THE MULTIPLE HOLOMORPHS OF
FINITE $p$-GROUPS OF CLASS TWO

A. CARANTI

Abstract. Let $G$ be a group, and $S(G)$ be the group of permutations on the set $G$. Define the holomorph of $G$ to be the normalizer of the image in $S(G)$ of the right regular representation,

$$\text{Hol}(G) = N_{S(G)}(\rho(G)) = \text{Aut}(G)\rho(G).$$

If $N$ is any regular subgroup of $S(G)$, then $N_{S(G)}(N)$ is isomorphic to the holomorph of $N$.

G.A. Miller has shown that the group $T(G) = N_{S(G)}(\text{Hol}(G))/\text{Hol}(G)$ acts regularly on the set of the regular subgroups $N$ of $S(G)$ which are isomorphic to $G$, and have the same holomorph as $G$, in the sense that $N_{S(G)}(N) = \text{Hol}(G)$.

If $G$ is non-abelian, inversion on $G$ yields an involution in $T(G)$. Other regular subgroups $N$ of $S(G)$ yield (other) involutions in $T(G)$. In the cases studied in the literature, $T(G)$ turns out to be a finite 2-group, which is often elementary abelian.

In this paper we exhibit an example of a finite $p$-group $G(p)$ of class 2, for $p > 2$ a prime, such that $T(G(p))$ is non-abelian, and not a 2-group. Moreover, $T(G(p))$ is not generated by involutions when $p > 3$.

More generally, we develop some aspects of a theory of $T(G)$ for $G$ a finite $p$-group of class 2, for $p > 2$; in particular, we show that for such a group $G$ there is an element of order $p - 1$ in $T(G)$.

Introduction

Let $G$ be a group, and $S(G)$ be the group of permutations on the set $G$. The image $\rho(G)$ of the right regular representation of $G$ is a regular subgroup of $S(G)$, and its normalizer is the semidirect product of $\rho(G)$ by the automorphism group $\text{Aut}(G)$ of $G$,

$$N_{S(G)}(\rho(G)) = \text{Aut}(G)\rho(G).$$

We will refer to this group as the holomorph $\text{Hol}(G)$ of $G$.

Date: 31 January 2018, 12:38 CET — Version 2.32.
2010 Mathematics Subject Classification. 20B35 20D15 20D45.
Key words and phrases. Holomorph, multiple holomorph, regular subgroups, finite $p$-groups, automorphisms.

The author is a member of INdAM—GNSAGA. The author gratefully acknowledges support from the Department of Mathematics of the University of Trento and from MIUR—Italy via PRIN 2015TW9LSR_005.
More generally, if \( N \) is a regular subgroup of \( S(G) \), then \( N_{S(G)}(N) \) is isomorphic to the holomorph of \( N \). Let us thus consider the set
\[
\mathcal{H}(G) = \{ N \leq S(G) : N \text{ is regular, } N \cong G \text{ and } N_{S(G)}(N) = \text{Hol}(G) \}.
\]
of the regular subgroups of \( S(G) \) which are isomorphic to \( G \), and have in some sense the same holomorph as \( G \).

G.A. Miller has shown \[Mil08\] that the so-called multiple holomorph of \( G \)
\[
\text{NHol}(G) = N_{S(G)}(\text{Hol}(G)) = N_{S(G)}(N_{S(G)}(\rho(G)))
\]
acts transitively on \( \mathcal{H}(G) \), and thus the group
\[
T(G) = \text{NHol}(G)/\text{Hol}(G)
\]
acts regularly on \( \mathcal{H}(G) \).

Let \( G \) be a non-abelian group. Then the inversion map \( \text{inv} : g \mapsto g^{-1} \) on \( G \), which conjugates \( \rho(G) \) to the image \( \lambda(G) \) of the left regular representation \( \lambda \), induces an involution in \( T(G) \). One expects \( T(G) \) to contain further involutions. In fact, if \( N \leq S(G) \) is a regular subgroup, so that \( N_{S(G)}(N) \) is isomorphic to \( \text{Hol}(N) \), the inversion map on \( N \) yields an involution in \( T(N) \). This corresponds to an involution in \( T(G) \) under the standard isomorphism \( S(G) \to S(N) \) induced by the bijection \( G \to N \) that maps \( g \in G \) to the element of \( N \) that maps 1 to \( g \). Of course different \( N \) need not induce different involutions in \( T(G) \).

Recently T. Kohl has described \[Koh15\] the set \( \mathcal{H}(G) \) and the group \( T(G) \) for \( G \) dihedral or generalized quaternion. In \[CDV17b\], we have redone, via a commutative ring connection, the work of Mills \[Mil51\], which determined \( \mathcal{H}(G) \) and \( T(G) \) for \( G \) a finitely generated abelian group. In \[CDV17a\] we have studied the case of finite perfect groups.

In all these cases, \( T(G) \) turns out to be an elementary abelian 2-group. T. Kohl mentions in \[Koh15\] an example where \( T(G) \) is a non-abelian 2-group, and in a personal communication has asked whether \( T(G) \) is always a 2-group when \( G \) is finite.

The first goal of this paper is to show that for \( p > 2 \) a prime, the group
\[
\mathcal{G}(p) = \langle x, y : x^{p^2}, y^{p^2}, [x, y] = x^p \rangle
\]
of order \( p^4 \) has \( T(\mathcal{G}(p)) \) of order \( p(p − 1) \), and it is isomorphic to \( \text{AGL}(1, p) \), that is, to the holomorph of a group of order \( p \). This we prove in Section 4. Thus \( T(\mathcal{G}(p)) \) is not a 2-group, and for \( p > 3 \) it is not even generated by involutions, as the subgroup generated by the involutions has index \( (p − 1)/2 \) in \( T(\mathcal{G}(p)) \).

