

STRONG DUALITY FOR METACYCLIC GROUPS

R. QUACKENBUSH and CS. SZABÓ

(Received 1 February 1999; revised 13 October 2001)

Communicated by B. Davey

Abstract

Davey and Quackenbush proved a strong duality for each dihedral group D_m with m odd. In this paper we extend this to a strong duality for each finite group with cyclic Sylow subgroups (such groups are known to be metacyclic).

2000 *Mathematics subject classification*: primary 20D10; secondary 08A05.

Keywords and phrases: metacyclic group, duality.

1. Introduction

The first strong natural duality for nonabelian groups was established by Davey and Quackenbush, see [2]. They showed that the dihedral group D_m admits a strong natural duality if m is odd. In this paper we generalize this result to finite groups having all Sylow subgroups cyclic. We assume that the reader is familiar with [2]. The definition of a (natural) duality is given in [1, 2]; here we give it for the special case of finite groups:

Let $\mathbf{G} = \langle G, \cdot \rangle$ be a finite group. We call $\tilde{G} = \langle G; F, P, R, \tau \rangle$ a (topological) dual structure on the same set G , if

- (a) each $f \in F$ is a group homomorphism $f : \mathbf{G}^n \rightarrow \mathbf{G}$ for some $n \in \mathbb{N}$,
- (b) each $f \in P$ is a group homomorphism $f : \text{dom}(f) \rightarrow \mathbf{G}$, where $\text{dom}(f)$ is a subgroup of \mathbf{G}^n for some $n \in \mathbb{N}$,
- (c) each $r \in R$ is a subgroup of \mathbf{G}^n for some $n \in \mathbb{N}$,
- (d) τ is the discrete topology.

The research of the authors was supported by a grant from the NSERC of Canada. The second author was also supported by grant F023436 from the Hungarian National Science Research Foundation.

© 2002 Australian Mathematical Society 1446-7887/2000 \$A2.00 + 0.00

The elements of F , P and R are called operations, partial operations and relations, respectively, and we say that the structure \tilde{G} is *algebraic over* \mathbf{G} . One consequence of this definition is that every n -ary group word is a continuous homomorphism from \tilde{G}^n to \tilde{G} .

Also as a consequence of this definition we have that for each group \mathbf{A} in the quasi-variety $\mathbb{L}\mathbb{S}\mathbb{P}(\mathbf{G})$, the set of homomorphisms from \mathbf{A} to \mathbf{G} , denoted $\tilde{X}_{\mathbf{A}} := \text{Hom}(\mathbf{A}, \mathbf{G})$, is a closed substructure of $\tilde{G}^{|\mathbf{A}|}$ and for each \tilde{X} in the topological quasivariety $\mathbb{L}\mathbb{S}_c\mathbb{P}(\tilde{G})$, the set of continuous homomorphisms from \tilde{X} to \tilde{G} , denoted $\mathbf{A}_{\tilde{X}} := \text{Hom}(\tilde{X}, \tilde{G})$, is a subgroup of $\mathbf{G}^{|\tilde{X}|}$. Moreover, for each group $\mathbf{A} \in \mathbb{L}\mathbb{S}\mathbb{P}(\mathbf{G})$ there is a natural embedding $e_{\mathbf{A}}$ of \mathbf{A} into its corresponding double dual $\mathbf{A}_{\tilde{X}_{\mathbf{A}}}$ given by the evaluation map $e_{\mathbf{A}}: \mathbf{A} \rightarrow \mathbf{A}_{\tilde{X}_{\mathbf{A}}}$ such that $e_{\mathbf{A}}(a)(f) = f(a)$ for each $f \in \tilde{X}_{\mathbf{A}}$. If $e_{\mathbf{A}}$ is an isomorphism for all $\mathbf{A} \in \mathbb{L}\mathbb{S}\mathbb{P}(\mathbf{G})$, then we say that \tilde{G} yields a (*natural*) *duality* for $\mathbb{L}\mathbb{S}\mathbb{P}(\mathbf{G})$. If the analogous map $e_{\tilde{X}}$ also is an isomorphism for each $\tilde{X} \in \mathbb{L}\mathbb{S}_c\mathbb{P}(\tilde{G})$, then we say that \tilde{G} yields a *full duality* for $\mathbb{L}\mathbb{S}\mathbb{P}(\mathbf{G})$.

For instance, if $\mathbf{G} = \mathbf{Z}_m = \langle Z_m; + \rangle$ and $\tilde{Z}_m = \langle Z_m; +, \tau \rangle$ with $F = \{+\}$, $P = \emptyset = R$, then \tilde{Z}_m yields a full duality for $\mathbb{L}\mathbb{S}\mathbb{P}(\mathbf{Z}_m)$, which in this case is the variety of abelian groups satisfying $mx = 0$; this is a fragment of the usual Pontryagin duality for all abelian groups.

Duality theory tells us that in order to show that \tilde{G} yields a full duality on $\mathbb{L}\mathbb{S}\mathbb{P}(\mathbf{G})$ it is enough to prove the following three conditions:

CLO: for each $n \in \mathbb{N}$, every continuous homomorphism $\phi: \tilde{G}^n \rightarrow \tilde{G}$ is a group word on \mathbf{G} .

INJ: \tilde{G} is injective in $\mathbb{L}\mathbb{S}_c\mathbb{P}(\tilde{G})$.

STR: for any $\tilde{X} \leq \tilde{G}^I$ where $I \neq \emptyset$, and for each $y \in \tilde{G}^I \setminus \tilde{X}$ there exists a continuous homomorphism $\phi: \tilde{G}^I \rightarrow \tilde{G}$ such that $\phi|_{\tilde{X}} = 1$ while $\phi(y) \neq 1$.

When these three conditions are satisfied we call this a *strong duality*; thus, a strong duality is a full duality. All known full dualities are actually strong dualities. It has long been conjectured that a full duality is always strong, but this remains an open, challenging problem. We shall exhibit a strong duality for groups having cyclic Sylow subgroups.

2. Preliminary results

For the main goal of the paper we need some structure theorems for groups. The first is from Robinson, [5, page 281].

THEOREM 2.1 (Hölder, Burnside, Zassenhaus). *A finite group \mathbf{G} has all its Sylow subgroups cyclic if and only if it has a representation $\mathbf{Z}_n \rtimes \mathbf{Z}_m$ such that $(m, n) = 1$; thus, it is metacyclic.*

Let $n = p_1^{\beta_1} \cdots p_k^{\beta_k}$ so that $\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{\beta_1}} \times \cdots \times \mathbf{Z}_{p_k^{\beta_k}}$ and $\text{Aut}(\mathbf{Z}_n) \cong \text{Aut}(\mathbf{Z}_{p_1^{\beta_1}}) \times \cdots \times \text{Aut}(\mathbf{Z}_{p_k^{\beta_k}})$. Then the semidirect product $\mathbf{Z}_n \rtimes \mathbf{H}$ is determined by a homomorphism $\rho = (\rho_1, \dots, \rho_k)$ from \mathbf{H} into $\text{Aut}(\mathbf{Z}_n)$, where ρ_i is the corresponding homomorphism from \mathbf{H} into $\text{Aut}(\mathbf{Z}_{p_i^{\beta_i}})$ and $\mathbf{Z}_{p_i^{\beta_i}} \rtimes \mathbf{H}$ is the corresponding semidirect product. The next theorem tells us how to build recursively a strong duality for $\mathbf{Z}_n \rtimes \mathbf{H}$ from those for the $\mathbf{Z}_{p_i^{\beta_i}} \rtimes \mathbf{H}$. As often happens in a recursive construction, we need to assume and prove something a bit stronger in order to prove that the recursive construction is correct. A strong duality for $\mathbf{K} = \mathbf{G} \rtimes \mathbf{H}$ will be called *semidirect* over \mathbf{H} if the following condition holds: let $\tilde{\mathbf{X}}$ be a closed substructure of $(\tilde{\mathbf{K}})'$, $\phi: \tilde{\mathbf{X}} \rightarrow \tilde{\mathbf{K}}$ a continuous structure preserving map and $\phi': (\tilde{\mathbf{H}})' \rightarrow \tilde{\mathbf{K}}$ a continuous structure preserving map extending the restriction of ϕ to $(\tilde{\mathbf{H}})'$; then there is a continuous structure preserving map $\psi: (\tilde{\mathbf{K}})' \rightarrow \tilde{\mathbf{K}}$ extending both ϕ and ϕ' .

