Every Finite Abelian p-Group Is the Schur Multiplier of a 2-Generated Metabelian Nonabelian Finite p-Group

Sen Cao
Wuchang Shouyi University, Wuhan, China

hexagon:2611.01375v1

Abstract

We give a complete, self-contained, constructive affirmative solution to Problem 15.30 of the Kourovka Notebook (posed by Ya. G. Berkovich in 2002): for every prime $p \geq 2$ (including $p = 2$) and every finite abelian p-group A, there exists a 2-generated metabelian finite nonabelian p-group G whose Schur multiplier $M(G) = H_2(G, \mathbb{Z})$ is isomorphic to A. The proof is entirely elementary and characteristic-free, combining a backwards-Euclidean two-polynomial realization of A, a division-by-2-free antisymmetric Laurent identification of exterior-square coinvariants, a non-split cyclic extension whose commutator structure forces $A \twoheadrightarrow M(G)$ directly from stem covers, and an explicit central stem extension yielding $M(G) \twoheadrightarrow A$.

Keywords: Schur multiplier; finite p-groups; metabelian groups; Kourovka Notebook Problem 15.30; central extensions.

MSC 2020: 20D15, 20J06, 20C25.

1 Introduction

In Issue 15 (2002) of the *Kourovka Notebook* [1], Ya. G. Berkovich posed the following open problem:

> **Problem 15.30 (Ya. G. Berkovich).** *Is it true that every finite abelian p-group is isomorphic to the Schur multiplier of some nonabelian finite p-group?*

Here $M(G) = H_2(G, \mathbb{Z})$ denotes the Schur multiplier of a finite group G. While the Schur multiplier of an abelian finite p-group $A \cong \bigoplus_{i=1}^{r} \mathbb{Z}/p^{e_i}\mathbb{Z}$ ($e_1 \geq \cdots \geq e_r \geq 1$) is simply the exterior square $\bigwedge^2 A \cong \bigoplus_{1 \leq i < j \leq r} \mathbb{Z}/p^{e_j}\mathbb{Z}$, which severely restricts the invariant factors that can arise from abelian p-groups, Berkovich's question asks whether passing to *nonabelian* finite p-groups removes all restrictions.

In the twenty-first edition of the Kourovka Notebook (2026) [1], Problem 15.30 remained open in general. Significant partial progress had been obtained for odd primes p: P. K. Rai [3] proved that every elementary abelian p-group (p odd) occurs as the Schur multiplier of a nonabelian finite p-group, and S. Hatui, T. N. Mavely, and S. Sabnam [4, Theorem 1.2] proved the realization for odd primes p across several further families, including homocyclic groups, products of up to three arbitrary cyclic p-groups, and certain direct products with a sufficiently large homocyclic summand (see [4, Theorem 1.2] for the exact hypotheses). While isolated small 2-groups (such as the dihedral group D_8 with $M(D_8) \cong \mathbb{Z}/2\mathbb{Z}$) and these restricted odd-p families were known, the uniform realization of arbitrary finite abelian p-groups—including products of four or more arbitrary cyclic factors for odd p and general finite abelian 2-groups—remained unresolved.

In this paper we completely settle Problem 15.30 in the affirmative for every prime $p \geq 2$ and every finite abelian p-group A, in fact within the narrow class of 2-generated metabelian finite nonabelian p-groups.

Theorem 1.1 (Main Theorem)**.** *For every prime $p \geq 2$ and every finite abelian p-group A, there exists a 2-generated metabelian finite nonabelian p-group G such that $M(G) \cong A$.*

The architecture of our proof is completely elementary and avoids both spectral-sequence machinery and characteristic-2 obstructions:

1. For $A = 1$, the classical 2-generated metabelian groups Q_8 ($p = 2$) and M_{p^3} (p odd) suffice (Section 2).
2. For any nontrivial $A \cong \bigoplus_{k=1}^{t} (\mathbb{Z}/p^{c_k}\mathbb{Z})^{m_k}$ ($c_1 > \cdots > c_t \geq 1$), a backwards-Euclidean recurrence produces polynomials $P(u), Q(u) \in \mathbb{Z}[u]$ such that $(\mathbb{Z}/p^s\mathbb{Z})[u]/(P(u), Q(u)) \cong A$ for $s = 2c_1 + 1$, with $P(u) \equiv u^r \pmod{p}$, $Q(u) \equiv 0 \pmod{p}$, and $1 \leq v_p(P(0)) \leq c_1$ (Lemma 3.1).
3. Lifting (P, Q) via the palindromic-skew polynomial $f_0(y) = y^r P(y + y^{-1} - 2) + y^r(y - 1)Q(y + y^{-1} - 2)$ defines a free $(\mathbb{Z}/p^s\mathbb{Z})$-module $N = (\mathbb{Z}/p^s\mathbb{Z})[y]/(f(y))$ of rank $2r$ with a p-power-order automorphism φ (multiplication by y) satisfying $(\bigwedge^2 N)_{\langle\varphi\rangle} \cong A$ *without any division by* 2, while the fixed subgroup $N^{\langle\varphi\rangle} = \ker(\varphi - I)$ is cyclic, generated by an element $u_0 \in p^{c_1+1}N$ (Lemma 3.2).
4. Taking G to be the non-split cyclic extension $1 \to N \to G \to C_{p^m} \to 1$ with $y^{-1}xy = \varphi(x)$ and $y^{p^m} = u_0$ ($m = m_0 + s$), a direct stem-cover argument shows that every stem cover of G has kernel covered by $(\bigwedge^2 N)_Q \cong A$, yielding $A \twoheadrightarrow M(G)$. Conversely, an explicit central stem extension $1 \to A \to E \to G \to 1$ constructed via a bilinear 2-cocycle ψ and a quadratic correction η (whose well-definedness modulo p^s and vanishing on u_0 hold unconditionally even for $p = 2$ because $s = 2c_1 + 1$ and $u_0 \in p^{c_1+1}N$) yields $M(G) \twoheadrightarrow A$ (Theorem 4.1). Since A is finite, $M(G) \cong A$.

In Section 5, we also give an explicit worked example and summarize independent exact Hopf-formula computations across 22 representative instances spanning $p \in \{2, 3, 5, 7\}$ and up to five distinct invariant-factor blocks.

2 Preliminaries and the Trivial Case $A = 1$

Throughout the paper, we use the commutator convention $[g, h] := g^{-1}h^{-1}gh$ and write $G' = [G, G]$ for the derived subgroup of a group G.

Recall that a *stem extension* of a finite group G is a central extension $1 \to Z \to \widehat{G} \xrightarrow{\pi} G \to 1$ such that $Z \leq Z(\widehat{G}) \cap \widehat{G}'$. By Schur's theorem (see, e.g., [2, Chapter 2]), every finite group G admits a *stem cover* (or Schur representation group) with $Z \cong M(G)$, and for every stem extension $1 \to K \to E \to G \to 1$ there exists a surjective homomorphism $M(G) \twoheadrightarrow K$. Moreover, if G is a finite p-group, then $M(G)$ is a finite abelian p-group.

