THE GROUP RING OF A CLASS OF INFINITE NILPOTENT GROUPS

S. A. JENNINGS

Introduction. In this paper we study the (discrete) group ring Γ of a finitely generated torsion free nilpotent group $\mathfrak{G}$ over a field of characteristic zero. We show that if Δ is the ideal of Γ spanned by all elements of the form $G - 1$, where $G \in \mathfrak{G}$, then

$$\Delta \supset \Delta^2 \supset \Delta^3 \supset \ldots \supset \Delta^w \supset \Delta^{w+1} \supset \ldots$$

and the only element belonging to Δ^w for all w is the zero element (c.f. (4.3) below). This fact enables us to topologize Γ in a natural way. We may then define for $\mathfrak{G}$ "dimensional subgroups" relative to the ideal Δ which are the analogues of those considered by Magnus **(7; 8; 9)** for a free group. In part II we associate a Lie algebra with $\mathfrak{G}$ in a natural manner via the group ring, and show that $\mathfrak{G}$ is a subgroup of the simply connected Lie group determined by this Lie algebra. To some extent these last results overlap those of Malcev **(11; 11)**. However, our approach differs greatly from his, since our methods are intrinsic in the sense that topological considerations from the theory of Lie groups do not intervene.

Part I: The Group Ring

1. Preliminary notions. We follow the notation in **(1)** and write

$$(H, K) = H^{-1}K^{-1}HK$$

for the commutator of elements H, K of a group $\mathfrak{G}$, while if $\mathfrak{H}$, $\mathfrak{K}$ are subgroups of $\mathfrak{G}$ then $(\mathfrak{H}, \mathfrak{K})$ is the subgroup of $\mathfrak{G}$ generated by all (H, K) with $H \in \mathfrak{H}$, $K \in \mathfrak{K}$, and similarly for higher commutators. The group $\mathfrak{G}$ is *nilpotent and of class c* if the lower central series of G is as follows:

$$\mathfrak{G} = \mathfrak{G}_1 \supset \mathfrak{G}_2 \supset \ldots \supset \mathfrak{G}_c \supset \mathfrak{G}_{c+1} = \{1\} \tag{1.0.1}$$

where $\mathfrak{G}_{i+1} = (\mathfrak{G}_i, \mathfrak{G})$ $(i = 1, 2, \ldots c)$. A series of normal subgroups

$$\mathfrak{G} = \mathfrak{K}_1 \supseteq \mathfrak{K}_2 \supseteq \ldots \supseteq \mathfrak{K}_m \supseteq \mathfrak{K}_{m+1} = \{1\} \tag{1.0.2}$$

is a *central series* if $(\mathfrak{K}_i, \mathfrak{G}) \subseteq \mathfrak{K}_{i+1}$ $(i = 1, 2, \ldots m)$ and the existence of a

Received July 29, 1953. Part I of this paper was presented to the American Mathematical Society, August 23, 1946. This paper was completed while the author was a Fellow at the Summer Research Institute of the Canadian Mathematical Congress, 1952 and 1953. The author wishes to express his thanks to the Board of Governors of the University of British Columbia for a research grant in connection with this investigation.

central series is necessary and sufficient for a group to be nilpotent. We recall also that for any central series we have

$$(\mathfrak{K}_j, \mathfrak{G}_i) \subseteq \mathfrak{K}_{i+j}, \qquad i, j = 1, 2, \ldots . \tag{1.0.3}$$

The upper central series of a nilpotent group G:

$$\mathfrak{G} = \mathfrak{Z}_c \supset \mathfrak{Z}_{c-1} \supset \ldots \supset \mathfrak{Z}_1 \supset \mathfrak{Z}_0 = \{1\} \tag{1.0.4}$$

is usually defined by taking $\mathfrak{Z}_1$, as the centre of $\mathfrak{G}$, and for $i > 1$, $\mathfrak{Z}_i$ as the subgroup in $\mathfrak{G}$ corresponding to the centre of $\mathfrak{G}/\mathfrak{Z}_{i-1}$ in the homomorphism $\mathfrak{G} \rightarrow \mathfrak{G}/\mathfrak{Z}_{i-1}$. The following equivalent definition of the series (1.0.4) is probably well known:

THEOREM 1.1. *$\mathfrak{Z}_i$ is the largest normal subgroup of $\mathfrak{G}$ such that*

$$(\mathfrak{Z}_i, \mathfrak{G}, \mathfrak{G}, \ldots \mathfrak{G}) = 1,$$

where the number of $\mathfrak{G}$'s in the above is i.

Proof. Since $\mathfrak{Z}_1$ may be defined as the largest normal subgroup for which $(\mathfrak{Z}_1, \mathfrak{G}) = 1$, assume the theorem true for $\mathfrak{Z}_{i-1}$, and let $\mathfrak{N}$ be any normal subgroup of $\mathfrak{G}$ such that

$$(\mathfrak{N}, \mathfrak{G}, \mathfrak{G}, \ldots \mathfrak{G}) = 1 \qquad \text{for } i \text{ factors } \mathfrak{G}.$$

Then

$$((\mathfrak{N}, \mathfrak{G}), \mathfrak{G}, \ldots \mathfrak{G}) = 1$$

and $(\mathfrak{N}, \mathfrak{G}) \subseteq \mathfrak{Z}_{i-1}$ by induction. That is, $\mathfrak{N}$ is in the centre of $\mathfrak{G}$ modulo $\mathfrak{Z}_{i-1}$ and hence $\mathfrak{N} \subseteq \mathfrak{Z}_i$, from which it follows that $\mathfrak{Z}_i$ is the maximal normal subgroup having the property $(\mathfrak{N}, \mathfrak{G}, \ldots \mathfrak{G}) = 1$ with i factors $\mathfrak{G}$.

A group will be said to be *torsion free* if every element of the group $\neq 1$ is of infinite order. Using (1.1) we now establish, in slightly more general form, a result due to Malcev (**9**, corollary 2).

THEOREM 1.2. *Let $\mathfrak{G}$ be a torsion free nilpotent group with upper central series*

$$\mathfrak{G} = \mathfrak{Z}_c \supset \mathfrak{Z}_{c-1} \supset \ldots \supset \mathfrak{Z}_1 \supset \mathfrak{Z}_0 = \{1\}.$$

Then $\mathfrak{Z}_i/\mathfrak{Z}_{i-1}$ is torsion free.

Proof. Suppose $G \in \mathfrak{Z}_i$ and $G \notin \mathfrak{Z}_{i-1}$, but $G^\alpha \in \mathfrak{Z}_{i-1}$ for some positive integer α: such a G certainly exists if $\mathfrak{Z}_i/\mathfrak{Z}_{i-1}$ is not torsion free. Then

$$(G^\alpha, G_1) \in \mathfrak{Z}_{i-2},$$

for all $G_1 \in \mathfrak{G}$, and because of the identity

$$(PQ, R) = (P, R)(P, R, Q)(Q, R)$$

we have

$$(G^\alpha, G_1) \equiv (G, G_1)^\alpha \equiv 1 \pmod{\mathfrak{Z}_{i-2}}.$$

Using $(G, G_1)^\alpha$ instead of G^α we show similarly that

$$(G^\alpha, G_1, G_2) \equiv (G, G_1, G_2)^\alpha \equiv 1 \pmod{\mathfrak{Z}_{i-3}},$$

and finally

$$(G, G_1, G_2, \ldots, G_{i-1})^\alpha \equiv 1 \pmod{\mathfrak{Z}_0},$$

for all $G_1, \ldots, G_{i-1} \in \mathfrak{G}$, or, since $\mathfrak{Z}_0 = \{1\}$ and $\mathfrak{G}$ is torsion free,

$$(G, G_1, G_2, \ldots G_{i-1}) = 1$$

for all $G_1, \ldots G_{i-1} \in \mathfrak{G}$. But by (1.1) this implies that $G \in \mathfrak{Z}_{i-1}$, which is a contradiction, so that our result is established.

COROLLARY 1.3. *If $\mathfrak{G}$ is a torsion free nilpotent group, then $\mathfrak{G}/\mathfrak{Z}_i$ $(i = 1, 2, \ldots c - 1)$ is torsion free.*

2. Finitely generated torsion free nilpotent groups. Infinite solvable groups with maximal condition for subgroups have been investigated by Hirsch **(3; 4; 5)**, who calls such groups "S-groups." We show first that every finitely generated nilpotent (and therefore a fortiori solvable) group is an S-group.

