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. The (abstract) holomorph of G is the natural semidirect product $\mathrm{Aut}(G)G$. We will write $\mathrm{Hol}(G)$ for the normalizer of the image in $S(G)$ of the right regular representation of G,

$$\mathrm{Hol}(G) = N_{S(G)}(\rho(G)) = \mathrm{Aut}(G)\rho(G) \cong \mathrm{Aut}(G)G,$$

and also refer to it as the holomorph of G. More generally, 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

$$T(G) = N_{S(G)}(\mathrm{Hol}(G))/\,\mathrm{Hol}(G)$$

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 $N_{S(G)}(N) = \mathrm{Hol}(G)$.

If G is non-abelian, inversion on G yields an involution in $T(G)$. Other non-abelian regular subgroups N of $S(G)$ having the same holomorph as 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 $\mathcal{G}(p)$ of class 2, for $p > 2$ a prime, which is the smallest p-group such that $T(\mathcal{G}(p))$ is non-abelian, and not a 2-group. Moreover, $T(\mathcal{G}(p))$ 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 $T(G)$, and exhibit examples where $|T(G)| = p - 1$, and others where $T(G)$ contains a large elementary abelian p-subgroup.

Date: 12 September 2018, 9:56 CEST — Version 5.06.

2010 *Mathematics Subject Classification.* 20B35 20D15 20D45.

Key words and phrases. Holomorph, multiple holomorph, regular subgroups, finite p-groups, automorphisms.

To appear in J. Algebra **516** (2018), 352–372.

10.1016/j.jalgebra.2018.09.031

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.

Introduction

Let G be a group, and $S(G)$ be the group of permutations on the set G, under left-to-right composition. 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 $\operatorname{Aut}(G)$ of G,

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

We will refer to this group, which is isomorphic to the *abstract holomorph* $\operatorname{Aut}(G)G$ of G, as the *holomorph* $\operatorname{Hol}(G)$ of G.

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

$$\mathcal{H}(G) = \left\{ N \le S(G) : N \text{ is regular, } N \cong G \text{ and } N_{S(G)}(N) = \operatorname{Hol}(G) \right\}.$$

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

$$\operatorname{NHol}(G) = N_{S(G)}(\operatorname{Hol}(G)) = N_{S(G)}(N_{S(G)}(\rho(G)))$$

acts transitively on $\mathcal{H}(G)$, and thus the group

$$T(G) = \operatorname{NHol}(G)/\operatorname{Hol}(G)$$

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

Let G be a non-abelian group. The inversion map $\operatorname{inv} : g \mapsto g^{-1}$ on G, which conjugates $\rho(G)$ to the image $\lambda(G)$ of the left regular representation λ, induces an involution in $T(G)$. More generally, let N be a non-abelian, regular subgroup of G that has the same holomorph as G (that is, such that $N_{S(G)}(N) = \operatorname{Hol}(G) = N_{S(G)}(\rho(G))$), and consider the group $S(N)$. As above, the inversion map inv_N on N yields an involution in $T(N)$. The bijection $N \to G$ that maps $n \in N$ to $1^n \in G$ yields an isomorphism $S(N) \to S(G)$ that maps $\rho(N)$ to N. Under this isomorphism, inv_N maps onto an involution in $T(G)$. So each such N yields an involution in $T(G)$, although 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 [CDV17], 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 [CDV18] 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] two examples where $T(G)$ is a non-abelian 2-group; it can be verified with GAP [GAP18] that for the finite 2-groups G of order up to 8 the $T(G)$ are elementary abelian 2-groups, and that there are exactly two groups G of order 16 such that $T(G)$ is non-abelian: for the first one $T(G)$ is isomorphic to the dihedral group D of order 8, while for the second one $T(G)$ is isomorphic to the direct product of D by a group of order 2. In a personal communication, Kohl has asked whether $T(G)$ is always a 2-group when G is finite.

In this paper we study the groups $T(G)$, for G a finite p-group of nilpotence class 2, where p is an odd prime.

In Section 3 we show that for such a G, the group $T(G)$ contains an element of order $p-1$ (Proposition 3.1). In Section 5 we show that this minimum order is attained by the two non-abelian groups of order p^3, and by the finite p-groups that are free in the variety of groups of class 2 and exponent p (Proposition 5.1 and Theorem 5.2).

In Section 4 we show that the group

$$\mathcal{G}(p) = \left\langle\, x, y : x^{p^2}, y^{p^2}, [x, y] = x^p \,\right\rangle,$$

of order p^4 and class 2, has $T(\mathcal{G}(p))$ of order $p(p-1)$, isomorphic to $\mathrm{AGL}(1, p)$, that is, to the holomorph of a group of order p. Thus $T(\mathcal{G}(p))$ is non-abelian, it 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 $T(\mathcal{G}(p))$.

Note that when G is an abelian p-group, with p odd, $T(G) = \{1\}$ [CDV17, Theorem 3.1 and Lemma 3.2]. Therefore for $p > 3$ the non-abelian groups of order p^3 are the smallest examples of finite p-groups such that $T(G)$ is not a 2-group, and $\mathcal{G}(p)$ is the smallest example of a finite p-group G, for $p > 2$, such that $T(G)$ is non-abelian, and not a 2-group.

