HOPF-GALOIS STRUCTURES ON CYCLIC EXTENSIONS AND SKEW BRACES WITH CYCLIC MULTIPLICATIVE GROUP

CINDY (SIN YI) TSANG

(Communicated by Benjamin Brubaker)

Abstract. Let $G$ and $N$ be two finite groups of the same order. It is known that the existences of the following are equivalent.

(a) a Hopf-Galois structure of type $N$ on any Galois $G$-extension
(b) a skew brace with additive group $N$ and multiplicative group $G$
(c) a regular subgroup isomorphic to $G$ in the holomorph of $N$

We shall say that $(G,N)$ is realizable when any of the above exists. Fixing $N$ to be a cyclic group, W. Rump has determined the groups $G$ for which $(G,N)$ is realizable. In this paper, fixing $G$ to be a cyclic group instead, we shall give a complete characterization of the groups $N$ for which $(G,N)$ is realizable.

1. Introduction

Let $G$ and $N$ be two finite groups of the same order. It is well-known that the existences of the following are equivalent (see [12, Chapter 2] and [17]).

(a) a Hopf-Galois structure of type $N$ on any Galois $G$-extension
(b) a skew brace with additive group $N$ and multiplicative group $G$
(c) a regular subgroup isomorphic to $G$ in the holomorph of $N$

Here, the holomorph of $N$ is defined to be

$$\text{Hol}(N) = \lambda(N) \rtimes \text{Aut}(N) = \rho(N) \rtimes \text{Aut}(N),$$

where $\lambda$ and $\rho$ denote the left and right regular representations

$$\lambda(\eta) = (x \mapsto \eta x), \quad \rho(\eta) = (x \mapsto x\eta^{-1}) \quad \text{for} \quad \eta, x \in N,$$

and a subgroup $G$ of $\text{Hol}(N)$ is called regular if $G \rightarrow N; \sigma \mapsto \sigma(1_N)$ is bijective. Following [13], we shall say that $(G,N)$ is realizable when any of the above conditions is satisfied. We remark that skew braces are ring-like structures introduced to study set-theoretic solutions to the Yang-Baxter equation.

Notice that $\lambda(N), \rho(N) \simeq N$ are regular subgroups of $\text{Hol}(N)$, so the pair $(G,N)$ is always realizable when $G \simeq N$. But whether $(G,N)$ is realizable depends upon the groups $G$ and $N$ when $G \not\simeq N$. It is therefore natural to ask which pairs $(G,N)$ are realizable. For example, when $G$ is fixed to be

- any group of squarefree order [1,3],
- any group of order $p^3$ with $p$ a prime [22],
- any non-abelian simple and more generally quasisimple group [9,28],

Received by the editors December 27, 2021, and, in revised form, May 29, 2022.
2020 Mathematics Subject Classification. Primary 20B35; Secondary 12F10, 16T05, 16T25.
Key words and phrases. Hopf-Galois structures, skew braces, regular subgroups, holomorph.
This work was supported by JSPS KAKENHI (Grant-in-Aid for Research Activity Start-up) Grant Number 21K20319.

©2022 by the author(s) under Creative Commons Attribution-NonCommercial 3.0 License (CC BY NC 3.0)
the symmetric group $S_n$ with $n \geq 5$ [25],

- the automorphism group of any sporadic simple group [27],

the groups $N$ for which the pair $(G, N)$ is realizable are completely known. There are also other papers (see [4,10,16,21,26] for example) which investigate necessary relations between $G$ and $N$ in order for $(G, N)$ to be realizable.

Cyclic groups have the simplest structure among all groups. It then seems natural to ask for which groups such cyclic group of order $n$. The purpose of this paper is to characterize all such $N$.

Let us first recall some known results. For $n$ an odd prime power, we have:

**Proposition 1.1.** Let $N$ be any group of order $p^m$ with $p$ an odd prime. Then the pair $(C_{p^m}, N)$ is realizable if and only if $N \simeq C_{p^m}$.

**Proof.** See [18, Theorem 4.5] or alternatively [24, Theorem 1.5]. □

For $n$ a power of 2, the situation is different but has also been solved. To state the result, we need some notation. For $m \geq 2$, write

$$D_{2m} = \langle r, s \mid r^{2m-1} = 1, s^2 = 1, sr^s = r^{-1} \rangle$$

for the dihedral group of order $2^m$, and note that $D_4$ is the Klein four-group. For $m \geq 3$, similarly write

$$Q_{2^m} = \langle r, s \mid r^{2^{m-1}} = 1, s^2 = r^{2^{m-2}}, sr^s = r^{-1} \rangle$$

for the generalized quaternion group of order $2^m$. It is known that:

**Proposition 1.2.** Let $N$ be any group of order $2^m$. Then:

(a) For $m \leq 2$, the pair $(C_{2^m}, N)$ is always realizable.

(b) For $m \geq 3$, the pair $(C_{2^m}, N)$ is realizable if and only if $N \simeq C_{2^m}, D_{2^m}, Q_{2^m}$.

**Proof.** See [6, Lemma 2] for (a) and [7, Corollary 5.3, Theorem 6.1] for (b). □

By [8, Theorem 1], using Propositions 1.1 and 1.2, we obtain a complete characterization of nilpotent groups $N$ for which $(C_n, N)$ is realizable. We remark that the exact number of Hopf-Galois structures of nilpotent type $N$ on any Galois $C_n$-extension is explicitly given in [8, Theorem 2]. But as the next proposition shows, the pair $(C_n, N)$ can also be realizable for non-nilpotent groups $N$.

A finite group is called a $C$-group (or $Z$-group) if all of its Sylow subgroups are cyclic. The terminology comes from [19], where a very nice description of $C$-groups was given. By [19, Lemma 3.5], every $C$-group may be presented as

$$C(e, d, k) = \langle x, y \mid x^e = 1, y^d = 1, yxy^{-1} = x^k \rangle$$

for $\gcd(e, d) = \gcd(e, k) = 1$, and the order of $k$ in $(\mathbb{Z}/e\mathbb{Z})^\times$ divides $d$. Then, it is essentially known by work in the literature that:

**Proposition 1.3.** For any $C$-group $N$ of order $n$, the pair $(C_n, N)$ is realizable.

**Proof.** Since $N$ is a $C$-group, by the above $N \simeq C_e \times C_d$ with $\gcd(e, d) = 1$. Then, it is known and we shall also explain in Proposition 2.4 that $(C_e \times C_d, N)$ is realizable. But $C_n \simeq C_e \times C_d$ since $n = ed$ with $\gcd(e, d) = 1$, and the claim now follows. □

For $n$ squarefree, every group $N$ of order $n$ is a $C$-group so the pair $(C_n, N)$ is always realizable. In fact, the number of Hopf-Galois structures of type $N$ on any Galois $C_n$-extension has been determined in terms of the orders of the center and
commutator subgroup of \( N \) (see [1]). Similarly for the number of skew braces with additive group \( N \) and multiplicative group \( C_n \) (see [3]).

For \( n \) arbitrary, however, not every group \( N \) of order \( n \) is a \( C \)-group and the pair \((C_n, N)\) can certainly be realizable for a non-\( C \)-group \( N \) because of Proposition 1.2.

The only known general restriction on \( N \) so far is:

**Proposition 1.4.** Let \( N \) be any group of order \( n \) such that \((C_n, N)\) is realizable. Then \( N \) is both supersolvable and metabelian.

**Proof.** See [26, Theorem 1.3(a),(b)]. \(\Box\)

Unfortunately, the converse of Proposition 1.4 is false. For example, we checked in MAGMA [5] that the group \( N = \text{SmallGroup}(84,8) \) is both supersolvable and metabelian, yet the pair \((C_{84}, N)\) is not realizable.

