A CLASSIFICATION OF METACYCLIC GROUPS BY GROUP INVARIANTS

ÀNGEL GARCÍA-BLÁZQUEZ AND ÁNGEL DEL RÍO

Departamento de Matemáticas, Universidad de Murcia, 30100, Murcia, Spain

Dedicated to Toma Albu and Constantin Năstăsescu in their 80th birthday

Abstract. We obtain a new classification of the finite metacyclic group in terms of group invariants. We present an algorithm to compute these invariants, and hence to decide if two given finite metacyclic groups are isomorphic, and another algorithm which computes all the metacyclic groups of a given order. A GAP implementation of these algorithms is given.

1. Introduction

Classifying groups is a fundamental problem in group theory. Unfortunately it is a task which seems out of reach except for restricted families of groups. One of the classes which have received much attention is that of finite metacyclic groups. It is well known that every finite metacyclic group has a presentation of the following form

$$\mathcal{G}_{m,n,s,t} = \left\langle a, b \mid a^m = 1, b^n = a^s, a^b = a^t \right\rangle$$

for natural numbers m, n, s, t satisfying $s(t-1) \equiv t^n - 1 \equiv 0 \mod m$. However, the parameters m, n, s and t are not invariants of the group. Traditionally the authors dealing with the classification of finite metacyclic group select distinguished values of m, n, s and t so that each isomorphism class is described by a unique election of the parameters (see [Zas99, Hal59, Bey72, Kin73, Lie96, Lie94, NX88, Réd89, Lin71, Sim94]). This approach was culminated by C.E. Hempel who presented a classification of all the finite metacyclic groups in [Hem00]. However it is not clear how to use this classification to describe the distinguished parameters identifying a given metacyclic group and how those distinguished parameters are connected with group invariants.

The aim of this paper is to present an alternative classification of the finite metacyclic using a slightly different approach in terms of group invariants which allows an easy implementation. Namely, we associate to every finite metacyclic group G a 4-tuple $\mathrm{MCINV}(G) = (m_G, n_G, s_G, \Delta_G)$ where m_G, n_G and s_G play the role of m, n and s in the presentation above and Δ_G is a cyclic subgroup of units modulo a divisor of m_G. Our main result consists in proving that $\mathrm{MCINV}(G)$ is an invariant of the group G which determines G up to isomorphism, i.e. if G and H are two finite metacyclic groups then they are isomorphic if and only if $\mathrm{MCINV}(G) = \mathrm{MCINV}(H)$ (Theorem A). Moreover, we describe in Theorem B the possible values (m, n, s, Δ) of $\mathrm{MCINV}(G)$ and for such value we show how to find an integer t such that $\mathrm{MCINV}(\mathcal{G}_{m,n,s,t}) = (m, n, s, \Delta)$ (Theorem C). This allows a computer implementation of the following function: one which computes $\mathrm{MCINV}(G)$ for any given finite metacyclic group, and hence of another function which decide whether two metacyclic groups are isomorphic, and another one which computes all the metacyclic subgroups of a given order.

To define $\mathrm{MCINV}(G)$ we need to introduce some notation. First of all, we adopt the convention that 0 is not a natural number, so $\mathbb{N}$ denotes the set of positive integers. Moreover by a prime we mean a prime in $\mathbb{N}$. If $m \in \mathbb{N}$, p is a prime, π is a set of primes and A a finite abelian group then we denote

E-mail address: `angel.garcia11@um.es, adelrio@um.es`.

1991 *Mathematics Subject Classification.* 20D10,20E99.

Key words and phrases. Finite groups, Metacyclic groups.

Partially supported Grant PID2020-113206GB-I00 funded by MCIN/AEI/10.13039/501100011033 and by Fundación Séneca (22004/PI/22).

$$\begin{array}{rcl}
\pi(m) & = & \text{set of primes dividing } m, \\
\mathcal{U}_m & = & \text{group of units of the ring } \mathbb{Z}/m\mathbb{Z}, \\
m_p & = & \text{maximum power of } p \text{ dividing } m, \\
m_\pi & = & \prod_{p\in\pi} m_p, \\
A_\pi & = & \text{Hall } \pi\text{-subgroup of } A, \\
A_{\pi'} & = & \text{Hall } \pi'\text{-subgroup of } A.
\end{array}$$

If $t \in \mathbb{Z}$ with $\gcd(t,m) = 1$ then $[t]_m$ denotes the element of $\mathcal{U}_m$ represented by t and $\langle t\rangle_m$ denotes the subgroup of $\mathcal{U}_m$ generated by $[t]_m$. If $q \mid m$ then $\mathrm{Res}_q : \mathcal{U}_m \to \mathcal{U}_q$ denotes the natural map, i.e. $\mathrm{Res}_q([t]_m) = [t]_q$.

Let T be a cyclic subgroup of $\mathcal{U}_m$. Then we define $[T] = (r, \epsilon, o)$

$$\begin{array}{rcl}
r & = & \text{greatest divisor of } m \text{ such that } \mathrm{Res}_{r_{2'}}(T) = 1 \text{ and } \mathrm{Res}_{r_2}(T) \subseteq \langle -1\rangle_{r_2}; \\
\epsilon & = & \begin{cases} -1, & \text{if } \mathrm{Res}_{r_2}(T) \neq 1; \\ 1, & \text{otherwise.} \end{cases} \\
o & = & |\mathrm{Res}_{m_\nu}(T_{\nu'})|, \text{ with } \nu = \pi(m) \setminus \pi(r).
\end{array}$$

If moreover, $n, s \in \mathbb{N}$ then we denote

$$[T, n, s] = m_\nu \prod_{p\in\pi(r)} m'_p$$

with m'_p defined as follows:

$$\text{if } \epsilon^{p-1} = 1 \text{ then } m'_p = \min\left(m_p, o_p r_p, \max\left(r_p, s_p, r_p \frac{s_p o_p}{n_p}\right)\right);$$

$$\text{if } \epsilon = -1 \text{ then } m'_2 = \begin{cases} r_2, & \text{if either } o_2 \leq 2 \text{ or } m_2 \leq 2r_2; \\ \frac{m_2}{2}, & \text{if } 4 \leq o_2 < n_2, 4r_2 \leq m, \text{ and if } s_2 \leq n_2 r_2 \text{ then } s_2 = m_2 < n_2 r_2; \\ m_2, & \text{otherwise.} \end{cases} \tag{1.1}$$

Let A be a cyclic group of order m. Then the map $\sigma_A : \mathcal{U}_m \to \mathrm{Aut}(A)$ associating $[r]_m$ with the map $a \mapsto a^r$, is a group isomorphism. If moreover A is a normal subgroup of a group G then we define

$$T_G(A) = \sigma_A^{-1}(\mathrm{Inn}_G(A)),$$

where $\mathrm{Inn}_G(A)$ is formed by the restriction to A of the inner automorphisms of G. We introduce notation for the entries of $T_G(A)$ by setting

$$(r_G(A), \epsilon_G(A), o_G(A)) = [T_G(A)].$$

Definition 1.1. *Let G be a group. A* metacyclic kernel *of G is a normal subgroup A of G such that A and G/A are cyclic. A* metacyclic factorization *of a group G is an expression $G = AB$ where A is a normal cyclic subgroup of G and B is a cyclic subgroup of G.*

A minimal kernel *of G is a kernel of G of minimal order.*

A metacyclic factorization $G = AB$ is said to be minimal *in G if $(|A|, r_G(A), [G : B])$ is minimal in the lexicographical order. In that case we denote $m_G = |A|$, $n_G = [G : A]$, $s_G = [G : B]$ and $r_G = r_G(A)$.*

Clearly a group is metacyclic if and only if it has metacyclic kernel if and only if it has a metacyclic factorization. Sometimes we abbreviate metacyclic kernel of G or metacyclic factorization of G and we simply say kernel of G or factorization of G.

If $G = AB$ is a metacyclic factorization of G then we denote

$$\Delta(AB) = \mathrm{Res}_{[T,n,s]}(T), \quad \text{with} \quad T = T_G(A), \quad n = [G : A] \quad \text{and} \quad s = [G : B].$$

We will prove that $\Delta(AB)$ is constant for all the minimal metacyclic factorizations (Corollary 3.7). This allows to define the desired invariant:

$$\mathrm{MCINV}(G) = (|A|, [G : A], [G : B], \Delta(AB)), \text{ with } G = AB \text{ minimal factorization of } G.$$

Our first result states that $\mathrm{MCINV}(G)$ determines G up to isomorphisms, formally:

Theorem A. *Two finite metacyclic groups G and H are isomorphic if and only if* $\mathrm{MCINV}(G) = \mathrm{MCINV}(H)$.

Our next result describes the values realized as $\mathrm{MCINV}(G)$ with G a finite metacyclic group.

Theorem B. *Let $m,n,s \in \mathbb{N}$ and let Δ be a cyclic subgroup of $\mathcal{U}_{m'}$ with $m' \mid m$. Let $[\Delta] = [r,\epsilon,o]$ and $\nu = \pi(m) \setminus \pi(r)$. Then the following conditions are equivalent:*

(1) $(m,n,s,\Delta) = \mathrm{MCINV}(G)$ *for some finite metacyclic group G.*

(2) *(a) s divides m, $|\Delta|$ divides n and $m_\nu = s_\nu = m'_\nu$.*

(b) (1.1) *holds for every $p \in \pi(r)$.*

(c) If $\epsilon = -1$ then $\frac{m_2}{r_2} \le n_2$, $m_2 \le 2s_2$ and $s_2 \ne n_2 r_2$. If moreover $4 \mid n$, $8 \mid m$ and $o_2 < n_2$ then $r_2 \le s_2$.

(d) For every $p \in \pi(r)$ with $\epsilon^{p-1} = 1$, we have $\frac{m_p}{r_p} \le s_p \le n_p$ and if $r_p > s_p$ then $n_p < s_p o_p$;

Our last result shows how to construct a metacyclic group G with given $\mathrm{MCINV}(G)$: If $m,n,s \in \mathbb{N}$ with $s \mid m$ then we define the following subgroup of $\mathcal{U}_m$:

$$\mathcal{U}_m^{n,s} = \{[t]_m : m \mid s(t-1), \quad \text{and} \quad t^n \equiv 1 \mod m\}.$$

If T is a cyclic subgroup of $\mathcal{U}_m^{n,s}$ generated by $[t]_m$ then we denote

$$\mathcal{G}_{m,n,s,T} = \mathcal{G}_{m,n,s,t} = \{a,b : a^m = 1, b^n = a^s, a^b = a^t\}.$$

It is easy to see that the isomorphism type of this group is independent of the election of the generator $[t]_m$ of T (Lemma 2.2.(5)). Moreover, the assumption $T \subseteq \mathcal{U}_m^{n,s}$ warranties that $|a| = m$, $|\mathcal{G}_{m,n,s,T}| = mn$ and $|b| = \frac{mn}{s}$.

Remark 1.2. *Suppose that m,n,s and $\Delta \le \mathcal{U}_{m'}$ satisfy the conditions of statement (2) in Theorem B and $[\Delta] = (r,\epsilon,o)$. Then $\mathrm{Res}_{m'_p}(\Delta) = \left\langle \epsilon^{p-1} + r_p \right\rangle_{m'_p}$ for every $p \in \pi(r)$ and hence there is an integer t' such that $\Delta = \langle t' \rangle_{m'}$ and $t' \equiv \epsilon^{p-1} + r_p \mod m'_p$ for every $p \in \pi(r)$. Using the Chinese Remainder Theorem we can select an integer t such that $t \equiv t' \mod m'$ and $t \equiv \epsilon^{p-1} + r_p \mod m_p$ for every $p \in \pi(r)$ and let $T = \langle t \rangle_m$. Then $T \subseteq \mathcal{U}_n^{n,s}$, $\mathrm{Res}_{m'}(T) = \Delta$ and $[T] = [\Delta]$. Then the following theorem ensures that $\mathrm{MCINV}(G_{m,n,s,T}) = (m,n,s,\Delta)$.*

Theorem C. *Let $m,n,s \in \mathbb{N}$ and let Δ be a cyclic subgroup of $\mathcal{U}_{m'}$ with $m' \mid m$. Suppose that they satisfy the conditions of (2) in Theorem B and let T be a cyclic subgroup of $\mathcal{U}_m^{n,s}$ such that $[T] = [\Delta]$ and $\mathrm{Res}_{m'}(T) = \Delta$. Then $(m,n,s,\Delta) = \mathrm{MCINV}(\mathcal{G}_{m,n,s,T})$.*

For implementation it is convenient to replace the fourth entry of $\mathrm{MCINV}(G)$ by a distinguished integer t_G so that $G \cong \mathcal{G}_{m_G,n_G,s_G,t_G}$ and $G \cong H$ if and only if $(m_G,n_G,s_G,t_G) = (m_H,n_H,s_H,t_H)$. We select t_G satisfying the conditions of Remark 1.2. In particular, $[t_G]_{m_\pi}$ is uniquely determined by the condition $t \equiv \epsilon^{p-1} + r_p \mod m_p$ for every $p \in \pi(r)$. However there is not any natural election of $[t_G]_{m_{\pi'}}$ and we simply take the minimum possible value. More precisely, if $(m,n,s,\Delta) = \mathrm{MCINV}(G)$, $(r,\epsilon,o) = [\Delta]$ and m' is given by (1.1) then define

$$t_G = \min\{t \ge 0 : \mathrm{Res}_{m'}(\langle t \rangle_m) = \Delta \quad \text{and} \quad t \equiv \epsilon^{p-1} + r_p \mod m_p \text{ for every } p \in \pi(r)\}.$$

We call (m_G,n_G,s_G,t_G) the list of *metacyclic invariants* of G. Clearly if H is another metacyclic group then $G \cong H$ if and only if G and H have the same metacyclic invariants. Moreover, by Theorem C, if (m,n,s,t) is the list of metacyclic invariants of G then $G \cong \mathcal{G}_{m,n,s,t}$.

We outline the contains of the paper: In Section 2 we introduce the general notation, not mentioned in this introduction, and present some preliminary technical results. In Section 3 we prove several lemmas on metacyclic factorizations aiming to an intrinsic description of when a metacyclic factorization is minimal. It includes an algorithm to obtain a minimal metacyclic factorization from an arbitrary one. This section concludes with Theorem 3.6 which is the keystone to prove Theorem A, Theorem B and Theorem C in Section 4. In Section 5 we introduce an algorithm to compute the metacyclic invariants of a given metacyclic group and use this to decide if two metacyclic groups are isomorphic, and another algorithm to construct all the metacyclic groups of a given order. We present also implementations in GAP [GAP12] of these algorithms.

