THE ALGEBRA OF DIMENSION-LINKING OPERATORS

R. H. Bruck

1. Introduction. In the course of preparing a book on group theory [1] with special reference to the Restricted Burnside Problem and allied problems I stumbled upon the concept of a dimension-linking operator. Later, when I lectured to the Third Summer Institute of the Australian Mathematical Society [2], G. E. Wall raised the question whether the dimension-linking operators could be made into a ring by introduction of a suitable definition of multiplication. The answer was easily found to be affirmative; the result was that the theory of dimension-linking operators became exceedingly simple.

My purpose in the present note is to develop the theory of dimension-linking operators in some detail. Then I shall give a brief indication (without proof) of the natural role of these operators in group theory.

2. The operators. If R is an associative ring and n is a positive integer, we shall denote by

$$R^{(n)} = R \times \ldots \times R \quad (n \text{ factors})$$

the n^{th} set-power of R.

By a dimension-linking operator, f, we mean an operator defined for every associative ring R and having the following properties:

(A) For every associative ring R and for each $n \geq 1$, f induces a single-valued mapping $f(n)$ from $R^{(n)}$ into R:

$$f(n) : (r_1, r_2, \ldots, r_n) \rightarrow f(r_1, r_2, \ldots, r_n) .$$

Moreover (where we write $r(i_t)$ instead of r_{i_t})

https://doi.org/10.4153/CMB-1965-016-4 Published online by Cambridge University Press

(2.1) $$f(r_1, \ldots, r_n) = \Sigma\, c(i_1, \ldots, i_n)\, r(i_1) \ldots r(i_n)$$

where the c's are integers independent of R and where the sum is over the $n!$ arrangements $i_1, \ldots, i_n$ of $1, \ldots, n$.

(B) For every associative ring R and for each $n \geq 2$, the mappings $f(n)$, $f(n-1)$ induced by f on $R^{(n)}$, $R^{(n-1)}$ are linked by $n-1$ commutation rules as follows:

(2.2) $$f(\ldots, r_i, r_{i+1}, \ldots) = f(\ldots, r_{i+1}, r_i, \ldots) + f(\ldots, [r_i, r_{i+1}], \ldots)$$

for $1 \leq i \leq n-1$. Here $[r, s]$ is a ring-commutator:

(2.3) $$[r, s] = rs - sr$$

for all r, s in R.

To illustrate the rule (A), we may note that, for example,

$$\begin{aligned} f(r) &= ar, \\ f(r, s) &= brs + b'sr, \\ f(r, s, t) &= crst + c'rts + dsrt + d'str + etrs + e'tsr \end{aligned}$$

for every (associative) ring R and for all r, s, t in R, where the coefficients $a, b, c, c', d, d', e, e'$ are integers depending only on f (and not upon R). The commutation rules (B) allow a "collection process". This is because, in (2.2), the first two terms concern $f(n)$ while the last concerns $f(n-1)$. For example, if $n = 2$ we have

(2.4) $$f(s, r) = f(r, s) + f([s, r]),$$

and if $n = 3$ we have

(2.5) $$\begin{aligned} f(t, r, s) &= f(r, t, s) + f([t, r], s) \\ &= f(r, s, t) + f(r, [t, s]) + f(s, [t, r]) + f([t, r, s]). \end{aligned}$$

Here we have used the standard abbreviation

$$[t, r, s] = [[t, r], s].$$

https://doi.org/10.4153/CMB-1965-016-4 Published online by Cambridge University Press

The rules (B) - and this is equally important - also allow an "unfolding process". For example,

$$f([r,s],[t,u]) = f(r,s,t,u) - f(r,s,u,t) - f(s,r,t,u) + f(s,r,u,t) .$$

When we combine (A), (B), it becomes clear that the integers $c(i_1, \ldots, i_n)$ in (2.1) must satisfy many conditions. For example, when we write out (2.4) in terms of the coefficients $a, \ldots, e'$ given above, we find that

$$brs + b'sr = bsr + b'rs + a[s,r]$$

or

$$(b-b'+a)[s,r] = 0 .$$

This suggests - what turns out to be correct - that we must have

$$b - b' + a = 0 .$$

Similarly, (2.5) gives rise to further conditions.

