STRUCTURE AND INVARIANTS OF FINITE p-GROUPS WITH A MINIMAL COMMUTATOR SUBGROUPS

Neli T. Keranova, Nako A. Nachev

ABSTRACT: *In this paper we consider an arbitrary finite p-group with a commutator subgroup G' of order p, where p is a prime. We define the concepts: a minimal group, a central commutator product, a symplectic pair, a symplectic product, a symplectic basis, a key group, a clean group etc. In the article there are two main results: the structural theorem for the considered groups and the determination of the full system of invariants of these groups.*

KEYWORDS: *p-group, commutator subgroup, invariant, isomorphic groups*

1. Introduction. Let G be a finite p-group with a commutator subgroup G' of order p, where p is a prime. Then G is called *a finite p-group with a minimal commutator subgroup*. We shall suppose, that $G' =< c >$, i.e. we shall fix the generating element c of G'.

In the section "Preliminary results" we define the concepts: a group of the central type and a group of the non-central type, a minimal group, a central commutator product, a clean group.

In the third part of this paper we study the structure of finite p-groups with a minimal commutator subgroups. We introduce the concept "a symplectic basis" and define its properties. We give definitions for a key subgroup, a symplectic pair and a symplectic product. We construct a symplectic linear space.

In the latter part of the article we determine a full system of invariants of the finite p-group G with a minimal commutator subgroup.

Glauberman [5, 6] has studied finite p-groups, but his attention is directed to various properties of such groups. Akinola [1] obtain

properties of some subgroups of finite p-groups. Finite p-groups are studied in [2, 3, 4, 8].

2. Preliminary results

Definition 2.1. Let G be an arbitrary multiplicative group and $x, y \in G$. Then the element

$$[x, y] = x^{-1}y^{-1}xy \in G$$

is called *a commutator* of the elements x and y in the group G.

The subgroup

$$G' = \langle [x, y] | x, y \in G \rangle$$

of G, which is generated by all commutators of G, is called *a commutator subgroup* of G.

Definition 2.2. Let the order of the commutator subgroup G' of G be p and let $G' =< c >$, $c^p = 1$, $c \neq 1$. Then G is called *a finite p-group with a minimal commutator subgroup.*

Theorem 2.3. If the order of G' is p, then G' is contained in the center Z of G .

Proof. Let $G' =< c >$. We must prove, that c commutes with all elements of the group G. Denote by $l = [c, a]$, where $a \in G$ is an arbitrary element of G. Then $c^{-1}a^{-1}ca = l$, hence $a^{-1}ca = cl$. We substitute $l = c^k$ and obtain $a^{-1}ca = c^{k+1}, k \in \mathbb{N}$ and by an induction, we obtain $a^{-p^\alpha}ca^{c\alpha} = c^{(k+1)^{p^\alpha}}$. Therefore, $(k+1)^{p^\alpha} \equiv 1(modp)$ and $k \equiv 0(modp)$, i.e. $l = 1$. □

Theorem 2.4. If a and b are arbitrary elements of the group G and $G' =< c >$, then

$(ab)^n = a^n b^n c^{\frac{n(n-1)}{2}}, n \in \mathbb{N}$.

Proof. Let $c = [b, a]$. Then $ba = abc$. We will prove this theorem by an induction.

1. For $n = 1$, $ab = ab$ holds.

2. Suppose, that the theorem is true for $n-1$, i.e. $(ab)^{n-1} = a^{n-1}b^{n-1}c^{\frac{(n-1)(n-2)}{2}}$.

3. We will prove the theorem for n . Namely,

$(ab)^n = (ab)^{n-1}(ab) = a^{n-1}b^{n-1}c^{\frac{(n-1)(n-2)}{2}}ab =$

$= a^{n-1}b^{n-1}abc^{\frac{(n-1)(n-2)}{2}} = a^nb^nc^{\frac{n(n-1)}{2}}$,

since $a^{-1}ba = bc$ implies $a^{-1}b^{n-1}a = b^{n-1}c^{n-1}$ and then $b^{n-1}a = ab^{n-1}c^{n-1}$.

Let either $p \neq 2$ or $p = 2$ and $n \neq 2$. Then, if either p divides n or p divides $n-1$, then $(ab)^n = a^nb^n$. □

Corollary 2.5. If either $p \neq 2$ or $p = 2$ and $n \geq 2$, then $(ab)^{p^n} = a^{p^n}b^{p^n}$.

Proof. We have proved $(ab)^n = a^nb^nc^{\frac{n(n-1)}{2}}$.

If $p \neq 2$, then $(ab)^{p^n} = a^{p^n}b^{p^n}c^{\frac{p^n(p^n-1)}{2}}$. However $c^{\frac{p^n(p^n-1)}{2}} = 1$ and consequently $(ab)^{p^n} = a^{p^n}b^{p^n}$.

If $p = 2$ and $n \geq 2$, then $\frac{p^n(p^n-1)}{2}$ is even and $c^{\frac{p^n(p^n-1)}{2}} = 1$.

If $p = 2$, $[b, a] = c$ and $n = 1$, then $(ab)^2 = a^2b^2c$. □

Definition 2.6. $G[p^n] \stackrel{def}{=} \{a \in G / a^{p^n} = 1\}$.

Definition 2.7. $G^{p^n} \stackrel{def}{=} \{a^{p^n} / a \in G\}$.

Theorem 2.8. If either $p \neq 2$ or $p = 2$ and $n \geq 2$, then $G[p^n]$ is a subgroup of G.

Theorem 2.9. If either $p \neq 2$ or $p = 2$ and $n \geq 2$, then G^{p^n} is a subgroup of G.

Proof. Let $a, b \in G^{p^n}$. Then $a = x^{p^n}$, $b = y^{p^n}$, $x, y \in G$. By Corollary 2.5, $ab = x^{p^n}y^{p^n} = (xy)^{p^n} \in G^{p^n}$. □

Lemma 2.10. The group G^{p^n} is an Abelian group.

Proof. It holds $a^{p^n}b^{p^n} = (ab)^{p^n}$. Then $b^{p^n}a^{p^n} = (ba)^{p^n} = (abc^l)^{p^n} = (ab)^{p^n} = a^{p^n}b^{p^n}, l \in Z$. □

Lemma 2.11.[7](Theorem 9.2.1. p. 138) The factor group G/G' is Abelian. If K is a normal subgroup of G , such that G/K is Abelian, then $K \supseteq G'$.

Definition 2.12. Let G be a finite p-group with a commutator subgroup G' of order p and let c be a generating element of G'. If the equation $x^{p^k} = c$ has a solution in G and the equation $x^{p^{k+1}} = c$ does not have solution in G, then the number p^k is called *a height of c in the group G* and it is denoted by $h_G(c)$. If this equation is considered in the center Z of the group G , then this number is called *a height of c in Z* and it is denoted by $h_Z(c)$.

If $h_Z(c) = p^k$, then either $h_G(c) = p^k$ or $h_G(c) = p^{k+1}$.