2. Notation and preliminaries

By default all the groups in this paper are finite. We use standard notation for a group G: $Z(G)$ = center of G, G' = commutator subgroup of G, $\mathrm{Aut}(G)$ = group of automorphisms of G. If $g,h \in G$ then $|g|$ = order of g, $g^h = h^{-1}gh$, $[g,h] = g^{-1}g^h$. If π is a set of primes then g_π and $g_{\pi'}$ denote the π-part and π'-part of g, respectively. When p is a prime we rather write g_p and $g_{p'}$ than $g_{\{p\}}$ and $g_{\{p\}'}$, respectively. Similarly, if G is a finite abelian group then G_p and $G_{p'}$ denote the p-part of G and the p'-part of G, respectively.

Let G be a metacyclic group. Observe that A is a kernel of G if and only if G has a metacyclic factorization of the form $G = AB$. In that case, if

$$m = |A|, \quad n = [G : A], \quad s = [G : B] \quad \text{and} \quad T = T_G(A) = \langle t \rangle_m ,$$

then $s \mid m$, $|B| = n\frac{m}{s}$, $T \subseteq \mathcal{U}_m^{n,s}$ and A and B have generators a and b, respectively, such that $b^n = a^s$ and $a^b = a^t$. Thus $G \cong \mathcal{G}_{m,n,s,T}$.

If p is a prime then v_p denotes the p-adic valuation on the integers.

Let $a \in \mathbb{Z}$ and $m \in \mathbb{N}$. If $\gcd(a, m) = 1$ then $o_m(a)$ denotes the order of $[a]_m$ i.e. $o_m(a) = \min\{n \in \mathbb{N} : a^n \equiv 1 \mod m\}$. If $a \neq 0$ then we denote

$$\mathcal{S}\left(a \mid m\right) = \sum_{i=0}^{m-1} a^i = \begin{cases} m, & \text{if } a = 1; \\ \frac{a^m-1}{a-1}, & \text{otherwise.} \end{cases}$$

This notation occurs in the following statement where g and h are elements of a group:

$$\text{If } g^h = g^a \text{ then } (hg)^m = h^m g^{\mathcal{S}(a|m)}. \tag{2.1}$$

The following lemma collects some useful properties of the operator $\mathcal{S}\left(- \mid -\right)$ which will be used throughout.

Lemma 2.1. *Let $p, R, m \in N$ with p prime and suppose that $R \equiv 1 \mod p$.*

(1) Suppose that either $p \neq 2$ or $p = 2$ and $R \equiv 1 \mod 4$. Then
  - *(a) $v_p(R^m - 1) = v_p(R - 1) + v_p(m)$ and $v_p(\mathcal{S}\left(R \mid m\right)) = v_p(m)$.*
  - *(b) $o_{p^m}(R) = p^{\max(0,m-v_p(R-1))}$.*
  - *(c) If $a = v_p(R - 1) \leq m$ then $\langle R \rangle_{p^m} = \{[1 + yp^a]_{p^m} : 0 \leq y < p^{m-a}\}$.*

(2) Suppose that $R \equiv -1 \mod 4$. Then
  - *(a)* $v_2(R^m - 1) = \begin{cases} v_2(R+1) + v_2(m), & \text{if } 2 \mid m; \\ 1, & \text{otherwise}; \end{cases}$

    and $v_2(\mathcal{S}\left(R \mid m\right)) = \begin{cases} v_2(R+1) + v_2(m) - 1, & \text{if } 2 \mid m; \\ 0, & \text{otherwise}; \end{cases}$.
  - *(b)* $o_{2^m}(R) = \begin{cases} 1, & \text{if } m \leq 1; \\ 2^{\max(1,m-v_2(R+1))}, & \text{otherwise} \end{cases}$.
  - *(c)* $v_2(R^m + 1) = \begin{cases} v_2(R+1), & \text{if } 2 \nmid m; \\ 1, & \text{otherwise.} \end{cases}$.

Proof. (1a) The first equality can be easily proven by induction on m. Then the second follows from $R^m - 1 = (R - 1)\mathcal{S}\left(R \mid m\right)$.

(1b) is a direct consequence of (1a).

(1c) By (1a) we have $\langle R \rangle_{p^m} \subseteq \{[1 + yp^a]_{p^m} : 0 \leq y < p^{m-a}\}$ and by (1b) the first set has p^{m-a} elements. As the second one has the same cardinality, equality holds.

(2a) Suppose that $R \equiv -1 \mod 4$. If $2 \nmid m$ then $R^m \equiv -1 \mod 4$ and hence $v_2(R^m - 1) = 1$. As $R^2 \equiv 1 \mod 4$, if $2 \mid m$ then, by (1a) we have $v_2(R^m - 1) = v_2((R^2)^{\frac{m}{2}} - 1) = v_2(R^2 - 1) + v_2\left(\frac{m}{2}\right) = v_2(R+1) + v_2(m)$. This proves the first part of (2a). Then the second part follows from $R^m - 1 = (R - 1)\mathcal{S}\left(R \mid m\right)$.

(2b) follows easily from (2a).

(2c) Since R is odd, both $R^m - 1$ and $R^m + 1$ and are even and exactly one of $v_2(R^m - 1)$ and $v_2(R^m + 1)$ equals 1. Thus, from (2a) we deduce that if $2 \mid m$ then $v_2(R^m + 1) = 1$. Suppose otherwise that m is odd and greater than 2. Then $v_2(R^{m-1} - 1) = v_2(R + 1) + v_2(m - 1) > v_2(R + 1)$, so that $v_2(R^m + 1) = v_2(R(R^{m-1} - 1 + 1) + 1) = v_2(R + 1 + R(R^{m-1} - 1)) = v_2(R + 1)$.

□

The following lemma follows by straightforward arguments.

Lemma 2.2. *Let $m, n, s \in \mathbb{N}$, let T be a cyclic subgroup of $\mathcal{U}_m$, and denote $(r, \epsilon, o) = [T]$, $m' = [T, n, s]$ and $\Delta = \mathrm{Res}_{m'}(T)$.*

(1) *If* $T = \langle t \rangle_m$ *then* $|T| = o_m(t)$, $r_{2'} = \gcd(m_{2'}, t-1)$, $r_2 = \max(\gcd(m_2, t-1), \gcd(m_2, t+1)) = \gcd(m_2, t-\epsilon)$ *and* $o = o_{m_\nu}(t)_{\nu'}$ *with* $\nu = \pi(m) \setminus \pi(r)$.
(2) $r \mid m' \mid m$ *and* $\pi(m) = \pi(m')$.
(3) $[T] = [\Delta]$.
(4) *For every* $p \in \pi(r)$ *we have* $\mathrm{Res}_{m_p}(T_p) = \left\langle \epsilon^{p-1} + r_p \right\rangle_{m_p}$ *and*

$$|\mathrm{Res}_{m_p}(T_p)| = \begin{cases} 2, & \text{if } p = 2, \epsilon = -1 \text{ and } r_2 = m_2; \\ \frac{m_p}{r_p}, & \text{otherwise.} \end{cases}$$

(5) *If* $s \mid m$ *and* $T \subseteq \mathcal{U}_m^{n,s}$ *then* $m_{\pi(r)} \mid rn$, $m_{\pi(r)} \mid rs$, $o \mid n_{\pi(m)\setminus\pi(r)}$ *and if* $\epsilon = -1$ *then* $m_2 \in \{s_2, 2s_2\}$. *If moreover* $T = \langle t \rangle_m = \langle u \rangle_m$ *then there is a* $k \in \mathbb{N}$ *with* $\gcd(k, |T|) = 1$ *and* $a \mapsto a^k$, $b \mapsto b^k$ *defines an isomorphism* $\mathcal{G}_{m,n,s,t} \to \mathcal{G}_{m,n,s,u}$.

Definition 2.3. *Given* $m, n, s \in \mathbb{N}$ *with* $s \mid m$ *and a cyclic subgroup of* $\mathcal{U}_m$, *we say that* T *is* (n,s)-canonical *if* $T \subseteq \mathcal{U}_m^{n,s}$ *and if* $(r, \epsilon, o) = [T]$ *then the following conditions are satisfied:*

(Can–) *If* $\epsilon = -1$ *then* $s_2 \neq r_2 n_2$. *If moreover,* $m_2 \geq 8$, $n_2 \geq 4$, $o_2 < n_2$ *then* $r_2 \leq s_2$.
(Can+) *For every* $p \in \pi$ *with* $\epsilon^{p-1} = 1$ *we have* $s_p \mid n$ *and* $r_p \mid s$ *or* $s_p o_p \nmid n$.

3. Metacyclic factorizations

In this section G is a finite metacyclic group. Moreover we fix the following notation:

$$\begin{aligned} \pi &= \text{set of prime divisors of } |G| \text{ such that } G \text{ has a normal Hall } p'\text{-subgroup}, \\ \pi' &= \pi(|G|) \setminus \pi, \\ o_G &= |\mathrm{Inn}_G(G'_{\pi'})|_\pi. \end{aligned}$$

In our first lemma we show that π, π' and o_G are determined by any kernel of G.

Lemma 3.1. *Let* $G = AB$ *be a metacyclic factorization and let* $m = |A|$, $s = [G : A]$, $r = r_G(A)$ *and* $o = o_G(A)$. *Then*

(1) *For every set of primes* μ, $A_\mu B_\mu$ *is a Hall* μ*-subgroup of* G.
(2) $p \in \pi'$ *if and only if* $G' \setminus Z(G)$ *has an element of order* p *if and only if* $A \setminus Z(G)$ *has an element of order* p.
(3) $G'_{\pi'} = A_{\pi'}$ *and* $A_{\pi'} \cap B_{\pi'} = 1$.
(4) $\pi' = \pi(m) \setminus \pi(r)$, $s_{\pi'} = m_{\pi'}$ *and* $o = o_G$.
(5) $G = A_{\pi'} \rtimes \left(B_{\pi'} \times \prod_{p \in \pi} A_p B_p \right)$. *In particular* $[B_{p'}, A_p] = 1$ *for every* $p \in \pi$.

Proof. (1) As A is normal in G, $A_\mu B_\mu$ is a μ-subgroup of G and $A_{\mu'} B_{\mu'}$ is a μ'-subgroup of G. Moreover $G = AB = A_\mu B_\mu A_{\mu'} B_{\mu'}$ and hence $[G : A_\mu B_\mu] = |A_{\mu'} B_{\mu'}|$. Thus $A_\mu B_\mu$ is a Hall μ-subgroup of G.

(2) As G/A is abelian, $G' \subseteq A$. Let $p \in \pi(|G|)$. If $p \nmid m$ then $AB_{p'}$ is a normal Hall p'-subgroup of G and hence $p \in \pi$. Suppose otherwise that $p \mid m$ and let C be the unique subgroup of order p in A. Since C is normal in G, it follows that $G' \setminus Z(G)$ has an element of order p if and only if $A \setminus Z(G)$ has an element of order p if and only if $C \not\subseteq Z(G)$. Since $\mathrm{Aut}(C)$ is cyclic of order $p-1$, if $p \in \pi$ and N is a normal Hall p'-subgroup of G then $G = N \rtimes P$ with P a Sylow p-subgroup of G containing C and as $[P, C] = 1$ it follows that $[G, C] \subseteq [N, C] \subseteq N \cap C = 1$ and hence $C \subseteq Z(G)$. Conversely, if $C \subseteq Z(G)$ then $[A_p, A_{p'} B_{p'}] = 1$ because the kernel of the restriction homomorphism $\mathrm{Aut}(A_p) \to \mathrm{Aut}(C)$ is a p-group. As $A_{p'} B$ normalizes $A_{p'} B_{p'}$ it follows that the latter is a normal Hall p'-subgroup of G and hence $p \in \pi$.

(3) Let $p \in \pi'$, c an element of order p in A and a a generator of A. Since $|\mathrm{Aut}(\langle c \rangle)| = p-1$ and $c \notin Z(G)$, we have that $a_p^b = a_p^k$ for some integer k such that $\gcd(k, p) = 1$. Moreover, $k-1$ is coprime with p because $1 \neq [c, b] = c^{k-1}$. Then $A_p = \left\langle a_p^{k-1} \right\rangle \subseteq G'$ and hence $A_p = G'_p$. Moreover, if $g \in A_p \cap B_p \setminus \{1\}$ then $[g, B] = 1$ and $c \in \langle g \rangle$, yielding a contradiction. Thus $A_p \cap B_p = 1$. Since this is true for each $p \in \pi'$, we have $A_{\pi'} = G'_{\pi'}$ and $A_{\pi'} \cap B_{\pi'} = 1$.

(4) is a direct consequence of (2) and (3).

(5) By (1) and (3), $A_{\pi'} B_{\pi'} = A_{\pi'} \rtimes B_{\pi'}$ is the unique Hall π'-subgroup of G and hence $G = (A_{\pi'} \rtimes B'_{\pi'}) \rtimes (A_\pi B_\pi)$. Moreover, if $p \in \pi$ and c is an element of order p in A_p then $c \in Z(G)$ by (2). This implies that $[B_{p'}, A_p] = 1$ because the kernel of $\mathrm{Res}_p : \mathrm{Aut}(A_p) \to \mathrm{Aut}(\langle c \rangle)$ is a p-group. Then $[B_{\pi'}, A_\pi B_\pi] = 1$ and $A_\pi B_\pi = \prod_{p \in \pi} A_p B_p$. $\square$

Next lemma shows that ϵ_G is determined by any minimal kernel of G.

Lemma 3.2. *If A is a minimal kernel of G then $\epsilon_G = \epsilon_G(A)$.*

Proof. Let $m = m_G = |A|$, $\epsilon = \epsilon_G(A)$ and $r = r_G(A)$. If $m_2 \le 2$ then $\epsilon = 1 = \epsilon_G$. Otherwise $4 \mid r_2$ and

$$G'_2 = \begin{cases} \langle a^{r_2} \rangle, & \text{if } \epsilon = 1; \\ \langle a^2 \rangle, & \text{if } \epsilon = -1. \end{cases}$$

Then

$$|G'_2| = \begin{cases} \frac{m_2}{r_2}, & \text{if } \epsilon = 1; \\ \frac{m_2}{2}, & \text{if } \epsilon = -1; \end{cases}$$

and hence $\epsilon = -1$ if and only if $m_2 = 2|G'_2| > 2$ if and only if $\epsilon_G = -1$. □

Let

$$R_G = \{r_G(A) : A \text{ is a minimal kernel of } G\}.$$

Next lemma shows that $|R_G| \le 2$ and in most cases $|R_G| = 1$.

Lemma 3.3. *Let $m = m_G$, $n = n_G$ and $o = o_G$. Then the following statements are equivalent:*

(1) $|R_G| > 1$.
(2) $n_2 \ge 4$, $m_2 \ge 8$, $\epsilon_G = -1$, $o_2 < n_2$ and $R_G = \{\frac{r}{2}, r\}$ for some r with $r_2 = m_2$.
(3) $n_2 \ge 4$, $m_2 \ge 8$, $\epsilon_G = -1$, $o_2 < n_2$, $r_2 \in \{\frac{m_2}{2}, m_2\}$ for some $r \in R_G$ and $[G : B]_2 = \frac{m_2}{2}$ for some metacyclic factorization $G = AB$ with $m = |A|$.
(4) $n_2 \ge 4$, $m_2 \ge 8$, $\epsilon_G = -1$, $o_2 < n_2$, $r_2 \in \{\frac{m_2}{2}, m_2\}$ for some $r \in R_G$ and $[G : B]_2 = \frac{m_2}{2}$ for every metacyclic factorization $G = AB$ with $m = |A|$.

