J. Austral. Math. Soc. (*Series A*) **45** (1988), 296–302

THE GROUP OF FORMAL POWER SERIES UNDER SUBSTITUTION

D. L. JOHNSON

(Received 20 March 1987; revised 29 July 1987)

Communicated by H. Lausch

Abstract

This is a study of formal power series under the binary operation of formal composition from a group-theoretical point of view. Various "large" properties are derived.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*) (1985 *Revision*): 20 F 99.

The aim of this article is to study formal power series, under the binary operation of formal substitution, from a group-theoretical point of view. This is prompted by [7], and is in the spirit of [9], [10], rather than of [1], [2], [4], [5], [6], [8], where both motivation and methodology come either from analysis or other areas of algebra. It seems to me that such an approach is justified on two grounds. First of all, ideas from group theory suggest new methods, and conversely, the groups involved arise in such a natural way as to be worthy of study in their own right.

It is a pleasure to acknowledge the hospitality of Monash University, the Australian National University, the National University of Singapore, and the University of Adelaide during the preparation of this article, and to record thanks to colleagues at these institutions and elsewhere for many valuable suggestions.

1. Definitions and notation

Given a commutative ring R with identity, let $G(R)$ denote the set of all formal power series

$$\alpha = \sum_{k\geq 0} a_k x^k \in R[[x]], \qquad a_0 = 0, a_1 = 1,$$

under formal substitution: given $\beta \in G(R)$, put $\alpha\beta = \sum_{k\geq 0} a_k \beta^k$. We write $\alpha = x + ax^n +$ to denote that $a_k = 0$ for $2 \leq k < n$. When $a = a_n \neq 0$, it is called the leading coefficient of α, $l(\alpha) = a$, and then n is called the degree of α, $n = d(\alpha)$. When $\alpha \in R[x]$, we write $\deg(\alpha)$ for its polynomial degree.

Now for each $n \in \mathbf{N}$, put $K_n = \{\alpha \in G(R) | d(\alpha) > n\}$, and define a relation on $G(R)$ by

$$\alpha \sim_n \beta \Leftrightarrow \alpha - \beta + x \in K_n,$$

that is, $\alpha - \beta = x^{n+1}\gamma$ for some $\gamma \in R[[x]]$.

LEMMA 1. *For each $n \in \mathbf{N}$,*
(i) *$\sim_n$ is an equivalence relation on $G(R)$,*
(ii) *$\sim_n$ respects composition: if $\alpha \sim_n \alpha'$ and $\beta \sim_n \beta'$, then $\alpha\beta \sim_n \alpha'\beta'$,*
(iii) *each $\sim_n$-class contains exactly one polynomial $\alpha \in G(R)$ with $\deg(\alpha) \leq n$.*

The proof is straightforward and we omit it.

Define $G_n(R) = G(R)/\sim_n$; formal substitution in $G(R)$ thus induces a binary operation in each $G_n(R)$, which may be thought of as composition of polynomials modulo x^{n+1}, and we have natural homomorphisms

$$\tau_n : G(R) \to G_n(R), \quad \sigma_n : G_{n+1}(R) \to G_n(R)$$

such that $\tau_{n+1}\sigma_n = \tau_n$ for all $n \in \mathbf{R}$. We think of these as truncating maps, and note that $\operatorname{Ker}\tau_n$, which is just the pre-image of the $\sim_n$-class containing x, is just K_n.

PROPOSITION 1. (i) *For each $n \in \mathbf{N}$, $G_n(R)$ is a group.*
(ii) *$G(R)$ is the inverse limit of the system $\{G_n, \sigma_n : G_{n+1} \to G_n | n \in \mathbf{N}\}$.*
(iii) *$G(R)$ is a group.*

The proof is again routine and we omit it, except to say that for the associative law in $G_n(R)$, use Lemma 1(iii) and the fact that composition of polynomials is associative (since $R[[x]]$ acts on R by substitution).

https://doi.org/10.1017/S1446788700031001 Published online by Cambridge University Press

2. Large properties

This section concerns four properties $G(R)$ shares with the free group F_2 of rank 2, under various restrictions on R.

