Advances in Group Theory and Applications

14 (2022), pp. 5–47 ISSN: 2499-1287
DOI: 10.32037/agta-2022-010

The Automorphism Group of certain 3-Generator p-Groups

Fernando Szechtman

(*Received July 6, 2021; Accepted June 12, 2022 — Communicated by E. Aljadeff*)

Abstract

A presentation as well as a structural description of the automorphism group of a family of 3-generator finite p-groups is given, p being an odd prime.

Mathematics Subject Classification (2020): 20D45, 20D15, 20D20

Keywords: automorphism group; p-group

1 Introduction

We fix a prime number p throughout the paper. The automorphism groups of finite p-groups have been widely studied. One line of investigation was related to the divisibility conjecture, to the effect that if G is a finite non-cyclic p-group of order larger than p^2, then $|G|$ divides $|\mathrm{Aut}(G)|$. While this holds true for several classes of p-groups, it has recently been shown to be false in general [7]. A thorough survey of this conjecture can be found in [4]. A second avenue of research is connected to the conjecture that every finite non-abelian p-group has a non-inner automorphism of order p. We refer the reader to [5] and references therein for the status of this conjecture. A third focus of attention has been the actual structure of $\mathrm{Aut}(G)$ when G is a finite p-group of one type or another. This has been the case, in

particular for metacyclic groups, as found in [1],[2],[3],[6],[8],[9],[12], for instance.

The present paper gives a presentation as well as a structural description of the automorphism group of a family of 3-generator finite p-groups, with p odd.

We assume henceforth that p is odd and that $i, n \in \mathbb{N}$ satisfy $n \geqslant 2$ and $1 \leqslant i \leqslant n-1$. Given an integer d that is not a multiple of p, the inverse of $1+dp$ modulo p^n is also of the form $1+ep$ for some integer e not divisible by p, so we have

$$p \nmid d, \ p \nmid e, \tag{1.1}$$

and

$$(1+dp)(1+ep) \equiv 1 \mod p^n. \tag{1.2}$$

Let Σ be the group with the following presentation, depending on whether $2i \leqslant n$ or $2i \geqslant n$:

$$\begin{aligned}\Sigma = \langle a, b, c \,|\, a^{p^i} = b^{p^{n-i}} = c^{p^{n-1}} = 1, [a,b] = c^{p^{n-i-1}}, \\ cac^{-1} = a^{1+ep}, cbc^{-1} = b^{1+dp} \rangle,\end{aligned} \tag{1.3}$$

or

$$\begin{aligned}\Sigma = \langle a, b, c \,|\, a^{p^{n-i}} = b^{p^{n-i}} = c^{p^{n-1}} = 1, [a,b] = c^{p^{i-1}}, \\ cac^{-1} = a^{1+ep}, cbc^{-1} = b^{1+dp} \rangle.\end{aligned} \tag{1.4}$$

This is a quotient of the finite Wamsley group [10] defined on 3 generators with 3 relations.

In this paper, we give a presentation of $\mathrm{Aut}(\Sigma)$ and its normal Sylow p-subgroup Π, and provide a structural description of these groups.

There is a noteworthy connection between Σ and automorphism groups. Let Υ be the semidirect product of a cyclic group C_{p^n} of order p^n by the unique subgroup of order p^{n-i} of the cyclic group $\mathrm{Aut}(C_{p^n})$. Thus

$$\Upsilon = \langle x, y \,|\, x^{p^n} = 1, y^{p^{n-i}} = 1, yxy^{-1} = x^{1+p^i} \rangle. \tag{1.5}$$

Then Σ is isomorphic to the normal Sylow p-subgroup of $\mathrm{Aut}(\Upsilon)$. A presentation for $\mathrm{Aut}(G)$ when G is a split metacyclic p-group can be found in [1]. This includes, in particular, the case when $G = \Upsilon$.

Consider the group Ψ with the following presentation, depending on whether $2i \leqslant n$ or $2i \geqslant n$:

$$\Psi = \langle a, b, d \mid a^{p^i} = b^{p^{n-i}} = d^{p^i} = 1, [a, b] = d, ad = da, bd = db \rangle,$$

$$\Psi = \langle a, b, d \mid a^{p^{n-i}} = b^{p^{n-i}} = d^{p^{n-i}} = 1, [a, b] = d, ad = da, bd = db \rangle.$$

Then Ψ is a p-group of Heisenberg type, and Σ is an extension of Ψ by a cyclic factor. Moreover, Σ cannot be generated by fewer than 3 elements, except in the extreme case $n = 2$, when Σ is the Heisenberg group of order p^3. Furthermore, Σ is a non-split extension of Ψ, except when $n = 2$, in which case $\Sigma = \Psi$.

The fact that Σ requires 3 generators makes the computation of $\mathrm{Aut}(\Sigma)$ particularly challenging. An appreciation of the obstacles involved can perhaps be gleaned from the following: Π requires 6 generators and 21 relations when $2i \geqslant n$ but $i \neq n-1$, while if $2i < n$ we utilize 8 generators and 38 relations for this purpose (although we could manage with slightly fewer). We feel that the groups Σ constitute a non-trivial addition to the reservoir of p-groups for which the automorphism group is known.

Our work begins in Section 2, where we describe properties of Σ and Ψ. Once this background information has been collected, Sections 3 and 4 describe $\mathrm{Aut}(\Sigma)$ and Π. In Section 3 we assume that $2i \geqslant n$; in this case, Ψ is a characteristic subgroup of Σ and our analysis of the image of the restriction homomorphism

$$\mathrm{Aut}(\Sigma) \to \mathrm{Aut}(\Psi)$$

allows us in Theorem 3.2 to obtain the desired presentations of $\mathrm{Aut}(\Sigma)$ and Π when $i < n-1$. Considerable effort is spent in Theorem 3.2 in finding suitable generators for Π, and we show that no smaller amount of generators is possible. In addition, Theorem 3.2 gives a presentation of $\mathrm{Out}(\Sigma)$, and shows that Π is the kernel of the canonical homomorphism

$$\mathrm{Aut}(\Sigma) \to \mathrm{Aut}(\Sigma/\Sigma^p).$$

The case $i = n-1$ is essentially different and is handled in Theorem 3.4, which gives presentations of Bruhat type for $\mathrm{Aut}(\Sigma)$ and $\mathrm{Aut}(\Psi)$. In Section 4 we suppose that $2i < n$; this case is considerably harder, as Ψ is not a characteristic subgroup of Σ. Let G be

the subgroup of $\mathrm{Aut}(\Sigma)$ preserving Ψ. Theorem 4.3 shows that

$$\mathrm{Aut}(\Sigma) = G\langle U\rangle,$$

where U is a suitable automorphism of Σ, and finds generators for G and so for $\mathrm{Aut}(\Sigma)$. Presentations and further descriptions of $\mathrm{Aut}(\Sigma)$ and Π can be found in Theorem 4.4 (which omits some relations from the case $n = 2i+1$). It turns out that $\Pi = \Phi\langle U\rangle$, where Φ is the kernel of the canonical homomorphism $\mathrm{Aut}(\Sigma) \to \mathrm{Aut}(\Sigma/\Sigma^p)$. Moreover, Π requires at least 7 generators.

An appendix contains a study of $\mathrm{Aut}(\Upsilon)$, independent of [1], and establishes the foregoing connection between Σ and $\mathrm{Aut}(\Upsilon)$. In particular, we somewhat simplify the presentation of $\mathrm{Aut}(\Upsilon)$ derived in [1] for an arbitrary split metacyclic p-group.

Given a finite p-group P, we write $z(P)$ for the minimum number of generators of P, that is, $z(P)$ is the dimension of the $\mathbb{Z}/p\mathbb{Z}$-vector space $P/\Phi(P)$, where $\Phi(P)$ is the Frattini subgroup of P. If G is an arbitrary finite group, we let $s(G)$ denote a Sylow p-subgroup of G. Thus $z(\Upsilon) = 2$, $s\big(\mathrm{Aut}(\Upsilon)\big) = \Sigma$ and $z(\Sigma) = 3$ when $n > 2$; also $s\big(\mathrm{Aut}(\Sigma)\big) = \Pi$ with $z(\Pi) = 6$ if $2i \geqslant n$, $i \neq n-1$, and $z(\Pi) = 7$ if $2i < n$. On the other hand, if P is an elementary abelian group of order p^m, then $z(P) = m$ and $z\big(s\big(\mathrm{Aut}(P)\big)\big) = m-1$. Prompted by these examples and others, and inspired by the divisibility conjecture, we wonder if it might be of interest to determine what classes of finite p-groups G satisfy $z\big(s\big(\mathrm{Aut}(G)\big)\big)/z(G) \geqslant 1$, including further information about this ratio.

Given a group G, we write

$$[a,b] = aba^{-1}b^{-1}, \quad a,b \in G,$$

and let $\delta : G \to \mathrm{Inn}(G)$ stand for the homomorphism $a \mapsto \delta_a$, where

$$\delta_a(b) = {}^a b = aba^{-1}, \quad a,b \in G.$$

The image of $\gamma \in \mathrm{Aut}(G)$ under the natural projection

$$\mathrm{Aut}(G) \to \mathrm{Out}(G)$$

will be denoted by $\overline{\gamma}$. Observe that

$$[ab,c] = {}^a[b,c][a,c],\ [a,b]^{-1} = [b,a],\ [c,ab] = [c,a]\,{}^a[c,b].$$

In particular, if $[G, G]$ is included in the center of G, then the bracket is a group homomorphism in each variable. We will repeatedly and implicitly use these facts throughout the paper.

2 Background material on Σ and Ψ

Proposition 2.1 *The group Σ cannot be generated by fewer than 3 elements, unless $n = 2$.*

Proof — Let E be an elementary abelian p-group of order p^3 and let a, b, c be generators of E. Consider the assignment

$$\mathfrak{a} \mapsto a, \ \mathfrak{b} \mapsto b, \ \mathfrak{c} \mapsto c. \tag{2.1}$$

The given presentation of Σ ensures that, except when $n = 2$, we can extend (2.1) to an epimorphism $\Sigma \to E$. Since E cannot be generated by fewer than 3 elements, neither can Σ. □

Proposition 2.2 *The derived subgroup of Σ is generated by $\mathfrak{a}^p, \mathfrak{b}^p, \mathfrak{c}^{p^{n-i-1}}$ if $2i \leqslant n$, and by $\mathfrak{a}^p, \mathfrak{c}^p, \mathfrak{c}^{p^{i-1}}$ if $2i \geqslant n$.*

Proof — Let T be the subgroup of Σ generated by the stated elements. The given presentation of Σ and (1.1) ensure that $T \subseteq [\Sigma, \Sigma]$, T is normal in Σ, and Σ/T is abelian, whence $T = [\Sigma, \Sigma]$. □

Given a ring R with $1 \neq 0$ and a right module M, the Heisenberg group $\mathrm{Heis}(R, M)$ consists of all matrices

$$\begin{pmatrix} 1 & u & v \\ 0 & 1 & r \\ 0 & 0 & 1 \end{pmatrix}, \quad r \in R, u, v \in M,$$

under the usual matrix multiplication, with the understanding that $1 \cdot u = u$ for $u \in M$. If $M = R$, we simply write $\mathrm{Heis}(R) = \mathrm{Heis}(R, M)$.

Proposition 2.3 *We have $\Psi \simeq \mathrm{Heis}\big(\mathbb{Z}/p^{n-i}\mathbb{Z}, \mathbb{Z}/p^i\mathbb{Z}\big)$ if $2i \leqslant n$ and $\Psi \simeq \mathrm{Heis}\big(\mathbb{Z}/p^{n-i}\mathbb{Z}\big)$ if $2i \geqslant n$. In particular, Ψ has order p^{n+i} if $2i \leqslant n$ and $p^{3(n-i)}$ if $2i \geqslant n$, and any element of Ψ can be written in one and only one way in the form ABD, where $A \in \langle \mathfrak{a} \rangle$, $B \in \langle \mathfrak{b} \rangle$, and $D \in \langle \mathfrak{d} \rangle$.*

PROOF — Note that the annihilator of the $\mathbb{Z}$-module $\mathbb{Z}/p^i\mathbb{Z}$ is $p^i\mathbb{Z}$; if $2i \leqslant n$ then $p^{n-i}\mathbb{Z}$ is contained in $p^i\mathbb{Z}$, so $\mathbb{Z}/p^i\mathbb{Z}$ becomes a $\mathbb{Z}/p^{n-i}\mathbb{Z}$-module. The given presentation of Ψ yields the decomposition $\Psi = \langle a\rangle\langle b\rangle\langle d\rangle$, and ensures that the assignment

$$a \mapsto \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \; b \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \; d \mapsto \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

extends to a group epimorphism $\Psi \to \mathrm{Heis}\big(\mathbb{Z}/p^{n-i}\mathbb{Z}, \mathbb{Z}/p^i\mathbb{Z}\big)$ if $2i \leqslant n$ and $\Psi \to \mathrm{Heis}\big(\mathbb{Z}/p^{n-i}\mathbb{Z}\big)$ if $2i \geqslant n$. It is an isomorphism as the presentation of Ψ bounds its order, from above, by the order of the corresponding Heisenberg group. Uniqueness follows from existence and $|\Psi|$. □

Lemma 2.4 *Let $a, b, c, \ell \in \mathbb{Z}$, where $a, c \geqslant 1$ and $b \geqslant 0$. Then*

$$(1 + \ell p^a)^{cp^b} \equiv 1 + c\ell p^{a+b} \mod p^{2a+b}. \tag{2.2}$$

PROOF — We assume first that $c = 1$ and show (2.2) by induction on b. If $b = 0$ there is nothing to do. Suppose (2.2) is true for some $b \geqslant 0$. Then there exists $s \in \mathbb{Z}$ such that

$$(1 + \ell p^a)^{p^b} = 1 + \ell p^{a+b} + sp^{2a+b} = 1 + p^{a+b}(\ell + sp^a).$$

Set $f = \ell + sp^a$. Then

$$(1 + \ell p^a)^{p^{b+1}} = (1 + p^{a+b}f)^p$$

$$= 1 + p^{a+b+1}f + \binom{p}{2}p^{2(a+b)}f^2 + \ldots + \binom{p}{p}p^{p(a+b)}f^p.$$

