On endomorphisms of groups of order 32
with maximal subgroups $C_8 \times C_2$

Piret Puusemp and Peeter Puusemp

Department of Mathematics, Tallinn University of Technology, Ehitajate tee 5, 19086 Tallinn, Estonia

Received 9 June 2014, revised 18 September 2014, accepted 26 September 2014, available online 20 November 2014

Abstract. It is proved that each group of order 32 which has a maximal subgroup isomorphic to $C_8 \times C_2$ is determined by its endomorphism semigroup in the class of all groups.

Key words: group, semigroup, endomorphism semigroup.

1. INTRODUCTION

It is well known that all endomorphisms of an Abelian group form a ring and many of its properties can be characterized by this ring. An excellent overview of the present situation in the theory of endomorphism rings of groups is given by Krylov et al. [6]. All endomorphisms of an arbitrary group form only a semigroup. The theory of endomorphism semigroups of groups is quite modestly developed. In a number of our papers we have made efforts to describe some properties of groups by the properties of their endomorphism semigroups. For example, we have proved that many well-known classes of groups are determined by their endomorphism semigroups in the class of all groups. Note that if $G$ is a fixed group and an isomorphism of semigroups $\text{End}(G)$ and $\text{End}(H)$, where $H$ is an arbitrary group, always implies an isomorphism of $G$ and $H$, then we say that the group $G$ is determined by its endomorphism semigroup in the class of all groups. Some of such groups are finite Abelian groups ([7], Theorem 4.2), generalized quaternion groups ([8], Corollary 1), torsion-free divisible Abelian groups ([11], Theorem 1), etc. On the other hand, there exist many examples of groups that are not determined by their endomorphism semigroups in the class of all groups. For example, the following result of Corner is well known [2]: any countable, reduced, torsion-free, associative ring with unity is an endomorphism ring for a continual number of countable, reduced, torsion-free Abelian groups. There exist finite groups that are semidirect products of cyclic groups and are not determined by their endomorphism semigroups in the class of all groups [10].

We know a complete answer to this problem for finite groups of order less than 32. It was proved in [12] that among the finite groups of order less than 32 only the alternating group $A_4$ (also called the tetrahedral group) and the binary tetrahedral group $\langle a, b \mid b^3 = 1, aba = bab \rangle$ are not determined by their endomorphism semigroups in the class of all groups. These two groups are non-isomorphic, but their endomorphism semigroups are isomorphic. In the light of this result it is natural to consider next the groups of order 32.

All groups of order 32 were described by Hall and Senior [5]. There exist exactly 51 non-isomorphic groups of order 32. In [5], these groups are numbered by 1, 2, ..., 51. We shall mark these groups

* Corresponding author, peeter.puusemp@ttu.ee
by \( \mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_{31} \), respectively. The groups \( \mathcal{G}_1-\mathcal{G}_7 \) are Abelian, and, therefore, are determined by their endomorphism semigroups in the class of all groups ([7], Theorem 4.2). In [3], it was proved that the groups of order 32 presentable in the form \( (C_4 \times C_4) \times C_2 \) (\( C_k \) – the cyclic group of order \( k \)) are determined by their endomorphism semigroups in the class of all groups. The groups of this type are \( \mathcal{G}_3, \mathcal{G}_4, \mathcal{G}_{16}, \mathcal{G}_{31}, \mathcal{G}_{34}, \mathcal{G}_{39}, \mathcal{G}_{41} \). In [4], it was proved that the groups of order 32 presentable in the form \( (C_8 \times C_2) \times C_2 \) are determined by their endomorphism semigroups in the class of all groups. The groups of this type are \( \mathcal{G}_4, \mathcal{G}_7, \mathcal{G}_{20}, \mathcal{G}_{26}, \mathcal{G}_{27} \). In [14], Theorem 1.1, it was proved that the groups of order 32 which have a maximal subgroup isomorphic to \( C_4 \times C_2 \times C_2 \) are determined by their endomorphism semigroup in the class of all groups. The groups of this type are \( \mathcal{G}_2, \mathcal{G}_8-\mathcal{G}_{14}, \mathcal{G}_{16}, \mathcal{G}_{20}, \mathcal{G}_{36}-\mathcal{G}_{38} \).

In this paper, we consider the groups of order 32 that have a maximal subgroup isomorphic to \( C_8 \times C_2 \) and prove the following theorem:

**Theorem 1.1.** Each group of order 32 which has a maximal subgroup isomorphic to \( C_8 \times C_2 \) is determined by its endomorphism semigroup in the class of all groups.

The groups of order 32 which have a maximal subgroup isomorphic to \( C_8 \times C_2 \) are:

\[ \mathcal{G}_4, \mathcal{G}_5, \mathcal{G}_6, \mathcal{G}_{17}, \mathcal{G}_{19}, \mathcal{G}_{20}, \mathcal{G}_{21}, \mathcal{G}_{22}, \mathcal{G}_{26}, \mathcal{G}_{27}, \mathcal{G}_{28}, \mathcal{G}_{29}, \mathcal{G}_{30}, \mathcal{G}_{32}. \]

To prove the theorem, the characterization of these groups by their endomorphism semigroups will be given. These characterization properties that are preserved by isomorphisms of endomorphism semigroups will then be used in the proofs.

We shall use the following notations:

- \( G \) – a group;
- \( \text{End}(G) \) – the endomorphism semigroup of \( G \);
- \( C_k \) – the cyclic group of order \( k \);
- \( Q_n = \{ a, b \mid a^n = 1, a^{2n-1} = b^2, b^{-1}ab = a^{-1}\} \); the generalized quaternion group \( (n \geq 2) \);
- \( Q = Q_2 \) – the quaternion group;
- \( Z_k \) – the ring of residual classes modulo \( k \);
- \( \langle K, g, \ldots \rangle \) – the subgroup generated by subsets \( K, \ldots \) and elements \( g, \ldots \);
- \( [a, b] = a^{-1}b^{-1}ab (a, b \in G) \);
- \( G' \) – the commutator-group of \( G \);
- \( \hat{g} \) – the inner automorphism of \( G \), generated by an element \( g \in G \);
- \( I(G) \) – the set of all idempotents of \( \text{End}(G) \);
- \( K(x) = \{ z \in \text{End}(G) \mid zx = xz = z \} \);
- \( J(x) = \{ z \in \text{End}(G) \mid zx = xz = 0 \} \);
- \( H(x) = \{ z \in \text{End}(G) \mid zx = z, xz = 0 \} \);
- \( o(g) \) – the order of an element \( g \in G \).

The sets \( K(x) \) and \( J(x) \) are subsemigroups of \( \text{End}(G) \). We shall write the mapping right from the element on which it acts.

2. GROUPS THAT HAVE A MAXIMAL SUBGROUP \( C_8 \times C_2 \)

According to Hall and Senior [5], the groups of order 32 that have a maximal subgroup isomorphic to \( C_8 \times C_2 \) are:

- \( \mathcal{G}_8 = C_2 \times C_2 \times C_8 \);
- \( \mathcal{G}_3 = C_4 \times C_8 \);
- \( \mathcal{G}_6 = C_2 \times C_{16} \);
- \( \mathcal{G}_7 = (a, b, c \mid a^4 = b^2 = c^2 = 1, ab = ba, ac = ca, c^{-1}bc = ba^4) = (\langle a \rangle \times \langle b \rangle ) \rangle \langle c \rangle = (C_8 \times C_2) \times C_2 \);
- \( \mathcal{G}_9 = (a, b \mid a^4 = b^8 = 1, ab^2 = b^2a, b^{-1}ab = ba^4) = (\langle a \rangle \mid a^4 = b^8 = 1, a^{-1}ba = b^5) = (\langle b \rangle ) \rangle \langle a \rangle = C_8 \times C_4 \);
- \( \mathcal{G}_{20} = (a, b, c \mid a^8 = b^2 = c^2 = 1, ab = ba, bc = cb, c^{-1}ac = ab) = (\langle a \rangle \times \langle b \rangle ) \rangle \langle c \rangle = (C_8 \times C_2) \times C_2 \).
Lemma 3.6. \( G \) is a finite non-Abelian 2-group, then \(|\text{End}(G)| \geq 20\).
Proof. Assume that \( G \) is a finite non-Abelian 2-group. Then the factor-group \( G/Z(G) \) is non-cyclic, i.e., \( |G/Z(G)| \geq 4 \) and \( G \) has at least 4 inner automorphisms. Therefore, \(|\text{Aut}(G)| \geq 4\). By [15], Theorem 5.3.1, there exists \( N \triangleleft G \) such that \( G/N \) is Abelian and non-cyclic. This implies that there exists \( M \triangleleft G \) such that \( N \subset M \) and \( G/M \cong C_2 \times C_2 \). Choose \( a_1, a_2 \in G \) such that 
\[
G/M = \langle a_1M \rangle \times \langle a_2M \rangle.
\]

If \( G \) has only one element of order two, then \( G \) is isomorphic to a generalized quaternion group ([15], Theorem 5.3.6) and \(|\text{End}(G)| \geq 28 \) ([9], Lemmas 2 and 3), i.e., the statement of the lemma is true. Assume that \( G \) has at least two elements of order two, for example, \( b \) and \( d \). We can assume that \( bd = db \). Then there exist 16 proper endomorphisms \( z_{ijkl} = \pi_{ijkl} \) of \( G \), where \( \pi : G \to G/M \) is the canonical homomorphism and
\[
G \xrightarrow{\pi} G/M \xrightarrow{\pi_{ijkl}} G, \quad (a_1M)z_{ijkl} = b^i d^j, \quad (a_2M)z_{ijkl} = b^k d^l
\]

\((i, j, k, l \in \mathbb{Z}_2)\). Since \(|\text{Aut}(G)| \geq 4\), we have \(|\text{End}(G)| \geq 4 + 16 = 20\). The lemma is proved.

