THE DERIVED SERIES OF
A p-GROUP

Thesis by

Charles Ray Hobby

In Partial Fulfillment of the Requirements

For the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

1960

ACKNOWLEDGMENTS

I wish to thank Doctor Olga Taussky Todd and Professor Hans Zassenhaus for many helpful suggestions. The research presented in this thesis was performed while the author held a National Science Foundation Summer Fellowship. My thanks are extended to Miss Evangeline Gibson for her patience and efficiency in typing the manuscript.

ABSTRACT

Olga Taussky (see W. Magnus, Math. Ann. vol. 111 (1935)) posed the problem of determining whether there is an infinite chain of p-groups $G_1, G_2, \ldots,$ such that G_1 is abelian, $G_n \cong G_{n+1}/G_{n+1}^{(n)}$, and $G_{n+1}^{(n)} \neq 1$ where $G_{n+1}^{(n)}$ is the nth derived group of G_{n+1}. N. Itô (Nagoya Math. J., vol. 1, (1950)) constructed such a chain for $p > 2$ and G_1 of type (p,p,p). It is shown (by an explicit construction) that if $p > 2$ there is a chain of the required kind for G_1 any non-cyclic abelian p-group. If $p = 2$ there is a chain of the required kind if G_1 contains a subgroup of type $(2^2,2^3)$, of type $(2^2,2^2,2^2)$, of type $(2,2,2^2,2^2)$, or of type $(2,2,2,2,2)$. As a consequence, for $p > 2$ it is impossible to estimate the length of the derived series of a non-abelian p-group G from the type of $G/G^{(1)}$. This gives a negative answer (for $p > 2$) to a question posed by O. Taussky (Research Problem 9, Bull. Amer. Math. Soc. vol. 64 (1958) pp. 124).

Chapter 1

Olga Taussky [9] posed the following problem on finite p-groups (i.e., groups of prime power order): Is it possible to estimate the length of the derived series of a p-group G from the type of $G/G^{(1)}$, where $G^{(n)}$ denotes the nth derived group of G? This question is known to have an affirmative answer in certain cases. For example, it follows from the Burnside Basis Theorem [11, page 111] that if $G/G^{(1)}$ is cyclic, then G is cyclic, and consequently $G^{(1)} = \langle 1 \rangle$. O. Taussky [10] has shown that for 2-groups G, with $G/G^{(1)}$ of type $(2,2)$, the derived group $G^{(1)}$ is cyclic and hence $G^{(2)} = \langle 1 \rangle$. This result was rediscovered by Blackburn [1] who showed that if G is a 2-group with $G/G^{(1)}$ of type $(2,2)$, then G contains a cyclic subgroup of index 2.

The following related result was obtained by Scholz and Taussky [8] for a large class of 3-groups. Let u, v, w be elements of a group G, and define symbolic powers by the rules: $u^v = v^{-1} u v$; $u^{v+w} = u^v u^w$. This enables us to consider polynomials as symbolic exponents, even though addition is not necessarily commutative. Let G be a 3-group having generators a, b and denote by H the subgroup of G generated by c^{a-1} and c^{b-1} where $c = a^{-1}b^{-1}ab$. Denote by M the ideal $\left(3, (a-1)^2, (a-1)(b-1), (b-1)^2\right)$ in the ring of all symbolic powers of elements of G. Let G^3 be the group generated by the third powers of the elements of G. Then the result of Scholz and Taussky can be stated as follows: If $c^m \in G^{(2)}$ for every $m \in M$, and if $H\,G^{(2)} \subseteq G^3\,G^{(2)}$, then $G^{(2)} = \langle 1 \rangle$. A stronger version of this result can be obtained from a recent theorem of Blackburn [2] which states that if G is a 3-group with $G^{(2)} \neq \langle 1 \rangle$, then the class of G is greater than four. The stronger version of the result of Scholz and Taussky is then: If $c^m \in G^{(2)}$ for every $m \in M$, then $G^{(2)} = \langle 1 \rangle$.

The obvious conjecture, "If G is a p-group with $G/G^{(1)}$ of type (p,p), then $G^{(2)} = \langle 1 \rangle$," is known to be false. Burnside [3] constructed (for every prime $p > 3$) a p-group G of order p^6 such that $G/G^{(1)}$ has type (p,p) and $G^{(2)} \neq \langle 1 \rangle$. However, as was noted by Blackburn [2], the construction of Burnside actually gives a group G of order 3^7 if $p = 3$, where again $G/G^{(1)}$ has type (p,p) and $G^{(2)} \neq \langle 1 \rangle$.

W. Magnus [6] first noted that the length of the derived series of a p-group cannot always be estimated from the type of $G/G^{(1)}$. He constructed, for every positive integer n, a 3-group G with $G/G^{(1)}$ of type $(3,3,3)$ and $G^{(n)} \neq \langle 1 \rangle$.

The result of Magnus was generalized by N. Itô who considered a problem which arose in the work of Scholz and Taussky [8] on class field towers. This problem can be stated as follows (see Magnus [6], [7]): Determine whether there is an infinite chain of p-groups $G_1, G_2, \ldots,$ such that G_1 is abelian, $G_n \cong G_{n+1}/G_{n+1}^{(n)}$, and $G_{n+1}^{(n)} \neq \langle 1 \rangle$. It is easy to see that, in such a chain, $G_n/G_n^{(1)} \cong G_1$ for every n. (See the proof of Theorem 1.) Thus, since $G_{n+1}^{(n)} \neq \langle 1 \rangle$, it follows from the existence of such a series that the first mentioned question of O. Taussky has a negative answer for any p-group G with $G/G^{(1)} \cong G_1$. Itô [5] constructed a chain of the kind described above, for every prime $p \neq 2$, with G_1 of type (p,p,p).

H. Zassenhaus, in an unpublished work, constructed a large number of such chains, for every prime $p \neq 2$, with G_1 of type (p,p,p). It follows that such a chain exists for G_1 any abelian p-group $(p \neq 2)$ having at least three generators. (See Theorem 1, Chapter 2.)

As noted earlier, the derived series of a p-group G must terminate if $G/G^{(1)}$ is either cyclic or of type $(2,2)$. Thus no chain of the type described above can exist for G_1 cyclic or of type $(2,2)$. It will be shown that such a chain exists in the following cases: $p \neq 2$ and G_1 has at least 2-generators (Theorem 3, Chapter 3); $p = 2$ and G_1 contains a subgroup having one of the types $(2^2,2^3)$, $(2^2,2^2,2^2)$, $(2,2,2^2,2^2)$, and $(2,2,2,2,2)$ (Theorems 4 and 6). It remains an open question whether an infinite chain exists with G_1 a non-cyclic 2-group which is neither of type $(2,2)$ nor contains a subgroup having one of the types listed above.

Chapter 2 contains preliminary lemmas which are valid for general groups. Two theorems are established which reduce the construction of an infinite chain of the kind described above to the construction of a single infinite group having factor groups of a specified form. Infinite chains with G_1 having two generators are constructed in Chapter 3. The chapter ends with a refinement of an inequality for p-groups of P. Hall (Theorem 5). Infinite chains with G_1 a 2-group having 3, 4, and 5 generators are constructed in Chapter 4.

Chapter 2

This chapter consists of notation, preliminary lemmas, and theorems which are valid for general groups. Theorems 1 and 2 give two reductions of the problem of constructing an infinite chain of p-groups $G_1, G_2, \ldots,$ with $G_n \cong G_{n+1}/G_{n+1}^{(n)}$, $G_{n+1}^{(n)} \neq \langle 1 \rangle$, and G_1 an abelian group of type $(p^{n_1}, p^{n_2}, \ldots, p^{n_k})$. Theorem 1 shows that it is sufficient to construct such a chain for G_1 of type $(p^{m_1}, p^{m_2}, \ldots, p^{m_s})$ where $m_i \leq n_i$ and $s \leq k$. Theorem 2 further reduces the problem to the construction of a group containing an infinite chain of normal subgroups satisfying certain conditions. The remaining chapters of this thesis are devoted to the construction of groups satisfying the conditions of Theorem 2.

The following notation will be used: (M,N) is the group generated by all $mnm^{-1}n^{-1}$ for m in M and n in N; $\langle x, y, \ldots, z \rangle$ is the group generated by $x, y, \ldots, z$; $H^{(n)}$ is the $n^{\underline{th}}$ derived group of the group H; R is the ring consisting of all expressions $u + v\sqrt{p}$ for u, v integers and p a fixed prime; P is the ideal of R generated by $\sqrt{p}$; I_2 and O_2 are, respectively, the 2×2 identity and zero matrices; X_2 is the set of all 2×2 matrices having elements in X, where X is an arbitrary ring.

Frequent use will be made of the following weak form of the Burnside Basis Theorem [11, page 111].

<u>Burnside's Basis Theorem.</u> <u>Let</u> G <u>be any</u> p-<u>group and let</u> $x_1, x_2, \ldots, x_n$ <u>be coset representatives of a minimal basis of the abelian group</u> $G/G^{(1)}$. <u>Then</u> $G = \langle x_1, x_2, \ldots, x_n \rangle$.

Theorem 1. Let $G_1, G_2, \ldots$ *be an infinite chain of p-groups such that* $G_n \cong G_{n+1}/G^{(n)}_{n+1}$, $G^{(n)}_{n+1} \neq \langle 1\rangle$, *and* G_1 *is abelian of type* $(p^{m_1}, p^{m_2}, \ldots, p^{m_s})$. *Then an infinite chain of p-groups* $H_1, H_2, \ldots$ *can be constructed with* H_1 *abelian of type* $(p^{n_1}, p^{n_2}, \ldots, p^{n_k})$, $H_n \cong H_{n+1}/H^{(n)}_{n+1}$ *and* $H^{(n)}_{n+1} \neq \langle 1\rangle$ *whenever* $n_i \geq m_i$ *and* $k \geq s$.