Since p is odd, we have $p|\binom{p}{2}$, so there is some $k \in \mathbb{Z}$ such that

$$\binom{p}{2}p^{2(a+b)}f^2 = p^{2a+2b+1}k.$$

Moreover, since $a \geqslant 1$, we have $i(a+b) \geqslant 2a+b+1$ for all $3 \leqslant i \leqslant p$. Therefore,

$$(1+\ell p^a)^{p^{b+1}} \equiv 1 + p^{a+b+1}(\ell + sp^a) \equiv 1 + \ell p^{a+(b+1)} \mod p^{2a+(b+1)}.$$

This proves (2.2) when $c = 1$. Now if $c \in \mathbb{N}$ is arbitrary then the previous case yields

$$(1 + \ell p^a)^{cp^b} = \big(1 + p^{a+b}(\ell + hp^a)\big)^c$$

for some $h \in \mathbb{Z}$. Since $i(a+b) \geqslant 2a+b$ for all $i \geqslant 2$, the binomial expansion implies

$$\big(1+p^{a+b}(\ell+hp^a)\big)^c \equiv 1+cp^{a+b}(\ell+hp^a) \equiv 1+c\ell p^{a+b} \mod p^{2a+b}.$$

This demonstrates (2.2) in general. □

Proposition 2.5 *The group Σ is an extension of Ψ by $C_{p^{n-i-1}}$ if $2i \leqslant n$ and by $C_{p^{i-1}}$ if $2i \geqslant n$. In particular, Σ has order p^{2n-1} if $2i \leqslant n$ and $p^{3n-2i-1}$ if $2i \geqslant n$, and any element of Σ can be written in one and only one way in the form ABC, where $A \in \langle \mathfrak{a} \rangle$, $B \in \langle \mathfrak{b} \rangle$, and $C \in \langle \mathfrak{c} \rangle$.*

Proof — By (1.1) and (1.2) there is an automorphism σ of Ψ such that $\mathfrak{a} \mapsto \mathfrak{a}^{1+ep}$, $\mathfrak{b} \mapsto \mathfrak{b}^{1+dp}$ and $\mathfrak{d} \mapsto \mathfrak{d}$. Setting $j = n-i-1$ if $2i \leqslant n$ and $j = i-1$ if $2i \geqslant n$, Lemma 2.4 implies that $\sigma^{p^j} = 1_\Psi = \delta_\mathfrak{d}$. As $\sigma(\mathfrak{d}) = \mathfrak{d}$, there is an extension $G = \Psi\langle \mathfrak{c} \rangle$ of Ψ with cyclic factor C_{p^j} and such that conjugation by $\mathfrak{c}$ acts on Ψ via σ (see [11], Chapter III, Section 7). The given presentation of Σ yields an epimorphism $\Sigma \to G$, which is an isomorphism as $|\Sigma| \leqslant |G|$. That $\Sigma = \langle \mathfrak{a} \rangle \langle \mathfrak{b} \rangle \langle \mathfrak{c} \rangle$ follows from $G = \Psi\langle \mathfrak{c} \rangle$ and Proposition 2.3, while uniqueness follows from existence and the given order of Σ. □

We henceforth view Ψ as a normal subgroup of Σ, as indicated in (the proof of) Proposition 2.5.

Lemma 2.6 *Let $A \in \langle \mathfrak{a} \rangle$, $B \in \langle \mathfrak{b} \rangle$, $D \in \langle \mathfrak{d} \rangle$, and $C \in \langle \mathfrak{c} \rangle$. Then*

$$(ABDC)^p = A_0 B_0 D_0 C^p,$$

for some $A_0 \in \langle \mathfrak{a}^p \rangle$, $B_0 \in \langle \mathfrak{b}^p \rangle$, and $D_0 \in \langle \mathfrak{d}^p \rangle$.

Proof — We have

$$(ABDC)^p = wC^p,$$

where

$$w = AB \cdot {}^C(AB) \cdot {}^{C^2}(AB) \dots {}^{C^{p-1}}(AB) D^p.$$

Now $C = \mathfrak{c}^r$, with $r \in \mathbb{N}$, so setting

$$j = (1+ep)^r, \; k = (1+dp)^r,$$

where d and e are as in (1.1) and (1.2), the defining relations of Σ then give

$$w = ABA^jB^kA^{j^2}B^{k^2}\dots A^{j^{p-1}}B^{k^{p-1}}D^p.$$

Recalling the comments on commutators made in the Introduction, we find that

$$w = A^{1+j+\dots+j^{p-1}}B^{1+k+\dots+k^{p-1}}D^pD_1,$$

where

$$D_1 = [B,A]^j[B,A]^{(1+k)j^2}\dots[B,A]^{(1+k+\dots+k^{p-2})j^{p-1}}.$$

Since

$$j \equiv 1 \equiv k \mod p,$$

we have

$$1+j+\dots+j^{p-1} \equiv 0 \equiv 1+k+\dots+k^{p-1} \mod p$$

and

$$\begin{aligned} &j+(1+k)j^2+\dots+\left(1+k+\dots+k^{(p-2)}\right)j^{p-1} \\ &\equiv 1+2+\dots+(p-1) \equiv 0 \mod p. \end{aligned}$$

Thus $w = A_0B_0D_0$, with $A_0 \in \langle a^p\rangle$, $B_0 \in \langle b^p\rangle$, and $D_0 \in \langle d^p\rangle$. □

If G is a group, then G^p stands for the subgroup of G generated by all elements g^p, with $g \in G$.

Proposition 2.7 *Suppose $n \neq 2$ and let $v \in \Sigma^p$. Then $v = ABC$ for unique elements $A \in \langle a^p\rangle$, $B \in \langle b^p\rangle$, and $C \in \langle c^p\rangle$.*

Proof — As $n \neq 2$, we have $d \in \langle c^p\rangle$. Let $u \in \Sigma$. Then Proposition 2.5 and Lemma 2.6 give

$$u^p = A_0B_0C_0, \tag{2.3}$$

where $A_0 \in \langle a^p\rangle$, $B_0 \in \langle b^p\rangle$, and $C_0 \in \langle c^p\rangle$. As Σ has finite order, v is a finite product of elements of the form (2.3), and it is easy to see that such a product will be also be of the stated form. This proves existence, while uniqueness follows from Proposition 2.5. □

Given a non-zero integer m, we write $\nu_p(m)$ for the p-valuation of m, so that $\nu_p(m) = a$, where a is the unique integer satisfying $a \geqslant 0$, $p^a|m$, and $p^{a+1} \nmid m$. We extend the use of ν_p to non-zero rational numbers in the usual way.

Proposition 2.8 *Let* Ω *in* $\mathrm{Aut}(\Sigma)$ *and* t *in* Ψ. *Set* $\ell = i$ *if* $2i \leqslant n$ *and* $\ell = n - i$ *if* $2i \geqslant n$. *Suppose that* $t^{p^\ell} = 1$. *Then* $\Omega(t) \in \Psi$. *In particular, if* $2i \geqslant n$ *then* Ψ *is a characteristic subgroup of* Σ.

Proof — If $n = 2$ then $\Psi = \Sigma$, so we assume that $n \neq 2$.

Let $\Omega \in \mathrm{Aut}(\Sigma)$ and $t \in \Psi$ be arbitrary. Then $t^p \in \langle a^p, b^p, d^p \rangle$ by Lemma 2.6. By Proposition 2.2, $\langle a^p, b^p, d \rangle = [\Sigma, \Sigma]$, which is a characteristic subgroup of Σ. Thus, setting $u = \Omega(t)$, we have

$$u^p = \Omega(t)^p = \Omega(t^p) \in \langle a^p, b^p, d \rangle \subset \Psi.$$

On the other hand, by Proposition 2.5, we have

$$u = AB c^r, \quad r \in \mathbb{Z}, \tag{2.4}$$

where $A \in \langle a \rangle$ and $B \in \langle b \rangle$. Thus Lemma 2.6 gives

$$u^p = A_0 B_0 D_0 c^{rp},$$

where $A_0 \in \langle a^p \rangle$, $B_0 \in \langle a^p \rangle$, and $D_0 \in \langle d^p \rangle$. From $u^p \in \Psi$ we infer $c^{rp} \in \Psi$. Since $c^{p^{n-\ell-1}} = d \in \Psi$ but $c^{p^{n-\ell-2}} \notin \Psi$, we deduce $\nu_p(r) \geqslant n - \ell - 2$, so

$$r = p^{n-\ell-2} f, \quad f \in \mathbb{Z}, \tag{2.5}$$

and therefore

$$u^p = A_0 B_0 D_0 d^f.$$

We now suppose for the first time that $t^{p^\ell} = 1$, so that $u^{p^\ell} = 1$. Then

$$(A_0 B_0 D_0 d^f)^{p^{\ell-1}} = 1,$$

that is

$$(A_0 B_0 D_0)^{p^{\ell-1}} d^{f p^{\ell-1}} = 1.$$

Referring to the normal form of the elements of Ψ, the d-component of $(A_0 B_0 D_0)^{p^{\ell-1}}$ is equal to

$$D_0^{p^{\ell-1}} [B_0, A_0][B_0, A_0]^2 \dots [B_0, A_0]^{p^{\ell-1}-1} = 1.$$

Therefore $d^{f p^{\ell-1}} = 1$, which implies $p | f$. Thus $\nu_p(r) \geqslant n - \ell - 1$ and $u \in \Psi$. □

Proposition 2.9 *The group Σ is a non-split extension of Ψ, unless $n = 2$ in which case $\Psi = \Sigma$.*

Proof — We may assume $n \neq 2$. Suppose, if possible, that there is an element $u \in \Sigma$ such that $\Sigma = \Psi \rtimes \langle u \rangle$, so that u has order q, with $q = p^{n-i-1}$ if $2i \leqslant n$ and $q = p^{i-1}$ if $2i \geqslant n$. Now $u = tc^j$, where $t \in \Psi$ and $j \in \mathbb{Z}$. Here $p \nmid j$, for otherwise $c \notin \Psi \rtimes \langle u \rangle$. Proposition 2.3 and a repeated application of Lemma 2.6 yield

$$1 = u^q = A_1 B_1 D_1 c^{jq} = A_1 B_1 D_1 d^j,$$

where $A_1 \in \langle a^p \rangle$, $B_1 \in \langle b^p \rangle$, and $D_1 \in \langle d^p \rangle$. The normal form of the elements of Ψ forces $D_1 d^j = 1$. As $p \nmid j$, we see that $D_1 d^j$ generates the non-trivial group $\langle d \rangle$, a contradiction. □

Proposition 2.10 *Let (d_0, e_0) be a pair of integers satisfying* (1.1) *and* (1.2)*, and let Σ_0 be the group associated with it via* (1.3) *and* (1.4)*. Then $\Sigma \simeq \Sigma_0$.*

Proof — Set $j = i$ if $2i \leqslant n$ and $j = n - i$ if $2i \geqslant n$.

Let H be the Sylow p-subgroup of the unit group $(\mathbb{Z}/p^{n-1}\mathbb{Z})^\times$. Then H is generated by the class of $1 + ep$. Since the class of $1 + e_0 p$ also generates H, there is an integer r, relatively prime to p, such that

$$(1 + ep)^r \equiv 1 + e_0 p \mod p^{n-1}.$$

Taking inverses modulo p^{n-1}, we infer

$$(1 + dp)^r \equiv 1 + d_0 p \mod p^{n-1}.$$

Consider the elements $A = a^r, B = b, C = c^r$. They generate Σ and satisfy

$$A^{p^j} = B^{p^{n-i}} = C^{p^{n-1}} = 1,\ [A, B] = C^{n-j-1},$$
$$CAC^{-1} = A^{1+e_0 p},\ CBC^{-1} = B^{1+d_0 p}.$$

This readily gives an isomorphism $\Sigma_0 \to \Sigma$. □

For future reference note that (1.2) implies $e \equiv -d \mod p$. Since p is odd and $p \nmid d$, we deduce

$$e \not\equiv d \mod p. \tag{2.6}$$

3 The automorphism group of Σ when $2i \geqslant n$

We assume throughout this section that $2i \geqslant n$. Using the matrix description of Ψ given in Proposition 2.3, we readily see that

$$Z(\Psi) = \langle \mathfrak{d} \rangle.$$

In particular, $\mathfrak{d} = c^{p^{i-1}}$ is central in Σ. More precisely, we have the following result.