THEOREM 2.1. *Every finitely generated nilpotent group satisfies the maximal condition for subgroups.*

Proof. Let $\mathfrak{G}$ be nilpotent and finitely generated by the elements $P_1, P_2, \ldots P_r$, and let the lower central series of $\mathfrak{G}$ be as in (1.0.1): then by **(1**, Theorem 2.81**)**,

$$\mathfrak{G}_w = \{Q_1, Q_2, \ldots Q_s, \mathfrak{G}_{w+1}\},$$

where $Q_1, Q_2, \ldots, Q_s$ are the various formally distinct commutators of weight w in $P_1, P_2, \ldots, P_r$, there being only a finite number of the Q's since there are only a finite number of the P's. Hence $\mathfrak{G}_w/\mathfrak{G}_{w+1}$ is an abelian group with a finite number of generators, and the series (1.0.1) satisfies the condition **(3**, (1.11)**)**, so that $\mathfrak{G}$ is an S-group, as required.

We recall **(4**, Theorem 2.22**)** that the elements of a finitely generated nilpotent group $\mathfrak{G}$ which are of finite order form a normal subgroup $\mathfrak{F}$, so that the quotient group $\mathfrak{G}/\mathfrak{F}$ is torsion free. In what follows we call any group which is torsion free, nilpotent and finitely generated an *N-group*. That such groups exist follows from the above remark.

Now Hirsch has shown also **(4**, Theorem 2.311**)** that in any finitely generated nilpotent group $\mathfrak{G}$ there exist series of subgroups, each normal in $\mathfrak{G}$:

(2.1.1) $$\mathfrak{G} = \mathfrak{A}_1 \supset \mathfrak{A}_2 \supset \mathfrak{A}_3 \supset \ldots \supset \mathfrak{A}_r \supset \mathfrak{A}_{r+1} = (1)$$

with the properties

(2.1.2) $\mathfrak{A}_i/\mathfrak{A}_{i+1}$ is either cyclic of prime order, or an infinite cyclic group.

(2.1.3) The number of infinite cyclic factors in any series (2.1.1) satisfying (2.1.2) is an invariant of the group $\mathfrak{G}$. **(4**, Theorem 2.23**)**.

We prove now that if $\mathfrak{G}$ is an N-group, we may find series (2.1.1) all of whose factors are infinite cyclic, and indeed such that the series itself is a central series:

THEOREM 2.2. *Any N-group $\mathfrak{G}$ has at least one central series*

$$\mathfrak{G} = \mathfrak{F}_1 \supset \mathfrak{F}_2 \supset \ldots \supset \mathfrak{F}_r \supset \mathfrak{F}_{r+1} = \{1\}, \tag{2.2.0}$$

such that

(1) $\mathfrak{F}_i/\mathfrak{F}_{i+1}$ $(i = 1, 2, \ldots r)$ *is an infinite cyclic group,*

(2) $(\mathfrak{F}_i, \mathfrak{G}) \subseteq \mathfrak{F}_{i+1}$.

The length r of any such series is an invariant of the group, which we call the rank of $\mathfrak{G}$.

Proof. The invariance of the rank will follow from (2.1.3). Now by (1.2), since $\mathfrak{G}$ is an N-group, the factors $\mathfrak{Z}_i/\mathfrak{Z}_{i-1}$ of the upper central series (1.0.4) of $\mathfrak{G}$ are torsion free, and by (**3**, Theorem 1.33), are finitely generated, so that $\mathfrak{Z}_i/\mathfrak{Z}_{i-1}$ is a direct product of a finite number of infinite cyclic groups. We may therefore refine the upper central series of $\mathfrak{G}$ so that between any two consecutive terms $\mathfrak{Z}_i$ and $\mathfrak{Z}_{i-1}$ we have a finite chain of subgroups

$$\mathfrak{Z}_i \supset \mathfrak{U}_{i1} \supset \mathfrak{U}_{i2} \supset \ldots \supset \mathfrak{U}_{iz_i} = \mathfrak{Z}_{i-1},$$

so that each factor is infinite cyclic. Since

$$(\mathfrak{Z}_i, \mathfrak{G}) \subseteq \mathfrak{Z}_{i-1}, \quad (\mathfrak{U}_{ij}, \mathfrak{G}) \subseteq \mathfrak{Z}_{i-1} \subseteq \mathfrak{U}_{i,j+1},$$

and hence the refinement forms part of a central series of $\mathfrak{G}$.

Any series satisfying (1) and (2) of (2.2) will be called an $\mathfrak{F}$-*series* of the N-group $\mathfrak{G}$. It can be readily verified that a group is an N-group if and only if it has $\mathfrak{F}$-series.

The following follows at once from (**4**, Theorem 2.312)

THEOREM 2.3. *Let $\mathfrak{G}$ be an N-group of rank r, and let $\mathfrak{H}$ be a normal subgroup of $\mathfrak{G}$ such that $\mathfrak{G}/\mathfrak{H}$ is an N-group of rank s. Then $\mathfrak{H}$ is of rank $r - s$, and there is an $\mathfrak{F}$-series of $\mathfrak{G}$ such that $\mathfrak{F}_{s+1} = \mathfrak{H}$.*

COROLLARY 2.4. *If $\mathfrak{G}$ has an $\mathfrak{F}$-series*

$$\mathfrak{G} = \mathfrak{F}_1 \supset \mathfrak{F}_2 \supset \ldots \mathfrak{F}_r \supset \mathfrak{F}_{r+1} = \{1\},$$

then $\mathfrak{G}/\mathfrak{F}_{i+1}$ is an N-group of rank i, and $\mathfrak{F}_{i+1}$ is of rank $r - i$,

$$(i = 1, 2, \ldots, r - 1).$$

Let $\mathfrak{G}$ be an N-group with $\mathfrak{F}$-series

$$\mathfrak{G} = \mathfrak{F}_1 \supset \mathfrak{F}_2 \supset \ldots \supset \mathfrak{F}_{r+1} = \{1\},$$

and let F_i be a representative in $\mathfrak{G}$ of a generating element of $\mathfrak{F}_i$ modulo $\mathfrak{F}_{i+1}$: then any element G of $\mathfrak{G}$ may be written uniquely in the form

$$G = F_1^{\alpha_1} F_2^{\alpha_2} \ldots F_r^{\alpha_r}, \tag{2.5.1}$$

https://doi.org/10.4153/CJM-1955-022-5 Published online by Cambridge University Press

where $\alpha_1, \ldots, \alpha_r$ are integers, positive, negative or zero. In what follows we assume that an $\mathfrak{F}$-series, and the elements $F_1, \ldots, F_r$ have been selected once and for all. We refer to the elements $F_1, \ldots, F_r$ as an *$\mathfrak{F}$-basis* for $\mathfrak{G}$, and to the representation (2.5.1) as the *$\mathfrak{F}$-representation* of $\mathfrak{G}$. Because of (2.2(2)) we have, since $(\mathfrak{F}_i, \mathfrak{F}_j) \subseteq \mathfrak{F}_k$, where $k > \max(i, j)$,

$$F_i^{\alpha_i} F_j^{\alpha_j} = F_j^{\alpha_j} F_i^{\alpha_i} F_k^{\gamma_k} F_{k+1}^{\gamma_{k+1}} \ldots F_r^{\gamma_r} \tag{2.5.2}$$

for some $k > \max(i, j)$ $(i, j = 1, 2, \ldots r)$. In particular we observe that F_r belongs to the centre of $\mathfrak{G}$, and in particular

$$F_r^{\alpha_r} F_j^{\alpha_j} = F_j^{\alpha_j} F_r^{\alpha_r} \tag{2.5.3}$$

for all j.

It is known that an N-group may be ordered, and indeed this follows easily from the existence of the $\mathfrak{F}$-representation (2.5.1) and the relations (2.5.2). We need only remark that if

$$G = F_1^{\alpha_1} \ldots F_r^{\alpha_r}, \quad H = F_1^{\beta_1} \ldots F_r^{\beta_r},$$

we may define $G < H$ when, for $1 \leqslant s \leqslant r$, $\alpha_1 = \beta_1, \alpha_2 = \beta_2, \ldots \alpha_{s-1} = \beta_{s-1}$, but $\alpha_s < \beta_s$. With this lexicographic ordering, it follows from (2.5.2) that if $G < H$ then $GK < HK$, $KG < KH$, for all $K \in \mathfrak{G}$, from which it follows that

$$\text{(2.5.4)} \qquad \textit{if } G_1 < H_1 \textit{ and } G_2 < H_2, \textit{ then } G_1G_2 < H_1H_2,$$

which is the condition that the relation "$<$" order the group.