Furthermore, suppose that $G = AB$ is a metacyclic factorization satisfying the conditions of (3) *and let a be a generator of A and b be a generator of B and $s = [G : B]$. Let $C = \left\langle b^{\frac{nm_{2'}}{2s_{2'}}} a \right\rangle$. Then $G = CB$ is another metacyclic factorization with $|C| = m$ and $r_G(C) \ne r_G(A)$.*

Proof. Let $\epsilon = \epsilon_G$, $o = o_G$, $R = R_G$ and for every $p \in \pi$ let $R_p = \{r_p : r \in R\}$. Fix a minimal kernel A of G and let $r = r_G(A)$.

Let $p \in \pi$. If $\epsilon^{p-1} = 1$ then $|G'_p| = \frac{m_p}{r_p}$. Thus in this case $|R_p| = 1$. Therefore $r_{2'}$ is constant for every $r \in R$ and hence $|R| = |R_2|$. Moreover, if $\epsilon = 1$ then $G'_2 = \frac{m_2}{r_2}$ and hence $R_2 = \{\frac{m_2}{|G'_2|}\}$. In this case none of the conditions (1)-(4) hold. Otherwise, $4 \mid r_G(A)_2 \mid m_2$. Thus, if $m_2 < 8$ then $r_G(A)_2 = 4$ for every minimal kernel A of G and hence $|R| = |R_2| = 1$, so that again none of the conditions (1)-(4) hold. Thus in the remainder of the proof we assume that $\epsilon = -1$ and $8 \le m_2$. Then $G'_2 = A^2$ and hence $\langle -1 + r_G(A)_2 \rangle_{\frac{m_2}{2}} = \mathrm{Res}_{\frac{m_2}{2}}(\mathrm{T}_G(A)) = \sigma_{G'_2}^{-1}(\mathrm{Inn}_G(G'_2))$, which is independent of A. This shows that if R_2 contains an element smaller than $\frac{m_2}{2}$ then it only has one element and hence again none of the conditions (1)-(4) hold. So in the remainder of the proof we assume that $R_2 \subseteq \{\frac{m_2}{2}, m_2\}$.

Suppose that $o_2 = n_2$. Then, by Lemma 3.1.(4), $C_G(G'_{\pi'})_2 = A_2$, and hence $\langle -1 + r_G(A)_2 \rangle_{m_2} = \mathrm{Res}_{m_2}(T_G(C_G(G'_{\pi'})_2))$ is independent of A. Therefore, in this case $|R_2| = 1$, so that $|R| = 1$. So again in this case none of the conditions (1)-(4) hold and in the remainder of the proof we also assume that $o_2 < n_2$.

Suppose that $n_2 < 4$. Then none of the condition (2)-(4) holds and as $\epsilon = -1$, we have $n_2 = 2$. By means of contradiction suppose that (1) holds. By the previous paragraph $R_2 = \{\frac{m_2}{2}, m_2\}$ and hence G has two minimal kernels A and C with $r_G(A)_2 = m_2$ and $r_G(C)_2 = \frac{m_2}{2}$. If $G = AB$ and $G = CD$ are metacyclic factorization of G then A_2B_2 and C_2D_2 are Sylow 2-subgroups of G and hence they are isomorphic. However, by Lemma 2.2.(5), $[A_2B_2 : B_2]$ is either m_2 or $\frac{m_2}{2}$. In the first case A_2B_2 is dihedral and in the second case A_2B_2 is quaternionic. This yields a contradiction because from $r_G(C)_2 = \frac{m_2}{2}$ it follows that C_2D_2 is neither dihedral nor quaternionic.

Thus in the remainder we assume that $m_2 \ge 8$, $n_2 \ge 4$, $o_2 < n_2$, $\epsilon = -1$ and $R_2 \subseteq \{\frac{m_2}{2}, m_2\}$. Moreover, by the above arguments we have that $R \subseteq \{\frac{r}{2}, r\}$ for some r with $r_2 = m_2$. Thus (1) and (2) are equivalent.

(4) implies (3) is clear.

(3) implies (2). Let $G = AB$ be a metacyclic factorization of G satisfying the conditions of (3). Let $s = [G : B]$ and $r = r_G(A)$. Select generators a of A and b of B and let $z = b^{\frac{nm_{2'}}{2s_{2'}}}$, $c = za$ and $C = \langle c \rangle$. We will prove that if $G = CB$ is another metacyclic factorization with $|C| = m$ and $r_G(C) \ne r$, so that (2) holds.

Indeed, since $o_2 < n_2$, we have $[z, a_{\pi'}] = 1$. Moreover, $[z_{p'}, a_p] = 1$ for every $p \in \pi$. If moreover, $p \neq 2$ then $[z_p, a_p] = 1$ because $[b^n, a] = 1$. Finally, $r_2 \in \{\frac{m_2}{2}, m_2\}$ and hence $o_{m_2}(-1+r_2) = 2$. As $4 \mid n$ and $a_2^{b_2} = a_2^{-1+r_2}$ it follows that $[z_2, a_2] = 1$. This shows that $z \in Z(G)$. As $s = [G : B]$ and $[G : A] = n$ we have $b^n = a^{sx}$ for some integer x coprime with m. Then $c^2 = a^{2+sx\frac{m_{2'}}{s_{2'}}} = a^{2+xs_2m_{2'}} = a^{2+x\frac{m}{2}} = a^{2+\frac{m}{2}}$. As $8 \mid m$ it follows that $|C| = m$. Suppose that $a^b = a^t$. Then $t+1 \equiv r_2 \mod m_2$. Let $r' \in \mathbb{N}$ with $r'_{2'} = r_{2'}$ and $\{r_2, r'_2\} = \{\frac{m_2}{2}, m_2\}$ and let t' be an integer such that $t' \equiv t \mod m_{2'}$ and $t' \equiv -1 + r'_2 \mod m_2$. As $8 \mid m$ we have $t' \equiv t \equiv -1 \mod 4$ and hence $t' = 1 + 2y$ for some odd integer y. Then $c^{t'} = zz^{t'-1}a^{t'} = zz^{2y}a^{t'} = za^{t'+y\frac{m}{2}}$. Moreover, $t' + y\frac{m}{2} \equiv t' \equiv t \mod m_{2'}$ and $t' + y\frac{m}{2} \equiv -1 + r'_2 + \frac{m_2}{2} \equiv -1 + r_2 \equiv t \mod m_2$. Therefore $c^{t'} = za^t = c^b$. This shows that C is a cyclic normal subgroup of G and clearly $G = CB$ is a metacyclic factorization satisfying the desired condition.

Before proving (1) implies (4) we prove that if $G = AB = CD$ are metacyclic factorizations with $|A| = |B| = m$ then $[G : B]_2 = [G : D]_2$. The assumption $\epsilon = -1$ implies that $G'_2 = A^2 = C^2$. As A_2B_2 and C_2D_2 are Sylow 2-groups of G we may assume that they are equal and hence if $A_2 = \langle a\rangle$ and $B = \langle b\rangle$ we may write $c = b^ia^j$ and $d = b^ka^l$. Since $c^2 \in C^2 = A^2$ we have $\frac{n_2}{2} \mid i$ and as $4 \mid n$, necessarily $2 \mid i$ and hence $2 \nmid k$. Then, using that $r_G(A), r_G(C) \in \{\frac{m_2}{2}, m_2\}$ we have that $d^2 = b^{2k}$ or $d^2 = b^{2k}a^{l\frac{m_2}{2}}$. In both cases $d^4 = b^4$ and hence $D^4 = B^4$. As $4 \mid n$ it follows that $A_2 \cap B_2 = B_2^{n_2} = D_2^{n_2} = C_2 \cap D_2$. Therefore, $[G : B]_2 = [A_2B_2 : B_2] = [A_2, A_2 \cap B_2] = [C_2 : C_2 \cap D_2] = [G, D]_2$, as desired.

(1) implies (4). Suppose that $|R| > 1$. By the assumptions and the previous arguments we know that the only condition from (4) which is not clear is that if $G = AB$ is a metacyclic factorization with $m = |A|$ and $s = [G : B]$ then $s_2 = \frac{m_2}{2}$. So suppose that $s_2 = m_2$. Since $|R| > 1$, there is a second metacyclic factorization $G = CD$ with $|C| = m$ and $\{r_G(A)_2, r_G(C)_2\} = \{\frac{m_2}{2}, m_2\}$. By the previous paragraph $[G : D]_2 = [G : B]_2 = 1$. By symmetry we may assume that $r_G(A)_2 = m_2$ and $r_G(C) = \frac{m_2}{2}$. As above we may assume that $A_2B_2 = C_2D_2$ and if $A_2 = \langle a\rangle$, $B_2 = \langle b\rangle$, $C_2 = \langle c\rangle$ and $D_2 = \langle d\rangle$ then $a^b = a^{-1}$, $c^d = c^{-1+\frac{m_2}{2}}$, $G'_2 = A_2^2 = C_2^2$, $A_2 \neq C_2$ and $A_2 \cap B_2 = C_2 \cap D_2 = 1$. Write $c = b^ia^j$ and $d = b^ka^l$ with $i, j, k, l \in \mathbb{N}$. Since $c^2 \in A$ we have that $\frac{n_2}{2} \mid i$ and as $4 \mid n_2$, we have that k is odd and $[b^i, a] = 1$. Thus $b^{2i} = c^2a^{-2j} \in A_2 \cap B_2 = 1$. Then $c^2 = a^{2j}$ and as $C^2 = A^2$, necessarily j is odd. However, from $b^{2i} = 1$, $[b^i, a] = 1$ and $8 \mid m$ we have $b_2^ia_2^{(-1+\frac{m_2}{2})j} = b_2^{(-1+\frac{m_2}{2})i}a_2^{(-1+\frac{m_2}{2})j} = c_2^{-1+\frac{m_2}{2}} = c_2^d = b_2^ia_2^{-j}$ and hence $2 \mid j$, a contradiction. □

In our next result we show a way to decide if a factorization of G is minimal and we prove that the following algorithm transforms a metacyclic factorization of G into a minimal one.

Algorithm 1. INPUT: *A metacyclic factorization $G = AB$ of a finite group G.*
OUTPUT: *$a, b \in G$ with $G = \langle a\rangle \langle b\rangle$ a minimal metacyclic factorization of G.*

(1) $m := |A|$, $n := [G : A]$, $s := [G : B]$,
(2) $a :=$ *some generator of* A, $b :=$ *some generator of* B, *and* $y \in \mathbb{N}$ *with* $b^n = a^y$.
(3) $r := r_G(A)$, $\epsilon := \epsilon_G(A)$ *and* $o = o_G(A)$.
(4) *for* $p \in \pi(r)$ *with* $\epsilon^{p-1} = 1$
 (a) *if* $s_p \nmid n$ *then* $b := ba_p$ *and* $s := s_{p'}n_p$.
 (b) *if* $r_p \nmid s$, $s_po_p \mid n$ *and* $t \in \mathbb{N}$ *satisfy* $a_p^{b_p} = a_p^t$, *compute* $x \in \mathbb{N}$ *satisfying* $x\mathcal{S}\left(t^{\frac{n}{s_p}} \mid s_p\right) \equiv r - y \mod m_p$ *and set* $a := b_p^{\frac{n}{s_p}}a_{p'}a_p^x$, $m := s_p\frac{m}{r_p}$, $n := n\frac{r_p}{s_p}$, *and*

$$(r, \epsilon) := \begin{cases} (4r_{2'}, -1), & \text{if } 8 \mid m, s_p = 2, \text{ and } r_2 = \frac{m_2}{2}; \\ (r_{p'}s_p, 1), & \text{otherwise.} \end{cases}$$

(5) *If* $\epsilon = -1$, $4 \mid n$, $8 \mid m$, $o_2 < n_2$ *and* $r_2 \nmid s$ *then* $a := b^{\frac{m_{2'}n}{2s_{2'}}}a$ *and* $r := r_{2'}s_2$
(6) *If* $\epsilon = -1$ *and* $s_2 = r_2n_2$ *then* $b := ba_2$ *and* $s := \frac{s}{2}$.
(7) *Return* (a, b).

Proposition 3.4. *Let $G = AB$ be a metacyclic factorization and let $m = |A|$, $n = [G : A]$, $s = [G : B]$ and $T = T_G(A)$. Then $G = AB$ is minimal as metacyclic factorization of G if and only if T is (n, s)-canonical.*

Furthermore, if the input of Algorithm 1 is a metacyclic factorization of G and its output is (a, b) then $G = \langle a\rangle \langle b\rangle$ is a minimal metacyclic factorization of G.

Proof. Let $(r,\epsilon,o)=[T_G(A)]$. By Lemma 3.1, $\pi'=\pi(m)\setminus\pi(r)$. Fix $y,t\in\mathbb{N}$ with $b^n=a^y$ and $a^b=a^t$. Then $s=\gcd(t,m)$, $\gcd(t,m)=1$, $r_{2'}=\gcd(m_{2'},t-1)$ and $r_2=\gcd(m_2,t-\epsilon)$. For every prime p let $G_p=A_pB_p$.

Claim 1. If condition (Can+) holds then A is a minimal kernel of G.

Suppose that condition (Can+) holds and let C be kernel of G. We want to prove that $|C|\ge m$ and for that it is enough to show that $|C_p|\ge m_p$ for every prime p. This is obvious if $m_p=1$, and it is a consequence of Lemma 3.1.(3), if $p\in\pi'$. So we suppose that $p\in\pi$ and $m_p\ne 1$. Hence $p\mid r$.

Suppose first that $\epsilon^{p-1}=-1$. Then $p=2$ and $A_2^2=G_2'\subseteq C_2$. However $C_2\not\subseteq A_2^2$ because G_2/A_2^2 is not cyclic. Therefore $|C_2|\ge 2|A_2^2|=m_2$.

