ON THE NILPOTENCY CLASS OF A GROUP OF EXPONENT FOUR

C. R. B. WRIGHT

Introduction. If G is a multiplicative group with elements $x, y, \cdots$, we define the commutator (x, y) by $(x, y) = x^{-1}y^{-1}xy$ and, inductively for length n, $(x_1, \cdots, x_{n-1}, x_n) = ((x_1, \cdots, x_{n-1}), x_n)$. We also use the notation $(x, \cdots, y; \cdots; z, \cdots, w)$ for the commutator $((x, \cdots, y), \cdots, (z, \cdots, w))$. For each positive integer n, let G_n be the subgroup of G generated by all commutators of length n.

A group, G, is of exponent 4 in case $x^4 = 1$ for every x in G but $y^2 \neq 1$ for some y in G. Let F be a free group of rank k, and let F^4 be the subgroup generated by fourth powers of elements of F. Let $B(k) = F/F^4$. Then $B(k)$ is clearly a group of exponent 4 on k generators. Moreover, every group of exponent 4 on k generators is a homomorphic image of $B(k)$.

I. N. Sanov has shown that $B(k)$ is finite. (See [2], pp. 324–325, or [3]). Unfortunately, his proof gives very little additional information about $B(k)$. The present paper is devoted to the study of relations between commutators in the group $B(k)$, a consequence of the relations obtained being that $B(k)_{3k} = 1$.

Preliminaries. Let G be a group of exponent 4, and let $a, b, \cdots$ be elements of G. Then

$$(a, b)^2 \equiv (a, b, b, b)(a, b, b, a)(a, b, a, a) \bmod G_4 \tag{1}$$

$$(a, b, a)^2 = (a, b, a, a, a) = (a, b, a; a, b) \tag{2}$$

$$(a, b, c) \equiv (b, c, a)(c, a, b) \bmod G_4 \tag{3}$$

$$(a, b; c, d) \equiv (a, c; b, d)(a, d; b, c) \bmod G_5 \tag{4}$$

$$(\boldsymbol{a}, b; \boldsymbol{c}, d; f) \equiv (\boldsymbol{a}, d; \boldsymbol{c}, f; b)(\boldsymbol{a}, f; \boldsymbol{c}, b; d) \bmod G_6 \tag{5}$$

where the bold-face type in (5) has no significance other than to point out which entries are left fixed while the others are cyclicly permuted—whenever bold-face type appears in a computation an application of (5) is about to be made. The relations (1) and (2) can be shown to hold in $B(2)$; hence they certainly hold in any group, G, of exponent 4. Relation (3) is simply the Jacobi identity (which holds in any group) adapted to exponent 4. Relations (4) and (5) were proved in [4] for the case in which the entries are of order 2, but the proofs clearly go through without this restriction, since in proving the relations we are simply

Received April 25, 1960. This work was supported by the Office of Naval Research under contract MR 044-213.

looking at the first significant terms of $(abcd)^4$ and $(abcdf)^4$ as collected by P. Hall's process. It should be noted that these relations are "identical" in the sense that they hold for every choice of a, b, c, d and f in G. This property gives us the freedom of substitution which we shall use later.

The following result, which appeared in a slightly different form as the Corollary to Lemma 3.2 in [4], is easily proved using (1) and (3).

(A). *Let G be a group of exponent* 4. *Let*

$$C = (x_1, \cdots, x_i, a, x_{i+1}, \cdots, x_{n-1})$$

where $x_1, \cdots, x_{n-1}$ and a are in G. Then, modulo G_{n+1}, C is a product of commutators of the form $(a, y_1, \cdots, y_i, x_{i+1}, \cdots, x_{n-1})$, where $y_1, \cdots, y_i$ are $x_1, \cdots, x_i$ in some order.

Finally, we need to know that if a and b are the generators of $B(2)$, then $B(2)_5$ is generated by $(b, a, a; b, a)$ and $(b, a, b; b, a)$, and $B(2)_6 = 1$. These results may be verified directly or deduced from Burnside's original work in [1].