3. The group ring of an N-group. For a moment, let $\mathfrak{G}$ be any group and let Φ be any field of characteristic 0. The (discrete) group ring Γ of $\mathfrak{G}$ over Φ will consist of all finite sums of the form

$$x = \sum \xi_i G_i, \qquad \xi_i \in \Phi,\ G_i \in \mathfrak{G}, \tag{3.0.1}$$

with addition, scalar multiplication, and ring multiplication defined in the natural manner. Γ may of course be of infinite rank over Φ, but in considerations involving only a finite number of elements of Γ of the form (3.0.1), we may assume that the summations run over the same group elements in each case. As usual we identify the prime subfield of Φ with the rationals, and the unit elements of Γ and of $\mathfrak{G}$ with the number 1. Thus there will be no confusion in supposing that, in an expression such as (2.5), the rational integers α_i belong to Φ: indeed we will often write, for example, if $F \in \mathfrak{G}$,

$$F^\alpha = 1 + \alpha(F-1) + \tfrac{1}{2}\alpha(\alpha-1)(F-1)^2 + \ldots,$$

where α is a positive integer and F^α is considered as an element of Γ.

Let $\mathfrak{G}_1$ be any subgroup of $\mathfrak{G}$: then the group ring Γ_1 of $\mathfrak{G}_1$ over Φ may be considered as a subalgebra of Γ. If $\mathfrak{G}_1$ is normal in $\mathfrak{G}$, and if $\mathfrak{G}' = \mathfrak{G}/\mathfrak{G}_1$, we may consider also the group ring Γ' of $\mathfrak{G}'$ over Φ. We recall **(6, §4)** first the relationship between Γ, Γ_1, Γ'.

Let Δ be the two-sided ideal of Γ spanned by all elements of the form $(G - 1)$, $G \in \mathfrak{G}$. A necessary and sufficient condition that an element $x \in \Gamma$,

$$x = \sum \xi_i G_i,$$

belong to Δ is that $\sum \xi_i = 0$, and clearly $\Gamma/\Delta \cong \Phi$ so that Δ is a maximal ideal of Γ. Similarly Δ_1 is the maximal ideal of Γ_1 spanned by the elements $G_1 - 1$ for all $G_1 \in \mathfrak{G}_1$. The homomorphism of $\mathfrak{G}$ onto $\mathfrak{G}'$ defined by

$$G \rightarrow G\,\mathfrak{G}_1$$

may be extended in a natural fashion to a homomorphism of Γ onto Γ' by means of the mapping

$$x = \sum \xi_i G_i \rightarrow x' = \sum \xi_i G_i \mathfrak{G}_1. \tag{3.0.2}$$

The kernel of this homomorphism (3.0.2) may be identified as follows. Let $\bar{G}_\alpha$ be a representative in $\mathfrak{G}$ of the coset $G_\alpha \mathfrak{G}_1$ and let $x = \sum \xi_i G_i$ be written in the form

$$x = \sum_{\alpha,\beta} \xi'_{\alpha\beta} \bar{G}_\alpha G_{1\beta}, \qquad G_{1\beta} \in \mathfrak{G}_1$$

then the mapping (3.0.2) may be written

$$x = \sum_{\alpha,\beta} \xi'_{\alpha\beta} \bar{G}_\alpha G_{1\beta} \rightarrow \sum_\alpha \left(\sum_\beta \xi'_{\alpha\beta} \right) G_\alpha \mathfrak{G}_1$$

and $x \rightarrow 0$ if and only if

$$\sum_\beta \xi'_{\alpha\beta} = 0$$

for all α. Hence if $x \rightarrow 0$, we may write

$$x = \sum_{\alpha,\beta} \xi'_{\alpha\beta} G_\alpha (G_{1\beta} - 1), \tag{3.0.3}$$

and conversely. Thus, we have proved

LEMMA 3.1. *The kernel of the homomorphism of* Γ *upon* Γ' *defined by* (3.0.2) *is the ideal* $\Gamma\Delta_1$, *where* Δ_1 *is the ideal of* Γ_1 *spanned by all elements of the form* $(G_{1\beta} - 1)$, $G_{1\beta} \in \mathfrak{G}_1$.

Suppose next that $\mathfrak{G}$ is an *ordered* group satisfying (2.5.4). Then Γ contains no divisors of zero, and no units other than scalar multiples of group elements. For consider two elements $x, y \neq 0$ of Γ;

$$x = \sum_{i=1}^{m} \alpha_i G_i, \qquad \alpha_1 \neq 0,\ \alpha_m \neq 0,$$

$$y = \sum_{j=1}^{n} \beta_j H_j, \qquad \beta_1 \neq 0,\ \beta_n \neq 0.$$

We may suppose $G_1 < G_2 < \ldots < G_m$, $H_1 < H_2 < \ldots < H_n$. Then in the product

$$xy = \alpha_1\beta_1 G_1 H_1 + \ldots + \alpha_m \beta_n G_m H_n$$

https://doi.org/10.4153/CJM-1955-022-5 Published online by Cambridge University Press

we have $G_1H_1 < G_iH_j < G_mH_n$ $(1 < i < m,\ 1 < j < m)$, so that if $xy = 0$, $\alpha_1\beta_1 = \alpha_m\beta_n = 0$, which is false, and hence $xy \neq 0$ for all m, n. Similarly if $xy = 1$, then $m = n = 1$ and $\alpha_1\beta_1 = 1$, $G_1H_1 = 1$, $H_1 = G_1^{-1}$.

In particular, since any N-group is ordered, we may state:

THEOREM 3.2. *The group ring Γ of an N-group $\mathfrak{G}$ has no proper divisors of zero, and no units other than scalar multiples of group elements.*

4. The structure of the ideal Δ. From now on $\mathfrak{G}$ will be an N-group. Let Δ be the ideal spanned by the elements $G - 1$, for $G \in \mathfrak{G}$ as in §3. Consider the element $G - 1 \in \Delta$. Because of (2.5.1), we may write

$$(G - 1) = (F_1^{\alpha_1} F_2^{\alpha_2} \ldots F_r^{\alpha_r} - 1), \tag{4.0.1}$$

and because of the identity

$$AB - 1 = (A - 1) + (B - 1) + (A - 1)(B - 1), \tag{4.0.2}$$

we may write $G - 1$ as a linear combination,

$$G - 1 = \sum_{\omega, \rho} \delta_{\omega, \rho} \pi_{\omega, \rho}. \tag{4.0.3}$$

Here the coefficients $\delta_{\omega,\rho}$ are integers and

$$\pi_{\omega, \rho} = (F_{i_1}^{\alpha_{i_1}} - 1)(F_{i_2}^{\alpha_{i_2}} - 1) \ldots (F_{i_s}^{\alpha_{i_s}} - 1), \tag{4.0.4}$$

$(i_1, \ldots i_s)$ is a subset of the integers $1, 2, \ldots, r$ with

$$1 \leqslant i_1 < i_2 < \ldots i_s \leqslant r.$$

Also $\alpha_{i_1}, \ldots, \alpha_{i_s}$ are the exponents of $F_{i_1}, \ldots, F_{i_s}$ in (4.0.1), where for brevity we have written $\rho = (i_1, \ldots, i_s)$ and

$$\omega = (\alpha_{i_1}, \ldots, \alpha_{i_s}).$$

Note also that the summation in (4.0.3) will extend over certain subsets ρ and ω determined by the $(\alpha_1, \ldots, \alpha_r)$ of (4.0.1) and the identity (4.0.2).

We have also the binomial identity, for integers α:

$$\begin{aligned}(A^{\alpha} - 1) &= \{1 + (A^{\pm 1} - 1)\}^{|\alpha|} - 1 \\ &= \sum_t \binom{|\alpha|}{t} (A^{\pm 1} - 1)^t, \qquad t = 1, 2, \ldots |\alpha|,\end{aligned} \tag{4.0.5}$$

the positive or negative exponent on the right being taken as α is positive or negative.

Consider now a product of the form

$$(F_{i_1}^{\pm 1} - 1)^{\delta_1}(F_{i_2}^{\pm 1} - 1)^{\delta_2} \ldots (F_{i_s}^{\pm 1} - 1)^{\delta_s} \tag{4.0.6}$$

where $1 \leqslant i_1 < i_2 < \ldots < i_s \leqslant r$ as in (4.0.4), $\delta_1, \ldots, \delta_s$ are positive integers, and where any combination of positive and negative exponents may occur, except that of course two factors

$$(F_j - 1) \text{ and } (F_j^{-1} - 1)$$

https://doi.org/10.4153/CJM-1955-022-5 Published online by Cambridge University Press

do not occur in the same product. We call $w = \delta_1 + \ldots + \delta_s$ the *degree* of such a product, and denote by

$$P_{w1}, P_{w2}, \ldots, P_{wl_w}, \qquad w = 1, 2, \ldots,$$

the various formally distinct products of degree w, since for fixed w there are only a finite number of such distinct products (4.0.6).