We record the standard Schreier criterion for cyclic extensions: given a group H, an automorphism $\alpha \in \mathrm{Aut}(H)$, an integer $q \geq 1$, and an element $h_0 \in H$ satisfying $\alpha^q = \mathrm{Inn}(h_0)$ (where $\mathrm{Inn}(h_0)(h) = h_0^{-1}hh_0$) and $\alpha(h_0) = h_0$, there exists a group E containing H as a normal subgroup with $E/H \cong C_q$, generated by H and an element t subject to $t^{-1}ht = \alpha(h)$ for all $h \in H$ and $t^q = h_0$.

Proposition 2.1 (Trivial Multiplier Case)**.** *For every prime $p \geq 2$, there exists a 2-generated metabelian finite nonabelian p-group G with $M(G) = 1$.*

Proof. For $p = 2$, let $G = Q_8 = \langle a, b \mid a^4 = 1,\ b^2 = a^2,\ b^{-1}ab = a^3 \rangle$, a 2-generated metabelian nonabelian 2-group of order 8. Let $1 \to Z \to \widehat{G} \xrightarrow{\pi} Q_8 \to 1$ be a stem cover with $Z \cong M(Q_8)$, and choose lifts $\widehat{a}, \widehat{b} \in \widehat{G}$ of a, b. Set $\widehat{N} = \pi^{-1}(\langle a \rangle) = \langle \widehat{a}, Z \rangle$. Since $Z \leq Z(\widehat{G})$, the subgroup $\widehat{N}$ is abelian, so conjugation $\widehat{\varphi}(x) = \widehat{b}^{-1}x\widehat{b}$ is an automorphism of $\widehat{N}$ and $\widehat{G}' = [\widehat{N}, \widehat{b}] = \{x^{-1}\widehat{\varphi}(x) : x \in \widehat{N}\}$. Take any $z \in Z \leq \widehat{G}'$ and write $z = x^{-1}\widehat{\varphi}(x)$ with $x \in \widehat{N}$. Projecting to $\langle a \rangle$ gives $a^{-k}a^{3k} = 1$, so $2 \mid k$, i.e., $\pi(x) \in \langle a^2 \rangle = \langle b^2 \rangle$. Thus $x = \widehat{b}^{2\ell}z'$ for some $\ell \in \mathbb{Z}$ and $z' \in Z$. Since $\widehat{b}$ commutes with both $\widehat{b}^{2\ell}$ and $z' \in Z(\widehat{G})$, we obtain $\widehat{\varphi}(x) = x$ and hence $z = 1$. Thus $M(Q_8) \cong Z = 1$.

For any odd prime p, let $G = M_{p^3} = \langle a, b \mid a^{p^2} = 1,\ b^p = 1,\ b^{-1}ab = a^{1+p} \rangle$, a 2-generated metabelian nonabelian p-group of order p^3. Let $1 \to Z \to \widehat{G} \xrightarrow{\pi} M_{p^3} \to 1$ be a stem cover with $Z \cong M(M_{p^3})$, and choose lifts $\widehat{a}, \widehat{b} \in \widehat{G}$ of a, b. Again $\widehat{N} = \langle \widehat{a}, Z \rangle$ is abelian, and $\widehat{a}^{p^2} = z_2 \in Z$, $\widehat{b}^{-1}\widehat{a}\widehat{b} = \widehat{a}^{1+p}z_1$ for some $z_1, z_2 \in Z$. Since $\widehat{b}^p \in Z \leq Z(\widehat{G})$ commutes with $\widehat{a}$, iterating conjugation p times yields

$$\widehat{a} = \widehat{b}^{-p}\widehat{a}\widehat{b}^p = \widehat{a}^{(1+p)^p}z_1^S, \qquad \text{where } S := \sum_{j=0}^{p-1}(1+p)^j.$$

Using $(1+p)^p - 1 = pS$, we rewrite this as $1 = \widehat{a}^{pS}z_1^S = (\widehat{a}^{p^2})^{S/p}z_1^S = (z_2z_1^p)^{S/p}$. Because p is odd,

$$\frac{S}{p} = \frac{(1+p)^p - 1}{p^2} = 1 + \binom{p}{2} + \sum_{j=3}^{p}\binom{p}{j}p^{j-2} \equiv 1 \pmod{p}.$$

Since Z is a finite p-group and $\gcd(S/p, p) = 1$, it follows that $z_2z_1^p = 1$. Now $\widehat{G}' = [\widehat{N}, \widehat{b}] = \langle [\widehat{a}, \widehat{b}] \rangle = \langle \widehat{a}^p z_1 \rangle$, and $(\widehat{a}^p z_1)^p = \widehat{a}^{p^2}z_1^p = z_2z_1^p = 1$. Hence $|\widehat{G}'| \leq p = |G'|$, which forces $Z = Z \cap \widehat{G}' = 1$, i.e., $M(M_{p^3}) = 1$. □

3 Two Lemmas for Nontrivial A

Fix a prime $p \geq 2$ and a nontrivial finite abelian p-group A. Grouping cyclic direct summands of equal order, we write

$$A \ \cong\ \bigoplus_{k=1}^{t}(\mathbb{Z}/p^{c_k}\mathbb{Z})^{m_k}, \qquad c_1 > c_2 > \cdots > c_t \geq 1, \quad m_k \geq 1, \quad t \geq 1. \tag{1}$$

Throughout the remainder of the paper, set

$$r := \sum_{k=1}^{t} m_k \geq 1, \qquad s := 2c_1 + 1, \qquad R := \mathbb{Z}/p^s\mathbb{Z}.$$

Let $v_p(n)$ denote the p-adic valuation of a nonzero integer n.

3.1 Backwards-Euclidean Two-Polynomial Realization

Lemma 3.1 (Two-Polynomial Realization)**.** *For A as in (1), define polynomials $g_0, g_1, \ldots, g_t \in \mathbb{Z}[u]$ recursively by*

$$g_0(u) := 1, \qquad g_1(u) := u^{m_1}, \qquad g_{k+1}(u) := u^{m_{k+1}}g_k(u) + p^{c_k - c_{k+1}}g_{k-1}(u) \quad (1 \leq k \leq t-1).$$

Set $P_0(u) := g_t(u)$, $Q(u) := p^{c_t}g_{t-1}(u)$, and

$$P(u) := \begin{cases} P_0(u) + p^{c_1} & \text{if } t \text{ is odd,} \\ P_0(u) & \text{if } t \text{ is even.} \end{cases}$$

Then:

(i) *$P_0(u)$ and $P(u)$ are monic of degree r, $\deg Q = r - m_t < r$, $P_0(u) \equiv P(u) \equiv u^r \pmod p$, and $Q(u) \equiv 0 \pmod p$.*

(ii) *As abelian groups, $\mathbb{Z}[u]/(P_0(u), Q(u)) \cong A$ and $R[u]/(P(u), Q(u)) \cong A$.*

(iii) *$P(0) \neq 0$, and its p-adic valuation $v_0 := v_p(P(0))$ satisfies $1 \leq v_0 \leq c_1$.*

Proof. (i) Set $d_0 := 0$ and $d_k := m_1 + \cdots + m_k$ for $1 \leq k \leq t$. By induction on k, each $g_k(u)$ is monic of degree d_k and satisfies $g_k(u) \equiv u^{d_k} \pmod p$ because $c_k - c_{k+1} \geq 1$. Since $d_t = r$, $d_{t-1} = r - m_t < r$, and $c_1, c_t \geq 1$, all congruences and degree assertions follow immediately.

