THE DERIVED SERIES OF A FINITE p-GROUP[1]

BY

CHARLES R. HOBBY

The Galois groups of a class field tower form a chain of finite groups $G_1, G_2, \cdots$, such that G_1 is abelian and $G_n \cong G_{n+1}/G_{n+1}^{(n)}$, where $G_{n+1}^{(n)}$ denotes the n^{th} derived group of G_{n+1}. The class field tower and the chain of groups terminate after n steps if $G_{n+1}^{(n)} = \langle 1 \rangle$. We shall consider the case where all G_n are p-groups. It is known [5] that the chain terminates if G_1 is cyclic, or if $p = 2$ and G_1 has type $(2, 2)$. Olga Taussky (see Magnus [4]) posed the problem of determining whether such a chain of p-groups must always terminate. N. Itô [3] gave a negative answer to this question by constructing an infinite chain of p-groups satisfying the above conditions with G_1 of type (p, p, p) and $p \neq 2$. The question of the existence or nonexistence of infinite chains with G_1 generated by two elements or with $p = 2$ remained open.

The main result of this paper is the following theorem.

THEOREM 1. *Suppose $p \neq 2$, and let G be a noncyclic abelian p-group. Then there exists an infinite chain of p-groups $G_1, G_2, \cdots$, such that*

$$G_1 \cong G, \quad G_n \cong G_{n+1}/G_{n+1}^{(n)}, \quad \text{and} \quad G_{n+1}^{(n)} \neq \langle 1 \rangle.$$

A weaker result is obtained if $p = 2$.

THEOREM 2. *Suppose G is an abelian 2-group which contains a subgroup having one of the types $(2^2, 2^3)$, $(2^2, 2^2, 2^2)$, $(2^2, 2^2, 2, 2)$, or $(2, 2, 2, 2, 2)$. Then there exists an infinite chain of 2-groups $G_1, G_2, \cdots$, such that $G_1 \cong G$, $G_n \cong G_{n+1}/G_{n+1}^{(n)}$, and $G_{n+1}^{(n)} \neq \langle 1 \rangle$.*

As we noted above, the chain $G_1, G_2, \cdots$ terminates if G_1 is cyclic, or if $p = 2$ and G_1 has type $(2, 2)$. The remaining cases not covered by Theorem 2 are undecided. The proof of Theorem 2 is similar to that of Theorem 1 and will not be given here. Full details can be found in the author's thesis [2].

A second question posed by Olga Taussky [6] can be stated as follows. Can a bound on the derived length of a p-group H be determined from the type of $H/H^{(1)}$? Such a bound exists if $H/H^{(1)}$ is cyclic or of type $(2, 2)$. W. Magnus [4] showed that there is no bound if $H/H^{(1)}$ has type $(3, 3, 3)$. A complete answer to this question for $p \neq 2$, and a partial answer for $p = 2$, is given by the next theorem.

THEOREM 3. *Suppose H is a p-group and $G = H/H^{(1)}$. The derived length*

Received June 11, 1960.

[1] This paper contains part of a doctoral thesis written at the California Institute of Technology. The author is indebted to Dr. Olga Taussky Todd for directing this research, Professor Hans Zassenhaus for many helpful suggestions, and the National Science Foundation for financial support.

of H cannot be determined from the type of G if G satisfies the hypothesis of either Theorem 1 or Theorem 2.

Theorem 3 follows immediately from the observation (see the proof of Lemma 1) that $G_1 \cong G_n/G_n^{(1)}$ in the chains of Theorems 1 and 2. Thus there is an infinite chain $G_1, G_2, \cdots$ with $G_n/G_n^{(1)} \cong H/H^{(1)}$ for every n, and $G_n^{(n-1)} \neq \langle 1 \rangle$.

Our first lemma reduces the proof of Theorem 1 to the case where G has type (p, p). We then give an explicit construction of the required chain $G_1, G_2, \cdots$, with G_1 of type (p, p). This construction proceeds as follows. We first introduce an infinite matrix group which we denote by A_1. The derived series of factor groups of A_1 are studied in detail. Then, for each n, we let G_n be a certain finite factor group of A_1. It follows from our discussion of A_1 that the chain $G_1, G_2, \cdots$ has the required properties.