Applying (4.0.5) to each of the factors

$$(F_{i_k}^{\alpha i_k} - 1)$$

in (4.0.4), we readily verify that every $\pi_{\omega,\rho}$, and hence by (4.0.3) every element $(G - 1)$, may be written as a linear combination, with integral coefficients, of products (4.0.6). Now every element x of Δ is expressible in the form

$$x = \sum \xi_i (G_i - 1), \qquad \xi_i \in \Phi,$$

and we see therefore that any element x of Δ may be written as a linear combination of products of the form (4.0.6),

$$(4.0.7) \qquad x = \gamma_1 P_{w_1 \nu_1} + \gamma_2 P_{w_2 \nu_2} + \ldots + \gamma_s P_{w_s \nu_s}, \qquad \gamma_i \in \Phi.$$

It is readily verified that the products $P_{w\nu}$ are linearly independent: for suppose

$$\gamma_1 P_{w_1 \nu_1} + \gamma_2 P_{w_2 \nu_2} + \ldots + \gamma_k P_{w_k \nu_k} = 0, \qquad \gamma_i \in \Phi,$$

where the products are distinct and all $\psi_i \neq 0$. An easy lexicographical argument similar to that used in establishing (3.2) shows that a relation of this type would imply one of the same kind among group elements of the form

$$G_i = F_1^{\alpha_1 i} \ldots F_r^{\alpha_r i}$$

where the $(\alpha_{1i}, \ldots, \alpha_{ri})$ are all distinct, which is impossible in view of the uniqueness of the representation (2.5.1). We omit the details, which may be supplied without difficulty. Thus we have proved

THEOREM 4.1. *The formally distinct products $P_{w\nu}$ of the form* (4.0.6) *are linearly independent and form a basis for the ideal Δ. The representation* (4.0.7) *is unique.*

As an immediate consequence of (4.1) we have:

COROLLARY 4.2. *A relation of the form*

$$p_0 + (F_\rho - 1)p_1 + \ldots + (F_\rho - 1)^n p_n = 0$$

where $p_0, p_1, \ldots, p_n$ are elements of the group ring of $\mathfrak{F}_{\rho+1}$ implies $p_k = 0$ $(k = 0, 1, \ldots, n)$.

We define the *weight* of any product of w factors $(F_{\rho_i}^{\pm 1} - 1)$:

$$(4.2.0) \qquad \prod (F_{\rho_i}^{\pm 1} - 1), \qquad i = 1, 2, \ldots, w,$$

https://doi.org/10.4153/CJM-1955-022-5 Published online by Cambridge University Press

where the factors occur in any order, and where

$$(F_{\rho_i} - 1), \quad (F_{\rho_i}^{-1} - 1)$$

may occur in the same product, to be

$$W = \sum 2^{\rho_i}, \tag{4.2.1}$$

where the summation is taken over the same ρ_i, $(i = 1, 2, \ldots, w)$ which occur in (4.2.0).

In particular, therefore, the weight W of a product

$$(F_1^{\pm 1} - 1)^{\alpha_1}(F_2^{\pm 1} - 1)^{\alpha_2} \ldots (F_r^{\pm 1} - 1)^{\alpha_r}$$

(α_i non-negative integers) will be

$$W = \alpha_1 2^1 + \alpha_2 2^2 + \ldots + \alpha_r 2^r.$$

Consider now the identity

$$\begin{aligned}(B - 1)(A - 1) &= (A - 1)(B - 1) + AB(B^{-1}A^{-1}BA - 1)\\ &= (A - 1)(B - 1) + (B^{-1}A^{-1}BA - 1)\\ &\quad + (A - 1)(B^{-1}A^{-1}AB - 1)\\ &\quad + (B - 1)(B^{-1}A^{-1}BA - 1)\\ &\quad + (A - 1)(B - 1)(B^{-1}A^{-1}BA - 1).\end{aligned} \tag{4.2.2}$$

If $\rho_i < \rho_j$, we have, because of (2.5.2),

$$F_{\rho_j}^{\mp 1} F_{\rho_i}^{\mp 1} F_{\rho_j}^{\pm 1} F_{\rho_i}^{\pm 1} = \prod_{\sigma} F_\sigma^{\alpha_\sigma}, \qquad \sigma = \rho_j + 1,\ \rho_j + 2, \ldots, r;$$

and hence by (4.0.7)

$$(F_{\rho_j}^{\mp 1} F_{\rho_i}^{\mp 1} F_{\rho_j}^{\pm 1} F_{\rho_i}^{\pm 1} - 1) = \sum \gamma_{w\nu} P^*_{w\nu}, \qquad \gamma_{w\nu} \in \Phi,$$

where $P^*_{w\nu}$ are products of the form (4.0.6) with all $\rho > \rho_j$. Now the weight $W(P^*_{w\nu})$ of every product $P^*_{w\nu}$ is at least 2^{ρ_j+1}, and since

$$W((F_{\rho_j}^{\pm 1} - 1)(F_{\rho_i}^{\pm 1} - 1)) = 2^{\rho_i} + 2^{\rho_j} < 2^{\rho_j+1},$$

we see, by using (4.2.2) with

$$A = F_{\rho_i}^{\pm 1}, B = F_{\rho_j}^{\pm 1},$$

that

$$(F_{\rho_j}^{\pm 1} - 1)(F_{\rho_i}^{\pm 1} - 1) = (F_{\rho_i}^{\pm 1} - 1)(F_{\rho_j}^{\pm 1} - 1) + \text{products } P_{w\gamma},$$

where

$$W(P_{w\nu}) > 2^{\rho_i} + 2^{\rho_j}.$$

By repeated application of this "straightening" process it may be verified that *every product of the form* (4.2.0) *of weight W may be expressed as a linear combination of products of weights no less than W in which the factors occur in the natural order.*

https://doi.org/10.4153/CJM-1955-022-5 Published online by Cambridge University Press

We observe that in these "straightened" products we may have consecutive factors of the form

$$(F_\rho^{-1} - 1)^{\alpha_\rho}(F_\rho - 1)^{\beta_\rho}.$$

For convenience let us denote a "straightened" product of weight W (containing perhaps both

$$(F_\rho^{-1} - 1)^{\alpha_\rho}, \quad (F_\rho - 1)^{\beta_\rho}$$

with $\alpha_\rho\, \beta_\rho \neq 0$) by

$$(4.2.3) \qquad Q_W = \prod_\rho (F_\rho^{-1} - 1)^{\alpha_\rho}(F_\rho - 1)^{\beta_\rho}, \qquad \rho = 1, 2, \ldots, r,$$

where

$$W = \sum_\rho (\alpha_\rho + \beta_\rho)\, 2^\rho,$$

and some of α_ρ, β_ρ may be zero.

We establish now the principal theorem of this section:

THEOREM 4.3. *For all w, Δ^{w+1} is a proper ideal of Δ^w, and* $\bigcap \Delta^w = 0$, i.e.

$$\Delta \supset \Delta^2 \supset \ldots \supset \Delta^w \supset \Delta^{w+1} \supset \ldots$$

and the only element in Δ^w for all w is 0.

Proof. Since $(F_1 - 1)^w \neq 0 \in \Delta^w$ for all w, it is clear that no power of Δ vanishes, and it will be enough to prove the following: "the only element x which belongs to Δ^w for all w is zero." The proof is by induction over the rank of $\mathfrak{G}$, and we show first that the theorem is true for groups of rank 1, that is, when $\mathfrak{G} = \{F\}$.

Suppose that $x \neq 0$ is an element of $\Delta(\mathfrak{G})$, where $\mathfrak{G} = \{F\}$, which is in Δ^u for arbitrarily large u. Now by (4.1) we may write x uniquely in the form

$$x = \sum \gamma_i (F^{-1} - 1)^i + \sum \delta_j (F - 1)^j, \qquad i = 1, \ldots, n; \; j = 1, \ldots, m.$$

If $x \in \Delta^u$ for arbitrary u, $y = F^\rho x$ has the same property for any integer ρ, and hence by choosing ρ large enough to cancel all negative powers in x above we may suppose that if there is an element $y \neq 0$ in Δ^u for all u it has the form

$$y = \gamma_1 (F - 1)^{\alpha_1} + \ldots + \gamma_n (F - 1)^{\alpha_n}, \qquad \gamma_i \in \Phi,$$

where $0 < \alpha_1 < \alpha_2 < \ldots < \alpha_n$ and $\gamma_k \neq 0$ $(k = 1, \ldots, n)$. Choose $u > \alpha_1$: then if $y \in \Delta^u$, y may be written as a finite sum of products with $\geqslant u$ factors:

$$y = \sum{}_i \delta_i (F^{-1} - 1)^{\beta_i}(F - 1)^{\beta'_i}, \qquad \beta_i + \beta'_i \geqslant u > \alpha_1,$$

and hence

$$\gamma_1 (F - 1)^{\alpha_1} + \ldots + \gamma_n (F - 1)^{\alpha_n} - \sum \delta_i (F^{-1} - 1)^{\beta_i}(F - 1)^{\beta'_i} = 0.$$

Now

$$(F^{-1} - 1)^{\beta_i} = \pm F^{-\beta_i}(F - 1)^{\beta_i},$$

and hence

$$(F-1)^{\alpha_1}[\gamma_1+\gamma_2(F-1)^{\alpha_2-\alpha_1}+\ldots+\gamma_n(F-1)^{\alpha_n-\alpha_1} \\ -\sum(\pm\delta_i)\,F^{-\beta_i}(F-1)^{\beta_i+\beta'_i-\alpha_1}]=0.$$

Since there are no divisors of zero in Γ, we have

$$[\gamma_1+\gamma_2(F-1)^{\alpha_2-\alpha_1}+\ldots\sum\pm\delta_i(F-1)^{\beta_i+\beta'_i-\alpha_1}F_i^{-\beta_i}]=0,$$

which implies $\gamma_1\equiv 0 \pmod{\Delta}$, since $\beta_i+\beta'_i-\alpha_1>0$, and hence $\gamma_i=0$, which is contra hypothesis.

