Proceedings of the Edinburgh Mathematical Society (1990) 33, 483–490 ©

THE EXPONENT OF CERTAIN FINITE p-GROUPS

by I. O. YORK

(Received 15th January 1990)

In this paper, for **R** a commutative ring, with identity, of characteristic p, we look at the group $\mathbf{G}(\mathbf{R})$ of formal power series with coefficients in **R**, of the form

$$\sum_{i=0}^{\infty} a_i x^i,\ a_0=0,\ a_1=1$$

and the group operation being substitution. The results obtained give the exponent of the quotient groups $\mathbf{G}_n(\mathbf{R})$ of this group, $n\in\mathbb{N}$.

1980 *Mathematics subject classification* (1985 Revision): 20D15.

Introduction

In this paper we will deal with the group $\mathbf{G}(\mathbf{R})$ of formal power series

$$f(x)=x+a_2x^2+a_3x^3+\dots$$

where the coefficients are elements of a commutative ring **R**, with identity, and the group operation is substitution. A study of this group is carried out in [3] and also of the groups $\mathbf{G}_n(\mathbf{R})$ whose elements can be considered as elements of $\mathbf{G}(\mathbf{R})$ truncated to n terms. Such objects were studied from other points of view in [1]. The groups when **R** is a commutative ring, with identity, of characteristic p are studied by the author as due to their large class they can often achieve, or at least approach, bounds on such properties as derived length of classes of p-groups studied by other authors. Often the power structure of the groups $\mathbf{G}_n(\mathbf{R})$, **R** a commutative ring, with identity, of characteristic p,needs to be known in order to show that they satisfy the conditions on the p-groups to which the bounds refer. Hence the purpose of this paper is to find the exponent of the groups $\mathbf{G}_n(\mathbf{R})$ for all $n\in\mathbb{N}$ and for **R** a commutative ring, with identity, of characteristic p.

1. The exponent of the groups $\mathbf{G}_n(\mathbf{R})$, where R is a commutative ring, with identity, of characteristic p, $p\geqq 3$

We start with some definitions and notation. If $\alpha\in\mathbf{G}(\mathbf{R})$, $\alpha\neq x$ and $\alpha=\sum_{i=1}^{\infty} a_i x^i$, $a_1=1$, $a_i=0$ (for $2\leqq i<n$) and $a_n\neq 0$ we say $deg(\alpha)=n$. Also define the subset $\mathbf{K}_r$ of $\mathbf{G}(\mathbf{R})$

by $\mathbf{K}_r = \{\alpha \in \mathbf{G}(\mathbf{R}): deg(\alpha) > r\}$, then $\mathbf{K}_r$ is a normal subgroup of $\mathbf{G}(\mathbf{R})$, the proof of which is in [1], and we define $\mathbf{G}_n(\mathbf{R})$ as the quotient group $\mathbf{G}(\mathbf{R})/\mathbf{K}_n$.

The following notation will be used in this paper: If $\alpha \in \mathbf{G}(\mathbf{R})$ then $\alpha^{(m)}$ is the mth iterate of α, while α^m is the mth power of α. Furthermore we shall denote by $\mathbf{R}[[x]]$ the algebra over $\mathbf{R}$ of all formal power series with indeterminant x and coefficients in $\mathbf{R}$, a commutative ring with identity.

Lemma 1. ([2, Theorem 2.5]) *If* $\mathbf{R}$ *has characteristic* p, *then* $\mathbf{K}_r^{(p)} \subseteq \mathbf{K}_{rp}$.

The question now asked is: what more can we say when $\mathbf{R}$ is a commutative ring, with identity?

Observation 2. *Let* $\mathbf{R}$ *be a commutative ring, with identity and* $\alpha \in \mathbf{G}(\mathbf{R})$. *Then the map* $\eta: \mathbf{R}[[x]] \to \mathbf{R}[[x]]$ *given by* $g(x) \mapsto g(\alpha)$, *is an* $\mathbf{R}$*-algebra automorphism. Further* η *preserves the ideal* (x).

The proof of Observation 2 is standard and hence is omitted.

Notation. Let z_n be defined as $z_n = p^n + p^{n-1} + \cdots + p + 2$.