In Section 5, besides the examples already mentioned above, we exhibit a class of finite p-groups G of class 2 (Theorem 5.5) for which $T(G)$ is non-abelian, and contains a large elementary abelian p-subgroup.

Section 1 collects some preliminary facts. In Section 2 we introduce a linear setting (Proposition 2.2) that simplifies the calculations in the later sections, and develop some more general aspects of a theory of $T(G)$ for finite p-groups G of class 2, for $p > 2$.

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 normalised 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.

We are very grateful to the referee for several useful suggestions.

1. Preliminaries

We recall some standard material from [CDV18], 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, under left-to-right composition.

Let
$$\begin{aligned} \rho : G &\to S(G) \\ g &\mapsto (h \mapsto hg) \end{aligned}$$
be the right regular representation of G

Definition 1.1. The *holomorph* of G is
$$\operatorname{Hol}(G) = N_{S(G)}(\rho(G)) = \operatorname{Aut}(G)\rho(G).$$

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

(1) A regular subgroup $N \trianglelefteq \operatorname{Hol}(G)$.

(2) A map $\gamma : G \to \operatorname{Aut}(G)$ such that for $g, h \in G$ and $\beta \in \operatorname{Aut}(G)$
$$\begin{cases} \gamma(gh) = \gamma(h)\gamma(g), \\ \gamma(g^\beta) = \gamma(g)^\beta. \end{cases} \tag{1.1}$$

(3) A group operation $\circ$ on G such that for $g, h, k \in G$
$$\begin{cases} (gh) \circ k = (g \circ k)k^{-1}(h \circ k), \\ \operatorname{Aut}(G) \le \operatorname{Aut}(G, \circ). \end{cases}$$

The data of (1)-(3) *are related as follows.*

(i) $g \circ h = g^{\gamma(h)}h$ for $g, h \in G$.

(ii) Each element of N can be written uniquely in the form $\nu(h) = \gamma(h)\rho(h)$, for some $h \in G$.

(iii) For $g, h \in G$ one has $g^{\nu(h)} = g \circ h$.

(iv) The map
$$\begin{aligned} \nu : (G, \circ) &\to N \\ h &\mapsto \gamma(h)\rho(h) \end{aligned}$$
is an isomorphism.

This is basically [CDV18, Theorem 5.2]; we recall briefly the main points.

Recall that a subgroup $N \le S(G)$ is *regular* if for each $h \in G$ there is a unique $\nu(h) \in N$ such that $1^{\nu(h)} = h$. (So $\nu : G \to N$ is the inverse of the bijection $N \to G$ given by $n \mapsto 1^n$, for $n \in N$.) Given a regular subgroup $N \trianglelefteq \operatorname{Hol}(G) = \operatorname{Aut}(G)\rho(G)$, there is a map $\gamma : G \to \operatorname{Aut}(G)$ such that $\nu(h) = \gamma(h)\rho(h)$, as $1^{\gamma(h)} = 1$. The equivalence of item (3) of Theorem 1.2 with the previous ones follows from the theory of skew braces [BCJ16].

Remark 1.3. *In the following, when discussing a subgroup N as in* (1) *of Theorem 1.2, we will use the other notation of the Theorem without further mention.*

We introduce the sets

$$\mathcal{H}(G) = \left\{N \le S(G) : N \text{ is regular, } N \cong G \text{ and } N_{S(G)}(N) = \operatorname{Hol}(G)\right\}$$

and

$$\mathcal{J}(G) = \{N \le S(G) : N \text{ is regular, } N \trianglelefteq \operatorname{Hol}(G)\} \supseteq \mathcal{H}(G)$$

As in [CDV17, CDV18], 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.

G.A. Miller has shown [Mil08] that $\mathcal{H}(G)$ is the orbit of $\rho(G)$ under conjugation by the *multiple holomorph*

$$\operatorname{NHol}(G) = N_{S(G)}(\operatorname{Hol}(G)) = N_{S(G)}(N_{S(G)}(\rho(G)))$$

of G, so that the group

$$T(G) = \operatorname{NHol}(G)/\operatorname{Hol}(G) = N_{S(G)}(N_{S(G)}(\rho(G)))/N_{S(G)}(\rho(G))$$

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

An element of $S(G)$ conjugating $\rho(G)$ to N can be modified by a translation, and assumed to fix 1. We have, using the notation $a^b = b^{-1}ab$ for conjugacy in a group, the following

Lemma 1.4. *Suppose $N \in \mathcal{H}(G)$, and let $\vartheta \in \operatorname{NHol}(G)$ such that $\rho(G)^\vartheta = N$ and $1^\vartheta = 1$. Then*

$$\vartheta : G \to (G, \circ)$$

is an isomorphism such that

$$\rho(g)^\vartheta = \nu(g^\vartheta) = \gamma(g^\vartheta)\rho(g^\vartheta), \tag{1.2}$$

for $g \in G$.