Definition 2.13. If $h_Z(c) = h_G(c)$, then the group G is called *a group of a central type*. If $h_G(c) = p.h_Z(c)$, then we will call the group G *a group of a non-central type* .

Definition 2.14. Let G be a finite p-group with a commutator subgroup of order p. The group G is called *a minimal group* if each its real subgroup is Abelian.

Lemma 2.15. The group G is a minimal group, if and only if G is generated by two non-commutative elements.

Proof.

1. Necessary: Let G be a minimal group. Since G is non-abelian, then G consists of a pair of non-commutative elements a and b . By Definition 2.14, $G = < a, b >$.

2. Sufficiency: Let G be generated by two non-commutative elements a and b, $[b, a] = c$, where $G' =< c >$. Let H be a non-commutative subgroup of G . Then H consists of a pair of non-commutative elements x and y and $x = a^\alpha b^\beta c^\gamma$, $y = a^\lambda b^\mu c^\nu$, where $\alpha, \beta, \gamma, \lambda, \mu, \nu \in \mathbb{Z}$. Let us define the commutator of x and y. Consider $[x, y] = [a^\alpha b^\beta c^\gamma, a^\lambda b^\mu c^\nu] = [a^\alpha, b^\mu].[b^\beta, a^\lambda] = [a, b]^{\alpha\mu}[b, a]^{\beta\lambda} = c^{\beta\lambda-\alpha\mu} \neq 1$. Therefore, p does not divide $\beta\lambda - \alpha\mu$. Then exists $\delta \in \mathbb{Z}$, such that $\delta(\alpha\mu - \beta\lambda) \equiv 1(mod p^t)$, where $o(a) = p^t$. From the

above representations of x and y we obtain $x^{\mu}y^{-\beta} = a^{\alpha\mu-\beta\lambda}c^{\gamma_1}$. Then $(x^{\mu}y^{-\beta})^{\delta} = ac^{\gamma_1\delta}$. Since $x, y, c \in H$, then $a \in H$. Analogously, we prove, that $b \in H$. Therefore, $H = G$. □

We will pay attention to the following p-groups with a commutator subgroup of order p:

First type: $G =< a, b >: a^{p^{\alpha}} = 1, b^{p^{\beta}} = 1, a^{-1}ba = bc, ac = ca, bc = cb, \alpha \geq 1, \beta \geq 1$,

Second type: $G =< a, b >: a^{p^{\alpha}} = 1, b^{p^{\beta}} = 1, a^{-1}ba = b^{1+p^{\beta-1}}$, $\alpha \geq 1, \beta \geq 2$,

Third type: Q_8.

Lemma 2.16. Each minimal group is isomorphic to the one of those three types groups.

Proof. We must first prove, that these three types groups are minimal groups. Really, each of them is generated by two non-commutative elements.

Further we will prove, that each minimal group is isomorphic to any of these three types groups. We consider the factor group G/G' . Since G is generated by two elements and G/G' is an Abelian group, then this factor group is a direct product of two cyclic groups. Let a and b be representatives of the forming elements of the cosets of G' of these cyclic groups. Since the group G is non-commutative, then a and b are non-commutative. Let $[b, a] = c$, where c is the forming element of G'. Then $a^{p^{\alpha}} = c^{\alpha_1}$ and $b^{p^{\beta}} = c^{\beta_1}$. We can choose the elements a and b so that α_1 and β_1 take values 0 or 1. We will consider three cases:

First case: $\alpha_1 = \beta_1 = 0$, $a^{p^{\alpha}} = 1, b^{p^{\beta}} = 1, a^{-1}ba = bc$ and since c is a central element, then $ac = ca, bc = cb$. Therefore, the group is isomorphic to a group of the first type.

Second case: $\alpha_1 = 0$ and $\beta_1 = 1$, $a^{p^{\alpha}} = 1, b^{p^{\beta}} = c, a^{-1}ba = bc$. Then we have a group of second type (analogously for $\alpha_1 = 1$ and $\beta_1 = 0$).

Third case: $\alpha_1 = \beta_1$, $a^{p^{\alpha}} = c, b^{p^{\beta}} = c, a^{-1}ba = bc$. We have two subcases:

3.1. If $p^\alpha = p^\beta = 2$, then $p = 2$, $\alpha = \beta = 1$. So we obtain the group Q_8.

3.2. Let at least one of the numbers p^α and p^β be different from 2. We can assume that $\alpha \leq \beta$. Then $1 = a^{p^\alpha} b^{p^{-\beta}} = \left(ab^{-p^{\beta-\alpha}}\right)^{p^\alpha}$. We put $x = ab^{-p^{\beta-\alpha}}$. Then $x^{p^\alpha} = 1$, $b^{p^\beta} = c$, $x^{-1}bx = bc$ and we obtain a group of the second type. □

Remark. The group D_8 may be considered as a group of the first or the second type. Really,

$< a, b >$: $a^2 = 1, b^2 = 1, a^{-1}ba = bc$ - first type;

$< x, y >$: $x^2 = 1, y^4 = 1, x^{-1}yx = y^3 : x = a, y = ab$ - second type.

Definition 2.17. Let $G_1, G_2, ..., G_k$ be subgroups of the group G, which satisfy the following conditions:

1. if $x_i \in G_i$, $y_j \in G_j$, then $x_i y_j = y_j x_i$, for $i \neq j$;
2. $G/(Z \cap G') = \prod_{i=1}^{k} G_i(Z \cap G')/(Z \cap G')$;
3. $G = G_1 G_2 ... G_k$.

Then G is called *a central commutator product* of the subgroups G_1,$G_2, ..., G_k$ and we shall denote it by

$G = G_1 * G_2 * ... * G_k = \prod_{i=1}^{k} {}^* G_i$.

Definition 2.18. Let G be a finite p-group with a commutator subgroup of order p . The group G is called *a clean group*, if it does not contain cyclic direct factors.

Remark. Each minimal group is a clean group.

Lemma 2.19. Each finite p-group with a commutator subgroup of order p is a direct product of a clean subgroup and an Abelian group.

Proof. Let us denote by A the maximal Abelian direct factor of G . Then $G = U \times A$. We will prove, that U is a clean group. Assume that U consists of a cyclic direct factor, i.e. $U = U_1 \times U_2$, where U_2

is a cyclic group. Then $G = U_1 \times U_2 \times A = U_1 \times (U_2 \times A)$. Since $U_2 \times A$ is a product of Abelian groups, it is an Abelian group, it is a direct factor and consists of A, then we obtain a contradiction to the fact, that A is a maximal group. Therefore, U is a clean group. □

Lemma 2.20. Let A and B be minimal groups. Then $A * B = C * D$, where C and D are minimal groups and at least one of them is of the first type.

