian field extensions of exponent p, of a given field k of characteristic $p \neq 0$, as follows.

Let k be a field of characteristic p, and let k^+ denote the additive group of the field k and $\bar{k}$ the algebraic closure of k. Define the map $\wp$ of $\bar{k}$ as follows:

$$\wp: \bar{k} \to \bar{k},$$
$$x \mapsto x^p - x.$$

Let $\wp k = \{x^p - x\colon\ x \in k\}$. Then $\wp k$ is a subgroup of k^+. Choose a subgroup of k^+, Ω, such that $\wp k \leq \Omega \leq k^+$ and $|\Omega/\wp k|$ is finite. Let $\wp^{-1}(\Omega) = \{\theta \in \bar{k}\colon \wp\theta \in \Omega\}$. Witt proved the following theorem.

THEOREM 1 (Witt [8, p. 47]). *Let* $\wp k \leq \Omega \leq k^+$, *where* $|\Omega/\wp k|$ *is finite. Then* $\mathrm{Gal}(k(\wp^{-1}\Omega)/k) \cong \Omega/\wp k$. *Further, for every abelian extension field* K *of* k *of exponent* p *there exists a group* Ω *such that* $K = k(\wp^{-1}\Omega)$.

After realising elementary abelian p-groups as Galois extensions, Witt considered the general finite p-group case, using an induction procedure based on the elementary abelian case [9].

Assume H is a finite p-group with a nontrivial Frattini subgroup, $\Phi(H)$. Let L be a cyclic subgroup of H of order p satisfying $L \leq Z(H) \cap \Phi(H)$, where $Z(H)$ denotes the centre of H. Also, suppose we already have $M \cong \mathrm{Gal}(K/k)$ for some extension field K of k, where $H/L \cong M$. Then, to find Galois extension fields $\hat{K}$ of k such that $\mathrm{Gal}(\hat{K}/k) \cong H$, proceed as follows.

(a) Fix a transversal of L in H such that if the elements of M are denoted by $\{\sigma, \tau, \ldots\}$ then the transversal is denoted by $\{u_\sigma, u_\tau, \ldots\}$. Next, define $l_{\sigma,\tau}, \ldots \in L$ such that $u_\sigma u_\tau = l_{\sigma,\tau} u_{\sigma\tau}$.

(b) Choose an explicit isomorphism

$$\Theta: M \to \mathrm{Gal}(K/k),$$
$$\sigma \mapsto s,$$
$$\tau \mapsto t.$$

(c) Choose a nonzero additive character χ of L.

(d) Choose a set $\{\delta_s\colon s \in \mathrm{Gal}(K/k)\} \subseteq K$ such that

$$\chi(l_{\sigma,\tau}) = \delta_s + s\delta_t - \delta_{st}, \qquad \forall\, s, t \in \mathrm{Gal}(K/k).$$

(e) Choose $\gamma \in K$ such that

$$\wp \delta_s = (s-1)\gamma, \qquad \forall\, s \in \mathrm{Gal}(K/k).$$

(f) Solve the equation $\wp x = \gamma$ and adjoin the root $\theta \in \overline{K}$ to K to obtain $\hat{K} = K(\theta)$.

Then $H \cong \mathrm{Gal}(\hat{K}/k)$ and a crossed product representation of the elements of $\mathrm{Gal}(\hat{K}/k)$ is given as follows. Suppose $l \in L$ and $s \in \mathrm{Gal}(K/k)$. Then define $\bar{l}, v_s \in \mathrm{Gal}(\hat{K}/k)$ in the following way:

$$\bar{l}(\theta) = \theta + \chi(l), \qquad \bar{l}(\alpha) = \alpha, \qquad \forall\, \alpha \in K,$$

and

$$v_s(\theta) = \theta + \delta_s, \qquad v_s(\alpha) = s(\alpha), \qquad \forall\, \alpha \in K.$$

Note that $\theta + \delta_s$ satisfies the equation $\wp x = s\gamma$.