We now assume our theorem for groups of rank $\leqslant r-1$, (and in particular for $\mathfrak{F}_2$), and prove it for groups $\mathfrak{G}$ of rank r. Suppose that $x\neq 0$ is an element of $\Delta(\mathfrak{G})$ which is in $\Delta^u(\mathfrak{G})$ for arbitrary large u. By (4.1) we have a unique expression

$$x=\sum\gamma_{wk}P_{wk}, \qquad \gamma_{wk}\in\Phi,$$

which we write

$$x=p_0+(F_1^{\pm1}-1)^{\alpha_1}p_1+\ldots+(F_1^{\pm1}-1)^{\alpha_n}p_n,$$

where p_0 is a sum of P_{wk} lying in $\Delta(\mathfrak{F}_2)$ of the form

$$P_{wk}=\prod(F_\rho^{\pm1}-1)^{\alpha_\rho}, \qquad \rho\geqslant 2, \tag{4.3.1}$$

and p_i, $i\geqslant 1$, is a similar sum with perhaps a term containing only an element of Φ. If x belongs to $\Delta^u(\mathfrak{G})$ for all u, so does $y=F^\sigma\,.\,x$, and we may once more suppose, therefore, that our x has the form

$$x=q_0+(F_1-1)^{\alpha_1}q_1+\ldots+(F_1-1)^{\alpha_n}q_n,$$

where $0<\alpha_1<\alpha_2<\ldots<\alpha_n$, and q_k $(k=0,\ldots,n)$ is also a sum of P_{wk} of the form (4.3.1) with $q_1,q_2,\ldots,q_n\neq 0$ and where q_0 may or may not be zero for the moment. Consider $q_0,\ldots,q_n$: they are all in $\Delta(\mathfrak{F}_2)$ since otherwise (4.3) is false for $\mathfrak{G}/\mathfrak{F}_2$. By our induction assumption if $q_0\neq 0$ there is an u' such that $q_0\notin\Delta^{u'}(\mathfrak{F}_2)$; if $q_0=0$ there is, since $q_1\neq 0$, a u'' such that $q_1\notin\Delta^{u''}(\mathfrak{F}_2)$. Let $w=u'$ or $u''+\alpha_1$ as $q_0\neq 0$, or $q_0=0$, and choose $u=2^rw$.

If $x\in\Delta^u(\mathfrak{G})$, x may be written as a sum of products of the form (4.2.0) $p'(u_i)$, each having at least u factors and, therefore, of weight $u_i\geqslant u$:

$$x=\sum\gamma(u_i)\prod_{j=1}^{u_i}(F_{\rho_j}^{\pm1}-1)=\sum\gamma(u_i)\,p'(u_i), \qquad \gamma(u_i)\in\Phi,$$

where $u_i\geqslant u$. Now as in (4.2.3) each of the products $p'(u_i)$ in this sum may be "straightened" without loss of weight so that

$$x=\sum\bar\gamma(v_i)\,Q(v_i), \qquad \bar\gamma(v_i)\in\Phi,$$

where the weights v_i of all $Q(v_i)$ are at least u. These products $Q(v_i)$ are of two types: those lying in $\Delta(\mathfrak{F}_2)$ and those containing a factor

$$(F_1^{-1}-1)^{\beta_i}\,(F_1-1)^{\beta'_i}$$

https://doi.org/10.4153/CJM-1955-022-5 Published online by Cambridge University Press

at the beginning. Denote a $Q(v_1)$ in $\Delta(\mathfrak{F}_2)$ by $Q'(v_i)$: then each $Q(v_i)$ is either a $Q'(v_i)$ or of the form

$$(F_1^{-1} - 1)^{\beta_i} \,.\, (F_1 - 1)^{\beta'_i} \,.\, Q'(v_j).$$

Because of our choice of u, every product $Q'(u_i)$ of weight $\geqslant u$ contains at least w factors, since the weight in $\Delta(\mathfrak{F}_2)$ of a product $Q'(u_i)$ is of the form (cf. (4.2.3)):

$$(\alpha_2 + \beta_2)2^1 + (\alpha_3 + \beta_3)2^2 + \ldots + (\alpha_r + \beta_r)2^{r-1},$$

and if this is greater than or equal to $u = 2^r w$, then certainly

$$(\alpha_2 + \beta_2) + \ldots + (\alpha_r + \beta_r) \geqslant w.$$

Hence each $Q'(u_i)$ is in $\Delta^w(\mathfrak{F}_2)$. Now we have

$$x = q_0 + (F_1 - 1)^{\alpha_1} q_1 + \ldots = \sum \{\gamma'_k Q'(u_k) + \delta_k (F_1^{-1} - 1)^{\beta_k} (F_1 - 1)^{\beta'_k} Q'(v_k)\},$$

where the right-hand side is in $\Delta^u(\mathfrak{G})$. If $q_0 \neq 0$ then

$$q_0 = \sum \gamma'_k Q'(u_k)$$

by (4.2). This is impossible, since $Q'(u_k) \in \Delta^w(\mathfrak{F}_2)$, and $w = u'$, where $q_0 \notin \Delta^{u'}(\mathfrak{F}_2)$. If $q_0 = 0$ we have

$$\sum \gamma'_k Q'(u_k) = 0$$

and hence,

$$(F_1 - 1)^{\alpha_1}[q_1 + (F_1 - 1)^{\alpha_2 - \alpha_1} q_2 + \ldots - (\sum \bar{\delta}_k Q'(\bar{u}_k) + \ldots)] = 0,$$

for it follows that $\beta_k + \beta_k' \geqslant \alpha_1$ for all k since if, for some k, $\beta_k + \beta_k' < \alpha_1$ we could remove the factor

$$(F_1 - 1)^{\beta_k + \beta'_k}$$

and get $Q'(u_k) = 0$. Again this implies a relation

$$q_1 = \sum \bar{\delta}_k Q'(\bar{u}_k)$$

where $Q'(\bar{u}_k)$ has at least $(u'' + \alpha_1) - \alpha_1$ factors and is therefore in $\Delta^{u''}(\mathfrak{F}_2)$ which is impossible, since $q_1 \notin \Delta^{u''}(\mathfrak{F}_2)$.

We have proved, therefore, that 0 is the only element in $\Delta^w(\mathfrak{G})$ for all w. It follows that for every element $x \neq 0 \in \Delta$ there exists a w such that $x \in \Delta^w$, $x \notin \Delta^{w+1}$. Moreover, Γ/Δ^{w+1} is an algebra of finite rank over Φ.

In view of (4.3) it is natural to introduce infinite sums into the ring Γ by means of a "Δ-adic" topology. Take the set $\{\Delta^w\}$ $(w = 1, 2, \ldots)$ as a fundamental system of neighbourhoods of the element 0 in Γ: then a sequence $a_1, a_2, \ldots, a_n \ldots$ of elements of Γ "converges" to $a \in \Gamma$ if, for given w, there exists an integer N such that $n > N$ implies that

$$(a_n - a) \in \Delta^w.$$

Let Γ^* be the completion of Γ in this topology, and let Δ^* be the completion of Δ. Clearly we may consider Γ^* to be the ring of all "power series" a^* of the form

(4.3.2) $$a^* = \alpha_0 + \sum \alpha_k d_k, \qquad \alpha_k \in \Phi, k = 1, 2, \ldots,$$

where $d_k \in \Delta^k$, while Δ^* consists of all elements a^* with $\alpha_0 = 0$. As usual, we identify Γ with its isomorphic image in Γ^*. We note that

(4.3.3) $$G^{-1} = 1 - (G-1) + (G-1)^2 - (G-1)^3 + \ldots,$$

in Γ^*, and that, more generally, if $a^* \notin \Delta^*$ then a^* is a unit in Γ^*.

