GROUPS WITH IDENTICAL SUBGROUP LATTICES IN ALL POWERS

KEITH A. KEARNES AND ÁGNES SZENDREI

Abstract. Suppose that G and H are groups with cyclic Sylow subgroups. We show that if there is an isomorphism $\lambda_2 \colon \mathrm{Sub}\,(G \times G) \to \mathrm{Sub}\,(H \times H)$, then there are isomorphisms $\lambda_k \colon \mathrm{Sub}\,(G^k) \to \mathrm{Sub}\,(H^k)$ for all k. But this is not enough to force G to be isomorphic to H, for we also show that for any positive integer N there are pairwise nonisomorphic groups $G_1, \ldots, G_N$ defined on the same finite set, all with cyclic Sylow subgroups, such that $\mathrm{Sub}\,(G_i^k) = \mathrm{Sub}\,(G_j^k)$ for all i, j, k.

1. Introduction

To what extent is a finite group determined by the subgroup lattices of its finite direct powers? Reinhold Baer proved results in 1939 implying that an abelian group G is determined up to isomorphism by $\mathrm{Sub}\,(G^3)$ (cf. [1]). Michio Suzuki proved in 1951 that a finite simple group G is determined up to isomorphism by $\mathrm{Sub}\,(G^2)$ (cf. [10]). Roland Schmidt proved in 1981 that if G is a finite, perfect, centerless group, then it is determined up to isomorphism by $\mathrm{Sub}\,(G^2)$ (cf. [6]). Later, Schmidt proved in [7] that if G has an elementary abelian Hall normal subgroup that equals its own centralizer, then G is determined up to isomorphism by $\mathrm{Sub}\,(G^3)$. It has long been open whether every finite group G is determined up to isomorphism by $\mathrm{Sub}\,(G^3)$. (For more information on this problem, see the books [8, 11].)

One may ask more generally to what extent a finite algebraic structure (or **algebra**) is determined by the subalgebra lattices of its finite direct powers. If $\mathbf{A} = (X; F)$ is an algebra on a finite set X with defining operations F, then a function $t \colon X^n \to X$ is called a **term operation** of $\mathbf{A}$ if t can be obtained from the operations in F by composition. It is known (Corollary 1.4 of [12]) that if $\mathbf{A}$ and $\mathbf{B}$ are algebras defined on the same finite set X, then $\mathrm{Sub}\,(A^k) = \mathrm{Sub}\,(B^k)$ for all finite k if and only if $\mathbf{A}$ and $\mathbf{B}$ have the same term operations (in which case we say that they are **term equivalent**). While this is as complete an answer as can be expected for arbitrary finite algebras, it raises natural questions about groups.

1991 *Mathematics Subject Classification.* Primary 20E15, Secondary 20D30, 08A40.

Key words and phrases. Identical subgroup lattices, term equivalence, weak isomorphism.

This material is based upon work supported by the Hungarian National Foundation for Scientific Research (OTKA) grants no. T 034175, and T37877.

Problem 1.1. [13] Must term equivalent finite groups be isomorphic?

Problem 1.2. If G and H are finite groups defined on the same set and $\mathrm{Sub}\,(G^3) = \mathrm{Sub}\,(H^3)$, must G and H be term equivalent?

Problem 1.3. If G and H are finite groups defined on possibly different sets and $\mathrm{Sub}\,(G^k) \cong \mathrm{Sub}\,(H^k)$ for all finite k, then must G be isomorphic to a group that is term equivalent to H? (I.e., must G be **weakly isomorphic** to H?)

In this paper we solve Problem 1.1 negatively. Our counterexamples show that, contrary to expectation, a finite group is not determined up to isomorphism by the subgroup lattices of its finite direct powers. In [3] we answer Problem 1.2 affirmatively for finite groups with abelian Sylow subgroups. We do not know the full answer to Problem 1.3, but we show here that if G and H have cyclic Sylow subgroups and $\mathrm{Sub}\,(G^2) \cong \mathrm{Sub}\,(H^2)$ then G must be weakly isomorphic to H.

2. Groups with cyclic Sylow subgroups

It is well known (see e.g. [5], p. 281) that if G is a finite group whose Sylow subgroups are cyclic, then

- the commutator subgroup G' of G has odd order, and G' is the product of some normal Sylow subgroups of G, hence
- G' and G/G' are cyclic groups of relatively prime order.

Therefore G is a semidirect product $G_0 \times_\varphi G'$ of G' by a cyclic subgroup $G_0 \cong G/G'$ of G. This means that, up to isomorphism, $G' = P_1 \times \cdots \times P_k$ is a product of cyclic groups of relatively prime, odd, prime power order, G_0 is cyclic with order relatively prime to $|G'|$, and the structure of $G = G_0 \times_\varphi G'$ is determined by a homomorphism

$$\varphi\colon G_0 \to \mathrm{Aut}\,(G') = \mathrm{Aut}\,(P_1 \times \cdots \times P_k) = \mathrm{Aut}\,(P_1) \times \cdots \times \mathrm{Aut}\,(P_k).$$

Any such homomorphism φ is determined by its components $\varphi_i\colon G_0 \to \mathrm{Aut}\,(P_i)$. It is easy to see that, in order for the semidirect product $G_0 \times_\varphi G'$ determined by the data G_0, $G' = P_1 \times \cdots \times P_k$, and $\varphi = (\varphi_1, \ldots, \varphi_k)$ to be a group whose commutator subgroup is exactly G', it is necessary and sufficient that all of the component functions φ_i be nonconstant (i.e., $|\varphi_i(G_0)| > 1$ for all i).

We cite a theorem below (Theorem 2.1) which says essentially this: if G_0 and $G' = P_1 \times \cdots \times P_k$ are fixed as above, and $\varphi = (\varphi_1, \ldots, \varphi_k)$ and $\psi = (\psi_1, \ldots, \psi_k)$ are homomorphisms $\varphi, \psi\colon G_0 \to \mathrm{Aut}\,(G')$ that determine two semidirect products of G' by G_0 in the manner just described (whose commutator subgroups are both G'), then the resulting semidirect products are isomorphic if and only if φ and ψ have the same image. (I.e., iff $\varphi(G_0) = \psi(G_0)$.) One of the main results that we prove in this section (Corollary 2.11) says essentially this: the resulting semidirect products are weakly isomorphic if and only if the component functions φ_i and ψ_i have the same image for all i. $\big($I.e., iff $\varphi_i(G_0) = \psi_i(G_0)$ for all i.$\big)$ Notice the difference in the conditions: if $\varphi(G_0) = \psi(G_0)$ then $\varphi_i(G_0) = \psi_i(G_0)$ for all i, since the latter are obtained from the former by projection. But the conditions $\varphi_i(G_0) = \psi_i(G_0)$ for all i imply only that $\varphi(G_0)$ and $\psi(G_0)$ are subdirect products of the same factor groups. The flexibility of the subdirect product construction allows us to construct examples where $\varphi(G_0) \neq \psi(G_0)$ even though $\varphi_i(G_0) = \psi_i(G_0)$ for all i, and hence to construct term equivalent groups that are not isomorphic.

Our goals are to do more than construct such examples. The tools used to construct these examples also apply to show that if G and H are groups with cyclic Sylow subgroups, and there is a lattice isomorphism $\lambda\colon \mathrm{Sub}\,(G) \to \mathrm{Sub}\,(H)$ that is **cardinality-preserving** in the sense that $|\lambda(S)| = |S|$ for every subgroup $S \subseteq G$, then G is weakly isomorphic to H. We show further that if G and H are groups with cyclic Sylow subgroups, and there is a lattice isomorphism $\lambda\colon \mathrm{Sub}\,(G^2) \to \mathrm{Sub}\,(H^2)$ (which is not assumed to be cardinality-preserving), then G is weakly isomorphic to H. To reach these goals we need to introduce some notation that allows us to compare two groups on different underlying sets.

Since G' is cyclic, the automorphisms of G' are the functions of the form $x \mapsto x^r$ for some fixed r satisfying $1 \leq r < |G'|$ and $\gcd(r, |G'|) = 1$. Hence the mapping that assigns to every automorphism of G' the corresponding exponent r mod $|G'|$ is an isomorphism between $\mathrm{Aut}\,(G')$ and the group $\mathbf{Z}^*_{|G'|}$ of units modulo $|G'|$. The isomorphism referred to here will be called the **standard isomorphism** between $\mathrm{Aut}\,(G')$ and $\mathbf{Z}^*_{|G'|}$. We will use the same language when refer to the isomorphism between $\mathrm{Aut}\,(P)$ and $\mathbf{Z}^*_{|P|}$ where P is a Sylow subgroup contained in G'.