4. GROUP \( G_{28} \)

In this section, we shall characterize the group
\[
G_{28} = \langle a, b, c \mid a^8 = b^2 = 1, \ ab = ba, \ c^2 = a^4, \ bc = cb, \ c^{-1}ac = a^{-1}b \rangle
\]
by its endomorphism semigroup. Clearly, \( G_{28} = \langle ba^6, c, ac^{-1} \rangle \). Denote next the elements \( ba^6, c \) and \( ac^{-1} \) by \( a, b \) and \( c \), respectively. Then \( G_{28} \) is given as follows:
\[
G_{28} = \langle a, b, c \mid c^4 = a^4 = 1, \ b^2 = a^2, \ b^{-1}ab = a^{-1}, \ c^{-1}ac = a^{-1}, \ c^{-1}bc = ba \rangle.
\]
The group \( G_{28} \) is a group of order 32 and the numbers of its elements of orders 2, 4, and 8 are 3, 20, and 8, respectively [5]. Clearly,
\[
G_{28} = \langle a, b \rangle \times \langle c \rangle = Q \times \langle c \rangle \cong Q \times C_4.
\]
It is easy to check that
\[
G'_{28} = \langle a \rangle \cong C_4, \quad Z(G'_{28}) = \langle a^2 \rangle \times \langle c^2 \rangle \cong C_2 \times C_2,
\]
\[
G'_{28}/G_{28} = \langle bG'_{28} \rangle \times \langle cG_{28} \rangle \cong C_2 \times C_4.
\]
Each element of \( G_{28} \) can be presented in the canonical form \( c^i x b^j a^k \), where \( j \in \{0, 1\}, i, k \in \mathbb{Z}_4 \).

Our aim is to prove the following theorem.

Theorem 4.1. A finite group \( G \) is isomorphic to \( G_{28} \) if and only if \(|\text{Aut}(G)| = 2^6 = 64\) and there exists \( x \in I(G) \) such that the following properties hold:
\begin{align*}
1^0 & \ K(x) \cong \text{End}(C_4); \\
2^0 & \ |J(x) \cap I(G)| = 0; \\
3^0 & \ |H(x)| = 8; \\
4^0 & \ \{y \in \text{End}(G) \mid xy = yx\} = 24; \\
5^0 & \ \{y \in H(x) \mid \{z \in K(x) \mid z^2 = 0\} \cdot y = \{0\}\} = 2; \\
6^0 & \ \{y \in \text{End}(G) \mid xy = yx, \ z \in K(x) \mid z^2 = 0\} \cdot y = \{0\}\} = 4.
\end{align*}

Proof. Necessity. Let \( G = G_{28} \). Denote by \( x \) the projection of \( G \) onto its subgroup \( \langle c \rangle \). Then \( \text{Im}(x) = \langle c \rangle \) and \( \ker(x) = \langle a, b \rangle \). By Lemma 3.2, \( K(x) \cong \text{End}(\text{Im}(x)) \cong \text{End}(\langle c \rangle) \cong \text{End}(C_4) \), i.e., property \( 1^0 \) holds.

Note that each endomorphism of \( G \) is uniquely determined by its images on generators \( a, b, \) and \( c \). By Lemma 3.3, \( z \in J(x) \) has the form
\[
cz = 1, \ az = b^i a^j, \ bz = b^k a^l; \ i, k \in \{0, 1\}, j, l \in \mathbb{Z}_4.
\]
The map \( z : G \rightarrow G \) given by (4.1) preserves the generating relations of \( G \) and induces an endomorphism of \( G \) if and only if \( i = k = j = 0 \) and \( l \equiv 0 \pmod{2} \). Hence

\[
J(x) = \{ z \mid az = cz = 1, bz = a^{2j}; \ l_0 \in \mathbb{Z}_2 \}
\]

and \( z^2 = 0 \) for each \( z \in J(x) \). Therefore, \( J(x) \cap I(G) = \{0\} \) and property \( 2^0 \) holds.

By Lemma 3.4, \( H(x) \) consists of endomorphisms \( y : G \rightarrow G \) such that

\[
ay = by = 1, \ cy = b' a^j
\]

for some \( i \in \{0, 1\}, j \in \mathbb{Z}_4 \). The map \( y \) given by (4.2) preserves the generating relations of \( G \) and induces an endomorphism of \( G \) for each values of \( i \) and \( j \). Hence

\[
H(x) = \{ y \mid ay = by = 1, cy = b'a^j, \ i \in \{0, 1\}, j \in \mathbb{Z}_4 \}
\]

and \( |H(x)| = 8 \), i.e., property \( 3^0 \) holds.

Since \( G = \text{Ker}_x \times \text{Im}_x \), we have

\[
\{ y \in \text{End}(G) \mid xy = y \} = \{ y \in \text{End}(G) \mid (\text{Ker}_x)y = (1) \}.
\]

Therefore, \( \{ y \in \text{End}(G) \mid xy = y \} \) is equal to the number of homomorphisms \( \text{Im}_x = \langle c \rangle \rightarrow G \), i.e., to the number of elements \( g \in G \) such that \( g^4 = 1 \). By [5], this number is 24. Hence property \( 4^0 \) is true.

By Lemma 3.2,

\[
K(x) = \{ z \mid az = bz = 1, cz = c^i, i \in \mathbb{Z}_4 \}.
\]

Hence

\[
\{ z \in K(x) \mid z^2 = 0 \} = \{ z \mid az = bz = 1, cz = c^{2j}, i_0 \in \mathbb{Z}_2 \}.
\]

By (4.3) and (4.5),

\[
\{ y \in H(x) \mid \{ z \in K(x) \mid z^2 = 0 \} \cdot y = \{0\} \} = \{ y \mid ay = by = 1, cy = b' a^j, (cy)^2 = 1, \ i \in \{0, 1\}, j \in \mathbb{Z}_4 \},
\]

\[
\{ y \in H(x) \mid \{ z \in K(x) \mid z^2 = 0 \} \cdot y = \{0\} \} = \{ \{ b' a^j \mid (b' a^j)^2 = 1, i \in \{0, 1\}, j \in \mathbb{Z}_4 \} = \{ \{ g \in Q \mid g^2 = 1 \} = 2,
\]

i.e., property \( 5^0 \) is true.

By (4.4) and (4.5),

\[
\{ y \in \text{End}(G) \mid xy = y, \{ z \in K(x) \mid z^2 = 0 \} \cdot y = \{0\} \}
\]

\[
\{ y \mid ay = by = 1, cy = g, g \in G, g^2 = 1 \} = \{ \{ g \in G \mid g^2 = 1 \} \}.
\]

By [5], the last number is 4. Therefore, property \( 6^0 \) holds. The necessity is proved.

**Sufficiency.** Let \( G \) be a finite group such that \( |\text{Aut}(G)| = 2^6 \) and there exists \( x \in I(G) \) which satisfies properties \( 1^0 \sim 6^0 \) of the theorem. Our aim is to prove that \( G \cong G_{28} \).

By Lemma 3.1, we have \( G = \text{Ker}_x \times \text{Im}_x \). Property \( 1^0 \) and Lemma 3.2 imply that \( \text{End}(\text{Im}_x) \cong \text{End}(C_4) \).

We have

\[
\text{Im}_x = \langle c \rangle \cong C_4, \ G = \text{Ker}_x \times \langle c \rangle, \ c \in G,
\]

because each finite Abelian group is determined by its endomorphism semigroup in the class of all groups ([17], Theorem 4.2).