At this point one might wonder whether there are operators, other than the zero operator, which satisfy (A) and (B); but there is a simple example at hand, namely the operator T defined by

(2.6) $$T(r_1, r_2, \ldots, r_n) = r_1 r_2 \ldots r_n$$

for every $n \geq 1$, every associative ring R, and all $r_1, r_2, \ldots, r_n$ in R.

The condition (A) on dimension-linking operators f tells us that we may consider each such operator f as a sequence of polynomials in associative but non-commutative indeterminates. Then we may define f as an operator by substitution. For this reason we now specialize the ring R.

3. <u>The algebra of operators.</u> Let

(3.1) $$X_1, X_2, \ldots, X_n, \ldots$$

be a countably infinite sequence of associative but non-commutative indeterminates, and let $\mathcal{A}$ be the free associative algebra over the ring of integers generated by the indeterminates (3.1). In terms of $\mathcal{A}$, a dimension-linking operator f can be characterized by the following two properties, together with the usual rule of substitution:

(A') For each $n \geq 1$, $f(X_1, X_2, \ldots, X_n)$ is either zero or a homogeneous polynomial, contained in $\mathcal{A}$, having degree 1 in each of $X_1, \ldots, X_n$ and total degree n.

(B') For each $n \geq 2$, and for $1 \leq i \leq n-1$,

$$(3.2)\quad f(\ldots, X_i, X_{i+1}, \ldots) = f(\ldots, X_{i+1}, X_i, \ldots) + f(\ldots, [X_i, X_{i+1}], \ldots).$$

Next we wish to define equality, addition and multiplication of two dimension-linking operators f, g. The first two definitions are obvious:

$$(3.3)\quad f = g \Longleftrightarrow f(X_1, \ldots, X_n) = g(X_1, \ldots, X_n), \qquad n = 1, 2, 3, \ldots .$$

$$(3.4)\quad (f+g)(X_1, \ldots, X_n) = f(X_1, \ldots, X_n) + g(X_1, \ldots, X_n), \quad n = 1, 2, 3, \ldots .$$

To define multiplication we need further concepts. By a simple set, J, (of positive integers) we mean a finite non-empty sequence

$$J = \{j(1), j(2), \ldots, j(m)\}, \qquad m \geq 1,$$

of positive integers in (strict) ascending order. We denote by X_J the ordered m-tuple

$$X_J = (X_{j(1)}, \ldots, X_{j(m)}).$$

Now we define, for every ordered pair of dimension-linking operators f, g and for all $n \geq 1$,

$$(3.5)\qquad (fg)(X_1, \ldots, X_n) = \Sigma\, f(X_J)\, g(X_K)$$

https://doi.org/10.4153/CMB-1965-016-4 Published online by Cambridge University Press

where the pair J,K ranges over all ordered pairs of disjoint simple subsets which partition the set

$$\{1, 2, \ldots, n\} .$$

For example:

$$(fg)(X_1) = 0 ;$$

$$(fg)(X_1, X_2) = f(X_1)\, g(X_2) + f(X_2)\, g(X_1) ;$$

$$(fg)(X_1, X_2, X_3) = f(X_1)\, g(X_2, X_3) + f(X_2)\, g(X_1, X_3) + f(X_3)\, g(X_1, X_2)$$
$$+ f(X_1, X_2)\, g(X_3) + f(X_1, X_3)\, g(X_2) + f(X_2, X_3)\, g(X_1).$$

Now we are ready for some theorems.

THEOREM 3.1. The set, $\mathcal{D}$, of dimension-linking operators constitutes an associative algebra, $(\mathcal{D}, +, \cdot)$, over the ring of integers.

Proof. Clearly it is enough to prove that if f, g are in $\mathcal{D}$, then so is fg. Since fg certainly satisfies (A'), we may restrict attention to (B'); that is, to

$$(3.6)\quad (fg)(\ldots, X_i, X_{i+1}, \ldots) - (fg)(\ldots, X_{i+1}, X_i, \ldots) = (fg)(\ldots, [X_i, X_{i+1}], \ldots),$$

where $1 \leq i \leq n-1$. If the first term on the left of (3.6) is given by (3.5), then the second term on the left comes from (3.5) by interchanging i and i+1. The terms of the sum on the right of (3.5) may be classified according to J, K as follows:

(a) J contains i and K contains i+1 .
(a') J contains i+1 and K contains i .
(b) J contains both i and i+1 .
(c) K contains both i and i+1 .