Proof. If at least one of the groups A and B is of the first type, then Lemma 2.20 is obvious. It remains to consider three cases:

1. Let A and B be of the second type. Then

$A =< a_1, a_2 >: a_1^{p^{\alpha_1}} = 1, a_2^{p^{\alpha_2 - 1}} = c = [a_2, a_1], \alpha_1 \geq 1, \alpha_2 \geq 2;$

$B =< b_1, b_2 >: b_1^{p^{\beta_1}} = 1, b_2^{p^{\beta_2 - 1}} = c = [b_2, b_1], \beta_1 \geq 1, \beta_2 \geq 2.$

We can assume that $\alpha_2 \geq \beta_2$. Let us put

$$x = \begin{cases} a_1, & \alpha_2 > \beta_2, \\ a_1 b_1, & \alpha_2 = \beta_2 \end{cases}$$

$$y = a_2^{p^{\alpha_2 - \beta_2}} b_2.$$

Then we put $C =< x, a_2 >$ and $D =< b_1, y >$. Therefore, C and D are minimal groups, D is of the first type and $A * B = C * D$.

2. Let $p = 2$, A be of the second type and $B \cong Q_8$. Then

$A =< a_1, a_2 >: a_1^{2^\alpha} = 1, a_2^{2^{\beta - 1}} = c, \alpha \geq 1, \beta \geq 2;$

$B =< b_1, b_2 >: b_1^2 = 1, b_2^2 = c.$

The preparation of the groups C and D is analogously to the first case.

3. Let $A \cong B \cong Q_8$. Then

$A =< a_1, a_2 >: a_1^2 = a_2^2 = c,$

$B =< b_1, b_2 >: b_1^2 = b_2^2 = c.$

We put $x = a_1 b_1$, $y = a_2 b_2$ and define the groups C and D by the following way:

$C =< x, a_2 >$, $D =< y, b_2 >$.

Then C and D are isomorphic to D_8 and $A * B = C * D$. □

Lemma 2.21. Let G be a clean p-group with a commutator subgroup of order p . Then G can be represented as a central commutator product of minimal groups and eventually one cyclic group.

Proof. We will prove Lemma 2.21 by an induction to the order of the group G.

Let G be of a minimal order. Then it is isomorphic to any of minimal groups.

Let G be of an arbitrary non-minimal order. Consider the factor group G/G' . It is an Abelian. Let a be a non-central element of G, such that aG' has the lowest order to the orders of the all cosets of G' , which have to representative a non-central element of G . Let b be an element, which does not commute with a, i.e. $[b,a]=c$, such that $o(bG') \leq o(yG')$, $y \in G$, $y \notin Z(G)$, by these elements, which do not commute with a . We form a minimal group by the elements a and b and denote it by $H =< a,b >$. Consider $C_G(a) \cap C_G(b)$. Then $Z(H) \leq C_G(a) \cap C_G(b)$, since all elements of $Z(H)$ commute with a and b together . The forming element c of the commutator subgroup is contained in $Z(H)$, since H is non-commutative. Therefore, it is contained in $C_G(a) \cap C(G(b)$. Then we can form the factor groups $Z(H)/G'$ and $(C_G(a) \cap C_G(b))/G'$, which satisfy the condition $Z(H)/G' \leq C_G(a) \cap C_G(b))/G'$. We will prove, that $Z(H)/G'$ is a direct factor of other factor group. We must prove that $Z(H)/G'$ is servant subgroup of $C_G(a) \cap C_G(b)$. Since H is generated by a and b, then $Z(H)/G' =< a^pG' > \times < b^pG' >$. We denote by $o(aG') = p^\alpha$, i.e. $a^{p^\alpha} \in G'$ and $o(bG') = p^\beta$, i.e. $b^{p^\beta} \in G'$, where $\alpha \leq \beta$.

Each element of the substratum of $Z(H)/G'$ is of the type $xG' = a^{\lambda p^{\alpha-1}} b^{\mu p^{\beta-1}} G'$, $\lambda, \mu \in \mathbb{Z}$ and at least one of the numbers λ and μ is not divisible by p . We consider two cases:

First case: When λ is not divisible by p , i.e. $(\lambda, p) = 1$. Then $h_{Z(H)/G'}(xG') = p^{\alpha-2}$. We must prove that $h_{C_G(a) \cap C(G(b))/G'}(xG') = p^{\alpha-2}$. We assume that there exists an element $yG' \in C_G(a) \cap C_G(b))/G'$, such that $(yG')^{p^{\alpha-1}} = a^{\lambda p^{\alpha-1}} b^{\mu p^{\beta-1}} G'$. Therefore, $y^{p^{\alpha-1}} G' = a^{\lambda p^{\alpha-1}} b^{\mu p^{\beta-1}} G'$ and $\left(y a^{-\lambda} b^{-\mu p^{\beta-\alpha}} \right)^{p^{\alpha-1}} \in G'$. The element

$ya^{-\lambda}b^{-\mu p^{\beta-\alpha}}$ is of order $p^{\alpha-1}$ and then $o(ya^{-\lambda}b^{-\mu p^{\beta-\alpha}}G') \leq p^{\alpha-1}$. On the one hand $p^{\alpha-1} < p^{\alpha}$ and the element a is of a minimal order of the non-central elements and $o(a) = p^{\alpha}$. On the other hand the element $ya^{-\lambda}b^{-\mu p^{\beta-\alpha}}$ is a non-central element, since $y \in C_G(a) \cap C_G(b)$ and a and b do not commute. Then we obtain a contradiction with the selection of the element a, which is of a minimal order.

Second case: Let p divide λ. Since $a^{p^{\alpha}} \in G'$, then $a^{\lambda p^{\alpha-1}} \in G'$. We consider the coset $xG' = b^{\mu p^{\beta-1}}G'$. Assume, that there exists the element $zG' \in C_G(a) \cap C_G(b)/G'$, such that $(zG')^{p^{\beta-1}} = b^{\mu p^{\beta-1}}G'$. Then $(zb^{-\mu})^{p^{\beta-1}} \in G'$ and hence $o(zb^{-\mu}) \leq p^{\beta-1}$. Since $p^{\beta-1} < p^{\beta}$, then we obtain a contradiction with the selection of the element b.

We have $C_G(a) \cap C_G(b))/G' = Z(H)/G' \times T/G'$, where $T \leq C_G(a) \cap C_G(b))/G'$. Therefore, $C_G(a) \cap C_G(b)) = Z(H).T$ and $Z(H) \cap T = G' =< c >$. On the other hand $G = H.(C_G(a) \cap C_G(b))$. Then $G = H.Z(H).T = H.T$. Let us define the intersection of H and T. We have $< c >= Z(H) \cap T \leq H \cap T$ and hence $< c > \leq H \cap T$. We must prove that $H \cap T \leq < c >$. Let us take an element $x \in H$. Therefore, $x = a^{\alpha}b^{\beta}$. Let $x \in T$. Then x commutes with a and b. If $(\alpha, p) = 1$, then a^{α} does not commute with b, since a and b do not commute. On the other hand the element b^{β} commutes with b . Then x does not commute with b. But x must commute with a and b. Therefore, α must divide of p. Analogously, we obtain that β must divide of p. The elements of the type a of degree, which is divided of p and b of degree, which is divided of p. belong to $Z(H)$. Then $x \in Z(H)$ and since $x \in T$, then $x \in Z(H) \cap T =< c >$. Therefore, $G = H.T$ and $H \cap T =< c >$. Hence $G = H * T$. Since T is of lower order of G. Then T is a central commutator product of minimal groups. Since H is a minimal group, then G is a central commutator product of minimal groups. □

3. Structure of finite p-groups with a minimal commutator subgroups

Lemma 3.1. Each clean finite $p-$group G with a commutator subgroup of order p can be represented as $G = W * B$, where W is

a cyclic p-group or a minimal group of the second or the third type and B is a central commutator product of minimal groups of the first type.