(ii) Let $I := (P_0(u), Q(u)) \subseteq \mathbb{Z}[u]$. We first show by downward induction on $k = t, t-1, \ldots, 1$ that

$$p^{c_k} g_{k-1}(u) \in I. \tag{2}$$

For $k = t$, we have $p^{c_t} g_{t-1}(u) = Q(u) \in I$. For $1 \leq k \leq t-1$, multiplying the defining recurrence of g_{k+1} by $p^{c_{k+1}}$ gives

$$p^{c_k} g_{k-1}(u) = p^{c_{k+1}} g_{k+1}(u) - u^{m_{k+1}} \big(p^{c_{k+1}} g_k(u)\big).$$

The second term lies in I by the induction hypothesis. For the first term: if $k = t-1$, then $g_{k+1} = g_t = P_0 \in I$; if $k \leq t-2$, then $p^{c_{k+1}} g_{k+1}(u) = p^{c_{k+1} - c_{k+2}} \big(p^{c_{k+2}} g_{k+1}(u)\big) \in I$ by the induction hypothesis. This proves (2).

Now pass to the quotient ring $R_0 := \mathbb{Z}[u]/(P_0(u))$, which is a free $\mathbb{Z}$-module of rank r. Because $\deg(u^j g_{k-1}(u)) = d_{k-1} + j$ runs bijectively through $0, 1, \ldots, r-1$ as $1 \leq k \leq t$ and $0 \leq j < m_k$, and each $u^j g_{k-1}(u)$ is monic, the family

$$\mathcal{B} := \{u^j g_{k-1}(u) : 1 \leq k \leq t,\ 0 \leq j < m_k\}$$

is a $\mathbb{Z}$-basis of R_0. Consider the $\mathbb{Z}$-submodule

$$J := \bigoplus_{k=1}^{t} \bigoplus_{j=0}^{m_k - 1} \mathbb{Z} \cdot \big(u^j p^{c_k} g_{k-1}(u)\big) \subseteq R_0.$$

Clearly $R_0/J \cong \bigoplus_{k=1}^{t} (\mathbb{Z}/p^{c_k}\mathbb{Z})^{m_k} = A$. By (2), every generator of J lies in the ideal $(Q)R_0$, so $J \subseteq (Q)R_0$. Conversely, $Q = p^{c_t} g_{t-1} \in J$, and J is closed under multiplication by u: for $0 \leq j < m_k - 1$ this is immediate, whereas for $j = m_k - 1$ we have

$$u^{m_k} \big(p^{c_k} g_{k-1}(u)\big) = \begin{cases} p^{c_1} g_1(u) & (k = 1), \\ p^{c_k} g_k(u) - p^{c_{k-1}} g_{k-2}(u) & (2 \leq k \leq t). \end{cases}$$

Here $p^{c_{k-1}} g_{k-2}(u) \in J$ (for $k \geq 2$), while $p^{c_k} g_k(u)$ vanishes in R_0 when $k = t$ (since $g_t = P_0$) and equals $p^{c_k - c_{k+1}} \big(p^{c_{k+1}} g_k(u)\big) \in J$ when $k < t$. Thus J is an ideal of R_0 containing Q, forcing $J = (Q)R_0$ and hence $\mathbb{Z}[u]/(P_0(u), Q(u)) \cong R_0/J \cong A$.

Next we pass to $R = \mathbb{Z}/p^s\mathbb{Z}$. Since $p^{c_1} A = 0$ and $s = 2c_1 + 1 > c_1$, we have $R[u]/(P_0(u), Q(u)) \cong A/p^s A = A$. If t is even, $P = P_0$ and we are done. If t is odd, then (2) at $k = 1$ gives $p^{c_1} = p^{c_1} g_0(u) \in (P_0(u), Q(u))$ in $\mathbb{Z}[u]$, so there exist $\alpha(u), \beta(u) \in \mathbb{Z}[u]$ satisfying

$$p^{c_1} = \alpha(u) P_0(u) + \beta(u) Q(u).$$

Reducing modulo p and using part (i) gives $0 \equiv \alpha(u) u^r \pmod p$. Since u^r is a non-zero-divisor in $\mathbb{F}_p[u]$, we must have $\alpha(u) \in p\mathbb{Z}[u]$. Therefore $\alpha(u)$ is nilpotent in $R[u]$, so $1 + \alpha(u)$ is a unit in $R[u]$. Because

$$P(u) = P_0(u) + p^{c_1} = (1 + \alpha(u)) P_0(u) + \beta(u) Q(u),$$

the ideals $(P(u), Q(u))$ and $(P_0(u), Q(u))$ coincide in $R[u]$. Consequently $R[u]/(P(u), Q(u)) \cong R[u]/(P_0(u), Q(u)) \cong A$.

(iii) Evaluating the recurrence at $u = 0$ gives $g_0(0) = 1$, $g_1(0) = 0$, and $g_{k+1}(0) = p^{c_k - c_{k+1}} g_{k-1}(0)$ for $k \geq 1$. By induction, $g_k(0) = 0$ for every odd k, and

$$g_{2\ell}(0) = \prod_{j=1}^{\ell} p^{c_{2j-1} - c_{2j}} \qquad (\ell \geq 1).$$

If $t = 2\ell$ is even, then $P(0) = P_0(0) = g_{2\ell}(0)$ has p-adic valuation

$$v_0 = \sum_{j=1}^{\ell} (c_{2j-1} - c_{2j}),$$

which satisfies $1 \leq v_0 \leq c_1 - c_t < c_1$ because $c_1 > c_2 > \cdots > c_t \geq 1$. If t is odd, then $P_0(0) = 0$, so $P(0) = p^{c_1}$ and $v_0 = c_1$. In both cases $1 \leq v_0 \leq c_1$. □

3.2 Characteristic-Free Antisymmetric-Laurent Identification

Lemma 3.2 (Antisymmetric-Laurent Module)**.** *Let $P(u), Q(u) \in \mathbb{Z}[u]$ be as in Lemma 3.1, and define*

$$f_0(y) := y^r P(y + y^{-1} - 2) + y^r (y - 1) Q(y + y^{-1} - 2) \in \mathbb{Z}[y]. \tag{3}$$