Lemma 3.1 *The center of Σ is generated by $c^{p^{n-i-1}}$.*

Proof — Let $z \in Z(\Sigma)$. Then $z = c^r t$ for some $t \in \Psi$ and $r \in \mathbb{N}$, so (1.4) yields

$$^t a = a\mathfrak{d}^a, \ ^t b = b\mathfrak{d}^b$$

for some $a, b \in \mathbb{Z}$, as well as

$$a = {}^z a = {}^{c^r}(a\mathfrak{d}^a) = a^{(1+ep)^r}\mathfrak{d}^a, \ b = {}^z b = {}^{c^r}(b\mathfrak{d}^b) = b^{(1+dp)^r}\mathfrak{d}^b,$$

so $t \in Z(\Psi) = \langle \mathfrak{d} \rangle$ and c^r commutes with a and b. Since c^r commutes with b, we see that $(1+dp)^r \equiv 1 \mod p^{n-i}$. As $p \nmid d$, Lemma 2.4 ensures that $1+dp$ has order p^{n-i-1} modulo p^{n-i}, so $p^{n-i-1} | r$. But $i - 1 \geqslant n - i - 1$, so $\mathfrak{d} \in \langle c^{p^{n-i-1}} \rangle$, and by above $Z(\Sigma) \subseteq \langle c^{p^{n-i-1}} \rangle$. As the reverse inclusion is clear, the result follows. □

Theorem 3.2 *Let p be an odd prime. Suppose $i, n \in \mathbb{N}$ satisfy $n \geqslant 2$, $1 \leqslant i \leqslant n-1$, and $2i \geqslant n$. Let $d, e \in \mathbb{Z}$ be chosen so that (1.1) and (1.2) hold, and let Σ be the group with presentation (1.4).*

Let $A, B, C \in \mathrm{Inn}(\Sigma)$ be the inner automorphisms of Σ associated with a, b, c, respectively. Let $D, E, F, G, H \in \mathrm{Aut}(\Sigma)$ be respectively the defined by

$$a \mapsto a^{1+p^{n-i-1}}, \ b \mapsto b, \ c \mapsto c^{1+p^{n-i-1}},$$

$$a \mapsto ab^{p^{n-i-1}}, \ b \mapsto b, \ c \mapsto c,$$

$$a \mapsto a, \ b \mapsto a^{p^{n-i-1}}b, \ c \mapsto c,$$

$$a \mapsto a^{g_0}, \ b \mapsto b^{h_0}, \ c \mapsto c,$$

$$a \mapsto b, \ b \mapsto a, \ c \mapsto c^{-1},$$

where g_0 is any integer of order $p-1$ modulo p^{n-i}, with inverse h_0 modulo p^{n-i}. Consider the homomorphism $\lambda : \mathrm{Aut}(\Sigma) \to \mathrm{Aut}(\Sigma/\Psi)$, whose

existence is ensured by Proposition 2.8*, as well as the normal subgroup* $\Delta = \ker \lambda$ *of* $\mathrm{Aut}(\Sigma)$*. Moreover, suppose that* $i \neq n-1$*. Then*

$$\mathrm{Aut}(\Sigma) = \langle A, B, C, D, E, F, G, H \rangle \tag{3.1}$$

is a group of order $2p^{3n-2i+1}(p-1)$*, and*

$$\Delta = \langle A, B, C, D, E, F, G \rangle,$$

$$\mathrm{Aut}(\Sigma) = \Delta \rtimes \langle H \rangle = \langle A, B, C, D, E, F \rangle \rtimes \big(\langle G \rangle \rtimes \langle H \rangle \big),$$

$$[\mathrm{Aut}(\Sigma) : \Delta] = 2,$$

$$\Delta = \mathrm{Inn}(\Sigma) \rtimes \langle D, E, F, G \rangle,$$

$$\mathrm{Inn}(\Sigma) = \langle A, B, C \rangle \simeq (\mathbb{Z}/p^{n-i}\mathbb{Z} \times \mathbb{Z}/p^{n-i}\mathbb{Z}) \rtimes \mathbb{Z}/p^{n-i-1}\mathbb{Z},$$

$$\langle D, E, F, G \rangle \simeq \mathbb{Z}/p^{i}\mathbb{Z} \times \big[(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes \mathbb{Z}/(p-1)\mathbb{Z} \big].$$

Furthermore, the generators A, B, C, D, E, F, G, H *of* $\mathrm{Aut}(\Sigma)$ *satisfy the defining relations*

$$A^{p^{n-i}} = 1,\ B^{p^{n-i}} = 1,\ C^{p^{n-i-1}} = 1,\ CAC^{-1} = A^{1+ep},$$

$$CBC^{-1} = B^{1+dp},\ AB = BA, D^{p^{i}} = 1,\ E^{p} = 1,\ F^{p} = 1,$$

$$G^{p-1} = 1,\ H^{2} = 1,\ DE = ED,\ DF = FD,\ DG = GD,\ EF = FE,$$

$$GEG^{-1} = E^{h_0^2},\ GFG^{-1} = F^{g_0^2}, HEH^{-1} = A^{-p^{n-i-1}}F,$$

$$HFH^{-1} = B^{p^{n-i-1}}E,\ HGH^{-1} = G^{-1},$$

$$DAD^{-1} = A^{1+p^{n-i-1}},\ DB = BD,\ DC = CD,$$

$$EAE^{-1} = AB^{p^{n-i-1}},\ EB = BE,\ EC = CE,$$

$$FA = AF,\ FBF^{-1} = A^{p^{n-i-1}}B,\ FC = CF,$$

$$GAG^{-1} = A^{g_0},\ GBG^{-1} = B^{h_0},\ GC = CG,$$

$$HAH^{-1} = B,\ HBH^{-1} = A,\ HCH^{-1} = C^{-1},\ HDH^{-1} = DC^{vp^{n-i-2}},$$

where $v \in \mathbb{Z}$ *satisfies* $dv \equiv 1 \mod p$*, and the generators* $\overline{D}, \overline{E}, \overline{F}, \overline{G}, \overline{H}$ *of*

$$\mathrm{Out}(\Sigma) \simeq \mathbb{Z}/p^{i}\mathbb{Z} \times \big[(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes (\mathbb{Z}/(p-1)\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}) \big] \tag{3.2}$$

satisfy the defining relations naturally arising from the above, and realizing (3.2).

In addition, $\Pi = \langle A, B, C, D, E, F\rangle$ *is a normal Sylow* p*-subgroup of* $\mathrm{Aut}(\Sigma)$*, with the above defining relations, excluding those involving* G *or* H*, and* Π *is the kernel of the natural homomorphism*

$$\Gamma : \mathrm{Aut}(\Sigma) \to \mathrm{Aut}(\Sigma/\Sigma^p).$$

Furthermore, Π *cannot be generated by fewer than 6 elements.*

Proof — That the maps defining D, E, F, G, H actually extend to automorphisms of Σ is a routine calculation involving the defining relations (1.4) of Σ and will be omitted.

The stated relations among A, B, C, D, E, F, G, H are easily verified. Moreover, any group generated by elements A through H subject to the given relations has order $\leqslant 2p^{3n-2i+1}(p-1)$.

We claim that $\mathrm{Inn}(\Sigma) \cap \langle D, E, F, G\rangle$ is trivial. Indeed, the defining relations of Σ yield

$$A^j(\mathfrak{c}) = \mathfrak{a}^{-jep}\mathfrak{c},\ B^j(\mathfrak{c}) = \mathfrak{b}^{-jdp}\mathfrak{c},\ A^j(\mathfrak{b}) = \mathfrak{b}\mathfrak{d}^j,$$

$$B^j(\mathfrak{a}) = \mathfrak{a}\mathfrak{d}^{-j}, \quad j \in \mathbb{Z}.$$

A general element of $\mathrm{Inn}(\Sigma)$ (resp. $\langle D, E, F, G\rangle$) has the form $A^jB^kC^m$ (resp. $D^aG^fE^bF^c$) for some $j, k, m \in \mathbb{Z}$ (resp. $a, b, c, f \in \mathbb{Z}$). Suppose that $A^jB^kC^m = D^aG^fE^bF^c$. We wish to show that this common element is trivial. On the one hand, we have

$$(A^jB^kC^m)(\mathfrak{c}) = \mathfrak{b}^{-kdp}\mathfrak{a}^{-jep}\mathfrak{d}^{-jkdp}\mathfrak{c}$$

and on the other hand

$$(D^aG^fE^bF^c)(\mathfrak{c}) = \mathfrak{c}^{(1+p^{n-i-1})^a}.$$

From the normal form of the elements of Σ deduce that $p^{n-i-1} | j$ and $p^{n-i-1} | k$. But then $\mathfrak{d}^{-jkdp} = 1$ and a fortiori

$$\mathfrak{c} = \mathfrak{c}^{(1+p^{n-i-1})^a}.$$

This forces $D^a = 1$. Now

$$(G^fE^bF^c)(\mathfrak{a}) = \mathfrak{a}^{g_0^f}\mathfrak{b}^{h_0^fbp^{n-i-1}},$$

while

$$(A^jB^kC^m)(a) = a^{(1+ep)^m}\mathfrak{d}^{-k(1+ep)^m}.$$

This implies that $p|b$, $p^{n-i}|k$, and $(1+ep)^m \equiv g_0^f \mod p^{n-i}$. The first two conditions yield that $E^b = 1$ and $B^k = 1$. As for the third, since the order of $(1+ep)^m$ modulo p^{n-i} is a p-power and that of g_0^f is a factor of $p-1$, both orders are equal to 1. This forces $G^f = 1$ and $C^m = 1$. Finally, we have $F^c(\mathfrak{b}) = a^{cp^{n-i-1}}\mathfrak{b}$, while $A^j(\mathfrak{b}) = \mathfrak{b}\mathfrak{d}^j$. Thus $p|c$ and $p^{n-i}|j$, whence $F^c = 1$ and $A^j = 1$. This proves the claim.

We show below that (3.1) holds. Since $\langle A, B, C, D, E, F, G\rangle \subseteq \Delta$ and $H \notin \Delta$, we infer

$$\Delta = \mathrm{Inn}(\Sigma) \rtimes \langle D, E, F, G\rangle,\ \mathrm{Aut}(\Sigma) = \Delta \rtimes \langle H\rangle,\ [\mathrm{Aut}(\Sigma) : \Delta] = 2.$$

On the other hand, the very definitions of D, E, F, G yield

$$\langle D, E, F, G\rangle \simeq \mathbb{Z}/p^i\mathbb{Z} \times \big[(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes \mathbb{Z}/(p-1)\mathbb{Z}\big],$$

while Lemma 3.1 gives

$$\mathrm{Inn}(\Sigma) \simeq \Sigma/Z(\Sigma) \simeq (\mathbb{Z}/p^{n-i}\mathbb{Z} \times \mathbb{Z}/p^{n-i}\mathbb{Z}) \rtimes \mathbb{Z}/p^{n-i-1}\mathbb{Z}.$$

Thus $|\mathrm{Aut}(\Sigma)| = 2p^{3n-2i+1}\ (p-1)$, consequently the given relations among A, B, C, D, E, F, G, H must be defining relations, and

$$\mathrm{Aut}(\Sigma) = \langle A, B, C, D, E, F\rangle \rtimes \big(\langle G\rangle \rtimes \langle H\rangle\big)$$

holds. This decomposition of $\mathrm{Aut}(\Sigma)$ yields (3.2), whence the given presentation of $\mathrm{Aut}(\Sigma)$ immediately gives one for $\mathrm{Out}(\Sigma)$.

That Π is a normal Sylow p-subgroup of $\mathrm{Aut}(\Sigma)$ with the stated defining relations follows directly from above. The very definition of A, B, C, D, E, F places them in $\ker\Gamma$. Thus $\ker\Gamma = \Pi$ provided we show that $\ker\Gamma \cap \big(\langle G\rangle \rtimes \langle H\rangle\big)$ is trivial. To this end, let $l \in \mathbb{Z}$ and suppose, if possible, that $G^lH \in \ker\Gamma$. This implies $c^2 \in \Sigma^p$, whence $c \in \Sigma^p$, against Proposition 2.7. Suppose next that $G^l \in \ker\Gamma$. This implies that $a^{g_0{}^l} \in \Sigma^p$, so $a^{g_0{}^l} = a^k$ for some multiple k of p, by Proposition 2.7. The order of this common element is a factor of $p-1$ as well as a p-power, whence this element is 1, which implies $G^l = 1$. This proves that $\ker\Gamma = \Pi$. The defining relations of Π make it clear that $[\Pi, \Pi] \subseteq \Pi^p$, which yields an epimorphism $\Pi \to V$, where V

is 6-dimensional $\mathbb{Z}/p\mathbb{Z}$-vector space. Thus Π cannot be generated by fewer than 6 elements.

We proceed to show (3.1). Let Ω be an arbitrary automorphism of Σ. By Proposition 2.8,

$$\Omega(a) = a^a b^b d^c,\ \Omega(b) = a^f b^j d^k,\ \Omega(c) = a^m b^q c^r, \tag{3.3}$$

where $a, b, c, f, j, k, m, q, r \in \mathbb{N}$. Since Ω is an automorphism, we have

$$\begin{aligned} {}^{\Omega(c)}\Omega(a) &= \Omega({}^c a) = \Omega(a)^{1+ep}, \\ {}^{\Omega(c)}\Omega(b) &= \Omega({}^c b) = \Omega(b)^{1+dp}. \end{aligned} \tag{3.4}$$

Using (3.3) and comparing the a-components of each side of (3.4) yields

$$a^{(1+ep)^r a} = a^{(1+ep)a},\ a^{(1+ep)^r f} = a^{(1+dp)f}. \tag{3.5}$$

By Proposition 2.8, Ω induces an automorphism in $\Psi/Z(\Psi)$. Let $M \in GL_2(\mathbb{Z}/p^{n-i}\mathbb{Z})$ be the matrix of this automorphism with respect to the basis formed by a, b when taken modulo $Z(\Psi)$. Then (3.3) gives

$$M = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{f} & \overline{j} \end{pmatrix},$$

where the bar indicates the passage from $\mathbb{Z}$ to $\mathbb{Z}/p^{n-i}\mathbb{Z}$. Since M is invertible, one of a, f is not divisible by p, whence by (3.5)

$$(1+ep)^r \equiv 1+ep \mod p^{n-i} \quad \text{or} \quad (1+ep)^r \equiv 1+dp \mod p^{n-i}.$$

Thus by (1.2)

$$(1+ep)^{r-1} \equiv 1 \mod p^{n-i} \quad \text{or} \quad (1+ep)^{r+1} \equiv 1 \mod p^{n-i}.$$

Since $p \nmid e$, Lemma 2.4 ensures that $1+ep$ has order p^{n-i-1} modulo p^n, whence

$$r \equiv 1 \mod p^{n-i-1} \quad \text{or} \quad r \equiv -1 \mod p^{n-i-1}.$$

In the second case, we replace Ω by $H\Omega$, so we may assume that the first case occurs. Thus

$$r \equiv 1 \mod p^{n-i-1}. \tag{3.6}$$

Taking into account (1.2), we deduce

$$\begin{aligned}(1+ep)^r &\equiv 1+ep \mod p^{n-i}, \quad \text{and} \\ (1+dp)^r &\equiv 1+dp \mod p^{n-i}.\end{aligned} \tag{3.7}$$

In view of (3.7), the automorphisms that conjugation by c^r and c induce on $\Psi/Z(\Psi)$ are identical. Let N be the matrix of this automorphism relative to the same basis used above. Then

$$N = \begin{pmatrix} \overline{1+ep} & \overline{0} \\ \overline{0} & \overline{1+dp} \end{pmatrix}.$$

Using once more that Ω is an automorphism of Σ, we see that for any $t \in \Psi$, we have

$$^{\Omega(c)}\Omega(t) = \Omega(^c t). \tag{3.8}$$

Since conjugation by c^r and c induce the same automorphism on $\Psi/Z(\Psi)$, (3.3) and (3.8) give $^c\Omega(t)\,Z(\Psi) = \Omega(^c t)\,Z(\Psi)$. In matrix terms, this means that $NM = MN$, which is equivalent to

$$b(e-d)p \equiv 0 \mod p^{n-i},\ f(e-d)p \equiv 0 \mod p^{n-i}. \tag{3.9}$$

It follows from (2.6) and (3.9) that

$$b \equiv 0 \equiv f \mod p^{n-i-1}. \tag{3.10}$$

We now use for the first time the hypothesis $i < n-1$. Since M is invertible, (3.10) implies

$$\overline{a}, \overline{j} \in (\mathbb{Z}/p^{n-i}\mathbb{Z})^\times. \tag{3.11}$$

Using (3.3) and (3.7), and carefully comparing the $\mathfrak{d}$-components of each side of (3.4) gives

$$\begin{aligned}\mathfrak{d}^{-(1+ep)aq}\mathfrak{d}^{(1+dp)bm}\mathfrak{d}^c &= \mathfrak{d}^{-abep(ep+1)/2}\mathfrak{d}^{c(1+ep)}, \\ \mathfrak{d}^{-(1+ep)fq}\mathfrak{d}^{(1+dp)jm}\mathfrak{d}^k &= \mathfrak{d}^{-fjdp(dp+1)/2}\mathfrak{d}^{k(1+dp)}.\end{aligned} \tag{3.12}$$

We claim that

$$q \equiv 0 \equiv m \mod p. \tag{3.13}$$

Indeed, using (3.10), that $n-1 > i$, and that $e(ep+1)$ (resp. $d(dp+1)$) is even, we deduce from the first (resp. second) equality in (3.12) that $\mathfrak{d}^{aq}$ (resp. $\mathfrak{d}^{jm}$) is in $\langle \mathfrak{d}^p \rangle$. Thus (3.11) yields $q \equiv 0 \mod p$ (resp. $m \equiv 0 \mod p$). This proves the claim.