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

This is [CDV18, Lemma 4.2].

The next Lemma shows that an isomorphism ϑ as in Lemma 1.4 determines γ uniquely.

Lemma 1.5. *Let $N \in \mathcal{H}(G)$. If*

$$\vartheta : G \to (G, \circ),$$

is an isomorphism, then

$$(gh)^\vartheta = (g^\vartheta)^{\gamma(h^\vartheta)} h^\vartheta, \tag{1.3}$$

for $g, h \in G$. It follows that the γ associated to N is given by

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

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 γ is well defined for the elements of $T(G)$.

Lemma 1.6. *Let $N \in \mathcal{H}(G)$, and let $\vartheta : G \to (G, \circ)$ be an isomorphism.*

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

Proof. It suffices to prove the second statement, which follows from the fact that the γ associated to $\alpha\vartheta$ is given, according to Lemma 1.5, by

$$\begin{aligned}(g^{(\alpha\vartheta)^{-1}} h^{(\alpha\vartheta)^{-1}})^{\alpha\vartheta} h^{-1} &= (g^{\vartheta^{-1}\alpha^{-1}} h^{\vartheta^{-1}\alpha^{-1}})^{\alpha\vartheta} h^{-1} \\ &= (g^{\vartheta^{-1}} h^{\vartheta^{-1}})^{\vartheta} h^{-1} \\ &= g^{\gamma(h)}.\end{aligned}$$

□

For a group G, denote by ι the morphism

$$\begin{aligned}\iota : G &\to \operatorname{Aut}(G) \\ g &\mapsto (h \mapsto h^g = g^{-1}hg)\end{aligned}$$

that maps $g \in G$ to the inner automorphism $\iota(g)$ it induces. The following Lemma is proved in [CDV18, Section 6].

Lemma 1.7. *Let G be a group, and let $N \trianglelefteq \operatorname{Hol}(G)$ be a regular subgroup of $S(G)$.*

The following general formulas hold in $\operatorname{Aut}(G)G$, for $g, h \in G$ and $\beta \in \operatorname{Aut}(G)$.

(1) $\gamma([\beta, g^{-1}]) = [\gamma(g), \beta]$,
(2) $\gamma([h, g^{-1}]) = \iota([\gamma(g), h])$,

Note that (2) is an instance of (1), for $\beta = \iota(h)$.

2. Some basic tools

If G is a group of nilpotence class two, we will use repeatedly the standard identity

$$(gh)^n = g^n h^n [h, g]^{\binom{n}{2}},$$

valid for $g, h \in G$ and $n \in \mathbb{N}$ [Rob96, 5.3.5].

We write $\operatorname{Aut}_c(G)$ for the group of central automorphisms of G, that is

$$\operatorname{Aut}_c(G) = \{\alpha \in \operatorname{Aut}(G) : [G, \alpha] \subseteq Z(G)\},$$

where the commutator is taken in $\operatorname{Aut}(G)G$.

Lemma 2.1. *Let G be a finite p-group of class two, and $N \trianglelefteq \operatorname{Hol}(G)$ a regular subgroup.*

The following are equivalent.

(1) $G' \le \ker(\gamma)$, *that is,* $\gamma(G') = 1$,

(2) $\gamma(G)$ *is abelian,*
(3) $[\gamma(G), G] \le Z(G)$*, that is,* $\gamma(G) \le \mathrm{Aut}_c(G)$*,*
(4) $[\gamma(G), G] \le \ker(\gamma)$.

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

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

Lemma 1.7(2) yields that $\gamma(G') = 1$ iff $[G, \gamma(G)] \le Z(G)$, that is, (1) is equivalent to (3).

Setting $\beta = \gamma(h)$ in 1.7(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 centralise the derived subgroup. □

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* $p > 2$.

There is a one-to-one correspondence between

(1) the regular subgroups $N \trianglelefteq \mathrm{Hol}(G)$ *such that*
  (a) $\gamma(G) \le \mathrm{Aut}_c(G)$*, and*
  (b) $[Z(G), \gamma(G)] = 1$,

  and

(2) the bilinear maps

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

such that

$$\Delta(g^\beta, h^\beta) = \Delta(g, h)^\beta \tag{2.1}$$

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

The correspondence is given by

$$\Delta(gZ(G), hG') = [g, \gamma(h)], \tag{2.2}$$

for $g, h \in G$.

Remark 2.3. *Clearly the commutator maps*

$$(gZ(G), hG') \mapsto [g, h]^c,$$

for some fixed integer c, satisfy the conditions of (2)*. See Section 3 for a discussion of the corresponding regular subgroups.*

Proof of Proposition 2.2. Let us start with the setting of (1). By assumption (1a), and Lemma 2.1, we have $[G, \gamma(G)] \le Z(G)$.

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

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

of (2.2), induced by $(g, h) \mapsto [g, \gamma(h)]$, is well defined.