We note that interchange of i, i+1 simply interchanges the terms of type (a) with the terms of type (a'). Hence, in computing the left-hand side of (3.6), we may ignore the terms of (3.5) of type (a) or (a'). When (b) (or (c)) occurs, i must lie directly to the left of i+1 in J (or K). Thus, in computing

https://doi.org/10.4153/CMB-1965-016-4 Published online by Cambridge University Press

the left-hand side of (3.6), a term

(3.7) $$f(X_J)\ g(X_K)$$

of (3.5) of type (b) is replaced by a term

$$f(X_{J*})\ g(X_K)\ ,$$

where X_{J*} is obtained from X_J by replacing the adjacent pair X_i, X_{i+1} by the commutator $[X_i, X_{i+1}]$. Similarly, a term (3.7) of type (c) is replaced by a term

$$f(X_J)\ g(X_{K*})\ .$$

It should now be clear that (3.6) holds, and this completes the proof of Theorem 3.1.

We repeat the definition of the operator T:

(3.8) $$T(X_1, \ldots, X_n) = X_1 \ldots X_n\ , \qquad n \geqq 1\ .$$

In view of Theorem 3.1, the positive powers, T^k, of T are also dimension-linking operators. We need the following:

LEMMA 3.2. *The polynomial*

$$T^k(X_1, \ldots, X_n)$$

is zero if $1 \leqq n < k$ *and is the elementary symmetric function in* $X_1, \ldots, X_n$ *if* $n = k$.

Proof. Since $T'(X_1) = T(X_1) = X_1$, the lemma is correct for $k = 1$. We assume inductively that the lemma is correct for some $k \geqq 1$, and we consider the operator

$$T^{k+1} = T^k T\ .$$

For any $n \geqq 1$, we have

https://doi.org/10.4153/CMB-1965-016-4 Published online by Cambridge University Press

$$(3.9) \qquad T^{k+1}(X_1, \ldots, X_n) = \Sigma\, T^k(X_J)\, T(X_K)$$

where the pair J, K range over all ordered pairs of simple sets which partition

$$\{1, 2, \ldots, n\} .$$

If $n \leqq k$, then, on the right-hand side of (3.9), since J has length at most $k-1$,

$$T^k(X_J) = 0$$

for every choice of J. Hence the left-hand side of (3.9) is zero in this case. If $n = k+1$, then, on the right-hand side of (3.9), we may drop all terms except those in which J has length k and K has length 1. But then we see easily that

$$T^{k+1}(X_1, \ldots, X_{k+1})$$

is the elementary symmetric function of $X_1, \ldots, X_{k+1}$. This proves Lemma 3.2. As some examples of Lemma 3.2,

$$T^2(X_1) = 0 ; \quad T^2(X_1, X_2) = X_1X_2 + X_2X_1 ;$$

$$T^3(X_1) = 0 ; \quad T^3(X_1, X_2) = 0 ;$$

$$T^3(X_1, X_2, X_3) = X_1X_2X_3 + X_1X_3X_2 + X_2X_1X_3 + X_2X_3X_1 + X_3X_1X_2 + X_3X_2X_1 .$$

THEOREM 3.3 (David Walkup). The algebra, $(\mathcal{D}, +, \cdot)$, of dimension-linking operators is isomorphic to the algebra of formal power-series without constant term in one indeterminate over the ring of integers. More explicitly, every element, f, of $\mathcal{D}$ has the form

$$(3.10) \qquad f = \sum_{k=1}^{\infty} c_k T^k$$

https://doi.org/10.4153/CMB-1965-016-4 Published online by Cambridge University Press

where the c_k are integers uniquely determined by f. Conversely, every operator of form (3.10), where the c_k are integers, is in $\mathcal{D}$.

