ON GROUPS OF EXPONENT FOUR WITH GENERATORS OF ORDER TWO

C. R. B. WRIGHT

1. If x, y, \cdots are elements of a group G, we define the commutator (x, y) of x and y by $(x, y) = x^{-1}y^{-1}xy$. More generally, we define extended commutators inductively by $(x, \dots, y, z) = ((x, \dots, y), z)$. In this paper we shall also be concerned with higher commutators of type $((a_1, \dots, a_s), (b_1, \dots, b_i), \dots, (c_1, \dots, c_r))$ which we denote by $(a_1, \dots, a_s; b_1, \dots, b_i; \dots; c_1, \dots, c_r)$. If we let G_i be the subgroup of G which is generated by all extended commutators of length i, (i.e., with i entries), then G_i is a characteristic subgroup of G, and the series $G = G_1 \supset G_2 \supset \cdots$ is called the *lower central series* of G.¹

Let G(n) $(n = 1, 2, \dots)$ be the freest group of exponent 4 on n generators of order 2. That is, G(n) is a group in which the fourth power of every element is the identity, 1, G(n) is generated by n elements of order 2, and if H is any other group with these properties, then H is a homomorphic image of G(n).

We prove $G(n)_{n+2} = 1$. For this purpose it may be assumed, since G(n) is finite² and hence nilpotent, that $G(n)_{n+3} = 1$. Moreover, it will be enough to show $(x_1, \dots, x_{n+2}) = 1$ for all choices of x_1, \dots, x_{n+2} from among the generators of G(n).

2. LEMMA 2.1. If x, y, \dots, z are elements of order 2 in a group of exponent 4, then $(x, y)^2 = 1, (x, y, \dots, z)^2 = 1$, and (x, y, x) = 1.

Proof. Since $(x, y) = xyxy = (xy)^2$, $(x, y)^2 = 1$. By induction, $(x, y, \dots, z)^2 = 1$, while (y, x) = yxyx = x(x, y)x = (x, y)(x, y, x), so that $(x, y, x) = (y, x)^2 = 1$.

The relation $(x, y, \dots, z)^2 = 1$ will be the justification for future substitutions and will be used without specific mention.

THEOREM 2.1. $G(2)_3 = 1$.

Proof. By Lemma 2.1, if the generators of G(2) are a and b, then (a, b, a) = (b, a, a) = (a, b, b) = (b, a, b) = 1.

3. LEMMA 3.1. If a, b and c are elements of order 2 in a group G of exponent 4, then

Received October 26, 1959. Presented to the Society on September 3, 1959. This work was supported by a National Science Foundation predoctoral fellowship.

¹ For properties of commutators and the lower central series see Hall, [1], Ch. 10.

² See Sanov, [2], or Hall, [1], pp. 324-325.

C. R. B. WRIGHT

(1)
$$(a, b, c) \equiv (b, c, a)(c, a, b) \operatorname{mod} G_{\mathfrak{s}}$$

$$(2) \qquad (a, b; c, a) = (a, c; b, a) \equiv (a, c, b, a) \mod G_{5}$$

$$(3) (a, b, c, a) \equiv (b, c, a, b)(c, a, b, c) \mod G_5$$

Proof. We may assume that a, b and c generate G. Now

$$abcabc = aba (a, c)b(b, c) = (a, b)(a, c)(a, c, b)(b, c)$$
.

Thus, modulo G_{5} , $(abc)^{2} = (a, b)(a, c)(b, c)(a, c, b)$. Hence

$$1 \equiv [(a, b)(a, c)(b, c)]^2 \mod G_5, \text{ so that, modulo } G_5,$$

$$1 = (a, b)(a, c)(b, c)(a, b)(a, c)(b, c) = (a, b)(a, c)(a, b)(a, b; b, c)(a, c)(a, c; b, c),$$

$$(4) 1 \equiv (a, b; a, c)(a, b; b, c)(a, c; b, c) \mod G_5.$$

But also

$$\begin{aligned} abc &= ca(a, c)b(b, c) \\ &= bc(c, b)a(a, b)(a, c)(a, c, b)(b, c) \\ &= ab(b, a)c(c, a)(c, b)(c, b, a)(a, b)(a, c)(a, c, b)(b, c) , \end{aligned}$$

so that 1 = (b, a)(b, a, c)(c, a)(c, b)(c, b, a)(a, b)(a, c)(a, c, b)(b, c), and hence, modulo G_5 ,

$$1 = (b, a)(c, a)(c, b)(a, b)(a, c)(b, c)(b, a, c)(c, b, a)(a, c, b)$$

= $[(a, b)(a, c)(b, c)]^{2}(a, b, c)(b, c, a)(c, a, b)$.