Suppose otherwise that $\epsilon^{p-1}=1$. Then $G_p'=A_p^{r_p}$ and $|G'{}_p|=\frac{m_p}{r_p}$. Assume that $r_p\mid s_p$. Then $G_p/G_p'=(A_p/G_p')\times(B_pG'{}_p/G'{}_p)$ and $r_p=|A_p/G'{}_p|\le n_p=[B_pG'{}_p:G'{}_p]$. As $(G_p/G'{}_p)/(C_p/G'{}_p)\cong G_p/C_p$ is cyclic, necessarily $r_p\mid[C_p:G'{}_p]$ and hence $m_p\mid|C_p|$, as desired. Assume otherwise that $r_p\nmid s_p$. By condition (Can+) we have $s_p\mid n_p$ and $s_po_p\nmid n_p$. In particular $p\mid o_p$. By Lemma 3.1.(3), $C_{\pi'}=A_{\pi'}$ and thence $C_p\subseteq C_{G_p}(A_{\pi'})_p=A_pB_p^{o_p}$. Using again that G_p/C_p is cyclic and $p\mid o_p$, we must have $C_p=\left\langle b_p^xa_p\right\rangle$ for $x\in\mathbb{N}$ with $o_p\mid x$ and $x\le n$. Let $R\in\mathbb{N}$ such that $a_p^{b_p^x}=a_p^R$. Then R satisfies the hypothesis of Lemma 2.1.(2c) and hence $v_p\left(\mathcal{S}\left(R\mid\frac{n}{x_p}\right)\right)=v_p(n)-v_p(x)\le v_p(n)-v_p(o)<v_p(s)=v_p(yx_{p'})$ and therefore $v_p\left(yx_{p'}+\mathcal{S}\left(R\mid\frac{n}{x_p}\right)\right)=v_p(n)-v_p(x)$. Then $|C_p|=\frac{n_p}{x_p}|(b_p^xa_p)^{\frac{n_p}{x_p}}|=\frac{n_p}{x_p}\left|a_p^{yx_{p'}+\mathcal{S}\left(R\mid\frac{n_p}{x_p}\right)}\right|=m_p$. This finishes the proof of Claim 1.

Claim 2. If $T_G(A)$ is (n,s)-canonical then for every metacyclic factorization $G=CD$ with $|C|=m$ one has $r_G(C)\ge r$ and $|D|\le|B|$.

If $r_G(C)<r$ then, by Lemma 3.3, $m_2\ge 8$, $n_2\ge 4$, $\epsilon=-1$, $o_2<n_2$, $r_G(C)_2=\frac{m_2}{2}=s_2$ and $r_2=m_2$, in contradiction with the second part of condition (Can–). Thus $r_G(C)\ge r$.

To prove that $|D|\le|B|$ we show that $|D_p|\le|B_p|$ for each prime p. This is clear if $p\nmid m$ and a consequence of Lemma 3.1.(4) if $p\in\pi'$. Otherwise $p\mid r$. Since both G_p and C_pB_p are Sylow p-subgroups of G we may assume that $G_p=C_pD_p$.

Assume first that $\epsilon^{p-1}=1$. Then by assumption $s_p\mid n_p$. Let $d=b_p^xa_p^y$ be a generator of D_p and let $R\in\mathbb{N}$ such that $a_p^{b_p^x}=a_p^R$. The assumption $\epsilon^{p-1}=1$ implies that R satisfies the hypothesis of Lemma 2.1.(1a) and hence $m_p\mid\mathcal{S}\left(R\mid m_p\frac{n_p}{s_p}\right)$ and from (2.1) we deduce that $d^{\frac{m_pn_p}{s_p}}=a_p^{y\mathcal{S}\left((1+r_p)^x\mid m_p\frac{n_p}{s_p}\right)}=1$ and hence $|D_p|\le\frac{m_pn_p}{s_p}=|b_p|$. Suppose otherwise that $\epsilon^{p-1}=-1$, i.e. $p=2$ and $\epsilon=-1$. Then $C_2^2=G'{}_2=A_2$ and $C_2\cap D_2\subseteq Z(G_2)\cap C_2=Z(G_2)\cap C_2^2=Z(G_2)A=A^{\frac{m_2}{2}}$ and hence $|C_2\cap D_2|\le 2$. Thus $|D_2|=[D_2:C_2\cap D_2]\,|C_2\cap D_2|=[G_2:C_2]\,|C_2\cap D_2|\in\{n_2,2n_2\}$. Similarly, $|B_2|\in\{n_2,2n_2\}$. If $|B_2|=2n_2$ then $|D_2|$ divides $|B_2|$ as desired. Suppose otherwise that $|B_2|=n_2$. Then $m_2=s_2$ and hence m_2 divides $\frac{r_2n_2}{2}$, by the hypothesis (Can–) and Lemma 2.2.(5). If $D_2\subseteq\left\langle a,b_2^2\right\rangle$ then $C_2=\left\langle b_2a_2^x\right\rangle$ for some integer x and hence $n_2=2$ because $C_2^2=\left\langle a_2^2\right\rangle$. Then $D_2\subseteq\langle a_2\rangle$ so that D_2 is normal in G_2 and hence $\left\langle a_2^2\right\rangle=C_2^2=[D_2,C_2]\subseteq C_2\cap D_2\subseteq\left\langle a_2^{\frac{m_2}{2}}\right\rangle\subseteq\left\langle a_2^2\right\rangle$. Then $m_2=4$ and G_2 is dihedral of order 8. Then every metacyclic factorization of G_2 is of the form $\langle a_2\rangle\langle c\rangle$ with $|c|=2$. Thus $|D_2|=2=|b_2|$, as wanted. Assume otherwise that $D_2\not\subseteq\left\langle a_2,b_2^2\right\rangle$. Then $D_2=\langle b_2a_2^x\rangle$ for some integer x and let $R\in\mathbb{N}$ such that $a_2^{b_2}=a_2^R$. The hypothesis $\epsilon=-1$ implies that R satisfies the hypothesis of Lemma 2.1.(2a). Since m_2 divides $\frac{r_2n_2}{2}$, we get $v_2(\mathcal{S}(R\mid n_2))=v_2(r_2)+v_2(n_2)-1\ge v_2(m_2)$ and hence $(b_2a_2^x)^{n_2}=a_2^{x\mathcal{S}(-1+r_2\mid n_2)}=1$. Then $|D_2|=n_2$, as desired. This finishes the proof of Claim 2.

The necessary part in the first statement of the proposition follows from claims 1 and 2.

Claim 3. If $p\mid r$, $\epsilon^{p-1}=1$ and $s_p\nmid n_p$ then $[G:ba_p]=s_{p'}n_p<s$.

First of all $n=|ba_pA|$ and hence n divides $|ba_p|$. Using (2.1) we have $(ba_p)^n=a_{p'}^ya_p^{y+\mathcal{S}(t\mid n)}$ and $v_p([G:\langle ba_p\rangle])=v_p(\mathcal{S}(t\mid n))=v_p(n)<v_p(s)=v_p(y)$, by Lemma 2.1.(1a) and the assumption. Thus $|ba_p|=n\frac{m}{s_{p'}n_p}$ and hence $[G:ba_p]=s_{p'}n_p$. This finishes the proof of Claim 3.

By Claim 3, if the first part of (Can+) fails then $G = AB$ is not minimal because $G = A\langle ba_p\rangle$ is a factorization with $[G : b] > [G : \langle ba_p\rangle]$. Moreover, the factorization $G = A\langle ba_p\rangle$ satisfies the first part of condition (Can+) and hence after step (4a) of Algorithm 1, the factorization $G = \langle a\rangle\langle b\rangle$ satisfies the first part of (Can+) for the prime p.

Claim 4. Suppose that $p \mid r$, $\epsilon^{p-1} = 1$, $s_p \mid n$, $r_p \nmid s$ and $s_p o_p \mid n$. Let $R \in \mathbb{N}$ with $a_p^{b_p^{\frac{n}{s_p}}} = a^R$. Then there is an integer x such that $r - y \equiv x\mathcal{S}(R \mid s_p) \mod m_p$. This justify the existence of x in step (4) of Algorithm 1. Let $c = b_p^{\frac{n}{s_p}} a_{p'} a_p^x$ and $C = \langle c\rangle$. Then $G = CB$ is a metacyclic factorization of G with $|C| = m\frac{s_p}{r_p} < |A|$. Moreover,

$$(r_G(C), \epsilon_G(C)) := \begin{cases} (4r_{2'}, -1), & \text{if } 8 \mid m, s_p = 2, \text{ and } r_2 = \frac{m_2}{2}; \\ (r_{p'}s_p, 1), & \text{otherwise.} \end{cases}$$

The assumption $s_p o_p \mid n_p$ implies that $o_p \mid \frac{n}{s_p}$ and hence $[b_p^{\frac{n}{s_p}}, a_{\pi'}] = 1$. As also $[b_p, a_{\pi\setminus\{p\}}] = 1$ we deduce that $[b_p^{\frac{n}{s_p}}, a_{p'}] = 1$. On the other hand, since $r_p \nmid s_p$, $v_p(y) = v_p(s) < v_p(r)$ and therefore $v_p(r - y) = v_p(s) = v_p(\mathcal{S}(t \mid s_p))$, by Lemma 2.1.(1a). Therefore there is an integer x coprime with p such that $r - y \equiv x\mathcal{S}(R \mid s_p) \mod m_p$. Using (2.1) we have $c^{s_p} = b_p^n a_{p'}^{s_p} a_p^{x\mathcal{S}(R|s_p)} = a_{p'}^{s_p} a_p^{y+x\mathcal{S}(R|s_p)} = a_{p'}^{s_p} a_p^r$. Then $G'_{p'} \subseteq \langle a_{p'}\rangle \subseteq C$ and $G'_p = \langle a_p^r\rangle \subseteq C$. Thus $G' \subseteq C$ and hence $G = CB$ is a metacyclic factorization of G with $|C| = s_p|a_{p'}||a_p^r| = m\frac{s_p}{r_p} < m = |A|$. As $C_{p'} = A_{p'}$, we have $r_G(C)_{p'} = r_G(A)_{p'} = r_{\pi'}$. If $\epsilon_G(C)^{p-1} = 1$ then $\frac{m_p}{r_p} = |G'_p| = \frac{|C_p|}{r_G(C)_p} = \frac{m_p s_p}{r_p r_G(C)_p}$ and hence in this case $r_G(C) = r_{p'}s_p$. Otherwise, i.e. if $p = 2$ and $\epsilon_G(C) = -1$ then $2|C_2| \le s_2 \le |C_2|$ and $4 \le r_G(C)_2 \le |C_2| = \frac{m_2 s_2}{r_2} = 2|G'_2| = \frac{2m_2}{r_2}$ and hence $s_2 = 2$, $|C_2| = 4 = r_G(C)_2$ and $r_2 = \frac{m_2}{2}$. Conversely, if $s_2 = 2$ and $r_2 = \frac{m_2}{2}$ then $|C_2| = 4$ and hence $r_G(C)_2 = 4$. Moreover, as G_2 is not commutative then $\epsilon_G(C) = -1$. This finishes the proof of Claim 4.

Claim 4 shows that if the first part of (Can+) holds but the second one fails then $G = AB$ is not minimal. It furthermore the parameters associated to the factorization $G = CB$, i.e. $|C|, [G : C], [G : B], r_G(C), \epsilon_G(C), o_G(C)$, satisfy condition (Can+) for the prime p and hence, after step (4b) of Algorithm 1, the current factorization $G = \langle a\rangle\langle b\rangle$ satisfies this condition. Moreover, if $\epsilon_G(C) = 1$ then $r_p(C) = s_p \le n_p$ and condition (C+) holds for the prime p. Thus when the algorithm finishes the loop in step (4), the metacyclic factorization satisfies condition (Can+) and hence the current value of $\langle a\rangle$ is a minimal kernel of G by Claim 1.

Observe that the modification of a and b in steps (4a) and (4b) for some prime p does not affect the subsequent calculations inside the loop. Indeed, suppose that p and q are two different divisors of r with $\epsilon^{p-1} = \epsilon^{q-1} = 1$, and the prime p has been considered before the prime q in step (4). This has affected a and b which have been transformed by first transforming b into $d = ba_p$ and then transforming a into $c = d_p a_{p'} a_p^x = b_p a_{p'} a_p^{1+x}$. In principal we should recalculate the natural number y computed in step (2) to a new y'. However, as $p \in \pi$, $[b_{p'}, a_p] = [b_{q'}, a_p] = 1$ and hence $a_{p'} = c_{p'}$ and $b_{p'} = d_{p'}$. Therefore $d_q = c_q^y$ and hence $y' \equiv y \mod m_q$. Therefore when in step (4b) for the prime q we compute x satisfying if $r - y \equiv x\mathcal{S}(R \mid s_q) \equiv \mod m_q$ we also have $r - y' \equiv x\mathcal{S}(R \mid s_q) \mod m_q$.

By Lemma 3.3, if the second part of condition (Can–) is satisfied then $r_G(A) = r_G$. Otherwise, $r_G(A) > r_G$, and hence the factorization $G = AB$ is not minimal, However, after step (5) the factorization $G = \langle a\rangle\langle b\rangle$ satisfy both $|a| = m_G$ and $r_G(\langle a\rangle) = r_G$. In the remainder of the algorithm the kernel $\langle a\rangle$ is not modified and hence this is going to be valid in the remainder of the algorithm.

Finally suppose that the first part of (Can–) fails, so that $p = 2$, $\epsilon = -1$ and $s_2 = r_2 n_2$. Then $4 \mid r$ and $\langle t\rangle_{m_2} = \langle -1 + r_2\rangle_{m_2}$. Moreover, by Lemma 2.2.(5), we have that $s_2 \in \{\frac{m_2}{2}, m_2\}$ and $m_2 \mid r_2 n_2$. Therefore $s_2 = m_2 = r_2 n_2$. Then $v_2(\mathcal{S}(t \mid n_2)) = v_2(r) + v_2(n) - 1 = v_2(m) - 1$, by Lemma 2.1.(2a). As in the proof of Claim 3, we use the metacyclic factorization of $G = A\langle ba_2\rangle$. If $G = AB$ is minimal then we have $n|(ba_2)^n| = |ba_2| \le |b| = n|a^s| = n\frac{m}{s}$. Therefore $|(ba_2)^n| \le \frac{m}{s}$. Using (2.1) once more and $[b_{2'}, a_2] = 1$, we obtain $(ba_2)^n = a^y a_2^{\mathcal{S}(t|n_2)} = a_{2'}^y a_2^{\frac{m_2}{2}}$. Thus $|(ba_2)^n| = 2\frac{m}{s}$ and hence $|ba_2| = 2\frac{ms}{s} = 2|B|$, contradicting the minimality. Thus $G = AB$ is not minimal. Moreover, the new metacyclic factorization satisfies (Can–) because, $|ba_2|_2 = 2|b|_2$ and hence if $s' = [G : \langle ba_2\rangle]$ then $s'_2 = \frac{m_2}{2} \neq m_2 = r_2 n_2$. □

In order to prove that the last entry of MCINV(G) is well defined and prove Theorem A we need one more lemma which is inspired in Lemmas 5.5 and 5.7 of [Hem00].