Then $f_0(y)$ is a genuine polynomial of degree $d := 2r$ whose leading coefficient is congruent to 1 modulo p (hence a unit in $R = \mathbb{Z}/p^s\mathbb{Z}$). Let $f(y) \in R[y]$ be the monic normalization of $f_0(y)$ modulo p^s, let

$$N := R[y]/(f(y)) \;\cong\; (\mathbb{Z}/p^s\mathbb{Z})^d,$$

and let $\varphi : N \to N$ be multiplication by y. Then:

- *(i) $f(y) \equiv (y - 1)^d \pmod{p}$, and φ is an automorphism of N of p-power order p^{m_0} for some integer $m_0 \geq 1$.*
- *(ii) Setting $Q := \langle \varphi \rangle$, the exterior-square coinvariants satisfy $(\bigwedge^2 N)_Q \cong A$ for every prime $p \geq 2$ (including $p = 2$).*
- *(iii) Write $f(y) - f(1) = (y - 1)q(y)$ in $R[y]$, where $q(y)$ is monic of degree $d - 1$. Then the fixed subgroup $N^Q = \ker(\varphi - I_N)$ is cyclic of order p^{v_0}, generated by*

$$u_0 := p^{s - v_0} q(y) \in p^{c_1 + 1} N.$$

Proof. Write $P(u) = \sum_{j=0}^{r} a_j u^j$ ($a_r = 1$) and $Q(u) = \sum_{j=0}^{r-1} b_j u^j$. Since $y(y + y^{-1} - 2) = (y - 1)^2$, expanding (3) gives

$$f_0(y) = \sum_{j=0}^{r} a_j y^{r-j} (y - 1)^{2j} + \sum_{j=0}^{r-1} b_j y^{r-j} (y - 1)^{2j+1} \in \mathbb{Z}[y].$$

Each P-summand has degree $r + j \leq 2r$ (attaining $2r$ uniquely at $j = r$ with leading coefficient $a_r = 1$), and each Q-summand has degree $r + j + 1 \leq 2r$ (attaining $2r$ only at $j = r - 1$ with coefficient $b_{r-1} \equiv 0 \pmod{p}$ by Lemma 3.1(i)). Hence $\deg(f_0) = d = 2r$ and its leading coefficient is $1 + b_{r-1} \equiv 1 \pmod{p}$, a unit in R.

(i) Reducing modulo p and applying Lemma 3.1(i) yields $f(y) \equiv f_0(y) \equiv (y - 1)^{2r} = (y - 1)^d \pmod{p}$. In particular $f(0) \equiv (-1)^d = 1 \pmod{p}$ is a unit in R, so y is invertible in N and $\varphi \in$

$\mathrm{Aut}(N)$. Moreover $(\varphi - I_N)^d \in p\,\mathrm{End}(N)$, so by the binomial theorem $\varphi^{p^k} = (I_N + (\varphi - I_N))^{p^k} \equiv I_N \pmod{p^s}$ for all sufficiently large k. Thus φ has p-power order p^{m_0} for some $m_0 \geq 1$.

(ii) Since $N = R[y]/(f(y))$ is generated over R by $\{y^k : k \in \mathbb{Z}\}$ and φ acts as multiplication by y, every elementary wedge in the coinvariants $(\bigwedge^2 N)_Q = (\bigwedge^2 N)/\langle \varphi(x) \wedge \varphi(x') - x \wedge x' \rangle$ satisfies

$$y^a \wedge y^b = \varphi^{-a}(y^a \wedge y^b) = 1 \wedge y^{b-a} \qquad (a, b \in \mathbb{Z}).$$

Consider the antisymmetric Laurent module over R:

$$\mathcal{A}_0 := \{h(y) \in R[y, y^{-1}] : h(y^{-1}) = -h(y) \text{ and } [y^0]h = 0\}.$$

As an R-module, $\mathcal{A}_0$ is free on the basis $\{y^k - y^{-k} : k \geq 1\}$. Define an R-linear surjection $\Psi : \mathcal{A}_0 \twoheadrightarrow (\bigwedge^2 N)_Q$ on this basis by

$$\Psi(y^k - y^{-k}) := 1 \wedge y^k \qquad (k \geq 1).$$

Crucially, this definition involves *no division by* 2 and holds uniformly for every prime $p \geq 2$. Since $1 \wedge y^{-k} = -(1 \wedge y^k)$ and $1 \wedge 1 = 0$ in $(\bigwedge^2 N)_Q$, the map Ψ satisfies $\Psi(y^k - y^{-k}) = 1 \wedge y^k$ for all $k \in \mathbb{Z}$. A defining presentation of $(\bigwedge^2 N)_Q$ on the generators $1 \wedge y^k$ ($k \in \mathbb{Z}$) consists of the antisymmetry relations ($1 \wedge y^{-k} = -(1 \wedge y^k)$, $1 \wedge 1 = 0$) together with the module relations $1 \wedge y^m f(y) = 0$ for all $m \in \mathbb{Z}$ (equivalently $1 \wedge y^m f_0(y) = 0$, as f and f_0 differ by a unit of R). Under Ψ, the relation $1 \wedge y^m f_0(y) = 0$ corresponds precisely to the antisymmetrized Laurent polynomial

$$\mathcal{R}_m(y) := y^m f_0(y) - y^{-m} f_0(y^{-1}) \in \mathcal{A}_0 \qquad (m \in \mathbb{Z}).$$

Hence $\ker(\Psi)$ is the R-span of $\{\mathcal{R}_m(y) : m \in \mathbb{Z}\}$.

Set $u := y + y^{-1} - 2 \in R[y, y^{-1}]$. Define polynomials $U_k(u) \in \mathbb{Z}[u]$ by $U_0(u) = 1$, $U_1(u) = u + 2$, and $U_k(u) = (u+2)U_{k-1}(u) - U_{k-2}(u)$ for $k \geq 2$. By induction, $U_k(u)$ is monic of degree k in u and satisfies

$$y^k - y^{-k} = (y - y^{-1})\, U_{k-1}(u) \qquad (k \geq 1).$$

Because $\{U_{k-1}(u) : k \geq 1\}$ is an R-basis of $R[u]$, we have $\mathcal{A}_0 = (y - y^{-1}) \cdot R[u]$, a free $R[u]$-module of rank 1.

