SUBSTITUTION GROUPS OF FORMAL POWER SERIES

S. A. JENNINGS

In this paper we are concerned with the group $\mathfrak{G} = \mathfrak{G}(R)$ of formal power series of the form

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

the coefficients being elements of a commutative ring R and the group operation being substitution. Little seems to be known of the properties of groups of this type, except in special cases, although groups of formal power series in several variables with complex coefficients have been investigated from a different point of view by Bochner and Martin (**1**, chap. I) and Gotô (**2**).

We study first some of the relations between properties of R and of $\mathfrak{G}$, and show in particular that $\mathfrak{G}$ may be topologized in a natural way, so that infinite products may be introduced in $\mathfrak{G}$. In §§3 and 4 we consider the case where the coefficients lie in a field F of characteristic 0: a reasonably complete discussion of the structure of $\mathfrak{G}(F)$ is obtained and it is shown that a Lie algebra can be associated with $\mathfrak{G}(F)$ in a natural way. In particular we show that $\mathfrak{G}(F)$ is generated by two one parameter subgroups. Finally, a brief discussion is given of some of the properties of $\mathfrak{G}(I)$, where I is the ring of ordinary integers.

1. Groups with a general coefficient ring. Let R be any commutative, associative ring, and let x be an indeterminate which commutes with every element of R. We consider the set of formal power series $f(x)$ of the form

$$f(x) = x + a_2x^2 + \ldots + a_nx^n + \ldots, \tag{1.1.1}$$

where $a_2, \ldots a_n, \ldots$ are elements of R. If $g(x)$ is another such power series

$$g(x) = x + b_2x^2 + \ldots b_nx^n + \ldots,$$

then, substituting formally, it follows readily that

$$g(f(x)) = x + \sum c_rx^r, \qquad r = 2, 3, \ldots\ ,$$

where

$$\begin{aligned} c_2 &= a_2 + b_2, \\ c_r &= a_r + b_r + \sum b_s\phi_s(a_2, \ldots a_s), \end{aligned} \tag{1.1.2}$$

$$s = 2, 3, \ldots r - 1; \qquad r = 3, 4, \ldots;$$

and ϕ_s is a polynomial in $a_2 \ldots a_s$ with integral coefficients of degree at most s,

Received March 10, 1954. This investigation was carried out while the author held a fellowship at the Summer Research Institute of the Canadian Mathematical Congress, 1952. The author also wishes to express his thanks to the Board of Governors of the University of British Columbia for a Research Grant in connection with this work.

https://doi.org/10.4153/CJM-1954-031-9 Published online by Cambridge University Press

without constant term. We note that ϕ_s is independent of the nature of the ring R.

Every $f(x)$ of the form (1.1.1) defines a mapping F of the set of all such power series on itself, via the substitution $x \rightarrow f(x)$. If $r(x)$ is any such power series, we define F to be the mapping:

$$F : r(x) \rightarrow r(f(x)).$$

We indicate the mapping which is determined by $f(g(x))$ by $FG : x \rightarrow f(g(x))$. The associativity of this multiplication is automatic. The existence of an inverse to $F : x \rightarrow f(x)$ follows from (1.1.2): for consider the function

$$\tilde{f}(x) = x + \sum \tilde{a}_r x^r, \qquad r = 2, 3, \ldots,$$

where the coefficients $\tilde{a}_r$ are defined inductively by

$$\begin{aligned} &\tilde{a}_2 = -a_2, \\ (1.1.3)\qquad & \\ &a_r = -a_r - \sum_{s=2}^{r-1} \tilde{a}_s \phi_s(a_2, \ldots a_s), \qquad r = 3, 4, \ldots. \end{aligned}$$

Clearly

$$\tilde{f}(f(x)) = x,$$

so that the mapping $F^{-1} : x \rightarrow \tilde{f}(x)$ is the inverse of $F : x \rightarrow f(x)$, and $f(\tilde{f}) = x$ also. We have established, therefore,

THEOREM 1.1. *The mappings $F : x \rightarrow f(x)$ of the set of all formal power series*

$$x + \sum a_r x_r, \qquad r = 2, 3, \ldots,$$

with coefficients in an arbitrary commutative ring R, into itself forms a group $\mathfrak{G}$.

When necessary to stress the dependence of $\mathfrak{G}$ upon the coefficient ring R we write $\mathfrak{G} = \mathfrak{G}(R)$. Occasionally in what follows we will write (1.1.1) in the form

$$f(x) = x(1 + a_2x + a_3x^2 + \ldots)$$

but this will be a matter of convenience involving no assumption that R contains a unit element. If R has a unit element 1 we identify $1.x$ and x, but if not, the element 1 which appears above can be considered as a unit formally adjoined to R in the usual manner.

We consider next subgroups of $\mathfrak{G}(R)$ of the type $\mathfrak{G}(S)$, where S is a subring of R. The elements of $\mathfrak{G}(S)$ are of the form

$$G: x \rightarrow x + \sum b_r x^r, \qquad r = 2, 3, \ldots$$

with $b_r \in S$. These elements form a subgroup $\mathfrak{G}(S)$ of $\mathfrak{G}(R)$ which is proper if S is a proper subring of R. If S is an *ideal* of R, consider $F^{-1}GF$ where $G \in \mathfrak{G}(S)$ and $F \in \mathfrak{G}(R)$. We have

$$GF : x \rightarrow g(f(x))$$

where

$$\begin{aligned} g(f(x)) &= f(x) + b_2 f^2 + \ldots + b_n f^n + \ldots \\ &= f(x) + g'(x) \end{aligned}$$

https://doi.org/10.4153/CJM-1954-031-9 Published online by Cambridge University Press

and $g'(x)$ is a power series of the form $b'_2x^2 + b'_3x^3 + \ldots$, all of whose coefficients are in S, since S is an ideal. Hence

$$F^{-1}GF : x \rightarrow \tilde{f}(g(f)) = \tilde{f}(f + g')$$

where

$$\begin{aligned} \tilde{f}(f + g') &= f + g' + a_2(f + g')^2 + a_3(f + g')^3 + \ldots \\ &= \tilde{f}(f) + 2a_2(fg' + g'^2) + \ldots \\ &= x + b''_2x^2 + b''_3x^3 + \ldots \end{aligned}$$

and $b''_2, b''_3, \ldots$ are in S. Hence if S is an ideal,

$$F^{-1}GF : x \rightarrow g''(x),$$

where all the coefficients of g'' are in S, and hence $F^{-1}GF \in \mathfrak{G}(S)$ and $\mathfrak{G}(S)$ is a normal subgroup of $\mathfrak{G}(R)$.

