Proceedings of the Edinburgh Mathematical Society (1999) **42**, 333–339 ©

SOME NATURAL SUBGROUPS OF THE NOTTINGHAM GROUP

by RACHEL CAMINA

(Received 14th May 1997)

The Nottingham group can be described as the group of normalized automorphisms of the ring $\mathbf{F}_p[[t]]$, namely, those automorphisms acting trivially on $t\mathbf{F}_p[[t]]/t^2\mathbf{F}_p[[t]]$. In this paper we consider certain proper subgroups of the Nottingham group. We prove that these subgroups are identical to their normalizers and that some of them are isomorphic to the Nottingham group.

1991 *Mathematics subject classification:* 20E18.

Introduction

There has been considerable interest in pro-p groups in recent years due, in part, to the publication of the book by Dixon *et al.* in 1991 [**2**]. In particular, pro-p group theory has been used in the proofs of the "coclass" conjectures for finite p-groups [**7, 8**]. As interest in pro-p groups has grown so has interest in the so-called Nottingham group, first introduced to a wider audience through the papers of Johnson and York [**6, 9**]. The Nottingham group is a finitely generated pro-p group of finite width which is neither soluble nor p-adic analytic, so it does not fit into any "understood" class of pro-p groups. Also, it has recently been proved that every countably-based pro-p group can be embedded in the Nottingham group [**1**]. This paper aims to increase the understanding of this interesting group.

The Nottingham group can be thought of as a group of formal power series under substitution [**5, 6, 10, 9**], as a group of automorphisms of the ring $\mathbf{F}_p[[t]]$ or as a group of automorphisms of the field $\mathbf{F}_p((t))$. This paper considers certain proper subgroups of the Nottingham group, some of which turn out to be isomorphic to the Nottingham group. They also have the property of being identical to their normalizers, illustrating a difference between finite and infinite pro-p group theory.

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 Prof. Charles Leedham-Green. The referee must also be thanked for many useful remarks and comments.

Preliminaries

For a general reference to pro-p group theory see the book by Dixon *et al.* [2].

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

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

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

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

Remarks. (i) J is a finitely generated pro-p group [6, Prop. 1].

(ii) A can be considered as a profinite group. In this setting, J is the closure of the derived subgroup of A when $p \neq 2$ or 3. The proof is straightforward and is therefore omitted. Note that for $p = 2$ it is clear that $J = A$ and when $p = 3$ it can be shown that $J > A' > J'$.

(iii) Define $e_n \in J$ for $n \geq 1$ by $te_n := t(1 + t^n)$.

Note. Defined above is the "classic" Nottingham group. However more generally one can define $J(R)$, where R is a commutative ring with identity, to be the set of all formal power series

$$F = t\left(1 + \sum_{k \geq 1} \alpha_k t^k\right) \in R[[t]],$$

under formal substitution: given $G \in J(R)$, put $FG = G(1 + \sum_{k \geq 1} \alpha_k G^k)$. It then follows that $J(R)$ is a group [6, Prop. 1].

In general we can set the formal power series F to be the action of a map f on the indeterminate t considered as an element of the ring $R[[t]]$ of formal power series over R. i.e. $tf := F$. Extending the action of f to the whole of $R[[t]]$ determines an automorphism of $R[[t]]$. A simple calculation shows that $tfg = FG$ and we thus have $J(R)$ embedded as a subgroup of $\mathrm{Aut}(R[[t]])$.

Although, in this article, we have restricted the statements and proofs to the classic

Nottingham group, the results hold more generally. In particular, the non-topological statement of Proposition 1 is true for $J(R)$ when R is a commutative ring with 1. Theorem 1 holds if we restrict to the case when R is an integral domain (with a simplified proof if $\operatorname{char}(R)=0$). It is an interesting question whether the result is true when R has zero divisors. A version of Theorem 2 holds when R is a field, although the result is dependent on $\operatorname{char}(R)$. If $\operatorname{char}(R)=0$ we have that $J_{(x)}(R)\cong J(R)$ for all $x\geq 1$.