The group \( \mathcal{G}(p) \) is of (nilpotence) class two. In Section 2 we introduce a linear setting that simplifies the calculations in the later sections (Proposition 2.2), and develop some more general aspects of a theory of \( T(G) \) for finite \( p \)-groups \( G \) of class two, for \( p > 2 \). We then show in Section 3 that for such a group there is an element of order \( p − 1 \) in \( T(G) \) (Proposition 3.1). In Section 5 we provide examples where
\(|T(G)|\) is as small as possible, that is, it has size \(p - 1\) (Proposition 5.1) and others (Proposition 5.4) where \(T(G)\) contains a large elementary abelian \(p\)-subgroup.

Section II collects some preliminary facts.

We note that regular subgroups of \(S(G)\) correspond to right skew braces structures on \(G\) (see [GV17]). Also, this work is related to the enumeration of Hopf-Galois structures on separable field extensions, as C. Greither and B. Pareigis have shown [GP87] that these structures can be described through those regular subgroups of a suitable symmetric group, that are normalized by a given regular subgroup; this connection is exploited in the work of L. Childs [Chi89], N.P. Byott [Byo96], and Byott and Childs [BC12].

The system for computational discrete algebra GAP [GAP18] has been invaluable for gaining the computational evidence which led to the results of this paper.

1. Preliminaries

We recall some standard material from [CDV17a], and complement it with a couple of Lemmas that will be useful in the rest of the paper.

Let \(G\) be a group. Denote by \(S(G)\) the group of permutations of the set \(G\). Let

\[
\rho : G \rightarrow S(G) \quad g \mapsto (h \mapsto hg)
\]

be the right regular representation of \(G\)

**Definition 1.1.** The **holomorph** of \(G\) is

\[\text{Hol}(G) = N_{S(G)}(\rho(G)) = \text{Aut}(G)\rho(G)\].

**Theorem 1.2.** Let \(G\) be a finite group. The following data are equivalent.

1. A regular subgroup \(N \leq \text{Hol}(G)\).
2. A map \(\gamma : G \rightarrow \text{Aut}(G)\) such that for \(g, h \in G\) and \(\beta \in \text{Aut}(G)\)

\[
\begin{cases}
\gamma(gh) = \gamma(h)\gamma(g), \\
\gamma(g^\beta) = \gamma(g)^\beta.
\end{cases}
\]

3. A group operation \(\circ\) on \(G\) such that for \(g, h, k \in G\)

\[
\begin{cases}
(gh) \circ k = (g \circ k)k^{-1}(h \circ k), \\
\text{Aut}(G) \leq \text{Aut}(G, \circ).
\end{cases}
\]

Under these assumptions

(i) \(g \circ h = g^{\gamma(h)}h\) for \(g, h \in G\).
(ii) For \(g, h \in G\) one has \(g^{\nu(h)} = g \circ h\).
(iii) The map

\[ \nu : (G, \circ) \to N \]
\[ h \mapsto \gamma(h) \rho(h) \]

is an isomorphism.

The equivalence of item (3) of Theorem 1.2 with the previous ones follows from the theory of braces [BCJ16].

In the following, when discussing a subgroup \( N \) as in (1) of Theorem 1.2, we will switch to the map \( \gamma \) of (2) and the operation \( \circ \) of (3) without further mention.

We introduce the sets

\[ \mathcal{H}(G) = \left\{ N \leq S(G) : N \text{ is regular, } N \cong G \text{ and } N_{S(G)}(N) = \text{Hol}(G) \right\} \]

and

\[ \mathcal{J}(G) = \left\{ N \leq S(G) : N \text{ is regular, } N \trianglelefteq \text{Hol}(G) \right\} \supseteq \mathcal{H}(G) \]

As in [CDV17b, CDV17a], for the groups \( G \) we consider we first determine \( \mathcal{J}(G) \), using Theorem 1.2, then check which elements of \( \mathcal{J}(G) \) lie in \( \mathcal{H}(G) \), and finally compute \( T(G) \), or part of it.

If \( N \in \mathcal{H}(G) \), G.A. Miller has shown [Mil08] that \( \rho(G) \) is conjugated to \( N \) under an element of the multiple holomorph

\[ \text{NHol}(G) = N_{S(G)}(\text{Hol}(G)) = N_{S(G)}(N_{S(G)}(\rho(G))) \]

of \( G \). Moreover the group

\[ T(G) = \text{NHol}(G)/\text{Hol}(G) \]

acts regularly on \( \mathcal{H}(G) \).

An element conjugating \( \rho(G) \) to \( N \) can be modified by a translation, and assumed to fix 1. We have

**Lemma 1.3.** Suppose \( N \in \mathcal{H}(G) \), and let \( \vartheta \in \text{NHol}(G) \) such that \( \rho(G)^\vartheta = N \) and \( 1^\vartheta = 1 \). Then

\[ \vartheta : G \to (G, \circ) \]

is an isomorphism such that

\[ (1.2) \quad \rho(g)^\vartheta = \nu(g^\vartheta) = \gamma(g^\vartheta) \rho(g^\vartheta), \]

for \( g \in G \).

Conversely, an isomorphism \( \vartheta : G \to (G, \circ) \) conjugates \( \rho(G) \) to \( N \).

The next Lemma shows that an isomorphism \( \vartheta \) as in Lemma 1.3 determines \( \gamma \) uniquely.

**Lemma 1.4.** Let \( N \in \mathcal{H}(G) \).

Given an isomorphism

\[ \vartheta : G \to (G, \circ), \]
then
\[(gh)^\vartheta = (g^\vartheta)^{\gamma(h^\vartheta)}h^\vartheta,\]
for \(g, h \in G\), It follows that the \(\gamma\) associated to \(N\) is given by
\[g^{\gamma(h)} = (g^{\alpha^{-1}h^{\alpha^{-1}}}h)^{\vartheta}h^{-1}.\]

**Proof.** The first formula comes from the definition of the operation \(\circ\) in Theorem 1.2(1.2), and the second one follows immediately from it. □

In the next lemma we note that \(\gamma\) is well defined for the elements of \(T(G)\).