Proof. Suppose that $k = s$ and let H_1 be an abelian group of type $(p^{n_1}, p^{n_2}, \ldots, p^{n_s})$ such that $H_1 \cap G_n = \langle 1\rangle$ and $(H_1, G_n) = \langle 1\rangle$ for every n. Then $H_1 = \langle h_1\rangle \times \langle h_2\rangle \times \cdots \times \langle h_s\rangle$ where each h_i is an element of order n_i.

If G is an arbitrary group and N is a normal subgroup of G, then $(G/N)^{(1)} = G^{(1)}N/N$. Thus it follows from $G_n \cong G_{n+1}/G^{(n)}_{n+1}$ that $G^{(1)}_n \cong G^{(1)}_{n+1}/G^{(n)}_{n+1}$, and hence $G_n/G^{(1)}_n \cong \left(G_{n+1}/G^{(n)}_{n+1}\right)\Big/\left(G^{(1)}_{n+1}\ G^{(1)}_{n+1}\right)$. Therefore $G_n/G^{(1)}_n \cong G_{n+1}/G^{(1)}_{n+1}$, and $G_1 = G_1/G^{(1)}_1 \cong G_n/G^{(1)}_n$. Thus, by the Burnside Basis Theorem, each G_n has k independent generators, and these generators have orders $p^{m_1}, p^{m_2}, \ldots, p^{m_k}$ modulo $G^{(1)}_n$.

Suppose $G_2 = \langle x_1, x_2, \ldots, x_k\rangle$ where the x_i are elements of order p^{m_i} modulo $G^{(1)}_2$. Define H_2 to be the subgroup of $G_2 \times H_1$ generated by $x_1h_1, x_2h_2, \ldots, x_kh_k$. That is, $H_2 = \langle x_1h_1, x_2h_2, \ldots, x_kh_k\rangle$. It is clear that $H^{(1)}_2 = G^{(1)}_2$ since each h_i commutes with every element of G_2. Since $n_i \geq m_i$ the order of h_i is not less than the order of x_i modulo $G^{(1)}_2$. Thus $H_2/H^{(1)}_2 \cong \langle h_1\rangle \times \langle h_2\rangle \times \cdots \times \langle h_k\rangle = H_1$. Also, $H^{(1)}_2 \neq \langle 1\rangle$ since $G^{(1)}_2$ was assumed to be different from $\langle 1\rangle$.

If $H_2, H_3, \ldots, H_n$ have been constructed by letting $H_i = < h_1 z_{i1}, \ldots, h_k z_{ik} >$ where $G_i = <z_{i1}, z_{i2}, \ldots, z_{ik}>$, and if $H_i \cong H_{i+1}/H_{i+1}^{(i)}$, $H_{i+1}^{(i)} \neq <1>$ for $i \leq n-1$, then H_{n+1} is constructed as follows. Let $G_n = < z_{n1}, z_{n2}, \ldots, z_{nk} >$, and let σz_{ni} be the coset of $G_{n+1}/G_{n+1}^{(n)}$ corresponding to z_{ni} in the isomorphism $G_n \cong G_{n+1}/G_{n+1}^{(n)}$. Then $G_{n+1}/G_{n+1}^{(n)} = <\sigma z_{ni}, \sigma z_{n2}, \ldots, \sigma z_{nk}>$. Let y_i be a coset representative of σz_{ni} in G_{n+1}. Then, by the Burnside Basis Theorem, $G_{n+1} = < y_1, y_2, \ldots, y_k >$. Define H_{n+1} to be the subgroup of $G_{n+1} \times H_1$ generated by $h_1 y_1, h_2 y_2, \ldots, h_k y_k$. That is, $H_{n+1} = < h_1 y_1, h_2 y_2, \ldots, h_k y_k >$. Clearly $H_{n+1}^{(1)} = G_{n+1}^{(1)}$ since each h_i commutes with every element of G_{n+1}. Also, $H_{n+1}/H_{n+1}^{(n)} = H_{n+1}/G_{n+1}^{(n)} = < h_1 y_1 G_{n+1}^{(n)}, \ldots, h_k y_k G_{n+1}^{(n)} >/G_{n+1}^{(n)}$. Thus $H_{n+1}/H_{n+1}^{(n)} = < h_1 \cdot \sigma z_{n1}, h_2 \cdot \sigma z_{n2}, \ldots, h_k \cdot \sigma z_{nk} >$ which is isomorphic to $< h_1 z_{n1}, h_2 z_{n2}, \ldots, h_k z_{nk} >$. That is, $H_{n+1}/H_{n+1}^{(n)} \cong H_n$. Also, $H_{n+1}^{(n)} = G_{n+1}^{(n)} \neq <1>$. The existence of the required chain $H_1, H_2, \ldots$ now follows by induction.

If $k > s$, let B be an abelian group of type $(p^{n_{s+1}}, p^{n_{s+2}}, \ldots, p^{n_k})$. Construct a chain $K_1, K_2, \ldots$ with K_1 of type $(p^{n_1}, p^{n_2}, \ldots, p^{n_k})$ by the method described above, and let $H_i = K_i \times B$. The chain $H_1, H_2, \ldots$ clearly has the required properties.

Theorem 2. Let H be a group having an infinite chain of normal subgroups $H = H_1 \supset H_2 \supset \dots$. Suppose $f(n)$ is a monotonic increasing, integer valued, positive function defined on the positive integers. Let $H_{f(n)} \subseteq H^{(n)}H_k$ for every $n, k \geq 1$ and define $G_n = H/H^{(n)}H_{f(n)}$. Then $G_n \cong G_{n+1}/G_{n+1}^{(n)}$ for every n.

Proof. It suffices to show that $G_{n+1}^{(n)} = H^{(n)}H_{f(n)}/H^{(n+1)}H_{f(n+1)}$, for then

$$G_{n+1}/G_{n+1}^{(n)} = \left(H/H^{(n+1)}H_{f(n+1)}\right)\Big/\left(H^{(n)}H_{f(n)}/H^{(n+1)}H_{f(n+1)}\right)$$

$$\cong H/H^{(n)}H_{f(n)} = G_n.$$

Note that $H^{(s)}H_{f(s+t)} = H^{(s)}H_{f(s)}$ for all positive integers s and t. For, by hypothesis, $H^{(s)}H_{f(s+t)} \supseteq H_{f(s)}$ and hence

$$H^{(s)}H_{f(s+t)} = H^{(s)}(H^{(s)}H_{f(s+t)}) \supseteq H^{(s)}H_{f(s)}.$$

The reverse inequality is trivial since $H_{f(s+t)} \subseteq H_{f(s)}$.

The first derived group of G_{n+1} is given by

$$G_{n+1}^{(1)} = H^{(1)}H^{(n+1)}H_{f(n+1)}/H^{(n+1)}H_{f(n+1)} = H^{(1)}H_{f(n+1)}/H^{(n+1)}H_{f(n+1)}.$$

Thus $G_{n+1}^{(1)} = H^{(1)}H_{f(1)}/H^{(n+1)}H_{f(n+1)}$ since $H^{(1)}H_{f(n+1)} = H^{(1)}H_{f(1)}$.

The proof will follow by induction if it is shown that $G_{n+1}^{(k)} = H^{(k)}H_{f(k)}/H^{(n+1)}H_{f(n+1)}$ implies $G_{n+1}^{(k+1)} = H^{(k+1)}H_{f(k+1)}/H^{(n+1)}H_{f(n+1)}$ whenever $1 \leq k < n$. But, if $G_{n+1}^{(k)}$ has the above form, then $G_{n+1}^{(k+1)} = \left(H^{(k)}H_{f(k)}\right)^{(1)}H^{(n+1)}H_{f(n+1)}/H^{(n+1)}H_{f(n+1)}$, and it only remains to show that

$$\left(H^{(k)}H_{f(k)}\right)^{(1)} H^{(n+1)}H_{f(n+1)} = H^{(k+1)}H_{f(k+1)}.$$

Note that $H^{(k+1)} \supseteq H^{(n+1)}$ since $k < n$. Clearly $\left(H^{(k)}H_{f(k)}\right)^{(1)} \supseteq H^{(k+1)}H^{(1)}_{f(k)}$. But $H_{f(k)} \subseteq H^{(k)}H_{f(n+1)}$, hence $H^{(1)}_{f(k)} \subseteq H^{(k+1)}H_{f(n+1)}$ since $H_{f(n+1)}$ is normal in H. These inequalities, and the fact that all groups considered are normal in H and hence commute, give

$$\left(H^{(k)}H_{f(k)}\right)^{(1)}H^{(n+1)}H_{f(n+1)} \supseteq H^{(k+1)}H^{(1)}_{f(k)}H^{(n+1)}H_{f(n+1)}$$

$$= H^{(k+1)}H_{f(n+1)} = H^{(k+1)}H_{f(k+1)}.$$

On the other hand, it follows from $H^{(k)}H_{f(k)} = H^{(k)}H_{f(k+1)}$ that

$$\left(H^{(k)}H_{f(k)}\right)^{(1)} = \left(H^{(k)}H_{f(k+1)}\right)^{(1)} \subseteq H^{(k+1)}H_{f(k+1)}$$

where the last inequality holds since $H_{f(k+1)}$ is normal in H. But $k < n$ implies that $H^{(k+1)} \supseteq H^{(n+1)}$ and $H_{f(k+1)} \supseteq H_{f(n+1)}$, hence

$$\left(H^{(k)}H_{f(k)}\right)^{(1)}H^{(n+1)}H_{f(n+1)} \subseteq H^{(k+1)}H_{f(k+1)}H^{(n+1)}H_{f(n+1)} = H^{(k+1)}H_{f(k+1)}$$

and the proof is complete.

The following lemma is due to H. Zassenhaus [12].