On the other hand, in view of (3.7), we have

$$\mathfrak{a}\mathfrak{c}^r\mathfrak{a}^{-1} = \mathfrak{a}^{-ep}\mathfrak{c}^r, \ \mathfrak{b}\mathfrak{c}^r\mathfrak{b}^{-1} = \mathfrak{b}^{-dp}\mathfrak{c}^r. \tag{3.14}$$

We deduce from (3.3), (3.13), and (3.14) that if we replace Ω by $\delta_s\Omega$, where $\delta_s \in \mathrm{Inn}(\Sigma)$ for a suitable $s \in \Psi$, the following will hold in (3.3):

$$q = 0 = m. \tag{3.15}$$

Making use of (3.6) and replacing Ω by $D^l\Omega$ for a suitable $l \in \mathbb{Z}$, we will have $q = 0 = m$ and $r = 1$ in (3.3), so that

$$\Omega(\mathfrak{c}) = \mathfrak{c}. \tag{3.16}$$

Taking into account that $\mathfrak{d}^{aj-bf} = [\Omega(\mathfrak{a}), \Omega(\mathfrak{b})] = \Omega([\mathfrak{a}, \mathfrak{b}]) = \Omega(\mathfrak{d}) = \mathfrak{d}$, and appealing to (3.10), we infer

$$aj \equiv 1 \mod p^{n-i}. \tag{3.17}$$

Going back to (3.12) and making use of (3.15), we see that

$$\mathfrak{d}^{abep(ep+1)/2} = \mathfrak{d}^{cep}, \ \mathfrak{d}^{fjdp(dp+1)/2} = \mathfrak{d}^{kdp}.$$

But $d(dp+1)$ and $e(ep+1)$ are even, so (3.10) yields

$$\mathfrak{d}^{cep} = 1 = \mathfrak{d}^{kdp}.$$

Since d and e are not divisible by p, we deduce

$$c \equiv 0 \equiv k \mod p^{n-i-1}. \tag{3.18}$$

Now $\mathfrak{a}^{p^{n-i-1}}$ and $\mathfrak{b}^{p^{n-i-1}}$ commute with $\mathfrak{c}$ and with each other, so replacing Ω by $\delta_s\Omega$, where $\delta_s \in \mathrm{Inn}(\Sigma)$ for a suitable $s \in \Psi$, (3.10) and (3.18) imply that (3.16) still holds and we further have $c = 0 = k$ in (3.3).

We next replace Ω by $\delta_s G^l\Omega$, for a suitable $l \in \mathbb{Z}$ and $\delta_s \in \mathrm{Inn}(\Sigma)$, with $s \in \langle \mathfrak{c} \rangle$. This will keep (3.16) and $c = 0 = k$, and, because

of (3.17), will further achieve $a = 1 = j$ in (3.3). Taking into account (3.10), we see that $E^uF^v\Omega = 1$ for suitable $u, v \in \mathbb{Z}$. This proves (3.1), completing the proof of the theorem. □

Proposition 3.3 *Let* $\Lambda : \mathrm{Aut}(\Sigma) \to \mathrm{Aut}(\Psi)$ *be the restriction homomorphism ensured by* Proposition 2.8. *Then* $\ker\Lambda$ *is the cyclic group of order* p^{i-1} *generated by*

$$a \mapsto a,\ b \mapsto b,\ c \mapsto c^{1+p^{n-i}}.$$

Proof — Let $\Omega \in \ker\Lambda$. Then $\Omega(c) = tc^s$, where $t \in \Psi$ and $s \in \mathbb{N}$. Since Ω is the identity on Ψ,

$$a^{1+ep} = \Omega(a^{1+ep}) = \Omega(cac^{-1})$$
$$= \Omega(c)\Omega(a)\Omega(c^{-1}) = tc^sac^{-s}t^{-1} = ta^{(1+ep)^s}t^{-1}.$$

Since conjugation by t sends a to itself times some power of d, this forces

$$(1+ep)^s \equiv (1+ep) \mod p^{n-i},$$

so

$$(1+ep)^{s-1} \equiv 1 \mod p^{n-i}.$$

As $p \nmid e$, Lemma 2.4 yields

$$s \equiv 1 \mod p^{n-i-1}.$$

We also deduce that t must commute with a^{1+ep} and hence with a. A like calculation with b instead of a forces t to commute with b, whence $t \in Z(\Psi) = \langle d \rangle$. Since $d = c^{p^{i-1}}$ and $i-1 \geqslant n-i-1$, we infer $\Omega(c) = c^k$, where $k \equiv 1 \mod p^{n-i-1}$. But Ω must fix d as well, so in fact $k \equiv 1 \mod p^{n-i}$. □

Note that if $i \neq n-1$ then, in the notation of Theorem 3.2, we have $\ker\Lambda = \langle D^p \rangle$.

Theorem 3.4 *Suppose* $i = n-1$, *so that* Σ *be the group of order* p^{n+1} *generated by* a, b, c, *with defining relations*

$$a^p = 1, b^p = 1, c^{p^{n-1}} = 1, [a,b] = c^{p^{n-2}}, ac = ca, bc = cb,$$

and $\Psi \simeq \mathrm{Heis}(\mathbb{Z}/p\mathbb{Z})$ *is the subgroup of* Σ *of order* p^3 *generated by* a, b *and* $c^{p^{n-2}} = d$.

Let $\Lambda : \mathrm{Aut}(\Sigma) \to \mathrm{Aut}(\Psi)$ *be the restriction homomorphism whose existence is ensured by* Proposition 2.8. *Then*

$$\mathrm{Aut}(\Sigma) \simeq \ker\Lambda \times \mathrm{Im}\Lambda,$$

where $\ker\Lambda$ *is a cyclic group of order* p^{n-2} *and* $\mathrm{Im}\Lambda = \mathrm{Aut}(\Psi)$ *is an extension of* $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ *by* $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. *More precisely, let* A, B *be the inner automorphisms of* Σ *associated with* a, b, *respectively. Let* C, D, E, F, G *in* $\mathrm{Aut}(\Sigma)$ *be respectively defined by*

$$a \mapsto a,\ b \mapsto ab,\ c \mapsto c,$$

$$a \mapsto b,\ b \mapsto a^{-1},\ c \mapsto c,$$

$$a \mapsto a^r,\ b \mapsto b^s,\ c \mapsto c,$$

$$a \mapsto a^r,\ b \mapsto b,\ c \mapsto c^r,$$

$$a \mapsto a,\ b \mapsto b,\ c \mapsto c^{1+p},$$

where r *is any integer of order* $p-1$ *modulo* p^{n-1} (*and hence modulo* p), *with inverse* s *modulo* p^{n-1} (*and hence modulo* p), *both of which are taken to be odd* (*as we are allowed to do*), *and further let* $t = r(r-1)/2$. *Then* $\ker\Lambda = \langle G\rangle$ *and* $\mathrm{Aut}(\Sigma)$ *is generated by* A, B, C, D, E, F, G, *with defining relations*

$$A^p = 1, B^p = 1, AB = BA,$$

$$C^p = 1, D^2 = E^{(p-1)/2}, E^{p-1} = 1, F^{p-1} = 1, G^{p^{n-2}} = 1,$$

$$DED^{-1} = E^{-1}, DFD^{-1} = E^{-1}F,$$

$$EF = FE, ECE^{-1} = A^{-t}C^{r^2}, FCF^{-1} = C^r,$$

$$A^{(r^k-1)/2}B^{-(s^k+1)/2}DC^{s^k}D = E^kC^{-s^k}DC^{-r^k}, \quad 0 \leqslant k < p-1,$$

$$CAC^{-1} = A, CBC^{-1} = AB, DAD^{-1} = B, DBD^{-1} = A^{-1},$$

$$EAE^{-1} = A^r, EBE^{-1} = B^s, FAF^{-1} = A^r, FBF^{-1} = B,$$

$$AG = GA, BG = GB, CG = GC, DG = GD, EG = GE, FG = GF.$$

Moreover, $\mathrm{Aut}(\Psi)$ *is generated by the restrictions to* Ψ *of* A *through* F, *say* A_0 *through* F_0, *respectively, with the above defining relations, mutatis mutandi* (*this means that we replace* A *through* F *by* A_0 *through* F_0 *and we*

remove all relations involving G). *Furthermore,*

$$|\mathrm{Aut}(\Sigma)| = p^{n+1}(p-1)^2(p+1),\ |\mathrm{Aut}(\Psi)| = p^3(p-1)^2(p+1).$$

Proof — That the maps defining A through G extend to automorphisms of Σ follows from the defining relations of Σ.

We have $\ker\Lambda = \langle G\rangle$, a group of order p^{n-2}, by Proposition 3.3. Let Z be the subgroup of $\mathrm{Aut}(\Psi)$ generated by A_0 through F_0. We claim that $Z = \mathrm{Aut}(\Psi)$. Indeed, we have a homomorphism

$$\Gamma : \mathrm{Aut}(\Psi) \to \mathrm{Aut}(\Psi/Z(\Psi))$$

whose kernel is easily seen to be $\mathrm{Inn}(\Psi)$. Relative to the basis $\{aZ(\Psi), bZ(\Psi)\}$ of the $\mathbb{Z}/p\mathbb{Z}$-vector space $\Psi/Z(\Psi)$, the matrices of $\Gamma(C_0)$ through $\Gamma(F_0)$ are respectively given by

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix}, \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}.$$

As these matrices generate $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, we see that the restriction of Γ to Z is surjective. Since $\mathrm{Inn}(\Psi) \subset Z$, it follows that $Z = \mathrm{Aut}(\Psi)$. We have shown, in particular, that $\mathrm{Aut}(\Psi)$ is an extension of

$$\ker\Gamma \simeq \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$$

by $\mathrm{Im}\Gamma \simeq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

The verification of the given relations among A through G is a routine calculation and will be omitted. We next show that these are defining relations.

Let P be the abstract group generated by elements A through G subject to the given relations. It suffices to show that

$$|P| \leqslant p^{n+1}(p-1)^2(p+1).$$

In this respect, it is clear that $\langle A, B, G\rangle$ is a normal subgroup of P of order $\leqslant p^n$. Let $Q = P/\langle A, B, G\rangle$ and let c, u, v, f be the images of C, D, E, F, respectively, under the canonical projection $P \to Q$. We further let $N = \langle c, v, f\rangle$. Then v, f commute and normalize $\langle c\rangle$, so $|N| \leqslant p(p-1)^2$. We claim that $Q = N \cup NuN$. This means that

$$Y = N \cup NuN$$

is a subgroup of Q. Now $u^{-1} = u^3 = uu^2$, with $u^2 \in N$, so Y is closed under inversion. That Y is closed under multiplication is respectively equivalent to $NuNuN \subset Y$, $uNu \subset Y$, and $uNu^{-1} \subset Y$. Now u conjugates v, f back into N, and $u\langle c\rangle u \subset Y$ by the given relations, so Y is closed under multiplication. Since $NuN = Nu\langle c\rangle$, we have

$$|NuN| \leqslant |N||\langle c\rangle| = p^2(p-1)^2,$$

and therefore

$$|Q| \leqslant |N| + |NuN| \leqslant p(p-1)^2 + p^2(p-1)^2 = p(p-1)^2(p+1),$$

whence

$$|P| = |\langle A, B, G\rangle||Q| \leqslant p^n p(p-1)^2(p+1) = p^{n+1}(p-1)^2(p+1),$$

as required. This shows that the stated relations are defining relations for $\mathrm{Aut}(\Sigma)$.

Now, F normalizes $\langle A, B, C, D, E\rangle$, every element of this group fixes c, while $F(c) = c^r$ and $G(c) = c^{1+p}$. Since r has order $p-1$ modulo p^{n-1} and $1+p$ has order p^{n-2} modulo p^{n-1} (where p^{n-1} is the order of c), it follows that the intersection of

$$\langle A, B, C, D, E, F\rangle = \langle A, B, C, D, E\rangle \rtimes \langle F\rangle$$

with $\langle G\rangle$ is trivial, so the restriction of Λ to $\langle A, B, C, D, E, F\rangle$ is an isomorphism and, since G is central, we have

$$\mathrm{Aut}(\Sigma) = \langle G\rangle \times \langle A, B, C, D, E, F\rangle.$$

The statement is proved. □

4 The automorphism group of Σ when $2i < n$

We assume throughout this section that $2i < n$.

Lemma 4.1 *The center of* Σ *is generated by* $\mathfrak{d}$ *and* $\mathfrak{b}^{p^{n-i-1}}$.