Now and later in the paper, we make use of the following group theoretic lemma from [2].

LEMMA 2.2. *Let \mathbf{G} be a group and let ϵ be a retraction of \mathbf{G} onto a subgroup \mathbf{H} . Let \mathbf{N} be the kernel of ϵ and let*

$$K := \{(u, v) \in G^2 \mid \epsilon(u) = \epsilon(v)\} = \bigcup \{(\epsilon^{-1}(h))^2 \mid h \in H\} \\ = \bigcup \{Nh \times Nh \mid h \in H\}$$

be the congruence corresponding to \mathbf{N} . Define a partial binary operation $*$, with domain K , by $xh * yh := xyh$ for all $x, y \in N$ and $h \in H$ (that is, define $u * v := u\epsilon(u)^{-1}v = u\epsilon(v)^{-1}v$ for all $(u, v) \in K$).

- (a) (The restriction of) $*$ is a well-defined group operation on Nh for each $h \in H$. Moreover, right translation by h is an isomorphism of $\langle N; \cdot \rangle$ onto $\langle Nh; * \rangle$.
- (b) The partial operation $*$ is associative wherever it is defined. It will be commutative wherever it is defined provided \mathbf{N} is abelian.
- (c) The map $*: \mathbf{K} \rightarrow \mathbf{G}$ is a homomorphism if and only if \mathbf{N} is abelian.

THEOREM 2.3. *Let $\mathbf{G}_1, \mathbf{G}_2, \mathbf{H}$ be finite groups with $\mathbf{G}_1, \mathbf{G}_2$ abelian, such that their sizes are pairwise relatively prime. If $\mathbf{K}_i = \mathbf{G}_i \rtimes \mathbf{H}$ (given by $\rho_i: \mathbf{H} \rightarrow \text{Aut}(\mathbf{G}_i)$) each admits a strong duality, then a strong duality holds for $\mathbf{G} = (\mathbf{G}_1 \times \mathbf{G}_2) \rtimes \mathbf{H}$ (given by $(\rho_1, \rho_2): \mathbf{H} \rightarrow \text{Aut}(\mathbf{G}_1) \times \text{Aut}(\mathbf{G}_2)$).*

PROOF. Let ϵ_i denote the retractions of \mathbf{G} to \mathbf{K}_i by \mathbf{G}_j for $(i, j) \in \{(1, 2), (2, 1)\}$, ϵ the retraction of \mathbf{G} to \mathbf{H} by $\mathbf{G}_1 \times \mathbf{G}_2$. Let $\tilde{\mathbf{K}}_i = \langle K_i; F_i, P_i, R_i, \tau \rangle$ yield a strong duality for $\mathbb{LSP}(\mathbf{K}_i)$. Let $s_i(n) = q_i(n)r_i(n)$ be the size of the n -generated free group, $F_i(n)$, in the variety generated by \mathbf{K}_i , where $(q_i(n), |\mathbf{G}_i|) = (r_i(n), |\mathbf{H}|) = 1$. Also,

let $*$ be the partial operation given by the translation of the group operation on $G_1 \times G_2$ as given by Lemma 2.2. We take

$$\tilde{G} = \langle G; \{\varepsilon_1, \varepsilon_2\}, F_1 \cup F_2 \cup P_1 \cup P_2 \cup \{*\}, R_1 \cup R_2, \tau \rangle;$$

note that full operations on G_i become partial operations on G . Also note that $\varepsilon_1\varepsilon_2 = \varepsilon_2\varepsilon_1 = \varepsilon$. We will use the fact that $\varepsilon_i|_{K_{1-i}}$ is the retraction of K_{1-i} onto \mathbf{H} by G_i . Because of our assumption of strong dualities, we may assume that $\varepsilon_i|_{K_{1-i}}$ is part of the duality for K_{1-i} .

Let $\underline{g} \in G^I$ for I finite or infinite, and let $\phi: \tilde{G}^I \rightarrow \tilde{G}$ be a continuous homomorphism. Then we have $\underline{g} = \underline{g}_1\underline{g}_2\underline{h}$ with $\underline{g}_i \in G_i^I$ and $\underline{h} \in H^I$. Then $\varepsilon_i(\underline{g}) = \underline{g}_i\underline{h}$. Since $\underline{g} = \underline{g}_1\underline{h} * \underline{g}_2\underline{h}$ and ϕ preserves $*$,

$$\phi(\underline{g}) = \phi(\underline{g}_1\underline{h}) * \phi(\underline{g}_2\underline{h}) = \phi(\varepsilon_1(\underline{g})) * \phi(\varepsilon_2(\underline{g})).$$

That is, $\phi(\underline{g})$ is uniquely defined once $\phi(\varepsilon_1(\underline{g}))$ and $\phi(\varepsilon_2(\underline{g}))$ are known.

First we show that **CLO** holds. Due to the semidirect products involved, each $F_i(n)$ is itself a semidirect product of a normal subgroup $N_i(n)$ and $F_H(n)$, the n -generated free group over \mathbf{H} . Moreover, $(|N_i(n)|, |F_H(n)|) = 1$. That is to say, $q_1(n) = q_2(n) := q(n)$ for all $n \geq 0$. As each K_i is a quotient of \mathbf{G} , we have $|F_G(n)| \geq q(n)r_1(n)r_2(n)$. We show that equality holds, as does **CLO**, by showing that there are at most $q(n)r_1(n)r_2(n)$ continuous homomorphisms $\phi: \tilde{G}^n \rightarrow \tilde{G}$. Since ϕ preserves $\{\varepsilon, \varepsilon_1, \varepsilon_2\}$, ϕ maps K_i^n to K_i and H^n to H . In view of the strong dualities assumed for each K_i , there are at most $q(n)r_1(n)r_2(n)$ restrictions of ϕ to $K_1^n \cup K_2^n$; we must show that this restriction has at most one extension to all of G^n . But that was done in the last paragraph.

In order to prove **INJ** and that the duality will be semidirect over \mathbf{H} , let $\tilde{X} \leq \tilde{G}^I$ be a closed substructure for some set I and $\phi: \tilde{X} \rightarrow \tilde{G}$ a continuous homomorphism. Since ϕ preserves the retractions, $\phi|_{K_i^I}$ is a continuous homomorphism from $\tilde{X} \cap \tilde{K}_i^I$ to \tilde{K}_i . Since **INJ** holds for \tilde{K}_i^I and the dualities are semidirect over \mathbf{H} , we proceed as follows: let ψ_0 be an extension of $\phi|_{H^I}$ to \tilde{H}^I and ψ_i an extension of $\psi_0 \cup \phi|_{K_i^I}$ to \tilde{K}_i^I for $i = 1, 2$, and note that $\psi_1|_{H^I} = \psi_2|_{H^I}$. Let $\underline{g} \in G^I$ where $\underline{g} = \underline{g}_1\underline{g}_2\underline{h}$ with $\underline{g}_i \in G_i^I$ and $\underline{h} \in H^I$. From what we have seen above, we must define ψ by $\psi(\underline{g}) := \psi_1(\varepsilon_1(\underline{g})) * \psi_2(\varepsilon_2(\underline{g}))$. If $\underline{g} \in \tilde{X}$, then $\psi(\varepsilon_i(\underline{g})) = \phi(\varepsilon_i(\underline{g}))$, so that ψ extends ϕ ; obviously, ψ extends ψ_0 . Since $\psi|_{K_i^I}$ is a homomorphism, to show that ψ is a homomorphism, it is enough to show that ψ preserves ε_i . Let $\underline{g} = \underline{g}_1\underline{g}_2\underline{h}$. On the one hand,

$$\psi(\varepsilon_1(\underline{g})) = \psi_1(\varepsilon_1(\varepsilon_1(\underline{g}))) * \psi_2(\varepsilon_2(\varepsilon_1(\underline{g}))) = \psi_1(\underline{g}_1\underline{h}) * \psi_2(\underline{h}).$$

On the other hand,

$$\varepsilon_1(\psi(\underline{g})) = \varepsilon_1(\psi_1(\underline{g}_1\underline{h}) * \psi_2(\underline{g}_2\underline{h})).$$