Lemma 1: *Let U and V be ideals of K, a commutative ring with identity. Define D_X for every ideal X of K as the set of all 2×2 matrices (α_{ij}) for α_{ij} in K such that $(\alpha_{ij}) - I_2 \equiv 0_2$* modulo X_2. *Then $(D_U, D_V) \subseteq D_{UV}$, where (D_U, D_V) is generated by the set of all $xyx^{-1}y^{-1}$ for x in D_U and y in D_V.*

<u>Proof</u>: It suffices to show that $xyx^{-1}y^{-1} - I_2$ is in $(UV)_2$ if x is in D_U and y is in D_V. But

$$xyx^{-1}y^{-1} - I_2 = (xy - yx)\, x^{-1}y^{-1}$$
$$= ((x - I_2)\,(y - I_2) - (y - I_2)\,(x - I_2))\, x^{-1}y^{-1}.$$

Now $x - I_2$ and $y - I_2$ belong to U_2 and V_2, respectively, hence $(x - I_2)(y - I_2) \in U_2V_2 \subseteq (UV)_2$, and $(y - I_2)(x - I_2) \in V_2U_2 \subseteq (VU)_2$. The ring R is commutative, hence $(UV)_2 = (VU)_2$. Since $(UV)_2$ is an ideal in the ring of all 2×2 matrices with elements in K, it follows from the above that

$$(x - I_2)(y - I_2) - (y - I_2)(x - I_2) \in (UV)_2,$$

and hence,

$$[(x - I_2)(y - I_2) - (y - I_2)(x - I_2)]\, x^{-1}y^{-1} \in (UV)_2.$$

<u>Lemma 2</u>: <u>Suppose the group</u> G <u>contains a descending chain of normal subgroups</u>, $G = G_1 \supset G_2 \supset \cdots$. <u>Let</u> H <u>be a subgroup of</u> G <u>such that, for</u> $1 \leq i < n$, H <u>contains a set of elements</u> X_i <u>which maps on a complete set of generators of</u> G_i/G_{i+1} <u>in the homomorphism</u> $G \to G/G_{i+1}$. <u>Then</u> $HG_n = G$.

<u>Proof</u>: The relations $< X_{n-1} > G_n/G_n \supseteq G_{n-1}/G_n$, and $X_{n-1} \subseteq H$ imply that $HG_n \supseteq G_{n-1}$. Suppose $HG_n \supseteq G_{n-k}$. Then

$< X_{n-k-1} > G_{n-k}/G_{n-k} \supseteq G_{n-k-1}/G_n$ and $X_{n-k-1} \subseteq H$ imply that

$HG_{n-k} \supseteq G_{n-k-1}$. Therefore $HG_n = H(HG_n) \supseteq HG_{n-k} \supseteq G_{n-k-1}$, and the proof follows by induction.

The next lemma is due to N. Blackburn.

Lemma 3. [2, Theorem 1.1]. Let G be a group generated by a set X of elements. Define subgroups $\gamma_i(G)$ recursively by the rules $\gamma_1(G) = G$, and $\gamma_{i+1}(G) = (G, \gamma_i(G))$ for $i \geq 1$. If Y is a set of elements which together with $\gamma_{i+1}(G)$ generate $\gamma_i(G)$, then $\gamma_{i+1}(G)$ is generated by $\gamma_{i+2}(G)$ together with all commutators $xyx^{-1}y^{-1}$ where x, y run through X, Y respectively. This is true for $i = 1, 2, \ldots$.

Chapter 3

The following theorems are proved in this chapter.

Theorem 3. *If* $p > 2$ *and* G_1 *is an arbitrary non-cyclic abelian p-group, then there exists an infinite chain of p-groups* $G_1, G_2, \ldots,$ *such that* $G_n \cong G_{n+1}/G_{n+1}^{(n)}$ *and* $G_{n+1}^{(n)} \neq \langle 1 \rangle$.

Theorem 4. *If* G_1 *is an arbitrary abelian 2-group which contains a subgroup of type* $(2^2, 2^3)$, *then there exists an infinite chain of 2-groups* $G_1, G_2, \ldots,$ *such that* $G_n \cong G_{n+1}/G_{n+1}^{(n)}$ *and* $G_{n+1}^{(n)} \neq \langle 1 \rangle$.

This chapter ends with a refinement of an inequality for p-groups of P. Hall (Theorem 5).

The notation of Chapter 2 is used.

Definition 1. The group generated by the matrices $a = \begin{pmatrix} 1 & \sqrt{p} \\ 0 & 1 \end{pmatrix}$ and $b = \begin{pmatrix} 1 & 0 \\ \sqrt{p} & 1 \end{pmatrix}$ is denoted by A.

Definition 2. The subgroup of A, consisting of all matrices X in A such that $X - I_2 \equiv O_2$, modulo P_2^n, is denoted by A_n.

Outline of the proof of Theorems 3 and 4: The subgroups $A = A_1 \supset A_2 \supset A_3 \supset \ldots$ are seen to form an infinite descending chain of normal subgroups of A. A monotonic increasing, integer valued, positive function $f(n)$ is defined on the positive integers, and it is shown that $A_{f(n)} \subseteq A^{(n)}A_k$ for every n and k. (The definition of $f(n)$ depends upon whether p is even or odd.) Groups G_n are defined by $G_n = A/A^{(n)}A_{f(n)}$, then by Theorem 2, $G_n \cong G_{n+1}/G_{n+1}^{(n)}$. It is seen that $G_{n+1}^{(n)} \neq \langle 1 \rangle$. If $p > 2$, then G_1 is abelian of type

(p,p), and Theorem 3 follows from Theorem 1. If $p = 2$, then G_1 is abelian of type $(2^2, 2^3)$, and Theorem 4 follows from Theorem 1.

The following lemmas establish some elementary properties of the group $A = A_1$.

Lemma 4: $(A_n, A_m) \subseteq A_{n+m}$.

Proof: This is an immediate consequence of Lemma 1 and the definition of A_n, if the ring K is chosen as R and the ideals U, V are taken as P^n and P^m.

Lemma 5: A_n is a normal subgroup of A.

Proof: This follows from Lemma 4 since

$$(A, A_n) = (A_1, A_n) \subseteq A_{n+1} \subseteq A_n.$$

Lemma 6: Let $X = \begin{pmatrix} 1+\alpha, & \beta \\ \gamma, & 1+\delta \end{pmatrix}$, $Y = \begin{pmatrix} 1+s, & t \\ u, & 1+v \end{pmatrix}$ be elements of A such that $X - Y \equiv 0_2$, modulo P_2^n. Then XY^{-1} is an element of A_n.

Proof: It suffices to show that $XY^{-1} - I_2 \equiv 0_2$ modulo P_2^n. By hypothesis, there exist s_1, t_1, u_1, v_1 in R such that $s = \alpha + p^{n/2}s_1$, $t = \beta + p^{n/2}t_1$, $u = \gamma + p^{n/2}u_1$, and $v = \delta + p^{n/2}v_1$. When these expressions are substituted in Y, it follows that

$$XY^{-1} = \begin{pmatrix} (1+\alpha+\delta+\alpha\delta-\beta\gamma) + p^{n/2}(v_1+\alpha v_1-\beta u_1), & p^{n/2}(\beta s_1-\alpha t_1-t_1) \\ p^{n/2}(\gamma v_1-u_1-\delta u_1), & (1+\alpha+\delta+\alpha\delta-\beta\gamma) + p^{n/2}(s_1+\delta s_1-\gamma t_1) \end{pmatrix}.$$

Since X belongs to A, the determinant of X must be 1. That is,

$1 + \alpha + \delta + \alpha\delta - \beta\gamma = 1$, and the lemma follows.

Lemma 7. *Let* n *be a positive integer. Then*

(1) A_{2n}/A_{2n+1} *is cyclic of order* p, *and*

(2) *if* $a^{p^n} \to \bar{a}$, $b^{p^n} \to \bar{b}$ *in the homomorphism* $A \to A/A_{2n+2}$, *then* $A_{2n+1}/A_{2n+2} = \langle \bar{a}, \bar{b} \rangle$, *where* $\langle \bar{a}, \bar{b} \rangle$ *is a non-cyclic group of order* p^2.

Proof of (1): If $X = \begin{pmatrix} 1+\alpha, & \beta \\ \gamma, & 1+\delta \end{pmatrix}$ is in the set difference $A_{2n} - A_{2n+1}$, then α and δ are integers, β and γ are integers multiplied by $\sqrt{p}$. (The generators of A have this property, and it is clearly preserved under multiplication.) Thus α and δ can be written as

$$\alpha = p^n \alpha_1 + p^{n+1} \alpha_2 + \cdots , \qquad 0 \leq |\alpha_i| < p,$$

and

$$\delta = p^n \delta_1 + p^{n+1} \delta_2 + \cdots , \qquad 0 \leq |\delta_i| < p.$$

Not both of α_1 and δ_1 can be zero, for this would imply that X belonged to A_{2n+1}.

Since X is in A, the determinant of X must be 1. That is, $\det X = 1 + \alpha + \delta + \alpha\delta - \beta\gamma = 1$. The coefficient of p^n in $\det X$ is $\alpha_1 + \delta_1$, hence

$$\alpha_1 + \delta_1 \equiv 0 \quad \text{modulo } (p).$$

Since not both $\alpha_1 = 0$ and $\delta_1 = 0$ can hold, it follows that $\alpha_1 \neq 0$ and $\delta_1 \neq 0$.

It is clear that α_1 can be assumed to be positive: for, if $\alpha_1 < 0$, then α can be written as $\alpha = (p + \alpha_1)p^n + (\alpha_2 - 1)p^{n+1} + \cdots$, where now $p + \alpha_1 > 0$.

