Note on finite p-groups

Haile Michael Bereda

University Paul Sabatier, Mathematiques 118, Route de Narbonne
31062 Toulouse Cedex 4, France

Abstract: In this note, we consider finite non-abelian p-groups \( p \geq 3 \) in which the derived group is cyclic. As far as we know, these groups have not yet been classified. This will be done in a forthcoming paper.

The notation and terminology employed will be as follows. If \( G \) is a p-group, \( G' \) stands for the derived group of \( G \). A subgroup of \( G \) is of type \( (p,p) \) if it is elementary abelian of order \( p^2 \). \( G \) is said to be regular if for every pair of elements \( a, b \) in \( G \),

\[
(ab)^p = a^pb^pc^p,
\]

Where \( c \) is an element of the derived group of the subgroup generated by \( a \) and \( b \). \([a,b] = a^{-1}b^{-1}ab\) as usual, for \( a, b \) in \( G \). For positive integers \( m \) and \( n \), \( m | n \) means \( m \) divides \( n \). Given a real number \( r \), \( i(r) \) is the integer parts of \( r \). If \( M \) and \( N \) are isomorphic groups, we write \( M \cong N \). \( M_n (n \geq 1) \) is the \( n^{th} \) term of the descending central series of \( M \). \( Z \) is the set of rational integers.

We use the following elementary but basic fact. If \( G \) is a finite nilpotent group, every normal subgroup of \( G \) different from the identity subgroup, \( \{1\} \), intersects the centre \( Z(G) \) of \( G \) non trivially.

We need the following lemmas.
Lemma 1
Let \( a, b \) be pair of elements of a group \( G \).

a) If \([a, b]\) commutes with \( a \), then for all \( n \in \mathbb{Z} \),
\[
[a^n, b] = [a, b]^n.
\]

b) If \([a, b]\) commutes with \( a \) and \( b \), then for all positive integers \( n \),
\[
(ab)^n = a^n b^n [b, a] \binom{n}{2}^n
\]
where \( \binom{n}{2} \) is the binomial coefficient \( \frac{n(n-1)}{2} \).

Proof
(a) We proceed by induction on \( n > 0 \) since \([a^0, b] = [1, b] = 1 = [a, b]^0\). For \( n = 1 \), there is nothing to prove. Suppose \( n > 1 \) and the assertion true for \( n-1 \). Then,
\[
[a^n, b] = [aa^{n-1}, b] = a^{n+1} [a, b] a^{n-1} [a^{n-1}, b] = [a, b] [a^{n-1}, b] = [a, b] [a, b]^{n-1} = [a, b]^n.
\]
Furthermore,
\[
1 = [a^0 a^n, b] = a^0 [a, b] a^n [a^n, b] = a^0 [a, b] a^n [a^n, b] = [a, b] a^n [a^n, b], \text{ hence}
[a^{n}, b] = [a, b]^{n}.
\]

(b) For \( n = 1 \), the assertion is trivial since \( \frac{1}{2} \cdot 0 \) by convention. Suppose \( n > 1 \) and the assertion true for \( n-1 \). Then,
\[
(ab)^n = (ab)^{n-1} ab = a^{n-1} b^{n-1} [b, a] \binom{n-1}{2} ab = a^{n-1} b^{n-1} ab [b, a] \binom{n-1}{2}
\]
\[
= a^{n-1} ab^{n-1} b^{-(n-1)} a^{-1} b^{n-1} ab [b, a] \binom{n-1}{2} = a^{n-1} b^{n-1} [b^{n-1}, a] b [b, a] \binom{n-1}{2}
\]
\[
= a^{n} b^{n-1} [b, a]^{n-1} b [b, a] \binom{n}{2} = a^{n} b^{n} [b, a]^{n} \binom{n}{2}
\]
Lemma 2
Let \(M\) and \(N\) be normal subgroups of a \(p\)-group \(G\) such that \(N \subseteq M\) and \(|M/N| = p^m\). Then, for all integers \(k\) satisfying \(0 \leq k \leq m\), there exists a normal subgroup \(R\) of \(G\) such that \(N \subseteq R \subseteq M\) and \(|R/N| = p^k\).