Proof. By Lemma 2.21, G can be represented as a central commutator product of minimal groups and eventually one cyclic group. If we take one pair of minimal groups of this central commutator product, then according to Lemma 2.20, this pair can be taken with other pair, where at least one of the groups is of the first type. Then in the central commutator product by successive replacements the minimal subgroups of the second and the third type can be reduced and will remain at most one such group.

If the group G is of a central type, then in the central commutator product after successive transformations will do not remain a group of the second or the third type. It will remain only one cyclic group.

If the group G is of a non-central type, then it will remain one group of the second or the third type. Let us denote the cyclic group or the group of the second or the third type by W. The central commutator product of other minimal groups denote by B . Then $G = W*B$. □

Theorem 3.2.(structural theorem for the finite p-groups with a commutator subgroup of order p). Each finite p-group G with a commutator subgroup of order p can be represented by the following way: $G = W*B\times A$, where the group W is a cyclic p-group or a minimal group of the second or the third type, B is a central commutator product of minimal subgroups of the first type and A is an Abelian group.

Proof. By Lemma 2.21, the group G can be represented as $G = U \times A$, where A is an Abelian group and U is a clean group. Lemma 3.1 implies the group U can be represented as $U = W * B$, where W is a cyclic group, or a minimal group of the second or the third type and the group B is a central commutator product of minimal groups of the first type. Therefore, $G = W * B \times A$. □

Definition 3.3. Let G be a finite p-group with a commutator

subgroup G' of order p and let c be the forming element of G'. Let G can be represented as $G = W * B \times A$, where W, B and A are the subgroups of Theorem 3.2. We will call the forming elements of the system of the forming elements of the minimal groups, which participate in the presentation of G as a central commutator product *a symplectic basis of* G.

Let $a_1, a_2, ..., a_s, b_1, b_2, ...b_s, c_1, c_2, ..., c_r$ be the elements, which form a symplectic basis of the group G. Then they hold the following properties:

1) for $i \in \{1, 2, ..., s\}$ it holds: $a_i^{-1} b_i a_i = b_i c$, and all other elements of A commute together ;

2) if G is of a central type, then the cyclic group $< c_1 >$ contains G' and the cyclic subgroups, which are generated by other generating elements do not contain G'. If the group G is of a non-central type and either $p \neq 2$ or $h_G(c) \geq 4$, then the cyclic group $< b_1 >$ contains G' and the other cyclic subgroups, which are generated by A, do not contain G'. If the group G is of a non-central type, $p = 2$ and $h_G(c) = 2$, then $< b_1 >$ contains G' and at most one of the subgroups $< a_i, b_i >$ is isomorphic to the quaternion group of order eight.

3) Any element of the group G is represented uniquely as a product

$$\prod_{\lambda=1}^{s} \prod_{\mu=1}^{s} \prod_{\nu=1}^{r} a_\lambda^{\alpha_\lambda} b_\mu^{\beta_\mu} c_\nu^{\gamma_\nu}$$

where the exponents $\alpha_\lambda, \beta_\mu, \gamma_\nu$ take values from 0 to the order of the corresponding coset in the factor group G/G', with the exception of the element c_1 for a group of central type and the element b_1 for a group of a non-central type. In this case the exponents take values from 0 to the order of c_1 (to the order of b_1, respectively).

Theorem 3.4. If $G = G_1 * G_2 * ... * G_k$, then each element of G is represented in the form $g = g_1 g_2 ... g_k$, where $g_i \in G_i$ for $i \in \{1, 2, ..., k\}$ and if the element g has other presentation $g = g_1' g_2' ... g_k'$, then $g_i' = g_i c_i$, $c_i \in G'$, $g_i' \in G_i$.

Proof. Let $g \in G$. According to condition 3 we obtain $g = g_1 g_2 ... g_k$. Furthermore, let $g = g'_1 g'_2 ... g'_k$ for $g_i \in G_i$, $i \in \{1, 2, ..., k\}$. Then $g'_i g_i^{-1} = g_1 g_1'^{-1} g_2 g_2'^{-1} ... g_{(i-1)} g_{(i-1)}'^{-1} g_{(i+1)} g_{(i+1)}'^{-1} ... g_k g_k'^{-1}$. Consequently, $g'_i g_i^{-1} \in G_i \cap \prod_{i \neq j, j=1}^{k} G_j = G'$. Then there is $c_i \in G'$, such that $g'_i = g_i c_i$. □

Definition 3.5. We will call the group W from the presentation of G in Theorem 3.2 *a key subgroup of the group G.*

Theorem 3.6. Let G be a finite p-group with a commutator subgroup of order p . If the key subgroup of G is isomorphic to the quaternion group Q_8, then G can be represented as a product of two groups A and B , which are normal subgroups of G and $A \cap B = G'$. If the key subgroup is not isomorphic to Q_8, then G can be represented as a semi-direct product of two Abelian groups.

Proof. We have proved, that G has a symplectic basis and its non-central elements can be separated into pairs. We form two Abelian groups A and B by the following way: we take one of the elements from each pair of one symplectic basis of the group G and we generate the group A by these elements . We generate the group B by taking the other element of the corresponding pair, as well as the central basis elements and G' . So we obtain: $A =< a_1, a_2, ..., a_s >$ and $B =< b_1, b_2, ..., b_s, c_1, c_2, ..., c_r, G' >$, where $c_1, c_2, ..., c_r$ are the central basis elements. Since $B \supseteq G'$, then B is a normal subgroup of G. Let $g \in G$. Then $g = {a_1}^{\alpha_1} ... {a_s}^{\alpha_s} {b_1}^{\beta_1} ... {b_s}^{\beta_s} {c_1}^{\gamma_1} ... {c_r}^{\gamma_r} \in AB$. Therefore, $G = AB$.

