NOVI SAD J. MATH.
VOL. 32, NO. 1, 2002, 101-107

DERIVAL AUTOMORHISMS OF GROUPS AND A CLASSIFICATION PROBLEM

Mihai Chiş[1], Codruţa Chiş[2]

Abstract. In this paper, we define a class of automorphisms of groups – the class of derival automorphisms, and determine all finite groups with no more than three orbits with respect to the action of their groups of derival automorphisms.

AMS Mathematics Subject Classification (2000): 20F28

Key words and phrases: automorphism, derival automorphism, commutator subgroup

1. Introduction

Let G be a group, N a characteristic subgroup of G, and α an automorphism of G. Since $\alpha(N) = N$, for any $g \in G$ holds $\alpha(gN) = \alpha(g)N$, so that we can define a function

$$\overline{\alpha} : G/N \longrightarrow G/N : gN \longmapsto \alpha(g)N,$$

which is obviously an automorphism of G/N.

Remark 1. *The function*

$$\alpha \longmapsto \overline{\alpha} : Aut(G) \longrightarrow Aut(G/N)$$

is a homomorphism of groups.

Proof. For any $g \in G$, and any $\alpha, \beta \in Aut(G)$ we have

$$\overline{\alpha \circ \beta}(gN) = (\alpha \circ \beta)(g)N = \alpha(\beta(g))N =$$

$$= \overline{\alpha}(\beta(g)N) = \overline{\alpha}(\overline{\beta}(gN)) = (\overline{\alpha} \circ \overline{\beta})(gN).$$

Definition 2. *The kernel of this homomorphism is a subgroup of the automorphism group of the group G. We shall call the elements of this kernel N-al automorpisms of the group G. They are precisely those automorphisms which leave invariant the cosets of the characteristic subgroup N.*

[1]Universitatea de Vest Timişoara, Facultatea de Matematică, b-dul V.Pârvan, nr.4, 1900, Timişoara, România
[2]Universitatea Banatului din Timişoara, Facultatea de Ştiinţe Economice, b-dul Pestalozzi, nr.22, 1900, Timişoara, România

Remark 3. *In the manner described above, one can define various classes of automorphisms of a group.*

Definition 4. *For $N = Z(G)$, the center of the group G, the automorphisms which invariate the cosets of $Z(G)$ are called the central automorphisms of G.*

Definition 5. *Taking $N = G'$, we shall call derival automorphisms of G the automorphisms which invariate the cosets of the commutator subgroup G' of the group G. The group of derival automorphisms of G will be denoted $\mathcal{D}(G)$.*

Lemma 6. *Every inner automorphism is a derival automorphism.*

Proof. Let $g \in G$ be an arbitrary element of G, and $i_g : G \longrightarrow G : x \longmapsto g^{-1}xg$ the inner automorphism associated with g. Then

$$i_g(x) = g^{-1}xg = xx^{-1}g^{-1}xg = x[x, g] \in xG', \quad (\forall)x \in G,$$

hence $i_g(xG') = xG', (\forall)x \in G$, and i_g is a derival automorphism of the group G. □

Corollary 7. *$Inn(G) \leq \mathcal{D}(G)$.*

Definition 8. *Let $\mathcal{N} \leq Aut(G)$ be a group of automorphisms of G. $\mathcal{N}$ acts naturally on G via*

$$(\nu, g) \longmapsto \nu(g), \quad (\forall)\nu \in \mathcal{N}, g \in G.$$

We shall call $\mathcal{N}$-orbits the orbits of G with respect to this action.

Remark 9. *Let $S \subseteq G$ be a subset of G which is invariant with respect to the action of $\mathcal{N}$, i.e. $\nu(S) = S$ holds for any $\nu \in \mathcal{N}$. Then S is a union of $\mathcal{N}$-orbits.*

Proof. Since S is $\mathcal{N}$-invariant, for any $s \in S$ we have

$$s \in orb_{\mathcal{N}}(s) = \{\nu(s)|\nu \in \mathcal{N}\} \subseteq S.$$

Hence $S \subseteq \bigcup_{s\in S} orb_{\mathcal{N}}(s) \subseteq S$, so that $S = \bigcup_{s\in S} orb_{\mathcal{N}}(s)$. □

Notation. We shall denote by $n(G)$ the number of $\mathcal{N}$-orbits of G. If $S \subseteq G$ is a $\mathcal{N}$-invariant subset of G, $n_G(S)$ will be the number of $\mathcal{N}$-orbits in which decomposes S.
Obviously, if S is a $\mathcal{N}$-invariant subset of G, then $G \setminus S$ is also $\mathcal{N}$-invariant, and the following equality holds:

$$n(G) = n_G(S) + n_G(G \setminus S).$$

Notation. For some particular classes of automorphisms of a group G we shall use the following notations:

• $\mathcal{N} = Aut(G)$: $a(G) = \#$ of $Aut(G)$-orbits, $a_G(S) = \#$ of $Aut(G)$-orbits in a characteristic subset S of G;
• $\mathcal{N} = Inn(G)$: $k(G) = \#$ of $Inn(G)$-orbits$= \#$ of conjugacy classes of G, $k_G(S) = \#$ of $Inn(G)$-orbits$= \#$ of conjugacy classes in a normal subset S of G;
• $\mathcal{N} = \mathcal{C}(G)$: $c(G) = \#$ of $\mathcal{C}(G)$-orbits, $c_G(S) = \#$ of $\mathcal{C}(G)$-orbits in a $\mathcal{C}(G)$-invariant subset S of G;
• $\mathcal{N} = \mathcal{D}(G)$: $d(G) = \#$ of $\mathcal{D}(G)$-orbits, $d_G(S) = \#$ of $\mathcal{D}(G)$-orbits in a $\mathcal{D}(G)$-invariant subset S of G.

Let $\mathcal{M}, \mathcal{N} \leq Aut(G)$ be subgroups of the automorphism group of a group G, with $\mathcal{M} \leq \mathcal{N}$. Then every $\mathcal{N}$-orbit is $\mathcal{M}$-invariant, hence it is a union of $\mathcal{M}$-orbits.

Corollary 10. *Let S be a $\mathcal{N}$-invariant subset of G, and let $n_G(S)$ and $m_G(S)$ be the number of $\mathcal{N}$-orbits, respectively $\mathcal{M}$-orbits of S. Then $n_G(S) \leq m_G(S)$.*

Proof. S decomposes into $\mathcal{N}$-orbits, which decompose into $\mathcal{M}$-orbits. The inequality is now obvious. □

2. Some bounds for $d(G)$

Theorem 11. *The number $d(G)$ of $\mathcal{D}(G)$-orbits of a group G is not greater than the number of conjugacy classes of G.*

Proof. This follows immediately from the fact that $Inn(G) \leq \mathcal{D}(G)$ and that the conjugacy classes of the group G are precisely the orbits with respect to the natural action of $Inn(G)$ on G. □

Theorem 12. *Let G be a group, $\mathcal{D}(G)$ the group of derival automorphisms of G, $\mathcal{N} \leq Aut(G)$ a subgroup of the automorphism group of G such that $\mathcal{D}(G) \leq \mathcal{N}$, and S an $\mathcal{N}$-invariant subset of G. Then the following inequalities hold:*

$$\begin{array}{rcl} d(G) & \geq & d_G(S) + n_G(G \setminus S) \\ d(G) & \geq & n_G(S) + d_G(G \setminus S) \\ d(G) & \geq & n(G). \end{array}$$

Proof. Since $\mathcal{D}(G) \leq \mathcal{N}$, we have the inequalities $d_G(S) \geq n_G(S)$ and $d_G(G \setminus S) \geq n_G(G \setminus S)$, which prove the result. □

Remark 13 *From the definition of derival automorphisms follows that every $\mathcal{D}(G)$-orbit is contained in a coset of the commutator subgroup G' in G. As a consequence we have the inequality*

$$d(G) \geq |G : G'|.$$

Corollary 14 *The following inequality holds:*

$$d(G) \geq d_G(G') + |G : G'| - 1.$$

Proof. $G \setminus G'$ is a $\mathcal{D}(G)$-invariant subset of G and $d_G(G \setminus G') \geq |G : G'| - 1 = \#$ of cosets of G' contained in $G \setminus G'$. □

Remark 15. *Since $\mathcal{D}(G) \leq Aut(G)$ and G' is a chracteristic subgroup of G, we can refine the previous inequality. We have $d_G(G') \geq a_G(G')$, hence*

$$d(G) \geq a_G(G') + |G : G'| - 1.$$

Theorem 16. *$d(G) = |G : G'|$ if and only if G is abelian.*

Proof. If G is abelian, then $G' = 1$ and $\mathcal{D}(G) = \{1_G\}$, so that $d(G) = |G| = |G : G'|$.
If $d(G) = |G : G'|$ then from the inequality above follows that $a_G(G') = 1$, hence $G' = 1$ and G is abelian. □

Theorem 17. *If G is a group with $|G : G'| = 2$, then $\mathcal{D}(G) = Aut(G)$ and $d(G) = a(G)$.*