Let $\psi_1(g_1 \underline{h}) = g_1 h$ and $\psi_2(g_2 \underline{h}) = g_2 h'$ where $g_i \in G_i$ and $h, h' \in H$. In order for $g_1 h * g_2 h'$ to be defined, we need to show that $h = h'$. We do this by showing that $\psi_1(\underline{h}) = h$ and $\psi_2(\underline{h}) = h'$; since $\psi_1(\underline{h}) = \psi_2(\underline{h})$, the result follows. Using the fact that ε_2 commutes with ψ_1 , we have

$$h = \varepsilon_2(g_1 h) = \varepsilon_2(\psi_1(g_1 \underline{h})) = \psi_1(\varepsilon_2(g_1 \underline{h})) = \psi_1(\underline{h}).$$

Similarly, $\psi_2(\underline{h}) = h'$. Then,

$$\varepsilon_1(\psi_1(g_1 \underline{h}) * \psi_2(g_2 \underline{h})) = \varepsilon_1(g_1 h * g_2 h) = \varepsilon_1(g_1 g_2 h) = g_1 h.$$

Finally, $g_1 h = g_1 h * h = \psi_1(g_1 \underline{h}) * \psi_2(\underline{h})$, showing that ψ preserves ε_1 . In a similar manner it preserves ε_2 and so it is a homomorphism.

To complete the proof of **INJ** we need to prove that ψ is continuous. By construction, both ψ_1 and ψ_2 are continuous. Using the same finite subset of I given by the continuity of ψ_i , it is straightforward to prove the continuity of $\psi_i \circ \varepsilon_i$. Note that $*$ is continuous because it has finite domain. Thus, ψ is a composition of continuous maps and so it is continuous. Moreover, we have shown that the duality is semidirect over **H**.

To show **STR** we first note that restricted to K'_i , **STR** holds. Also recall that ϕ is defined on $\underline{g} \in G'$ if and only if it is defined on $\varepsilon_i(\underline{g}) \in K'_i$ for $i = 1, 2$. Let $\tilde{X} \leq \tilde{G}'$ be a closed substructure and $\underline{y} \in G' - X$ for some set $I \neq \emptyset$; we define $\phi(\underline{x}) := 1$ for all $\underline{x} \in X$. Then, without loss of generality, we may assume that either $\underline{y} \in H'$ or $\varepsilon_1(\underline{y}) \notin \varepsilon_1(X)$; in either case, $\varepsilon_1(\underline{y}) \notin \varepsilon_1(X)$. Now we invoke **STR** for \tilde{K}'_1 with respect to $\varepsilon_1(\underline{y})$ and proceed as in the proof of **INJ** for \tilde{G}' , and we are done. We leave to the reader the verification that the value of this extension at \underline{y} is not 1. □

3. The case $n = p^\beta$

Thus, we can build up our strong duality for finite metacyclic groups from that for metacyclic groups of the form $\mathbf{G} = \mathbf{Z}_{p^\beta} \rtimes \mathbf{Z}_m$, where $(p, m) = 1$. In this section we show that there is a strong duality semidirect over \mathbf{Z}_m for these groups. We assume that \mathbf{G} is not abelian.

Let $\mathbf{Z}_{p^\beta} = \langle a \rangle$, $\mathbf{Z}_m = \langle b \rangle$ and $a^b (= bab^{-1}) = a^k$ for some $k \in \mathbb{N}$. Let $\gamma \in \text{Aut}(\mathbf{Z}_{p^\beta})$ be such that $\gamma(a) = a^b$ and let the order of γ be d (this means that $ba = a^k b$ and that $a = \gamma^d(a) = a^{k^d}$, so that $p^\beta | (k^d - 1)$). As \mathbf{G} is not abelian, $d > 1$; for the same reason, $p > 2$, and so $\text{Aut}(\mathbf{Z}_{p^\beta}) \cong \mathbf{Z}_{p^{\beta-1}(p-1)}$. On the one hand, as there is a group homomorphism from \mathbf{Z}_m to $\text{Aut}(\mathbf{Z}_{p^\beta})$ sending b to γ , $d|m$ and so $(d, p) = 1$. On the other hand, as $d|p^{\beta-1}(p-1)$ and $(d, p) = 1$, we have that $d|(p-1)$. Thus,

$b^d a = a^{k^d} b^d = ab^d$ and so $\langle b^d \rangle$ is in the center of \mathbf{G} . Let us suppose that $ab^j = b^j a$. Then $a = (a)^{b^j} = a^{k^j}$; hence, $\gamma^j(a) = a$ and so d divides j . Thus,

$$\begin{aligned} C_G(a^i) &= \langle a, b^d \rangle, & C_G(b^j) &= \langle b \rangle \text{ if } d \nmid j, \\ C_G(b^j) &= \mathbf{G} \text{ if } d \mid j, & Z(\mathbf{G}) &= \langle b^d \rangle. \end{aligned}$$

When $Z(\mathbf{G}) \neq 1$ (that is, $d < m$), there are some complications. For instance, consider the case $p^\beta = 3, m = 4$ and $a^b = a^{-1}$. In this 12-element group we have $Z(\mathbf{G}) = \langle b^2 \rangle$ and $\mathbf{G}/Z(\mathbf{G}) \cong S_3$. But S_3 is not in the quasivariety generated by \mathbf{G} (as S_3 is monolithic but not a subgroup of \mathbf{G}). Thus, the quasivariety generated by \mathbf{G} is not the variety generated by \mathbf{G} . However, the variety generated by \mathbf{G} is the quasivariety generated by $\mathbf{Z}_4 \times S_3$, see Olshanskii [3]. In general, the variety generated by $\mathbf{G} = \mathbf{Z}_{p^\beta} \rtimes \mathbf{Z}_m$ is the quasivariety generated by

$$\mathbf{Z}_m \times (\mathbf{G}/Z(\mathbf{G})) \cong \mathbf{Z}_m \times (\mathbf{Z}_{p^\beta} \rtimes (\mathbf{Z}_m/Z(\mathbf{G}))) \cong \mathbf{Z}_m \times (\mathbf{Z}_{p^\beta} \rtimes \mathbf{Z}_d).$$

In case $Z(\mathbf{G}) \neq 1$, we will need to work ‘over the center’ by using the following partial operation.

LEMMA 3.1. *The mapping $\star: \mathbf{G} \times Z(\mathbf{G}) \rightarrow \mathbf{G}$ such that $g \star c = gc$ is a group homomorphism.*

We shall show that $\mathbb{S}_c\mathbb{P}(\tilde{\mathbf{G}})$ is a dual quasivariety of $\mathbb{S}\mathbb{P}(\mathbf{G})$, where

$$\tilde{\mathbf{G}} = \langle G; 1, \alpha, +, *, \circ, \star, \tau \rangle.$$

Here, 1 is the constant operation and α is the automorphism of \mathbf{G} fixing a and mapping b to ab (we omit the routine but ugly computation that shows that such an α exists). The four operations $+, *, \circ, \star$ are each obtained from the restriction of the group operation \cdot to certain subgroups of \mathbf{G}^2 ; each operation is a homomorphism. Thus, $+$ is the restriction of the group operation \cdot to the abelian group $\mathbf{Z}_m = \langle b \rangle$. Next, $*$ is the binary partial operation obtained via Lemma 2.2 from \mathbf{Z}_{p^β} and \mathbf{Z}_m . More precisely, the domain of $*$ is $\bigcup_{i=0}^{m-1} (\mathbf{Z}_{p^\beta} b^i \times \mathbf{Z}_{p^\beta} b^i)$, and the operation is the translation of the group multiplication: $a^i b^j * a^k b^j = a^{i+k} b^j$. By Lemma 2.2, $*$ is an algebraic binary partial operation. Let $\varepsilon: \mathbf{G} \rightarrow \mathbf{Z}_m$ where $\varepsilon(a^i b^j) = b^j$ is the retraction of \mathbf{G} onto \mathbf{Z}_m by $\mathbf{Z}_{p^\beta} = \langle a \rangle$. Note that if a map preserves $*$ then it automatically preserves ε , since $\varepsilon(a^i b^j) = a^i b^j * a^{-i} b^j$ and $a^{-i} b^j$ is generated from $a^i b^j$ by $*$. The binary partial operation \circ is the restriction of the group operation \cdot to the abelian group $\mathbf{Z}_{p^\beta} \times Z(\mathbf{G})$. Finally, the binary partial operation \star is as given by Lemma 3.1. As always, τ is the discrete topology.

