1985

Commutator Identities Obtained by the Magnus Algebra

Anthony M. Gaglione
United States Naval Academy

Dennis Spellman
Sacred Heart University

HOUSTON JOURNAL OF MATHEMATICS, Volume 11, No. 4, 1985.

COMMUTATOR IDENTITIES OBTAINED BY THE MAGNUS ALGEBRA

Anthony M. Gaglione* and Dennis Spellman

I. Introduction. In this paper, two related commutator identities are established through the use of the Magnus Algebra (the algebra of noncommutative formal power series with integral coefficients). These identities are connected with identities of P. Hall (Theorem 12.3.1 of [1] and Theorem 3.1 and 3.2 of [2]) and of R. R. Struik (equation (56) of [4] and Theorem 1 of [5]). They involve basic commutators. The basic commutators derived from the generators of a free group are implicit in the work of P. Hall [2] and have been studied extensively by many others: e.g., see M. Hall, Jr. [1], M. A. Ward [7], H. V. Waldinger and A. M. Gaglione [5,6].

This work arose as the result of research on the lower central series of a free product of cyclic groups [6]. Identity (2.6) of Theorem 2.2 (one of the main results) is very useful in computations involving the factor groups of the lower central series of such free products (see Section 4 of [6]). Moreover, the identities established here should be of interest in themselves and be important for solving other group theoretical problems.

The identities of [1, 2, 4] were obtained through the "collection process" of P. Hall and required complicated existence and precedence conditions. (See Theorem 3.1 of [2], Theorem 12.3.1 of [1] and Lemma 4 of [4].) Here we proceed through the use of the Magnus Algebra and thus avoid these complicated conditions but require instead elementary properties of binomial coefficients.

In order to proceed with our proofs, we give a discussion of the requisite group theoretical foundations from the commutator calculus in the next section. Furthermore, we also give a preliminary discussion of the Magnus Algebra in Section II. As a reference for all properties of the Magnus Algebra, see Chapter 5 of [3].

Finally the authors would like to thank H. V. Waldinger for his encouragement

*The research of this author was supported by a grant from the Naval Academy Research Council.

while preparing this paper, for reading the manuscript and making helpful criticisms.

II. Preliminaries on the commutator calculus.

II(a). Group theoretical foundations. We start by giving some notation and definitions used throughout this paper. Let Z be the set of integers, Z_+ be the set of positive integers and Z_{0+} be the set of nonnegative integers. Let F be the free group of rank r $(1 < r < \infty)$, i.e.,

(2.1) $F = \langle c_1, c_2, \ldots, c_r \rangle.$

If $x, y \in F$ then the commutator

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

The lower central series of F is an infinite sequence of subgroups

$$F = F_1 \supseteq F_2 \supseteq \cdots \supseteq F_n \supseteq F_{n+1} \supseteq \cdots$$

defined by setting $F_{n+1} = (F_n, F)$, i.e., the group generated by all commutators of the form (x_n, y) with $x_n \in F_n$ and $y \in F$. Also the left-normed commutator $(\ldots((a_1,a_2),a_3),\ldots,a_n)$ will often be abbreviated as $(a_1,a_2,\ldots,a_n)$.

We now construct and order the basic commutators. This is done by induction.

DEFINITION 2.1. The basic commutators of weight one are the free generators in some fixed but arbitrary order. Having defined and ordered basic commutators of weight less than n $(n \in Z_+)$, we use these to get the ones of weight n. The basic commutators of weight n are commutators of the form

$$c_k = (c_i, c_j)$$

where c_i and c_j are basic commutators with weights $W(c_i)$ and $W(c_j)$ respectively, such that (i) $n = W(c_i) + W(c_j)$, (ii) $c_i > c_j$, and (iii) if $c_i = (c_s, c_t)$, then $c_j \geqslant c_t$. Basic commutators of the same weight are put in a fixed but arbitrary order. Moreover, a basic commutator of weight n is greater than any of weight less than n.

We shall assume that the subscripts for the basic commutators are chosen so that c_i is the i-th basic commutator in their ordering. It can be shown that a basic commutator of weight n is in F_n but not in F_{n+1}. Moreover since the intersection of all terms of the lower central series of F is the identity, i.e., F is residually nilpotent (see [3]), for any nontrivial element $g \in F$ there exists a $n \in Z_+$ with $g \in F_n$ but $g \notin F_{n+1}$. We call n the weight, W(g), of g.

Furthermore, we use the following subscript notation. Let $n \in Z_+$ and $c_1, c_2, \ldots, c_{q(n)}$ be the basic commutators of weight less than or equal to n in their assigned order, i.e., q(n) is the number of basic commutators of weight less than or equal to n in F. The name basic commutator is appropriate in the sense of the following theorem [1]:

THEOREM 2.1. *Let* $n \in Z_+$. *An arbitrary* $g \in F$ *has a unique representation*

$$(2.3)\quad g \equiv \Pi_{i=1}^{q(n)} c_i^{\epsilon_i} \bmod F_{n+1}.$$

Moreover, the basic commutators of weight n *form a basis for the free Abelian group* F_n/F_{n+1}.