**Lemma 1.5.** Let \(N \in \mathcal{H}(G)\), and let \(\vartheta : G \to (G, \circ)\) be an isomorphism.

If \(\alpha \in \text{Aut}(G)\), Then \(\alpha \vartheta\) represents the same element of \(T(G)\), and has the same associated \(\gamma\).

**Proof.** It suffices to prove the second statement, which follows from the fact that the \(\gamma\) associated to \(\alpha \vartheta\) is given, according to Lemma 1.4, by
\[(g^{(\vartheta)}h^{(\vartheta)})^{\alpha \vartheta}h^{-1} = (g^{\alpha^{-1}h^{\alpha^{-1}}}h^{\alpha^{-1}})^{\vartheta}h^{-1} = g^{\gamma(h)}.\]

□

For a group \(G\), denote by \(\iota\) the morphism
\[\iota : G \to \text{Aut}(G)\]
\[g \mapsto (h \mapsto h^g = g^{-1}hg)\]
that maps \(g \in G\) to the inner automorphism \(\iota(g)\) it induces. The following Lemma is proved in [CDV17a].

**Lemma 1.6.** Let \(G\) be a group, and let \(N \trianglelefteq \text{Hol}(G)\) be a regular subgroup of \(S(G)\).

The following general formulas hold, for \(g, h \in G\) and \(\beta \in \text{Aut}(G)\).
\[
\begin{align*}
(1) & \quad \gamma([\beta, g^{-1}]) = [\gamma(g), \beta], \\
(2) & \quad \gamma([h, g^{-1}]) = \iota([\gamma(g), h]),
\end{align*}
\]

2. SOME BASIC TOOLS

If \(G\) is a group of nilpotence class two, we will use repeatedly the standard identity
\[(gh)^n = g^n h^n [h, g]^{n \choose 2},\]
valid for \(g, h \in G\) and \(n \in \mathbb{N}\).

We write \(\text{Aut}_c(G)\) for the group of central automorphisms of \(G\), that is
\[\text{Aut}_c(G) = \{\alpha \in \text{Aut}(G) : [G, \alpha] \subseteq Z(G)\}.\]
Lemma 2.1. Let $G$ be a finite $p$-group of class two, and $N \trianglelefteq \text{Hol}(G)$ a regular subgroup.

The following are equivalent.

(1) $G' \leq \ker(\gamma)$, that is, $\gamma(G') = 1$,
(2) $\gamma(G)$ is abelian,
(3) $[\gamma(G), G] \leq Z(G)$, that is, $\gamma(G) \leq \text{Aut}_c(G)$,
(4) $[\gamma(G), G] \leq \ker(\gamma)$.

Moreover, these conditions imply $[G', \gamma(G)] = 1$.

Proof. (1) and (2) are clearly equivalent.

Lemma 1.6(2) yields that $\gamma(G') = 1$ iff $[G, \gamma(G)] \leq Z(G)$, that is, (1) is equivalent to (3).

Setting $\beta = \gamma(h)$ in 1.6(1), for $h \in G$ we get
$$\gamma([\gamma(h), g^{-1}]) = [\gamma(g), \gamma(h)],$$
which shows that (2) and (4) are equivalent.

As to the last statement, it is a well known and elementary fact that central automorphisms centralize the derived subgroup. \hfill \Box

We now introduce a linear technique that will simplify the calculations in the next sections. Here and in the following, we will occasionally employ additive notation for the abelian groups $G/Z(G), G/G'$ and $Z(G)$.

Proposition 2.2. Let $G$ be a finite $p$-group of class two, for $p > 2$.

The following sets of data are equivalent.

(1) A regular subgroup $N \trianglelefteq \text{Hol}(G)$ such that

(a) $\gamma(G) \leq \text{Aut}_c(G)$, and

(b) $[Z(G), \gamma(G)] = 1$.

(2) A bilinear map $\Delta : G/Z(G) \times G/G' \rightarrow Z(G)$ such that

$$\Delta(g^\beta, h^\beta) = \Delta(g, h)^\beta$$

for $g \in G/Z(G)$, $h \in G/G'$ and $\beta \in \text{Aut}(G)$.

The connection between the two sets of data is given by

$$\Delta(gZ(G), hG') = [g, \gamma(h)],$$

for $g, h \in G$.

Proof. Let us start with the setting of (1). By assumption (1a) we have $[G, \gamma(G)] \leq Z(G)$.

If $z \in Z(G)$ we have
$$[gz, \gamma(h)] = [g, \gamma(h)]^z[z, \gamma(h)] = [g, \gamma(h)],$$
as by assumption (1b) $[Z(G), \gamma(G)] = 1$. If $w \in G'$ we have
$$[g, \gamma(hw)] = [g, \gamma(w)\gamma(h)] = [g, \gamma(h)],$$
as assumption (1a) implies $G' \leq \ker(\gamma)$ by Lemma 2.1. Therefore the map

$$\Delta : G/Z(G) \times G/G' \to Z(G)$$

induced by $(g, h) \mapsto [g, \gamma(h)]$ is well defined.

We now prove that $\Delta$ is bilinear. For $g, h \in G/Z(G)$, and $k \in G/G'$ we have

$$\Delta(g + h, k) = [g + h, \gamma(k)]$$

$$= [g, \gamma(k)]h + [h, \gamma(k)]$$

$$= [g, \gamma(k)] + [h, \gamma(k)]$$

$$= \Delta(g, k) + \Delta(h, k),$$

since $[G, \gamma(G)] \in Z(G)$. For $g \in G/Z(G)$ and $h, k \in G/G'$ we have

$$\Delta(g, h + k) = [g, \gamma(h + k)]$$

$$= [g, \gamma(h) + \gamma(k)]$$

$$= [g, \gamma(h)] + [g, \gamma(k)] \gamma(h)$$

$$= [g, \gamma(h)] + [g, \gamma(k)]$$

$$= \Delta(g, h) + \Delta(g, k),$$

since $[g, \gamma(k)] \in Z(G)$, and $[Z(G), \gamma(G)] = 1$.