Remark. Note that if f has form (3.10), then, by Lemma 3.2,

$$(3.11) \qquad f(X_1, \ldots, X_n) = \sum_{k=1}^{n} c_k T^k (X_1, \ldots, X_n), \qquad n \geqq 1$$

Proof. In view of the Remark, we need only show that if f is in $\mathcal{D}$, then f has form (3.10). We do this inductively, using (3.11) as a guide. By (A')

$$f(X_1) = a X_1$$

for some integer a. Hence (3.11) holds for n=1 provided we take $c_1 = a$. Now suppose, inductively, that (3.11) holds for some $n \geqq 1$ and for fixed integers $c_1, \ldots, c_n$. We define

$$(3.12) \qquad g = f - \sum_{k=1}^{n} c_k T^k$$

and note that g is in $\mathcal{D}$ and satisfies

$$(3.13) \qquad g(X_1, \ldots, X_n) = 0$$

for the given value of n. In view of (3.13) and the commutation rules (B'), the polynomial

$$g(X_1, \ldots, X_n, X_{n+1})$$

remains unchanged when any two adjacent X's are interchanged, and therefore when the X's are permuted arbitrarily. By this and Lemma 3.2,

$$(3.14) \qquad g(X_1, \ldots, X_{n+1}) = c_{n+1} T^{n+1} (X_1, \ldots, X_{n+1})$$

https://doi.org/10.4153/CMB-1965-016-4 Published online by Cambridge University Press

where the integer c_{n+1} is the (uniquely defined) coefficient of the monomial

$$X_1 X_2 \ldots X_{n+1}$$

in the left-hand side of (3.14). Now, by combining (3.14), (3.12), we get (3.11) with n replaced by $n+1$. This completes the inductive proof of Theorem 3.3.

Next we assign to each f in $\mathcal{D}$ a formal power-series

$$(3.15) \qquad H(f;X) = \sum_{n=1}^{\infty} \frac{s(f;n)}{n!} X^n ,$$

where $s(f;n)$ denotes the sum of the coefficients of $f(X_1, \ldots, X_n)$ and where X is an indeterminate over the field of rationals. Clearly

$$(3.16) \qquad s(f;n)X^n = f(X, \ldots, X) \qquad (n \text{ arguments } X) .$$

Hence, by the definitions of addition and multiplication in $\mathcal{D}$,

$$(3.17) \qquad H(f+g;X) = H(f;X) + H(g;X) ,$$

$$(3.18) \qquad H(fg;X) = H(f;X)\, H(g;X)$$

for all f, g in $\mathcal{D}$. Since, in particular, $H(T;n) = 1$, $n \geq 1$, we see that, by (3.18),

$$(3.19) \quad H(T^k;X) = (e^X - 1)^k = \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} e^{iX} , \qquad k \geq 1 .$$

LEMMA 3.4.

(i) (Dwight Paine) The sum, $s(T^k;n)$, of the coefficients of $T^k(X_1, \ldots, X_n)$ is equal to the number of ordered partitions of the first n natural numbers into k non-empty (unordered) subsets. Hence $s(T^k;n)$ is divisible by $k!$.

https://doi.org/10.4153/CMB-1965-016-4 Published online by Cambridge University Press

(ii) We have

$$(3.20) \qquad s(T^k;n) = \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} i^n .$$

Proof. To prove (ii) we take $f = T^k$ in (3.15) and compare the result with (3.19). To prove (i) we need only consider the form of $T^k(X_1, \ldots, X_n)$ when expressed in terms of k factors T. (Here we must generalize (3.5) to a formula for k factors.)

Finally we wish to relate dimension-linking operators to the elementary symmetric functions

$$(3.21) \qquad S_n(X_1, \ldots, X_n) .$$

The polynomial (3.21) is the sum of the $n!$ monomials

$$Y_1 Y_2 \ldots Y_n$$

in which $Y_1, Y_2, \ldots, Y_n$ are $X_1, X_2, \ldots, X_n$ in some order. In particular, S_n is not a dimension-linking operator, although (by Lemma 3.2),

$$(3.22) \quad T^n(X_1, \ldots, X_n) = S_n(X_1, \ldots, X_n) , \qquad n \geq 1 .$$

It will be convenient to use the following inductive definition of an elementary ring commutator:

(a) Each indeterminate X_i is an elementary ring commutator.

