J. Austral. Math. Soc. (*Series A*) 27 (1979), 313–318

COMMUTATIVE SUBSEMIGROUPS OF THE COMPOSITION SEMIGROUP OF FORMAL POWER SERIES OVER AN INTEGRAL DOMAIN

HERMANN KAUTSCHITSCH

(Received 16 June; revised 11 October 1977)

Communicated by H. Lausch

Abstract

Let R be a commutative ring with identity. $R[[x]]$ denotes the ring of formal power series, in which we consider the composition $\circ$, defined by $f(x)\circ g(x) = f(g(x))$. This operation is well defined in the subring $R_+[[x]]$ of formal power series of positive order. The algebra $\mathfrak{H} = \langle R_+[[x]], \circ\rangle$ is clearly a semigroup, which is not commutative for $|R| > 1$. In this paper we consider all those commutative subsemigroups of $\mathfrak{H}$, which consist of power series of all positive orders, which are called 'permutable chains'.

Subject classification (*Amer. Math. Soc.* (*MOS*) *1970*): primary 16 A 02; secondary 08 A 25.

1. Introduction

Let R be a commutative ring with identity and let x be an indeterminate over R. Then $R[[x]]$ denotes the ring of formal power series, in which a third operation $\circ$ called composition, given by

$$f(x)\circ g(x) = f(g(x))$$

is defined besides addition and multiplication. We consider the subring $R_+[[x]]$ of formal power series of positive order, in which the composition is well defined. The algebra $\mathfrak{H} = \langle R_+[[x]], \circ\rangle$ is clearly a semigroup with the identity x, which is not commutative for $|R| > 1$. Two formal power series are called permutable if

$$f(x)\circ g(x) = g(x)\circ f(x).$$

$\mathfrak{H}$ contains commutative subsemigroups, for example the subsemigroup $\{g\}$ generated by $g \in R_+[[x]]$, but the problem of determining all the commutative subsemigroups of $\mathfrak{H}$ has not yet been solved. If R is an integral domain, then $\{g\}$ contains only power series of those orders, which are powers of the order of g.

In this paper we shall determine all those commutative subsemigroups of $\mathfrak{h}$ which consist of power series of all positive orders. These commutative subsemigroups are called permutable chains, or P-chains. By Kautschitsch (1970) any P-chain of $R[[x]]$, where R is an integral domain, contains exactly one power series of order m, for every $m \geqslant 1$. In the case that R is a field K all P-chains over K have been determined (see Kautschitsch (1970)). The result is:

Each P-chain $\mathfrak{P}$ over a field K is of the form

$$\mathfrak{P} = \{l^{-1} \circ x^m \circ l \mid m \in \mathbf{N}\},$$

where l is any power series of first order of $K[[x]]$.

Henceforth let R be an integral domain.

2. P-chains $\mathfrak{P}_\varepsilon$ over $R[[x]]$ whose elements have units as first coefficients

Each P-chain in the quotient field of R is of the form $\{l^{-1} \circ x^i \circ l \mid i \in \mathbf{N}\}$. If $l = \varepsilon x + \sum_{j=2}^{\infty} \lambda_j x^j$, then $l^{-1} = \varepsilon^{-1} x + \sum_{j=2}^{\infty} \mu_j x^j$ and $l^{-1} \circ x^i \circ l$ is of the form $\varepsilon^{i-1} x^i + \sum_{j=i+1}^{\infty} a_{j,i} x^j$. Therefore each such P-chain is of the form

$$\mathfrak{P}_\varepsilon = \{x, \varepsilon^{i-1} x^i + \sum_{j=i+1}^{\infty} a_{j,i} x^j \mid i \geqslant 2\}, \quad \varepsilon \text{ is a unit in } R.$$

For example, the 'P-chain of powers' $\mathfrak{P}_P = \{x, x^2, x^3, \dots\}$ is of this form. We shall show, that all the P-chains of this section can be constructed from $\mathfrak{P}_P$. We need the following formulae.