Throughout this paper we shall be concerned with the relations between commutators in $B(k)$. Our first lemma gives us a method of reducing our problems to a few relatively tractable cases.

LEMMA 1. *Suppose $(x_1, \cdots, x_n)$ is a commutator of length n in a group, G, of exponent* 4. *If one of $x_3, \cdots, x_n$ is a and one b, then, modulo G_{n+1}, $(x_1, \cdots, x_n)$ is a product of commutators of length n of the following four types*:

(i) $(x, y, \cdots, a, b, \cdots)$

(ii) $(x, y, \cdots, b, a, \cdots)$

(iii) $(x, y, \cdots, a, z, b)$

(iv) $(x, y, \cdots, b, z, a)$.

Loosely stated, Lemma 1 says that we may bring a and b more or less together and keep them out of the first two positions.

Proof of Lemma 1. Observe first that we can rewrite (3) as

$$(a, b, c) \equiv (a, c, b)(a; b, c) \bmod G_4 .$$

Using this form and working modulo G_7 we have

$$\begin{aligned}(x, y, a, z, b, w) &\equiv (x, y, a, b, z, w)(\boldsymbol{x}, \boldsymbol{y}, a; \boldsymbol{b}, z; w)\\ &\equiv (x, y, a, b, z, w)(x, y, z; b, w; a)(x, y, w; b, a; z)\\ &\equiv (x, y, a, b, z, w)(x, y, z, b, w, a)(x, y, z, w, b, a)\\ &\qquad \cdot(x, y, w, b, a, z)(x, y, w, a, b, z) .\end{aligned}$$

Let $G(n, a, b)$ be the (normal) subgroup of G generated by G_{n+1} and all commutators of length n of types (i) and (ii). Let $G^*(n, a, b)$ be the (normal) subgroup of G generated by $G(n, a, b)$ and all commutators of length n of types (iii) and (iv). Then certainly if w is in $G(n, a, b)$ and g is in G, (w, g) is in $G(n+1, a, b)$, and by the relation just proved, if z is in $G^*(n, a, b)$, then (z, g) is in $G^*(n+1, a, b)$. Thus it will be sufficient to prove the lemma under the assumption that x_n is either a or b (say b).

We have reduced the problem to showing that if C has length n and if $C = (x_1, x_2, \cdots, x_i, a, \cdots, b)$, then C is in $G^*(n, a, b)$. If $2 \leqq n - i \leqq 3$, then C is in $G^*(n, a, b)$. We proceed by induction on $n - i$. Suppose for induction that for some $j \geqq 4$ and all $n \geqq j + 2$, C is in $G^*(n, a, b)$ whenever $n - i < j$. We shall show that if $n - i = j$, then C is in $G^*(n, a, b)$, so that by finite induction we shall have C in $G^*(n, a, b)$ for all i such that $2 \leqq n - i \leqq n - 2$, i.e., such that $2 \leqq i \leqq n - 2$. Thus the lemma will be proved.

Let $i = n - j$. By the inductive assumption and (3) we have, modulo $G^*(n, a, b)$,

$$(x_1, x_2, \cdots, x_i, a, \cdots, x_{n-3}, x_{n-2}, b) \equiv (X, x_i; A, x_{n-3}; x_{n-2}; b) ,$$

where $X = (x_1, \cdots, x_i)$, and where $A = (a, \cdots, x_{n-4})$ if $n - 4 > i$ but $A = a$ if $n - 4 = i$. Now, modulo G_{n+1}, using (4), (3) and (5),