Proof — Let $z \in Z(\Sigma)$. Then $z = c^r t$, where $t \in \Psi$. The first part of the proof of Lemma 3.1 shows that $t \in Z(\Psi)$, that c^r commutes with $\mathfrak{a}$ and $\mathfrak{b}$, and that $p^{n-i-1} | r$. In this case, $Z(\Psi) = \langle \mathfrak{d}, \mathfrak{b}^{p^i}\rangle$.

As $\mathfrak{d} = \mathfrak{c}^{p^{n-i-1}}$, we infer $Z(\Sigma) \subseteq \langle \mathfrak{b}^{p^i}, \mathfrak{d} \rangle$. Here $\mathfrak{d}$ actually belongs to $Z(\Sigma)$, so $Z(\Sigma) = \langle \mathfrak{b}^{p^j}, \mathfrak{d} \rangle$, where $j \geqslant i$ is large enough so that $\mathfrak{c}$ commutes with $\mathfrak{b}^{p^j}$, that is, $j \geqslant n-i-1$. Since $n-i-1 \geqslant i$, the proof is complete. □

Lemma 4.2 *Let $a, b \in \mathbb{N}$ and $z \in \mathbb{Z}$ be such that*

$$z^{p^a} \equiv 1 \mod p^b. \tag{4.1}$$

Then

$$1 + z + z^2 + \ldots + z^{p^a-1} \equiv p^a \mod p^b.$$

Proof — It follows from (4.1) that $z \equiv 1 \mod p$. Indeed, the order of z modulo p must be a factor of both p^a and $p-1$ (which is the order of $(\mathbb{Z}/p\mathbb{Z})^\times$), so z has order 1 modulo p.

If $z = 1$ the result is obvious. If not, $z = 1 + hp^s$, where $h \in \mathbb{Z}$ not divisible by p and $s \geqslant 1$. Then by Lemma 2.4,

$$z^{p^a} \equiv (1 + hp^s)^{p^a} \equiv 1 + hp^{s+a} \mod p^{2s+a},$$

so for some integer f, we have

$$z^{p^a} = 1 + hp^{s+a} + fp^{2s+a} = 1 + p^{s+a}(h + fp^s).$$

Here $p \nmid (h + fp^s)$, because $s \geqslant 1$. It follows from (4.1) that $b \leqslant s + a$. Now

$$\begin{aligned} 1 + z + z^2 + \ldots + z^{p^a-1} &\equiv (z^{p^a} - 1)/(z-1) \\ &\equiv p^{s+a}(h + fp^s)/hp^s \mod p^b. \end{aligned}$$

Here $z - 1$ divides $z^{p^a} - 1$, so hp^s divides $p^{s+a}(h + fp^s)$. But hp^s also divides hp^{s+a}, so hp^s divides $p^{s+a}fp^s$, that is h divides $p^{s+a}f$. Since h is relatively prime to p, we infer that h divides f. As $b \leqslant s + a$, we conclude that

$$p^{s+a}(h + fp^s)/hp^s \equiv p^a + fp^{s+a}/h \equiv p^a \mod p^b.$$

This completes the proof of the lemma. □

Theorem 4.3 *Let p be an odd prime. Suppose $i, n \in \mathbb{N}$ satisfy $n \geqslant 2$, $1 \leqslant i \leqslant n-1$, and $2i < n$. Let $d, e \in \mathbb{Z}$ be chosen so that* (1.1) *and* (1.2) *hold, and let Σ be the group with presentation* (1.3).

Let $L, M, N \in \mathrm{Inn}(\Sigma)$ *be the inner automorphisms of* Σ *associated with* a, b, c*, respectively. Let* $U, V, W, X, Y, Z \in \mathrm{Aut}(\Sigma)$ *be respectively the defined by*

$$a \mapsto a,\ b \mapsto bc^{p^{n-i-2}},\ c \mapsto a^{-e}c,$$

$$a \mapsto a,\ b \mapsto b^{1+p^{n-i-1}},\ c \mapsto c^{1+p^{n-i-1}},$$

$$a \mapsto ab^{p^{n-i-1}},\ b \mapsto b,\ c \mapsto c,$$

$$a \mapsto a,\ b \mapsto a^{p^{i-1}}b,\ c \mapsto c,$$

$$a \mapsto ac^{p^{n-2}},\ b \mapsto b,\ c \mapsto c,$$

$$a \mapsto a^{g_0},\ b \mapsto b^{h_0},\ c \mapsto c,$$

where g_0 *is any integer of order* $p-1$ *modulo* p^{n-i}*, with inverse* h_0 *modulo* p^{n-i}*. Let* G *be the subgroup of* $\mathrm{Aut}(\Sigma)$ *preserving* Ψ*. Then*

$$G = \langle L, M, N, V, W, X, Y, Z\rangle \tag{4.2}$$

and

$$\mathrm{Aut}(\Sigma) = G\langle U\rangle = \langle U\rangle G.$$

Proof — Let $\Omega \in \mathrm{Aut}(\Sigma)$. Since $a^{p^i} = 1$, Proposition 2.8 ensures that $\Omega(a) \in \Psi$, so $\Omega(a) = PQR$ for some $P \in \langle a\rangle$, $Q \in \langle b\rangle$, and $R \in \langle d\rangle$. Now the order of b is p^{n-i}, with $n-i > i$, but equation (2.5) from Proposition 2.8 still gives $\Omega(b) = t_0c_0$, where $t_0 \in \Psi$ and $c_0 \in \langle c^{p^{n-i-2}}\rangle$. Using the normal form of elements of Ψ, it follows that

$$\Omega(b) = ABc^{sp^{n-i-2}}$$

for some $A \in \langle a\rangle$, $B \in \langle b\rangle$, and $s \in \mathbb{N}$. As $\Omega(c) \in \Sigma$, we have

$$\Omega(c) = CDc^r$$

for some $C \in \langle a\rangle$, $D \in \langle b\rangle$, and $r \in \mathbb{N}$. Thus

$$\Omega(b) = ABc^{sp^{n-i-2}},\ \Omega(a) = PQR,\ \Omega(c) = CDc^r. \tag{4.3}$$

Since $\Omega(b), \Omega(a), \Omega(c)$ must generate Σ, we see that $p \nmid r$.

Claim 1. $Q \in \langle b^{p^{n-2i}}\rangle$.

Since $1 = \Omega(a^{p^i}) = (PQR)^{p^i} = P^{p^i}Q^{p^i}R^u$, $u \in \mathbb{Z}$, and the order of b is p^{n-i}, the result follows.

Claim 2. P generates $\langle a\rangle$, B generates $\langle b\rangle$ and $\Omega(d)$ generates $\langle d\rangle$.

Set $f = p^{n-i-2}s$. We then have

$$\Omega(d) = \Omega([a,b]) = [\Omega(a),\Omega(b)] = [PQR, ABc^f].$$

Here

$$\begin{aligned}[PQR, ABc^f] &= [PQR, A]\cdot {}^{A}[PQR, Bc^f]\\ &= [PQR, A]\cdot {}^{A}[PQR, B]\cdot {}^{AB}[PQR, c^f],\end{aligned}$$

where

$$[PQR, A]\cdot {}^{A}[PQR, B] = [Q, A][P, B],$$

$$[c^f, PQR] = [c^f, P]\cdot {}^{P}[c^f, QR] = [c^f, P]\cdot {}^{P}[c^f, Q].$$

Using Lemma 2.4, $P^{p^i} = 1$, and $n-i-1 \geqslant i$, we see that

$$[c^f, P] = P^{(1+ep)^f}P^{-1} = P^{1+sep^{n-i-1}}P^{-1} = 1.$$

Moreover, by Claim 1, $Q^{p^i} = 1$. Using again Lemma 2.4 and the fact that $n-i-1 \geqslant i$, we obtain

$$[c^f, Q] = Q^{(1+dp)^f}Q^{-1} = Q^{1+sdp^{n-i-1}}Q^{-1} = 1.$$

Therefore,

$$\Omega(d) = [PQR, ABc^f] = [Q, A][P, B] \in \langle d\rangle.$$

This shows that $\langle d\rangle$ is a characteristic subgroup of Σ, whence $\Omega(d)$ generates $\langle d\rangle$. In particular, $[Q, A][P, B]$ has order p^i. But $Q \in \langle b^{p^{n-2i}}\rangle$ by Claim 1, so

$$[Q, A] \in \langle d^{p^{n-2i}}\rangle$$

has order $< p^i$. Since $[P, B]$ commutes with $[Q, A]$, it follows that $[P, B]$ has order p^i. Thus $\langle P\rangle = \langle a\rangle$ and $\langle B\rangle = \langle b\rangle$.

Claim 3. $r \equiv 1 \mod p^{n-i-1}$.

We have ${}^{\Omega(c)}\Omega(b) = \Omega(b)^{1+dp}$. Setting $f = p^{n-i-2}s$, this translates into

$${}^{CDc^r}(ABc^f) = (ABc^f)^{1+dp}.$$

The b-component of the left hand side is equal to $B^{(1+dp)^r}$. As for the b-component of the right hand side, we have

$$(ABc^f)^p = ABA^{(1+ep)^f}B^{(1+dp)^f}\dots A^{(1+ep)^{f(p-1)}}B^{(1+dp)^{f(p-1)}}d^s.$$

Using Lemma 4.2 with $z = (1+dp)^f$, $a = 1$ and $b = n-i$ we see that the b-component of $(ABc^f)^p$ is B^p and that the a-component of $(ABc^f)^p$ is A^p. Reordering the factors, it follows that

$$(ABc^f)^p = A^p B^p d^u, \quad u \in \mathbb{Z}.$$

Thus

$$(ABc^f)^{dp} = A^{pd} B^{pd} d^q, \quad q \in \mathbb{Z}.$$

so

$$(ABc^f)^{1+dp} = (ABc^f)(ABc^f)^{dp} = ABc^f A^{pd} B^{pd} d^q,$$

and therefore

$$(ABc^f)^{1+dp} = AA^{(1+ep)^f pd} BB^{(1+dp)^f pd} c^f d^l, \quad l \in \mathbb{Z}.$$

Now by Lemma 2.4,

$$(1+dp)^f pd \equiv pd \mod p^{n-i},$$

so the b-component of $(ABc^f)^{1+dp}$ is B^{1+dp}. All in all, we deduce

$$B^{(1+dp)^r} = B^{1+dp}.$$

Since B has order p^{n-i} by Claim 2, we infer from $p \nmid d$ and Lemma 2.4 that

$$r \equiv 1 \mod p^{n-i-1}.$$

Claim 4. The map defining U extends to an automorphism of Σ.

It is clear that the images of c, a, b generate Σ. We need to verify that the defining relations of Σ are preserved. We proceed to do this, labeling each step with the corresponding relation of Σ.

- $b^{p^{n-i}} = 1$. Set $f = p^{n-i-2}$ and $z = (1+dp)^f$. Then

$$(bc^f)^p = b^u d,$$

where

$$u = 1 + z + \ldots + z^{p-1} \mod p^{n-i}.$$

But $z^p \equiv 1 \mod p^{n-i}$, so Lemma 4.2 implies $u \equiv p \mod p^{n-1}$, whence

$$(bc^f)^p = b^p d. \tag{4.4}$$

This element has order p^{n-i-1}, since the factors commute, d has order p^i, and $n-i-1 \geqslant i$.

- $a^{p^i} = 1$. This step is clear.
- $[a,b] = c^{p^{n-i-1}}$. We need to verify that

$$\left[a, bc^{p^{n-i-2}}\right] = (a^{-e}c)^{p^{n-i-1}}.$$

On the one hand, we have

$$\left[a, bc^{p^{n-i-2}}\right] = [a,b] \cdot {}^b\left[a, c^{p^{n-i-2}}\right] = [a,b] = c^{p^{n-i-1}},$$

because $c^{p^{n-i-2}}$ commutes with a, since $(1+ep)^{p^{n-i-2}} \equiv 1 + ep^{n-i-1} \bmod p^{n-i}$, $n-i-1 \geqslant i$, and a has order p^i. On the other hand,

$$(a^{-e}c)^{p^{n-i-1}} = c^{p^{n-i-1}} \tag{4.5}$$

applying Lemma 4.2 with $z = 1+ep$, $a = n-i-1$, and $b = n-i$, and using $n-i-1 \geqslant i$.

- $c^{p^{n-1}} = 1$. This step follows from (4.5).
- ${}^c a = a^{1+ep}$. This step is clear because a^{-e} commutes with a.
- ${}^c b = b^{1+dp}$. Set $f = p^{n-i-2}$. We need to verify that

$${}^{a^{-e}c}(bc^f) = (bc^f)^{1+dp}. \tag{4.6}$$

Using (4.4) and the fact that d is central in Σ, we have

$$(bc^f)^{dp} = b^{dp}d^d,$$

so

$$(bc^f)^{1+dp} = (bc^f)(bc^f)^{dp} = bc^f b^{dp} d^d.$$

Here c^f and b^{dp} commute, since $dp(1+dp)^{p^{n-i-2}} \equiv dp \mod p^{n-i}$ by Lemma 2.4. Thus

$$(bc^f)^{1+dp} = b^{1+dp} c^f d^d.$$

On the other hand, since $n-i-1 \geqslant i$, c^f commutes with a, so

$${}^{a^{-e}c}(bc^f) = {}^{a^{-e}}(b^{1+dp}c^f) = b^{1+dp} d^{-e(1+dp)} c^f.$$

Now from $(1+dp)(1+ep) \equiv 1 \mod p^n$ we infer $e+d+edp \equiv 0 \mod p^{n-1}$, so $d \equiv -e(1+dp) \equiv p^i$. This completes the proof of Claim 4.

Recall that $\langle B\rangle = \mathfrak{b}$ by Claim 2. Using (4.3), we see that $U^l\Omega$ preserves Ψ for a suitable l. This proves that $\mathrm{Aut}(\Sigma) = \langle U\rangle G$. Since this is a subgroup, it follows that $\langle U\rangle G = G\langle U\rangle$.

We proceed to prove (4.2). The verification that the maps defining V, W, X, Y, Z extend to automorphisms of Σ is routine and will be omitted.