First we show that the condition **CLO** holds.

LEMMA 3.2. $|\text{Hom}(\tilde{G}^n, \tilde{G})| \leq m^n (p^\beta)^{(d^n-1)(n-1)+n}$.

PROOF. The proof is essentially the same as that of Proposition 4 of [2]. Let $\phi \in \text{Hom}(\tilde{G}^n, \tilde{G})$. Since $+$ is the original group operation on Z_m , and ϕ preserves $+$, the restriction, $\phi|_{(Z_m)^n}$, is an abelian group homomorphism into Z_m . There are m^n such homomorphisms. Next, we examine the possible extensions of each such homomorphism. Let $h = (h_1, \dots, h_n) \in (Z_m)^n$ and $\varepsilon^{-1}(h) = Z_{p^\beta} h_1 \times \dots \times Z_{p^\beta} h_n = S_h$. S_h is an abelian group isomorphic to $(Z_{p^\beta})^n$ under the operation $*$ with h as its identity element. S_h must be mapped into $\varepsilon^{-1}(\phi(h))$ which under $*$ is isomorphic to a subgroup of Z_{p^β} , and $\phi|_{S_h}$ must be an abelian group homomorphism from $\langle S_h, * \rangle$ to its image. Since ϕ preserves α , it is already defined on $\alpha(h)$, hence on $\langle \alpha(h), * \rangle$ which is a subgroup of size p^β of $\langle S_h, * \rangle$ if $h \neq 1$, and is $\{h\}$ if $h = 1$. So there are at most $(p^\beta)^{n-1}$ extensions to S_h if $h \neq 1$ and at most $(p^\beta)^n$ if $h = 1$. Finally, let $h' \in (Z_m)^n$ be such that $h^{-1}h' \in (Z(G))^n$. Then because of \star , if we know ϕ on S_h , then we know ϕ on $S_{h'}$. Since $|Z_m/Z(G)| = d$, the number of continuous homomorphisms from \tilde{G}^n to \tilde{G} is not more than $m^n (p^\beta)^{(d^n-1)(n-1)+n}$. \square

In [2], the proof is completed by a reference to the known result that this upper bound is the size of the n -generated free group in the variety generated by the given group. In the present case, we do not have such a formula at hand. However, since every word is a continuous homomorphism, we only need to construct an n -generated group of the appropriate size in the variety generated by G . One of the referees of an earlier version of this paper gave an alternate proof by showing that the variety generated by G is the product variety $\mathcal{A}_{p^\beta} \mathcal{A}_d$, whose free spectrum is known. The proof we give here is more elementary and has the advantage that it is a more general approach to producing dualities – one ‘merely’ constructs sufficiently large n -generated algebras.

LEMMA 3.3. Let $\underline{a} \in \langle a \rangle^q$ and $\underline{g} \in G^q$ be such that if $(g)_i = b^i a^s$, then $0 \leq t \leq d - 1$. Then for every $0 \leq t \leq d - 1$ the group generated by \underline{a} and \underline{g} contains a vector \underline{a}_t such that $(\underline{a}_t)_i = (\underline{a})_i$ if $(g)_i = b^i a^s$ and $(\underline{a}_t)_i = 1$, otherwise.

PROOF. Consider $\underline{a} = (a^{w_1}, \dots, a^{w_q})$ and $\underline{g} = (b^{i_1} a^{t_1}, \dots, b^{i_q} a^{t_q})$. Without loss of generality, we may assume that $i_u \neq i_v$ for $u, v \leq s$ and that for $v > s$ there is $u \leq s$ with $i_u = i_v$. Form the $s \times s$ matrix whose (u, v) component is the exponent of a in the v -th component of $\underline{a} \underline{g}^v$. Then this matrix is a constant multiple of the Vandermonde-matrix $V = V(k^{i_1}, k^{i_2}, \dots, k^{i_s})$, where the constant is

$$\left(\prod_{j=1}^q w_j \right) k^{(\sum_{j=1}^n i_j)}.$$

Notice that this constant is not divisible by p . The determinant of V is

$$\det V = \prod_{0 < j < l \leq s} (k^j - k^l).$$

As $k^j - k^l = k^l(k^{j-l} - 1)$ is coprime with p , $\det V$ is a unit in \mathbf{Z}_{p^s} ; hence, V is invertible and the vectors asserted by the lemma are expressible in the terms of the vectors $\underline{a}^{\underline{g}}$. □

DEFINITION. Let $\underline{a} \in \langle a \rangle^k$ and $\underline{g} \in \mathbf{G}^k$. The vectors created in the previous lemma are called the *separation of \underline{a} by \underline{g} at the exponent t* .

EXAMPLE 1. Let $\underline{a} = (1, a, a^2, 1, a^3, a, a)$ and $\underline{g} = (b, a, ba^2, b^3a, b, b^5a, b^3)$. Then $\underline{a}_0 = (1, a, 1, 1, 1, 1, 1)$, $\underline{a}_1 = (1, 1, a^2, 1, a^3, 1, 1)$, $\underline{a}_3 = (1, 1, 1, 1, 1, 1, a)$. It is clear that $\underline{a} = \prod_{i=0}^{m-1} \underline{a}_i$, and $\underline{a}_t = (1, \dots, 1)$ if t does not occur in \underline{g} as an exponent of a in some component.

We exhibit an n -generated subgroup \mathbf{D} of $\mathbf{G}^{(d^n-1)(n-1)+n}$ of the appropriate size. We define an n -by- $[(d^n - 1)(n - 1) + n]$ matrix M with entries from \mathbf{G} , and take the group generated by its rows. We define M by giving its columns. Take all the vectors \bar{b} from $\langle b \rangle^n$ such that if $(\bar{b})_i = b^r$, then $0 \leq r \leq d - 1$. For each such \bar{b} take the vectors \bar{b}_i ($1 \leq i \leq n$), that are the same as \bar{b} except that the i -th coordinate is multiplied by a from the right. For each \bar{b} we omit the first \bar{b}_i which does not contain a as a coordinate. For example if $\bar{b} = (1, 1, b, b^2, b^3, 1, b)^T$ we omit $\bar{b}_3 = (1, 1, ba, b^2, b^3, 1, b)^T$. We get n vectors from $(1, \dots, 1)^T$ and $n - 1$ from each $\bar{b} \neq (1, \dots, 1)^T$. These vectors will be the columns of M . Given an element $\bar{v} \in \mathbf{G}^{(d^n-1)(n-1)+n}$, we will index the coordinates of \bar{v} by the columns of M .

DEFINITION. \bar{b} is called the *b-part* of \bar{b}_i ; a column of M distinct from \bar{b}_i but with the same b -part is called a *b-mate* of \bar{b}_i . A row vector of length $(d^n - 1)(n - 1) + n$ with an a in coordinate \bar{b}^i , and a 1 in all other coordinates is called the *a-part* of \bar{b}_i .

LEMMA 3.4. *In the variety generated by \mathbf{G} , there is an n -generated group of size at least $m^n (p^\beta)^{(d^n-1)(n-1)+n}$.*

PROOF. We show that \mathbf{D} , the group generated by the rows of M , is a group of the required size. We show that \mathbf{D} contains

- (1) a subgroup \mathbf{H}_1 of size $(p^\beta)^{(d^n-1)(n-1)+n}$;
- (2) a subgroup \mathbf{H}_2 of size m^n .

Since the orders of \mathbf{H}_1 and \mathbf{H}_2 are coprime, the group generated by them has size at least $m^n (p^\beta)^{(d^n-1)(n-1)+n}$.