$$\begin{aligned}(X, x_i; A, x_{n-3}; x_{n-2}; b) &\equiv (X, x_{n-3}; A, x_i; x_{n-2}; b)(x_i, x_{n-3}; A, X; x_{n-2}; b)\\ &\equiv (X, x_{n-3}, x_{n-2}; A, x_i; b)(\boldsymbol{A}, \boldsymbol{x}_i, x_{n-2}; X, \boldsymbol{x}_{n-3}; b)\\ &\qquad \cdot(\boldsymbol{A}, \boldsymbol{X}, x_{n-2}; x_i, \boldsymbol{x}_{n-3}; b)(\boldsymbol{A}, X; \boldsymbol{x}_i, \boldsymbol{x}_{n-3}, x_{n-2}; b)\\ &\equiv (X, x_{n-3}, x_{n-2}; A, x_i; b)(A, x_i, X; b, x_{n-3}; x_{n-2})(A, x_i, b; x_{n-2}, x_{n-3}; X)\\ &\qquad \cdot(A, X, x_i; b, x_{n-3}; x_{n-2})(A, X, b; x_{n-2}, x_{n-3}; x_i)\\ &\qquad \cdot(A, x_{n-2}; x_i, x_{n-3}, b; X)(A, b; x_i, x_{n-3}, X; x_{n-2}) .\end{aligned}$$

But by the inductive assumption $(X, x_{n-3}, x_{n-2}; A, x_i; b)$, $(A, x_i, b; x_{n-2}, x_{n-3}; X)$, $(x_i, x_{n-3}, b; A, x_{n-2}; X)$ and $(A, b; x_{n-3}, x_i, X; x_{n-2})$ are all in $G^*(n, a, b)$. Further,

$$\begin{aligned}&(A, x_i, X; b, x_{n-3}; x_{n-2})(A, X, x_i; b, x_{n-3}; x_{n-2})\\ &\qquad\qquad \equiv (X, x_i, A; b, x_{n-3}; x_{n-2}) \bmod G_{n+1} .\end{aligned}$$

Thus, modulo $G^*(n, a, b)$,

$$\begin{aligned}&(X, x_i; A, x_{n-3}; x_{n-2}; b)\\ &\qquad \equiv (\boldsymbol{X}, \boldsymbol{x}_i, A; \boldsymbol{b}, x_{n-3}; x_{n-2})(A, X, b; x_{n-2}, x_{n-3}; x_i)\\ &\qquad \equiv (X, x_i, x_{n-3}; b, x_{n-2}; A)(X, x_i, x_{n-2}; b, A; x_{n-3})\\ &\qquad\quad \cdot(A, X; x_{n-2}, x_{n-3}, b; x_i)(x_{n-2}, x_{n-3}; A, X; b; x_i)\end{aligned}$$

$$\begin{aligned}
&\equiv (\boldsymbol{A}, X; \boldsymbol{x}_{n-2}, \boldsymbol{x}_{n-3}, b; x_i)(\boldsymbol{x}_{n-2}, x_{n-3}; \boldsymbol{A}, X; b; x_i)\\
&\equiv (A, b; x_{n-2}, x_{n-3}, x_i; X)(A, x_i; x_{n-2}, x_{n-3}, X; b)\\
&\qquad \cdot(x_{n-2}, X; A, b; x_{n-3}; x_i)(x_{n-2}, b; A, x_{n-3}; X; x_i)\\
&\equiv (x_{n-2}, b; A, x_{n-3}; X; x_i)\\
&\equiv (\boldsymbol{x}_{n-2}, b; \boldsymbol{A}, x_{n-3}; x_i; X)(\boldsymbol{x}_{n-2}, b; A, \boldsymbol{x}_{n-3}; X, x_i)\\
&\equiv (x_{n-2}, x_{n-3}; A, x_i; b; X)(x_{n-2}, x_i; A, b; x_{n-3}; X)\\
&\qquad \cdot(x_{n-2}, A; X, x_i, x_{n-3}; b)(X, x_i, x_{n-2}; b, x_{n-3}; A)\\
&\equiv 1 .
\end{aligned}$$

Hence, $(x_1, x_2, \cdots, x_i, a, \cdots, x_{n-3}, x_{n-2}, b)$ is in $G^*(n, a, b)$, as desired. Thus the lemma is proved.