II(b). Statement of the commutator identities. We are now ready to state our identities.

THEOREM 2.2. *Let*

$$(2.4)\quad c = c_j = (f_1, f_2, \ldots, f_s)$$

be a left-normed basic commutator such that each f_i $(1 \leqslant i \leqslant s)$ *is a generator and each generator* c_i $(1 \leqslant i \leqslant r)$ *in the presentation* (2.1) *of* F *occurs at least once among* $f_1, f_2, \ldots, f_s$. *(Note that if every generator does not occur among the* f_i*'s, then we can consider a free group,* F, *of smaller rank.) Let* $\alpha \in Z_+$ *and* p *be a fixed positive prime. Let* $n \in Z_+$ *be such that* $n > s$. *For a fixed* $k \in Z_+$ *with* $1 < k \leqslant s$, *let*

$$(2.5)\quad c_\lambda = (f_1, f_2, \ldots, f_{k-1}, \underbrace{f_k, f_k, \ldots f_k}_{\text{p-times}}, f_{k+1}, \ldots f_s).$$

Then

$$(2.6a)\quad C = (f_1, f_2, \ldots f_{k-1}, f_k^{p^\alpha}, f_{k+1}, \ldots, f_s)$$

$$(2.6b)\quad \equiv c_j^{p^\alpha} (\Pi_{i=q(s)+1}^{q(n)} c_i^{\phi_i p^{\beta_i}}) \bmod F_{n+1}$$

where

(i) $\phi_i \in Z$,

(ii) $\beta_i = \alpha$ *for* $s < W(c_i) \leqslant s + p - 1$ *and* $i \neq \lambda$,

(iii) $\phi_\lambda p^{\beta_\lambda} \equiv p^{\alpha - 1} \bmod p^\alpha$,

(iv) $\beta_i = \alpha - 1$ *for* $s + p \leqslant W(c_i) < s + p^2 - 1$,

(v) $\beta_i = \alpha - m$ *for* $s + p^m \leqslant W(c_i) + 1 < s + p^{m+1}$ *and* $2 \leqslant m < \alpha$,

(vi) $\beta_i = 0$ *for* $s + p^\alpha - 1 \leqslant W(c_i)$.

THEOREM 2.3. *Let* F, p *and* α *be as in Theorem* 2.2. *Let* $n \in Z_+$. *Then*

$$(2.7)\quad P = (c_1 c_2 \cdots c_r)^{p^\alpha} \equiv \Pi_{j=1}^{q(n)} c_j^{\phi_j p^{\beta_j}} \bmod F_{n+1}$$

where

(i) $\phi_j \in Z$,

(ii) $\phi_j = 1$ *for* $1 \leqslant j \leqslant r$,

(iii) $\beta_j = \alpha - m$ *for* $p^m \leqslant W(c_j) < p^{m+1}$ *and* $0 \leqslant m < \alpha$,

(iv) $\beta_j = 0$ *for* $p^\alpha \leqslant W(c_j)$.

We note that (2.6) becomes an identity of R. R. Struik [4, 5] for $\alpha = 1$, $s = 2$ and $n = p + 1$. Also (2.7) becomes an identity of P. Hall (Theorem 3.2 of [2]) in a special case. Moreover by reason of Lemma 2.1, which occurs in the next subsection, (2.7) is implied by Theorem 12.3.1 of [1].

II(c). Preliminaries on the Magnus Algebra. Corresponding to the free group F in (2.1), we introduce the free associative algebra A (called A(Z,r) in [3]) having the free generators $x_1, x_2, \ldots, x_r$. Here A is the algebra of noncommutative formal power series in $x_1, x_2, \ldots, x_r$ with coefficients in Z. Then F is embedded in A by means of the substitutions

(2.8a) $c_i = 1 + x_i$,

(2.8b) $c_i^{-1} = 1 - x_i + x_i^2 - x_i^3 + \cdots$

for i = 1,2,...r. If $a \in F$, then the substitutions (2.8) yield

$$(2.9)\quad a = 1 + \Sigma_{n=1}^{\infty} X_n(a) = 1 + \sigma(a)$$

uniquely, where $X_n(a)$ is the homogeneous component of degree n of the representation of a in A. Moreover, our representation of F given by equations (2.8) is known to conform to Theorems 2.4, 2.5 and 2.6 below.