Now suppose that G and H are finite groups whose Sylow subgroups are cyclic. There is a simple criterion for G and H to be isomorphic.

Theorem 2.1. (Exercise 10.1.9 of [5]) *Let $G = G_0 \times_\varphi G'$ and $H = H_0 \times_\psi H'$ be finite groups whose Sylow subgroups are cyclic. Then $G \cong H$ if and only if*

(a) $|G| = |H|$, $|G'| = |H'|$, *and*
(b) $\varphi(G_0)$ *and* $\psi(H_0)$ *are corresponding subgroups of* $\mathrm{Aut}\,(G')$ *and* $\mathrm{Aut}\,(H')$ *under the standard isomorphisms* $\mathrm{Aut}\,(G') \cong \mathbf{Z}^*_{|G'|} \cong \mathrm{Aut}\,(H')$.

In [2], Honda found a necessary and sufficient condition for the existence of a cardinality-preserving isomorphism between the subgroup lattices of G and H provided all Sylow subgroups of G and H are cyclic. Using the semidirect decomposition of G and H as in Theorem 2.1 we can rephrase Honda's criterion as follows.

Theorem 2.2. *Let $G = G_0 \times_\varphi G'$ and $H = H_0 \times_\psi H'$ be finite groups whose Sylow subgroups are cyclic. Write $G' = P_1 \times \cdots \times P_k$ and $H' = Q_1 \times \cdots \times Q_l$ as products of Sylow subgroups, and write $\varphi = (\varphi_1, \ldots, \varphi_k)$ and $\psi = (\psi_1, \ldots, \psi_l)$ in terms of their components. There exists a cardinality-preserving isomorphism between the subgroup lattices of G and H if and only if*

(a) $|G| = |H|$, $|G'| = |H'|$, *and*
(b) *if* $|P_i| = |Q_j|$, *then the subgroup* $\varphi_i(G_0)$ *of* $\mathrm{Aut}\,(P_i)$ *has the same order as the subgroup* $\psi_j(H_0)$ *of* $\mathrm{Aut}\,(Q_j)$.

Note that since G' has odd order, the automorphism groups $\mathrm{Aut}\,(P_i) \cong \mathbf{Z}^*_{|P_i|} \cong \mathrm{Aut}\,(Q_j)$ are cyclic. Therefore the condition in (b) is equivalent to requiring that $\varphi_i(G_0)$ and $\psi_j(H_0)$ are corresponding subgroups of $\mathrm{Aut}\,(P_i)$ and $\mathrm{Aut}\,(Q_j)$ under the standard isomorphisms $\mathrm{Aut}\,(P_i) \cong \mathbf{Z}^*_{|P_i|} \cong \mathrm{Aut}\,(Q_j)$.

Example 2.3. Suppose that $\lambda\colon \mathrm{Sub}\,(G) \to \mathrm{Sub}\,(H)$ is an isomorphism. It is clear that if λ is cardinality-preserving, then $|G| = |H|$. The converse is not true, even for finite groups G, H whose Sylow subgroups are cyclic. Indeed, let p_1, p_2, p_3 be distinct primes such that $p_1p_2 \mid p_3 - 1$, and for $i = 1, 2$ let $G_i = S_i \times Z_i$ where S_i is a noncommutative group of order p_ip_3 and Z_i (the center of G_i) is a cyclic group of order p_{3-i}. Then $|G_1| = |G_2| = p_1p_2p_3$, and for each $i = 1, 2$, the subgroup lattice of G_i is the direct product of the subgroup lattices of S_i and Z_i. Thus the subgroup lattice of G_1 as well as that of G_2 is isomorphic to the direct product of the height 2 lattice with $p_3 + 1$ atoms and the 2-element chain. However, every isomorphism λ between the subgroup lattices of G_1 and G_2 must map Z_1 to Z_2, because Z_i is the only atom in the subgroup lattice of G_i that has more than two covers. Therefore λ is not cardinality-preserving.

In [9], A. P. Street used Honda's theorem to construct a group G and a binary term $\circ$ in the language of G so that $(G; \circ)$ is also a group, and there exists a cardinality-preserving isomorphism between the subgroup lattices of G and $(G; \circ)$, although G and $(G; \circ)$ are not isomorphic. It is not stated or proved in [9], but one can show that the group $(G; \circ)$ in this example is term equivalent to G. In Theorem 2.10 below we will prove that if finite groups G and H have cyclic Sylow subgroups and a cardinality-preserving isomorphism between their subgroup lattices, then G is weakly isomorphic to H.

If G is a group, then we will call a binary term $\circ$ in the language of G a **group term for** G if $\circ$ induces a group operation on G. To prepare for Theorem 2.10 we prove a type of "Chinese Remainder Theorem" that shows how to find a single group term on a group G from given group terms on some quotients of G. The upcoming lemma will concern the situation where G has normal subgroups $M_1, \ldots, M_k$ satisfying the conditions

- $|M_i|$ and $|M_j|$ are relatively prime for all $i \neq j$, and
- G/K is abelian, where $K = M_1 \cdots M_k$ is the join of the M_i.

Part of the normal subgroup lattice of G is depicted in Figure 1 for the case $k = 3$.

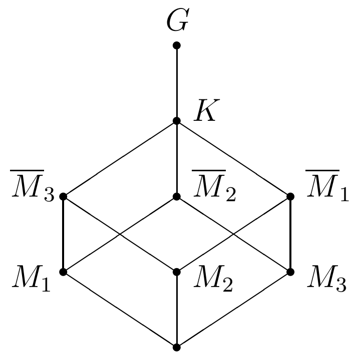

FIGURE 1

If $\overline{M}_i = M_1 \cdots M_{i-1}M_{i+1} \cdots M_k$, and $\circ_i$ is a group term for $G/\overline{M}_i$ for each i, then the lemma proves that there is a single group term $\circ$ for G such that $x \circ y = x \circ_i y$ in $G/\overline{M}_i$ for all i.

Lemma 2.4. *Let G be a finite group, let M_i $(i = 1, \ldots, k)$ be normal subgroups of G of pairwise relatively prime order such that G/K is abelian for $K = M_1 \cdots M_k$. Let $\overline{M}_i = M_1 \cdots M_{i-1}M_{i+1} \cdots M_k$ $(i = 1, \ldots, k)$. Suppose that for every i, $\circ_i$ is a binary term in the language of G that is a group term for $G/\overline{M}_i$. Then*

(1) *there exists a binary term $\circ$ such that, for each i, $\circ$ induces the same operation on $G/\overline{M}_i$ as $\circ_i$;*
(2) *$\circ$ is a group term for G, and the operation induced by $\circ$ on G is uniquely determined by the requirement in (1); moreover*
(3) *if the group $(G/\overline{M}_i; \circ_i)$ is term equivalent to $G/\overline{M}_i$ for all i, then $(G; \circ)$ is term equivalent to G.*

Proof. It is easy to see that for any group H, two terms t, t' induce the same operation on H if and only if the identity $t = t'$ holds in H. Such terms will be called in this proof *H-equivalent*. It is also clear that H-equivalent terms induce the same operation on all quotients of H as well.

Let us write the binary term $\circ_i$ in the form $x \circ_i y = xyc_i(x, y)$ where $c_i(x, y) = x^{u_1}y^{v_1} \cdots x^{u_r}y^{v_r}$. Since $\circ_i$ is a group term for $G/\overline{M}_i$, the identities $x = x \circ_i 1 = x \cdot x^{u_1+\cdots+u_r}$ and $y = 1 \circ_i y = y \cdot y^{v_1+\cdots+v_r}$ hold in $G/\overline{M}_i$. Hence the identities $x^{u_1+\cdots+u_r} = 1 = y^{v_1+\cdots+v_r}$ hold in $G/\overline{M}_i$. This implies that the term

$$xyc_i(x, y)x^{-(u_1+\cdots+u_r)}y^{-(v_1+\cdots+v_r)} = xy(x^{u_1}y^{v_1} \cdots x^{u_r}y^{v_r}x^{-(u_1+\cdots+u_r)}y^{-(v_1+\cdots+v_r)})$$

is $G/\overline{M}_i$-equivalent to $\circ_i$, and in the parentheses on the right hand side the exponents of the x's and the exponents of the y's sum up to 0. Therefore we can assume without loss of generality that the term $\circ_i$ was selected so that in $c_i(x, y)$ we have $u_1 + \cdots + u_r = 0 = v_1 + \cdots + v_r$. This condition is equivalent to requiring that $c_i(x, y)$ is a product of commutators.