Let $Y = \begin{pmatrix} 1+\alpha', & \beta' \\ \gamma', & 1+\delta' \end{pmatrix}$ be an arbitrary element of $A_{2n} - A_{2n+1}$ such that

$$\alpha' = p^n\alpha_1' + p^{n+1}\alpha_2' + \cdots, \qquad 0 \leq |\alpha_i'| < p.$$

It will be shown that if $\alpha_1' = \alpha_1$, then XY^{-1} belongs to A_{2n+1}. This will imply that the order of A_{2n}/A_{2n+1} is at most p.

Suppose now that $\alpha_1' = \alpha_1$. Then

$$XY^{-1} = \begin{pmatrix} 1+\alpha, & \beta \\ \gamma, & 1+\delta \end{pmatrix} \begin{pmatrix} 1+\delta', & -\beta' \\ -\gamma', & 1+\alpha' \end{pmatrix} = \begin{pmatrix} 1+\alpha+\delta'+\alpha\delta'-\beta\gamma', & * \\ *, & 1+\delta+\alpha'+\alpha'\delta-\beta'\gamma \end{pmatrix}$$

where it is clear that the off-diagonal elements belong to P^{2n+1} since this is already true for the off-diagonal elements of X and Y^{-1}. Now α, δ, α', and δ' belong to P^{2n}; β, β', γ, and γ' belong to P^{2n+1}. Therefore

$$\alpha\delta' - \beta\gamma' \equiv 0 \quad \text{modulo } P^{2n+1},$$

and

$$\alpha'\delta - \beta'\gamma \equiv 0 \quad \text{modulo } P^{2n+1}.$$

Thus it is only necessary to show that

$$1 + \alpha + \delta' \equiv 1 \quad \text{modulo } P^{2n+1},$$

and

$$1 + \delta + \alpha' \equiv 1 \quad \text{modulo } P^{2n+1},$$

in order to verify that XY^{-1} is an element of A_{2n+1}. But $\delta + \alpha'$ can be written as

$$\delta + \alpha' = (\delta_1 + \alpha_1')\, p^n + (\delta_2 + \alpha_2')\, p^{n+1} + \cdots ,$$

and, since $\alpha_1' = \alpha_1$, the coefficient of p^n is $\alpha_1 + \delta_1$. Since $\alpha_1 + \delta_1 \equiv 0$ modulo p, it follows that

$$1 + \delta + \alpha' \equiv 1 \quad \text{modulo } p^{2n+1}.$$

The other congruence is proved similarly.

The order of A_{2n}/A_{2n+1} has been shown to be at most p. This is a p-group, which is not the identity group since

$$a^{p^{n-1}}\, b\, a^{-p^{n-1}}\, b^{-1} = \begin{pmatrix} 1, & p^{n-1}\sqrt{p} \\ 0, & 1 \end{pmatrix} \begin{pmatrix} 1, & 0 \\ \sqrt{p}, & 1 \end{pmatrix} \begin{pmatrix} 1, & -p^{n-1}\sqrt{p} \\ 0, & 1 \end{pmatrix} \begin{pmatrix} 1, & 0 \\ -\sqrt{p}, & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 + p^n + p^{2n}, & -p^{2n-1}\sqrt{p} \\ p^n\sqrt{p}, & 1 - p^n \end{pmatrix}$$

belongs to $A_{2n} - A_{2n+1}$. Therefore A_{2n}/A_{2n+1} has order p, and hence must be cyclic.

<u>Proof of (2)</u>. Note that $a^{p^n} = \begin{pmatrix} 1, & p^n\sqrt{p} \\ 0, & 1 \end{pmatrix}$ and $b^{p^n} = \begin{pmatrix} 1, & 0 \\ p^n\sqrt{p}, & 1 \end{pmatrix}$ belong to $A_{2n+1} - A_{2n+2}$. Also,

$$(a^{p^n})^s\, (b^{p^n})^t = \begin{pmatrix} 1, & sp^n\sqrt{p} \\ 0, & 1 \end{pmatrix} \begin{pmatrix} 1, & 0 \\ tp^n\sqrt{p}, & 1 \end{pmatrix} = \begin{pmatrix} 1+stp^{2n+1}, & sp^n\sqrt{p} \\ tp^n\sqrt{p}, & 1 \end{pmatrix}$$

is in A_{2n+2} if, and only if, $s \equiv t \equiv 0$ modulo p. By Lemma 4, $(A_{2n+1}, A_{2n+1}) \subseteq A_{4n+2} \subseteq A_{2n+2}$, hence A_{2n+1}/A_{2n+2} is abelian. Thus, if $a^{p^n} \to \bar{a}$, and $b^{p^n} \to \bar{b}$ in the homomorphism $A \to A/A_{2n+2}$, then $< \bar{a}, \bar{b} >$ is a non-cyclic subgroup of order p^2 of A_{2n+1}/A_{2n+2}.

Now let $x = \begin{pmatrix} 1+\alpha, & \beta \\ \gamma, & 1+\delta \end{pmatrix}$ be an arbitrary element of $A_{2n+1} - A_{2n+2}$. Since α and δ are integers divisible by $p^{(2n+1)/2}$, it follows that they must be divisible by p^{n+1}. Also, $\beta = up^n\sqrt{p}$ and $\gamma = vp^n\sqrt{p}$ for some integers u and v. Therefore

$$x\, a^{-up^n}\, b^{-vp^n} = \begin{pmatrix} 1+\alpha, & \beta \\ \gamma, & 1+\delta \end{pmatrix}\begin{pmatrix} 1, & -up^n\sqrt{p} \\ 0, & 1 \end{pmatrix}\begin{pmatrix} 1, & 0 \\ -vp^n\sqrt{p}, & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1+\alpha+\alpha uvp^{2n+1}, & -\alpha up^n\sqrt{p} \\ -\delta vp^n\sqrt{p}+\gamma uvp^{2n+1}, & 1-\gamma up^n\sqrt{p}+\delta \end{pmatrix}$$

clearly belongs to A_{2n+2}. Thus the homomorphism $A \to A/A_{2n+2}$ maps $x \to \bar{x}$ where $\bar{x}\bar{a}^{-u}\bar{b}^{-v} = 1$. That is, $A_{2n+1}/A_{2n+2} = < \bar{a}, \bar{b} >$, and the proof is complete.

The following three equations will be used to determine the derived series of the group A.

Let $h(s,t) = a^{p^s} b^{p^t} a^{-p^s} b^{-p^t}$. Then

$$\text{(I)} \qquad h(s,t) = \begin{pmatrix} 1 + p^{s+t+1} + p^{2s+2t+2}, & -p^{2s+t+1}\sqrt{p} \\ p^{s+2t+1}\sqrt{p}, & 1 - p^{s+t+1} \end{pmatrix}.$$

Also,

$$\text{(II)} \qquad a^{p^q}\, h(s,t)\, a^{-p^q}\, h(s,t)^{-1} = \begin{pmatrix} \alpha_{11}, & \alpha_{12} \\ \alpha_{21}, & \alpha_{22} \end{pmatrix}$$

where

$\alpha_{11} = 1 + p^{s+2t+q+2} + p^{2s+3t+q+3} + p^{2s+4t+2q+4} + p^{3s+4t+q+4}$,

$$\alpha_{12} = -2p^{s+t+q+1}\sqrt{p} - p^{s+2t+q+2}\sqrt{p}\,(p^q + p^{s+t+q+1} + 3p^s + 2p^{2s+t+1} + p^{2s+2t+q+2} + p^{3s+2t+2}),$$

$$\alpha_{21} = p^{2s+4t+q+3}\sqrt{p},$$

and

$$\alpha_{22} = 1 - p^{s+2t+q+2} - p^{2s+3t+q+3} - p^{3s+4t+q+4}.$$

The corresponding identity for b is given by

$$\text{(III)} \qquad b^{p^q}\,h(s,t)\,b^{-p^q}\,h(s,t)^{-1} = \begin{pmatrix} \beta_{11}, & \beta_{12} \\ \beta_{21}, & \beta_{22} \end{pmatrix}$$

where

$$\beta_{11} = 1 + p^{2s+t+q+2} - p^{3s+2t+q+3},$$

$$\beta_{12} = p^{4s+2t+q+3}\sqrt{p},$$

$$\beta_{21} = 2p^{s+t+q+1}\sqrt{p} - p^{2s+t+q+2}\sqrt{p}\left(p^t - p^q + p^{s+t+q+1}\right),$$

and

$$\beta_{22} = 1 - p^{2s+t+q+2} + p^{3s+2t+q+3} + p^{4s+2t+2q+4}.$$

Lemma 8. Suppose $p \neq 2$. Then

(1) the homomorphism $A \to A/A_{2s+2t+3}$ maps $h(s,t)$ on a generator of the cyclic group $A_{2s+2t+2}/A_{2s+2t+3}$ for every $s,\ t \geq 0$;

(2) the homomorphism $A \to A/A_{2s+2t+2q+4}$ maps $a^{p^q}h(s,t)a^{-p^q}h(s,t)^{-1}$ and $b^{p^q}h(s,t)b^{-p^q}h(s,t)^{-1}$ on a complete set of generators of $A_{2s+2t+2q+3}/A_{2s+2t+2q+4}$ for every $s,\ t,\ q \geq 0$.

Proof of (1). This is an immediate consequence of equation I and statement (1) of Lemma 7.

Proof of (2). Equation II and Lemma 6 imply that

$$a^{p^q} h(s,t)\, a^{-p^q} h(s,t)^{-1} \equiv a^{-2p^{s+t+q+1}} \qquad \text{modulo } A_{2s+2t+2q+4}.$$

Similarly, using III,

$$b^{p^q} h(s,t)\, b^{-p^q} h(s,t)^{-1} \equiv b^{2p^{s+t+q+1}} \qquad \text{modulo } A_{2s+2t+2q+4}.$$

The proof now follows from statement (2) of Lemma 7, since $p \neq 2$.