To prove (2.1) we compute, for $g \in G/Z(G)$, $h \in G/G'$ and $\beta \in \text{Aut}(G)$,

$$\Delta(g^\beta, h^\beta) = [g^\beta, \gamma(h^\beta)]$$

$$= [g^\beta, \gamma(h)]^\beta$$

$$= g^{-\beta}(g^\beta)^{\beta-1}\gamma(h)^\beta$$

$$= g^{-\beta}g^{\gamma(h)\beta}$$

$$= [g, \gamma(h)]^\beta$$

$$= \Delta(g, h)^\beta.$$

Conversely, given $\Delta$ as in (2), and defining $\gamma$ via (2.2), we have immediately $[G, \gamma(G)] \leq Z(G)$, and because $\Delta$ is a well-defined map, $[Z(G), \gamma(G)] = 1$. It is then easy to see, reversing the arguments above, that $\gamma$ satisfies the conditions of Theorem 1.2(2). \qed

Lemma 2.3. Let $G$ be a finite $p$-group of class two, and $N \leq \text{Hol}(G)$ a regular subgroup.

Suppose

(1) $\gamma(G) \leq \text{Aut}_e(G)$, and

(2) $[Z(G), \gamma(G)] = 1$. 

Lemma 2.3.
Then for \( g, h \in G \) we have

\[
\nu(g, h) = \nu([g, h][g, \gamma(h)][h, \gamma(g)]^{-1}) = \nu([g, h] + \Delta(g, h) - \Delta(h, g)).
\]

Proof. Note that \( \nu(g^{-1}) : k \mapsto k^{\gamma(g)^{-1}}g^{-\gamma(g)^{-1}}. \)

It suffices to compute, using the fact that \( \gamma(G) \) is abelian, according to Lemma 2.4

\[
1^{[\nu(g), \nu(h)]} = (((((g^{-1}\gamma(g)^{-1})\gamma(h)^{-1}(h^{-1}\gamma(h)^{-1})\gamma(g)\gamma(h))y
\]
\[
= (g^{-1}\gamma(g)\gamma(h)(h^{-1}\gamma(h)^{-1})\gamma(g)\gamma(h)g\gamma(h)h
\]
\[
= g^{-1}\gamma(h)^{-1}\gamma(g)g\gamma(h)h
\]
\[
= [g, h][h^{-1}, \gamma(g)][g, \gamma(h)]
\]
\[
= [g, h][g, \gamma(h)][h, \gamma(g)]^{-1},
\]
where we have used the facts that \( [G, \gamma(G)] \leq Z(G) \) and \( \gamma(G) \) is abelian.

Lemma 2.4. Let \( G \) be a finite \( p \)-group of class two, and \( N \leq \text{Hol}(G) \) a regular subgroup.

Suppose

1. \( \gamma(G) \leq \text{Aut}_e(G) \), and
2. \( [Z(G), \gamma(G)] = 1 \).

Then for \( g \in G \) we have

\[
\nu(g^n) = \nu((g^n)^{\gamma(g^{(n-1)/2})}) = g^n \cdot \Delta(g, g)^{(n/2)}. \]

In particular, under the hypotheses of the Lemma the elements of \( G \) retain their orders under \( \nu \).

Proof. This follows from

\[
1^{[\nu(g)^n]} = g^{\gamma(g)^{(n-1)/2}}g^{\gamma(g)^{(n-2)/2}} \cdots g^{\gamma(g)}g
\]
\[
= g^n[g, \gamma(g)]^{n-1}[g, \gamma(g)]^{n-2} \cdots [g, \gamma(g)]
\]
\[
= g^n[g, \gamma(g)]^{(n/2)} = g^n \cdot \Delta(g, g)^{(n/2)}
\]
\[
= g^n[\gamma(g)^{(n-1)/2}]
\]
\[
= (g^n)^{\gamma(g)^{(n-1)/2}},
\]
where we have used the facts that \( [G, \gamma(G)] \leq Z(G) \) and \( [Z(G), \gamma(G)] = 1 \).

3. Power Isomorphisms

Let \( G \) be a finite \( p \)-group of class two, for \( p > 2 \).

For integers \( d \) coprime to \( p \), consider the bijection \( \vartheta_d \in S(G) \) given by the \( d \)-th power map, \( \vartheta_d : x \mapsto x^d \) on \( G \), and write \( d' \) for the inverse of \( d \) modulo \( \exp(G) \).
For \( g, h \in G \) we have
\[
h^{\rho(g)\vartheta_d} = (h^{d^1})^{\rho(g)\vartheta_d} = (h^{d^2} g)^d = h g^d (g^{(1-d)/2})^d = h^{(g^{(1-d)/2})\rho(g^d)},
\]
so that
\[
(3.1) \quad \rho(g)^{\vartheta_d} = \iota(g^{(1-d)/2})\rho(g^d) \in \text{Aut}(G)\rho(G) = \text{Hol}(G).
\]
Since we have also
\[
[\text{Aut}(G), \vartheta_d] = 1,
\]
it follows that \( \vartheta_d \in \text{NHol}(G) = N_{S(G)}(\text{Hol}(G)) \), and thus \( \vartheta_d \) induces an element of \( T(G) \). To determine the \( \gamma_d \) associated to \( \vartheta_d \), one can apply \((1.2)\) to \((3.1)\) to get \( \gamma_d(g^{\vartheta_d}) = \gamma_d(g^d) = \iota(g^{(1-d)/2}) \), and then, taking \( d' \)-th powers,
\[
\gamma_d(g) = \iota(g^{(d'-1)/2}).
\]
(We could have also used Lemma \( \text{[1.4]} \) to obtain the same result.)

The \( \vartheta_d \) and \( \gamma_d \) are all distinct as \( d \) ranges in the integers coprime to \( p \) between 1 and \( \exp(G/Z(G)) - 1 \). Clearly \( \vartheta_{d_1}\vartheta_{d_2} = \vartheta_{d_1d_2} \), so that the \( \vartheta_d \) yield a subgroup of \( T(G) \) isomorphic to the units of the integers modulo \( \exp(G/Z(G)) \). We have obtained

**Proposition 3.1.** Let \( G \) be a finite \( p \)-group of class two, for \( p > 2 \).

Let \( p^r = \exp(G/Z(G)) \).