PROPOSITION 2. *If R^+ is torsionfree, then so is $G(R)$.*

PROOF. If $\alpha, \beta \in G(R) \setminus \{x\}$ then a direct calculation shows that

$$d(\alpha) = d(\beta) \Rightarrow l(\alpha\beta) = l(\alpha) + l(\beta), \tag{1}$$

where we interpret $l(x) = 0$. It follows that

$$l(\alpha^n) = nl(\alpha), \qquad n \in \mathbf{Z},\ \alpha \in G(R), \tag{2}$$

from which the assertion is obvious.

LEMMA 2. *If $\alpha = x + ax^m +$, $\beta = x + bx^n +$, then*

$$\alpha^{-1}\beta^{-1}\alpha\beta = x + ab(m-n)x^{m+n-1} + . \tag{3}$$

PROOF. Put

$$\alpha = x + ax^m + x^{m+1}f(x), \qquad \beta = x + bx^n + x^{n+1}g(x),$$

where $f(x), g(x) \in R[[x]]$ and work in $G_{m+n-1}(R)$, that is, modulo x^{m+n}:

$$\begin{aligned} \alpha\beta &= \beta + a(x + bx^n + x^{n+1}g(x))^m + (x + bx^n + x^{n+1}g(x))^{m+1}f(\beta) \\ &= \beta + ax^m + mabx^{m+n-1} + x^{m+1}f(x) \\ &= \alpha + \beta + mabx^{m+n-1} - x. \end{aligned} \tag{4}$$

Hence, by (2) with $n = -1$,

$$\alpha^{-1}\beta^{-1} = \alpha^{-1} + \beta^{-1} + mabx^{m+n-1} - x,$$

and so

$$\begin{aligned} \alpha^{-1}\beta^{-1}\alpha &= x + \beta^{-1}\alpha + mab\alpha^{m+n-1} - \alpha \\ &= x + (\beta^{-1} + \alpha - nabx^{m+n-1} - x) + mabx^{m+n-1} - \alpha, \quad \text{by (4)}, \\ &= \beta^{-1} + ab(m-n)x^{m+n-1}. \end{aligned}$$

Finally,

$$\alpha^{-1}\beta^{-1}\alpha\beta = x + ab(m-n)\beta^{m+n-1} = x + ab(m-n)x^{m+n-1}.$$

PROPOSITION 3. *$G(R)$ is residually nilpotent.*

PROOF. It follows at once from (3) that $\gamma_2(G(R)) = G(R)' \subseteq K_3$ (see Section 1), and by induction on n that $\gamma_n(G(R)) \subseteq K_{n+1}$. Since $\bigcap_{n\in\mathbf{N}} K_n = \{x\}$, the result follows.

https://doi.org/10.1017/S1446788700031001 Published online by Cambridge University Press

LEMMA 3 [1, PROPOSITION 2.1]. *Let R be an integral domain of characteristic zero. Given $\alpha = x + ax^m + \varepsilon G(R)$, $a \neq 0$, and $b \in R$, there is at most one $\beta = x + bx^m + \varepsilon G(R)$ that commutes with α.*

PROOF (J. S. WILSON). If β' also commutes with α and satisfies $d(\beta') = m$ and $l(\beta') = b$, then α commutes with $\beta'\beta^{-1}$. But by (1), $d(\beta'\beta^{-1}) > m$, whereas it follows from (3) that commuting elements of $G(R) \setminus \{x\}$ have the same degree. Thus, $\beta' = \beta$.

The next result was proved independently, using essentially the same method, by W. D. Nichols.

PROPOSITION 4. *Let R be a principal ideal domain of characteristic zero. If $\alpha, \beta \in G(R)$ commute, then α and β are powers of a common element. Commutation is an equivalence relation on $G(R) \setminus \{x\}$.*

PROOF. Assume that $\alpha\beta = \beta\alpha$, where $\alpha, \beta \in G \setminus \{x\}$, so that (by (3) again),

$$\alpha = x + ax^m +, \qquad \beta = x + bx^m +, \qquad ab \neq 0.$$

Putting $h = (a, b)$, the highest common factor, we have

$$h = ra + sb, \qquad a = ha', \qquad b = hb',$$

for some $r, s, a', b' \in R$. Now define

$$\gamma = \alpha^r \beta^s = x + hx^m +,$$

by (1) and (2). Now α commutes with $\gamma^{a'} = x + ax^m +$, whence $\alpha = \gamma^{a'}$, by Lemma 3. Similarly, $\beta = \gamma^{b'}$.