It is clear that we have the following:

THEOREM 4.4. *For any integer* n, $\Gamma/\Delta^{n+1} \cong \Gamma^*/\Delta^{*(n+1)}$ *and* $\bigcap \Delta^{*w} = 0$.

Because of (4.4) we can work with either Γ^* or Γ in what follows.

5. The dimensional sub-groups of $\mathfrak{G}$. The concept of dimensional subgroup relative to the ideal Δ (or Δ^*) is now natural. Let $\mathfrak{D}_w$ $(w = 1, 2, \ldots)$ be the set of all elements $D_w \in \mathfrak{G}$ such that

$$D_w \equiv 1 \pmod{\Delta^{*w}}.$$

If $D_w \equiv D_w' \equiv 1 \pmod{\Delta^{*w}}$ we have

$$D_w = 1 + d_w,\ D_w' = 1 + d_w'; \qquad d_w, d_w' \in \Delta^{*w}$$

and hence

$$D_w D_w' = 1 + d_w + d_w' + d_w d_w' \equiv 1 \pmod{\Delta^{*w}},$$

while

$$D^{-1} = 1 - d_w + d_w^2 - d_w^3 + \ldots \equiv 1 \pmod{\Delta^{*w}}.$$

Further, if G is any element of $\mathfrak{G}$, we have

$$G^{-1} D_w G = 1 + G^{-1} d_w G \equiv 1 \pmod{\Delta^{*w}},$$

so that $\mathfrak{D}_w$ is a normal subgroup of $\mathfrak{G}$. We have also

$$D_w^{-1} D_v^{-1} D_w D_v = 1 + D_w^{-1} D_v^{-1} (d_w d_v - d_v d_w) \equiv 1 \pmod{\Delta^{*w+v}},$$

where $D_v = 1 + d_v$, $d_v \in \Delta^{*v}$, and hence $(\mathfrak{D}_w, \mathfrak{D}_v) \subseteqq \mathfrak{D}_{w+v}$. In particular $(\mathfrak{D}_w, \mathfrak{G}) \subseteqq \mathfrak{D}_{w+1}$. These results may be summarized in

THEOREM 5.1. *The set $\mathfrak{D}_w$ of elements D_w of $\mathfrak{G}$ which are congruent to* 1 mod Δ^{*w} *form a normal subgroup of $\mathfrak{G}$, and the series*

$$\mathfrak{G} = \mathfrak{D}_1 \supseteqq \mathfrak{D}_2 \supseteqq \ldots$$

is a central series of $\mathfrak{G}$ with the property $(\mathfrak{D}_w, \mathfrak{D}_v) \subseteqq \mathfrak{D}_{w+v}$ $(w, v = 1, 2, \ldots)$.

The subgroups $\mathfrak{D}_w$ we shall call **(6; 7; 8)** the *dimensional subgroups of* $\mathfrak{G}$.

Suppose D_w belongs to $\mathfrak{D}_w$ but not to $\mathfrak{D}_{w+1}$. We have

$$D_w = 1 + d_w$$

https://doi.org/10.4153/CJM-1955-022-5 Published online by Cambridge University Press

where $d_w \in \Delta^{*w}$ and $d_w \notin \Delta^{*w+1}$, and hence

$$D_w^n = (1 + d_w)^n \equiv 1 + nd_w \bmod \Delta^{*w+1}.$$

Now since Φ is of characteristic 0, $nd_w \not\equiv 0$ (Δ^{*w+1}) for any integer n, and hence

$$D_w^n \in \mathfrak{D}_{w+1}$$

only if $n = 0$. Hence if $\mathfrak{D}_w \neq \mathfrak{D}_{w+1}$, $\mathfrak{D}_w/\mathfrak{D}_{w+1}$ is torsion free. By refining the dimensional series (5.1) we obtain an $\mathfrak{F}$-series of the form (2.2.0). It follows that the dimensional series of $\mathfrak{G}$ is of finite length. We have, therefore:

THEOREM 5.2. *The dimensional subgroups of $\mathfrak{G}$ form a central series of finite length $\mathfrak{G} = \mathfrak{D}_1 \supseteqq \mathfrak{D}_2 \supseteqq \ldots \supseteqq \mathfrak{D}_m \supseteqq \mathfrak{D}_{m+1} = \{1\}$; and are such that if $\mathfrak{D}_w \supset \mathfrak{D}_{w+1}$ then $\mathfrak{D}_w/\mathfrak{D}_{w+1}$ is a direct product of infinite cyclic groups.*

The problem of identifying the dimensional subgroups of $\mathfrak{G}$ we leave to a later paper. However, in view of (**6**, Theorem 5.5), it is natural to suspect that they are the minimal subgroups enjoying the properties indicated in (5.2), and this is indeed the case, as we shall prove.

PART II: THE LIE ALGEBRA OF AN N-GROUP

6. The Campbell-Hausdorff Formula in Γ^*. For the rest of this paper we work with Γ^* and Δ^*, since the possibility of infinite sums, which was inconvenient in most of Part I, is now essential.

Let x^* be any element of Δ^*: then we may form

$$\exp(x^*) = 1 + x^* + \frac{x^{*2}}{2!} + \ldots + \frac{x^{*n}}{n!} + \ldots \tag{6.0.1}$$

where the series on the right certainly converges in the Δ-adic topology of §4 to an element of Γ^*. Clearly $X^* = \exp x^*$ is a unit in Γ^*, and

$$\exp(\alpha x^*) \exp(\beta x^*) = \exp(\alpha + \beta)x^* \tag{6.0.2}$$

for all $\alpha, \beta \in \Phi$. We note that if $\exp x^* = 1$, then $x^* = 0$, for $(\exp x^*) - 1 = x^* u = 0$, where

$$u = 1 + \frac{x^*}{2!} + \frac{x^{*2}}{3!} + \ldots$$

is a unit in Γ^*.

Similarly, if $y^* \in \Delta^*$ we may define

$$\log(1 + y^*) = y^* - \tfrac{1}{2}y^{*2} + \tfrac{1}{3}y^{*3} - \tfrac{1}{4}y^{*4} + \ldots, \tag{6.0.3}$$

where again the series on the right converges to an element of Δ^*. It is clear that $\exp \log (1 + y^*) = 1 + y^*$ and $\log \exp x^* = x^*$. In general, of course, exponentials and logarithms will not be defined for all elements of Γ^*, since for example the existence of $\exp(\alpha + x^*)$ would imply the existence of

$\exp\alpha$ in Φ. In particular, however, $\log G$ is defined for all elements $G \in \mathfrak{G}$, and we have

(6.0.4)
$$g = \log G = (G-1) - \tfrac{1}{2}(G-1)^2 + \ldots,$$
$$G = \exp g.$$

Now with Δ^* we may associate the Lie algebra $\Lambda^* = (\Delta^*)_l$ in the usual fashion by defining the binary operation of commutation in $(\Delta^*)_l$ by means of

$$x^* \circ y^* = x^*y^* - y^*x^*,$$

for all $x^*, y^* \in \Delta^*$. Clearly Λ^* is of infinite rank over Φ. Let Θ^* be an ideal of Δ^*, and let $\mathrm{M}^* = (\Theta^*)_l$; then M^* is an ideal of the Lie algebra Λ^*. In particular we have

(6.0.5)
$$\Lambda^* = (\Delta^*)_l \supset (\Delta^{*2})_l \supset (\Delta^{*3})_l \supset \ldots.$$

Let us define the "lower central series" of Λ^* by setting $\Lambda^* = \Lambda^*{}_1$, and $\Lambda^*{}_{k+1} = \Lambda^*{}_k \circ \Lambda^*$, where $\Lambda^*{}_k \circ \Lambda^*$ is the ideal spanned by all elements of the form $l^*{}_k \circ l^*$ with $l^*{}_k \in \Lambda^*{}_k$ and $l^* \in \Lambda^*$. Then certainly

$$\overset{*}{\Lambda}_w \subseteq (\Delta^{*w})_l, \qquad w = 1, 2, \ldots,$$

so that

(6.0.6)
$$\overset{*}{\Lambda} = \overset{*}{\Lambda}_1 \supset \overset{*}{\Lambda}_2 \supset \ldots \supset \overset{*}{\Lambda}_w \supset \overset{*}{\Lambda}_{w+1} \supset \ldots,$$

and the only element belonging to $\Lambda^*{}_w$ for all w is zero. Hence Λ^* is "generalized nilpotent" in the usual sense. We note also

Lemma 6.1. *If $l^*{}_k \in \Lambda^*{}_k$ $(k = 1, 2, \ldots)$, then the infinite series*

$$\overset{*}{l}_1 + \overset{*}{l}_2 + \ldots + \overset{*}{l}_k + \ldots$$

is an element of Λ^*.