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

$$\begin{aligned}\Delta(g + h, k) &= [g + h, \gamma(k)]\\ &= [g, \gamma(k)]^h + [h, \gamma(k)]\\ &= [g, \gamma(k)] + [h, \gamma(k)]\\ &= \Delta(g, k) + \Delta(h, k),\end{aligned}$$

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

$$\begin{aligned}\Delta(g, h + k) &= [g, \gamma(h + k)]\\ &= [g, \gamma(k) + \gamma(h)]\\ &= [g, \gamma(h)] + [g, \gamma(k)]^{\gamma(h)}\\ &= [g, \gamma(h)] + [g, \gamma(k)]\\ &= \Delta(g, h) + \Delta(g, k),\end{aligned}$$

since $[G, \gamma(G)] \leq Z(G)$, and $[Z(G), \gamma(G)] = 1$.

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

$$\begin{aligned}\Delta(g^\beta, h^\beta) &= [g^\beta, \gamma(h^\beta)]\\ &= [g^\beta, \gamma(h)^\beta]\\ &= g^{-\beta}(g^\beta)^{\beta^{-1}\gamma(h)\beta}\\ &= g^{-\beta}g^{\gamma(h)\beta}\\ &= [g, \gamma(h)]^\beta\\ &= \Delta(g, h)^\beta.\end{aligned}$$

Conversely, let Δ be as in (2), and define a function γ on G via (2.2), that is

$$g^{\gamma(h)} = g \cdot \Delta(gZ(G), hG').$$

The fact that Δ is linear in the first component, and takes values in the centre, implies that $\gamma(h) \in \mathrm{Aut}(G)$ for every $h \in G$. The fact that Δ is linear in the second component implies that $\gamma : G \to \mathrm{Aut}(G)$ is a morphism. It now follows immediately from (2.2) that $[G, \gamma(G)] \leq Z(G)$, so that by Lemma 2.1 γ satisfies (1a) and the first condition of (1.1). Also, $[Z(G), \gamma(G)] = 1$, so that γ satisfies (1b). Moreover, (2.1) implies that

$$g^{\gamma(h)^\beta} = g^{\beta^{-1}\gamma(h)\beta} = (g^{\beta^{-1}} \Delta(g^{\beta^{-1}} Z(G), hG'))^\beta = g\Delta(gZ(G), h^\beta G') = g^{\gamma(h^\beta)},$$

that is, the second condition of (1.1) holds. □

We now record two consequences of Proposition 2.2 concerning commutators and powers.

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

Suppose

(1) $\gamma(G) \le \operatorname{Aut}_c(G)$, and
(2) $[Z(G), \gamma(G)] = 1$.

Then for $g, h \in G$ we have

$$(2.3)\qquad \begin{aligned}[\nu(g), \nu(h)] &= \nu([g, h][g, \gamma(h)][h, \gamma(g)]^{-1})\\ &= \nu([g, h] + \Delta(g, h) - \Delta(h, g)).\end{aligned}$$

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

Since an element $\nu(x)$ of the subgroup N is determined by the element x to which it takes 1, it suffices to compute the following

$$\begin{aligned}1^{[\nu(g),\nu(h)]} &= (((((g^{-1})^{\gamma(g)^{-1}})^{\gamma(h)^{-1}} (h^{-1})^{\gamma(h)^{-1}})^{\gamma(g)} x)^{\gamma(h)})y\\ &= (g^{-1})^{[\gamma(g),\gamma(h)]} (h^{-1})^{\gamma(h)^{-1}\gamma(g)\gamma(h)} g^{\gamma(h)} h\\ &= g^{-1}(h^{-1})^{\gamma(g)} g^{\gamma(h)} h\\ &= [g, h][h^{-1}, \gamma(g)][g, \gamma(h)]\\ &= [g, h][g, \gamma(h)][h, \gamma(g)]^{-1},\end{aligned}$$

where we have used the facts that $[G, \gamma(G)] \le Z(G)$ and $\gamma(G)$ is abelian, according to Lemma 2.1. □

Lemma 2.5. *Let G be a finite p-group of class two, and $N \trianglelefteq \operatorname{Hol}(G)$ a regular subgroup.*

Suppose

(1) $\gamma(G) \le \operatorname{Aut}_c(G)$, and
(2) $[Z(G), \gamma(G)] = 1$.

Then for $g \in G$ we have

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

In particular, under the hypotheses of the Lemma the elements of G retain their orders under ν.

Proof. This follows from

$$\begin{aligned}
1^{\nu(g)^n} &= g^{\gamma(g)^{n-1}} g^{\gamma(g)^{n-2}} \cdots g^{\gamma(g)} g\\
&= g^n [g, \gamma(g)^{n-1}][g, \gamma(g)^{n-2}] \cdots [g, \gamma(g)]\\
&= g^n [g, \gamma(g)]^{\binom{n}{2}} = g^n \cdot \Delta(g, g)^{\binom{n}{2}}\\
&= g^n [g^n, \gamma(g)^{(n-1)/2}]\\
&= (g^n)^{\gamma(g)^{(n-1)/2}},
\end{aligned}$$

where we have used the fact that $[G, \gamma(G)] \le Z(G)$, according to Lemma 2.1. □