If S, T are two ideals of R with $S{\cdot}T = 0$, then $\mathfrak{G}(S)$ and $\mathfrak{G}(T)$ permute elementwise. For if $b_i \in S$, $c_j \in T$, then $b_ic_j = 0$ and hence by (1.1.2), if

$$g(x) = x + \sum b_rx^r, \qquad h(x) = x + \sum c_rx^r,$$

$$\begin{aligned} h(g(x)) &= g(h(x)) \\ &= x + (b_2 + c_2)\,x^2 + \ldots + (b_2 + c_2)\,x^2 + \ldots . \end{aligned}$$

In particular, if $R = S \oplus T$, then it follows at once that

$$\mathfrak{G}(R) = \mathfrak{G}(S) \times \mathfrak{G}(T).$$

The above may be summarized in

THEOREM 1.2. *The set of elements $x + \Sigma b_rx^r$ with coefficients in a subring S of R defines a subgroup $\mathfrak{G}(S)$ of $\mathfrak{G}(R)$. If S is an ideal, $\mathfrak{G}(S)$ is normal in $\mathfrak{G}(R)$. If S and T annihilate each other, then $\mathfrak{G}(S)$ and $\mathfrak{G}(T)$ permute elementwise. In particular, if $R = S \oplus T$, then*

$$\mathfrak{G}(R) = \mathfrak{G}(S) \times \mathfrak{G}(T).$$

If $\bar{R}$ is a homomorphic image of R, we consider next the relationship between $\mathfrak{G}(R)$ and $\mathfrak{G}(\bar{R})$.

THEOREM 1.3. *If S is an ideal of R, and $\bar{R} = R/S$, then*

$$\mathfrak{G}(\bar{R}) \cong \mathfrak{G}(R)/\mathfrak{G}(S).$$

Proof. Consider $\mathfrak{G}(\bar{R})$: an element $\bar{F}$ is of the form

$$F\colon x \rightarrow x + \sum \bar{a}_rx^r, \qquad \bar{a}_r \in \bar{R};\ r = 2, 3, \ldots .$$

Now if in the homomorphism of R onto $\bar{R}$, $a_r \rightarrow \bar{a}_r$, then we have also a mapping $\mathfrak{G}(R) \rightarrow \mathfrak{G}(\bar{R})$ via

$$\{F\colon x \rightarrow x + \sum a_rx^r\} \rightarrow \{\bar{F}\colon x \rightarrow x + \sum \bar{a}_rx^r\}$$

which is a homomorphism, since, by (1.1.2), if

https://doi.org/10.4153/CJM-1954-031-9 Published online by Cambridge University Press

$$a_r \rightarrow \bar{a}_r, \quad b_r \rightarrow \bar{b}_r$$

then

$$[a_r + b_r + \sum b_s\phi_s(a_2 \ldots a_s)] \rightarrow [\bar{a}_r + \bar{b}_r + \sum \bar{b}_s\phi_s(\bar{a}_2 \ldots \bar{a}_s)].$$

That is, if $F \rightarrow \bar{F}$ and $G \rightarrow \bar{G}$ then $FG \rightarrow \bar{F}\bar{G}$. The kernel of this homomorphism consists of all elements of $\mathfrak{G}(R)$ with coefficients in S, that is, $\mathfrak{G}(S)$, and hence

$$\mathfrak{G}(R)/\mathfrak{G}(S) \cong \mathfrak{G}(\bar{R})$$

as required. We may therefore write

$$\mathfrak{G}(R/S) \cong \mathfrak{G}(R)/\mathfrak{G}(S).$$

The following considerations throw some light on the nature of the group $\mathfrak{G}(R)$. Let us assume that R has a unit element, and let $\mathbf{P}$ be the ring of all formal power series in x with coefficients in R. A typical element of $\mathbf{P}$ is then of the form

$$p(x) = r_0 + r_1x + r_2x^2 + \ldots, \qquad r_0, r_1, r_2, \ldots \in R.$$

The set $\mathbf{M}_i$ of all power series in $\mathbf{P}$ of the form

$$p_i(x) = r_ix^i + r_{i+1}x^{i+1} + \ldots$$

is an ideal of $\mathbf{P}$ for all $i = 1, 2, \ldots$ and $\mathbf{P}/\mathbf{M}_1 = R$. We consider **(3**, p. 117**)** the automorphisms of $\mathbf{P}$ over R, that is, those automorphisms which leave the elements of R fixed, and in particular the subgroup $\mathfrak{A}$, which leaves the elements of $\mathbf{M}_1$ modulo $\mathbf{M}_2$ unchanged. If A is any element of $\mathfrak{A}$, then the mapping A of $\mathbf{M}_1$ will be completely determined by a knowledge of what happens to x under A. However, since $\mathbf{M}_1$ modulo $\mathbf{M}_2$ is fixed under A, we have

$$A : x \rightarrow x + p_2(x) = x + a_2x^2 + a_3x^3 + \ldots$$

and for any element $p_1(x) \in \mathbf{P}$,

$$A : p_1(x) \rightarrow p_1(x + p_2(x)).$$

The mapping A, therefore, is precisely an element of $\mathfrak{G}(R)$, and conversely any mapping

$$F : x \rightarrow f(x)$$

of $\mathfrak{G}(R)$ gives rise to an automorphism of $\mathfrak{A}$,

$$F : p_1(x) \rightarrow p_1(f(x)).$$

We have thus proved

THEOREM 1.4. *The group $\mathfrak{G}(R)$ is the group of relative automorphisms of* $\mathbf{P}$ *over R which leave* $\mathbf{M}_1$ *modulo* $\mathbf{M}_2$ *fixed.*

We note that $\mathbf{M}_1/\mathbf{M}_{n+1}$ is a nilpotent ring, and the homomorphism $\mathbf{M}_1 \rightarrow \mathbf{M}_1/\mathbf{M}_{n+1}$ may be realized by setting $x^{n+1} = 0$ in all calculations with elements of $\mathbf{M}_1$. The group of automorphisms $\mathfrak{A}'$ of $\mathbf{M}_1/\mathbf{M}_{n+1}$ over R which

https://doi.org/10.4153/CJM-1954-031-9 Published online by Cambridge University Press

leaves the elements of $\mathbf{M}_1/\mathbf{M}_{n+1}$ (mod $\mathbf{M}_2/\mathbf{M}_{n+1}$) fixed consists of the mappings

$$\bar{F} : x \to x + a_2x^2 + \ldots + a_nx^n = \bar{f}(x),$$
$$\bar{G} : x \to x + b_2x^2 + \ldots + b_nx^n = \bar{g}(x),$$

etc., where $\bar{F}\bar{G}$ is obtained by forming $\bar{f}(\bar{g}(x))$ and setting $x^{n+1} = 0$ in the result, viz.,

$$\bar{F}\bar{G} : x \to \bar{f}(\bar{g}(x)) \qquad (\text{mod } x^{n+1}).$$

2. Commutators and the subgroup topology. The commutator structure of $\mathfrak{G}(R)$ is revealed by considerations involving a different type of subgroup. For given R, let $\mathfrak{G}_r(R)$ be the set of all elements of the form

$$F_r : x \to x + a_{r+1}\,x^{r+1} + a_{r+2}\,x^{r+2} + \ldots.$$

From (1.1.2) and (1.1.3) it follows that the set $\mathfrak{G}_r$ is a subgroup. If $G : x \to x + \Sigma c_s x^s$ is any element of $\mathfrak{G}(R)$, it is easily verified that $G^{-1}F_rG$ is given by a series of the form

$$x + a_{r+1}\,x^{r+1} + a'_{r+2}\,x^{r+2} + \ldots, \quad a'_{r+s} \in R, \qquad s \geqslant 2,$$

so that $\mathfrak{G}_r$ is normal in $\mathfrak{G} = \mathfrak{G}_1$. Indeed, we have the descending chain of normal subgroups

$$\mathfrak{G} = \mathfrak{G}_1 \supset \mathfrak{G}_2 \supset \mathfrak{G}_3 \supset \ldots. \tag{2.1.1}$$