(b) If r, s are elementary ring commutators, so is $[r, s] = rs - sr$.

LEMMA 3.4. If k, n are positive integers, with $n \geq k$, and if $p(n, k)$ is the product of the factorials $t!$, $k+1 \leq t \leq n$, then

$$(3.23) \qquad p(n, k) \; T^k(X_1, \ldots, X_n)$$

https://doi.org/10.4153/CMB-1965-016-4 Published online by Cambridge University Press

is an algebraic sum of polynomials

(3.24) $$S_t(r_1, r_2, \ldots, r_t), \qquad k \leqq t \leqq n,$$

where $r_1, r_2, \ldots, r_t$ are elementary ring commutators.

Proof. By (3.22), the lemma is true with $n = k$, provided we make the convention that

$$p(k, k) = 1 .$$

As a consequence, we may derive the proof by induction on $n-k$. If $Y_1, \ldots, Y_n$ is one of the $n!$ arrangements of $X_1, \ldots, X_n$, the commutation rule allows us to write

(3.25) $$T^k(Y_1, \ldots, Y_n) = T^k(X_1, \ldots, X_n) + w(Y_1, \ldots, Y_n)$$

where $w(Y_1, \ldots, Y_n)$ is a sum of terms of form

(3.26) $$T^k(r_1, \ldots, r_{n-1})$$

in which each of the $n-1$ elements r_i is an elementary ring-commutator. If we sum (3.25) over the $n!$ arrangements, and note that the corresponding left hand side is a symmetric function of $X_1, \ldots, X_n$, we get

(3.27) $$s(T^k, n)\, S_n(X_1, \ldots, X_n) = n!\; T^k(X_1, \ldots, X_n) + w ,$$

where $s(T^k, n)$ is given by (3.20) and w is a sum of terms (3.26). The result now comes by multiplying (3.27) by $p(n-1, k)$ and applying the lemma for the case $n-1, k$. This proves Lemma 3.4.

If we note that, for $t \geqq k$, the elementary symmetric function S_t can be expressed in terms of the elementary symmetric function S_k, we may rephrase Lemma 3.4 as follows:

THEOREM 3.5. To each pair of positive integers k, n with $n \geq k$ there corresponds a (least) positive integer $b(n, k)$ such that

$$(3.28) \qquad b(n, k)\, T^k(X_1, \ldots, X_n)$$

may be expressed in terms of the elementary symmetric function S_k as an algebraic sum of terms of form

$$(3.29) \qquad MS_k(r_1, r_2, \ldots, r_k)$$

where $r_1, r_2, \ldots, r_k$ are elementary ring-commutators and where either $M = 1$ or M is a non-empty monomial. Moreover, the prime factors of $b(n, k)$ are divisors of $n!$.

We could, indeed, give Theorem 3.5 a sharper form in terms of the concepts of basic ring-commutator and basic product. But we shall ignore these concepts in the present note.

4. Two connections with group theory. Let P be the algebra of all formal power series in the (associative but non-commutative) indeterminates (3.1) with integer coefficients. We wish P to have the integer 1 as identity element. Hence the elements of P are formal power series

$$(4.1) \qquad c(0) + \Sigma\, c(M)M$$

where the components (or coefficients) c are integers and where M ranges over all (non-empty) monomials

$$(4.2) \qquad M = Y_1 Y_2 \ldots Y_n\,, \qquad n \geq 1\,,$$

with the Y's chosen from the indeterminates (3.1). Equality and addition are componentwise. Multiplication is defined as for ordinary power series - except that we must remember that multiplication of monomials is associative but non-commutative.

It is easy to see that an element (4.1) of P has a multiplicative inverse in P precisely when $c(0) = 1$ or -1. In particular, the elements

https://doi.org/10.4153/CMB-1965-016-4 Published online by Cambridge University Press

$$(4.3) \qquad 1 + X_i, \qquad i = 1, 2, \ldots,$$

generate a multiplicative group F which turns out to be a free group with the generators (4.2) as a free set of generators.