Proof. Because $|G/G'| = 2$, we have $Aut(G/G') = \{1_{G/G'}\}$, hence the kernel of the group homomorphism

$$\alpha \mapsto \overline{\alpha} : Aut(G) \longrightarrow Aut(G/G')$$

is $Aut(G)$. But $\mathcal{D}(G)$ was defined to be exactly this kernel. We obtain $\mathcal{D}(G) = Aut(G)$ and then obviously $d(G) = a(G)$. □

3. Groups with few $\mathcal{D}(G)$-orbits

In this section we are going to determine all finite groups G with no more than three $\mathcal{D}(G)$-orbits. We shall discuss seperately the cases $d(G) = 1$, $d(G) = 2$, and $d(G) = 3$.

3.1. The case $d(G) = 1$

Theorem 18. *$d(G) = 1$ if and only if $G = 1$.*

Proof. Obviously, if $G = 1$, then $d(G) = 1$.
Suppose now that $d(G) = 1$. Because $d(G) \geq a(G)$, we have $a(G) = 1$. The group G has only one orbit with respect to the action of $Aut(G)$. Hence all elements of G have the same order, and since $o(1) = 1$, this order is 1. G contains then only the unit element, so $G = 1$. □

3.2. The case $d(G) = 2$

Theorem 19 $d(G) = 2$ *if and only if* $G \cong \mathbf{Z}_2$.

Proof. If $G \cong \mathbf{Z}_2$ then $d(G) = d(\mathbf{Z}_2) = 2$.
Let now G be a finite group with $d(G) = 2$. Since $G \neq 1$, we have a number of $Aut(G)$-orbits $a(G) \neq 1$. But then, because $a(G) \leq d(G)$, we must have $a(G) = 2$. $1\, char\, G$, so that one $Aut(G)$-orbit is $\{1\}$. The second $Aut(G)$-orbit is then $G \setminus \{1\}$. The elements in this orbit must have the same order, a number $p \in \mathbf{N}$ with $p \geq 2$. This number is necessarily a prime. Hence G is a p-group.

If G is nonabelian, then $p^2 \mid |G : G'|$. Because of the inequality $|G : G'| \leq d(G) = 2$, we obtain $p^2 \leq 2$, which is impossible for any prime p. The group G is then abelian, so that $|G| = |G : G'| = d(G) = 2$. But then $G \cong \mathbf{Z}_2$. □

3.3. The case $d(G) = 3$

Theorem 20. $d(G) = 3$ *if and only if* $G \cong \mathbf{Z}_3$ *or* $G \cong (\wedge D_p)^n$, *the product with amalgamated factor groups of* n *copies of the dihedral group* D_p, *where* p *is a prime and* $n \in \mathbf{N}$, $n \geq 1$.

Proof. We shall prove first that $d(\mathbf{Z}_3) = d((\wedge D_p)^n) = 3$.
$\mathbf{Z}_3$ is abelian, hence $d(\mathbf{Z}_3) = |\mathbf{Z}_3| = 3$. $(\wedge D_p)^n$ is nonabelian and has the following presentation

$$(\wedge D_p)^n =< a_1, a_2, \ldots, a_n, b | (a_i)^p = 1, [a_i, a_j] = 1, b^2 = 1, (a_i b)^2 = 1 > .$$

We determine first the $Aut(G)$-orbits of $G = (\wedge D_p)^n$. The following subsets of G are obviously characteristic: 1, $G' \setminus \{1\} =< a_1 > \times < a_2 > \times \ldots \times < a_n > \setminus \{1\}$, $G \setminus G' = G'b$. We shall prove that they are precisely the $Aut(G)$-orbits of G:

- The orbit of the unit element is $\{1\}$.
- Any two elements a_i and a_j, with $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$, lie in the same orbit, because if $\tau = (i, j)$, then the function given by $a_k \longmapsto a_{\tau(k)}, (\forall) k = \overline{1, n}$ and $b \longmapsto b$ can be extended to an automorphism of G, which interchanges a_i and a_j.

If now $a \in G' \setminus \{1, a_1, a_2, \ldots, a_n\}$, then a belongs to the orbit of a_1, because the function $a_1 \longmapsto a$, $a_i \longmapsto a_i, (\forall) i = \overline{2, n}$, $b \longmapsto b$ can be extended to an automorphism of G, which sends a_1 into a.
These two remarks prove that the characteristic subset $G' \setminus \{1\}$ is one $Aut(G)$-orbit of G.

- Any element $c \in G \setminus G'$ belongs to the orbit of the element b, because the function given by $a_i \longmapsto a_i, (\forall) i = \overline{1, n}$, $b \longmapsto c$ can be extended to an automorphism of G. This proves that $G \setminus G'$ is also one $Aut(G)$-orbit of G.