Since \( \text{Aut}(G) \) is a 2-group, we have \( \hat{g} = 1 \) for each 2'-element \( g \in G \). Therefore, each 2'-element of \( G \) belongs into the centre of \( G \). Hence \( G \) splits into the direct product \( G = G_2 \times G_{2'} \) of its Sylow 2-subgroup \( G_2 \) and Hall 2'-subgroup \( G_{2'} \). Each 2'-element of \( G \) belongs into \( \text{Ker}_x \), i.e., \( G_{2'} \subset \text{Ker}_x \). Denote by \( z \) the
projection of $G$ onto its subgroup $G_x$. Then $z \in J(x) \cap I(G)$. By property $2^0$, $z = 0$, i.e., $G_x = \langle 1 \rangle$ and $G$ is a 2-group. Clearly, $Ker x \neq \{1\}$.

Choose an element $d \in Ker x$ such that $d^2 = 1$ and define an endomorphism $y = \pi_\tau \circ G$, where $\pi$ is the projection of $G$ onto its subgroup $\text{Im} x = \langle c \rangle$ and

$$G \xrightarrow{\pi} \text{Im} x = \langle c \rangle \xrightarrow{\tau} Ker x, \ c\tau = d.$$ 

Then $xy = y, yx = 0$, i.e., $y \in H(x)$. By Lemma 3.2, $K(x)$ consists of maps $z$, where $(Ker x)z = \langle 1 \rangle$, $cz = c^i, i \in \mathbb{Z}_4$. This $z$ satisfies $z^2 = 0$ if and only if $i = 2i_0, i_0 \in \mathbb{Z}_2$, and for such $z$ the equality $zy = 0$ is true. Therefore, by property $5^0$, the subgroup $Ker x$ of $G$ has only one element of order two. By [15], Theorem 5.3.6, $Ker x$ is a generalized quaternion group or cyclic.

Assume that $Ker x$ is cyclic: $Ker x = \langle a \rangle \cong C_{2^n}$. Then $n \geq 2$, because otherwise $G = \langle a \rangle \times \langle c \rangle$ and the projection of $G$ onto $\langle a \rangle$ belongs into $J(x) \cap I(G)$ and is non-zero. This contradicts property $2^0$. By Lemma 3.4,

$$H(x) = \{ y \mid ay = 1, cy = a^b2^{n-2}, i_0 \in \mathbb{Z}_4 \}$$

and hence $|H(x)| = 4$. This contradicts property $3^0$. The obtained contradiction implies that $Ker x$ cannot be cyclic. Therefore, $Ker x$ is a generalized quaternion group $Q_n, n \geq 2:$

$$Ker x = Q_n = \langle a, b \mid a^{2^n} = 1, b^2 = a^{2^{n-1}}b^{-1}ab = a^{-1} \rangle.$$ 

By Lemma 3.4,

$$H(x) = \{ y \mid ay = 1, cy = g, g \in Ker x = Q_n, \ g^4 = 1 \}.$$ 

Since

$$\{ g \in Q_n \mid g^4 = 1 \} = \{ ba^i, a^{2^{n-2}}i \in \mathbb{Z}_{2^n}, j \in \mathbb{Z}_4 \},$$

we have $|H(x)| = 2^n + 4$. Property $3^0$ implies that $2^n + 4 = 8$, i.e., $n = 2$ and $Ker x$ is the quaternion group $Q = Q_2$. It follows also that $|G| = |Ker x| \cdot |\text{Im} x| = 8 \cdot 4 = 32$, i.e., $G$ is a non-Abelian group of order 32.

Let us find the numbers of elements $g \in G$ such that $g^4 = 1$ or $g^2 = 1$. Each homomorphism $y_0 : \text{Im} x = \langle c \rangle \rightarrow G$ can be uniquely extended to an endomorphism $y$ of $G$ such that $xy = y y$ by setting $(Ker x)y = \langle 1 \rangle$. Denote this $y$ by $y_0$. Conversely, each $y \in \text{End}(G)$ such that $xy = y$ is obtained in this way. Therefore,

$$\{ y \in \text{End}(G) \mid xy = y \} = \{ \tilde{y}_0 \mid y_0 \in \text{Hom}(\langle c \rangle, G) \}, 
\{ y \in \text{End}(G) \mid xy = y \} = |\text{Hom}(\text{Im} x, G)| \cdot |\text{Hom}(\langle c \rangle, G)| = |\{ g \in G \mid g^4 = 1 \}|,$$

i.e., by property $4^0$, the number of elements $g \in G$ such that $g^4 = 1$ is 24.

Denote

$$\mathcal{E} = \{ y \in \text{End}(G) \mid xy = y, \ z \in K(x) \mid z^2 = 0 \} : y = \{ 0 \} \}.$$ 

By property $6^0$, $|\mathcal{E}| = 4$. In view of (4.6),

$$\mathcal{E} = \{ \tilde{y}_0 \mid y_0 \in \text{Hom}(\langle c \rangle, G), \ z \in K(x) \mid z^2 = 0 \} : y_0 = \{ 0 \} \}.$$ 

By Lemma 3.2, $K(x)$ consists of maps $z : G \rightarrow G$, where $(Ker x)z = \langle 1 \rangle$ and $cz = c^i, i \in \mathbb{Z}_4$. For those $z, z^2 = 0$ if and only if $i = 2i_0, i_0 \in \mathbb{Z}_2$. In this case, $c(zy) = (cy)^{2i_0} = (cy_0)^{2i_0}$ for each $y = \tilde{y}_0$. Therefore, $\tilde{y}_0 \in \mathcal{E}$ if and only if $(c\tilde{y}_0)^2 = 1$. Hence

$$|\mathcal{E}| = |\{ y_0 \in \text{Hom}(\langle c \rangle, G) \mid (cy_0)^2 = 1 \}| = |\{ g \in G \mid g^2 = 1 \}| = 4.$$ 

It follows that the group $G$ has 3 elements of order two. Since the number of elements $g$ such that $g^4 = 1$ is 24, the group $G$ has 20 elements of order 4. By [5], there exists only one non-Abelian group of order 32 such that $|\text{Aut}(G)| = 2^5$ and which has 3 elements of order two and 20 elements of order 4. This group is $\mathcal{F}_28$. Therefore, $G \cong \mathcal{F}_28$. The sufficiency is proved.

The theorem is proved.
Theorem 4.2. The group $G_{28}$ is determined by its endomorphism semigroup in the class of all groups.

Proof. Let $G^*$ be a group such that the endomorphism semigroups of $G^*$ and $G_{28}$ are isomorphic:

$$\text{End}(G^*) \cong \text{End}(G_{28}).$$  \hfill (4.7)

Denote by $z^*$ the image of $z \in \text{End}(G_{28})$ in isomorphism (4.7). Since $\text{End}(G^*)$ is finite, so is $G^*$ ([1], Theorem 2). By Theorem 4.1, $|\text{Aut}(G_{28})| = 2^6 = 64$ and there exists $x \in I(G_{28})$, satisfying properties $1^0$–$6^0$ of Theorem 4.1. These properties are formulated so that they preserve in isomorphism (4.7). Therefore, $|\text{Aut}(G^*)| = 2^6 = 64$ and the idempotent $x^*$ of $\text{End}(G^*)$ satisfies properties similar to properties $1^0$–$6^0$ (it is necessary to change everywhere $z \in \text{End}(G_{28})$ by $z^* \in \text{End}(G^*)$). Using now Theorem 4.1 for $G^*$, it follows that $G^*$ and $G_{28}$ are isomorphic. The theorem is proved.

5. GROUP $G_{32}$

In this section, we shall characterize the group $G_{32} = \langle a, c \mid a^8 = 1, a^4 = c^4, c^{-1}ac = a^{-1} \rangle$

by its endomorphism semigroup. The group $G_{32}$ is a group of order 32 and the numbers of its elements of orders 2, 4, and 8 are 3, 4, and 24, respectively [5]. It is easy to check that

$G'_{32} = \langle a^2 \rangle \cong C_4,$ $\text{Z}(G_{32}) = \langle c^2 \rangle \cong C_4,$

$G_{32}/G'_3 \cong \langle cG'_{32} \rangle \times \langle dG'_{32} \rangle \cong C_4 \times C_2.$

Each element of $G_{32}$ can be presented in the canonical form $c^ja^l$, where $i \in \{0, 1, 2, 3\}$ and $j \in \mathbb{Z}_8$.

Our aim is to prove the following theorem.