Now reindex $\mathcal{R}_m$ by setting $m = k - r$ ($k \in \mathbb{Z}$). From (3), we have $y^{-r} f_0(y) = P(u) + (y-1)Q(u)$ and $y^r f_0(y^{-1}) = P(u) + (y^{-1} - 1)Q(u)$, whence

$$\mathcal{R}_{k-r}(y) = (y^k - y^{-k})P(u) + (y^{k+1} - y^k - y^{-k-1} + y^{-k})Q(u).$$

We analyze this spanning set of $\ker(\Psi)$ in two steps:

- For $k = 0$: $\mathcal{R}_{-r}(y) = (y - y^{-1})Q(u)$.
- For $k \geq 1$: adding $\mathcal{R}_{k-r}(y)$ and $\mathcal{R}_{-k-r}(y)$ cancels the $P(u)$ terms and yields

  $$\mathcal{R}_{k-r}(y) + \mathcal{R}_{-k-r}(y) = (y^{k+1} - y^{k-1} + y^{-k+1} - y^{-k-1})Q(u) = (y - y^{-1})(y^k + y^{-k})Q(u).$$

  Define $T_k(u) := y^k + y^{-k} \in \mathbb{Z}[u]$ ($T_1 = u + 2$, $T_2 = (u+2)^2 - 2$, $T_k = (u+2)T_{k-1} - T_{k-2}$). For every $k \geq 1$, $T_k(u)$ is monic of degree k in u. Together with the constant 1 from $k = 0$, the family $\{1, T_1(u), T_2(u), \dots\}$ forms an R-basis of $R[u]$. Thus the R-span of $\{\mathcal{R}_{-r}\} \cup \{\mathcal{R}_{k-r} + \mathcal{R}_{-k-r} : k \geq 1\}$ is the entire submodule $(y - y^{-1}) \cdot R[u]Q(u)$.
- Modulo $(y - y^{-1}) \cdot R[u]Q(u)$, each remaining generator $\mathcal{R}_{k-r}(y)$ ($k \geq 1$) reduces to $(y^k - y^{-k})P(u) = (y - y^{-1})U_{k-1}(u)P(u)$ (and $\mathcal{R}_{-k-r} \equiv -\mathcal{R}_{k-r}$ adds nothing new). Since $\{U_{k-1}(u) : k \geq 1\}$ is an R-basis of $R[u]$, these generate precisely $(y - y^{-1}) \cdot R[u]P(u)$.

Therefore $\ker(\Psi) = (y - y^{-1}) \cdot (P(u), Q(u))R[u]$. By Lemma 3.1(ii),

$$(\bigwedge^2 N)_Q \;\cong\; \mathcal{A}_0/\ker(\Psi) \;\cong\; R[u]/(P(u), Q(u)) \;\cong\; A.$$

(iii) Since $f(y)$ is monic of degree d, Euclidean division in $R[y]$ gives $f(y) - f(1) = (y-1)q(y)$ with $q(y) \in R[y]$ monic of degree $d-1$. Every element of N has a unique representative $g(y) \in R[y]$ of degree $< d$. Then $g(y) \bmod f(y)$ lies in $N^Q = \ker(\varphi - I_N)$ if and only if $(y-1)g(y)$ is divisible by $f(y)$ in $R[y]$; comparing degrees and leading coefficients, this holds if and only if $(y-1)g(y) = c \cdot f(y)$ in $R[y]$ for some $c \in R$. Evaluating at $y = 1$ forces $c \cdot f(1) = 0$ in $R = \mathbb{Z}/p^s\mathbb{Z}$. By (3), $f_0(1) = P(0)$, so $f(1)$ equals $P(0)$ times a unit of R modulo p^s. By Lemma 3.1(iii), $v_p(f(1)) = v_p(P(0)) = v_0 \in \{1, \dots, c_1\}$. Thus $c \cdot f(1) = 0$ in $\mathbb{Z}/p^s\mathbb{Z}$ if and only if $c \in p^{s-v_0}R$. For each such c, we have $c \cdot f(y) = c(y-1)q(y)$ in $R[y]$; since $y - 1$ is monic (hence a non-zero-divisor in $R[y]$), this forces $g(y) = cq(y)$. Because $q(y)$ is monic of degree $d-1$, the element $u_0 := p^{s-v_0}q(y) \in N$ has exact additive order p^{v_0} and generates N^Q. Finally, since $s = 2c_1 + 1$ and $v_0 \le c_1$, we have $s - v_0 \ge c_1 + 1$, whence $u_0 \in p^{c_1+1}N$. □

4 The Non-Split Cyclic Extension and Proof of the Main Theorem

Theorem 4.1 (Nontrivial Case)**.** *Let $p \ge 2$ be any prime, let A be a nontrivial finite abelian p-group as in (1), and let N, φ, m_0, u_0 be as in Lemma 3.2. Set $m := m_0 + s$ (where $s = 2c_1 + 1$), and let G be the cyclic extension*

$$1 \longrightarrow N \longrightarrow G \longrightarrow C_{p^m} \longrightarrow 1 \tag{4}$$

generated by N and an element y subject to the relations

$$y^{-1}xy = \varphi(x) \quad (x \in N) \qquad \text{and} \qquad y^{p^m} = u_0.$$

Then (4) is a non-split extension, and G is a 2-generated metabelian finite nonabelian p-group of order p^{2rs+m} with $M(G) \cong A$.

Proof. We divide the proof into four steps.

Step 1: Group existence, non-splitting, and structure. Since $\varphi^{p^{m_0}} = I_N$ and $m = m_0 + s > m_0$, we have $\varphi^{p^m} = I_N = \mathrm{Inn}_N(u_0)$ (as N is abelian), and $\varphi(u_0) = u_0$ because $u_0 \in N^Q$. By Schreier's cyclic-extension criterion, G is a well-defined finite group of order $|N| \cdot p^m = p^{ds+m} = p^{2rs+m}$. Moreover, the norm operator of C_{p^m} on N vanishes:

$$\sum_{j=0}^{p^m-1} \varphi^j = p^s \sum_{j=0}^{p^{m_0}-1} \varphi^j = 0 \qquad \text{on } N,$$

because $\varphi^{p^{m_0}} = I_N$ and $p^s N = 0$. Writing N additively, any lift xy ($x \in N$) of the generator of $G/N \cong C_{p^m}$ therefore satisfies

$$(xy)^{p^m} = \left(\sum_{j=0}^{p^m-1} \varphi^j(x) \right) + y^{p^m} = u_0 \neq 0 \quad \text{in } N,$$

as u_0 has exact order $p^{v_0} \ge p$. Hence no lift of the generator has order p^m, so (4) does not split.

Since both N and $G/N \cong C_{p^m}$ are abelian, G is metabelian. Because $d = 2r \ge 2$, the basis element $1_N \in N = R[y]/(f(y))$ satisfies $\varphi(1_N) = y \neq 1_N$, so G is nonabelian. Moreover, N is generated as a $\mathbb{Z}[\varphi]$-module by 1_N, so $G = \langle 1_N, y \rangle$ is 2-generated.

Step 2: Upper bound $A \twoheadrightarrow M(G)$ via stem covers. Let $1 \to Z \to \widehat{G} \xrightarrow{\pi} G \to 1$ be a stem cover of G, so that $Z \le Z(\widehat{G}) \cap \widehat{G}'$ and $Z \cong M(G)$. Set $\widehat{N} := \pi^{-1}(N) \trianglelefteq \widehat{G}$, and choose a lift $\widehat{y} \in \widehat{G}$ of $y \in G$.

