Finite p-groups with few normal subgroups (II)

Gheorghe Silberberg

Abstract

The paper investigates the finite nonabelian p-groups G of nilpotency class 2, with the property that every normal subgroup of G either contains the commutator subgroup G', or is contained in the center of G.

1   Introduction

Let G be a finite group. Denote by $\mathcal{S}(G)$ the set of all the subgroups of G, by $\mathcal{N}(G)$ the set of the normal subgroups of G, by $(H]$ the principal ideal generated by the element H in the lattice $(\mathcal{S}(G), \subseteq)$, and by $[H)$ the principal co-ideal generated by the element H in the same lattice. Then:

$$(Z(G)] \cup [G') \subseteq \mathcal{N}(G) \subseteq \mathcal{S}(G). \tag{1}$$

Both inclusions are becoming equalities if G is an abelian group. It is natural to ask whether there exist finite nonabelian groups for which at least one inclusion is actually an equality. In the case of the right inclusion, the answer to this question is well-known: the Dedekindian groups. So, we are left with the case of the left inclusion.

Definition 1.1. *A nonabelian group G is called* FNS-group *("Few Normal Subgroups") if:*

$$H \trianglelefteq G \Leftrightarrow H \geq G' \ or \ H \leq Z(G) \quad \forall H \in \mathcal{S}(G) . \tag{2}$$

In contrast to the Dedekindian groups, the finite FNS-groups have as few normal subgroups as possible. In particular, all the finite simple groups are FNS-groups. This remark shows that the study of all the finite FNS-groups is extremely difficult. Therefore, we will consider here only the family of the finite FNS-p-groups for any prime p.

In a recent article [4], we proved same results about FNS-p-groups.

Proposition 1.2. *Let p be a prime. Every nonabelian group of order p^3 or p^4 is an FNS-group.*

Proof. This is Proposition 2.1 from [4]. ∎

Proposition 1.3. *The nilpotency class of each finite nonabelian FNS-p-group is at most* 3.

Proof. This is Proposition 2.3 from [4]. ∎

In the same article, a complete description of the FNS-p-groups of class 3 was given.

Theorem 1.4. *Let p be a prime. The only FNS-p-groups of class* 3 *are:*
a) D_{16}, SD_{16} and Q_{16}, if $p = 2$.
b) The 4 groups of order p^4 and class 3, and the $p + 7$ direct descendants of order p^5 of the nonabelian group of order p^3 and exponent p in M. F. Newman's graph $\mathcal{K}_p$, if $p \neq 2$.

Proof. This is Theorem 3.4 from [4]. ∎

A complete classification of all finite FNS-p-groups of class 2 is still open. In the present paper we treat the case where the group has order p^5 (see below for motivation).

All the notation is standard.

2   Preliminary Results

In this section we formulate some necessary and/or sufficient conditions for a finite (p-)group of nilpotency class 2 to be an FNS-group.

Proposition 2.1. *Let G be a finite group. Then G is an FNS-group if and only if:*

$$G' \leq \langle x^G \rangle \quad \text{for every } x \in G \setminus Z(G) . \tag{3}$$

Proof. Suppose G is an FNS-group, and let $x \in G \setminus Z(G)$. Then $H = \langle x^G \rangle$ is a normal subgroup of G, and it is not contained in $Z(G)$. It follows that $G' \leq H$.

Conversely, suppose G satisfies relation (3). Let H be a normal subgroup of G, not contained in the center of G. For any $x \in H \setminus Z(G)$ we have $G' \leq \langle x^G \rangle \leq H$, hence G is an FNS-group. ∎

It is not easy to verify condition (3) in an arbitrary group. Therefore, the utility of Proposition 2.1 is not very high. Anyway, it can be used for proving the next statement.

Proposition 2.2. *Let G be a finite group of nilpotency class 2, which satisfies:*

$$Z(G/M) = Z(G)/M \quad \text{for every maximal subgroup } M \text{ of } G' . \qquad (4)$$

Then G is an FNS-group .