Lemma 3.5. *Let p be a prime and consider the group $P=\mathcal{G}_{m,n,s,\epsilon+r}$ with m and n powers of p, r and s divisors of m and $\epsilon\in\{1,-1\}$ satisfying the following conditions: $p\mid r$, $m\mid rn$, if $4\mid m$ then $4\mid r$, if $\epsilon=1$ then $m\mid rs$ and if $\epsilon=-1$ then $2\mid n$, $4\mid m$ and $m\mid 2s$. Let o be a divisor of n and $N=\langle a,b^o\rangle$. Denote*

$$w=\begin{cases}\min(o,\frac{m}{r},\max(1,\frac{s}{r},\frac{so}{n})), & \text{if } \epsilon=1;\\ 1, & \text{if } \epsilon=-1 \text{ and }, o\mid 2 \text{ or } m\mid 2r;\\ \frac{m}{2r}, & \text{if } \epsilon=-1, 4\mid o<n, 4r\mid m, \text{ and if } s\neq nr \text{ then } 2s=m<nr;\\ \frac{m}{r}, & \text{otherwise.}\end{cases}$$

If y is an integer coprime with p then the following conditions are equivalent:

(1) There are $c\in N$ and $d\in b^yN$ such that $P=\langle c,d\rangle$, $|c|=m$, $d^n=c^s$ and $c^d=c^{\epsilon+r}$.

(2) $y\equiv 1 \mod w$.

Proof. Observe that N is the unique subgroup of G of index o containing a. We will make a wide use of (2.1) and Lemma 2.1, sometimes without specific mention. We consider separately the cases $\epsilon=1$ and $\epsilon=-1$.

Case 1. Suppose $\epsilon=1$.

(1) implies (2). Suppose that c and d satisfy the conditions of (1). If $w=1$ then obviously (2) holds. So we may assume that $w\neq 1$ and in particular $p\mid o$ and $pr\mid m$. The first implies that $N\subseteq\langle a,b^p\rangle$ and the second that $P/\langle a^p,b^p\rangle$ is not cyclic. Therefore $c\notin\langle a^p,b^p\rangle$ and hence $\langle c\rangle=\langle b^{xv}a\rangle$ with $o\mid v\mid n$ and $p\nmid x$. Write $d=b^{y_1}a^z$ with $y_1,z\in\mathbb{Z}$. From the assumption $d\in b^yN$ we have that $y_1\equiv y \mod o$ and hence $y\equiv y_1 \mod w$. Therefore, it suffices to prove that $y_1\equiv 1 \mod w$. From $c^d=c^{1+r}$ we have

$$b^{xv}a^{z(1-(1+r)^{xv})+(1+r)^{y_1}}=(b^{xv}a)^{b^{y_1}a^z}=(b^{xv}a)^{1+r}=b^{xv}ab^{xvr}a^{\mathcal{S}((1+r)^{xv}|r)}.$$

Then $n\mid vr$ and $b^{xvr}=a^{xs\frac{vr}{n}}$. Thus

$$z(1-(1+r)^{xv})+(1+r)^{y_1}-1\equiv xs\frac{vr}{n}+\mathcal{S}\left((1+r)^{xv}\mid r\right) \mod m.$$

This implies that that r divides $xs\frac{vr}{n}$, since r divides m. As r is coprime with x, it follows that n divides sv. Moreover, $(1+r)^{xv}\equiv 1 \mod rv$, by Lemma 2.1.(1a), and hence $\mathcal{S}\left((1+r)^{xv}\mid r\right)\equiv r \mod rv$. As r,v,m and s are powers of p we deduce that

$$(1+r)^{y_1}\equiv 1+r \mod \min(m,rv,\frac{svr}{n}).$$

Using Lemma 2.1.(1b) it follows that $y_1\equiv 1 \mod \min(\frac{m}{r},v,\frac{sv}{n})$.

Suppose that $y_1\not\equiv 1 \mod w$. Then

$$\min\left(\frac{m}{r},o,\frac{so}{n}\right)\le\min\left(\frac{m}{r},v,\frac{sv}{n}\right)<w=\min\left(\frac{m}{r},o,\max\left(1,\frac{s}{r},\frac{so}{n}\right)\right)$$

and hence $\frac{s}{r}>\left(1,\frac{so}{n}\right)$ and $\frac{m}{r}\ge w=\min\left(o,\frac{s}{r}\right)>\min\left(\frac{m}{r},v,\frac{sv}{n}\right)$. Thus

$$\frac{s}{r}\ge w=\min\left(o,\frac{s}{r}\right)>\min\left(v,\frac{sv}{n}\right)\ge\min\left(o,\frac{so}{n}\right).$$

Since $n\mid vr$ it follows that $\min(v,\frac{sv}{n})<\frac{s}{r}\le\frac{sv}{n}$ and hence $o\le v=\min(v,\frac{vs}{n})<\min(o,\frac{s}{r})$, a contradiction.

(2) implies (1). We now suppose that $y\equiv 1 \mod w$ and we have to show that there is $c\in N$ and $d\in b^yN$ satisfying the conditions in (1). If $y\equiv 1 \mod o$ then $bN=b^yN$ and hence $c=a$ and $d=b$ satisfy the desired condition. If $(1+r)^y\equiv 1+r \mod m$ then $a^{b^y}=a^{1+r}$ and hence $c=a^y$ and b^y satisfy the desired conditions. So we suppose that $y\not\equiv 1 \mod o$ and $(1+r)^y\not\equiv 1+r \mod m$. The first implies that $w<o$ and the second that $y-1$ is not multiple of $o_m(1+r)=\frac{m}{r}$, by Lemma 2.1.(1b) and hence $w<\frac{m}{r}$. Thus $w=\max(1,\frac{s}{r},\frac{os}{n})<\min(o,\frac{m}{r})$.

By Lemma 2.1.(1b) we have $(1+r)^y=1+r(1+xu)$ with $p\nmid x$, u a power of p and $v_p(w)\le v_p(u)=v_p(y-1)<v_p(\frac{m}{r})\le v_p(s)$. Moreover, if $u=1$ then $p\nmid 1+x$. Let $c_1=b^{x\frac{nu}{s}}a$. We now prove that $|c_1|=m$. Observe that $\frac{nu}{s}\ge\frac{nw}{s}\ge o$. Therefore $c_1\in N$. Moreover, as $v_p(u)<v_p(s)$ it follows that $|c_1\langle a\rangle|=\frac{s}{u}$ and $c_1^{\frac{s}{u}}=a^{xs+\mathcal{S}\left((1+r)^{x\frac{nu}{s}}\mid\frac{s}{u}\right)}$. If $u\neq 1$ then $v_p(r)\ge v_p(\frac{s}{w})\ge v_p(\frac{s}{u})=v_p(\mathcal{S}\left((1+r)^{x\frac{nu}{s}}\mid\frac{s}{u}\right))=v_p(xs+\mathcal{S}\left((1+r)^{x\frac{nu}{s}}\mid\frac{s}{u}\right))$ and therefore $G'=\langle a^r\rangle\subseteq\langle c_1\rangle$ and $|c_1|=m$, as desired. Otherwise, i.e. if $u=1$ then $w=1$ and hence $s\le r$ and $p\mid o\mid\frac{n}{s}$. Then $xs+\mathcal{S}\left((1+r)^{x\frac{nu}{s}}\mid s\right)\equiv s(x+1)\not\equiv 0 \mod pr$ because

$s \le r$ and $p \nmid x+1$. Therefore also in this case $v_p(r) \le v_p(xs + \mathcal{S}\left((1+r)^{x\frac{nu}{s}} \mid s\right))$ and hence $G' \subseteq \langle c_1 \rangle$ and $|c_1| = m$, as desired.

Since $(1+r)^{x\frac{nu}{s}} \equiv 1 \mod r\frac{nu}{s}$ we have $\mathcal{S}\left((1+r)^{x\frac{nu}{s}} \mid r\right) \equiv r \mod r\frac{nu}{s}$. Therefore $(1+r)^y - 1 - xru - \mathcal{S}\left((1+r)^{x\frac{nu}{s}} \mid r\right) \equiv 0 \mod \frac{rnu}{s}$. Moreover, $v_p(1-(1+r)^{x\frac{nu}{s}}) = v_p(r\frac{nu}{s})$, and hence there is an integer z satisfying

$$z(1-(1+r)^{x\frac{nu}{s}}) + (1+r)^y \equiv 1 + xru + \mathcal{S}\left((1+r)^{xu} \mid r\right) \mod m.$$

Let $d = b^y a^z \in b^y N$. Using that $u \ge w \ge \frac{s}{r}$ we have

$$c_1^d = (b^{x\frac{nu}{s}} a)^{b^y a^z} = b^{x\frac{nu}{s}} a^{z(1-(1+r)^{x\frac{nu}{s}})+(1+r)^y} = b^{x\frac{nu}{s}} a^{1+xru+\mathcal{S}\left((1+r)^{x\frac{nu}{s}}|r\right)} = c_1^{1+r},$$

On the other hand

$$d^n = (b^y a^z)^n = a^{sy+z\mathcal{S}((1+r)^y|n)}$$

and

$$c_1^s = (b^{x\frac{nu}{s}} a)^s = a^{xus+\mathcal{S}\left((1+r)^{x\frac{nu}{s}}|s\right)}.$$

if $s \ge n$ then $o > w = \max(\frac{so}{n}, \frac{s}{r}) \ge \frac{so}{n} \ge o$, a contradiction. Therefore, s is a proper divisor of n and hence $v_p(sy + z\mathcal{S}\left((1+r)^y \mid n\right)) = s$. Then d^n and c_1^s are elements of $\langle a \rangle$ of the same order. Therefore $b^n = c^{ks}$ for some integer k coprime with p. Then $c = c_1^k$ and d satisfy the conditions of (1).

Case 2. Suppose that $\epsilon = -1$.

(1) implies (2). Suppose that c and $d = b^y a^z$ satisfy the conditions of (1). Then $4 \mid r$ and $G' = \langle a^2 \rangle = \langle c^2 \rangle$. As in Case 1 we may assume that $w \ne 1$. Then both o and $\frac{m}{r}$ are multiple of 4 and we must prove, on the one hand that $y \equiv 1 \mod \frac{m}{2r}$ and, on the other hand that $y \equiv 1 \mod \frac{m}{r}$, if one of the following conditions hold: $o = n$ or, $s = m \ne nr$, or $2s = m = nr$. From $4 \mid o$ and $G/\langle c \rangle$ being cyclic we deduce $\langle c \rangle = \langle b^{xv} a \rangle$ with $o \mid v \mid n$ and $2 \nmid x$. From $G' = \langle a^2 \rangle = \langle c^2 \rangle$ it follows that $\frac{n}{2} \mid v$ so that v is either n or $\frac{n}{2}$. If $v = n$ then $\langle c \rangle = \langle a \rangle$. Therefore $a^{-1+r} = a^d = a^{(-1+r)^y}$ and hence $(-1+r)^{y-1} \equiv 1 \mod 2^m$. Then $y \equiv 1 \mod \frac{m}{r}$ by Lemma 2.1.(2b). This proves the result if $o = n$ because in that case v is necessarily n.

Suppose otherwise that $v = \frac{n}{2}$. Then we distinguish the cases $m < nr$ and $m = nr$.

Assume that $m < nr$. Then, as $4 \mid o \mid v$ we have $o_m(-1+r) = \max\left(2, \frac{m}{r}\right) \le \frac{n}{2} = v$ and hence b^v is central in G. Then, having in mind that $4 \mid r$ and $m \mid 2s$, we have

$$b^{xv} a^{(-1+r)^y} = (b^{xv} a)^{b^y a^z} = (b^{xv} a)^{-1+r} = b^{xv} a (b^{xv} a)^{r-2} = b^{xv} a^{r-1+xs(\frac{r}{2}-1)} = b^{xv} a^{-1+s+r}.$$

Therefore $(-1+r)^y \equiv -1+r+s \mod m$ and in particular $(-1+r)^y \equiv -1+r \mod s$, since $s \mid m$. Using Lemma 2.1 once more we deduce that $y \equiv 1 \mod \frac{m}{2r}$ and if $s = m$ then $y \equiv 1 \mod \frac{m}{r}$.

Suppose otherwise that $m = nr$. Then, from Lemma 2.1.(2a) we have $v_2((-1+r)^v - 1) = v_2(r) + v_2(v) = v_2(r) + v_2(n) - 1 = v_2(\frac{m}{2})$ so that $a^{b^v} = a^{1+\frac{m}{2}}$ and $(b^{xv} a)^2 = a^{2+s+\frac{m}{2}}$ and hence $(b^{xv} a)^4 = a^4$. As $4 \mid o$ it follows that $(b^{xv} a)^n = a^n$. On the other hand, as y is odd, it follows that $v_2((-1+r)^y + 1) = v_2(r) \ge 2$, by Lemma 2.1.(2c). Therefore, $v_2(\mathcal{S}\left((-1+r)^y \mid n\right)) = v_2(rn) - 1 = v_2(m) - 1$, by Lemma 2.1.(2a). Then $\mathcal{S}\left((-1+r)^y \mid n\right) \equiv \frac{m}{2} \mod m$ an hence, having in mind that $8 \mid \frac{m}{2} \mid s$ we deduce that $a^s = c^s = d^n = a^{ys+z\mathcal{S}((-1+r)^y|n)} = a^{s+z\frac{m}{2}}$. Therefore z is even. On the other hand from $c^d = c^{-1+r}$ and having in mind that $(-1+r)^v - 1 \equiv \frac{m}{2} \mod m$ and z is even, we obtain

$$b^{xv} a^{(-1+r)^y} = (b^{xv} a)^{b^y a^z} = (b^{xv} a)^{-1+r} = b^{xv} a (b^{xv} a)^{r-2} = b^{xv} a (a^{xs+2+\frac{m}{2}})^{\frac{r}{2}-1} = b^{xv} a^{-1+s+r+\frac{m}{2}}.$$

Therefore $(-1+r)^y \equiv -1+r+s+\frac{m}{2} \mod m$. Again, from $m \mid 2s$ and Lemma 2.1.(2b) we deduce that $y \equiv 1 \mod \frac{m}{2r}$ and if $s = \frac{m}{2}$ then $y \equiv 1 \mod \frac{m}{r}$.

(2) implies (1). Suppose that $y \equiv 1 \mod w$. As y is odd, if $o \mid 2$ then $b \in b^y N$ and hence a and b satisfy condition (1). So we assume from now on that $4 \mid o$. In particular $4 \mid n$. Suppose that $m \mid 2r$, i.e. r is either m or $\frac{m}{2}$ and let $c = a^y$ and $d = b^y a^2$. In this case b^2 is central in P and hence $c^d = c^b = c^{-1+r}$ and applying statements (2a) and (2c) of Lemma 2.1 we obtain $d^n = a^{ys+\mathcal{S}((-1+r)^y|n)} = a^{ys} = c^s$. Hence c and d satisfy the conditions of (1).