Since $Z \le Z(\widehat{G})$ and $\widehat{N}/Z \cong N$ is abelian, we have $[\widehat{N}, \widehat{N}] \le Z \le Z(\widehat{G})$. Thus the commutator pairing $(\widehat{x}, \widehat{x}') \mapsto [\widehat{x}, \widehat{x}']$ depends only on the cosets $x = \pi(\widehat{x}), x' = \pi(\widehat{x}') \in N$, is bilinear and alternating, and induces a homomorphism $\kappa : \bigwedge^2 N \to Z$ with $\mathrm{im}(\kappa) = [\widehat{N}, \widehat{N}]$. Because $Z \le Z(\widehat{G})$, conjugation by $\widehat{y}$ acts trivially on Z, so

$$\kappa(\varphi(x), \varphi(x')) = [\widehat{y}^{-1}\widehat{x}\widehat{y},\ \widehat{y}^{-1}\widehat{x}'\widehat{y}] = \widehat{y}^{-1}[\widehat{x}, \widehat{x}']\widehat{y} = [\widehat{x}, \widehat{x}'] = \kappa(x, x')$$

for all $x, x' \in N$. Hence κ factors through a homomorphism

$$\bar{\kappa} : (\textstyle\bigwedge^2 N)_Q \longrightarrow Z \qquad \text{with } \mathrm{im}(\bar{\kappa}) = [\widehat{N}, \widehat{N}].$$

We claim that $Z = [\widehat{N}, \widehat{N}]$. Pass to the quotient $\bar{G} := \widehat{G}/[\widehat{N}, \widehat{N}]$, and denote the images of $\widehat{N}, Z, \widehat{y}$ by $\bar{N}, \bar{Z}, \bar{y}$, respectively. Then $\bar{N}$ is an *abelian* normal subgroup of $\bar{G}$, $\bar{Z} \le Z(\bar{G}) \cap \bar{G}'$, $\bar{N}/\bar{Z} \cong N$, and $\bar{G} = \langle \bar{N}, \bar{y} \rangle$. Let $\bar{\varphi} \in \mathrm{Aut}(\bar{N})$ denote conjugation by $\bar{y}$, i.e., $\bar{\varphi}(\bar{x}) := \bar{y}^{-1}\bar{x}\bar{y}$. Writing the abelian group $\bar{N}$ additively, set $D := (\bar{\varphi} - I)(\bar{N}) \le \bar{N}$. Since $\bar{\varphi}$ commutes with $\bar{\varphi} - I$, the subgroup D is invariant under conjugation by $\bar{y}$; since $\bar{N}$ is abelian, every element of $\bar{N}$ centralizes D. Hence $D \trianglelefteq \langle \bar{N}, \bar{y} \rangle = \bar{G}$. In the quotient $\bar{G}/D$, conjugation by $\bar{y}D$ acts trivially on the abelian subgroup $\bar{N}/D$, so $\bar{G}/D$ is abelian and therefore $\bar{G}' \le D$. Conversely, every element $(\bar{\varphi} - I)(\bar{x}) = \bar{x}^{-1}\bar{y}^{-1}\bar{x}\bar{y} = [\bar{x}, \bar{y}]$ of D is a commutator in $\bar{G}$, so $D \le \bar{G}'$. Thus $\bar{G}' = D = (\bar{\varphi} - I)(\bar{N})$.

Now take any $\bar{z} \in \bar{Z}$. Since $\bar{Z} \le \bar{G}' = (\bar{\varphi} - I)(\bar{N})$, there exists $\bar{x} \in \bar{N}$ such that $\bar{z} = (\bar{\varphi} - I)(\bar{x})$. Projecting this equation to $\bar{N}/\bar{Z} \cong N$ yields $(\varphi - I)(x) = 0$, where $x \in N$ is the image of $\bar{x}$. Thus $x \in N^Q = \langle u_0 \rangle$ by Lemma 3.2(iii), so $x = ku_0$ in N for some integer $k \in \mathbb{Z}$. On the other hand, $\bar{y}^{p^m} \in \bar{N}$ projects to $y^{p^m} = u_0 \in N$, so $\bar{x}$ and $(\bar{y}^{p^m})^k$ lie in the same $\bar{Z}$-coset of $\bar{N}$; that is, in multiplicative notation,

$$\bar{x} = (\bar{y}^{p^m})^k \cdot \bar{z}' \qquad \text{for some } \bar{z}' \in \bar{Z} \le Z(\bar{G}).$$

Conjugation by $\bar{y}$ fixes both $\bar{y}^{p^m}$ and $\bar{z}' \in Z(\bar{G})$, so $\bar{\varphi}(\bar{x}) = \bar{x}$ and therefore $\bar{z} = (\bar{\varphi} - I)(\bar{x}) = 0$. Since $\bar{z} \in \bar{Z}$ was arbitrary, $\bar{Z} = 1$, which means $Z = [\widehat{N}, \widehat{N}] = \mathrm{im}(\bar{\kappa})$. Combining this with Lemma 3.2(ii) gives a surjection $A \cong (\bigwedge^2 N)_Q \twoheadrightarrow Z \cong M(G)$.

Step 3: Lower bound $M(G) \twoheadrightarrow A$ via an explicit stem extension. Identify A with $(\bigwedge^2 N)_Q$ via Lemma 3.2(ii), and let $\pi_\wedge : \bigwedge^2 N \twoheadrightarrow A$ be the canonical projection. Note that $p^{c_1}A = 0$. Fix the R-basis $e_0, e_1, \ldots, e_{d-1}$ of N given by $e_i := y^i \bmod f(y)$.

Define a bilinear map $\psi : N \times N \to A$ on basis elements by

$$\psi(e_i, e_j) := \begin{cases} \pi_\wedge(e_i \wedge e_j) & \text{if } i < j, \\ 0 & \text{if } i \ge j, \end{cases}$$

extended $\mathbb{Z}$-bilinearly. Since $p^{c_1}A = 0$ and $s = 2c_1 + 1 > c_1$, ψ is well-defined on $N \times N$ and satisfies

$$\psi(x, x') - \psi(x', x) = \pi_\wedge(x \wedge x') \qquad (x, x' \in N). \tag{5}$$

Define a central extension $1 \to A \to \widetilde{N} \to N \to 1$ on the set $\widetilde{N} := N \times A$ with group law

$$(x, a) \cdot (x', a') := \big(x + x',\ a + a' + \psi(x, x')\big).$$

Associativity holds because ψ is bilinear (hence a 2-cocycle). By (5), the commutator in $\widetilde{N}$ is

$$[(x, a), (x', a')] = \big(0,\ \psi(x, x') - \psi(x', x)\big) = \big(0,\ \pi_\wedge(x \wedge x')\big),$$

so the central subgroup $A = \{(0, a) : a \in A\}$ coincides with $[\widetilde{N}, \widetilde{N}] \le Z(\widetilde{N})$.