The following notation will be used: $(x, y) = xyx^{-1}y^{-1}$; (X, Y) is the group generated by the set of all (x, y) for $x \in X$ and $y \in Y$; $\langle x, y, \cdots, z \rangle$ is the group generated by $x, y, \cdots, z$; $H^{(n)}$ is the n^{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 odd 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.

LEMMA 1. *Suppose $G_1, G_2, \cdots$ is an infinite chain of p-groups such that G_1 is abelian of type (p, p), $G_n \cong G_{n+1}/G_{n+1}^{(n)}$, and $G_{n+1}^{(n)} \neq \langle 1 \rangle$. Let K be a non-cyclic abelian p-group. Then there exists an infinite chain of p-groups $K_1, K_2, \cdots$, such that $K_1 \cong K$, $K_n \cong K_{n+1}/K_{n+1}^{(n)}$, and $K_{n+1}^{(n)} \neq \langle 1 \rangle$.*

Proof. Write K as $K = S \times T$ where S has two independent generators' say $S = \langle u, v \rangle$. We will construct an infinite chain of p-groups $S_1, S_2, \cdots$, such that $S_1 \cong S$, $S_n \cong S_{n+1}/S_{n+1}^{(n)}$, and $S_{n+1}^{(n)} \neq \langle 1 \rangle$. The lemma will then follow if we let $K_n = S_n \times T$.

Observe that $G_n/G_n^{(1)} = (G_{n+1}/G_{n+1}^{(n)})/(G_{n+1}^{(1)}/G_{n+1}^{(n)}) \cong G_{n+1}/G_{n+1}^{(1)}$; thus $G_n/G_n^{(1)} \cong G_1$ for every n. It follows from the Burnside Basis Theorem [7, page 111] that G_n can be generated by two elements. Let $G_1 = \langle a_1, b_1 \rangle$, and, recursively, let a_{n+1}, b_{n+1} be coset representatives in G_{n+1} of the images of a_n, b_n under the isomorphism $G_n \cong G_{n+1}/G_{n+1}^{(n)}$. Then $G_n = \langle a_n, b_n \rangle$ for every n. Let S_n be the subgroup of $G_n \times S$ which is generated by ua_n and vb_n. Then $S_n^{(t)} = G_n^{(t)}$ for every $t \geqq 1$, and hence $S_{n+1}^{(n)} \neq \langle 1 \rangle$. The mapping $u \leftrightarrow u$, $v \leftrightarrow v$, $a_n \leftrightarrow a_{n+1} S_{n+1}^{(n)}$, $b_n \leftrightarrow b_{n+1} S_{n+1}^{(n)}$ clearly induces an isomorphism between S_n and $S_{n+1}/S_{n+1}^{(n)}$. This completes the proof.

The group A_1

Let A_1 be the group generated by the two matrices

$$a = \begin{pmatrix} 1 & \sqrt{p} \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 1 & 0 \\ \sqrt{p} & 1 \end{pmatrix}.$$

Denote by A_n the set of all $x \in A_1$ such that $x - I_2$ has elements in P^n (i.e.,

$x - I_2 \equiv O_2(P^n))$. It is clear that A_n is a subgroup of A_1, and that $A_1 \supset A_2 \supset \cdots$. It follows from the next lemma that A_n is even normal in A_1.[2]

LEMMA 2. $(A_n, A_m) \subseteq A_{n+m}$.

Proof. Let $x \in A_n$ and $y \in A_m$. Then

$$x - I_2 \equiv O_2(P^n) \quad \text{and} \quad y - I_2 \equiv O_2(P^m).$$

Also,

$$\begin{aligned} xyx^{-1}y^{-1} - I_2 &= (xy - yx)x^{-1}y^{-1} \\ &= [(x - I_2)(y - I_2) - (y - I_2)(x - I_2)]x^{-1}y^{-1}. \end{aligned}$$

Therefore $xyx^{-1}y^{-1} - I_2 \equiv O_2(P^{n+m})$. That is, $(x, y) \in A_{n+m}$.