Thus (1) is proved. Replacing b by (a, b) in (1) gives $(a, b, c, a)(c, a; a, b) \equiv 1 \mod G_5$ or (2). And (2) and (4) together give (3).

LEMMA 3.2. If x_1, \dots, x_k and a are elements of order 2 in a group G of exponent 4, then $(x_1, \dots, x_k, a) \equiv X \mod G_{k+2}$, where X is a product of commutators of form (a, y_1, \dots, y_k) with y_1, \dots, y_k from among x_1, \dots, x_k .

COROLLARY. If $x_1, \dots, x_k, z_1, \dots, z_s$ and a are elements of order 2 in a group G of exponent 4, then

$$(x_1, \cdots, x_k, a, z_1, \cdots, z_s) \equiv X \mod G_{k+s+2}$$

where X is a product of commutators of form $(a, y_1, \dots, y_k, z_1, \dots, z_s)$ with y_1, \dots, y_k from among x_1, \dots, x_k .

Proof of Lemma 3.2. Certainly the lemma and corollary are true if k = 1. Assume for induction that both are true for $k = n - 1 \ge 1$.

Now by (1), modulo G_{n+2} , $(x_1, \dots, x_{n-1}, x_n, a) = (x_1, \dots, x_{n-1}, a, x_n)(x_1, \dots, x_{n-1}; a, x_n)$. But by the inductive assumption $(x_1, \dots, x_{n-1}, a, x_n)$ is a product of terms $(a, y_1, \dots, y_{n-1}, x_n)$, and $(x_1, \dots, x_{n-1}; a, x_n)$ is a product of terms $(a, x_n, y_1, \dots, y_{n-1})$. The lemma and its immediate corollary follow by induction.

THEOREM 3.1. $G(3)_5 = 1$.

Proof. Let a, b and c be the generators of G(3). Consider any commutator $C = (x_1, x_2, x_3, x_4, x_5)$ in arguments a, b and c. We show C = 1. There is no loss of generality in taking $x_5 = a$. If a does not appear again in C, then by Theorem 2.1, $C = (1, x_5) = 1$. If a appears again, then by Lemma 3.2 and the assumption that $G(3)_6 = 1$, we may suppose $C = (a, x_2, x_3, x_4, a)$. By Lemma 2.1, if a appears a third time, then C = 1. Thus we may take C = (a, b, c, b, a). Now (a, b, c, b, a) =(b, c, a, b, a)(c, a, b, b, a) = (b, c, a, b, a) by (1). Replacing c by (b, c) in (3) gives (a, b; b, c; a) = (b; c, a, b, a). Hence, C = (a, b, c, b, a) = (b, c, a, b, a) =(a, b; b, c; a) = 1, and the theorem is proved.

COROLLARY 1. If a, b and c are elements of order 2 in a group of exponent 4, then

$$(1') (a, b, c) = (b, c, a)(c, a, b)$$

$$(2') (a, b; c, a) = (a, b, c, a)$$

$$(3') (a, b, c, a) = (b, c, a, b)(c, a, b, c)$$

Proof. These follow from Lemma 3.1.

COROLLARY 2. If $x_1, \dots, x_k, y_1, \dots, y_s, z_1, \dots, z_t$ $(s \ge 2)$ are elements of order 2 in a group G of exponent 4, then

$$(x_1, \cdots, x_k; y_1, \cdots, y_s; z_1; \cdots; z_t) \equiv AB \mod G_{k+s+t+1}$$

where

$$A = (x_1, \dots, x_k; y_1, \dots, y_{s-1}; y_s; z_1; \dots; z_t)$$

$$B = (x_1, \dots, x_k, y_s; y_1, \dots, y_{s-1}; z_1; \dots; z_t).$$

Proof. This follows from (1').

The following corollary lists some relations for future use.