THEOREM 2.4. *Let* $a \in F$ *have weight* $W(a) = n \in Z_+$. *Then* $W(a) = 1$ *if and only if* $X_1(a) \neq 0$. *Moreover,* $W(a) = n > 1$ *if and only if* (i) $X_n(a) \neq 0$ *and* $X_k(a) = 0$ *for* $k < n$. (If $W(a) = n$, then we will also denote $X_n(a)$ by $\delta(a)$ just as in Definition 5.6 of [3].)

THEOREM 2.5. *Suppose* $a \in F$, $W(a) = 1$ *and*

$$a \equiv \Pi_{i=1}^{r} c_i^{\epsilon_i} \bmod F_2.$$

Then

(2.10) $\delta(a) = \Sigma_{i=1}^{r} \epsilon_i x_i.$

Next if $c = (a,b) \in F$ *such that* $c \neq 1$ *and* $W(c) = W(a) + W(b)$, *then*

(2.11) $\delta(c) = \delta(a)\delta(b) - \delta(b)\delta(a)$

i.e., $\delta(c) = [\delta(a),\delta(b)]$, *the ring commutator of* $\delta(a)$ *and* $\delta(b)$. *Moreover for* $a = 1 + x$, $b = 1 + y$ *with* $x,y \in A$,

(2.12) $c = 1 + \Sigma_{n=0}^{\infty} \Sigma_{s=0}^{n} (-1)^n x^s y^{n-s} [x,y].$

(cf. with equation (7a) on page 314 of [3].)

Before we state Theorem 2.6, we introduce some more notation and we also give one definition. Let c_k be the k-th basic commutator in the ordering of Definition 2.1. We denote $\delta(c_k)$ by z_k and we call it the k-th basic Lie element.

DEFINITION 2.2. Let $\eta_1,\eta_2,\ldots,\eta_m \in Z$ and $\epsilon_1,\epsilon_2,\ldots,\epsilon_f \in Z_+$. Any sum

(2.13) $\Sigma_{j=1}^{m} \eta_j z_j$

is said to be a Lie element. A product of the form

(2.14) $\Pi_{j=1}^{f} z_{k_j}^{\epsilon_j}$,

where (i) $f \in Z_+$ and (ii) $k_1 < k_2 < \cdots < k_f$ if $f > 1$, is said to be a basic product. If $c_{q(d-1)+1}, c_{q(d-1)+2}, \ldots, c_{q(d)}$ are the basic commutators of weight d (note $q(0) = 0$), then the Lie element

(2.15) $\Sigma_{j=q(d-1)+1}^{q(d)} \eta_j z_j$

is siad to be a homogeneous Lie element of degree d.

THEOREM 2.6. *The basic Lie elements form a basis for the Lie elements of* A_o. *(Here* A_o *is the subalgebra of* A *which consists of all linear sums of finitely many monomials.) The basic products together with* 1 *form a basis for all the elements of* A_o. *If* $a \in F$ *and* $W(a) = d$, *then* $\delta(a)$ *is a unique homogeneous Lie element of degree* d. *Moreover if* $\delta(a)$ *is the sum* (2.15), *then*

(2.16) $a \equiv \Pi_{j=q(d-1)+1}^{q(d)} c_j^{\eta_j} \bmod F_{d+1}.$

We will prove our identities by the use of the binomial theorem. For this purpose, we require

REMARK 2.1. The binomial theorem is used as follows: let $a \in F$. Then

(2.17) $a^m = (1 + \sigma(a))^m = \Sigma_{j=0}^{\infty}\binom{m}{j}(\sigma(a))^j$

where $m \in Z$, $\binom{m}{j} = m(m-1)(m-2)\cdots(m-j+1)/j!$ if $j > 0$, $(\sigma(a))^o = 1$ and $\binom{m}{o} = 1$. We observe that if $m \in Z_+$ the sum (2.17) is finite and reduces to the "ordinary terminating binomial expansion" since $j > m$ yields a factor of $(m - m) = 0$ in the numerator of $\binom{m}{j}$. Of course, $\sigma(a)$ itself might be a formal infinite sum.

In addition to the notation introduced in (2.9), we also require

CONVENTION 2.1. For $n \in Z_+$, the Magnus symbol Σ_n shall represent any element of the Magnus Algebra A which contains no term of degree less than n. The possibility that $\Sigma_n = 0$ shall not be excluded. We also denote by X_m either zero or any homogeneous polynomial of degree m in the generators $x_1,x_2,\ldots,x_r$ of A. Our principal use of the X_m will be to denote the homogeneous component of degree m in Σ_n whenever $m \geqslant n$. The reader should be clear that the Magnus symbols Σ_n as well as the symbols X_m are used analogously to the Landau symbols and may represent different quantities within the same context.