So, Witt proves the following result, where $d(H)$ denotes the number of generators of H and

$$[k : \wp k] = p^N$$

defines N. If $[k: \wp k]$ is unbounded we let $N = \infty$.

THEOREM 2 (Witt [9, p. 240]). *Let H be a finite p-group and k a field of characteristic p. Then there is a Galois extension field $\hat{K}$: k such that* $\mathrm{Gal}(\hat{K}/k) \cong H$ *if and only if $d(H) \leq N$.*

Now, a few remarks about this algorithm which will be useful later.

(i) Identify H with $\mathrm{Gal}(\hat{K}/k)$ and M with $\mathrm{Gal}(K/k)$; then the canonical homomorphism

$$\pi : H \to H/L \cong M$$

sends $v_s \bar{l} \mapsto s$. This is simply the map $v_s \bar{l} \mapsto v_s \bar{l}|_K$.

(ii) Witt actually takes L to be the maximal subgroup of H such that $L \leq \Phi(H) \cap Z(H)$. He does this so that he can later calculate the number of possible field extensions. However, his proof also covers the case when L is not maximal. Therefore, it is possible to construct the required field extension in smaller steps, that is, at each stage to take L such that $L \leq \Phi(H) \cap Z(H)$ and $|L| = p$, as we have described.

(iii) Later, we will be considering the case where $k = \mathbf{F}_p((t))$. In this case, Witt's extensions are totally ramified, assuming that the initial elementary abelian extension is. Although Witt does not prove this directly, his proof that γ is linearly independent with respect to $\wp K$ also proves this fact.

To apply Theorem 2 to the Nottingham group, we let $k = \mathbf{F}_p((t))$. We need the following lemma, which views the elementary abelian additive group $\mathbf{F}_p((t))/\wp(\mathbf{F}_p((t)))$ as a vector space over $\mathbf{F}_p$.

LEMMA 2. *A basis for* $\mathbf{F}_p((t))/\wp(\mathbf{F}_p((t)))$ *is given by the image of*

$$\{1\} \cup \left\{t^{-i} : i \in \mathbf{Z}^+ \text{ and } i \not\equiv 0 \ (\operatorname{mod} p)\right\}.$$

We are now ready to prove the following theorem.

THEOREM 3 (Leedham-Green and Weiss). *The Nottingham group, J, contains a copy of every finite p-group.*

Proof. Let H be a finite p-group. Then, by Theorem 2 and Lemma 2, there exists an extension field K of $\mathbf{F}_p((t))$ such that $H \cong \operatorname{Gal}(K/\mathbf{F}_p((t)))$. Now, K is a finite, totally ramified extension of $\mathbf{F}_p((t))$ so $K \cong \mathbf{F}_p((t))$ [7, Theorem 8]. Thus, we have that $H \leq \operatorname{Aut}(\mathbf{F}_p((t)))$. By Lemma 1, J has index $p-1$ in $\operatorname{Aut}(\mathbf{F}_p((t)))$, and since $p-1$ is prime to p and $H = p^n$, for some n, we must have that $H \leq J$, as required. ∎

The next result is a direct consequence of this theorem, since the derived length of soluble linear groups in a given dimension is bounded [6, 3.7].

COROLLARY 1. *J is not linear over any field.*

SOME INTRODUCTORY LEMMAS

We will now prove a few lemmas which will be useful when applying Witt's work to the Nottingham group. The following lemma is just a different way of viewing Lemma 2.

LEMMA 3. *Let $\gamma \in \mathbf{F}_p((t)) \setminus \wp(\mathbf{F}_p((t)))$. Then there exists $\hat{\gamma}, \mu \in \mathbf{F}_p((t))$ such that*

$$\gamma = \hat{\gamma} + \wp\mu,$$

where $v(\hat{\gamma}) \leq 0$, and if $v(\hat{\gamma}) < 0$ then $v(\hat{\gamma}) \not\equiv 0 \bmod p$.