Let $\Omega \in G$. Then

$$\Omega(\mathfrak{b}) = ABS,\ \Omega(\mathfrak{a}) = PQR,\ \Omega(\mathfrak{c}) = CD\mathfrak{c}^r. \tag{4.7}$$

Here $A, P, C \in \langle\mathfrak{a}\rangle$, $B, Q, D \in \langle\mathfrak{b}\rangle$, and $R, S \in \langle\mathfrak{d}\rangle$. We know from Claim 3 that $r \equiv 1 \mod p^{n-i-1}$. Thus, replacing Ω by $V^j\Omega$ for a suitable j, we will have $r = 1$ in (4.7).

For any $t \in \Psi$, we have

$${}^{\Omega(\mathfrak{c})}\Omega(t) = \Omega({}^{\mathfrak{c}}t).$$

Taking $t = \mathfrak{a}$, we get

$$\begin{aligned} {}^{(CD\mathfrak{c})}PQR &= {}^{\Omega(\mathfrak{c})}\Omega(\mathfrak{a}) = \Omega({}^{\mathfrak{c}}\mathfrak{a}) \\ &= \Omega(\mathfrak{a}^{1+ep}) = \Omega(\mathfrak{a})^{1+ep} = (PQR)^{1+ep}. \end{aligned} \tag{4.8}$$

Comparing the $\mathfrak{b}$-components in (4.8), we see that

$$Q^{1+dp} = Q^{1+ep}.$$

It follows from (2.6) that $Q^p = 1$ and therefore

$$Q \in \left\langle \mathfrak{b}^{p^{n-i-1}} \right\rangle. \tag{4.9}$$

Comparing the $\mathfrak{d}$-components in (4.8), we find that

$$[C,Q]^{1+dp}[D,P]^{1+ep}R = [Q,P][Q,P]^2 \dots [Q,P]^{ep}R^{1+ep}. \tag{4.10}$$

This implies that

$$[C,Q][D,P] \in \langle\mathfrak{d}^p\rangle.$$

Now $n-i-1 \geqslant 1$ because $2i < n$, so (4.9) implies $[C,Q] \in \langle\mathfrak{d}^p\rangle$,

whence $[D, P] \in \langle \mathfrak{d}^p \rangle$. Since P generates $\langle \mathfrak{a} \rangle$, we infer

$$D \in \langle \mathfrak{b}^p \rangle. \tag{4.11}$$

Likewise, taking $t = \mathfrak{b}$, we must have

$$\begin{aligned} {}^{(CD\mathfrak{c})}ABS &= {}^{\Omega(\mathfrak{c})}\Omega(\mathfrak{b}) = \Omega({}^{\mathfrak{c}}\mathfrak{b}) = \Omega(\mathfrak{b}^{1+dp}) \\ &= \Omega(\mathfrak{b})^{1+dp} = (ABS)^{1+dp}. \end{aligned} \tag{4.12}$$

Comparing the $\mathfrak{a}$-components in (4.12), we see that

$$A^{1+ep} = A^{1+dp}.$$

Since $d \not\equiv e \mod p$, this forces $A^p = 1$, whence

$$A \in \left\langle \mathfrak{a}^{p^{i-1}} \right\rangle. \tag{4.13}$$

Comparing the $\mathfrak{d}$-components in (4.12), we see that

$$[C, B]^{1+dp}[D, A]^{1+ep}S = [B, A][B, A]^2 \dots [B, A]^{dp} S^{1+dp}. \tag{4.14}$$

Thus $[C, B][D, A] \in \langle \mathfrak{d}^p \rangle$. In view of (4.11), we have $[D, A] \in \langle \mathfrak{d}^p \rangle$. Since B generates $\langle \mathfrak{b} \rangle$, we infer

$$C \in \langle \mathfrak{a}^p \rangle. \tag{4.15}$$

Making use of (4.11) and (4.15) we see that if we replace Ω by $\delta_s\Omega$, where $\delta_s \in \mathrm{Inn}(\Sigma)$ for a suitable $s \in \Psi$, we will have $C = 1 = D$ in (4.7). Since $r \equiv 1 \mod p^{n-i-1}$, a further replacement of Ω by $V^l\Omega$ for a suitable l will maintain $C = 1 = D$ and ensure $r = 1$ in (4.7). We then have

$$\begin{aligned} \mathfrak{d} &= \Omega(\mathfrak{d}) = \Omega([\mathfrak{a}, \mathfrak{b}]) \\ &= [PQR, ABS] = [P, B][Q, A] = [P, B]. \end{aligned} \tag{4.16}$$

Here $[Q, A] = 1$ because (4.9) and (4.13) ensure that

$$[Q, A] \in \langle \mathfrak{c}^{p^{(n-i-1)+(n-i-1)+(i-1)}} \rangle,$$

and $n - i - 1 \geqslant 1$ as just noted above. On the other hand, we have

$$P = \mathfrak{a}^a, \ B = \mathfrak{b}^j,$$

where a, j are relatively prime to p by Claim 2. By virtue of (4.16) we obtain the sharper statement

$$aj \equiv 1 \mod p^i. \tag{4.17}$$

Going back to (4.14) with $C = 1 = D$ and using $A \in \langle a^{p^{i-1}} \rangle$, we deduce $S^{dp} = 1$ and hence

$$S \in \langle \mathfrak{d}^{p^{i-1}} \rangle.$$

Since $a^{p^{i-1}}$ commutes with c, replacing Ω by $\delta_s\Omega$, where $\delta_s \in \mathrm{Inn}(\Sigma)$ for a suitable $s \in \langle a \rangle$, we obtain $S = 1$ in (4.7).

We next go back to (4.10) with $C = 1 = D$. Using $Q \in \langle b^{p^{n-i-1}} \rangle$, we infer $R^{ep} = 1$ and therefore

$$R \in \langle \mathfrak{d}^{p^{i-1}} \rangle. \tag{4.18}$$

We next replace Ω by $\delta_s Z^l \Omega$, $\delta_s \in \mathrm{Inn}(\Sigma)$, for suitable $l \in \mathbb{Z}$ and $s \in \langle c \rangle$. This will keep $C = 1 = D$ as well as $r = 1$; moreover, because of (4.17), we get $P = a$ and $B = b$ in (4.7). Taking into account (4.9), (4.13), and (4.18), we see that $W^a X^b Y^c \Omega = 1$ for suitable a, b, c. This proves (3.1), and completes the proof of the theorem. □

Theorem 4.4 *Keep the hypotheses and notation of* Theorem 4.3, *and take* h_0 *odd. Then*

$$|\mathrm{Aut}(\Sigma)| = p^{2n+2}(p-1), [\mathrm{Aut}(\Sigma) : G] = p;$$

$$\begin{gathered} \mathrm{Inn}(\Sigma) = \langle L, M, N \rangle \simeq \\ (\mathbb{Z}/p^i\mathbb{Z} \times \mathbb{Z}/p^{n-i-1}\mathbb{Z}) \rtimes \mathbb{Z}/p^{n-i-1}\mathbb{Z}; \end{gathered} \tag{4.19}$$

$$\begin{gathered} G/\langle L, M, N \rangle \simeq \\ \mathbb{Z}/p^i\mathbb{Z} \times \big[(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes \mathbb{Z}/(p-1)\mathbb{Z}\big], \end{gathered} \tag{4.20}$$

with

$$\begin{gathered} G = \langle L, M, N \rangle \rtimes \langle V, W, X, Y, Z \rangle \text{ if } i > 1; \\ \Phi = \langle L, M, N, V, W, X, Y \rangle \end{gathered} \tag{4.21}$$

is the kernel of the natural homomorphism $\Gamma : \mathrm{Aut}(\Sigma) \to \mathrm{Aut}(\Sigma/\Sigma^p)$, *and*

hence a normal subgroup of $\mathrm{Aut}(\Sigma)$*;*

$$\Pi = \langle L, M, N, U, V, W, X, Y\rangle = \langle M, N, U, V, W, X, Y\rangle = \Phi\langle U\rangle$$

is a normal Sylow p*-subgroup of* $\mathrm{Aut}(\Sigma)$*;*

$$\mathrm{Aut}(\Sigma) = \Pi \rtimes \langle Z\rangle = \Phi\langle U\rangle \rtimes \langle Z\rangle = \langle M, N, U, V, W, X, Y, Z\rangle.$$

Moreover, the following relations hold:

$$L^{p^i} = 1, M^{p^{n-i-1}} = 1, N^{p^{n-i-1}} = 1, {}^N L = L^{1+ep}, {}^N M = M^{1+dp},$$

$$LM = ML, U^p = L, V^{p^i} = 1, W^p = 1, X^p = 1, Y^p = 1, Z^{p-1} = 1,$$

$$VW = WV, VY = YV, VZ = ZV, VX = XV,$$

$${}^Z L = L^{g_0}, {}^Z M = h^{g_0}, ZN = NZ, {}^Y L = L, {}^Y M = M, YN = NY,$$

$${}^X L = L, {}^X M = L^{p^{i-1}} M, XN = NX, {}^W L = L, {}^W M = M, WN = NW,$$

$${}^V L = L, {}^V M = M, {}^V N = N, {}^U L = L, {}^U M = MN^{p^{n-i-2}}, {}^U N = L^{-e} N,$$

$$WX = XW, {}^Y X = X \text{ if } i > 1, {}^Y X = LX \text{ if } i = 1, WY = YW,$$

$${}^Z W = W^{h_0^2}, {}^Z X = X^{g_0^2}, {}^Z Y = Y^{h_0},$$

as well as the following relations, subject to the indicated conditions:

$${}^U Y = V^{ep^{i-1}} Y (i > 1), {}^U Y = N^{p^{n-3}} V^e Y (i = 1, n > 3),$$

$${}^U W = M^{p^{n-i-2}} W (n > 2i+1), {}^U V = V (n > 2i+1),$$

$${}^U X = X (n > 2i+1), {}^U Z = ZN^{p^{n-i-2}(h_0-1)/2} U^{h_0-1} (n > 2i+1).$$

Furthermore, suppose that $n \neq 2i+1$*. Then the above are defining relations for* $\mathrm{Aut}(\Sigma)$*, as well as for* Π*, once all relations involving* Z *are removed;* Π *cannot be generated by fewer than 7 elements;* G *is not a normal subgroup of* $\mathrm{Aut}(\Sigma)$*.*

Proof — The verification of the stated relations is a routine calculation that will be omitted. We do mention, in connection with the relations involving conjugation by U, that U satisfies

$$a \mapsto a,\ ba^{-ep^{n-i-2}} c^{-p^{n-i-2}} \mapsto b,\ a^e c \mapsto c,$$

so U^{-1} is given by

$$a \mapsto a,\ b \mapsto ba^{-ep^{n-i-2}}c^{-p^{n-i-2}},\ c \mapsto a^e c.$$

It should be noted that if $n > 2i+1$ then U^{-1} satisfies $b \mapsto bc^{-p^{n-i-2}}$.

We claim that G has index p in $\mathrm{Aut}(\Sigma)$. Indeed, the definition of U implies $U \notin G$. Thus, our relations $U^p = L$ and $L^{p^i} = 1$ imply that $\langle U\rangle$ is p-group satisfying $U \notin G$ but $U^p \in G$, which yields $G \cap \langle U\rangle = \langle U^p\rangle$. On the other hand, we have $\mathrm{Aut}(\Sigma) = G\langle U\rangle$ by Theorem 4.3, and therefore

$$[\mathrm{Aut}(\Sigma) : G] = [\langle U\rangle : G \cap \langle U\rangle] = [\langle U\rangle : \langle U^p\rangle] = p.$$

This proves the claim. Thus $|\mathrm{Aut}(\Sigma)| = p^{2n+2}(p-1)$ is equivalent to $|G| = p^{2n+1}(p-1)$, which follows immediately from (4.19) and (4.20). Now (4.19) is a consequence of Lemma 4.1, and we proceed to prove (4.20). Our relations yield an epimorphism

$$\begin{aligned}\mathbb{Z}/p^i\mathbb{Z} \times \left[(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes \mathbb{Z}/(p-1)\mathbb{Z}\right]\\ \to G/\langle L, M, N\rangle \simeq \langle \overline{V}, \overline{W}, \overline{X}, \overline{Y}, \overline{Z}\rangle,\end{aligned}$$

and we need to see that this is injective. This is equivalent to the following: if $v \in \langle V\rangle$, $w \in \langle W\rangle$, $x \in \langle X\rangle$, $y \in \langle Y\rangle$, $z \in \langle Z\rangle$, and $u = vwxyz \in \mathrm{Inn}(\Sigma)$ then

$$v = w = x = y = z = 1.$$

Suppose then that such u is an inner automorphism of Σ, associated to an element t of Σ. Successively applying u to c, b, and a, we see that $v = 1$, $x = 1 = z$, and $w = 1$. Thus

$$u = y = Y^l$$

for some l. Hence $t = a^i b^j c^k$ must commute with b and c. As t commutes with c, we infer $\nu_p(j) \geqslant n-i-1$. But $b^{p^{n-i-1}} \in Z(\Sigma)$ by Lemma 4.1, and we may assume that $t = a^i c^k$. Since t commutes with b, we deduce

$$\nu_p(k) \geqslant n-i-1.$$

But $c^{p^{n-i-1}} = d \in Z(\Sigma)$, so we may assume that $t = a^i$. Thus $u(a) = a$ and $u(a) = ac^{lp^{n-2}}$, whence $\nu_p(l) \geqslant 1$ and therefore $y = 1$, as re-

quired. This proves (4.20). Note that if $i > 1$ our relations show that

$$\langle V, W, X, Y, Z\rangle = \langle V\rangle \times \big[(\langle W\rangle \times \langle X\rangle \times \langle Y\rangle) \rtimes \langle Z\rangle\big],$$

and the above argument then proves that $\langle V, W, X, Y, Z\rangle \cap \langle L, M, N\rangle$ is trivial, whence (4.21) holds.

By (4.19) and (4.20), Φ has order p^{2n+1}, so it is normal in a Sylow p-subgroup of $\mathrm{Aut}(\Sigma)$ (having index p there). But Φ is also normalized by Z, so Φ is normal in $\mathrm{Aut}(\Sigma)$. It is in fact the kernel of Γ, being clearly included there, and using the fact that the index $[\mathrm{Aut}(\Sigma) : \ker\Gamma]$ is divisible by p and $p-1$ (look at U and Z). On the other hand, Sylow's theorem implies that Π is normal in $\mathrm{Aut}(\Sigma)$ (the only positive integer that is a factor of $p-1$ and is congruent to 1 modulo p is 1).