In this paper, by building upon the four propositions mentioned above, we shall give a complete characterization of the groups \( N \) of order \( n \) for which \((C_n, N)\) is realizable, without imposing any assumptions on \( n \) or \( N \). By Proposition 1.3, it is enough to consider non-\( C \)-groups \( N \). Our main theorem is:

**Theorem 1.5.** Let \( N \) be any non-\( C \)-group of order \( n \). Then \((C_n, N)\) is realizable if and only if \( N \simeq M \rtimes_{\alpha} P \) for some \( C \)-group \( M \) of odd order and \((P, \alpha)\) satisfying one of the following conditions:

1. \( P = D_4 \) or \( P = Q_8 \), and \( \alpha(P) \) has order 1 or 2;
2. \( P = D_{2m} \) with \( m \geq 3 \) or \( P = Q_{2m} \) with \( m \geq 4 \), and \( \alpha(r) = \text{Id}_M \).

Here \( \alpha : P \to \text{Aut}(M) \) is the homomorphism that defines the semidirect product, and \( r \) is the element of \( P \) in the presentation (1.1) or (1.2).

**Corollary 1.6.** Let \( N \) be any group of order \( n \) for \( n \not\equiv 0 \pmod{4} \). Then \((C_n, N)\) is realizable if and only if \( N \) is a \( C \)-group.

**Proof.** The forward implication holds by Theorem 1.5 because there \( M \) is a group of odd order while \( P \) is a 2-group of order at least 4. The backward implication is Proposition 1.3. \(\Box\)

**Remark 1.7.** Instead of fixing \( G \) to be cyclic, one can also fix \( N \) to be cyclic and ask for which groups \( G \) is the pair \((G, C_n)\) realizable. This case has already been solved completely in [20, Corollary 1 to Theorem 2], which states that

\((G, C_n)\) is realizable \iff \(G\) is solvable, 2-nilpotent, almost Sylow-cyclic.

Here \( G \) being 2-nilpotent means that it has a normal Hall 2'-subgroup \( M \). By the Schur-Zassenhaus theorem, this simply means that \( G = M \rtimes P \), where \( P \) denotes any Sylow 2-subgroup of \( G \). The term *almost Sylow-cyclic* means that every Sylow \( p \)-subgroup is cyclic for odd primes \( p \) and any non-trivial Sylow 2-subgroup admits a cyclic subgroup of index 2. We then see that the pair \((G, C_n)\) is realizable if and only if \( G \simeq M \rtimes_{\alpha} P \), where

- (a) \( M \) is any \( C \)-group of odd order,
- (b) \( P \) is trivial or any 2-group admitting a cyclic subgroup of index 2,

and there is no restriction on the homomorphism \( \alpha : P \to \text{Aut}(M) \). Notice that such a group \( G \) is always solvable because \( C \)-groups are solvable.

Comparing this with our Theorem 1.5, we deduce that realizability of \((C_n, \Gamma)\) implies that of \((\Gamma, C_n)\), but the converse fails to hold for certain values of \( n \).
2. Methods to study realizability

Let $G$ and $N$ be two finite groups of the same order. Below, we review a couple of techniques that can be used to study the realizability of $(G,N)$.

2.1. Characteristic subgroups and induction. To prove that the pair $(G,N)$ is not realizable, one approach is to use characteristic subgroups $M$ of $N$, namely subgroups $M$ such that $\pi(M) = M$ for all $\pi \in \text{Aut}(N)$. This was developed by the author in [24, Section 4] and was inspired by work of [9].

First, recall that given $f \in \text{Hom}(G,\text{Aut}(N))$, a map $g : G \rightarrow N$ is said to be a crossed homomorphism (with respect to $f$) if it satisfies

\[
  g(\sigma \tau) = g(\sigma) \cdot f(\sigma)(g(\tau)) \quad \text{for all } \sigma, \tau \in G.
\]

Let us write $Z_1^1(G,N)$ for the set of all such crossed homomorphisms.

**Proposition 2.1.** The regular subgroups of $\text{Hol}(N)$ isomorphic to $G$ are precisely the subsets of $\text{Hol}(N)$ of the form

\[
  \{\rho(g(\sigma)) \cdot f(\sigma) : \sigma \in G\}, \quad \text{where } \begin{cases} f \in \text{Hom}(G,\text{Aut}(N)), \\ g \in Z_1^1(G,N) \text{ is bijective.} \end{cases}
\]

**Proof.** This is because $\text{Hol}(N) = \rho(N) \rtimes \text{Aut}(N)$; or see [24, Proposition 2.1]. \hfill \Box

The next proposition gives us a way to show that $(G,N)$ is not realizable using characteristic subgroups $M$ of $N$ and induction (by passing to the subgroup $M$ or the quotient $N/M$). We remark that (a) was previously known but (b) is new.

**Proposition 2.2.** Let $f \in \text{Hom}(G,\text{Aut}(N))$ and let $g \in Z_1^1(G,N)$ be bijective. Let $M$ be any characteristic subgroup of $N$ and define $H = g^{-1}(M)$. Then:

(a) $H$ is a subgroup of $G$ and the pair $(H,M)$ is realizable;

(b) $H$ is a normal subgroup of $G$ and the pair $(G/H,N/M)$ is realizable, as long as $H$ lies in the center $Z(G)$ of $G$.

**Proof.** By [2.1] and the fact that $M$ is a characteristic subgroup of $N$, plainly $H$ is a subgroup of $G$, which has the same order as $M$ because $g$ is bijective.

That $(H,M)$ is realizable was shown in [26, Proposition 3.3]. The idea was that via restriction $f$ induces a homomorphism

\[
  \tilde{f}_M \in \text{Hom}(H,\text{Aut}(M)); \quad \tilde{f}_M(\tau) = (\eta \mapsto f(\tau)(\eta))
\]

since $M$ is characteristic, and $g$ induces a bijective crossed homomorphism

\[
  \tilde{g}_M \in Z_1^1(H,M); \quad \tilde{g}_M(\tau) = g(\tau)
\]

since $M = g(H)$. From Proposition 2.1 we then get a regular subgroup of $\text{Hol}(M)$ isomorphic to $H$, whence the pair $(H,M)$ is realizable.

Suppose now that $H$ lies in $Z(G)$. It is clear that $H$ is a normal subgroup of $G$. First, we show that $f$ induces a well-defined homomorphism

\[
  \tilde{f}_M \in \text{Hom}(G/H,\text{Aut}(N/M)); \quad \tilde{f}_M(\sigma H) = (\eta M \mapsto f(\sigma)(\eta)M).
\]

For any $\sigma \in G$ and $\tau \in H$, since $H$ lies in $Z(G)$, by [2.1] we have

\[
  g(\tau) \cdot f(\tau)(g(\sigma)) = g(\sigma \tau) = g(\sigma \cdot f(\sigma)(g(\tau))) = g(\sigma) \cdot f(\sigma)(g(\tau)).
\]

But $M = g(H)$ is characteristic, so reducing mod $M$ then yields

\[
  f(\tau)(g(\sigma)) \equiv g(\sigma) \pmod{M}.
\]
Since \( g \) is bijective, it follows that \( f(\tau) \) induces the identity automorphism on \( N/M \) for all \( \tau \in H \), so indeed \( \overline{f}_M \) is well-defined. Similarly \( g \) induces a bijective crossed homomorphism

\[
\overline{g}_M \in Z^1_m(G/H, N/M); \quad \overline{g}_M(\sigma H) = g(\sigma)M,
\]
which is well-defined by Proposition 2.1 since \( M = g(H) \) is characteristic. From Proposition 2.1, we then get a regular subgroup of \( \text{Hol}(N/M) \) isomorphic to \( G/H \), whence the pair \((G/H, N/M)\) is realizable. □

2.2. Fixed point free pairs of homomorphisms. To prove that \((G, N)\) is realizable, one approach is to use homomorphisms \( f, h \in \text{Hom}(G, N) \) such that \((f, h)\) is fixed point free, namely \( f(\sigma) = h(\sigma) \) if and only if \( \sigma = 1_G \). This was introduced by N. P. Byott and L. N. Childs in [11].