Proof. Let x be an arbitrary element in $G \setminus Z(G)$. Suppose $G' \not\leq \langle x^G \rangle$. Then $[x, G] < G'$, thus there exists a maximal subgroup M of G' such that $[x, G] \leq M$. Obviously,

$$\langle x, M \rangle / M \leq Z(G/M) = Z(G)/M .$$

Hence $\langle x, M \rangle \leq Z(G)$, in contradiction with the choice of x.
Therefore $G' \leq \langle x^G \rangle$ and, by Proposition 2.1, G is an FNS-group. ∎

Although neither condition (4) is easy to verify in general, it has a remarkable particular case.

Corollary 2.3. *Every finite p-group whose commutator subgroup has order p, is an FNS-group.*

Proof. Let us observe that any group which satisfies the hypothesis has class 2 and that the unique maximal subgroup of its commutator is trivial. The conclusion follows from Proposition 2.2. ∎

Corollary 2.3 offers many examples of finite FNS-p-groups of class 2. But what about the finite FNS-p-groups whose commutator subgroup has an order bigger than p? If G is such a group, then $p^2 \leq |G'| \leq |Z(G)| \leq \frac{|G|}{p^3}$, hence $|G| \geq p^5$. The complete classification of these groups seems to be very difficult to achieve. Therefore we restrict ourselves to the groups of this type, having order p^5. In this case, the commutator subgroup must have order p^2 and $G' = Z(G)$.

3   The Case $p = 2$

We will prove that there exists a unique group with the above mentioned properties.

Theorem 3.1. *The unique FNS-group of order 32, of class 2, whose commutator has order 4, is:*

$$\langle a, b, c \mid a^4 = b^4 = c^2 = [a, b] = 1, [a, c] = b^2, [b, c] = a^2 b^2 \rangle .$$

Proof. Let G be an FNS-group of order 32, of class 2, with $|G'| = 4$. At the end of the previous section we derived $G' = Z(G)$.

The group $G/Z(G)$ is an abelian group of order 8. It cannot be isomorphic either to $\mathbf{Z}_8$, or to $\mathbf{Z}_4 \times \mathbf{Z}_2$ (see [2], Lemma 3.1, p. 13). Hence $G/Z(G) \cong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$, which implies $G' = \Phi(G) = Z(G)$. By Proposition 2.13, p. 266, from [3], we get $exp(G') \leq exp(G/G') = 2$, thus $G' \cong \mathbf{Z}_2 \times \mathbf{Z}_2$. Furthermore, $exp(\Phi(G)) = 2$ implies $exp(G) = 4$.

We know that every normal subgroup of G must be comparable (with respect to inclusion) to G'. In particular, G' is the unique normal subgroup of order 4 in G. If x is a nontrivial element in G', then $G'/\langle x \rangle$ is the unique normal subgroup of order 2 in the group $G/\langle x \rangle$, hence the center of $G/\langle x \rangle$ is cyclic and it contains $G'/\langle x \rangle = (G/\langle x \rangle)'$. By [3], Proposition 13.7, p. 353, $Z(G/\langle x \rangle) \cong \mathbf{Z}_4$. Consequently, there exists an element $b \in G$ such that $[b, G] \le \langle x \rangle$, $b^4 \in \langle x \rangle$, $b^2 \notin \langle x \rangle$. We obtain:

$$|b| = 4 = exp(G) , \quad [b, G] = \langle x \rangle , \quad |C_G(b)| = |G : [b, G]| = 16 .$$

Furthermore, $Z(C_G(b)) \ge \langle b, Z(G) \rangle$, thus $C_G(b)$ is abelian.