Now it follows from (2) and Lemma 3 that nth roots, when they exist, are unique in $G(R)$. It follows that if $\alpha^k \beta^l = \beta^l \alpha^k$ for $k, l \in \mathbf{Z} \setminus \{0\}$, then $\alpha\beta = \beta\alpha$ and α, β are again powers of a common γ. The standard argument then proves transitivity of commutation.

PROPOSITION 5. *If $1 \in R$ has infinite order in R^+, then $G(R)$ contains a copy of F_2.*

PROOF (J. S. WILSON). It is shown in [9] that the functions

$$\lambda\colon z \mapsto z + 1, \qquad \mu\colon z \mapsto z^3$$

generate a copy of F_2 in $\mathrm{Sym}(\mathbf{R})$, and thus in $\mathrm{Sym}(\mathbf{R}^*)$, where $\mathbf{R}^* = \mathbf{R} \cup \{\infty\}$. Then the same is true for their conjugates by $\xi\colon z \mapsto 1/z$, namely

$$\xi^{-1}\lambda\xi = \lambda'\colon z \mapsto \frac{z}{1+z}, \qquad \xi^{-1}\mu\xi = \mu.$$

https://doi.org/10.1017/S1446788700031001 Published online by Cambridge University Press

By the Nielsen-Schreier theorem, the same is true of

$$\lambda', \mu^{-1}\lambda'\mu = \lambda'' \colon z \mapsto z(1+z^3)^{-1/3},$$

and finally of the conjugates of these by $\eta \colon z \mapsto 3z$,

$$\eta^{-1}\lambda'\eta \colon z \mapsto \frac{z}{1+3z}, \qquad \eta^{-1}\lambda''\eta \colon z \mapsto z(1+(3z)^3)^{-1/3},$$

and both of these lie in $G(\mathbf{Z}) \subseteq G(R)$.

EXAMPLE. The main result of [8] suggests that the polynomials in $G(\mathbf{Z})$ are close to forming a free monoid. However, it is not hard to find polynomials α_2, α_3, β_3, $\beta_2 \in G(\mathbf{Z})$ that are irreducible with respect to composition and satisfy $\alpha_2\alpha_3 = \beta_3\beta_2$. For example, take

$$\alpha_2 = x + 27x^2, \qquad \beta_3 = x + 32x^2 + 256x^3,$$
$$\alpha_3 = x + 8x^2 + 16x^3, \quad \beta_2 = x + 3x^2.$$

3. The lower central series

From the proof of Proposition 3, we already know that $\gamma_\eta(G(R)) \subseteq K_{n+1}$ for all $n \geq 2$ and all R. In this section, we obtain a partial converse in the case when R is the field $\mathbf{Z}_p$ of p elements for any prime $p \geq 5$, and (following a suggestion of J. S. Wilson) the full converse where R is the field $\mathbf{Q}$ of rational numbers.

PROPOSITION 6. *Let p be a prime and n a positive integer. Then the class of $G_n(\mathbf{Z}_p)$ is equal to*

$$n - 2 - \left[\frac{n-3}{p}\right], \quad \textit{when } p \geq 3$$

and to

$$\left[\frac{n}{2}\right], \quad \textit{when } p = 2.$$

This is a result of I. O. York; we hope that a proof will appear in a future paper.