Proposition 2.3. Let there exist \( f, h \in \text{Hom}(G, N) \) such that \((f, h)\) is fixed point free. Then \((G, N)\) is realizable.

Proof. Since elements in \( \lambda(N) \) and \( \rho(N) \) commute, plainly

\[
\{ \rho(h(\sigma))\lambda(f(\sigma)) : \sigma \in G \}
\]
is a subgroup of \( \text{Hol}(N) \) isomorphic to \( G \), whose regularity follows from the fixed-point freeness of \((f, h)\); see [11] Proposition 1 for a proof. Let us note that in the notation of Proposition 2.1, this corresponds to

\[
\text{conj}(\eta) = (x \mapsto \eta x \eta^{-1}) \quad \text{denotes conjugation by} \ \eta,
\]
which is bijective because \((f, h)\) is fixed point free. □

The next proposition is from [10] Lemma 7.1.

Proposition 2.4. Suppose that \( N = N_1N_2 \) for subgroups \( N_1 \) and \( N_2 \) such that \( N_1 \cap N_2 = 1 \). Then \((N_1 \times N_2, N)\) is realizable.

Proof. Trivially \((f, h)\) is a fixed point free pair for \( f, h \in \text{Hom}(N_1 \times N_2, N) \) defined by \( f(\eta_1, \eta_2) = \eta_1 \) and \( h(\eta_1, \eta_2) = \eta_2 \). The claim then holds by Proposition 2.3. □

As noted in Proposition 1.3, an easy application of Proposition 2.4 shows that \((C_n, N)\) is always realizable for \( C\)-groups \( N \) of order \( n \). However, as we shall prove below, there is no fixed point free pair of homomorphisms from \( C_n \) to \( N \) for non-\( C\)-groups \( N \). Therefore, we cannot simply use Proposition 2.3 to show realizability in Theorem 1.5. We shall exhibit the existence of a cyclic regular subgroup in \( \text{Hol}(N) \) using a direct approach.

Proposition 2.5. Let \( N \) be any group of order \( n \) such that there is a fixed point free pair \((f, h)\) with \( f, h \in \text{Hom}(C_n, N) \). Then \( N \) is a \( C\)-group.

Proof. Let \( \sigma \) be a generator of \( C_n \), and put

\[
d_f = |f(\sigma)|, \quad d_h = |h(\sigma)|, \quad g = \gcd(d_f, d_h).
\]
Then \( \sigma^{d_fd_h/g} = 1_G \) because \((f, h)\) is fixed point free and

\[
f(\sigma)^{d_f(d_h/g)} = 1_N = h(\sigma)^{d_h(d_f/g)}.
\]
But $d_f d_h / g$ divides $n$ since both $d_f, d_h / g$ divide $n$ and $\gcd(d_f, d_h / g) = 1$. It then follows that $d_f d_h / g = n$ and so $n = \lcm(d_f, d_h)$. Hence, we may write

$$d_f = p_1^{e_1} \cdots p_a^{e_a} g_f$$

and

$$d_h = p_{a+1}^{e_{a+1}} \cdots p_b^{e_b} g_h,$$

where $p_1, \ldots, p_a, p_{a+1}, \ldots, p_b$ are distinct primes and $g_f, g_h \in \mathbb{N}$, such that

$$n = p_1^{e_1} \cdots p_a^{e_a} p_{a+1}^{e_{a+1}} \cdots p_b^{e_b}$$

is the prime factorization of $n$. Then

$$|f(\sigma)^{g_f}| = p_1^{e_1} \cdots p_a^{e_a}, \quad |h(\sigma)^{g_h}| = p_{a+1}^{e_{a+1}} \cdots p_b^{e_b}, \quad |f(\sigma)^{g_f}| |h(\sigma)^{g_h}| = n.$$ 

We deduce that $N = \langle f(\sigma)^{g_f}, h(\sigma)^{g_h} \rangle$ is the product of two cyclic subgroups of coprime orders, and thus $N$ is a $C$-group. \hfill $\square$

3. Preliminary Restriction

Let us first prove a preliminary version of Theorem 1.5.

**Theorem 3.1.** Let $N$ be any group of order $n$ such that $(C_n, N)$ is realizable. Then either $N$ is a $C$-group or $N \simeq M \times P$ for some $C$-group $M$ of odd order and for $P = D_{2m}$ with $m \geq 2$ or $P = Q_{2m}$ with $m \geq 3$.

**Proof.** Let $n = p_1^{e_1} \cdots p_b^{e_b}$ be the prime factorization of $n$ with $p_1 > \cdots > p_b$. For each $1 \leq a \leq b$, let $P_a$ be a Sylow $p_a$-subgroup of $N$. Put

$$M = P_1 \cdots P_{b-1}$$

and $P = P_b$.

Since $N$ has to be supersolvable by Proposition 1.4 by [23] Corollary VII.5.h] for example, we know that $M$ is a normal subgroup of $N$ and $N = M \times P_b$. But plainly $M$ is a characteristic subgroup of $N$, so by Proposition 2.2 there is a subgroup $H$ of $C_n$ (of the same order as $M$) such that the pairs $(H, M)$ and $(C_n/H, N/M)$ are both realizable. Note that

$$H \simeq C_{p_1^{e_1} \cdots p_{b-1}^{e_{b-1}}}$$

and

$$N/H \simeq C_{p_b^{e_b}}$$

are both cyclic. Thus, we may prove the claim using induction on $b$.

First, consider the case when $n$ is odd. For $b = 1$, we know by Proposition 1.1 that $N \simeq C_{p_1^{e_1}}$ is a $C$-group. For $b \geq 2$, by induction we may assume that $M$ is a $C$-group, which implies that $P_1, \ldots, P_{b-1}$ are all cyclic. But $P \simeq N/M$ is cyclic by Proposition 1.1 whence $N$ is a $C$-group.

Next, consider the case when $n$ is even, so then $p_b = 2$. Since $M$ has odd order, we already know that $M$ must be a $C$-group. If $P$ is cyclic, then $N$ is a $C$-group as above. If $P \simeq N/M$ is non-cyclic, then necessarily

$$P \simeq D_4$$

when $e_b = 2$ and

$$P \simeq D_{2^{e_b}}, Q_{2^{e_b}}$$

when $e_b \geq 3$

by Proposition 1.2. This completes the proof of the theorem. \hfill $\square$

**Remark 3.2.** The converse of Theorem 3.1 is false. For example, as mentioned in the introduction, the pair $(C_{84}, N)$ is not realizable for $N = \text{SmallGroup}(84, 8)$ but $N \simeq C_{21} \rtimes D_4$, as one can check using MAGMA [5]. Alternatively, this group $N$ corresponds to the case when $\alpha : D_4 \to \text{Aut}(C_{21})$ embeds $D_4$ into the unique Sylow 2-subgroup of $\text{Aut}(C_{21})$. One sees that $N \simeq D_{14} \times D_6$. Since both factors $D_{14}$ and $D_6$ are characteristics, we have

$$\text{Hol}(N) \simeq \text{Hol}(D_{14}) \times \text{Hol}(D_6).$$
The automorphism group of dihedral groups is well-understood (see [14] Theorem 1.4 for example). It is not hard to see that \( \text{Hol}(D_{14}) \) and \( \text{Hol}(D_6) \) do not have any elements of order 4. This means that \( \text{Hol}(N) \) does not even have a cyclic subgroup of order 84, let alone a regular one. Hence, indeed \( (C_{84},N) \) is not realizable.