Lemma 9. Suppose $p \neq 2$. Define $f(n)$ for every positive integer n as follows: $f(1) = 2$; if $f(n)$ is even, then $f(n+1) = 2f(n) + 1$; if $f(n)$ is odd, then $f(n+1) = 2f(n)$. Then $A_{f(n)} \subseteq A^{(n)} A_k$ for every $k \geq 1$.

Proof: Clearly $h(0,t)$, $ah(0,t)\, a^{-1} h(0,t)^{-1}$, and $bh(0,t)b^{-1}h(0,t)^{-1}$ belong to $A^{(1)}$ for every $t \geq 0$. Take $s = q = 0$ in Lemma 8. Then, for $m \geq 2$, $A^{(1)}$ is seen to contain elements mapped by the homomorphism $A \to A/A_{m+1}$ on a complete set of generators of A_m/A_{m+1}. It follows from Lemma 2 that $A_2 \subseteq A^{(1)} A_k$ for every $k \geq 1$. That is, $A_{f(1)} \subseteq A^{(1)} A_k$.

Let n be chosen such that $A_{f(n)} \subseteq A^{(n)} A_k$ for every $k \geq 1$. The lemma will follow by induction if it is shown that $A_{f(n+1)} \subseteq A^{(n+1)} A_k$ for every $k \geq 1$. But, if $A_{f(n)} \subseteq A^{(n)} A_k$, then $A^{(1)}_{f(n)} \subseteq \left(A^{(n)} A_k\right)^{(1)} \subseteq A^{(n+1)} A_k$ since A_k is normal in A. Thus $A^{(1)}_{f(n)} A_k \subseteq A^{(n+1)} A_k$, hence it will suffice to show that $A_{f(n+1)} \subseteq A^{(1)}_{f(n)} A_k$ for every $k \geq 1$.

If $f(n)$ is even, say $f(n) = 2m$, then $a^{p^{m+k}}$, $b^{p^{m+k}}$, and

$h(0,m-1)$ belong to $A_{f(n)} = A_{2m}$ whenever $k \geq 0$. Thus $h(m+k,m)$, $a^{p^{m+k}} h(0,m-1)a^{-p^{m+k}} h(0,m-1)^{-1}$, and $b^{p^{m+k}} h(0,m-1)b^{-p^{m+k}} h(0,m-1)^{-1}$ belong to $A^{(1)}_{f(n)} = A^{(1)}_{2m}$ for every $k \geq 0$. Therefore, whenever $w \geq 4m + 1$, it follows from Lemma 8 that $A^{(1)}_{f(n)}$ contains elements mapped by the homomorphism $A \to A/A_{w+1}$ on a complete set of generators of A_w/A_{w+1}. Thus, by Lemma 2, $A_{4m+1} \subseteq A^{(1)}_{f(n)}A_k$ for every $k \geq 1$; that is, $A_{f(n+1)} \subseteq A^{(1)}_{f(n)}A_k$.

If $f(n)$ is odd, say $f(n) = 2m + 1$, then $a^{p^{m+k}}$, $b^{p^{m+k}}$, and $h(0,m)$ belong to $A_{f(n)}$ for every $k \geq 0$. Thus $h(m+k,m)$, $a^{p^{m+k}} h(0,m)a^{-p^{m+k}} h(0,m)^{-1}$, and $b^{p^{m+k}} h(0,m)b^{-p^{m+k}} h(0,m)^{-1}$ belong to $A^{(1)}_{f(n)}$. Therefore, whenever $w \geq 4m + 2$, it follows from Lemma 8 that $A^{(1)}_{f(n)}$ contains elements mapped by the homomorphism $A \to A/A_{w+1}$ on a complete set of generators of A_w/A_{w+1}. Thus, by Lemma 2, $A_{4m+2} \subseteq A^{(1)}_{f(n)} A_k$ for every $k \geq 1$; that is, $A_{f(n+1)} \subseteq A^{(1)}_{f(n)} A_k$. This completes the proof.

Proof of Theorem 3: Let $G_n = A/A^{(n)}A_{f(n)}$ where $f(n)$ is the function defined in Lemma 9. It follows from Lemma 9 and Theorem 2 that $G_n \cong G_{n+1}/G^{(n)}_{n+1}$. Clearly $G_1 = A/A_2$ has type (p,p). If it is shown that $G^{(n)}_{n+1} \neq \langle 1 \rangle$ the proof will follow from Theorem 1.

Let k be the smallest integer such that $A_k \cap A^{(n)}$ contains an element, say x, which does not belong to $A_{k+1} \cap A^{(n)}$. Then $A^{(n)} \subseteq A_k$, and $A^{(n+1)} \subseteq (A_k,A_k)$. By Lemma 4, $(A_k,A_k) \subseteq A_{2k}$. Thus $A^{(n+1)} \subseteq A_{2k} \subseteq A_{k+1}$, and $A^{(n+1)}A_{k+1} = A_{k+1}$. Therefore, since $x \notin A_{k+1}$, $x \notin A^{(n+1)}$ $A^{(n+1)}A_{k+1} \supseteq A^{(n+1)}A_{f(n+1)}$. It follows from the proof of Theorem 2 that $G_{n+1}^{(n)} = A^{(n)}A_{f(n)}/A^{(n+1)}A_{f(n+1)}$. Thus $G_{n+1}^{(n)} \neq \langle 1 \rangle$ since $x \in A^{(n)}A_{f(n)}$ and $x \notin A^{(n+1)}A_{f(n+1)}$. This completes the proof.

An analogue of Lemma 8, for the case $p = 2$, is needed in the proof of Theorem 4.

Lemma 10. Suppose $p = 2$. Then

(1) the homomorphism $A \to A/A_{2s+2t+3}$ maps $h(s,t)$ on a generator of $A_{2s+2t+2}/A_{2s+2t+3}$ whenever $s, t \geq 0$;

(2) the homomorphism $A \to A/A_{2s+2t+2q+6}$ maps

$a^{p^q}h(s,t)a^{-p^q}h(s,t)^{-1}$ and $b^{p^q}h(t,s)b^{-p^q}h(t,s)^{-1}$ on a complete set of generators of $A_{2s+2t+2q+5}/A_{2s+2t+2q+6}$ whenever $t \geq 1$, $s, q \geq 0$.

Proof of (1): This is an immediate consequence of equation I and statement (1) of Lemma 7.

Proof of (2): Equation II and Lemma 6 imply that

$$a^{p^q}h(s,t)a^{-p^q}h(s,t)^{-1} \equiv a^{-2^{s+t+q+2}} \quad \text{modulo } A_{2s+2t+2q+6}.$$

Similarly, by III and Lemma 6,

$$b^{p^q}h(s,t)b^{-p^q}h(s,t)^{-1} \equiv b^{2^{s+t+q+2}} \quad \text{modulo } A_{2s+2t+2q+6}.$$

The proof now follows from statement (2) of Lemma 7.

The next lemma gives a sharper version of Lemma 4 for the special case $p = 2$.

Lemma 11. If $p = 2$, then $(A_1, A_{2m}) \subseteq A_{2m+2}$.

Proof: It follows from Lemma 7 and equation I that $A_{2m}=\langle h(0,m-1)\rangle A_{2m+1}$. By Lemma 4, $(A_1,A_{2m+1}) \subseteq A_{2m+2}$. Since $A_1 = \langle a,b \rangle$ it follows from equations II and III that $(A_1,\langle h(0,m-1)\rangle) \subseteq A_{2m+2}$. The proof now follows from the commutator identity

$$(x,yz) = (x,y)\ (x,z)\ ((z,x),y).$$

Lemma 12: Let $p = 2$. Define $f(n)$ for every positive integer n as follows: $f(1) = 6$, and $f(n+1) = 2f(n) + 2$ for $n \geq 1$. Then $A_{f(n)} \subseteq A^{(n)}A_k$ for every $k \geq 1$.

Proof: If $m \geq 6$ then, by Lemma 10, $A^{(1)}$ contains elements mapped on a complete set of generators of A_m/A_{m+1} by the homomorphism $A \to A/A_{m+1}$. Thus, by Lemma 2, $A_6 \subseteq A^{(1)}A_k$ for every $k \geq 1$.

Let n be chosen such that $A_{f(n)} \subseteq A^{(n)}A_k$ for every $k \geq 1$. The proof will follow by induction if it is shown that $A_{f(n+1)} \subseteq A^{(n+1)}A_k$ for every $k \geq 1$. But, if $A_{f(n)} \subseteq A^{(n)}A_k$, then $A^{(1)}_{f(n)} \subseteq A^{(n+1)}A_k$ since A_k is normal in A. Thus

$$A^{(1)}_{f(n)}A_k \subseteq \left(A^{(n+1)}A_k\right) A_k = A^{(n+1)}A_k,$$

and it will suffice to show that $A_{f(n+1)} \subseteq A^{(1)}_{f(n)}A_k$ for every $k \geq 1$.

By definition, $f(n)$ is an even number, say $2m$. Therefore, by I, $a^{p^{m+k}}$, $b^{p^{m+k}}$, $h(m-1,0)$, and $h(0,m-1)$ belong to $A_{f(n)} = A_{2m}$ for every $k \geq 0$. Thus $h(m+k,m)$, $a^{p^{m+k}}h(0,m-1)a^{-p^{m+k}}h(0,m-1)^{-1}$, and $b^{p^{m+k}}h(m-1,0)b^{-p^{m+k}}h(m-1,0)^{-1}$ belong to $A^{(1)}_{f(n)} = A^{(1)}_{2m}$ for every $k \geq 0$. Therefore, whenever $w \geq 4m + 2$, it follows from Lemma 10 that $A^{(1)}_{f(n)}$ contains elements mapped by the homomorphism $A \to A/A_{w+1}$ on a complete set of generators of A_w/A_{w+1}. Thus, by Lemma 2, $A_{4m+2} \subseteq A^{(1)}_{f(n)} A_k$ for every $k \geq 1$. This is just the statement that $A_{f(n+1)} \subseteq A^{(1)}_{f(n)} A_k$, and the proof is complete.