By assumption the orders of the normal subgroups M_i $(i = 1, \ldots, k)$ of G are pairwise relatively prime. Therefore, by the classical Chinese Remainder Theorem, there exist integers m_i such that $m_i \equiv 1 \pmod{|M_i|}$ and $m_i \equiv 0 \pmod{|M_j|}$ for all $j \neq i$. Now we define the term $\circ$ as follows:

$$x \circ y = xy\big(c_1(x,y)\big)^{m_1} \cdots \big(c_k(x,y)\big)^{m_k}.$$

To check (1) let $g, h \in G$. Since $c_i(x,y)$ is a product of commutators, $c_i(g,h)$ belongs to the commutator subgroup G' of G. However, by assumption G/K is abelian, so $G' \subseteq K$. Thus $c_i(g,h) \in K = M_1 \cdots M_k$. Since $M_1, \ldots, M_k$ are normal subgroups of pairwise relatively prime order, K is the direct product of $M_1, \ldots, M_k$. So the choice of m_i with the property that $|M_j|$ divides m_i for all $j \neq i$ implies that $\big(c_i(g,h)\big)^{m_i} \in M_i$ for all i. Moreover, since $m_i \equiv 1 \pmod{|M_i|}$, we have $\big(c_i(g,h)\big)^{m_i}\overline{M}_i = c_i(g,h)\overline{M}_i$. This shows that $\circ$ induces the same operation on $G/\overline{M}_i$ as $\circ_i$.

The intersection of the normal subgroups $\overline{M}_i$ $(i = 1, \ldots, k)$ is trivial, therefore the mapping

$$\nu\colon G \to \prod_{i=1}^{k}(G/\overline{M}_i), \quad g \mapsto (g\overline{M}_1, \ldots, g\overline{M}_k)$$

is an embedding. Since $\circ$ is a term and by the requirement in (1) we have $(G/\overline{M}_i; \circ) = (G/\overline{M}_i; \circ_i)$ for all i, the mapping ν is also an embedding of the algebra $(G; \circ)$ into the direct product of the algebras $(G/\overline{M}_i; \circ_i)$. This uniquely determines the operation induced on G by $\circ$. Furthermore, since each $(G/\overline{M}_i; \circ_i)$ is a group, and every subalgebra of a finite group is a group, we conclude that $(G; \circ)$ is a group. This finishes the proof of (2).

Finally, assume that each group $(G/\overline{M}_i; \circ) = (G/\overline{M}_i; \circ_i)$ $(i = 1, \ldots, k)$ is term equivalent to $G/\overline{M}_i$. Then for each i there is a binary term $\star_i$ in the language of the group $(G; \circ)$ such that $(G/\overline{M}_i; \star_i) = (G/\overline{M}_i; \cdot)$ where $(G/\overline{M}_i; \cdot)$ is the quotient group $G/\overline{M}_i$ with its original multiplication $\cdot$ inherited from G. Now we can apply parts (1) and (2) of this lemma to the group $(G; \circ)$ in place of G and to the groups $(G/\overline{M}_i; \star_i)$ in place of $(G/\overline{M}_i; \circ_i)$ to conclude the following: there exists a term $\star$ in the language of $(G; \circ)$ such that

$$(G/\overline{M}_i; \star) = (G/\overline{M}_i; \cdot) \quad \text{for all } i, \tag{2.1}$$

and the operation induced by $\star$ on G is the unique operation for which these equalities hold. Since the original operation of G, in place of $\star$, obviously satisfies (2.1), we get that $\star$ induces the original group operation on G. Hence $(G; \circ)$ is term equivalent to G. □

The version of Lemma 2.4 that concerns weak isomorphism rather than term equivalence is a little more complicated, but it is a version that we will find useful.

Theorem 2.5. *Let G be a finite group with normal subgroups $K, M_i, \overline{M}_i$ $(i = 1, \dots, k)$ satisfying the hypotheses of Lemma 2.4, and let H also be a finite group with normal subgroups $L, N_i, \overline{N}_i$ $(i = 1, \dots, k)$ satisfying these hypotheses. Suppose that for each $1 \le i \le k$ there is an isomorphism*

$$\beta_i \colon H/\overline{N}_i \to (G/\overline{M}_i; \circ_i)$$

where $(G/\overline{M}_i; \circ_i)$ is a group term equivalent to $G/\overline{M}_i$. If these isomorphisms satisfy $\beta_i(h\overline{N}_i)K = \beta_j(h\overline{N}_j)K$ for all $h \in H$ and all $1 \le i, j \le k$, then there is an isomorphism $\beta \colon H \to (G; \circ)$ where $(G; \circ)$ is term equivalent to G.

Proof. Since G, K, M_i and $\overline{M}_i$ satisfy the hypotheses of Lemma 2.4, there is a group term $\circ$ for G that induces the same operation on $G/\overline{M}_i$ as $\circ_i$ for each i. By part (3) of that lemma, $(G; \circ)$ is term equivalent to G. To complete the proof we must exhibit an isomorphism $\beta \colon H \to (G; \circ)$.

Since $\beta_i \colon H/\overline{N}_i \to (G/\overline{M}_i; \circ)$ is an isomorphism for all i, it follows that

$$\textstyle\prod \beta_i \colon \prod H/\overline{N}_i \to \prod (G/\overline{M}_i; \circ)$$

is an isomorphism. Since $\bigcap \overline{N}_i = \{1\}$, the natural map $\alpha \colon H \to \prod H/\overline{N}_i$ is an embedding, as is the natural map $\gamma \colon (G; \circ) \to \prod (G/\overline{M}_i; \circ)$. The desired isomorphism is $\beta = \gamma^{-1} \circ (\prod \beta_i) \circ \alpha$. To show this, it suffices to prove that β is a bijective function, and for this it suffices to prove that $\prod \beta_i$ maps the image of α bijectively onto the image of γ. In fact, since $\prod \beta_i$ is injective and α and γ are forced to have images of the same size, it suffices to prove that $\prod \beta_i$ maps the image of α into the image of γ.

The image of the natural homomorphism

$$\alpha \colon H \to \prod H/\overline{N}_i, \ h \mapsto (h\overline{N}_1, \dots, h\overline{N}_k)$$

is the set of tuples of the form $(h\overline{N}_1, \dots, h\overline{N}_k)$. If we apply $\prod \beta_i$ to such a tuple we obtain $\big(\beta_1(h\overline{N}_1), \dots, \beta_k(h\overline{N}_k)\big)$, which is a tuple of the form $(g_1\overline{M}_1, \dots, g_k\overline{M}_k)$ (since β_i maps cosets of $\overline{N}_i$ to cosets of $\overline{M}_i$). In order for this tuple to be in the image of γ, it is necessary and sufficient that it equal a tuple of the form $(g\overline{M}_1, \dots, g\overline{M}_k)$. In other words, there must exist a $g \in G$ such that $g\overline{M}_i = g_i\overline{M}_i = \beta_i(h\overline{N}_i)$ for all i. If there is such a g, then clearly

$$gK = \beta_1(h\overline{N}_1)K = \cdots = \beta_k(h\overline{N}_k)K,$$

so the condition in the theorem statement must hold. Conversely, since K is a product of the M_i, and the $\overline{M}_i$ are the kernels of the coordinate projections of this product, any sequence of cosets $g_1\overline{M}_1, \dots, g_k\overline{M}_k$ contained in the same coset of K have a common coset representative. Thus, if $\beta_1(h\overline{N}_1)K = \cdots = \beta_k(h\overline{N}_k)K$, then there is a g such that $g\overline{M}_i = \beta_i(h\overline{N}_i)$ for all i. This completes the proof that β is an isomorphism. □

For later applications let us analyze what it means in Theorem 2.5 that the isomorphisms $\beta_1, \dots, \beta_k$ satisfy the condition that

$$\beta_i(h\overline{N_i})K = \beta_j(h\overline{N_j})K \quad \text{for all } h \in H \text{ and all } 1 \le i, j \le k. \tag{2.2}$$

Suppose all other assumptions of Theorem 2.5 hold for $G, K, M_i, \overline{M}_i$ and $H, L, N_i, \overline{N}_i$ and the isomorphisms β_i ($i = 1, \dots, k$). Note that these assumptions force $|G| = |H|$, $|K| = |L|$, and $|M_i| = |N_i|$, $|\overline{M}_i| = |\overline{N}_i|$ for all i.