Since $|G : G'| = 2$, every automorphism of G is a derival automorphism, hence $d(G) = a(G) = 3$.
We have proved that the groups $\mathbf{Z}_3$ and $(\wedge D_p)^n$ have each exactly three $\mathcal{D}(G)$-orbits. We shall prove now that every finite group G with exactly three $\mathcal{D}(G)$-orbits is isomorphic either with $\mathbf{Z}_3$ or with $(\wedge D_p)^n$ for some prime p and some

natural number n.
Let G be a finite group with $d(G) = 3$. Because of the inequality $a(G) \leq d(G)$, we have $a(G) \in \{1, 2, 3\}$. Obviously, the case $a(G) = 1$ is impossible.
If $a(G) = 2$, then as in the case $d(G) = 2$ follows that G is an abelian p-group, and then $|G| = |G : G'| = d(G) = 3$, hence $G \cong \mathbf{Z}_3$.
Let now $a(G) = 3$. The two nontrivial $\mathcal{D}(G)$-orbits coincide with the two nontrivial $Aut(G)$-orbits. Let x and y be representatives of these two nontrivial orbits. One could encounter then the following situations:

(a) $o(x) = o(y) = p$, with p a prime.

(b) $o(x) = p$, $o(y) = p^2$, with p a prime.

(c) $o(x) = p$, $o(y) = q$, with p and q different primes.

In the cases **(a)** or **(b)**, the group G would be a p-group, which cannot be nonabelian, since then we would have $3 = d(G) \geq |G : G'| = p^2 > 3$. But if G is abelian then $|G| = |G : G'| = d(G) = 3$, and $G \cong \mathbf{Z}_3$. This is impossible because $a(\mathbf{Z}_3) = 2$.
Hence the only possible case is **(c)**, and G is nonabelian. Then we have $G' \neq 1$, and $a_G(G') \geq 2$. From the inequality $d(G) \geq |G : G'| + a_G(G') - 1$ we obtain that $|G : G'| \leq 2$.
From the theorem of Cauchy, we know that for any prime r which divides the order of a finite group there is an element of order r in that group. Since in the group G there are only elements of orders 1, p, and q, the only primes which divide $|G|$ are p and q. From Burnside's $p^a q^b$- theorem follows that G is a soluble group, hence $G \neq G'$, and $|G : G'| \geq 2$.
We conclude that $|G : G'| = 2$, so that 2 is divisor of $|G|$, and the orbits of G with respect to the action of $Aut(G)$ and $\mathcal{D}(G)$ are 1, $G' \setminus \{1\}$, and $G \setminus G'$. We can assume that $q = 2$ and p is an odd prime. Since $|G : G'| = 2$, the orbit of elements of order 2 is $G \setminus G'$, and the orbit of elements of order p is $G' \setminus \{1\}$. G' is thus a p-group with all elements of order p. Also, G' cannot have any characteristic subgroup, because such a subgroup would then be a characteristic subgroup H of G, and G would have at least 4 $Aut(G)$-orbits: 1, $H \setminus \{1\}$, $G' \setminus H$, and $G \setminus G'$. Hence, G' is a characteristic simple p-group. Thus it is an elementary abelian p-group. Let $\{a_1, a_2, \ldots, a_n\}$ be a minimal generating set for G' and $b \in G \setminus G'$. Because every element of the orbit $G \setminus G' = G'b$ of b has order 2, the group G has the following presentation:

$$G =< a_1, a_2, \ldots, a_n, b | (a_i)^p = 1, [a_i, a_j] = 1, b^2 = 1, (a_i b)^2 = 1 > .$$

The group G is then the product with amalgamated factor groups of the n groups $< a_i, b >$, $i = \overline{1, n}$, which are all isomorphic with the dihedral group D_p. We conclude that in this case $G \cong (\wedge D_p)^n$.
This completes the proof. $\square$

References

[1] Chiş, M., Deaconescu, M., Silberberg, Gh., Groups with few central automorphism orbits, P.U.M.A. 1998

[2] C.Chiş, C., Chiş, M., Probleme elementare de Teoria Grupurilor, Ed. Mirton, Timişoara, 1997

[3] Coxeter, H. S. M., Moser, W. O. J., Generators and Relators for Discrete Groups, 3rd ed (Russian transl.), Ed."Nauka", Moscow, 1980

[4] Huppert, B., Endliche Gruppen, Springer-Verlag, Berlin, Heidelberg, New York, 1967

Received by the editors December 20, 2000.