An immediate consequence of Lemma 1 is the following.

COROLLARY. *If $C = (x_1, \cdots, x_n)$ and if two of $x_3, \cdots, x_n$ are a, then modulo G_{n+1}, C is a product of commutators of length n of the forms:*

(i) $(x, y, \cdots, a, a, \cdots)$

(ii) $(x, y, \cdots, a, z, a)$.

We next observe that, using (1),

$$\begin{aligned}
(x_1, \cdots, x_m, a^2) &= (x_1, \cdots, x_m, a)^2(x_1, \cdots, x_m, a, a)\\
&\equiv (x_1, \cdots, x_m, a, a) \bmod G_{m+3} .
\end{aligned}$$

Hence,

$$(6) \qquad (x_1, \cdots, x_i, a, a, x_{i+1}, \cdots, x_n) \equiv (x_1, \cdots, x_i, a^2, x_{i+1}, \cdots, x_n)$$

modulo G_{n+3}.

We may now prove the following useful result.

LEMMA 2. *Let G be a group of exponent 4, and let $(x_1, \cdots, x_n)$ be a commutator of length n in elements of G. If some three of $x_3, \cdots, x_n$ are a, then modulo G_{n+1}, $(x_1, \cdots, x_n)$ is a product of commutators of the forms:*

(i) $(y_1, y_2, \cdots, y_{n-3}, a, a, a)$

(ii) $(y_1, y_2, \cdots, y_{n-4}, a, a, y_{n-3}, a)$.

Proof. We first derive two shifting relations. Using (1) and (3) we obtain modulo G_7,

$$\begin{aligned}
(x, y, a, a, a, z) \equiv ((x, y, a)^2, z) \equiv (x, y, a, z)^2 &\equiv (x, y; a, z)^2(x, y, z, a)^2\\
&\equiv (x, y, z, a)^2 \equiv (x, y, z, a, a, a) .
\end{aligned}$$

Hence,

$$(7) \qquad (x, y, a, a, a, z) \equiv (x, y, z, a, a, a) \bmod G_7 .$$

Thus, modulo longer commutators, a string of three a's can be shifted to the right.

We also have, modulo G_7,

$$(x, y, a, a, z, a) \equiv (x, y, a, z, a, a)\cdot(x, y, \boldsymbol{a}; z, \boldsymbol{a}; a) \equiv (x, y, a, z, a, a) .$$

Thus

$$(8) \qquad (x, y, a, z, a, a) \equiv (x, y, a, a, z, a) \bmod G_7 .$$

Further, modulo G_8,

$$\begin{aligned}(x, y, a, a, z, a, w) &\equiv (x, y, a, a, a, z, w)(x, y, a, a; a, z; w)\\ &\equiv (x, y, a, a, a, z, w)(\boldsymbol{x}, \boldsymbol{y}, a^2; \boldsymbol{a}, z; w)\\ &\equiv (x, y, a, a, a, z, w)(x, y, z; a, w; a^2)\\ &\equiv (x, y, a, a, a, z, w)(x, y, z, a, w, a, a)(x, y, z, w, a, a, a) .\end{aligned}$$

Applying (7) and (8) we get

$$(9) \qquad (x, y, a, a, z, a, w) \equiv (x, y, z, a, a, w, a) \bmod G_8 .$$

Thus, modulo longer commutators, a trio of a's with one gap may be shifted to the right.

It is clear from (7) and (9) that it is sufficient to prove the lemma under the assumption that $x_n = a$. Considering $(x_1, \cdots, x_{n-1})$ now, it is clear from the Corollary of Lemma 1 that we may restrict ourselves to the consideration of commutators of the following two types:

I $(x_1, x_2, \cdots, a, a, \cdots, x_{n-1}, a)$

II $(x_1, x_2, \cdots, a, x_{n-1}, a, a)$.