COROLLARY 3. If a, b, c, d and f are elements of order 2 in a group G of exponent 4, then

C. R. B. WRIGHT

$$(a, b, c, d, c) \equiv (a, b, d, c, d) \mod G_6$$

$$(6) \qquad (b, c, a; d, f, a) \equiv 1 \mod G$$

(7) (a, f; b, d, c) = (a, f, c; b, d)(a, f; b, d; c)

(8)
$$(b, f, d; a, c)(d, f, b; a, c) \equiv (b, d, f; a, c) \mod G_8$$
.

Proof. By (3'), with a replaced by (a, b) and b replaced by d, (a, b, d, c; a, b) = (d, c; a, b; d)(c; a, b; d; c) = (a, b; d, c; d)(a, b, c, d, c), so that, since (a, b; d, c; d) = (a, b, d, c, d), (5) is true. By (2') and (3') with b replaced by (b, c) and c replaced by (d, f), (b, c, a; d, f, a) = (a; b, c; d, f; a) = (b, c; d, f; a; b, c)(d, f; b, c; a; d, f), so that (6) is true. Finally, (7) and (8) are obvious from (1').

4. LEMMA 4.1. If a, b, c and d are elements of order 2 in a group G of exponent 4, then

$$(9) (a, b; c, d) \equiv (a, c; b, d)(a, d; b, c) \mod G_5.$$

Proof. First, working modulo G_5 and collecting as we did in the proof of Lemma 3.1 we obtain $(abcd)^2 = T_2T_3T_4$ where

$$egin{aligned} T_2 &= (a,\,b)(a,\,c)(b,\,c)(a,\,d)(b,\,d)(c,\,d) \ T_3 &= (a,\,c,\,b)(a,\,d,\,c)(a,\,d,\,b)(b,\,d,\,c) \ T_4 &= (a,\,d,\,b,\,c) \ . \end{aligned}$$

Note that modulo G_5 , T_2 , T_3 and T_4 commute, and $T_3^2 = T_4^2 = 1$. Hence, modulo G_5 , $1 = (abcd)^4 = T_2^2$. Collecting the (a, d)'s in T_2^2 we obtain $1 = XABCY \mod G_5$, where

$$\begin{split} X &= [(a, b)(a, c)(b, c)]^2 \\ A &= (b, c; b, d)(b, c; c, d)(b, d; c, d) \\ B &= (a, c; a, d)(a, c; c, d)(a, d; c, d) \\ C &= (a, b; a, d)(a, b; b, d)(a, d; b, d) \\ Y &= (a, b; c, d)(a, c; b, d)(a, d; b, c) \;. \end{split}$$

Now modulo G_5 , X = 1, while A = B = C = 1 by (2') and (3'). Hence, $1 \equiv (a, b; c, d)(a, c; b, d)(a, d; b, c) \mod G_5$, which is (9).

COROLLARY 1. If x_1, \dots, x_k and a are elements of order 2 in a group G of exponent 4, then for $i = 2, \dots, k$,

$$(x_1, a, x_2, a, \dots, x_i, \dots, x_k) \equiv (x_1, x_2, \dots, a, x_i, a, \dots, x_k) \mod G_{k+3}$$

Hence, if two of x_1, \dots, x_k , a are equal, $(x_1, a, x_2, a, \dots, x_k) \equiv 1 \mod G_{k+3}$.

Proof. Let a, b, c and d be elements of order 2 in G. Then modulo $G_{\mathfrak{s}}$,

$$(b, a, c, a, d) = (b, a;, c, a; d)$$

= (b, a, d; c, a)(c, a, d; b, a)
= (b, a, c; d, a)(c, a, b; d, a)
= (b, c, a; d, a)
= (b, c, a, d, a) .

The first statement follows. Now the second statement is clearly true if a appears a third time, since then $(x_1, a, x_2, a, \dots, a, \dots, x_k) =$ $(x_1, x_2, \dots, a, a, a, a, \dots, x_k) = 1$. If some x_i appears twice, then modulo $G_{k+3}(x_1, a, x_2, a, \dots, x_i, \dots, x_k) = (x_1, \dots, a, x_i, a, \dots, x_k) = (x_1, x_2, \dots, x_i, a, x_i, \dots, x_k) = (x_1, x_i, x_2, x_i, \dots, a, \dots, x_k)$ (the second step following from (5)), and we are back to the case of three appearances of a. Thus the corollary is proved.