Theorem 5.1. A finite group $G$ of order $\geq 32$ is isomorphic to $G_{32}$ if and only if it satisfies the following properties:

$1^0 |\text{Aut}(G)| = 64$;
$2^0 |\text{End}(G) \setminus \text{Aut}(G)| = 32$;
$3^0$ the only idempotents of $\text{End}(G)$ are 0 and 1;
$4^0 |\{z \in \text{End}(G) \setminus \text{Aut}(G) \mid z^2 = 0\}| = 20$;
$5^0$ there exist $z, w \in \text{End}(G) \setminus \text{Aut}(G)$ such that $z^2 = w^2 = 0$ and $wz \neq 0$;
$6^0 |\{y \in \text{Aut}(G) \mid x \in \text{End}(G) \setminus \text{Aut}(G) \implies yx = x\}| = 16$.

Proof. Necessity. Let $G = G_{32}$. To prove properties $1^0$–$6^0$ for $G$, we have to find the endomorphisms of $G$. An endomorphism of $G$ is fully determined by its action on the generators $c$ and $a$. Choose $z \in \text{End}(G)$. Then

$$az = c^j a^l, \quad cz = c^k a^l$$ \hfill (5.1)

for some $i, j, k, l$. The map $z$ given by (5.1) induces an endomorphism of $G$ if and only if it preserves the defining relations of $G$. After easy calculations, we obtain that the map $z$ given by (5.1) is an endomorphism of $G$ only in the following three cases:

$$cz = c^{2k_0} a^{2l_0}, \quad az = a^{4l_0}, \quad j_0, k_0 \in \{0, 1\}, \quad l_0 \in \mathbb{Z}_4,$$ \hfill (5.2)

$$cz = c^{2k_0} a^{2l_0}, \quad az = c^2 a^{2+4l_0}, \quad j_0, k_0 \in \{0, 1\}, \quad l_0 \in \mathbb{Z}_4,$$ \hfill (5.3)

$$cz = c^{2l_0+1} a^j, \quad az = a^j; \quad k_0 \in \{0, 1\}, \quad j, l \in \mathbb{Z}_8, \quad j \equiv 1 \pmod{2}.$$ \hfill (5.4)
The endomorphisms given by (5.2) and (5.3) are proper endomorphisms and the endomorphisms given by (5.4) are automorphisms. The numbers of endomorphisms of these three types are 16, 16, and 64, respectively. Hence $G$ satisfies properties $1^0$ and $2^0$.

Immediate calculations show that 0 and 1 are only idempotents of $\text{End}(G)$. Similarly, immediate calculations show that $z^2 = 0$ only for the following proper endomorphisms $z$:

$$cz = a^{2j_0}, \quad az = a^{4j_0}, \quad l_0 \in \mathbb{Z}_4, \quad j_0 \in \mathbb{Z}_2,$$

$$cz = c^2a^2, \quad az = a^{4j_0}, \quad j_0 \in \mathbb{Z}_2,$$

$$cz = c^2a^0, \quad az = a^{4j_0}, \quad j_0 \in \mathbb{Z}_2,$$

$$cz = 1, \quad az = c^2a^{2+4j_0}, \quad j_0 \in \mathbb{Z}_2,$$

$$cz = a^4, \quad az = c^2a^{2+4j_0}, \quad j_0 \in \mathbb{Z}_2,$$

$$cz = c^2a^2, \quad az = c^2a^{2+4j_0}, \quad j_0 \in \mathbb{Z}_2,$$

$$cz = c^2a^0, \quad az = c^2a^{2+4j_0}, \quad j_0 \in \mathbb{Z}_2.$$

The number of such endomorphisms is $8 + 6 \cdot 2 = 20$. Hence $G$ satisfies properties $3^0$ and $4^0$.

Property $5^0$ is satisfied for the proper endomorphisms $z$ and $w$, where

$$cz = a^2, \quad az = 1, \quad cw = 1, \quad aw = c^2a^2.$$

Let us prove property $6^0$. Choose an arbitrary $y \in \text{Aut}(G)$:

$$cy = c^{2k+1}a^l, \quad ay = a^l; \quad k \in \{0, 1\}; \quad j, l \in \mathbb{Z}_8, \quad j \equiv 1 \pmod{2}.$$  

We have to find $k, l, j$ so that $yx = x$ for each $x \in \text{End}(G) \setminus \text{Aut}(G)$. If $x$ is given by (5.2), then

$$a(yx) = a^lx = a^{4j_0}a^{4j_0} = ax,$$

$$c(yx) = (c^{2k_0}a^{2l_0})^{2k_1+1}a^{4j_0} = c^{2k_0(2k_1+1)}a^{2l_0(2k_1+1)}a^{4j_0} = c^{2k_0}a^{4k_0k_1+4l_0k+2l_0+4j_0l},$$

$$cx = c^{2k_0}a^{2l_0},$$

and $yx = x$ if and only if

$$4k_0k + 4l_0k + 4j_0l \equiv 0 \pmod{8}.$$  

The last congruence is satisfied for each $j_0, k_0, l_0$ if and only if

$$k = 0, \quad l \equiv 0 \pmod{2}.$$  

(5.5)

Assume that $x$ is given by (5.3). In view of (5.5) and $c^{2l_0}a^{2j} = c^2a^2$ for odd $j$, we have

$$a(yx) = a^l = (c^{2k_0}a^{2l_0})^{2j_0} = c^{2k_0}a^{2j_0} = c^{2k_0}a^{4j_0} = ax,$$

$$c(yx) = (ca^l)x = c^{2k_0}a^{2l_0}(c^{2k_0}a^{2+4j_0})^l = c^{2k_0}c^{2l_0+1(2+4j_0)} = c^{2k_0}c^{2j_0}a^{2l_0+2j} = c^{2k_0}a^{4l_0+2l_0} = c^{2k_0}a^{2l_0} = cx.$$  

Therefore, if $x$ is given by (5.3), then always $yx = x$. It follows that $yx = x$ for each $x \in \text{End}(G) \setminus \text{Aut}(G)$ if and only if $k$ and $l$ satisfy (5.5). Since $j \equiv 1 \pmod{2}$, the number of such automorphisms $y$ is $4 \cdot 4 = 16$. Property $6^0$ is proved.

The necessity is proved.

**Sufficiency.** Let $G$ be a finite group of order $\geq 32$ which satisfies properties $1^0 \cdots 6^0$. Our aim is to prove that $G \cong \mathcal{G}_{32}$. We shall now introduce a series of lemmas which give the proof.
Lemma 5.1. The group $G$ is a non-Abelian 2-group and it is not a generalized quaternion group. The group has at least two elements of order two.

Proof. By property $1^0$, $\hat{g} = 1$ for each 2'-element $g$ of $G$. Hence all 2'-elements of $G$ belong into its centre $Z(G)$. Therefore, the group $G$ splits into the direct product $G = G_2 \times G_2$ of its Hall 2'-subgroup $G_2$ and Sylow 2-subgroup $G_2$. Denote by $z$ the projection of $G$ onto its subgroup $G_2$. By property $3^0$, $z = 0$ or $z = 1$. Assume that $z = 1$. Then $G = G_2$ is Abelian and, again by property $3^0$, $G$ is cyclic, i.e., $G = C_n$ for an odd integer $n$. By properties $1^0$ and $2^0$, we have $|\text{End}(G)| = n = 64 + 32 = 96$. This contradicts the fact that $n$ is odd. Hence $z = 0$ and $G$ is a 2-group. The group $G$ is non-Abelian, because otherwise, by property $3^0$, $G$ would be cyclic and $|G| = |\text{End}(G)| = 2^m = 96$ for an integer $m$, which is impossible. Since a generalized quaternion group has only four proper endomorphisms ([8], Lemma 2), the group $G$ cannot be a generalized quaternion group. The last statement of the lemma follows from [15], Theorem 5.3.6. The lemma is proved.

The factor-group $G/G'$ splits into a direct product

$$G/G' = \langle a_1G' \rangle \times \ldots \times \langle a_nG' \rangle; \ a_1, \ldots, a_n \in G \setminus G'.$$

Denote further by $\epsilon$ the canonical homomorphism $\epsilon : G \longrightarrow G/G'$.

Lemma 5.2. $n = 2$.

Proof. Remark that $G/G'$ is not cyclic ([15], Theorem 5.3.1). Hence $n \geq 2$. Assume that $n \geq 3$. By Lemma 5.1, $G$ has at least two elements of order two, for example $b$ and $d$. We can assume that $bd = db$, and, therefore, $G$ has at least 64 proper endomorphisms $z_{ijklst}$:

$$z_{ijklst} = \epsilon \pi_{ijklst} : G \xrightarrow{\epsilon} G/G' \xrightarrow{\pi_{ijklst}} \langle b, d \rangle,$$

$$(a_1G')\pi_{ijklst} = b^i d^j, \ (a_2G')\pi_{ijklst} = b^k d^l, \ (a_3G')\pi_{ijklst} = b^t d^s,$$

$$(a_nG')\pi_{ijklst} = 1, \ u \geq 3; \ i, j, k, l, s, t \in \mathbb{Z}_2.$$

This contradicts property $2^0$. Therefore, $n < 3$ and $n = 2$. The lemma is proved.