We shall consider the following two cases:

1. Let in the basis one pair generate the quaternion group of order eight and let this pair be a_1, b_1 and $p = 2$. Then $A \cap B$ consists of the commutator subgroup and it is generated by $a_1^2 = b_1^2$. Let $g \in A \cap B$. Then $g = {a_1}^{\alpha_1} ... {a_s}^{\alpha_s} \in A$ and $g = {b_1}^{\beta_1} ... {b_s}^{\beta_s} {c_1}^{\gamma_1} ... {c_r}^{\gamma_r} t \in B$, $t \in G'$. Hence,

$$(3.1) \qquad {a_1}^{\alpha_1} ... {a_s}^{\alpha_s} {b_1}^{-\beta_1} ... {b_s}^{-\beta_s} {c_1}^{-\gamma_1} ... {c_r}^{-\gamma_r} t^{-1} = 1.$$

Let $Q_8 =< a_1, b_1 >$. In (3.1.) the element t^{-1} can be included in the element $b_1^{-\beta_1}$, since the elements, which participate in (3.1), are from a symplectic basis of G. Then all factors, except for a_1 and b_1, will be equal to the unit and this equation will be reduced to $a_1^{\alpha_1} b_1^{-\beta_1} = 1$. However the obtained equation is an equation in Q_8 and it is possible only when α_1 and β_1 are even numbers. Therefore, $A \cap B$ coincides with G'.

2. In the symplectic basis of the group G there is not a pair, which generates Q_8. Then we consider again the equation (3.1). In this case $< a_i > \cap < b_i > = 1$, where a_i and b_i form a pair in the basis and then in (3.1) each factor will be equal to the unit. Hence $A \cap B = 1$ and therefore, in this case the group G is a semi-direct product of A and B. □

Lemma 3.7. Let G be a finite p-group and let G' have an order p. Suppose, that G is represented according to Theorem 3.6. Then $|A/Z \cap A| = p^s$, $|B/Z \cap B| = p^s$ and $|G/Z| = p^{2s}$, where Z is the center of the group G.

Proof. Consider two cases:

1. Let G be a semi-direct product of the subgroups A and B. Then $|G| = |A|.|B|$, since $A \cap B = 1$. Furthermore

$$Z = (Z \cap A)(Z \cap B).$$

Therefore,

$$|Z| = |Z \cap A||Z \cap B|,$$

$$|G/Z| = \frac{|G|}{|Z|} = \frac{|A|.|B|}{|Z \cap A||Z \cap B|} = \frac{|A|}{|Z \cap A|}\frac{|B|}{|Z \cap B|} =$$
$$= |A/(Z \cap A)||B/(Z \cap B)|.$$

However

$$A =< a_1, a_2, ..., a_s >, B =< b_1, b_2, ..., b_s, c_1, c_2, ..., c_r > .$$

Since each element of degree p commutes with all elements of G, then we have $A^p \subseteq Z$. We consider the factor group $A/(Z \cap A)$. Since $(a_i(Z \cap A))^p = a_i^p(Z \cap A) = Z \cap A$, then $A/(Z \cap A)$ is an elementary Abelian group. Therefore, the generating elements have an order p. Hence the whole group is an elementary Abelian group of order p^s and the elements $a_1, a_2, ..., a_s$ form its basis. Then $|A/(Z \cap A)| = p^s$. Analogously, $|B/(Z \cap B)| = p^s$. Then $|G/Z| = p^s p^s = p^{2s}$.

2. Let $G = A.B$. Then

$$|G| = \frac{|A||B|}{|A \cap B|} = \frac{|A||B|}{|G'|} = \frac{|A||B|}{p} = \frac{|A||B|}{2} = \frac{1}{2}|A||B|;$$

$$|Z| = \frac{1}{2}|Z \cap A||Z \cap B|;$$

$$|G/Z| = \frac{|G|}{|Z|} = \frac{|A||B|}{|Z \cap A||Z \cap B|}$$

and analogously to the first case we obtain that $|G/Z| = p^{2s}$. □

Definition 3.8. We will say, that the elements $a, b \in G$ form *a symplectic pair* , if the following conditions are hold:

1) $[b, a] = c$;

2) the element a has a minimal order in the coset $aC_G(b)$ and

3) the element b has a minimal order in the coset $bC_G(a)$.

Definition 3.9. If a and b form a symplectic pair, the order of a is p^i and the order of b is p^j, then the pair (a, b) is called *a pair of the type* (i, j). The number of the symplectic pairs of the type (i, j) we will denote by δ_{ij}, $i, j \in \{1, 2, ..., k\}$.

It is not hard to see, that the factor group G/Z is an elementary Abelian p-group. Therefore, it can be considered as a linear space over the field $GF(p)$ of p-elements. The operations in this linear space are determined by

$$aZ + bZ =^{def} abZ, \tag{3.2.}$$

(3.3.) $$\lambda(aZ) =^{def} a^{\lambda}Z.$$

We shall prove, that the operations of (3.2) and (3.3) are correct.

In fact $a_1Z = aZ$ implies $a_1 = az_1$ and $b_1Z = bZ$ implies $b_1 = bz_2$, $z_1, z_2 \in Z$. Then

$$a_1Z + b_1Z =^{def} a_1b_1Z = abZ =^{def} aZ + bZ$$

and

$$\lambda(a_1Z) =^{def} a_1^{\lambda}Z = (az_1)\lambda^Z = a^{\lambda}z_1^{\lambda}Z = a^{\lambda}Z =^{def} \lambda(aZ).$$

Let $a, b \in G$. Since $[a, b] \in G' =< c >$, then $[a, b] = c^{\alpha}$, $\alpha \in GF(p)$.

Then we denote by $\alpha = log_c[a, b]$.

Definition 3.10. In the obtained linear space G/Z over the field $GF(p)$ we introduce *a symplectic product* (aZ, bZ), where $aZ, bZ \in G/Z$ by the following way: $(aZ, bZ) = log_c[a, b]$.

We shall prove, that the Definition 3.10 is correct. In fact $a_1Z = aZ$ implies $a_1 = az_1$ and $b_1Z = bZ$ implies $b_1 = bz_2$, $z_1, z_2 \in Z$. Let $(aZ, bZ) = log_c[a, b]$ and $(a_1Z, b_1Z) = log_c[a_1, b_1]$. Then

$$(a_1Z, b_1Z) = log_c[a_1, b_1] = log_c[az_1, bz_2] =$$
$$= log_c([a, b][a, z_2][z_1, b][z_1, z_2]) = log_c[a, b] = (aZ, bZ).$$

Lemma 3.11. The symplectic product $(x, y) \in GF(p)$ has the following properties:

1) $(x, y) = -(y, x)$;
2) $(x_1 + x_2, y) = (x_1, y) + (x_2, y)$;
3) $(x, y_1 + y_2) = (x, y_1) + (x, y_2)$;
4) $(x, x) = 0$;
5)$(\lambda x, y) = \lambda(x, y)$ and

6) $(x, \lambda y) = \lambda(x, y)$

for $x, y, x_1, x_2, y_1, y_2 \in G/Z$, $\lambda \in Z$.

Proof. We put $x = aZ$, $y = bZ, x_1 = a_1Z, x_2 = a_2Z$. Suppose, that $\lambda, \lambda_1, \lambda_2 \in GF(p)$.