COROLLARY 2. If a, b, c, d and f are elements of order 2 in a group G of exponent 4, then

(10)
$$1 \equiv (a, f, b; c, d)(a, f, c; b, d)(a, f, d; b, c) \mod G_6$$

(11)
$$(a, c; d, f; b)(a, d; c, f; b) \equiv (c, d; a, f; b) \mod G_6$$
.

Proof. These follow from (9).

THEOREM 4.1. $G(4)_6 = 1$.

Proof. Let the generators of G(4) be a, b, c and d and consider any commutator $C = (x_1, x_2, x_3, x_4, x_5, x_6)$ in a, b, c and d. It will be sufficient to prove C = 1 under the assumption that $G(4)_7 = 1$. As in the proof of Theorem 3.1, we may suppose that $C = (a, x_2, x_3, x_4, x_5, a)$. Moreover, if x_2, x_3, x_4 or x_5 is a, then by Theorem 2.1 or Corollary 1 of Lemma 4.1, C = 1. It will thus be sufficient to prove (a, b, c, b, d, a) = 1, (a, b, c, d, b; a) = 1, and (a, c, b, d, b, a) = 1. Now by Corollary 1 of Lemma 4.1, (a, b, c, b, d, a) = (a, c, b, d, b, a) = 1, while by (1'), (a, b, c; b, d, a) = (a, c, b; b, d; a), so that by (6) (a, b, c; b, d; a) = 1. Thus (a, b, c, d, b, a) = (a, b, c, b, d, a)(a, b, c; b, d; a) = 1, and the theorem is proved.

5. The main result, that $G(n)_{n+2} = 1$, has now been proved for n = 2, 3 and 4. In this section we derive an identity analogous to (1) and (9) for five generators. This identity enables us to prove, in §6, that $G(n)_{n+2} = 1$ for $n \ge 5$.

LEMMA 5.1. If a, b, c, d and f are elements of order 2 in a group G of exponent 4, then

```
C. R. B. WRIGHT
```

(12)
$$(a, b; c, d; f) \equiv (c, b; f, d; a)(f, b; a, d; c) \mod G_6$$

COROLLARY. If (x_1, \dots, x_k) , (y_1, \dots, y_j) , (z_1, \dots, z_m) , a and b $(k, j, m \ge 1)$ are elements of order 2 in a group G of exponent 4, then

(13) $(x_1, \dots, x_k, a; y_1, \dots, y_j, b; z_1, \dots, z_m) \equiv C_1 C_2 \mod G_{k+j+m+3}$

where

$$egin{aligned} & C_1 = (y_1,\,\cdots,\,y_j;\,z_1,\,\cdots,\,z_m;\,x_1,\,\cdots,\,x_k,\,b;\,a) \ & C_2 = (x_1,\,\cdots,\,x_k;\,z_1,\,\cdots,\,z_m;\,y_1,\,\cdots,\,y_j,\,a;\,b) \ . \end{aligned}$$

Proof of Lemma 5.1. First, working modulo G_5 , we collect f's in the expression $(abcdf)^2$ to get $(abcdf)^2 = (abcd)a(a, f)b(b, f)c(c, f)d(d, f)$. Then collecting b, c and d in that order we obtain $(abcdf)^2 = (abcd)^2S_2S_3S_4$ where

$$\begin{split} S_2 &= (a, f)(b, f)(c, f)(d, f) \\ S_3 &= (a, f, d)(a, f, c)(a, f, b)(b, f, d)(b, f, c)(c, f, d) \\ S_4 &= (a, f, c, d)(a, f, b, d)(a, f, b, c)(b, f, c, d) . \end{split}$$