4. Groups of the shape \( M \rtimes_\alpha P \)

Throughout this section, let \( M \) denote the \( C \)-group
\[
C(e,d,k) = \langle x,y \mid x^e = 1, y^d = 1, yxy^{-1} = x^k \rangle
\]
for \( \gcd(e,d) = \gcd(e,k) = 1 \), and the order \( \text{ord}_e(k) \) of \( k \) in \( (\mathbb{Z}/e\mathbb{Z})^\times \) divides \( d \). Also, let \( P \) denote the dihedral group
\[
D_{2m} = \langle r,s \mid r^{2m-1} = 1, s^2 = 1, srs^{-1} = r^{-1} \rangle
\]
with \( m \geq 2 \) or the generalized quaternion group
\[
Q_{2m} = \langle r,s \mid r^{2m-1} = 1, s^2 = r^{2m-2}, srs^{-1} = r^{-1} \rangle
\]
with \( m \geq 3 \). To prove Theorem 1.5, we shall need to understand the structure of the semidirect products \( M \rtimes_\alpha P \) for \( \alpha \in \text{Hom}(P, \text{Aut}(M)) \).

4.1. Automorphism group of \( C \)-groups. Let us first determine the automorphism group \( \text{Aut}(M) \) of \( M \) in a way that is analogous to [12] Lemma 4.1], which treats the special case when \( ed \) is squarefree.

For \( h \in \mathbb{Z} \) and \( \ell \in \mathbb{N}_{\geq 0} \), let us define
\[
S(h,\ell) = \sum_{a=0}^{\ell-1} h^a = 1 + h + \cdots + h^{\ell-1},
\]
with the empty sum \( S(h,0) \) representing 0. For \( i,j \in \mathbb{Z} \), a simple calculation using induction on \( \ell \) and the relation \( yxy^{-1} = x^k \) yields
\[
(x^iy^j)^\ell = x^{iS(k,\ell)}y^{j\ell}.
\]
We shall use this identity without reference in what follows. Also put
\[
z = \gcd(e,k-1) \quad \text{and} \quad g = e/z.
\]

Further, consider the multiplicative groups
\[
U(e) = (\mathbb{Z}/e\mathbb{Z})^\times \quad \text{and} \quad U_k(d) = \{ v \in (\mathbb{Z}/d\mathbb{Z})^\times \mid v \equiv 1 \pmod{\text{ord}_e(k)} \}.
\]
Recall that \( \text{ord}_e(k) \) denotes the order of \( k \) in \( (\mathbb{Z}/e\mathbb{Z})^\times \) and it divides \( d \).

Lemma 4.1. For any \( u \in U(e) \) and \( v \in U_k(d) \), the definitions
\[
\begin{align*}
\theta(x) &= x \\
\phi_u(x) &= x^u \\
\psi_v(x) &= x \\
\phi_u(y) &= y \\
\psi_v(y) &= y^v
\end{align*}
\]
extend to automorphisms on \( M \). Moreover, we have the relations
\[
\theta^g = \text{Id}_M, \quad \phi_u\theta\phi_u^{-1} = \theta^u, \quad \theta\psi_v = \psi_v\theta, \quad \phi_u\psi_v = \psi_v\phi_u.
\]
Proof. We may assume that \( k \neq 1 \), for otherwise \( M \simeq C_e \times C_d \) (with \( z = e \) and so \( \theta \) is the identity), in which case all of the claims are trivial.

First, let us check that the three relations \( x^e = 1, y^d = 1, xy^{-1} = x^k \) in the presentation of \( M \) are preserved under these maps. Clearly
\[
\theta(x)^e = \phi_u(x)^e = \psi_v(x)^e = 1 \quad \text{and} \quad \phi_u(y)^d = \psi_v(y)^d = 1
\]
are satisfied. We compute that
\[
\theta(y)^d = (x^z y)^d = x^{zS(k,d)} y^d = x^{zS(k,d)}.
\]
Since \( \text{ord}_e(k) \) divides \( d \), we have
\[
\left( \frac{k-1}{z} \right) zS(k,d) \equiv k^d - 1 \equiv 0 \pmod{e}.
\]
But \( \gcd\left( \frac{k-1}{z}, e \right) = 1 \), so then \( zS(k,d) \equiv 0 \pmod{e} \) and we obtain \( \theta(y)^d = 1 \). A simple calculation also yields
\[
\theta(y)\theta(x)\theta(y)^{-1} = (x^z y) (x^z y)^{-1} = x^k = \theta(x)^k,
\]
\[
\phi_u(y)\phi_u(x)\phi_u(y)^{-1} = y x^u y^{-1} = x^{u_k} = \phi_u(x)^k,
\]
\[
\psi_v(y)\psi_v(x)\psi_v(y)^{-1} = y^v x y^{-v} = x^{k^v} = x^k = \psi_v(x)^k,
\]
where \( x^{k^v} = x^k \) because \( v \in U_k(d) \) implies \( k^v \equiv k \pmod{e} \). Thus, all of \( \theta, \phi_u, \psi_v \) extend to endomorphisms on \( M \). It is clear that their images all contain \( x, y \), so in fact \( \theta, \phi_u, \psi_v \) extend to automorphisms on \( M \).

Next, let us verify the relations in (4.1). The first and last equalities are both obvious. For the second equality, a simple calculation shows that
\[
(\phi_u \theta)(x) = x^u = (\theta^u \phi_u)(x) \quad \text{and} \quad (\phi_u \theta)(y) = x^{uz} y = (\theta^u \phi_u)(y).
\]
For the third equality, plainly \( (\theta \psi_v)(x) = x = (\psi_v \theta)(x) \). We also have
\[
(\theta \psi_v)(y) = (x^z y)^v = x^{zS(k,v)} y^v \quad \text{and} \quad (\psi_v \theta)(y) = x^z y^v.
\]
But \( v \in U_k(d) \) implies that \( k^v \equiv k \pmod{e} \), so then
\[
\left( \frac{k-1}{z} \right) zS(k,v) \equiv k^v - 1 \equiv k - 1 \equiv \left( \frac{k-1}{z} \right) z \pmod{e}.
\]
Since \( \gcd\left( \frac{k-1}{z}, e \right) = 1 \), this implies that
\[
(4.2) \quad zS(k,v) \equiv z \pmod{e} \quad \text{and hence} \quad (\theta \psi_v)(y) = (\psi_v \theta)(y).
\]
It follows that \( \theta \psi_v = \psi_v \theta \), as desired. \hfill \Box

**Proposition 4.2.** We have
\[
\text{Aut}(M) = \left( \langle \theta \rangle \times \{ \phi_u \}_{u \in U(e)} \right) \times \{ \psi_v \}_{v \in U_k(d)}.
\]

**Proof.** It is easy to see that \( \langle \theta \rangle, \{ \phi_u \}_{u \in U(e)} \), \( \{ \psi_v \}_{v \in U_k(d)} \) are subgroups of \( \text{Aut}(M) \) having trivial pairwise intersections. By the relations in (4.1), it is then enough to show that every \( \pi \in \text{Aut}(M) \) lies in their product.