Then \( T(G) \) contains a cyclic subgroup of order \( \varphi(p^r) = (p-1)p^r - 1 \).

In particular, \( T(G) \) contains an element of order \( p - 1 \).

**4. Computing \( T(G(p)) \)**

Let \( p > 2 \) be a prime, and define
\[
G(p) = \left< x, y : x^p, y^p, [x, y] = x^p \right>.
\]
This is a group of order \( p^4 \) and nilpotence class two, such that \( G(p)' = \langle x^p \rangle \) has order \( p \), and \( G(p)^p = \text{Frat}(G(p)) = Z(G(p)) = \langle x^p, y^p \rangle \) has order \( p^2 \).

It is a well-known fact and an easy exercise that \( \text{Aut}(G(p)) \) induces on the \( \mathbb{F}_p \)-vector space \( V = G(p)/\text{Frat}(G(p)) \) the group of matrices
\[
\left\{ \begin{bmatrix} a & 0 \\ b & 1 \end{bmatrix} : a \in \mathbb{F}_p^*, b \in \mathbb{F}_p \right\}
\]
with respect to the basis induced by \( x, y \). (Our automorphisms operate on the right, therefore our vectors are row vectors.) The same group is induced on the vector space \( W = G(p)^p = Z(G(p)) = \text{Frat}(G(p)) \), with respect to the basis given by \( x^p, y^p \).

We first note that Lemma \( \text{[1.6]} \) implies

**Lemma 4.1.** Let \( \alpha \in Z(\text{Aut}(G)) \).

Then
\[
[G, \alpha] = \left\{ g^{-1}g^\alpha : g \in G \right\} \leq \ker(\gamma).
\]
In the group $G(p)$, the power map $\alpha : x \mapsto x^{1+p}$ is an automorphism lying in the centre of $\text{Aut}(G(p))$. Hence

**Lemma 4.2.** Let $N \in K(G(p))$. Then

$$G(p)' \leq Z(G(p)) = \text{Frat}(G(p)) = G(p)^p \leq \ker(\gamma).$$

It follows that $G(p)$ satisfies the equivalent conditions of Lemma 2.1. In particular, $\gamma(G(p)) \leq \text{Aut}_c(G(p))$. Moreover,

\begin{equation}
[Z(G(p)), \gamma(G(p))] = [G(p)^p, \gamma(G(p))] = [G(p), \gamma(G(p))]^p = 1,
\end{equation}

as $[G(p), \gamma(G(p))] \leq Z(G(p))$, and $Z(G(p))$ has exponent $p$.

We may thus appeal to the $\Delta$ setting of Proposition 2.2. Since $\gamma(\text{Frat}(G(p))) = 1$ by Lemma 4.2, $\Delta$ is well-defined as a map $V \times V \to W$.

For a $\Delta$ as in Proposition 2.2, and $\beta \in \text{Aut}(G)$ which induces

\begin{equation}
\begin{bmatrix}
a & 0 \\
b & 1
\end{bmatrix},
\end{equation}

on $V$, we have

$$\Delta(x, x)^\beta = \Delta(x^\beta, x^\beta) = \Delta(ax, ax) = a^2 \Delta(x, x).$$

If $p > 3$, and we choose $a \neq 1, -1$, we obtain that if $\Delta(x, x) \neq 0$, then $\Delta(x, x) \in W$ is an eigenvector for $\beta$ with respect to the eigenvalue $a^2 \neq a, 1$. It follows that $\Delta(x, x) = 0$.

If $p = 3$, we first choose $a = -1$ and $b = 0$ to obtain that $\Delta(x, x) \in \langle y^p \rangle$. We then choose $a = -1$ and $b = 1$ to obtain that $\Delta(x, x) \in \langle x^3y^p \rangle$, so that $\Delta(x, x) = 0$ in this case too. (We could have used this argument also for $p > 3$.)

We have also

$$\Delta(x, y)^\beta = \Delta(x^\beta, y^\beta) = \Delta(ax, bx + y) = a \Delta(x, y).$$

Taking $b = 0$ and $a \neq 1$ in $\beta$, we see that $\Delta(x, y) = sx^p$ for some $s$.

Similarly, $\Delta(y, x) = tx^p$ for some $t$. We have also

$$\Delta(y, y)^\beta = \Delta(y^\beta, y^\beta) = \Delta(bx + y, bx + y) = b(s + t)x^p + \Delta(y, y).$$

If $\Delta(y, y) = uy^p + vx^p$, we have

$$uy^p + (ub + va)x^p = \Delta(y, y)^\beta = (b(s + t) + v)x^p + uy^p.$$ 

Setting $a = 1$ we get $u = s + t$, and then setting $a = -1$ we get $v = 0$.

Therefore the $\gamma$ for $G(p)$ are given by

\begin{equation}
\gamma_{s, t}(x) : \begin{cases} 
x \mapsto x \\
y \mapsto x^{ps}y
\end{cases} \quad \gamma_{s, t}(y) : \begin{cases} 
x \mapsto x^{1+pt} \\
y \mapsto y^{1+p(s+t)}
\end{cases}
\end{equation}

for $s, t \in \mathbb{F}_p$. 
Lemma 2.3 yields that for the regular subgroup $N \triangleleft \text{Hol}(G)$ corresponding to $\gamma_{s,t}$ one has

$$
\left[ \nu(x), \nu(y^d) \right] = \nu([x, y] [x, \gamma_{s,t}(y)] [y, \gamma_{s,t}(x)]^{-1}) = \nu(x^p x^{pt} x^{-ps}) = \nu([x, y]^{d(1+t-s)}) = \nu(x^{pd(1+t-s)}).
$$

Therefore for $t - s + 1 = 0$ we have $G(p) \not\cong (G(p), \circ)$, as the latter is abelian, and the corresponding regular subgroup $N$ lies in $\mathcal{J}(G) \setminus \mathcal{H}(G)$.