1) Let $(aZ, bZ) = \alpha$, i.e. $[a, b] = c^{\alpha}$. Then $[b, a] = c^{-\alpha}$, i.e. $(aZ, bZ) = -(bZ, aZ)$.

2) Let $(a_1Z, bZ) = log_c[a_1, b]$, $(a_2Z, bZ) = log_c[a_2, b]$. Then

$(x_1 + x_2, y) = (a_1Z + a_2Z, bZ) =^{def} (a_1a_2Z, bZ) =$

$= log_c[a_1a_2, b] = log_c[a_1, b][a_2, b] =$

$= (x_1, y) + (x_2, y) = (a_1Z, bZ) + (a_2Z, bZ) =$

$= log_c[a_1, b] + log_c[a_2, b] = log_c([a_1, b][a_2, b])$.

3) The proof is analogously to 2).

4) $(x, x) = (aZ, aZ) = log_c[a, a] = log_c 1 = 0$.

5) $(\lambda x, y) = (\lambda aZ, bZ) = (a^{\lambda}Z, bZ) = log_c[a^{\lambda}, b] = log_c[a, b]^{\lambda} = \lambda log_c[a, b] = \lambda(x, y)$.

6) The proof is analogously to 5). □

Definition 3.12. A linear space, where a symplectic product is determined , is called *a symplectic space*.

4. Invariants of finite p-groups with a minimal commutator subgroups

We introduce the following indications:

$G_{ij} = G[p^i] \cap C_G(G[p^{j-1}])$,

i.e. G_{ij} consists of all elements of the group G, whose orders are less than or equal to p^i and which commute with all elements of order less than or equal to p^{j-1}.

Lemma 4.1. If $i_1 \leq i$ or $j \leq j_1$, then $G_{i_1j_1} \subseteq G_{ij}, i, i_1, j, j_1 \in \mathbb{N}$.

Proof. The inequality $i_1 \leq i$ implies $G[p^{i_1}] \subseteq G[p^i]$. Then $j-1 \leq j_1 - 1$ implies $C_G(G[p^{j_1-1}]) \subseteq C_G(G[p^{j-1}])$ and $G_{i_1j_1} \subseteq G_{ij}$. □

Let $i < j$ and let the number of the symplectic pairs of the type (i, j) in one fixed basis of G be s . Let these pairs be $(x_1, y_1), (x_2, y_2), ...,$

(x_s, y_s). We form the group $H = \langle x_1, x_2, ..., x_s \rangle$, where x_k are of order p^i and y_k are of order p^j, for $i, j, k \in \{1, 2, ..., s\}$. The group H is an Abelian group, since if we take two different symplectic pairs, then each element of one pair will commute with each element of the other pair. These elements form a basis, since they are from the basis of G. The group H decomposes into the direct product $H =< x_1 > \times < x_2 > \times ... \times < x_s >$.

Lemma 4.2. Let $i < j$. Then $G_{ij} = HG_{i-1j}G_{ij+1}$, $i, j \in \mathbb{N}$.

Proof. The definitions for $G_{ij} = G[p^i] \cap C_G(G[p^{j-1}])$ and $H =< x_1 > \times < x_2 > \times ... \times < x_s >$ imply $H \subseteq G$. Hence, by lemma 4.1, we obtain $HG_{i-1j}G_{ij+1} \subseteq G_{ij}$.

Let $x \in G_{ij}$. Denote by G_i the subgroup of G, which is generated by all non-central basis elements of G of order p^i. This subgroup can be represented as $G_i = H.F.T$, where F is generated by the basis elements of G_i, which commute with the elements of $G[p^i]$ and T is generated by the remaining basis elements of G_i. We can see at once that $F \subseteq G_{ij+1}$. It holds $x \in G_{ij} \subseteq G[p^i]$. Therefore, $x = x_1 x'$, where $x \in G[p^{i-1}]$, $x' \in G_i$. Then $x' = x_2 x_3 x_4$, where $x_2 \in H$, $x_3 \in F$, $x_4 \in T$. Then $x = x_1 x_2 x_3 x_4$. Since $x_2 \in h \subseteq G_{ij}$ and $x_3 \in F \subseteq G_{ij+1} \subseteq G_i j$, then $x_2 x_3 \in G_{ij}$. Hence, in view of $x \in G_{ij}$ it follows $x_1 x_4 \in G_{ij}$. Let $x_4 = t_1^{\alpha_1} t_2^{\alpha_2} ... t_k^{\alpha_k} c^{\alpha}$, where $t_1, t_2, ..., t_k$ are the generating elements of T. Let $(t_1, t_1'), (t_2, t_2'), , , (t_k, t_k')$ be the corresponding symplectic pairs of the basis of G. The definitions of the groups H, F and T imply $t_l' \in G[p^{j-1}]$ for $l \in \{1, 2, ..., k\}$. Then $x_1 x_4$ commutes with t_l' for $l \in \{1, 2, ..., k\}$. Since t_l' commutes with all basis elements of G except t_l, then α_l is divided by p for $l \in \{1, 2, ..., k\}$. Consequently, the element x_4 has an order less than or equal to p^{i-1}. Besides $|x_1| \leq p^{i-1}$. Hence $x_1 x_4 \in G[p^{i-1}]$. Then $x_1 x_4 \in G_{ij}$ implies $x_1 x_4 \in G_{i-1j}$ and $G_{ij} \subseteq HG_{i-1j}G_{ij+1}$.

Note, that in the reasoning $x = x_1 x_2 x_3 x_4$ the factor x_4 can move to the second place, since G_{ij+1} is a normal subgroup of G and x_4 commutes with x_2.

We shall also note, that all reflections in the proof of this lemma are led for $i \geq 2$. If $i = 1$ these reflections are still in force assuming

that $G_{i-1j} = 1$. The lemma is proved. □

Theorem 4.3.[7](Theorem 4.7.2. p. 112) If H is a subgroup of G and K is a normal subgroup of G, then $H \cap K$ is a normal subgroup of H and $HK/K \cong H/(H \cap K)$.

Consider $HG_{i-1j}G_{ij+1}/G_{i-1j}G_{ij+1}$. Then, by Lemma 3.6 and Theorem 3.7,

$$G_{ij}/G_{i-1j}G_{ij+1} = HG_{i-1j}G_{ij+1}/G_{i-1j}G_{ij+1} \cong H/(H \cap G_{i-1j}G_{ij+1}).$$

Lemma 4.4. If $i < j$, then $H \cap G_{i-1j}G_{ij+1} = H^p$, $i, j \in \mathbb{N}$.

Proof. We have $H^p \subseteq H$. Besides $H^p \subseteq Z$. Hence $H^p \subseteq C(G[p^{j-1}])$. The elements of H are of order, less than or equal to p^i. Therefore, $H^p \subseteq G[p^{i-1}]$, $H^p \subseteq G_{i-1j} \subseteq G_{i-1j}G_{ij+1}$ and $H^p \subseteq H \cap G_{i-1j}G_{ij+1}$.