We repeat now the entire argument, replacing x with b^2. We deduce that there exists an element $a \in G$ such that $|a| = 4$, $[a, G] = \langle b^2 \rangle$, $a^2 \notin [a, G]$ (otherwise $\langle a \rangle$ would be a normal subgroup in G, which is not contained in $Z(G)$ and which does not contain G'). One obtains:

$$\langle a^2 \rangle \cap \langle b^2 \rangle = \{1\}, \ G' = \Phi(G) = \langle a^2, b^2 \rangle \cong \mathbf{Z}_2 \times \mathbf{Z}_2, \ |C_G(a)| = 16, \ C_G(a) \text{ abelian} .$$

If $C_G(a) \ne C_G(b)$, then $C_G(a) \cap C_G(b)$ would have order 8 and each element in this intersection would commute with all elements in the subgroup $C_G(a) \cdot C_G(b) = G$. This would imply $C_G(a) \cap C_G(b) \le Z(G)$, a contradiction. Hence, $C_G(a) = C_G(b) \cong \mathbf{Z}_4 \times \mathbf{Z}_4$.

The subgroup $[b, G]$ is a subgroup of order 2 in G'. It must coincide either with $\langle a^2 \rangle$, or with $\langle b^2 \rangle$, or with $\langle a^2 b^2 \rangle$.
If $[b, G] = \langle b^2 \rangle$, then $\langle b \rangle \triangleleft G$, $\langle b \rangle \nleq Z(G)$, $\langle b \rangle \ngeq G'$, a contradiction.
If $[b, G] = \langle a^2 \rangle$, then $[ab, G] = \langle a^2 b^2 \rangle$, and $\langle ab \rangle \triangleleft G$, $\langle ab \rangle \nleq Z(G)$, $\langle ab \rangle \ngeq G'$, a contradiction.
We are left with $[b, G] = \langle a^2 b^2 \rangle$.

Let c be an element in $G \setminus C_G(a)$. Then:

$$G = \langle a, b, c \rangle , \quad [a, c] = \langle b^2 \rangle , \quad [b, c] = \langle a^2 b^2 \rangle , \quad c^2 \in G' .$$

If $c^2 = a^2$, then $(bc)^2 = b^2 c^2 [b, c] = 1$.
If $c^2 = b^2$, then $(abc)^2 = a^2 b^2 c^2 [ab, c] = 1$.
If $c^2 = a^2 b^2$, then $(ac)^2 = a^2 c^2 [a, c] = 1$.
Thus we can choose c such that $c^2 = 1$. We have actually proved that:

$$G = \langle a, b, c | a^4 = b^4 = c^2 = [a, b] = 1, [a, c] = b^2, [b, c] = a^2 b^2 \rangle .$$

Conversely, let G be the group which has the above presentation, and let M be the subgroup of G generated by elements a and b. Obviously, $M \cong \mathbf{Z}_4 \times \mathbf{Z}_4$. Since $c^{-1}ac = a \cdot [a, c] = ab^2 \in M$ and $c^{-1}bc = b \cdot [b, c] = ba^2 b^2 \in M$, it follows that M is a normal subgroup in G. Moreover, G/M is generated by the coset $c \cdot M$, which has order 2. Hence $|G| = |M| \cdot |G/M| = 16 \cdot 2 = 32$.
We may write:

$$c^{-1}a^2 c = (c^{-1}ac)^2 = (ab^2)^2 = a^2 , \quad c^{-1}b^2 c = (c^{-1}bc)^2 = (ba^2 b^2)^2 = b^2 .$$

Thus the subgroup $K = \langle a^2, b^2 \rangle$ is contained in $Z(G)$. Moreover, $K = \langle a^2 b^2, b^2 \rangle = \langle [b, c], [a, c] \rangle \le G'$. Hence, $Z(G) = K$. Let us observe that the group G/K is abelian, because all its generators commute. Hence $G' \le K$, thus $G' = Z(G) = K \cong \mathbf{Z}_2 \times \mathbf{Z}_2$.