<u>Lemma 13. Let</u> $p = 2$. <u>Then</u> $A/A^{(1)}A_6$ <u>is an abelian group of type</u> $(2^2,2^3)$.

<u>Proof</u>: It is clear that $A/A^{(1)}A_6$ is an abelian 2-group. The order of A/A_6 is, by Lemma 7, equal to 2^8. The order of $A^{(1)}A_6/A_6$ will be shown to be 2^3. Thus the order of $A/A^{(1)}A_6$ is 2^5. Since $A = < a,b >$, and a^8, b^8 both belong to A_6, no element of the abelian group $A/A^{(1)}A_6$ can have order greater than 8. Thus this group, having order 2^5, must have 2 generators. The lemma will follow, since an abelian 2-group having two generators, order 2^5, and no elements of order greater than 2^3, must have type $(2^2,2^3)$.

Let $\gamma_i(A)$ be the subgroup of A defined in Lemma 3. Since $A = < a,b >$, it follows from Lemma 3 that

$$\gamma_2(A) = < h, \gamma_3(A) >,$$

where $h = h(0,0) = aba^{-1}b^{-1}$, and

$$\gamma_3(A) = < aha^{-1}h^{-1},\ bhb^{-1}h^{-1},\ \gamma_4(A) >.$$

By Lemma 4, $\gamma_2(A) = (A_1,A_1) \subseteq A_2$; hence, by Lemma 11,

$$\gamma_3(A) = (A, \gamma_2(A)) \subseteq (A_1,A_2) \subseteq A_4,$$

and

$$\gamma_4(A) = (A, \gamma_3(A)) \subseteq (A_1,A_4) \subseteq A_6.$$

Thus $\gamma_2(A) = < h, aha^{-1}h^{-1}, bhb^{-1}h^{-1}, \gamma_4(A) >$ is included in $< h, aha^{-1}h^{-1}, bhb^{-1}h^{-1}, A_6 >$. Note that $\gamma_2(A) = A^{(1)}$, hence $A^{(1)}A_6/A_6$ is generated by images of h, $aha^{-1}h^{-1}$, and $bhb^{-1}h^{-1}$ in the homomorphism $A \to A/A_6$.

By equation I,

$$h = h(0,0) = \begin{pmatrix} 1 + 2 + 4, & -2\sqrt{2} \\ 2\sqrt{2} &, \ 1 - 2 \end{pmatrix} \varepsilon A_2 - A_3,$$

hence

$$h^2 = \begin{pmatrix} 1 + 5\cdot 2^3, & -3\cdot 2^2\sqrt{2} \\ 3\cdot 2^2\sqrt{2}, & 1 - 2^3 \end{pmatrix} \varepsilon A_5 - A_6,$$

and $h^4 \varepsilon A_6$. Since, by Lemma 4, $(A_1, A_5) \subseteq A_6$, the group $< h^2 > A_6$ is normal in A. Clearly $< h^2 > A_6/A_6$ has order 2. It remains to show that $A^{(1)}A_6/< h^2 > A_6$ has order 4.

It is easy to see that the square of

$$aha^{-1}h^{-1} = \begin{pmatrix} 1 + 4\cdot 11, & -4\cdot 19\sqrt{2} \\ 8\sqrt{2} &, \ 1 - 4\cdot 7 \end{pmatrix}$$

is in A_6. Also, h and $aha^{-1}h^{-1}$ map on independent generators of $A^{(1)}A_6/< h^2 > A_6$, since $(aha^{-1}h^{-1})\, h^{-1} \notin A_5$ and $A_5 \supset < h^2 > A_6$. But

$$bhb^{-1}h^{-1} = \begin{pmatrix} 1 - 4, & 8\sqrt{2} \\ -4\sqrt{2}, & 1 + 4\cdot 5 \end{pmatrix},$$

and

$$(bhb^{-1}h^{-1})(aha^{-1}h^{-1}) = \begin{pmatrix} 1 - 8, & 12\sqrt{2} \\ -12\sqrt{2}, & 41 \end{pmatrix} = h^{-2}.$$

That is, $aha^{-1}h^{-1}$ and $bhb^{-1}h^{-1}$ map onto the same element of

$A^{(1)}A_6/\langle h^2\rangle A_6$. Also, $(aha^{-1}h^{-1})\,h = aha^{-1}$, hence $(aha^{-1}h^{-1})\,h$ has order 2 modulo $\langle h^2\rangle A_6$. Thus $A^{(1)}A_6/\langle h^2\rangle A_6$ has two independent generators of order 2 whose product has order 2, hence the group has order 4. This completes the proof.

Proof of Theorem 4: Let $G_n = A/A^{(n)}A_{f(n)}$ where $p = 2$ and $f(n)$ is the function defined in Lemma 12. It follows from Lemma 12 and Theorem 2 that $G_n \cong G_{n+1}/G_{n+1}^{(n)}$. By Lemma 13, G_1 has type $(2^2, 2^3)$. The argument used in the proof of Theorem 3 shows that $G_{n+1}^{(n)} \neq \langle 1\rangle$. Theorem 4 is now an immediate consequence of Theorem 1.

Remark. The full strength of Lemma 13 is not needed for the proof of Theorem 4. It would suffice to know that $A/A^{(1)}A_6$ has type $(2^n, 2^m)$ for $n \leq 2$, $m \leq 3$. The exact type of $A/A^{(1)}A_6$ was determined in order to show that Theorem 4 is the strongest result obtainable from the group A.

Refinement of an Inequality of P. Hall.

The groups A_n can be used to obtain a refinement of an inequality of P. Hall. This inequality is contained in the following theorem [4, Theorem 2.57]: *If $p \neq 2$ and G is a p-group of minimal order for which $G^{(n)} \neq \langle 1\rangle$, then $|G|$ (the order of G) satisfies*

$$p^{2^n+n} \leq |G| \leq p^{2^{n-1}(2^n+1)}.$$

The upper bound of this inequality was refined by N. Itô [4] to $p^{3\cdot 2^n}$. An additional refinement is given by the next theorem.

Theorem 5: *If* $p \neq 2$ *and* G *is a* p-*group of minimal order for which* $G^{(n)} \neq \langle 1 \rangle$, *then* $|G|$ *satisfies*

$$p^{2^n+n} \leq |G| \leq p^{2^{n+1}-1}.$$

Remark. It is interesting to note that $p^{2^{n+1}-1}$ is precisely the upper bound found by Hall in the special case $p = 2$.

Proof of Theorem 5: Suppose $p \neq 2$ and let $f(n)$ be the function defined in Lemma 9. It is clear that, for any fixed $n \geq 1$, a normal subgroup H of $A_{f(n)}$ can be found such that $|A_{f(n)}/H| = p$ and $H \supseteq A_{f(n)+1}$. Since $(A_1, H) \subseteq (A_1, A_{f(n)}) \subseteq A_{f(n)+1} \subseteq H$, it follows that H is normal in A. The required refinement of Hall's inequality will be obtained by showing that $|A/H| = p^{2^{n+1}-1}$ and $(A/H)^{(n)} \neq \langle 1 \rangle$. Theorem 5 will then follow from the theorem of Hall.

By Lemma 9, $A_{f(m)} \subseteq A^{(m)}A_k$ for every m, $k \geq 1$. Consequently, $(A/H)^{(1)} = A^{(1)}H/H \supseteq A^{(1)}A_{f(1)}/H$ since $A_{f(1)} \subseteq A^{(1)}A_{f(n+1)}$ and $H \supseteq A_{f(n+1)}$. Suppose $(A/H)^{(k)} \supseteq A^{(k)}A_{f(k)}/H$. Then
$(A/H)^{(k+1)} \supseteq (A^{(k)}A_{f(k)})^{(1)}H/H$. But
$(A^{(k)}A_{f(k)})^{(1)}H \supseteq A^{(k+1)}A^{(1)}_{f(k)}H \supseteq A^{(k+1)}A_{f(k+1)}$, hence
$(A/H)^{(k+1)} \supseteq A^{(k+1)}A_{f(k+1)}/H$. Therefore, by induction,
$(A/H)^{(n)} \supseteq A^{(n)}A_{f(n)}/H$, which is not the identity group since
$|A_{f(n)}/H| = p$.

It follows from the definition of $f(n)$ that

$$f(2k+1) = 2 + 2^3 + 2^5 + \dots + 2^{2k+1} = \frac{2^{2k+3}-2}{3} \qquad \text{for} \quad k \geq 0,$$

and

$$f(2k) = 1 + 2^2 + 2^4 + \cdots + 2^{2k} = \frac{2^{2k+2} - 1}{3} \quad \text{for} \quad k \geq 1.$$

It is easy to see from Lemma 7 that

$$|A/A_m| = p^{3 \cdot \frac{m-1}{2}} \quad \text{if } m \text{ is odd,}$$

and

$$|A/A_m| = p^{3 \cdot \frac{m}{2} - 1} \quad \text{if } m \text{ is even.}$$

Thus, if n is even, $f(n)$ is odd, and

$$|A/A_{f(n)}| = p^{\frac{3}{2}\left(\frac{2^{n+2}-1}{3} - 1\right)} = p^{2^{n+1}-2}.$$

If n is odd, then $f(n)$ is even, and

$$|A/A_{f(n)}| = p^{\frac{3}{2}\left(\frac{2^{n+2}-2}{3}\right) - 1} = p^{2^{n+1}-2}.$$

That is, $|A/A_{f(n)}| = p^{2^{n+1}-2}$ for $n = 1, 2, \ldots$. But $|A_{f(n)}/H| = p$, hence $|A/H| = p^{2^{n+1}-1}$. This completes the proof.