Let $F_r \in \mathfrak{G}_r$, $G_s \in \mathfrak{G}_s$. Then we may write

$$F_r\colon x \to x + a_{r+1}x^{r+1} + a_{r+2}x^{r+2} + \ldots = x + x^{r+1}f,$$
$$F_r^{-1}\colon x \to x - a_{r+1}x^{r+1} + \tilde{a}_{r+2}x^{r+2} + \ldots = x + x^{r+1}\tilde{f},$$
$$G_s\colon x \to x + b_{s+1}x^{s+1} + b_{s+2}x^{s+2} + \ldots = x + x^{s+1}g,$$
$$G_s^{-1}\colon x \to x - b_{s+1}x^{s+1} + \tilde{b}_{s+2}x^{s+2} + \ldots = x + x^{s+1}\tilde{g},$$

where $f = a_{r+1} + a_{r+2}\,x + \ldots$, etc. We assume $a_r, b_s \neq 0$. Then an easy but somewhat tedious calculation using (1.1.2) and (1.1.3) shows that

$$(F_r, G_s) = F_r^{-1}\,G_s^{-1}\,F_r\,G_s$$

is given by

$$x + (r - s)\,a_{r+1}\,b_{s+1}\,x^{r+s+1} + c_{r+s+2}\,x^{r+s+2} + \ldots, \tag{2.1.2}$$

where the c_t are polynomials in the a_i and b_j. It follows that

$$(\mathfrak{G}_r, \mathfrak{G}_s) \subseteq \mathfrak{G}_{r+s}, \tag{2.1.3}$$

and indeed, if $r = s$, $(\mathfrak{G}_r, \mathfrak{G}_r) \subseteq \mathfrak{G}_{2r+1}$ since in this case, as is easily verified,

$$(F_r, G_r) = x + (r + 2)(a_{r+2}\,b_{r+1} + a_{r+1}\,\tilde{b}_{r+2})\,x^{2r+2} + \ldots, \qquad r > 1,$$

and

$$(F_1, G_1) = x + (a_3b_2 + a_2\tilde{b}_3 - a_2b_2^2 - a_2^2b_2)\,x^4 + \ldots, \qquad r = 1. \tag{2.1.4}$$

In particular, since $(\mathfrak{G}_r, \mathfrak{G}) \subseteq G_{r+1}$, the chain (2.1.1) is a central series of $\mathfrak{G}$.

https://doi.org/10.4153/CJM-1954-031-9 Published online by Cambridge University Press

We note too that the only element common to all the subgroups $\mathfrak{G}_r$ is the element $x \to x$, the unit element of $\mathfrak{G}$.

THEOREM 2.1. *The elements of* $\mathfrak{G}(R)$ *of the form*

$$F_r : x \to x + a_{r+1}\, x^{r+1} + \ldots , \qquad r = 1, 2, \ldots ,$$

form a normal subgroup $\mathfrak{G}_r\,(R)$. *The descending chain* (2.1.1) *is a central series of* $\mathfrak{G}$ *with the stronger property* (2.1.2) *and* $\mathfrak{G}$ *is* generalized nilpotent *in the sense that the intersection of all terms of the central series* (2.1.1) *consists of the unit element.*

We may introduce a subgroup topology in $\mathfrak{G}$ by taking the normal subgroups $\{\mathfrak{G}_r\}$ as a system of neighbourhoods of the identity in $\mathfrak{G}$. In particular, if G_n is a sequence of elements of $\mathfrak{G}$, we will say that $\lim G_n = G$, where $G \in \mathfrak{G}$, if for any integer N we can find another integer N_0 such that $G_n \equiv G \bmod \mathfrak{G}_N(R)$ for all $n > N_0$. The group $\mathfrak{G}$ topologized in this fashion is 0-dimensional, and the subgroups $\mathfrak{G}_r$ are both open and closed. Indeed, we remark that any subgroup of the form $\mathfrak{G}\ (S)$, where S is a subring of R, is closed in this topology. For if G is a limit point of $\mathfrak{G}(S)$, there exists a sequence of elements $H_1, H_2, \ldots$ belonging to $\mathfrak{G}(S)$, and such that

$$\lim H_r = G.$$

That is, for given N, there exists N_0 such that

$$G = H_r\, G_N$$

for all $r > N_0$, or in other words, the coefficients of $x^2, x^3, \ldots x^n$ of G are the same as those of H_r for $r > N_0$, and since these last belong to S, the coefficients of G all belong to S, N being arbitrary.

We consider now the factor groups $\mathfrak{G}/\mathfrak{G}_n$. If F is any element of $\mathfrak{G}$, with

$$F : x \to x + a_2x^2 + \ldots a_nx^n + a_{n+1}\, x^{n+1} + \ldots ,$$

we show that there exists an element F_n in $\mathfrak{G}_n$ such that if $\bar{F}$ is given by

$$\text{(2.2.1)} \qquad \bar{F}\colon x \to x + a_2x^2 + \ldots + a_nx^n = x + \bar{f},$$

then

$$\text{(2.2.2)} \qquad F = \bar{F}\, F_n.$$

For, since $\mathfrak{G}$ is a group, we may solve the equation $F = \bar{F}X$ and get

$$X\colon x \to x + \sum c_sx^s = x + g(x), \qquad s = 2, 3, \ldots .$$

Substituting in (2.2.2) we get

$$x + \sum a_sx^s = x + g(x) + a_2(x + g)^2 + \ldots + a_n(x + g)^n$$

and since $x + \sum a_sx^s = x + \bar{f} + a_{n+1}\, x^{n+1} + \ldots$ we have

$$\text{(2.2.3)} \qquad x + \bar{f} + a_{n+1}x^{n+1} + \ldots = x + \bar{f} + g(x) + a_2(2xg + g^2) + \ldots + a_n(nx^{n-1}g + \ldots + g^n).$$

https://doi.org/10.4153/CJM-1954-031-9 Published online by Cambridge University Press

Comparing both sides of (2.2.3) we see that

$$a_{n+1}\,x^{n+1} + \ldots = g(x)\,[1 + 2a_2xg + \ldots]$$

and hence $c_2 = c_3 = \ldots c_n = 0$, which establishes (2.2.2).