By Lemma 5.2, we can fix $c, a \in G \setminus G'$ in the following way:

$$G/G' = \langle cG' \rangle \times \langle aG' \rangle \cong C_2 \times C_2$$

(5.6)

and

$$o(cG') = 2^s, \ o(aG') = 2^t, \ s \geq t \geq 1.$$  

By property $3^0$, $G$ does not split into a nontrivial semidirect product. Hence

$$c^{2^s} \neq 1, \ a^{2^t} \neq 1.$$  

(5.7)

If $g, h \in G$ such that $gh = hg$ and $o(g) \leq 2^s, \ o(h) \leq 2^t$, then there exists a proper endomorphism $y(g; h) = \epsilon \cdot \pi$ of $G$ defined as follows:

$$G \xrightarrow{\epsilon} G/G' = \langle cG' \rangle \times \langle aG' \rangle \xrightarrow{\pi} G, \ (cG')\pi = g, \ (aG')\pi = h.$$  

In the further proofs, we shall use proper endomorphisms of this kind a number of times.

Next we shall prove that $G'$ is cyclic and determine the values of $s$ and $t$.

Lemma 5.3. The derived group $G'$ of $G$ has an element of order four.


Therefore, the number of such endomorphisms is $g^2 = 1$ for each $g \in G'$. Then $G'$ is Abelian and splits into a direct product

$$G' = \langle b_1 \rangle \times \ldots \times \langle b_n \rangle \cong C_2 \times \ldots \times C_2, \ n \geq 1,$$

and there exist proper endomorphisms $y(b_1^i \ldots b_n^i; b_1^{i_1} \ldots b_n^{i_n})$, where $i_1, \ldots, i_n, j_1, \ldots, j_n \in \mathbb{Z}_2$. The number of such endomorphisms is $2^n \cdot 2^n = 2^{2n}$, and, by property $2^n$, $2^{2n} \leq 32 = 2^5$, $2n \leq 5$, i.e. $n \leq 2$. Let us consider the cases $n = 1$ and $n = 2$ separately.

Assume that $n = 1$. By (5.7), we have

$$[c, a] = c^{-1}a^{-1}ca \in Z(G), \ c^2 \cdot a = a \cdot c^2, \ a^2 \cdot c = c \cdot a^2. \quad \text{(5.8)}$$

Therefore, there exist proper endomorphisms $y(c^{2i}a^{2i}; c^{2i+1}a^{2i+1})$. We get all elements of the form $c^{2i}a^{2i}$ if we take $i_1 \in \mathbb{Z}_2$, and $i_2 = 0, 1, 2, \ldots, 2^n - 1$. Similarly, we get all elements of the form $c^{2i+1}a^{2i+1}$ if we take $j_1 \in \mathbb{Z}_2$, and $j_2 = 0, 1, 2, \ldots, 2^n - 1$. It follows that the number of endomorphisms $y(c^{2i}a^{2i}; c^{2i+1}a^{2i+1})$ is $2^i \cdot 2^t - 1$, $2^i \cdot 2^t - 1 = 2^i + 3t - 2$. By property $2^n$,

$$2^i + 3t - 2 \leq 32 = 2^5, \ 4t \leq s + 3t \leq 7, \ t = 1.$$

In view of (5.6), (5.8), and $t = 1$, each element $g \in G$ of order two is $c^2$ or has a form $g = ac^2$ for a suitable integer $i$. If $g = ac^2$, then $G = \langle c \rangle \times \langle g \rangle$ and the projection of $G$ onto $\langle g \rangle$ is non-zero and non-identity idempotent of $\text{End}(G)$. This contradicts property $3^n$. Hence $G$ has only one element of order two (it is $c^2$) and, therefore, is cyclic or a generalized quaternion group. This contradicts Lemma 5.1. It follows that $n \neq 1$.

Assume that $n = 2$. Then

$$G' \cong C_2 \times C_2, \ |G| = 2^{s+t+2}.$$ 

The case $s = t = 1$ is impossible, because $|G| \geq 32$. Hence

$$s \geq t, \ s \geq 2.$$

Assume that $s > t$. Choose $g \in \langle c^2, a, G' \rangle$. Then $g^2 = 1$ and there exists the proper endomorphism $y(g; 1)$ of $G$. The number of such endomorphisms is $|G|/2 = 2^{s+t+1}$. Choose $g \in \langle c^{2i+1}, a^2, G' \rangle$. Then $g^2 = 1$ and there exists the proper endomorphism $y(1; g)$ of $G$. The number of such endomorphisms is $2^{2(i-1)+2} = 2^{2i}$. Among endomorphisms $y(g; 1)$ and $y(1; g)$ only zero is a common endomorphism. Therefore, the number of such endomorphisms is $2^{s+t+1} + 2^t - 1$, and, by property $2^n$, $2^{s+t+1} + 2^t - 1 \leq 32$. The only solution of this inequality under conditions $s > t, \ s \geq 2$ is

$$t = 1, \ s = 2. \quad \text{(5.9)}$$

Choose $g, d, b \in G$ such that

$$g \in \langle c^2, a, G' \rangle, \ d \in Z(G), \ o(d) = 2, \ b \in G, \ o(b) = 2, \ b \neq d.$$

By (5.9), we have $g^4 = 1$ and there exist proper endomorphisms $y(g; d^i), i \in \mathbb{Z}_2$, and $y(1; b)$ of $G$. The number of those endomorphisms is $2 \cdot |\langle c^2, a, G' \rangle| + 1 = 33$. This contradicts property $2^n$. Therefore, the inequality $s > t$ is false and

$$s = t \geq 2, \ |G| = 2^{2s+2}. \quad \text{(5.10)}$$

Choose $g_1, g_2, g_3, g_4 \in G$ such that

$$g_1, g_2 \in \langle c^2, a^2, G' \rangle, \ o(g_3) = o(g_4) = 2, \ g_3 \neq g_4.$$
Then $g_1^2 = g_2^2 = 1$ and there exist proper endomorphisms $y(g_1; 1), y(1; g_2), y(g_3; g_3)$, and $y(g_4; g_4)$ of $G$. Among these endomorphisms only zero appears twice, and, therefore, their number is

$$2 \cdot |\langle e^2, a^2, G' \rangle| - 1 + 2 = 2 \cdot 2^{2s} + 1.$$ 

By property 2\textsuperscript{0},

$$2 \cdot 2^{2s} + 1 \leq 32, \quad 2 \cdot 2^{2s} \leq 31, \quad 2 \cdot 2^{2s} \leq 30, \quad 2 \cdot 2^{2s} \leq 15, \quad 2^{2s} \leq 8 = 2^3, \quad 2s \leq 3, \quad s = 1.$$

This contradicts (5.10). The obtained contradiction implies that the derived group $G'$ contains an element of order four. The lemma is proved.

**Lemma 5.4.** The derived group $G'$ has only one element of order two or $s = t = 1$.

**Proof.** Assume that $s \geq 2$ and $G'$ has at least two different elements $b$ and $d$ of order two. We can assume that $bd = db$. In view of Lemma 5.3, there exists an element $h \in G'$ of order four. It is possible to choose so that $h^2 = b$. There exist proper endomorphisms $z_{ijk} = y(b^d; b^k d)$ and $w_{\alpha\beta} = y(h^\alpha; b^\beta) = y(h^\alpha; h^2 b^\beta)$ of $G$, where $i, j, k, l, \beta \in \mathbb{Z}_2$; $\alpha \in \{1, 3\}$. By the construction, $z_{ijk}^2 = w_{\alpha\beta}^2 = 0$. The number of endomorphisms $z_{ijk}$ and $w_{\alpha\beta}$ is $2^4 + 2^2 = 20$. By property 4\textsuperscript{0}, each proper endomorphism $z$ of $G$ which satisfies $z^2 = 0$ has one of these two forms.

Let us consider the cases $dh \neq hd$ and $dh = hd$ separately. Assume that $dh = hd$. There exist proper endomorphisms $\tau_{\alpha\beta} = y(h^\alpha; h^2 b^\beta)$, where $\alpha \in \{1, 3\}$, $\beta \in \mathbb{Z}_2$. By the construction, $\tau_{\alpha\beta}^2 = 0$ and $\tau_{\alpha\beta}$ differs from $z_{ijk}$ and $w_{\alpha\beta}$. This contradicts the previous part of the proof. Hence $dh \neq hd$. Since $(w_{10} \cdot d)^2 = 0$, we have $w_{10} \cdot d = w_{00}$ for some $\alpha \in \{1, 3\}$. Therefore,

$$c(w_{10} \cdot d) = hd = d^{-1}hd = cw_{\alpha\beta} = h^\alpha,$$

i.e., $d^{-1}hd = h^{-1}$. It follows from here that $dh$ is an element of order two and there exists a proper endomorphism $z = y(1; dh)$. By the construction, $z^2 = 0$ and $z$ differs from $z_{ijk}$ and $w_{\alpha\beta}$. This contradicts the first part of the proof. Therefore, the case $dh \neq hd$ is also impossible. Consequently, the assumption that $s \geq 2$ and $G'$ has at least two different elements $b$ and $d$ of order two is false. This implies that $s = 1$ (i.e., $s = t = 1$), because $s \geq t$ or $G'$ has only one element of order two. The lemma is proved.