Proof
Consider the normal series \(\{1\} \subseteq N \subseteq M \subseteq G\). This can be refined into a series of normal subgroups of \(G\) (Huppert, 1967, I,11.7) in such a way that the factor group of any two consecutive members of this series of normal subgroups is of order \(p\). Hence, \(R\) can be chosen among the members of this series such that \(|R/N| = p^k\).

Lemma 3
Let \(p\) be an odd prime and \(N\) a normal non-cyclic subgroup of a \(p\)-group \(G\). Then, \(N\) contains a normal subgroup \(A\) of \(G\) of type \((p,p)\).

Proof
We proceed by induction on \(|G|\), i.e., we suppose the lemma true for all \(p\)-groups of order less than \(|G|\) and prove that it remains true for \(G\). If \(|G| = p^2\), then \(G = N = A\).

Suppose \(|G| > p^2\). By virtue of Lemma 2, \(N\) contains a normal subgroup \(L\) of \(G\) such that \(|L| = p\). Consider \(G/L\).

If \(N/L\) is cyclic, then \(N\) is abelian since \(L \subseteq Z(G)\). Since \(N\) is not cyclic, we have \(m(N) = 2\), where \(m(N)\) denotes the minimal number of generators of \(N\). \(A = \langle x \in N \mid x^p = 1 \rangle\) is a characteristics subgroup of \(N\) of type \((p,p)\). Since \(N\) is normal in \(G\), \(A\) is normal in \(G\) as a characteristics subgroup of a normal subgroups of \(G\).

Suppose now \(N/L\) non-cyclic. Since the order of \(G/L\) is less than \(|G|\), by the inductive hypothesis there exists a normal subgroup \(M\) of \(G\) such that \(L \subseteq M \subseteq N\) and \(M/L\) is of type \((p,p)\). we have \(|M| = p^3\). If \(M\) is of exponent \(p\), by virtue of Lemma 2, there exists a normal subgroup \(A\) of \(G\) of type \((p,p)\). Suppose then
M is of exponent greater than \( p \). If \( M \) is abelian, we are done. Suppose \( M \) non-abelian. It is well known that \( |M/M'| \geq p^2 \) (Huppert, 1967, III, 7.1), hence \( |M'| = p \) since \( p^2 = |M| = (M:M')|M'| \). We have also \( M' \subseteq Z(M) \), because \( M' \) is characteristic in \( M \). By Lemma 1(b), for all \( x, y \in M \),

\[(xy)^p = x^p y^p [y, x]^{\binom{p}{2}},\]

and since \( p \) is odd, we have \( [y, x]^{\binom{p}{2}} = 1 \). Hence,

\[(x^p y^p)^p = x^p y^p.\]

Consequently \( a \mapsto a^p \) is an endomorphism, say \( f \), of \( M \). Since \( M \) is an exponent greater than \( p \), we have \( f(M) \neq \{1\} \). From \( M/M' \) is of type \( (p, p) \) it follows that \( f(M) \subseteq M' \), hence \( |f(M)| = p \). Ker \( (f) = A \) is then of order \( p^2 \) and in fact of type \( (p, p) \). Since \( A = \langle X \in M \mid X^p = 1 \rangle \) is characteristic in the normal subgroup \( M \) of \( G \), \( A \) is normal in \( G \).

**Theorem 1**

Let \( p \) be an odd prime and \( G \) a non-abelian \( p \)-group of order \( p^n \) in which \( G' \) is cyclic. Then \( P_{i}^{\binom{n}{2} + 1} \) divides \( |G/G'| \).

**Proof**

We carry out the proof by contradiction. Let \( G \) be a counterexample of minimal order. That is, the conclusion of the theorem holds for all \( p \)-groups of order less than \( |G| \) but it does not hold for \( G \). Then \( P_{i}^{\binom{n}{2}} \) divides \( |G/G'| \), and since \( G' \), is cyclic, every subgroup of \( G' \) is normal in \( G \). Let \( A \) be the subgroup of \( G' \) of order \( p \). Then \( A \) is normal in \( G \) and \( A \subseteq Z(G) \). Let \( s: G \to G/A \) be the natural homomorphism. \( s(G') = (s(G))' \) is a cyclic group and \( |s(G)| < |G| \).