Note. If the addition of a "root" of γ, that is, an element θ such that $\wp\theta = \gamma$, gives a totally ramified extension of $\mathbf{F}_p((t))$, then in the preceding result we have the stronger conclusion that $v(\hat{\gamma}) < 0$. This will be the case when we apply this lemma later.

The rest of the lemmas in this section will be proved under the following hypothesis.

HYPOTHESIS. *Suppose* $\mathbf{F}_p((\hat{T}))$ *is a separable finite field extension of* $\mathbf{F}_p((T))$ *of degree p, that is,* $[\mathbf{F}_p((\hat{T}))\colon \mathbf{F}_p((T))] = p$. *Let* v_T *be the usual valuation of* $\mathbf{F}_p((T))$ *where* $v_T(T) = 1$. *Then* v_T *can be uniquely extended to give a valuation of* $\mathbf{F}_p((\hat{T}))$ *with* $v_T(\hat{T}) = 1/p$. *We then have an expression for T of the following form*:

$$T = \sum_{i=p}^{\infty} a_i \hat{T}^i,$$

where $a_i \in \mathbf{F}_p$ *and* $a_p \neq 0$. *Also, suppose* a_u *is the first nonzero coefficient in* $\sum_{i=p}^{\infty} a_i \hat{T}^i$ *such that* $u \not\equiv 0 \bmod p$. *Such an* a_u *exists, since if not T is a pth power in* $\mathbf{F}_p((\hat{T}))$ *and so the extension is inseparable, a contradiction.*

LEMMA 4. *Under the conditions of the* hypothesis, *if*

$$g \in \mathrm{Gal}\Big(\mathbf{F}_p\big((\hat{T})\big)/\mathbf{F}_p\big((T)\big)\Big) \cap J(\hat{T})$$

and g is given by

$$\hat{T}g = \hat{T} + \sum_{j=k+1}^{\infty} \alpha_j \hat{T}^j, \qquad \alpha_j \in \mathbf{F}_p, \qquad \alpha_{k+1} \neq 0,$$

then $u = k(p-1) + p$.

Proof. Compare the following expressions for Tg:

$$\begin{aligned} \sum_{i=p}^{\infty} a_i \hat{T}^i &= T \\ &= Tg \\ &= \sum_{i=p}^{\infty} a_i \left(\hat{T} + \sum_{j=k+1}^{\infty} \alpha_j \hat{T}^j \right)^i . \end{aligned}$$

Delete the initial $\sum_{i=p}^{\infty} a_i \hat{T}^i$ term from both sides of the equation. The remaining terms on the right-hand side of the equation must cancel. For this to happen the following must hold:

$$a_p \alpha_{k+1} \hat{T}^{p(k+1)} + u a_u \alpha_{k+1} \hat{T}^{u-1} \hat{T}^{k+1} = 0.$$

Thus, in particular, $p(k+1) = u + k$, that is, $u = k(p-1) + p$. ∎

LEMMA 5. *Given the conditions of the* hypothesis, *suppose* $g \in J(\hat{T})$ *and*

$$\hat{T}g = \hat{T} + \sum_{l=n+1}^{\infty} \alpha_l \hat{T}^l, \qquad \alpha_l \in \mathbf{F}_p, \qquad \alpha_{n+1} \neq 0,$$

and

$$Tg = T + \sum_{j=k+1}^{\infty} \beta_j T^j, \qquad \beta_j \in \mathbf{F}_p, \qquad \beta_{k+1} \neq 0.$$

Also, suppose $u = r(p-1) + p$ *where* $r > k$. *Then* $n = k$.