**Lemma 5.5.** The case $s = t = 1$ is impossible, i.e., $s \geq 2$.

**Proof.** On the contrary, assume that $s = t = 1$. Then all elements of order two of $G$ belong to $G'$, because otherwise the group $G$ would split into a non-trivial semidirect product, which contradicts property 3\textsuperscript{0}. By Lemma 5.1, $G'$ has at least two different elements $b$ and $d$ of order two. We can assume that $b \in Z(G)$. We get 16 proper endomorphisms $z_{ijkl} = y(b^i d^j; b^k d^l)$ of $G$ (i, j, k, l $\in \mathbb{Z}_2$). By the construction, $z_{ijkl}^2 = 0$.

If $G$ has an element $h$ of order two such that $h \notin \langle b, d \rangle$, then $h \in G'$ and we get six additional proper endomorphisms $y(b^h; b^i h)$, $y(h; 1)$, and $y(1; h)$ of $G$ such that $y(b^h; b^i h)^2 = y(h; 1)^2 = y(1; h)^2 = 0$ (i, j $\in \mathbb{Z}_2$). Hence we have already $16 + 6 = 22$ proper endomorphisms $z$ of $G$ such that $z^2 = 0$. This contradicts property 4\textsuperscript{0}. Therefore, all elements of order two of $G$ belong to $\langle b, d \rangle = \langle b \rangle \times \langle d \rangle \subset G'$.

Let $z$ be a proper endomorphism of $G$ such that $\text{Im} z$ is Abelian. Then $G/Ker z$ is Abelian, $G' \subset Ker z$ and $z = \gamma y$ for a homomorphism $y : G/G' \rightarrow \langle b \rangle \times \langle d \rangle$. Hence $z$ is equal to $z_{ijkl}$ for some $i, j, k, l$. By property 4\textsuperscript{0}, there exists a proper endomorphism $w$ of $G$ such that $w^2 = 0$ and $\text{Im} w$ is non-Abelian. Fix $w$ of this kind. Define $w_{\alpha} = w \cdot \alpha \in \text{End}(G)$ for each $\alpha \in \text{End}(\text{Im} w)$. By the construction,

$$w_{\alpha}w_{\beta} = w_{\alpha}w_{\beta} = 0 \cdot \beta = 0, \quad w_{\alpha}^2 = 0 \quad (5.11)$$

($\alpha, \beta \in \text{End}(\text{Im} w)$). Lemma 3.6 implies that the number of such endomorphisms $w_{\alpha}$ is at least 20. Therefore, by property 4\textsuperscript{0}, each proper endomorphism $z$ of $G$ for which $z^2 = 0$ can be presented in the form $w_{\alpha}$ for some $\alpha$. In view of (5.11), $z_1 z_2 = 0$ for each $z_1$ and $z_2$ such that $z_1^2 = z_2^2 = 0$. This contradicts property 5\textsuperscript{0}. It follows that the case $s = t = 1$ is impossible and $s \geq 2$. The lemma is proved.
Lemma 5.6. The derived group $G'$ is cyclic.

Proof. Lemmas 5.4 and 5.5 imply that $G'$ has only one element of order two. By [15], Theorem 5.3.6, $G'$ is cyclic or a generalized quaternion group. Assume that $G'$ is a generalized quaternion group $Q_n$, $n \geq 2$:

$$G' = Q_n = \langle a_0, b_0 \mid a_0^{2n} = 1, b_0^{2n-1} = b_0^2, b_0^{-1}a_b0 = a_0^{-1} \rangle.$$

The elements of order four of $Q_n$ are

$$a_0^{2n-2}, b_0^2, b_0^{-1}, b_0, i \in \mathbb{Z}_{2n}.$$

The number of them is $2^n + 2$. Choose an element $h \in G \setminus G'$ of order two. By Lemma 5.1, it is possible. Then $h = c^{a_{2n-1}} a^{2n-1} d$ for some $u, v \in \mathbb{Z}_2$ and $d \in G$. If $t = 1$, then $v = 0$, because otherwise $h = c^{a_{2n-1}} d \cdot G = \langle c, G' \rangle \cdot \langle h \rangle$ and the projection of $G$ onto $\langle g \rangle$ would be non-zero and non-identity idempotent of $\text{End}(G)$, which contradicts property $3^0$. Let $g \in G'$ be an element of order four. Since $a_0^{2n-1} \in Z(G)$ and $s \geq 2$, there exist proper endomorphisms $z_{ijkl} = y(g^2; a_0^{2n-1})$ and $z_{ijkl} = y(h^2; a_0^{2n-1}, h^k a_0^{2n-1})$ ($i, j, k, l \in \mathbb{Z}_2$). Clearly, $z_{ijkl} = 0$. The following calculations show that $z_{ijkl}^2 = 0$:

$$cz_{ijkl}^2 = (h_i^2 a_0^{2n-1})z_{ijkl}^2 = (h_i z_{ijkl})^2 = (((h_i^2 a_0^{2n-1})^2z_{ijkl})^2)^2 = (((h_i^4 a_0^{4n-2})^2z_{ijkl})^2)^2 = 1.$$

The number of endomorphisms $z_{ijkl}$ and $z_{ijkl}$ is $2(2^n + 2) + 2^4 = 2^{n+1} + 20$, which contradicts property $4^0$. Therefore, $G'$ cannot be a generalized quaternion group. The lemma is proved.

It is now possible to find the values of $s$ and $t$.

Lemma 5.7. $t = 1$.

Proof. Assume that $t \geq 2$. Choose $g \in G'$ of order four and $h \in G \setminus G'$ of order two. By Lemmas 5.1 and 5.3, it is possible. Then $h = c^{a_{2n-1}} a^{2n-1} d$ for some $u, v \in \mathbb{Z}_2$ and $d \in G$'. Clearly, $g^2 \in Z(G)$. Therefore, there exist proper endomorphisms $z_{ij} = y(g_i^2; g^1), w_{kl} = y(h_k^2; h^2), w_{1ij} = 1$ ($i, j, k, l \in \mathbb{Z}_2$). Clearly, $z_{ij}^2 = z^2 = 0$. Similarly to the proof of Lemma 5.6, one can prove that $w_{ijkl} = 0$. The number of endomorphisms $z_{ij}, w_{ijkl}$ and $z = 16 + 4 + 1 = 21$. This contradicts property $4^0$. Therefore, $t = 1$. The lemma is proved.

Lemma 5.8. Let $b \in G'$ be an element of order four and $h \in G \setminus G'$ be an element of order two. Then $h = c^{a_{2n-1}} d$ for some $d \in G'$ and

$$\{z \in \text{End}(G) \mid \text{Aut}(G) \mid z^2 = 0\} = \{z_{ijkl}, w_{\alpha \beta} \mid \beta, i, j, k, l \in \mathbb{Z}_2; \alpha = \pm 1\},$$

where $z_{ijkl} = y(h^2; b^2)$ and $w_{\alpha \beta} = y(b^\alpha; b^\beta)$.

Proof. Let $b \in G'$ be an element of order four and $h \in G \setminus G'$ be an element of order two. By Lemmas 5.1, 5.4, and 5.6, there exist those elements. Then $h = c^{a_{2n-1}} a^{2n-1} d = c^{a_{2n-1}} a d$ for some $u, v \in \mathbb{Z}_2$ and $d \in G$'. If $v = 1$, then $G = \langle c, G' \rangle \cdot \langle h \rangle$, which contradicts property $3^0$. Therefore, $v = 0, u = 1$, and $h = c^{2n-1} d$.

Since $b^2 \in Z(G)$, the maps $z_{ijkl}$ and $w_{\alpha \beta}$ given in the lemma are the proper endomorphisms of $G$. Evidently, $w_{ijkl} = 0$. Since $G' z_{ijkl} = 1$ and

$$cz_{ijkl}^2 = (h_i^2 b^2)z_{ijkl} = (h_i z_{ijkl})^2 = ((c^{2n-1} d)z_{ijkl})^2 = (h_i^2 b^2)^2 = 1,$$

$$cz_{ijkl}^2 = (h_i^2 b^2)z_{ijkl} = (h_i z_{ijkl})^2 = ((c^{2n-1} d)z_{ijkl})^2 = (h_i^2 b^2)^2 = 1,$$

we have $z_{ijkl}^2 = 0$. The number of endomorphisms $z_{ijkl}$ and $w_{\alpha \beta}$ is $2^4 + 2 \cdot 2 = 20$. Property $4^0$ implies the second statement of the lemma. The lemma is proved.
Lemma 5.9. The group $H = \langle a, G' \rangle$ is cyclic.