Lemma 3. *Let* $\alpha \in \mathbf{G}(\mathbf{R})$ *and* η *be as defined in Observation 2. Then on the basis* $x, x^2, \ldots, x^m, \ldots$ *of* (x), *the action of* η *is given by:*

$$\begin{pmatrix} x \\ x^2 \\ x^3 \\ \vdots \end{pmatrix} \mapsto \mathbf{M} \begin{pmatrix} x \\ x^2 \\ x^3 \\ \vdots \end{pmatrix},$$

where $\mathbf{M} = (m_{i,j})$ *is the matrix such that* $m_{i,j}$ = *coefficient of* x^j *in* α^i.

Proof. As by Observation 2 η preserves (x), we know the action of η on the given basis elements of (x) is in the form of the lemma for some $\mathbf{M}$. By the definition of η, $\eta(x^j) = \alpha^j$. Thus we need to prove that the jth row of the vector

$$\mathbf{M} \begin{pmatrix} x \\ x^2 \\ x^3 \\ \vdots \end{pmatrix} \text{ is } \alpha^j.$$

Now by the definition of $\mathbf{M}$ the jth row in this vector is

$$\sum_{i=1}^{\infty} (\text{coefficient of } x^i \text{ in } \alpha^j)\, x^i = \alpha^j.$$

Lemma 4. *If* $\alpha_1, \alpha_2 \in \mathbf{G}(\mathbf{R})$, *and the maps* $\eta_i: \mathbf{R}[[x]] \to \mathbf{R}[[x]]$ *are given by* $g(x) \mapsto g(\alpha_i)\,(i=1,2)$, *and if* $\mathbf{M}_i$ *is the matrix of Lemma 3 corresponding to* α_i, $(i=1,2)$ *then* $\mathbf{M}_1\mathbf{M}_2$ *is the matrix corresponding to* $\alpha_1(\alpha_2) \in \mathbf{G}_n(\mathbf{R})$.

Proof. Now we have that if $\eta: \mathbf{R}[[x]] \to \mathbf{R}[[x]]$ is given by $g(x) \mapsto g(\alpha_1(\alpha_2))$ then

$$\begin{aligned}
\eta(x^i) &= (\alpha_1(\alpha_2))^i \\
&= \alpha_1^i(\alpha_2) \\
&= \sum_{j=1}^{\infty} \sum_{k=1}^{\infty} (\text{coefficient of } x^k \text{ in } \alpha_1^i)(\text{coefficient of } x^j \text{ in } \alpha_2^k)\, x^j \\
&= i\text{th row in the vector } \mathbf{M}_1\mathbf{M}_2 \begin{pmatrix} x \\ x^2 \\ x^3 \\ \vdots \end{pmatrix}
\end{aligned}$$

because using the definition of $\mathbf{M}_1$ and $\mathbf{M}_2$

$$(\mathbf{M}_1\mathbf{M}_2)_{i,j} = \sum_{k=1}^{\infty} (\text{coefficient of } x^k \text{ in } \alpha_1^i)\,(\text{coefficient of } x^j \text{ in } \alpha_2^k).$$

Lemma 5. *Let* $\mathbf{M}$ *be defined as in Lemma 3, define* Δ *by* $\mathbf{M} = I + \Delta$ *where* I *is the identity matrix, then*

$$(\Delta^{p^m})_{1,d} = \sum_{\mathbf{j}} \Delta_{1,j_1} \Delta_{j_1,j_2} \cdots \Delta_{j_l,d} \tag{1}$$

where $l = p^m - 1$ *and* $\mathbf{j} = \{(j_1, \ldots, j_l) : 2 \leqq j_1 < j_2 < \cdots < j_l \leqq d-1\}$.

Further if $d \not\equiv 0 \pmod p$ *and the set* $(j_1, \ldots, j_l)$ *gives a non-zero term in the right hand side of* (1) *then* $j_i \not\equiv 0 \pmod p\,(1 \leqq i \leqq l)$.

Proof. Equation (1) follows directly from the definitions. We prove by contradiction that if $d \not\equiv 0 \pmod p$ then for a term in the right hand side of (1) to be non-zero it is necessary that,

$$j_i \not\equiv 0 \pmod p\,(1 \leqq i \leqq p^m - 1).$$

Thus we assume that in a non-zero term in the right hand side of (1), $j_i \equiv 0 \pmod p$

for some i, $1 \leqq i \leqq p^m - 1$, and show by an inductive argument that this implies that $d \equiv 0 \pmod{p}$ which is the required contradiction.