So let $t - s + 1 \neq 0$, and choose $d = (1 + t - s)'$, so that $[\nu(x), \nu(y^d)] = \nu(x^p)$. Since by Lemma 2.3 $\nu(x^p) = \nu(x)^p$, and $\langle \nu(x), \nu(y^d) \rangle$ have each order $p^2$, and intersect trivially, we have that $G \cong (G, \circ)$, via the isomorphism defined by

\begin{equation}
(4.4) \\
\vartheta_{d,s} : \begin{cases} 
  x \mapsto x \\
  y \mapsto y^d 
\end{cases}
\end{equation}

and by the accompanying $\gamma_{s,t}$ as above, for $t = d' + s - 1$.

\begin{remark}
One might wonder where the power isomorphisms $\vartheta_d$ of Section 3 have gone in (4.4). They can be recovered using Lemma 1.5, with $\alpha$ defined on $V$ by (1.2), for $a = d$ and $b = 0$, and $\vartheta = \vartheta_{d,(1-d')/2}$.
\end{remark}

We now determine the structure of the group $T(G)$. Note first that we may take $d \in F_p^*$ in (4.4). To see this, apply Lemma 1.5 with $\alpha$ chosen to be the central automorphism defined by

$$
\alpha : \begin{cases} 
  x \mapsto x \\
  y \mapsto y^{1+pd'u} 
\end{cases}
$$

for some $u$. We obtain that

$$
\alpha \vartheta_{d,s} : \begin{cases} 
  x \mapsto x \\
  y \mapsto y^{d+pu} 
\end{cases}
$$

yields the same element of $T(G(p))$ with respect to the same $\gamma$.

We now want to show

\begin{theorem}
(4.4)
$$
\vartheta_{d,s} \vartheta_{e,u} \equiv \vartheta_{de,se'+u}.
\end{theorem}

Therefore

$$
T(G) = \left\{ \vartheta_{d,s} : d \in F_p^*, s \in F_p \right\},
$$

a group of order $p(p-1)$, is isomorphic to $\text{AGL}(1, p)$, that is, to the holomorph a group of order $p$. 

Proof. Note first that it follows from Lemma 2.4 and $x^\vartheta_{d,s} = x$ and $x^{\gamma_{s,t}(x)} = x$ that
\begin{equation}
(x^i)^{\vartheta_{d,s}} = x^i
\end{equation}
for all $i$.

Similarly, note first that combining Theorem 1.2(iii) and Lemma 1.3 we obtain that for all $i$
\[\nu((y^i)^{\vartheta_{d,s}}) = \nu((y^i)^i),\]
so that Lemma 2.4 yields
\begin{equation}
(y^i)^{\vartheta_{d,s}} = y^{(d)i(1+pd(i-1)/2(s+t))}
\end{equation}
Now consider another $\vartheta_{e,u}$, and let $v = e' + u - 1$. From (4.6) we obtain
\[y^{\vartheta_{d,s} \vartheta_{e,u}} = y^{de \varphi(x(p^4) \varphi(u+v)).}\]
Using Lemma 1.5 again, if we choose $\alpha$ to be the inner automorphism $\iota((x d-1/2(u+v)):
\begin{align*}
x & \mapsto x \\
y & \mapsto y x^{-\varphi(x(p^4) \varphi(u+v))}
\end{align*}
we obtain $\alpha^{\vartheta_{d,s} \vartheta_{e,u}} = \vartheta_{de,w}$ for some $w$, so that we can take $f = de$. Set $z = f' + w - 1$.
To determine $w$, we compute $(h g)^{\vartheta_{d,s} \vartheta_{e,u}}$ in two ways. We compute first
\begin{align*}
(y x)^{\vartheta_{d,s} \vartheta_{e,u}} &= (y^{\vartheta_{d,s} \vartheta_{e,u}})^{\gamma_{w,z}(x)} x^{\vartheta_{d,s} \vartheta_{e,u}} \\
&= (h y^{d})^{\vartheta_{e,u}} x^{\gamma_{w,z}(x)} \\
&= (y^{de})^{\gamma_{w,z}(x)} x y^{p(4)} \varphi(u+v),
\end{align*}
where we have used (4.5), (4.6), and (4.1).

We then compute
\begin{align*}
(y x)^{\vartheta_{d,s} \vartheta_{e,u}} &= (y^{\vartheta_{d,s} \vartheta_{e,u}})^{\gamma_{w,z}(x)} x^{\vartheta_{d,s} \vartheta_{e,u}} \\
&= (y^{d} x^{\varphi(p(d))})^{\vartheta_{e,u}} \\
&= (y^{de})^{\gamma_{w,z}(x)} x y^{p(4)} \varphi(u+v) x^{1 + pd + pdeu},
\end{align*}
where we have used (4.1).

From (4.7) and (4.8) we obtain
\[y^{de} \gamma_{w,z}(x) = y^{de} x^{p(ds + deu)}.\]
Taking \((d'c')\)-th powers we get

\[y^{\gamma_{w,z}(g)} = y_{x'}^{p(s'e' + u)}\]

so that

\[\vartheta_{d,s} \vartheta_{e,u} \equiv \vartheta_{de,se'} + u\]

as claimed.

5. More Examples

In this section we exhibit two examples \(G\) of \(p\)-groups of class two, for \(p > 2\). In the first example \(T(G)\) is as small as possible according to Proposition 3.1, that is, of order \(p - 1\). In the second example \(T(G)\) contains a large elementary abelian \(p\)-subgroup.

5.1. A small \(T(G)\). We claim the following

**Proposition 5.1.** Let \(G\) be the free \(p\)-group of class two and exponent \(p > 2\) on \(n \geq 2\) generators.

Then \(T(G)\) is (cyclic) of order \(p - 1\).