Thus from now on we assume that 4 divides both o and $\frac{m}{r}$. Suppose that $y \equiv 1 \mod \frac{m}{r}$. Then $a^{b^y} = a^b = a^{-1+r}$ because $b^{\frac{m}{r}}$ is central in P. Moreover, as $m \mid 2s$ and y is odd we have $(b^y)^n = a^{sy} = a^s$. Therefore $c = a$ and $d = b^y$ satisfy condition (1) and this finishes the proof of the lemma if $w = \frac{m}{r}$ and it also proves that for $w = \frac{m}{2r}$ we may assume that $y \not\equiv 1 \mod \frac{m}{r}$. So suppose that $w = \frac{m}{2r}$ and $y \not\equiv 1 \mod \frac{m}{r}$. Then

$y \equiv 1 + \frac{m}{2r} \mod \frac{m}{r}$, $o < n$ and either $m = s = nr$ or $2s = m < nr$. Let $c = b^{\frac{n}{2}}a$ and $d = b^y$. Then, in both cases, $c^2 = a^{2+\frac{m}{2}}$ and, as $\frac{m}{2}$ is multiple of 4 we have that $G' = \langle a^2 \rangle = \langle c^2 \rangle$, $|c| = m$ and $c^s = a^s$. Moreover,

$$c^{-1+r} = (b^{\frac{n}{2}}a)^{-1+r} = b^{\frac{n}{2}}a(b^{\frac{n}{2}}a)^{r-2} = b^{\frac{n}{2}}aa^{(2+\frac{m}{2})(\frac{r}{2}-1)} = b^{\frac{n}{2}}a^{-1+r+\frac{m}{2}} = b^{\frac{n}{2}}a^{(-1+r)(1+\frac{m}{2})} = (b^{\frac{n}{2}}a)^{b^{1+\frac{m}{2r}}} = c^d$$

and

$$d^n = a^{s(1+\frac{m}{2r})} = a^s = c^s.$$

Then c and d satisfy the conditions of (1). □

Theorem 3.6. *Let $m, n, s \in \mathbb{N}$ with $s \mid m$ and let T and $\bar{T}$ be (n, s)-canonical cyclic subgroups of $\mathcal{U}_m$. Set $[r, \epsilon, o] = [T]$, $[\bar{r}, \bar{\epsilon}, \bar{o}] = [\bar{T}]$, $\pi = \pi(r) \cup (\pi(n) \setminus \pi(m))$, $\bar{\pi} = \pi(\bar{r}) \cup (\pi(n) \setminus \pi(m))$, $m' = [T, n, s]$ and $\bar{m}' = [\bar{T}, n, s]$.*

Then the following statements are equivalent.

(1) $\mathcal{G}_{m,n,s,T}$ and $\mathcal{G}_{m,n,s,\bar{T}}$ are isomorphic.
(2) $\mathrm{Res}_{m'}(T) = \mathrm{Res}_{\bar{m}'}(\bar{T})$.
(3) $\pi = \bar{\pi}$, $\mathrm{Res}_{m_{\pi'}}(T_{\pi'}) = \mathrm{Res}_{m_{\pi'}}(\bar{T}_{\pi'})$ and $\mathrm{Res}_{m_{\pi'}m'_p}(T_p) = \mathrm{Res}_{m_{\pi'}m'_p}(\bar{T}_p)$ for every $p \in \pi$.

Proof. Let $G = \mathcal{G}_{m,n,s,T}$ and $\bar{G} = \mathcal{G}_{m,n,s,\bar{T}}$. To distinguish the generators a and b in the presentation of G and $\bar{G}$ we denote the latter by $\bar{a}$ and $\bar{b}$. We also denote $A = \langle a \rangle$, $B = \langle b \rangle$, $\bar{A} = \langle \bar{a} \rangle$ and $\bar{B} = \langle \bar{b} \rangle$. The hypothesis warrants that $G = AB$ and $\bar{G} = \bar{A}\bar{B}$ are minimal metacyclic factorizations by Proposition 3.4. In particular, $|A| = |\bar{A}| = m = m_G = m_{\bar{G}}$, $[G : A] = [\bar{G} : \bar{A}] = n = n_G = n_{\bar{G}}$, $[G : B] = [\bar{G} : \bar{B}] = s = s_G = s_{\bar{G}}$, $T = T_G(A)$ and $\bar{T} = T_{\bar{G}}(\bar{A})$.

(2) implies (3) Suppose that statement (2) holds. Then, using that $\pi(m) = \pi(m') = \pi(\bar{m}')$, we have $\mathrm{Res}_p(T) = \mathrm{Res}_p(\mathrm{Res}_{m'}(T)) = \mathrm{Res}_p(\mathrm{Res}_{m'}(\bar{T})) = \mathrm{Res}_p(\bar{T})$ for every prime p dividing m. Thus, $\pi' = \bar{\pi}'$ and, as $m_{\pi'} = m'_\pi$, we have $\mathrm{Res}_{m_{\pi'}}(T_{\pi'}) = \mathrm{Res}_{m'_{\pi'}}(T)_\pi = \mathrm{Res}_{m'_{\pi'}}(\bar{T})_\pi = \mathrm{Res}_{m_{\pi'}}(\bar{T}_{\pi'})$ and $\mathrm{Res}_{m_{\pi'}m'_p}(T_p) = \mathrm{Res}_{m'_{\pi'\cup\{p\}}}(T)_p = \mathrm{Res}_{m'_{\pi'\cup\{p\}}}(\bar{T})_p = \mathrm{Res}_{m_{\pi'}m'_p}(\bar{T}_p)$ for every $p \in \pi(m) \setminus \pi'$.

(1) implies (2). Suppose that $G \cong \bar{G}$. Then, as T and $\bar{T}$ are (n, s)-canonical they yield the same parameters, i.e. $\pi' = \bar{\pi}'$, $o = \bar{o}$, etc.

Let $f : \bar{G} \to G$ be an isomorphism and let $c = f(\bar{a})$, $d = f(\bar{b})$, $C = \langle c \rangle$ and $D = \langle d \rangle$. Then $C_{\pi'} = f(\bar{G}'_{\pi'}) = G'_{\pi'} = A_{\pi'}$, by Lemma 3.1.(3). Furthermore, $C_{\pi'}D_{\pi'} = A_{\pi'}B_{\pi'}$ because AB and $\bar{A}\bar{B}$ are the unique Hall π'-subgroup of G and $\bar{G}$, respectively. Then $\mathrm{Res}_{m_{\pi'}}(T) = T_G(A_{\pi'}) = T_G(C_{\pi'}) = \mathrm{Res}_{m_{\pi'}}(\bar{T})$. As $\mathrm{Res}_{m_\pi}(T_{\pi'}) = \mathrm{Res}_{m_\pi}(\bar{T}_{\pi'}) = 1$ it follows that $\mathrm{Res}_{m'}(T_{\pi'}) = \mathrm{Res}_{m'}(\bar{T}_{\pi'})$. Since T and $\bar{T}$ are cyclic, it remains to prove that $\mathrm{Res}_{m'}(T_p) = \mathrm{Res}_{m'}(\bar{T}_p)$ for every $p \in \pi$. Moreover, as G and $\bar{G}$ have the same parameters ϵ and r we have $\mathrm{Res}_{m_p}(T_p) = \mathrm{Res}_{m_p}(\bar{T}_p) = \langle \epsilon^{p-1} + r_p \rangle_{m_p}$. Denote $R = \epsilon^{p-1} + r_p$ and select generators t of $\mathrm{Res}_{m_{\pi'}m'_p}(T_p)$ and $\bar{t}$ of $\mathrm{Res}_{m_{\pi'}m'_p}(T_p)$ such that $\mathrm{Res}_{m_p}(t) = \mathrm{Res}_{m_p}(\bar{t})[R]_{m_p}$. We already know that $\mathrm{Res}_{m'_{\pi'}}(T) = \mathrm{Res}_{m'_{\pi'}}(\bar{T})$ and in particular, there is an integer x coprime with p such that $\bar{t} = t^x \mod m_{\pi'}$. If $o_p \le 2$ then $\mathrm{Res}_{m'_{\pi'}}(t) = \mathrm{Res}_{m'_{\pi'}}(\bar{t})$ and if $o_{m'_p}(R) \le 2$ then $\mathrm{Res}_{m'_p}(t^x) = [R^x]_{m'_p} = [R]_{m_p} = \mathrm{Res}_{m'_p}(\bar{t})$. In both cases $\mathrm{Res}_{m_{\pi'}m'_p}(T) = \langle t \rangle = \langle t^x \rangle = \mathrm{Res}_{m_{\pi'}m'_p}(\bar{T})$, as desired. Therefore, in the remainder we may assume that both o_p and $o_{m'_p}(R)$ are greater than 2 and, in particular, $o_{m'_p}(R) = \frac{m'_p}{r_p} = \mathrm{Res}_{m'_p}(T)$ and this number coincides with the w in Lemma 3.5.

On the other hand A_pB_p and $f(\bar{A}_p\bar{B}_p) = C_pD_p$ are Sylow p-subgroup of G and hence they are conjugate in G. Composing f with an inner automorphism of G we may assume that $C_pD_p = A_pB_p$. Then $\langle c, d^{o_p} \rangle = f(\langle \bar{a}, \bar{b}^{o_p} \rangle) = f(C_{\bar{G}_p}(\bar{G}'_{\pi'})) = C_{G_p}(G'_{\pi'}) = \langle a, b^{o_p} \rangle$. By Lemma 3.5 we have $d = b^y g$ for some $g \in C_{G_p}(G'_{\pi'})$ and $y \equiv 1 \mod w$. Thus $\mathrm{Res}_{m_{\pi'}}(\bar{t}) = \mathrm{Res}_{m_{\pi'}}(t^y)$ and $\mathrm{Res}_{m'_p}(\bar{t}) = \mathrm{Res}_{m'_p}(t) = \mathrm{Res}_{m'_p}(R) = \mathrm{Res}_{m'_p}(R^y) = \mathrm{Res}_{m'_p}(t^y)$, because $y \equiv 1 \mod o_{m'_p}(R)$. Thus $\mathrm{Res}_{m'_{\pi'}m'_p}(\bar{T}_p) = \mathrm{Res}_{m'_{\pi'}m'_p}(\bar{t}) = \mathrm{Res}_{m'_{\pi'}m'_p}(t^y) = \mathrm{Res}_{m'_{\pi'}m'_p}(T_p)$, as desired.

(3) implies (1) Suppose that the conditions of (3) holds. We may assume that $a = \bar{a}$ and take generators t of T and $\bar{t}$ of $\bar{T}$ so that $G = \langle a, b \rangle$, $\bar{G} = \langle a, \bar{b} \rangle$, with $|a| = m$, $[G : \langle a \rangle] = n$, $b^n = a^s$, $a^b = a^t$, $a^{\bar{b}} = a^{\bar{t}}$. Moreover, from the assumption we may assume $a^{b_{\pi'}} = a^{\bar{b}_{\pi'}}$ and for every $p \in \pi$ we have $\mathrm{Res}_{m_{\pi'}m'_p}(T_p) = \mathrm{Res}_{m_{\pi'}m'_p}(\bar{T}_p)$. In particular, for every $p \in \pi$, we have $\langle \epsilon^{p-1} + r_p \rangle_{m'_p} = \mathrm{Res}_{m'_p}(T_p) = \mathrm{Res}_{m'_p}(\bar{T}_p) = \langle \bar{\epsilon}^{p-1} + \bar{r}_p \rangle$. Since $r_p \mid m'_p \mid m_p$ it follows that $\epsilon = \bar{\epsilon}$ and $r_p = \bar{r}_p$. Thus $r = \bar{r}$.

We claim that for every $p \in \pi$ we can rewrite $G_p = \langle a_p, b_p\rangle$ as $G_p = \langle c_p, d_p\rangle$ with $c_p \in \left\langle a_p, b_p^{o_p}\right\rangle = C_{G_p}(a_{\pi'})$ and $d_p \in b^y C_{G_p}(a_{\pi'})$ such that $|c_p| = m_p$, $c_p^{d_p} = c_p^{R_p}$, $a_{\pi'}^{d_p} = a_{\pi'}^{\bar{b}_p}$ and $d_p^{n_p} = c_p^{s_p}$.

Indeed, let $p \in \pi$. The assumption $\left\langle \operatorname{Res}_{m_{\pi'} m'_p}(t_p)\right\rangle = \left\langle \operatorname{Res}_{m_{\pi'} m'_p}(\bar{t}_p)\right\rangle$ implies that there is an integer y coprime with $|\operatorname{Res}_{m_{\pi'} m'_p}(t_p)|$ such that $\operatorname{Res}_{m_{\pi'} m'_p}(\bar{t}_p) = \operatorname{Res}_{m_{\pi'} m'_p}(t_p)^y$. If $o_p \le 2$ or $o_{m_p}(R) \le 2$ then, as in the proof of (1) implies (2) we have that $\operatorname{Res}_{m_{\pi'} m_p}(t) = \operatorname{Res}_{m_{\pi'} m_p}(\bar{t})$ so that $c_p = a_p$ and $d_p = b_p$ satisfies the desired conditions. So assume that $o_p > 2$ and $o_{m_p}(R) > 2$. From the equality $a_p^{b_p} = a_p^{\bar{b}_p}$ we deduce that $R^y \equiv R \mod m'_p$ and this implies that $y \equiv 1 \mod w$ where $w = o_{m'_p}(R) = \frac{m'_p}{r_p}$ and again this w coincides with the one in Lemma 3.5. Applying Lemma 3.5 we deduce that $\langle a_p, b_p\rangle$ contain elements $c_p \in \left\langle a_p, b_p^o\right\rangle = C_{G_p}(a_{\pi'})$ and $d_p \in b^y C_{G_p}(a_{\pi'})$ such that $\langle a_p, b_p\rangle = \langle c_p, d_p\rangle$, $|c_p| = m_p$, $a_{\pi'}^{d_p} = a_{\pi'}^{b_p^y} = a_{\pi'}^{\bar{b}_p}$, $c_p^{d_p} = c_p^{R_p}$ and $d_p^{n_p} = c_p^{s_p}$, as desired. This finishes the proof of the claim.

For every $p \in \pi$ let c_p and d_p as in the claim and set $c = a_{\pi'} \prod_{p\in\pi} c_p$ and $d = b_{\pi'} \prod_{p\in\pi} d_p$ we deduce that $G = \langle c, d\rangle$ with $|c| = m$, $d^n = c^s$ and $c^d = a^{\bar{t}}$. Therefore $G \cong \bar{G}$. □

The following corollary is a direct consequence (1) implies (2) of Theorem 3.6. It shows that Δ_G is well defined.