Let K be the quotient field of R and $l(x) = \lambda_1 x + \lambda_2 x^2 + \dots \in K[[x]]$, $\lambda_1 \neq 0$, and $A_{j,k}$ be the coefficient of the power x^{j+k} in $(l(x))^j$. By Gradstkeyn and Ryzhik (1965) we get:

$$A_{j,k} = \frac{1}{\lambda_1 k} \sum_{l=1}^{k} (lj - k + 1) \lambda_{1+l} A_{j,k-l}, \qquad A_{j,0} = \lambda_1^j, \tag{1}$$

whence $A_{j,k}$ depends only on $\lambda_1, \dots, \lambda_{1+k}$. Therefore we get for

$$l^{-1}(x) \in \mathfrak{h} : l^{-1}(x) = \sum_{i=1}^{\infty} \mu_i x_i$$

with

$$\mu_1 = \lambda_1^{-1}, \quad \vdots \quad \mu_r = -\lambda_1^{-r} \left(\mu_1 \lambda_r + \sum_{i=2}^{\infty} \mu_i A_{i,r-i} \right), \quad \text{for } r \geqslant 2, \tag{2}$$

whence μ_r depends only on $\lambda_1, \dots, \lambda_r$.

Now we compute $l^{-1} \circ x_n \circ l = \sum_{i=n}^{\infty} d_i x^i$, for $n \geqslant 2$:

$$d_n = \lambda_1^{n-1},$$

(3)
$$d_{n+1} = \mu_1 A_{n,1},$$
$$d_{2n} = \mu_1 A_{n,n} + \mu_2 \lambda_1^{2n},$$
$$d_{kn+j} = \mu_1 A_{n,(k-1)n+j} + \mu_2 A_{2n,(k-2)n+j} + \dots + \mu_k A_{kn,j}$$

where $0 \leqslant j < n$ for $k \geqslant 1$.

From (2) we see that, in the semigroup $\langle R[[x]], \circ \rangle$, the elements which have inverses are just the power series

(4)
$$l(x) = \varepsilon x + \sum_{i=2} \lambda_i x^i, \quad \varepsilon \text{ is a unit in } R.$$

It can also be seen that $\mathfrak{P}_\varepsilon' = \{l^{-1} \circ f_i \circ l \mid i \in \mathrm{N},\ f_i \in \mathfrak{p}_\varepsilon\}$ is a P-chain. $\mathfrak{P}_\varepsilon'$ is called a conjugate (in $\langle R[[x]], \circ \rangle$) of $\mathfrak{P}_\varepsilon$. Also $l^{-1} \circ f_i \circ l$ is called conjugate to f_i. Since the power series of the form (4) form a group with respect to the operation$\circ$, conjugacy is an equivalence relation on the set of all P-chains over R. Thus all the P-chains over R will be known as soon as we know a representative for each class of this partition.

The next theorem shows that there is only one class containing P-chains whose elements have units as first coefficients.

THEOREM 1. *Every P-chain over R whose elements have a unit in R as first coefficient is a conjugate of the P-chain of powcrs.*

PROOF Let K be again the quotient field of R. By the above statements, all the P-chains over K whose elements have a unit in R as first coefficient are of the form

$$\{l^{-1} \circ x^n \circ l \mid n \in \mathrm{N},\ l = \varepsilon x + \sum_{i=2}^{\infty} \lambda_i x^i,\ \varepsilon \text{ is a unit in } R\}.$$

First we show that $l^{-1} \circ \mathfrak{p}_P \circ l$ is a P-chain over R if and only if $\lambda_i \in R$ for $i \geqslant 2$. Let $l^{-1} \circ \mathfrak{p}_P \circ l$ be any P-chain over R. Then both

$$l^{-1} \circ x^2 \circ l = \varepsilon x^2 + \sum_{i=3}^{\infty} d_i x^i \quad \text{and} \quad l^{-1} \circ x^3 \circ l = \varepsilon^2 x^3 + \sum_{i=4}^{\infty} e_i x^i$$

belong to $R[[x]]$. In the first case we get from (3) and (1):

$$d_3 = 2\lambda_2$$
$$\vdots$$
$$d_{2k+j} = \frac{1}{(k-1)2+j} [(k-1)2+j]\, 2\lambda_{1+(k-1)2+j} + F(\varepsilon, \dots, \lambda_{(k-1)2+j})$$

https://doi.org/10.1017/S1446788700012428 Published online by Cambridge University Press

or

$$d_3 = 2\lambda_2$$

(5)

$$d_i = 2\lambda_{i-1} + F(\varepsilon, \lambda_2, \ldots, \lambda_{i-2}), \quad i \geqslant 4.$$

In the second case we get analogously:

$$e_4 = 3\varepsilon\lambda_2$$

(6)

$$e_i = 3\varepsilon\lambda_{i-2} + G(\varepsilon, \lambda_2, \ldots, \lambda_{i-3}), \quad i \geqslant 5.$$