PROPOSITION 17. *For all $n \geq 2$, $\gamma_n(G(\mathbf{Q})) = K_{n+1}$.*

PROOF. This follows from the fact that $\gamma_n(G(Q)) \subseteq K_{n+1}$, together with the claim:

$$K_n \subseteq [\alpha, K_{n-1}], \qquad n \geq 3, \tag{5}$$

https://doi.org/10.1017/S1446788700031001 Published online by Cambridge University Press

where $\alpha = x + x^2$, *by a simple induction on* n. *To prove (5), fix* $n \geq 3$ *and* $\gamma \in K_n$; then we have to solve the equation

$$\alpha\beta = \beta\alpha\gamma \tag{6}$$

for $\beta \in K_{n-1}$. Let

$$\gamma = \sum_{k\geq 0} c_k x^k = x + c_{n+1}x^{n+1} +,$$
$$\beta = x + b_n x^n + = \sum_{r\geq 0} b_r x^r,$$

so that $b_n = c_{n+1}/(2-n)$, from (3). We obtain an equation for b_{k-1} in terms of known c_i and earlier b_i by comparing coefficients of x^k in (6) for $k > n$.

Now the left-hand side of (6) is

$$\alpha\beta = \beta + \beta^2 = \sum_{k\geq 0} b_k x^k + \sum_{k\geq 0}\left(\sum_{i=0}^{k} b_i b_{k-i}\right) x^k,$$

in which the coefficient of x^k is equal to

$$b_k + 2b_{k-1} + f(b_2, \ldots, b_{k-2}), \tag{7}$$

for $k > n \geq 3$, where f is some polynomial. On the other hand, the right-hand side is

$$\beta\alpha\gamma = \beta\left(\sum_{s\geq 0}\left(c_s + \sum_{i=0}^{s} c_i c_{s-i}\right) x^s\right) = \sum_{r>0} b_r \left(\sum_{s\geq 0} d_s x^s\right)^r,$$

where $d_s = c_s + \sum_{i=0}^{s} c_i c_{s-i}$, and the coefficient of x^k is the same as that in

$$b_k x^k + b_{k-1}(x + d_2 x^2)^{k-1} + \cdots + b_2(x + \cdots + d_{k-1}x^{k-1})^2 + (x + \cdots + d_k x^k),$$

namely,

$$b_k + b_{k-1}(k-1)d_2 + g(b_2, \ldots, b_{k-2}, d_2, \ldots, d_k). \tag{8}$$

Comparing (7) and (8), b_k cancels, and as $d_2 = c_2 + c_1^2 = 1$, there remains an expression for $(k-3)b_{k-1}$ in terms of known d_i and earlier b_i, which recursively yields the b_{k-1} $(k > n \geq 3)$.

REMARK. This proof shows that the β so determined is unique, and it follows that the maps

$$\left.\begin{array}{l} K_2 \to K_{n+1} = \gamma_n(G(\mathbf{Q})) \\ \delta \to [\delta, \underbrace{\alpha, \ldots, \alpha}_{n}] \end{array}\right\}, \qquad n \geq 2,$$

are all bijective.

https://doi.org/10.1017/S1446788700031001 Published online by Cambridge University Press

References

[1] I. N. Baker, 'Permutable power series and regular iteration', *J. Austral. Math. Soc.* **2** (1961/1962), 265–294.
[2] E. Jacobsthal, 'Über vertauschbare Polynome', *Math. Z.* **63** (1955), 243–276.
[3] A. Joyal, 'Un théorie combinatorie des séries formelles', *Adv. in Math.* **42** (1981), 1–82.
[4] G. Julia, 'Mémoire sur la permutabilité des fractions rationelles', *Ann. Sci. Ecole Norm. Sup.* (3) **39** (1922), 131–215.
[5] H. Lausch and W. Nöbauer, *Algebra of polynomials* (North-Holland, Amsterdam, 1973).
[6] W. D. Nichols, 'Pointed irreducible bialgebras', *J. Algebra* **57** (1979), 64–76.
[7] M. J. Pearl, Query no. 304, *Notices Amer. Math. Soc.* **31** (1984), 376.
[8] J. F. Ritt, 'Prime and composite polynomials', *Trans. Amer. Math. Soc.* **23** (1922), 51–66.
[9] S. White, 'The group generated by $x \mapsto x + 1$ and $x \mapsto x^p$ is free', Preprint, Berkeley 1986.
[10] H. J. Zassenhaus, 'On a problem of Harvey Friedman', *Comm. Algebra* **6** (16) (1978), 1629–1634.

Department of Mathematics
The University of Nottingham
Nottingham NG7 2RD
England