We have to prove the converse, namely $H \cap G_{i-1j}G_{ij+1} \subseteq H^p$. Let $x \in H \cap G_{i-1j}G_{ij+1}$ be an arbitrary element. Then $x \in H$ and therefore, $x = x_1^{\alpha_1}x_2^{\alpha_2}...x_s^{\alpha_s}$. We have to prove, that each exponent α_i is divided by p. Namely then x will belong to H^p. We have $x = yz$, where $y \in G_{i-1j}$ and $z \in G_{ij+1}$. Consequently, $x_1^{\alpha_1}x_2^{\alpha_2}...x_s^{\alpha_s} = yz$. We choose an arbitrary factor $x_t^{\alpha_t}$. Our aim is to show that α_t is divided by p . The element x_t is from the basis of G and participates in the symplectic pair (x_t, y_t) of the type (i, j). Since $z \in G_{ij+1}$, then $z \in C_G(G[p^j])$, the order of y_t is p^j and $y_tz = zy_t$. Besides $y \in G_{i-1j}$ implies $y \in G[p^{i-1}]$. Hence y is expressed by the elements of the basis, which are of order less than or equal to p^{i-1} and the order of (x_t) is p^i. Therefore, x_t can not participate in the presentation of y by elements of the basis. Then y_t will commute with y, since y_t does not commute only with x_t . Consequently, , $yy_t = y_ty$. On the other hand y_t commutes with y and with z. Hence y_t commutes with yz and $x_1^{\alpha_1}x_2^{\alpha_2}...x_s^{\alpha_s} = yz$ implies y_t commutes with $x_1^{\alpha_1}x_2^{\alpha_2}...x_s^{\alpha_s}$. But y_t commutes with all factors except x_t and if α_t is not divided by p, then y_t does not commute with $x_t^{\alpha_t}$. Therefore, α_t is divided by p. Since α_t was selected arbitrary, then all exponents are divided by p and $x \in H^p$. □

Theorem 4.5. Let $i < j$. Then $G_{ij}/G_{i-1j}G_{ij+1} \cong H/H^p$, $i, j \in \mathbb{N}$.

Proof. By application of Lemma 4.2, Theorem 4.3 and Lemma 4.4 we obtain

$$G_{ij}/G_{i-1j}G_{ij+1} = HG_{i-1j}G_{ij+1}/G_{i-1j}G_{ij+1} \cong$$

$$\cong H/(H \cap G_{i-1j}G_{ij+1}) = H/H^p.$$

□

It is obvious, that $\delta_i = \sum_{j=1}^{n} \delta_{ij}$, where δ_i is the $i-$th Ulm-Kaplansky invariant of G/G'. Then δ_i is an invariant of G. Therefore, it can be proved, that δ_{ii} are invariants of the group G.

Lemma 4.6. If the key subgroup is not cyclic, then it is a minimal group of the second or the third type and its forming elements form a symplectic pair.

Proof. Let the key subgroup be of the second type. Then $a^{p^\alpha} = 1, b^{p^{\beta-1}} = c$. We have to prove, that the element a has the lowest order in the coset $aC_G(b)$ and the element b has the lowest order in the coset $bC_G(a)$. The key subgroup is one of the factors in the decomposition in a central commutator product. Then we can determine $C_G(a)$ and $C_G(b)$. Since $G = K * T$ and K is the key subgroup, we consider $C_G(a) =< a > \times < b^p > \times T$, . Therefore, $T \subseteq C_G(a)$ and $T \subseteq C_G(b)$.

Let us consider the elements of $bC_G(a)$. They are of the type: $a^\lambda b^{1+\mu p} t$. We raise in degree $p^{\alpha-1}$ and then $\left(a^\lambda b^{1+\mu p} t\right)^{p^{\beta-1}} \neq 1$, i.e. $a^{\lambda p^{\beta-1}} b^{p^{\beta-1}} b^{\mu p^\beta} t^{p^{\beta-1}} \neq 1$. We assume, that $a^{\lambda p^{\beta-1}} b^{p^{\beta-1}} t^{p^{\beta-1}} = 1$. Then $a^{\lambda p^{\beta-1}} = 1$, $b^{p^{\beta-1}} = 1$, $t^{p^{\beta-1}} = 1$. Since $b^{p^{\beta-1}} \neq 1$, then we obtain a contradiction. Analogously, we consider $C_G(b) =< a^p > \times < b > \times T$ and obtain the same result. □

Theorem 4.7. The key subgroup of the group G is unique up to isomorphism.

Proof. We will first consider the case, when G is of the central type. Then the key subgroup of G is cyclic and its order is $ph_Z(c)$ and $ph_Z(c) = ph_G(c)$. Since $h_Z(c)$ is an invariant of c , then this cyclic subgroup is defined up to isomorphism.

Let G be a group of a non-central type. Let W_1 be the key subgroup of G and let the order of G be greater or equal to 16. Let G be not isomorphic to the following group:

$$(*) \qquad a^4 = 1, b^2 = c, [b, a] = c.$$

Then W_1 will generate by the elements a_1 and b_1 , so that

$a_1^{p^{\alpha_1}} = 1, b_1^{p^{\beta-1}} = c, [b_1, a_1] = c.$

In this case the elements a_1 and b_1 form a symplectic pair.

Let $p^{\beta-1} \neq 2$ and let W_2 be other key subgroup of G . Then it is generated by the elements a_2 and b_2. Here the condition $b_2^{p^{\beta-1}} = c$ is hold, since $h_G(c) = p^{\beta-1}$ and this height is an invariant of G . In this case the group W_2 has an order greater or equal to 16. Furthermore W_2 is not cyclic, since the group G is of a non-central type. Therefore, W_2 is of the type:

$a_2^{p^{\alpha_2}} = 1, b_2^{p^{\beta-1}} = c, [b_2, a_2] = c.$

The equations $b_1^{p^{\beta-1}} = c$ and $b_2^{p^{\beta-1}} = c$ imply $b_1^{p^{\beta-1}} = b_2^{p^{\beta-1}}$. Since $p^{\beta-1} > 2$, then the last equation implies $(b_1 b_2^{-1})^{p^{\beta-1}} = 1$. If the element b_2 commutes with a_1, then $b_2^{-1} \in C_G(a_1)$. Then $b_1 b_2^{-1} \in b_1 C_G(a_1)$. This element has an order $p^{\beta-1} < p^{\beta} = o(b_1)$. Since in the coset $b_1 C_G(a_1)$ the element b_1 has the lowest order , then we obtain a contradiction with the fact that $b_1 b_2^{-1}$ has lower order, since the elements a_1 and b_1 form a symplectic pair. Therefore, b_2 does not commute with a_1 , i.e. $a_1 \notin C_G(b_2)$. Since each element, which does not belong to $C_G(b_2)$, has an order, greater or equal to the order of a_2, then $o(a_1) \geq o(a_2)$. By symmetry proves that $o(a_2) \geq o(a_1)$. Then $o(a_1) = o(a_2)$ and $\alpha_1 = \alpha_2$. Therefore, $W_1 \cong W_2$.