From (5) and (6) we get:

$$2\lambda_2 \in R \quad \text{and} \quad 3\varepsilon\lambda_2 \in R \quad \text{and so} \quad \lambda_2 \in R.$$

If now $\lambda_2, \lambda_3, \ldots, \lambda_j$ belong to R, then also $2\lambda_{j+1} \in R$, $3\lambda_{j+1} \in R$ and therefore $\lambda_{j+1} \in R$, because $F(\varepsilon, \lambda_2, \ldots, \lambda_j)$ and $G(\varepsilon, \lambda_2, \ldots, \lambda_{j-1})$ are polynomials in $\varepsilon, \lambda_2, \ldots, \lambda_j$ with coefficients in R. Furthermore, if $\lambda_i \in R$, $i \geqslant 2$, then

$$l^{-1} \circ x^n \circ l \in R[[x]] \quad \text{for } n \geqslant 1,$$

because $A_{j,k}$ is clearly a polynomial of $R[x]$ in $\varepsilon, \lambda_2, \ldots, \lambda_{1+k}$, and so $A_{j,k} \in R$ and $\mu_i \in R$. By (3) each coefficient of $l^{-1} \circ x^n \circ l$ belongs to $R[[x]]$.

SUMMARY We get all the P-chains over an integral domain R, whose elements have units as first coefficients, if we form the P-chains

$$\mathfrak{P} = \{l^{-1} \circ x^n \circ l \mid n \in N\},$$

where l is any invertible power series of $\langle R[[x]], \circ \rangle$.

3. P-chains $\mathfrak{P}_\alpha$ over R with any elements as first coefficients

As stated above each such P-chain is of the form

$$\mathfrak{P}_\alpha = \{x, \alpha^{i-1} x^i + \sum_{j=i+1} a_{j,i} x^j \mid i \geqslant 2, \alpha \in R\}.$$

In this case there may be more than one class of conjugate P-chains.

Let K be again the quotient field of R. First we determine a sufficient condition under which power series of the form $l^{-1} \circ x^n \circ l$ belong to $R[[x]]$ for $l \in K[[x]]$.

LEMMA 1. *Let* $l(x) = \sum_{i=1}^{\infty} \lambda_i x^i \in K[[x]]$. $l^{-1} \circ x^n \circ l \in R[[x]]$ *for all* $n \geqslant 1$ *if* $\lambda_i \in R$ *for* $i \geqslant 1$ *and* $\lambda_i \equiv 0 \bmod \lambda_1$ *for* $i \geqslant 2$.

PROOF. From (1) we see by induction on k that $A_{j,k}$ is divisible by λ_1^j if $\lambda_i \equiv 0 \bmod \lambda_1$ for $i \geqslant 2$. From (2) we see again by induction on k that $\lambda_1^k \cdot \mu_k \in R$, because $\mu_1 \lambda_r = \lambda_1^{-1} \ \lambda_r \in R$ and $\mu_i \cdot A_{i,r-i} \in R$ for $i < k$ by the induction hypothesis and by the property of $A_{j,k}$ stated above. We conclude by (3) that all coefficients d_{kn+j} of $l^{-1}ox^n ol$ belong to R, because $\lambda_1^{kn}\cdot\mu_k \in R$ for all $n \geqslant 1$.

Now we can prove:

THEOREM 2. *Let R be an integral domain. Then the P-chains*

$$\left(\alpha x + \sum_{i=2}^{\infty} l_i x^i\right)^{-1} o \mathfrak{P}_P o \left(\alpha x + \sum_{i=2}^{\infty} l_i x^i\right)$$

and

$$\left(\bar{\alpha} x + \sum_{i=2}^{\infty} \bar{l}_i x^i\right)^{-1} o \mathfrak{P}_P o \left(\bar{\alpha} x + \sum_{i=2}^{\infty} \bar{l}_i x^i\right),$$

where α, $\bar{\alpha}$, l_i, $\bar{l}_i \in R$, $l_i \equiv 0 \bmod \alpha$, $\bar{l}_i \equiv 0 \bmod \bar{\alpha}$ and $\mathfrak{P}_P$ is the P-chain of powers, are conjugate in $R[[x]]$, if and only if α and $\bar{\alpha}$ are associates.