Let x be a noncentral element of G. We will prove that $G' \leq \langle x, [x, G] \rangle$.
Suppose $x \notin M$. Then $|C_G(x)| \in \{8, 16\}$. Anyway, $Z(C_G(x)) \geq \langle x, Z(G) \rangle > Z(G)$,
thus $C_G(x)$ is abelian. If $|C_G(x)| = 16$, then from:

$$M \cdot C_G(x) = G \ , \quad |M \cap C_G(x)| = 8 \ , \quad M \cap C_G(x) \leq Z(G) \ ,$$

we would get a contradiction. Hence $|C_G(x)| = 8$ and $|[x, G]| = 4$. Then $[x, G] = G'$
and so $G' \leq \langle x, [x, G] \rangle$.
Suppose $x \in M$. We have 3 possibilities:

1. $x \in a \cdot Z(G) \Rightarrow [x, G] = \langle [a, c] \rangle = \langle b^2 \rangle$, $\langle x, [x, G] \rangle \geq \langle x^2, [x, G] \rangle = \langle a^2, b^2 \rangle = G'$,

2. $x \in b \cdot Z(G) \Rightarrow [x, G] = \langle [b, c] \rangle = \langle a^2 b^2 \rangle$, $\langle x, [x, G] \rangle \geq \langle x^2, [x, G] \rangle = \langle b^2, a^2 b^2 \rangle = G'$,

3. $x \in (ab) \cdot Z(G) \Rightarrow [x, G] = \langle [ab, c] \rangle = \langle a^2 \rangle$, $\langle x, [x, G] \rangle \geq \langle x^2, [x, G] \rangle = \langle a^2 b^2, a^2 \rangle = G'$.

We actually proved that:

$$G' \leq \langle x, [x, G] \rangle \quad \text{for every } x \in G \setminus Z(G) \ ,$$

which leads, by Proposition 2.1, to the conclusion that G is an FNS-group of order
32, of class 2, whose commutator subgroup has order 4. ∎

4 The Case $p \neq 2$

Here we have a similar result to the previous one, but the structure of the FNS-group
is not uniquely determined by the hypothesis.

Theorem 4.1. *Let p be an odd prime, and let G be a group of order p^5, of class 2,
with the commutator subgroup of order p^2. The following statements are equivalent:*
a) G is an FNS-group.
b) There exist $k, l \in \mathbf{Z}_p$, where $l^2 + 4k$ is not a square in $\mathbf{Z}_p$, such that

$$G \cong G_p^{(k,l)} = \langle a, b, c | a^{p^2} = b^{p^2} = c^p = [a, b] = 1, [a, c] = b^p, [b, c] = a^{kp} b^{lp} \rangle \ .$$

Proof. Suppose first that G is an FNS-group. As in the proof of Theorem 3.1,
we get:
$$G' = \Phi(G) = Z(G) \cong \mathbf{Z}_p \times \mathbf{Z}_p \ , \quad G/G' \cong \mathbf{Z}_p \times \mathbf{Z}_p \times \mathbf{Z}_p \ ,$$

and there exist elements $a, b \in G$ such that:

$$|a| = |b| = p^2 \ , \quad [a, b] = 1 \ , \quad M = \langle a, b \rangle \cong \mathbf{Z}_{p^2} \times \mathbf{Z}_{p^2} \ ,$$

$$G' = \mho(G) = \langle a^p, b^p \rangle \cong \mathbf{Z}_p \times \mathbf{Z}_p \ , \quad [a, b] = \langle b^p \rangle \ .$$

Since the nilpotency index of G is less than p, we know that G is a regular group,
thus $|\Omega(G)| = |G : \mho(G)| = p^3$ (see [3], Proposition 10.2, p. 322, and Proposition
10.7, p. 327). Since $|\Omega(G) : Z(\Omega(G))| \leq |\Omega(G) : Z(G)| = p$, we get that $\Omega(G)$ is an
elementary abelian p-group.