If condition (2.2) is satisfied, then for any element $l = n_1 \cdots n_k$ from $L = N_1 \cdots N_k$ ($n_i \in N_i$) and for arbitrary indices $i \neq j$ we have

$$\beta_i(l\overline{N_i})K = \beta_i(n_i\overline{N_i})K = \beta_j(n_i\overline{N_j})K = \beta_j(\overline{N}_j)K = \overline{M}_jK = K.$$

Thus each β_i maps the normal subgroup $L/\overline{N}_i$ of $H/\overline{N}_i$ into the normal subgroup $K/\overline{M}_i$ of $G/\overline{M}_i$. For cardinality reasons the map is onto. Hence

$$\beta_i(L/\overline{N}_i) = K/\overline{M}_i \quad \text{for all } i. \tag{2.3}$$

Thus β_i induces an isomorphism between the quotient of $H/\overline{N}_i$ modulo $L/\overline{N}_i$ and the quotient of $(G/\overline{M}_i; \circ_i)$ modulo $K/\overline{M}_i$. Alternatively, (2.3) implies that each β_i induces an isomorphism

$$\overline{\beta}_i \colon H/L \to (G/K; \circ_i), \quad hL \mapsto \beta_i(h\overline{N}_i)K.$$

Now condition (2.2) can be restated in terms of the $\overline{\beta}_i$ as follows: $\overline{\beta}_i(hL) = \overline{\beta}_j(hL)$ for all $h \in H$ and $1 \le i, j \le k$. Equivalently,

$$\overline{\beta}_1 = \cdots = \overline{\beta}_k. \tag{2.4}$$

This shows that condition (2.2) implies conditions (2.3) and (2.4). The converse is also true: if (2.3) and (2.4) hold for the β_i, then (2.3) ensures that the induced isomorphisms $\overline{\beta}_i$ exist, and as was observed earlier, (2.4) just restates condition (2.2) in terms of the $\overline{\beta}_i$. This proves that condition (2.2) is equivalent to the conjunction of conditions (2.3) and (2.4).

Next we prove a lemma on term equivalent groups that will imply that under the assumptions on $G, K, M_i, \overline{M}_i$ as above, every operation $\circ_i$ on G/K coincides with the original operation $\cdot$ on G/K.

Lemma 2.6. *If $G = (G; \cdot)$ is a finite group and $(G; \circ)$ is a group term equivalent to G, then*

1. *G and $(G; \circ)$ have the same subgroups, the same normal subgroups, and the same sections;*
2. *the operation $\circ$ coincides with the original group operation $\cdot$ on every abelian section of G; and*
3. *a section is abelian as a section of G if and only if it is abelian as a section of $(G; \circ)$.*

Proof. Since G and $(G;\circ)$ are term equivalent, they have the same subgroups, and G^2 and $(G^2;\circ)$ have the same subgroups that are equivalence relations on G. The latter means that G and $(G;\circ)$ have the same congruences, hence the same normal subgroups. If S is a subgroup $\big($of both G and $(G;\circ)\big)$, then S and $(S;\circ)$ are also term equivalent, and hence they have the same normal subgroups. Thus G and $(G;\circ)$ have the same sections. This proves (1).

To prove (2), recall that by the argument at the beginning of the proof of Lemma 2.4, we can express $\circ$ in terms of the original operation $\cdot$ of G as follows: $x \circ y = xyc(x,y)$ for all $x, y \in G$ where $c(x,y)$ is a product of commutators. The same equality holds for all elements x, y of any section S/N of G as well. Therefore, if S/N is abelian, then $x \circ y = xy$ for all $x, y \in S/N$. Item (3) follows from (2). $\square$

By assumption, the groups $(G/\overline{M}_i;\circ_i)$ and $G/\overline{M}_i$ are term equivalent, and the quotient G/K of $G/\overline{M}_i$ is abelian, therefore by Lemma 2.6, the operations $\circ_i$ and $\cdot$ coincide on G/K. Thus the target group $(G/K;\circ_i)$ of each $\overline{\beta}_i$ is in fact the group G/K with its original operation inherited from G. Hence the $\overline{\beta}_i$'s are all isomorphisms from H/L to G/K. So, to check that the $\overline{\beta}_i$'s are equal, it suffices to check on a generating set for H/L. In symbols, it suffices to check that for some elements $h_1, \dots, h_t$ such that $h_1L, \dots, h_tL$ generate H/L, we have

$$\overline{\beta}_1(h_jL) = \cdots = \overline{\beta}_k(h_jL) \quad \text{for all } j,$$

or, equivalently,

$$\beta_1(h_j\overline{M}_1)K = \cdots = \beta_k(h_j\overline{M}_k)K \quad \text{for all } j. \tag{2.5}$$

If $G = K$ (and hence $H = L$) in Theorem 2.5, then condition (2.2) is automatically satisfied. Thus we get the following corollary.

Corollary 2.7. *Assume that G_i $(i = 1, \dots, k)$ are finite groups of pairwise relatively prime order. If G_i is weakly isomorphic to H_i for each i, then $G = \prod G_i$ is weakly isomorphic to $H = \prod H_i$.*

Next we study the relation of term equivalence within the class of subdirectly irreducible finite groups with cyclic Sylow subgroups.

Let p be a prime, $n \geq 1$, and let $1 \leq r < p^n$ be an integer such that neither r nor its order m modulo p^n is divisible by p. Let $\mathcal{G}_{p^n,r}(a,c)$ denote the group generated by the elements a, c subject to the relations

$$a^{p^n} = 1, \quad c^m = 1, \quad \text{and} \quad c^{-1}ac = a^r.$$

The lemma below summarizes some basic properties of this group. The case $r = 1$ when $\mathcal{G}_{p^n,r}(a,c)$ is the cyclic group $\langle a \rangle$ of order p^n will be excluded from the lemma.

Lemma 2.8. *If p is a prime, $n \geq 1$, and $2 \leq r < p^n$ is an integer such that neither r nor its order m modulo p^n is divisible by p, then the group $G = \mathcal{G}_{p^n,r}(a,c)$ has the following properties.*

(1) *The cyclic group* $P = \langle a\rangle$ *is a normal Sylow* p*-subgroup of* G*, and* $G_0 = \langle c\rangle$ *is a complement of* P *in* G*.*
(2) *The Sylow subgroups of* G *are cyclic and* $G' = P$*.*
(3) $G = P \cup \bigcup\bigl(a^{-l}G_0a^l : 0 \le l < p^n\bigr)$*.*
(4) *The order of every element of* $G \setminus P$ *divides* m*.*
(5) G *is subdirectly irreducible with minimal normal subgroup* $\langle a^{p^{n-1}}\rangle$*.*

Proof. (1) follows from the defining relations of G. Thus every element of G can be written uniquely in the form c^ia^j with $0 \le i < m$ and $0 \le j < p^n$. For elements of this form we have

$$(c^ia^j)(c^ka^l) = c^{i+k}a^{r^kj+l}.$$

In particular, $a^{-l}c^ia^l = c^ia^{(1-r^i)l}$. It is easy to check that $r^i \not\equiv 1 \pmod p$ for all $1 \le i < m$. For, otherwise, the order d of r modulo p is a proper divisor of m, and $r^d = 1+pt$ for some integer t. Hence $(r^d)^{p^{n-1}} \equiv 1 \pmod{p^n}$. Thus $d \ne m \mid dp^{n-1}$, implying that $p \mid m$. This contradicts our assumption on m, and proves $r^i \not\equiv 1 \pmod p$ for all $1 \le i < m$. The consequence of this is that every element of G of the form c^ia^j ($1 \le i < m$, $0 \le j < p^n$) is a conjugate of c^i by a unique power a^l of a. This proves (3). (4) follows immediately from (3).