3. Power Isomorphisms

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

As noted in Remark 2.3, the maps

$$\begin{aligned}
\Delta_c : G/Z(G) \times G/G' &\to G'\\
(gZ(G), hG') &\mapsto [g, h]^c,
\end{aligned}$$

for integers c, satisfy the conditions (2) of Proposition 2.2. To Δ_c we then associate the γ_c given by

$$g^{\gamma_c(h)} = g\Delta_c(g, h) = g[g, h]^c = g^{h^c},$$

that is,

$$\gamma_c(h) = \iota(h^c). \tag{3.1}$$

All these γ_c yields regular subgroups $N \trianglelefteq \mathrm{Hol}(G)$. To see which γ_c yield subgroups $N \in \mathcal{H}(G)$, consider, for integers d coprime to p, 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

$$h^{\rho(g)^{\vartheta_d}} = (h^{d'})^{\rho(g)\vartheta_d} = (h^{d'} g)^d = hg^d [g, h^{d'}]^{\binom{d}{2}} = h^{\iota(g^{(1-d)/2})\rho(g^d)},$$

so that

$$\rho(g)^{\vartheta_d} = \iota(g^{(1-d)/2})\rho(g^d) \in \mathrm{Aut}(G)\rho(G) = \mathrm{Hol}(G). \tag{3.2}$$

Since we have also

$$[\mathrm{Aut}(G), \vartheta_d] = 1,$$

it follows that $\vartheta_d \in \mathrm{NHol}(G) = N_{S(G)}(\mathrm{Hol}(G))$, and thus ϑ_d induces an element of $T(G)$. To determine the γ associated to ϑ_d, one can apply (1.2) to (3.2) to get $\gamma(g^{\vartheta_d}) = \gamma(g^d) = \iota(g^{(1-d)/2})$, and then, replacing g by $g^{d'}$,

$$\gamma(g) = \iota(g^{(d'-1)/2}).$$

(We could have also used Lemma 1.5 to obtain the same result.)

Clearly for a given c the equation $c = (d' - 1)/2$ has a solution d coprime to $\exp(G)$ if and only if $c \ne -1/2$ modulo $\exp(G)$, so that for these c the γ_c of (3.1) correspond to elements $N \in \mathcal{H}(G)$. (The regular subgroup corresponding to $\gamma_{-1/2}$ is abelian, and thus not isomorphic to G, see Remark 5.3.)

(3.2) shows that the ϑ_d are all distinct as d ranges in the integers coprime to p between 1 and $\exp(G/Z(G)) - 1$. Clearly $\vartheta_{d_1}\vartheta_{d_2} = \vartheta_{d_1 d_2}$, so that the ϑ_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 $T(\mathcal{G}(p))$

Let $p > 2$ be a prime, and define

$$\mathcal{G}(p) = \left\langle x, y : x^{p^2}, y^{p^2}, [x, y] = x^p \right\rangle.$$

This is a group of order p^4 and nilpotence class two, such that $\mathcal{G}(p)' = \langle x^p \rangle$ has order p, and $\mathcal{G}(p)^p = \operatorname{Frat}(\mathcal{G}(p)) = Z(\mathcal{G}(p)) = \langle x^p, y^p \rangle$ has order p^2.

It is a well-known fact and an easy exercise that $\operatorname{Aut}(\mathcal{G}(p))$ induces on the $\mathbf{F}_p$-vector space $V = \mathcal{G}(p)/\operatorname{Frat}(\mathcal{G}(p))$ the group of matrices

$$\left\{ \begin{bmatrix} a & 0 \\ b & 1 \end{bmatrix} : a \in \mathbf{F}_p^*, b \in \mathbf{F}_p \right\}$$

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 $W = \mathcal{G}(p)^p = Z(\mathcal{G}(p)) = \operatorname{Frat}(\mathcal{G}(p))$, with respect to the basis given by x^p, y^p.

We first note that Lemma 1.7(1) implies

Lemma 4.1. *Let G be a group, and $N \trianglelefteq \operatorname{Hol}(G)$ a regular subgroup.*
Let $\alpha \in Z(\operatorname{Aut}(G))$.
Then

$$[G, \alpha] = \left\{ g^{-1} g^{\alpha} : g \in G \right\} \le \ker(\gamma).$$

In the group $\mathcal{G}(p)$, the power map $\alpha : g \mapsto g^{1+p}$ is an automorphism lying in the centre of $\operatorname{Aut}(\mathcal{G}(p))$. Hence

Lemma 4.2. *Let $N \in \mathcal{J}(\mathcal{G}(p))$. Then*

$$\mathcal{G}(p)' \le Z(\mathcal{G}(p)) = \operatorname{Frat}(\mathcal{G}(p)) = \mathcal{G}(p)^p \le \ker(\gamma).$$

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

$$(4.1) \qquad [Z(\mathcal{G}(p)), \gamma(\mathcal{G}(p))] = [\mathcal{G}(p)^p, \gamma(\mathcal{G}(p))] = [\mathcal{G}(p), \gamma(\mathcal{G}(p))]^p = 1,$$

as $[\mathcal{G}(p), \gamma(\mathcal{G}(p))] \le Z(\mathcal{G}(p))$, and $Z(\mathcal{G}(p))$ has exponent p.