There are many cases - though it would take too long to give a proper theory in this note - where a group-theoretic problem can be rephrased as a problem concerning the free group F or the algebra P relative to an ideal of P. We shall be content to sketch two cases where a study of ideals of P defined by dimension-linking operators is appropriate. What we shall omit to establish is the exact connection between the properties of the ideals and the appropriate group-theoretical property.

We will begin with the simpler case. (This is discussed in great detail in [2].) Let k be a fixed positive integer and let

$$(4.4) \qquad J(k)$$

be the smallest ideal of P containing all elements of P of form

$$(4.5) \qquad (x-1)^k, \qquad x \in F.$$

In the study of the k^{th} Engel condition in groups it is appropriate to ask whether there exist positive integers n and b such that

$$(4.6) \qquad b X_1 X_2 \ldots X_n \equiv 0 \quad \mod J(k).$$

When (4.6) is true for some n, b, it remains true when the X_i are replaced by arbitrary elements (4.1) with $c(0) = 0$. Consequently, (4.6) is a type of nilpotency condition for the ring P. Moreover, if (4.6) is true for some n, b there will exist a least positive integer n(k) and a least positive integer b(k) such that (4.6) is true for all $n \geqq n(k)$ and for every integral multiple, b, of b(k).

As a first step, we need to know more about J(k). First let n be an arbitrary positive integer and set

$$(4.7) \qquad \epsilon = \epsilon(1)\, \epsilon(2) \ldots \epsilon(n)$$

where each $\epsilon(i)$ is either 1 or -1. The element

(4.8) $$x = (1+X_1)^{\epsilon(1)} (1+X_2)^{\epsilon(2)} \dots (1+X_n)^{\epsilon(n)}$$

is in F, and so is every element obtained by replacing one or more of the X_i by 0. Consequently, if we compute (4.5) with x given by (4.8), express the result as a formal power series, and delete all monomial terms except those in which each of $X_1, \dots, X_n$ occurs at least once, the result must be in J(k). This tells us (once we have thought our way through the necessary calculations) that J(k) contains all elements of form

(4.9) $$\epsilon T^k(X_1, \dots, X_n) + \epsilon F_{k,n}(X_1, \dots, X_n)$$

where T^k is the dimension-linking operator discussed in section 3 and where

(4.10) $$F_{k,n}(X_1, \dots, X_n) = F_{k,n}(\epsilon_1, \dots, \epsilon_n; X_1, \dots, X_n)$$

is a definite formal power series (4.1) in which the coefficient c(M) of a monomial M is zero unless M is a monomial of degree at least one in each of $X_1, \dots, X_n$ and of total degree at least n+1. By contrast, the first term,

$$\epsilon T^k(X_1, \dots, X_n),$$

is the leading homogeneous part of (4.9), being a polynomial of degree 1 in each of $X_1, \dots, X_n$ and of total degree n.

It is, moreover, quite easy to see that J(k) is the smallest ideal of P containing all elements of form

$$T^k(Y_1, Y_2, \dots, Y_n) + F_{k,n}(\epsilon_1, \dots, \epsilon_n; Y_1, \dots, Y_n)$$

where n is a positive integer and the Y's are chosen from the indeterminates (3.1).

As a simplification, it is convenient to introduce an ideal

https://doi.org/10.4153/CMB-1965-016-4 Published online by Cambridge University Press

(4.11) $$P^*$$

defined as follows: P^* is the set of all formal power series (4.1) in which $c(0) = 0$ and $c(M) = 0$ except possibly when M contains an indeterminate more than once. Then the enlarged ideal

(4.12) $$J(k) + P^*$$

is the smallest ideal containing P^* and all polynomials

$$T^k(Y_1, \ldots, Y_n)$$

where n is a positive integer and $Y_1, \ldots, Y_n$ are distinct indeterminates chosen from (3.1).

It turns out that the easier problem in which (4.6) is replaced by

(4.13) $$b X_1 X_2 \ldots X_n \equiv 0 \quad \mathrm{mod}\ J(k) + P^*$$

not only has great group-theoretical importance in its own right but is extremely difficult for $k > 2$. We shall say a little more about this in the next section.