If M is a normal subgroup of G such that $M \not\subseteq P$, then by (3) there is an element c^i with $1 \le i < m$ such that $a^{-l}c^ia^l \in M$ for some, and hence for all l. We saw in the preceding paragraph that $\{a^{-l}c^ia^l : 0 \le l < p^n\} = \{c^ia^j : 0 \le j < p^n\}$. Since the elements of this set belong to M and include c^i, it follows that $P \subseteq M$. Thus every normal subgroup of P is comparable to P, so G has a unique minimal normal subgroup: the subgroup of P of order p. This proves (5).

Finally, we prove (2). The fact that the Sylow subgroups of G are cyclic follows from (1) and the assumption that m is not divisible by p. Thus G' is the product of some normal Sylow subgroups. However, every normal subgroup of G is comparable to P, therefore the only normal Sylow subgroup of G is P. Since G is non-abelian, we get that $G' = P$. □

Lemma 2.9. *Let* $G = \mathcal{G}_{p^n,r}(a,c)$ *where* p *is a prime,* $n \ge 1$*, and* $1 \le r < p^n$ *is an integer such that neither* r *nor its order* m *modulo* p^n *is divisible by* p*. Then for every integer* $1 \le s < p^n$ *such that* $p \nmid s$ *and the order of* s *modulo* p^n *is* m*, there exist a group* $(G;\circ)$ *on the underlying set of* G *and an isomorphism* $\delta\colon \mathcal{G}_{p^n,s}(a,c) \to (G;\circ)$ *with* $\delta(a) = a$*,* $\delta(c) = c$ *such that* $(G;\circ)$ *is term equivalent to* G*.*

Proof. If the common order of r and s modulo p^n is $m = 1$, then $r = s = 1$. In this case we have nothing to prove. Note also that the assumptions on p, r and m imply that $m = 1$ if $p = 2$. Therefore we assume from now on that p is odd and $m > 1$, hence $2 \le r, s < p^n$. Since r and s are of the same order m modulo p^n and the group $\mathbf{Z}^*_{p^n}$ of units modulo p^n is cyclic, therefore there is an integer t with $\gcd(t,m) = 1$ such that $s \equiv r^t \pmod{p^n}$. Since m is not divisible by p, we can choose t so that it satisfies the additional condition $t \equiv 1 \pmod{p^n}$. By interchanging the role of r and s we see that there exists an integer t' with $\gcd(t', m) = 1$ such that $r \equiv s^{t'} \pmod{p^n}$ and $t' \equiv 1 \pmod{p^n}$. Thus $r \equiv s^{t'} \equiv r^{tt'} \pmod{p^n}$ and $tt' \equiv 1 \pmod{p^n}$. Since the order of r modulo p^n is m, the first congruence implies that $tt' \equiv 1 \pmod{m}$. It follows that the identity $x^{tt'} = x$ holds in G, because by Lemma 2.8 (4) the order of every element of G divides p^n or m. Consequently, $\tau(x) = x^t$ and $\tau'(x) = x^{t'}$ are term operations of G such that $\tau' = \tau^{-1}$.

Now let $\circ$ be the binary term operation of G defined by

$$x \circ y = \tau'\big(\tau(x) \cdot \tau(y)\big) = \tau^{-1}\big(\tau(x) \cdot \tau(y)\big).$$

It is clear from this definition that $(G; \circ)$ is a group. For every element $g \in G$, τ restricts to the cyclic group $\langle g \rangle$ as an automorphism, therefore $\circ$ coincides with $\cdot$ on $\langle g \rangle$. Hence the powers of g with respect to these two group operations are the same. We will use the notation g^n ($n \in \mathbf{Z}$) for the n-th power of g in both groups G and $(G; \circ)$. Thus, in particular, in the group $(G; \circ)$ we have $a^{p^n} = 1$ and $c^m = 1$. Furthermore, since $\tau(a) = a^t = a$, we have

$$c^{-1} \circ a \circ c = \tau'\big(\tau(c^{-1}) \cdot \tau(a) \cdot \tau(c)\big) = \tau'(c^{-t} a c^t) = \tau'(a^{r^t}) = \tau'(a^s) = a^s.$$

This proves that there exists an isomorphism $\delta \colon \mathcal{G}_{p^n,s}(a, c) \to (G; \circ)$ that satisfies $\delta(a) = a$ and $\delta(c) = c$.

It remains to show that $(G; \circ)$ is term equivalent to G. By construction, $\circ$ is a term operation of G. To see that $\cdot$ is a term operation of $(G; \circ)$, observe first that $\cdot$ can be expressed via $\circ$ as follows:

$$xy = \tau\big(\tau^{-1}(x) \circ \tau^{-1}(y)\big) = \tau\big(\tau'(x) \circ \tau'(y)\big).$$

Here τ and τ' are term operations of $(G; \circ)$ because the powers of elements with respect to the group operations $\cdot$ and $\circ$ are the same. Thus $\cdot$ is a term operation of $(G; \circ)$, proving that $(G; \circ)$ is term equivalent to G. □

Now we are able to prove our first main result.

Theorem 2.10. *Let G and H be finite groups whose Sylow subgroups are cyclic. If there is a cardinality-preserving isomorphism from* $\mathrm{Sub}\,(G)$ *to* $\mathrm{Sub}\,(H)$*, then G is weakly isomorphic to H.*

Proof. Let G and H satisfy the assumptions of the theorem. Since the Sylow subgroups of G and H are cyclic, $G = G_0 \times_\varphi G'$ and $H = H_0 \times_\psi H'$ where G_0 and G' are cyclic of relatively prime order and similarly H_0 and H' are cyclic of relatively prime order. Since there is a cardinality-preserving isomorphism between the subgroup lattices of G and H, conditions (a)–(b) from Theorem 2.2 hold for G and H. In particular, by condition (a), we have $|G_0| = |H_0|$ and $|G'| = |H'|$. Let $P_1, \dots, P_k$ be the Sylow subgroups of G contained in G', and let $Q_1, \dots, Q_k$ be the Sylow subgroups of H contained in H' so that $|P_i| = |Q_i|$ for all i. Then, up to isomorphism, we have $G' = P_1 \times \cdots \times P_k$ and $H' = Q_1 \times \cdots \times Q_k$. Write $\varphi = (\varphi_1, \dots, \varphi_k)$ and $\psi = (\psi_1, \dots, \psi_k)$ in terms of their components.

Let $P_i = \langle u_i\rangle$, $Q_i = \langle v_i\rangle$ $(i = 1, \dots, k)$, and $G_0 = \langle g_0\rangle$, $H_0 = \langle h_0\rangle$. Furthemore, let $\varphi_i(g_0)$ be the automorphism $x \mapsto x^{r_i}$ and let $\psi_i(h_0)$ be the automorphism $x \mapsto x^{s_i}$ where r_i and s_i are relatively prime to $|P_i| = |Q_i|$ $(i = 1, \dots, k)$. According to condition (b) from Theorem 2.2, the subgroup $\varphi_i(G_0) = \langle\varphi_i(g_0)\rangle$ of $\mathrm{Aut}\,(P_i)$ has the same order as the subgroup $\psi_i(H_0) = \langle\psi_i(h_0)\rangle$ of $\mathrm{Aut}\,(Q_i)$ for all i; equivalently, r_i and s_i have the same multiplicative order m_i modulo $|P_i|$ for all i. This order divides $|G_0|$, so it is relatively prime to $|P_i|$. The kernel of φ_i is the subgroup $C_i = C_{G_0}(P_i)$ of G_0, which is normal in G_0P_i. Therefore the quotient group G_0P_i/C_i has order $m_i|P_i|$ and is generated by the elements $\tilde{a} = u_iC_i$ and $\tilde{c} = g_0C_i$ which satisfy the defining relations of the group $\mathcal{G}_{|P_i|,r_i}(a, c)$. Since $\mathcal{G}_{|P_i|,r_i}(a, c)$ also has order $m_i|P_i|$, we conclude that $G_0P_i/C_i \cong \mathcal{G}_{|P_i|,r_i}(a, c)$. In fact, there is an isomorphism $\iota_i\colon \mathcal{G}_{|P_i|,r_i}(a, c) \to G_0P_i/C_i$ such that $\iota_i(a) = u_iC_i$ and $\iota_i(c) = g_0C_i$. Similarly, the kernel of ψ_i is the subgroup $D_i = C_{H_0}(Q_i)$ of H_0, which is normal in H_0Q_i, and there is an isomorphism $\kappa_i\colon \mathcal{G}_{|P_i|,s_i}(a, c) \to H_0Q_i/D_i$ such that $\kappa_i(a) = v_iD_i$ and $\kappa_i(c) = h_0D_i$.