Using the coefficients in

$$F^{-1} : x \rightarrow x + \tilde{a}_2x^2 + \ldots,$$

we set

$$F^{\circ} = x + \tilde{a}_2x^2 + \ldots + \tilde{a}_nx^n;$$

then by the above there exists an element G_n of $\mathfrak{G}_n$ such that

$$F^{-1} = F^{\circ}G_n,$$

and hence $F \cdot F^{\circ}$ is in $\mathfrak{G}_n$, that is,

$$F^{\circ} \equiv F^{-1} \equiv \bar{F}^{-1} \qquad (\text{mod } \mathfrak{G}_n).$$

Similarly, if $G \equiv \bar{G}$ (mod $\mathfrak{G}_n$), with

$$\bar{G} : x \rightarrow x + b_2x^2 + \ldots + b_nx^n,$$

then

$$F\,G \equiv \bar{H} \qquad (\text{mod } \mathfrak{G}_n),$$

where $\bar{H}$ is obtained by substituting

$$x + b_2x^2 + \ldots + b_nx^n$$

into

$$x + a_2x^2 + \ldots + b_nx^n$$

and setting $x^{n+1} = 0$ in the result. It follows that $\mathfrak{G}$ modulo $\mathfrak{G}_n$ is isomorphic to the group $\mathfrak{A}'$ discussed in §1. We have therefore proved

THEOREM 2.2. *The group $\mathfrak{G}/\mathfrak{G}_{n-1}$ is isomorphic to the group $\mathfrak{A}'$ of relative automorphisms of the ring $\mathbf{M}/\mathbf{M}_{n+1}$ which leave the elements of $\mathbf{M}/\mathbf{M}_1$ invariant.*

We observe that, both because of (2.1.2) and also by (2.2) the group $\mathfrak{G}/\mathfrak{G}_n$ is nilpotent, in the usual sense, and of class $n - 1$ at most. Indeed, $\mathfrak{G}/\mathfrak{G}_3$ is abelian.

We investigate now the orders of elements of $\mathfrak{G}$.

THEOREM 2.3. *If α is an integer, and if F is given by*

$$F : x \rightarrow x + a_{r+1}\,x^{r+1} + \ldots \text{ with } a_{r+1} \neq 0,$$

then F^{α} is given by

$$F^{\alpha} : x \rightarrow x + \alpha a_{r+1}\,x^{r+1} + \ldots.$$

In particular, if a_{r+1} is such that $\alpha a_{r+1} = 0$ implies $\alpha = 0$, then F is an element of infinite order.

COROLLARY 2.4. *If R is of characteristic zero, (that is, if $\alpha a = 0$, $\alpha \neq 0$ implies $a = 0$ for all $a \in R$) then every element of $\mathfrak{G}(R)$ other than the identity is of infinite order.*

https://doi.org/10.4153/CJM-1954-031-9 Published online by Cambridge University Press

Theorem 2.5. *If R is of prime characteristic p (i.e., if $pa=0$ for all $a \in R$), then*

$$\mathfrak{G}_r^{(p)} \subseteq \mathfrak{G}_{rp},$$

that is, the pth power of every element in $\mathfrak{G}_r$ is in $\mathfrak{G}_{rp}$.

Theorem 2.3 follows at once from (1.1.2) while 2.4 follows from 2.3. We will prove 2.5 by establishing first the following:

Lemma 2.6 *If $f_s = 1 + a_1x^s + \dots$, and $f_r = 1 + b_1x^r + \dots$, where a_i, b_j are in R, then there exists an f_{r+s},*

$$f_{r+s} = 1 + c_1x^{r+s} + \dots,$$

with coefficients in R such that

$$f_s(xf_r) = f_s \cdot f_{r+s},$$

where $f_s \,.\, f_{r+s}$ is the formal product of the series on the right.

Proof of 2.6. Consider

$$(2.6.1) \quad 1 + a_1x^s(1 + b_1x^r + \dots)^s + a_2x^{s+1}(1 + a_1x^r + \dots)^{s+1} + \dots$$
$$= 1 + a_1x^s + \dots + a_rx^{s+r-1} + sa_1b_1x^{r+s} + \dots.$$

On the other hand,

$$(2.6.2) \quad (1 + a_1x^s + \dots + a_rx^{s+r-1} + a_{r+1}x^{s+r} + \dots)(1 + c_1x^{r+s} + \dots)$$
$$= 1 + a_1x^s + \dots + a_rx^{s+r-1} + (a_{r+1} + c_1)x^{r+s} + (a_{r+2} + c_2)x^{r+s+1} + \dots,$$

so that, equating coefficients of x^{s+r}, $x^{s+r+1} \dots$ in (2.6.1) and (2.6.2) in succession, we may obtain the c_k as polynomials in the coefficients a_i and b_j.

Proof of 2.5. Let $F_r : x \to x + a_{r+1}\,x^{r+1} + \dots$ be any element of $\mathfrak{G}_r(R)$. We set

$$x + a_{r+1}\,x^{r+1} + \dots = xf_r(x),$$

where $f_r = 1 + a_{r+1}\,x^r + \dots$ is as in Lemma 2.6. Then

$$F_r^2\colon\ x \to xf_rf_r(xf_r),$$

and by (2.6) there exists an $f_{2r} = 1 + b_{2r}x^{2r} + \dots$ such that

$$F_r^2\colon\ x \to xf_r^2 \cdot f_{2r}.$$

We prove by induction that, for α an integer,

$$(2.6.3) \qquad F_r^\alpha\colon\ x \to x\, f_r^{\binom{\alpha}{1}} f_{2r}^{\binom{\alpha}{2}} f_{3r}^{\binom{\alpha}{3}} \dots f_{\alpha r}^{\binom{\alpha}{\alpha}},$$

where f_{kr} is defined inductively by

$$f_{(k-1)r}(xf_r) = f_{(k-1)r}(x) \,.\, f_{kr}$$

and is therefore of the form

$$f_{kr} = 1 + d_{kr}\,x^{kr} + \dots, \qquad d_{kr}, d_{kr+1}, \dots \in R,$$

and $\binom{\alpha}{\beta}$ is the usual binomial coefficient. For if (2.6.3) holds for given α, then

$$F_r^{\alpha+1} = F_r^\alpha F_r \colon x \to x f_r f_r^{\binom{\alpha}{1}} (xf_r) \ldots f_{kr}^{\binom{\alpha}{k}} (xf_r) \ldots f_{\alpha r}^{\binom{\alpha}{\alpha}} (xf_r)$$
$$= x f_r^{\binom{\alpha}{1}+1} f_{2r}^{\binom{\alpha}{2}+\binom{\alpha}{1}} \ldots f_{kr}^{\binom{\alpha}{k}+\binom{\alpha}{k-1}} \ldots f_{(\alpha+1)r}(x)$$

and hence

$$F_r^{\alpha+1} \colon x \to x f_r^{\binom{\alpha+1}{1}} f_{2r}^{\binom{\alpha+1}{2}} \ldots f_k^{\binom{\alpha+1}{k}} \ldots,$$

which establishes (2.6.3) for all α.