Finally, let us deal briefly with the Burnside Problem. This concerns a positive integer N and all groups G subject to the identical relation

(4.14) $$x^N = 1 .$$

The original Burnside Problem for exponent N asks whether all finitely generated groups subject to (4.14) are finite. The Restricted Burnside Problem for exponent N and r generators (r being a positive integer) asks whether among the finite groups on r generators satisfying (4.14) there is one of maximal order.

In the study of the Burnside problems for exponent N it is appropriate to consider the ideal

(4.15) $$B(N)$$

https://doi.org/10.4153/CMB-1965-016-4 Published online by Cambridge University Press

of P defined as follows: B(N) is the smallest ideal of P containing all elements of form

$$(4.16) \qquad x^N - 1 , \qquad x \in F .$$

Just as before, we are led to study the ideal $P^* + B(N)$. Here the role of T^k is taken over by the dimension-linking operator

$$(4.17) \qquad f_N = \sum_{k=1}^{N} \binom{N}{k} T^k .$$

The fact that f_N is a dimension-linking operator can be used to explain the known connection between the Restricted Burnside Problem and the theory of Lie rings.

5. Permutation ideals. As in section 3, let $\mathfrak{A}$ be the free associative algebra over the integers, generated by the countably infinite set of indeterminates (3.1). Let k be a fixed positive integer. By the permutation ideal,

$$(5.1) \qquad I(k) ,$$

of T^k we mean the smallest ideal of $\mathfrak{A}$ containing all polynomials of form

$$T^k(Y_1, Y_2, \ldots, Y_n) , \qquad n \geq 1 ,$$

where $Y_1, Y_2, \ldots, Y_n$ are chosen from the indeterminates (3.1). In addition, we define

$$(5.2) \qquad n(k) , \quad a(k)$$

as follows: If there exists a positive integer n such that

$$(5.3) \qquad a X_1 X_2 \ldots X_n \equiv 0 \quad \bmod I(k)$$

for at least one positive integer a, then n(k) is the least such positive integer n. Otherwise, $n(k) = \infty$. If $n(k) < \infty$, then a(k) is the least positive integer a such that (5.3) holds with $n = n(k)$. If $n(k) = \infty$, then $a(k) = \infty$.

https://doi.org/10.4153/CMB-1965-016-4 Published online by Cambridge University Press

Relatively little is known at present about $n(k)$, $a(k)$, although these numbers are precisely what we need to know in connection with the problem (4.13). We would, indeed, be happy to have an upper bound for $n(k)$ (proving that $n(k)$ is finite) and as much information as possible about the prime factors of $a(k)$. It is easy to prove the following:

(5.4) <u>If</u> $n(k) < \infty$, <u>then</u> $k!$ <u>divides</u> $a(k)$.

Indeed, (5.4) is a direct consequence of Lemma 3.2 (i). We also know the following:

(5.5) $$n(1) = 1 = a(1),$$

(5.6) $$n(2) = 2 = a(2),$$

(5.7) $$n(3) = 8 \text{ or } 9.$$

(5.8) The prime divisors of $a(3)$ are 2, 3 and (possibly) 5.

Here, (5.5) is trivial, and (5.6) can be deduced from (5.4) and the identity

(5.9) $$2X_1X_2X_3 = T^2(X_1, X_2, X_3) - X_2T^2(X_1, X_3) - T^2(X_1, X_3)X_2.$$

The proof of (5.7), (5.8) is very much deeper; in particular, there is very little hope of proving (5.7) by explicit formulas comparable to (5.9). Indeed, (5.7), (5.8) were proved by David Walkup in his Ph. D. thesis (University of Wisconsin, August 1963) by a skillful combination of the classical theory of representations of the symmetric group, the theory of Lie rings, and the theory of polynomial identical relations.