By (8), commutators of type II are already of type (ii), Further,

$$(x_1, x_2, \cdots, a, a, \cdots, x_{n-1}, a) \equiv (x_1, x_2, \cdots, a^2, \cdots, x_{n-1}, a) \bmod G_{n+1} .$$

Now applying Lemma 1 with b replaced by a^2 we find that modulo G_{n+1}, $(x_1, x_2, \cdots, a^2, \cdots, x_{n-1}, a)$ is a product of commutators of form $(y_1, y_2, \cdots, a, a, a, \cdots)$ and commutators of form $(y_1, y_2, \cdots, a, a, y_{n-1}, a)$. Thus, by (7), any commutator of type I is a product to commutators of types (i) and (ii) modulo G_{n+1}. The lemma follows.

The main theorems.

In this section we derive more consequences of Lemma 1 and find an upper bound on the nilpotency class of $B(k)$. The first theorem is much like Lemma 2.

THEOREM 1. *Let G be a group of exponent* 4, *and suppose* $(x_1, \cdots, x_n)$

is a commutator of length n with entries from G such that some four (or more) of $x_1, \cdots, x_n$ are a. If $n \geqq 6$, then $(x_1, \cdots, x_n)$ is in G_{n+1}.

Proof. If $(x_1, \cdots, x_n) \neq 1$, then since four entries of $(x_1, \cdots, x_n)$ are a, it follows that at least three of $x_3, \cdots, x_n$ are a. By Lemma 2 and (A) we may restrict attention to commutators of the following types:

(i) $(a, x_2, \cdots, x_{n-3}, a, a, a)$

(ii) $(a, x_2, \cdots, a, a, x_{n-3}, a)$.

Applying (7) and (9), we may confine our study to commutators of the following types:

(i′) $(a, x_2, a, a, a, x_3, \cdots, x_{n-3})$

(ii′) $(a, x_2, a, a, x_3, a, \cdots)$.

But now, modulo G_7, using (2) and (5),

$$(a, x, a, a, a, y) \equiv (a, x, a; a, x; y) \equiv (a^2, \boldsymbol{x}; \boldsymbol{a}, x; y) \equiv 1 ,$$

and

$$\begin{aligned}(a, x, a, a, y, a) &\equiv (a, x, a^2, y, a) \equiv (a, x, y, a^2, a)(\boldsymbol{a}, x; \boldsymbol{a}^2, y; a) \\ &\equiv (a, x, y, a, a, a) \equiv (a, x, a, a, a, y) = 1 .\end{aligned}$$

Thus a commutator of type (i′) or (ii′) is in G_{n+1}. The theorem follows.

Let $x_1, \cdots, x_k$ be generators of $B(k)$. Then it is easy to show that $x_1, \cdots, x_{k-1}$ generate a group isomorphic to $B(k-1)$. We may thus consider $B(k-1)$ as imbedded in $B(k)$.

If A and B are subgroups of a group, G, we define (A, B) as the subgroup of G generated by all commutators (a, b) with a in A and b in B.

THEOREM 2. *For each positive integer k,*

$$(B(k)_{3k-1}, B(k+1)) \subseteqq B(k+1)_{3k+1} .$$

Proof. We first show that the theorem holds for $k = 2$, then we proceed by induction on k. Thus suppose first that $k = 2$. Now as noted above, $B(2)_5$ is generated by $(x_1, x_2, x_1; x_1, x_2)$ and $(x_2, x_1, x_2; x_2, x_1)$. But if y is in $B(3)$, then modulo $B(3)_7$,

$$(x_1, x_2, x_1; x_1, x_2; y) = (x_1^2, \boldsymbol{x}_2; \boldsymbol{x}_1, x_2; y) \equiv 1 .$$

Similarly, $(x_2, x_1, x_2; x_1, x_2; y) \equiv 1$ modulo $B(3)_7$. Thus the theorem is true if $k = 2$.