Examination of (1) gives that to complete the inductive argument and obtain the required contradiction we only need prove that

$$r \equiv 0 \pmod{p},\ s \not\equiv 0 \pmod{p} \Rightarrow \Delta_{r,s} \equiv 0 \pmod{p}.$$

Now we know,

$$\alpha^{pt} = \sum_{j=1}^{\infty} m_{pt,j} x^j.$$

It is clear that $\theta: \alpha \mapsto \alpha^p$ is a endomorphism of the ring of formal power series. So we obtain,

$$\alpha^{pt} = (\alpha^t)^p = \sum_{j=1}^{\infty} (m_{t,j} x^j)^p$$

$$= \sum_{j=1}^{\infty} m_{t,j}^p x^{pj}.$$

Thus we conclude that,

$$m_{pt,j} = \begin{cases} m_{t,k}^p & \text{if } j = pk \\ 0 & \text{if } j \not\equiv 0 \pmod{p}. \end{cases}$$

Therefore as,

$$\Delta_{r,s} = \text{coefficient of } x^s \text{ in } \alpha^r$$

we have the contradiction.

Theorem 6. *Let* $\mathbf{R}$ *be a commutative ring, with identity of characteristic* $p \geqq 3$ *and* z_m *as defined above. Then for* $n < z_m$ *the exponent of* $\mathbf{G}_n(\mathbf{R})$ *is at most* p^m.

Proof. (In fact the proof of the following equivalent statement: If $\mathbf{R}$ is a commutative ring, with identity, of characteristic $p \geqq 3$ and z_m is as defined above. Then for all $\alpha \in \mathbf{G}(\mathbf{R})$, $\alpha^{(p^m)} \in \mathbf{K}_{z_m - 1}$.)

Let $\alpha \in \mathbf{G}(\mathbf{R})$

The map $\eta: \mathbf{R}[[x]] \to \mathbf{R}[[x]]$, given by

$$g(x) \mapsto g(\alpha)$$

is an **R**-algebra automorphism, by Observation 2.

By Lemma 3 the action of η on the basis $x, x^2, \dots, x^n, \dots$ of (x) is given by:

$$\begin{pmatrix} x \\ x^2 \\ x^3 \\ \vdots \end{pmatrix} \mapsto \mathbf{M} \begin{pmatrix} x \\ x^2 \\ x^3 \\ \vdots \end{pmatrix},$$

where $\mathbf{M} = (m_{ij})$ is the matrix such that m_{ij} = coefficient of x^j in α^i.

By Lemma 4 the action of the **R**-algebra automorphism of $\mathbf{R}[[x]]$, given by $g(x) \mapsto g(\alpha^{(r)})$ on the basis $x, \dots, x^n, \dots$ is given by:

$$\begin{pmatrix} x \\ x^2 \\ x^3 \\ \vdots \end{pmatrix} \mapsto \mathbf{M}^r \begin{pmatrix} x \\ x^2 \\ x^3 \\ \vdots \end{pmatrix}. \tag{3}$$

Put $\mathbf{M} = I + \Delta$, where I is the identity matrix, so that $\mathbf{M}^{p^k} \equiv I + \Delta^{p^k} \pmod p$. Now (3) gives us that:

$$(M^{p^k})_{1,i} = \text{coefficient of } x^i \text{ in } \alpha^{(p^k)} \tag{4}$$

Hence in order to prove the theorem we require that,

$$(\Delta^{p^m})_{1,i} \equiv 0 \pmod p \quad \text{for all} \quad 1 \leqq i \leqq z_m - 1.$$

We now proceed to prove this by induction on m. For $m=0$: $(\Delta)_{1,i} \equiv 0 \pmod p$ for all $1 \leqq i \leqq z_0 - 1 = 1$ as Δ has 0 on and below the main diagonal. Now we assume for $j < m$ that

$$(\Delta^{p^j})_{1,i} \equiv 0 \pmod p \quad \text{for all} \quad 1 \leqq i \leqq z_j - 1.$$