I would conjecture that $n(k)$ is finite for every $k \geq 1$ and also that the prime divisors of $a(k)$ are the prime divisors of $k!$

The connection between the problem of the finiteness of $n(k)$ and the theory of representations of the symmetric group may be given as follows: Consider some fixed positive integer n and form the vector space V over the field of rationals with a basis consisting of the $n!$ monomials obtained from the monomial

https://doi.org/10.4153/CMB-1965-016-4 Published online by Cambridge University Press

$$X_1 X_2 \ldots X_n$$

by permuting the subscripts. Then V provides the regular representation (over the field of rationals) of the symmetric group on $1, 2, \ldots, n$. On the other hand, V has a subspace, V_o, spanned by all polynomials of form

$$MS_k(r_1, r_2, \ldots, r_k)$$

which are homogeneous of degree 1 in each of $X_1, \ldots, X_n$ and in which M is a monomial (possibly the empty monomial 1) and the r_i are elementary ring-commutators. The subspace V_o also provides a representation of the symmetric group on $1, 2, \ldots, n$. Hence we will have $V_o = V$ precisely when V_o yields each irreducible representation of the symmetric group on $1, 2, \ldots, n$ as often as the degree of the representation. On the other hand, as should be clear from Theorem 3.5 and the definition of $I(k)$, it is true that $n(k)$ is the least integer n such that $V = V_o$ (if such an n exists).

By exploiting the connection between $n(k)$ and the properties of the elementary symmetric function, one may deduce from a result of Graham Higman [3] that

$$n(k) > k^2 e^{-2} \tag{5.10}$$

for all sufficiently large k.

We shall conclude with a specific application to group theory. First we need some definitions. If π is a set of primes, an element, x, of the group G is said to be a <u>π-element</u> provided x has finite order n and each prime divisor of n is in π. If y, x are group elements, we define

$$(y, x) = y^{-1} x^{-1} y x .$$

Furthermore, if i is a non-negative integer, we define

$$(y, x; 0) = y , \qquad (y, x; i+1) = ((y, x; i), x) .$$

https://doi.org/10.4153/CMB-1965-016-4 Published online by Cambridge University Press

THEOREM 5.1. Let k be a positive integer such that n(k) is finite. Then there exists a finite set π of primes with the following property: Let G be any group containing an Abelian normal subgroup A such that (i) A has no π-elements and (ii) the identity

$$(5.11) \qquad (a, x; k) = 1$$

holds for all a in A and x in G. Then A is contained in the $n(k)^{th}$ term of the ascending central series of G. Here the set π must contain every prime divisor of a(k) but need not contain any additional primes greater than

$$(5.12) \qquad (k-1)(k-[k/2]) .$$

In (5.12), [x] denotes the "greatest integer in x". The proof of Theorem 5.1 is given in detail in [2]. For the case k = 2, since n(2) = a(2) = 2, we may take $\pi = \{2\}$. For k=3, we know that n(3) = 8 or 9 and that the prime divisors of a(3) are 2, 3 and (possibly) 5. Here we may take $\pi = \{2, 3, 5\}$. An earlier result of Heineken [4] for k=3 used $\pi = \{2, 3, 5, 7\}$ together with the estimate

$$n(3) \leqq 3^9 .$$

In a sequel he improved this estimate to

$$n(3) \leqq 3^5 .$$

In [2], several distinct but equivalent definitions of n(k) are given. One of these is the following: n(k) is the least positive integer (if one exists) such that a conclusion of the type in Theorem 5.1 holds for all groups G. Other definitions concern groups imbedded in associative rings and nilpotency properties of Lie rings.

REFERENCES

1. R.H. Bruck, What Makes a Group Finite? A book being written under contract with Prentice-Hall.

https://doi.org/10.4153/CMB-1965-016-4 Published online by Cambridge University Press

2. R. H. Bruck, Engel conditions in groups and related questions. Mimeographed notes based on a series of 11 lectures delivered (during Jan. 8 - Jan. 22, 1963) to the Third Summer Research Institute of the Australian Mathematical Society, meeting Jan. 8 - Feb. 15, 1963 in Canberra A. C. T.

3. Graham Higman, On a conjecture of Nagata, Proc. Cambridge Phil. Soc. 52 (1956), 1-4.

4. Hermann Heineken, Endomorphismenringe und engelsche Elemente, Archiv der Math. 13 (1962), 29-37.

University of Wisconsin
Madison, Wisconsin

https://doi.org/10.4153/CMB-1965-016-4 Published online by Cambridge University Press