Let c be an arbitrary element in $\Omega(G) \setminus Z(G)$. Then $|c| = p$ and $[a, c] \in \langle b^p \rangle \setminus \{1\}$. We may assume (replacing, if necessary, c with a power of itself) that $[a, c] = b^p$. Since $[b, c] \in G'$, there exist $k, l \in \mathbf{Z}_p$ such that $[b, c] = a^{kp}b^{lp}$. One obtains $[a^i b^j, c] = [a, c]^i \cdot [b, c]^j = a^{jkp} \cdot b^{(i+jl)p}$ for every $i, j \in \mathbf{Z}_p$. If there would exist $(i, j) \in \mathbf{Z}_p \times \mathbf{Z}_p \setminus \{(\hat{0}, \hat{0})\}$ such that $[a^i b^j, c] \in \langle a^i b^j \rangle$, then the subgroup generated in G by the element $a^i b^j$ would be normal, would be not contained in $Z(G)$, and would not contain G', a contradiction. Hence, $a^{jkp} \cdot b^{(i+jl)p} \notin \langle a^i b^j \rangle$ for every $(i, j) \in \mathbf{Z}_p \times \mathbf{Z}_p \setminus \{(\hat{0}, \hat{0})\}$. In other words, each nonzero vector (i, j) in the linear space $\mathbf{Z}_p \times \mathbf{Z}_p$ is linearly independent, over $\mathbf{Z}_p$, from the vector $(jk, i + jl)$. This yields:

$$\begin{vmatrix} i & j \\ jk & i + jl \end{vmatrix} \neq \hat{0} \quad \forall (i, j) \in \mathbf{Z}_p \times \mathbf{Z}_p \setminus \{(\hat{0}, \hat{0})\} \ ,$$

or $i^2 + ijl - j^2 k \neq \hat{0} \ \forall (i, j) \in \mathbf{Z}_p \times \mathbf{Z}_p \setminus \{(\hat{0}, \hat{0})\}$. According to [1], Theorem 10, ch. 6.1, the discriminant $l^2 + 4k$ of this quadratic form is not a square.

Conversely, let $G = G_p^{(k,l)}$, where $l^2 + 4k$ is not a square in $\mathbf{Z}_p$. As in the proof of Theorem 3.1, we get:

$$M = \langle a, b \rangle \cong \mathbf{Z}_{p^2} \times \mathbf{Z}_{p^2} \ , \quad |G| = p^5 \ , \quad G' = Z(G) = \langle a^p, b^p \rangle \cong \mathbf{Z}_p \times \mathbf{Z}_p \ ,$$

$$[x, G] = G' \quad \forall x \in G \setminus M \ .$$

If $x \in M \setminus Z(G)$, then $|x| = p^2$ and there exist $(i, j) \in \mathbf{Z}_p \times \mathbf{Z}_p \setminus \{(\hat{0}, \hat{0})\}$, $z \in Z(G)$, such that $x = a^i b^j z$. Obviously, $C_G(x) = M$ and $|[x, G]| = p$. Furthermore,

$$[x, G] = \langle [x, c] \rangle = \langle [a^i b^j z, c] \rangle = \langle [a, c]^i \cdot [b, c]^j \rangle = \langle a^{jkp} \cdot b^{(i+jl)p} \rangle \ .$$

Since $l^2 + 4k$ is not a square in $\mathbf{Z}_p$, it follows, by Theorem 10, ch. 6.1, from [1], that $i^2 + ijl - j^2 k \neq \hat{0}$, i. e.:

$$\begin{vmatrix} i & j \\ jk & i + jl \end{vmatrix} \neq \hat{0} \ .$$

This last relation says that $[x, c] \notin \langle x^p \rangle$, which implies $\langle x, [x, G] \rangle \geq \langle x^p, [x, c] \rangle = G'$.

Using Proposition 2.1, we get that G is an FNS-group with the desired properties. ∎

Thus we got a large family of FNS-groups of order p^5, of class 2, with the commutator subgroup of order p^2. But some groups in this list may be isomorphic. Therefore, we will eliminate all the repetitions from the list, obtaining thus a complete set of pairwise nonisomorphic groups of this type.