Proof. Consider the following expressions for Tg:

$$\begin{aligned}\sum_{i=p}^{\infty} a_i \hat{T}^i + \sum_{j=k+1}^{\infty} \beta_j \left(\sum_{i=p}^{\infty} a_i \hat{T}^i \right)^j &= T + \sum_{j=k+1}^{\infty} \beta_j T^j \\ &= Tg \\ &= \left(\sum_{i=p}^{\infty} a_i \hat{T}^i \right) g \\ &= \sum_{i=p}^{\infty} a_i \left(\hat{T} + \sum_{l=n+1}^{\infty} \alpha_l \hat{T}^l \right)^i .\end{aligned}$$

Delete the initial $\sum_{i=p}^{\infty} a_i \hat{T}^i$ term from both sides of the equation and compare the resulting first terms.

In the first expression the first term is given by $\beta_{k+1} a_p^{k+1} \hat{T}^{(k+1)p}$.

In the last expression the first term is either $a_p \alpha_{n+1} \hat{T}^{(n+1)p}$, $a_u \hat{T}^{u-1} u \alpha_{n+1} \hat{T}^{n+1}$ or these two terms cancel.

However, we know that $u = r(p-1) + p$ and $r > k$. Suppose, for a contradiction, that $n \geq r$. Then, clearly, $n(p-1) \geq r(p-1)$ and

$$\begin{aligned} np + p &\geq rp - r + p + n = u + n \\ &\geq (r+1)p \\ &> (k+1)p. \end{aligned}$$

Therefore, $(n+1)p \geq u + n > (k+1)p$, a contradiction.

So, we must have $n < r$. Hence $(n+1)p < u + n$ and consequently for the first terms to compare $(n+1)p = (k+1)p$, that is, $n = k$ as required. ∎

FINITE SUBGROUPS OF J

We now analyse "where," in terms of depth (see Definition 2), the finite subgroups of J lie. The first result in this direction is due to Weiss and considers cyclic subgroups of order p. To embed such a group in J, we construct field extensions K of our field $\mathbf{F}_p((t))$, such that $\mathrm{Gal}(K/\mathbf{F}_p((t)))$ is cyclic of order p. To do this, we choose an element $\gamma \in \mathbf{F}_p((t)) \setminus \wp(\mathbf{F}_p((t)))$ and set $K = \mathbf{F}_p((t))(\theta)$ where $\theta \in \overline{\mathbf{F}_p((t))}$, the algebraic closure of $\mathbf{F}_p((t))$, and $\theta^p - \theta = \gamma$. If we insist our extension is totally ramified, we choose γ such that $v(\gamma) < 0$. By Lemma 3, we can then assume that $v(\gamma) = -n$, where n is a positive integer not divisible by p, and in this case $K = \mathbf{F}_p((T))$ for some indeterminate T. Let $\langle g \rangle = \mathrm{Gal}(\mathbf{F}_p((T))/\mathbf{F}_p((t)))$. Then, as the order of g is p, it follows that $g \in J(T)$. Weiss proved the following result.

LEMMA 6 (Weiss). $D_T(g) = n$.

Proof. As $\theta^p - \theta = \gamma$ and $v(\gamma) = -n$, $v(\theta) = -n/p$ in the extended valuation. Since p and n are coprime, there exist integers c and d such that $cp - dn = 1$. Without loss of generality, set $T = \theta^d t^c$. Then $v(T) = 1/p$ and $K = \mathbf{F}_p((T))$. We can assume $\theta g = \theta + 1$, so then

$$\begin{aligned} Tg &= \theta^d t^c g \\ &= (\theta + 1)^d t^c \\ &= T + dT/\theta + \cdots + T/\theta^d. \end{aligned}$$

Now $v(T/\theta^x) = v(T) - xv(\theta) = 1/p + xn/p$, which is minimal when $x = 1$. So, as $d \not\equiv 0 \bmod p$, $v(T(g-1)) = (n+1)/p$ and $g \in J(T)_n \setminus J(T)_{n+1}$, as required. ∎

Note that in the preceding proof the choice of T does not affect the result, since all automorphisms of $\mathbf{F}_p((T))$ are continuous and hence respect the depth function.