Since \(G\) is free in a variety, and \(\text{Frat}(G) = Z(G)\), we have that \(\text{Aut}(G)/\text{Aut}_c(G) \cong \text{GL}(n, p)\). The conditions in (1.1) imply that \(\gamma(G)\) is a \(p\)-group, which is normal in \(\text{Aut}(G)\). Therefore \(\gamma(G) \leq \text{Aut}_c(G)\).

Moreover Lemma 2.1 implies

\[[Z(G), \gamma(G)] = [G', \gamma(G)] = 1.\]

We can thus use the the \(\Delta\) setting of Proposition 2.2. Here \(V = G/G' = G/Z(G)\) and \(W = G'\) are \(F_p^\ast\)-vector space, and \(W\) is naturally isomorphic to the exterior square \(\wedge^2 V\) of \(V\).

5.1.1. The case \(p > 3\). Take first \(0 \neq g \in V\), and complete it to a basis of \(V\).

When \(p > 3\), we can choose \(a \in F_p^\ast \setminus \{1, -1\}\). Consider the automorphism \(\beta\) of \(V\) (and thus of \(G\)), that fixes \(g\), and multiplies all other basis elements by \(a\). Then \(\beta\) fixes \(\Delta(g, g)\), but there are no fixed points of \(\beta\) in \(W \cong \wedge^2 V\), as \(\beta\) multiplies all natural basis elements of \(\wedge^2 V\) by \(a \neq 1\) or \(a^2 \neq 1\). Thus \(\Delta(g, g) = 0\).

Take now two independent elements \(g\) and \(h\) of \(V\), and complete them to a basis of \(V\). Consider the automorphism \(\beta\) of \(V\) which fixes \(g, h\), and multiplies all other basis elements by \(a \in F_p^\ast \setminus \{1, -1\}\). Then the only fixed points of \(\beta\) in \(W\) are the multiples of \([g, h]\), so that \(\Delta(g, h) = \lambda[g, h]\) for some \(\lambda\). Consider another basis elements \(k \notin \langle g, h \rangle\), so that \(\Delta(g, k) = \mu[g, k]\), and \(\Delta(g, h + k) = \lambda[g, h] + \mu[g, k]\). Since \(\Delta(g, h + k)\) must also be a multiple of \([g, h + k]\), we see that \(\lambda = \mu\) uniformly, so that, reverting to multiplicative notation,

\[g^{\gamma(h)} = g\Delta(g, h) = g[g, h]^\lambda = g^{h^\lambda}.\]

that is, \(\gamma(h) = \iota(h^\lambda)\). For \(\lambda \neq -1/2\), this is uniquely associated, as we have seen in Section 3 to \(g^{\beta d} = g^d\), where \(d = (1 + 2\lambda)'\).
Remark 5.2. There is no such \( \vartheta_d \) when \( \lambda = -1/2 \). In fact in this case Lemma 2.3 shows that

\[
[\nu(g), \nu(h)] = \nu([g, h] + \Delta(g, h) - \Delta(h, g))
= \nu([g, h] - \frac{1}{2} [g, h] + \frac{1}{2} [h, g])
= \nu(0) = 1,
\]

that is, \( N \cong (G, \circ) \) is abelian, and thus \( N \) is not isomorphic to \( G \).

Note that this is a particular case of the Baer correspondence [Bae38], which is in turn an approximation of the Lazard correspondence and the Baker-Campbel-Hausdorff formulas [Khu98, Ch. 9 and 10].

5.1.2. The case \( p = 3 \). The method described in the following works for a general \( p > 2 \), although it is slightly more cumbersome than the previous one.

Let \( 0 \neq g \in V = G/G' = G/Z(G) \), and let \( C \) be a complement to \( \langle g \rangle \) in \( G \). Consider the automorphism \( \beta \) of \( V \) which fixes \( g \), and acts as scalar multiplication by \( -1 \) on \( C \). Then \( \Delta(g, g) \in \wedge^2 C \). Letting \( C \) range over all complements of \( \langle g \rangle \), we obtain that \( \Delta(g, g) = 0 \).

Similarly, given two independent elements \( g, h \) of \( V \), let \( C \) be a complement to \( \langle g, h \rangle \) in \( V \). Define the automorphism \( \beta \) of \( V \) which fixes \( g, h \), and acts as scalar multiplication by \( -1 \) on \( C \). Then

\[
\Delta(g, h) \in \langle g \wedge h \rangle + \wedge^2 C.
\]

Letting \( C \) range over all complements of \( \langle g, h \rangle \), we obtain that \( \Delta(g, h) \in \langle g \wedge h \rangle \).

5.2. A biggish \( T(G) \). For the second class of examples, we will use the \( p \)-groups of [Car16].

Theorem 5.3 [Car16]. Let \( p > 2 \) be a prime, and \( n \geq 4 \).

Consider the presentation

\[
G = \langle x_1, \ldots, x_n : [[x_i, x_j], x_k] = 1 \text{ for all } i, j, k, \]
\[
x^p_i = \prod_{j < k} [x_j, x_k]^{a_{i,j,k}} \text{ for all } i, \rangle,
\]

where \( a_{i,j,k} \in \mathbb{F}_p \).

There is a choice of the \( a_{i,j,k} \in \mathbb{F}_p \) such that the following hold.

- \( G \) has nilpotence class two,
- \( G \) has order \( p^{n+\binom{n}{2}} \),
- \( G/\text{Frat}(G) \) has order \( p^n \),
- \( G' = \text{Frat}(G) = Z(G) \) has order \( p^{\binom{n}{2}} \) and exponent \( p \),
- \( \text{Aut}(G) = \text{Aut}_c(G) \), that is, all of the automorphism of \( G \) are central.

We claim the following
Proposition 5.4. Let $G$ be one of the groups of Theorem [5.3].
Then $T(G)$ contains a non-abelian subgroup of order
$$(p - 1) \cdot p^{(n^2)/2},$$
which is the extension of an $F_p$-vector space of dimension $\binom{n}{2} \binom{n+1}{2}$ by the multiplicative group $F_p^*$ acting naturally.