First, since \( \gcd(e,d) = 1 \), clearly
\[
\pi(x) = x^u \quad \text{with} \quad u \in U(e), \quad \text{and let us write} \quad \pi(y) = x^v y^v.
\]
We must have \( \gcd(v,d) = 1 \), for otherwise there would exist \( \ell \in \mathbb{N} \) which is strictly less than \( d \) such that \( d \) divides \( v \ell \), and
\[
\pi(y)^\ell = (x^v y^v)^\ell = x^{\ell S(k^v, \ell)} y^{\ell v} = x^{\ell S(k^v, \ell)}.
\]
But \((\pi(y))\), which has order \(d\), cannot contain a non-trivial element of order dividing \(e\) because \(\gcd(e, d) = 1\). This then implies that \(\pi(y)^{\ell} = 1\), which is impossible since \(1 \leq \ell \leq d - 1\). Next, observe that
\[
x^{uk^v} = (x^c y^v) x^u (x^c y^v)^{-1} = \pi(y) \pi(x) \pi(y)^{-1} = \pi(x)^k = x^{uk}.
\]
Since \(\gcd(u, e) = 1\), it follows that
\[k^v \equiv k \pmod{e},\] and hence \(v \in U_k(d)\).

We also have the equalities
\[1 = \pi(y)^d = (x^c y^v)^d = x^{cS(k^v, d)} y^{dv} = x^{cS(k^v, d)}.
\]
Recall that \(z = \gcd(e, k - 1)\). Then, the above in particular implies that
\[cd \equiv cS(1, d) \equiv cS(k^v, d) \equiv 0 \pmod{z},\]
and so \(c\) is divisible by \(z\) because \(\gcd(z, d) = 1\).

Finally, we compute that
\[
(\theta^{\frac{c}{d}} \phi_u \psi_v)(x) = (\theta^{\frac{c}{d}} \phi_u)(x) = \theta^{\frac{c}{d}} (x^u) = x^u,
\]
\[
(\theta^{\frac{c}{d}} \phi_u \psi_v)(y) = (\theta^{\frac{c}{d}} \phi_u)(y^v) = \theta^{\frac{c}{d}} (y^v) = (x^{\frac{c}{d}} y^v) = x^{zS[k, v]} y^v = x^cy^v,
\]
where the last equality follows from the congruence in (1.2). Thus \(\pi = \theta^{\frac{c}{d}} \phi_u \psi_v\), and this completes the proof. \(\square\)

4.2. Dihedral and generalized quaternion groups. Let us record a few facts that we shall need concerning the commutator subgroup \(P'\) of \(P\) and the automorphism group \(\text{Aut}(P)\) of \(P\).

**Lemma 4.3.** We have \(P' = \langle r^2 \rangle\) and \(P/P' \simeq D_4\).

**Proof.** Note that \(r^2 \in P'\) because \(srs^{-1} r^{-1} = r^{-2}\), and clearly \(\langle r^2 \rangle\) is a normal subgroup of order \(2^{m-2}\). Since \(P/\langle r^2 \rangle\) has order 4, whose exponent is easily seen to be 2, we must have \(P/\langle r^2 \rangle \simeq D_4\). The fact that \(r^2 \in P'\) and \(P/\langle r^2 \rangle\) is abelian implies that \(P' = \langle r^2 \rangle\). \(\square\)

**Proposition 4.4.** The following hold.

(a) The definitions \(\{\kappa_1(r) = s, \kappa_1(s) = r\}\) and \(\{\kappa_2(r) = rs, \kappa_2(s) = s\}\) extend to automorphisms on \(D_4\).

(b) The definitions \(\{\kappa_1(r) = s, \kappa_1(s) = rs^2\}\) and \(\{\kappa_2(r) = rs, \kappa_2(s) = r\}\) extend to automorphisms on \(Q_8\).

(c) Assume that \(P = D_{2m}\) with \(m \geq 3\) or \(P = Q_{2m}\) with \(m \geq 4\). For any \(a, b \in \mathbb{Z}\) with \(a\) odd, the definition \(\{\kappa(r) = r^a, \kappa(s) = r^b s\}\) extends to an automorphism on \(P\). Conversely, all automorphisms on \(P\) arise in this way.

**Proof.** Part (a) is obvious and part (b) follows from a simple calculation. As for part (c), see [13] Theorem 1.4 and [15] Theorem 4.7. \(\square\)

**Remark 4.5.** In Proposition 4.4, the \(\kappa_1, \kappa_2\) in (a) do not extend to automorphisms on \(D_{2m}\) for \(m \geq 3\), and those in (b) do not extend to automorphisms on \(Q_{2m}\) for \(m \geq 4\). This is the reason why there are two cases to consider in Theorem 1.3.
4.3. Properties of the homomorphism $\alpha$. Let $\alpha \in \text{Hom}(P, \text{Aut}(M))$ be fixed, and let $N = M \rtimes_\alpha P$ be the semidirect product defined by $\alpha$. For each $t \in P$, let us write $\alpha_t = \alpha(t)$ for short. Then, in the group $N$ we have
\[ txx^{-1} = \alpha_t(x) \text{ and } tyt^{-1} = \alpha_t(y). \]
We shall study properties of $\alpha$ using results from the previous subsections.

**Assumptions.** Henceforth, we shall assume that the order $ed$ of $M$ is odd since this is the only case of interest for us. In the presentation of $M$, by [19], without loss of generality, we may assume that $\text{ord}_e(k)$, which has to divide $d$, is divisible by all prime factors of $d$.

**Lemma 4.6.** The homomorphism $\alpha$ satisfies the following:

(a) $\alpha(P)$ lies in $\langle \theta \rangle \rtimes \{ \phi_u \}_{u \in U(e)}$;

(b) $\ker(\alpha)$ contains $P'$;

(c) $\alpha(P)$ is elementary 2-abelian of order 1, 2, or 4;

(d) $\alpha_t(x) = \alpha_{t^2}(x)$ implies $\alpha_{t_1} = \alpha_{t_2}$ for any $t_1, t_2 \in P$.

**Proof.** Since $\text{ord}_e(k)$ is divisible by all prime factors of $d$, the order of $U_k(d)$ divides $d$ and so is odd. Since $P$ is a 2-group, the projection of $\alpha(P)$ onto $\{ \phi_u \}_{u \in U_k(d)} \simeq U_k(d)$ must then be trivial. This gives (a).

The order of $\langle \theta \rangle$ divides $e$ by (4.1) and so is also odd. This means that $\{ \phi_u \}_{u \in U(e)}$ contains a Sylow 2-subgroup of $\text{Aut}(M)$. But $\{ \phi_u \}_{u \in U(e)} \simeq U(e)$ is abelian, whence $\alpha(P)$ is abelian. This proves (b), and (c) follows as well by Lemma 4.3.

Let $t_1, t_2 \in P$ be such that $\alpha_{t_1}(x) = \alpha_{t_2}(x)$. By (a), we may write
\[ \alpha_{t_1} = \theta^{c_1} \phi_{u_1} \text{ and } \alpha_{t_2} = \theta^{c_2} \phi_{u_2}, \]
where $c_1, c_2 \in \mathbb{Z}, u_1, u_2 \in U(e)$.

That $\alpha_{t_1}(x) = \alpha_{t_2}(x)$ means $x^{u_1} = x^{u_2}$ and hence $\phi_{u_1} = \phi_{u_2}$. By (c), we know that $\alpha_{t_1}, \alpha_{t_2}$ have order dividing 2 and they commute. It follows that
\[ \alpha_{t_1} \cdot \alpha_{t_2}^{-1} = \theta^{c_1} \phi_{u_1} \cdot \phi_{u_2}^{-1} \theta^{-c_2} = \theta^{c_1 - c_2} \]
also has order dividing 2. But $\theta$ has odd order, so we have $\theta^{c_1} = \theta^{c_2}$. Thus, indeed $\alpha_{t_1} = \alpha_{t_2}$, and this proves (d).