But as in the proof of Lemma 4.1, $(abcd)^2 \equiv T_2T_3T_4 \mod G_5$, where

$$T_{2} = (a, b)(a, c)(a, d)(b, d)(c, d)$$

$$T_{3} = (a, c, b)(a, d, c)(a, d, b)(b, d, c)$$

$$T_{4} = (a, d, b, c) .$$

Thus, modulo G_5 , $(abcdf)^2 = T_2T_3T_4S_2S_3S_4$. But then, modulo G_6 ,

$$egin{aligned} 1 &= (abcdf)^4 = T_2 T_3 T_4 S_2 S_3 T_2 T_3 T_4 S_2 S_3 \ &= T_2 T_3 T_4 T_2 S_2 (S_2, \ T_2) S_3 (S_3, \ T_2) T_3 T_4 S_2 S_3 \ &= (T_2 T_3 T_4)^2 S_2 (S_2, \ T_3) (S_2, \ T_2) S_3 (S_3, \ T_2) S_2 S_3 \ &= S_2 (S_2, \ T_3) (S_2, \ T_2) S_3 (S_3, \ T_2) S_2 S_3 \ &= S_2^2 (S_2, \ T_3) (S_2, \ T_2) S_3 (S_3, \ S_2) (S_3, \ T_2) S_3 \ &= S_2^2 (S_2, \ T_3) (S_2, \ T_2) S_3 (S_3, \ S_2) (S_3, \ T_2) S_3 \ &= S_2^2 (S_2, \ T_3) (S_2, \ T_2) S_3^2 (S_3, \ S_2) (S_3, \ T_2) \ . \end{aligned}$$

But modulo G_6 , $S_3^2 = 1$, while S_2^2 is a product of commutators of weight 4. Thus the last relation may be rewritten as $1 \equiv A \mod G_6$ where Ais a product of commutators in a, b, c, d and f of weight 4 or 5; hence the factors of A commute modulo G_6 . Let A'_a be the product of all factors of A which do not contain a as argument, and let A_a be the product of the remaining factors of A. Then $1 \equiv A'_a A_a \mod G_6$, so that, setting $a = 1, 1 \equiv A'_a \mod G_6$, and hence $1 \equiv A_a \mod G_6$. Continuing this argument we finally arrive at $1 \equiv A_{abcdf} \mod G_6$, where A_{abcdf} is the product of all factors of A which contain each of a, b, c, d and f. But what are

these factors? Clearly S_2^2 and (S_2, T_2) do not contain any such factors; and since each factor of S_2 and S_3 contains f, (S_3, S_2) cannot contain any such factors. We are left with (S_2, T_3) and (S_3, T_2) . The product of the desired factors of (S_2, T_3) is clearly

$$(a, f; b, d, c)(b, f; a, d, c)(c, f; a, d, b)(d, f; a, c, b)$$
,

while the product of the desired factors of (S_3, T_2) is

 $(a, f, d; b, c)(a, f, c; b, d)(a, f, b; c, d)(b, f, d; a, c)(b, f, c; a, d)(c, f, d; a, b) \ .$

Hence, modulo G_6 ,

$$1 = (a, f; b, d, c)(b, f; a, d, c)(c, f; a, d, b)(d, f; a, c, b)$$

$$\cdot (a, f, d; b, c)(a, f, c; b, d)(a, f, b; c, d)$$

$$\cdot (b, f, d; a, c)(b, f, c; a, d)(c, f, d; a, b) .$$

so that by (10)

$$1 = (a, f; b, d, c)(b, f; a, d, c)(c, f; a, d, b)(d, f; a, c, b)$$

$$\cdot (b, f, d; a, c)(b, f, c; a, d)(c, f, d; a, b) .$$

Using (7) on the first four factors gives, modulo G_6 ,

$$\begin{split} 1 &= (a, f, c; b, d)(a, f; b, d; c)(b, f, c; a, d)(b, f; a, d; c) \\ &\cdot (c, f, b; a, d)(c, f; a, d; b)(d, f, b; a, c)(d, f; a, c; b) \\ &\cdot (b, f, d; a, c)(b, f, c; a, d)(c, f, d; a, b) \\ &= (a, f, c; b, d)(a, f; b, d; c)(b, f; a, d; c)(c, f, b; a, d)(c, f; a, d; b) \\ &\cdot (d, f, b; a, c)(d, f; a, c; b)(b, f, d; a, c)(c, f, d; a, b) \\ &= (a, f, c; b, d)(a, f; b, d; c)(b, f; a, d; c)(c, f, b; a, d) \\ &\cdot (c, f; a, d; b)(d, f; a, c; b)(b, d, f; a, c)(c, f, d; a, b) , \end{split}$$

where the last step follows from (8). Now applying (11) twice gives

$$1 = (a, f, c; b, d)(a, b; d, f; c)(c, f, b; a, d)(a, f; c, d; b)$$

$$\cdot (b, d, f; a, c)(c, f, d; a, b) ,$$

so that by (10)

1 = (a, f, c; b, d)(a, b; d, f; c)(a, f; c, d; b)(b, d, f; a, c)(c, f, a; b, d)and hence by (8)

$$1 = (a, b; d, f; c)(a, f; c, d; b)(b, d, f; a, c)(a, c, f; b, d)$$
.