In order to show (1), let $\bar{g} = (b^{t_1}, \dots, b^{t_1}a, \dots, b^{t_n})$ be a column of M , \underline{v}_i the row of M with $b^{t_i}a$ entry in coordinate \bar{g} . First we construct a vector $\underline{w}' \in D$ having a as its \bar{g} coordinate, and 1 in all coordinates which are b -mates of \bar{g} . Let $\underline{w}' = \underline{v}_i$ if $t_i = 0$; notice that at a b -mate coordinate of \bar{g} the entry is 1. If $t_i \neq 0$, consider \bar{g} and its b -mates (in total, $n - 1$ columns). Then by the construction of M there is a unique row \underline{v} which contains no a in any of these columns, but only a fixed power of b , b^r ; this row corresponds to the first component of the b -part of \bar{g} which is not 1. If m does not divide $[r, t_i]$, let $\underline{w}'' = \underline{v}^{m - [r, t_i]/r} \cdot \underline{v}_i^{[r, t_i]/t_i}$. Then the \bar{g} coordinate of \underline{w}'' is a^z , where

$$z = \frac{k^{[r, t_i]} - 1}{k^{[r, t_i]/t_i} - 1},$$

and the coordinate of every b -mate of \bar{g} is 1. Since m does not divide $[r, t_i]$, p does not divide z and so there is a $u \in \mathbb{N}$ such that

$$zu \equiv 1 \pmod{p^\beta}.$$

Hence, $(a^z)^u = a$. Let $\underline{w}' = (\underline{w}'')^u$. If m divides $[r, t_i]$, then m does not divide $[r + t_i, t_i]$; so let us use $\underline{v} \cdot \underline{v}_i$ instead of \underline{v}_i to construct \underline{w}'' and \underline{w}' . The \bar{g} coordinate of \underline{w}' is a , and the coordinate of every b -mate of \bar{g} is 1.

We next construct $\underline{w}_0 \in D \cap \langle a \rangle^{(d^n - 1)(n - 1) + n}$ with the same property. Since $(m, p) = 1$, there is an $x \in \mathbb{N}$ such that

$$x \equiv 1 \pmod{p^\beta}; \quad x \equiv 0 \pmod{m}.$$

Let $\underline{w}_0 = (\underline{w}')^x$. Then $\underline{w}_0 \in D \cap \langle a \rangle^{(d^n - 1)(n - 1) + n}$ with a in its \bar{g} coordinate, and the coordinate of every b -mate of \bar{g} is 1.

Now we recursively construct the a -part of \bar{g} . Suppose for $\bar{h} \neq \bar{g}$ that $(\underline{w}_0)_{\bar{h}} \neq 1$. Then the b -part of \bar{h} differs from the b -part of \bar{g} , say at component j . Look at \underline{w}_1 , the separation of \underline{w}_0 by the j -th row of M at the exponent t_j , where t_j is the j -th component of the b -part of \bar{g} . Then $(\underline{w}_1)_{\bar{g}} = a$ and $(\underline{w}_1)_{\bar{h}} = 1$. As separation preserves the entry 1, iteration eventually produces the a -part of \bar{g} . Clearly, the set of all a -parts of the columns of M generates a group of the required size.

In order to show (2), express $\varepsilon(\underline{v}_i)$ with \underline{v}_i and \mathbf{H}_1 . These elements belong to $\langle b \rangle^{(d^n - 1)(n - 1) + n}$ and clearly generate a group \mathbf{H}_2 of order m^n . □

Now we have everything to show that **CLO** holds:

THEOREM 3.5. *Each continuous homomorphism from \tilde{G}^n to \tilde{G} is a word.*

PROOF. By construction, each word is a continuous homomorphism. But by Lemma 3.2 and Lemma 3.4, there are at most as many continuous homomorphisms as there are words. □

COROLLARY 3.6. *The size of the n -generated free group in the variety generated by G is $m^n(p^\beta)^{(d^n-1)(n-1)+n}$ and the n -generated free group is a semidirect product:*

$$(Z_{p^\beta})^{(d^n-1)(n-1)+n} \rtimes Z_m^n.$$

Let us now try to prove **INJ** and **STR** and show that the duality is semidirect over Z_m . Thus, choose $\tilde{X} \leq \tilde{G}'$ with I not empty, $\underline{y} \in \tilde{G}' - \tilde{X}$, and $\phi \in \text{Hom}(\tilde{X}, \tilde{G})$. We want to extend ϕ to $\psi \in \text{Hom}(\tilde{G}', \tilde{G})$ so that if $\phi \equiv 1$, then $\psi(\underline{y}) \neq 1$. Also, if $\phi' \in \text{Hom}(\tilde{Z}'_m, \tilde{G})$ and extends $\phi|_{Z'_m}$, then we want to find $\psi \in \text{Hom}(\tilde{G}', \tilde{G})$ extending both ϕ and ϕ' .

DEFINITION. Define $X_m := X \cap Z'_m$, $X_p := X \cap (Z_{p^\beta} \times Z(\mathbf{G}))'$, and for $\underline{b} \in Z'_m - (Z(\mathbf{G}))'$, define $X_{\underline{b}} := X \cap \langle a \rangle^I \underline{b}$. Note that $\underline{1} \in X_m$, $\underline{1} \in X_p$, but that $X_{\underline{b}}$ may be empty. Each of $X_m, X_p, X_{\underline{b}}$ is closed.

- LEMMA 3.7.** (a) $+$ is fully defined on X_m and $\langle X_m; +, \tau \rangle$ is a closed substructure of $\langle Z'_m; +, \tau \rangle$, to which Pontryagin duality for abelian groups of exponent m applies;
 (b) \circ is fully defined on X_p and $\langle X_p; \circ, \tau \rangle$ is a closed substructure of $\langle (Z_{p^\beta} \times Z(\mathbf{G}))'; \circ, \tau \rangle$, to which Pontryagin duality for abelian groups of exponent $p^\beta m/d$ applies;
 (c) for $\underline{b} \in Z'_m - (Z(\mathbf{G}))'$, $*$ is fully defined on $X_{\underline{b}}$ and $\langle X_{\underline{b}}; *, \tau \rangle$ is a closed substructure of $\langle \langle a \rangle^I \underline{b}; *, \tau \rangle$, to which Pontryagin duality for abelian groups of exponent p^β applies;
 (d) the effect of $*$ is that for any $\underline{c} \in X \cap Z(\mathbf{G})'$, $\langle X_{\underline{b}}; *, \alpha, \tau \rangle$ is isomorphic to $\langle X_{\underline{bc}}; *, \alpha, \tau \rangle$ via multiplication by \underline{c} .

PROOF. Everything is clear except for part (d) where we need to prove closure under α and its preservation under multiplication. This follows from the fact that in \mathbf{G} , $\alpha(bc) = \alpha(b)c$, which we now prove. Since $\alpha(bc) = \alpha(b)\alpha(c)$, we need to show that $\alpha(c) = c$. Recalling that $Z(\mathbf{G}) = \langle b^d \rangle$, this reduces to showing that $\alpha(b^d) = b^d$. But $\alpha(b^d) = (\alpha(b))^d = (ab)^d = a^s b^d$ for some s . On the other hand, we must have $\alpha(b^d) \in Z(\mathbf{G})$. This means that $a^s = 1$ and $\alpha(b^d) = b^d$. □

Thus, $\phi|_{X_p}$ is a continuous \circ -homomorphism. By Pontryagin duality for abelian groups of exponent $p^\beta m/d$, there is a continuous \circ -homomorphism $\phi_1: (Z_{p^\beta} \times Z(\mathbf{G}))' \rightarrow Z_{p^\beta} \times Z(\mathbf{G})$ which extends $\phi|_{X_p}$. Also, since $Z(\mathbf{G}) \leq Z_m$ and $(p, m) = 1$, we may assume that ϕ_1 extends $\phi'|_{Z(\mathbf{G})'}$.

Now define $X'_m := X_m(Z(\mathbf{G}))'$; clearly, X'_m is closed under $+$. Define $\phi_2: X'_m \rightarrow Z_m$ by $\phi_2(\underline{x}\underline{c}) := \phi(\underline{x})\phi_1(\underline{c})$ for $\underline{x} \in X_m$ and $\underline{c} \in Z(\mathbf{G})'$.

LEMMA 3.8. X'_m is a closed subset of Z'_m , and ϕ_2 is a continuous $+$ -homomorphism.