Before proceeding, let us make two observations. First, recall that $P' = \langle \tau^2 \rangle$ by Lemma 4.3 and that $\ker(\alpha)$ contains $P'$ by Lemma 4.6(b). It follows that $\ker(\alpha)$ is equal to one of the following:

(4.3)
\[ \langle \tau^2 \rangle, \langle \tau^2, s \rangle, \langle \tau^2, rs \rangle, \langle \tau \rangle, \langle r, s \rangle. \]

For these five possibilities, the order of $\alpha(P)$ is respectively given by
\[ 4, 2, 2, 2, 1. \]

Second, notice that $M$, whose order is assumed to be odd, is a characteristic subgroup of $N$. Then $\langle x \rangle$, being characteristic in $M$ because $\gcd(e, d) = 1$, is also a characteristic and in particular normal subgroup of $N$.

**Lemma 4.7.** Elements in $N$ of order a power of 2 all lie in $\langle x \rangle \rtimes_\alpha P$.

**Proof.** Let $x^iy^jt \in N$ be of order $2^\ell$ with $t \in P$. By Lemma 4.6(a), we have
\[ \alpha_t(y) \equiv y \pmod{\langle x \rangle}, \]
so then $y$ and $t$ commute modulo $\langle x \rangle$. It follows that
\[ y^{2^\ell}t^{2^\ell} \equiv (y^t)^{2^\ell} \equiv (x^iy^t)^{2^\ell} \equiv 1 \pmod{\langle x \rangle}. \]
Proposition 4.8. Let \( \kappa \in \text{Aut}(P) \) be in the image of \((4.4)\).

(a) We always have \( \kappa(r) \equiv r \pmod{\ker(\alpha)} \) and \( \kappa(s) \equiv s \pmod{\ker(\alpha)} \).

(b) Assume that \( P = D_{2m} \) with \( m \geq 3 \) or \( P = Q_{2m} \) with \( m \geq 4 \). If \( \alpha_r \neq \text{Id}_M \), then we have \( \kappa(r) \equiv r \pmod{P'} \) and \( \kappa(s) \equiv s \pmod{P'} \),

Proof of (a). By Lemma 4.6(d), it suffices to show that
\[
\alpha_{\kappa(r)}(x) = \alpha_r(x) \quad \text{and} \quad \alpha_{\kappa(s)}(x) = \alpha_s(x).
\]
Let \( \xi \in \text{Aut}(N) \) be such that its image under \((4.4)\) is \( \kappa \). Since \( \xi(P) \) lies in \( \langle x \rangle \rtimes_\alpha P \) by Lemma 4.7, we may write
\[
\xi(r) = x^{i_1}\kappa(r) \quad \text{and} \quad \xi(s) = x^{i_2}\kappa(s).
\]
Since \( \langle x \rangle \) is characteristic in both \( M \) and \( N \), we also have
\[
\alpha_t(x) \in \langle x \rangle \quad \text{for all} \quad t \in P \quad \text{and} \quad \xi(x) = x^u \quad \text{for some} \quad u \in U(e).
\]
Now, applying \( \xi \) to the relation \( rxr^{-1} = \alpha_r(x) \) yields
\[
x^{i_1}\kappa(r) \cdot x^u \cdot \kappa(r)^{-1}x^{-i_1} = \alpha_r(x)^u \quad \text{and so} \quad \alpha_{\kappa(r)}(x^u) = \alpha_r(x^u).
\]
Similarly, applying \( \xi \) to the relation \( sxs^{-1} = \alpha_s(x) \) yields
\[
x^{i_2}\kappa(s) \cdot x^u \cdot \kappa(s)^{-1}x^{-i_2} = \alpha_s(x)^u \quad \text{and so} \quad \alpha_{\kappa(s)}(x^u) = \alpha_s(x^u).
\]
Since \( \gcd(u, e) = 1 \), it follows that \((4.5)\) indeed holds, as desired.

Proof of (b). Since \( P = D_{2m} \) with \( m \geq 3 \) or \( P = Q_{2m} \) with \( m \geq 4 \), we know from Proposition 4.4(c) that there exist \( a, b \in \mathbb{Z} \) with \( a \) odd such that
\[
\kappa(r) = r^a \quad \text{and} \quad \kappa(s) = r^bs.
\]
We then have \( \kappa(r)r^{-1} \in P' \) because \( a - 1 \) is even. We also have \( \kappa(s)s^{-1} \in \ker(\alpha) \) by (a). Since \( \alpha_r \neq \text{Id}_M \), the last two possibilities in \((4.3)\) are ruled out. Thus, for \( \kappa(s)s^{-1} \) to lie in \( \ker(\alpha) \), necessarily \( b \) is even, which means that \( \kappa(s)s^{-1} \in P' \) as well. This completes the proof.

To prove sufficiency in Theorem 1.5, we first show that \( \alpha \) may be modified to satisfy certain nice conditions.

Proposition 4.9. The following hold.

(a) Assume that \( P = D_4 \) or \( P = Q_8 \), and \( \alpha(P) \) has order 1 or 2. Then there exists \( \beta \in \text{Hom}(P, \text{Aut}(M)) \) with \( \beta_r = \text{Id}_M \) such that \( N \simeq M \rtimes_\beta P \).

(b) There always exists \( \beta \in \text{Hom}(P, \text{Aut}(M)) \) with \( \beta_s \in \{ \phi_u \}_{u \in U(e)} \) such that \( \alpha_t, \beta_t \) are conjugates in \( \text{Aut}(M) \) for all \( t \in P \) and \( N \simeq M \rtimes_\beta P \).
Proof of (a). Since $\alpha(P)$ has order 1 or 2, from \([4.3]\) we see that
\[
\alpha_{e} = \text{Id}_{M} \text{ for at least one } e \in \{r, s, rs\}.
\]
Since $P = D_{4}$ or $P = Q_{8}$, by Proposition \([4.4(a), (b)]\), there exists $\kappa \in \text{Aut}(P)$ such that $\kappa(r) = e$. Let us take
\[
\beta \in \text{Hom}(P, \text{Aut}(M)); \quad \beta(t) = \alpha(\kappa(t)).
\]
Then clearly $\beta_{r} = \alpha_{e} = \text{Id}_{M}$. To show that $N \simeq M \rtimes_{\beta} P$, define
\[
\begin{cases}
\xi(\eta) = \eta & \text{for } \eta \in M, \\
\xi(t) = \kappa^{-1}(t) & \text{for } t \in P,
\end{cases}
\]
where the inputs are regarded as elements of $M \rtimes_{\alpha} P$ and the outputs as elements of $M \rtimes_{\beta} P$. The relation $t\eta t^{-1} = \alpha_{t}(\eta)$ in $N$ is preserved under $\xi$ because
\[
\xi(t)\xi(\eta)\xi(t)^{-1} = \kappa^{-1}(t)\eta\kappa^{-1}(t)^{-1} = \beta_{\kappa^{-1}(t)}(\eta) = \alpha_{t}(\eta) = \xi(\alpha_{t}(\eta)).
\]
It follows that $\xi$ extends to a homomorphism from $N = M \rtimes_{\alpha} P$ to $M \rtimes_{\beta} P$, which is easily seen to be an isomorphism.