The subgroups $J_{(x)}$

Let x be a positive integer and define the subset $J_{(x)}$ of J as follows

$$J_{(x)}=\left\{g\in J: tg=t\left(1+\sum_{k=1}^{\infty}\alpha_k t^{kx}\right)\right\}.$$

Proposition 1. *$J_{(x)}$ is a closed infinite subgroup of J for $x\geq 1$. Further, $J_{(x)}$ is not open for $x>1$.*

Proof. Let $g,h\in J_{(x)}$, suppose $tg=t(1+\sum_{k=1}^{\infty}\alpha_k t^{kx})$ and $th=t(1+\sum_{i=1}^{\infty}\beta_i t^{ix})$. Then

$$\begin{aligned} tgh &= t\left(1+\sum_{i=1}^{\infty}\beta_i t^{ix}\right)\left(1+\sum_{k=1}^{\infty}\alpha_k t^{kx}\left(1+\sum_{i=1}^{\infty}\beta_i t^{ix}\right)^{kx}\right)\\ &= t\left(1+\sum_{j=1}^{\infty}\gamma_j t^{jx}\right)\end{aligned}$$

for some $\gamma_j\in\mathbf{F}_p$. In particular $gh\in J_{(x)}$.

The closure of $J_{(x)}$ follows from the fact that any sequence of elements in $J_{(x)}$ that converges in J clearly converges in $J_{(x)}$. So $J_{(x)}$ is compact and closed under multiplication and consequently closed under forming inverses.

Clearly $e_{kx}\in J_{(x)}$ for all $k\geq 1$, so $J_{(x)}$ is infinite. Finally, for $x>1$ the subgroup $J_{(x)}$ is of infinite index in J and therefore is not open. □

In a finite p-group the normalizer of a proper subgroup is always strictly greater than the subgroup. Consequently the following proposition, although simple, is of interest.

Theorem 1. $N_J(J_{(x)})=J_{(x)}$.

Proof. We prove this result by contradiction. Let $h\in N_J(J_{(x)})$ and suppose $h\notin J_{(x)}$. So if

https://doi.org/10.1017/S0013091500020289 Published online by Cambridge University Press

$$th = t\left(1+\sum_{i=1}^{\infty}\alpha_i t^i\right),$$

let α_k be the first non-zero coefficient such that k is not divisible by x. Then, consideration of h^{-1} shows that

$$th^{-1} = t\left(1+\sum_{j=1}^{\infty}\beta_j t^j\right)$$

for some $\beta_j \in \mathbf{F}_p$, where the first non-zero coefficient β_j such that j is not divisible by x is β_k and in fact $\beta_k = -\alpha_k$. Consider the coefficient of t^{x+k+1} in $h^{-1}e_x h$;

$$\begin{aligned} th^{-1}e_x h &= t\left(1+\sum_{i=1}^{\infty}\alpha_i t^i\right)\left(1+t^x\left(1+\sum_{i=1}^{\infty}\alpha_i t^i\right)^x\right) \\ &\quad\times\left(1+\sum_{j=1}^{\infty}\beta_j t^j\left(1+\sum_{i=1}^{\infty}\alpha_i t^i\right)^j\left(1+t^x\left(1+\sum_{i=1}^{\infty}\alpha_i t^i\right)^x\right)^j\right) \\ &= t\left(1+\sum_{i=1}^{\infty}\alpha_i t^i\right)\left(1+\sum_{j=1}^{\infty}\beta_j t^j\left(1+\sum_{i=1}^{\infty}\alpha_i t^i\right)^j\left(1+t^x\left(1+\sum_{i=1}^{\infty}\alpha_i t^i\right)^x\right)^j\right) \\ &\quad+t^{x+1}\left(1+\sum_{i=1}^{\infty}\alpha_i t^i\right)^x\left(1+\sum_{i=1}^{\infty}\alpha_i t^i\right) \\ &\quad\times\left(1+\sum_{j=1}^{\infty}\beta_j t^j\left(1+\sum_{i=1}^{\infty}\alpha_i t^i\right)^j\left(1+t^x\left(1+\sum_{i=1}^{\infty}\alpha_i t^i\right)^x\right)^j\right). \end{aligned}$$

Note that by the definition of h^{-1}

$$t = t\left(1+\sum_{i=1}^{\infty}\alpha_i t^i\right)\left(1+\sum_{j=1}^{\infty}\beta_j t^j\left(1+\sum_{i=1}^{\infty}\alpha_i t^i\right)^j\right),$$

so the expression of $th^{-1}e_x h$ above simplifies.