LEMMA 3. *If $x, y \in A_1$, and if $x - y \equiv O_2(P^n)$, then $xy^{-1} \in A_n$.*

Proof. It follows from $x - y \equiv O_2(P^n)$ that $xy^{-1} - I_2 \equiv O_2(P^n)$; hence $xy^{-1} \in A_n$.

We will need the following relations on commutators of elements of A_1.

$$\text{(I)} \quad (a^{mp^s}, b^{np^t}) = \begin{pmatrix} 1 + mnp^{s+t+1} + m^2n^2p^{2s+2t+2} & -m^2np^{2s+t+1}\sqrt{p} \\ mn^2p^{s+2t+1}\sqrt{p} & 1 - mnp^{s+t+1} \end{pmatrix}.$$

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

$$\text{(III)} \quad (b^{p^q}, (a^{p^s}, b^{p^t})) \equiv b^{2p^{s+t+q+1}} \quad \text{modulo } A_{2s+2t+2q+4}.$$

The first of these relations can be verified by direct computation. The next two follow from a computation of the commutators on the left and an application of Lemma 3.

LEMMA 4. *Every element of A_1 has the form*

$$\begin{pmatrix} 1 + x & y\sqrt{p} \\ u\sqrt{p} & 1 + v \end{pmatrix}$$

where x, y, u, v are integers.

Proof. The generators of A_1 have this form, and it is clearly preserved under multiplication.

We wish to determine the derived series of certain factor groups A_1/A_m of A_1. As a first step, we determine the structure of A_n/A_{n+1} for arbitrary n.

LEMMA 5. (1) $[A_{2k+1}:A_{2k+2}] = p^2$ *and* $A_{2k+1} = \langle A_{2k+2}, a^{p^k}, b^{p^k}\rangle$ *if* $k \geqq 0$.
(2) $[A_{2k}:A_{2k+1}] = p$ *and* $A_{2k} = \langle (a^{mp^{k-1}}, b), A_{2k+1}\rangle$ *if* $k \geqq 1$, *and m is any integer prime to p.*

---

[2] The author wishes to thank Professor Hans Zassenhaus for calling his attention to the group A_1 and for suggesting the present short proof of Lemma 2.

Proof of (1). Observe that a^{p^k} and b^{p^k} are in A_{2k+1}. Also,

$$a^{sp^k} b^{tp^k} = \begin{pmatrix} 1 + stp^{2k+1} & sp^k \sqrt{p} \\ tp^k \sqrt{p} & 1 \end{pmatrix}$$

belongs to A_{2k+2} if, and only if, both of s and t are divisible by p. The result will follow if we show that $A_{2k+1} = \langle A_{2k+2}, a^{p^k}, b^{p^k} \rangle$. Suppose $x \in A_{2k+1}$ where

$$x = \begin{pmatrix} 1 + u & v \\ w & 1 + z \end{pmatrix}.$$

Then u and z are divisible by p^{k+1} since they are integers (Lemma 4) divisible by $p^k\sqrt{p}$. Write $v = sp^k\sqrt{p}$ and $w = tp^k\sqrt{p}$, where s and t are integers. It follows from Lemma 3 that $a^{sp^k}b^{tp^k}x^{-1} \in A_{2k+2}$.

Proof of (2). Suppose $x \in A_{2k}$ where

$$x = \begin{pmatrix} 1 + u & v \\ w & 1 + z \end{pmatrix}.$$

Then w and v are integers multiplied by $\sqrt{p}$ (Lemma 4); hence they belong to P^{2k+1}. By hypothesis, u and z are in P^{2k}. Thus $u = mp^k$ and $z = np^k$ for some integers m and n. Observe that x, as an element of A_1, must have determinant 1. It follows that $m + n \equiv 0\,(p)$. Therefore, by (I) and Lemma 3, $(a^{mp^{k-1}}, b)x^{-1} \in A_{2k+1}$. This shows that A_{2k} is generated by A_{2k+1} and elements of the form $(a^{mp^{k-1}}, b)$. We see from (I) and Lemma 3 that there are precisely p such elements which are distinct modulo A_{2k+1}. Therefore A_{2k}/A_{2k+1} is cyclic of order p. This completes the proof.