Next, for any $x = \sum_{i=0}^{d-1} x_i e_i \in N$ with integer representatives $x_i \in \mathbb{Z}$, define $\eta : N \to A$ by

$$\eta(x) := \sum_{i=0}^{d-1} \binom{x_i}{2} \psi(\varphi(e_i), \varphi(e_i)) + \sum_{0 \le i < j < d} x_i x_j \Big(\psi(\varphi(e_i), \varphi(e_j)) - \psi(e_i, e_j) \Big). \tag{6}$$

We verify four properties of η:

1. *Well-definedness modulo p^s (including $p = 2$).* Replacing x_i by $x_i + p^s$ shifts $\binom{x_i}{2}$ by $x_i p^s + \frac{p^s(p^s-1)}{2}$ and shifts $x_i x_j$ by a multiple of p^s. Since $s = 2c_1 + 1$, we have $p^{s-1} \mid \frac{p^s(p^s-1)}{2}$ for every prime $p \ge 2$, and $s - 1 = 2c_1 \ge c_1$. Because $p^{c_1} A = 0$, $\eta(x)$ is independent of the choice of integer representatives $x_i \bmod p^s$.

2. *Exact coboundary identity.* For all $x = \sum x_i e_i$ and $x' = \sum x'_i e_i$ in N, using $\binom{x_i + x'_i}{2} - \binom{x_i}{2} - \binom{x'_i}{2} = x_i x'_i$ gives

$$\begin{aligned} \eta(x + x') - \eta(x) - \eta(x') = &\sum_{i=0}^{d-1} x_i x'_i \, \psi(\varphi(e_i), \varphi(e_i)) \\ &+ \sum_{0 \le i < j < d} (x_i x'_j + x_j x'_i) \Big(\psi(\varphi(e_i), \varphi(e_j)) - \psi(e_i, e_j) \Big). \end{aligned}$$

   In $A = (\bigwedge^2 N)_{\mathbb{Q}}$, we have $\pi_\wedge(\varphi(e_i) \wedge \varphi(e_j)) = \pi_\wedge(e_i \wedge e_j)$, which by (5) implies

$$\psi(\varphi(e_i), \varphi(e_j)) - \psi(\varphi(e_j), \varphi(e_i)) = \psi(e_i, e_j) - \psi(e_j, e_i),$$

   i.e., $\psi(\varphi(e_i), \varphi(e_j)) - \psi(e_i, e_j)$ is *symmetric* in (i, j) (and $\psi(e_i, e_i) = 0$). Therefore

$$\eta(x+x') - \eta(x) - \eta(x') = \sum_{i,j=0}^{d-1} x_i x'_j \Big(\psi(\varphi(e_i), \varphi(e_j)) - \psi(e_i, e_j) \Big) = \psi(\varphi(x), \varphi(x')) - \psi(x, x'). \tag{7}$$

3. *Vanishing of the p^m-orbit sum.* Since $\varphi^{p^{m_0}} = I_N$ and $m = m_0 + s$, the orbit $(\varphi^j(x))_{0 \le j < p^m}$ repeats the p^{m_0}-cycle exactly p^s times. Because $p^s A = 0$,

$$\sum_{j=0}^{p^m - 1} \eta(\varphi^j(x)) = p^s \sum_{j=0}^{p^{m_0} - 1} \eta(\varphi^j(x)) = 0 \qquad (x \in N). \tag{8}$$

4. *Vanishing on u_0.* By Lemma 3.2(iii), $u_0 \in p^{c_1+1} N$, so every integer coordinate $u_{0,i}$ of u_0 satisfies $p^{c_1+1} \mid u_{0,i}$. Hence $p^{c_1} \mid u_{0,i}$ gives $\psi(x, u_0) = \psi(u_0, x) = 0$ in A for all $x \in N$. Furthermore, since $p^{c_1+1} \mid u_{0,i}$, we have

$$p^{c_1} \,\Big|\, \binom{u_{0,i}}{2} = \frac{u_{0,i}(u_{0,i} - 1)}{2}$$

   for every coordinate $u_{0,i}$ (including $u_{0,i} = 0$) and every prime $p \ge 2$, as well as $p^{2c_1+2} \mid u_{0,i} u_{0,j}$. Because $p^{c_1} A = 0$, every term in (6) vanishes at $x = u_0$, so $\eta(u_0) = 0$.

Now define $\Phi : \widetilde{N} \to \widetilde{N}$ by $\Phi(x, a) := (\varphi(x), a + \eta(x))$. By (7), Φ is a group homomorphism, and since φ is bijective, $\Phi \in \mathrm{Aut}(\widetilde{N})$. Iterating Φ and using (8) gives $\Phi^{p^m}(x, a) = (\varphi^{p^m}(x), a + \sum_{j=0}^{p^m-1} \eta(\varphi^j(x))) = (x, a)$, so $\Phi^{p^m} = \mathrm{id}_{\widetilde{N}}$. Set $\widetilde{u}_0 := (u_0, 0) \in \widetilde{N}$. By property 4 above, $\psi(x, u_0) = \psi(u_0, x) = 0$ for all $x \in N$, so $\widetilde{u}_0 \in Z(\widetilde{N})$ and $\mathrm{Inn}_{\widetilde{N}}(\widetilde{u}_0) = \mathrm{id}_{\widetilde{N}} = \Phi^{p^m}$; moreover, $\Phi(\widetilde{u}_0) = (\varphi(u_0), \eta(u_0)) = (u_0, 0) = \widetilde{u}_0$.

By Schreier's cyclic-extension criterion, there exists a finite group E containing $\widetilde{N}$ as a normal subgroup with $E/\widetilde{N} \cong C_{p^m}$, generated by $\widetilde{N}$ and an element $\widetilde{y}$ subject to $\widetilde{y}^{-1} z \widetilde{y} = \Phi(z)$ $(z \in \widetilde{N})$ and $\widetilde{y}^{p^m} = \widetilde{u}_0$. Since $A \leq Z(\widetilde{N})$ and $\Phi(0, a) = (0, a)$ for all $a \in A$, we have $A \leq Z(E)$. Since $A = [\widetilde{N}, \widetilde{N}] \leq E'$, we have $A \leq Z(E) \cap E'$. Finally, $E/A \cong G$. Therefore $1 \to A \to E \to G \to 1$ is a stem extension of G with kernel A, which induces a surjective homomorphism $M(G) \twoheadrightarrow A$.

Step 4: Conclusion. From Steps 2 and 3 we have surjections $A \twoheadrightarrow M(G)$ and $M(G) \twoheadrightarrow A$ between finite groups. Hence $|A| \geq |M(G)| \geq |A|$, so both surjections are isomorphisms and $M(G) \cong A$. □

Proof of Theorem 1.1. Combine Proposition 2.1 (for $A = 1$) and Theorem 4.1 (for $A \neq 1$). □

Remark 4.2. In homological terms, Step 2 of Theorem 4.1 corresponds to the vanishing of $E^{\infty}_{1,1}$ in the Lyndon–Hochschild–Serre spectral sequence $E^2_{i,j} = H_i(C_{p^m}, H_j(N, \mathbb{Z})) \Rightarrow H_{i+j}(G, \mathbb{Z})$, where $E^2_{1,1} = N^Q / \mathrm{Norm}_Q(N) = \langle u_0 \rangle$ is killed by the transgression $d^2_{3,0} : H_3(C_{p^m}, \mathbb{Z}) \to H_1(C_{p^m}, N)$. The stem-cover proof in Step 2 achieves the same conclusion directly in a few elementary lines without invoking spectral sequences.