Lemma 4.2. *If p is an odd prime, and k, l are elements in $\mathbf{Z}_p$ such that $l^2 + 4k$ is not a square, then in the group*

$$G_p^{(k,l)} = \langle a, b, c \mid a^{p^2} = b^{p^2} = c^p = [a, b] = 1, [a, c] = b^p, [b, c] = a^{kp}b^{lp} \rangle \ ,$$

the subgroup $M = \langle a, b \rangle$ is the only abelian subgroup of order p^4, and the subgroup $N = \Omega(G_p^{(k,l)}) = \langle a^p, b^p, c \rangle$ is the only elementary abelian subgroup of order p^3.

Proof. Suppose M_1 is an abelian subgroup of order p^4 of $G_p^{(k,l)}$, $M_1 \neq M$. Then $M \cdot M_1 = G_p^{(k,l)}$, $|M \cap M_1| = p^3$, and $M \cap M_1 \leq Z(G_p^{(k,l)})$, a contradiction.

Suppose N_1 is an elementary abelian subgroup of order p^3 of $G_p^{(k,l)}$. Then $N_1 \leq \Omega(G_p^{(k,l)}) = N$, thus $N_1 = N$. ∎

Proposition 4.3. *Let $k_1, l_1, k_2, l_2 \in \mathbf{Z}_p$ such that $l_1^2 + 4k_1$ and $l_2^2 + 4k_2$ are not squares in $\mathbf{Z}_p$. The following statements are equivalent:*
a) $G_p^{(k_1,l_1)} \cong G_p^{(k_2,l_2)}$.
b) There exists $w \in \mathbf{Z}_p \setminus \{\hat{0}\}$ such that $l_1 = wl_2$ and $k_1 = w^2 k_2$.

Proof. Suppose a) is true and let $\varphi : G_p^{(k_1,l_1)} \to G_p^{(k_2,l_2)}$ be an isomorphism. By Lemma 4.1, we get $\varphi(M_1) = M_2$ and $\varphi(N_1) = N_2$, where M_1, M_2, N_1, N_2 have obvious meanings. There exist

$$x, y, u, v, w \in \mathbf{Z}_p \ , \quad w \neq \hat{0} \ , \quad \begin{vmatrix} x & y \\ u & v \end{vmatrix} \neq \hat{0}$$

and $z, z', z'' \in Z(G_p^{(k_2,l_2)})$ such that

$$\begin{cases} \varphi(a_1) &= a_2^x \cdot b_2^y \cdot z \ , \\ \varphi(b_1) &= a_2^u \cdot b_2^v \cdot z' \ , \\ \varphi(c_1) &= c_2^w \cdot z'' \ . \end{cases}$$

The equalities $[a_1, c_1] = b_1^p$, $[b_1, c_1] = a_1^{k_1 p} \cdot b_1^{l_1 p}$ imply:

$$(S) \quad \begin{cases} k_2 yw &= u \\ xw + l_2 yw &= v \\ k_2 vw &= k_1 x + l_1 u \\ uw + l_2 vw &= k_1 y + l_1 v \end{cases}$$

If x, y, u, v are unknowns and w is a parameter, the system (S) must have nontrivial solutions. Hence, its determinant must be zero. The equality:

$$\begin{vmatrix} \hat{0} & k_2 w & \widehat{-1} & \hat{0} \\ w & l_2 w & \hat{0} & \widehat{-1} \\ k_1 & \hat{0} & l_1 & -k_2 w \\ \hat{0} & k_1 & -w & l_1 - l_2 w \end{vmatrix} = \hat{0}$$

becomes:

$$(k_1 - k_2 w^2)^2 + l_2 w (k_1 - k_2 w^2)(l_1 - l_2 w) - k_2 w^2 (l_1 - l_2 w)^2 = \hat{0} \ .$$

The discriminant of this quadratic form,

$$(l_2 w)^2 + 4k_2 w^2 = w^2(l_2^2 + 4k_2) \ ,$$

is not a square. By Theorem 10, ch. 6.1, from [1], we have $k_1 - k_2 w^2 = l_1 - l_2 w = \hat{0}$.