Chapter 4

Let G_1 be an arbitrary abelian 2-group which contains a subgroup having one of the types $(2^2,2^2,2^2)$, $(2,2,2^2,2^2)$, or $(2,2,2,2,2)$. An infinite chain of 2-groups $G_1, G_2, \ldots$ will be constructed such that $G_n \cong G_{n+1}/G_{n+1}^{(n)}$ and $G_{n+1}^{(n)} \neq <1>$.

The method of construction will be similar to that used in Chapter 3. However, instead of considering the group A, three new groups are introduced. The notation of Chapter 2 is used. The prime p used in the definition of R and P is assumed to be 2.

<u>Definition 3</u>. Let $c = \begin{pmatrix} 1+\sqrt{2}, & 0 \\ 0, & 1+\sqrt{2}-2 \end{pmatrix}$, $u = \begin{pmatrix} 1, & 2 \\ 0, & 1 \end{pmatrix}$, and $v = \begin{pmatrix} 1, & 0 \\ 2, & 1 \end{pmatrix}$. Groups B, C, and D are defined as follows:

$$B = < A, c >,$$

$$C = < B, u >,$$

$$\text{and} \quad D = < C, v >.$$

<u>Definition 4</u>. The subgroup of D consisting of all matrices $x \in D$ such that

$$x - I_2 \equiv 0_2 \text{ modulo } P_2^n, \qquad n \geq 1,$$

is denoted by D_n. Subgroups B_n and C_n of B and C, respectively, are defined similarly. That is, $B_n = B \cap D_n$; $C_n = C \cap D_n$.

<u>Lemma 14</u>: $(B_n, B_m) \subseteq B_{n+m}$; $(C_n, C_m) \subseteq C_{n+m}$; $(D_n, D_m) \subseteq D_{n+m}$.

<u>Proof</u>: This is an immediate consequence of Lemma 1 and Definition 4.

Lemma 15: B_n is normal in B; C_n is normal in C; D_n is normal in D.

Proof: This follows from Lemma 14.

The next lemma will be used to determine generators of B_n/B_{n+1}, C_n/C_{n+1}, and D_n/D_{n+1} for $n = 1, 2, \ldots$.

Lemma 16: Let H be a group of 2×2 matrices with elements in R. Let H_n, for $n = 1, 2, \ldots$, be the subgroup of H consisting of all matrices $X \in H$ such that $\det X = 1$ and $X - I_2 \equiv 0_2$ modulo P_2^n. Suppose H_n contains elements X, Y, Z such that

$$X - \theta \equiv 0_2 \text{ modulo } P_2^{n+1},$$

$$Y - \phi \equiv 0_2 \text{ modulo } P_2^{n+1},$$

$$\text{and } Z - \psi \equiv 0_2 \text{ modulo } P_2^{n+1},$$

where $\theta = \begin{pmatrix} 1, & (\sqrt{2})^n \\ 0, & 1 \end{pmatrix}$, $\phi = \begin{pmatrix} 1, & 0 \\ (\sqrt{2})^n, & 1 \end{pmatrix}$, and

$\psi = \begin{pmatrix} 1 + (\sqrt{2})^n, & 0 \\ 0, & 1 + (\sqrt{2})^n \end{pmatrix}$. Then $H_n = \langle X, Y, Z, H_{n+1} \rangle$, and $H_n : H_{n+1} = 8$.

Proof: It is easy to see that

$$X^r Y^s Z^t - \theta^r \phi^s \psi^t \equiv 0_2 \text{ modulo } P_2^{n+1}$$

for any integers r, s, and t. Let W be an arbitrary element of $H_n - H_{n+1}$. Then

$$W = \begin{pmatrix} 1+\alpha, & \beta \\ \gamma, & 1+\delta \end{pmatrix}$$

where $\alpha \equiv \alpha_1 (\sqrt{2})^n$ modulo $(\sqrt{2})^{n+1}$,

$\beta \equiv \beta_1 (\sqrt{2})^n$ modulo $(\sqrt{2})^{n+1}$,

$\gamma \equiv \gamma_1 (\sqrt{2})^n$ modulo $(\sqrt{2})^{n+1}$,

and $\delta \equiv \delta_1 (\sqrt{2})^n$ modulo $(\sqrt{2})^{n+1}$,

for α_1, β_1, γ_1, δ_1 each either 0 or 1. Since $W \varepsilon H_n$, $\det W = 1 + (\alpha+\delta) + \alpha\delta - \beta\gamma = 1$. Therefore $\alpha_1 + \delta_1 \equiv 0$ modulo 2. A simple computation shows that $\theta^{\beta_1} \phi^{\gamma_1} \psi^{\alpha_1} - W \equiv O_2$ modulo P_2^{n+1}. Therefore

$$X^{\beta_1} Y^{\gamma_1} Z^{\alpha_1} - W \equiv O_2 \text{ modulo } P_2^{n+1},$$

and it follows that $H_n = \langle X, Y, Z, H_{n+1} \rangle$.

By Lemma 1, $(H_n, H_n) \subseteq H_{n+1}$, hence $H_n = \langle X^r Y^s Z^t, H_{n+1} \rangle$ where r, s and t range over the integers. It is easy to see that

$$\theta^r \phi^s \psi^t - I_2 \equiv O_2 \text{ modulo } P_2^{n+1}$$

if, and only if, 2 divides each of r, s, t. It follows that $X^r Y^s Z^t \varepsilon H_{n+1}$ if, and only if, 2 divides each of r, s, and t. Therefore $H_n : H_{n+1} = 8$, and the proof is complete.

<u>Lemma 17</u>: <u>Define</u> $f(n)$, <u>for every positive integer</u> n, <u>as follows</u>: $f(1) = 5$, <u>and</u> $f(n+1) = 3f(n) + 4$ <u>for</u> $n \geq 1$. <u>Then, for all positive integers</u> n <u>and</u> k, $B_{f(n)} \subseteq B^{(n)}B_k$; $C_{f(n)} \subseteq C^{(n)}C_k$; $D_{f(n)} \subseteq D^{(n)}D_k$.

Proof: Note that $a^{-2}cac^{-1}a^{-1} = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} = u^2$, and

$b^{-2}c^{-1}bcb^{-1} = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix} = v^2$, belong to B. Thus, for $t \geq 0$, the following three matrices belong to $B^{(1)}$:

$$c\,u^{2^{t+1}}\,c^{-1}\,u^{-2^{t+1}} = \begin{pmatrix} 1, & (2+2\sqrt{2})2^{t+2} \\ 0, & 1 \end{pmatrix},$$

$$c^{-1}\,v^{2^{t+1}}\,c\,v^{-2^{t+1}} = \begin{pmatrix} 1 & , & 0 \\ (2+2\sqrt{2})2^{t+2}, & & 1 \end{pmatrix},$$

and
$$a^{2^{t+2}}\,b\,a^{-2^{t+2}}\,b^{-1} = \begin{pmatrix} 1 + 2^{t+3} + 2^{2t+6}, & -2^{2t+5}\sqrt{2} \\ 2^{t+3}\sqrt{2} \quad , & 1 - 2^{t+3} \end{pmatrix}.$$

Taking these matrices as the elements X, Y, and Z of Lemma 16, with $H = B$ and $H_n = B_n$, it follows from Lemma 16 that, for every $t \geq 0$, $B^{(1)}$ contains elements mapped by the homomorphism $B \to B/B_{2t+7}$ on a complete set of generators of B_{2t+6}/B_{2t+7}. The three matrices

$$c\,a^{2^{t+1}}\,c^{-1}\,a^{-2^{t+1}} = \begin{pmatrix} 1, & (2+2\sqrt{2})2^{t+1}\sqrt{2} \\ 0, & 1 \end{pmatrix},$$

$$c^{-1}\,b^{2^{t+1}}\,c\,b^{-2^{t+1}} = \begin{pmatrix} 1 & , & 0 \\ (2+2\sqrt{2})2^{t+1}, & & 1 \end{pmatrix},$$

and
$$a^{2^t}\,v^2\,a^{-2^t}\,v^{-2} = \begin{pmatrix} 1 + 2^{t+2}\sqrt{2} + 2^{2t+5}, & -2^{2t+3} \\ 2^{t+4}\sqrt{2} \quad , & 1 - 2^{t+2}\sqrt{2} \end{pmatrix},$$

also belong to $B^{(1)}$ for every $t \geq 0$. Taking these three matrices as X, Y, and Z in Lemma 16, and letting $H = B$, $H_n = B_n$, it follows that $B^{(1)}$ contains elements mapped by the homomorphism $B \to B/B_{2t+6}$

on a complete set of generators of B_{2t+5}/B_{2t+6} whenever $t \geq 0$. Combining these results, and using Lemma 2, it is seen that $B^{(1)}B_k \supseteq B_5$ for every $k \geq 1$.

The proof (for B) will follow by induction if it is shown that $B_{f(n)} \subseteq B^{(n)}B_k$ implies $B_{f(n+1)} \subseteq B^{(n+1)}B_k$. If $B_{f(n)} \subseteq B^{(n)}B_k$, then, since B_k is normal in B,

$$B^{(1)}_{f(n)} \subseteq (B^{(n)}B_k)^{(1)} \subseteq B^{(n+1)}B_k. \quad \text{Therefore}$$

$$B^{(1)}_{f(n)}B_k \subseteq (B^{(n+1)}B_k)B_k = B^{(n+1)}B_k,$$

and it will suffice to show that $B_{f(n+1)} \subseteq B^{(1)}_{f(n)}B_k$.

By definition, $f(n)$ is odd, say $f(n) = 2m + 1$ where $m \geq 2$. It is easy to see that $a^{2^{m+t}}$, $b^{2^{m+t}}$, $c^{2^{m+t}}$, $u^{2^{m+t}}$, and $v^{2^{m+t}}$ belong to B_{2m+1} whenever $t \geq 0$.