Suppose next that $n \neq 2i+1$. An abstract group generated by elements $L, M, N, U, V, W, X, Y, Z$ satisfying the stated relations is easily seen to have order $\leqslant p^{2n+2}(p-1)$. This implies that the stated relations are defining relations for $\mathrm{Aut}(\Sigma)$. A similar argument applies to Π.

The given relations allow us to define an epimorphism $\Pi \to B$, where B is a 7-dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$, so Π cannot be generated by fewer than 7 elements.

The last stated relation implies $UZU^{-1} \notin G$, as $Z, N \in G$ but $U \notin G$ and $h_0 \not\equiv 1 \mod p$. □

5 Appendix. The automorphism group of Υ

Lemma 5.1 *If $s \in \mathbb{N}$, $r \in \mathbb{Z}$, where $r \neq 0$ and $\nu_p(r) \geqslant 1$, then*

$$\nu_p\left((1+r)^s - 1\right) = \nu_p(r) + \nu_p(s).$$

Proof — We have $r = \ell p^a$ and $s = cp^b$, where $a, b, c, \ell \in \mathbb{Z}$, $a, c \geqslant 1$, $b \geqslant 0$, $p \nmid c$ and $p \nmid \ell$. According to Lemma 2.4, there is some $k \in \mathbb{Z}$ such that

$$(1+r)^s - 1 = c\ell p^{a+b} + kp^{2a+b} = p^{a+b}(c\ell + kp^a).$$

Since $c\ell$ is relatively prime to p, we infer

$$\nu_p\big((1+r)^s - 1\big) = a + b = \nu_p(r) + \nu_p(s).$$

The statement is proved. □

Lemma 5.2 *Let* $a, b \geqslant 1$. *Then the order of the element* $z = x^a y^b$ *of* Υ *is* p^s, *where*

$$s = \max\{n - \nu_p(a), n - i - \nu_p(b), 0\}.$$

In particular, the order of z *is* p^n *if and only if* $p \nmid a$.

Proof — Given $m \geqslant 1$, we have $z^m = x^k y^\ell$, where

$$k = a\frac{(1+p^i)^{bm} - 1}{(1+p^i)^b - 1} \quad \text{and} \quad \ell = bm.$$

By Lemma 5.1, we have

$$\nu_p\left(\frac{(1+p^i)^{bm} - 1}{(1+p^i)^b - 1}\right) = \nu_p(m),$$

so the smallest m such that $x^k = 1$ is $m = 1$ if $\nu_p(a) \geqslant n$ and $m = p^{n-\nu_p(a)}$ otherwise. On the other hand, the smallest m such that $y^\ell = 1$ is $m = 1$ if $\nu_p(b) \geqslant n - i$ and $m = p^{n-i-\nu_p(b)}$ otherwise. □

Lemma 5.3 *Let* $a, b \geqslant 1$, *where* $p \nmid a$, *and set* $z = x^a y^b \in \Upsilon$. *Then* $\langle z\rangle$ *is a normal subgroup of* Υ *if and only if* $x^{p^i} \in \langle z\rangle$. *Equivalently,* $\langle z\rangle$ *is normal if and only if* $\nu_p(b) \geqslant n - 2i$.

Proof — Since y and z generate Υ, it follows that $\langle z\rangle$ is normal if and only if $yzy^{-1} \in \langle z\rangle$, which translates as $x^{a(1+p^i)}y^b \in \langle z\rangle$ or, alternatively, $x^{ap^i}z \in \langle z\rangle$, that is, $x^{ap^i} \in \langle z\rangle$, where x^{p^i} is a power of x^{ap^i}.

Suppose next $\langle z\rangle$ is normal. Then, by above, $x^{p^i} = z^m$ for some $m \geqslant 1$. Now $z^m = x^k y^\ell$, where k, ℓ are as in the proof of Lemma 5.2. Since $\nu_p(p^i) = i$, it follows that $\nu_p(m) = i$. As $y^\ell = 1$, we infer that $\nu_p(b) \geqslant n - 2i$.

Assume conversely that $\nu_p(b) \geqslant n - 2i$. Set $m = p^i$. Then $z^m = x^k y^\ell$, where k, ℓ are as in the proof of Lemma 5.2, so that $\nu_p(k) = i$. Since $y^{p^{n-i}} = 1$ and $\nu_p(b) \geqslant n - 2i$, we have that $y^\ell = 1$. All in all, $z^m = x^{cp^i}$, where $p \nmid c$. Since $x^{p^i} \in \langle x^{cp^i}\rangle$, we deduce that x^{p^i} belongs to $\langle z\rangle$. □

Lemma 5.4 *The assignment*

$$y \mapsto y,\ x \mapsto \begin{cases} xy^{p^{n-2i}} & \text{if } 2i \leqslant n, \\ xy & \text{if } 2i \geqslant n, \end{cases} \tag{5.1}$$

extends to an automorphism, say α, of Υ having order p^i if $2i \leqslant n$ and p^{n-i} if $2i \geqslant n$.

Proof — Set $m = 1 + p^i$ as well as $b = p^{n-2i}$ if $2i \leqslant n$, and $b = 1$ if $2i \geqslant n$. Taking into account Lemma 5.2, it suffices to verify that

$$y(xy^b)y^{-1} = (xy^b)^m.$$

On the one hand, we have $y(xy^b)y^{-1} = x^m y^b$, and on the other $(xy^b)^m = x^k y^\ell$, where

$$k = 1 + m^b + m^{2b} + \ldots + m^{p^i b} \quad \text{and} \quad \ell = bm.$$

Since $y^{p^{n-i}} = 1$, it follows that $y^\ell = y^b$. Set $j = n - i$ if $2i \leqslant n$ and $j = i$ if $2i \geqslant n$. Then Lemma 2.4 yields

$$k \equiv 1 + p^i + p^j(1 + 2 + \ldots + p^i) \equiv 1 + p^i + p^j p^i(p^i + 1)/2 \mod p^n.$$

Since $i + j \geqslant n$ and p is odd, it follows that $k \equiv 1 + p^i \mod p^n$, as required. □

Since $\mathrm{Aut}(C_{p^n})$ is abelian, it is clear that Υ is a normal subgroup of the holomorph of C_{p^n}, namely the semidirect product

$$\mathrm{Hol}(C_{p^n}) = C_{p^n} \rtimes \mathrm{Aut}(C_{p^n})$$

of C_{p^n} by its full automorphism group. Thus, for any integer r relatively prime to p there is an automorphism, say Ω_r, of Υ defined by

$$x \mapsto x^r,\ y \mapsto y, \tag{5.2}$$

namely the restriction to Υ of a suitable inner automorphism of $C_{p^n} \rtimes \mathrm{Aut}(C_{p^n})$.

We proceed to select integers g, h, t, d and e for further use within this section. It is well known that the group of units $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is

cyclic and we fix throughout

$$\text{an integer } g \text{ that has order } p^{n-1}(p-1) \text{ modulo } p^n. \tag{5.3}$$

We accordingly set

$$\beta = \Omega_g, \tag{5.4}$$

and let h be an odd positive integer satisfying

$$gh \equiv 1 \mod p^n. \tag{5.5}$$

By Lemma 2.4, $1+p^i$ has order p^{n-i} modulo p^n. Since $g^{p^{i-1}(p-1)}$ also has order p^{n-i} modulo p^n, there is an integer t, relatively prime to p, such that

$$g^{p^{i-1}(p-1)t} \equiv 1+p^i \mod p^n. \tag{5.6}$$

Thus

$$\beta^{p^{i-1}(p-1)t} = \delta_y. \tag{5.7}$$

Now $g^{(p-1)t}$ and $h^{(p-1)t}$ have order p^{n-1} modulo p^n, so there exist integers d and e satisfying

$$g^{(p-1)t} = 1+dp, h^{(p-1)t} = 1+ep \tag{5.8}$$

as well as (1.1) and (1.2).

Proposition 5.5 *We have* $\mathrm{Aut}(\Upsilon) = \mathrm{Inn}(\Upsilon)\langle\alpha,\beta\rangle$.

Proof — Let $\gamma \in \mathrm{Aut}(\Upsilon)$. By Lemma 5.2, we have $\gamma(x) = x^a y^b$, where $p \nmid a$. Thus $\beta^r\gamma(x) = xy^b$ for some r. As $\langle x\rangle$ is normal in Υ, it follows from Lemmas 5.3 and 5.4 that $\alpha^s\beta^r\gamma(x) = x$ for some s. Since $\alpha^s\beta^r\gamma$ must preserve the relation $yxy^{-1} = x^{1+p^i}$, we see that

$$\alpha^s\beta^r\gamma(y) = x^c y$$

for some c. Here Lemma 5.2 implies that $v_p(c) \geqslant i$, so there is an integer t such that $\delta_x^t\alpha^s\beta^r\gamma$ fixes x and y. Since $\mathrm{Inn}(\Upsilon)$ is normal in $\mathrm{Aut}(\Upsilon)$, we infer that $\gamma \in \mathrm{Inn}(\Upsilon)\langle\alpha,\beta\rangle$. □

Lemma 5.6 *Let* r *be any integer relatively prime to* p, *and let* s *be any odd positive integer satisfying*

$$rs \equiv 1 \mod p^n,$$

whose existence is guaranteed by the fact that p^n *is odd. Let* $\gamma = \Omega_r$ *in* $\mathrm{Aut}(\Upsilon)$*, as defined in* (5.2)*, and set*

$$f = \begin{cases} p^{n-2i}(s-1)/2 & \text{if } 2i \leqslant n, \\ (s-1)/2 & \text{if } 2i \geqslant n. \end{cases}$$

Then $\gamma\alpha\gamma^{-1} = \delta_y^f \alpha^s$.

Proof — Set

$$j = \begin{cases} i & \text{if } 2i \leqslant n, \\ n-i & \text{if } 2i \geqslant n, \end{cases} \quad \text{and} \quad \ell = \begin{cases} p^{n-2i} & \text{if } 2i \leqslant n, \\ 1 & \text{if } 2i \geqslant n. \end{cases}$$

We then have $\gamma\alpha\gamma^{-1}(x) = \gamma\alpha(x^s) = \gamma(xy^\ell)^s = x^{rk}y^{\ell s}$, where

$$k = 1 + (1+p^i)^\ell + \ldots + (1+p^i)^{\ell(s-1)}.$$

Here Lemma 2.4 yields

$$\begin{aligned} rk &\equiv r\big[s + p^{n-j}(1+2+\ldots+(s-1))\big] \\ &\equiv 1 + p^{n-j}rs(s-1)/2 \equiv 1 + p^{n-j}(s-1)/2 \mod p^n. \end{aligned}$$

On the other hand, we have

$$\delta_y^f \alpha^s(x) = \delta_y^f(xy^{\ell s}) = \delta_y^f(x)y^{\ell s} = x^{(1+p^i)^f}y^{\ell s},$$

where, according to Lemma 2.4,

$$(1+p^i)^f \equiv 1 + p^{n-j}(s-1)/2 \mod p^n.$$

The statement is proved. □

Recalling the meanings of β and h from (5.4) and (5.5), respectively, Lemma 5.6 ensures that if $2i \leqslant n$, then

$$\beta\alpha\beta^{-1} = \delta_y^{p^{n-2i}(h-1)/2}\alpha^h, \tag{5.9}$$

while if $2i \geqslant n$ then

$$\beta\alpha\beta^{-1} = \delta_y^{(h-1)/2}\alpha^h. \tag{5.10}$$

Lemma 5.7 *The order of* $\overline{\beta} \in \mathrm{Out}(\Upsilon)$ *is* $p^{i-1}(p-1)$.

Proof — This is the order of $g\langle 1+p^i\rangle \in (\mathbb{Z}/p^n\mathbb{Z})^\times/\langle 1+p^i\rangle$. □

Proposition 5.8 *If* $2i \leqslant n$ *then* $\mathrm{Out}(\Upsilon)$ *has order* $p^{2i-1}(p-1)$ *and presentation*

$$\mathrm{Out}(\Upsilon) \simeq \langle a, b \mid a^{p^i} = 1, b^{p^{i-1}(p-1)} = 1, bab^{-1} = a^h\rangle \simeq \mathrm{Hol}(\mathbb{Z}/p^i\mathbb{Z}),$$

while if $2i \geqslant n$ *then* $\mathrm{Out}(\Upsilon)$ *has order* $p^{n-1}(p-1)$, *presentation*

$$\mathrm{Out}(\Upsilon) \simeq \langle a, b \mid a^{p^{n-i}} = 1, b^{p^{i-1}(p-1)} = 1, bab^{-1} = a^h\rangle,$$

and is isomorphic to

$$\mathrm{Hol}(\mathbb{Z}/p^i\mathbb{Z})/(p^{n-i}\mathbb{Z}/p^i\mathbb{Z}) \simeq (\mathbb{Z}/p^{n-i}\mathbb{Z}) \rtimes (\mathbb{Z}/p^i\mathbb{Z})^\times.$$

Proof — Let F be the free group on $\{a, b\}$ and consider the homomorphism $\Delta : F \to \mathrm{Out}(\Upsilon)$

$$a \mapsto \overline{\alpha},\ b \mapsto \overline{\beta}.$$

This is surjective by Proposition 5.5. Set $j = i$ if $2i \leqslant n$ and $j = n - i$ if $2i \geqslant n$. By Lemma 5.4, Lemma 5.7, and equations (5.9)–(5.10) we have $Y = \{a^{p^j}, b^{p^{i-1}(p-1)}, bab^{-1}a^{-h}\} \subset \ker\Delta$. Let N be the normal closure of Y in F and let $\Gamma : F/N \to \mathrm{Out}(\Upsilon)$ be epimorphism associated to Δ. It is clear that $|F/N| \leqslant p^{i+j-1}(p-1)$. On the other hand, the definitions (5.1), (5.2), and (5.4) of α and β yield that $\beta^k = \alpha^\ell\delta_u$ implies $\alpha^\ell = 1$. In particular, α and $\overline{\alpha}$ have the same order, and $\langle\overline{\alpha}\rangle \cap \langle\overline{\beta}\rangle$ is trivial. Thus, Lemmas 5.4 and 5.7 give $|\mathrm{Out}(\Upsilon)| = p^{i+j-1}(p-1)$, whence Γ is an isomorphism. □

Lemma 5.9 *We have* $Z(\Upsilon) = \langle x^{p^{n-i}}\rangle$, *so that* $\mathrm{Inn}(\Upsilon)$ *has order* $p^{2(n-i)}$ *and presentation*

$$\mathrm{Inn}(\Upsilon) = \langle u, v \mid u^{p^{n-i}} = 1, v^{p^{n-i}} = 1, vuv^{-1} = u^{1+p^i}\rangle \simeq C_{p^{n-i}} \rtimes C_{p^{n-i}}.$$

This is an abelian group if and only if $2i \geqslant n$.