For example, suppose that

(2.18) $a = 1 + (x_1 + x_2) \in A.$

Then

(2.19) $a^2 = 1 + 2\,\sigma(a) + (\sigma(a))^2$

where $\sigma(a) = x_1 + x_2$. Calculating further, we obtain

(2.20) $a^2 = 1 + 2(x_1 + x_2) + (x_1^2 + x_1x_2 + x_2x_1 + x_2^2).$

We may write variously as we prefer

(2.21) $a^2 = 1 + \Sigma_1$

(2.22) $a^2 = 1 + \Sigma_1 + \Sigma_2$

or

(2.23) $a^2 = 1 + 2\Sigma_1 + \Sigma_2$

where $\Sigma_1 = X_1 + X_2 = 2(x_1 + x_2) + (x_1^2 + x_1x_2 + x_2x_1 + x_2^2)$ in (2.21);

$\Sigma_1 = X_1 = 2(x_1 + x_2)$ or $\Sigma_1 = 2X_1 = 2(x_1 + x_2)$ and $\Sigma_2 = X_2 = x_1^2 + x_1x_2 + x_2x_1 + x_2^2$ in (2.22); and $\Sigma_1 = X_1 = x_1 + x_2$ and $\Sigma_2 = X_2 = x_1^2 + x_1x_2 + x_2x_1 + x_2^2$ in (2.23).

Our proofs of the commutator identities (2.6) and (2.7) rest on known properties of binomial coefficients here stated as

LEMMA 2.1. *For* $n \in Z_+$, *let* $e(n)$ *be the largest exponent* t *such that* $n \equiv 0 \bmod p^t$. *Let* $\alpha, j \in Z_+$ *and* $j \leqslant p^\alpha$ *(*p *is a fixed positive prime). Then*

(2.24) $e\binom{p^\alpha}{j} = \alpha - e(j)$.

Moreover,

(2.25) $\binom{p^\alpha}{p} \equiv p^{\alpha-1} \bmod p^\alpha$.

PROOF. We note that

(2.26) $\binom{p^\alpha}{j} = \dfrac{p^\alpha(p^\alpha-1)\cdots(p^\alpha-(j-1))}{j!} = \dfrac{Np^\alpha}{j}$

where $N = 1$ for $j = 1$ but $N = \binom{p^\alpha - 1}{j - 1}$ for $1 < j \leqslant p^\alpha$. Hence $N \in Z_+$ and $N \not\equiv 0 \bmod p$. Thus (2.26) implies (2.24). Finally, we find (2.25) by computing N for $j = p$.

For the proof of identity (2.6), we also require Lemma2.2 which follows from an easy induction on k.

LEMMA 2.2. *Let* $x,y \in A$. *Put* $y_0 = y$ *and* $y_{k+1} = [y_k, x]$ *for* $k \in Z_{0+}$. *Then*

(2.27) $y_k = \Sigma_{j=0}^k (-1)^j \binom{k}{j} x^j y x^{k-j}$.

III. **Proof of the identities.** Let $n,d \in Z_+$ and $a \in F$ have $W(a) = d$. Suppose that $d \leqslant n$. We wish to express a uniquely in the form

(3.1) $a \equiv \Pi_{i=1}^{q(n)} c_i^{\epsilon_i} \bmod F_{n+1}$

according to Theorem 2.1. For this purpose, we describe a procedure here called the n-representation computation of a. (Note if $d > 1$, then $\epsilon_1 = \epsilon_2 = \cdots = \epsilon_{q(d-1)} = 0$.)

DEFINITION 3.1. The elementary d-representation computation of a determines the exponents $\epsilon_{q(d-1)+1}, \epsilon_{q(d-1)+2}, \ldots, \epsilon_{q(d)}$ occuring in (3.1) in two steps as follows: (i) $X_d(a)$ is found by the substitutions (2.8). (Note that $X_h(a) = 0$ for $1 \leqslant h < d$ by Theorem 2.4.) (ii) We express every monomial in $X_d(a)$ and thus $X_d(a)$ itself as a sum of basic products, according to Theorem 2.6. Since $X_d(a) = \delta(a)$ is a homogeneous Lie element of degree d, by the same theorem, all the basic products in this representation of $X_d(a)$ which are not basic Lie elements have coefficients equal to 0. Thus the sum for $X_d(a)$ has the form (2.15) so that a has the form (2.16). This gives the required ϵ_i.

Continuing with our definition, let $a_1 = a$. For $n > d$, let

$$a_\nu = (\Pi_{i=q(d-1)+1}^{q(d+\nu-2)} c_i^{\epsilon_i})^{-1} a_1$$

where $\nu = 2,3,\ldots,(n-d+1)$. The n-representation computation of a finds $\epsilon_{q(d-1)+1}, \epsilon_{q(d-1)+2}, \ldots, \epsilon_{q(n)}$ by first carrying out the elementary d-representation computation of a_1, then the elementary $(d+1)$-representation computation of a_2, etc., finally carrying out the elementary n-representation computation of a_{n-d+1}. This completes Definition 3.1.