We now want to analyse "where" an arbitrary finite subgroup of J lies, or more exactly, where it is possible for such a subgroup to lie. To embed an arbitrary finite p-group, H, in J using Witt's algorithm, we proceed inductively, first embedding factor groups of H in J. We prove that once a nontrivial homomorphic image of an element of H has been defined in J then, given suitable choices of further field extensions, its depth has been fixed.

Recall that to embed an arbitrary finite p-group H in J, we construct field extensions $\hat{K}$ of $\mathbf{F}_p((t))$ such that $\mathrm{Gal}(\hat{K}/\mathbf{F}_p((t))) \cong H$. To find $\hat{K}$, we assume that we already have an extension field K of $\mathbf{F}_p((t))$ such that $\mathrm{Gal}(K/\mathbf{F}_p((t))) \cong M$, where $H/L \cong M$, $L \leq Z(H) \cap \Phi(H)$, and $|L| = p$.

Now Witt's algorithm tells us to find a solution γ and "root" θ, satisfying $\wp\theta = \gamma$. Then we set $\hat{K} = K(\theta)$. By induction, $K = \mathbf{F}_p((T))$ for some indeterminate T, and our extension is totally ramified, so $\hat{K} = \mathbf{F}_p((\hat{T}))$ for some indeterminate $\hat{T}$. If $g \in \mathrm{Gal}(\mathbf{F}_p((\hat{T}))/\mathbf{F}_p((t)))$, then the order of g is a power of p and so $g \in J(\hat{T})$. Let π be the natural homomorphism $H \to M$. This defines a map

$$\pi : \mathrm{Gal}\Big(\mathbf{F}_p\big((\hat{T})\big)/\mathbf{F}_p\big((t)\big)\Big) \to \mathrm{Gal}\Big(\mathbf{F}_p\big((T)\big)/\mathbf{F}_p\big((t)\big)\Big),$$

which is just

$$g \mapsto g^{\pi} = g|_{\mathbf{F}_p((T))}.$$

We have the following theorem.

THEOREM 4. *Let* $g \in \mathrm{Gal}(\mathbf{F}_p((\hat{T}))/\mathbf{F}_p((t)))$ *with* $g^{\pi} \neq 1$. *Then there exists a* γ *and hence* $\hat{K} = \mathbf{F}_p((\hat{T}))$ *such that* $D_T(g^{\pi}) = D_{\hat{T}}(g)$.

Proof. Suppose that $v_T(\hat{T}) = 1/p$ and $v_T(T) = 1$. As in Lemma 3, rewrite γ as an element of $\mathbf{F}_p((T))$ in the form

$$\gamma = \hat{\gamma} + \wp(\mu),$$

where $\hat{\gamma}, \mu \in \mathbf{F}_p((T))$ and $v_T(\hat{\gamma}) = -n$, where $n > 0$ and $n \not\equiv 0 \bmod p$.

Suppose $1 \neq g \in \mathrm{Gal}(\mathbf{F}_p((T))/\mathbf{F}_p((t)))$. We require $v_T(\hat{\gamma}) < -D_T(g)$. To achieve this aim, we modify γ by adding a b of sufficiently low valuation which lies in the image of $\mathbf{F}_p((t))/\wp(\mathbf{F}_p((t))) \to \mathbf{F}_p((T))/\wp(\mathbf{F}_p((T)))$ induced by the inclusion of $\mathbf{F}_p((t))$ in $\mathbf{F}_p((T))$. Such a modified γ is still a solution, that is, satisfies (e). We need to show that such a b can be chosen. In view of the basis of $\mathbf{F}_p((T))/\wp(\mathbf{F}_p((T)))$ given in Lemma 2, it suffices to show that $\mathrm{im}(\mathbf{F}_p((t))/\wp(\mathbf{F}_p((t))) \to \mathbf{F}_p((T))/\wp(\mathbf{F}_p((T))))$ has infinite $\mathbf{F}_p$-dimension. This will follow from $\ker(\mathbf{F}_p((t))/\wp(\mathbf{F}_p((t))) \to \mathbf{F}_p((T))/\wp(\mathbf{F}_p((T))))$ being finite dimensional. An analysis of the cohomology of the map $\wp$ on the separable closure of $\mathbf{F}_p((t))$ shows that