Let us fix an index i $(1 \le i \le k)$. By Lemma 2.9 there exist a group $(\mathcal{G}_{|P_i|,r_i}(a, c); \diamond_i)$ and an isomorphism $\delta_i\colon \mathcal{G}_{|P_i|,s_i}(a, c) \to (\mathcal{G}_{|P_i|,r_i}(a, c); \diamond_i)$ with $\delta_i(a) = a$ and $\delta_i(c) = c$ such that $(\mathcal{G}_{|P_i|,r_i}(a, c); \diamond_i)$ is term equivalent to $\mathcal{G}_{|P_i|,r_i}(a, c)$. Using the isomorphisms ι_i and κ_i we can carry over this result to the groups G_0P_i/C_i and H_0Q_i/D_i as follows: the mapping $\gamma_i' = \iota_i \circ \delta_i \circ \kappa_i^{-1}$ is an isomorphism

$$\gamma_i'\colon H_0Q_i/D_i \to (G_0P_i/C_i; \diamond_i) \quad \text{with} \quad \gamma_i'(v_iD_i) = u_iC_i \quad \text{and} \quad \gamma_1'(h_0D_i) = g_0C_i$$

where $(G_0P_i/C_i; \diamond_i)$ is a group term equivalent to G_0P_i/C_i. Since $G_0P_i/P_i \cong G_0$ and $H_0Q_i/Q_i \cong H_0$ are isomorphic cyclic groups with g_0 generating G_0 and h_0 generating H_0, there is an isomorphism

$$\gamma_i''\colon H_0Q_i/Q_i \to G_0P_i/P_i = (G_0P_i/P_i, \cdot) \quad \text{with} \quad \gamma_i''(h_0Q_i) = g_0P_i.$$

We have $\gamma_i''(v_iQ_i) = \gamma_i''(Q_i) = P_i = u_iP_i$.

Now we want to apply the special case $k = 2$ of Theorem 2.5 to the group G_0P_i and its normal subgroups C_iP_i, P_i, C_i in place of G and $K, M_1 = \overline{M}_2, M_2 = \overline{M}_1$, to the group H_0Q_i and its normal subgroups D_iQ_i, Q_i, D_i in place of H and $L, N_1 = \overline{N}_2, N_2 = \overline{N}_1$, and to the isomorphisms γ_i' and γ_i'' in place of β_1, β_2. The assumptions of Lemma 2.4 hold for G_0P_i and its normal subgroups P_i and C_i, because P_i and C_i $(\subseteq G_0)$ have relatively prime order and $G_0P_i/C_iP_i \cong G_0/C_i$ is cyclic. Similarly, the assumptions of Lemma 2.4 hold for H_0Q_i and its normal subgroups Q_i and D_i. To see that all assumptions of Theorem 2.5 hold, it remains to verify the condition expressed by (2.2) on the relationship between γ_i' and γ_i''. By the remarks following the proof of Theorem 2.5 it suffices to show that condition (2.3) holds for γ_i' and γ_i'', and that condition (2.5) holds for γ_i' and γ_i'' and the generating element $h_0(D_iQ_i)$ of the cyclic group H_0Q_i/D_iQ_i. Explicitly, these conditions require that the following equalities hold:

$$\gamma_i'(D_iQ_i/D_i) = C_iP_i/C_i, \quad \gamma_i''(D_iQ_i/Q_i) = C_iP_i/P_i,$$

and

$$\gamma_i'(h_0D_i)(C_iP_i) = \gamma_i''(h_0Q_i)(C_iP_i).$$

The third equality holds, because $\gamma_i'(h_0D_i) = g_0C_i$ and $\gamma_i''(h_0Q_i) = g_0P_i$. The second equality holds, because γ_i'' is an isomorphism between cyclic groups and D_iQ_i/Q_i and C_iP_i/P_i are subgroups of the same order in these cyclic groups. To establish the first equality recall that $\gamma_i' = \iota_i \circ \delta_i \circ \kappa_i^{-1}$. Thus the first equality holds if and only if $\delta_i(V_i) = U_i$ for the subgroup $U_i = \iota_i^{-1}(C_iP_i/C_i)$ of $(\mathcal{G}_{|P_i|,r_i}(a,c); \diamond_i)$ and the subgroup $V_i = \kappa_i^{-1}(D_iQ_i/Q_i)$ of $\mathcal{G}_{|P_i|,s_i}(a,c)$. We have $|U_i| = |V_i| = |P_i|$, therefore U_i is the cyclic subgroup of $(\mathcal{G}_{|P_i|,r_i}(a,c); \diamond_i)$ generated by a, while V_i is the cyclic subgroup of $\mathcal{G}_{|P_i|,s_i}(a,c)$ generated by a. The construction of the operation $\diamond_i$ in Lemma 2.9 shows that $\diamond_i$ coincides with the original group operation $\cdot$ on every cyclic subgroup of $\mathcal{G}_{|P_i|,r_i}(a,c)$. Hence U_i coincides with the cyclic subgroup of $\mathcal{G}_{|P_i|,r_i}(a,c)$ generated by a. Since $\delta_i(a) = a$, it follows that $\delta_i(V_i) = U_i$, and hence that the first equality above holds.

Thus we can apply Theorem 2.5 to conclude that for each i, there is an isomorphism $\gamma_i\colon H_0Q_i \to (G_0P_i; \circ_i)$ where the group $(G_0P_i; \circ_i)$ is term equivalent to G_0P_i. According to the proof of Theorem 2.5, the image of h_0 under γ_i is the unique element $g \in G_0P_i$ such that $\big(\gamma_i'(h_0D_i), \gamma_i''(h_0Q_i)\big) = (gC_i, gP_i)$. This equality holds for $g = g_0$, therefore $\gamma_i(h_0) = g_0$ for all i. The isomorphism γ_i also satisfies $\gamma_i(Q_i) = P_i$ for all i, because P_i is a normal Sylow subgroup of G_0P_i, and hence of $(G_0P_i; \circ_i)$ as well (cf. Lemma 2.6), Q_i is a normal Sylow subgroup of H_0Q_i, and $|P_i| = |Q_i|$.

Now we want to apply Theorem 2.5 again, this time to the group G and its normal subgroups $K = P_1 \cdots P_k$, P_i and $\overline{P}_i = P_1 \cdots P_{i-1}P_{i+1} \cdots P_k$, to the group H and its normal subgroups $L = Q_1 \cdots Q_k$, Q_i and $\overline{Q}_i = Q_1 \cdots Q_{i-1}Q_{i+1} \cdots Q_k$, and to some isomorphisms β_i to be defined later. The assumptions of Lemma 2.4 hold for G, K, P_i: the P_i's are of relatively prime order, and $G/K \cong G_0$ is cyclic. Similarly, the assumptions of Lemma 2.4 hold for H, L, Q_i. To define the isomorphisms β_i notice that H_0Q_i is a complement of $\overline{Q}_i$ in H, therefore the natural map $\nu_i\colon H_0Q_i \to H/\overline{Q}_i$, $h \mapsto h\overline{Q}_i$ is an isomorphism. Similarly, $\mu_i\colon G_0P_i \to G/\overline{P}_i$, $g \mapsto g\overline{P}_i$ is an isomorphism. Since $(G_0P_i; \circ_i)$ is term equivalent to G_0P_i, μ_i is also an isomorphism $(G_0P_i; \circ_i) \to (G/\overline{P}_i; \circ_i)$ for some group $(G/\overline{P}_i; \circ_i)$ that is term equivalent to $G/\overline{P}_i$. Thus the mappings $\beta_i = \mu_i \circ \gamma_i \circ \nu_i^{-1}$ yield isomorphisms $\beta_i\colon H/\overline{Q}_i \to (G/\overline{P}_i; \circ_i)$ for all i. The properties of γ_i established earlier imply that the equalities $\beta_i(h_0\overline{Q}_i) = g_0\overline{P}_i$ and $\beta_i(L/\overline{Q}_i) = K/\overline{P}_i$ hold for all i. As a consequence of the first equality, we have $\beta_i(h_0\overline{Q}_i)K = (g_0\overline{P}_i)K = g_0K$ for all i. Hence $\beta_1(h_0\overline{Q}_1)K = \cdots = \beta_k(h_0\overline{Q}_k)K$ where h_0L is a generating element of the group H/L. Thus conditions (2.3) and (2.5) are satisfied. Therefore, by the remarks following the proof of Theorem 2.5, condition

(2.2) is also satisfied. This shows that all assumptions of Theorem 2.5 are met. Hence we get that there is an isomorphism $\beta\colon H \to (G;\circ)$ where the group $(G;\circ)$ is term equivalent to G. This concludes the proof that G is weakly isomorphic to H. $\square$

The preceding result combined with Theorem 2.2 leads to the following corollary, which is also one of our main results.