Due to the properties of k, the only way we can form t^{x+k+1} is as $t \times t^x \times t^k$ or $t^{x+1} \times t^k$. After consideration of the above equations we see that the coefficient of t^{x+k+1} in $th^{-1}e_x h$ is

$$k\beta_k + x\alpha_k = (x-k)\alpha_k.$$

Thus since $h \in N_J(J_{(x)})$ we must have $x \equiv k \bmod p$. So in particular $N_J(J_{(p)}) = J_{(p)}$.

For the result when $x \not\equiv 0 \bmod p$, consider the coefficient of t^{2x+k+1} in $th^{-1}e_{2x}h$. In a similar way to above, if $h^{-1}e_{2x}h$ is to lie in $J_{(x)}$ it follows that $2x \equiv k \bmod p$. However then $x \not\equiv k \bmod p$ and $h^{-1}e_x h \notin J_{(x)}$, a contradiction, and no such α_k exists.

Now suppose $x = p^n$ and $k = \bar{k}p^s$, where $(\bar{k}, p) = 1$ and $s < n$. Consider the coefficient of t^{xp^s+k+1} in $th^{-1}e_x h$. In the first summand the coefficient is $\bar{k}\beta_k$; however in the second summand this term does not appear. Thus $\beta_k = 0$ and such an h does not exist.

The last case to consider is when $x = \bar{x}p^n$ and $(\bar{x}, p) = 1$. By the argument of the previous paragraph we can assume that $h \in J_{(p^n)}$. So suppose $k = \bar{k}p^n$ and that k is not a multiple of x (so $\bar{k}$ is not a multiple of $\bar{x}$). If $\bar{x} < \bar{k}$ consider the coefficient of t^{xp^n+k+1} in $th^{-1}e_x h$. Again the coefficient in the first summand is given by $\bar{k}\beta_k$ and the term does not appear in the second summand, hence the result. If $\bar{k} < \bar{x}$ consider the coefficient of t^{kp^n+x+1}. This term appears in the second summand with coefficient $\bar{x}\alpha_k$ but does not appear in the first summand and thus $\alpha_k = 0$. □

We also have the following theorem. To ease notation we denote $J(\mathbf{F}_p((t^x)))$ by $J(t^x)$ for x a positive integer.

Theorem 2.

$$\begin{aligned} J_{(x)} &\cong J \quad \text{if } x \not\equiv 0 \pmod{p}, \\ &\not\cong J \quad \text{if } x \equiv 0 \pmod{p}. \end{aligned}$$

Proof. Let $g \in J(t)_{(x)}$; then

$$tg = t\left(1 + \sum_{k=1}^{\infty} \alpha_k t^{kx}\right)$$

for some $\alpha_k \in \mathbf{F}_p$. So

$$\begin{aligned} t^x g &= (tg)^x \\ &= t^x \left(1 + \sum_{k=1}^{\infty} \alpha_k t^{kx}\right)^x \end{aligned}$$

and thus $g|_{\mathbf{F}_p((t^x))} \in J(t^x)$. So we can define the following map θ

$$\begin{aligned} \theta : J(t)_{(x)} &\to J(t^x) \\ g &\mapsto g|_{\mathbf{F}_p((t^x))}. \end{aligned}$$

We show that when $x \not\equiv 0 \bmod p$, θ is an isomorphism. Then, as $J(t^x) \cong J(t)$, since

$\mathbf{F}_p((t^x)) \cong \mathbf{F}_p((t))$, we have the result for this case. Since θ is clearly a homomorphism we just have to show that given $h \in J(t^x)$ then there exists a unique element $g \in J(t)$ such that $(t^x)h = (t^x)g$ and in fact this unique solution g actually lies in $J(t)_{(x)}$. The existence of g is equivalent to solving an equation of the following type:

$$\begin{aligned} t^x\left(1+\sum_{i=1}^{\infty}\beta_i t^{ix}\right) &= (t^x)h \\ &= (t^x)g \\ &= (tg)^x \\ &= t^x\left(1+\sum_{j=1}^{\infty}\alpha_j t^j\right)^x, \end{aligned}$$

where h and hence the β_i are given, and g and so the α_j are to be found.