$$\frac{\mathbf{F}_p((t)) \cap \wp\big(\mathbf{F}_p((T))\big)}{\wp\big(\mathbf{F}_p((t))\big)} \cong H^1\big(M, \mathbf{F}_p\big).$$

Consequently, we can choose a b with the required properties. So, without loss of generality, we may assume that $\hat{\gamma}$ has the required properties, and as we can replace γ with $\gamma - \wp\alpha$ for $\alpha \in \mathbf{F}_p((T))$ we may assume that γ has these properties.

Recall that $\wp(\theta) = \gamma$. We can construct $\hat{T}$ so that $\mathbf{F}_p((T))(\theta) = \mathbf{F}_p((\hat{T}))$ and we can prove that $D_{\hat{T}}(\bar{l}) = n$ where $L = \langle l \rangle$, as in the proof of Lemma 6. So

$$\hat{T}\bar{l} = \hat{T} + \sum_{k=n+1}^{\infty} \alpha_k \hat{T}^k$$

for some $\alpha_k \in \mathbf{F}_p$ and $\alpha_{n+1} \neq 0$. Also, $T\bar{l} = T$. As $[\mathbf{F}_p((\hat{T})): \mathbf{F}_p((T))] = p$, we have an expression for T in terms of $\hat{T}$ of the following form:

$$T = \sum_{k=p}^{\infty} a_k \hat{T}^k, \qquad a_p \neq 0.$$

Let a_u be the first nonzero coefficient in $\sum_{k=p}^{\infty} a_k \hat{T}^k$ such that $u \not\equiv 0 \bmod p$. Then, since the conditions of the hypothesis are satisfied, by Lemma 4, $u = n(p-1) + p$.

Now consider $g \in \operatorname{Gal}(\mathbf{F}_p((\hat{T}))/\mathbf{F}_p((t)))$, such that $g|_{\mathbf{F}_p((T))} \neq 1$. Suppose

$$Tg = T + \sum_{i=m+1}^{\infty} \beta_i T^i, \qquad \beta_i \in \mathbf{F}_p, \qquad \beta_{m+1} \neq 0,$$

and

$$\hat{T}g = \hat{T} + \sum_{i=q+1}^{\infty} \gamma_i \hat{T}^i, \qquad \gamma_i \in \mathbf{F}_p, \qquad \gamma_{q+1} \neq 0.$$

As the conditions of the hypothesis are satisfied and $u = n(p-1) + p$ with $n > m$, apply Lemma 5 to prove that $q = m$, as required. ∎

INFINITE SUBGROUPS OF J

We can now prove the main result of this paper.

THEOREM 5. *Every finitely generated pro-p group can be embedded, as a closed subgroup, in J.*

Proof. Let P be a finitely generated pro-p group. Then $P \cong \varprojlim P_i$, where $\{P_i\}$ is a tower of finite p-groups. By the Witt algorithm, we can successively embed the groups P_i into $J(T_i)$ where $\mathbf{F}_p((T_i))$ is a proper subfield of $\mathbf{F}_p((T_{i+1}))$. We do this in the way described in the previous section, so that Theorem 4 will be applicable.