Thus using the inductive hypothesis and (4) we have that

$$\alpha^{(p^{m-1})} \in \mathbf{K}_{z_{m-1}-1}$$

and thus by Lemma 1 that

$$\alpha^{(p^m)} \in \mathbf{K}_{p(z_{m-1}-1)}.$$

Hence by again using (4), in order to complete the inductive step it is only now necessary to prove that:

$$(\Delta^{p^m})_{1,z_m-1} \equiv 0 \pmod p.$$

By Lemma 5,

$$(\Delta^{p^m})_{1,z_m-1} = \sum_{\mathbf{j}} \Delta_{1,j_1} \Delta_{j_1,j_2} \cdots \Delta_{j_l,z_m-1} \tag{5}$$

where $l = p^m - 1$ and

$$\mathbf{j} = \{(j_1, j_2, \ldots, j_{p^m-1}) : 2 \leqq j_1 < j_2 < \cdots < j_{p^m-1} \leqq z_m - 2\}.$$

Now the number of integers in the range 2 to $z_m - 2$ divisible by p is $p^{m-1} + p^{m-2} + \cdots + 1$, hence the number of integers in this range not divisible by p is $p^m - 2$. By definition, $z_m - 1 \equiv 1 \not\equiv 0 \pmod p$ so we know by Lemma 5 that for a non-zero term in the right hand side of (5) we are required to choose an ordered set of integers $(j_1, \ldots, j_{p^m-1})$ such that

$$2 \leqq j_1 < j_2 < \cdots < j_{p^m-1} \leqq z_m - 2 \quad \text{and} \quad j_s \not\equiv 0 \pmod p \, (1 \leqq s \leqq p^m - 1),$$

which is not possible as there are only $p^m - 2$ integers in the range 2 to $z_m - 2$ not divisible by p. Hence $(\Delta^{p^m})_{1,z_m-1} \equiv 0 \pmod p$, which completes the inductive step.

We thus have the required result that,

$$(\Delta^{p^m})_{1,i} \equiv 0 \pmod p \quad \text{for all} \quad 1 \leqq i \leqq z_m - 1.$$

Having obtained a bound for the exponent we now consider the powers of a specific element in order to show that the bound is achieved.

Theorem 7. *Let z_k be as defined above, $\mathbf{R}$ be any commutative ring, with identity, of characteristic p, $p \geqq 3$. Then for all $k \in \mathbb{N}$, the p^kth iterate of $x + x^2$ over $\mathbf{R}$ is $x + x^{z_k} + \cdots$.*

Proof. We consider the map η defined in Observation 2 in the special case of $\alpha = x + x^2$. Then as before putting $\mathbf{M} = I + \Delta$, where I is the identity matrix, so that $\mathbf{M}^{p^k} \equiv I + \Delta^{p^k} \pmod p$, where $\mathbf{M}$ is the matrix defined in Lemma 3 in the special case $\alpha = x + x^2$.

By Theorem 6 we have that $(x + x^2)^{(p^k)} \in \mathbf{K}_{z_k - 1}$ and thus by the definition of $\mathbf{M}$ and Δ,

$$(\Delta^{p^k})_{1,q} \equiv 0 \pmod p \, (2 \leqq q \leqq z_k - 1).$$

It is clear by definition that

$$\Delta_{i,j} = \begin{cases} \dbinom{i}{j-1} & \text{if} \quad 1 < j \leqq 2i \\ 0 & \text{otherwise.} \end{cases}$$

In this case it is thus obvious that all non-zero terms in the right hand side of (1) with $d=z_k$ have $j_1=2$. So

$$(\Delta^{p^k})=\sum_{\mathbf{j}'}\Delta_{2,j_2}\dots\Delta_{j_l,z_k} \tag{6}$$

where $\mathbf{j}'=\{(j_2,\dots,j_l): 3\leqq j_2<j_3<\dots<j_l\leqq z_k-1\}$ and $l=p^k-1$.