Corollary 2.11. *Let $G = G_0 \times_\varphi G'$ and $H = H_0 \times_\psi H'$ be finite groups whose Sylow subgroups are cyclic. Write $G' = P_1 \times \cdots \times P_k$ and $H' = Q_1 \times \cdots \times Q_l$ as products of Sylow subgroups, and write $\varphi = (\varphi_1, \ldots, \varphi_k)$ and $\psi = (\psi_1, \ldots, \psi_l)$ in terms of their components. Then G and H are weakly isomorphic if and only if*

(a) *$|G| = |H|$, $|G'| = |H'|$, and*
(b) *if $|P_i| = |Q_j|$, then the subgroup $\varphi_i(G_0)$ of $\mathrm{Aut}\,(P_i)$ has the same order as the subgroup $\psi_j(H_0)$ of $\mathrm{Aut}\,(Q_j)$.*

Proof. The sufficiency of conditions (a) and (b) follows from Theorems 2.2 and 2.10. To prove their necessity let H be weakly isomorphic to G, that is, H is isomorphic to a group $(G;\circ)$ term equivalent to G. We may assume without loss of generality that $H = (G;\circ)$, because if (a) and (b) hold for G and $H = (G;\circ)$, then they also hold for G and any group H isomorphic to $(G;\circ)$. By Lemma 2.6, G and $(G;\circ)$ have the same normal subgroups and the same abelian quotients. Since the commutator subgroup is the largest normal subgroup modulo which the quotient group is abelian, it follows that G and $(G;\circ)$ have the same commutator subgroups. This proves that (a) holds for G and $H = (G;\circ)$. Thus $k = l$, and we may assume that $Q_i = P_i$ for all i. Condition (b) is independent on the choice of the subgroups G_0 and H_0, because the complements of the commutator subgroup are conjugate in G as well as in $(G;\circ)$. Therefore we may assume that $G_0 = H_0$. The order of $\varphi_i(G_0)$ is the index of the centralizer of P_i in G_0 where the centralizer is computed in G. Similarly, the order of $\psi_i(G_0)$ is the index of the centralizer of P_i in G_0 where the centralizer is computed in $(G;\circ)$. Since P_i is abelian, the centralizer of P_i in G_0 — whether computed in G or $(G;\circ)$ — is the largest subgroup $S \subseteq G_0$ whose join with P_i is abelian. Since by Lemma 2.6 the groups G and $(G;\circ)$ have the same subgroups and the same abelian subgroups, this condition determines the same subgroup in G as in $(G;\circ)$. Thus condition (b) is satisfied. $\square$

The next corollary has a direct bearing on Problem 1.1. See Example 2.14 for the complete negative answer.

Corollary 2.12. *Let G and H be finite groups whose Sylow subgroups are cyclic. If there is a cardinality-preserving isomorphism between the subgroup lattices of G and H, then G^κ and H^κ have isomorphic subgroup lattices for all cardinals κ.*

Proof. If G, H are finite groups such that the Sylow subgroups of G, H are cyclic and there exists a cardinality-preserving isomorphism between the subgroup lattices of

G and H, then by Theorem 2.10 the group G is term equivalent to a group $(G;\circ)$ that is isomorphic to H. Since G and $(G;\circ)$ have the same term operations, G^κ and $(G;\circ)^\kappa$ have the same subgroups for all κ. Since $(G;\circ) \cong H$, the subgroup lattices of $(G;\circ)^\kappa$ and H^κ are isomorphic for all κ. Thus G^κ and H^κ have isomorphic subgroup lattices for all κ. □

Our earlier results can be modified to a result concerning purely abstract lattice isomorphisms between subgroup lattices.

Theorem 2.13. *Let G, H be finite groups whose Sylow subgroups are cyclic. If there is a lattice isomorphism $\lambda\colon \mathrm{Sub}\,(G^2) \to \mathrm{Sub}\,(H^2)$, then G is weakly isomorphic to H.*

Proof. The proof given here was suggested by the referee, and is based on Corollary 2.11. It is shorter than our original proof, which was based on Theorem 2.5. We will argue that it is possible to determine the order of G, the order of G', and the index of the centralizer of each Sylow subgroup of G' within some complement G_0 of G' from the lattice structure of $\mathrm{Sub}\,(G^2)$. It then follows from Corollary 2.11 that $\mathrm{Sub}\,(G^2)$ determines G up to term equivalence.

We first argue that, for any finite group G, the lattice structure of $\mathrm{Sub}\,(G^2)$ determines the order of every subgroup of G^2. Let M be a minimal subgroup of G^2. M has prime order p. Consider all height-two intervals $I = [\{1\}, N]$ in $\mathrm{Sub}\,(G^2)$ that contain M. $I \cong \mathrm{Sub}\,(N)$ is isomorphic to the subgroup lattice of a group whose order is divisible by two primes, so this interval has either one atom (if $N \cong \mathbb{Z}_{p^2}$), or two atoms (if $N \cong \mathbb{Z}_p \times \mathbb{Z}_q$), or $p+1$ atoms (if $N \cong \mathbb{Z}_p \times \mathbb{Z}_p$), or $\max(p,q)+1$ atoms (if N is nonabelian of order pq). Moreover, for at least one interval I we must have $p+1$ atoms. Therefore p is the smallest integer $n > 1$ such that there is an interval I of height two with $n+1$ atoms that contains M. This shows that the order of any minimal $M \leq G^2$ can be determined. Now, a subgroup $P \leq G^2$ is a p-subgroup if and only if all minimal subgroups contained in P have order p. The order of a p-subgroup P is p^h where h is the height of P in $\mathrm{Sub}\,(G^2)$. If $H \leq G^2$ is an arbitrary subgroup, then its Sylow p-subgroups are its maximal p-subgroups, which as we have seen can be determined. The order of H can be determined by multiplying the orders of its Sylow p-subgroups for different p.

Now we restrict the argument to groups G whose Sylow subgroups are cyclic. A Sylow subgroup $P \leq G^2$ is normal if and only if it is the unique subgroup of its order. If P is a normal Sylow subgroup of G^2, then $P \leq Z(G^2)$ if and only if P centralizes every other Sylow subgroup Q. This happens if and only if PQ is abelian. Since PQ is isomorphic to the square of a finite group, it follows from [4] that PQ is abelian if and only if the interval $[\{1\}, P \vee Q] \cong \mathrm{Sub}\,(PQ)$ is modular. Therefore we can determine from the structure of $\mathrm{Sub}\,(G^2)$ which normal Sylow subgroups are contained in $Z(G^2)$. This allows us to determine the location of $(G^2)' = (G')^2$ in $\mathrm{Sub}\,(G^2)$, and therefore its order, since the commutator group is the join of all normal Sylow subgroups $P \leq G^2$ such that $P \not\leq Z(G^2)$.

From the orders of G^2 and $(G^2)'$ we derive the orders of G and G' by taking square roots. It remains to show that for each Sylow subgroup contained in G' we can determine the index i of its centralizer in some complement G_0 of G'. Since the square of a Sylow p-subgroup contained in G' is simply a Sylow p-subgroup $P \leq (G^2)'$, and any complement C of $(G^2)'$ in $\mathrm{Sub}\,(G^2)$ is conjugate to the square of any complement G_0 of G' in $\mathrm{Sub}\,(G)$, it follows that the index of the centralizer of P in C is i^2. Therefore we can determine i by finding the index of the centralizer of P in C and then taking its square root.