Now if $\alpha = p$, a prime, we have, since p divides all of

$$\binom{p}{1}, \binom{p}{2}, \ldots \binom{p}{p-1},$$

$$F_r^p \colon x \to x f_r^p f_{2r}^{\beta_2 p} \ldots f_{(p-1)r}^{\beta_{p-1}} f_{pr}; \tag{2.6.4}$$

where the β_i are integers and hence, since if R is of characteristic p,

$$(1 + d_{kr} x^{kr} + \ldots)^p = 1 + d_{kr}^p x^{krp} + \ldots,$$

we see that $F_r{}^p$ has the form

$$F_r{}^p : x \to x(1 + e_1 x^{rp} + \ldots),$$
$$= x + e_1 x^{rp+1} + \ldots,$$

where $e_1, e_2, \ldots$ depend on $a_{r+1}, \ldots$. Hence $F_r{}^p \in \mathfrak{G}_{rp}$ if $F_r \in \mathfrak{G}_r$.

COROLLARY 2.7. *If $pR = 0$ and $r \leqslant p^\beta$ then G/G_r is a group all of whose elements are of order at most p^β.*

THEOREM 2.8. *If R is nilpotent, with $R^\lambda = 0$, then the lower central series of $\mathfrak{G}$ is of finite length, that is, $\mathfrak{G}(R)$ is nilpotent in the usual sense.*

Proof of 2.8. As in (2.1.2), we may readily verify that the mappings

$$F : x \to x + a_2 x^2 + \ldots$$

and

$$G : x \to x + b_2 x^2 + \ldots$$

yield

$$(F, G) = x + c_4 x^4 + c_5 x^5 + \ldots, \tag{2.8.1}$$

where each coefficient in (2.8.1) is the product of two or more coefficients a_i, b_j. Hence

$$(F, G) \in G(R^2)$$

and in general we verify that

$$C_n \in G(R^n), \tag{2.8.2}$$

where C_n is any commutator of weight n in the elements of $G(R)$. If $R^\lambda = 0$, then $C_\lambda = 1$ as required. Indeed, we remark that, more generally, if S and T are ideals of R, and $G_r(S) \in \mathfrak{G}_r(S)$, $G_s(T) \in \mathfrak{G}_s(T)$ then

$$(G_r(S), G_s(T)) \in \mathfrak{G}_{r+s}(S \cdot T). \tag{2.8.3}$$

https://doi.org/10.4153/CJM-1954-031-9 Published online by Cambridge University Press

For satisfactory definition of the lower central series of $\mathfrak{G}(R)$ we introduce the notion of a *topological generating set*. Let K be any set of elements of $G(R)$ and let $\mathfrak{K}$ be the smallest closed subgroup of $\mathfrak{G}$ containing K. Then we say that $\mathfrak{K} = [K]$ and that $\mathfrak{K}$ is generated (topologically) by K. In particular, if $\mathfrak{A}$, $\mathfrak{B}$ are normal closed subgroups of $\mathfrak{G}$, we define $[\mathfrak{A}, \mathfrak{B}]$ as the smallest closed subgroup generated by all elements of the form $(A, B) = A^{-1}B^{-1}AB$ where $A \in \mathfrak{A}$ and $B \in \mathfrak{B}$. In general $[\mathfrak{A}, \mathfrak{B}]$ is normal, since if

$$C = \lim G_n$$

then

$$G^{-1}\, C\, G = \lim\, (G^{-1}\, G_n\, G).$$

In our case $[\mathfrak{A}, \mathfrak{B}]$ is a proper subgroup of both $\mathfrak{A}$ and $\mathfrak{B}$, since if $\mathfrak{A} \subseteqq \mathfrak{G}_r$ but $\mathfrak{A} \not\subset \mathfrak{G}_{r+1}$, $\mathfrak{B} \subseteqq \mathfrak{G}_s$ but $\mathfrak{B} \not\subset \mathfrak{G}_{s+1}$, then $[\mathfrak{A}, \mathfrak{B}] \subseteqq \mathfrak{G}_{r+s}$, so that $[\mathfrak{A}, \mathfrak{B}] \neq \mathfrak{A}, \mathfrak{B}$.

We may now define the lower central series of $\mathfrak{G}(R)$:

$$\mathfrak{G} = \mathfrak{H}_1 \supset \mathfrak{H}_2 \supset \ldots \supset \mathfrak{H}_i \supset \ldots \tag{2.9.1}$$

by setting $\mathfrak{G} = \mathfrak{H}_1$, and $\mathfrak{H}_{i+1} = [\mathfrak{H}_i, \mathfrak{G}]$ for $i \geqslant 1$. By the above, $\mathfrak{H}_i \subseteqq G_i(R)$ and hence in the series (2.9.1) $\bigcap \mathfrak{H}_i = 1$, so that $\mathfrak{G}$ is generalized nilpotent in the usual sense.

3. Power series groups over a field of characteristic zero. If the ring R satisfies suitable chain conditions then it has a nilpotent radical N and R/N is a direct sum of fields. In this case $\mathfrak{G}(N)$ is a normal subgroup, which by (2.8) is nilpotent in the usual sense, while by (1.2) $\mathfrak{G}(R/N)$ is a direct product of groups $\mathfrak{G}(F_i)$ where the F_i are fields. For groups of the type $\mathfrak{G}(F)$, where F is a field, two cases arise, according as F is of characteristic 0, or characteristic $p \neq 0$. We consider in the present paper only the case when F is of characteristic 0. The case where F is of characteristic p will be discussed elsewhere.

In what follows in the rest of this section, therefore, *the coefficient ring will be a field F of characteristic zero*: we will write $\mathfrak{G} = \mathfrak{G}(F)$. Our first result deals with certain one parameter subgroups of $\mathfrak{G}$.