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

For Δ as in Proposition 2.2, and $\beta \in \mathrm{Aut}(G)$ which induces

$$\begin{bmatrix} a & 0 \\ b & 1 \end{bmatrix}, \tag{4.2}$$

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 β 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 $\Delta(x, x) \in \langle\, x^p y^{2p} \,\rangle$, 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 β, we see that $\Delta(x, y) = tx^p$ for some t.

Similarly, $\Delta(y, x) = sx^p$ for some s. 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 γ for $\mathcal{G}(p)$ are given by

$$\gamma_{s,t}(x) : \begin{cases} x \mapsto x \\ y \mapsto x^{ps} y \end{cases} \qquad \gamma_{s,t}(y) : \begin{cases} x \mapsto x^{1+pt} \\ y \mapsto y^{1+p(s+t)} \end{cases} \tag{4.3}$$

for $s, t \in \mathbf{F}_p$.

Lemma 2.4 yields that for the regular subgroup $N \trianglelefteq \mathrm{Hol}(G)$ corresponding to $\gamma_{s,t}$ one has

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

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

If $t - s + 1 \neq 0$, we choose $d = (1 + t - s)'$, so that $[\nu(x), \nu(y^d)] = \nu(x^p)$. Since by Lemma 2.5 $\nu(x^p) = \nu(x)^p$, and $\langle\, \nu(x) \,\rangle, \left\langle\, \nu(y^d) \,\right\rangle$ have each order p^2, and intersect trivially, we have that $\mathcal{G}(p) \cong (\mathcal{G}(p), \circ)$, via the isomorphism defined by

$$\vartheta_{d,s} : \begin{cases} x \mapsto x \\ y \mapsto y^d \end{cases} \tag{4.4}$$

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

Remark 4.3. *One might wonder where the power isomorphisms ϑ_d of Section 3 have gone in* (4.4)*. They can be recovered using Lemma 1.6, with $\alpha = \beta$ defined on V by* (4.2)*, for $a = d$ and $b = 0$, and $\vartheta = \vartheta_{d,(1-d')/2}$.*

We now determine the structure of the group $T(\mathcal{G}(p))$. Note first that we may take $d \in \mathbf{F}_p^*$ in (4.4). To see this, apply Lemma 1.6 with α 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 $T(\mathcal{G}(p))$ with respect to the same γ.

We now want to show

Theorem 4.4.

$$\vartheta_{d,s}\vartheta_{e,u} \equiv \vartheta_{de,se'+u}.$$

Therefore

$$T(\mathcal{G}(p)) = \left\{\vartheta_{d,s} : d \in \mathbf{F}_p^*, s \in \mathbf{F}_p\right\},$$

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

Proof. Note first that it follows from Lemma 2.5, and $x^{\vartheta_{d,s}} = x$ and $x^{\gamma_{s,t}(x)} = x$ that

$$(x^i)^{\vartheta_{d,s}} = x^i \tag{4.5}$$

for all i.

Similarly, note first that combining Theorem 1.2(iv) and Lemma 1.4 we obtain that for all i

$$\nu((y^i)^{\vartheta_{d,s}}) = \nu(y)^i,$$

so that Lemma 2.5 yields

$$\begin{aligned}(y^i)^{\vartheta_{d,s}} &= (y^{di})^{\gamma(y^{d(i-1)/2})}\\ &= y^{(di)(1+pd(i-1)/2(s+t)}\\ &= y^{di+pd\binom{i}{2}(s+t)}.\end{aligned} \tag{4.6}$$

Now consider another $\vartheta_{e,u}$, and let $v = e' + u - 1$. From (4.6) we obtain

$$y^{\vartheta_{d,s}\vartheta_{e,u}} = (y^d)^{\vartheta_{e,u}} = y^{de} x^{p\binom{d}{2}e(u+v)}.$$

Using Lemma 1.6 again, if we choose α to be the inner automorphism

$$\iota(x^{\frac{d-1}{2}(u+v)}) : \begin{cases} x \mapsto x \\ y \mapsto yx^{-p\frac{d-1}{2}(u+v)} \end{cases}$$

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 $(hg)^{\vartheta_{d,s}\vartheta_{e,u}}$ in two ways. We compute first

$$\begin{aligned}(yx)^{\vartheta_{d,s}\vartheta_{e,u}} &= (y^{\vartheta_{d,s}\vartheta_{e,u}})^{\gamma_{w,z}(x)} x^{\vartheta_{d,s}\vartheta_{e,u}} \\ &= ((hy^d)^{\vartheta_{e,u}})^{\gamma_{w,z}(x)} x \\ &= (y^{de})^{\gamma_{w,z}(x)} x y^{p\binom{d}{2}e(u+v)},\end{aligned} \tag{4.7}$$

where we have used (4.5), (4.6), and (4.1).