P is topologically finitely generated, so $P \cong \overline{\langle s^{(1)}, \dots, s^{(r)} \rangle}$ for some elements $s^{(1)}, \dots, s^{(r)}$ of P. We can write $s^{(j)} = \{s_i^{(j)}\} \in \varprojlim P_i$ where $s_i^{(j)} \in P_i$. Using the embedding $P_i \hookrightarrow J(T_i)$, we can map $s_i^{(j)} \mapsto \overline{s_i^{(j)}} \in J(T_i)$. Now, define the maps θ_i:

$$\theta_i \colon J(T_i) \to J(T),$$

where $J(T)$ is the Nottingham group defined over $\mathbf{F}_p((T))$ for some indeterminate T. If $g \in J(T_i)$ is defined by

$$T_i g = T_i + \sum_{j=2}^{\infty} \alpha_j T_i^j, \qquad \alpha_j \in \mathbf{F}_p,$$

then

$$T(g\theta_i) = T + \sum_{j=2}^{\infty} \alpha_j T^j.$$

Clearly, the θ_i are isomorphisms and are depth invariable, that is,

$$D_{T_i}(g) = D_T(g\theta_i).$$

So, now each generator, $s^{(j)}$, of P defines a sequence, $\{\overline{s_i^{(j)}}\theta_i\}$, of elements in $J(T)$.

Let J denote $J(T)$. Now consider the sequence

$$\left\{\left(\overline{s_i^{(1)}}\theta_i, \dots, \overline{s_i^{(r)}}\theta_i\right)\right\} \in J \times \cdots \times J.$$

Since J is compact and countably based, so is $J \times \cdots \times J$ and consequently this sequence has a convergent subsequence, $\{(\widehat{s_i^{(1)}}, \dots, \widehat{s_i^{(r)}})\}$ say, and the limit $(x^{(1)}, \dots, x^{(r)}) = \lim\{(\widehat{s_i^{(1)}}, \dots, \widehat{s_i^{(r)}})\}$ lies in $J \times \cdots \times J$.

Now define a word w to be an element of the free pro-p group on r generators. Let $h \in P$. Then $h = w(s^{(1)}, \dots, s^{(r)})$ for some word w; note w need not be of finite length. Next, define a map from P to J in the following way:

$$\Theta\colon P \to J,$$
$$h = w(s^{(1)}, \dots, s^{(r)}) \mapsto w(x^{(1)}, \dots, x^{(r)}).$$

First we need to check that Θ is well defined.

For the map to be well defined, it is sufficient to prove the following:

$$w(s^{(1)}, \dots, s^{(r)}) = 1 \Rightarrow w(x^{(1)}, \dots, x^{(r)}) = 1.$$

We fix the word w being considered and think of it as a map

$$w\colon \underbrace{J \times \cdots \times J}_{r} \to J.$$

Then w is a continuous map. If w is finite, continuity follows directly from the fact that J is a topological group. If w is infinite, continuity follows from the fact that $J \cong \lim_{\leftarrow} J/J_n$ and each map $w_n = w\pi_n$, where π_n: $J \to J/J_n$, is continuous. So, as $w(s^{(1)}, \dots, s^{(r)}) = 1$ we have that $w(s_i^{(1)}, \dots, s_i^{(r)}) = 1$ for all i and therefore $w(\widehat{s_i^{(1)}}, \dots, \widehat{s_i^{(r)}}) = 1$ for all i. Thus

$$\begin{aligned} w(x^{(1)}, \dots, x^{(r)}) &= w\left(\lim\left\{\left(\widehat{s_i^{(1)}}, \dots, \widehat{s_i^{(r)}}\right)\right\}\right) \\ &= \lim\left\{w\left(\widehat{s_i^{(1)}}, \dots, \widehat{s_i^{(r)}}\right)\right\} \\ &= \lim 1 \\ &= 1, \end{aligned}$$

as required.

So, Θ is well defined. The map Θ is clearly a homomorphism and as a homomorphism from a finitely generated pro-p group to a profinite group it is continuous [1, Corollary 1.21(i)]. So, now we just have to check injectivity.