Proof. By Lemmas 5.6 and 5.8, $H$ has only one element of order two. Therefore, $H$ is cyclic or a generalized quaternion group

$$Q_n = \langle a_0, b_0 \mid a_0^{2^n} = 1, b_0^2 = a_0^{2^{n-1}}, b_0^{-1} a_0 b_0 = a_0^{-1} \rangle, \ n \geq 2,$$

([15], Theorem 5.3.6). Assume that $H = Q_n$. The elements $b_0 a_0^y (y \in \mathbb{Z}_{2^n})$ are the elements of order four and there exist proper endomorphisms $x_\gamma = y(b_0 a_0^y; 1)$ of $G$. By the construction, $x_\gamma^2 = 0$. Since the number of such endomorphisms is $2^n \geq 4$, some of them are different from the endomorphisms given in Lemma 5.8. This contradiction implies that $H \neq Q_n$. Hence $H$ is cyclic. The lemma is proved.

Lemma 5.10. $s = 2$.

Proof. On the contrary, assume that $s \geq 3$. If the order of $c^k$ is two, then the order of $c^{2^{-1}}$ is four and there exist a proper endomorphism $z = y(c^{2^{-1}}; 1)$. We have $z^2 = 0$:

$$cz^2 = c^{2^{-1}} z = (c^{2^{-1}})^{2^{s-2}} = 1, \ acz^2 = 1.$$

The endomorphism $z$ differs from the endomorphisms which were given in Lemma 5.8. Therefore, $o(c^k) \neq 2$ and there exists an integer $k$ such that the order of $c^{2^k}$ is four. By Lemma 5.8, there exist an element $h = c^{2^{s-1}} d$ of order two, where $d \in G'$. Since $c^{2^k} \in G'$, the elements $c^{2^k}$ and $h$ commute. Hence there exists the proper endomorphism $z = y(c^{2^k}; h)$. In this case also $z^2 = 0$:

$$c^2 = c^{2^k} z = (c^{2^k})^{2^k} = 1,$$

$$acz^2 = h z = (c^{2^{s-1}} d) z = (c z)^{2^{s-1}} = (c^{2^k})^{2^{s-1}} = 1.$$

The endomorphism $z$ differs from the endomorphisms which were given in Lemma 5.8. Therefore, the case $s \geq 3$ is impossible. The lemma is proved.

By Lemma 5.9, the group $\langle a, G' \rangle$ is cyclic. Therefore, we can assume that $\langle a, G' \rangle = \langle a \rangle \cong C_{2^m}$ for some $m$. By (5.6) and Lemmas 5.3, 5.7, and 5.10, $m \geq 3$ and $c^4 = a^{2u}$ for some $u \in \mathbb{Z}_{2^{m-1}}$. Let us present $u$ in the form

$$u = u_0 2^n, \ u_0 \equiv 1 \pmod{2}, \ 0 \leq n \leq m - 2$$

(by (5.7), $n \neq m - 1$). We can assume that $u_0 = 1$, because we can replace $a$ with suitable $a'$, where $i \equiv 1 \pmod{2}$. By (5.6), $c^{-1} ac = a'$ for some $r \in \mathbb{Z}_{2^m}, \ r \equiv 1 \pmod{2}$. Since $c^{-1} ac = a'$ and $c^4 = a^{2u}$, we have $r^4 \equiv 1 \pmod{2^m}$.

Let us summarize the obtained results on the group $G$:

$$G = \langle c, a \mid a^{2^m} = 1, c^4 = a^{2^{s+1}}, c^{-1} ac = a' \rangle,$$

where

$$r^4 \equiv 1 \pmod{2^m}, \ m \geq 3, \ 0 \leq n \leq m - 2.$$

Since $r = 1 + 2v$ for an integer $v$, we have

$$r^2 = 1 + 4v + 4v^2, \ r^2 \equiv 1 \pmod{4}, \ \text{and} \ 1 + r^2 = 2(1 + 2v + 2v^2) = 2(1 + (2v)^2).$$

Our next aim is to find all elements $g \in G$ such that $g^4 = 1$ and to prove that these elements commute with each other. Using the obtained results, we find the proper endomorphisms of $G$ and certain automorphisms of $G$. It allows us to prove that $m = 3$ and $n = 1$. Finally, this implies the order structure of elements of $G$ and the isomorphism $G \cong G_{32}$. 


Lemma 5.11. If \( g \in G \) and \( g^4 = 1 \), then
\[
g = a^{2^{m-2}} \quad \text{or} \quad g = c^2 a^{-2^n(1+2v_0)^{-1}+s2^{m-2}},
\]
where \( s \in \mathbb{Z}_4 \).

Proof. Clearly, if \( g = a^i \), \( i \in \mathbb{Z}_{2^n} \), then \( g^4 = 1 \) if and only if \( g = a^{2^{m-2}} \) for some \( s \in \mathbb{Z}_4 \). Assume \( g \not\in \langle a \rangle \) and \( g^4 = 1 \). Then \( g = c^i a^j \) for some \( k \in \{1, 2, 3\} \) and \( i \in \mathbb{Z}_{2^n} \). If \( k = 1 \) or \( k = 3 \), then \( G = \langle a \rangle \otimes \langle g \rangle \) and the projection of \( G \) onto \( \langle g \rangle \) contradicts property 3. Hence \( g = c^i a^j \) for some \( i \in \mathbb{Z}_{2^n} \) and
\[
g^2 = c^i a^j \cdot c^2 a^j = c^i \cdot c^2 a^i \cdot c^j \cdot a^j = a^{2^{m-1}} \cdot a^{i+j} = a^{2^{m-1}+i(1+r^2)},
\]
for some \( s \in \mathbb{Z}_4 \). The lemma is proved.

Similarly, using (5.14), we get
\[
g^4 = (c^2 a^i)^4 = a^{2^{m-2}+2i(1+r^2)}.
\]

Lemma 5.12. If \( g \in G \) and \( g^5 = 1 \), then
\[
g = a^{w2^{m-1}} \quad \text{or} \quad g = c^2 a^{-2^n(1+2v_0)^{-1}+w2^{m-1}},
\]
where \( w \in \mathbb{Z}_2 \).

Lemma 5.13. If \( g, h \in G \) and \( g^4 = h^4 = 1 \), then \( gh = hg \).

Proof. By (5.12) and (5.13),
\[
c^2 a^{-2^{m-2}} \cdot c^2 = a^{-2^{m-2}} = a^{2^{m-2}}, \quad c^2 \cdot a^{-2^{m-2}} = a^{2^{m-2}} \cdot c^2.
\]

By Lemma 5.11, if \( g = a^{2^{m-2}} \) (\( s \in \mathbb{Z}_4 \)), then \( gh = hg \) for each \( h \in G \) such that \( h^4 = 1 \). Assume that
\[
g = c^2 a^{-k_12^{m-2}}, \quad h = c^2 a^{-k_22^{m-2}},
\]
where \( k = -2^n(1+2v_0)^{-1} \). Then
\[
gh = c^2 a^{-k_12^{m-2}} \cdot c^2 a^{-k_22^{m-2}} = c^2 \cdot a^{-k_12^{m-2} - k_22^{m-2} - k_12^{m-2} - k_22^{m-2}},
\]
\[
= a^{2^{m-1} \cdot a^{k_12^{m-2} + k_22^{m-2}}}, \quad a^{2^{m-1} + k(1+r^2) + (s_1 + s_2)2^{m-2}},
\]
because
\[
r^2(k + s_12^{m-2}) \equiv r^2k + (1 + 4v + 4v^2)s_12^{m-2} \equiv r^2k + s_12^{m-2} \pmod{2^m}.
\]
It follows from here that \( gh = hg \). The lemma is proved.
Lemma 5.14. We have

\[ \text{End}(G) \setminus \text{Aut}(G) = \{ y(g ; h) \mid g, h \in G; g^4 = h^2 = 1 \}. \]  

(5.15)

If \( x \in \text{End}(G) \setminus \text{Aut}(G) \), then

\[ G' \subset \text{Ker}x. \]  

(5.16)

Proof. In view of Lemma 5.13 and \( \langle cG' \rangle \times \langle aG' \rangle \cong C_4 \times C_2 \), the proper endomorphism \( y(g ; h) \) exists for each \( g, h \in G \) such that \( g^4 = h^2 = 1 \). By Lemmas 5.11 and 5.12, the numbers of elements \( g \) and \( h \), satisfying \( g^4 = h^2 = 1 \), are 8 and 4, respectively. Therefore, the number of proper endomorphisms \( y(g ; h) \) of \( G \) is \( 8 \cdot 4 = 32 \). Property \( 2^0 \) implies that each proper endomorphism of \( G \) has this form. Hence (5.15) holds. It follows also that \( \text{Im}x \) is Abelian and hence \( G' \subset \text{Ker}x \) for each proper endomorphism \( x \) of \( G \). The lemma is proved.