Since $m \geq 2$, a calculation shows that

$$\left(a^{2^m}, b^{2^m}\right) u^{2^{m+t}} \left(a^{2^m}, b^{2^m}\right)^{-1} u^{-2^{m+t}} \equiv \begin{pmatrix} 1, & 2^{3m+3+t} \\ 0, & 1 \end{pmatrix} \text{ modulo } B_{6m+2t+7},$$

and

$$\left(a^{2^m}, b^{2^m}\right)^{-1} v^{2^{m+t}} \left(a^{2^m}, b^{2^m}\right) v^{-2^{m+t}} \equiv \begin{pmatrix} 1 & , & 0 \\ 2^{3m+t+3}, & & 1 \end{pmatrix} \text{ modulo } B_{6m+2t+7}.$$

Also, by equation I,

$$\left(a^{2^{2m+t}}, b^{2^{m+2}}\right) = \begin{pmatrix} 1 + 2^{3m+t+3} + 2^{6m+2t+6}, & -2^{5m+2t+3}\sqrt{2} \\ 2^{4m+t+5}\sqrt{2} & , \quad 1 - 2^{3m+t+3} \end{pmatrix}.$$

These elements belong to $B^{(1)}_{f(n)} = B^{(1)}_{2m+1}$ whenever $t \geq 0$. Hence, by Lemma 16 (with the above matrices as X, Y, Z and $H = B$, $H_n = B_n$),

$B^{(1)}_{f(n)}$ contains elements mapped by the homomorphism $B \to B/B_{6m+2t+7}$ on a complete set of generators of $B_{6m+2t+6}/B_{6m+2t+7}$.

It follows from Lemma 6 and equations II and III that

$$a^{2^{m+t+1}} h(m,m)\, a^{-2^{m+t+1}} h(m,m)^{-1} \equiv \begin{pmatrix} 1, & -2^{3m+t+3}\sqrt{2} \\ 0, & 1 \end{pmatrix} \text{modulo } B_{6m+2t+8},$$

and

$$b^{2^{m+t+1}} h(m,m)\, b^{-2^{m+t+1}} h(m,m)^{-1} \equiv \begin{pmatrix} 1 & , & 0 \\ 2^{3m+t+3}\sqrt{2}, & & 1 \end{pmatrix} \text{modulo } B_{6m+2t+8}.$$

Another computation gives

$$\left(a^{2^{2m+t+2}}, v^{2^m} \right) = \begin{pmatrix} 1 + 2^{3m+t+3}\sqrt{2} + 2^{6m+2t+7}, & -2^{5m+2t+6} \\ 2^{4m+t+4}\sqrt{2} & , \quad 1 - 2^{3m+t+3}\sqrt{2} \end{pmatrix}.$$

These elements belong to $B^{(1)}_{2m+1}$ whenever $t \geq 0$. Hence, by Lemma 16 (with the above matrices as X, Y, Z and $H = B$, $H_n = B_n$), $B^{(1)}_{f(n)} = B^{(1)}_{2m+1}$ contains elements mapped by the homomorphism $B \to B/B_{6m+2t+8}$ on a complete set of generators of $B_{6m+2t+7}/B_{6m+2t+8}$. Thus $B^{(1)}_{f(n)}$ contains elements mapped by the homomorphism $B \to B/B_{w+1}$ on a complete set of generators of B_w/B_{w+1} whenever $w \geq 6m + 6$. It follows from Lemma 2 that $B^{(1)}_{f(n)}B_k \supseteq B_{6m+6}$ for every $k \geq 1$. In particular, $B^{(1)}_{f(n)}B_k \supseteq B_{6m+7} = B_{3f(n)+4} = B_{f(n+1)}$. This completes the proof of the statement $B_{f(n)} \subseteq B^{(n)}B_k$.

The above proof remains valid if B is replaced, throughout, by either C or D. The lemma follows.

<u>Theorem 6:</u> <u>Let</u> G_1 <u>be an arbitrary abelian</u> 2-<u>group which contains a subgroup of one of the types</u> $(2^2, 2^2, 2^2)$, $(2, 2, 2^2, 2^2)$, <u>or</u> $(2, 2, 2, 2, 2)$. <u>Then there exists an infinite chain of</u> 2-<u>groups</u> $G_1, G_2, \ldots$ <u>such that</u> $G_n \cong G_{n+1}/G_{n+1}^{(n)}$ <u>and</u> $G_{n+1}^{(n)} \neq \langle 1 \rangle$.

<u>Proof</u>: Let $H_n = B/B^{(n)}B_{f(n)}$, $K_n = C/C^{(n)}C_{f(n)}$, and $L_n = D/D^{(n)}D_{f(n)}$. It follows from Lemma 17 and Theorem 2 that $H_n \cong H_{n+1}/H_{n+1}^{(n)}$, $K_n \cong K_{n+1}/K_{n+1}^{(n)}$, and $L_n \cong L_{n+1}/L_{n+1}^{(n)}$. The argument used in the proof of Theorem 3 shows that $H_{n+1}^{(n)} \neq \langle 1 \rangle$, $K_{n+1}^{(n)} \neq \langle 1 \rangle$, and $L_{n+1}^{(n)} \neq \langle 1 \rangle$. Theorem 5 will follow from Theorem 1 if it is shown that: H_1 can be generated by three elements of order less than or equal to 4; K_1 can be generated by four elements, two of which have order 2 while the remaining two generators have order less than or equal to 4; L_1 can be generated by five elements of order 2.

Since $B = \langle a, b, c \rangle$, where a^4, b^4, and c^4 belong to $B_5 = B_{f(1)}$, the group $H_1 = B/B^{(1)}B_{f(1)}$ can be generated by three elements of order less than or equal to 4.

Since $C = \langle a, b, c, u \rangle$, the group $K_1 = C/C^{(1)}C_5$ can be generated by four elements. It is easy to see that b^4 and c^4 belong to C_5. But

$$u^2(c, u) = \begin{pmatrix} 1, & 4\sqrt{2} + 8 \\ 0, & 1 \end{pmatrix} \varepsilon\, C_5 \subseteq C^{(1)}C_5,$$

and

$$a^2(c, a) = (c, u),$$

hence u^2 and a^2 belong to $C^{(1)}C_5$. Thus two of these generators have order 2, while the remaining two generators have order less than or equal to 4.

Since $D = < a,b,c,u,v >$, the group $L_1 = D/D^{(1)}D_5$ can be generated by five elements. Clearly $C^{(1)}C_5 \subseteq D^{(1)}D_5$, hence u^2 and a^2 belong to $D^{(1)}D_5$. Also, $v^2(c^{-1},v) = \begin{pmatrix} 1 , & 0 \\ 4\sqrt{2}+8, & 1 \end{pmatrix} \varepsilon D_5 \subseteq D^{(1)}D_5$, and $b^2(c^{-1},b) = (c^{-1},v)$. Therefore b^2 and v^2 belong to $D^{(1)}D_5$.

Note that $u^2 = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}$, $v^2 = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}$, and $(a^2,b) = \begin{pmatrix} 21 , & -8\sqrt{2} \\ 4\sqrt{2}, & 1-4 \end{pmatrix}$. Thus, by Lemma 16,

$$D_4 = < u^2,v^2,(a^2,b),D_5 >.$$

Similarly,

$$D_3 = < a^2,b^2,(a,v),D_4 >.$$

Since a^2,b^2,u^2, and v^2 belong to $D^{(1)}D_5$, it follows that $D^{(1)}D_5 \supseteq D_3$. It is easy to see that

$$c^2(a,b) = \begin{pmatrix} 21+14\sqrt{2}, & -6\sqrt{2}-8 \\ 6\sqrt{2}-8 , & -3+2\sqrt{2} \end{pmatrix} \varepsilon D_3.$$

Thus $c^2 \varepsilon D^{(1)}D_5$, and hence L_1 can be generated by five elements of order 2. This completes the proof of Theorem 6.

Remark. An argument similar to that used in the proof of Lemma 13 shows that $B/B^{(1)}B_5$ has type $(2^2,2^2,2^2)$, $C/C^{(1)}C_5$ has type $(2,2,2^2,2^2)$, and $D/D^{(1)}D_5$ has type $(2,2,2,2,2)$. Thus Theorem 6 is the strongest result obtainable from the groups B, C, and D. Whether Theorem 6 is the best possible result, for G_1 a 2-group with at least three generators, remains an open question.

REFERENCES

[1] N. Blackburn, On prime power groups with two generators, Proc. Camb. Phil. Soc. Vol. 54 (1958), pp. 327-337.

[2] N. Blackburn, On prime power groups in which the derived group has two generators, Proc. Camb. Phil. Soc. Vol. 53 (1957), pp. 19-27.

[3] W. Burnside, Some properties of groups whose orders are powers of primes, Proc. Lond. Math. Soc. (2), Vol. 11 (1912), pp. 225-245.

[4] P. Hall, A contribution to the theory of groups of prime power order, Proc. Lond. Math. Soc. (2), Vol. 36 (1933), pp. 29-95.

[5] N. Itô, Note on p-groups, Nagoya Math. J. Vol. 1 (1950), pp. 113-116.

[6] W. Magnus, Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring, Math. Ann. Vol. 111 (1935), pp. 259-280.

[7] W. Magnus, Neuere Ergebnisse über auflösbare Gruppen, Jber. Deutsch. Math. Verein. Vol. 47 (1937), pp. 69-79.

[8] A. Scholz and O. Taussky, Die Hauptideale der kubischen Klassenkörper imaginärquadratischer Zahlkörper, Journal für Math. Vol. 171 (1934), pp. 19-41.

[9] O. Taussky, Research Problem 9, Bull. Amer. Math. Soc. Vol. 64 (1958), pp. 124.

[10] O. Taussky, A remark on the class field tower, J. Lond. Math. Soc. Vol. 12 (1937), pp. 82-85.

[11] H. Zassenhaus, Theory of Groups, (trans.) New York, Chelsea, (1949).

[12] H. Zassenhaus, Unpublished.