For injectivity we need

$$w(s^{(1)}, \dots, s^{(r)}) \neq 1 \Rightarrow w(x^{(1)}, \dots, x^{(r)}) \neq 1.$$

As before, $w(x^{(1)}, \dots, x^{(r)}) = \lim\{w(\widehat{s_i^{(1)}}, \dots, \widehat{s_i^{(r)}})\}$. Now, as $w(s^{(1)}, \dots, s^{(r)}) \neq 1$ we have that $w(s_i^{(1)}, \dots, s_i^{(r)}) \neq 1$ for sufficiently large i, and therefore $w(\widehat{s_i^{(1)}}, \dots, \widehat{s_i^{(r)}}) \neq 1$ for sufficiently large i. So, $w(\widehat{s_i^{(1)}}, \dots, \widehat{s_i^{(r)}})$ has a depth, call it k_i. By applying Theorem 4 to P and noting that the θ_i are depth invariable, we see that all the k_i must be equal, to k say. Thus

$$D\big(w(x^{(1)}, \dots, x^{(r)})\big) = D\Big(\lim\Big\{w\Big(\widehat{s_i^{(1)}}, \dots, \widehat{s_i^{(r)}}\Big)\Big\}\Big) = k,$$

that is, $w(x^{(1)}, \dots, x^{(r)}) \neq 1$, as required.

So, θ defines an embedding of P into J. Also, since P is compact and J is Hausdorff, P is embedded as a closed subgroup of J. ∎

A simple corollary of this result is a positive answer to the conjecture, posed by Shalev [5, Problem 12], as to whether a free abstract group of rank 2 can be embedded in J. This answer was expected, although, until now, it had not been proved. However, the fact that a free pro-p group of rank 2 can be embedded in J is very surprising. A positive answer is also given to Shalev's question as to whether the Nottingham group has a closed subgroup isomorphic to $C_p \wr \mathbf{Z}_p$ where $\mathbf{Z}_p$ denotes the p-adic integers and C_p denotes the cyclic group of order p [5, Problem 11].

The following result, due to Lubotzky and Wilson [4], is of a similar nature to Theorem 5.

THEOREM 6 (Lubotzky and Wilson [4]). *There exists a* 2*-generator pro-p group in which all countably based pro-p groups can be embedded.*

Theorems 5 and 6 together give the following corollary.

COROLLARY 2. *Every countably based pro-p group can be embedded, as a closed subgroup, in* J.

ACKNOWLEDGMENTS

This work was carried out whilst the author held a studentship from EPSRC at Queen Mary and Westfield College, London. The author would like to thank EPSRC and her supervisors Dr. Susan McKay and Dr. Charles Leedham-Green. She would also like to thank both referees for their useful comments, in particular, for the improvements to the proof of Theorem 4.

REFERENCES

1. J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal, ''Analytic pro-p Groups,'' London Math. Soc. Lecture Note Series, Vol. 157, Cambridge University Press, 1991.
2. S. A. Jennings, Substitution groups of formal power series, *Canad. J. Math.* **6** (1954), 325–340.
3. D. L. Johnson, The group of formal powers series under substitution, *J. Austral. Math. Soc.* **45** (1988), 296–302.
4. A. Lubotzky and J. S. Wilson, An embedding theorem for profinite groups, *Arch. Math.* **42** (1984), 397–399.
5. A. Shalev, Some problems and results in the theory of pro-p groups, *in* ''Groups '93 Galway/St Andrews,'' London Math. Soc. Lecture Note Series, Vol. 212, Cambridge University Press, 1995.
6. B. A. F. Wehrfritz, ''Infinite Linear Groups,'' Springer-Verlag, Berlin, 1973.
7. A. Weil, ''Basic Number Theory,'' Springer-Verlag, Berlin, 1967.
8. E. Witt, Der Existenzsatz für abelsche Funktionenkörper, *J. Math.* **173** (1935), 43–51.
9. E. Witt, Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f, *J. Math.* **174** (1936), 237–245.
10. I. O. York, ''Group of Formal Power Series,'' Ph.D. thesis, Nottingham University, 1990.