ISOMORPHISM OF FINITE HAMILTONIAN GROUPS

Yordan Epitropov, Nako Nachev

Abstract. *In this paper we find the necessary and sufficient condition for isomorphism of finite Hamiltonian groups. Namely, if G and H are finite Hamiltonian groups, then $G \cong H$ if and only if $G/G^{(1)} \cong H/H^{(1)}$, where $G^{(1)}$ and $H^{(1)}$ are, respectively, the commutator subgroups of G and H.*

Key words: Hamiltonian Group, Central Involution, Commutator Subgroup, Quaternion Group.

1. Introduction

If the group G has the property that every subgroup of it is normal, then G is called Dedekind group.

For example, every Abelian group is a Dedekind group. The norm of each group is also Dedekind group. Every nilpotent T-group is a Dedekind group, and every Dedekind group is a T-group.

It turns out that there are noncommutative groups with this property which are called Hamiltonian groups.

Definition 1.1. *[2, p. 190] A group G is called Hamiltonian if it is non-Abelian and every subgroup of G is normal.*

The finite Hamiltonian groups were introduced by R. Dedekind in 1895.

In [2, Theorem 12.5.4] the following representation of Hamiltonian groups is given directly:

Theorem 1.1. *A Hamiltonian group is the direct product of a quaternion group with an Abelian group in which every element is of finite odd order and an Abelian group of exponent two.*

Thus, the quaternion group is the Hamiltonian group of the smallest order. Every Hamiltonian group is locally finite.

Important results for Hamiltonian groups have been published in recent years. In [3, Proposition 2] is given the number of Hamiltonian groups of an arbitrary order $n = 2^e o$, where o is an odd number. In [6, Theorem 2.1] it is calculated the number of elements of a given order and in [6, Theorem 2.5] the total number of subgroups in a finite Hamiltonian group. In addition, we will note the interesting work [4], in which are examined Hamiltonian groups with perfect order classes.

Hamiltonian groups have applications in diverse fields, including Number Theory, Geometry, Physics, and Cryptography. Their properties make them suitable for the implementations of some computer algorithms.

The authors are not aware of any other necessary and sufficient conditions for isomorphism of finite Hamiltonian groups, other than the direct product from Theorem 1.1 and it's other forms. That makes the condition for isomorphism in Theorem 3.1 particularly valuable.

2. Results on Hamiltonian groups

Lemma 2.1. *A noncommutative group G is a Hamiltionian group if and only if each of its cyclic subgroups is a normal subgroup of G.*

Proof: The necessity follows from the definition of Hamiltonian group.

To prove the sufficiency let us take a subgroup H of the given Hamiltonian group and an element $a \in H$. Then all elements conjugate of a lie in the cyclic subgroup $\langle a \rangle$. Since $\langle a \rangle$ is a subgroup of H, then H contains a together with all elements conjugated of a. From this follows that H is a normal subroup of G.

$\square$

Definition 2.1. *[5, Section 1.13, p. 10] Every element of order 2 of one group is called an involution.*

Proposition 2.1. *The group G is Hamiltonian if and only if the following conditions are fulfilled:*

(2.1) the order of the commutator subgroup $G^{(1)}$ of G is 2;

(2.2) every involution is a central element of G;

(2.3) the second power of every element of order 4 is a generator of $G^{(1)}$;

(2.4) G does not contain an element of order 8.

Proof: The necessity immediately follows from Theorem 1.1.

To prove the sufficiency Lemma 2.1 is used. From condition (2.1) it follows that the Hamiltonian group G is noncommutative.

Let $b \in G$ be an element of odd order. We will prove that b is a central element of the group G. Suppose there exists an element a of G, which does not commute with b. Then we have the equality $a^{-1}ba = bc$, where $\langle c \rangle = G^{(1)}$ and $c^2 = 1$, $c \neq 1$. By raising the equality to the power of m, where m is the order of b, and considering that c is a central element we obtain $c^m = 1$. But since m is an odd natural number and the order of c is 2 then $c^m = c$. From here it follows that $c = 1$, which leads to a contradiction. This proves that every cyclic subgroup of G of odd order is contain in the center of G and thus it is normal.

Condition (2.4) implies that the order of every element of the group G is not divisible by 8. Therefore, every cyclic subgroup of it can be decomposed into a direct product of two cyclic groups, where one of them is of an odd order and the other is of an order of 1, 2 or 4. The unit subgroup is normal and from condition (2.2) follows that the subgroups of order 2 are also normal. From that follows that a cyclic subgroup, whose order is not divisible by 4 is a normal subgroup of G.