PROOF. Let $\underline{z} \notin X'_m$, and so $\underline{z} \notin X_m$. Thus, there is a finite $F \subseteq I$ such that $\underline{z}'|_F = \underline{z}|_F$ implies that $\underline{z}' \notin X_m$. For $\underline{c} \in Z(\mathbf{G})^F$ choose $d(\underline{c}) \in Z(\mathbf{G})^I$ with $d(\underline{c})|_F = \underline{c}$ and with $d(\underline{c}^{-1}) = (d(\underline{c}))^{-1}$; note that there are only finitely many such $d(\underline{c})$. Then $\underline{z}d(\underline{c}) \notin X'_m$ as $\underline{z} \notin X'_m$, implying that $\underline{z}d(\underline{c}) \notin X_m$. Consequently, there is a finite $E_{\underline{c}} \subseteq I$ such that $\underline{w}|_{E_{\underline{c}}} = \underline{z}d(\underline{c})|_{E_{\underline{c}}}$ implies that $\underline{w} \notin X_m$. Define $E := F \cup \bigcup \{E_{\underline{c}} \mid \underline{c} \in Z(\mathbf{G})^F\}$; E is finite. Choose \underline{z}' so that $\underline{z}'|_E = \underline{z}|_E$. Suppose that $\underline{z}' \in X'_m$; then $\underline{z}' = \underline{x}'\underline{c}'$ for some $\underline{x}' \in X_m$ and $\underline{c}' \in Z(\mathbf{G})^I$. Take $\underline{c} := \underline{c}'|_F$. Then $\underline{z}'d(\underline{c}^{-1}) \in X'_m$ as $\underline{z}' \in X'_m$. But $\underline{z}'d(\underline{c}^{-1})|_{E_{\underline{c}^{-1}}} = \underline{z}d(\underline{c}^{-1})|_{E_{\underline{c}^{-1}}}$ so that $\underline{z}'d(\underline{c}^{-1}) \notin X'_m$, implying that $\underline{z}' \notin X'_m$. Thus, the clopen set $\{\underline{z}' \mid \underline{z}'|_E = \underline{z}|_E\}$ is disjoint from X'_m and X'_m is closed.

Next, we need to see that ϕ_2 is well defined; let $\underline{x}\underline{c} = \underline{x}'\underline{c}'$ with $\underline{x}, \underline{x}' \in X_m$ and $\underline{c}, \underline{c}' \in Z(\mathbf{G})^I$. We need to see that $\phi'(\underline{x})\phi_1(\underline{c}) = \phi'(\underline{x}')\phi_1(\underline{c}')$. But in X'_m we have $\underline{c}'\underline{c}^{-1} = (\underline{x}')^{-1}\underline{x} \in X_m$, so that $\phi_1(\underline{c}')\phi_1(\underline{c}^{-1}) = \phi_1(\underline{c}'\underline{c}^{-1}) = \phi'(\underline{c}'\underline{c}^{-1}) = \phi'(\underline{c}')\phi'(\underline{c}^{-1})$. From $\underline{x} = \underline{x}'\underline{c}'\underline{c}^{-1}$ and as $\underline{c}'\underline{c}^{-1} \in X_m$, we have $\phi'(\underline{x}) = \phi'(\underline{x}'\underline{c}'\underline{c}^{-1}) = \phi'(\underline{x}')\phi'(\underline{c}'\underline{c}^{-1}) = \phi'(\underline{x}')\phi_1(\underline{c}')\phi_1(\underline{c}^{-1})$, and the result follows.

Finally, continuity follows since ϕ' and ϕ_1 are continuous by assumption, \cdot is continuous since it has a finite domain and thus, ϕ_2 is a composition of continuous functions, and so is continuous. □

If ϕ_1 extends $\phi'|_{Z(\mathbf{G})^I}$, then $\phi_2 = \phi'|_{Z(\mathbf{G})^I}$. By Pontryagin duality for abelian groups of exponent m , there is a continuous $+$ -homomorphism $\phi_3: (Z_m)^I \rightarrow Z_m$ which extends ϕ_2 ; we may assume that $\phi_3 = \phi'$. Thus, if we can prove **INJ** and **STR**, then the duality will be semidirect over Z_m . We now describe \tilde{Y} , the substructure of \tilde{G}^I generated by $Z_m^I \cup (Z_{p^s} \times Z(\mathbf{G}))^I$, prove that \tilde{Y} is closed, define an extension ϕ_4 of ϕ' to \tilde{Y} and prove that ϕ_4 is a continuous homomorphism.

DEFINITION. We define Y to be $\bigcup \{Y_{\underline{b}} \mid \underline{b} \in (Z_m)^I\}$, where

- (a) for $\underline{b} \in Z(\mathbf{G})^I$, $Y_{\underline{b}} := \langle \alpha \rangle^I \underline{b}$, else
- (b) for $\underline{b} \in X_m$, $Y_{\underline{b}} := X_{\underline{b}}$, else
- (c) for $\underline{b} \in X'_m$ with $\underline{b} = \underline{b}'\underline{c}$ where $\underline{b}' \in X_m$ and $\underline{c} \in Z(\mathbf{G})^I$, $Y_{\underline{b}} := X_{\underline{b}'\underline{c}}$, else
- (d) $Y_{\underline{b}} := \langle \alpha(\underline{b}) \rangle$.

LEMMA 3.9. Y is a closed subset of \tilde{G}^I .

PROOF. Let $Y' = \bigcup \{Y_{\underline{b}} \mid \underline{b} \in X'_m\}$, and note that $Y' = X(Z(\mathbf{G}))^I$. Then $Y = \bigcup_i \langle \alpha^i(Z_m^I) \rangle \cup Y'$. As Z_m^I is closed, so is each $\langle \alpha^i(Z_m^I) \rangle$. As α has finite order, there are only finitely many such sets. Thus, we need only prove that Y' is closed. Let $\underline{y}' \notin Y'$. First suppose that $\varepsilon(\underline{y}') \notin X'_m$. As X'_m is closed, there is a finite $F_{\underline{y}'}$ $\subseteq I$ such that $\underline{z}|_{F_{\underline{y}'}} = \underline{y}'|_{F_{\underline{y}'}}$ implies that $\varepsilon(\underline{z}) \notin X'_m$, so that $\underline{z} \notin Y'$. Otherwise, let $\varepsilon(\underline{y}') = \underline{b}' = \underline{b}\underline{c}$ with $\underline{b} \in X_m$ and $\underline{c} \in Z(\mathbf{G})^I$. Define $\underline{y} := \underline{y}'\underline{c}^{-1}$ and note that $\underline{y} \in Y_{\underline{b}} - X$. As X is closed, there is a finite $F_{\underline{y}} \subseteq I$ such that $\underline{z}|_{F_{\underline{y}}} = \underline{y}|_{F_{\underline{y}}}$ implies that $\underline{z} \notin X$. Hence, if

$\underline{z}'|_{F_y} = \underline{y}'|_{F_y}$, then $\underline{z}'\underline{c}^{-1}|_{F_y} = \underline{y}|_{F_y}$ and so $\underline{z}'\underline{c}^{-1} \notin Y_b$ implying that $\underline{z}' \notin Y'$. That is, we have shown that if $\underline{y}' \notin Y'$, then there is an open neighbourhood of \underline{y}' disjoint from Y' , so that Y' is closed. \square

LEMMA 3.10. Y is a substructure of \tilde{G}^I .

PROOF. This readily follows from Lemma 3.7. \square

DEFINITION. We define $\phi_4: Y \rightarrow G$ by choosing $\underline{y} \in Y_b$ where $\underline{b} \in Z_m^I$:

- (a) for $\underline{b} \in Z(\mathbf{G})^I$, define $\phi_4(\underline{y}) := \phi_1(\underline{y})$, else
- (b) for $\underline{b} \in X_m$, define $\phi_4(\underline{y}) := \phi'(\underline{y})$, else
- (c) for $\underline{b} \in X'_m$ with $\underline{b} = \underline{b}'\underline{c}$ where $\underline{b}' \in X_m$ and $\underline{c} \in Z(\mathbf{G})^I$, define $\phi_4(\underline{y}) := \phi'(\underline{y}\underline{c}^{-1})\phi_1(\underline{c})$, else
- (d) $\underline{b} \in Z_m^I - X'_m$ with $\alpha(\underline{b}) = \underline{a}\underline{b}$ for some $\underline{a} \in \langle a^i \rangle^I$ so that $\underline{y} = (\underline{a}^i)\underline{b}$ for some i , and we define $\phi_4(\underline{y}) := \phi_1(\underline{a}^i)\phi_3(\underline{b})$.

LEMMA 3.11. $\phi_4 \in \text{Hom}(\tilde{Y}, \tilde{G})$.