Let $p^{\beta-1} = 2$. Then we consider the groups:

$W_1 : a_1^{2^{\alpha_1}} = 1, b_1^2 = c, [b_1, a_1] = c;$

$W_2 : a_2^{2^{\alpha_2}} = 1, b_2^2 = c, [b_2, a_2] = c.$

First, we will prove, that if $2^{\alpha_1} > 4$, then b_1 and b_2 commute. Consider $C_G(b_1)$. The index of $C_G(b_1)$ in the group G is 2 and the cosets of G by $C_G(b_1)$ are $C_G(b_1)$ and $a_1C_G(b_1)$. If b_2 does not commute with b_1 , then $b_2 \in a_1C_G(b_1)$. In this coset each element has order greater or equal to the order of a_1, but $o(a_1) = 2^{\alpha_1}$ and $2^{\alpha_1} > 4$. This is a contradiction. Therefore, b_1 and b_2 commute. Then $(b_1b_2)^2 = b_1^2b_2^2 = c.c = 1$ and hence $o(b_1b_2) = 2$.

We assume that b_2 does not commute with a_1. Then the element $b_1b_2 \in b_1C_G(a_1)$ has an order 2 and the minimal order is $o(b_2) = 4$. Then we obtain a contradiction and a_1 and b_2 do not commute, i.e. $a_1 \notin C_G(b_2)$. All elements, which do not belong to $C_G(b_2)$, have order, greater or equal to $o(a_2)$. Then $o(a_1) \geq o(a_2)$. Analogously, $o(a_2) \geq o(a_1)$. Then $o(a_1) = o(a_2)$. Therefore, when $p^{\beta-1} > 2$ or $p^{\beta-1} = 2$ and $2^{\alpha_1} > 4$, we obtain, that the key subgroup of G is unique. We will consider the cases, when the key subgroup is isomorphic to the group $(*)$, or to D_8, or to Q_8.

Let G be a group, which has a key subgroup and this key subgroup is isomorphic to one of the three above-mentioned groups. Then G is decomposed as a central commutator product of key subgroup of selected type and minimal groups of first type and eventually groups of the type D_8 . Consider the subgroup $G[4]$. We know, that it is an invariant of G. Consider $G[4]/C$. We obtain an elementary Abelian 2-group. The number of the direct factors of order 2 in this group is defined by the number of the minimal groups of the first type, the groups of the type D_8 and the key subgroup. It is proved, that the number of the minimal groups of the first type is an invariant. Then the number of the groups of the type D_8 and the key subgroup is an invariant. Hence, we obtain an invariant of the group G. This group is decomposed as a central commutator product of the selected key subgroup and groups of the type D_8 . We denote the total number of the factors by n. One of these factors is the key subgroup and the number of the groups of the type D_8 is $n-1$, where$n \in \mathbb{N}$. We define the number of the elements of order 2 in this group. It can be verified by immediate calculations, that the number of the elements of order

2 in these three cases of groups is:

First case: if $W \cong (*)$, then the number of involutions is $4^n - 1$.

Second case: if $W \cong Q_8$, then the number of involutions is $4^n - 2^n - 1$.

Third case: if $W \cong D_8$, then the number of involutions is $4^n + 2^n - 1$.

Therefore, in this case the key subgroup of G is unique up to isomorphism. □

Lemma 4.8. Let the group G be represented in the form: $G = W * B \times A$. Then

$$Z^{p^i}[p]/G^{p^{i+1}}[p] \cong A^{p^i}[p]/A^{p^{i+1}}[p].$$

Proof. Let G be represented in the form: $G = W * B \times A$. Then

$$Z = W^p \times B^p \times A.$$

Hence

$$Z^{p^i} = W^{p^{i+1}} \times B^{p^{i+1}} \times A^{p^i}.$$

Then

$$Z^{p^i}[p] = W^{p^{i+1}}[p] \times B^{p^{i+1}}[p] \times A^{p^i}[p]$$

and

$$G^{p^{i+1}}[p] = W^{p^{i+1}}[p] \times B^{p^{i+1}}[p] \times A^{p^{i+1}}[p].$$

Therefore,

$$Z^{p^i}[p]/G^{p^{i+1}}[p] \cong A^{p^i}[p]/A^{p^{i+1}}[p].$$

□

Theorem 4.9. Let G be a finite p-group with a commutator subgroup of order p. Then the invariants of the key subgroup of G, the numbers δ_i , δ_{ij} for $i < j$, $(i < j,\ i, j \in \mathbb{N})$ and $Z^{p^i}[p]/G^{p^{i+1}}[p]$ form a full system of invariants of the group G.

The following theorem is a main result of the paper and it gives a criterion for isomorphism of finite p-groups with a commutator subgroup of order p.

Theorem 4.10. Let G be a finite p-group with a commutator subgroup of order p and let H be an arbitrary group. Then the groups G and H are isomorphic if and only if H is a finite p-group with a commutator subgroup of order p and the following conditions hold:

1) the key subgroups W_G and W_H of the group G and H are isomorphic;

2) $\delta_{ij}(G) = \delta_{ij}(H)$ for $i < j$;

3) $\delta_i(G) = \delta_i(H)$ and

4) $|Z_G^{p^i}[p]/G^{p^{i+1}}[p]| = |Z_H^{p^i}[p]/H^{p^{i+1}}[p]|$.

The proofs of the Theorems 4.9 and 4.10 imply directly of the assertions, which are proved earlier. □

An announcement of the results of this paper is submitted for publication in [9].

REFERENCES

[1]Akinola, A. D. , *On subgroups of a finite p-groups*, *International Journal of Scientific and Engineering Research* , **2**(Oct-2011), 1-4.

[2]Berkovich, Ya.G. , *On the order of the commutator subgroup and the Schur multiplier of a finite p-group*, *Journal of Algebra* , **144**(15.Dec.1991), 269-272.

[3] Cheng, Y. , *On finite p-groups with cyclic commutator subgroup, Archiv der Mathematik* , **39**(8.10.1982), 295-298.

[4] Finogenov, A.A. , *Finite p-groups with a cyclic commutator subgroup*, *Algebra and Logic* , **34**(March-April, 1995), 125-129.

[5] Glauberman, G., *Centrally large subgroups of finite p-groups*, *Journal of Algebra*, **300**(2006), 480-508.

[6] Glauberman, G., *Large subgroups of small class in finite p-groups*, *Journal of Algebra*, **272**(2004), 128-153.

[7] Hall, M., *The Theory of Groups*, *New York, Maximilian company*, (1959).

[8]Miech, R.J. , *On p-groups with a cyclic commutator subgroup*, *J.Austral. Math. Soc.*, **20**(1975), 178-198.

[9]Keranova, N., Nachev, N., *Invariants of finite p-groups with a minimal commutator subgroup*, *Compt. rend. Acad. bulg. Sci.*, **68**(No 1), (2015), 5-10