Now suppose inductively that for some n the theorem is true for all k such that $2 \leqq k < n$. We shall show that

$$(B(n)_{3n-1}, B(n+1)) \subseteqq B(n+1)_{3n+1} .$$

It will be sufficient to show that if $y_1, \cdots, y_{3n-1}$ are chosen in any way from $x_1, \cdots, x_n$ and if z is in $B(n+1)$, then $(y_1, \cdots, y_{3n-1}, z)$ is in $B(n+1)_{3n+1}$. Now if four of $y_1, \cdots, y_{3n-1}$ are equal, then by Theorem 2 $(y_1, \cdots, y_{3n-1}, z)$ is in $B(n+1)_{3n+1}$. Thus suppose the contrary, i.e., suppose that each of (say) $x_2, \cdots, x_n$ appears three times among $y_1, \cdots, y_{3n-1}$ and that x_1 appears twice. By (A) we may restrict attention to the case in which $y_1 = x_1$. But in this case, since $n \geqq 3$, we must have at least one (say x_n) of $x_2, \cdots, x_n$ appearing three times among $y_3, \cdots, y_n$, so that by Lemma 2 we may restrict ourselves to consideration of commutators of the following types:

(i) $(y_1, y_2, \cdots, y_{3n-4}, x_n, x_n, x_n, z)$

(ii) $(y_1, y_2, \cdots, x_n, x_n, y_{3n-4}, x_n, z)$,

where x_1 appears twice among $y_1, \cdots, y_{3n-4}$ and each of $x_2, \cdots, x_{n-1}$ appears three times. Now by (9),

$$(y_1, y_2, \cdots, x_n, x_n, y_{3n-4}, x_n, z) \equiv (y_1, \cdots, y_{3n-4}, x_n, x_n, z, x_n)$$

modulo $B(n+1)_{3n+1}$. But $(y_1, \cdots, y_{3n-4})$ is in $B(n-1)_{3(n-1)-1}$ so that, by the inductive assumption, a commutator of type (i) or type (ii) is in $B(n+1)_{3n+1}$. The theorem follows.

Finally, we have the principal goal of this paper.

THEOREM 3. *For each positive integer* k, $B(k)_{3k} = 1$.

Proof. It follows immediately from Theorem 2 that $B(k)_{3k} = B(k)_{3k+1}$ so that, since $B(k)$ is nilpotent, $B(k)_{3k} = 1$.

One may apply the foregoing results to obtain numerical estimates of the derived length and order of $B(k)$. It follows immediately from Theorem 3 that if $B(k)^{(m)} \neq 1$, then $2^m < 3k$, so that the derived length of $B(k)$ is at most $\log_2 (3k-1)$. By means of the Witt formulae (see, for example, [2], p. 169) one can also obtain an upper bound on the order of $B(k)$ using Theorems 2 and 3. Such estimates, both of derived length and order, are easily seen to be imprecise. For example, the Witt formula calculations give the order of $B(3)$ as at most 2^{484}, whereas a little direct computation shows that the order is at most 2^{70}. Also, $\log_2 (3 \cdot 3 - 1) = 3$, but one can show that $B(3)''' = 1$.

Finally we would like to point out that it can be shown that $B(k)_k \neq 1$, so that perhaps the upper bound on the class given here is not too far from the true class. Indeed, the bound is precise for $k = 2$, and preliminary work suggests that it may be precise for $k = 3$.

BIBLIOGRAPHY

1. W. Burnside, *On an unsettled question in the theory of discontinuous groups,* Quart. J. Pure and Appl. Math., **33** (1902), 230-238.
2. M. Hall, Jr., *The Theory of Groups,* the Macmillan Co., 1959.
3. I. N. Sanov, *Solution of Burnside's problem for exponent* 4, Leningrad State Univ. Ann., **10** (1940), 166-170.
4. C. R. B. Wright, *On groups of exponent four with generators of orders two,* Pacific, J. Math., **10**, (1960), 1097-1105.

CALIFORNIA INSTITUTE OF TECHNOLOGY