To obtain identities (2.6) and (2.7) by the computations of Definition 3.1, we first express C and P (see (2.6a) and (2.7)) through the substitutions (2.8). For this purpose, let us first suppose that the generator, f_k, in (2.5) is $1 + x_i$ from the substitutions (2.8). Using the binomial theorem (Remark 2.1), the notation of Convention 2.1 and Lemma 2.1, we find that

$$(3.2)\quad \begin{cases} f_k^{p^\alpha} = \Sigma_{j=0}\binom{p^\alpha}{j} x_i^j \\ \quad = 1 + p^\alpha \Sigma_1 + p^{\alpha-1} x_i^p + p^{\alpha-1} \Sigma_{p+1} \\ \quad + p^{\alpha-2} \Sigma_{p^2} + \cdots + p \Sigma_{p^{\alpha-1}} + \Sigma_{p^\alpha} \end{cases}$$

where we may take

$$(3.3)\quad \Sigma_1 = \Sigma_{j=1}^{p-1} \frac{1}{p^\alpha}\binom{p^\alpha}{j} x_i^j + \frac{1}{p^\alpha}[\binom{p^\alpha}{p} - p^{\alpha-1}] x_i^p,$$

$$(3.4)\quad \Sigma_{p+1} = \Sigma_{j=p+1}^{p^2-1} \frac{1}{p^{\alpha-1}}\binom{p^\alpha}{j} x_i^j,$$

$$(3.5)\quad \Sigma_{p^2} = \Sigma_{j=p^2}^{p^3-1} \frac{1}{p^{\alpha-2}}\binom{p^\alpha}{j} x_i^j,$$

$\ldots,$

$$(3.6)\quad \Sigma_{p^{\alpha-1}} = \Sigma_{j=p^{\alpha-1}}^{p^\alpha-1} \frac{1}{p}\binom{p^\alpha}{j} x_i^j,$$

and $\Sigma_{p^\alpha} = x_i^{p^\alpha}$. Note that (2.25) was used in writing the second term on the right hand side of (3.3). Moreover, an easy induction on $s = W(c)$ together with Theorem 2.5 and equation (3.2) shows that

(3.7) $\delta(C) = p^{\alpha}\delta(c)$

where C and c are as in (2.6a) and (2.4), respectively.

To facilitate the rest of our computation, put $c' = (f_1, f_2, \ldots, f_{k-1})$. Then Theorem 2.4 implies that

(3.8) $c' = 1 + \Sigma_{k-1}$.

We observe that for each fixed $x \in A$, the "derivation"

(3.9) $A \xrightarrow{D_x} A$

defined by

(3.10) $D_x(u) = [x,u] = xu - ux$

for all $u \in A$ is an endomorphism of A as a Z-module. Letting $x = \Sigma_{k-1}$,

$$y = f_k^{p^\alpha} - 1 = p^\alpha \Sigma_1 + p^{\alpha-1} x_i^p + p^{\alpha-1}\Sigma_{p+1} + \cdots + \Sigma_{p^\alpha}$$

and

$$z = \Sigma_{n=1}^{\infty} \Sigma_{s=0}^{n} (-1)^n x^s y^{n-s},$$

we have by virtue of equations (2.12), (3.2) and (3.8) the following:

$$\begin{aligned}
(3.11)\quad (c', f_k^{p^\alpha}) &= (1 + x, 1 + y) = 1 + (1 + z)[x,y] \\
&= 1 + (1 + z)D_x(y) \\
&= 1 + (1 + z)D_x(p^\alpha\Sigma_1 + p^{\alpha-1}x_i^p + p^{\alpha-1}\Sigma_{p+1} + \cdots + \Sigma_{p^\alpha}) \\
&= 1 + (1 + z)(p^\alpha D_x(\Sigma_1) + p^{\alpha-1}D_x(x_i^p) + p^{\alpha-1}D_x(\Sigma_{p+1}) \\
&\quad + p^{\alpha-2}D_x(\Sigma_{p^2}) + \cdots + pD_x(\Sigma_{p^{\alpha-1}}) + D_x(\Sigma_{p^\alpha})) \\
&= 1 + (1 + z)(p^\alpha[\Sigma_{k-1}, \Sigma_1] + p^{\alpha-1}(\Sigma_{k-1}x_i^p - x_i^p\Sigma_{k-1}) \\
&\quad + p^{\alpha-1}[\Sigma_{k-1}, \Sigma_{p+1}] + p^{\alpha-2}[\Sigma_{k-1}, \Sigma_{p^2}] + \cdots \\
&\quad + p[\Sigma_{k-1}, \Sigma_{p^{\alpha-1}}] + [\Sigma_{k-1}, \Sigma_{p^\alpha}])
\end{aligned}$$

$$= 1 + (1+z)(p^{\alpha}\Sigma_k + p^{\alpha-1}(\Sigma_{k-1}x_i^p - x_i^p\Sigma_{k-1})$$