Conversely, let k_2, l_2, w be three elements in $\mathbf{Z}_p$ such that $l_2^2 + 4k_2$ is not a square, and w is nonzero. We define an isomorphism $\varphi : G_p^{(k_1,l_1)} \to G_p^{(k_2,l_2)}$, where $k_1 = w^2 k_2$ and $l_1 = wl_2$.
Put $\varphi(a_1) = a_2$, $\varphi(b_1) = b_2^w$, $\varphi(c_1) = c_2^w$, and extend φ on $G_p^{(k_1,l_1)}$ by multiplication. While $\{a_1, b_1, c_1\}$ is a generating set for $G_p^{(k_1,l_1)}$, it is sufficient to show that $\{\varphi(a_1), \varphi(b_1), \varphi(c_1)\}$ is a generating set for $G_p^{(k_2,l_2)}$ which satisfies the same relations in $G_p^{(k_2,l_2)}$ as a_1, b_1, c_1 satisfy in $G_p^{(k_1,l_1)}$.

The condition that $\{\varphi(a_1), \varphi(b_1), \varphi(c_1)\}$ is a generating set in $G_p^{(k_2,l_2)}$ is obviously true.

$(\varphi(a_1))^{p^2} = a_2^{p^2} = 1$;

$(\varphi(b_1))^{p^2} = (b_2^w)^{p^2} = (b_2^{p^2})^w = 1$;

$(\varphi(c_1))^p = (c_2^w)^p = (c_2^w)^p = 1$;

$[\varphi(a_1), \varphi(b_1)] = [a_2, b_2^w] = [a_2, b_2]^w = 1$;

$[\varphi(a_1), \varphi(c_1)] = [a_2, c_2^w] = [a_2, c_2]^w = (b_2^p)^w = (b_2^w)^p = (\varphi(b_1))^p$;

$[\varphi(b_1), \varphi(c_1)] = [b_2^w, c_2^w] = [b_2, c_2]^{w^2} = a_2^{w^2 k_2 p} \cdot b_2^{w^2 l_2 p} = (\varphi(a_1))^{w^2 k_2 p} \cdot (\varphi(b_1))^{w l_2 p} = (\varphi(a_1))^{k_1 p} \cdot (\varphi(b_1))^{l_1 p}$.

It follows that φ is indeed a group isomorphism. ∎

We may now eliminate all the repetitions from the list of groups given in Theorem 4.1.

Theorem 4.4. *Let p be an odd prime. There exist exactly $\frac{p+1}{2}$ pairwise non-isomorphic FNS-groups of order p^5, of class 2, with the commutator subgroup of order p^2, namely:*

$G_p^{(q,\hat{0})}$, *where q is a fixed non-square in $\mathbf{Z}_p$;*

$G_p^{(r,\hat{1})}$, *where r runs through the set of all elements of $\mathbf{Z}_p$ with the property that $4r + \hat{1}$ is non-square.*

Proof. By Theorem 4.1 all these groups are FNS-groups and have the required properties, and by Proposition 4.3 they are pairwise non-isomorphic. It remains to prove that every group in Theorem 4.1 is isomorphic to a group in our list, but this is easy to check. ∎

References

[1] Z. I. BOREWICZ, I. R. SAFAREVIC, Zahlentheorie, Birkhäuser Verlag, Basel-Stuttgart, 1966

[2] M. HALL jr., J. K. SENIOR, The groups of order 2^n ($n \leq 6$), MacMillan, New York, 1964

[3] B. HUPPERT, Endliche Gruppen I, Springer Verlag, Berlin-Heidelberg-New York, 1967

[4] G. SILBERBERG, Finite p-groups with few normal subgroups, Bulletin of the Belgian Mathematical Society-Simon Stevin Vol. 7 (2000), No. 3, pp. 365-376

Department of Economics, Central European University,
Nador u. 9, 1051 Budapest, Hungary
e-mail: cphsig01phd.ceu.hu