Hence, \( P_{i}^{\binom{n-1}{2} + 1} \) divides \( |s(G)/s(G')| \). But \( s(G)/s(G') \approx G/G' \), so
If $n = 2m + 1$, then $i \left( \frac{n}{2} \right) = i \left( m + \frac{1}{2} \right) = m, i \left( \frac{n-1}{2} \right) = m$, hence $P^{\left( \frac{n}{2} \right)^{\ast 1}} \mid G/G'$ and we get a contradiction.

If $n = 2m$, then $i \left( \frac{n}{2} \right) = m, i \left( \frac{n-1}{2} \right) = i \left( m - \frac{1}{2} \right) = m - 1$ and $p^m \mid G/G'$, $p^{m\ast 1}$ does not divide $|G/G'|$, hence $|G/G'| = p^m = p^{\frac{n}{2}}$ and $|G'| = p^m$.

Set $A = \langle a \rangle$. We have $a \in Z(G)$. Let $M$ be a normal subgroup of $G$ of type $(p, p)$. $M$ exists by virtue of Lemma 3. We have $M \not\subset G'$ and $G' \not\subset M$. Consequently, $G/M$ is not abelian, $|G/M| = p^{2m - 2}$ and, by the choice of $G$, $p^m \mid (G/M)'$. But $(G/M)' = G'M/M \approx G'/G' \cap M$ and $G'/G' \cap M$ is cyclic as a factor group of a cyclic group. Hence, by comparing orders, we get $M \cap G' = \{1\}$. It follows that $M \subset Z(G)$. Let $x \in M \setminus \{1\}$. Then $N = \langle x, a \rangle$ is of type $(p, p)$ and normal in $G$ since $N \subset Z(G)$. This shows that we again get a contradiction because $a \in G'$ and $N \cap G' \neq \{1\}$. The proof is complete.

The bound as stated in Theorem 1 is the best possible. Indeed, there are non-abelian $p$-groups $(p \geq 3)$ of order $p^n$ such that $|G/G'|$ is equal to $P^{\left( \frac{n}{2} \right)^{\ast 1}}$.

If $n = 2m + 1$, then take $G = \langle x, y : y^{p^m} = x^{p^m} = 1, y^{-1}xy = x^{1+p} \rangle$. We obtain

$$|G/G'| = p^{m+1} = P^{\left( \frac{n}{2} \right)^{\ast 1}}.$$ 

When $n = 2m$, consider $G = \langle x, y : y^{p^m} = x^{p^m} = 1, y^{-1}xy = x^{1+p} \rangle$. In this case, we get $|G'| = | \langle x^{p^2} \rangle | = P^{m-1}$ and $|G/G'| = P^{m+1} = P^{\left( \frac{n}{2} \right)^{\ast 1}}$.

The case of 2-groups is completely different from that of $p$-groups where $p$ is odd as shown by the following result.
Theorem 2
For any integers \(m\) and \(n\) satisfying \(2 \leq n \leq m\), there exists a group \(G\) such that 
\[ |G| = 2^m, \quad |G/G'| = 2^n, \quad G' \text{ is cyclic.} \]

Proof
Let \(M\) be any abelian group of order \(2^{m-2}\) and let \(N\) denote the dihedral group of order \(2^{m-n-2}\). Let \(G\) be the direct product of \(M\) and \(N\). Then \(|G| = 2^m\), \(G' = N'\) is cyclic of order \(2^{m-n}\) and \(|G/G'| = 2^n\).

Theorem 3
The group in Theorem 1 is regular.

Proof
Let \(H = \langle a, b \rangle\) be a subgroup of \(G\), where \(a\) and \(b\) do not commute; this is possible, since \(G\) is non-abelian. \(H' \subset G'\) and \(G'\) is cyclic imply that \(H'\) is cyclic. Let \(H' = \langle c \rangle\). Then \(\{1\} \subset H_3 \subset H'\) with \(H_3 \neq H'\) and consequently \(H_3 \subset \langle c^p \rangle\). We can now apply Lemma 1(b) to \(H/H_3\): there exists \(d \in H_3 \subset \langle c^p \rangle\) such that
\[
(a, b)^p = a^p b^p [b, a]^{(p)}_{2} d.
\]
Since \(p \geq 3\), \(\binom{p}{2}\) is a multiple of \(p\). Hence \(\binom{p}{2} d = c^{mp}\). The proof of Theorem 3 is complete.

ACKNOWLEDGEMENT
I am grateful to the anonymous referees of SINET for their constructive comments.

REFERENCES