Proof. Since $l^*{}_k \in \Lambda^*{}_k \subseteq (\Delta^{*k})_l$, $l^*{}_k$, considered as an element of Δ^*, belongs to Δ^{*k}, so that the series in (6.1) converges to an element in Δ^* and therefore is an element of $(\Delta^*)_l = \Lambda^*$.

Now as we have seen in §4, if $X = 1 + x^*$, $Y = 1 + y^*$, where $x^*, y^* \in \Delta^*$, then

$$XY = 1 + x^* + y^* + x^*y^* = 1 + z^*,$$
$$X^{-1} = 1 - x^* + x^{*2} - x^{*3} + \ldots = 1 + \bar{x}^*,$$

where z^*, $\bar{x}^*$ belong to Δ^*, so that the set of all elements of the form $1 + x^*$ forms a group $\mathfrak{G}^*$ under multiplication. Indeed, $\mathfrak{G}^*$ is a normal subgroup of the unit group of Γ^*, consisting of all elements of the form $\alpha + x^*$, where $\alpha \neq 0 \in \Phi$ and $x^* \in \Delta^*$. The group $\mathfrak{G}^*$ is generalized nilpotent, for if $\mathfrak{D}^*{}_k$ is the normal subgroup of $\mathfrak{G}^*$ consisting of elements of the form $1 + x^*{}_k$, where $x^*{}_k \in \Delta^{*k}$, then

(6.1.1)
$$\overset{*}{\mathfrak{G}} = \overset{*}{\mathfrak{D}}_1 \supset \overset{*}{\mathfrak{D}}_2 \supset \overset{*}{\mathfrak{D}}_3 \supset \ldots$$

is a central series of $\mathfrak{G}^*$, and

(6.1.2)
$$\overset{*}{\mathfrak{D}}_w \supseteq \overset{*}{\mathfrak{G}}_w, \qquad w = 1, 2, \ldots,$$

where $\mathfrak{G}^*{}_w$ is the wth term of the lower central series (1.0.1) of $\mathfrak{G}^*$. Clearly, therefore, $\mathfrak{G}^*_w \neq \mathfrak{G}^*_{w+1}$ for all w, and the only element common to all the $\mathfrak{G}^*_w$ will be the unit element. In particular $\mathfrak{G}$ itself is a subgroup of $\mathfrak{G}^*$.

We recall now the well-known Campbell-Hausdorff formula **(2**; **9**; **10)** which reveals the intimate connection between the group $\mathfrak{G}^*$ and the Lie algebra Λ^*. Let $X = 1 + x^*$, $Y = 1 + y^*$ be elements of $\mathfrak{G}^*$: then by (6.0.1):

$$(6.1.3) \qquad X = \exp x, \quad Y = \exp y, \quad XY = \exp z,$$

where $x = \log (1 + x^*)$, $y = \log (1 + y^*)$ and $z = \log (1 + x^* + y^* + x^*y^*)$. Then the Campbell-Hausdorff formula gives z explicitly in terms of x and y as follows **(2**, formula 26; **9**, formula **10)**:

$$(6.1.4) \quad z = x + y + \tfrac{1}{2}(x \circ y) + \tfrac{1}{12}(x \circ y \circ y) + \tfrac{1}{12}(y \circ x \circ x) + \tfrac{1}{24}(y \circ x \circ x \circ y) + \dots,$$

where $x \circ y = xy - yx$ as usual, where we have written, for example, $x \circ y \circ y = (x \circ y) \circ y$, $y \circ x \circ x \circ y = ((y \circ x) \circ x) \circ y$, etc., and where the right side of (6.1.4) is an infinite sum of the type considered in (6.1) and therefore convergent. All the coefficients on the right are known to be rational and therefore belong to any Φ of characteristic 0.

For later use we note that, if $X^{-1}Y^{-1}XY = (X, Y) = \exp c$, then

$$(6.1.5) \qquad c = (x \circ y) + \tfrac{1}{2}(x \circ y \circ x) + \tfrac{1}{2}(x \circ y \circ y) + \dots,$$

where the right side is again an infinite sum of commutators in x and y. For convenience we introduce the notation

$$x[i_1, i_2, \dots, i_s] = x_{i_1} \circ x_{i_2} \circ \dots \circ x_{i_s}.$$

From (6.1.5) it follows that, if $X_i = \exp (x_i)$ and if $(X_1, X_2, \dots, X_n) = \exp c_n$, then

$$(6.1.6) \qquad c_n = (x_1 \circ x_2 \circ \dots \circ x_n) + \sum l_w, \qquad w = n + 1, n + 2, \dots$$

where each l_w is a rational linear combination of simple commutators of the form $x[i_1, i_2, \dots, i_w]$ with $w \geqslant n + 1$, and where $i_1, i_2, \dots, i_w$ is a permutation of the integers $1, 2, \dots, n$ with repetitions allowed, but with each of $1, 2, \dots n$ occuring at least once.

7. The Lie algebra of an N-group. Consider now the module $\mathfrak{L}$ of Λ^* spanned by all elements of the form $g = \log G$, where G runs over the N-group $\mathfrak{G}$. The principal theorem of this section is to the effect that $\mathfrak{L}$ is a Lie algebra of finite rank r over Φ, where r is the dimension of $\mathfrak{G}$. As a first step towards this result we prove:

LEMMA 7.1. *If $w > c$, the class of $\mathfrak{G}$, and if $g_i = \log G_i$, $i = 1, 2, \dots w$ where $G_1, G_2, \dots, G_w \in G$, then*

$$g_1 \circ g_2 \circ \dots \circ g_w = 0.$$

Proof. By (6.1.6) we know that, if $w > c$,

$$1 = (G_1, G_2, \dots, G_w) = \exp (g_1 \circ g_2 \circ \dots \circ g_w + \textstyle\sum l_u), \qquad u = w + 1, w + 2, \dots,$$

where l_u is a linear combination of commutators of the form $g[i_1, i_2, \ldots, i_u]$, so that

(7.1.1) $$g_1 \circ g_2 \circ \ldots \circ g_w = -\sum l_u, \qquad u = w+1, w+2, \ldots.$$

Now every element of the form $g[i_1, i_2, \ldots, i_u] \in \Delta^{*u}$, so that (7.1.1) implies that *every* commutator $g_1 \circ g_2 \circ \ldots \circ g_w \in \Delta^{*w+1}$. In particular, every $g[i_1, i_2, \ldots, i_u] \in \Delta^{*u+1}$, and again (7.1.1) implies that $g_1 \circ g_2 \circ \ldots \circ g_w \in \Delta^{*w+2}$. Continuing in this way we can show that

$$g_1 \circ g_2 \circ \ldots \circ g_w \in \Delta^{*w+N}$$

for all values of N, and therefore $g_1 \circ g_2 \circ \ldots \circ g_w = 0$, since zero is the only element common to all Δ^{w*+N}.

It follows from (7.1) that the Lie algebra *generated* by all $g = \log G$ is nilpotent of class c. We prove now

LEMMA 9.2. *Let $F_1, F_2, \ldots, F_r$ be any $\mathfrak{F}$-basis for $\mathfrak{G}$ as in* (2.2), *and let $f_i = \log F_i$ $(i, = 1, 2, \ldots, r)$. Then if $g = \log G$, where $G \in \mathfrak{G}$, there exist rational numbers $\gamma_1, \gamma_2, \ldots \gamma_r$ so that*

$$g = \gamma_1 f_1 + \gamma_2 f_2 + \ldots + \gamma_r f_r.$$

In other words, the module L spanned by the elements $g = \log G$ for all $G \in \mathfrak{G}$ is of finite rank r over Φ.

Proof. By an easy application of the Campbell-Hausdorff formula (6.1.4) we may show that

(7.2.1) $$\begin{aligned} F_1^{\alpha_1} F_2^{\alpha_2} \ldots F_r^{\alpha_r} &= \exp(\alpha_1 f_1) \exp(\alpha_2 f_2) \ldots (\exp a_r f_r) \\ &= \exp(\alpha_1 f_1 + \alpha_2 f_2 + \ldots + a_r f_r + \sum \beta_\rho c_\rho) \qquad \rho = 1, 2, \ldots, s, \end{aligned}$$

where $\alpha_1, \ldots, \alpha_r$ are integers, $\beta_1, \beta_2, \ldots \beta_s$ are rational, and $c_1, c_2, \ldots, c_s$ are commutators in $f_1, \ldots, f_r$ of the form $f[i_1, i_2, \ldots, i_t]$ with $t \leqslant c$. (Note that because of (7.1) only a finite number of commutators c_ρ will occur in (7.2.1).) Since every G may be written

$$G = F_1^{\alpha_1} \ldots F_r^{\alpha_r},$$

it will be sufficient to prove that, for all integers t,

(7.2.2) $$f_{i_1} \circ f_{i_2} \circ \ldots \circ f_{i_t} = \sum \gamma_j f_j, \qquad j = 1, 2, \ldots, r$$

where the $\gamma_1, \ldots, \gamma_r$ are rational.