THEOREM 3.1. *Let $G_k(\alpha)$ be the element of $\mathfrak{G}(F)$ defined by the mapping*

$$G_k(\alpha)\colon\, x \rightarrow \frac{x}{(1 - k\alpha x^k)^{1/k}}, \tag{3.1.1}$$

where $\alpha \in F$, $k = 1, 2, \ldots$ and

$$\frac{x}{(1 - k\alpha x^k)^{1/k}} = x + \alpha x^{k+1} + \frac{(1+k)\alpha^2 x^{2k+1}}{2!} + \ldots \tag{3.1.2}$$
$$\ldots + \frac{(1+k)(1+2k)\ldots(1+(n-1)k)\alpha^n x^{nk+1}}{n!} + \ldots$$

is the power series, with coefficients in F, obtained by expanding $x(1-k\alpha x^k)^{-1/k}$ formally by the binomial theorem. Then for fixed k the set of elements $\{G_k(\alpha)\}$, as α runs over F, is an abelian subgroup of $\mathfrak{G}$ contained in $\mathfrak{G}_k$, with

https://doi.org/10.4153/CJM-1954-031-9 Published online by Cambridge University Press

$$G_k(\alpha)\cdot G_k(\beta) = G_k(\alpha+\beta),$$

(3.1.3)
$$G_k(0) = 1,$$
$$G_k(-\alpha) = G_k^{-1}(\alpha).$$

Proof. The fact that $G_k(\alpha)\,G_k(\beta) = G_k(\alpha+\beta)$ may be verified by direct substitution in (3.1.1).

THEOREM 3.2. *The one parameter subgroups* $\{G_k(\alpha)\}$ $k = 1, 2, \ldots$ *determine a uniqueness basis for* $\mathfrak{G}$ *in the sense that every element* G *of* $\mathfrak{G}$ *may be written uniquely*

$$G = G_1(\alpha_1)\,G_2(\alpha_2)\ldots G_n(\alpha_n)\ldots.$$

The infinite product on the right is to be interpreted as

$$\lim_{n\to\infty}\quad G_1(\alpha_1)\ldots G_n(\alpha_n)$$

in the subgroup topology.

Proof. Let G be given by

$$G : x \to x + a_2x^2 + \ldots + a_sx^s + \ldots.$$

It will suffice to prove that, for any n, there exist elements $\alpha_1, \alpha_2, \ldots \alpha_n$ of F such that

$$G \equiv G_1(\alpha_1)\ldots G_n(\alpha_n) \qquad (\text{mod } G_{n+1}).$$

For $n = 1$, it is clear that

$$G \equiv G_1(a_2) \qquad (\text{mod } G_2)$$

and $\alpha_1 = a_2$. Assume that for given k there exist coefficients $\bar{\alpha}_1, \ldots, \bar{\alpha}_k$ which are polynomials in $a_2, \ldots, a_{k+1}$ so that

(3.2.1)
$$G \equiv G_1(\bar{\alpha}_1)\ldots G_k(\bar{\alpha}_k) \qquad (\text{mod } G_{k+1}).$$

If we consider

$$G_1(\alpha_1)\ldots G_k(\alpha_k) : x \to x + \beta_2x^2 + \ldots + \beta_{k+1}x^{k+1} + \beta_{k+2}x^{k+2} + \ldots$$

for $\alpha_1, \ldots, \alpha_k$ arbitrary, the coefficients β_i, for all i, are polynomials in $\alpha_1, \ldots a_k$. By our induction, when

$$\alpha_i = \bar{\alpha}_i, \quad \beta_2 = a_2, \ldots \quad \beta_{k+1} = a_{k+1} \text{ and } \beta_{k+2} = \bar{\beta}_{k+2}$$

say, where $\bar{\beta}_{k+2}$ is now a polynomial in $\bar{\alpha}_1\ldots\bar{\alpha}_k$ and hence in $a_2, \ldots a_{k+1}$. Consider now

$$G_1(\alpha_1)\ldots G_k(\alpha_k)G_{k+1}\,(\alpha_{k+1}) : x \to x + \beta_2x^2 + \ldots$$
$$+ \beta_{k+1}\,x^{k+1} + (\alpha_{k+1} + \beta_{k+2})\,x^{k+2} + \ldots.$$

Define $\bar{\alpha}_{k+1} = a_{k+2} - \bar{\beta}_{k+2}$. Then $\bar{\alpha}_{k+1}$ is a polynomial in $a_2, \ldots, a_{k+2}$ and when $\alpha_2 = \bar{\alpha}_2, \ldots a_k = \bar{\alpha}_k$, $\alpha_{k+1} = \bar{\alpha}_{k+1}$, we have

$$G_1(\bar{\alpha}_1)\ldots G_{k+1}(\bar{\alpha}_{k+1}) : x \to x + a_2x^2 + \ldots + a_{k+1}x^{k+1} + a_{k+2}x^{k+2} + \ldots.$$

https://doi.org/10.4153/CJM-1954-031-9 Published online by Cambridge University Press

Our induction is complete, and in particular (3.2.1) holds for all k, which proves our theorem, and shows indeed that the $\alpha_1, \ldots \alpha_k, \ldots$ of (3.2) are such that

$$\alpha_k = a_k + p_k(a_2, \ldots, a_{k-1}),$$

where p_k is a polynomial with coefficients in F. We note in passing that (3.1) and (3.2) may be generalized to groups $\mathfrak{G}(R)$ if R is a ring of characteristic zero which admits the rational field.

THEOREM 3.3. *$\mathfrak{G}$ is generated (topologically) by the subgroups $\{G_1(\alpha)\}$ and $\{G_2(\beta)\}$.*

THEOREM 3.4. *Every element G given by*

$$G : x \rightarrow x + a_{r+3}x^{r+3} + \ldots, \qquad r = 1, 2, \ldots,$$

can be written as an infinite product of the form

$$G = C_r\, C_{r+1} \ldots,$$

where each C_k is a commutator of weight $k + 1$ in elements of $G_1(\alpha)$ and $G_2(\beta)$ of the form

$$C_k = (G_2(\beta), G_1(\alpha_1), G_1(\alpha_2) \ldots G_1(\alpha_k)).$$

COROLLARY 3.5. *$\mathfrak{G} = \mathfrak{H}_1$, $\mathfrak{G}_{s+1} = \mathfrak{H}_s$, $s = 2, 3, \ldots$, where $\mathfrak{H}_1 \supset \mathfrak{H}_2 \supset \ldots$ is the lower central series of $\mathfrak{G}$ in the sense of* (2.9.1).