$$+ p^{\alpha-1}\Sigma_{k+p} + p^{\alpha-2}\Sigma_{k+p^2-1} + \cdots + p\,\Sigma_{k+p^{\alpha-1}-1} + \Sigma_{k+p^{\alpha}-1})$$

$$= 1 + p^{\alpha}(1+z)\Sigma_k + p^{\alpha-1}(1+z)\Sigma_{k-1}x_i^p - p^{\alpha-1}(1+z)x_i^p\Sigma_{k-1}$$

$$+ p^{\alpha-1}(1+z)\Sigma_{k+p} + \cdots + (1+z)\Sigma_{k+p^{\alpha}-1}.$$

Absorbing the $(1 + z)$ factor into the Magnus symbols, we have

$$(3.12)\quad (c',f_k^{p^{\alpha}}) = 1 + p^{\alpha}\Sigma_k + p^{\alpha-1}\Sigma_{k-1}x_i^p - p^{\alpha-1}(x_i^p\Sigma_{k-1} + zx_i^p\Sigma_{k-1})$$

$$+ p^{\alpha-1}\Sigma_{k+p} + \cdots + \Sigma_{k+p^{\alpha}-1}.$$

But the term $p^{\alpha-1}z\,x_i^p\Sigma_{k-1}$ is absorbed into $p^{\alpha-1}\Sigma_{k+p}$ if z has terms of positive degree in the free generators of the ring A_0 whose completion is A; otherwise $p^{\alpha-1}z\,x_i^p\Sigma_{k-1}$ is absorbed into $p^{\alpha-1}x_i^p\Sigma_{k-1}$. Hence in either event,

$$(3.13)\quad \begin{cases} (c',f_k^{p^{\alpha}}) = 1 + p^{\alpha}\Sigma_k + p^{\alpha-1}(\Sigma_{k-1}x_i^p - x_i^p\Sigma_{k-1}) \\ \qquad + p^{\alpha-1}\Sigma_{k+p} + p^{\alpha-2}\Sigma_{k+p^2-1} + \cdots + p\Sigma_{k+p^{\alpha-1}-1} + \Sigma_{k+p^{\alpha}-1}. \end{cases}$$

Furthermore, Theorem 2.5 and Lemma 2.2 imply that

$$(3.14)\quad \delta(c',\underbrace{f_k,\ldots,f_k}_{p\text{-times}}) = \Sigma_{j=0}^{p}(-1)^j\binom{p}{j}x_i^jX_{k-1}(c')x_i^{p-j}$$

where $X_{k-1}(c') = \delta(c') = \delta(1 + \Sigma_{k-1})$ and here Σ_{k-1} is as in (3.8) (also see equation (2.9) and Convention 2.1). In lieu of Lemma 2.1 together with the observation that p does not divide the $\binom{p}{j}$ in (3.14) precisely for $j = 0$ and $j = p$, we conclude from equation (3.14) that

$$(3.15)\quad \delta(c',\underbrace{f_k,\ldots,f_k}_{p\text{-times}}) = X_{k-1}(c')x_i^p - x_i^pX_{k-1}(c') + pX_{k+p-1}$$

where X_{k+p-1} is a homogeneous polynomial of degree k+p-1. We claim that (3.15) holds for $p = 2$ just as well as for odd primes p. This is seen as follows: for $p = 2$, equation (3.15) becomes $\delta(c',f_k,f_k) = X_{k-1}(c')x_i^2 + x_i^2X_{k-1}(c') + 2X_{k+1}$. But $x_i^2X_{k-1}(c') = -x_i^2X_{k-1}(c') + 2x_i^2X_{k-1}(c')$ and so the term $2x_i^2X_{k-1}(c')$ can be absorbed into $2\ X_{k+1}$. This gives $\delta(c', f_k, f_k) = X_{k-1}(c')x_i^2 - x_i^2 X_{k-1}(c') + 2\ X_{k+1}$ which shows that (3.15) does indeed hold for $p = 2$.

Now to go from $(c', f_k^{p^\alpha})$ in (3.13) to C in (2.6a), we must commute $(c', f_k^{p^\alpha})$ with $f_{k+1}, f_{k+2}, \ldots, f_s$. Thus calling $f_{k+1} = 1 + x_t$, Theorem 2.5 applied as in the computation (3.8) - (3.13), used to obtain equation (3.13), yields

$$(3.16)\quad \begin{cases} (c', f_k^{p^\alpha}, f_{k+1}) = 1 + p^\alpha \Sigma_{k+1} + p^{\alpha-1}(\Sigma_{k-1}x_i^p - x_i^p\Sigma_{k-1})x_t \\ \qquad - p^{\alpha-1}x_t(\Sigma_{k-1}x_i^p - x_i^p\Sigma_{k-1}) + p^{\alpha-1}\Sigma_{k+1+p} \\ \qquad + p^{\alpha-2}\Sigma_{k+1+p^2-1} + \cdots + p\Sigma_{k+1+p^{\alpha-1}-1} + \Sigma_{k+1+p^\alpha-1}. \end{cases}$$