As $z_k\equiv 2\not\equiv 0 \pmod p$, by Lemma 5 we obtain that for a non-zero term in the right hand side of (6) we must have,

$$j_s\not\equiv 0 \pmod p \quad \text{for all} \quad 2\leqq s\leqq p^k-1.$$

As we are required to choose an ordered set $(j_2,\dots,j_{p^k-1})$ of integers such that $3\leqq j_2<j_3<\dots<j_{p^k-1}\leqq z_k-1$, and there are p^k-2 integers in the range 3 to z_k-1 not divisible by p, there can only be one non-zero term; which is

Case (*a*): $p>3$

$(\Delta^{p^k})_{1,z_k}=$

$$\binom{2}{1}\binom{3}{1}\cdots\binom{p-2}{1}\binom{p-1}{2}\binom{p+1}{1}\cdots\binom{2p-2}{1}\binom{2p-1}{2}\binom{2p+1}{1}\cdots\binom{dp-1}{2}\binom{dp+1}{1}$$

where

$$z_k=dp+2,\ d\in\mathbb{N}.$$

Now we know that for $f\in\mathbb{N}$ that,

$$\begin{aligned}\binom{fp+2}{1}\binom{fp+3}{1}\cdots\binom{fp+p-2}{1}&=(fp+2)\dots(fp+p-2)\\ &\equiv 2.3\dots(p-2) \pmod p\\ &\equiv 1 \pmod p\ \text{(By Wilson's Theorem)}\end{aligned}$$

$$\text{Further}\ \binom{fp-1}{2}\binom{fp+1}{1}\equiv 1 \pmod p\ \text{for all}\ f\in\mathbb{N}.$$

Case (*b*): $p=3$

$$(\Delta^{p^k})_{1,z_k}=\binom{4}{1}\binom{5}{2}\binom{7}{1}\binom{8}{2}\cdots\binom{3d-1}{2}\binom{3d+1}{1}$$

where

$$z_k=3d+2,\ d\in\mathbb{N}.$$

Now we know that for $f\in\mathbb{N}$ that,

$$\binom{3f+1}{1} \equiv 1 \pmod p$$

and

$$\binom{3f+2}{2} \equiv 1 \pmod p.$$

Hence the result follows in both cases.

Combining Theorems 6 and 7 we readily obtain the following theorem.

Theorem 8. *Let* $\mathbf{R}$ *be a commutative ring, with identity, of characteristic* $p \geqq 3$ *and* z_m *be as defined as above. Then for* $z_{m-1} \leqq n < z_m$ *the exponent of* $\mathbf{G}_n(\mathbf{R})$ *is* p^m.

2. The exponent of the groups $\mathbf{G}_n(\mathbf{R})$, where $\mathbf{R}$ is an integral domain of characteristic 2

This case differs substantially from the case of odd p. For example the exponent is the order of $x+x^3$ rather than $x+x^2$ for $\mathbf{R}=\mathbb{Z}_2$ and is the order of $x+x^2+ax^3$ (where $a \in \mathbf{R}$, $a \neq 0$, $a \neq 1$) when $\mathbf{R} \neq \mathbb{Z}_2$. As this case is of less interest from the point of view of the applications indicated in the introduction we merely summarize.

Theorem 9. *The exponent of* $\mathbf{G}_n(\mathbb{Z}_2)$ *is* 2^m, *where* $2^m+1 \leqq n < 2^{m+1}+1$ *for* $n \geqq 5$.

Theorem 10. *The exponent of* $\mathbf{G}_n(\mathbf{R})$, *where* $\mathbf{R}$ *is an integral domain of characteristic-two and* $\mathbf{R} \neq \mathbb{Z}_2$ *is* 2^m, *where* $2^m \leqq n < 2^{m+1}$, *i.e.* $m=[\log_2 n]$.

Acknowledgements. I wish to express my gratitude to R. W. K. Odoni who by proving Theorem 7 in the special case of $k=1$ provided the underlying method used in this paper. I would also like to thank the referee for his comments which gave a simpler and shorter proof of Lemma 5, as well as pointing out that the working in Section 1 applied not only to fields of characteristic p but to all the rings studied in the section.

REFERENCES

1. I. N. Baker, Permutable power series and regular iteration, *J. Austral. Math. Soc.* **2** (1961–62), 265–294.

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 power series under substitution, *J. Austral. Math. Soc.* **45** (1988), 296–302.

University of Nottingham
University Park
Nottingham
NG7 2RP