It remains to be proven that the cyclic subgroups of order 4 are normal subgroups of the group G and to apply Lemma 2.1. Let $d \in G$ be an element of order 4. Condition (2.3) implies that $d^2 = c$. Let f be an element of G which does not commute with d. Then it holds $f^{-1}df = dc = d^3 \in \langle d \rangle$. This shows that $\langle d \rangle$ is a normal subgroup of G.

□

Note 2.1. *The fact that the commutator subgroup of a Hamiltonian group is a cyclic group of order 2, i.e. condition (2.1), can also be found in [1, Lemma 3, (ii)].*

3. Main result

Theorem 3.1. *If G and H are finite Hamiltonian groups, then $G \cong H$ if and only if $G/G^{(1)} \cong H/H^{(1)}$.*

Proof: *Necessity.* Since the commutator subgroup of every group is a fully characteristic subgroup of this group, then every isomorphism $\varphi : G \to H$

induces isomorphism $\varphi^{(1)} : G^{(1)} \to H^{(1)}$. From here immediately follows the isomorphism $\bar{\varphi} : G/G^{(1)} \to H/H^{(1)}$.

Sufficiency. Let us denote the quaternion group of order 8 with Q_8. From Theorem 1.1 we have the direct decompositions

$$G = A \times B \times C \quad \text{and} \quad H = D \times E \times F, \tag{1}$$

where $A \cong Q_8$ and $D \cong Q_8$, B and E are finite groups of odd order, C and F are finite groups with exponent 2. Since $G^{(1)} \leq A$ and $H^{(1)} \leq D$ then

$$G/G^{(1)} \cong A/G^{(1)} \times B \times C \;\text{ and }\; H/H^{(1)} \cong D/H^{(1)} \times E \times F.$$

The isomorphism of those quotient groups implies that

$$A/G^{(1)} \times B \times C \cong D/H^{(1)} \times E \times F. \tag{2}$$

The subgroups B and E coincide with the sets of all elements of odd order of the respective quotient groups and due to that they are fully characteristic subgroups of those quotient groups. Then from the isomorphism (2) follows $B \cong E$. For the cardinality of C and F from this isomorphism it follows the equality $1 + |C| = 1 + |F|$ from where $|C| = |F|$. But since C and F are Abelian with exponent 2, then from the equality of their cardinality follows $C \cong F$. And so we obtain

$$A \cong D, \quad B \cong E \;\text{ and }\; C \cong F.$$

From those isomorphisms and the direct decomposition (1) it finally follows $G \cong H$.

□

4. An open question

Let G be a finite Hamiltonian group, H be an arbitrary finite group and F be a such field, that the group algebra FG is semisimple. Is it true that $FG \cong FH$ if and only if $G \cong H$?

Solving this problem is important, because the minimal ideals of the group algebra FG are used in Coding theory for the construction of codes with a variety of properties.

References

[1] W. Emerson, Power-Translation Invariance in Discrete Groups – A Characterization of Finite Hamiltonian Groups, *J Comb Theory*, 1970, Vol. 9, pp. 6–26, ISSN: 0097-3165, DOI: https://doi.org/10.1016/S0021-9800(70)80051-5.

[2] M. Hall, *The Theory of Groups*, Courier Dover Publications, 2018, ISBN: 0486816907.

[3] B. Horvat, G. Jaklic, T. Pisanski, On the Number of Hamiltonian Groups, *Math Commun*, 2005, Vol. 10, pp. 89–94, ISSN: 1331-0623, DOI: https://hrcak.srce.hr/664.

[4] J. McCarron, Hamiltonian Groups with Perfect Order Classes, *Math Proc R Ir Acad*, 2021, Vol. 121A, pp. 1–8, ISSN: 1393-7197, DOI: https://doi.org/10.1353/mpr.2021.0001

[5] J. Rose, *A Course on Group Theory*, Dover Publications, 2012, ISBN: 0486681947.

[6] M. Tarnauceanu, Some Combinatorial Aspects of Finite Hamiltonian Groups, *B Iran Math Soc*, 2013, Vol. 39, pp. 841–854, ISSN: 1017-060X.

Yordan Epitropov[1], Nako Nachev[2]
[1,2] Paisii Hilendarski University of Plovdiv,
Faculty of Mathematics and Informatics,
236 Bulgaria Blvd., 4003 Plovdiv, Bulgaria
Corresponding author: epitropov@uni-plovdiv.bg