We then compute

$$\begin{aligned}(yx)^{\vartheta_{d,s}\vartheta_{e,u}} &= ((y^{\vartheta_{d,s}})^{\gamma_{s,t}(x)} x)^{\vartheta_{e,u}} \\ &= (y^d x^{psd} x)^{\vartheta_{e,u}} \\ &= ((y^d)^{\vartheta_{e,u}})^{\gamma_{u,v}(x)} (x^{1+psd})^{\vartheta_{e,u}} \\ &= (y^{de+p\binom{d}{2}e(u+v)})^{\gamma_{u,v}(x)} (x^{1+psd})^{\vartheta_{e,u}} \\ &= y^{de+p\binom{d}{2}e(u+v)} x^{1+psd+pdeu},\end{aligned} \tag{4.8}$$

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 $(d'e')$-th powers we get

$$y^{\gamma_{w,z}(x)} = yx^{p(se'+u)}$$

so that

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

as claimed. □

5. More Examples

In this section we first show that for $p > 2$ the non-abelian groups G of order p^3, and the groups G of class 2 and exponent p have $T(G)$ of order $p - 1$, that is, according to Proposition 3.1, as small as possible.

We then exhibit a family of finite p-groups G of class 2, for $p > 2$ with minimum number of generators $n \geq 4$ for which $T(G)$ is non-abelian, and contains an elementary abelian subgroup of order $p^{\binom{n}{2}\binom{n+1}{2}}$.

5.1. **A group of order p^3.** Let $p > 2$ be a prime, and H_p the group of order p^3 and exponent p^2, so that

$$H_p = \left\langle x, y : x^{p^2}, y^p, [x, y] = x^p \right\rangle.$$

We claim

Proposition 5.1. *$T(H_p)$ is a cyclic group of order $p - 1$.*

The arguments are similar to those for $\mathcal{G}(p)$ in Section 4, so we only sketch them briefly.

$\operatorname{Aut}(H_p)$ induces on the $\mathbf{F}_p$-vector space $V = H_p/\operatorname{Frat}(H_p)$ the group of matrices

$$\left\{ \begin{bmatrix} a & 0 \\ b & 1 \end{bmatrix} : a \in \mathbf{F}_p^*, b \in \mathbf{F}_p \right\}$$

with respect to the basis induced by x, y. Clearly such an automorphism sends, using additive notation, x^p to ax^p.

Arguing as in Section 4, one sees that the γ for H_p are given by

$$\gamma_t(x) : \begin{cases} x \mapsto x \\ y \mapsto x^{-pt} y \end{cases} \qquad \gamma_t(y) : \begin{cases} x \mapsto x^{1+pt} \\ y \mapsto y \end{cases},$$

for $t \in \mathbf{F}_p^*$.

For the regular subgroup $N \trianglelefteq \operatorname{Hol}(G)$ corresponding to γ_t we have

$$[\nu(x), \nu(y^d)] = \nu(x^{pd(1+2t)}).$$

Therefore N is abelian when $t = -1/2$. (See Remark 5.3 below.)

When $t \neq -1/2$, we choose $d = (1 + 2t)' \in \mathbf{F}_p^*$, so that $H_p \cong (H_p, \circ)$, via the isomorphism defined by

$$\vartheta_d : \begin{cases} x \mapsto x \\ y \mapsto y^d \end{cases}$$

and by the accompanying γ_t as above. Since we have $p - 1$ choices for ϑ_d, it follows from Proposition 3.1 that $T(H_p)$ is cyclic of order $p - 1$.

5.2. **Groups of exponent p.** We claim the following

Theorem 5.2. *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 $\operatorname{Frat}(G) = Z(G)$, we have that the group $\operatorname{Aut}(G)/\operatorname{Aut}_c(G)$ is isomorphic to $\operatorname{GL}(n, p)$. The conditions in (1.1) imply that $\gamma(G)$ is a p-group, which is normal in $\operatorname{Aut}(G)$. Therefore $\gamma(G) \leq \operatorname{Aut}_c(G)$. Moreover Lemma 2.1 implies

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

We can thus use the the Δ setting of Proposition 2.2. Here $V = G/G' = G/Z(G)$ and $W = G'$ are $\mathbf{F}_p$-vector spaces, and W is naturally isomorphic to the exterior square $\bigwedge^2 V$ of V.

5.2.1. *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 $a \in \mathbf{F}_p^* \setminus \{1, -1\}$. Consider the automorphism β of V (and thus of G), that fixes g, and multiplies all other basis elements by a. Then β fixes $\Delta(g, g)$, but there are no fixed points of β in $W \cong \bigwedge^2 V$, as β multiplies all natural basis elements of $\bigwedge^2 V$ 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 β of V which fixes g, h, and multiplies all other basis elements by $a \in \mathbf{F}_p^* \setminus \{1, -1\}$. Then the only fixed points of β in W are the multiples of $[g, h]$, so that $\Delta(g, h) = c[g, h]$ for some c. Consider another basis elements $k \neq g, h$, so that $\Delta(g, k) = c'[g, k]$, and $\Delta(g, h + k) = c[g, h] + c'[g, k]$. Since $\Delta(g, h + k)$ must also be a multiple of $[g, h + k]$, we see that $c' = c$ uniformly, so that, reverting to multiplicative notation,

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

that is, $\gamma(h) = \iota(h^c)$. For $c \neq -1/2$, this is uniquely associated, as we have seen in Section 3, to $g^{\vartheta_d} = g^d$, where $d = (1 + 2c)'$.