PROOF. We have already proved that \tilde{Y} is a closed substructure of \tilde{G}^I . Inspection of the definition of ϕ_4 shows that it is a function from Y into G . Since ϕ_4 extends ϕ_3 , it preserves $+$, and since ϕ_4 extends ϕ_1 , it preserves \circ . It is easily checked that ϕ_4 preserves $*$ on each Y_b . For $*$, cases (a) - (c) are straightforward; we prove case (d). Note that both \underline{b} and $\underline{b}\underline{c}$ fall into case (d). Let $\underline{y} \in Y$ and $\underline{c} \in Z(\mathbf{G})^I$; we must show that $\phi_4(\underline{y} \star \underline{c}) = \phi_4(\underline{y}) \star \phi_4(\underline{c})$. Thus, $\phi_4(\underline{y} \star \underline{c}) = \phi_4(\underline{y}\underline{c}) = \phi_4(\underline{a}^i(\underline{b}\underline{c})) = \phi_1(\underline{a}^i)\phi_3(\underline{b}\underline{c}) = (\phi_1(\underline{a}^i)\phi_3(\underline{b}))\phi_3(\underline{c}) = \phi_4(\underline{a}^i)\phi_1(\underline{c}) = \phi_4(\underline{y})\star\phi_4(\underline{c})$. Finally, using the fact that α fixes each element of $Z_m \times Z(\mathbf{G})$ and that α commutes with multiplication by any element of $Z(\mathbf{G})^I$, we see that ϕ_4 preserves α . That is, ϕ_4 is a homomorphism. For continuity, recall that $Y = \bigcup_i \langle a^i(Z_m^I) \rangle \cup X(Z(\mathbf{G}))^I$. Now, $\phi_4|_{\langle Z_m \rangle^I} = \phi_3$ is continuous. Likewise for each i , $\phi_4|_{\langle a^i(Z_m^I) \rangle}$ is continuous. Next, note that for $\underline{y} \in Y_{\underline{b}\underline{c}}$ where $\underline{b} \in X_m$ and $\underline{c} \in Z(\mathbf{G})^I$, $\phi_4(\underline{y}) = \phi'(\underline{y}\underline{c}^{-1})\phi_1(\underline{c})$ is the composition of continuous functions and so is continuous. Thus, we have decomposed Y into finitely many closed sets such that the restriction of ϕ_4 to each is continuous. Consequently, ϕ_4 is continuous. \square

THEOREM 3.12. Without loss of generality, we may assume that $Z_m^I \cup (Z_{p^\#} \times Z(\mathbf{G}))^I \subseteq X$.

PROOF. By Lemma 3.9 - Lemma 3.11, \tilde{Y} is a closed substructure of \tilde{G}^I containing \tilde{X} , and $\phi_4 \in \text{Hom}(\tilde{Y}, \tilde{G})$ extends ϕ' . We need to verify that for $\underline{y} \in Y - X$, we could have chosen ϕ_4 so that $\phi_4(\underline{y}) \neq 1$. If $\underline{y} \in (Z_{p^\#} \times Z(\mathbf{G}))^I$, then we could have chosen ϕ_1 so that $\phi_4(\underline{y}) = \phi_1(\underline{y}) \neq 1$. Now let $\underline{y} \in Y_b$ for $\underline{b} \notin Z(\mathbf{G})^I$. As $Y_b \subseteq X$ for $\underline{b} \in X_m$, we have either $\underline{b} \in X'_m - X_m$ or $\underline{b} \in Z_m^I - X'_m$. In the first case, $\underline{b} = \underline{b}'\underline{c}$ with

$\underline{b}' \in X, \underline{c} \in Z(\mathbf{G})^I - X$ and $\underline{y}\underline{c}^{-1} \in X$. Then $\phi_4(\underline{y}) = \phi'(\underline{y}\underline{c}^{-1})\phi_1(\underline{c})$; if $\phi'(\underline{y}\underline{c}^{-1}) \neq 1$, then we could have taken $\phi_1(\underline{c}) = 1$, and otherwise have taken $\phi_1(\underline{c}) \neq 1$. Finally, if $\underline{b} \in Z_m^I - X'_m$, then we could have taken $\phi_3(\underline{b}) \neq 1$; as $\phi_4(\underline{y}) = a^i \phi_3(\underline{b})$ for some i , $\phi_4(\underline{y}) \neq 1$. □

THEOREM 3.13. *Let $\underline{b} \in Z_m^I$; without loss of generality, we may assume that $(a)^I \underline{b}(Z(\mathbf{G}))^I \subseteq X$.*

PROOF. We assume that $Z_m^I \cup (Z_{p^\beta} \times Z(\mathbf{G}))^I \subseteq X$. The proof is similar to that of Theorem 3.12 and the lemmas preceding it. We state, but do not prove, how to proceed. Let $Y = X \cup (a)^I \underline{b}(Z(\mathbf{G}))^I$; \tilde{Y} is a closed substructure of $(\tilde{G})^I$ containing \tilde{X} . Next, $X_{\underline{b}}$ is a closed substructure of $\langle (a)^I \underline{b}; *, \tau \rangle$, and $\phi'|_{X_{\underline{b}}}$ is a continuous homomorphism. Hence, by Pontryagin duality for abelian groups of exponent p^β , there is a continuous homomorphic extension ϕ_5 of $\phi'|_{X_{\underline{b}}}$ to $(a)^I \underline{b}$. Now define $\phi_6: Y \rightarrow G$ by $\phi_6(\underline{y}) := \phi'(\underline{y})$ for $\underline{y} \in X$, and otherwise for $\underline{y} \in X_{\underline{b}}\underline{c}$, define $\phi_6(\underline{y}) := \phi_5(\underline{y}\underline{c}^{-1})\phi'(\underline{c})$. Then ϕ_6 is a well-defined continuous homomorphism on \tilde{Y} extending ϕ' . If $\underline{y} \in Y - X$, then we may assume $\underline{y} \in (a)^I \underline{b}$ and so could have chosen ϕ_5 so that $\phi_6(\underline{y}) = \phi_5(\underline{y}) \neq 1$. □

We note two immediate corollaries.

COROLLARY 3.14. *If INJ holds, then so does STR.*

COROLLARY 3.15. *If I is finite, then this special case of INJ, where \tilde{X} is a substructure (necessarily closed) of \tilde{G}^I , holds.*

It is tempting to invoke the second corollary by noting that as ϕ' is continuous, it depends only on some finite subset $F \subseteq I$. Just project X into G^F and extend the projection of ϕ' . Unfortunately, since \tilde{G} involves proper partial functions, the projection of X need not be a substructure and the projection of ϕ' need not be extendable to a structure preserving map on G^F . We can invoke Theorem 3.13 to extend ϕ' to a homomorphism on \tilde{G}^I , but we have no reason to believe that this extension is continuous. The following lemma from [2] is the key to ensuring continuity of an extension.

LEMMA 3.16. *Let A and I be sets with A finite. Suppose that, for every finite $F \subseteq I$, each element of A^F is labeled either 'good' or 'bad' and that if $F' \subseteq F$ and $\underline{x} \in A^F$ is 'bad', then so is $\underline{x}|_{F'} \in A^{F'}$. Then either there is a finite $F \subseteq I$ such that each element of A^F is 'good' or there is an $\underline{x} \in A^I$ such that $\underline{x}|_F$ is 'bad' for each finite $F \subseteq I$.*

Let us apply Lemma 3.16 to Z_m^I . For $\underline{b} \in Z_m^I$ and finite $F \subseteq I$, define

$$\Gamma_F^{\underline{b}} := \{(\underline{x}|_F, \phi'(\underline{x})) \mid \underline{x} \in X \text{ and } \varepsilon(\underline{x}|_F) = \underline{b}|_F\}.$$

Notice that $\Gamma_F^{\underline{b}} = \Gamma_F^{\underline{b}'}$ if $\underline{b}|_F = \underline{b}'|_F$. Call $\underline{b}|_F$ ‘good’ if $\Gamma_F^{\underline{b}}$ is a subset of the graph of a $*$ -preserving map defined on $\varepsilon^{-1}(\underline{b}|_F) = \varepsilon^{-1}(\underline{b})|_F$; otherwise, call $\underline{b}|_F$ ‘bad’. Let $F' \subseteq F$ and let π denote the natural restriction map from $\varepsilon^{-1}(\underline{b})|_F$ to $\varepsilon^{-1}(\underline{b})|_{F'}$. If γ is an extension of $\Gamma_{F'}^{\underline{b}}$ to a $*$ -preserving map on the $*$ -substructure generated by $\varepsilon^{-1}(\underline{b}|_{F'})$, then $\gamma \circ \pi$ is an extension of $\Gamma_F^{\underline{b}}$ to a $*$ -preserving map on the $*$ -substructure generated by $\varepsilon^{-1}(\underline{b}|_F)$. Hence ‘badness’ is hereditary in the sense required by Lemma 3.16. Thus, by Lemma 3.16, either

- (a) there is a finite subset F of I such that every member \underline{b} of Z_m^F is ‘good’,
- or
- (b) there exists $\underline{b} \in Z_m^I$ such that for all finite $F \subseteq I$, $\underline{b}|_F$ is ‘bad’.