We now construct a solution to the above equation and hence show that g exists. If $(t^x)h = t^x$, simply set $tg = t$, and we are done. If $(t^x)h \neq t^x$, then β_r, the first non-zero coefficient in $\sum_{i=1}^{\infty} \beta_i t^i$, is well-defined. So, we want

$$\begin{aligned} t^x\left(1+\sum_{i=1}^{\infty}\beta_i t^{ix}\right) &= t^x + \beta_r t^{(r+1)x} + \cdots \\ &= t^x\left(1+\sum_{j=1}^{\infty}\alpha_j t^j\right)^x. \end{aligned}$$

As $x \not\equiv 0 \bmod p$ we must choose the first non-zero coefficient in $\sum_{j=1}^{\infty} \alpha_j t^j$ to be α_s, where $s = rx$ and $x\alpha_s = \beta_r$.

Now we proceed inductively. Suppose α_j has been chosen for $1 \leq j \leq l-1$, and is zero if j is not divisible by x. Then, as all non-zero powers of t in $(t^x)h$ are powers of t^x, we choose α_l to be non-zero only if l is divisible by x. In this case α_l is uniquely defined. Thus we can construct a unique solution g, of the required form.

$J_{(x)}$, unlike J, does not contain any elements of finite order when $x \equiv 0 \bmod p$ [**10**, Thm 5.5.4]. Hence $J_{(x)} \not\cong J$ in this case. □

The author thanks the referee for the following remarks.

Remarks. (i) Suppose $(x, p) = 1$. The isomorphism θ, from the previous proof, is a natural isomorphism between $J_{(x)}$ and J. If $g \in J_{(x)}$ is such that $tg = t(1 + \sum_{k=1}^{\infty} \alpha_k t^k)$ then $(g)\theta \in J$ is defined by $t(g)\theta = t(1 + \sum_{k=1}^{\infty} \alpha_k t^k)^x$. Thus $J_{(x)(y)}$ is naturally defined and is equal to $J_{(xy)}$.

(ii) If $J_{(x)}$ were properly contained in its normaliser then, since its centraliser is trivial, it would have a non-trivial group of p outer automorphisms. By a theorem of Gaschütz [**4**, Satz 19.1] a finite p-group of order greater than p does have outer automorphisms of order p. This is known to fail for some pro-p groups [**3**, Chapter III, Section (e)]. The previous two theorems suggest it will also fail for J.

REFERENCES

1. R. Camina, Subgroups of the Nottingham group, *J. Algebra* **196** (1997), 101–113.

2. J. D. Dixon, M. P. F. du Sautoy, A. Mann and D. Segal, *Analytic pro-p Groups* (London Mathematical Society Lecture Note Series **157**, Cambridge University Press, Cambridge, 1991).

3. G. Klaas, C. R. Leedham-Green and W. Plesken, *Linear Pro-p-Groups of Finite Width* (Lecture Notes in Mathematics **1674**, Springer-Verlag, Berlin-Heidelberg, 1997).

4. B. Huppert, *Endliche Gruppen I* (Springer-Verlag, Berlin-Heidelberg, 1967).

5. S. A. Jennings, Substitution groups of formal power series, *Canad. J. Math.* **6** (1954), 325–340.

6. D. L. Johnson, The group of formal power series under substitution, *J. Austral. Math. Soc.* **45** (1988), 296–302.

7. C. R. Leedham-Green, The structure of finite p-groups, *J. London Math. Soc.* **50** (1994), 49–67.

8. A. Shalev, The structure of finite p-groups: effective proof of the coclass conjectures, *Invent. Math.* **115** (1994), 315–345.

9. I. O. York, The exponent of certain p-groups, *Proc. Edinburgh Math. Soc.* **33** (1990), 483–490.

10. I. O. York, *The group of formal power series* (Ph.D Thesis, Nottingham University, 1990).

Department of Mathematics and Computing Science
University of the South Pacific
Suva
Fiji Islands
E-mail address: camina_r@manu.usp.ac.fj

https://doi.org/10.1017/S0013091500020289 Published online by Cambridge University Press