As in (4.2.1) let us define the weight of f_i to be 2^i, and the weight of a commutator $f[i_1, i_2, \ldots, i_t]$ to be

$$W(t) = 2^{i_1} + 2^{i_2} + \ldots + 2^{i_t}.$$

Now because of (7.1) all commutators $f[i_1, i_2, \ldots, i_t]$ with $t > c$ vanish, and since $i_1, i_2, \ldots, i_t$ are all at most r, any commutator in the f_i of weight sufficiently great vanishes (e.g., any commutator of weight greater than $r^{2^c} = W_0$; so that W_0 is an upper bound to the weight of non-vanishing commutators, although by no means the least). Hence (7.2.2) is satisfied trivially for all commutators $f[i_1, i_2, \ldots, i_t]$ of weight $> W_0$. Assume therefore that (7.2.2) holds for all commutators of weight greater than $W(t)$. Now by (6.1.6) and (7.1) we have

$$(7.2.3) \quad (F_{i_1}, F_{i_2}, \ldots, F_{i_t}) = \exp(f_{i_1} \circ f_{i_2} \circ \ldots \circ f_{i_t} + \sum \beta'_\rho c'_\rho), \qquad \rho = 1, 2, \ldots, s',$$

where β_ρ' are rational, and each c_ρ' is a commutator of the form $f[j_1, j_2, \ldots j_u]$ of weight $W(u)$ greater than $W(t)$ since $i_1, \ldots, i_t$ are contained among $j_1, j_2, \ldots, j_u$. By our assumption, therefore, $\sum \beta_\rho' c_\rho'$ can be expressed as a rational linear combination of the $f_1, \ldots, f_r$, and we re-write (7.2.3) in the form

$$(7.2.4) \quad (F_{i_1}, F_{i_2}, \ldots, F_{i_t}) = \exp(f_{i_1} \circ f_{i_2} \circ \ldots \circ f_{i_t} + \sum \beta_j f_j), \qquad j = 1, 2, \ldots, r.$$

On the other hand, by (2.5.2) we have

$$(7.2.5) \qquad (F_{i_1}, F_{i_2}, \ldots, F_{i_t}) = F_k^{\alpha_k} F_{k+1}^{\alpha_{k+1}} \ldots F_r^{\alpha_r},$$

where $k \geqslant t - 1 + m$, $m = \max(i_1, i_2, \ldots, i_t)$. Consider any f_s with $s \geqslant t - 1 + m$; the weight of f_s is 2^s and we have, since certainly $i_1 \neq i_2$,

$$(7.2.6) \qquad W = 2^{i_1} + \ldots + 2^{i_t} < t\, 2^m \leqslant 2^{t-1} 2^m \leqslant 2^s.$$

Now (7.2.5) may be re-written, as in (7.2.1), in the form

$$(7.2.7) \qquad (F_{i_1}, F_{i_2}, \ldots, F_{i_t}) = \exp(\alpha_k f_k + \ldots + \alpha_r f_r + \sum \beta_\rho'' c_\rho'')$$

where β_ρ'' are rational and each c_ρ'' is a commutator of the form $f[k_1, k_2, \ldots, k_\tau]$ with $k_1, \ldots, k_\tau \geqslant k$, so that the weight of each c_ρ'' is greater than W by (7.2.6). By our assumption, therefore, we may express each c_ρ'' rationally in terms of $f_1, \ldots, f_r$ and (7.2.7) may be re-written

$$(7.2.8) \qquad (F_{i_1}, F_{i_2}, \ldots, F_{i_t}) = \exp(\sum \delta_j f_j), \qquad j = 1, 2, \ldots, r,$$

with rational δ_j. Equating the right-hand sides of (7.2.3) and (7.2.8), we see that (7.2.2) holds for any commutator of weight W if it holds for all commutators of weight $> W$, which proves that (7.2.2) is true in general.

Since in particular we have proved that

$$(7.2.9) \qquad f_i \circ f_j = \sum \gamma_{ijk} f_k, \qquad i, j, k = 1, 2, \ldots, r,$$

where the γ_{ijk} are rational, we may now state our main result:

THEOREM 7.3. *The elements $g = \log G$ for all $G \in \mathfrak{G}$ span a Lie algebra $\mathfrak{L}$ of rank r over Φ, where r is the dimension of $\mathfrak{G}$. A basis for $\mathfrak{L}$ may be taken as the set $f_1 = \log F_1, \ldots, f_r = \log F_r$, where $F_1, F_2, \ldots, F_r$ is any $\mathfrak{F}$-basis of $\mathfrak{G}$. The structure constants of $\mathfrak{L}$ relative to a basis of this type are rational.*

8. The Lie group associated with $\mathfrak{G}$. Suppose now that Φ is the real field. We show that $\mathfrak{G}^*$, the group of all elements of the form $1 + x^*$ with $x^* \in \Delta^*$,

https://doi.org/10.4153/CJM-1955-022-5 Published online by Cambridge University Press

now contains as a subgroup a real simply connected nilpotent Lie group $\mathfrak{A}$ whose Lie algebra is the algebra $\mathfrak{L}$ determined by $\mathfrak{G}$ as in (7.3). The N-group $\mathfrak{G}$ is a subgroup of $\mathfrak{A}$, so that in particular we establish a theorem of Malcev (**10**, theorem 6).

For any G belonging to the N-group $\mathfrak{G}$ let us define $\mathfrak{G}^\xi$ for real ξ by the equation

$$G^\xi = \exp(\xi g), \tag{8.0.1}$$

and let $\mathfrak{A}$ be the set of all such elements G^ξ. Because of (7.2) we may write

$$G^\xi = \exp(\xi_1 f_1 + \ldots + \xi_r f_r), \tag{8.0.2}$$

where $\xi_1, \ldots, \xi_r$ are real. If $G^\eta = \exp(\eta_1 f_1 + \ldots + \eta_r f_r)$ then we have $G^\xi G^\eta = G^\zeta$, where

$$G^\zeta = \exp(\zeta_1 f_1 + \ldots + \zeta_r f_r)$$

and

$$\zeta_i = p_i(\xi_1, \ldots, \xi_r;\ \eta_1, \ldots, \eta_r),$$

p_i being a polynomial in the $\xi_1, \ldots, \xi_r;\ \eta_1, \ldots, \eta_r$ determined in the usual fashion by the constants γ_{ijk} of (7.2.9), so that if we take $(\xi_1, \ldots, \xi_2)$ as the coordinates of G^ξ it is clear that $\mathfrak{A}$ is a Lie group. Indeed $(\xi_1 \ldots \xi_r)$ are canonical, and certainly the Lie algebra of $\mathfrak{A}$ is $\mathfrak{L}$. We obviously have $\mathfrak{G}$ as a discrete subgroup of $\mathfrak{A}$. Hence we have:

THEOREM 8.1. *The set of all elements* $\exp(\xi g)$, *where ξ is real and* $g = \log G$, $G \in \mathfrak{G}$, *forms under multiplication a real simply connected Lie group $\mathfrak{A}$ whose Lie algebra is the rational Lie algebra $\mathfrak{L}$ determined by $\mathfrak{G}$. In particular, therefore, every N-group $\mathfrak{G}$ is a discrete subgroup of a Lie group $\mathfrak{A}$ with rational Lie algebra.*

REFERENCES

1. P. Hall, *A contribution to the theory of groups of prime power orders*, Proc. London Math. Soc. (2), *36* (1933), 29–95.

2. F. Hausdorff, *Die symbolische Exponentialformel in der Gruppentheorie*, Sitz. der Sachsischen Akad. Wiss. (Math.-phys. Klasse), *58* (1906), 19–48.

3. K. A. Hirsch, *Infinite soluble groups* I, Proc. London Math. Soc. (2) *44* (1938), 53–60.

4. ———, II, *ibid.*, 336–345.

5. ———, III, *ibid.*, *49* (1946), 184–194.

6. S. A. Jennings, *The group ring of a p-group over a modular field*, Trans. Amer. Math. Soc., *50* (1941), 175–185.

7. W. Magnus, *Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring*, Math. Ann., *111* (1935), 259–280.

8. ———, *Ueber Beziehungen zwischen höheren Kommutatoren*, J. reine angew. Math., *177* (1937), 105–115.

9. ———, *Ueber Gruppen und zugeordnete Liesche Ringe, ibid.*, *182* (1940), 142–149.

10. A. I. Malcev, *On a class of homogeneous spaces*, Izvestiya Akad. Nauk SSSR Ser. Mat., *13* (1949) 9–32 (AMS Translation No. 39).

11. ———, *Nilpotent torsion-free groups*, *ibid.*, 201–212.

University of British Columbia