Proof of (b). We saw in the proof of Lemma \([4.6(b)]\) that $\{\phi_{u}\}_{u \in U(e)}$ has to contain a Sylow 2-subgroup of $\text{Aut}(M)$. Since $\alpha_{s}$ has order dividing 4, it follows that there exists $\pi \in \text{Aut}(M)$ such that $\pi \alpha_{s} \pi^{-1} \in \{\phi_{u}\}_{u \in U(e)}$. Let us take
\[
\beta \in \text{Hom}(P, \text{Aut}(M)); \quad \beta(t) = \pi \alpha(t) \pi^{-1}.
\]
Then clearly $\beta_{s} = \pi \alpha_{s} \pi^{-1} \in \{\phi_{u}\}_{u \in U(e)}$. To show that $N \simeq M \rtimes_{\beta} P$, define
\[
\begin{cases}
\xi(\eta) = \pi(\eta) & \text{for } \eta \in M, \\
\xi(t) = t & \text{for } t \in P,
\end{cases}
\]
where the inputs are regarded as elements of $M \rtimes_{\alpha} P$ and the outputs as elements of $M \rtimes_{\beta} P$. The relation $t\eta t^{-1} = \alpha_{t}(\eta)$ in $N$ is preserved under $\xi$ because
\[
\xi(t)\xi(\eta)\xi(t)^{-1} = t\pi(\eta)t^{-1} = \beta_{t}(\pi(\eta)) = \pi(\alpha_{t}(\eta)) = \xi(\alpha_{t}(\eta)).
\]
It follows that $\xi$ extends to a homomorphism from $N = M \rtimes_{\alpha} P$ to $M \rtimes_{\beta} P$, which is easily seen to be an isomorphism.$\square$

**Proposition 4.10.** Assume that $\alpha_{r} = \text{Id}_{M}$ and $\alpha_{s} \in \{\phi_{u}\}_{u \in U(e)}$. Then
\[
\xi(\eta) = (\alpha_{s} \phi_{k}^{-1})(\eta) \text{ for } \eta \in M, \quad \xi(r) = r^{-1}, \quad \xi(s) = rs
\]
extend to an automorphism on $N$ of order dividing $2d$, and
\[
(4.6) \quad N = \{\eta_{0}\xi(\eta_{0})\cdots\xi^{\ell-1}(\eta_{0}) : \ell \in \mathbb{N}\} \text{ with } \eta_{0}\xi(\eta_{0})\cdots\xi^{n-1}(\eta_{0}) = 1
\]
for the element $\eta_{0} = e y r s$ and for $n = 2^{m}ed$.

**Proof.** First, a straightforward calculation (c.f. Proposition \([4.4(c)]\)) shows that the relations in $P$ are preserved under $\xi$. Put $\pi = \alpha_{s} \phi_{k}^{-1}$. That $\alpha_{r} = \text{Id}_{M}$ implies the relation $r\eta r^{-1} = \alpha_{r}(\eta) = \eta$ is preserved under $\xi$ because
\[
\xi(r)\xi(\eta)\xi(r)^{-1} = r^{-1}\pi(\eta)r = \alpha_{r}(\pi(\eta)) = \pi(\eta) = \xi(\eta).
\]
Similarly, that $\alpha_{s} \in \{\phi_{u}\}_{u \in U(e)}$ implies $\alpha_{s}$ and $\pi$ commute, so then $s\eta s^{-1} = \alpha_{s}(\eta)$ is also preserved under $\xi$ because
\[
\xi(s)\xi(\eta)\xi(s)^{-1} = rs\pi(\eta)\pi^{-1} = (\alpha_{r} \alpha_{s} \pi)(\eta) = (\pi \alpha_{s})(\eta) = \xi(\alpha_{s}(\eta))
\]
We deduce that $\xi$ extends to an endomorphism on $N$, which clearly has to be an automorphism. That $\alpha_s \in \{\phi_u\}_{u \in U(e)}$ implies $\alpha_s$ and $\phi_k^{-1}$ commute, so

$$\pi^{2d} = (\alpha_s \phi_k^{-1})^{2d} = \alpha_s^{2d} \phi_k^{-1} = \text{Id}_M.$$  

Here $\alpha_s^2 = \text{Id}_M$ by Lemma 4.6(c) and $k^d \equiv 1 \pmod{e}$ because $\text{ord}_c(k)$ divides $d$. Since $\xi^2$ is clearly the identity on $P$, indeed $\xi$ has order dividing $2d$.

Next, we shall use induction on $\ell \in \mathbb{N}$ to show that

$$(4.7) \quad (xyrs)\xi(xyrs) \cdots \xi^{\ell-1}(xyrs) = \begin{cases} x^\ell y^r t^{\ell+1} s^\ell & \text{for } \ell \text{ odd,} \\ x^\ell y^r t^\ell s^\ell & \text{for } \ell \text{ even.} \end{cases}$$

The case $\ell = 1$ is clear. For $\ell$ odd, observe that

$$\xi^\ell(xyrs) = \pi^\ell(xy) \cdot r^{-1} \cdot rs = (\alpha_s^\ell \phi_k^{-1})(xy)s = (\alpha_s \phi_k^{-1})(xy)s.$$  

Assuming that (4.7) holds for $\ell$, we compute that

$$(xyrs)\xi(syrs) \cdots \xi^{\ell}(xyrs) = x^\ell y^r t^{\ell+1} s^\ell \cdot (\alpha_s \phi_k^{-1})(xy)s = x^\ell y^r \cdot (\alpha_s^\ell \phi_k^{-1})(xy) \cdot r^{\ell+1} s^\ell \cdot rs.$$  

$$= x^\ell y^r \cdot x^{k-\ell} y \cdot r^{\ell+1} s^{\ell+1} \quad (\text{since } \alpha_s, \alpha_s^2 = \text{Id}_M)$$

$$= x^{\ell+1} y^r t^{\ell+1} r^{\ell+1} s^{\ell+1}$$

and so (4.7) also holds for $\ell + 1$. Similarly, for $\ell$ even, observe that

$$\xi^\ell(xyrs) = \pi^\ell(xy) \cdot r \cdot rs = (\alpha_s^\ell \phi_k^{-1})(xy)rs = \phi_k^{-1}(xy)rs.$$  

Assuming that (4.7) holds for $\ell$, we compute that

$$(xyrs)\xi(xyrs) \cdots \xi^{\ell}(xyrs) = x^\ell y^r t^\ell s^\ell \cdot \phi_k^{-1}(xy)rs = x^\ell y^r \cdot (\alpha_s^\ell \phi_k^{-1})(xy) \cdot t^\ell s^\ell \cdot rs$$

$$= x^\ell y^r \cdot x^{k-\ell} y \cdot r^{\ell+1} s^{\ell+1} \quad (\text{since } \alpha_s, \alpha_s^2 = \text{Id}_M)$$

$$= x^{\ell+1} y^r t^\ell r^{\ell+1} s^{\ell+1}.$$  

and so (4.7) also holds for $\ell + 1$. Hence, by induction, indeed we have (4.7) for all $\ell \in \mathbb{N}$, and this immediately implies the second equality in (4.6).