The next lemma is rather technical. It will be used in the proof of Lemma 7.

LEMMA 6. *Let N be a normal subgroup of A_1. If $NA_{n+r} \supseteq A_n$ for some n and some $r \geqq 1$, then $NA_{n+m} \supseteq A_n$ for every $m \geqq r$.*

Proof. We proceed by induction on m (where we need only consider $m \geqq 2$), and suppose that $NA_{n+m-1} \supseteq A_n$. The lemma will follow if we show that $NA_{n+m} \supseteq A_{n+m-1}$, for then $NA_{n+m} = N \cdot NA_{n+m} \supseteq NA_{n+m-1} \supseteq A_n$.

Observe that $NA_{n+m-1} \supseteq A_{n+m-2}$ since $NA_{n+m-1} \supseteq A_n$ and $m \geqq 2$. Suppose $n + m - 2 = 2k$. Then, by Lemma 5, $c = (a^{p^{k-1}}, b)$ belongs to NA_{n+m-1}; hence $c = xy$ for some $x \in N$, $y \in A_{n+m-1}$. Since N is normal in A_1 and $(A_1, A_{n+m-1}) \subseteq A_{n+m}$, we have $(a, xy) \equiv (a, x)$ modulo A_{n+m} where $(a, x) \in N$. Similarly, $(b, xy) \equiv (b, x)$ modulo A_{n+m} where $(b, x) \in N$. It now follows from (II), (III), and Lemma 5, that

$$A_{n+m-1} = \langle A_{n+m}, (b, xy), (a, xy) \rangle;$$

hence $A_{n+m-1} \subseteq NA_{n+m}$.

If $n + m - 2 = 2k + 1$, then $a^{p^k} \in A_{n+m-2}$. Therefore $a^{p^k} = xy$ for some $x \in N$, $y \in A_{n+m-1}$. Then $(xy, b) \equiv (x, b)$ modulo A_{n+m}, where $(x, b) \in N$. By Lemma 5, $A_{n+m-1} = A_{2k+2} = \langle A_{n+m}, (x, b) \rangle$; hence $A_{n+m-1} \subseteq NA_{n+m}$. This completes the proof.

LEMMA 7. *Let $g(m) = m + 2[m/2] + 1$, where $[m/2]$ denotes the greatest integer in $m/2$. Then $A_m^{(1)}A_t = A_{g(m)}$ if $t \geqq g(m)$.*

Proof. If $m = 2k$, then, by Lemma 4, A_m/A_{m+1} is cyclic. Therefore $A_m^{(1)} = (A_m, A_{m+1}) \subseteq A_{2m+1} = A_{g(m)}$. Observe that $(a^{p^{k-1}}, b)$, a^{p^k}, and b^{p^k} belong to A_m. It follows from (II) and (III) that $A_m^{(1)}$ contains elements congruent to $a^{-2p^{2k}}$ and $b^{2p^{2k}}$ modulo $A_{4k+2} = A_{2m+2}$. Thus, by Lemma 5, $A_m^{(1)}A_{2m+2} \supseteq A_{2m+1}$ since $p \neq 2$. Therefore, by Lemma 6, $A_m^{(1)}A_t \supseteq A_{g(m)}$ for every $t \geqq g(m)$.

If $m = 2k + 1$, then $A_m^{(1)} = (A_m, A_m) \subseteq A_{2m} = A_{g(m)}$. Also, a^{p^k} and b^{p^k} belong to A_m, so $(a^{p^k}, b^{p^k}) \in A_m^{(1)}$. We see from (I) that (a^{p^k}, b^{p^k}) is congruent to $(a^{p^{2k}}, b)$ modulo A_{4k+3}. Thus, by Lemma 5, $A_m^{(1)}A_{4k+3} \supseteq A_{4k+2}$. It follows from Lemma 6 that $A_m^{(1)}A_t \supseteq A_{4k+2} = A_{g(m)}$ for every $t \geqq g(m)$. This completes the proof.