5 Explicit Example and Exact Computational Verification

Example 5.1 ($p = 2$, $A = \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$)**.** Here $t = 3$ (odd), $(c_1, c_2, c_3) = (3, 2, 1)$, $(m_1, m_2, m_3) = (1, 1, 1)$, $r = 3$, $d = 6$, and $s = 2c_1 + 1 = 7$ ($R = \mathbb{Z}/128\mathbb{Z}$). Lemma 3.1 yields:

$$g_0(u) = 1, \quad g_1(u) = u, \quad g_2(u) = u^2 + 2, \quad P_0(u) = g_3(u) = u^3 + 4u,$$
$$Q(u) = 2(u^2 + 2) = 2u^2 + 4, \qquad P(u) = P_0(u) + 8 = u^3 + 4u + 8.$$

Explicitly, $8 = -2u\, P_0(u) + (u^2 + 2)\, Q(u)$ in $\mathbb{Z}[u]$, so $\alpha(u) = -2u \in 2\mathbb{Z}[u]$ and $1 + \alpha(u) = 1 - 2u$ is a unit in $(\mathbb{Z}/128\mathbb{Z})[u]$; moreover $P(0) = 8$ has $v_0 = 3 = c_1$. The polynomial $f_0(y) = y^3 P(y + y^{-1} - 2) + y^3(y - 1)Q(y + y^{-1} - 2)$ has degree 6 and leading coefficient $1 + 2 = 3$ (whose inverse modulo 128 is 43). Normalizing modulo 128 produces the monic polynomial

$$f(y) \equiv y^6 + 80y^5 + 57y^4 + 28y^3 + 95y^2 + 40y + 43 \pmod{128},$$

with $f(1) \equiv 43 \cdot 8 \equiv 88 \pmod{128}$ ($v_2(88) = 3 = v_0$), $u_0 = 2^{7-3} q(y) = 16q(y) \in 16N = 2^{c_1+1}N$, minimal order exponent $m_0 = 9$, and $m = m_0 + s = 16$. The resulting 2-generated metabelian 2-group G of order $2^{6 \cdot 7 + 16} = 2^{58}$ has exact Schur multiplier $M(G) \cong \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

To provide an independent exact computational verification across representative instances of our construction, we checked 22 test cases using exact integer and polynomial arithmetic (zero floating-point operations, exact Smith Normal Form via SymPy) in the companion script `verify_kourovka_1530.py`. Besides checking the 4 trivial base cases (Q_8 and M_{p^3} for $p \in \{3, 5, 7\}$) directly from their presentations, for each of the 18 nontrivial instances the script independently verifies:

1. Lemma 3.1: both $\mathbb{Z}[u]/(P_0, Q) \cong A$ over $\mathbb{Z}$ and $R[u]/(P, Q) \cong A$ over R;
2. Lemma 3.2: direct Smith Normal Form of $(\bigwedge^2 N)_Q$ and $N^Q = \langle u_0 \rangle$, together with $u_0 \in p^{c_1+1}N$ and $p^{c_1} \mid \binom{u_{0,i}}{2}, \binom{p^s}{2}$;
3. Theorem 4.1: direct Hopf-formula computation $M(G) \cong (R_F \cap [F, F])/[F, R_F]$ from the full polycyclic presentation of G via all confluence overlaps and exact Smith Normal Form.

Table 1 summarizes the 22 certified instances (4 trivial base cases and 18 nontrivial cases spanning $p \in \{2, 3, 5, 7\}$ and up to 5 distinct invariant-factor blocks), all passing with exact agreement.

Table 1: Summary of independent exact Hopf-formula computations across 22 representative instances (all 22/22 passed).

Prime p	Target Abelian Group A (exponents)	$d = 2r$	$s = 2c_1 + 1$	m_0	$m = m_0 + s$	$\lvert G\rvert$	Certified $M(G)$
2	1 (group Q_8)	—	—	—	—	2^3	1 (PASS)
$3, 5, 7$	1 (groups M_{p^3})	—	—	—	—	p^3	1 (PASS)
2	$[1]$	2	3	3	6	2^{12}	$[1]$ (PASS)
2	$[2]$	2	5	5	10	2^{20}	$[2]$ (PASS)
2	$[4, 2]$	4	9	10	19	2^{55}	$[4, 2]$ (PASS)
2	$[3, 2, 1]$	6	7	9	16	2^{58}	$[3, 2, 1]$ (PASS)
2	$[5, 4, 3]$	6	11	13	24	2^{90}	$[5, 4, 3]$ (PASS)
2	$[4, 3, 2, 1]$	8	9	11	20	2^{92}	$[4, 3, 2, 1]$ (PASS)
2	$[4, 4, 2, 1, 1]$	10	9	12	21	2^{111}	$[4, 4, 2, 1, 1]$ (PASS)
3	$[1]$	2	3	2	5	3^{11}	$[1]$ (PASS)
3	$[3]$	2	7	7	14	3^{28}	$[3]$ (PASS)
3	$[4, 2]$	4	9	10	19	3^{55}	$[4, 2]$ (PASS)
3	$[5, 4, 3]$	6	11	12	23	3^{89}	$[5, 4, 3]$ (PASS)
3	$[5, 4, 3, 2]$	8	11	12	23	3^{111}	$[5, 4, 3, 2]$ (PASS)
3	$[5, 4, 3, 2, 1]$	10	11	13	24	3^{134}	$[5, 4, 3, 2, 1]$ (PASS)
3	$[4, 4, 2, 2]$	8	9	10	19	3^{91}	$[4, 4, 2, 2]$ (PASS)
3	$[3, 3, 3]$	6	7	8	15	3^{57}	$[3, 3, 3]$ (PASS)
5	$[3, 2, 1]$	6	7	8	15	5^{57}	$[3, 2, 1]$ (PASS)
5	$[4, 3, 2, 1]$	8	9	10	19	5^{91}	$[4, 3, 2, 1]$ (PASS)
7	$[4, 2, 1]$	6	9	9	18	7^{72}	$[4, 2, 1]$ (PASS)

References

[1] E. I. Khukhro and V. D. Mazurov (eds.), *The Kourovka Notebook: Unsolved Problems in Group Theory*, 21st edition, arXiv:1401.0300v50 (November 2026), Problem 15.30 (Ya. G. Berkovich, Issue 15, 2002).

[2] G. Karpilovsky, *The Schur Multiplier*, London Mathematical Society Monographs, New Series, Vol. 2, Clarendon Press, Oxford, 1987.

[3] P. K. Rai, *On the occurrence of elementary abelian p-groups as the Schur multiplier of non-abelian p-groups*, Comptes Rendus Mathématique **361** (2023), 803–806, doi:10.5802/crmath.445.

[4] S. Hatui, T. N. Mavely, and S. Sabnam, *On the Schur multiplier of p-groups with abelianization s-elementary abelian*, arXiv:2605.00810v1 (May 2026).