PROOF. By Lemma 1, these P-chains are P-chains over R. By considering the power series of order 2, one can easily check that any two distinct P-chains of this form are not conjugate over R: Let

$$f = \left(\alpha x + \sum_{i=2}^{\infty} l_i x^i\right)^{-1} o x^2 o \left(\alpha x + \sum_{i=2}^{\infty} l_i x^i\right)$$

and

$$g = \left(\bar{\alpha} x + \sum_{i=2}^{\infty} \bar{l}_i x^i\right)^{-1} o x^2 o \left(\bar{\alpha} x + \sum_{i=2}^{\infty} \bar{l}_i x^i\right).$$

If we assume that f and g were conjugate, then there exists a power series $l = \varepsilon x + \sum_{i=2}^{\infty} n_i x^i$ (ε is a unit in R) with $g = l^{-1} o f o l$. By comparing the coefficients of x^2 we get $\varepsilon\bar{\alpha} = \alpha$, so that α and $\bar{\alpha}$ were associates. On the other hand, if $\bar{\alpha} \in R$, $\bar{l}_i \in R$, $\bar{l}_i \equiv 0 \bmod \bar{\alpha}$ and if α and $\bar{\alpha}$ are associates, then $\bar{l}_i \equiv 0 \bmod \alpha$.

Now we can find a power series $\varepsilon x + \sum_{i=2}^{\infty} v_i x^i \in R[[x]]$ such that

$$\bar{\alpha} x + \sum_{i=2}^{\infty} \bar{l}_i x^i = \left(\alpha x + \sum_{i=2}^{\infty} l_i x^i\right) o \left(\varepsilon x + \sum_{i=2}^{\infty} v_i x^i\right), \quad l_i \equiv 0 \bmod \alpha.$$

Let $A_{j,k}$ be the coefficient of x^{k+j} in $(\varepsilon x + \sum_{i=2}^{\infty} v_i x^i)^j$. We get by comparing the coefficients of powers of x:

$$x: \quad \bar{\alpha} = \alpha \cdot \varepsilon,$$

$$x^n: \quad \bar{l}_n = \alpha v_n + l_2 A_{2,n-2} + \dots + l_n \varepsilon^n.$$

Hence $\alpha v_n = (\bar{l}_n - l_2 A_{2,n-2} + \dots - l_n \varepsilon^n) \in R$, for $\bar{l}_n \equiv 0 \bmod \alpha$, $l_i \equiv 0 \bmod \alpha$ and $A_{i,n-i} \in R$. We can check that $v_n \in R$ by induction on n. Therefore

$$\left(\bar{\alpha} x + \sum_{i=2}^{\infty} \bar{l}_i x^i\right)^{-1} o \mathfrak{p}_P o \left(\bar{\alpha} x + \sum_{i=2}^{\infty} \bar{l}_i x^i\right),$$

https://doi.org/10.1017/S1446788700012428 Published online by Cambridge University Press

is conjugate in $\langle R[[x]], \circ\rangle$ to the chain

$$\left(\alpha x + \sum_{i=2}^{\infty} l_i x^i\right)^{-1} \circ \mathfrak{P}_p \circ \left(\alpha x + \sum_{i=2}^{\infty} l_i x^i\right).$$

This theorem shows that there is more than one class of conjugate P-chains. For this consider the P-chains over $R[[x]]$ of the form

$$\left(\alpha x + \sum_{i=2}^{\infty} l_i x^i\right)^{-1} \circ \mathfrak{P}_P \circ \left(\alpha x + \sum_{i=2}^{\infty} l_i x^i\right),$$

where $l_i \equiv 0 \bmod \alpha$, $\mathfrak{p}_P$ is the P-chain of powers and α runs through a system of representatives for the non-zero classes of associative elements of R. It is an open problem whether these P-chains form a full system of representatives in the case that R is an integrally closed domain.

Acknowledgement

I wish to thank the referee, whose suggestions were essential for the elaboration of the final version.

References

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

J. S. Gradstkeyn and J. M. Ryzhik (1965), *Table of integrals, series and products* (Academic Press, New York).

H. Kautschitsch (1970), 'Kommutative Teilhalbgruppen der Kompositionshalbgruppe von Polynomen und formalen Potenzreihen', *Monatsh. f. Math.* **74**, 421–436.

H. Lausch and W. Nöbauer (1973), *Algebra of polynomials* (North-Holland Mathematical Library, Vol. 5, Amsterdam and London).

Universität für Bildungswissenschaften
A—9010 Klagenfurt, Universitätsstrasse 67
Austria