But

$$(3.17)\quad p^{\alpha-1}((\Sigma_{k-1}x_i^p - x_i^p\Sigma_{k-1})x_t - x_t(\Sigma_{k-1}x_i^p - x_i^p\Sigma_{k-1}))$$
$$= p^{\alpha-1}(\Sigma_{k+p} - x_i^p\Sigma_k - \Sigma_k x_i^p).$$

Putting $-\Sigma_k x_i^p = \Sigma_k x_i^p - 2\ \Sigma_k x_i^p$ and letting the term $-2\ \Sigma_k x_i^p$ get absorbed into Σ_{k+p} the second line of (3.17) becomes

$$p^{\alpha-1}(\Sigma_{k+p} + \Sigma_k x_i^p - x_i^p\Sigma_k).$$

Substituting this into (3.16) yields

$$(c', f_k^{p^\alpha}, f_{k+1}) = 1 + p^\alpha\Sigma_{k+1} + p^{\alpha-1}(\Sigma_k x_i^p - x_i^p\Sigma_k)$$
$$+ p^{\alpha-1}\Sigma_{k+p} + p^{\alpha-2}\Sigma_{k+1+p^2-1} + \cdots + \Sigma_{k+1+p^\alpha-1}.$$

Continuing in this way and repeatedly applying Theorem 2.5, we get

$$(3.18)\quad \begin{cases} C = 1 + p^\alpha\Sigma_s + p^{\alpha-1}(\Sigma_{s-1}x_i^p - x_i^p\Sigma_{s-1}) + p^{\alpha-1}\Sigma_{s-1+p} \\ \quad + p^{\alpha-2}\Sigma_{s+p^2-1} + \cdots + p\Sigma_{s+p^{\alpha-1}-1} + \Sigma_{s+p^\alpha-1}. \end{cases}$$

Next to go from $(c', f_k, \ldots, f_k)$ in (3.15) to c_λ in (2.5), we must also commute with $f_{k+1}, f_{k+2}, \ldots, f_s$. Applying Theorem 2.5 repeatedly and proceeding in a manner exactly analogous to that of equations (3.16) - (3.18), we have that

$$(3.19)\quad \delta(c_\lambda) = X_{s-1}x_i^p - x_i^p X_{s-1} + X_{s+p-1}) + p\ X_{s+p-1}$$

where the leading term of $(\Sigma_{s-1}x_i^p - x_i^p\ \Sigma_{s-1} + \Sigma_{s+p-1})$ in (3.18) is precisely the homogeneous polynomial $(X_{s-1}x_i^p - x_i^p X_{s-1} + X_{s+p-1})$ in (3.19). This follows because the computation involved in going from (3.13) to (3.18) and (3.15) to (3.19), i.e., commuting with $f_{k+1},\dots,f_s$ does exactly the same thing to the leading term of $\Sigma_{k-1}x_i^p - x_i^p\Sigma_{k-1}$ in (3.13), which is $X_{k-1}(c')x_i^p - x_i^pX_{k-1}(c')$ in (3.15), in both expressions.

Finally, substituting (3.19) into (3.18) and also using (3.7) yields

$$(3.20)\quad \begin{cases} C = 1 + p^\alpha\delta(c) + p^\alpha\Sigma_{s+1} + p^{\alpha-1}\delta(c_\lambda) + p^{\alpha-1}\Sigma_{s+p} \\ \quad + p^{\alpha-2}\Sigma_{s+p^2-1} + \cdots + p\Sigma_{s+p^{\alpha-1}-1} + \Sigma_{s+p^\alpha-1}. \end{cases}$$

We now consider $P = (c_1c_2 \cdots c_r)^{p^\alpha}$. Evidently, the substitutions (2.8) yield

$$\Pi_{j=1}^r c_j = \Pi_{j=1}^r(1 + x_j) = 1 + \Sigma_{j=1}^r\delta(c_j) + \Sigma_2.$$

Putting $\Sigma_1 = \Sigma_{j=1}^r\delta(c_j) + \Sigma_2$ in accordance with Convention 2.1 and using Remark 2.1 yields

$$P = (1 + \Sigma_1)^{p^\alpha} = \Sigma_{j=0}^{\infty}\binom{p^\alpha}{j}(\Sigma_1)^j.$$

So that Convention 2.1 and Lemma 2.1 imply that

$$(3.21)\quad \begin{cases} P = 1 + p^\alpha\Sigma_{j=1}^r\delta(c_j) + p^\alpha\Sigma_2 + p^{\alpha-1}\Sigma_p \\ \quad + p^{\alpha-2}\Sigma_{p^2} + \cdots + p\Sigma_{p^{\alpha-1}} + \Sigma_{p^\alpha}. \end{cases}$$