Corollary 3.7. *If $G = AB = CD$ are two minimal factorizations of G then $\Delta(AB) = \Delta(CD)$.*

4. Proofs of the main results

Proof of Theorem A. Let G and $\bar{G}$ be finite metacyclic groups and let $G = AB$ and $\bar{G} = \bar{A}\bar{B}$ be minimal metacyclic factorizations of G and $\bar{G}$ respectively. Denote $m = |A|$, $\bar{m} = |\bar{A}|$, $n = [G : A]$, $\bar{n} = [\bar{G} : \bar{A}]$, $s = [G : B]$, $\bar{s} = [\bar{G} : \bar{B}]$, $T = T_G(A)$ and $\bar{T} = T_{\bar{G}}(\bar{A})$. We also denote $m' = [T, n, s]$, $\bar{m}' = [\bar{T}, \bar{n}, \bar{s}]$, $\Delta = \operatorname{Res}_{m'}(T)$ and $\bar{\Delta} = \operatorname{Res}_{\bar{m}'}(\bar{T})$. Then $G \cong \mathcal{G}_{m,n,s,T}$, $\bar{G} \cong \mathcal{G}_{\bar{m},\bar{n},\bar{s},\bar{T}}$, $m = m_G$, $n = n_G$, $s = s_G$, $\bar{n} = n_{\bar{G}}$, $\bar{m} = m_{\bar{G}}$, $s = s_{\bar{G}}$, T is (n,s)-canonical and $\bar{T}$ is $(\bar{n},\bar{s})$-canonical. Moreover, $\Delta = \Delta_G$ and $\bar{\Delta} = \Delta_{\bar{G}}$.

If $G \cong G'$ then $m = \bar{m}$, $n = \bar{n}$, $s = \bar{s}$ and, by Theorem 3.6 we have $\Delta = \bar{\Delta}$. Thus $\mathrm{MCINV}(G) = \mathrm{MCINV}(\bar{G})$.

Conversely, if $\mathrm{MCINV}(G) = \mathrm{MCINV}(\bar{G})$ then $m = |A| = m_G = m_{\bar{G}} = |\bar{A}| = \bar{m}$ and similarly $n = \bar{n}$ and $s = \bar{s}$. Moreover, $\operatorname{Res}_{m'}[T] = \Delta_G = \Delta_{\bar{G}} = \operatorname{Res}_{\bar{m}'}(\bar{T})$. Then $G \cong \bar{G}$ by Theorem 3.6. □

In the remainder of the section we use the notation in Theorem B.

Proof of (1) implies (2) in Theorem B. Suppose that $(m, n, s, \Delta) = \mathrm{MCINV}(G)$ for some metacyclic group G and let $G = AB$ be a minimal factorization of G. Then $m = m_G = |A|$, $n = n_G = [G : A]$, $s = s_G = [G : B]$ and if $T = T_G(A)$ then $\Delta = \Delta(AB) = \operatorname{Res}_{m'}(T)$. In particular, $s \mid m$, T is a cyclic subgroup of $\mathcal{U}_m^{n,s}$, $[T] = [\Delta]$ and $m'_\nu = m_\nu$. Moreover, $\nu = \pi(m') \setminus \pi(r)$ and $s_\nu = m_\nu$, by Lemma 3.1. Moreover, $|\Delta|$ divides n, because it divides $|T|$, which in turn divides n. Then conditions (2a) and (2b) of Theorem B hold. By Lemma 2.2, Lemma 3.1 and Lemma 3.2 we have $\pi = \pi_G$, $\pi'_G = \nu$, $o = o_G$, $\epsilon = \epsilon_G$ and $r = r_G$. Let $p \in \pi(r)$. If $\epsilon^{p-1} = 1$ then $\frac{m_p}{r_p} = |\operatorname{Res}_{m_p}(T_p)| \le n_p$ and if $\epsilon = -1$ then $\max(2, \frac{m_2}{r_2}) = |\operatorname{Res}_{m_2}(T_2)| \le |T_2| \le n_2$ and $m_2 \le 2s_2$. As the metacyclic factorization $G = AB$ is minimal, T is (n,s)-canonical by Proposition 3.4. Then the remaining conditions in (2c) and (2d) follow. □

Proofs of Theorem C and (2) implies (1) in Theorem B. Suppose that m, n, s and Δ satisfy the conditions of (2) in Theorem B. By Remark 1.2 there is a cyclic subgroup T of $\mathcal{U}_m^{n,s}$ with $\operatorname{Res}_{m'}(T) = \Delta$ and $[T] = [\Delta]$. Let $t \in \mathbb{N}$ with $T = \langle t\rangle_m$. Let $G = \mathcal{G}_{m,n,s,t}$ and denote $A = \langle a\rangle$ and $B = \langle b\rangle$. We will prove that $G = AB$ is a minimal factorization of G that $m = |A|$, $n = [G : A]$, $s = [G : B]$ and $\Delta = \Delta(AB)$. This will complete the proofs of Theorem B and Theorem C.

Of course $G = AB$ is a metacyclic factorization of G and $T = T_G(A)$. Since $m_\nu = s_\nu$, n is multiple of $|\Delta|$ and $|\operatorname{Res}_{m_\nu}(T)| = |\operatorname{Res}_{m_\nu}(\Delta)|$, it follows that $|\operatorname{Res}_{m_\nu}(T)|$ divides n and $s(t-1)$. On the other hand if $p \mid r$ then $t \equiv \epsilon^{p-1} + r_p \mod m_p$. Therefore, if $\epsilon^{p-1} = 1$ then $o_{m_p}(t) = \frac{m_p}{r_p} \mid n$ and $s(t-1) \equiv sr_p \equiv 0 \mod m_p$. Otherwise, i.e. if $\epsilon = -1$ and $p = 2$, then $2 \mid |\Delta| \mid n$ and $\frac{m_2}{r_2} \le n_2$ and $m_2 \mid 2s$. Thus $o_{m_2}(t) = o_{m_2}(-1 + r_2) = \max(2, \frac{m_2}{r_2}) \le n_2$ and $m_2 \mid t(s-1)$. This shows that m divides both $t^n - 1$ and $s(t-1)$, i.e. $T \subseteq \mathcal{U}_m^{n,s}$. Then $|A| = m$ and $[G : A] = n$, and hence $[G : B] = s$. From condition (2b) we have that $\Delta = \mathrm{Res}_{m'}(T_G(A)) = \Delta(AB)$ and from conditions (2d) and (2c) it follows that T is (n,s)-canonical. Then the metacyclic factorization $G = AB$ is minimal by Proposition 3.4. $\square$

Having in mind that a metacyclic group is nilpotent if and only if $o_G = 1$ one can easily obtain from Theorem B a description of the finite nilpotent metacyclic groups or equivalently the values of the lists of metacyclic invariants of the finite nilpotent metacyclic groups. Observe that (1) corresponds to cyclic groups, (2) to 2-generated abelian groups, (3) to non-abelian nilpotent metacyclic groups G with $\epsilon_G = 1$ and (4) to metacyclic nilpotent groups with $\epsilon_G = -1$.

Corollary 4.1. *Let $m, n, s \in \mathbb{N}$ and $t \in \mathbb{N} \cup \{0\}$. Then (m, n, s, t) is the list of metacyclic invariants of a finite metacyclic nilpotent group if and only if $s \mid m$, $t < m$ and one of the following conditions hold:*

(1) $m = 1$.
(2) $t = 1$ *and* $s = m \le n$.
(3) $\pi(t-1) = \pi(m)$, $\mathrm{lcm}\left(t-1, \frac{m}{t-1}\right) \mid s \mid n$ *and if* $4 \mid m$ *then* $4 \mid t-1$.
(4) There is a divisor r of $s_{2'}m_2$ such that $\pi(r) = \pi(m)$, $4 \mid r$, $t \equiv 1 + r_{2'} \mod m_{2'}$, $t \equiv -1 + r_2 \mod m_2$, $\frac{m_{2'}}{r_{2'}} \mid s_{2'} \mid n_{2'}$, $\max\left(2, \frac{m_2}{r_2}\right) \le n_2$, $m_2 \le 2s_2$ and $s_2 \ne n_2 r_2$. If moreover $4 \mid n$ and $8 \mid m$ then $r_2 \le s_2$.

In that case $\mathcal{G}_{m,n,s,t}$ is nilpotent with metacyclic invariants (m, n, s, t).

5. A GAP implementation

In this section we show how we can use the result in previous sections to construct some GAP functions for calculations with finite metacyclic groups. The code of these function is available in
`https://www.um.es/adelrio/MetaCyc.php`

We start with two auxiliar functions. We call *metacyclic parameters* to any list (m, n, s, t) with $m, n, s \in \mathbb{N}$ and $[t]_m \in \mathcal{U}_m^{n,s}$, i.e. $s(t-1) \equiv t^n - 1 \mod m$. In that case `MetacyclicGroupPC([m,n,s,t])` outputs the group $\mathcal{G}_{m,n,s,t}$ with a power-conjugation presentation. The boolean function `IsMetacyclic` returns `true` if the input is a finite metacyclic and `false` otherwise.

```
gap> G:=MetacyclicGroupPC([10,20,5,3]);
<pc group of size 200 with 5 generators>
gap> IsMetacyclic(G);
true
gap> Filtered([1..16],x->IsMetacyclic(SmallGroup(100,x)));
[ 1, 2, 3, 4, 5, 6, 8, 9, 14, 16 ]
```

To introduce the next function we start presenting an algorithm that uses Algorithm 1 to compute $\mathrm{MCINV}(G)$ for a given metacyclic group G. Observe that in Algorithm 1 the values of $m = |a|$, $n = [G : \langle a \rangle]$, $s = [G : \langle a \rangle]$ and $(r, \epsilon, o) = [T_G(\langle a \rangle)]$ are updated along the calculations. We use this in step (2) of the following algorithm.

Algorithm 2. Input*: A finite metacyclic group G.*
Output*:* $\mathrm{MCINV}(G)$.

(1) Compute a metacyclic factorization $G = AB$ of G.
(2) Perform Algorithm 1 with input (A, B) saving not only the output $(\langle a \rangle, \langle b \rangle)$ but also m, n, s, r, ϵ and o computed along.
(3) Compute m' using (1.1) and $t \in \mathbb{N}$ such that $a^b = a^t$.
(4) Return $(m, n, s, \mathrm{Res}_{m'}(\langle t \rangle_m))$.

A slight modification of Algorithm 2 allows the computation of the list of metacyclic invariants of a finite metacyclic group:

Algorithm 3. Input*: A finite metacyclic group G.*
Output*: The list of metacyclic invariants of G.*

(1) Compute a metacyclic factorization $G = AB$ of G.
(2) Perform Algorithm 1 with input (A, B) saving not only the output $(\langle a \rangle, \langle b \rangle)$ but also m, n, s, r and ϵ computed along.

(3) *Compute* m' *using* (1.1) *and* $t \in \mathbb{N}$ *such that* $a^b = a^t$ *and set* $\Delta := \mathrm{Res}_{m'}(\langle t \rangle_m)$.
(4) *Use the Chinese Remainder Theorem to compute the unique* $1 \le t \le m_{\pi(r)}$ *such that* $t \equiv \epsilon^{p-1} + r_p \mod m_p$ *for every* $p \in \pi(r)$.
(5) *While* $\gcd(t, m') \neq 1$ *or* $\langle t \rangle_{m'} \neq \Delta$, $t := t + m_{\pi(r)}$.
(6) *Return* (m, n, s, t).

Observe that $G = \langle a \rangle \langle b \rangle$ is a minimal metacyclic factorization at step (2) of Algorithm 3, and $m = m_G$, $n = n_G$ and $s = s_G$. At step (3), we have $T_G(\langle a \rangle) = \langle t \rangle_m$ and hence $G \cong \mathcal{G}_{m,n,s,t}$ and $\Delta = \Delta_G = \mathrm{Res}_{m'}(\langle t \rangle_m)$. However, this t is not t_G yet. The t at step Item 4 is the smallest one with $t \equiv \epsilon^{p-1} + r_p \mod m_p$ for every $p \in \pi(r)$ and the next steps search for the first integer t satisfying this condition as well as representing an element of $\mathcal{U}_m$ with $\mathrm{Res}_{m'}(\langle t \rangle_m) = \Delta$.

The GAP function `MetacyclicInvariants` implements Algorithm 3. For example in the following calculations one computes the metacyclic invariants of all the metacyclic groups of order 200.

```
gap> mc200:=Filtered([1..52],i->IsMetacyclic(SmallGroup(200,i)));;
gap> List(mc200,i->MetacyclicInvariants(SmallGroup(200,i)));
[[25,8,25,24],[1,200,1,0],[25,8,25,7],[100,2,50,99],[100,2,50,49],[100,2,100,99],
[50,4,50,49],[2,100,2,1],[4,50,4,3],[4,50,2,3],[50,4,50,7],[5,40,5,4],[5,40,5,1],
[5,40,5,2],[20,10,10,19],[20,10,10,9],[20,10,20,19],[10,20,10,9],[10,20,10,1],
[20,10,20,11],[20,10,10,11],[10,20,10,3]]
```

The GAP functions `MCINV` and `MCINVData` implement Algorithm 2 representing $\mathrm{MCINV}(G)$ in two different ways. While `MCINV(G)` outputs $\mathrm{MCINV}(G)$ if G is a metacyclic group, `MCINVData(G)` ouputs a 5-tuple `[m,n,s,m',t]` such that $\mathrm{MCINV}(G) = (m, n, s, \langle t \rangle_{m'})$. The input data `G` can be replaced by metacyclic parameters $[m, n, s, t]$ representing the group $\mathcal{G}_{m,n,s,t}$:

```
gap> G:=SmallGroup(384,533);
<pc group of size 384 with 8 generators>
gap> MetacyclicInvariants(G);
[ 8, 48, 4, 5 ]
gap> x:=MCINV(G);
[ 8, 48, 4, <group of size 1 with 1 generator> ]
gap> y:=MCINVData(G);
[ 8, 48, 4, 4, 1 ]
gap> x[4]=Group(ZmodnZObj(y[5],y[4]));
true
gap> H:=MetacyclicGroupPC([8,48,4,5]);
<pc group of size 384 with 8 generators>
gap> IdSmallGroup(H);
[ 384, 533 ]
gap> MetacyclicInvariants([20,4,8,11]);
[ 4, 20, 4, 3 ]
gap> MCINVData([20,4,8,11]);
[ 4, 20, 4, 4, 3 ]
```

Observe that two finite metacyclic groups G and H are isomorphic if and only if $\mathrm{MCINV}(G) = \mathrm{MCINV}(G)$ if and only if they have the same metacyclic invariants. The function `AreIsomorphicMetacyclicGroups` uses this to decide if two metacyclic groups G and H are isomorphic. It outputs `true` if G and H are isomorphic finite metacyclic groups and `false` if they are finite metacyclic groups but they are not isomorphic. In case one of the inputs is not a finite metacyclic group then it fails. The input data `G` and `H` can be replaced by metacyclic parameters of them.

```
gap> H:=MetacyclicGroupPC([100,30,10,31]);
<pc group of size 3000 with 7 generators>
gap> K:=MetacyclicGroupPC([300,30,10,181]);
<pc group of size 9000 with 8 generators>
gap> AreIsomorphicMetacyclicGroups(H,K);
false
gap> AreIsomorphicMetacyclicGroups([300,10,10,31],K);
```

```
false
gap> G:=MetacyclicGroupPC([300,10,10,31]);
<pc group of size 3000 with 7 generators>
gap> MetacyclicInvariants(G);
[ 100, 30, 10, 31 ]
gap> MetacyclicInvariants(H);
[ 100, 30, 10, 31 ]
gap> MetacyclicInvariants(K);
[ 50, 180, 10, 31 ]
```