LEMMA 3.17. *Case (b) cannot occur.*

PROOF. Assume that $\underline{b} \in Z_m^I$ such that for all finite $F \subseteq I$, $\underline{b}|_F$ is ‘bad’; that is, for every finite subset F of I , the set

$$\Gamma_F^{\underline{b}} = \{(\underline{x}|_F, \phi'(\underline{x})) \mid \underline{x} \in X \text{ and } \varepsilon(\underline{x}|_F) = \underline{b}|_F\}$$

is not a subset of a $*$ -preserving map defined on the $*$ -substructure generated by $\varepsilon^{-1}(\underline{b}|_F)$. Define $Y := X \cup \langle a \rangle \underline{b}(Z(\mathbf{G}))^I$. Then by Theorem 3.13, \tilde{Y} is a closed substructure of \tilde{G}^I and ϕ' can be extended to a continuous homomorphism ϕ'' on \tilde{Y} . Consequently, ϕ'' depends only on some finite $F \subseteq I$; that is, for $\underline{x}, \underline{x}' \in Y$ with $\underline{x}|_F = \underline{x}'|_F$, we have $\phi''(\underline{x}) = \phi''(\underline{x}')$. Since $\varepsilon(\underline{b}|_F) = \varepsilon(\underline{b})|_F$ and since $\varepsilon^{-1}(\underline{b}) \subseteq Y$, we have

$$\begin{aligned} \Gamma_F^{\underline{b}} &= \{(\underline{x}|_F, \phi'(\underline{x})) \mid \underline{x} \in X \text{ and } \varepsilon(\underline{x}|_F) = \underline{b}|_F\} \\ &\subseteq \{(\underline{x}|_F, \phi''(\underline{x})) \mid \underline{x} \in Y \text{ and } \varepsilon(\underline{x}|_F) = \underline{b}|_F\} \\ &= \{(\underline{x}|_F, \phi''(\underline{x})) \mid \underline{x} \in \langle a \rangle^I(\underline{b})\}. \end{aligned}$$

But this latter set is the projection of the graph of a $*$ -homomorphism on a total $*$ -algebra, and so is the graph of a $*$ -homomorphism on $\langle a \rangle^F$ which extends $\Gamma_F^{\underline{b}}$, contrary to assumption. This contradiction shows that Case (b) cannot occur. □

Thus, we are left with Case (a). Let F be a finite subset of I such that every member \underline{b} of Z_m^F is good. Let Y be the $*$ -closure of $X|_F$ in G^F .

LEMMA 3.18. *\tilde{Y} is a closed substructure of \tilde{G}^F .*

PROOF. As \tilde{G}^F is finite, every subset is closed. By assumption, Y is closed under $*$. As $Z_m^I \cup (Z_{p^\beta} \times (Z(\mathbf{G}))^I) \subseteq X$, $Z_m^F \cup (Z_{p^\beta} \times (Z(\mathbf{G}))^F) \subseteq X|_F$; thus, Y is closed under $+$ and \circ . As X is closed under $*$ and contains $Z(\mathbf{G})^I$, it is clear that Y is closed under $*$. For closure under α , let $\underline{ab}, \underline{a'b} \in X|_F$. Then $\alpha(\underline{a'b}) = \underline{a'\alpha(b)} \in X|_F$ and $\underline{aa'b} \in Y$. Thus, $\alpha(\underline{aa'b}) = \underline{aa'\alpha(b)} = \underline{ab} * \alpha(\underline{a'b}) \in Y$. Inductively, we see that Y is closed under α . □

Next, we want to define a homomorphism $\psi: \tilde{Y} \rightarrow \tilde{G}$ whose graph extends the union of the $\Gamma_F^{\underline{b}}$. By our assumption on F , we can do this on each $Y_{\underline{b}} := Y \cap \langle a \rangle^F \underline{b}$ for each $\underline{b} \in Z_m^F$. But unless we take care, we will not preserve $*$. Let $\psi_{\underline{b}}: Y_{\underline{b}} \rightarrow G$ be one such extension. Then for each $\underline{c} \in Z(\mathbf{G})^F$, we must define $\psi_{\underline{bc}}(\underline{y}) := \psi_{\underline{b}}(\underline{y}\underline{c}^{-1})\underline{c}$. With this definition used for all cosets of $Z(\mathbf{G})^F$ in Z_m^F , we can readily verify that ψ extends the union of the $\Gamma_F^{\underline{b}}$ and is a homomorphism. Since F is finite, ψ is automatically continuous.

THEOREM 3.19. *INJ holds in $\mathbb{I}\mathbb{S}_c\mathbb{P}(\tilde{G})$.*

PROOF. By Corollary 3.15, we can extend ψ to a continuous homomorphism $\phi_F: G^F \rightarrow G$. Now define ϕ so that for $\underline{x} \in G^I$, $\phi(\underline{x}) := \phi_F(\underline{x}|_F)$. Then ϕ is a continuous homomorphism extending ϕ' . □

THEOREM 3.20. *The structure \tilde{G} yields a strong duality semidirect over Z_m on $\mathbb{I}\mathbb{S}\mathbb{P}(\mathbf{G})$, where $\mathbf{G} = Z_{p^\beta} \rtimes Z_m$ with $(m, p) = 1$.*

PROOF. By Theorem 3.5, condition **CLO** holds. By Theorem 3.19, condition **INJ** holds. By Corollary 3.14, condition **STR** holds. □

THEOREM 3.21. *Groups having all Sylow subgroups cyclic are dualizable.*

PROOF. By Theorem 2.1 all these groups \mathbf{G} can be represented as a semidirect product of cyclic groups $\mathbf{G} = Z_m \rtimes Z_n$ where $(m, n) = 1$. If $m = \prod p_i^{a_i}$, then $Z_m = \prod Z_{p_i^{a_i}}$, where $(p_i, n) = 1$. As by Theorem 3.20 there is a strong duality for the groups $Z_{p_i^{a_i}} \rtimes Z_m$, Theorem 2.3 implies that \mathbf{G} is dualizable. □

In a companion article [4] we prove that no finite group containing a non-abelian nilpotent subgroup is dualizable. That is, in order for a finite group to be dualizable, it must have abelian Sylow subgroups. From Olshanskii [3] we know that these are exactly the finite groups generating residually small varieties. We conjecture that every finite group with abelian Sylow subgroups is dualizable. We have only rudimentary results in this direction; for instance, we know that the alternating group A_5 is dualizable.

References

- [1] D. M. Clark and B. A. Davey, *Natural dualities for the working algebraist* (CUP, Cambridge, 1998).
- [2] B. A. Davey and R. W. Quackenbush, 'Natural duality for dihedral groups', *J. Austral. Math. Soc. (Ser. A)* **61** (1996), 216–228.
- [3] A. Ju. Olshanskii, 'Varieties of finitely approximable groups', *Math. USSR—Izvestia* **3** (1969), 867–877.
- [4] R. Quackenbush and Cs. Szabó, 'Nilpotent groups are not dualizable', *J. Aust. Math. Soc.* **72** (2001), 173–179.
- [5] D. J. S. Robinson, *A course in the theory of groups* (Springer, New York, 1982).

Department of Mathematics
University of Manitoba
Winnipeg, Manitoba R3T 2N2
Canada
e-mail: qbush@cc.umanitoba.ca

Department of Algebra and Number Theory
ELTE
Budapest
Hungary
e-mail: csaba@cs.elte.hu