Making use of Definition 3.1, let us carry out the n-representation computation of C as given by (3.20) and the n-representation computation of P as given by (3.21). We note that since $X_s(C) = p^\alpha\delta(c) = p^\alpha\delta(c_j) = p^\alpha z_j$ (see equations (2.9) and (2.4)), the elementary s-representation computation of C gives $\epsilon_j = p^\alpha(q(s-1) + 1 \leqslant j \leqslant q(s))$ but $\epsilon_i = 0$ for $q(s-1) + 1 \leqslant i \leqslant q(s)$ and $i \neq j$. According to Definition 3.1, we let $C_1 = C$ and put $C_2 = (c_j^{\epsilon_j})^{-1}C_1$. Now Theorem 2.4 implies that

$$c = c_j = 1 + \Sigma_s = 1 + \delta(c_j) + \Sigma_{s+1}.$$

Thus Remark 2.1 gives

$$(3.22)\quad c_j^{p^\alpha} = \Sigma_{i=0}^{\infty}\binom{p^\alpha}{i}(\Sigma_s)^i.$$

So that when we multiply C by $(c_j^{\epsilon_j})^{-1}$, we cancel the term $p^\alpha\delta(c)$ in (3.20) but we do not change the divisibility properties of any of the terms of higher degree in (3.20) – this follows from Lemma 2.1 applied to (3.22), i.e., the divisibility properties of the coefficients of (3.22). Thus we get

$$C_2 = 1 + p^{\alpha}\Sigma_{s+1} + p^{\alpha-1}\delta(c_\lambda) + p^{\alpha-1}\Sigma_{s+p}$$

$$+ p^{\alpha-2}\Sigma_{s+p^2-1} + \cdots + p\,\Sigma_{s+p^{\alpha-1}-1} + \Sigma_{s+p^{\alpha}-1}.$$

Moreover, at every stage of the n-representation computation of C, the same thing happens. In particular we cancel the leading term but do not disturb the divisibility properties of any of the terms of higher degree in (3.20). This means that we can see the divisibility properties of the exponents found by the n-representation computation by just reading them from (3.20). In summary, we find the following

$$(3.23)\quad C_\nu = \begin{cases} 1 + p^{\alpha-m}X_{s+\nu-1} + \Sigma_{s+\nu} \text{ for} \\ p^m \leqslant \nu < p^{m+1},\ \nu \neq p \text{ and } 0 \leqslant m < \alpha; \\ 1 + p^{\alpha-1}\delta(c_\lambda) + p^{\alpha}X_{s+p-1} + \Sigma_{s+p} \\ \text{for } \nu = p; \\ 1 + \Sigma_{s+\nu-1} \text{ for } \nu \geqslant p^{\alpha}, \end{cases}$$

for $\nu = 2,3,\ldots,n - s + 1$.

Proceeding in the same manner with the n-representation computation of P as given by (3.21), we find that

$$(3.24)\quad P_\nu = \begin{cases} 1 + p^{\alpha-m}X_\nu + \Sigma_{\nu+1} \text{ for} \\ p^m \leqslant \nu < p^{m+1} \text{ and } 0 \leqslant m < \alpha; \\ 1 + \Sigma_\nu \text{ for } \nu \geqslant p^{\alpha}, \end{cases}$$

for $\nu = 2,3,\ldots,n$.

It is evident that (3.23) and (3.24) yield the required identities (2.6) and (2.7), respectively by virtue of Definition 3.1 and Theorem 2.6.

REFERENCES

1. M. Hall, Jr., *The Theory of Groups,* Macmillan, New York, 1959.
2. P. Hall, *A contribution to the theory of groups of prime power order,* Proc. London Math. Soc., 36(1934), 29-95.
3. W. Magnus, A. Karass, and D. Solitar, *Combinatorial Group Theory: Presentation of Grouns in Terms of Generators and Relations,* Pure and Appl. Math., 13, Interscience, New York, 1966.
4. R. R. Struik, *On nilpotent products of cyclic groups, II,* Canad. J. Math., 13(1961), 557-568.

5. H. V. Waldinger, *Two theorems in the commutator calculus,* Trans. Amer. Math. Soc., 167(1972), 389-397.
6. H. V. Waldinger and A. M. Gaglione, *On nilpotent products of cyclic groups – reexamined by the commutator calculus,* Canad. J. Math., 27(1975), 1185-1210.
7. M. A. Ward, *Basic commutators,* Phil. Trans. Royal Soc. London Ser. A., 264(1969), 343-412.

U. S. Naval Academy
Annapolis, Maryland 21402

Sacred Heart University
Bridgeport, Connecticut 06606

Received November 2, 1981
Revised Version Received September 9, 1984