A complement C of $(G^2)'$ is isomorphic to the square of a cyclic group. Although the factorization of C into two factors is not unique, we can certainly locate subgroups D and E in $[\{1\}, C] \cong \mathrm{Sub}\,(C)$ which are complements within this interval and for which $[\{1\}, D]$ and $[\{1\}, E]$ are distributive. D and E must be isomorphic cyclic subgroups of C whose product is C. There is a unique cardinality-preserving isomorphism $\mu\colon [\{1\}, D] \to [\{1\}, E]$, so we can determine which subgroups are squares with respect to this direct factorization of C. But the centralizer of P within C is a square with respect to any representation of C as a square, so the centralizer of P in C is the largest subgroup $F \leq C$ that is a square with respect to this factorization and has the property that PF is abelian. As PF is isomorphic to the square of a finite group, it is abelian if and only if $[\{1\}, P \vee F] \cong \mathrm{Sub}\,(PF)$ is a modular interval of $\mathrm{Sub}\,(G^2)$. Therefore we can locate F, determine i, and we are done. □

Next we describe the example promised in the abstract of the paper.

Example 2.14. We show that for any positive integer N there is a finite set X and N binary operations on X, $\circ_1, \dots, \circ_N$, such that the structures $G_i = (X; \circ_i)$ are pairwise nonisomorphic term equivalent groups. To show this, it is enough to exhibit N weakly isomorphic finite groups that are pairwise nonisomorphic. For if $G_1, \dots, G_N$ are pairwise weakly isomorphic and pairwise nonisomorphic, then we can take X to be the underlying set of G_1, and then replace each G_i, $i > 1$, with an isomorphic copy $\widetilde{G}_i$ defined on X and term equivalent to G_1. Then $G_1, \widetilde{G}_2, \dots, \widetilde{G}_N$ will be term equivalent groups defined on X that are pairwise nonisomorphic.

To construct a large collection of groups that are pairwise weakly isomorphic and nonisomorphic, let $p_1, \dots, p_k$ be distinct primes congruent to 1 modulo 3 where k is an integer to be determined later. Each G_i will be a group of the form $\mathbb{Z}_3 \times_\varphi (\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_k})$ where φ is a homomorphism

$$\varphi\colon \mathbb{Z}_3 \to \mathrm{Aut}\,(\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_k}) = \mathrm{Aut}\,(\mathbb{Z}_{p_1}) \times \cdots \times \mathrm{Aut}\,(\mathbb{Z}_{p_k}).$$

Any such homomorphism $\varphi = (\varphi_1, \dots, \varphi_k)$ is determined by its components $\varphi_i\colon \mathbb{Z}_3 \to \mathrm{Aut}\,(\mathbb{Z}_{p_i})$. Since each p_i is congruent to 1 modulo 3, for each i there are exactly three homomorphisms $\varphi_i\colon \mathbb{Z}_3 \to \mathrm{Aut}\,(\mathbb{Z}_{p_i})$, and they are $x \mapsto x, x \mapsto x^{m_i}$ and $x \mapsto x^{(m_i^{-1})}$ where m_i is a fixed element of multiplicative order 3 in $\mathbb{Z}_{p_i}^*$. Thus we may represent $\varphi = (\varphi_1, \dots, \varphi_k)$ by the sequence $(\varepsilon_1, \dots, \varepsilon_k)$ where $\varepsilon_i \in \{1, m_i, m_i^{-1}\}$ and φ_i is

$x \mapsto x^{\varepsilon_i}$. If $(\varepsilon_1, \ldots, \varepsilon_k)$ is any sequence where $\varepsilon_i \in \{m_i, m_i^{-1}\}$ for each i, then each φ_i will be nonconstant, hence the resulting group will have commutator subgroup equal to $\{0\} \times \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_k}$. Moreover, when each φ_i is nonconstant we have $|\varphi_i(\mathbb{Z}_3)| = 3$. Therefore it follows from Corollary 2.11 that any two tuples $(\varepsilon_1, \ldots, \varepsilon_k)$ and $(\varepsilon'_1, \ldots, \varepsilon'_k)$, where $\varepsilon_i, \varepsilon'_i \in \{m_i, m_i^{-1}\}$ for all i, represent weakly isomorphic groups. This yields a family of 2^k pairwise weakly isomorphic groups. We can determine the isomorphism relation on this family using Theorem 2.1. Namely, that theorem indicates that tuples $(\varepsilon_1, \ldots, \varepsilon_k)$ and $(\varepsilon'_1, \ldots, \varepsilon'_k)$ (with $\varepsilon_i, \varepsilon'_i \in \{m_i, m_i^{-1}\}$) represent isomorphic groups if and only if the tuples $(\varepsilon_1, \ldots, \varepsilon_k)$ and $(\varepsilon'_1, \ldots, \varepsilon'_k)$ generate the same multiplicative subgroup of $\mathbb{Z}^*_{p_1} \times \cdots \times \mathbb{Z}^*_{p_k}$, and since the two tuples have order three this will happen if and only if $(\varepsilon'_1, \ldots, \varepsilon'_k) = (\varepsilon_1, \ldots, \varepsilon_k)$ or $(\varepsilon_1^{-1}, \ldots, \varepsilon_k^{-1})$. Thus, the isomorphism relation on our family of groups partitions the family into 2-element subsets. It follows that the family contains a subfamily of 2^{k-1} pairwise weakly isomorphic and nonisomorphic groups. If k is chosen so that $2^{k-1} \geq N$, then we have a family of the targeted size.

This example gives a negative solution to Problem 1.1 and to Problem 7.6.11 (a) in Schmidt [8] (which asks whether the isomorphism types of the subgroup lattices of finite powers of a group G are sufficient to determine the isomorphism type of G).

References

[1] R. Baer, *The significance of the system of subgroups for the structure of the group*, Amer. J. Math. **61** (1939), 1–44.

[2] K. Honda, *On finite groups, whose Sylow-groups are all cyclic*, Comment. Math. Univ. St. Paul. **1** (1952), 5–39.

[3] K. A. Kearnes and Á. Szendrei, *Term equivalence of groups*, preprint.

[4] E. Lukács and P. P. Pálfy, *Modularity of the subgroup lattice of a direct square*, Arch. Math. (Basel) **46** (1986), no. 1, 18–19.

[5] D. J. S. Robinson, *A Course in the Theory of Groups*, Graduate Texts in Mathematics, vol. 80, Springer-Verlag, New York, Heidelberg, Berlin, 1993.

[6] R. Schmidt, *Der Untergruppenverband des direkten Produktes zweier isomorpher Gruppen*, (German) [The lattice of subgroups of the direct product of two isomorphic groups] J. Algebra **73** (1981), no. 1, 264–272.

[7] R. Schmidt, *Untergruppenverbände endlicher Gruppen mit elementarabelschen Hallschen Normalteilern*, (German) [Subgroup lattices of finite groups with elementary abelian Hall normal subgroups] J. Reine Angew. Math. **334** (1982), 116–140.

[8] R. Schmidt, *Subgroup lattices of groups*, de Gruyter Expositions in Mathematics, vol. 14, Walter de Gruyter & Co., Berlin, 1994.

[9] A. P. Street, *Subgroup-determining functions on groups*, Illinois J. Math. **12** (1968), 99–120.

[10] M. Suzuki, *On the lattice of subgroups of finite groups*, Trans. Amer. Math. Soc. **70** (1951), 345–371.

[11] M. Suzuki, *Structure of a group and the structure of its lattice of subgroups*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Heft 10. Springer-Verlag, Berlin, Göttingen, Heidelberg, 1956.

[12] Á. Szendrei, *Clones in Universal Algebra,* Séminaire de Mathématiques Supérieures, vol. 99, Les Presses de l'Université de Montréal, Montréal, 1986.
[13] L. Zádori, *Categorical equivalence of finite groups*, Bull. Austral. Math. Soc. **56** (1997), no. 3, 403–408.

(Keith Kearnes) Department of Mathematics, University of Colorado, Boulder, CO 80309-0395, U.S.A.
E-mail address: kearnes@euclid.colorado.edu

(Ágnes Szendrei) Bolyai Institute, University of Szeged, Aradi vértanúk tere 1, H–6720 Szeged, Hungary, and Department of Mathematics, University of Colorado, Boulder, CO 80309-0395, U.S.A.
E-mail address: a.szendrei@math.u-szeged.hu, szendrei@euclid.colorado.edu