We now explain a method to compute all the metacyclic group of a given order N. We start producing all the tuples (m,n,s,r,ϵ,o) such that $\mathrm{MCINV}(G)=(m,n,s,\Delta)$ and $[\Delta]=(r,\epsilon,o)$ for some finite metacyclic group G and some cyclic subgroup Δ of $\mathcal{U}_{m'}$ with m' as in (1.1). For such group G we denote $\mathrm{IN}(G)=(m,n,s,r,\epsilon,o)$. The following lemma characterizes when a given tuple (m,n,r,s,r,ϵ,o) equals $\mathrm{IN}(G)$ for some finite metacyclic group:

Lemma 5.1. *Let $m,n,s,r,o\in\mathbb{N}$ and $\epsilon\in\{1,-1\}$ and let $\pi'=\pi(m)\setminus\pi(r)$ and $\pi=\pi(mn)\setminus\pi'$. Then $\mathrm{IN}(G)=(m,n,s,r,\epsilon,o)$ for some finite metacyclic group G if and only if the following conditions hold:*

(A) $s\mid m$, $r\mid m$, $o\mid n_\pi$, $m_\pi\mid rn$, $m_\pi\mid rs$, $s_{\pi'}=m_{\pi'}$ and if $4\mid m$ then $4\mid r$.
(B) If $p\in\pi(r)$ and $\epsilon^{p-1}=1$ then $s_p\mid n$ and either $r_p\mid s$ or $s_po_p\nmid n$.
(C) If $\epsilon=-1$ then $2\mid n$, $4\mid m$, $m_2\mid 2s$, $s_2\neq n_2r_2$. If moreover $4\mid n$, $8\mid m$ and $o_2<n_2$ then $r_2\mid s$.
(D) $o\mid \mathrm{lcm}\{q-1:q\in\pi'\}$ and for every $q\in\pi'$ with $\gcd(o,q-1)=1$ there is $p\in\pi'\cap\pi(n)$ with $p\mid q-1$.

Proof. Suppose first that $(m,n,s,r,\epsilon,o)=\mathrm{IN}(G)$ for some finite metacyclic group G. Then $\mathrm{MCINV}(G)=(m,n,s,\Delta)$ for some cyclic subgroup Δ of $\mathcal{U}_{m'}$ with $[\Delta]=(r,\epsilon,o)$. Then the conditions in statement (2) of Theorem B hold and this implies that conditions (A)–(C) hold. To prove (D) we fix a metacyclic factorization $G=AB$ and observe that $o=o_G(A)=|\mathrm{Res}_{m_{\pi'}}(T_G(A))_\pi|$ and $\mathrm{Res}_{m_{\pi'}}(T_G(A))_\pi$ is a cyclic subgroup of $(\mathcal{U}_{m_{\pi'}})_\pi$. Then o divides the exponent of $(\mathcal{U}_{m_{\pi'}})_\pi$ which is $\mathrm{lcm}\{(q-1)_\pi:q\in\pi'\}$. This proves the first part of (D). To prove the second one we take $q\in\pi'$ such that $\gcd(o,q-1)=1$. By Lemma 3.1.(4), we have $\mathrm{Res}_q(T_G(A))\neq 1$. However $\mathrm{Res}_q(T_G(A))_\pi\mid\gcd(o,q-1)=1$ and hence, if p is a divisor of $\mathrm{Res}_q(T_G(A))$ then $p\mid |U_q|=q-1$, $p\mid[G:A]=n$ and $p\notin\pi$, so that $p\in\pi'$. This finishes the proof of (D).

Conversely, suppose that conditions (A)-(D) hold. By condition (D), $2\notin\pi'$ and hence if $q\in\pi'$ then $\mathcal{U}_{m_q}$ is cyclic of order $\varphi(m_q)$. Therefore for every $q\in\pi'$, the group $\mathcal{U}_q$ contains a cyclic subgroup of order $q-1$. Therefore $\mathcal{U}_m$ contains a cyclic subgroup of order $k=\mathrm{lcm}\{q-1:q\in\pi'\}$. Furthermore, by (D), for every $p\in\pi$ we have that $o_p\mid k$ and hence $o_p\mid q-1$ for some $q\in\pi'$. Then $\mathcal{U}_{m_q}$ contains an element of order o_p and, as $\mathcal{U}_{m_{\pi'}}\cong\prod_{q\in\pi'}\mathcal{U}_{m_q}$, it follows that $\mathcal{U}_{m_{\pi'}}$ contains an element of order o. Let $\tau=\{q\in\pi':\gcd(o,q-1)=1\}$. By (D), for every $q\in\tau$ there is $p_q\in\pi'\cap\pi(n)$ such that $p_q\mid q-1$. Let $h=\prod_{q\in\tau}p_q$. For every $q\in\tau$, there is an element in $\mathcal{U}_{m_q}$ of order p_q. Then $\mathcal{U}_{m_\tau}$ has an element of order h. As $o\mid n_\pi$ and $h\mid n_{\pi'}$, $\mathcal{U}_{m_{\pi'}}$ has a cyclic subgroup S of order oh. Then $\mathrm{Aut}(C_m)$ has a cyclic subgroup T such that $\mathrm{Res}_{m_{\pi'}}(T)=S$ and $\mathrm{Res}_{m_p}(T)=\mathrm{Res}_{m_p}(T)=\left\langle\epsilon^{p-1}+r_p\right\rangle_{m_p}$ for every $p\in\pi$. By condition (B), if $p\in\pi(r)$ and $\epsilon^{p-1}=1$ then $|\mathrm{Res}_{m_p}(T)|=\frac{m_p}{r_p}\mid n_p$. By condition (C), if $\epsilon=-1$ then $2\in\pi$, $2\mid n$ and $\frac{m_2}{r_2}\mid n$ by (A). Thus $|\mathrm{Res}_{m_p}(T)|=\max(2,\frac{m_2}{r_2})\mid n$. Then $|\mathrm{Res}_{m_p}(T)|$ divides n for every $p\in\pi$. This implies that $|T|=\mathrm{lcm}(|S|,|\mathrm{Res}_{m_p}(T)|,p\in\pi)$ and this number divides n. On the one hand we have $s_{p'}=m_{\pi'}$ and if $p\in\pi$ then either $m_p\mid rs$ or $p=2$, $\epsilon=-1$ and $2m_2\mid s$. Using this it is easy to see that $\mathrm{Res}_{\frac{m}{s}}(T)=1$. This proves that $T\subseteq\mathcal{U}_m^{n,s}$ and by the election of T it follows that $[T]=(r,\epsilon,o)$. Moreover, from conditions (B) and (C), it follows that T is (n,s)-canonical and hence $\mathcal{G}_{m,n,s,T}=\langle a\rangle\langle b\rangle$ is a minimal factorization. Thus $\mathrm{IN}(\mathcal{G}_{m,n,s,T})=(m,n,s,r,\epsilon,o)$, as desired. □

Our last algorithm is based in Lemma 5.1 and compute a list containing exactly one representative of each isomorphism class of the metacyclic groups of a given order.

Algorithm 4. Input*: A positive integer N.*

Output*: A list containing exactly one representative of each isomorphism class of the metacyclic groups of order N.*

(1) $M:=[\,]$, an empty list, $\pi':=\pi(m)\setminus\pi(r)$, $\pi':=\pi(N)\setminus\pi'$.
(2) $P:=\{(m,n,s,r,\epsilon,o):n,m,s,r,o\in\mathbb{N},\epsilon\in\{1,-1\},N=mn$ and conditions (A)-(D) hold$\}$.

(3) *For each* $(m, n, s, r, \epsilon, o) \in P$*:*
  (a) $m' := m_{\pi'} \prod_{p \in \pi(r)} m'_p$ *with* m'_p *as in* (1.1) *and* $s' := \frac{sm'}{m}$.
  (b) *For every cyclic subgroup* Δ *of* $\mathcal{U}_{m'}^{n,s'}$ *with* $[\Delta] = (r, \epsilon, o)$*:*
    - *Select a cyclic subgroup* T *of* $\mathcal{U}_m$ *such that* $\mathrm{Res}_{m'}(T) = \Delta$.
    - *Add* $\mathcal{G}_{m,n,s,T}$ *to the list* M.

(4) *Return the list* M.

Observe that if $(m, n, s, r, \epsilon, o)$ satisfy conditions (A)-(D) then m divides sm'. Indeed, if $p \nmid r$ then $m_p = m'_p$. If $\epsilon = -1$ then $\frac{m_2}{2}$ divides s and $2 \mid m'$, hence in this case $\frac{m_2}{s_2} \mid m'$. Finally, if $p \in \pi(r)$ and $\epsilon^{p-1} = 1$. Then $p \in \pi$ and hence $m_p \le r_p s_p$ by condition (A). Therefore $\frac{m_p}{s_p} \le \min(m_p, r_p o_p)$. If $r_p \mid s_p$ then also $\frac{m_p}{s_p} \le s_p$. Otherwise $s_p o_p \nmid n$ and hence $r_p \frac{s_p o_p}{n_p} > r_p \ge \frac{m_p}{s_p}$. This proves that $\frac{m_p}{s_p} \mid m'$ for every prime p, so that $m \mid sm'$, as desired. This justify that $s' \in \mathbb{N}$ is step (3a).

On the other hand if T is as in (3b) then $T \subseteq \mathcal{U}_m^{n,s}$. Indeed, $\frac{m}{s} = \frac{m'}{s'}$ and hence $\mathrm{Res}_{\frac{m}{s}}(T) = \mathrm{Res}_{\frac{m'}{s'}}(\Delta) = 1$. Moreover $\mathrm{Res}_{m_{\pi'}}(T) = \mathrm{Res}_{m'_{\pi'}}(\Delta)$ and hence $|\mathrm{Res}_{m_{\pi'}}(T)|$ divides n. On the other hand $[T] = (r, \epsilon, o) = [T]$ and hence if $\epsilon^{p-1} = 1$ then $|\mathrm{Res}_{m_p}(T)| = \frac{m_p}{r_p} \mid n$, by (A). Otherwise $|\mathrm{Res}_{m_2} T_2| = \max(2, \frac{m_2}{r_2})$ which divides n by (A) and (C).

The function `MetacyclicGroupsByOrder(N)` implements a combination of Algorithm 3 and Algorithm 4 and returns the complete list of metacyclic invariants of metacyclic groups of order N.

```
gap> MetacyclicGroupsByOrder(200);
[[1,200,1,0],[2,100,2,1],[4,50,2,3],[4,50,4,3],[5,40,5,1],[5,40,5,2],[5,40,5,4],
[10,20,10,1],[10,20,10,3],[10,20,10,9],[20,10,10,9],[20,10,10,11],[20,10,10,19],
[20,10,20,11],[20,10,20,19],[25,8,25,7],[25,8,25,24],[50,4,50,7],[50,4,50,49],
[100,2,50,49],[100,2,50,99],[100,2,100,99]]
gap> MetacyclicGroupsByOrder(8*3*5*7);
[[1,840,1,0],[2,420,2,1],[3,280,3,2],[4,210,2,3],[4,210,4,3],[5,168,5,2],[5,168,5,4],
[6,140,6,5],[7,120,7,2],[7,120,7,6],[7,120,7,3],[10,84,10,3],[10,84,10,9],[12,70,6,5],
[12,70,6,11],[12,70,12,11],[14,60,14,3],[14,60,14,9],[14,60,14,13],[15,56,15,2],
[15,56,15,14],[20,42,10,9],[20,42,10,19],[20,42,20,19],[21,40,21,20],[28,30,14,3],
[28,30,14,5],[28,30,14,11],[28,30,14,13],[28,30,14,27],[28,30,28,3],[28,30,28,11],
[28,30,28,27],[30,28,30,17],[30,28,30,29],[35,24,35,2],[35,24,35,3],[35,24,35,4],
[35,24,35,13],[35,24,35,19],[35,24,35,34],[42,20,42,41],[60,14,30,29],[60,14,30,59],
[60,14,60,59],[70,12,70,3],[70,12,70,9],[70,12,70,13],[70,12,70,19],[70,12,70,23],
[70,12,70,69],[84,10,42,41],[84,10,42,83],[84,10,84,83],[105,8,105,62],[105,8,105,104],
[140,6,70,9],[140,6,70,19],[140,6,70,39],[140,6,70,69],[140,6,70,89],[140,6,70,139],
[140,6,140,19],[140,6,140,39],[140,6,140,139],[210,4,210,83],[210,4,210,209],
[420,2,210,209],[420,2,210,419],[420,2,420,419]]
```

References

[Bey72] F. R. Beyl, *The classification of metacyclic p-groups, and other applictations to homological algebra to group theory*, ProQuest LLC, Ann Arbor, MI, 1972, Thesis (Ph.D.)–Cornell University. MR 2622614

[GAP12] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.5.6*, 2012.

[Hal59] M. Hall, Jr., *The theory of groups*, The Macmillan Company, New York, N.Y., 1959. MR 0103215

[Hem00] C. E. Hempel, *Metacyclic groups*, Communications in Algebra **28** (2000), no. 8, 3865–3897.

[Kin73] B. W. King, *Presentations of metacyclic groups*, Bull. Austral. Math. Soc. **8** (1973), 103–131. MR 323893

[Lie94] S. Liedahl, *Presentations of metacyclic p-groups with applications to K-admissibility questions*, J. Algebra **169** (1994), no. 3, 965–983. MR 1302129

[Lie96] ———, *Enumeration of metacyclic p-groups*, J. Algebra **186** (1996), no. 2, 436–446. MR 1423270

[Lin71] W. Lindenberg, *Struktur und Klassifizierung bizyklischer p-Gruppen*, Gesellschaft für Mathematik und Datenverarbeitung, Bonn, 1971, BMBW-GMD-40. MR 0285609

[NX88] M. F. Newman and M. Xu, *Metacyclic groups of prime-power order*, Adv. in Math. (Beijing) **17** (1988), 106–107. MR 0404441

[Réd89] L. Rédei, *Endliche p-Gruppen*, Akadémiai Kiadó, Budapest, 1989. MR 992619

[Sim94] Hyo-Seob Sim, *Metacyclic groups of odd order*, Proc. London Math. Soc. (3) **69** (1994), no. 1, 47–71. MR 1272420

[Zas99] H. J. Zassenhaus, *The theory of groups*, Dover Publications, Inc., Mineola, NY, 1999, Reprint of the second (1958) edition. MR 1644892