To show the first equality in (4.6), since $N$ has order $n = 2^{m+1}d$, it suffices to show that the set in (4.6) has at least $n$ elements. So suppose that

$$(4.8) \quad (xyrs)\xi(xyrs) \cdots \xi^{\ell-1}(xyrs) = (xyrs)\xi(xyrs) \cdots \xi^{\ell-1}(xyrs).$$

By (4.7), this implies that $s^{\ell_1} \equiv s^{\ell_2}$ (mod $\langle r \rangle$) in the group $P$. But then $\ell_1, \ell_2$ have the same parity because $\langle s \rangle \cap \langle r \rangle = \langle s^2 \rangle$. Again by (4.7), we have

$$\begin{cases} x^{\ell_1} y^r t^{\ell_1+1} s^{\ell_1} = x^{\ell_2} y^r t^{\ell_2+1} s^{\ell_2} & \text{for } \ell_1, \ell_2 \text{ odd,} \\ x^{\ell_1} y^r t^{\ell_1} s^{\ell_1} = x^{\ell_2} y^r t^{\ell_2} s^{\ell_2} & \text{for } \ell_1, \ell_2 \text{ even.} \end{cases}$$

Since $N = M \rtimes \alpha_1 P$ and $M = \langle x \rangle \rtimes \langle y \rangle$, in both cases, we deduce that $x^{\ell_1} = x^{\ell_2}$ and $y^{\ell_1} = y^{\ell_2}$, which respectively imply that

$$\ell_1 \equiv \ell_2 \pmod{e}$$

and $\ell_1 \equiv \ell_2 \pmod{d}$.

In both cases, we also have $r^{\frac{\ell_1-\ell_2}{2}} = s^{\ell_2-\ell_1}$. Let us now prove that $s^{\ell_2-\ell_1} = 1$ so in particular $r^{\frac{\ell_1-\ell_2}{2}} = 1$. Note that $\ell_2 - \ell_1$ is always even.
• For \( P = D_{2^m} \) with \( m \geq 2 \), since \( s \) has order 2, clearly \( s_\ell^2 = 1 \).

• For \( P = Q_{2^m} \) with \( m \geq 3 \), since \( s \) has order 4, clearly \( s_\ell^2 = 1 \) unless \( \ell_2 - \ell_1 \equiv 2 \pmod{4} \). So suppose that \( \ell_2 - \ell_1 \equiv 2 \pmod{4} \). Then

\[
r = \frac{\ell_1 - \ell_2}{2} = s_\ell^2 - \ell_1 - 2, s^2 = r^{2m-2} \quad \text{and so} \quad \frac{\ell_1 - \ell_2}{2} \equiv 2^{m-2} \pmod{2^{m-1}}.
\]

But \( m - 1 \geq 2 \), so we obtain \( \ell_1 - \ell_2 \equiv 0 \pmod{4} \), which is a contradiction.

This means that \( \ell_2 - \ell_1 \equiv 2 \pmod{4} \) does not occur.

We have thus shown that \( r^{\ell_1 - \ell_2} = 1 \), which implies

\[
\frac{\ell_1 - \ell_2}{2} \equiv 0 \pmod{2^{m-1}} \quad \text{and thus} \quad \ell_1 \equiv \ell_2 \pmod{2^m}.
\]

Since \( 2^m, c, d \) are pairwise coprime, it now follows that \( \ell_1 \equiv \ell_2 \pmod{n} \). Therefore, indeed the set in (4.6) contains at least \( n \) distinct elements. \( \square \)

5. PROOF OF THEOREM 1.5

Let \( N \) be a non-\( C \)-group of order \( n \). By Theorem 3.1 we may assume that

\[
N = M \rtimes \alpha P \quad \text{with} \quad \alpha \in \Hom(P, \Aut(M)),
\]

where \( M \) is a \( C \)-group of odd order, and \( P \) is either \( D_{2^m} \) with \( m \geq 2 \) or \( Q_{2^m} \) with \( m \geq 3 \). We wish to show that \((C_n, N)\) is realizable if and only if

\[
\left\{
\begin{array}{ll}
\alpha(P) \text{ has order 1 or 2} & \text{ when } P = D_4 \text{ or } P = Q_8, \\
\alpha(r) = \Id_M & \text{ otherwise.}
\end{array}
\right.
\]

(5.1)

The main ingredients are Propositions 4.8, 4.9 and 4.10.

First, suppose that \((C_n, N)\) is realizable. By Proposition 2.1 this implies that there exist \( f \in \Hom(C_n, \Aut(N)) \) and a bijective \( g \in Z_1^1(C_n, N) \). Let us consider the characteristic subgroup \( M_0 = M \rtimes \alpha P' \) of \( N \). Put \( H = g^{-1}(M_0) \), which is a subgroup of \( C_n \) by Proposition 2.2. Trivially \( H \) lies in the center of \( C_n \), so by the proof of Proposition 2.2(b), we have a well-defined homomorphism

\[
\tilde{f}_{M_0} \in \Hom(C_n/H, \Aut(N/M_0)); \quad \tilde{f}_{M_0} = (\eta M_0 \mapsto f(\eta)(M_0)),
\]

and a well-defined bijective crossed homomorphism

\[
\bar{g}_{M_0} \in Z_2^1(C_n/H, N/M_0); \quad \bar{g}_{M_0} = (\sigma H \mapsto g(\sigma)M_0).
\]

Observe that \( \tilde{f}_{M_0} \) cannot be trivial, for otherwise \( \bar{g}_{M_0} \) would be an isomorphism by (2.1), which cannot happen because \( C_n/H \) is cyclic while \( N/M_0 \simeq P/P' \simeq D_4 \) by Lemma 4.3.

Now, assume for contradiction that (5.1) does not hold. Then \( \ker(\alpha) = P' \) when \( P = D_4 \) or \( P = Q_8 \) in view of (4.3), and \( \alpha(r) \neq \Id_M \) otherwise. From Proposition 4.8 it follows that the canonical homomorphism

\[
\Aut(N) \xrightarrow{\xi \mapsto \eta M_0 \mapsto \xi(\eta)M_0} \Aut(N/M_0) \xrightarrow{\text{identification}} \Aut(P/P'),
\]

is trivial. But then \( \tilde{f}_{M_0} \) would be trivial, which we know is impossible. This implies that (5.1) must hold, as desired.

Conversely, assume that (5.1) holds. Then, by Proposition 4.9 we may modify \( \alpha \) (without changing the isomorphism class of \( N \)) if necessary so that the hypothesis of Proposition 4.10 is satisfied. Thus, there exist \( \xi \in \Aut(N) \) and \( \eta_0 \in N \) such that

(i) \( \xi^n = \Id_N \) and \( \eta_0 \xi(\eta_0) \cdots \xi(\eta_0)^{n-1} = 1; \)
(ii) \( N = \{ \eta_0 \xi(\eta_0) \cdots \xi^{\ell-1}(\eta_0) : \ell \in \mathbb{N} \} \).
Consider \( \rho(\eta_0) \xi \), which is an element of \( \text{Hol}(N) \). For any \( \ell \in \mathbb{N} \), we have
\[
(\rho(\eta_0) \xi)^\ell = \rho(\eta_0 \xi(\eta_0) \cdots \xi^{\ell-1}(\eta_0)) : \ell.
\]
Then \( \rho(\eta_0) \xi \) has order dividing \( n \) by (i) and \( \langle \rho(\eta_0) \xi \rangle \) acts transitively on \( N \) by (ii).

It follows that \( \langle \rho(\eta_0) \xi \rangle \) is a regular subgroup of \( \text{Hol}(N) \) whose order is exactly \( n \).
This proves that \((C_n, N)\) is realizable.

**ACKNOWLEDGMENT**

The author thanks the referee for suggesting the discussion in Remark 1.7 and the proof in Remark 3.2.

**REFERENCES**


Department of Mathematics, Ochanomizu University, 2-1-1 Otsuka, Bunkyo-ku, Tokyo, Japan
Email address: tsang.sin.yi@ocha.ac.jp
URL: http://sites.google.com/site/cindysinyitsang/