Proof of (3.3)-(3.5). By (2.1.2) we have

$$C_1 = (G_2(\beta), G_1(\alpha_1)) = x + \alpha_1\beta x^4 + \ldots$$

and in general, if

$$C_k = (G_2(\beta), G_1(\alpha_1), G_1(\alpha_2) \ldots, G_1(\alpha_k)),$$

then

$$C_k : x \rightarrow x + k!\alpha_1\alpha_2 \ldots \alpha_k\beta x^{k+3} + \ldots.$$

Without giving details we note that we may proceed in a perfectly straightforward manner as in the proof of (3.2) to show that if

$$G : x \rightarrow x + a_{r+3}x^{r+3} + \ldots, \qquad r = 1, 2, \ldots,$$

then it is possible to choose $\beta, \alpha_1, \alpha_2, \ldots$ so that, for all integers $n = 0, 1, 2, \ldots$,

$$G \equiv C_r C_{r+1} \ldots C_{r+n} \qquad (\text{mod } \mathfrak{G}_{n+r+3}).$$

However, this will imply that

$$G = \lim_{n\rightarrow\infty} C_r C_{r+1} \ldots C_{r+n}$$

in our topology, and establish (3.4). To prove (3.3) we remark that for any G given by

$$G : x \rightarrow x + a_2x^2 + a_3x^3 + \ldots,$$

we may write

$$G \equiv G_1(a_2)\, G_2(a_3 - a_2^2) \pmod{\mathfrak{G}_3} \tag{3.5.1}$$

since

$$G_1(a_2)\colon x \to x + a_2x^2 + a_2^2x^3 + \dots$$

and

$$G_2(a_3 - a_2^2)\colon x \to x + (a_3 - a_2^2)\, x^3 + \dots,$$

and therefore

$$G_1(a_2)\, G_2(a_3 - a_2^2)\colon x \to x + a_2x^2 + a_3x^3 + e_4x^4 + e_5x^5 + \dots,$$

where $e_4, e_5, \dots$ depend on a_2 and a_3.

From (3.5.1) there is an element G_3 of $\mathfrak{G}_3$ such that

$$\begin{aligned} G &= G_1(a_2)\, G_2(a_3 - a_2^2)\, G_3 \\ &= G_1(a_2)\, G_2(a_3 - a_2^2)\, C_3C_4 \dots \end{aligned}$$

by (3.4).

To prove (3.5) we observe that we have proved that every element of $\mathfrak{G}_{s+1}$ belongs to $\mathfrak{H}_s$, $s \geqslant 2$, since any G_{s+1} is expressible as a product of commutators of weight at least s in the elements of $\mathfrak{G}$. If $H_s \in \mathfrak{H}_s$, then let

$$H_s = x + \alpha_\sigma x^\sigma + \dots.$$

H_s is either a product of commutators of weight s in elements of $\mathfrak{G}$, or the limit of such a product. However, any commutator of weight s is in $\mathfrak{G}_{s+1}$, and and hence $\sigma \geqslant s + 1$, that is $\mathfrak{H}_s = \mathfrak{G}_{s+1}$ and we have our corollary.

4. The Lie algebra of a group $\mathfrak{G}(F)$. To conclude our discussion of groups $\mathfrak{G}(F)$, where F is of characteristic 0, we remark that we may associate with $\mathfrak{G}$ a Lie algebra $\mathfrak{L}$ over F which determines $\mathfrak{G}$ in the usual fashion. For consider the algebra $\mathfrak{L}$ whose basis over F consists of the operators $x^2D, x^3D, \dots$, where D is the formal operation of differentiation with respect to x. Let us set

$$\mu_1 = x^2D \quad \mu_2 = x^3D, \dots, \quad \mu_k = x^{k+1}D, \dots.$$

Then

$$[\mu_i, \mu_j] = \mu_i\mu_j - \mu_j\mu_i = (j - i)x^{i+j+1}D = (j - i)\mu_{i+j} \tag{4.1.1}$$

for $i, j = 1, 2, \dots$.

The Lie algebra $\mathfrak{L}$ spanned by the μ_i over F is generalized nilpotent in the sense that the chain of ideals

$$\mathfrak{L} = \mathfrak{L}_1 \supset \mathfrak{L}_2 \supset \dots \supset \mathfrak{L}_k \supset \dots,$$

where $\mathfrak{L}_{i+1} = [\mathfrak{L}_i, \mathfrak{L}]$, has intersection 0. $\mathfrak{L}_k$ is spanned by the elements $\mu_{k+1}, \mu_{k+2}, \dots$. We may therefore introduce infinite sums of the type

$$\lambda = \alpha_1\mu_1 + \alpha_2\mu_2 + \dots, \qquad \alpha_i \in F \tag{4.1.2}$$

into $\mathfrak{L}$, and consider, formally at least, the differential operators

https://doi.org/10.4153/CJM-1954-031-9 Published online by Cambridge University Press

$$\exp \lambda = \left(1 + \lambda + \frac{\lambda^2}{2!} + \ldots\right), \qquad \lambda \in \mathfrak{L}.$$

If we form

$$(\exp \lambda)x$$

we obtain

$$(\exp \lambda)x = x + a_2x^2 + \ldots, \tag{4.1.2}$$

where for $k = 1, 2, \ldots$, the coefficients a_{k+1} are polynomials in $\alpha_1, \alpha_2, \ldots, \alpha_k$. That is, to every λ in $\mathfrak{L}$ we may associate a $G(\lambda) \in \mathfrak{G}$, $G(\lambda) : x \rightarrow (\exp \lambda)x$. Since the coefficients $a_2, a_3, \ldots$ are determined as functions

$$a_{k+1} = a_{k+1}(\alpha_1, \ldots, \alpha_k),$$

we may consider the $\alpha_1, \alpha_2, \ldots$ as *canonical parameters* in $\mathfrak{G}$: they have the familiar property that if $G(\lambda)$ is the G determined by λ above, then, for all $t, \tau \in F$,

$$G(t\lambda)\, G(\tau\lambda) = G((t + \tau)\lambda) :$$

that is, the set $G(t\lambda)$ is a one parameter subgroup as t runs over F. In particular the one parameter subgroups (3.1.2) obtained earlier are given by

$$G_k(\alpha) : x \rightarrow (\exp \alpha\mu_k)\, x = x(1 - k\alpha x^k)^{-1/k}.$$

We note too that if $\lambda_i \in \mathfrak{L}_i$, then $(\exp \lambda_i)\, x = H_i$ is in $\mathfrak{H}_i = \mathfrak{G}_{i+1}$; that is, the ideals $\mathfrak{L}_i$ determine the lower central series of $\mathfrak{G}$.

If we adjoin the operator $\mu_0 = xD$ to $\mathfrak{L}$ we get a Lie algebra $\mathfrak{L}^*$ spanned by the elements μ_k $(k = 0, 1, 2, \ldots)$ which has $\mathfrak{L}$ as its derived algebra. For $[\mu_0, \mu_i] = i\mu_i$, so that the commutator rules (4.1.1) hold in $\mathfrak{L}^*$ for $i, j = 0, 1, 2, \ldots$. If F is a field in which e^α is defined for all $\alpha \in F$, then the element

$$\lambda^* = \alpha_0\mu_0 + \alpha_1\mu_1 + \ldots$$

determines, via the operator $\exp(\lambda^*)$, a transformation

$$x \rightarrow (\exp \lambda^*)\, x = b_1x + \sum b_sx^s, \qquad s = 2, 3, \ldots,$$

where

$$b_1 = e^{\alpha_0} \neq 0.$$

Even if exponentials are not defined in F, it is easy to verify that the group of transformations $\mathfrak{G}^*$ consisting of all mappings of the form

$$x \rightarrow b_1x + \sum b_sx^s, \qquad b_1 \neq 0,$$

is such that

$$(\mathfrak{G}^*, \mathfrak{G}^*) = \mathfrak{G}.$$

This group $\mathfrak{G}^*$ is the group of all automorphisms of $\mathbf{M}_1$ over F, as in (1.4) above.