Proof — Since $\langle y\rangle$ acts faithfully on $\langle x\rangle$, the central elements of $\Upsilon = \langle x\rangle \rtimes \langle y\rangle$ are the elements of $\langle x\rangle$ that are fixed by all elements of $\langle y\rangle$, which are readily seen to be the powers of $x^{p^{n-i}}$. □

Lemma 5.10 *Let* $G = \langle a, b, c\rangle$ *be a group, where* c *normalizes* $\langle a, b\rangle$, a *and* b *commute with* $[a, b]$, *and* $[a, b] \in \langle c\rangle$. *Then* $G = \langle a\rangle\langle b\rangle\langle c\rangle$.

Proof — By hypothesis, $G = \langle a, b\rangle\langle c\rangle$ and $\langle a, b\rangle = \langle a\rangle\langle b\rangle\langle [a, b]\rangle$. As $[a, b] \in \langle c\rangle$, the result follows. □

Theorem 5.11 *The order of* $\mathrm{Aut}(\Upsilon)$ *is* $p^{2n-1}(p-1)$ *if* $2i \leqslant n$, *and* $p^{3n-2i-1}(p-1)$ *if* $2i \geqslant n$. *Moreover, if*

$$\mu = \delta_x^{\ell}\beta\delta_x^{-\ell}, \tag{5.11}$$

then $\mathrm{Aut}(\Upsilon)$ *is generated by* α, δ_x, μ *for any* $\ell \in \mathbb{Z}$, *and the choice*

$$2\ell \equiv 1 \mod p^n, \tag{5.12}$$

yields the following defining relations, depending on whether $2i \leqslant n$ *or* $2i \geqslant n$*:*

$$\begin{cases} \alpha^{p^i} = 1, \delta_x^{p^{n-i}} = 1, \mu^{p^{n-1}(p-1)} = 1, \\ \alpha\delta_x\alpha^{-1} = \delta_x\mu^{p^{n-i-1}(p-1)t}, \mu\delta_x\mu^{-1} = \delta_x^g, \\ \mu\alpha\mu^{-1} = \alpha^h, \end{cases} \tag{5.13}$$

or

$$\begin{cases} \alpha^{p^{n-i}} = 1, \delta_x^{p^{n-i}} = 1, \mu^{p^{n-1}(p-1)} = 1, \\ \alpha\delta_x\alpha^{-1} = \delta_x\mu^{p^{i-1}(p-1)t}, \mu\delta_x\mu^{-1} = \delta_x^g, \\ \mu\alpha\mu^{-1} = \alpha^h. \end{cases} \tag{5.14}$$

Moreover, if $\sigma \in \mathrm{Aut}(\Upsilon)$, *then* $\sigma = ABC$ *for unique elements* $A \in \langle\alpha\rangle$, $B \in \langle\delta_x\rangle$, *and* $C \in \langle\mu\rangle$.

Proof — Set

$$j = \begin{cases} i & \text{if } 2i \leqslant n, \\ n-i & \text{if } 2i \geqslant n, \end{cases} \quad k = \begin{cases} p^{n-2i} & \text{if } 2i \leqslant n, \\ 1 & \text{if } 2i \geqslant n. \end{cases}$$

By Proposition 5.8 and Lemma 5.9, we have

$$|\mathrm{Out}(\Upsilon)| = p^{i-1+j}(p-1),\ |\mathrm{Inn}(\Upsilon)| = p^{2(n-i)},$$

so

$$|\mathrm{Aut}(\Upsilon)| = p^{2(n-i)+i-1+j}(p-1),$$

as claimed.

We have $\delta_y = \beta^{p^{i-1}(p-1)t}$ by (5.7), so α, δ_x, β generate $\mathrm{Aut}(\Upsilon)$ by Proposition 5.5. We next verify the analogs of (5.13)–(5.14) for these generators. By Lemma 5.4, we have $\alpha^{p^j} = 1$. Since g has order $p^{n-1}(p-1)$ modulo p^n, it follows that $\beta^{p^{n-1}(p-1)} = 1$. On the other hand, Lemma 5.9 implies $\delta_x^{p^{n-i}} = 1$. Moreover, according to Lemma 5.4,

$$\alpha\delta_x\alpha^{-1} = \delta_{\alpha(x)} = \delta_x\delta_y^k = \delta_x\beta^{kp^{i-1}(p-1)t}, \tag{5.15}$$

while the very definition of β yields

$$\beta\delta_x\beta^{-1} = \delta_{\beta(x)} = \delta_x^g.$$

Furthermore, by (5.9) and (5.10), we have

$$\beta\alpha\beta^{-1} = \delta_y^{k(h-1)/2}\alpha^h. \tag{5.16}$$

This completes the required verification.

It is clear that for any integer ℓ, the elements α, μ, δ_x still generate $\mathrm{Aut}(\Upsilon)$. We next show that (5.13)–(5.14) hold for a suitable choice of ℓ. It is evident that

$$\mu^{p^{n-1}(p-1)} = 1,\ \mu\delta_x\mu^{-1} = \delta_x^g,$$

Observe next that

$$\delta_y^k \in Z\big(\mathrm{Aut}(\Upsilon)\big). \tag{5.17}$$

Indeed, we have

$$\delta_y^k\delta_x\delta_y^{-k} = \delta_u,$$

where, by Lemma 2.4,

$$u = x^{(1+p^i)^k} = x^{1+p^{n-j}}.$$

Since $x^{p^{n-j}} \in Z(\Upsilon)$, it follows that δ_y^k commutes with δ_x. As δ_y is a power of β, they commute. Since $\alpha(y) = y$, it follows that α and δ_y also commute. This proves (5.17).

Since δ_x^ℓ commutes with $\delta_y^k = \beta^{kp^{i-1}(p-1)t}$, it follows that

$$\mu^{kp^{i-1}(p-1)t} = \beta^{kp^{i-1}(p-1)t}, \tag{5.18}$$

whence (5.15) gives

$$\alpha\delta_x\alpha^{-1} = \delta_x\mu^{kp^{i-1}(p-1)t}. \tag{5.19}$$

Suppose next that $2\ell \equiv 1 \mod p^n$. We claim that

$$\mu\alpha\mu^{-1} = \alpha^h.$$

Indeed, conjugating each side of (5.16) by δ_x^ℓ and using that δ_y^k is central yields

$$\mu(\delta_x^\ell\alpha\delta_x^{-\ell})\mu^{-1} = \delta_y^{k(h-1)/2}(\delta_x^\ell\alpha\delta_x^{-\ell})^h. \tag{5.20}$$

To compute with (5.20), note that $[\delta_x^{-1}, \alpha] = \delta_y^k$ by (5.15). As δ_y^k is central, $[\delta_x, \alpha]^{-1} = \delta_y^k$, so $\delta_x\alpha\delta_x^{-1} = \delta_y^{-k}\alpha$, and therefore

$$\delta_x^r\alpha\delta_x^{-r} = \delta_y^{-rk}\alpha, \quad r \in \mathbb{Z}. \tag{5.21}$$

Successively using (5.17), (5.21), (5.20), (5.21), and (5.17), we infer that

$$\begin{aligned}\delta_y^{-\ell k}\mu\alpha\mu^{-1} &= \mu\delta_y^{-\ell k}\alpha\mu^{-1} = \mu(\delta_x^\ell\alpha\delta_x^{-\ell})\mu^{-1}\\ &= \delta_y^{k(h-1)/2}(\delta_x^\ell\alpha\delta_x^{-\ell})^h = \delta_y^{k(h-1)/2}\delta_y^{-\ell hk}\alpha^h.\end{aligned}$$

Since $\ell(h-1) \equiv (h-1)/2 \mod p^n$, the claim follows.

Thus the generators α, μ, δ_x satisfy the relations (5.13) if $2i \leqslant n$ and (5.14) if $2i \geqslant n$.

Let G any group generated by elements α, μ, δ_x that satisfy (5.13) if $2i \leqslant n$ and (5.14) if $2i \geqslant n$. Set $\delta_y = \mu^{p^{i-1}(p-1)t}$. Then (5.13) and (5.14) imply that $\langle\delta_x, \delta_y\rangle$ is a normal subgroup of G having order $\leqslant p^{2(n-i)}$, with $|G/\langle\delta_x, \delta_y\rangle| \leqslant p^{i-1+j}(p-1)$, so that

$$|G| \leqslant p^{2(n-i)+i-1+j}(p-1).$$

This shows that (5.13) and (5.14) are defining relations for $\mathrm{Aut}(\Upsilon)$.

It follows from Lemma 5.10 that

$$\mathrm{Aut}(\Upsilon) = \langle\alpha\rangle\langle\beta\rangle\langle\mu\rangle.$$

As $|\mathrm{Aut}(\Upsilon)| = |\langle\alpha\rangle||\langle\beta\rangle||\langle\mu\rangle|$, we obtain the stated normal form for the elements of $\mathrm{Aut}(\Upsilon)$. □

Let μ be defined as in (5.11) with ℓ chosen so that (5.12) holds. Recalling the meaning t from (5.6), we set

$$\nu = \mu^{(p-1)t}. \tag{5.22}$$

Proposition 5.12 *Let Σ_0 be the subgroup of $\mathrm{Aut}(\Upsilon)$ generated by α, δ_x, ν. Then Σ_0 is a normal Sylow p-subgroup of $\mathrm{Aut}(\Upsilon)$ with the following defining relations, depending on whether $2i \leqslant n$ or $2i \geqslant n$:*

$$\begin{cases} \alpha^{p^i} = 1, \nu^{p^{n-1}} = 1, \delta_x^{p^{n-i}} = 1, \\ \alpha\delta_x\alpha^{-1} = \delta_x\nu^{p^{n-i-1}}, \nu\delta_x\nu^{-1} = \delta_x^{1+dp}, \\ \nu\alpha\nu^{-1} = \alpha^{1+ep}, \end{cases} \tag{5.23}$$

or

$$\begin{cases} \alpha^{p^{n-i}} = 1, \nu^{p^{n-1}} = 1, \delta_x^{p^{n-i}} = 1, \\ \alpha\delta_x\alpha^{-1} = \delta_x\nu^{p^{i-1}}, \nu\delta_x\nu^{-1} = \delta_x^{1+dp}, \\ \nu\alpha\nu^{-1} = \alpha^{1+ep}. \end{cases} \tag{5.24}$$

In particular, Σ_0 is isomorphic to Σ.

Proof — Theorem 5.11 shows that Σ_0 is normal in $\mathrm{Aut}(\Upsilon)$ and that

$$\mathrm{Aut}(\Upsilon)/\Sigma_0 \simeq \Sigma_0\langle\mu\rangle/\Sigma_0 \simeq \langle\mu\rangle/(\Sigma_0 \cap \langle\mu\rangle) \simeq \langle\mu\rangle/\langle\nu\rangle \simeq C_{p-1},$$

so Σ_0 is a Sylow p-subgroup of $\mathrm{Aut}(\Upsilon)$.

The relations (5.23)–(5.24) follow easily from (5.13)–(5.14). Set $j = i$ if $2i \leqslant n$ and $j = n - i$ if $2i \geqslant n$. That (5.23)–(5.24) are defining relations follows from the fact that any group G generated by elements α, ν, δ_x satisfying these relations has order less than or equal to $p^{2(n-i)+i-1+j}$, since $\langle\delta_x, \nu^{p^{i-1}}\rangle$ is normal in G of order $\leqslant p^{2(n-i)}$ with $|G/\langle\delta_x, \nu^{p^{i-1}}\rangle| \leqslant p^{i-1+j}$. □

6 Acknowledgment

We are very indebted to the referee for a careful reading of the paper and valuable feedback. This research was partially supported by NSERC grant RGPIN-2020-04062

REFERENCES

[1] J.N.S Bidwell – M.J. Curran: "The automorphism group of a split metacyclic p-group", *Arch. Math. (Basel)* 87 (2006), 488–497.

[2] M.J. Curran: "The automorphism group of a split metacyclic 2-group", *Arch. Math. (Basel)* 89 (2007), 10–23.

[3] M.J. Curran: "The automorphism group of a nonsplit metacyclic p-group", *Arch. Math.(Basel)* 90 (2008), 483–489.

[4] J. Dietz: "The history of the divisibility conjecture for automorphism groups of finite p-groups", *Adv. Group Theory Appl.* 8 (2019), 49–84.

[5] S.M. Ghoraishi: "On noninner automorphisms of finite p-groups that fix the center elementwise", *Int. J. Group Theory* 8 (2019), 1–9.

[6] M. Golasiński – D. Gonçalves "On automorphisms of split metacyclic groups", *Manuscripta Math.* 128 (2009), 251–273.

[7] J. González-Sánchez – A. Jaikin-Zapirain: "Finite p-groups with small automorphism group", *Forum Math. Sigma* 3 (2015) e7, 11pp.

[8] I. Malinowska: "The automorphism group of a split metacyclic 2-group and some groups of crossed homomorphisms", *Arch. Math. (Basel)* 93 (2009) 99–109.

[9] I. Malinowska: "On the structure of the automorphism group of a minimal nonabelian p-group (metacyclic case)", *Glas. Mat.* 47(67) (2012), 153–164.

[10] J.W. Wamsley: "A class of three-generator, three-relation, finite groups", *Canad. J. Math.* 22 (1970), 36–40.

[11] H.J. Zassenhaus: "The Theory of Groups", *Dover*, New York (1999).

[12] F. Zhou – H. Liu: "Automorphism groups of semidirect products", *Arch Math. (Basel)* 91 (2008), 193–198.

Fernando Szechtman
Department of Mathematics and Statistics
University of Regina
SK S4S 0A2, Regina (Canada)
e-mail: fernando.szechtman@gmail.com