Remark 5.3. *Similarly to what happened in Subsection 5.1, there is no such ϑ_d when $c = -1/2$. In fact in this case Lemma 2.4 shows that*

$$\begin{aligned}
[\nu(g), \nu(h)] &= \nu([g, h] + \Delta(g, h) - \Delta(h, g)) \\
&= \nu([g, h] - \frac{1}{2}[g, h] + \frac{1}{2}[h, g]) \\
&= \nu(0) = 1,
\end{aligned}$$

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-Campbell-Hausdorff formulas* [Khu98, Ch. 9 and 10].

5.2.2. *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 β of V which fixes g, and acts as scalar multiplication by -1 on C. Then $\Delta(g, g) \in \bigwedge^2 C$. 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 β of V which fixes g, h, and acts as scalar multiplication by -1 on C. Then

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

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

5.3. **A biggish $T(G)$.** For the next class of examples, we will use the p-groups of [Car16].

Theorem 5.4 ([Car16]). *Let $p > 2$ be a prime, and $n \geq 4$.*
Consider the presentation

$$G = \langle x_1, \dots, x_n : [[x_i, x_j], x_k] = 1 \text{ for all } i, j, k, \quad x_i^p = \prod_{j<k} [x_j, x_k]^{a_{i,j,k}} \text{ for all } i, \rangle , \tag{5.1}$$

where $a_{i,j,k} \in \mathbf{F}_p$.
There is a choice of the $a_{i,j,k} \in \mathbf{F}_p$ such that the following hold.

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

We claim the following

Theorem 5.5. *Let G be one of the groups of Theorem 5.4.*
Then $T(G)$ contains a non-abelian subgroup of order

$$(p-1) \cdot p^{\binom{n}{2}\binom{n+1}{2}},$$

which is the extension of an $\mathbf{F}_p$-vector space of dimension $\binom{n}{2}\binom{n+1}{2}$ by the multiplicative group $\mathbf{F}_p^*$ acting naturally.

Here again $V = G/G' = G/Z(G)$ and $W = G'$ can be regarded as $\mathbf{F}_p$-vector spaces, and W is naturally isomorphic to $\bigwedge^2 V$. The conditions of Proposition 2.2 apply, so we can use the Δ setting. Because of Theorem 5.4, condition (2.1) of Proposition 2.2 holds trivially, so that we are simply looking at all bilinear maps $\Delta : V \times V \to W$ here.

Consider all such Δ which are symmetric with respect to the basis of V induced by the x_i. Under the pointwise operation of W, these Δ form a vector space $\mathfrak{D}$ of dimension $\binom{n}{2}\binom{n+1}{2}$ over $\mathbf{F}_p$. For the regular subgroup $N \trianglelefteq \operatorname{Hol}(G)$ of $S(G)$ corresponding to such a Δ, Lemma 2.4 yields, for $1 \leq i < j \leq n$,

$$[\nu(x_i), \nu(x_j)] = \nu([x_i, x_j] + \Delta(x_i, x_j) - \Delta(x_j, x_i)) = \nu([x_i, x_j]) \tag{5.2}$$

and Lemma 2.5 yields, for $1 \leq i \leq n$,

$$\nu(x_i)^p = \nu(x_i^p \cdot \Delta(x_i, x_i)^{\binom{p}{2}}) = \nu(x_i^p),$$

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 $\vartheta_\Delta : G \to (G, \circ)$ such that $x_i \mapsto x_i$ for each i. Since the composition of ϑ_Δ followed by ν is an isomorphism $G \to N$, 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, ϑ_Δ fixes the elements of G'.

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

$$\begin{aligned}(x_i x_j)^{\vartheta_{\Delta_1}\vartheta_{\Delta_2}} &= (x_i x_j \Delta_1(x_i, x_j))^{\vartheta_{\Delta_2}}\\ &= x_i x_j \Delta_2(x_i, x_j)\Delta_1(x_i, x_j),\end{aligned}$$

where we have applied Lemma 1.5(1.3), using the facts that ϑ_Δ 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 ϑ_d of Section 3, we readily obtain Theorem 5.5.

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

[CDV17] A. Caranti and F. Dalla Volta, *The multiple holomorph of a finitely generated abelian group*, J. Algebra **481** (2017), 327–347. MR 3639478

[CDV18] ———, *Groups that have the same holomorph as a finite perfect group*, J. Algebra **507** (2018), 81–102.

[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)

[Rob96] Derek J. S. Robinson, *A course in the theory of groups*, second ed., Graduate Texts in Mathematics, vol. 80, Springer-Verlag, New York, 1996. MR 1357169 (96f:20001)

(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/