Let $g(m) = m + 2[m/2] + 1$, and define a new function f on the positive integers by

$$f(1) = 2 = g(1), \qquad f(n) = g(f(n-1)) \quad \text{if} \quad n > 1.$$

Then the next lemma is just a restatement of Lemma 7.

LEMMA 8. *If $t \geqq f(n)$, then $(A_1/A_t)^{(n)} = A_{f(n)}/A_t$.*

We can now prove Theorem 1.

Proof of Theorem 1. Let $G_n = A_1/A_{f(n)}$ for $n = 1, 2, \cdots$. Then, by Lemma 5, $G_1 = A_1/A_2$ is a noncyclic group of order p^2, and consequently G_1 is abelian of type (p, p). By Lemma 8, $G_{n+1}^{(n)} = A_{f(n)}/A_{f(n+1)}$; hence $G_{n+1}/G_{n+1}^{(n)} = (A_1/A_{f(n+1)})/(A_{f(n)}/A_{f(n+1)}) \cong A_1/A_{f(n)} = G_n$. Also,

$$G_{n+1}^{(n)} = A_{f(n)}/A_{f(n+1)} \neq \langle 1 \rangle$$

since $f(n) < f(n+1)$. Theorem 1 now follows from Lemma 1.

Remark 1. We state without proof two further properties of the p-groups A_1/A_n. These properties are easy consequences of (I), (II), (III) and Lemmas 5 and 6.

1. The lower central series of A_1/A_n is $A_1/A_n, A_2/A_n, A_3/A_n, \cdots$.
2. The upper central series of A_1/A_n is $A_{n-1}/A_n, A_{n-2}/A_n, A_{n-3}/A_n, \cdots$.

Remark 2. P. Hall [1, Theorem 2.57] showed that if $p \neq 2$ and if G is a p-group of minimal order for which $G^{(n)} \neq \langle 1 \rangle$, then $|G|$ (the order of G) satisfies

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

The upper bound of this inequality was refined by N. Itô [3] to $p^{3\cdot 2^n}$. An additional refinement can be obtained from the group A_1. To do this, pick a subgroup H of A_1 such that $A_{f(n)+1} \subseteq H \subset A_{f(n)}$ and $[A_{f(n)}:H] = p$. Then H is normal in A_1. If $G = A_1/H$, then $G^{(n)} = A_{f(n)}/H \neq \langle 1 \rangle$. It follows from Lemma 5 and the definition of $f(n)$ that G has order $p^{2^{n+1}-1}$. Therefore the upper bound in Hall's inequality can be reduced to $p^{2^{n+1}-1}$. It is interesting to note that this is precisely the upper bound found by Hall in the special case $p = 2$.

REFERENCES

1. P. HALL, *A contribution to the theory of groups of prime-power order*, Proc. Lond. Math. Soc. (2), vol. 36 (1933), pp. 29–95.
2. C. HOBBY, *The derived series of a p-group*, Thesis, California Institute of Technology, 1960.
3. N. ITÔ, *Note on p-groups*, Nagoya Math. J., vol. 1 (1950), pp. 113–116.
4. W. MAGNUS, *Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring*, Math. Ann., vol. 111 (1935), pp. 259–280.
5. O. TAUSSKY, *A remark on the class field tower*, J. Lond. Math. Soc., vol. 12 (1937), pp. 82–85.
6. ———, *Research Problem 9*, Bull. Amer. Math. Soc., vol. 64 (1958), p. 124.
7. H. ZASSENHAUS, *The theory of groups*, (trans.) New York, Chelsea, 1949.

CALIFORNIA INSTITUTE OF TECHNOLOGY
PASADENA, CALIFORNIA