5. Groups with integral coefficients. We conclude this paper with one or two remarks about the group $\mathfrak{G}(I)$ where I is the ring of integers. For convenience we write $\mathfrak{J} = \mathfrak{G}(I)$. Let p be any prime, and let I_α be the ideal (p^α) of all integers divisible by p^α, $\alpha = 1, 2, \ldots$. If we set $I_0 = I$, then corresponding to the ideals

$$I = I_0 \supset I_1 \supset I_2 \ldots$$

we have the chain of normal subgroups

$$\mathfrak{J} = \mathfrak{P}_0 \supset \mathfrak{P}_1 \supset \mathfrak{P}_2 \supset \ldots, \tag{5.0.1}$$

where $\mathfrak{P}_\alpha = \mathfrak{G}(I_\alpha)$. If G_α is any element of $\mathfrak{P}_\alpha$ then

$$G_\alpha : x \rightarrow x + a_2x^2 + a_3x^3 + \ldots,$$

where $p^\alpha | a_k$ for all $k = 2, 3, \ldots$. Now by (1.3),

$$\mathfrak{G}(I_0/I_1) \cong \mathfrak{G}(I_0)/\mathfrak{G}(I_1),$$

and since $I_0/I_1 \cong GF(p)$, we see that the factor group $\mathfrak{J}/\mathfrak{P}_1$ is a group $\mathfrak{G}(F)$, where F is the prime field of characteristic p. Groups of this type have a rather complicated structure, some indication of which will be given in a later paper. The structure of the group $\mathfrak{P}_1$ is simpler to consider, and we prove, in fact:

THEOREM 5.1. *The groups* (5.0.1) *have the properties*;

(1) $$(\mathfrak{P}_\alpha, \mathfrak{P}_\beta) \leqslant \mathfrak{P}_{\alpha+\beta}, \qquad \alpha, \beta = 0, 1, 2, \ldots.$$

(2) If $G_\alpha \in \mathfrak{P}_\alpha$, *where* $\alpha \geqslant 1$, *then*

$$G_\alpha^p \in \mathfrak{P}_{\alpha+1}.$$

Proof. If $G_\alpha \in \mathfrak{P}_\alpha$, $G_\beta \in \mathfrak{P}_\beta$, then we have

$$\begin{aligned} G_\alpha &: x \rightarrow x + a_2x^2 + a_3x^3 + \ldots, \\ G_\beta &: x \rightarrow x + b_2x^2 + b_3x^3 + \ldots, \end{aligned}$$

where $p^\alpha | a_s$ and $p^\beta | b_s$, $s = 2, 3, \ldots$. Then

$$G_\alpha G_\beta : x \rightarrow x + c_2x^2 + c_3x^3 + \ldots$$

yields, by (1.1.2),

$$\begin{aligned} c_2 &= a_2 + b_2, \\ c_r &= a_r + b_r + \sum a_s\phi_s(b_2, \ldots, b_s), \\ &\qquad s = 2, 3, \ldots r-1; \qquad r = 2, 3, \ldots. \end{aligned}$$

Now since $p^\beta | b_s$ for all s, $p^\beta | \phi_s$ for all s, and hence $p^{\alpha+\beta} | a_s\phi_s$ for all s. Hence

$$c_r \equiv a_r + b_r \pmod{p^{\alpha+\beta}}, \qquad r = 2, 3, \ldots. \tag{5.1.3}$$

If (5.1.3) holds, and if C is given by

$$C : x \rightarrow x + (a_2 + b_2)x^2 + (a_3 + b_3)x^3 + \ldots,$$

then $G_\alpha G_\beta \equiv C \pmod{\mathfrak{P}_{\alpha+\beta}}$; for in the homomorphism $\mathfrak{G}(I) \rightarrow \mathfrak{G}(I/I_{\alpha+\beta})$ induced by $I \rightarrow I/I_{\alpha+\beta}$, as in the proof of (1.3), the elements $G_\alpha G_\beta$ and C map into the same element in $\mathfrak{G}(I/I_{\alpha+\beta})$. However, if we form $G_\beta G_\alpha$ we have

https://doi.org/10.4153/CJM-1954-031-9 Published online by Cambridge University Press

$$G_\beta\, G_\alpha\colon\ x \rightarrow x + c_2'x^2 + c_3'x^3 + \ldots$$

where

$$c_2' = b_2 + a_2,$$
$$c_r' = b_r + a_r + \sum b_s\phi_s(a_2, \ldots, a_s),$$

so that

$$c_r' \equiv a_r + b_r \equiv c_r \qquad (\text{mod } p^{\alpha+\beta}),$$

and hence, as before,

$$G_\beta\, G_\alpha \equiv C \equiv G_\alpha\, G_\beta \qquad (\text{mod } \mathfrak{P}_{\alpha+\beta}),$$

which proves (1) of (5.1). To establish (2) we form, for $\alpha \geqslant 1$ and any integer n

$$G_\alpha^{\ n} : x \rightarrow x + c_2(n)x^2 + c_3(n)x^3 + \ldots$$

and observe that, by (1.1.2),

$$c_r(n) = na_r + \Phi_r(n), \qquad r = 2, 3, \ldots,$$

where $\Phi_r(n)$ is a polynomial in $a_2, a_3, \ldots, a_r$ whose term of lowest degree is at least of degree 2. Now if p^α divides $a_2, \ldots, a_r$, $p^{2\alpha}$ divides $\Phi_r(n)$ and *a fortiori* so does $p^{\alpha+1}$. Hence

$$c_r(n) \equiv na_r \qquad (\text{mod } p^{\alpha+1}),$$
$$c_r(p) \equiv 0 \qquad (\text{mod } p^{\alpha+1}),$$

so that $G_\alpha^{\ p} \in \mathfrak{P}_{\alpha+1}$ as required.

COROLLARY 5.2. *The factor groups $\mathfrak{P}_\alpha/\mathfrak{P}_{\alpha+1}$ are infinite direct products, for $\alpha \geqslant 1$, of elementary abelian groups of order p.*

REFERENCES

1. S. Bochner and W. T. Martin, *Several Complex Variables* (Princeton, 1948).
2. M. Gotô, *On the group of formal analytic transformations*, Kodai Math. Sem. Reports, No. 3 (1950), 45–46.
3. N. Jacobson, *Classes of restricted Lie algebras of characteristic p*, II. Duke Math. J., *10* (1943), 107–121.

University of British Columbia

https://doi.org/10.4153/CJM-1954-031-9 Published online by Cambridge University Press