Thus, by (7)

$$1 \equiv (a, b; d, f; c)(a, f; c, d; b)(a, c; b, d; f) \mod G_{\epsilon}$$
,

so that interchanging a with b and c with f we get

$$1 \equiv (a, b; c, d; f)(c, b; f, d; a)(f, b; a, d; c) \mod G_{\mathfrak{s}}$$

which is (12). Thus the lemma is proved.

The corollary follows immediately.

6. Having proved the crucial relation (12), we are now in a position to prove the main theorem.

THEOREM 6.1. Let G(n), $(n = 1, 2, \dots)$ be the freest group of exponent 4 generated by n elements of order 2. Then $G(n)_{n+2} = 1$.

Proof. The proof is by induction on n. We have the result for n = 1, 2, 3 and 4. Assuming the result true for n we now prove it for n + 1. As before, we may assume $G(n + 1)_{n+4} = 1$. Consider a commutator $C = (y_1, y_2, \dots, y_{n+3})$ in the generators x_1, \dots, x_n , a and b of G(n + 1). As before, we may restrict attention to the case $C = (a, y_2, \dots, y_{n+2}, a)$. There are two possibilities to consider—*Case* 1: a appears again; *Case* 2: b appears twice. In either case we may assume that every x_i appears once, since otherwise, by the inductive assumption, C = 1.

Case 1. The proof in this case is by induction on the position of the middle a. Clearly $(a, y_2, a, \dots, a) = 1$. Assume that for some $i \ge 3$, $(a, y_2, \dots, y_{i-1}, a, \dots, a) = 1$. Then

where the last step follows from $G(n)_{n+2} = 1$. But by (13),

$$(a, y_2, \cdots, y_{i-1}; y_i, a; a, y_{n+2}, \cdots, y_{i+1}) = C_1 C_2$$

where

$$egin{aligned} C_1 &= (a,\,y_2,\,\cdots,\,y_{i-2},\,y_i;\,a,\,y_{n+2},\,\cdots,\,y_{i+1},\,a;\,y_{i-1})\ C_2 &= (a,\,y_2,\,\cdots,\,y_{i-2};\,a,\,y_{n+2},\,\cdots,\,y_{i+1};\,y_{i-1},\,a;\,y_i) \ . \end{aligned}$$

Since y_i and y_{i-1} appear only once, by the assumption that $G(n)_{n+2} = 1$ we have $C_1 = C_2 = 1$. Hence, by induction, C = 1 if a appears three times.

Case 2. In this case also the proof is by induction, this time on the distance between the b's. Let

$$C = (a, z_1, \dots, z_i, b, z_{i+1}, \dots, z_j, b, z_{j+1}, \dots, z_{n-1}, a)$$

where $0 \leq i < j \leq n-1$ (that is, there might be no entries between

the a's and the b's). If j-i=1, then clearly C=1. Assume that C=1 for $j-i=k\geq 1$. Then as in Case 1,

where

Thus C = 1 for j - i = k + 1, so that by induction C = 1 if b appears twice.

Since C = 1 in both cases, we conclude that $G(n + 1)_{n+3} = 1$, so that by induction $G(n)_{n+2} = 1$ for $n = 1, 2, \cdots$.

7. The author conjectures that the class of G(n) is precisely n + 1 for n > 2. As supporting evidence, he has constructed G(n)/G(n)'' and shown that its class is exactly n. Moreover, for n = 3 and n = 4, G(n)'' is fairly large, and $G(n)_{n+1} \neq 1$.

BIBLIOGRAPHY

1. M. Hall, Jr., The Theory of Groups, the Macmillan Co., 1959.

2. I. N. Sanov, Solution of Burnside's problem for exponent 4, Leningrad State Univ. Ann. 10, (1940), 166-170.

UNIVERSITY OF WISCONSIN CALIFORNIA INSTITUTE OF TECHNOLOGY