Here again $V = G/G' = G/Z(G)$ and $W = G'$ can be regarded as $F_p$-vector spaces, and $W$ is naturally isomorphic to $\wedge^2 V$. The conditions of Proposition [2.2] apply, so we can use the $\Delta$ setting. Because of Theorem [5.3], condition (2.1) of Proposition [2.2] holds trivially, so that we are simply looking at all bilinear maps $\Delta : V \times V \rightarrow W$ here.

Consider all such $\Delta$ which are symmetric with respect to the basis of $V$ induced by the $x_i$. Under the pointwise operation of $W$, these $\Delta$ form a vector space $\mathfrak{D}$ of dimension $\binom{n}{2} \binom{n+1}{2}$ over $F_p$. For the regular subgroup $N \trianglelefteq \text{Hol}(G)$ of $S(G)$ corresponding to such a $\Delta$, Lemma [2.3] yields, for $1 \leq i < j \leq n$,

$$\nu(x_i, x_j) = \nu([x_i, x_j] + \Delta(x_i, x_j) - \Delta(x_j, x_i)) = \nu([x_i, x_j])$$

and Lemma [2.4] yields, for $1 \leq i \leq n$,

$$\nu(x_i)^p = \nu(x_i^p \cdot \Delta(x_i, x_i) (\xi^p)) = \nu(x_i^p),$$

since $\Delta(x_i, x_i) \in Z(G)$, and the latter group has exponent $p$. Thus in the corresponding group $(G, \circ) \cong N$ commutators and $p$-th powers of generators are preserved, so that in view of (5.1) for each $\Delta \in \mathfrak{D}$ there is an isomorphism $\vartheta_{\Delta} : G \rightarrow (G, \circ)$ such that $x_i \mapsto x_i$ for each $i$. Since the composition of $\vartheta_{\Delta}$ followed by $\nu$ is an isomorphism $G \rightarrow N$, we obtain from (5.2)

$$\nu([x_i, x_j]^{\vartheta_{\Delta}}) = [\nu(x_i^{\vartheta_{\Delta}}), \nu(x_j^{\vartheta_{\Delta}})] = [\nu(x_i), \nu(x_j)] = \nu([x_i, x_j]),$$

that is, $\vartheta_{\Delta}$ fixes the elements of $G'$.

If $\Delta_1, \Delta_2 \in \mathfrak{D}$, then for $1 \leq i, j \leq n$ we have, since the $\Delta$ take values in $G'$,

$$(x_i x_j)^{\vartheta_{\Delta_1} \vartheta_{\Delta_2}} = (x_i x_j \Delta_1(x_i, x_j))^{\vartheta_{\Delta_2}} = x_i x_j \Delta_2(x_i, x_j) \Delta_1(x_i, x_j),$$

where we have applied Lemma [1.4][1.3], using the facts that $\vartheta_{\Delta}$ fixes the elements of $G' = Z(G)$, and $\gamma(G') = 1$.

Therefore $\{ \vartheta_{\Delta} : \Delta \in \mathfrak{D} \} \cong \mathfrak{D}$ is an elementary abelian group of order $p^{\binom{n}{2} \binom{n+1}{2}}$. Considering also the $\vartheta_d$ of Section [4], we readily obtain Proposition [5.4].
References

[Bae38] Reinhold Baer, Groups with abelian central quotient group, Trans. Amer. Math. Soc. 44 (1938), no. 3, 357–386. MR 1501972

[BC12] Nigel P. Byott and Lindsay N. Childs, Fixed-point free pairs of homomorphisms and nonabelian Hopf-Galois structures, New York J. Math. 18 (2012), 707–731. MR 2991421

[BCJ16] David Bachiller, Ferran Cedó, and Eric Jespers, Solutions of the Yang-Baxter equation associated with a left brace, J. Algebra 463 (2016), 80–102. MR 3527540

[Byo96] N. P. Byott, Uniqueness of Hopf Galois structure for separable field extensions, Comm. Algebra 24 (1996), no. 10, 3217–3228. MR 1402555

[Car16] A. Caranti, A simple construction for a class of $p$-groups with all of their automorphisms central, Rend. Semin. Mat. Univ. Padova 135 (2016), 251–258. MR 3506071

[CDV17a] A. Caranti and F. Dalla Volta, Groups that have the same holomorph as a finite perfect group, 2017, arXiv:1612.03573 [math.GR].

[CDV17b] A. Caranti and F. Dalla Volta, The multiple holomorph of a finitely generated abelian group, J. Algebra 481 (2017), 327–347. MR 3639478

[Chi89] Lindsay N. Childs, On the Hopf Galois theory for separable field extensions, Comm. Algebra 17 (1989), no. 4, 809–825. MR 990979

[GAP18] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.8.10, 2018.

[GP87] Cornelius Greither and Bodo Pareigis, Hopf Galois theory for separable field extensions, J. Algebra 106 (1987), no. 1, 239–258. MR 878476

[GV17] L. Guarnieri and L. Vendramin, Skew braces and the Yang-Baxter equation, Math. Comp. 86 (2017), no. 307, 2519–2534. MR 3647970

[Khu98] E. I. Khukhro, $p$-Automorphisms of Finite $p$-Groups, London Mathematical Society Lecture Note Series, vol. 246, Cambridge University Press, Cambridge, 1998. MR 1615819

[Koh15] Timothy Kohl, Multiple holomorphs of dihedral and quaternionic groups, Comm. Algebra 43 (2015), no. 10, 4290–4304. MR 3366576

[Mil08] G. A. Miller, On the multiple holomorphs of a group, Math. Ann. 66 (1908), no. 1, 133–142. MR 1511494

[Mil51] W. H. Mills, Multiple holomorphs of finitely generated abelian groups, Trans. Amer. Math. Soc. 71 (1951), 379–392. MR 0045117 (13,530a)

(A. Caranti) Dipartimento di Matematica, Università degli Studi di Trento, via Sommarive 14, I-38123 Trento, Italy
E-mail address: andrea.caranti@unitn.it
URL: http://www.science.unitn.it/~caranti/