Lemma 5.15. The map \( y : G \to G \) given by

\[ cy = c^{i+4i} = ca^{2^{n+1}}, \quad ay = a^j, \quad i \in \mathbb{Z}_{2^m-1}, \quad j \in \mathbb{Z}_{2^n}, \]  

(5.17)

on the generators of \( G \), induces an endomorphism of \( G \) if and only if

\[ j \equiv 1 + 4i (\text{mod} 2^{m-n-1}). \]  

(5.18)

The number of such endomorphisms is \( 2^m \) and those endomorphisms are automorphisms of \( G \).

Proof. The map \( y \) given by (5.17) induces an endomorphism of \( G \) if and only if it preserves the generating relations (5.12) of \( G \), i.e.,

\[ (ay)^{2^m} = 1, \quad (cy)^4 = (ay)^{2^{n+1}}, \quad (cy)^{-1}(ay)(cy) = (ay)' \].  

(5.19)

Clearly, \((ay)^{2^m} = 1\) for all values of \( i \) and \( j \). The last equation of (5.19) holds also for all values of \( i \) and \( j \):

\[ (cy)^{-1}(ay)(cy) = c^{-i(1+4i)}a^ic^{1+4i} = a^{i+4i} = a^i = (ay)'. \]

Since

\[ (cy)^4 = c^4(1+4i) = a^{2^{n+1}(1+4i)}, \quad (ay)^{2^{n+1}} = a^{2^{n+1}}, \]

the second equation of (5.19) holds if and only if equivalence (5.18) is true. The first part of the lemma is proved.

In view of (5.18) and (5.19), we have \( j \equiv 1 \) (mod 2), and, therefore, \( G = \langle c, a \rangle = \langle cy, ay \rangle \), i.e., \( y \) is an automorphism of \( G \). The solutions of (5.19) are

\[ i \in \mathbb{Z}_{2^m-n-1}, \quad j = 1 + 4i + 2^{m-n-1}, \quad s \in \mathbb{Z}_{2^{n+1}} \]

and the number of solutions is \( 2^{m-n-1} \cdot 2^{n+1} = 2^m \). The lemma is proved.

Lemma 5.16. \( m \leq 4, \quad n \leq m - 2 \leq 2 \).

Proof. Assume that \( x \) is a proper endomorphism of \( G \) and let \( y \) be an automorphism of \( G \) given by Lemma 5.15. Then

\[ c^{-1} \cdot cy, \quad a^{-1} \cdot ay \in \langle a^2 \rangle = G'. \]

By (5.16),

\[ (c^{-1} \cdot cy)x = (a^{-1} \cdot ay)x = 1, \quad c(yx) = cx, \quad a(yx) = ax, \]

i.e., \( yx = x \). Property \( 6^0 \) and Lemma 5.15 follow \( m \leq 4 \). Hence \( n \leq m - 2 \leq 2 \). The lemma is proved.
Lemma 5.17. \( m = 3 \).

**Proof.** Let us examine the map \( y : G \longrightarrow G \) given as follows:

\[ cy = ca^{2^i}, \quad ay = a^j, \quad (c^w d') y = (cy)^w (ay)^j, \]

where \( i \in \mathbb{Z}_{2^{n-1}} \), \( j, t \in \mathbb{Z}_{2^n} \), \( w = 0, 1, 2, 3 \). It is easy to check that the map \( y \) preserves the generating relations and induces an endomorphism of \( G \) if and only if

\[ 2^{n+1} + 2i(1 + r)(1 + r^2) \equiv j2^{n+1} \pmod{2^m}. \]

The solution of the last congruence is

\[ j \equiv 1 + 2^{2-n}i(1 + v)(1 + 2v_0) \pmod{2^{m-n-1}}, \]

i.e.,

\[ j \equiv 1 + 2^{2-n}i(1 + v)(1 + 2v_0) + 2^{m-n-1}, s \in \mathbb{Z}_{2^{m+1}}. \tag{5.20} \]

By Lemma 5.16, \( m = 3 \) or \( m = 4 \). Assume on the contrary that \( m = 4 \).

If \( v \) is odd, then similarly to Lemma 5.16, the obtained endomorphism is an automorphism and \( yx = x \) for each proper endomorphism of \( G \). Therefore, by property 6, the number of solutions (5.20) is \( \leq 16 \). The numbers of possible values for \( i \) and \( s \) are \( 2^{m-1} = 2^3 \) and \( 2^{n+1} \), respectively. Hence the number of automorphisms \( y \) is \( 2^3 \cdot 2^{n+1} = 2^{n+4} \). By property 6, \( 2^{n+4} \leq 16 \), i.e., \( n = 0 \).

If \( v \) is even and \( n < 2 \), then similarly to the previous segment, \( n = 0 \). If \( v \) is even and \( n = 2 \), then we can choose \( s = 0 \) and \( i \) such that

\[ i(1 + v)(1 + 2v_0) \equiv 1 \pmod{16}. \]

In this case, we get an endomorphism

\[ cy = ca^{2^i}, \quad ay = a^2, \]

which is a proper endomorphism and \( ay \) is of order eight. This contradicts Lemma 5.14.

We have proved that if \( m = 4 \), then \( n = 0 \) and \( G \) is given by the relations

\[ a^{16} = 1, \quad c^4 = a^2, \quad c^{-1}ac = a^r \]

or, equivalently, by the relations

\[ c^{32} = 1, \quad a^2 = c^4, \quad a^{-1}ca = c^\rho \]

for some \( \rho \neq 1 \) such that

\[ \rho^2 \equiv 1 \pmod{32}. \tag{5.21} \]

Congruence (5.21) is satisfied only for \( \rho \in \{15, -15, -1\} \). If \( \rho = 15 \), then \([c, a] = c^{14} \) and \( c^2 \in G' \), which is impossible. Similarly, the case \( \rho = -1 \) is impossible. If \( \rho = -15 \), then \([c, a] = c^{-16} = c^{16} \in \mathbb{Z}(G) \) and \( G' = \langle c^{16} \rangle \cong C_2 \), which is also impossible. Therefore, the case \( m = 4 \) is impossible and \( m = 3 \). The lemma is proved.

By Lemmas 5.16 and 5.17, the group \( G \) is a group of order 32 and it is given by the relations

\[ a^8 = 1, \quad c^4 = a^{3n+1}, \quad c^{-1}ac = a^r, \quad 0 \leq n \leq 1. \]

Similarly to the last part of the proof of Lemma 5.17, it is easy to check that the case \( n = 0 \) is impossible. Hence \( n = 1 \) and

\[ c^4 = a^4. \]

We have \( r \neq 1 \), because \( G \) is non-Abelian. Also \( r \neq -3 \), because otherwise \([a, c] = a^{-4} \), and we have \( G' = \langle a^4 \rangle \cong C_2 \), which is impossible. Hence \( r = 3 \) or \( r = -1 \). In both cases the numbers of elements of order two is 3, of order four is 4, and of order eight is 24. By [5], there is only one non-Abelian group of order 32 which has this order structure of its elements. This group is \( D_{24} \). The theorem is proved.
Theorem 5.2. The group $G_{32}$ is determined by its endomorphism semigroup in the class of all groups.

Proof. Let $G^*$ be a group such that the endomorphism semigroups of $G^*$ and $G_{32}$ are isomorphic:

$$\text{End}(G^*) \cong \text{End}(G_{32}). \quad (5.22)$$

Since $\text{End}(G^*)$ is finite, so is $G^*$ ([1], Theorem 2). The group $G_{32}$ satisfies properties $1^0$–$6^0$ of Theorem 5.1. In view of isomorphism $(5.22)$, the group $G^*$ satisfies also these properties. Properties $1^0$–$3^0$ imply that $G^*$ is a 2-group. By Lemma 3.5 and isomorphism $(5.22)$, $|G^*| \geq 32$. Theorem 5.1 implies the isomorphism $G^* \cong G_{32}$. The theorem is proved.

ACKNOWLEDGEMENT

This work was partially supported by the Estonian Ministry of Education and Research (project SF0140011s09).

REFERENCES